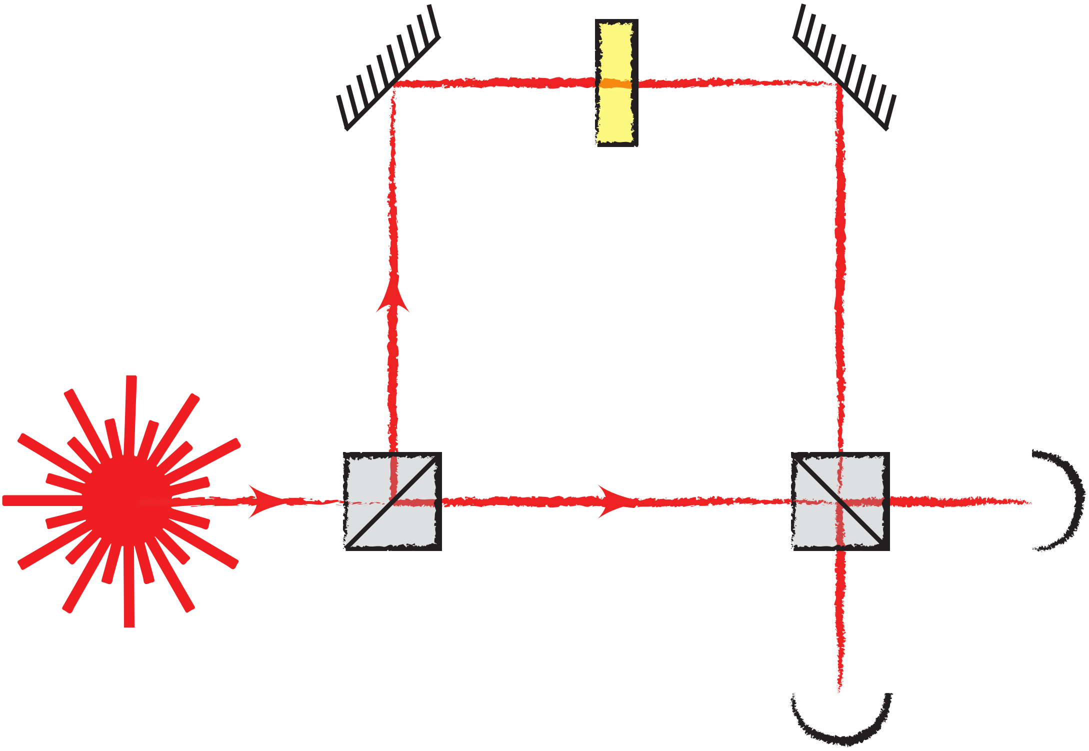
Linköping Studies in Science and Technology
Dissertation No. 1875

Breaking the Unbreakable:

Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography

Jonathan Jogenfors



LINKÖPING
UNIVERSITY

Linköping Studies in Science and Technology
Dissertations, No. 1875

Breaking the Unbreakable
Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography

Jonathan Jogenfors

Akademisk avhandling

som för avläggande av doktorsexamen vid Linköpings Universitet kommer att offentligt försvaras i sal Ada Lovelace, hus B, universitetsområde Valla, fredagen den 17 november 2017 kl. 13:00. Fakultetsopponent är Professor Marek Żukowski, Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański.

Abstract

In this thesis we study device-independent quantum key distribution based on energy-time entanglement. This is a method for cryptography that promises not only perfect secrecy, but also to be a practical method for quantum key distribution thanks to the reduced complexity when compared to other quantum key distribution protocols. However, there still exist a number of loopholes that must be understood and eliminated in order to rule out eavesdroppers. We study several relevant loopholes and show how they can be used to break the security of energy-time entangled systems. Attack strategies are reviewed as well as their countermeasures, and we show how full security can be re-established.

Quantum key distribution is in part based on the profound no-cloning theorem, which prevents physical states to be copied at a microscopic level. This important property of quantum mechanics can be seen as Nature's own copy-protection, and can also be used to create a currency based on quantum mechanics, i.e., quantum money. Here, the traditional copy-protection mechanisms of traditional coins and banknotes can be abandoned in favor of the laws of quantum physics. Previously, quantum money assumes a traditional hierarchy where a central, trusted bank controls the economy. We show how quantum money together with a blockchain allows for Quantum Bitcoin, a novel hybrid currency that promises fast transactions, extensive scalability, and full anonymity.

URL: `http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-140912`

ISBN 978-91-7685-460-0 ISSN 0345-7524

Linköping Studies in Science and Technology
Dissertations, No. 1875

Breaking the Unbreakable

Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography

Jonathan Jogenfors

LINKÖPING UNIVERSITY

Information Coding Group
Department of Electrical Engineering
Linköping University
SE-581 83 Linköping, Sweden

Linköping 2017

Breaking the Unbreakable: Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography

Jonathan Jogenfors

Author e-mail: jonathan.jogenfors@liu.se

Cover image

Layout of the Franson interferometer, a scheme used for testing the Bell inequality using energy-time entanglement.

Edition 1:1

Copyright © 2017 Jonathan Jogenfors unless otherwise stated.

All product names, logos, and brands are property of their respective owners.

ISBN 978-91-7685-460-0
ISSN 0345-7524
URL http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-140912

Typeset using LuaLaTeX

Printed by LiU-Tryck, Linköping, Sweden 2017

To Anna

Abstract

In this thesis we study device-independent quantum key distribution based on energy-time entanglement. This is a method for cryptography that promises not only perfect secrecy, but also to be a practical method for quantum key distribution thanks to the reduced complexity when compared to other quantum key distribution protocols. However, there still exist a number of loopholes that must be understood and eliminated in order to rule out eavesdroppers. We study several relevant loopholes and show how they can be used to break the security of energy-time entangled systems. Attack strategies are reviewed as well as their countermeasures, and we show how full security can be re-established.

Quantum key distribution is in part based on the profound no-cloning theorem, which prevents physical states to be copied at a microscopic level. This important property of quantum mechanics can be seen as Nature's own copy-protection, and can also be used to create a currency based on quantum mechanics, i.e., quantum money. Here, the traditional copy-protection mechanisms of traditional coins and banknotes can be abandoned in favor of the laws of quantum physics. Previously, quantum money assumes a traditional hierarchy where a central, trusted bank controls the economy. We show how quantum money together with a blockchain allows for Quantum Bitcoin, a novel hybrid currency that promises fast transactions, extensive scalability, and full anonymity.

Populärvetenskaplig sammanfattning

En viktig konsekvens av kvantmekaniken är att okända kvanttillstånd inte kan klonas. Denna insikt har gett upphov till kvantkryptering, en metod för två parter att med perfekt säkerhet kommunicera hemligheter. Ett komplett bevis för denna säkerhet har dock låtit vänta på sig eftersom en attackerare i hemlighet kan manipulera utrustningen så att den läcker information. Som ett svar på detta utvecklades apparatsoberoende kvantkryptering som i teorin är immun mot sådana attacker.

Apparatsoberoende kvantkryptering har en mycket högre grad av säkerhet än vanlig kvantkryptering, men det finns fortfarande ett par luckor som en attackerare kan utnyttja. Dessa kryphål har tidigare inte tagits på allvar, men denna avhandling visar hur även små svagheter i säkerhetsmodellen läcker information till en attackerare. Vi demonstrerar en praktisk attack där attackeraren aldrig upptäcks trots att denne helt kontrollerar systemet. Vi visar också hur kryphålen kan förhindras med starkare säkerhetsbevis.

En annan tillämpning av kvantmekanikens förbud mot kloning är pengar som använder detta naturens egna kopieringsskydd. Dessa kvantpengar har helt andra egenskaper än vanliga mynt, sedlar eller digitala banköverföringar. Vi visar hur man kan kombinera kvantpengar med en blockkedja, och man får då man en slags "kvant-Bitcoin". Detta nya betalningsmedel har fördelar över alla andra betalsystem, men nackdelen är att det krävs en kvantdator.

Acknowledgments

I would like to express gratitude to my advisor, Jan-Åke Larsson, for his support, patience and encouragement throughout my graduate studies. His guidance has helped me tremendously, and thanks to him I was able to overcome the many hurdles I encountered in the process of performing this research.

My thanks also go to my co-supervisor, Associate Professor Fredrik Karlsson for his guidance.

I could not have done this without my awesome wife Anna. Writing this thesis has required long days and late nights, and she has supported me all this time. Thank you, Anna, for your love and understanding. I am so fortunate to have you by my side.

My colleagues at the Information Coding Group and the Department of Electrical Engineering made me feel welcome from the first day. Special thanks to Niklas Johansson and Vahid Keshmiri, who have endured sharing an office with me all these years.

I am indebted to all those who have supported me, including Monica, Jan-Erik, and Andreas.

Last but not least I would thank my parents, Eva and Stefan, and my sisters, Susanna and Elisabeth, for their continued support and love.

Jonathan
Jönköping, October 2017

Contents

Abstract vii

Acknowledgments xi

Contents xiii

List of Figures xvii

List of Tables xxi

List of Theorems xxiii

List of Acronyms xxvii

List of Symbols xxxi

Preface xxxix

1 Introduction 1

1.1 History of Cryptography 1
1.2 Fundamental Principles of Cryptography 3
1.3 Public-Key Cryptography 6
1.4 Cryptography and the Quantum World 8
1.5 Outline 11
1.6 Included Publications 13

2 Basic Concepts 19

2.1 Linear Algebra 19

2.2 Probability Theory 20
2.3 Fundamental Quantum Mechanics 21

3 Quantum Key Distribution 29
3.1 The BB84 Protocol 31
3.2 Security Analysis of BB84 34

4 Bell's Theorem 37
4.1 EPR and Hidden Variables 37
4.2 Intuitive Explanation 41
4.3 The Black Box Model 44
4.4 Ekert's QKD Protocol 49
4.5 Device-Independent QKD 51

5 Loopholes in Bell Experiments 57
5.1 The Detection Loophole 59
5.2 The Coincidence-Time Loophole 63
5.3 Experimental Bell testing 67
5.4 Conclusions 70

6 Energy-Time Entanglement 71
6.1 The Franson Interferometer 72
6.2 The Postselection Loophole 76

7 Quantum Hacking 81
7.1 The LHV Attack 82
7.2 The Blinding Attack 84
7.3 Optical Considerations 86
7.4 Experimental Demonstration 91

8 Countermeasures to Quantum Hacking 95
8.1 Chaining the Bell Inequality 98
8.2 Interferometric Visibility 105
8.3 Modified Franson Setups 110
8.4 Conclusions 115

9 Quantum Bitcoin 117

9.1 Hashcash 118
9.2 Bitcoin 121
9.3 Further Blockchain Developments 124
9.4 Quantum Money 125

10 Conclusions **131**
10.1 Future Work 134

Index **137**

Bibliography **143**

Publications **171**

A Energy-Time Entanglement, Elements of Reality, and Local Realism **171**

B Hacking the Bell Test Using Classical Light in Energy-Time Entanglement–Based Quantum Key Distribution **189**

C Tight Bounds for the Pearle-Braunstein-Caves Chained Inequality Without the Fair-Coincidence Assumption **199**

D High-Visibility Time-Bin Entanglement for Testing Chained Bell Inequalities **207**

E Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics **217**

F Comment on “Franson Interference Generated by a Two-Level System” **237**

List of Figures

1.1 Basic communication scheme for cryptography, adapted from Trappe and Washington [11, p. 3]. Alice and Bob use cryptography to communicate securely in the presence of an eavesdropper, Eve. The message is encrypted using an encryption key, turning the plaintext into a ciphertext before it is broadcast over a public channel. Bob then uses the decryption key to recover the message. 5

3.1 The BB84 QKD protocol. This is a prepare-and-measure QKD protocol, where Alice encodes information using photons polarized in non-orthogonal bases. Bob randomly chooses from two measurement settings. 33

4.1 The EPR-Bohm thought experiment. A π meson decays into a positron and electron with opposite spin, and these particles are measured by Alice and Bob. The spin of the two particles is opposite to each other, so Alice and Bob's measurement outcomes will be anti-correlated. 39

4.2 A simple thought experiment for deriving Bell's inequality. Alice and Bob each randomly choose between two measurement settings for each trial, and they then compute the correlation of their outcomes. 42

4.3 The black box model hides the inner workings of the analysis stations and only deals with the measurement settings (two push buttons) and measurement outcomes (+1 or −1). 45
4.4 The E91 QKD protocol. A π meson decays into two polarization-correlated entangled particles, which are measured along different axes by Alice and Bob. The resulting correlations violate Bell's inequality. 49

6.1 The Franson interferometer. The source emits time-correlated photons, which are sent to Alice and Bob. At their respective analysis stations, they perform measurements along angles ϕ_A and ϕ_B, respectively, and record the outcome as well as time of detection. 73

7.1 LHV model by Aerts et al. [138] for faking a Bell-CHSH violation in the Franson interferometer. These models take as input the hidden variables r and θ, and analysis station settings ϕ_A and ϕ_B. The upper graph shows Alice's prescribed measurement outcomes (A) while the lower shows Bob's (B). The LHV model returns the sign (+1 or −1) and timeslot (E for early and L for late). 83
7.2 Part of the equipment used by Gerhardt et al. [141] to break the security of a commercial Quantum Key Distribution (QKD) system. Depicted here is Eve's photon detection unit and the faked-state generator, which contains semiconductor lasers, polarization controllers, and control electronics. Note the $|\Phi\rangle$ Jolly Roger logo for quantum hacking. Photo copyright © 2009 Vadim Makarov, reused with permission. . . . 85

7.3 Schematic of a beam splitter manufactured by joining two triangular prisms with different refractive indices. The beam splitter depicted here has a high refractive index in the lower left region and a low refractive index in the top right. Two incident beams are combined into two output beams. The beam from the left receives no phase shift, but the beam from the top receives a π phase shift when reflected off the higher refractive index region. 87

7.4 Close-up of figure 6.1, which shows Bob's analysis station in the Franson interferometer. The left beam splitter is the *splitter* wile the right beam splitter is the *combiner*. 89

7.5 Experimental setup for hacking the Franson interferometer as done in publication B. In the back is the mechanically dampened optical table with optical components on top of it. The white polystyrene boxes are for thermal insulation of the components inside, and the components are connected with optical fibers. To the right is a rack with four InGaAs avalanche photodiodes from Princeton Lightwave. Picture taken at AlbaNova, Stockholm University. 91

7.6 Experimentally measured faked Bell values $S_M(2)$ in our attack on the Franson interferometer compared to the Bell-CHSH bound (theorem 4.7), Cirel'son's bound (theorem 4.8), and the trivial Bell value (theorem 4.6). Each measurement run is 27 s long. When aiming for the quantum prediction $2\sqrt{2}$, the produced Bell value is averages to 2.5615 ± 0.0064 (solid black line). It is possible to boost the faked Bell value as high as 3.6386 ± 0.0096 (dotted blue line). 93

8.1 The black box method for $N \geq 2$ settings per observer. This is a generalization of figure 4.3 that instead uses N push buttons. The analysis stations still return the outcomes +1 or −1. 98

8.2 Hugging interferometers, or Genuine Energy-Time Entanglement (GETE). This setup has many of the properties of the original Franson setup but allows the postselection loophole to be closed. 112
8.3 Energy-Time Entanglement (ETE) with optical switches synchronized with the source. An early photon would take the long, delayed, path while a late photon is immediately detected. This results in a setup without the postselection loophole. 113

9.1 Quantum banknote in Wiesner's quantum money scheme with 20 qubits as depicted by Bennett [187]. Note the classical serial number printed on the bottom of the banknote. 126

List of Tables

8.1 Comparison of quantum prediction $S_{QM}(N)$ vs. the Pearle-Braunstein-Caves (PBC) bound $S_C(N)$ for the Franson interferometer with fast switching and $N \geq 2$ settings per observer. 103

8.2 Minimum visibility required in order for the quantum-mechanical prediction $S_{QM}(N)$ to violate the PBC inequality in the Franson interferometer when using fast switching. Note that the case $N = 2$ (Bell-CHSH) does not allow for a violation of local realism while all $N \geq 3$ do. In fact, the least restrictive number of settings is $N = 5$ where the critical visibility is 94.63 %. 109

List of Theorems

Contributed

6.1 Bell-CHSH for the Franson Interferometer 76
6.2 Outcomes from Early Events 78
6.3 Outcomes from Late Events 78
6.4 Bell-CHSH for the Franson Interferometer with Fast Switching 79

8.7 Trivial Detection Efficiency for Pearle-Braunstein-Caves 101
8.9 Pearle-Braunstein-Caves for the Franson Interferometer 101
8.10 Pearle-Braunstein-Caves for the Franson Interferometer with Fast Switching 102
8.11 Pearle-Braunstein-Caves with Detection Efficiency for the Franson Interferometer with Fast Switching 102
8.12 Trivial Chained Detection Efficiency for the Franson Interferometer with Fast Switching 103
8.13 Critical Chained Detection Efficiency for the Franson Interferometer with Fast Switching 104
8.14 Pearle-Braunstein-Caves with Coincidence Probability 104
8.15 Trivial Coincidence Probability for Pearle-Braunstein-Caves 105
8.16 Critical Coincidence Probability for Pearle-Braunstein-Caves 105
8.21 Critical Visibility for the Franson Interferometer with Fast Switching 108
8.22 Bell-CHSH with Path Realism 111

9.2 Distributed Ledger Scheme 124

Full list

2.1 Invariance of Inner Product under Unitary Transformation 20
2.6 State Vector 22
2.7 Quantum Measurement 22
2.9 Uncertainty Principle 23
2.10 Unitary Evolution 25
2.11 Indistinguishability of Non-Orthogonal States 26
2.12 No-Cloning Theorem 27

4.6 Trivial Bell Value 47
4.7 Bell-CHSH 47
4.8 Quantum Prediction of the Bell Value 47

5.4 Detection Efficiency for Local Realist Systems 61
5.5 Bell-CHSH with Detection Efficiency 62
5.6 Trivial Detection Efficiency for Bell-CHSH 62
5.7 Critical Detection Efficiency for Bell-CHSH 63
5.9 Bell-CHSH with Coincidence Probability 66
5.10 Trivial Coincidence Probability for Bell-CHSH 66
5.11 Critical Coincidence Probability for Bell-CHSH 67

6.1 Bell-CHSH for the Franson Interferometer 76
6.2 Outcomes from Early Events 78
6.3 Outcomes from Late Events 78
6.4 Bell-CHSH for the Franson Interferometer with Fast Switching 79

8.2 Trivial Chained Bell Value 99
8.3 Pearle-Braunstein-Caves 99
8.4 Quantum Prediction of the Chained Bell Value 100
8.6 Pearle-Braunstein-Caves with Detection Efficiency . . 100
8.8 Critical Detection Efficiency for Pearle-Braunstein-Caves 101

8.9 Pearle-Braunstein-Caves for the Franson Interferometer 101
8.10 Pearle-Braunstein-Caves for the Franson Interferometer with Fast Switching 102
8.11 Pearle-Braunstein-Caves with Detection Efficiency for the Franson Interferometer with Fast Switching 102
8.14 Pearle-Braunstein-Caves with Coincidence Probability 104
8.19 Critical Visibility for Bell-CHSH 107
8.20 Critical Visibility for Pearle-Braunstein-Caves 108
8.21 Critical Visibility for the Franson Interferometer with Fast Switching 108
8.22 Bell-CHSH with Path Realism 111

List of Acronyms

AES Advanced Encryption Standard

APD Avalanche Photo-Diode

ASIC Application-Specific Integrated Circuit

BB84 Bennett and Brassard's 1984 Quantum Key Distribution Protocol

BBBW Bennett, Brassard, Breidbart, and Wiesner

CH Clauser-Horne

CHSH Clauser-Horne-Shimony-Holt

COW Coherent One-Way

CW Continuous-Wave

DES Data Encryption Standard

DH Diffie-Hellman

DI Device-Independent

DI-QKD Device-Independent Quantum Key Distribution

DoS Denial of Service

DPS Differential Phase-Shift

E91 Ekert's 1991 Quantum Key Distribution Protocol

ECDSA Elliptic-Curve Digital Signature Algorithm

EPR Einstein, Podolsky, and Rosen

ETE Energy-Time Entanglement

GCHQ Government Communications Headquarters

GETE Genuine Energy-Time Entanglement

ITS Information-Theoretic Security

LHV Local Hidden Variable

LWE Learning With Errors

MDI-QKD Measurement-Device-Independent Quantum Key Distribution

MZ Mach-Zehnder

OTP One-Time Pad

PBC Pearle-Braunstein-Caves

PoW Proof of Work

PQC Post-Quantum Cryptography

PR Popsecu-Rohrlich

PRA Physical Review A

PRL Physical Review Letters

PRNG Pseudo-Random Number Generator

QKD Quantum Key Distribution

QRNG Quantum Random Number Generator

RFC Request For Comments

R-LWE Ring-Learning With Errors

RNG Random Number Generator

RSA Rivest-Shamir-Adleman

SIDH Supersingular Isogeny Diffie–Hellman

SPD Single Photon Detector

SPDC Spontaneous Parametric Down-Conversion

TCP Transmission Control Protocol

TRNG True Random Number Generator

WCA Wegman-Carter Authentication

List of Symbols

Mathematics

$\mathbb{R}$ The set of real numbers.

$\mathbb{C}$ The set of complex numbers.

$\mathbb{C}^n$ Complex vector space with n dimensions.

$\mathbb{F}_2$ The set containing 0 and 1.

$\mathbb{F}_2^n$ The set of bit strings of length n.

z^* Complex conjugate of z.

$\mathcal{H}$ Hilbert space.

I Identity matrix.

$(\cdot, \cdot)$ Inner product.

$\cap$ Set intersection

$A^\dagger$ Hermitian conjugate of A.

A^T Matrix transpose of A.

$\times$ Multiplication

P Probability measure.

X Random variable.

$E(X)$ Expected value of the random variable X.

$\subset$ Subset

$\otimes$ Tensor product

U Unitary map.

Physics

c The speed of light in vacuum, 299 792 458 m s^{-1}.

e^- Electron.

e^+ Positron.

γ_0 Free gamma photon.

I_0 Incident optical intensity to a beam splitter.

I_B Optical output intensity at the bottom exit of a beam splitter.

I_R Optical output intensity at the right exit of a beam splitter.

I_T Optical intensity threshold for a blinded Avalanche Photo-Diode (APD) locked in linear mode.

π^0 Pi meson.

Quantum Mechanics

$\langle\cdot|$ Bra vector.

$|\cdot\rangle$ Ket vector.

$\langle\cdot\,|\,\cdot\rangle$ Bra-ket inner product.

$+$ Rectilinear, or computational, basis.

$\times$ Diagonal basis.

$|\Phi^-\rangle, |\Phi^+\rangle, |\Psi^-\rangle, |\Psi^+\rangle$ The Bell states; four specific maximally entangled quantum states of two qubits.

$\hbar$ Reduced Planck constant.

$|0\rangle$ Computational (rectilinear) basis state 0.

$|1\rangle$ Computational (rectilinear) basis state 1.

$|-\rangle$ Diagonal basis state $-$.

$|+\rangle$ Diagonal basis state $+$.

M_m Quantum general measurement operator.

σ_x Pauli-X matrix.

σ_y Pauli-Y matrix.

σ_z Pauli-Z matrix.

Experimental Interferometry

A_i Random variable describing Alice's local realist measurement outcome.

B_j Random variable describing Bob's local realist measurement outcome.

$A_{i,j}$ Random variable describing Alice's realist measurement outcome.

$B_{i,j}$ Random variable describing Bob's realist measurement outcome.

ΔT Time difference of the upper and lower optical path in the analysis stations of the Franson interferometer.

$\Delta\tau$ Time window in a bipartite experiment inside which events are considered coincident.

r, θ Local hidden variables used in breaking the security of the Franson interferometer.

I_L^- Optical intensity of the late pulse at the minus detector in the Franson interferometer.

I_L^+ Optical intensity of the late pulse at the plus detector in the Franson interferometer.

I_E^- Optical intensity of the early pulse at the minus detector in the Franson interferometer.

I_E^+ Optical intensity of the early pulse at the plus detector in the Franson interferometer.

λ Hidden variable.

Λ Sample space of hidden variables.

Λ_X Subset of a set Λ, on which the random variable X is defined.

ω_E Phase shift between the first and second pulse in the Franson interferometer attack.

ω_L Phase shift between the second and third and second pulse in the Franson interferometer attack.

ϕ_A Measurement angle at Alice's analysis station.

ϕ_B Measurement angle at Bob's analysis station.

T^A Detection time at Alice's analysis station.

T^B Detection time at Bob's analysis station.

τ_0 Lifetime of the middle level in a three-level system.

τ Length of the classical pulses of light used in the attack on the Franson interferometer.

V_N Interferometric (fringe) visibility.

V_{critical} The minimum interferometric visibility at which $S_{QM}(2)$, the Bell value predicted by quantum mechanics, coincides with the local realist Bell bound $S(2)$.

$V_{\text{critical},N}$ The minimum interferometric visibility at which $S_{QM}(N)$, the chained Bell value predicted by quantum mechanics, coincides with the local realist Pearle-Braunstein-Caves (PBC) bound $S(N)$.

$V_{\text{critical},N,F}$ The minimum interferometric visibility at which $S_{QM}(N)$, the chained Bell value predicted by quantum mechanics, coincides with the local realist Pearle-Braunstein-Caves (PBC) bound $S(N)$ for the Franson interferometer when using fast switching.

Bell's Theorem

$S(2)$ Bell value.

$S(2)_{\text{max}}$ Trivial, algebraic limit of the Bell value.

$S_{QM}(2)$ Quantum prediction for the Bell value.

$S_C(2)$ Bell value, taking only coincident events into account.

N Number of settings per observer in a bipartite Pearle-Braunstein-Caves (PBC) experiment.

$S(N)$ Chained Bell value.

$S(N)_{\text{max}}$ Trivial, algebraic limit on the chained Bell value.

$S_{QM}(N)$ Quantum prediction for the chained Bell value.

$S_C(N)$ Chained Bell value, taking only coincident events into account.

$S_B(N)$ Any local realist bound.

$S_M(N)$ Experimentally measured chained Bell value.

$S_M(2)$ Experimentally measured Bell value.

Detection Efficiency

η Overall detection efficiency in a bipartite Bell experiment.

η_N Overall detection efficiency in a bipartite Pearle-Braunstein-Caves (PBC) experiment.

η_A The detection efficiency of Alice's analysis station.

η_B The detection efficiency of Bob's analysis station.

η_{critical} The minimum detection efficiency at which $S_{QM}(2)$, the Bell value predicted by quantum mechanics, coincides with the local realist detection efficiency Bell bound $S(2)$.

$\eta_{\text{critical,N}}$ The minimum detection efficiency at which $S_{QM}(N)$, the chained Bell value with N settings per observer predicted by quantum mechanics, coincides with the local realist detection efficiency Pearle-Braunstein-Caves (PBC) bound $S(N)$.

$\eta_{\text{critical,N,F}}$ The minimum detection efficiency at which $S_{QM}(N)$, the chained Bell value with N settings per observer predicted by quantum mechanics, coincides with $S(N)$, the local realist detection efficiency Pearle-Braunstein-Caves (PBC) bound in the Franson interferometer when using fast switching.

η_{trivial} The minimum detection efficiency at which $S(2)_{\text{max}}$, the trivial Bell value, coincides with the local realist detection efficiency Bell bound $S(2)$.

$\eta_{\text{trivial,N}}$ The minimum detection efficiency at which $S(N)_{\text{max}}$, the trivial chained Bell value with N settings per observer coincides with the local realist detection efficiency Pearle-Braunstein-Caves (PBC) bound $S(N)$.

$\eta_{\text{trivial,N,F}}$ The minimum detection efficiency at which $S_{QM}(N)$, the trivial chained Bell value with N settings per observer, coincides with $S(N)$, the local realist detection efficiency Pearle-Braunstein-Caves (PBC) bound in the Franson interferometer when using fast switching.

Coincidence Probability

γ The probability of coincidence in a bipartite Bell experiment.

γ_N The probability of coincidence in a bipartite Pearle-Braunstein-Caves (PBC) experiment.

γ_{critical} The minimum coincidence probability at which $S_{QM}(2)$, the Bell value predicted by quantum mechanics, coincides with the local realist coincidence-time Bell bound $S(2)$.

$\gamma_{\text{critical},N}$ The minimum coincidence probability at which $S_{QM}(N)$, the quantum-mechanical prediction of the chained Bell value with N settings per observer, coincides with the local realist coincidence-time Pearle-Braunstein-Caves (PBC) bound $S(N)$.

γ_{trivial} The minimum coincidence probability at which $S(2)_{\text{max}}$, the trivial Bell value, coincides with the local realist coincidence-time bound $S(2)$.

$\gamma_{\text{trivial},N}$ The minimum coincidence probability at which $S(N)_{\text{max}}$ the trivial chained Bell value with N settings per observer, coincides with the local realist coincidence-time Pearle-Braunstein-Caves (PBC) bound $S(N)$.

Quantum Bitcoin

$||$ Concatenation of strings.

H Hash function.

$\mathcal{L}$ Distributed ledger scheme.

$\mathcal{M}$ Quantum money mini-scheme.

$|\$\rangle$ Quantum money state.

s Classical serial number.

Preface

This doctoral thesis contains results from research performed by the author at the Information Coding Group at the Department of Electrical Engineering at Linköping University, Sweden between 2012 and 2017. Parts of the material have been presented at international conferences, and six published or submitted research publications are enclosed at the end of the thesis.

Supervisor: Professor Jan-Åke Larsson, Information Coding Group, Department of Electrical Engineering, Linköping University.

Co-supervisor: Associate Professor Fredrik Karlsson, Semiconductor Materials, Department of Physics, Chemistry and Biology, Linköping University.

There is a remarkably close parallel between the problems of the physicist and those of the cryptographer. The system on which a message is enciphered corresponds to the laws of the universe, the intercepted messages to the evidence available, the keys for a day or a message to important constants which have yet to be determined. The correspondence is very close, but the subject matter of cryptography is very easily dealt with by discrete machinery, physics not so easily.

— Alan Turing, 1948 [1, p. 9]

Chapter 1

Introduction

This chapter will give a brief, historic overview of how cryptography has evolved from ancient Egypt and Greece, all the way to the modern invention of quantum cryptography. The history of increasingly sophisticated cryptographic methods will lead up to our goal of a provably secure cryptographic system. At the same time, codebreakers have been busy refining their methods, and in that spirit we will also show how the ostensibly perfect security of quantum cryptography can be broken in practice.

1.1 History of Cryptography

The art of *cryptography*, or secret writing, appears to be as old as writing itself. The ancient Egyptian civilization left behind documents of hieroglyphs in the Giza pyramids, some of which are believed to be an early example of secret writing. Before the Rosetta stone was discovered it was impossible to comprehend the complicated hieroglyphs, and therefore the script itself can be seen as an early example of secret writing. Even with the Rosetta stone, however, there are documents from Giza that still defy translation [2].

From the very beginning, cryptography has put its mark on history by influencing major events and especially wars. In ancient Greece the *skytale* was used as an early form of transposition cipher. A piece of parchment, cloth, or leather is wound around a rod of a certain diameter, and it is then possible to write a message along the length of the rod. When the parchment is unwound, it becomes difficult to comprehend the meaning of the letters that now have moved around, and the recipient can recover the message by winding around a rod of similar diameter. It is believed [2] that the Spartan general Lysander used the *skytale* to send encrypted messages during a battle against the Persians in 405 BC. His subsequent victory had a lasting impact on early European history. The idea that the *skytale* was used as a cryptographic device dates back to Cicero (106–43 BC) [3], however this has come under scrutiny in recent times. In 1998, after studying the available Greek source material, Kelly [4] claimed that "the *skytale* was nothing more than a piece of leather or parchment attached to a stick" [4, p. 260].

Closely related to cryptography, the field of *cryptanalysis* concerns itself with analyzing cryptographic systems in order to find weaknesses, hidden properties, and even break their security. Together with cryptography, the two fields make up the science of *cryptology*.

In contrast to the many other advances the Chinese civilization managed to achieve, it did not contribute to the development of cryptography as their language lacked a simple alphabet [5]. Instead, it was in the Italian city-states of the Renaissance where the first seeds of modern cryptography were sown. An early example of what we now call a *substitution cipher* can be found in correspondence between the Vatican and its nuncios some time after the year 1330 [3, p. 280]. Venice and other Italian city-states came to possess some cryptological expertise, and a prime example is the Florentine cryptographer Leon Battista Alberti. His 25-page manuscript *De componendis cyfris* from 1466 or 1467 is the oldest surviving text on cryptanalysis in the western world [3, p. 280], and Kahn [6, p. 125] described Alberti as the "Father of Western Cryptology".

1.2 Fundamental Principles of Cryptography

The word “cryptography” is constructed from Greek, where *kryptós* means “hidden” and *graphein* means “writing”. Ever since the Renaissance, cryptographers have been in a cat-and-mouse game with cryptanalysts where the former tries to create cryptographic systems that the latter is unable to break. At the same time, cryptanalysts attempt to mount better and better attacks in order to defeat the cryptography and recover the encrypted messages.

While it is debated whether or not the previously-mentioned *skytale* was used for cryptography, Herodotus (ca. 486–425 BC) [7] tells the story of a related cryptographic technique. Demeratus, a Greek at the Persian court, sent a secret message by hiding it in a writing tablet. He removed its wax surface, and after inscribing a secret message on the wooden backing, he applied a fresh layer of wax. This made the tablet appear blank while it actually carried a hidden message. According to Herodotus, the deception was so effective that it fooled not only the Persian customs, but almost the recipient as well.

This method of Demeratus', disguising a message where nobody would look, is called *steganography*, which should not to be confused with the handwriting technique of *stenography*. There are numerous ways in which steganography has been used throughout history. Invisible ink and microdots are famous examples from spy novels, but there are ways of hiding information in even more plain sight. A digital image can be altered so that the least significant bits constitute a message without the human eye noticing, and a carefully written letter can look innocent while, say, every 21st letter makes up a hidden message. Steganography is one of three basic types of cryptography and truly lives up to the description “hidden message”.

The two other basic types of cryptography are *codes* and *ciphers*. Codes are used to replace specific words, names or sentences with other words or symbols using a code book, and this method was famously used by Mary, Queen of Scots in a failed attempt to conquer the English throne in the late 16th century [8, pp. 32–44]. Codes and code books are however cumbersome to use, and in modern times the focus has instead shifted towards ciphers. While the definition of a cipher partially overlaps with that of a code, ciphers generally operate on a lower level. The *skytale*, for instance, is a cipher that operates on individual letters and performs a transposition.

As we have seen in these brief examples, cryptography has historically only been used to ensure secrecy when communicating over an untrusted channel. This has changed dramatically with the digital revolution, and new developments in cryptography have led to applications such as authentication, digital signatures, secret sharing, and so on. These successes have made technologies like online banking, credit cards, electronic commerce, etc., to be secure enough to be appealing to the general public. Cryptography has also led to the development of decentralized cryptographic currencies like Bitcoin [9] and Ethereum [10] which offer an alternative to traditional currencies.

The basic communication scheme for cryptography is depicted in figure 1.1. Two parties, Alice and Bob, wish to communicate securely in the presence of an eavesdropper Eve. Alice encrypts her message, called the *plaintext*, with a predetermined encryption algorithm using an encryption *key*. This turns the plaintext into a *ciphertext*, which is transmitted over an untrusted channel to Bob. During transmission it is assumed that Eve has full knowledge of the ciphertext. Bob decrypts the ciphertext with the decryption key and, if the process is performed correctly, recovers the message.

Before any further analysis of cryptography can be made, however, we must establish a fundamental principle of cryptology known as Kerckhoff's principle: *The enemy knows the system*. The importance of this assumption cannot be understated, as the only way to know that a cryptographic system really is secure is if it can withstand the best cryptanalysis. Were Alice and Bob to choose a cryptographic system that in any way relies on Eve not knowing the inner workings of their system, they will probably fool themselves. If Eve happens to learn the trick (or several tricks)

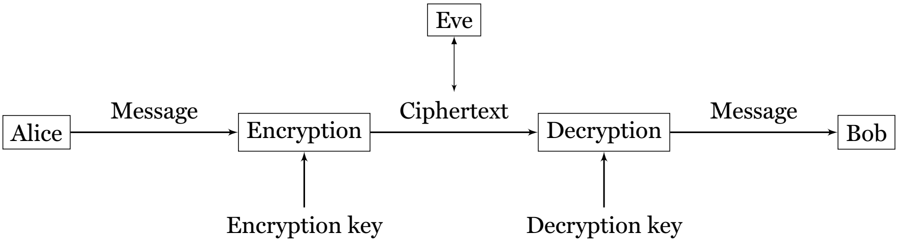


Figure 1.1: Basic communication scheme for cryptography, adapted from Trappe and Washington [11, p. 3]. Alice and Bob use cryptography to communicate securely in the presence of an eavesdropper, Eve. The message is encrypted using an encryption key, turning the plaintext into a ciphertext before it is broadcast over a public channel. Bob then uses the decryption key to recover the message.

Alice and Bob have used, she will instantly be able to break their security. It is better to let only the key be secret.

In fact, if Alice and Bob invent their own cryptographic algorithms, there is a large probability that their creation will be insecure. This is encapsulated in Schneier's law [12], which states that "anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he or she himself cannot break". Alice and Bob are therefore best advised to rely on methods and algorithms that have been tested and tried by repeated cryptanalysis. The temporary gain that might arise from introducing a secret trick pales in comparison to the permanent damage caused by an unknown flaw in the design[1]. Our scheme in figure 1.1 must therefore be extended with the assumption that the only thing Eve does not know is the key and the message itself.

Cryptographic systems in violation of Kerckhoff's principle are said to rely on *security through obscurity*. It should be obvious that

[1] In contrast to what many designers of quantum key distribution systems seem to believe, Schneier's law applies to quantum systems, too. It appears an addendum to Schneier's law is called for: "Any physicist can construct a quantum key distribution system that can be proved secure under some restrictions the physicist prefers."

a cryptographic system that in any way relies on steganography is guilty of this flawed security practice.

1.3 Public-Key Cryptography

> [public-key cryptography] turned out to be the most important innovation in cryptology since the advent of the computer and it took only a decade to become an indispensable technology for the protection of computer networks.
>
> — Karl de Leeuw, 2007 [13, p. 17]

In figure 1.1 there are two keys; one for encryption and one for decryption. Up until the early 1970s, all cryptographic protocols used *symmetric* algorithms, i.e., the two keys are identical. Examples of symmetric algorithms include the Data Encryption Standard (DES) [14], the Advanced Encryption Standard (AES) [15], and Blowfish [16]. The invention of *asymmetric*, or *public-key* cryptography, revolutionized the field of cryptology by instead using *different* keys for encryption and decryption. The two keys are usually referred to as the *public* and *private* keys. The advantage of public-key cryptography is especially obvious in today's age of the Internet, as Alice and Bob can encrypt information without needing a pre-shared key.

Care must be taken, however, as public-key cryptography does not solve the problem of authentication. Eve can perform a so-called *man-in-the-middle attack* where she impersonates both Alice and Bob, and the end result is complete information leakage without leaving a trace. The man-in-the-middle attack is prevented by authenticating both parties before sending information over the channel, and this requires some form of pre-shared key. Thus, public-key cryptography should not be described as "not requiring a pre-shared key", but rather "requiring less pre-shared key than symmetric cryptography".

The first discovery of a public-key algorithm was long credited to the groundbreaking work of Diffie and Hellman in 1976 [17]. Their algorithm, Diffie-Hellman (DH) key exchange, allows Alice and Bob to exchange a key over an untrusted channel. It would turn out, however, that DH was not the first invention of its kind. In 1997, the Government Communications Headquarters (GCHQ) in the United Kingdom declassified information that revealed a similar discovery made several years before Diffie and Hellman [8, pp. 283–290]. Due to the secret nature of intelligence work, the original inventors at GCHQ had to wait over two decades before their achievement was publicly recognized. The original motivation for the research that led to this discovery by the GCHQ was to reduce the cost of distributing symmetric keys [8, p. 282].

Public-key cryptography can be created from a special type of mathematical functions that are *one-way*. This is a function f with the property that, given x, computing $y = f(x)$ is easy while it is computationally infeasible to find x so that $f(x) = y$. If the one-way function also has a *trapdoor* there exists a way to find x, but only with some extra information, known only to the designer of said function. It should be computationally infeasible for someone else to determine this trapdoor information [11, p. 191]. Trapdoor one-way functions allow us to create algorithms for public-key cryptography.

From a very large family of such functions, Bob generates one in such a way that only he has the corresponding trapdoor information. He then publishes his function f as his public encryption algorithm. Alice, who wants to send Bob the message m, computes the ciphertext $c = f(m)$ and sends this to Bob. He can then compute the message m using the trapdoor information, but Eve cannot. Using a one-way trapdoor function, we now create a public-key cryptosystem where Alice and Bob can communicate securely without a pre-shared key.

The one-way trapdoor function used in DH is *modular exponentiation* [17], and in order to reverse the trapdoor one needs to solve the *discrete logarithm problem*, which is considered hard. The GCHQ public-key algorithm, however, uses a different one-way trapdoor function based on the *factorization problem*. Computing $f(m) = m^e \pmod{n}$ is easy given e and n, but without knowing the prime factors p and q of n (i.e., the trapdoor information), the reverse is computationally infeasible for large n. The same method was independently discovered by Rivest et al. [18] 1978, and is named Rivest-Shamir-Adleman (RSA) after the inventors. RSA remains the most popular public-key algorithm in use today [19, p. 17], although the newer Elliptic-Curve Digital Signature Algorithm (ECDSA) [20] (based on elliptic curves over finite fields) is gaining momentum.

It must be pointed out that the difficulty of the discrete logarithm problem and the factorization problem has never been proven. It is unlikely, but theoretically possible, that there will be a major breakthrough tomorrow that makes these problems easy. Such a discovery would immediately break the security of RSA. However, the peculiar properties of prime numbers have been studied since at least Euclid's time (300 BC), and it is likely that prime factors will remain difficult to compute for the foreseeable future. Another theoretical weakness of public-key algorithms is that he existence of one-way functions themselves is an open conjecture.

1.4 Cryptography and the Quantum World

Research into the factorization problem took an unexpected turn in 1994, when Shor [21] published an efficient quantum algorithm for finding prime factors. The difference to previous factoring algorithms is that Shor's algorithm requires a *quantum computer*, a device operating on *qubits* instead of ordinary, classical bits. As a consequence, a working quantum computer would break the security of RSA. In addition, Shor's algorithm can also break DH key exchange and ECDSA. Now, the prime factors used in RSA are very large, typically hundreds of digits long, but today's experimental realizations of Shor's algorithm are only able to factor small numbers [22–29]. In the near future, Shor's algorithm remains a theoretical rather than practical threat, however the mere idea of a quantum computer has led researchers to search for algorithms that remain strong even if a revolution in quantum computing were to occur.

This relatively new area of research is called Post-Quantum Cryptography (PQC) and aims to find new cryptographic algorithms safe from Shor's algorithm. While RSA would be compromised by quantum computers, many cryptographic algorithms will remain secure [30, pp. 1–2]. Generally, symmetric algorithms are considered quantum-safe, although the key size must be increased to prevent attacks due to Grover's quantum algorithm [31]. However, all public-key cryptosystems in wide use today (RSA, DH, ECDSA) are easily broken by Shor's algorithm and, finding quantum-safe equivalents is of high priority.

There are several proposals for post-quantum cryptosystems. Lattice-based systems include algorithms based on Learning With Errors (LWE) [32] (Frodo [33], Ring-Learning With Errors (R-LWE) [34], NewHope [35]) and NTRU [36]. Other methods include Supersingular Isogeny Diffie–Hellman (SIDH) [37], and McEliece's code-based crypto [38]. See Bernstein and Lange [39] for a review of PQC algorithms. In comparison to the "industry-standard" algorithms of RSA, DH, and ECDSA, the current quantum-safe counterparts are generally slower, have a large communication overhead, and/or require large keys. In addition, the new mathematical foundations are relatively new and unproven, leading to a worry that further developments find weaknesses in their security.

We will now turn our attention to a cryptosystem that achieves security without resorting to not-yet-proven assumptions on a problem being difficult. The One-Time Pad (OTP) has *unconditional* security [19, pp. 15–17, 11, pp. 39–41] and no matter what computing power Eve possesses, she will not be able to break it. OTP has been described as "the Holy Grail of cryptography" [8, p. 122], but the disadvantage is that it requires rigorous key management. For every bit of information to be encrypted, one bit of key is needed. Add to it the key must be random, secret, and never re-used, and it becomes clear that OTP is very costly to use in practice. Therefore, it has primarily been used in low-bandwidth applications with ultra-high security requirements [19, p. 17].

It is easy to see why the one-time pad has unconditional security. Consider the binary plaintext `10001100` encrypted by taking bitwise `xor` with the key `01101100`. The resulting ciphertext is `11100000`, which can be decrypted by again taking a bitwise `xor` with the key. Now, an attacker can try all possible keys (there are only 2^8=256 keys to try) and find all possible plaintexts. Unfortunately, all of these plaintexts are equally probable so there is no way of knowing when the correct plaintext is found.

Unconditional security, as the name implies, is the highest level of security and resists *any* attack, even those allowed by quantum mechanics. It places no further restriction on the attacker who can be assumed to have unbounded computational resources. As in the example of OTP, even if Eve can try all combinations of the key she will not break the cryptosystem. Another name commonly found in the literature is Information-Theoretic Security (ITS).

If unconditional security cannot be achieved, a lower level of security can be found in *complexity-theoretic security*. Here, we place restrictions on the number of queries that can be performed by the attacker. Currently, we call a problem *intractable* when it requires at least 2^{128} queries to brute-force. If we further assume the attacker to have access to a quantum computer, we require quantum-safe complexity-theoretic security.

If Alice and Bob want to base their security on OTP and transfer, say, a gigabyte of information, they will need a gigabyte of key. If their key runs out, they cannot reuse any part of it and will have to negotiate more key bits. It is, of course, possible to use a public-key algorithm to generate such a key, but the chain cannot be stronger than the weakest link and this would be a pointless implementation of OTP. As it stands, Alice and Bob will have to rely on a trusted courier to exchange keys and let him or her carry the entire burden of securing their communication.

In the classical world this is as good as it gets. OTP gives ultimate security, but shifts the *entire* problem of encryption into a problem of key management. There is simply no way around it; Alice and Bob must meet in person or use a courier. Unless, of course, they to invoke quantum mechanics. The peculiar properties of a *quantum channel* allows Alice and Bob to set up a communications system where the laws of physics, instead of vague concepts of "computational complexity" guarantee the security. The same physical laws also make the system robust against an attacker with access to a working quantum computer.

The idea is that Alice and Bob use the quantum channel to randomly, and secretly, generate a key, which then can be used in OTP. The result is Quantum Key Distribution (QKD), and this key distribution method can give perfect security. QKD is a field currently undergoing tremendous development and there are several working protocols as will be shown later. Recently, research into so-called Energy-Time Entanglement (ETE) has begun leading the way towards a practical method for QKD. It has been suggested that a design by Franson [40] could be used to achieve the same unconditional security as traditional entanglement-based QKD protocols. Several experiments have evaluated this Franson-type setup [41–50], however this thesis will point to complications when basing QKD on Energy-Time Entanglement (ETE).

1.5 Outline

This thesis will present our contributions in quantum cryptography given in publications A to F. The chapters leading up to these six publications are intended to give an overview of the fields of quantum key distribution, quantum hacking, experimental Bell testing, quantum money, and the blockchain.

We begin in chapter 2 by establishing notation, followed by some basic results from linear algebra and probability theory. These basic results are then used to discuss a few basic postulates in quantum theory, which will have important consequences for quantum key distribution. We further build on those postulates and prove the important theorems of no-cloning and non-distinguishability of non-orthogonal quantum states.

Chapter 3 introduces QKD and presents two major categories of such protocols: those of the type called “prepare-and-measure”, and those based on entanglement. We then present, and discuss the security of, the pioneering BB84 protocol, which uses two sets of mutually unbiased bases.

Many QKD protocols rely on Bell’s Theorem, and we therefore dedicate chapter 4 to an introduction of this fundamental result in quantum theory. We give a historic background, followed by a first intuitive explanation before stating the theorem itself. Important applications include the E91 QKD protocol and the beautiful theory of *Device-Independent* (DI) QKD.

Next, chapter 5 discuss a number of loopholes in Bell’s Theorem, which requires us to understand and quantify the amount by which real-world implementations of QKD deviate from the ideal situation. We emphasize the detection loophole and the coincidence-time loopholes, both of which can be used to break the security assumptions of Device-Independent Quantum Key Distribution (DI-QKD).

Energy-Time Entanglement (ETE) is introduced in chapter 6, and we show what advantages this method has over traditional, polarization-based QKD. We also present the Franson interferometer, a scheme that employs ETE and promises to be a method for usable quantum cryptography. However, we then reveal a serious weakness of the Franson setup, and the subsequent exploit is presented in detail in chapter 7 and publications A and B.

Importantly, our ultimate goal is not to break the security of QKD. On the contrary, we wish to make the protocols stronger! Chapter 8 discusses a number of methods for re-establishing security, some of which are contained in publications A and B. One method is to invoke a generalized, chained, version of Bell’s Theorem and we show this to be experimentally viable in publication D. Then, in order to prevent the coincidence-time loophole in this generalized setting we had to develop new theoretical results given in publication C.

The thesis then takes a detour in order to introduce publication E and our invention of Quantum Bitcoin. Chapter 9 introduces necessary concepts, including Bitcoin, the blockchain, quantum money, and finally our construction for a blockchain-endowed quantum currency.

We conclude the thesis in chapter 10 by returning to the bigger picture. Here, we show that while the results of publications A and B have been known for years, there are recent papers that still ascribe unconditional security to the Franson interferometer. Publication F is a comment to one such paper, which led to the authors publishing an errata in the same journal. We end the chapter by discussing ideas for future work.

1.6 Included Publications

Publications A and B have previously been included in the thesis author's Licenciate thesis published in 2015 [51]. The Swedish Licenciate degree comprises 120 ECTS credits of postgraduate studies.

Publication A: Energy-time entanglement, elements of reality, and local realism

Published in Journal of Physics A: Mathematical and Theoretical on the 24th of October 2014 [52].

Authors

Jonathan Jogenfors and Jan-Åke Larsson.

Abstract

The Franson interferometer, proposed in 1989 [J. D. Franson, Phys. Rev. Lett. 62:2205-2208 (1989)], beautifully shows the counter-intuitive nature of light. The quantum description predicts sinusoidal interference for specific outcomes of the experiment, and these predictions can be verified in experiment. In the spirit of Einstein, Podolsky, and Rosen it is possible to ask if the quantum-mechanical description (of this

setup) can be considered complete. This question will be answered in detail in this paper, by delineating the quite complicated relation between energy-time entanglement experiments and Einstein-Podolsky-Rosen (EPR) elements of reality. The mentioned sinusoidal interference pattern is the same as that giving a violation in the usual Bell experiment. Even so, depending on the precise requirements made on the local realist model, this can imply a) no violation, b) smaller violation than usual, or c) full violation of the appropriate statistical bound. Alternatives include a) using only the measurement outcomes as EPR elements of reality, b) using the emission time as EPR element of reality, c) using path realism, or d) using a modified setup. This paper discusses the nature of these alternatives and how to choose between them. The subtleties of this discussion needs to be taken into account when designing and setting up experiments intended to test local realism. Furthermore, these considerations are also important for quantum communication, for example in Bell-inequality-based quantum cryptography, especially when aiming for device independence.

Contribution

The thesis author performed the theoretical analysis.

Publication B: Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution

Published in Science Advances on the 18th of December 2015 [53]. Raw experimental data available online [54].

Authors

Jonathan Jogenfors, Ashraf Mohamed Elhassan, Johan Ahrens, Mohamed Bourennane, and Jan-Åke Larsson.

Abstract

Photonic systems based on energy-time entanglement have been proposed to test local realism using the Bell inequality. A violation of this inequality normally also certifies security of device-independent quantum key distribution (QKD) so that an attacker cannot eavesdrop or control the system. We show how this security test can be circumvented in energy-time entangled systems when using standard avalanche photodetectors, allowing an attacker to compromise the system without leaving a trace. We reach Bell values up to 3.63 at 97.6 % faked detector efficiency using tailored pulses of classical light, which exceeds even the quantum prediction. This is the first demonstration of a violation-faking source that gives both tunable violation and high faked detector

efficiency. The implications are severe: the standard Clauser-Horne-Shimony-Holt inequality cannot be used to show device-independent security for energy-time entanglement setups based on Franson's configuration. However, device-independent security can be reestablished, and we conclude by listing a number of improved tests and experimental setups that would protect against all current and future attacks of this type.

Contribution

The thesis author devised the attack, designed the experiment, performed statistical analysis and post-processed the raw experimental data.

Publication C: Tight Bounds for the Pearle-Braunstein-Caves Chained Inequality Without the Fair-Coincidence Assumption

Published in Physical Review A (PRA) on the 1st of August 2017 [55].

Authors

Jonathan Jogenfors and Jan-Åke Larsson.

Abstract

In any Bell test, loopholes can cause issues in the interpretation of the results, since an apparent violation of the inequality may not correspond to a violation of local realism. An important example is the coincidence-time loophole that arises when detector settings might influence the time when detection will occur. This effect can be observed in many experiments where measurement outcomes are to be compared between remote stations because the interpretation of an ostensible Bell violation strongly depends on the method used to decide coincidence. The coincidence-time loophole has previously been studied for the Clauser-Horne-Shimony-Holt and Clauser-Horne inequalities, but recent experiments have shown the need for a generalization. Here, we study the generalized "chained" inequality by Pearle, Braunstein, and Caves (PBC) with $N \geq 2$ settings per observer. This inequality has applications in, for instance, quantum key distribution where it has been used to reestablish security. In this paper we give the minimum coincidence probability for the PBC inequality for all $N \geq 2$ and show that this bound is tight for a violation free of the fair-coincidence assumption. Thus, if an experiment has a coincidence probability exceeding the critical value derived here, the coincidence-time loophole is eliminated.

Contribution

The thesis author performed the theoretical analysis and proved the theorem.

Publication D: High-visibility time-bin entanglement for testing chained Bell inequalities

Published in PRA on the 9th of March 2017 [56].

Authors

Marco Tomasin, Elia Mantoan, Jonathan Jogenfors, Giuseppe Vallone, Jan-Åke Larsson, and Paolo Villoresi.

Abstract

The violation of Bell's inequality requires a well-designed experiment to validate the result. In experiments using energy-time and time-bin entanglement, initially proposed by Franson in 1989, there is an intrinsic loophole due to the high postselection. To obtain a violation in this type of experiment, a chained Bell inequality must be used. However, the local realism bound requires a high visibility in excess of 94.63 % in the time-bin entangled state. In this work, we show how such a high visibility can be reached in order to violate a chained Bell inequality with six, eight, and ten terms.

Contribution

The thesis author performed the theoretical analysis.

Publication E: Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics

Preprint submitted to arXiv on the 5th of April 2016 [57].

Author

Jonathan Jogenfors.

Abstract

The digital currency Bitcoin has had remarkable growth since it was first proposed in 2008. Its distributed nature allows currency transactions without a central authority by using cryptographic methods and a data structure called the blockchain. Imagine that you could run the Bitcoin protocol on a quantum computer. What advantages can be had over classical Bitcoin? This is the question we answer here by introducing Quantum Bitcoin which, among other features, has immediate local verification of transactions. This is a major improvement over classical Bitcoin since we no longer need the computationally-intensive and time-consuming method of recording all transactions in the blockchain. Quantum Bitcoin is the first distributed quantum currency, and this paper introduces the necessary tools including a novel two-stage quantum mining process. In addition, Quantum Bitcoin resist counterfeiting, have fully anonymous and free transactions, and have a smaller footprint than classical Bitcoin.

Contribution

As this is a single-author publication, the thesis author is the sole contributor.

Publication F: Comment on "Franson Interference Generated by a Two-Level System"

This is a comment to a paper by Peiris et al. [58] published by Physical Review Letters (PRL) on the 19th of January 2017. We submitted our comment to arXiv and PRL on the 15th of March 2017 [59]. The comment was not accepted by PRL, but our contribution was acknowledged in the form of an erratum to the original paper published on the 18th of August 2017 [60]. This erratum references our comment and thanks us for bringing the issues to their attention.

Authors

Jonathan Jogenfors, Adán Cabello, and Jan-Åke Larsson.

Abstract

In a recent Letter [Phys. Rev. Lett. 118, 030501 (2017)], Peiris, Konthasinghe, and Muller report a Franson interferometry experiment using pairs of photons generated from a two-level semiconductor quantum dot. The authors report a visibility of 66 % and claim that this visibility "goes beyond the classical limit of 50 % and approaches

the limit of violation of Bell's inequalities (70.7 %)." We explain why we do not agree with this last statement and how to fix the problem.

Contribution

The thesis author performed the theoretical analysis and wrote the comment.

Chapter 2

Basic Concepts

The battle between cryptology and cryptanalysis has largely played out within the field of mathematics. Quantum mechanics, whose laws have been discovered through experiment and theory, has led to significant developments in modern society. In order to understand QKD, one needs to know its mathematical foundations and how they apply to our purposes of securing communications. This chapter will present the notation used in the rest of the thesis followed by important concepts in linear algebra and probability theory. Then we move on to discuss a few essential postulates of quantum theory and their implications.

2.1 Linear Algebra

Linear algebra is used in many applied fields, and the wide variety of flavors has led different authors to adapt conflicting standards to how concepts translate into notation. For the rest of this thesis we will work with the vector space $\mathbb{C}^n$ unless otherwise stated. A vector within this space is written $|\psi\rangle$, where the ψ is the actual label of our vector. The entire object is called a *ket*, and its vector dual is the *bra* $\langle\psi|$. This useful bra-ket notation was introduced by Dirac [61] in 1939.

The complex conjugate of z is written z^*. Similarly, the element-wise complex conjugate of a matrix A is A^*. The identity matrix is denoted I, the transpose of a matrix A is A^T and the Hermitian conjugate is $A^\dagger \overset{\text{def}}{=} \left(A^T\right)^*$. Given a vector $|\psi\rangle$, its vector dual $\langle\psi|$ can be computed as the Hermitian conjugate $\langle\psi| = (|\psi\rangle)^\dagger$. This allows us to elegantly write the inner product of two states in the bra-ket notation as $\langle\phi\,|\,\psi\rangle$. We then call an operator A *Hermitian* if it satisfies $A^\dagger = A$.

The inner product is a function that takes two vectors on a Hilbert space $\mathcal{H}$ and produces a complex number. We write this as $(\cdot,\cdot)$: $\mathcal{H}\times\mathcal{H}$ to $\mathbb{C}$. We can write the inner product of two vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ as $\langle\psi_1\,|\,\psi_2\rangle$. Two vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ are said to be *orthogonal* if their inner product is zero.

Of particular interest is a class of maps that are *unitary*, that is, they fulfill

$$UU^\dagger = U^\dagger U = I. \tag{2.1}$$

Later, in Postulate 2.10 we will see that unitary maps play an important role in quantum mechanics. Next, we have an important property of the inner product:

Theorem 2.1 (**Invariance of Inner Product under Unitary Transformation**) *The inner product is invariant under unitary transformation.*

Proof *Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two vectors in a Hilbert space. Then*

$$\left(U|\psi_1\rangle, U|\psi_2\rangle\right) = \langle\psi_1|\,U^\dagger U\,|\psi_2\rangle = \langle\psi_1|\,I\,|\psi_2\rangle = \langle\psi_1\,|\,\psi_2\rangle\,. \tag{2.2}$$

This shows us that the inner product between two vectors does not change if they undergo the same unitary transformation.

2.2 Probability Theory

Next, we need some basic results from probability theory.

Definition 2.2 (**Probability Space**) *Let* Λ *be a sample space,* $\mathcal{F}$ *the corresponding* σ*-algebra, and*

$$P : \mathcal{F} \to [0,1] \tag{2.3}$$

a probability measure. Then $(\Lambda, \mathcal{F}, P)$ *is a* probability space.

Definition 2.3 (**Random Variable**) *Let* $(\Lambda, \mathcal{F}, P)$ *be a probability space and* V *a measurable space. Then if*

$$X : \Lambda \to V \tag{2.4}$$

is a measurable function we call it a random variable *defined on a probability space* $(\Lambda, \mathcal{F}, P)$.

Definition 2.4 (**Expected Value**) *If* X *is an integrable random variable defined on a probability space* $(\Lambda, \mathcal{F}, P)$*, then the expected value of* X*, denoted* $E(X)$*, is defined as the Lebesgue integral*

$$E(X) \overset{\text{def}}{=} \int_{\Lambda} X(\omega) dP(\omega). \tag{2.5}$$

We will sometimes define random variables on *subsets* of Λ. Then, in order for the expectation to be well-defined, we condition the expectation on this subset, which gives us

Definition 2.5 (**Conditional Expectation**) *If* X *is an integrable random variable defined on a set* $\Lambda_X \in \mathcal{F}$ *in a probability space* $(\Lambda, \mathcal{F}, P)$*, we define the* conditional expectation *of* X*, denoted* $E(X|\Lambda_X)$*, as*

$$E(X|\Lambda_X) \overset{\text{def}}{=} \int_{\Lambda_X} X(\omega) \frac{dP(\omega)}{P(\Lambda_X)}. \tag{2.6}$$

2.3 Fundamental Quantum Mechanics

We will now briefly review some important concepts of quantum mechanics. For a more complete description, see the textbook by Nielsen and Chuang [62].

Postulate 2.6 (State Vector) *An isolated physical system is associated with a complex Hilbert space $\mathcal{H}$, known as the* state space. *The system is completely described by its* state vector, *which is a unit vector in the state space of the system.*

The state vector is usually written as the ket vector $|\psi\rangle$. A quantum system whose the state is known exactly is said to be in a *pure state*. Note that Postulate 2.6 only deals with *isolated* systems. If the universe only consisted of isolated systems it would be a very dull place, so we need a way for them to interact. Therefore, the next postulate has to do with measurement:

Postulate 2.7 (Quantum Measurement) *A collection of* measurement operators $\{M_m\}$ *operating on the state space make up a quantum measurement if they satisfy the* completeness relation*:*

$$\sum_m M_m^\dagger M_m = I. \tag{2.7}$$

The index m refers to the possible measurement outcomes, and the probability of observing outcome m from a system with state $|\psi\rangle$ is

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{2.8}$$

We can also identify a special case of measurements where the M_m are orthogonal projectors, i.e., Hermitian. These measurements are called *projective*, and we define a Hermitian operator M with the spectral decomposition

$$M \overset{\text{def}}{=} \sum_m m P_m, \tag{2.9}$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. Equation (2.7) then gives

$$\sum_m P_m = \sum_m M_m^\dagger M_m = I. \tag{2.10}$$

Any quantity measured by a Hermitian operator is called an *observable*, and the eigenvalues m represent the possible outcomes of measuring that observable. It is now easy to compute the expected value of a projective measurement:

$$\begin{aligned} E(M) &= \sum_m m p(m) \\ &= \sum_m m \langle\psi| P_m |\psi\rangle \\ &= \langle\psi| \Big(\sum_m m P_m\Big) |\psi\rangle \\ &= \langle\psi| M |\psi\rangle . \end{aligned} \tag{2.11}$$

Note that, in general, quantum measurements do not commute. In fact, we have the following:

Definition 2.8 (Commutator) *The* commutator *of Hermitian operators A and B is defined as*

$$[A, B] = AB - BA. \tag{2.12}$$

We can now give an important result by Heisenberg [63] relating to the precision of quantum measurements:

Theorem 2.9 (Uncertainty Principle) *Suppose A and B are two Hermitian operators. We then have*

$$\Delta(A)\Delta(B) \geq \frac{1}{2}\big|E\big([A, B]\big)\big|. \tag{2.13}$$

Proof *See Nielsen and Chuang [62, p. 89].*

Theorem 2.9 gives a lower bound to how precisely we can determine two non-commuting observables. For instance, the position and momentum of a particle cannot be determined with certainty. Another important example of a family of non-commuting Hermitian operators are the Pauli matrices:

$$\begin{aligned} \sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \\ \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned} \tag{2.14}$$

The Pauli matrices are all unitary, have eigenvalues −1 and +1, and the corresponding normalized eigenvectors are

$$\begin{aligned} \psi_{x-} &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}, & \psi_{x+} &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \\ \psi_{y-} &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}, & \psi_{y+} &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \\ \psi_{z-} &\overset{\text{def}}{=} \begin{pmatrix}0\\1\end{pmatrix}, & \psi_{z+} &\overset{\text{def}}{=} \begin{pmatrix}1\\0\end{pmatrix}. \end{aligned} \tag{2.15}$$

We can combine quantum systems by using the *tensor product* on their state vectors. The tensor product of the systems $|\psi_1\rangle$ and $|\psi_2\rangle$ is written

$$|\psi_1\rangle \otimes |\psi_2\rangle \overset{\text{def}}{=} |\psi_1\rangle\,|\psi_2\rangle \overset{\text{def}}{=} |\psi_1\psi_2\rangle\,, \tag{2.16}$$

and we will frequently make use of this shorthand notation. An important example of states defined using the tensor product are the four *Bell states*:

$$\begin{aligned} |\Phi^+\rangle &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big), \\ |\Phi^-\rangle &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big), \\ |\Psi^+\rangle &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big), \\ |\Psi^-\rangle &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big), \end{aligned} \tag{2.17}$$

where, for example, $|01\rangle = |0\rangle \otimes |1\rangle$ just like in equation (2.16). Here, the state vectors $|0\rangle$ and $|1\rangle$ make up what we call the *computational basis*:

$$\begin{aligned} |0\rangle &\overset{\text{def}}{=} \begin{pmatrix}0\\1\end{pmatrix} = \psi_{z-}, \\ |1\rangle &\overset{\text{def}}{=} \begin{pmatrix}1\\0\end{pmatrix} = \psi_{z+}. \end{aligned} \tag{2.18}$$

Note the equality with some of the eigenvectors in equation (2.15). We will sometimes refer to the computational basis $\{|0\rangle, |1\rangle\}$ as the *rectilinear basis*, denoted $+$. In contrast, the *diagonal basis* is denoted $\times$, and its basis states $\{|+\rangle, |-\rangle\}$ can be expressed in the computational basis as

$$\begin{aligned} |+\rangle &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \psi_{x+}, \\ |-\rangle &\overset{\text{def}}{=} \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \psi_{x-}. \end{aligned} \tag{2.19}$$

We previously discussed pure states. The opposite of a pure state is a *mixed state*, which is a state consisting of several pure states in a statistical ensemble. We can describe mixed states using a *density matrix*:

$$\rho = \sum_j p_j \, |\psi_j\rangle \langle\psi_j| \, . \tag{2.20}$$

Here, the p_j coefficients are probabilities, i.e., $0 \leq p_j \leq 1$ for all j and they obey $\sum_j p_j = 1$. Finally we deal with how quantum systems evolve over time and use the previously mentioned unitary maps:

Postulate 2.10 (Unitary Evolution) *An isolated quantum system evolves over time by unitary transformation. If the state of a system at a given point in time is $|\psi\rangle$, the state at a later time is $U|\psi\rangle$ where U is a unitary operator that only depends on the start and end times.*

In the classical world we can use measurements to exactly determine the state of a system. A simple example is a flipped coin, where we observe the outcome just by looking at it when it lands. The quantum world, however, is not as straightforward. If we have a collection of possible quantum states $\{\psi_i\}$ and want to distinguish between them, *we can only do this reliably when the states are orthogonal.* To see how orthogonal states are distinguished, we define measurement operators[1] $M_i \stackrel{\text{def}}{=} |\psi_i\rangle\langle\psi_i|$ for all i. We can now see that a state $|\psi_i\rangle$ gives the measurement outcome i with probability $p(i) = \langle\psi_i| M_i |\psi_i\rangle = 1$ because $\langle\psi_i | \psi_i\rangle = 1$. Therefore, we can distinguish between orthogonal states with certainty. Conversely, we have

Theorem 2.11 (**Indistinguishability of Non-Orthogonal States**) *Non-orthogonal states cannot be reliably distinguished*

Proof *Proof by contradiction, adapted from Nielsen and Chuang [62, p. 87]. Suppose $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal, and that it is possible to distinguish between them. When distinguishing between these states we perform a quantum measurement $\{M_m\}$ and get an outcome j. We then use some rule f so that, when the state $|\psi_1\rangle$ was prepared, the probability of measuring j so that $f(j) = 1$ is 1. Similarly, when $|\psi_2\rangle$ was prepared, we have unity probability of measuring j so that $f(j) = 2$. Now define the quantity*

$$E_i \stackrel{\text{def}}{=} \sum_{j:f(j)=i} M_j^\dagger M_j, \tag{2.21}$$

and rewrite the rule function f as

$$\langle\psi_1| E_1 |\psi_1\rangle = 1 \text{ and } \langle\psi_2| E_2 |\psi_2\rangle = 1. \tag{2.22}$$

Using the completeness relation $\sum_i E_i = I$ we see that $\sum_i \langle\psi_1| E_i |\psi_1\rangle = 1$, and together with equation (2.22) we have $\langle\psi_1| E_2 |\psi_1\rangle = 0$, which gives us $\sqrt{E_2}\,|\psi_1\rangle = 0$. We now rewrite $|\psi_2\rangle$ as a linear combination of $|\psi_1\rangle$ and some other state vector $|\phi\rangle$ orthonormal to $|\psi_1\rangle$ in the following way:

$$|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\phi\rangle\,. \tag{2.23}$$

We know that $|\alpha|^2 + |\beta|^2 = 1$, and since $|\psi_1\rangle$ is not orthogonal to $|\psi_2\rangle$ we have $\beta < 1$. We now note that

$$\langle\phi| E_2 |\phi\rangle \leq \sum_i \langle\phi| E_i |\phi\rangle = \langle\phi|\phi\rangle = 1, \tag{2.24}$$

[1] We also need to define an operator M_0 so that the completeness relation is fulfilled, but we skip this part for brevity.

and since $\sqrt{E_2}\,|\psi_2\rangle = \beta\sqrt{E_2}\,|\phi\rangle$ *we get*

$$\langle\psi_2|\,E_2\,|\psi_2\rangle = |\beta|^2\,\langle\phi|\,E_2\,|\phi\rangle \leq |\beta|^2 < 1. \tag{2.25}$$

Note that equation (2.25) is in contradiction to equation (2.22), which states that the probability must be 1.

When non-orthogonal states are measured, there will therefore be a nonzero probability of error. Another important feature of quantum mechanics is the *no-cloning theorem*:

Theorem 2.12 (No-Cloning Theorem) *It is impossible to make a copy of an unknown quantum state.*

The following proof is adapted from Nielsen and Chuang [62, p. 532]:

Proof *Assume cloning is possible. We can then build a quantum machine that performs quantum cloning and has one input and one output slot. We put an unknown, but pure, state* $|\psi\rangle$ *into the input slot, and the machine copies this state into the output slot. The output slot of the machine is in some state* $|\chi\rangle$ *just before the cloning process starts. We write this as*

$$|\psi\rangle \otimes |\chi\rangle\,. \tag{2.26}$$

We now let this system evolve unitarily according to Postulate 2.10, which gives us

$$U\big(|\psi\rangle \otimes |\chi\rangle\big) = |\psi\rangle \otimes |\psi\rangle\,. \tag{2.27}$$

In particular, we assume that this general machine copies two pure states $|\psi\rangle$ *and* $|\phi\rangle$*:*

$$\begin{aligned} U\big(|\psi\rangle \otimes |\chi\rangle\big) &= |\psi\rangle \otimes |\psi\rangle\,, \\ U\big(|\phi\rangle \otimes |\chi\rangle\big) &= |\phi\rangle \otimes |\phi\rangle\,. \end{aligned} \tag{2.28}$$

Theorem 2.1 now allows us to compute the following inner product:

$$\begin{aligned} \langle\phi\,|\,\psi\rangle &= \big(\langle\phi| \otimes \langle\chi|\big)\big(\langle\psi| \otimes \langle\chi|\big) \\ &= \big(\langle\phi| \otimes \langle\phi|\big)\big(\langle\psi| \otimes \langle\psi|\big) = \big(\langle\phi\,|\,\psi\rangle\big)^2. \end{aligned} \tag{2.29}$$

The only solutions in $\mathbb{C}$ *are* $\langle \phi \,|\, \psi \rangle = 0$ *and* $\langle \phi \,|\, \psi \rangle = 1$. *Since a state vector always has length 1 it, follows that the only time it is possible to clone an unknown quantum state is when they are equal or orthogonal.*

See section 9.4 for historical notes on the no-cloning theorem. Quantum mechanics therefore only allows *measurement outcomes* to be copied, not general states. This will be important for a QKD system since Eve is prevented from copying the quantum channel.

Chapter 3

Quantum Key Distribution

> One fine afternoon in late October 1979, I was swimming at the beach of a posh hotel in San Juan, Puerto Rico. Imagine my surprise when this complete stranger swims up to me and starts telling me, without apparent provocation on my part, how to use quantum mechanics to design unforgeable banknotes! This was probably the most bizarre, and certainly the most magical, moment in my professional life. [...] Thus was born a wonderful collaboration that was to spin out [...] quantum cryptography.
>
> — Gilles Brassard, 2005 [64]

As with many other advances in science, the discovery of QKD begins with a good story. Five years before they would publish their seminal paper that created the field of quantum cryptography [65], Charles Bennett and Gilles Brassard met while swimming in the Atlantic Ocean outside of San Juan, and they started thinking about encoding information sent between Alice and Bob onto polarized photons. This could prevent Eve from intercepting their message since a quantum system cannot be measured without affecting the state, likely in the form of noise. They realized that this noise would then be detected by Alice and Bob, and they could take appropriate actions to protect their secrets. This mechanism of using quantum mechanics to transfer information could be used to generate a key for an OTP session.

As shown in chapter 1, OTP is only as secure as its method for distributing the key. Now follows the motivation for QKD in general and this thesis in particular: A quantum system together with OTP can provide Alice and Bob with a *provably secure* method of generating a secret key. Combined with the *provably secure* OTP, the result is a *provably secure* communication method.

We will discuss QKD protocols where Alice and Bob want to communicate without leaking information to Eve. They share a device for communication, which in this thesis is called an *interferometer*. At each end of this device, Alice and Bob each have an apparatus for performing measurements on the quantum state, and this will be called their respective *analysis stations*.

In addition to the quantum channel, Alice and Bob need an authenticated classical channel to discuss basis choices and perform OTP encryption after the quantum transmission is complete. This channel is public, and any transmission is assumed to be known to Eve. However, since the channel is authenticated, Eve will not be able to perform a man-in-the-middle attack. Note that the authentication scheme needs unconditional security, and a suitable scheme is Wegman-Carter Authentication (WCA) [66], which requires Alice and Bob to have a pre-shared, secret key. Traditional, “non-unconditionally secure” authentication methods such as ECDSA, only require a constant amount of key which can be used for authenticating any amount of data. In comparison, WCA requires at least $\log N$ bits of key for authenticating a message of length N. However, as a QKD protocol produces secret key bits by itself, the initial pre-shared key can be used for authenticating the initial protocol steps. Next, the logarithmic key consumption of WCA allows the QKD protocol to be self-sustaining.

The QKD protocols discussed in this thesis fall into two general categories: *prepare-and-measure* and *entanglement-based*. In a prepare-and-measure scheme, Alice prepares a quantum state and sends it to Bob who then makes an appropriate measurement.

The entanglement-based protocol is slightly more complex. In addition to Alice's and Bob's analysis stations there is a source device responsible for generating the quantum states. Some examples of entanglement-based protocols is Ekert's E91 protocol (see section 4.4) and designs based on the Franson interferometer (see section 6.1). In addition to the above protocols, notable proposals are Coherent One-Way (COW) [67], Differential Phase-Shift (DPS) [68], and Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) [69].

3.1 The BB84 Protocol

The first published QKD protocol was BB84, named after the inventors Charles Bennett and Gilles Brassard, and the year it was first published in print, 1984 [64]. BB84 is a prepare-and-measure protocol, and the qubits are individual polarized photons. The following description of the protocol is adapted from the textbook of Nielsen and Chuang [62, pp. 587–588].

In the preparation phase, Alice prepares photons, each polarized along an angle chosen uniformly at random from the angles corresponding to basis states of the rectilinear and diagonal bases defined in equations (2.18) and (2.19):

$$|\psi_{00}\rangle \overset{\text{def}}{=} |0\rangle\,, \qquad |\psi_{10}\rangle \overset{\text{def}}{=} |1\rangle\,, \tag{3.1}$$

$$|\psi_{01}\rangle \overset{\text{def}}{=} |+\rangle\,, \qquad |\psi_{11}\rangle \overset{\text{def}}{=} |-\rangle\,. \tag{3.2}$$

For each state $|\psi_{ij}\rangle$, i is the bit value and j represents the basis in which the photon is polarized (rectilinear + or diagonal ×). Again, the basis states coincide with the eigenvectors of the Pauli matrices σ_x and σ_z in equation (2.15).

Since the states in equation (3.1) are not pairwise orthogonal they cannot be distinguished by quantum measurements (recall theorem 2.11). Now let δ be an integer ≥ 0. Alice randomly generates two secret bit strings a and b, each of length $(4 + \delta)n$. Next, she prepares the quantum state

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} \left|\psi_{a_k b_k}\right\rangle, \tag{3.3}$$

where the subscript k is the k^{th} bit of the strings. The resulting state $|\psi\rangle$ is the tensor product of the base states in equation (3.1). Now Alice sends $|\psi\rangle$ over the quantum channel to Bob. He will receive the state, possibly affected by noise and Eve, announces this to Alice over the public channel, and randomly generates a bit string b' of his own, again of length $(4+\delta)n$.

Bob performs quantum measurements on his received state according to these random bits. If the bit value is 0, he measures σ_X and if it is 1 he measures σ_Z. The measurement result will in every case be either 0 or 1, and Bob stores this data in a new bit string a'. At this point, Alice and Bob have gathered what is called the *raw key*. This raw key needs to be processed and analyzed in several steps before it can be used to encrypt the message. Bob tells Alice over a public channel that he has performed his quantum measurements, and Alice then broadcasts her basis choices b. Bob also broadcasts his basis choices b'. It might seem peculiar that Alice broadcasts her measurement settings. Could this not be used by Eve to gather the raw key? The answer is no, because she does not hold a faithful copy of the quantum state thanks to the no-cloning theorem. The basis information will not help her gain information about the key.

The next stage of the protocol is *sifting*. Alice and Bob compare basis choices, and wherever $b \neq b'$ (different bases) they discard the corresponding key bits from a and a'. On average, half of the key will be discarded in this step and the result is the *sifted key*. We assume that δ is sufficiently large so that with high probability, the sifted key is at least $2n$ bits long.

Alice's and Bob's sifted keys have an important property: they are equal between Alice and Bob, assuming no influence of noise or Eve. In theory, this could already be used to perform OTP encryption as the sifted key (nearly) has all three properties we

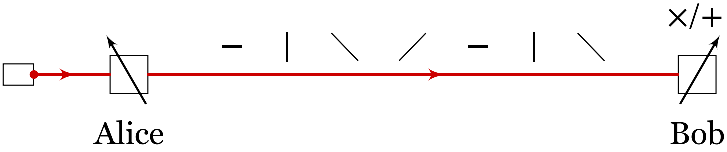


Figure 3.1: The BB84 QKD protocol. This is a prepare-and-measure QKD protocol, where Alice encodes information using photons polarized in non-orthogonal bases. Bob randomly chooses from two measurement settings.

required in section 1.4: It is randomly generated, never reused (a new key bit can be created for every bit of data to be sent), and (nearly) secret. The rest of the protocol is dedicated to improving the secrecy of the key and shut Eve out of the loop.

Still assuming that the sifted key is $2n$ bits long, Alice and Bob agree on a subset of n of these bits, broadcast them and compare values. If more than a predetermined proportion of these *check bits* disagree, they abort their transmission. Either Eve is present or there was noise on the channel, however there is no way of distinguishing between these possibilities. It can be shown [62, p. 602] that a necessary condition for security is an error rate below 11 %. To be precise, this limit is on the error rate *after* two more steps of the protocol, *information reconciliation* and *privacy amplification*. These steps are important for the security of the protocol, however a detailed discussion is beyond the scope of this thesis. Instead we refer to Abidin [70], which also discusses the authentication step and its key consumption.

The BB84 protocol thus allows Alice and Bob to agree on a secret key usable in an OTP session. Any attempt by Eve to eavesdrop will be noticed by Alice and Bob who then abort the protocol. There is no way for Eve to learn the value of the key, and due to the provable security of the OTP, the QKD session is perfectly secure. Of course, Eve could perform a Denial of Service (DoS) attack by cutting or sabotaging the quantum channel, but such an attack will not give her any information about the message.

We have now given a short description of the BB84 protocol. Again, this is a prepare-and-measure setup, so Alice and Bob must establish a hierarchy of who is the sender and who is the receiver. The situation will be different in the entanglement-based protocols such as E91 (shown in section 4.4), and protocols based on the Franson interferometer (section 6.1). These two new protocols instead rely on a violation of the *Bell inequality* for security, a concept we will introduce in chapter 4.

3.2 Security Analysis of BB84

Bennett and Brassard [65] originally proved the security of BB84 against a number of attacks, similar to our discussion in the previous section. However, unconditional security is much more stringent and requires a proof of security against *any* attacker restricted only by the laws of physics. This section will discuss security proofs of BB84.

The first full proof is by Mayers [71] (the first version of which appeared in 1996). This proof is relatively complex (the paper is 56 pages long) and assumes Alice's source to be perfect, but places no constraints on Bob's detector [72]. Later, Koashi and Preskill [73] proved security under the converse condition, i.e., Bob's detector being perfect and no constraint on the source as long as Alice's basis choice does not leak to Eve.

In 1999, Lo and Chau [74] proved the security even when the quantum channel is noisy, however this proof assumes fault-tolerant quantum computers. The proof by Lo and Chau is based on previous observations by Bennett et al. [75] and Deutsch et al. [76], both published in 1996. In 2000, Shor and Preskill [77] proved the security in a new way, this time basing it on the theory of quantum error correction and the proof by Lo and Chau [74]. This proof is relatively simple compared to previous works, but still makes assumptions on source and detector flaws [78].

Note the assumptions on perfect or almost perfect devices in the above security proofs. Alice and Bob therefore must rely on their device to function correctly at all times in order to achieve unconditional security. This has severe implications for the security as will be discussed in section 4.5.

Chapter 4

Bell's Theorem

> The experimental verification of violations of Bell's inequality for randomly set measurements at space-like separation is the most astonishing result in the history of physics.
>
> — Tim Maudlin, 2014 [79]

Bell's Theorem [80] is of considerable importance when trying to understand the very fundamentals of quantum mechanics. The theorem has consequences not only for physics, but also leads to consequences for philosophical interpretations of reality. The ideas presented in this chapter do in some sense go against human intuition because we will have to abandon the ideas of "locality" and "realism". In 1975, Stapp [81, p. 271] claimed that "Bell's theorem is the most profound discovery of science".

4.1 EPR and Hidden Variables

In 1935, the early days of quantum mechanics, Einstein, Podolsky, and Rosen (EPR) published a paper [82] where they asked if quantum mechanics could be considered complete. In the paper, they started with a few basic assumptions and used the laws of quantum mechanics to produce an apparent contradiction. The argument, which will be presented now, is sometimes referred to as the "EPR paradox".

Here, we show a later modification of the EPR paradox described by Bohm [83] in 1951. Recall the Bell state $|\Psi^-\rangle$ defined in equation (2.17):

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big). \tag{4.1}$$

Again, $|01\rangle$ is the tensor product of the computational basis states $|0\rangle$ and $|1\rangle$. The Bell state in equation (4.1) can be experimentally realized in several ways, but we will consider π meson decay. The π meson (also called pion) is a subatomic particle that can decay in several ways. One such way is

$$\pi^0 \to \gamma_0 + e^- + e^+, \tag{4.2}$$

where the decay products are one gamma photon γ_0, one electron e^- and one positron e^+.

If we require the π meson to be at rest, it will have zero angular momentum and according to the law of conversation of angular momentum, the sum of the angular momenta of the particles on the left-hand side of equation (4.2) must be zero as well. A photon has zero angular momentum and therefore the electron and positron will have opposite spin. These particles, whose intrinsic spin always takes on the values $\pm\hbar/2$, will have two possible configurations: one where the positive spin component is given to the positron and one where it is given to the electron. We write this as $e^+ \uparrow$ and $e^- \downarrow$, or conversely, $e^+ \downarrow$ and $e^- \uparrow$. The basis states are then $|\uparrow\rangle$ and $|\downarrow\rangle$ and the system will be in the state

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle_{e-} \otimes |\downarrow\rangle_{e+} - |\downarrow\rangle_{e-} \otimes |\uparrow\rangle_{e+}), \tag{4.3}$$

which coincides with the Bell state $|\Psi^-\rangle$ defined in equation (2.17) if we let $|\uparrow\rangle = |0\rangle$ and $|\downarrow\rangle = |1\rangle$ for both the electron and positron.

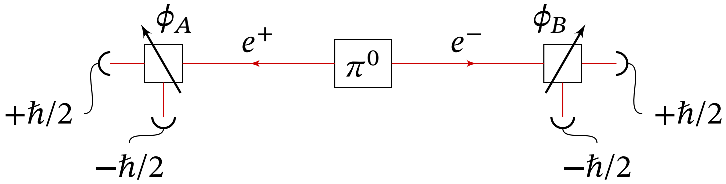


Figure 4.1: The EPR-Bohm thought experiment. A π meson decays into a positron and electron with opposite spin, and these particles are measured by Alice and Bob. The spin of the two particles is opposite to each other, so Alice and Bob's measurement outcomes will be anti-correlated.

Now EPR present their argument. Let the electron-positron pair carefully move very far away from each other in a way that retains their angular momenta (figure 4.1). Alice receives the positron and Bob the electron, and if Alice measures the spin of her positron along the z axis she will get either the result $+\hbar/2$ or $-\hbar/2$. Spin can be measured along different axes, and according to the uncertainty principle in theorem 2.9, the spin along orthogonal axes cannot be determined with certainty. Therefore, it is not possible to precisely know the spin along the z and x axes simultaneously.

Now Bob can act independently of Alice and measure the spin of his electron along the x axis. But from equation (4.2) this means Bob can predict the spin of Alice's electron along the x axis since it will be the opposite of what he measured. If Alice and Bob perform their measurements simultaneously, it will be possible to know the spin of Alice's positron along two orthogonal axes with certainty, a violation of the uncertainty principle. Therefore, according to EPR, one of the following must be true:

1. The particles are exchanging information faster than the speed of light, or

2. The behavior of the particles is not predetermined by some "hidden variables".

The first possibility of instantaneous information exchange was rejected by EPR as it would violate the "principle of locality". In a later paper, Einstein wrote [84]

> The following idea characterises the relative independence of objects far apart in space, A and B: external influence on A has no direct influence on B; this is known as the Principle of Local Action[1], which is used consistently only in field theory. If this axiom were to be completely abolished, the idea of the existence of quasienclosed systems, and thereby the postulation of laws which can be checked empirically in the accepted sense, would become impossible.

EPR therefore concluded that the principle of locality should apply to their thought experiment and therefore rejected the idea of "spooky action at a distance" [82]. The logical consequence of this line of thought is that quantum mechanics is somehow incomplete, since the state vectors do not give a complete description of the individual particles. But if the state vectors are not a complete description, we are in violation of Postulate 2.6, which asserts that an isolated quantum system *is* described by its state. Per the previous discussion, the logical conclusion must be that there exist some kind of *hidden variables*, unavailable to the experimenter that determine the measurement outcomes according to some pre-determined formula. Baggott [85, p. 107] defines hidden variables in the following way:

> Any theory which rationalizes the behaviour of a system in terms of parameters that are for some reason inaccessible to experiment is a hidden variable theory.

Hidden variable theories have had extraordinary success in the history of science. For instance, the relation between the volume, pressure and temperature of a gas is very complicated, but when taking the individual atoms into account these properties emerge

[1] The modern term for this principle is Locality.

naturally from statistical mechanics. In the case of the gas, the atoms are the hidden variables. Therefore it was no big leap of imagination for EPR to assume that the resolution of their paradox would come in terms of some hidden variable carried by the particles.

The existence of hidden variables could imply the existence of deeper, more fundamental laws of physics than quantum mechanics. According to Baggott [85, p. 140], Einstein had “hinted at a statistical interpretation” in a similar spirit to the emergent gas properties we just described. Perhaps such a theory would allow for a universe where outcomes are deterministic in contrast to the quantum-mechanical laws? In any case, hidden variables are a problem for our goals of secure QKD since it could open up the possibility for cloning unknown quantum states. With cloning, Eve can make copies of the qubit sent between Alice and Bob and then measure the copies in any base she wants. When they announce the measurement bases, she can select the correct measurement outcomes and then she has the key.

4.2 Intuitive Explanation

> Anyone who is not shocked by quantum theory has not understood it.
>
> — Niels Bohr, 1934 [86]

No real solution to the EPR paradox was found up in the decades following the EPR paper. It took until 1964 when Bell published his celebrated theorem [80], which puts limits on what correlations can be achieved by hidden-variable theories. Bell’s contribution was to show that Nature experimentally invalidates EPR’s view of the world [62, p. 114]. We will now present another thought experiment, the second so far in this chapter. The current thought experiment will show how quantum mechanics goes against “common sense” and is adapted from the textbook by Nielsen and Chuang [62, pp. 114–117].

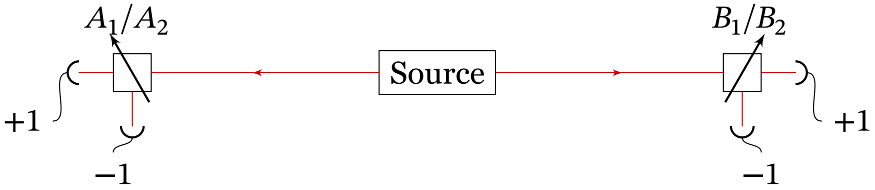


Figure 4.2: A simple thought experiment for deriving Bell's inequality. Alice and Bob each randomly choose between two measurement settings for each trial, and they then compute the correlation of their outcomes.

Similar to the EPR experiment in section 4.1, Alice and Bob each have an analysis station, which receives particles from a source. The source prepares pairs of particles and sends one to Alice and one to Bob. Alice has a choice of two settings for her analysis station, either measure some properties A_1 or A_2 while Bob can measure some properties B_1 or B_2. For example, we can choose to measure spin along two different directions, just like in the EPR example in section 4.1. Note, however, that the reasoning below will be general to *any* choice of measurements that gives outcomes ±1. Alice and Bob randomly determine which of their two respective measurements they perform, but it is important that this choice is done at the last possible instant, i.e., when the particles are received. Otherwise, Alice might be able to see Bob's measurement setting in advance and vice versa. We let Alice and Bob be very far away from each other and arrange the timing so that the measurements are performed simultaneously. Since physical influences cannot propagate faster than light, Alice's measurements cannot influence those made by Bob. The experiment is depicted in figure 4.2.

Continuing the thought experiment, we write down the quantity $|A_1B_1 + A_2B_1| + |A_1B_2 - A_2B_2|$ and perform some algebraic manipulations:

$$|A_1B_1+A_2B_1|+|A_1B_2-A_2B_2| = |(A_1+A_2)B_1|+|(A_1-A_2)B_2|. \quad (4.4)$$

The only possible values for A_1 and A_2 are +1 or −1. Therefore, they are either equal or have opposite signs, so either we have

$(A_1 + A_2)B_1 = 0$ or $(A_1 - A_2)B_2 = 0$. Either way, the only value equation (4.4) can attain is 2. If we also let $p(a_1, a_2, b_1, b_2)$ represent the probability of the particles being in the state $A_1 = a_1$, $A_2 = a_2$, $B_1 = b_1$, and $B_2 = b_2$ before being measured, we calculate the expected value of equation (4.4):

$$\begin{aligned} &E\Big(|A_1B_1 + A_2B_1| + |A_1B_2 - A_2B_2|\Big) \\ &\quad = \sum_{a_1,a_2,b_1,b_2} p(a_1, a_2, b_1, b_2)\Big(|a_1b_1 + a_2b_1| + |a_1b_2 - a_2b_2|\Big) \\ &\quad \leq \sum_{a_1,a_2,b_1,b_2} p(a_1, a_2, b_1, b_2) \times 2 \\ &\quad = 2. \end{aligned} \tag{4.5}$$

Next, we use the linearity of expectation and get

$$\begin{aligned} &E\Big(|A_1B_1 + A_2B_1| + |A_1B_2 - A_2B_2|\Big) \\ &\quad = \Big|E(A_1B_1) + E(A_2B_1)\Big| + \Big|E(A_1B_2) - E(A_2B_2)\Big|, \end{aligned} \tag{4.6}$$

which works because all outcomes are ±1, and if we put inequality (4.5) and equation (4.6) together we obtain the *Bell inequality*

$$\Big|E(A_1B_1) + E(A_2B_1)\Big| + \Big|E(A_1B_2) - E(A_2B_2)\Big| \leq 2. \tag{4.7}$$

The Bell inequality bounds the correlations obtained from any “common-sense” system. Now we ask ourselves what predictions a quantum-mechanical system would give. In this quantum experiment (also depicted in figure 4.2) the source does not prepare classical particles, but qubits. These qubits are in the Bell state defined in equation (2.17) and just like before, one qubit goes to Alice and one to Bob. We now define Alice’s and Bob’s measurement operators in terms of the Pauli matrices introduced in section 2.3:

$$\begin{aligned} A_1 &= \sigma_z, \\ A_2 &= \sigma_x, \\ B_1 &= -\frac{1}{\sqrt{2}}(\sigma_Z + \sigma_X), \\ B_2 &= \frac{1}{\sqrt{2}}(\sigma_Z - \sigma_X). \end{aligned} \tag{4.8}$$

We now compute the expected values of these observables

$$\begin{aligned} E(A_1B_1) &= \frac{1}{\sqrt{2}}, & E(A_2B_1) &= \frac{1}{\sqrt{2}}, \\ E(A_1B_2) &= -\frac{1}{\sqrt{2}}, & E(A_2B_2) &= \frac{1}{\sqrt{2}}, \end{aligned} \tag{4.9}$$

and summing it all up we get

$$\left|E(A_1B_2) + E(A_2B_1)\right| + \left|E(A_1B_2) - E(A_2B_2)\right| = 2\sqrt{2}. \tag{4.10}$$

This is a profound result. Equation (4.10) is larger than the bound in inequality (4.7) [62, pp. 114–117] and it would appear that quantum mechanics is in contradiction with the "common-sense" rules we previously defined. How is this possible? Surely every step of our previous thought experiment was correct, right? We have to scrutinize our intuition of "common sense" and explicitly write down what we mean by it.

We will find two basic and intuitive ideas [62, p. 117]. So basic and intuitive, in fact, that EPR rather rejected quantum mechanics than forego them. The two ideas, stated informally, are:

1. Physical properties corresponding to the values A_1, A_2, B_1, and B_2 exist no matter if we are observing them or not. This is called *realism*.

2. Alice's measurement does not influence the results of Bob's measurements and vice versa. This is, as we previously saw when discussing EPR, called *locality*.

The next section will give a formal definition of realism and locality and look closely at Bell's Theorem. Then we will discuss the consequences of the theorem and put it to use in QKD.

4.3 The Black Box Model

> I recall that during one walk Einstein suddenly stopped, turned to me and asked whether I really believed that the moon exists only when I look at it. The

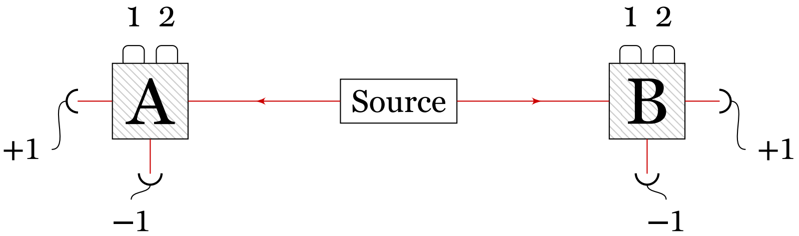


Figure 4.3: The black box model hides the inner workings of the analysis stations and only deals with the measurement settings (two push buttons) and measurement outcomes (+1 or −1).

> rest of this walk was devoted to a discussion of what a physicist should mean by the term "to exist".
>
> — Abraham Pais, 1979 [87, p. 907]

To give a definition of realism and locality, we first begin by abstracting away all device-specific information of the interferometer. By ignoring everything about the design, we can create a formal model for measurements and outcomes, which can be applied to any such setup. The analysis stations will be replaced by *black boxes* as shown in figure 4.3, where the interface consists of the quantum channel, a number of push buttons as input, and an +1 and −1 as output. This *black box model* simplifies the security analysis and will be useful for our discussion of Bell's Theorem.

We use the symbol λ for the hidden variable that can take values in a sample space Λ. We further assume that Λ has a probability P, which induces the expectation value from definition 2.5. Next, we formally define realism and locality:

Definition 4.1 (Realist Systems) *A system is said to be* realist *if the following is true P-almost everywhere: The analysis stations can be described by two families of real-valued random variables. $A_{i,j} : \Lambda \to \mathbb{R}$ is Alice's analysis station and $B_{i,j} : \Lambda \to \mathbb{R}$ is Bob's analysis station. $A_{i,j}$ maps a hidden variable $\lambda \in \Lambda$ to $A_{i,j}(\lambda)$ and similarly $B_{i,j}$ maps $\lambda \in \Lambda$ to $B_{i,j}(\lambda)$.*

Definition 4.2 (Bounded Systems) *A realist system is said to be* bounded *if the absolute values of the outcomes are not greater than 1:*

$$\left|A_{i,j}(\lambda)\right| \leq 1 \qquad \textit{and} \qquad \left|B_{i,j}(\lambda)\right| \leq 1. \tag{4.11}$$

Definition 4.3 (Local Systems) *A realist system is said to be* local *if the following is true P-almost everywhere: Outcomes only depend on the local settings, e.g. for integers $k \neq i$, $l \neq j$ we have*

$$A_{i,j}(\lambda) = A_{i,l}(\lambda) \qquad \textit{and} \qquad B_{i,j}(\lambda) = B_{k,j}(\lambda). \tag{4.12}$$

As a local system only depends on local settings, so the following shorthand is useful and well-defined:

$$A_i \overset{\text{def}}{=} A_{i,j}(\lambda) \qquad \text{and} \qquad B_j \overset{\text{def}}{=} B_{i,j}(\lambda). \tag{4.13}$$

We will often study systems that have all three of the above properties. Therefore the following definition is convenient:

Definition 4.4 (Bounded Local Realist Systems) *A bounded local realist system is a system that fulfills definitions 4.1 to 4.3.*

For the rest of this thesis, all systems are assumed to be bounded, so we will simply refer to these systems as "local realist". Looking back at hidden variables, we see that they (i) are defined as underlying mechanisms that result in a specific outcome, thereby implying realism, and they (ii) only affect the local system, thereby implying locality. This shows that any system described by hidden variables is a local realist system, so we will refer to such systems as "being governed by an Local Hidden Variable (LHV) model".

We now move to the main result of this chapter and present a modified version of Bell's Theorem [80]. This modification is due to Clauser et al. [88] and overcomes the limitation of Bell's original theorem where outcomes are only allowed to have the values +1 and −1. In the literature, this modified inequality is referred to as the Clauser-Horne-Shimony-Holt (CHSH) inequality after the authors, but for clarity we will refer to it as *Bell-CHSH*. Here, we are concerned with the following quantity:

Definition 4.5 (Bell Value) *The Bell value for a system with two settings per observer is defined as*

$$\begin{aligned} S(2) \overset{\text{def}}{=} & \left|E(A_1B_1) + E(A_2B_1)\right| \\ & + \left|E(A_1B_2) - E(A_2B_2)\right|. \end{aligned} \tag{4.14}$$

The reason for this notation will become apparent in section 8.1. Before we give any further information on the behavior of $S(2)$, however, we note the important *algebraic* bound of the Bell value:

Theorem 4.6 (Trivial Bell Value) *Algebraically, the maximum value of the Bell value in equation (4.14) for a bounded system is*

$$S(2)_{\max} = 4. \tag{4.15}$$

Proof *For a bounded system, the absolute values of the outcomes are not greater than 1. As a consequence, the absolute values of the expectations $E(A_iB_j)$ are bounded by 1, and the result follows because there are four such expectations.*

We now present the Bell-CHSH inequality [80, 88]:

Theorem 4.7 (Bell-CHSH) *The Bell value for a local realist system with two settings per observer obeys*

$$S(2) \leq 2. \tag{4.16}$$

Proof *We have essentially given the proof in section 4.2. For a more formal approach, refer to Bell [80] Clauser et al. [88].*

Thanks to the black box formalism we were able to state theorem 4.7 independently of quantum mechanics. What happens if we take a quantum system and compute its Bell value using the predictions of quantum mechanics? Refer again to the discussion in section 4.2, which gives us the following:

Theorem 4.8 (Quantum Prediction of the Bell Value) *Quantum mechanics can produce the Bell value*

$$S_{QM}(2) = 2\sqrt{2}. \tag{4.17}$$

Proof *See section 4.2 and publication A.*

In fact, the value given in theorem 4.8 is an *upper bound* to the Bells value produced by quantum mechanics. This was shown in 1980 by Cirel'son [89], and the bound in equation (4.17) is sometimes referred to as *Cirel'son's bound*.

We note that the quantum prediction in theorem 4.8 violates theorem 4.7. This implies that quantum mechanics is in violation of the Bell-CHSH inequality, or alternatively, that *quantum mechanics violates local realism*. This insight is usually referred to as *Bell's Theorem* and it rules out all LHV descriptions of quantum mechanics. Recall from our discussion in section 4.1 that EPR then argues that we must accept "spooky action at a distance", i.e., the existence of a connection between distant particles that acts faster than the speed of light. Therefore, the paradox of EPR is resolved by letting go of our implicit assumption that Nature behaves in the "common-sense" manner of locality and realism.

From the above reasoning we must conclude that there exists a phenomenon where distant particles form a system that cannot be divided into independent subsystems. This is called *entanglement*. An example of quantum states exhibiting entanglement are the Bell states in equation (2.17), because there exist no states $|\Psi_A\rangle$ and $|\Psi_B\rangle$ so that the tensor product $|\Psi_A\rangle \otimes |\Psi_B\rangle$ equals a Bell state. Conversely, states that *can* be factored in this way are called *separable*. Consider the following:

$$\begin{aligned}&\frac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big)\\ &\quad= \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big).\end{aligned} \tag{4.18}$$

Such a state can be described in terms of its subsystems, and it is therefore separable.

Entanglement is indeed a peculiar phenomenon that has no equivalent in the classical world. The human mind is used to phenomena that are local and realist – which entanglement clearly is not. Nielsen and Chuang write that entanglement can be used to

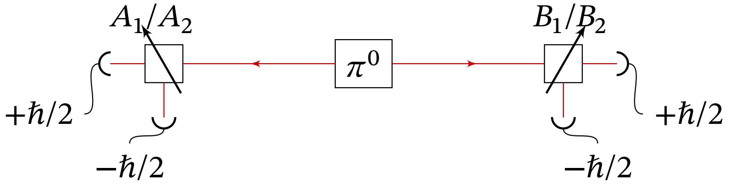


Figure 4.4: The E91 QKD protocol. A π meson decays into two polarization-correlated entangled particles, which are measured along different axes by Alice and Bob. The resulting correlations violate Bell's inequality.

create other peculiar phenomena, such as quantum teleportation and quantum error-correcting codes [62, pp. 25–28], all building blocks for a future quantum computer. We end this section with the following broad outlook:

> Entanglement is a uniquely quantum mechanical *resource* that plays a key role in many of the most interesting applications of quantum computation and quantum information; entanglement is iron to the classical world's bronze age.
>
> — Nielsen and Chuang [62, p. 11]

4.4 Ekert's QKD Protocol

In 1991, Arthur Ekert [90] published a paper that detailed a QKD protocol that uses entanglement. As this discovery was made seven years after BB84, it was not the first QKD protocol, however it was the first protocol based on Bell's Theorem. In addition, Ekert was unaware of the work by Bennett and Brassard [65] so this discovery was made independently of theirs. The protocol is called E91, and in this setting there there is no hierarchy between Alice and Bob. Instead, their roles are very similar and the state preparation task is instead given to a *source device*.

E91 works in a similar way to the EPR thought experiment in section 4.1 and uses the same spin-1/2 particles[2]. We therefore use a π meson as an entanglement source just like EPR, and the setup is depicted in figure 4.4. An important difference to BB84 is that it is not a prepare-and-measure protocol. Instead, we refer to it as a being *entanglement-based*. Interestingly, an eavesdropper cannot gain knowledge about the key from eavesdropping on the channel, as no information is encoded there. In the words of Ekert [90],

> The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards.

This, of course, relies on the impossibility of faster-than-light influences [91]. In addition, more significant attacks are possible such as replacing the source device with a Trojan device of the attacker's own making. This *Trojan-horse attack*, however, will be detected by Alice and Bob when they test for a violation of Bell's inequality. Alice and Bob orient their detectors in order to measure spin in the plane orthogonal to the spin axis. In this plane, Alice chooses measurement angles $A_1 = 0$ and $A_2 = \pi/2$, while Bob chooses $B_1 = \pi/4$ and $B_2 = 3\pi/4$. Again, Alice's and Bob's outcomes are ± 1, so for $1 \leq i, j \leq 2$ we have

$$\begin{aligned} E(A_iB_j) = P(A_i &= +1, B_j = +1) \\ -P(A_i &= -1, B_j = +1) \\ -P(A_i &= +1, B_j = -1) \\ +P(A_i &= -1, B_j = -1), \end{aligned} \tag{4.19}$$

which is the correlation between Alice's and Bob's measurement outcomes when Alice performs measurement A_i and Bob performs B_j. Following the method of Ekert [90] we compute

$$E(A_iB_j) = -\cos(\phi_A - \phi_B), \tag{4.20}$$

[2] It should be noted that while Ekert's original paper called for spin-1/2 particles, experimental realizations have instead used polarized photons as they are easier to handle.

where ϕ_A is the angle along which Alice performs measurement A_i, and ϕ_B is the corresponding angle for Bob's measurement B_j. The four correlations are then identical to those in equation (4.9) so the quantum prediction of the Bell value for the E91 setup is

$$\begin{aligned} S_{QM}(2) = &\left|E(A_1B_1) + E(A_2B_1)\right| \\ &+ \left|E(A_1B_2) - E(A_2B_2)\right| = 2\sqrt{2}, \end{aligned} \tag{4.21}$$

in agreement with theorem 4.8. Alice and Bob now perform a Bell test, i.e., measure the value $S(2)$ and compare it with the bound in theorem 4.7. If there is no violation (i.e., $0 \leq S(2) \leq 2$) Eve might have attempted an attack, and Alice and Bob have to stop communicating. This is the failure state of the Bell test. If they instead have $2 < S(2) \leq 2\sqrt{2}$, the test passes and they can continue with the rest of the protocol. In other words, the Bell test acts as a *security test* that the system must pass before it can be trusted[3].

4.5 Device-Independent QKD

The black box model described in section 4.3 allows the designer of a QKD system to greatly simplify the security analysis. It is a problem in both prepare-and-measure and entanglement-based protocols that some kind of trust must be placed in the source and the analysis stations. What if the analysis station manufacturer is infiltrated by Eve? Who do we trust?

In our discussion of the BB84 protocol in section 3.1, Alice and Bob perform measurements on a random subset of the raw bits and compare these with each other. They will then know [92] whether or not the communication is to be trusted. A full security proof of unconditional security in this scenario, however, requires intimate knowledge of the analysis stations and trust in their manufacturing process. In theory, there *do* exist proofs for QKD being unconditionally secure (section 3.2), however the proofs assume

[3] Note that we have omitted some details in the E91 protocol required to actually produce a secret key.

ideal situations that cannot be achieved in the general experimental case. Scarani [93] describes a number of such complications.

The E91 protocol instead uses a violation of the Bell inequality to certify the system as secure. Instead of having to perform tedious proofs that involve the complicated inner workings of the analysis stations like in BB84, the Bell test *only involves measurement outcomes*. After Ekert's initial publication [90], subsequent works by various authors provided a few more pieces to the puzzle [91, 94] but as Acin et al. [95] points out, these results either did not give the whole picture, nor did they prove the general case with noise. In 2002, Larsson [96] pointed out that non-ideal devices is a serious problem for E91 and explicitly showed how this can be exploited to perform a Trojan-horse attack while still violating the Bell-CHSH inequality. Instead, a breakthrough came with the development of *device-independent* QKD (DI-QKD), a term coined by Acin et al. [95] in 2007. The history of events that led up to this new idea is documented by Scarani [93, pp. 56–58].

DI-QKD takes a step back from traditional QKD and only assumes Eve to be constrained by quantum mechanics. This is a considerable relaxation over traditional QKD protocols thatnot only assumes hostile control of the source, but also of the quantum channel and the analysis stations. To only be constrained by quantum mechanics means Eve can do almost anything she wants with only a few exceptions such as the *no signaling principle*, which forbids communication faster than the speed of light. Acin et al. [95] write:

> The only data available to Alice and Bob to bound Eve's knowledge are the observed relation between the measurement settings and outcomes, without any assumption on how the measurements are actually carried out or on what system they operate.

In addition to the above security assumption of Eve obeying the laws of quantum mechanics, Alice and Bob are also assumed to be free to choose secret measurement settings, and that the outcomes they measure are kept secret [95]. Usually, these two last assumptions are referred to as saying that “no information should leak out of Alice’s and Bob’s laboratories”. It is also important that their measurement settings are random, i.e., unpredictable by Eve, which means that settings must be decided by a Random Number Generator (RNG). Two approaches are possible here, either a Pseudo-Random Number Generator (PRNG), which is a deterministic algorithm which generates random numbers using an initial *seed*, or a True Random Number Generator (TRNG), which generates truly random numbers. An important type of TRNG is the Quantum Random Number Generator (QRNG), which generates true randomness by observing some quantum phenomenon.

It is important to note that a QKD protocol must rely on a Bell inequality violation in order to function with DI security assumptions. To illustrate this, we study an entanglement-based variant of BB84 and follow an example adapted from Pironio et al. [92]. This modified BB84 protocol produces only the outcomes $+1$ and -1 in a similar way to E91. Alice and Bob perform measurements on a quantum system, and they randomly choose between measurement operators A_1, A_2, B_1, and B_2 in the usual way. Here, A_1 and B_1 measure σ_x while A_2 and B_2 measure σ_z.

Suppose now that Alice and Bob observe perfectly correlated outcomes if their measurement settings agree, and uncorrelated, random outcomes if they disagree. Rewriting this in Dirac’s bra-ket notation we get

$$\begin{aligned} \langle\psi|\left(\sigma_x \otimes \sigma_x\right)|\psi\rangle = \langle\psi|\left(\sigma_z \otimes \sigma_z\right)|\psi\rangle &= 1, \\ \langle\psi|\left(\sigma_x \otimes \sigma_z\right)|\psi\rangle = \langle\psi|\left(\sigma_z \otimes \sigma_x\right)|\psi\rangle &= 0, \end{aligned} \tag{4.22}$$

and the only state fulfilling the requirements of equation (4.22) is the Bell state $|\Phi^+\rangle$, which allows Alice and Bob to safely extract a secret key without the influence of Eve [92].

However, if the same protocol is used with the relaxed security assumptions of DI-QKD, Alice and Bob will have a problem. They can no longer assume that their measurement operators correspond to the previously defined Pauli matrices, nor do they know *what state is actually being measured upon.* Remember that DI security assumptions assume the devices to be under hostile control. With the conditions favoring her this time, Eve hijacks the source device and modifies it so it produces a state consisting of four qubits [97] described by the following density matrix:

$$\rho = \frac{1}{4}\Big(|00\rangle\langle 00|_z + |11\rangle\langle 11|_x\Big) \otimes \Big(|00\rangle\langle 00|_x + |11\rangle\langle 11|_z\Big). \quad (4.23)$$

Eve sends the first and third qubits to Alice, and the second and fourth to Bob. They perform the measurements A_1, A_2, B_1, and B_2, however as Eve manufactured their devices, they do not what measurements are actually performed. In any way, they find correlations in agreement with equation (4.22), even though they no longer measure a Bell state. In fact, equation (4.23) is a *separable* state, which means that Eve can learn the secret key if Alice and Bob were to extract it [92, 97]. Specifically, Eve was able to fool Alice and Bob into using a higher-dimensional system than they expected, because the DI security assumptions do not guarantee the dimensionality of the underlying system.

If a suitable protocol is used, DI-QKD *does* work because any state producing the Bell value $2\sqrt{2}$ is a Bell state or a state isomorphic to it [98]. In the words of Pironio et al. [92], non-locality is "the physical principle on which all DI security proofs are based". Indeed, the security assumptions of DI-QKD only work for protocols that violate Bell's inequality, and BB84 is not such a protocol.

An important fact about Bell's Theorem is its independence from the underlying description of the universe. The derivation in section 4.2 only assumes locality and realism, so the Bell inequality applies to *any* "common-sense" system with remote correlations. We only invoke quantum mechanics when we show that *quantum mechanics is in violation of it.* Analyzing the Bell value does not involve thinking about "paths in an interferometer", "Hilbert spaces", "photons" and so on. Therefore, if the measurement outcomes of a QKD system violates the Bell inequality, it follows that the state is *not classical* and the corresponding QKD system can be certified as secure (bar any loopholes that will be discussed in the next chapter).

We can conclude that DI-QKD allows Alice and Bob to use Bell's inequality as a *security test* for a whole QKD system without requiring trust in either the source, quantum channels, or the analysis stations. As long as they are free to secretly choose settings for their analysis station and observe a violation of Bell's inequality, they can rule out the presence of Eve.

Chapter 5

Loopholes in Bell Experiments

> But power supplies make noise, *and not the same noise for the different voltages needed for different polarizations*. So, we could literally hear the photons as they flew, and zeroes and ones made different noises. Thus, our prototype was unconditionally secure *against any eavesdropper who happened to be deaf!*
>
> — Gilles Brassard, 2005 [64, p. 20]

The theory of DI-QKD is appealing due to its elegance and simplicity. In theory, the Bell test works thanks to Bell's Theorem: no LHV model can mimic Alice's and Bob's measurement outcomes if they measured a quantum system. In practice, however, there will be complications introduced by the reality of performing delicate physical experiments in the real world. The above story told by Gilles Brassard highlights such a reality, where the sound made by the power supplies controlling the polarizers leaked information about the setting.

In section 4.5 we stated one of the requirements of DI-QKD — secrecy of setting. If Eve learns the settings Alice and Bob choose for the trials (i.e., which button is pressed in the black-box model of figure 4.3), she can hijack the quantum channel and send tailored signals to the analysis stations. If done correctly, such an attack allows Eve to prescribe the measurement outcomes, and therefore lets her *fake* a Bell value that violates the Bell-CHSH inequality even though the system is classical, i.e., local realist. If Alice and Bob are attempting QKD, Eve will also know Alice's and Bob's secret key!

Analysis stations that leak setting information therefore break the security of QKD by allowing LHV models to produce Bell values in violation of theorem 4.7. Such an undesired condition is called a *loophole*, and there are many different ways in which a Bell test can be subverted. The situation described by Gilles Brassard in the introduction to this chapter is an example of the *locality loophole*, where the noise is a so-called *side-channel* that leaks the setting to Eve. Again, the black-box model assumes Alice and Bob to be able to *secretly* choose measurement settings, and noisy power supplies breaks this assumption.

Even worse, the black box model fails even in the absence of an intentional attacker. The mere hypothetical *possibility* of source emissions being affected by the measurement settings is enough to invalidate the experiment. While we have no model to describe how Nature would tailor the source emissions, we do not want to assume that Nature behaves in a certain way. Rather, we want to test the Bell inequality in an experiment where the no-signaling principle light rules out communication from the analysis station to the source. By eliminating the locality loophole, we rule out both intentional attackers, and tricks played by Nature herself.

A sufficient condition for closing the locality loophole is to spatially separate the event of choosing the measurement setting from the source device. If the separation is large enough, the emission event of the source is outside of the forward light cone of the setting choice. This way, any signal travelling from the analysis station to the source will arrive after the source emission has occurred. The rest of this chapter will discuss a number of loopholes that affect the interpretation of Bell experiments.

5.1 The Detection Loophole

> Closing the locality loophole needs a system that is easy to transport while keeping entanglement intact. The system of choice is photons, and photon detectors are inefficient—more accurately, photon correlation experiments are inefficient.
>
> — Jan-Åke Larsson, 2014 [99, p. 16]

The first study of a loophole in the context of Bell's Theorem was made in 1970, when Pearle [100] realized that an ostensible violation of the Bell-CHSH inequality can be fabricated from a local realist system. Pearle discovered that by carefully excluding some of the events from being counted towards the Bell value, it can be artificially inflated. Pearle's example shows that care must be taken whenever implementing a Bell test as losing too many events causes a "fake" violation. This loophole, the *detection loophole*, is an inherent problem in any experimental Bell test as optical fibers, beam splitters, and detectors have inherent losses. If losses are too high, the experimenter must make the *fair-sampling assumption*: that the statistical distribution of lost events is identical to those that *are* detected. This is a dangerous assumption to make as there is no way of proving its correctness, possibly opening up the system to attack. In some cases, the experimental design itself causes losses even when using ideal components, as will be shown in the case of the Franson interferometer in section 6.1.

Whenever we are dealing with a lossy system, the losses must be quantified and studied. Next, we must find an upper bound to the losses, i.e. when does the quantum-mechanical prediction in equation (4.17) no longer violate the bound in theorem 4.7? This question was formally answered by Larsson [101] and models non-detections as the random variables A and B being *undefined* at the respective points in Λ. Consequently, we now work on *subspaces* of Λ, and in general these subspaces will not be independent of the measurement settings i and j:

Definition 5.1 (**Subsets of the Sample Space**) *We define Λ_X as the subset of Λ where the random variable X is defined.*

We now use conditional expectations from definition 2.5 to restrict the expected value onto these subsets. This is needed because the expectation values $E(A_iB_j)$ in definition 4.5 are no longer well-defined. Instead, we define new random variables

$$(A_iB_j)(\lambda) \overset{\text{def}}{=} A_i(\lambda) \times B_j(\lambda) \tag{5.1}$$

for $1 \leq i, j \leq 2$, and note that they are defined on $\Lambda_{A_iB_j} \subset \Lambda$.

We now give the Bell value for a system under the influence of detector losses. Therefore, we modify definition 4.5 by replacing all $E(A_iB_j)$ with expectation values conditioned on subsets of Λ where A and B are defined, i.e., $E(A_iB_j|\Lambda_{A_iB_j})$. We then get

Definition 5.2 (**Bell Value, Conditioned on Coincidence**) *The Bell value for a system with two settings per observer is defined as*

$$\begin{aligned} S_C(2) \overset{\text{def}}{=} &\left|E\left(A_1B_1|\Lambda_{A_1B_1}\right) + E\left(A_2B_1|\Lambda_{A_2B_1}\right)\right| \\ &+ \left|E\left(A_1B_2|\Lambda_{A_1B_2}\right) - E\left(A_2B_2|\Lambda_{A_2B_2}\right)\right|. \end{aligned} \tag{5.2}$$

if only coincident events are considered.

Note that definition 5.2 coincides with definition 4.5 if the random variables A and B are defined for all $\lambda \in \Lambda$.

Our new framework allows us to take non-detections into account and therefore is more flexible than our previous definitions in section 4.3. Next, we quantify the non-detections using conditional probabilities and adopt the notation of Cabello et al. [102]:

Definition 5.3 (**Detection Efficiency**) *The detection efficiencies at the individual analysis stations are*

$$\begin{aligned} \eta_A &\overset{\text{def}}{=} \min_{i,j,k,l} P\left(\Lambda_{A_{i,k}}|\Lambda_{B_{l,j}}\right), \\ \eta_B &\overset{\text{def}}{=} \min_{i,j,k,l} P\left(\Lambda_{B_{l,j}}|\Lambda_{A_{i,k}}\right), \end{aligned} \tag{5.3}$$

and the overall efficiency is

$$\eta \overset{\text{def}}{=} \min \eta_A, \eta_B. \tag{5.4}$$

Note that when we define $\Lambda_{A_iB_j}$ in terms of detection efficiency, it can be factored because detection is a local process:

$$\Lambda_{A_iB_j} = \Lambda_{A_i} \cap \Lambda_{B_j}. \tag{5.5}$$

We now get the following:

Theorem 5.4 (Detection Efficiency for Local Realist Systems) *For local realist systems, definition 5.3 reduces to*

$$\begin{aligned} \eta_A &\overset{\text{def}}{=} \min_{i,j} P\left(\Lambda_{A_i} | \Lambda_{B_j}\right), \\ \eta_B &\overset{\text{def}}{=} \min_{i,j} P\left(\Lambda_{B_j} | \Lambda_{A_i}\right). \end{aligned} \tag{5.6}$$

Proof *Realism implies that measurement outcomes can be described by random variables $A_{i,j}$ and $B_{i,j}$. Definition 4.3 shows that locality implies $\Lambda_{A_{i,j}} = \Lambda_{A_{i,l}}$ and $\Lambda_{B_{i,j}} = \Lambda_{B_{k,l}}$for all $k \neq i$ and $l \neq j$. Therefore, we can drop the j index for the random variable A and the i index for the random variable B.*

The question now is if theorem 4.7 still applies to the Bell value in definition 5.2. The answer is no, because when we attempt to use the proof for theorem 4.7 we quickly run into the following expression:

$$\begin{aligned} &\left|E(A_1B_1) + E(A_2B_1)\right| \\ &= \left| \int_{\Lambda_{A_1B_1}} A_1(\lambda)B_1(\lambda)dP(\lambda) + \int_{\Lambda_{A_2B_1}} A_2(\lambda)B_1(\lambda)dP(\lambda) \right|. \end{aligned} \tag{5.7}$$

The next step is to rewrite the integrals as one, but this cannot be done because $\Lambda_{A_1B_1} \neq \Lambda_{A_2B_1}$ in general. We must therefore generalize theorem 4.7 in order to take these coincident subspaces into account. We have the following result:

Theorem 5.5 (Bell-CHSH with Detection Efficiency) *A local realist system with two settings per observer and detection efficiency* $0 < \eta \leq 1$ *obeys*

$$S_C(2) \leq \frac{4}{\eta} - 2. \tag{5.8}$$

Proof *See Larsson [101].*

In the beginning of this section we noted that the Bell value can be artificially inflated by removing events from the statistical ensemble. Thanks to theorem 5.5 we can now take these losses into account and compare this inflated value with the new bound in inequality (5.8). Importantly, the right-hand side of the inequality goes up as the detection efficiency goes down. For $\eta = 1$ we recover theorem 4.7, but even small losses will have dramatic effects for the interpretation of an experiment.

Let us compare the right-hand value of inequality (5.8) with other bounds previously discussed in section 4.3. First is the trivial, algebraic limit in theorem 4.6. We want to solve the equation where the algebraic maximum $S(2)_{\max}$ in theorem 4.6 coincides with the right-hand-side of inequality (5.8) and solve for η:

$$4 = \frac{4}{\eta} - 2. \tag{5.9}$$

We then get the following:

Remark 5.6 (Trivial Detection Efficiency for Bell-CHSH) *For* $0 < \eta \leq 1$, *equation* (5.9) *has a unique solution in*

$$\eta_{\text{trivial}} \overset{\text{def}}{=} \frac{2}{3} \approx 0.6667. \tag{5.10}$$

In other words, a detection efficiency below 66.67 % will lead to an experiment where it is impossible for $S_C(2)$ to violate inequality (5.8), no matter what physical reality governs our universe.

Of greater importance is the efficiency threshold where the right-hand side of inequality (5.8) coincides with $S_{QM}(2)$ – the prediction of quantum mechanics given in theorem 4.8. We solve the following equation for η:

$$2\sqrt{2} = \frac{4}{\eta} - 2. \tag{5.11}$$

We then get the following:

Remark 5.7 (Critical Detection Efficiency for Bell-CHSH) *For* $0 < \eta \leq 1$, *equation* (5.11) *has a unique solution in*

$$\eta_{\text{critical}} \overset{\text{def}}{=} 2\left(\sqrt{2} - 1\right) \approx 0.8284. \tag{5.12}$$

This is the minimum detection efficiency, below which even the quantum-mechanical prediction does not violate local realism. *Any* experiment that intends to violate the Bell-CHSH inequality without the detection loophole must have a detection efficiency of at least η_{critical}=82.84 %.

Note that there exists an equivalent Bell-type inequality that allows a lower level of detection efficiency than theorem 4.7. The 1974 Clauser-Horne (CH) inequality [103] works down to η_{critical} =2/3≈66.67 % if a non-maximally entangled state is used. The drawback of CH compared to Bell-CHSH is the need to estimate *probabilities*, which is more difficult than simply measuring the correlations $E(A_iB_j)$.

5.2 The Coincidence-Time Loophole

Our rigorous study of the detection loophole gave us the minimum detection efficiency required to close the detection loophole. However, as previously mentioned, there still remain a number of loopholes that can lead to alternate explanations for an ostensible Bell violation. See Larsson [99] for a review of loopholes in Bell experiments.

We next study another important effect that arises in many experiments. The expectations in definitions 4.5 and 5.2 are taken of *products* of random variables, which implies they are to be studied as pairs. In the ideal case this is simple, but most detectors have *dark counts*, a property makes them click even when no input has been given. In addition to dark counts, there are non-detections (compare the detection loophole), and jitter, all of which turns pair-determination into a non-trivial problem.

This practical consideration of Bell testing is compounded by the discovery of Hess and Philipp [104] that there exists a tacit assumption of time invariance in the Bell value, which is not sufficiently motivated. In fact, Hess and Philipp argue that the time of detection can be dependent on the setting of the analysis station.

During an experimental run, Alice's and Bob's detectors record a stream of clicks. These clicks must then be reconciled in order to compute the pairwise expectations $E(A_iB_j)$. A common method is to fix a time window[1] $\Delta\tau$ centered around Alice's click, and a detection event on Bob's side that falls within this window is considered coincident. The larger the window, the better the chance that both detections belonging to a pair are coincident. However, this also increases noise as spurious detections within the window count towards the expectation. Noise is easy to notice, while non-detections happen silently. Therefore, experimenters are usually biased to choose a very small time window as this excludes noise and leads to a larger Bell value.

However, a small time window can also exclude truly coincident events from the Bell measurement. This effect is essentially the same as discussed in section 5.1, where removing events from the statistical ensemble skews the results. In fact, if coincidences are lost, it must be assumed that the output statistics are not affected. This is the "fair-coincidence" assumption [105] and it is argued by Larsson et al. [105] that this assumption has been made, consciously or not, by virtually every reported Bell experiment up to at least 2014.

[1] Commonly, ΔT is the preferred symbol for the time window size, however we use $\Delta\tau$ here in order to prevent confusion with the Franson interferometer time difference in section 6.1.

If an experiment is performed where coincidences are incorrectly assumed to be fair, the measured Bell value can be artificially inflated, which leads to a new loophole, called the *coincidence-time* loophole. Some experimental configurations are more affected than others, for instance Spontaneous Parametric Down-Conversion (SPDC) has a large variance in emission time and must take this loophole into account. Experiments that are optically pulsed [56] or use ion traps [106], however, are generally immune.

A formal treatment of the coincidence-time loophole for the Bell-CHSH inequality was performed by Larsson and Gill [107] in 2004, who treated the lost coincidences in a similar way to the lost detections in section 5.1. Here, Alice's arrival time T^A and Bob's arrival time T^B are random variables that depend on the hidden variable λ:

$$\begin{aligned} T^A_{i,j} : \Lambda &\to \mathbb{R} \\ \lambda &\mapsto T^A_{i,j}(\lambda), \\ T^B_{i,j} : \Lambda &\to \mathbb{R} \\ \lambda &\mapsto T^B_{i,j}(\lambda). \end{aligned} \tag{5.13}$$

Using the time-window approach, a coincidence occurs when the arrival times differ by at most $\Delta\tau$. This allows us to define subsets of Λ as the sets on which Alice's and Bob's measurement settings give coincident outcomes. We define

$$\Lambda_{i,j} \overset{\text{def}}{=} \left\{\lambda : \left|T^A_{i,j}(\lambda) - T^B_{i,j}(\lambda)\right| < \Delta\tau\right\}, \tag{5.14}$$

which allows us to quantify the coincidence probability:

Definition 5.8 (Probability of Coincidence) *The probability of coincidence of a Bell experiment*

$$\gamma \overset{\text{def}}{=} \inf_{i,j} P(\Lambda_{i,j}). \tag{5.15}$$

Note that, in contrast to the detection loophole, the coincidence probability is a *non-local* property of the experiment. In other words, the coincidence probability cannot be determined by Alice and Bob alone; the property applies to the system as a whole. Therefore, the subsets of coincidence probability cannot be factored in a way analogous to equation (5.5).

Next, we modify theorem 4.7 to depend on the coincidence probability. We can reuse definition 5.2 for the Bell value $S_C(2)$ and get [107]

Theorem 5.9 (Bell-CHSH with Coincidence Probability) *A local realist system with two settings per observer and probability of coincidence* $0 < \gamma \leq 1$ *obeys*

$$S_C(2) \leq \frac{6}{\gamma} - 4, \tag{5.16}$$

where $S_C(2)$ *corresponds to the Bell value in definition 5.2.*

Proof *See Larsson and Gill [107].*

Just as for the detection efficiency case, theorem 5.9 reduces to theorem 4.7 when $\gamma = 1$. What bounds can be placed on the coincidence probability? Again, we first compare the left-hand side of inequality (5.16) with the trivial bound in theorem 4.6. The condition is

$$4 = \frac{6}{\gamma} - 4. \tag{5.17}$$

Remark 5.10 (Trivial Coincidence Probability for Bell-CHSH) *For* $0 < \gamma \leq 1$, *equation* (5.17) *has a unique solution in*

$$\gamma_{\text{trivial}} \overset{\text{def}}{=} \frac{3}{4} = 0.75. \tag{5.18}$$

Just like the detection efficiency case, a coincidence probability below 75 % makes it impossible for $S_C(2)$ to violate inequality (5.16), with or without quantum mechanics. Next, we solve the following equation for γ:

$$2\sqrt{2} = \frac{6}{\gamma} - 4. \tag{5.19}$$

Remark 5.11 (Critical Coincidence Probability for Bell-CHSH) *For* $0 < \gamma \leq 1$*, equation* (5.19) *has a unique solution in*

$$\gamma_{\text{critical}} \overset{\text{def}}{=} 3 - \frac{3}{\sqrt{2}} \approx 0.8787. \tag{5.20}$$

Therefore, for the quantum-mechanical prediction to violate local realism, the coincidence probability must be at least 87.87 %.

5.3 Experimental Bell testing

Eight years after Bell's initial paper [80] in 1964, the first preliminary experimental trial of a Bell-type inequality was reported by Freedman and Clauser [108] in 1972. Freedman did not perform a full Bell test, but instead tested Freedman's inequality, a "single-channel" variant that uses only one detector each for Alice and Bob.

In the following years, a number of Bell experiments were reported [109–115], however the results were inconclusive (see section 8.2). It took until the early 1980s and the celebrated three experiments by Alain Aspect's group in Orsay, Paris for the first reasonably convincing indication that Bell's Theorem was indeed true. This was the start of a decades-long hunt for a conclusive test of local realism by a number of research groups worldwide.

The three *Aspect experiments* used a photon source consisting of ^{40}Ca atoms undergoing cascade transitions. The first experiment [116] was similar to that of Freedman and Clauser in that only a single-channel Bell inequality was tested. Here, a violation of nine standard deviations was shown. The second experiment [117] tested the full Bell-CHSH inequality and measured a Bell value of 2.697 ± 0.015. This experiment is interesting because the authors *explicitly* make the fair-coincidence assumption and give a motivation as to why it is applicable. The corresponding coincidence-time loophole was only discovered 22 years later, in 2004 [107]!

The third [118] experiment by Aspect's group was published in 1982, and according to Gilder [119, p. 285], this experiment was so difficult to perform that Aspect put the machinist Gérard Roger on the author list. Importantly, the locality loophole was closed by separating the analysis stations by a spatial distance of 13 m, or 43 ns at the speed of light. However, Alice's and Bob's measurement settings were sinusoidally switched, which allows them to be predicted. In addition, the detection loophole remained open:

> ...the detection efficiency in each channel is well below unity [...] . An advocate of hidden variable theories could then argue that we are not sure that the sample on which the measurement bears, remains the same when the orientations of the polarimeters are changed.
>
> — Alain Aspect, 2002 [120, p. 23]

In 1998, Weihs et al. [121] were able to close the locality loophole by an experiment performed in Innsbruck, Austria. While the detection efficiency was at a mere 5 %, the spatial separation was 400 m, corresponding to a 1.3 µs time window in which measurement settings had to be (and were!) chosen. Notably, settings were chosen randomly using a QRNG in order to make them unpredictable.

The detection loophole was first closed by Rowe et al. [106] in their 2001 experiment where $^9\mathrm{Be}^+$ ions were trapped in a dynamic electrical field trap [122]. As ions are heavy, and therefore much less fragile than photons, a very high detection efficiency was achieved. However, the separation of a mere 3 µm only corresponds to 10 fs at the speed of light, which opens up the locality loophole.

For photons, the detection loophole was finally closed in May of 2013 by Giustina et al. [123]. Similarly, the first closure of the coincidence-time loophole with photons was performed by Christensen et al. [124] in September of 2013. One year later, in

September of 2014, Larsson et al. [105] derived a modified Bell inequality that allowed previous experiments to be analyzed in greater detail. With these new statistical tools it could be seen that also the 2013 experiment by Giustina et al. [123] closed the coincidence-time loophole.

So far, experiments closing one loophole had to make a trade-off that opens up another loophole. Individually, all significant loopholes had been closed in separate experiments, however no individual experiment was able to simultaneously close all at once. This changed in 2015 when three separate groups, Giustina et al. [125], Shalm et al. [126], and Hensen et al. [127] independently verified violations of the Bell-CHSH inequality, free of all significant loopholes. It should be noted that while the results of Hensen et al. were published three months before the other two, that experiment only achieved a p value as high as 3.9 % and thus had a relatively high chance of being a statistical anomaly. In contrast, the p value of Giustina et al. [125] is no greater than 3.74×10^{-31}.

The experiments from 2015 provide near-irrefutable proof that Bell's Theorem is correct, i.e., that quantum mechanics is incompatible with local realism. Only the most exotic of hypotheses remain for an explanation of why these empirical results still should be bounded by a Bell-like inequality.

> Thus, to maintain a local hidden-variable theory in the face of the existing experiments would appear to require belief in a very peculiar conspiracy of nature.
>
> — Anthony James Leggett, 2003 [128, pp. 1469–1470]

This conspiracy described by Leggett is a hypothetical class of theories known as superdeterminism [129]. According to Bell, "...it involves absolute determinism in the universe, the complete absence of free will" [130]. In superdeterminism, all processes that appear random have really been determined back when the universe came into existence. The experimenter did not choose to perform an experiment testing Bell's Theorem — rather, it was fate.

5.4 Conclusions

Bell's Theorem, that no physical theory of local hidden variables can reproduce all of the predictions of quantum mechanics, can be algebraically proven in a few simple steps as we found in section 4.2. However, the delicate nature of qubits made it difficult to find experimental evidence, and it took 51 years for the profound theorem to be confirmed. By simultaneously closing all significant loopholes there is no way to explain the results in any other way than by rejecting local realism. For the purposes of our thesis this is good news as DI-QKD is possible only when the Bell test can distinguish between local realist states and those who are not. In a later chapter, we will push the Bell inequality to the limit by exploring a number of ways to circumvent the security test. This is what we call *quantum hacking*.

Chapter 6

Energy-Time Entanglement

> Even before unconditional security was technically proved, “security based on the laws of physics” became the selling slogan of QKD. [...] Of course, a pause of reflection shows that the statement cannot possibly be as strong as that. For instance, the laws of physics do not prevent someone from reading the outcomes of a detector; however, if the adversary has access to that information, security is clearly compromised! But many people were just carried away by the power of the slogan – fair enough, this does not happen only with QKD.
>
> — Scarani and Kurtsiefer, 2014 [131, p. 28]

Up to this point we have discussed entanglement by means of polarization as seen in the E91 protocol of section 4.4. Even though this method is a viable building block for QKD, we need protocols that are robust not only in a laboratory, but over long distances and in tough conditions as well. Polarization-based protocols have drawbacks because that the degree of polarization through an optical fiber is heavily dependent on environmental factors [132]. Changes in temperature [133], magnetic field [134], and mechanical stress [135] influence the relative polarization as photons travel through the fiber.

In an uncontrolled environment, these changes must be quantified and compensated for. Otherwise, the measurement outcomes for Alice and Bob will drift and give rise to errors in the data. The standard way of correcting polarization drift is through a mechanical stretcher, where an optical fiber is stretched by a piezo-electric device [132]. Unfortunately, this compensator is a device that requires moving parts, and would be complicated and expensive to manufacture and maintain in the field.

In recent years there has been an increase in interest for replacing polarization with a method not requiring expensive compensating equipment. This chapter will discuss one such proposal where the non-commuting observables of energy and time are used instead of non-orthogonal polarization states. This method can be used with entanglement and is therefore called *Energy-Time Entanglement* (ETE). Originally, the idea was unintentionally introduced by Einstein in the clock-in-a-box thought experiment as early as 1930 [85, pp. 94–97, 136]. The thought experiment was intended to find a contradiction in quantum mechanics, but Bohr was famously able to resolve Einstein's riddle by showing that energy and time are non-commuting observables just like position and momentum.

6.1 The Franson Interferometer

The first proposal for a device based on ETE was published in 1989 by Franson [40]. This device, depicted in figure 6.1, consists of the usual parts found in an entanglement-based QKD interferometer: a source and two analysis stations. Franson's original proposal described the source as follows: An excited atom is in a relatively stable high-energy state at time $t = 0$ with a relatively long average lifetime ΔT. A photon is emitted, which brings the atom to a middle level with a short lifetime $\tau_0 \ll \Delta T$. When the atom goes back to the ground state, a second photon is emitted. The atom is

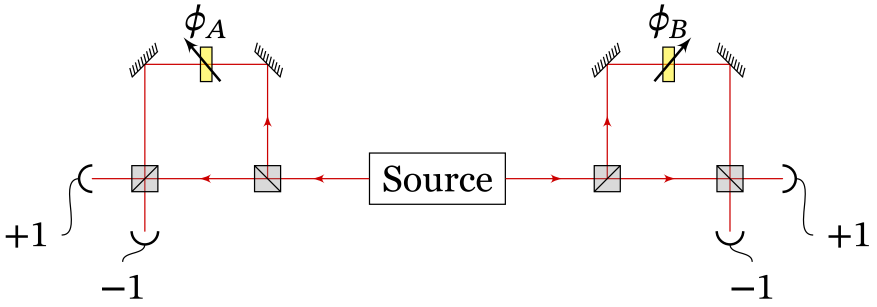


Figure 6.1: The Franson interferometer. The source emits time-correlated photons, which are sent to Alice and Bob. At their respective analysis stations, they perform measurements along angles ϕ_A and ϕ_B, respectively, and record the outcome as well as time of detection.

therefore a three-level system with two photons emitted within a small time window τ_0. The source will therefore emit two photons almost simultaneously, but the *time* of emission is uncertain over a long timescale ΔT.

Alice and Bob each have identical analysis stations consisting of unbalanced Mach-Zehnder (MZ) interferometers, i.e., two optical paths of different length. The upper path is longer than the lower by a path difference $c\Delta T$ and also contains a variable phase modulator (setting) ϕ. The beam is split into the two paths by a 50:50 beam splitter and they are intermixed using another one. The second beam splitter does not combine the beams into one, but has two outputs. Each of these beam splitter outputs is connected to one of the two photodetectors +1 or −1.

This device is referred to as the *Franson interferometer* and Alice and Bob use it in the following way: The three-level atom in the source is excited to the semi-stable high-energy state described above. An unknown moment in time later (standard deviation ΔT), the two photons are emitted and are sent to Alice and Bob, who randomly choose the settings ϕ for their analysis stations.

The path difference of the analysis station results in a possible delay to the photon, and the phase modulator setting ϕ affects the way the paths combine at the second beam splitter. Remember that photons are quantum objects and do not take a specific "path" through the analysis station. At the end of the analysis station the photon is detected by one of the two detectors, resulting in a measurement outcome of +1 or −1. When registering these detections, Alice and Bob also record the *time* at which the detection occurred.

If the detection times at Alice's and Bob's detectors are equal, there is quantum-mechanical interference between the two cases (i) early source emission, photons were delayed by both Alice's and Bob's analysis stations, and (ii) late source emission, neither analysis station caused a delay. Alice and Bob will not know which of the two cases actually occurred, however if there is a detection time mismatch, calculating the emission time is trivial (publication A) and there will be no quantum interference. Alice and Bob must therefore remove all events with differing detection times in order to force interference and this is called *postselection*. On average, postselection discards half of all events.

The photons created at the source have now been measured, and one trial of the Franson interferometer is therefore complete. This process is repeated a number of times, so that Alice and Bob each have a list of measurement outcomes and detection times. They compute the correlation between the postselected (coincident) measurement outcomes, which is

$$E\Big(A(\phi_A)B(\phi_B)|\text{ coincidence }\Big) = \cos(\phi_A + \phi_B). \qquad (6.1)$$

Note that equation (6.1) is the expectation value conditioned on coincidence for the setting ϕ_A, ϕ_B. Also note the difference between equation (6.1) and the corresponding correlation found in E91, equation (4.20). In the Franson setup, the angles are *added together* while other systems depend on their *difference*.

Alice and Bob now test the Bell-CHSH inequality in the usual way. After publicly announcing the measurement settings ϕ_A and ϕ_B, they postselect, and then compute the correlation for each setting pair by using equation (6.1). In order to maximise the Bell value, they picked measurement angles $\pi/4$ apart when the experiment started. This way, the correlations will coincide with those in equation (4.9), so the result will be a Bell value of $2\sqrt{2}$ in agreement with theorem 4.8 and equation (4.21). Now, in the words of Franson [40, p. 2207],

> [...] the quantum-mechanical predictions violate Bell's inequality and are inconsistent with any local hidden-variable theory.

Alice and Bob use the Bell-CHSH inequality as a test for DI security. If they measure $S(2) > 2$, the test passes, and they can continue their QKD session. However, the aforementioned post-selection is an important difference to the traditional BB84 and E91 protocols. In those protocols, sifting can be performed immediately after receiving the raw key, while the Franson scheme must postselect before this can be done. Postselection will have serious and far-reaching consequences to the security of Franson-based QKD, and we will discuss this in depth in section 6.2 and chapter 7.

Equation (6.1) shows that, if Alice's and Bob's measurement angle are opposite ($\phi_A + \phi_B = 0$), the measurement outcomes are perfectly correlated. Similarly, for settings $\phi_A + \phi_B = (2n + 1)\pi$ where n is an integer, Alice's outcomes will be opposite (that is, anti-correlated) to Bob's. Therefore, Alice performs a bit flip on the anti-correlated bits and then Alice and Bob essentially share a randomly generated bit string (modulo noise and the presence of Eve). They then continue with the next steps of the protocol: information reconciliation and privacy amplification, in order to generate a secret key.

Again, it is impossible to distinguish between an eavesdropper and experimental noise, and both will have the effect of lowering the measured Bell value (see section 8.2). For the duration of the QKD session, Alice and Bob constantly monitor the Bell value, and if it ever falls to 2 or lower, they must abort the transmission.

We have now shown a way to test the Bell-CHSH inequality using energy and time instead of polarization. Since Franson's publication in 1989, the device has been experimentally tested by several groups [41–50], and it is often assumed to be a workable proposal for QKD. Again, we stress that the Franson scheme requires a postselection step. On average, this postselection discards 50 % of the events, which is a significant amount.

6.2 The Postselection Loophole

We have now seen that the Franson interferometer is believed (i) to violate local realism, and (ii) to allow secure ETE DI-QKD. However, as discussed in chapter 5, the Bell test must always be viewed in the context of loopholes, and a special case of the detection loophole has particular consequences for the Franson setup as is shown in publication A.

Theorem 5.5 showed that the lower bound on detection efficiency is 82.83 % when using the original CHSH inequality. This percentage does not only include actual experimental losses in fiber couplings and photon detectors, but in fact any loss incurred by either experiment or protocol. Needless to say, the 50 % postselection step must also be included and as a consequence, not even an ideally constructed Franson experiment can reliably test the Bell-CHSH inequality!

This loophole, a special case of the detection loophole of section 5.1, is referred to as the *postselection loophole* to stress that it originates from the core design of the experiment and not from experimental losses. In fact, we have the following result:

Theorem 6.1 (Bell-CHSH for the Franson Interferometer) *The outcomes from a local realist system with two settings per observer in the Franson interferometer obey*

$$\begin{aligned}\Big|E\big(A_1B_1|\Lambda_{A_1B_1}\big) + E\big(A_2B_1|\Lambda_{A_2B_1}\big)\Big| \\ + \Big|E\big(A_1B_2|\Lambda_{A_1B_2}\big) - E\big(A_2B_2|\Lambda_{A_2B_2}\big)\Big| \leq 4.\end{aligned} \tag{6.2}$$

The outcomes are therefore not bounded by the Bell-CHSH inequality.

Proof *We will assume no experimental losses. Therefore we have* $\eta = 0.5$ *due to the postselection step alone. Any local realist model with losses is governed by theorem 5.5, which for the given* η *gives*

$$S_C(2) \leq 6. \tag{6.3}$$

However, theorem 4.6 states that the algebraic maximum value of $S_C(2)$ *is 4, so we modify the right-hand side of inequality (6.3) accordingly. The proof now follows from definition 5.2.*

Theorem 6.1 shows that the Bell-CHSH inequality for the Franson interferometer is trivial. Therefore, even though any system – whether quantum or classical – can give any violation of the *Bell-CHSH inequality* in the Franson interferometer, no system actually violate *local realism*! This is an undesirable situation, as ETE gives us hope for a practical way of achieving QKD. The Bell-CHSH security test is therefore unable to provide DI-QKD in the Franson interferometer. Obviously, we must try to remedy the problem, and this will be discussed in detail in chapter 8. However, one countermeasure, fast switching of analysis station settings, is of immediate relevance and will be presented now.

In the introduction to chapter 5, we briefly mentioned the locality loophole and the importance of putting the event of source emission outside of the forward light cone of the choice of measurement setting at the analysis station. This is still true in the Franson setup, however there is an extra complication because the emission *time* is randomly chosen to be either early or late, a difference of ΔT. Now, if Alice and Bob randomly select new settings for their analysis stations faster than $1/\Delta T$, it is possible that the (hypothetical) early and late events encounter different measurement settings.

Without loss of generality we can assume that the event in question will be recorded as coincident, i.e., Alice's and Bob's detection times agree. This implies that Alice's and Bob's analysis stations either both "caused a delay" or both "did not cause a delay", although there is no method for discerning between these two cases. Therefore, either the early event occurred and the analysis station had a corresponding setting, or the late event occurred with another, possibly different measurement setting.

Publication A discusses fast switching in greater detail and mentions a number of precautions that must be observed for it to actually occur, but the following observation is important: The setting of the analysis station determines whether a delay occurs or not, *but only for the early setting.* When the late setting is read off, time cannot be reversed, so the late event cannot be turned into an early one. The consequence is that we have *two* governing equations when fast switching is used: one for early events, and one for late.

Lemma 6.2 (Outcomes from Early Events) *When using fast switching, outcomes from early events in a local realist model in the Franson interferometer are only bounded by the trivial Bell inequality.*

Proof *The early events behave in the exact same way as in theorem 6.1.*

Lemma 6.3 (Outcomes from Late Events) *When using fast switching, outcomes from late events in a local realist model in the Franson interferometer obey*

$$\begin{aligned}&\left|E(A_1B_1|\Lambda_{A_1B_1}) + E(A_2B_1|\Lambda_{A_2B_1})\right|\\&\quad+\left|E(A_1B_2|\Lambda_{A_1B_2}) + E(A_2B_2|\Lambda_{A_2B_2})\right| \leq 2.\end{aligned} \tag{6.4}$$

Proof *Late events fulfilling the prerequisites for fast switching described in publication A cannot be turned into early detections. Therefore, late events are always detected as late, both for Alice and Bob. Consequently, there will be no postselection, so theorem 5.5 applies with $\eta = 1$ (assuming no experimental losses). The proof follows from definition 5.2.*

We are now ready to conclude this section about fast switching with the full theorem:

Theorem 6.4 (**Bell-CHSH for the Franson Interferometer with Fast Switching**) *When using fast switching, the outcomes from any local realist model in the Franson interferometer with two settings per observer obey*

$$\begin{aligned} &\left|E\left(A_1B_1|\Lambda_{A_1B_1}\right) + E\left(A_2B_1|\Lambda_{A_2B_1}\right)\right| \\ &\quad+\left|E\left(A_1B_2|\Lambda_{A_1B_2}\right) + E\left(A_2B_2|\Lambda_{A_2B_2}\right)\right| \le 3. \end{aligned} \tag{6.5}$$

Proof *Half of all source emissions are early and half are late, so we take average of the Bell-CHSH inequalities in lemmas 6.2 and 6.3.*

Adopting the method of fast switching in the Franson interferometer strengthens the local realist bound from 4 down to 3. The reason is the mix-in of 50 % of events that are not affected by postselection (lemma 6.3).

Still, after all this work, the quantum prediction $2\sqrt{2}$ (theorem 4.8) falls short of the local realist bound 3 (theorem 6.4), so *Franson interferometer is insecure even when using fast switching*. So far we have failed in re-establishing a violation of local realism, but we will show additional methods in chapter 8. In the meantime, the next chapter shows how an attacker can break the security of systems that lack a proper violation in order to to obtain Alice's and Bob's secret key.

Chapter 7

Quantum Hacking

> [...] what is proved by impossibility proofs is lack of imagination.
>
> — John Stewart Bell, 1982 [137, p. 997]

The postselection loophole causes the local realist bound in the Franson interferometer to weaken to the extent that not even the quantum-mechanical prediction gives a violation. This chapter will show how far-reaching the consequences can be for applications such as QKD, and detail how an insecure system can be exploited in practice. Whenever we turn theoretical weaknesses of QKD devices into practical exploits, we engage in *quantum hacking*.

If a loophole is discovered in a system relying on a Bell inequality violation, the first step for an attacker is to verify the loophole by creating an LHV model that mimics all behaviors of quantum mechanics, including the produced Bell value. An LHV model is a list of *a priori* outcomes that are to be produced by the analysis stations in order to reach that goal. Just as the name suggests, such a pre-recorded list of measurements implies locality and realism, and all such outcomes are governed by a relevant Bell-type inequality.

7.1 The LHV Attack

An LHV attack is an attack on an interferometer that implements an LHV model in order to contradict the corresponding security proof. It is a powerful method for exploiting loopholes, and allows for a simple way to predict correlations $E(A_iB_j)$. For the Franson interferometer, an initial LHV model was introduced by Aerts et al. [138] in 1999 and is depicted in figure 7.1. This model consists of two two-dimensional probability distributions: one for Alice and one for Bob. The source device picks hidden variables θ and r uniformly at random from the sets $0 \leq \theta < 2\pi$ and $0 \leq r < 1$, and then computes $\theta_A = \theta - \phi_A \pmod{2\pi}$ and $\theta_B = \theta + \phi_B \pmod{2\pi}$, where ϕ_A and ϕ_B are Alice's and Bob's local settings, respectively. Alice's measurement outcome can now be predicted at coordinate (θ_A, r) in her probability distribution, Bob's outcome is predicted at (θ_B, r) in his.

Note that the LHV model by Aerts et al. not only prescribes the sign of the measurement outcome (± 1) but also the *arrival time*, early/late. This is important as Alice and Bob postselect their outcomes depending on the arrival time before computing the conditional expectation values of definition 5.2. Cleverly, the LHV model *exploits* postselection so that Alice and Bob measure $S_C(2) = 2\sqrt{2}$, an exact mimic of the quantum prediction. Without postselection, the LHV attack would be impossible.

Let us briefly review what just happened. A local realist system (the LHV model in figure 7.1) was able to prescribe measurement outcomes of distant analysis stations, so that the measured correlations coincide with those produced by an entangled system. Given any (expensive) experiment involving delicate free-space photons, trapped ions, or optical fibers, an attacker can then construct a machine *indistinguishable* from that experiment, using only a (cheap) classical system. Remember: we are still in the black-box model, so systems are only evaluated by their measurement outcomes, not the way they are built.

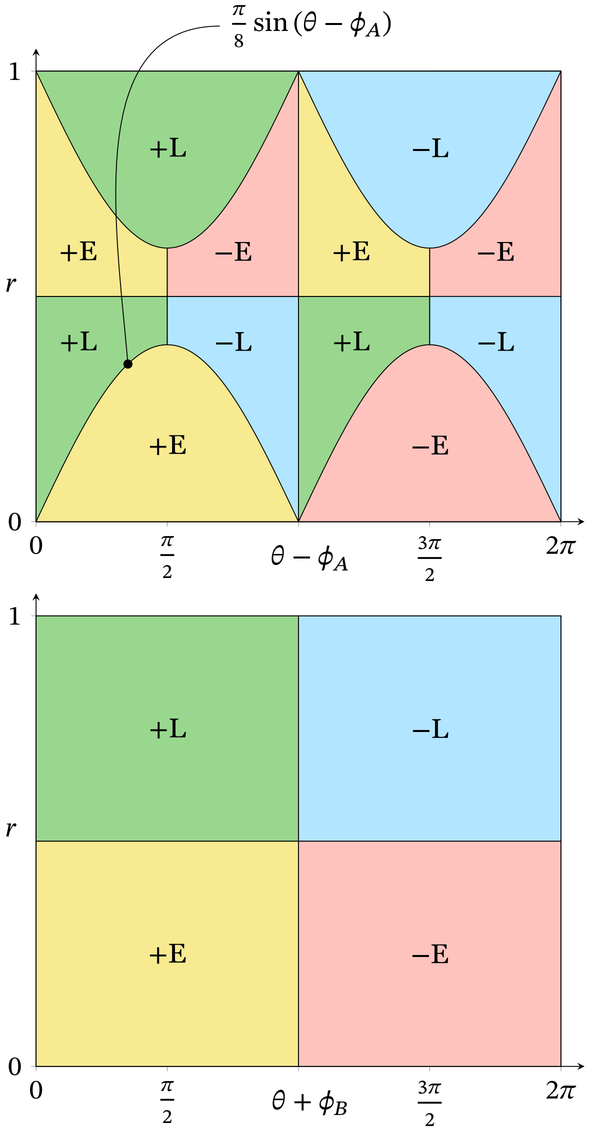


Figure 7.1: LHV model by Aerts et al. [138] for faking a Bell-CHSH violation in the Franson interferometer. These models take as input the hidden variables r and θ, and analysis station settings ϕ_A and ϕ_B. The upper graph shows Alice's prescribed measurement outcomes (A) while the lower shows Bob's (B). The LHV model returns the sign (+1 or −1) and timeslot (E for early and L for late).

The consequences for QKD are even more sinister. A successful LHV attack not only allows a faked Bell value, but also a subversion of the security test. On the surface, Alice and Bob see nothing wrong with their device — all measurements they perform at their analysis stations have exactly the statistical distributions they expect. However, with a compromised security test, Eve can perform additional attacks that either leak the secret key, or allows her to control the key bit generation. In publication B we experimentally mounted an LHV attack on the Franson interferometer that resulted in full freedom for Eve to decide the secret key.

7.2 The Blinding Attack

In order to turn the LHV attack into a practical exploit, publication B uses a technique called *blinding*. An optical QKD implementation is very sensitive to variations in photon counts because if the source accidentally generates two identical photons instead of one, Eve can keep one and send the other to Alice/Bob. This is called the *photon-number-splitting attack*. Measurements on the extra photon can then be performed without influencing the noise rate, and therefore Eve breaks the security but remains undetected. As a consequence, it is important to build source devices that are very accurate in sending precisely one single photon each to Alice and Bob.

Naturally, single-photon sources require Alice and Bob to use very sensitive detection equipment, i.e., Single Photon Detectors (SPD:s). A common type of SPD is the Avalanche Photo-Diode (APD), which according to Lydersen et al. [139] is used in most QKD implementations today. It was discovered by Makarov [140] that APD:s are vulnerable to a side-channel attack that allows an attacker to remotely control how and when the detector gives a click. Normally, an APD is supposed to react to even a single incoming photon, but by studying the quenching mechanisms of commonly used APD:s, Makarov found that these detectors are vulnerable to blinding.

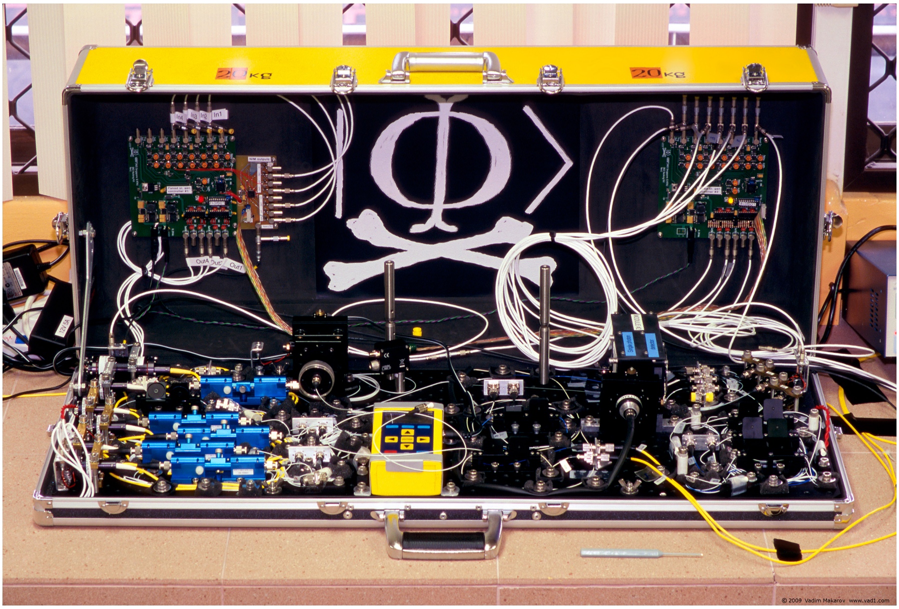


Figure 7.2: Part of the equipment used by Gerhardt et al. [141] to break the security of a commercial QKD system. Depicted here is Eve's photon detection unit and the faked-state generator, which contains semiconductor lasers, polarization controllers, and control electronics. Note the $|\Phi\rangle$ Jolly Roger logo for quantum hacking. Photo copyright © 2009 Vadim Makarov, reused with permission.

By shining a strong Continuous-Wave (CW) laser into the APD, the quenching circuit becomes overloaded and has to re-charge before being able to react to a single photon. In the meantime (approximately 1 µs [140]), the detector will not function as intended. The practical consequence is that the CW laser turns the detector into *linear mode*, allowing attacker to control when and how the detector should click. Linear mode means the detector clicks only above a certain optical intensity I_T, and not below. In other words, it is possible for a nonzero number of photons to enter the detector without it clicking. Obviously, this is not how a SPD is supposed to work – even a single incoming photon should be detected.

While illuminating the detector with the blinding CW beam, the attacker can input additional pulses of light into the detector.

If these pulses are strong enough to exceed the threshold I_T, the detector will finally click. This attack vector was soon exploited to mount a full attack on commercial QKD implementations. In 2010, Lydersen et al. [139] gave a proof of concept for controlling detectors in two commercial QKD solutions, and the next year, Gerhardt et al. [141] developed the concept into a full attack. This full attack uses the intercept-resend method, where Eve cuts the fiber between Alice and Bob and measures the photons before sending a *faked state* to Bob. Thanks to blinding, these faked states stop Bob from receiving data sent in the incorrect basis, and therefore Alice and Bob never notice the attack. Eve's faked-state generator is depicted in figure 7.2, and this device was able to intercept the entire secret key in a commercial QKD device.

The same year, 2011, Gerhardt et al. [142] blinded detectors in an E91 setup and used classical pulses of light to produce a faked Bell value. A classical pulse of light is always local and realist, so as previously discussed, the corresponding Bell value should be bounded by 2. Still, the attack resulted in Alice and Bob measuring a Bell value of 2.381 ± 0.036 and this makes them believe the system passes the security test even though Eve has intercepted their key.

7.3 Optical Considerations

In publication B we adopted the blinding attack to the Franson interferometer in order to control the measurement outputs of Alice's and Bob's detectors. Normally, Alice and Bob defend against Trojan-horse attacks with a Bell test, but if the Bell test is subverted, an attack can be made without raising the alarm. Our Trojan source sends input time-delayed pulses of classical light overlaid on a bright CW blinding laser to Alice and Bob, and in order to produce the correct pulses one needs a good understanding of how the analysis stations work.

The most important part of a Franson analysis station is the beam splitter, sometimes called a "half-silvered mirror", which

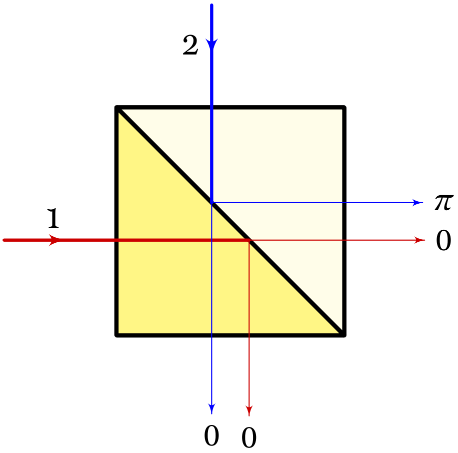


Figure 7.3: Schematic of a beam splitter manufactured by joining two triangular prisms with different refractive indices. The beam splitter depicted here has a high refractive index in the lower left region and a low refractive index in the top right. Two incident beams are combined into two output beams. The beam from the left receives no phase shift, but the beam from the top receives a π phase shift when reflected off the higher refractive index region.

splits and combines light beams. Here, each analysis station contains two beam splitters, so the total number of beam splitters in the Franson interferometer is four. Beam splitters can be manufactured in a variety of ways, but the operation is the same. Two edges are inputs and two are outputs, and along the diagonal line there is a mirror-like interface. Each input beam is split into the two output beams, however the output intensity also depends on interference, which in turn depends on the relative phases of the incident beams. The easiest way to understand how beam splitters affect the phase is to consider a beam splitter consisting of two triangular pieces of glass with different indices of refraction as depicted in figure 7.3.

We let the first incident beam have intensity $I_0/2$ and enter the region with higher refractive index from left. The second incident beam, also with intensity $I_0/2$, enters from the top. Assuming we are dealing with an ideal 50 : 50 beam splitter, each beam is split into two at the interface without loss. According to Träger [143, pp. 124–125], the total intensity of all output beams remains I_0 so conservation of energy is fulfilled. For the first beam there is no reflection off a transition from low to high refractive index, so no phase shift occurs. The second beam also gets no phase shift when transmitted into the high refractive index region, however the component that is reflected has its phase shifted by π. Therefore, three of the output beams have no change in phase while the fourth has. At each output port (right and bottom) the beams now interfere. The output intensities I_R (right exit) and I_B (bottom exit) then depend on the phases ϕ_1 and ϕ_2 of the input beams in the following way:

$$\begin{aligned} I_R &= \frac{I_0}{2}\Big(1 + \cos(\phi_1 - \phi_2 + \pi)\Big), \\ I_B &= \frac{I_0}{2}\Big(1 + \cos(\phi_1 - \phi_2)\Big). \end{aligned} \tag{7.1}$$

We see that the total output intensity I_R+I_B sums to I_0 for all phases ϕ_1 and ϕ_2, which shows that equation (7.1) conserves energy. In order to control the constructive and destructive interference at the output ports we therefore must produce beams of light with a relative phase of either 0 or $\pi/2$. The first case, zero relative phase, directs all incoming light out of the bottom port, while a relative phase of $\pi/2$ directs all incoming light out of the right port.

We have now shown that the optical intensities exiting the beam splitter depends on the relative phase of the incoming beams. In the Franson interferometer, the output intensity of the second beam splitter in the analysis station can therefore be manipulated with the local phase setting ϕ_A or ϕ_B. We call the first beam splitter the *splitter* and the second one the *combiner*, see figure 7.4 for a close-up of Bob's analysis station. If we input a strong pulse of classical light with intensity I_0 into the analysis station, the pulse will divide in two pulses at the first beam splitter. The pulse taking the upper path will be delayed by ΔT and phase shifted by ϕ_B before being combined with the lower path at the second beam splitter.

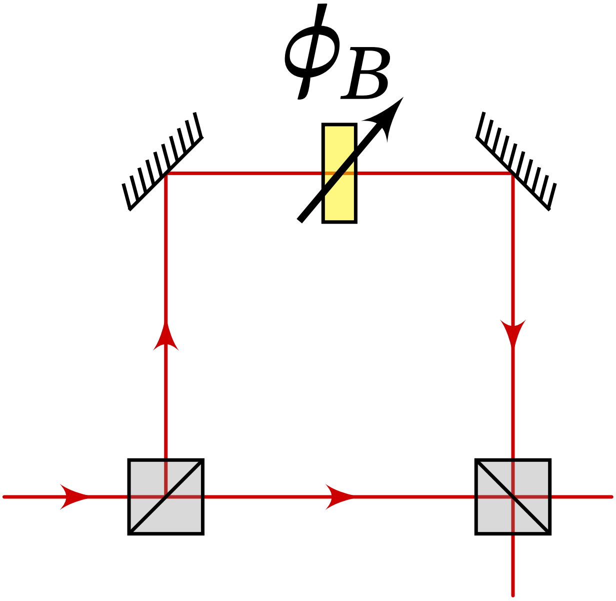


Figure 7.4: Close-up of figure 6.1, which shows Bob's analysis station in the Franson interferometer. The left beam splitter is the *splitter* wile the right beam splitter is the *combiner*.

Assuming the pulses have a pulse length of $\tau \ll \Delta T$, there will be no first-order interference at the combiner. Therefore, two pulses of intensity $I_0/2$ separated by ΔT will enter the detectors, independently of the phase setting ϕ_B. If we instead input *three* short pulses separated by ΔT, pulses will interfere at the combiner, so the output will be the following *four* pulses:

1. One pulse with fixed intensity $I_0/4$.
2. One pulse whose intensity depends on ϕ_A and the relative phase between the first and second incoming pulses. “Early”.
3. One pulse whose intensity depends on ϕ_A and the relative phase between the second and third incoming pulses. “Late”.
4. One pulse with fixed intensity $I_0/4$.

Pulses 2 and 3 are the important ones, and we refer to these as the *middle pulses*. Specifically, pulse 2 is the *early* pulse, and pulse 3 the *late*. If we define ω_E as the relative phase difference between the first and second *incoming* pulse and ω_L as the difference between the second and third, we can derive intensities of all four middle pulses from equation (7.1) as shown in publication B:

$$\begin{aligned} I_E^+(\phi_B, \omega_E) &= I_0 \cos^2\left(\frac{\phi_B + \omega_E}{2}\right), \\ I_E^-(\phi_B, \omega_E) &= I_0 \sin^2\left(\frac{\phi_B + \omega_E}{2}\right), \\ I_L^+(\phi_B, \omega_L) &= I_0 \cos^2\left(\frac{\phi_B + \omega_L}{2}\right), \\ I_L^-(\phi_B, \omega_L) &= I_0 \sin^2\left(\frac{\phi_B + \omega_L}{2}\right). \end{aligned} \tag{7.2}$$

Again, note that ω_E and ω_L depend on the pulses that are sent *into* the analysis station, not the pulses that leave it. Eve now tweaks the intensity of the incoming pulses so that $I_0/4$ is just below the linear mode threshold I_T of the detectors. This way, the first and last pulses are not detected by the blinded APD, and we can control the clicks of the middle pulses by varying ω_E and ω_L according to equation (7.2). With this information, Eve can control not only which detector is supposed to click, but also in which which timeslot the click should occur. In order to produce a faked Bell value that violates the Bell-CHSH bound in theorem 4.7, she uses the recipe given in the LHV model of section 7.1.

That model mimics the quantum-mechanical Bell value prediction $S_{QM}(2) = 2\sqrt{2}$ from theorem 4.8. Therefore, Eve can make Alice and Bob measure exactly $S_C(2) = 2\sqrt{2}$. However, the sinusoidal patterns of the LHV model in figure 7.1 cannot be reproduced with a finite number of trials, so a real attack will have a small deviation from $2\sqrt{2}$. This is of no concern as this error can be made arbitrarily small, and the discretized LHV model in publication B is indistinguishable from a quantum experiment because of noise.

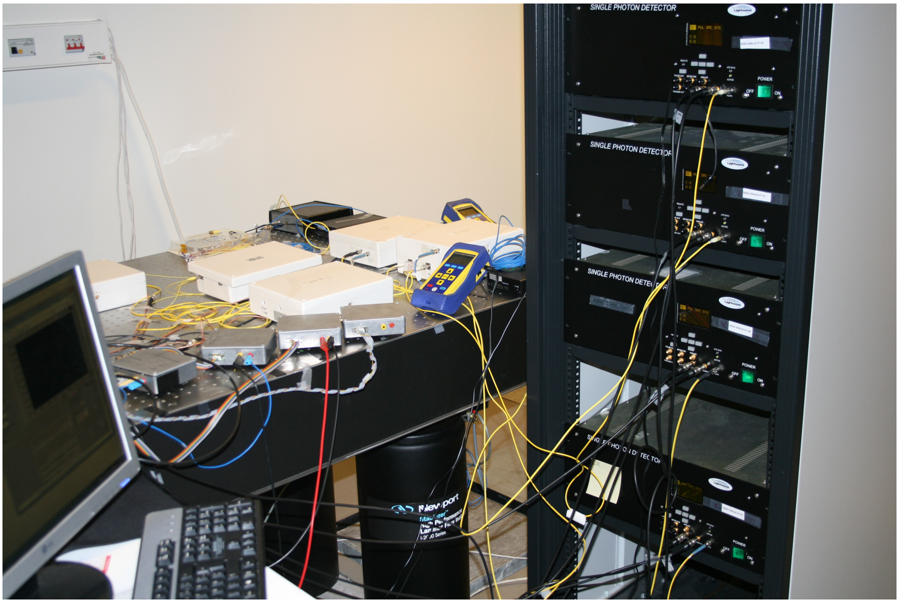


Figure 7.5: Experimental setup for hacking the Franson interferometer as done in publication B. In the back is the mechanically dampened optical table with optical components on top of it. The white polystyrene boxes are for thermal insulation of the components inside, and the components are connected with optical fibers. To the right is a rack with four InGaAs avalanche photodiodes from Princeton Lightwave. Picture taken at AlbaNova, Stockholm University.

7.4 Experimental Demonstration

Our attack in publication B was experimentally verified at AlbaNova at Stockholm University using passive fiber-optic components. We used commercial InGaAs APD:s from Princeton Lightwave with a detection wavelength range of 1300 nm to 1500 nm and dark count rate of $5 \times 10^{-5}\,\mathrm{ns}^{-1}$ at the operating temperature 218 K. These detectors, depicted in figure 7.5, have a maximum detection efficiency $\eta = 20\,\%$ and were attacked by blinding them with a CW laser with overlaid attack pulses as chosen from the LHV model. Interestingly, publication B appears to be the first publication that reproduced the blinding attack in section 7.2

where no author is affiliated with the researchers that first discovered the effect [139, 140, 142].

In the first step of the attack, Alice and Bob measured a faked Bell value of 2.5615 ± 0.0064, which violates the Bell-CHSH inequality (see figure 7.6). The raw experimental data is available online [54], but this Bell value is somewhat lower than what we aimed for (see section 8.2 for an explanation why). We can, however, raise it higher in the next step. If the experimental noise is fixed and known to Eve, she can *tune* the LHV attack in order to compensate. Recall from theorem 6.1 that the governing Bell inequality in the Franson interferometer is trivial, so *any* system should be able to produce *any* Bell value between 0 and 4. Exact details are given in publication B, but the end result is a Bell value up to 3.6386 ± 0.0096, which even happens to violate Cirel'son's bound in theorem 4.8!

We do not recommend an attacker to aim for a Bell value as high as 3.6, as it would leave Alice and Bob very suspicious. In theory, the only known way to produce the Bell value 4 is with a Popsecu-Rohrlich (PR) box [144], however this device is forbidden by the laws of quantum physics. The point is instead that our attack is tunable, which allows a Bell-CHSH violation to be produced even in the presence of high levels of experimental noise.

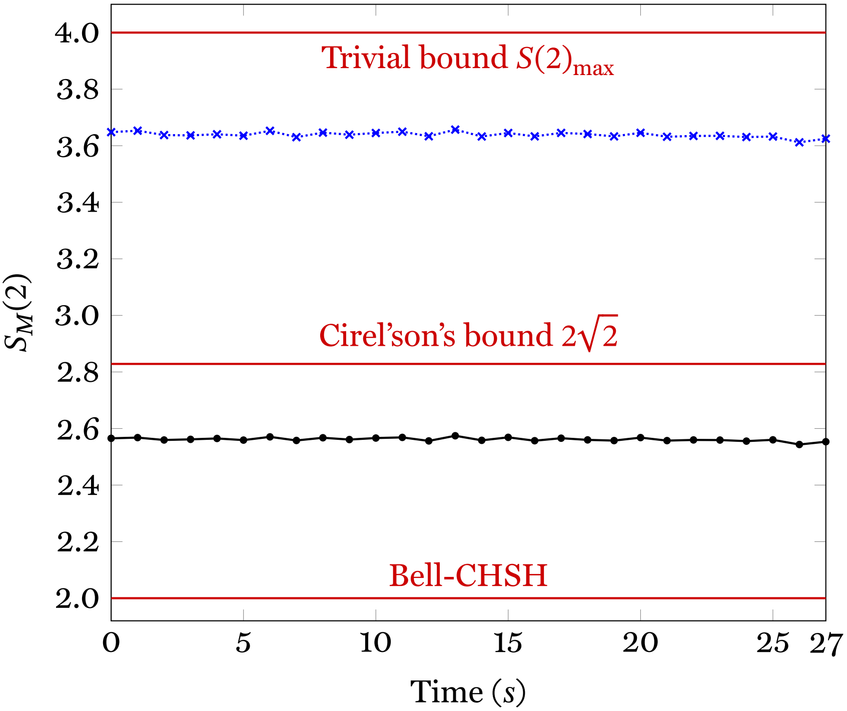


Figure 7.6: Experimentally measured faked Bell values $S_M(2)$ in our attack on the Franson interferometer compared to the Bell-CHSH bound (theorem 4.7), Cirel'son's bound (theorem 4.8), and the trivial Bell value (theorem 4.6). Each measurement run is 27 s long. When aiming for the quantum prediction $2\sqrt{2}$, the produced Bell value is averages to 2.5615 ± 0.0064 (solid black line). It is possible to boost the faked Bell value as high as 3.6386 ± 0.0096 (dotted blue line).

Chapter 8

Countermeasures to Quantum Hacking

> Suppose for a moment that all the possible issues related to the implementation are under control. Can one finally rest in peace and trust the laws of physics? In principle one can, *provided* all the assumptions, under which the security bounds were derived, are fulfilled by the implementation. Indeed, another dangerous shortcut consists in associating "unconditional security" with "no assumptions": no assumptions should be made on the power of the eavesdropper, but assumptions *must* be made on what Alice and Bob are doing.
>
> — Scarani and Kurtsiefer, 2014 [131, p. 29]

Chapter 7 listed techniques for hacking QKD setups in general, and the Franson interferometer in particular. By now it should be well-established that the Bell-CHSH inequality is insufficient as a security test for devices with high postselection. In the present chapter we will discuss countermeasures that can be used to reestablish unconditional security in such devices.

However, before suggesting patches and hotfixes for the security of QKD devices, we have to go back to section 1.2 and re-iterate some basic fundamentals about designing cryptosystems. We always have to assume that the enemy knows the system (Kerckhoff's principle), so any reliance on security by obscurity puts us in peril. In addition, the selling point of QKD is *unconditional* security, so security must be based on stringent proofs and not assumptions on what an attacker can or cannot do (except follow the laws of quantum physics!).

For an enlightening example, consider the blinding attack by Lydersen et al. [139]. As a countermeasure, Yuan et al. [145] suggested using a *monitoring device* to sound an alarm if bright illumination entered the detector. The idea is to eliminate the blinding attack by simply looking for it; if the incoming light is too bright, the device is under attack and the communication is aborted. As a QKD device produces a secret key for *later* use in an OTP system, early warning systems can alert the user before any ciphertext encrypted with that key is sent over an untrusted channel.

At first glance, a monitoring device is appealing since the short-term consequence is that the BB84 and E91 protocols become immune to precisely the attack described by Makarov [140] and Lydersen et al. [139]. However, adding specific countermeasures to individual attacks introduces extra, unproven assumptions into the security model [146]. Unless the security theorem itself is corrected to factor in (and prove!) these assumptions, countermeasures will not provide unconditional security of the modified system. In a follow-up correspondence, Lydersen et al. [147] responded to the suggestion of a monitoring device as follows:

> It seems that the countermeasure proposed by Yuan et al. [148] does not prevent our general attack of tailored bright illumination. So far, we have been able to blind and control every APD-based detector that we have looked at thoroughly (albeit with different techniques), including three different passively quenched

> detectors [140], one actively quenched detector [149] and two different gated detectors [139, 150, 151].

Please note the crucial "not" in the second row of the above quote. As it happened, a practical attack on these pulse monitoring devices was later demonstrated by Sajeed et al. [152]. There, a pulse train was input to a detector in such a way that blinding occurred, even though the monitor never reported an intrusion. The monitor itself is a device with imperfections, and it was discovered that a design flaw allowed very short blinding pulses to go by undetected. Just as predicted, a previously unknown attack not covered by a countermeasure was able to induce unexpected behavior, which in turn compromised the system.

Again, it could be argued that the design flaw in the monitoring device can be fixed, which eliminates the specific attack by Sajeed et al. [152]. Quickly, however, this would turn into the same type of cat-and-mouse-game so common in, for example, classical information security, where hackers try to find flaws and exploits in software that developers attempt to fix. We must instead remind ourselves that QKD plays a completely different game. *Unconditional* security requires stringent proofs, and unless QKD (which is very expensive and complicated!) can be*formally* proven secure, there will never be demand for it.

Our attack in publication B uses blinding as a vector to gain access to Alice's and Bob's measurement outcomes, so the same discussion applies here. However, while the attacks of Lydersen et al. [139] and Gerhardt et al. [142] broke the security of "proven" systems, our attack is on a system with a flawed proof. It can certainly be argued that the Franson interferometer can be attacked without the need for blinding, which is a refinement of the attack in publication B that certainly should be attempted in future works.

The rest of this chapter is dedicated to methods that re-establish unconditional security in the Franson setup without relying on simple countermeasures such as the aforementioned monitoring device. We will discuss modified Bell inequalities and

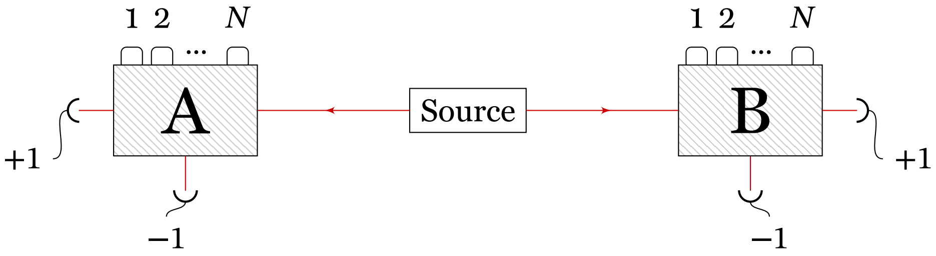


Figure 8.1: The black box method for $N \geq 2$ settings per observer. This is a generalization of figure 4.3 that instead uses N push buttons. The analysis stations still return the outcomes $+1$ or -1.

variations in interferometer design in our quest for true violations of local realism.

8.1 Chaining the Bell Inequality

The first technique for correcting the security proof is a technique called *chaining*. The standard Bell-CHSH inequality assumes Alice and Bob to each have two measurement settings to choose from. Chaining, however, generalizes the number of settings to any $N \geq 2$. As will be shown later on, chained Bell inequalities have more stringent experimental requirements than the standard version, but remember that Bell-CHSH is insufficient for the Franson setup anyway. Therefore, if a chained inequality can re-establish unconditional security it will be worth the cost.

The idea of chaining Bell inequalities came from Pearle [100] in 1970, however the concept was developed into usable inequalities by Braunstein and Caves [153] twenty years later. In recent works, the chained inequality has usually been referred to as the "Braunstein-Caves" inequality, however a more correct name would be Pearle-Braunstein-Caves (PBC) as this acknowledges the contribution of Pearle.

We will now formally define the PBC inequality, generalizing the black-box model from section 4.3. This time, the black boxes have N push buttons each, as shown in figure 8.1. Just like before, the black boxes hide the inner workings of the analysis stations, and we will only care about measurement settings (i.e. push buttons) and their corresponding outcomes (+1 and −1). Alice chooses measurement settings uniformly at random from the set $\{A_i\}_{i=1}^N$, while Bob does the same from $\{B_j\}_{j=1}^N$. We can now define the new, chained Bell value:

Definition 8.1 (Chained Bell Value) *The Bell value for a system with $N \geq 2$ settings per observer is defined as*

$$\begin{aligned} S(N) \overset{\text{def}}{=} &\left|E(A_1B_1) + E(A_2B_1)\right| + \left|E(A_2B_2) + E(A_3B_2)\right| \\ &+ \cdots + \left|E(A_NB_N) - E(A_1B_N)\right|. \end{aligned} \tag{8.1}$$

Note that equation (8.1) with $N = 2$ reduces to equation (4.14) as we expect.

Theorem 8.2 (Trivial Chained Bell Value) *Algebraically, the maximum value Bell value $S(N)_{\text{max}}$for a bounded system is*

$$S(N)_{\text{max}} = 2N. \tag{8.2}$$

Proof *Each expected value $E(A_iB_j)$ in a bounded system is bounded in magnitude by 1. There are $2N$ expectations in equation (8.1), so the algebraic maximum of $S(N)$ is $2N$.*

Definitions 4.1 to 4.4 still apply to the PBC case, so we are ready to formally define the PBC theorem [153]:

Theorem 8.3 (Pearle-Braunstein-Caves) *The Bell value for a local realist system with N settings per observer obeys*

$$S(N) \leq 2N - 2. \tag{8.3}$$

Proof *See Braunstein and Caves [153].*

Note that in their original paper, Braunstein and Caves [153] defined N as the number of *summation terms* in the chained Bell value. More recent works have switched to the more flexible convention of defining N as the number of *settings*. We will use this modern convention. Next, we find the maximum value of the chained Bell value predicted by quantum mechanics.

Theorem 8.4 (Quantum Prediction of the Chained Bell Value) *Quantum theory can produce the Bell value*

$$S_{QM}(N) = 2N\cos\frac{\pi}{2N} \tag{8.4}$$

for any $N \geq 2$.

Proof *See publication A.*

Again, if $N = 2$ is inserted in equation (8.4) we recover equation (4.17). As will be shown now, the PBC inequality can re-establish unconditional security in the Franson interferometer. To see this, we must first investigate the effect of the detection efficiency in section 5.1 to the chained inequality. We can immediately generalize definition 5.2 to the PBC case which gives

Definition 8.5 (Chained Bell Value, Conditioned on Coincidence) *The Bell value for a system with $N \geq 2$ settings per observer is defined as*

$$\begin{aligned} S_C(N) \overset{\text{def}}{=} &\left|E(A_1B_1|\Lambda_{A_1B_1}) + E(A_2B_1|\Lambda_{A_2B_1})\right| \\ &+ \left|E(A_2B_2|\Lambda_{A_2B_2}) + E(A_3B_2|\Lambda_{A_3B_2})\right| + \cdots \\ &+ \left|E(A_NB_N|\Lambda_{A_NB_N}) - E(A_1B_N|\Lambda_{A_1B_N})\right|, \end{aligned} \tag{8.5}$$

if only coincident events are considered.

Next, we study the effect of losses by generalizing theorem 5.5 to N settings per observer.

Theorem 8.6 (Pearle-Braunstein-Caves with Detection Efficiency) *A local realist system with $N \geq 2$ settings per observer and detection efficiency $0 < \eta_N \leq 1$ obeys*

$$S(N) \leq 2(N-1)\left(\frac{2}{\eta_N} - 1\right). \tag{8.6}$$

Proof *See Cabello et al. [102].*

Note that theorem 8.6 with $N = 2$ reduces to theorem 5.5. We continue by finding the trivial and critical detection efficiencies for all $N \geq 2$:

Remark 8.7 (Trivial Detection Efficiency for Pearle-Braunstein-Caves) *For $0 < \eta_N \leq 1$ and every $N \geq 2$, the equation*

$$2N = 2(N-1)\left(\frac{2}{\eta_N} - 1\right) \tag{8.7}$$

has a unique solution in

$$\eta_{\text{trivial,N}} \overset{\text{def}}{=} \frac{2N-2}{2N-1}. \tag{8.8}$$

Remark 8.8 (Critical Detection Efficiency for Pearle-Braunstein-Caves) *For $0 < \eta_N \leq 1$ and every $N \geq 2$, the equation*

$$2N\cos\frac{\pi}{2N} = 2(N-1)\left(\frac{2}{\eta_N} - 1\right) \tag{8.9}$$

has a unique solution in

$$\eta_{\text{critical,N}} \overset{\text{def}}{=} \frac{2}{\frac{N}{N-1}\cos\left(\frac{\pi}{2N}\right) + 1}. \tag{8.10}$$

The next step is to investigate the effect of postselection on the Franson interferometer with the PBC inequality. Formally, we have

Theorem 8.9 (Pearle-Braunstein-Caves for the Franson Interferometer) *When using the Franson interferometer, the corresponding PBC inequality is trivial for all $N \geq 2$.*

Proof *The effect of postselection in the Franson interferometer is modelled as η =0.5 in theorem 8.6. This gives*

$$S_C(N) \leq 6N - 6. \tag{8.11}$$

This bound, however, is weaker than the trivial bound in theorem 8.2 so the proof follows.

Unfortunately, chaining the Bell inequality did not immediately give unconditional security to the Franson interferometer as the governing inequality remains trivial. However, we will now employ the fast switching method introduced in section 6.2. Recall that in this setting and $N = 2$, half of all events are bounded by the standard Bell-CHSH inequality, while the other half is unrestricted (theorem 6.4). This gives us the chained theorem for fast switching:

Theorem 8.10 (Pearle-Braunstein-Caves for the Franson Interferometer with Fast Switching) *When using fast switching, the outcomes from any local realist model in the Franson interferometer with $N \geq 2$ settings per observer obey*

$$\begin{aligned}&\left|E\big(A_1B_1|\Lambda_{A_1B_1}\big) + E\big(A_2B_1|\Lambda_{A_2B_1}\big)\right| \\ &\quad + \left|E\big(A_2B_2|\Lambda_{A_2B_2}\big) + E\big(A_3B_2|\Lambda_{A_3B_2}\big)\right| + \cdots \\ &\quad + \left|E\big(A_NB_N|\Lambda_{A_NB_N}\big) - E\big(A_1B_N|\Lambda_{A_1B_N}\big)\right| \leq 2N - 1.\end{aligned} \tag{8.12}$$

Proof *Half of all source emissions are early and half are late, so we take the average of the trivial and standard PBC inequality* (8.3) *and equation* (8.2).

This bound is stronger than theorem 8.9, so fast switching has made a difference. Let us see if it this new bound strong enough by comparing it with the quantum prediction $S_{QM}(N)$ in theorem 8.4. Table 8.1 lists the bounds and quantum predictions for all $2 \leq N \leq 6$ and we see that fast switching allows the quantum correlation to be in violation for $N \geq 3$. In other words, the postselection loophole has been eliminated, and unconditional security the Franson interferometer has been re-established – all by modifying the security proof!

We now investigate the minimum detection efficiency required in the Franson interferometer when fast switching is used.

Theorem 8.11 (Pearle-Braunstein-Caves with Detection Efficiency for the Franson Interferometer with Fast Switching)

Number of settings	PBC bound	Quantum prediction
2	3	$4\cos(\pi/4) \approx 2.828$
3	5	$6\cos(\pi/6) \approx 5.196$
4	7	$8\cos(\pi/4) \approx 7.391$
5	9	$10\cos(\pi/10) \approx 9.511$
6	11	$12\cos(\pi/12) \approx 11.59$
$N \geq 7$	$2N - 1$	$2N\cos(\pi/2N)$

Table 8.1: Comparison of quantum prediction $S_{QM}(N)$ vs. the PBC bound $S_C(N)$ for the Franson interferometer with fast switching and $N \geq 2$ settings per observer.

When using fast switching, the outcomes from any local realist model in the Franson interferometer with $N \geq 2$ *settings per observer and detection efficiency* $0 < \eta_N \leq 1$ *obeys*

$$\begin{aligned}
&\left|E(A_1B_1|\Lambda_{A_1B_1}) + E(A_2B_1|\Lambda_{A_2B_1})\right| \\
&\quad + \left|E(A_2B_2|\Lambda_{A_2B_2}) + E(A_3B_2|\Lambda_{A_3B_2})\right| + \cdots \\
&\quad + \left|E(A_NB_N|\Lambda_{A_NB_N}) - E(A_1B_N|\Lambda_{A_1B_N})\right| \\
&\leq N + (N-1)\left(\frac{2}{\eta_N} - 1\right).
\end{aligned} \tag{8.13}$$

Proof *Half of all events are early, for which only the trivial PBC inequality from theorem 8.9 applies. The other events are late and are governed by the PBC inequality with detection efficiency* η_N *from inequality (8.6). The average of these two inequalities gives the result.*

Note that the bound in inequality (8.13) depends on the detection efficiency that remains *after* the 50 % postselection has been taken into account. We can now find the critical and trivial bounds:

Remark 8.12 (Trivial Chained Detection Efficiency for the Franson Interferometer with Fast Switching) *For* $0 < \eta_N \leq 1$

and every $N \geq 2$, the equation

$$2N = N + (N-1)\left(\frac{2}{\eta_N} - 1\right) \tag{8.14}$$

has a unique solution in

$$\eta_{\text{trivial,N,F}} \overset{\text{def}}{=} \frac{2N}{2N-1}. \tag{8.15}$$

Remark 8.13 (Critical Chained Detection Efficiency for the Franson Interferometer with Fast Switching) *For $0 < \eta_N \leq 1$ and every $N \geq 2$, the equation*

$$2N \cos\frac{\pi}{2N} = N + (N-1)\left(\frac{2}{\eta_N} - 1\right) \tag{8.16}$$

has a unique solution

$$\eta_{\text{critical,N,F}} \overset{\text{def}}{=} \frac{2N-2}{2N\cos\left(\frac{\pi}{2N}\right) - 1}. \tag{8.17}$$

Even if the detection and postselection loopholes are closed, the coincidence-time loophole must also be considered. Just as in the case of detection efficiency, theorem 5.9 must be generalized to all $N \geq 2$. This will allow us to find the trivial and critical coincidence probabilities required for a violation of the PBC inequality.

The definitions in section 5.2 are general enough to allow for adding more measurement settings. We can therefore present publication C, where a full derivation of the PBC inequality with coincidence probability was performed. The main result is the following:

Theorem 8.14 (Pearle-Braunstein-Caves with Coincidence Probability) *A local realist system with $N \geq 2$ settings per observer and coincidence probability $0 < \gamma_N \leq 1$ obeys*

$$S_C(N) \leq \frac{4N-2}{\gamma_N} - 2N. \tag{8.18}$$

Proof *See publication C.*

Analogous to previous results, we derive trivial and critical coincidence probabilities for all $N \geq 2$.

Remark 8.15 (Trivial Coincidence Probability for Pearle-Braunstein-Caves) *For* $0 < \gamma_N \leq 1$ *and every* $N \geq 2$*, the equation*

$$2N = \frac{4N-2}{\gamma_N} - 2N \tag{8.19}$$

has a unique solution in

$$\gamma_{\text{trivial},N} \overset{\text{def}}{=} \frac{4N-2}{4N}. \tag{8.20}$$

Remark 8.16 (Critical Coincidence Probability for Pearle-Braunstein-Caves) *For* $0 < \gamma_N \leq 1$ *and every* $N \geq 2$*, the equation*

$$2N \cos\frac{\pi}{2N} = \frac{4N-2}{\gamma_N} - 2N \tag{8.21}$$

has a unique solution in

$$\gamma_{\text{critical},N} \overset{\text{def}}{=} \frac{2N-1}{2N}\left(1 + \tan^2\left(\frac{\pi}{4N}\right)\right). \tag{8.22}$$

Publication C showed that the bound in theorem 8.14 is tight, which means that any coincidence probability below $\gamma_{\text{critical},N}$ allows for an LHV attack. We prove this constructively, i.e., by explicitly giving an LHV model that reproduces the same output statistics as a quantum system would.

This concludes our discussion on chaining the Bell inequality. Note that the PBC inequality is more difficult to test in experiment, compared to the Bell-CHSH case. This will be discussed in the next section.

8.2 Interferometric Visibility

> Unfortunately, with this experiment, whenever you're looking for a stronger correlation, any kind of systematic error you can imagine typically weakens it and

> moves it toward the hidden-variable range. It was a hard experiment. In those days, at any rate, with the kind of equipment I had, and ...well, what can I say? [...] I screwed up.

The above anecdote is told by physicist Richard Holt [119, p. 286] and refers to his 1973 attempt [109] at an experimental test of Bell's then-new theorem. The result of the experiment was negative, i.e., that the Bell inequality was indeed *not* violated by quantum mechanics. As Holt explains, it was later shown that systematic errors artificially reduced the measured Bell value in this experiment and made the conclusion incorrect. Specifically, one of several such errors was "found in the form of stresses in the walls of the Pyrex bulb used to contain the electron gun and mercury vapour" [154, p. 1910]. The effect of general experimental effects (systematic errors, dark counts, detector noise) on the interpretation of a measured Bell value will be discussed in this section.

Using the chained PBC inequality as a security test will, in theory, prevent the postselection loophole by allowing quantum mechanics to violate local realism even with 50 % postselection. As just shown, experimental errors can skew the outcome to the point where an incorrect conclusion is drawn, similar to the detection loophole. While a low detection efficiency leads to lost events (i.e., A_i and/or B_j undefined), a low *interferometric visibility*, sometimes called *fringe visibility*, is more general and can cause spurious detections. For example, an event that should give -1 can instead be recorded as $+1$.

The lower the experimental visibility, the lower the measured Bell value [120, p. 17], so we must quantify it before interpreting the results of a Bell test:

Definition 8.17 (Visibility) *The* visibility *of a Bell experiment with N settings per observer is defined as*

$$V_N \overset{\text{def}}{=} \frac{S_M(N)}{S_{QM}(N)}, \tag{8.23}$$

where $S_M(N)$ is the experimentally measured Bell value.

Visibility therefore represents the experimental deviation from the desired (and possibly chained) Bell value. Analogous to the previously discussed imperfections, we can find a critical visibility:

Definition 8.18 (Critical Visibility) *There exists a unique visibility $0 < V_N \leq 1$ so that the measured Bell value with N settings per observer will not exceed the bound in theorem 8.3. This critical visibility is defined as*

$$V_{\text{critical},N} \overset{\text{def}}{=} \frac{S_B(N)}{S_{QM}(N)}, \tag{8.24}$$

where $S_B(N)$ is the relevant local realist bound.

When using the standard Bell-CHSH inequality, that is, $N = 2$ settings per observer, the critical visibility reduces to

Remark 8.19 (Critical Visibility for Bell-CHSH) *The critical visibility for the Bell-CHSH inequality is*

$$V_{\text{critical}} \overset{\text{def}}{=} \frac{1}{\sqrt{2}} \approx 70.71\,\%. \tag{8.25}$$

In experimental papers, the threshold in remark 8.19 is often [155–157] correctly used as a sufficient condition for violating local realism. The same assertion is made in a recent publication by Peiris et al. [58], which states that their achieved visibilities of 66 % in a Franson setup "approach the visibility required to violate Bell's inequalities (70.7 %)". However, this conclusion is inaccurate for the Franson interferometer, as our discussion on the postselection loophole in section 6.2 shows. When using the Bell-CHSH inequality in this setting, there is no way to violate local realism, so *the critical visibility exceeds 100 %.*

In order to notify the authors of this observation we prepared a comment paper, publication F, and sent it to the journal, Physical Review Letters (PRL). There, we briefly reviewed the complications of measuring the Bell value in a system with 50 % post-selection and interpreting the results as a violation of local realism. While our paper was not accepted by PRL for publication, the authors published an erratum [60] to their paper where the quote in the previous paragraph was replaced with "with improved experimental capabilities our approach can lead to a violation of Bell's inequalities". The erratum references our comment (as published on arXiv) and thanks us for bringing the issue to their attention.

Continuing on our discussion on visibility, the next step is the critical visibility for the chained PBC inequality:

Theorem 8.20 (Critical Visibility for Pearle-Braunstein-Caves) *The critical visibility when using $N \geq 2$ settings per observer is*

$$V_{\text{critical},N} = \frac{2N-2}{2N\cos\frac{\pi}{2N}}. \tag{8.26}$$

Proof *The local realist bound for the PBC inequality, $2N-2$ is found in theorem 8.3. Therefore, we put $S_B(N) = 2N-2$ and $S_{QM}(N)$ from theorem 8.4 into definition 8.18 and the result follows.*

Let us now find the critical visibility that must be achieved when performing the PBC security test in the Franson interferometer with fast switching.

Theorem 8.21 (Critical Visibility for the Franson Interferometer with Fast Switching) *The critical visibility for the Franson interferometer when using fast switching and $N \geq 2$ settings per observer is*

$$V_{\text{critical},N,F} \overset{\text{def}}{=} \frac{2N-1}{2N\cos\frac{\pi}{2N}}. \tag{8.27}$$

Proof *With fast switching, the local realist bound for the PBC inequality in the Franson interferometer is $2N-1$ as shown in*

N	$V_{\text{critical},N,F}$	Note
2	>100 %	No security
3	96.23 %	
4	94.71 %	
5	94.63 %	Least restrictive
6	94.90 %	
$N \geq 7$	increasing with N	

Table 8.2: Minimum visibility required in order for the quantum-mechanical prediction $S_{QM}(N)$ to violate the PBC inequality in the Franson interferometer when using fast switching. Note that the case $N = 2$ (Bell-CHSH) does not allow for a violation of local realism while all $N \geq 3$ do. In fact, the least restrictive number of settings is $N = 5$ where the critical visibility is 94.63 %.

theorem 8.10. Therefore, we put $S_B(N) = 2N - 1$ and $S_{QM}(N)$ from theorem 8.4 into definition 8.18 and the result follows.

The quantity $V_{\text{critical},N,F}$ depends on N and encapsulates the degree of violation produced by the PBC inequality. At $N = 2$, the critical visibility is 106 %, which obviously exceeds 100 % and therefore is unattainable. Table 8.2 lists the critical visibilities for $2 \leq N \leq 6$, and it can be seen that the minima is attained at $N = 5$. As the number of settings increase beyond this point, $V_{\text{critical},N,F}$ is strictly increasing and approaches 1 as $N \to \infty$.

Let us compare table 8.2 with the critical visibility required in a traditional Bell-CHSH experiment (remark 8.19). The lowest critical visibility, 94.63 %, is much higher in the Franson setting than in traditional experiments, where only 70.71 % is required. Compared to traditional devices, it is therefore more difficult to reach the required experimental visibility in the Franson interferometer. At the time of writing publication A, the visibilities in table 8.2 were believed to be too difficult to attain.

However, in 2017 we published publication D, which disproves this belief. This publication reports of an experiment at the University of Padova, Italy, which *did* attain very high visibilities in the

Franson interferometer using the PBC inequality. Naturally, such high visibilities require a very stable setup, and we achieved this by independently stabilizing the analysis stations, which allows both phase mismatch due to the path and phase mismatch due to the pump laser to be minimized. This negates environmental disturbances such as temperature variations, which in turn stabilizes the wavelength of the laser, keeping the phase stable and visibility high.

Very high visibilities (up to 99 %) were achieved for $N = 3, 4$, and 5 settings per observer, which would be enough to close the postselection loophole in a full experiment. However, fast switching was not used, and we therefore did not truly violate local realism in the Franson interferometer. Still, it shows that high enough visibilities can be achieved experimentally and paves the way for future, loophole-free Franson experiments. As of yet, no experimental realization of the Franson interferometer has closed the postselection loophole and this remains an important goal for the future.

Before December 2016, no experimental test of the PBC inequality had been announced, and publication D was very close to being the first of its kind when it was uploaded to arXiv on December 12th. As it turns out, Tan et al. [158] had performed a related experiment where trapped $^9\mathrm{Be}^+$ ions were used to test the PBC inequality for all $2 \leq N \leq 15$ with a high detection efficiency. That paper was submitted to PRL on the 5th of December, exactly one week before we publicly announced publication D. Still, our experiment was the first test of a chained Bell inequality using photons.

8.3 Modified Franson Setups

We have now seen how chaining the Bell inequality opens up the possibility for secure QKD based on the Franson interferometer. By combining fast switching with three to five settings per observer in a high-visibility experiment, the postselection loophole is nearly closed. However, there are other possibilities worth mentioning that potentially re-establish security. In this section we will not focus on modifying the security proof, but instead discuss these options for modifying the setup of the Franson interferometer. It must be pointed out that these modifications deviate significantly from the original proposal by Franson [40], and they must therefore be considered to be separate devices altogether. A more extensive discussion on modified setups can be found in publication A.

Path Realism

We begin with a possibility that does not require *physical* modifications to the Franson setup, yet immediately closes the postselection loophole. In theory, it is possible to re-establish security by discarding the DI security assumptions and instead require that *paths* inside the analysis stations be realist properties. This concept is referred to as *path realism*, and essentially forces the photons to behave like particles. When a photon enters an analysis station it will encounter the first beam splitter and "decide" whether to "take" the long path or the short path. Such a "decision" must occur before it can "read" the setting of the phase modulator, which, in turn, forces it to be independent of the *local* setting. Compare to standard Bell experiments, where only independence of the *remote* setting is required.

With path realism, there is no difference between the cases "both photons taking the short path" and "both photons taking the long path" as the existence of delay cannot depend on the local setting. Therefore, even though we must condition on coincidence, the standard Bell-CHSH bound in theorem 4.7 applies separately to both paths. With path realism we therefore have

Theorem 8.22 (Bell-CHSH with Path Realism) *The outcomes from a local realist system with path as a realist, setting-*

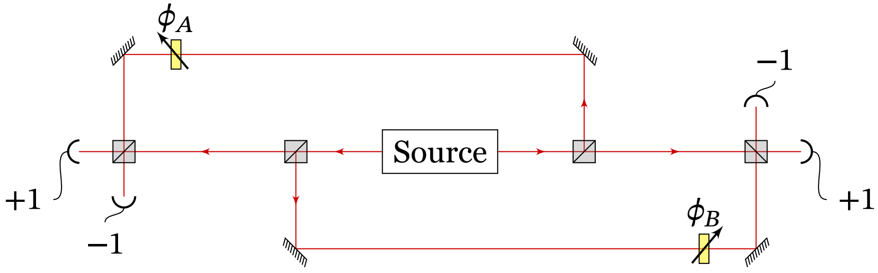


Figure 8.2: Hugging interferometers, or Genuine Energy-Time Entanglement (GETE). This setup has many of the properties of the original Franson setup but allows the postselection loophole to be closed.

independent property and two settings per observer obey

$$\begin{aligned} &\left|E(A_1B_1|\Lambda_{A_1B_1}) + E(A_2B_1|\Lambda_{A_2B_1})\right| \\ &\quad + \left|E(A_1B_2|\Lambda_{A_1B_2}) + E(A_2B_2|\Lambda_{A_2B_2})\right| \leq 2. \end{aligned} \tag{8.28}$$

Proof *See publication A.*

Note that with path realism, quantum mechanics can violate the local realist bound, even when we take postselection into account. Can this be used to re-establish unconditional security in the Franson interferometer? No, not by itself. Recall that path realism discards the DI security assumptions, and therefore a Bell inequality no longer qualifies as a security proof. Instead, the situation is closer to traditional DI setups, like BB84, where security depends on low-level properties. We discuss path realism in detail in publication A, but the conclusion must be that it is not a way forward for practical QKD.

Genuine Energy-Time Entanglement

Another countermeasure discussed in publications A and B consists of installing a *second* quantum channel between the source device and Alice's and Bob's analysis stations (figure 8.2). This is the "hugging" configuration and was first suggested by Cabello

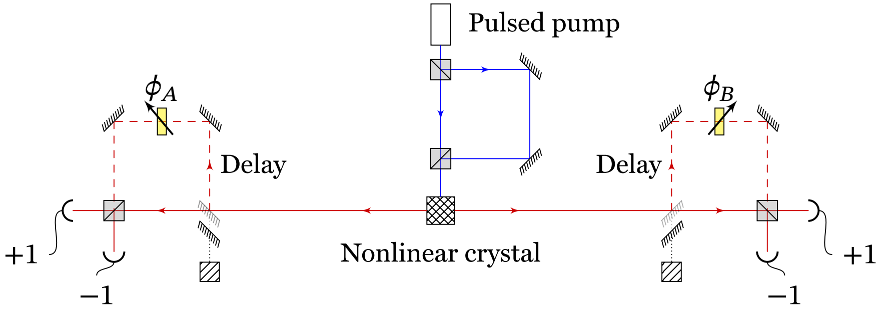


Figure 8.3: Energy-Time Entanglement (ETE) with optical switches synchronized with the source. An early photon would take the long, delayed, path while a late photon is immediately detected. This results in a setup without the postselection loophole.

et al. [159] in 2009. This device is often referred to as Genuine Energy-Time Entanglement (GETE) and requires postselection just like the Franson setup. Here, a local measurement can predict the path taken in the remote analysis station. As a consequence, theorem 8.22 applies, the quantum prediction violates the local realist bound, and we can prove DI security even in the face of postselection.

The drawback of GETE is the added cost of an extra quantum channel. However, the combination of a quantum violation of local realism and a DI security proof without relying on delicate polarization states, has led to increased interest from experimentalists. The first experimental violation of Bell-CHSH using GETE was reported in 2013 by Cuevas et al. [160], where Alice and Bob were separated by 1 km. Later, Carvacho et al. [161] used an existing optical fiber network with a total length 3.7 km to close the postselection loophole in a similar experiment.

Switched Interferometer

Another setup discussed in publication A is a proposal by Brendel et al. [162] from 1999 where the first beam splitter is replaced by an electrically controlled switch, see figure 8.3. The source device is an unbalanced MZ interferometer where a pulsed single-photon laser pumps a nonlinear crystal in order to produce a pair of time-entangled photons in either the early or late timeslot. This is called *time-bin encoding*. The time difference between the early and late timeslots is ΔT, which precisely matches the time difference between the short and long paths in the analysis stations.

An early photon arriving at the analysis station will be routed into the long path by the optical switch, which is synchronized with the pump. The optical switch is then fast enough to switch to the other position, in order to route the inoming late photon into the short path. As the path difference ΔT matches the ΔT of the source, the two possible photons will interfere at the "combiner" beam splitter before detection. As shown in publication A, there will be no need for postselection, so the standard Bell-CHSH inequality in theorem 4.7 applies without the need for conditioning.

The challenge for the switched interferometer is the need for a very fast and controllable optical switch. In their proposal, Brendel et al. [162] use a time difference ΔT as small as 1.2 ns. With the exception for the switch, the rest of the proposal is relatively simple to construct, needs only one quantum channel, does not need polarization, has an attractively simple security proof and only needs the standard Bell-CHSH visibility of 70.71 % (remark 8.19).

Seeing as the optical switch is the Achilles heel of the switched interferometer, we want to propose a novel, and previously unpublished, modification to the setup that retains the advantages but allows for cheaper, more slow-moving switches to be used. By making the time difference ΔT very large, the switch will have more time to operate. However, merely increasing the time difference will adversely affect the key rate as the bit rate is at most $1/\Delta T$. The following trick, however, allows fast key rates with a large ΔT: The pump emits k photons at a rate much faster than $k/\Delta T$ before turning off until the cycle repeats.

The optical switch still switches between the two paths in unison with the source, so all early photons are routed into the long path, while the late photons take the short path. The key rate therefore increases by a factor of k compared to only sending one photon per cycle. The drawback is that the three optical delay paths of length ΔT become more difficult to stabilize as they are long. Still, this approach allows the designer to make a trade-off between difficulty of stabilization and, the cost of the optical switches while maintaining key rate.

8.4 Conclusions

We have reviewed a number of options for re-establishing unconditional security in the Franson interferometer. Importantly, the security must stem from a correct security proof and not ad hoc countermeasures to specific known attacks.

Chaining the Bell inequality together with fast switching allows the postselection loophole to be closed, however the cost is a marked increase in required visibility, detection efficiency, and coincidence probability. Modified setups such as the hugging configuration or using optical switches also provide testable security guarantees and appear experimentally viable. Publication A discusses an additional modified Franson setup.

Chapter 9

Quantum Bitcoin

> So maybe that's the reason for No-Cloning: because God wanted us to have e-commerce, and didn't want us to have to bother with blockchains (and certainly not with credit card numbers).
>
> — Scott Aaronson, 2016 [163]

The goal of this chapter is to present publication E, a contribution that for the first time combines the two research areas of quantum money and blockchain technology. We begin with a short history of computer networks and build up to the motivation for Quantum Bitcoin.

Packet-switching networks made their breakthrough with the advent of ARPANET, the first predecessor of what we today call the Internet [164]. Packet switching allows digital information to be grouped into distinct blocks, or packets, which can then be transmitted over a medium together with other packets to and from other applications and/or users. This method is different from circuit switching, where two peers connect by allocating a dedicated point-to-point connection [165].

With packet switching, different traffic flows can be routed independently of each other as they are traverse a network. If the network topology changes, routing protocols automatically update, ensuring uninterrupted traffic flow. Lost packets can be detected and, if needed, re-transmitted transparently to the user. Packet switching and automatic routing protocols gives the Internet a high degree of tolerance against random faults and the semi-decentralized design of applications such as web browsing and e-mail, make them highly resilient and difficult to censor. Even the loss of a large number of nodes is unlikely to disrupt all providers simultaneously.

For the end user, these developments allowed cheap and reliable means of communication. Anybody can send messages to anybody else as long as they use the same protocol. E-mail servers listen for incoming connections on open ports exposed to the Internet, facilitating delivery no matter where the sender is located. However, communications became so cheap that it also became easy to send *unsolicited* messages, which is popularly known as *spam*. This was first recognized in a Request For Comments (RFC) as early as 1975 [166], and Denning [167] called it “Receiver’s Plight” in 1982.

9.1 Hashcash

As the Internet grew more and more popular, so did spam. By 2010, it was estimated that 89 % of all email messages on the Internet could be attributed to spam [168]. In comparison, a study from 1997 estimated the spam volume at that time to be between 2 % to 10 %, so there was a remarkable increase during the 2000s. One contributing factor to the spam problem was identified by Cranor and LaMacchia [169] to be the low cost of sending large volumes of e-mail. They argued that a bulk mailer can send hundreds of thousands of messages every day and turn a profit “even if only a tiny fraction of the messages they send out result in sales” [169].

Dwork and Naor [170] suggested a system of usage fees as a prevention method for increasing sender cost, which in turn discourages spam. In their paper, published as early as 1992, we can identify the first trace of a method that today is a cornerstone of the Bitcoin protocol: By requiring a sender to compute a "moderately easy" function $f(x)$ for every e-mail to be sent, legitimate usage remains cheap. Unsolicited bulk e-mail, however, becomes expensive enough to prevent abuse. The function argument x depends on the contents of the e-mail to be sent, in order to force a new computation for every recipient. This idea was independently invented by Back [171] who developed Hashcash in 1997 (paper published in 2002).

Hashcash is a refinement of the above idea of a "moderately easy" function. In order to send an e-mail, the sender has to solve a Proof of Work (PoW) puzzle in order to prove to the recipient that a certain amount of computing power (or equivalently, energy) has been spent to send it. In other words, the client has to pay to send messages! More precisely, we want a PoW puzzle to have the following properties:

Definition 9.1 (Properties of Proof-of-Work Puzzles) *A PoW puzzle must have the following four properties:*

- *Difficult to find a solution.*
- *Easy to verify (or disqualify) a solution.*
- *The difficulty of finding a solution should be scalable.*
- *The problem depends on the message to be sent.*

When sending a message to a server using Hashcash, the server responds with a puzzle. This puzzle depends on the message, and possibly some additional data such as a timestamp and a random number. The client will then have to find a solution, send the solution, puzzle[1], and message back to the server. The

[1] In order to prevent against flooding, the server never stores the puzzle. Instead, the client must include the original puzzle in the response and the server can verify the authenticity with, for instance, a symmetric key. A similar method is used in the Transmission Control Protocol (TCP) to prevent an attacker from using up all resources of another peer on the network.

server can compare the given puzzle with the solution provided by the client, and if the solution is correct it means the client has spent energy to find it. In that case, the server delivers the message to the recipient. If the solution is incorrect, the message is simply discarded. In times of heavy load, the server can scale the difficulty for the client in order to reduce load and further discourage unsolicited messages.

Back [171] introduced a PoW scheme based on *hash functions*. A hash function is a map from k to n bits where n is fixed:

$$\begin{aligned} H &: \mathbb{F}_2^k \to \mathbb{F}_2^n \\ m &\mapsto H(m). \end{aligned} \tag{9.1}$$

Normally, k is much greater than n. In other words, a hash function takes any binary string as input and outputs a fixed-length binary string. In addition, Hashcash requires the hash function to be *cryptographically secure*, which means hash function must be *pre-image resistant* and *collision resistant*. Pre-image resistance is the requirement that the hash function is one-way, that is, given a hash value h it should be difficult to find m so that $H(m) = h$ (see section 1.3). Collision resistance means it should be difficult to find messages with the same hash value, i.e., given m with the hash value $H(m)$, it should be difficult to find $m' \neq m$ such that $H(m') = H(m)$. Note that because the hash function has a fixed-length output but takes arbitrary length inputs, it is not injective.

The Hashcash PoW puzzle uses *partial hash collisions*: Let H be a public, cryptographically secure hash function with fixed output length n. Given a message m, the server can compute a challenge in the form of a binary string c and a threshold k. Normally c depends on not only m, but also on a timestamp and some random number, in order to make c unpredictable. The puzzle is to find a binary string x so that $H(c||x)$ is smaller than the threshold k. Here, the $||$ indicates concatenation of strings.

Since H is a cryptographically secure hash function, the output is unpredictable, and the only method for finding a solution x is a costly exhaustive search. Note that because a hash function is not injective, several solutions are possible, but when a solution is found, it takes just one hash operation ($H(c||x)$ to verify that the solution is correct. In addition, the threshold k allows dynamic scaling of the difficulty. Therefore, finding partial hash collisions is a PoW puzzle that fulfills all requirements of definition 9.1.

While Hashcash never found success as an anti-spam measurement for e-mail, PoW was found to be useful to protect against a *Sybil attack*. An attacker performing a Sybil attack presents multiple identities to the network [172]. For example, the aforementioned problem of spam is a simple example of a Sybil attack because one spammer usually pretends to be a different sender for each message sent. A more complex example is an online voting system, or even a poll on a website. If the authentication is weak, an attacker may cast several votes instead of just one, thereby gaining an inflated amount of power.

9.2 Bitcoin

Another application of PoW is in cryptographic currencies, of which Bitcoin [9] is the most prominent example. Bitcoin is a peer-to-peer currency where transactions are verified by a network of users instead of an intermediator. Here, a Sybil attack is a serious threat, but we will show how this is prevented with a PoW mechanism. The mystery surrounding the identity of Bitcoin's pseudonymous inventor Satoshi Nakamoto is the fuel for legends, but since the 2008 whitepaper was published the currency has seen remarkable adoption. At the heart of the protocol is a *consensus mechanism*, where a heterogenous and dynamically changing group of peers agree on the state of the system without a central clearing house.

This consensus mechanism is used by Bitcoin to prevent the problem of *doublespending*, i.e., spending the same unit of currency twice. Doublespending is probably the most serious concern in any digital currency, since digital information in contrast to physical banknotes and coins can be copied at will. If a single peer is able to perform a doublespend, it is safe to assume that the currency will fail completely.

The consensus mechanism in Bitcoin, reminiscent of a traditional voting system, therefore introduces a significant amount of complexity in preventing such doublespends. If a peer announces a new state transition (i.e., currency transaction), the other peers either accept or refuse this new state. Note that these other peers cannot be trusted on an individual basis, and there is no way of knowing the number of peers in such a heterogenous and dynamically-changing network as that of Bitcoin. Therefore, it is impossible to use traditional majority voting since there is no way of knowing when a majority is achieved. In addition, an attacker can perform a Sybil attack and flood the network with invalid confirmations in order to make it accept a doublespend.

Bitcoin uses a variant on the PoW puzzle in Hashcash to prevent these invalid votes. No traditional authentication method of the voting peer is satisfactory, however a proof of spent energy is an authentication method in itself. If a confirmation is paired with such a proof, the rest of the peers can verify the difficulty of casting that vote. In contrast to Hashcash, the PoW puzzle in Bitcoin is designed to be extremely difficult to solve. For example, in July 2017 the Bitcoin network required the first 68 bits of the hash value to be zero. As the hash algorithm H is SHA-256 [173], and assuming this to be a cryptographically secure hash algorithm, all output values are equally probable. The success probability of a single trial is then $2^{-68} \approx 3.39 \times 10^{-21}$.

A reasonable performance figure for a powerful, generic computer is ten million SHA-256 hashes per second, or $10\,\mathrm{Mhash\,s^{-1}}$ [174]. With such hardware it will, on average, require a million years to solve the PoW puzzle once. A specialized state-of-the art machine is much faster, but still requires large amounts of energy to succeed. In Bitcoin today, peers use Application-Specific Integrated Circuit (ASIC) computers and achieve hash rates of approximately 10^{12} hashes per second [174]. ASIC computers are highly energy efficient and use

1.5 Ghash J^{-1} [174]. On average, an ASIC will therefore require 63 MW h to solve the PoW puzzle, which is equivalent to the energy released by burning 42 barrels of crude oil!

Clearly, the PoW puzzle in Bitcoin is much more difficult than a practical e-mail spam prevention system could ever be. However, because those who solve Bitcoin PoW puzzles are rewarded, it has become a lucrative enterprise to spend energy to do so. In July 2017, the global hash rate of the Bitcoin network exceeded 7×10^{18} hashes per second, and it has been estimated [175] that the corresponding energy consumption is 14 TW h per year, which is more than the entire country of Slovenia in 2016 [176].

Note that Bitcoin has no explicit mechanism for "voting against" a transition. Instead, peers who disagree explicitly confirm their own version of the new *block* (Bitcoin jargon for a state transition), and whoever solves the PoW puzzle first has the deciding vote. In addition, each block is numbered, and the puzzle for block $n + 1$ depends on the hash value of block n. Therefore, a confirmation implicitly confirms all prior blocks, and the blocks form a long chain ("blockchain") leading back all the way to the initial "genesis" block.

The protection against a Sybil attack in Bitcoin therefore works as follows: An attacker must spend a large amount of resources in order to solve the current PoW puzzle. This is done in competition with other peers on the network who also solve puzzles. Not only must the attacker solve the puzzle faster than the rest of the network, he or she must do so several times in a row. In Bitcoin, clients typically require a block to have been *confirmed* six times by new, consecutive blocks, so an attacker controlling as much as 1 % of the global hashing power has a success probability of only $0.01^6 = 10^{-12}$.

Nakamoto [9] showed that, as long as a majority of hashing power is controlled by "honest" peers (i.e., they only confirm "valid" blocks), the success probability of the attacker is exponentially small in the number of required confirmations. In addition, peers are only rewarded for successful PoW solutions after 50 consecutive blocks, so there is a strong economic incentive in place to reward miners who stay hones.

In Bitcoin, new transactions are initiated by a peer by broadcasting signed transaction messages that indicate to and from which accounts the funds are to be transferred. Accounts are randomly generated and identified by their hash values. The digital signature algorithm is ECDSA, and the public-private key pair is related to the address of the account. We will not give further details of the Bitcoin protocol – a more detailed account is given in Nakamoto [9].

9.3 Further Blockchain Developments

Nakamoto invented the blockchain and used it to construct a digital currency. It was later discovered that this type of distributed, tamper-proof database is useful for other purposes than just money. Of particular note is Ethereum, published by Buterin [10] in 2013. Here, the blockchain is used as envisioned in section 9.2: as a state machine where transactions provide transitions between states. Importantly, Ethereum combines this state machine with a Turing-complete programming language to allow this “blockchain computer” to run computer programs called *smart contracts*.

Smart contracts, just like computer programs, can be programmed for a wide variety of applications. Examples include distributed data storage [177], voting and governance systems [178], supply chain management [179], and financial technology (fintech) [180].

For the purposes of this thesis we are primarily interested in storing small amounts of data with very high integrity requirements. Publication E introduces the following model for a blockchain-based storage system:

Definition 9.2 (Distributed Ledger Scheme) *A distributed ledger scheme $\mathcal{L}$ consists of the following classical algorithms:*

- $\mathsf{Append}_{\mathcal{L}}$ *is an algorithm that takes some key-value pair* (k, d) *as input. The algorithm fails if the key k is already in the blockchain, and stores* (k, d) *otherwise.*
- $\mathsf{Lookup}_{\mathcal{L}}$ *is a polynomial-time algorithm that takes as input a key* k' *and returns* d *if there exists a key-value pair* (k, d) *such that* $k = k'$*. If not, the algorithm fails.*

We end this section with a short discussion on the security of blockchain architectures. Bitcoin uses ECDSA with the elliptic curve `secp256k1`, and most blockchain systems have followed the same path. However, as mentioned in section 1.4, Shor's algorithm can defeat ECDSA, so Bitcoin and blockchain systems are generally not quantum-safe. The obvious solution is to use a PQC digital signature scheme, however Kiktenko et al. [181] proposed a different solution where a blockchain is implemented over QKD links. As QKD supposedly resists any attack, this would make the system secure even if quantum computers become a reality. However, as we have discussed in this thesis, the security of QKD is not as clear-cut as some it is sometimes described.

9.4 Quantum Money

Until recently, the no-cloning theorem was attributed to the 1982 paper by Wootters and Zurek [182]. Recently, however, an obscure paper by Park [183] has been discovered, where an explicit proof of the theorem was given as early as 1970 [184]. An even earlier allusion can be traced back to 1968, when Wiesner [185] described "conjugate coding", i.e., the coding of classical information onto quantum basis states that cannot simultaneously be measured. Wiesner, however, did not publish this manuscript until 1983 [186].

Wiesner's paper is groundbreaking because it is the first application of quantum information to cryptography, predating even the 1984 paper on BB84 by Bennett and Brassard [65]. In addition, it started the field of *quantum money*, which uses the

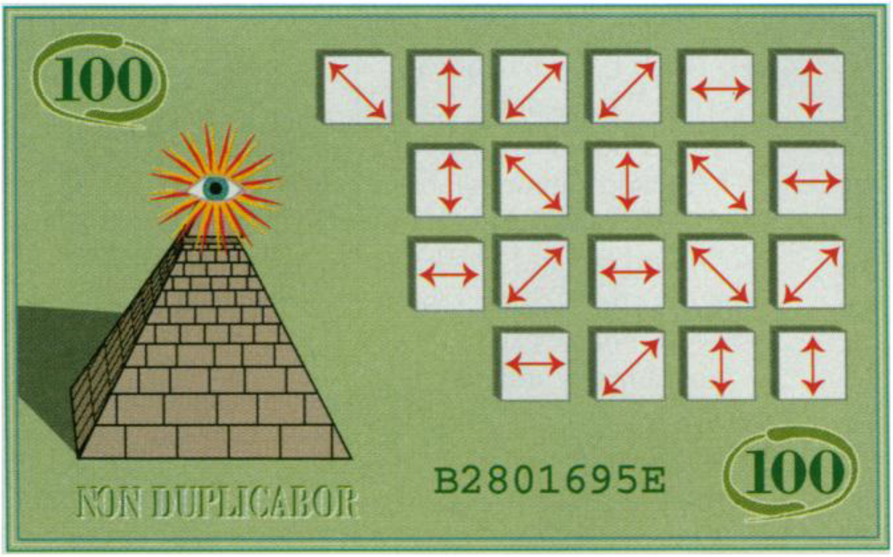


Figure 9.1: Quantum banknote in Wiesner's quantum money scheme with 20 qubits as depicted by Bennett [187]. Note the classical serial number printed on the bottom of the banknote. Image copyright © 1992 The American Association for the Advancement of Science, reused with permission[2].

no-cloning theorem to create money tokens that are impossible to forge. Wiesner's quantum money scheme consists of *quantum banknotes* with a number of qubits and ostensibly has unconditional security. The mint is a trusted entity who creates banknotes by randomly selecting a public serial number s. Next, it chooses a private key $k^{(s)} \in \{0, 1, +, -\}^n$ and creates a *quantum money state*

$$|\$\rangle \overset{\text{def}}{=} \left|k_1^{(s)}\right\rangle \otimes \left|k_2^{(s)}\right\rangle \otimes \cdots \otimes \left|k_n^{(s)}\right\rangle, \tag{9.2}$$

where $|0\rangle$, $|1\rangle$, $|-\rangle$, and $|+\rangle$ are the computational and diagonal bases defined in equations (2.18) and (2.19). The pair $(s, |\$\rangle)$ is the quantum banknote and the bank stores a list of all issued serial numbers and corresponding private keys. Figure 9.1 shows an artist's depiction of a quantum banknote in Wiesner's scheme.

[2] RightsLink license number 4174141186211.

If Alice wants to spend a Wiesner banknote, she must go to the bank, as it is the only entity able to perform verification. Therefore, let Alice send a (potentially forged) Wiesner banknote $(s, |\psi\rangle)$ to the bank. The bank will measure each qubit in the banknote in a basis that depends on the private key. The i^{th} qubit is measured in the $\{|0\rangle, |1\rangle\}$ basis if the corresponding private key $k_i^{(s)}$ is 0 or 1. Conversely, if $k_i^{(s)}$ is $+$ or $-$, the measurement will be performed in the $\{|+\rangle, |-\rangle\}$ basis. If all measurement outcomes agree with the private key, the banknote is deemed valid.

A counterfeiter wanting to duplicate the banknote cannot straight up copy the qubits due to the no-cloning theorem. Instead, the qubits can be prepared randomly, and the success probability will be $(3/4)^n$. According to Aaronson and Christiano [188], Wiesner's scheme suffers from three distinct drawbacks:

1. The "Verifiability Problem": Only the bank can verify banknotes.
2. The "Online Attack Problem": A bank that returns invalid banknotes to the sender allows a counterfeiter to break the system [188–190].
3. The "Giant Database Problem": The bank must store the serial numbers and private keys for all banknotes in circulation.

In 1982, Bennett, Brassard, Breidbart, and Wiesner (BBBW) [191] proposed a modification to Wiesner's scheme that eliminated the giant database problem, at the cost of the scheme no longer being unconditionally secure. However, both these protocols were broken in 2014 by Brodutch et al. [192]. Another protocol was published by Mosca and Stebila [193] in 2009, where all tokens for a given denomination are identical, and the scheme is therefore called quantum *coins* in contrast to *banknotes*. Several other protocols and attacks have been published in the last decade, [194–196] and the common feature of most of these protocols is that they are *private-key*. Private-key quantum money means that the bank must be involved whenever a banknote is to be verified (compare with the "Verifiability Problem" above). Of course, requiring the bank to take part in every transaction is clumsy, so private-key money becomes cumbersome to use. Compare this to "classical" banknotes where the security features are made to be easily verified to a high degree by anyone.

The drawbacks of private-key money has led to an interest in *public-key* quantum money, where the bank only deals with creating the money states – verification can be done by anyone. Quoting Aaronson and Christiano [188, p. 4]:

> As with public-key cryptography in the 1970s, it is far from obvious *a priori* whether public-key quantum money is possible at all. Can a bank publish a description of a quantum circuit that lets people feasibly recognize a state $|\psi\rangle$, but does not let them feasibly prepare or even copy $|\psi\rangle$?

This question has not been satisfactorily answered. The first attempt at a public-key quantum money system was due to Aaronson [189] in 2009, but this scheme was broken by Lutomirski et al. [197] within a few months. Another approach by Farhi et al. [198] uses knot theory, and while this system is unbroken a complete security proof remains elusive.

An important contribution to public-key quantum money is the *reduction scheme* [197, 198], where the quantum money scheme is constructed in a two-step process. The first step is a *mini-scheme* $\mathcal{M}$, which can mint and verify one single unit of currency. Together with a digital signature scheme, the mini-scheme can then be extended to a fully-fledged currency that handles any finite amount of money. The reason for a two-step construction is a security reduction: If the mini-scheme can be proven secure, then the full quantum money system is secure given a secure digital signature scheme [188]. Aaronson and Christiano [188] introduced three proposals for public-key quantum money. The first is an abstract scheme, which uses a random oracle and is proven secure. The second and third schemes are explicit and are based on multivariate polynomials but lack a security proof. Consequently, the noiseless version was broken by Pena et al. [199] but the noisy version remains unbroken for the time being.

Up until this point, all proposed quantum money schemes have had the same underlying topology: a central bank that issues (and possibly verifies) quantum money states, and users who perform transactions and possibly perform verification. This is similar to what digital money looked like before the advent of Bitcoin, with central points of authority having almost ultimate power and responsibility. The first proposal to break this topology came in 2016 with our introduction of *Quantum Bitcoin* in publication E, which is the first attempt at a quantum money scheme with a distributed trust model.

Quantum Bitcoin can either be seen as a blockchain-powered quantum money scheme, or a quantum version of Bitcoin. Either way, publication E shows how any secure public-key quantum money scheme can be used to construct a distributed (bitcoin-like) quantum money scheme. The basic idea is not complicated: Allow anybody to mint new quantum money, but for the money to be valid its serial number must be registered in a blockchain. This mechanism ensures only a fixed rate of new currency is added, similar to the way inflation is controlled in Bitcoin. In contrast to Bitcoin, however, the quantum version does not need to record transactions in order to prevent doublespending as this is already prevented by the no-cloning theorem.

Quantum Bitcoin can therefore be argued to have less complexity than classical Bitcoin, as doublespend protection is a significant part of the latter protocol. The only part of Quantum Bitcoin that requires an expensive, slow call to $\mathsf{Append}_{\mathcal{L}}$, is when new money is issued. As this happens very rarely in comparison to transactions, the protocol is highly efficienct. Peers not performing minting only need to call $\mathsf{Lookup}_{\mathcal{L}}$, which in contrast is a very fast operation. The consequence is instant transactions. Furthermore, as transactions are never recorded, there is no paper trail which makes the currency fully anonymous and untraceable. A more complete review of differences between Quantum Bitcoin, Bitcoin and other money schemes is given in publication E.

The security analysis of Quantum Bitcoin shows it to be secure if at most 15 % of miners are dishonest. This level is lower than the corresponding 50 % limit of classical Bitcoin and is the primary technical challenge faced by the proposal. In addition, Quantum Bitcoin, just like the public-key quantum money scheme by Aaronson and Christiano [188], is not unconditionally secure. Instead, counterfeiting resistance is complexity-theoretic and is shown to require an exponential number of oracle queries in the number of qubits n.

Quantum Bitcoin is the first proposal for a decentralized quantum money system and introduced a number of new ideas and concepts. A follow-up work by Ikeda [200] in 2017 introduced another scheme, dubbed “qBitcoin”, which uses a “quantum chain” instead of the classical blockchain of Quantum Bitcoin. We hope that distributed quantum money schemes will be subject to more research in the future as there are interesting applications.

Chapter 10

Conclusions

This thesis has briefly outlined the history of cryptography leading up to the modern developments of Device-Independent Quantum Key Distribution (DI-QKD) and Energy-Time Entanglement (ETE). In essence, QKD is the ultimate method for communicating secret information as it, in theory, remains secure to any eavesdropper – even in a future where quantum computers are a reality. The slogan of QKD has been "security based on the laws of physics" [93], but as pointed out by Scarani and Kurtsiefer [131], the same laws "do not prevent someone from reading the outcomes of a detector". Just because unconditional security can be proved in theory, it does not mean the system is immune to real-life attacks such as those mentioned in chapter 7. We reiterate the quote by Bell: "what is proved by impossibility proofs is lack of imagination." [137, p. 997].

In chapter 1 we mentioned Schneier's law, which states that cryptographic systems must be exposed to cryptanalysis and extensively tested before they can be trusted to secure sensitive information. Schneier's law also applies to QKD, and as the field is relatively new there is a chance (or risk!) that wonderful discoveries will be made in the near future. Such discoveries could either mean better, improved protocols – but also new avenues for quantum hackers to find exploits. As we are unable to tell the future, we must subject QKD devices and protocols to great scrutiny before marketing them to a wider audience.

It is difficult to prove the security of traditional QKD protocols such as BB84. Even the slightest imperfection can lead to security problems, which ultimately allow an attacker to break the security. As shown in publication A, a security proof based on incorrect assumptions allows an attacker to exploit the system. In contrast, the security test in DI-QKD certifies the whole system in a single step, and by combining DI-QKD with ETE we get a more robust setup compared to systems using polarized photons. As we have conclusively shown in this thesis and publication B, the Franson interferometer together with the Bell-CHSH inequality has a serious weakness that allows Eve to break the security and gain knowledge of Alice's and Bob's secret key.

It is interesting to note that the insufficiency of the original Franson setup has been known for almost 20 years. The first evidence can be found in 1999 when the effect of postselection on the Bell-CHSH inequality in the Franson interferometer was studied by Aerts et al. [138]. Still, the same security test has been used in numerous experiments ever since [41–50]. We consider the lack of security in the standard Franson interferometric setup to be proven beyond doubt, but it is obvious we still have ways to go in educating the scientific community on this issue. In fact, publication F is a comment on an experimental paper that was published as recently as 2017 [58].

In order to make the Franson interferometer immune to our attack, a QKD designer might be tempted to simply add a monitoring device in order to detect bright incoming light. Such a modification would certainly make the specific method in publication B impossible, but it only gives a temporary gain in security. We show in chapter 8 that there is nothing stopping an attacker from modifying modify the attack in order to circumvent the monitoring device. The result is a never-ending cat-and-mouse game no better than the situation of classical cryptography. Instead, a correct security proof relies on a violation of the Bell inequality and cannot be substituted by any patchwork of systems looking for specific attacks. Indeed, we must rely on primitives that can be proven secure and make them robust enough to work in experimental, non-ideal conditions.

There are several ways to construct better primitives, and we have extensively reviewed such methods in chapter 8, including modifying the physical setup and improving the security test. Of particular note is the Pearle-Braunstein-Caves (PBC) inequality, a chained version of the Bell-CHSH inequality, which in publication A was shown to allow a true violation of local realism in the Franson scheme. Testing the PBC inequality, just like any Bell inequality, requires eliminating a number of loopholes. The coincidence-time loophole is a significant consideration in most experimental settings, but its effect on the PBC inequality was not known before publication C. Here, we derived necessary and sufficient conditions for a chained experiment, free of the fair-coincidence assumption. In addition, the PBC inequality has stricter requirements on interferometric visibility than the Bell-CHSH version. In fact, we first believed these requirements were too strict to ever be tested in experiment, but fortunately we were wrong and publication D is exactly such an experiment. Here, we achieved visibilities up to 99 % when testing three different PBC inequalities.

Bridging the gap between the research topics of quantum mechanics and Bitcoin is not a trivial task. Nevertheless, our proposal of Quantum Bitcoin in publication E is the first ever attempt at such a combination. The results are still early, with a relatively weak security proof, but nevertheless a number of advantages over classical Bitcoin can be identified. In fact, publication E argues that, if the proposal can be implemented, the advantages over other forms of currency are significant. Counterfeiting is prohibited by the laws of Nature via the no-cloning theorem, new money can be minted in a transparent, distributed fashion, transactions are instant, and the system can scale to any transaction volume.

10.1 Future Work

In our discussion of loopholes in Bell's Theorem we have reviewed the detection, coincidence-time, and postselection loopholes as well as the effect of visibility. We have provided tight bounds on how far we can stray from the ideal situation before the quantum prediction stops violating local realism. The limitation is that we only studied the different effects individually, and not their joint impact. An experiment with detection efficiency and coincidence probability just above the respective critical limits will probably be vulnerable to an attack as the actual local realist bound is higher than expected. We do expect a real-world experiment to be influenced by visibility, detection efficiency, and coincidence probability all at once, and we should strive towards a general bound taking all this into account. Naturally, the behaviour will probably be complicated and will possibly require numerical computation, but results like these would be of immense help for an experimenter to understand if a trial did show a correct violation.

As discussed in section 8.2, no full experiment that closes the postselection loophole in the Franson interferometer has ever been reported. Publication D comes close, but lacks the necessary fast switching. In the near future, it should be possible to combine high visibilities with fast switching, so we have high hopes for this future work.

We have also assumed Alice and Bob to have access to a perfect RNG for choosing measurement settings. However, non-ideal randomness might allow Eve to predict their choice, thereby allowing an intercept-resend attack. We previously mentioned the use of QRNGs in Bell tests [201, 202], but these cannot be assumed perfect just because they are based on quantum phenomena. In recent years, flaws have been found in popular QRNGs [203, 204], which motivates further study into the effect of bad randomness on the local realist bound. As a first step, we could, for instance, construct a simple model that introduces a certain level of randomness bias. What is the critical bias level where a violation of local realism is no longer possible?

We want to end this thesis by emphasizing that we believe the Franson design to be the way forward for achieving practical QKD. Energy-Time Entanglement allows for a robust physical foundation that requires fewer moving parts than other methods, and by combining this with a Device-Independent security proof we can rule out eavesdroppers more effectively. Short-term, the next step is a full security proof of ETE DI-QKD. Long-term, the recent loophole-free Bell experiments [125–127] is a major breakthrough in our understanding of physics that puts DI-QKD on a solid theoretical foundation. In the future we believe the same level of loophole elimination to be possible on a massive scale in commercial QKD devices.

Index

AES, 6
Alberti, Leon Battista, 2
Alice, 4
analysis station, 30
ARPANET, 117
arrival time, 65, 82
Aspect experiments, 67
Aspect, Alain, 67
assumption
    of fair coincidence, 64, 67
    of fair sampling, 59
attack
    blinding, 84, 97
    intercept-resend, 86, 134
    LHV, 82, 92, 105
    man-in-the-middle, 6, 30
    photon-number-splitting, 84
    Sybil, 121, 122
    Trojan horse, 50, 52
    Trojan-horse, 86
authentication, 4, 6
    Wegman-Carter, 30

basis
    computational, 24, 38, 126
    diagonal, 25, 31, 126
    rectilinear, 25, 31
BB84, 31, 34, 51
BBBW, 127
beam splitter, 86
Bell inequality
    see inequality, Bell-CHSH, 34
Bell state, 24, 38, 48, 53, 54
Bell test, 51, 52, 57, 59
Bell value, 47
    chained, 99
    chained, conditioned, 100
    conditioned, 60
    faked, 58, 59, 84, 86, 90, 92
    quantum prediction, 47
    quantum prediction, chained, 100
    trivial, 47
    trivial, chained, 99
Bell's Theorem, *see* inequality, Bell-CHSH
Bennett, Charles H., 29
Bitcoin, 119, 121, 125
    quantum, *see* quantum, Bitcoin
black box model, 45, 51
block, 123
    genesis, 123
blockchain, 123, 124
Blowfish, 6
Bob, 4
boundedness, *see* system, bounded
bra, *see* bra-ket notation
bra-ket notation, 19
Brassard, Gilles, 29

chaining, *see* inequality, Pearle-Braunstein-Caves
check bits, 33
CHSH, *see* inequality, Bell-CHSH
cipher, 3

substitution, 2
ciphertext, 4
circuit switching, 117
Cirel'son's bound, 48, 92
code, 3
coherent one-way, 31
coincidence probability, 65
critical, 67, 105
trivial, 66
trivial, chained, 105
coincidence-time, *see* loophole, coincidence-time
combiner, 88, 114
commutator, 23
completeness relation, 22
computational basis, *see* basis, computational
conjugate coding, 125
consensus mechanism, 121
cryptanalysis, 2, 19, 131
cryptography, 1, 3
assymetric, *see* cryptography, public-key
lattice-based, 9
post-quantum, 9, 10, 125
public-key, 6
symmetric, 6

dark counts, 64, 91, 106
denial of service, 33
density matrix, 25, 54
DES, 6
detection efficiency, 60, 61
critical, 63, 101
critical, chained, Franson, fast switching, 104
trivial, 62, 101
trivial, chained, Franson, fast switching, 103
device independence, 52, 54, 57
diagonal basis, *see* basis, diagonal
differential phase-shift, 31
digital signature, 4, 124
discrete logarithm, 7
doublespending, 121, 129

E91, 31, 49, 52, 86
ECDSA, 9, 124
Ekert, Arthur, 49
electron, 38
elliptic curve, 8, 125
energy-time entanglement, *see* entanglement, energy-time
entanglement, 48, 49
energy-time, 11, 72
protocol based on, 30, 34, 50, 51, 53, 72
EPR, 37
EPR-Bohm, 38
Ethereum, 124
Eve, 4

factorization problem, 8
fair-coincidence assumption, *see* assumption, of fair coincidence
fair-sampling assumption, *see* assumption, of fair sampling
fast switching, 77, 102
Franson interferometer, 31, 72, 76, 79, 81, 82, 84, 86, 97, 100, 102, 107, 109, 110
variants, 110
fringe visibility, *see* visibility
Frodo, 9
function
hash, *see* hash function
one-way, 7, 120
trapdoor function, 7

gamma photon, 38
GCHQ, 7
giant database problem, 127
Grover's algorithm, 9

half-silvered mirror, *see* beam splitter

hash function, 120
collision resistant, 120
cryptographically secure, 120
pre-image resistant, 120
Hashcash, 119, 122
Hermitian conjugate, 20
Hermitian operator, 20
Herodotus, 3
hidden variable, 39–41, 46, 75, 82
Hilbert space, 20

inequality
Bell, 43, *see* inequality, Bell-CHSH
Bell-CHSH, 46, 54, 75, 98, 111
Bell-CHSH with coincidence probability, 66
Bell-CHSH with detection efficiency, 62
Bell-CHSH, Franson, 76
Bell-CHSH, Franson, fast switching, 79
CHSH, *see* inequality, Bell-CHSH
Cirel'son's, *see* Cirel'son's bound
Freedman's, 67
Pearle-Braunstein-Caves, 98, 99
Pearle-Braunstein-Caves with coincidence probability, 104
Pearle-Braunstein-Caves with coincidence probability, critical, 105
Pearle-Braunstein-Caves with coincidence probability, trivial, 105
Pearle-Braunstein-Caves with detection efficiency, 100
Pearle-Braunstein-Caves with detection efficiency, Franson, fast switching, 103
Pearle-Braunstein-Caves, Franson, 101
Pearle-Braunstein-Caves, Franson, fast switching, 102
information reconciliation, 33, 75
information-theoretic security, *see* security, unconditional
inner product, 20
bra-ket notation, 20
unitary invariance, 20
interferometer, 30
Franson, 73
hugging, 112
Mach-Zehnder, 73
switched, 114
interferometric visibility, *see* visibility
Internet, 117
intractable problem, 10

Kerckhoff's principle, 4, 96
ket, *see* bra-ket notation
key, 4
private, 6, 124
public, 6, 124
raw, 32
secret, 30, 33, 53, 58, 75
sifted, 32

learning with errors, 9
ring, 9
LHV model, 46, 81, 82, 90
linear mode, 85, 90
local hidden variable model, *see* model, local hidden variable
local realism, *see* system, local realist
locality, *see* system, local
loophole, 55, 58, 81
coincidence-time, 65, 67–69
detection, 59, 68, 76, 106

locality, 58, 68
postselection, 76, 102, 107
superdeterminism, 69

Mary, Queen of Scots, 3
measurement
general, 22
projective, 22
measurement-device-independent, 31
message, 4, 32
middle pulse, 90
mini-scheme, 128
modular exponentiation, 7
monitoring device, 96, 97

Nakamoto, Satoshi, 121
NewHope, 9
no-cloning theorem, 27, 125
no-signaling principle, 52, 58
NTRU, 9

observable, 22
online attack problem, 127

packet switching, 117
partial hash collision, 120
path realism, 111
Pauli matrix, 23, 31, 43
Pearle-Braunstein-Caves, *see* inequality, Pearle-Braunstein-Caves
Pearle-Braunstein-Caves value, *see* Bell value, chained
π meson, 38, 50
pion, *see* π meson
plaintext, 4, 10
positron, 38
postselection, 74, 75, 101
postselection loophole, *see* loophole, postselection
prepare-and-measure protocol, 30, 31, 34, 50, 51
principle of local action, *see* system, local
privacy amplification, 33, 75
probability space, 21
proof of work, 119
pump, 114

qBitcoin, 130
quantum
key distribution, 29
algorithm, 8
banknote, 126
bit, *see* qubit
Bitcoin, 129
channel, 11
coins, 127
computer, 8, 49, 131
error correction, 34
state, *see* state
teleportation, 49
quantum hacking, 81
quantum money, 125
distributed, 129
private-key, 127
public-key, 128
state, 126
Wiesner's, 125
quantum-safe
see cryptography
post-quantum, 125
qubit, 8, 31, 43, 54, 126
quenching, 84, 96

random variable, 21
random number generator, 53
pseudo-random, 53
quantum, 53, 68, 134
true, 53
realism, *see* system, realist
rectilinear basis, *see* basis, rectilinear
reduction scheme, 128
refractive index, 87

Rosetta stone, 1
RSA, 8, 9

Schneier's law, 5, 131
secp256k1, 125
secret sharing, 4
security
  by obscurity, 5, 96
  complexity-theoretic, 10
  quantum-safe, *see* cryptography, post-quantum
  unconditional, 9, 96, 97
security test, 51, 55, 77
seed, 53
serial number, 126
SHA-256, 122
Shor's algorithm, 8, 125
side-channel, 58
SIDH, 9
sifting, 32, 75
Skytale, 2
smart contract, 124
source device, 31, 49
spam, 118
spin, 38, 39, 50
splitter, 88
spooky action at a distance, *see* entanglement
state, 22
  faked, 86
  mixed, 25
  non-orthogonal, indistinguishability of, 26
  pure, 22
  separable, 48, 54
  space, 22
  vector, 22, 28
steganography, 3
stenography, 3
system
  bounded, 46
  local, 40, 44, 46, 81
  local realist, 46, 81
  realist, 44, 45, 81

tensor product, 24, 48
time-bin encoding, 114
trapped ion, 68, 110

uncertainty principle, 23, 39
unitarity, 25
unitary map, 20

vector
  orthogonal, 20
verifiability problem, 127
visibility, 106, 107
  critical, 107
  critical, chained, 108
  critical, chained, Franson, fast switching, 108

Bibliography

[1] A. Turing. *Intelligent Machinery*. National Physical Laboratory, July 1948, p. 22.

[2] M. Willett. “Cryptography Old and New”. *Computers & Security* 1.2 (June 1982), pp. 177–186. DOI: 10.1016/0167-4048(82)90010-4.

[3] G. F. Strasser. “The Rise of Cryptology in the European Renaissance”. In: *The History of Information Security*. Ed. by K. D. Leeuw and J. Bergstra. Amsterdam: Elsevier Science B.V., 2007, pp. 277–325. ISBN: 978-0-444-51608-4.

[4] T. Kelly. “The Myth of the Skytale”. *Cryptologia* 22.3 (July 1998), pp. 244–260. DOI: 10.1080/0161-119891886902.

[5] D. Davies. “A Brief History of Cryptography”. *Information Security Technical Report* 2.2 (Jan. 1997), pp. 14–17. DOI: 10.1016/s1363-4127(97)81323-4.

[6] D. Kahn. *The Codebreakers: The Story of Secret Writing*. Macmillan, 1967.

[7] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. “Information Hiding-a Survey”. *Proc. IEEE* 87.7 (July 1999), pp. 1062–1078. DOI: 10.1109/5.771065.

[8] S. Singh. *The Code Book : The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*. New York: Doubleday, 1999. ISBN: 0-385-49531-5.

[9] S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. *Consulted* 1.2012 (2008), p. 28.

[10] V. Buterin. “Ethereum White Paper”. *Consulted* (2013).

[11] W. Trappe and L. Washington. *Introduction to Cryptography: With Coding Theory*. Featured Titles for Cryptography Series. Pearson Prentice Hall, 2006. ISBN: 978-0-13-186239-5.

[12] B. Schneier. “Memo to the Amateur Cipher Designer”. *Crypto-Gram* (Oct. 15, 1998).

[13] K. de Leeuw. “Introduction”. In: *The History of Information Security*. Ed. by K. de Leeuw and J. Bergstra. Amsterdam: Elsevier Science B.V., 2007, pp. 1–25. ISBN: 978-0-444-51608-4.

[14] *FIPS 46-3: Data Encryption Standard (DES)*. Information Technology Laboratory, National Institute of Standards and Technology, July 1977.

[15] *FIPS 197: Advanced Encryption Standard (AES)*. Information Technology Laboratory, National Institute of Standards and Technology, Nov. 26, 2001.

[16] B. Schneier. “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”. In: *Fast Software Encryption*. International Workshop on Fast Software Encryption. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Dec. 9, 1993, pp. 191–204. ISBN: 978-3-540-58108-6. DOI: 10.1007/3-540-58108-1_24.

[17] W. Diffie and M. Hellman. “New Directions in Cryptography”. *IEEE Transactions on Information Theory* 22.6 (Nov. 1976), pp. 644–654. DOI: 10.1109/tit.1976.1055638.

[18] R. L. Rivest, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. DOI: 10.1145/359340.359342.

[19] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, 1996. ISBN: 978-0-471-12845-8.

[20] *FIPS 186-4: Digital Signature Standard (DSS)*. Information Technology Laboratory, National Institute of Standards and Technology, July 2013.

[21] P. W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, NM: IEEE Computer Society Press, Nov. 1994, pp. 124–134.

[22] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt. "Realization of a Scalable Shor Algorithm". *Science* 351.6277 (Mar. 2016), pp. 1068–1070. DOI: 10.1126/science.aad9480.

[23] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland, and J. M. Martinis. "Computing Prime Factors with a Josephson Phase Qubit Quantum Processor". *Nature Physics* 8.10 (Oct. 2012), pp. 719–723. DOI: 10.1038/nphys2385.

[24] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien. "Experimental Realization of Shor's Quantum Factoring Algorithm Using Qubit Recycling". *Nature Photonics* 6.11 (Nov. 2012), pp. 773–776. DOI: 10.1038/nphoton.2012.259.

[25] A. Politi, J. C. F. Matthews, and J. L. O'Brien. "Shor's Quantum Factoring Algorithm on a Photonic Chip". *Science* 325.5945 (Sept. 2009), pp. 1221–1221. DOI: 10.1126/science.1173731.

[26] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan. "Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits". *Physical Review Letters* 99.25 (Dec. 2007), p. 250504. DOI: 10.1103/PhysRevLett.99.250504.

[27] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White. "Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement". *Physical Review Letters* 99.25 (Dec. 2007), p. 250505. DOI: 10.1103/PhysRevLett.99.250505.

[28] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. "Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance". *Nature* 414.6866 (Dec. 2001), pp. 883–887. DOI: 10.1038/414883a.

[29] N. Johansson and J.-Å. Larsson. "Realization of Shor's Algorithm at Room Temperature". *arXiv:1706.03215 [quant-ph]* (June 2017). arXiv: 1706.03215 [quant-ph].

[30] D. J. Bernstein, J. Buchmann, and E. Dahmen, eds. *Post-Quantum Cryptography*. 2009 edition. Berlin: Springer, Nov. 17, 2008. 246 pp. ISBN: 978-3-540-88701-0.

[31] L. K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. New York, NY, USA: ACM, 1996, pp. 212–219. ISBN: 978-0-89791-785-8. DOI: 10.1145/237814.237866.

[32] O. Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography". In: *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*. STOC '05. New York, NY, USA: ACM, 2005, pp. 84–93. ISBN: 978-1-58113-960-0. DOI: 10.1145/1060590.1060603.

[33] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila. “Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’16. New York, NY, USA: ACM, 2016, pp. 1006–1018. ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978425.

[34] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila. “Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem”. In: *2015 IEEE Symposium on Security and Privacy*. 2015 IEEE Symposium on Security and Privacy. May 2015, pp. 553–570. DOI: 10.1109/SP.2015.40.

[35] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. “Post-Quantum Key Exchange - a New Hope”. In: *Proceedings of the 25th USENIX Security Symposium*. Nov. 2015. ISBN: 978-1-931971-32-4.

[36] J. Hoffstein, J. Pipher, and J. H. Silverman. “NTRU: A Ring-Based Public Key Cryptosystem”. In: *Algorithmic Number Theory*. International Algorithmic Number Theory Symposium. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, June 21, 1998, pp. 267–288. ISBN: 978-3-540-64657-0. DOI: 10.1007/BFb0054868.

[37] D. Jao and L. D. Feo. “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies”. In: *Post-Quantum Cryptography*. International Workshop on Post-Quantum Cryptography. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Nov. 29, 2011, pp. 19–34. ISBN: 978-3-642-25404-8. DOI: 10.1007/978-3-642-25405-5_2.

[38] R. J. McEliece. “A Public-Key Cryptosystem Based on Algebraic Coding Theory”. *DSN progress report* 42.44 (1978), pp. 114–116.

[39] D. J. Bernstein and T. Lange. “Post-Quantum Cryptography”. *Nature* 549.7671 (Sept. 2017), pp. 188–194. doi: 10.1038/nature23461.

[40] J. D. Franson. “Bell Inequality for Position and Time”. *Phys. Rev. Lett.* 62.19 (1989), pp. 2205–2208. doi: 10.1103/PhysRevLett.62.2205.

[41] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin. “Experimental Demonstration of Quantum Correlations over More than 10 Km”. *Physical Review A* 57.5 (May 1998), pp. 3229–3232. doi: 10.1103/physreva.57.3229.

[42] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. “Violation of Bell Inequalities by Photons More Than 10 Km Apart”. *Phys. Rev. Lett.* 81.17 (Oct. 1998), pp. 3563–3566. doi: 10.1103/physrevlett.81.3563.

[43] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. “Quantum Cryptography Using Entangled Photons in Energy-Time Bell States”. *Phys. Rev. Lett.* 84.20 (May 2000), pp. 4737–4740. doi: 10.1103/physrevlett.84.4737.

[44] Z. Ou, X. Zou, L. Wang, and L. Mandel. “Observation of Nonlocal Interference in Separated Photon Channels”. *Phys. Rev. Lett.* 65.3 (July 1990), pp. 321–324. doi: 10.1103/physrevlett.65.321.

[45] P. R. Tapster, J. G. Rarity, and P. C. M. Owens. “Violation of Bell’s Inequality over 4 Km of Optical Fiber”. *Phys. Rev. Lett.* 73.14 (Oct. 1994), pp. 1923–1926. doi: 10.1103/physrevlett.73.1923.

[46] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin. “Distribution of Time-Bin Entangled Qubits over 50 Km of Optical Fiber”. *Phys. Rev. Lett.* 93.18 (Oct. 2004). doi: 10.1103/physrevlett.93.180502.

[47] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue. “Entanglement Distribution over 300 Km of Fiber”. *Opt. Express* 21.20 (2013), p. 23241. DOI: 10.1364/oe.21.023241.

[48] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro. “Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry”. *Physical Review Letters* 112.12 (Mar. 2014), p. 120506. DOI: 10.1103/PhysRevLett.112.120506.

[49] D. Grassani, S. Azzini, M. Liscidini, M. Galli, M. J. Strain, M. Sorel, J. E. Sipe, and D. Bajoni. “Micrometer-Scale Integrated Silicon Source of Time-Energy Entangled Photons”. *Optica* 2.2 (2015), p. 88. DOI: 10.1364/optica.2.000088.

[50] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, Alessandro Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong. “Photon-Efficient Quantum Key Distribution Using Time-Energy Entanglement with High-Dimensional Encoding”. *New Journal of Physics* 17.2 (2015), p. 022002. DOI: 10.1088/1367-2630/17/2/022002.

[51] J. Jogenfors. *A Classical-Light Attack on Energy-Time Entangled Quantum Key Distribution, and Countermeasures*. Linköping University Electronic Press, Feb. 2015. ISBN: 978-91-7519-118-8. DOI: 10.3384/lic.diva-114073.

[52] J. Jogenfors and J.-Å. Larsson. “Energy-Time Entanglement, Elements of Reality, and Local Realism”. *Journal of Physics A: Mathematical and Theoretical* 47.42 (Oct. 24, 2014), p. 424032. DOI: 10.1088/1751-8113/47/42/424032.

[53] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson. "Hacking the Bell Test Using Classical Light in Energy-Time Entanglement–based Quantum Key Distribution". *Science Advances* 1.11 (Dec. 18, 2015), e1500793. doi: 10.1126/sciadv.1500793.

[54] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson. *Data from: Hacking the Bell Test Using Classical Light in Energy-Time Entanglement–based Quantum Key Distribution*. 2015. doi: 10.5061/dryad.81b74.

[55] J. Jogenfors and J.-Å. Larsson. "Tight Bounds for the Pearle-Braunstein-Caves Chained Inequality without the Fair-Coincidence Assumption". *Physical Review A* 96.2 (Aug. 1, 2017), p. 022102. doi: 10.1103/PhysRevA.96.022102.

[56] M. Tomasin, E. Mantoan, J. Jogenfors, G. Vallone, J.-Å. Larsson, and P. Villoresi. "High-Visibility Time-Bin Entanglement for Testing Chained Bell Inequalities". *Physical Review A* 95.3 (Mar. 9, 2017), p. 032107. doi: 10.1103/PhysRevA.95.032107.

[57] J. Jogenfors. "Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics" (Apr. 5, 2016). arXiv: 1604.01383 [quant-ph].

[58] M. Peiris, K. Konthasinghe, and A. Muller. "Franson Interference Generated by a Two-Level System". *Physical Review Letters* 118.3 (Jan. 19, 2017), p. 030501. doi: 10.1103/PhysRevLett.118.030501.

[59] J. Jogenfors, A. Cabello, and J.-Å. Larsson. "Comment on "Franson Interference Generated by a Two-Level System"" (Mar. 15, 2017). arXiv: 1703.05055 [quant-ph].

[60] M. Peiris, K. Konthasinghe, and A. Muller. “Erratum: Franson Interference Generated by a Two-Level System [Phys. Rev. Lett. 118, 030501 (2017)]”. *Physical Review Letters* 119.7 (Aug. 2017), p. 079904. DOI: 10.1103/PhysRevLett.119.079904.

[61] P. A. M. Dirac. “A New Notation for Quantum Mechanics”. *Mathematical Proceedings of the Cambridge Philosophical Society* 35.03 (July 1939), p. 416. DOI: 10.1017/s0305004100021162.

[62] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000. ISBN: 978-0-521-63503-5.

[63] W. Heisenberg. “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik”. *Zeitschrift für Physik* 43 (3-4 Mar. 1927), pp. 172–198. DOI: 10.1007/BF01397280.

[64] G. Brassard. “Brief History of Quantum Cryptography: A Personal Perspective”. In: *Theory and Practice in Information-Theoretic Security, 2005. IEEE Information Theory Workshop On*. IEEE, 2005, pp. 19–23.

[65] C. H. Bennett and G. Brassard. “Quantum Cryptography: Public Key Distribution and Coin Tossing”. In: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India: IEEE New York, 1984, pp. 175–179.

[66] J. L. Carter and M. N. Wegman. “Universal Classes of Hash Functions”. *J. Comput. Syst. Sci.* 18 (1979), pp. 143–154. DOI: 10.1016/0022-0000(79)90044-8.

[67] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden. “Fast and Simple One-Way Quantum Key Distribution”. *Applied Physics Letters* 87.19 (2005), p. 194108.

[68] K. Inoue, E. Waks, and Y. Yamamoto. “Differential Phase-Shift Quantum Key Distribution”. In: *Photonics Asia 2002*. International Society for Optics and Photonics, 2002, pp. 32–39.

[69] H.-K. Lo, M. Curty, and B. Qi. “Measurement-Device-Independent Quantum Key Distribution”. *Physical Review Letters* 108.13 (Mar. 2012), p. 130503. doi: 10.1103/PhysRevLett.108.130503.

[70] A. Abidin. *Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions*. Linköping University Electronic Press, 2013. isbn: 978-91-7519-625-1.

[71] D. Mayers. “Unconditional Security in Quantum Cryptography”. *J. ACM* 48.3 (May 2001), pp. 351–406. doi: 10.1145/382780.382781.

[72] C. Bennett, G. Brassard, A. Ekert, C. Fuchs, and J. Preskill. “Summary of the Theory Component of Quantum Key Distribution and Quantum Cryptography”. *Report of the quantum cryptography technology experts panel, Advanced Research and Development Activity (ARDA)* (2004).

[73] M. Koashi and J. Preskill. “Secure Quantum Key Distribution with an Uncharacterized Source”. *Physical Review Letters* 90.5 (Feb. 6, 2003), p. 057902. doi: 10.1103/PhysRevLett.90.057902.

[74] H.-K. Lo and H. F. Chau. “Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances”. *Science* 283.5410 (Mar. 1999), pp. 2050–2056. doi: 10.1126/science.283.5410.2050.

[75] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. “Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels”. *Physical Review Letters* 76.5 (Jan. 29, 1996), pp. 722–725. doi: 10.1103/PhysRevLett.76.722.

[76] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels". *Physical Review Letters* 77.13 (Sept. 23, 1996), pp. 2818–2821. DOI: 10.1103/PhysRevLett.77.2818.

[77] P. Shor and J. Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". *Phys. Rev. Lett.* 85.2 (July 2000), pp. 441–444. DOI: 10.1103/physrevlett.85.441.

[78] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. "Security of Quantum Key Distribution with Imperfect Devices". *Quantum Info. Comput.* 4.5 (Sept. 2004), pp. 325–360.

[79] T. Maudlin. "What Bell Did". *Journal of Physics A: Mathematical and Theoretical* 47.42 (2014), p. 424010. DOI: 10.1088/1751-8113/47/42/424010.

[80] J. S. Bell. "On the Einstein-Podolsky-Rosen Paradox". *Physics (Long Island City, N. Y.)* 1 (1964), pp. 195–200.

[81] H. P. Stapp. "Bell's Theorem and World Process". *Nuovo Cim B* 29.2 (Oct. 1975), pp. 270–276. DOI: 10.1007/bf02728310.

[82] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Physical Review* 47.10 (May 1935), pp. 777–780. DOI: 10.1103/physrev.47.777.

[83] D. Bohm. *Quantum Theory*. Dover Books on Physics Series. Prentice-Hall, 1951. ISBN: 978-0-486-65969-5.

[84] A. Einstein. "Quanten-Mechanik Und Wirklichkeit". *Dialectica* 2.3-4 (Nov. 1948), pp. 320–324. DOI: 10.1111/j.1746-8361.1948.tb00704.x.

[85] J. Baggott. *The Meaning of Quantum Theory: A Guide for Students of Chemistry and Physics (Oxford Science Publications)*. Oxford University Press, 1992. isbn: 0-19-855575-X.

[86] N. Bohr. *The Philosophical Writings of Niels Bohr*. The Philosophical Writings of Niels Bohr. Ox Bow Press, 1934.

[87] A. Pais. "Einstein and the Quantum Theory". *Reviews of Modern Physics* 51.4 (Oct. 1979), pp. 863–914. doi: 10.1103/RevModPhys.51.863.

[88] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. "Proposed Experiment to Test Local Hidden-Variable Theories". *Phys. Rev. Lett.* 23.15 (1969), pp. 880–884. doi: 10.1103/PhysRevLett.23.880.

[89] B. S. Cirel'son. "Quantum Generalizations of Bell's Inequality". *Letters in Mathematical Physics* 4.2 (Mar. 1980), pp. 93–100. doi: 10.1007/BF00417500.

[90] A. K. Ekert. "Quantum Cryptography Based on Bell's Theorem". *Phys. Rev. Lett.* 67 (1991), pp. 661–663. doi: 10.1103/PhysRevLett.67.661.

[91] J. Barrett, L. Hardy, and A. Kent. "No Signaling and Quantum Key Distribution". *Physical Review Letters* 95.1 (June 2005), p. 010503. doi: 10.1103/PhysRevLett.95.010503.

[92] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani. "Device-Independent Quantum Key Distribution Secure against Collective Attacks". *New J. Phys.* 11.4 (Apr. 2009), p. 045021. doi: 10.1088/1367-2630/11/4/045021.

[93] V. Scarani. "The Device-Independent Outlook on Quantum Physics". *Acta Physica Slovaca* 62.4 (2009), pp. 347–409. doi: 10.2478/v10155-012-0003-4.

[94] D. Mayers and A. Yao. “Quantum Cryptography with Imperfect Apparatus”. In: *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*. FOCS ’98. Washington, DC, USA: IEEE Computer Society, 1998, pp. 503–. ISBN: 0-8186-9172-7.

[95] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. “Device-Independent Security of Quantum Cryptography against Collective Attacks”. *Phys. Rev. Lett.* 98 (2007), p. 230501. DOI: 10.1103/PhysRevLett.98.230501.

[96] J.-Å. Larsson. “A Practical Trojan Horse for Bell-Inequality-Based Quantum Cryptography”. *Quantum Info. Comput.* 2.6 (Oct. 2002), pp. 434–442.

[97] A. Acin, N. Gisin, and L. Masanes. “From Bell’s Theorem to Secure Quantum Key Distribution”. *Phys. Rev. Lett.* 97.12 (Sept. 2006), p. 120405. DOI: 10.1103/PhysRevLett.97.120405.

[98] S. Popescu and D. Rohrlich. “Which States Violate Bell’s Inequality Maximally?” *Physics Letters A* 169.6 (Oct. 1992), pp. 411–414. DOI: 10.1016/0375-9601(92)90819-8.

[99] J.-Å. Larsson. “Loopholes in Bell Inequality Tests of Local Realism”. *Journal of Physics A* 47.42 (Oct. 2014), p. 424003. DOI: 10.1088/1751-8113/47/42/424003.

[100] P. Pearle. “Hidden-Variable Example Based upon Data Rejection”. *Phys. Rev. D* 2 (1970), pp. 1418–1425. DOI: 10.1103/PhysRevD.2.1418.

[101] J.-Å. Larsson. “Bell’s Inequality and Detector Inefficiency”. *Physical Review A* 57.5 (May 1, 1998), pp. 3304–3308. DOI: 10.1103/PhysRevA.57.3304.

[102] A. Cabello, J.-Å. Larsson, and D. Rodriguez. "Minimum Detection Efficiency Required for a Loophole-Free Violation of the Braunstein-Caves Chained Bell Inequalities". *Phys. Rev. A* 79.6 (June 2009), p. 062109. doi: 10.1103/PhysRevA.79.062109.

[103] J. F. Clauser and M. A. Horne. "Experimental Consequences of Objective Local Theories". *Physical Review D* 10.2 (July 1974), pp. 526–535. doi: 10.1103/PhysRevD.10.526.

[104] K. Hess and W. Philipp. "A Possible Loophole in the Theorem of Bell". *Proceedings of the National Academy of Sciences* 98.25 (Apr. 12, 2001), pp. 14224–14227. doi: 10.1073/pnas.251524998. pmid: 11724941.

[105] J.-Å. Larsson, M. Giustina, J. Kofler, B. Wittmann, R. Ursin, and S. Ramelow. "Bell-Inequality Violation with Entangled Photons, Free of the Coincidence-Time Loophole". *Phys. Rev. A* 90.3 (Sept. 2014), p. 032107. doi: 10.1103/PhysRevA.90.032107.

[106] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. "Experimental Violation of a Bell's Inequality with Efficient Detection". *Nature* 409.6822 (Feb. 15, 2001), pp. 791–794. doi: 10.1038/35057215.

[107] J.-Å. Larsson and R. D. Gill. "Bell's Inequality and the Coincidence-Time Loophole". *EPL (Europhysics Letters)* 67.5 (Sept. 2004), p. 707. doi: 10.1209/epl/i2004-10124-7.

[108] S. J. Freedman and J. F. Clauser. "Experimental Test of Local Hidden-Variable Theories". *Physical Review Letters* 28.14 (Apr. 3, 1972), pp. 938–941. doi: 10.1103/PhysRevLett.28.938.

[109] R. Holt and F. M. Pipkin. “Quantum Mechanics vs. Hidden Variables: Polarization Correlation Measurement on an Atomic Mercury Cascade”. *Preprint, Physics Dept., University of Southern Ontario, Canada* (1973).

[110] J. F. Clauser. “Experimental Investigation of a Polarization Correlation Anomaly”. *Physical Review Letters* 36.21 (May 1976), pp. 1223–1226. DOI: 10.1103/PhysRevLett.36.1223.

[111] E. S. Fry and R. C. Thompson. “Experimental Test of Local Hidden-Variable Theories”. *Physical Review Letters* 37.8 (Aug. 1976), pp. 465–468. DOI: 10.1103/PhysRevLett.37.465.

[112] L. R. Kasday, J. D. Ullman, and C. S. Wu. “Angular Correlation of Compton-Scattered Annihilation Photons and Hidden Variables”. *Il Nuovo Cimento B (1971-1996)* 25.2 (Feb. 1975), pp. 633–661. DOI: 10.1007/BF02724742.

[113] A. R. Wilson, J. Lowe, and D. K. Butt. “Measurement of the Relative Planes of Polarization of Annihilation Quanta as a Function of Separation Distance”. *Journal of Physics G: Nuclear Physics* 2.9 (1976), p. 613. DOI: 10.1088/0305-4616/2/9/009.

[114] M. Bruno, M. D’Agostino, and C. Maroni. “Measurement of Linear Polarization of Positron Annihilation Photons”. *Il Nuovo Cimento B (1971-1996)* 40.1 (July 1977), pp. 143–152. DOI: 10.1007/BF02739186.

[115] M. Lamehi-Rachti and W. Mittig. “Quantum Mechanics and Hidden Variables: A Test of Bell’s Inequality by the Measurement of the Spin Correlation in Low-Energy Proton-Proton Scattering”. *Physical Review D* 14.10 (Nov. 1976), pp. 2543–2555. DOI: 10.1103/PhysRevD.14.2543.

[116] A. Aspect, P. Grangier, and G. Roger. “Experimental Tests of Realistic Local Theories via Bell’s Theorem”. *Physical Review Letters* 47.7 (Aug. 17, 1981), pp. 460–463. DOI: 10.1103/PhysRevLett.47.460.

[117] A. Aspect, P. Grangier, and G. Roger. “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell’s Inequalities”. *Physical Review Letters* 49.2 (July 12, 1982), pp. 91–94. doi: 10.1103/PhysRevLett.49.91.

[118] A. Aspect, J. Dalibard, and G. Roger. “Experimental Test of Bell’s Inequalities Using Time-Varying Analyzers”. *Physical Review Letters* 49.25 (Dec. 20, 1982), pp. 1804–1807. doi: 10.1103/PhysRevLett.49.1804.

[119] L. Gilder. *The Age of Entanglement: When Quantum Physics Was Reborn*. 1st Printing edition. New York: Vintage, Nov. 10, 2009. 464 pp. isbn: 978-1-4000-9526-1.

[120] A. Aspect. “Bell’s Theorem: The Naive View of an Experimentalist”. In: *Quantum [Un]Speakables*. Springer, Berlin, Heidelberg, 2002, pp. 119–153. doi: 10.1007/978-3-662-05032-3_9.

[121] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. “Violation of Bell’s Inequality under Strict Einstein Locality Conditions”. *Physical Review Letters* 81.23 (Dec. 7, 1998), pp. 5039–5043. doi: 10.1103/PhysRevLett.81.5039.

[122] W. Paul and H. Steinwedel. “Ein Neues Massenspektrometer Ohne Magnetfeld”. *Zeitschrift Naturforschung Teil A* 8 (July 1, 1953), pp. 448–450. doi: 10.1515/zna-1953-0710.

[123] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger. “Bell Violation Using Entangled Photons without the Fair-Sampling Assumption”. *Nature* 497.7448 (May 2013), pp. 227–230. doi: 10.1038/nature12012.

[124] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. "Detection-Loophole-Free Test of Quantum Nonlocality, and Applications". *Phys. Rev. Lett.* 111.13 (Sept. 2013), p. 130406. DOI: 10.1103/PhysRevLett.111.130406.

[125] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons". *Physical Review Letters* 115.25 (Dec. 16, 2015), p. 250401. DOI: 10.1103/PhysRevLett.115.250401.

[126] L. K. Shalm et al. "Strong Loophole-Free Test of Local Realism". *Physical Review Letters* 115.25 (Dec. 16, 2015), p. 250402. DOI: 10.1103/PhysRevLett.115.250402.

[127] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. "Loophole-Free Bell Inequality Violation Using Electron Spins Separated by 1.3 Kilometres". *Nature* 526.7575 (Oct. 29, 2015), pp. 682–686. DOI: 10.1038/nature15759.

[128] A. J. Leggett. "Nonlocal Hidden-Variable Theories and Quantum Mechanics: An Incompatibility Theorem". *Foundations of Physics* 33.10 (2003), pp. 1469–1493. DOI: 10.1023/a:1026096313729.

[129] A. Shimony, M. A. Horne, and J. F. Clauser. "Comment on "The Theory of Local Beables"". *Epistemological letters* 13.1 (1976).

[130] P. C. W. Davies and J. R. Brown, eds. *The Ghost in the Atom: A Discussion of the Mysteries of Quantum Physics*. Reissue edition. Cambridge: Cambridge University Press, July 30, 1993. 176 pp. ISBN: 978-0-521-45728-6.

[131] V. Scarani and C. Kurtsiefer. "The Black Paper of Quantum Cryptography: Real Implementation Problems". *Theoretical Computer Science* 560 (Dec. 2014), pp. 27–32. DOI: 10.1016/j.tcs.2014.09.015.

[132] J. Bogdanski, J. Ahrens, and M. Bourennane. "Single Mode Fiber Birefringence Compensation in Sagnac and "Plug & Play" Interferometric Setups". *Opt. Express* 17.6 (2009), p. 4485. DOI: 10.1364/oe.17.004485.

[133] K. Borzycki and M. Jaworski. "Temperature Dependence of PMD in Optical Fibres and Cables Textquestiondown Part II". In: *2006 International Conference on Transparent Optical Networks*. IEEE, June 2006. DOI: 10.1109/icton.2006.248541.

[134] A. M. Smith. "Polarization and Magnetooptic Properties of Single-Mode Optical Fiber". *Applied Optics* 17.1 (Jan. 1978), pp. 52–56. DOI: 10.1364/AO.17.000052.

[135] E. M. Frins and W. Dultz. "Rotation of the Polarization Plane in Optical Fibers". *J. Lightwave Technol.* 15.1 (1997), pp. 144–147. DOI: 10.1109/50.552122.

[136] V. Hnizdo. "On Bohr's Response to the Clock-in-the-Box Thought Experiment of Einstein". *European journal of physics* 23.4 (2002), pp. L9–L13.

[137] J. S. Bell. "On the Impossible Pilot Wave". *Foundations of Physics* 12.10 (Oct. 1982), pp. 989–999. DOI: 10.1007/BF01889272.

[138] S. Aerts, P. Kwiat, J.-Å. Larsson, and M. Żukowski. "Two-Photon Franson-Type Experiments and Local Realism". *Physical Review Letters* 83.15 (Oct. 11, 1999), pp. 2872–2875. DOI: 10.1103/PhysRevLett.83.2872.

[139] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. “Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination”. *Nat. Photon.* 4 (2010), pp. 686–689. DOI: 10.1038/nphoton.2010.214.

[140] V. Makarov. “Controlling Passively Quenched Single Photon Detectors by Bright Light”. *New Journal of Physics* 11.6 (2009), p. 065003. DOI: 10.1088/1367-2630/11/6/065003.

[141] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. “Full-Field Implementation of a Perfect Eavesdropper on a Quantum Cryptography System”. *Nature Communications* 2 (June 2011), ncomms1348. DOI: 10.1038/ncomms1348.

[142] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer. “Experimentally Faking the Violation of Bell’s Inequalities”. *Phys. Rev. Lett.* 107 (2011), p. 170404. DOI: 10.1103/PhysRevLett.107.170404.

[143] F. Träger. *Springer Handbook of Lasers and Optics*. Springer handbooks. Springer, 2007. ISBN: 978-0-387-30420-5.

[144] S. Popescu and D. Rohrlich. “Quantum Nonlocality as an Axiom”. *Foundations of Physics* 24.3 (Mar. 1994), pp. 379–385. DOI: 10.1007/BF02058098.

[145] Z. L. Yuan, J. F. Dynes, and A. J. Shields. “Resilience of Gated Avalanche Photodiodes against Bright Illumination Attacks in Quantum Cryptography”. *Applied Physics Letters* 98.23 (June 6, 2011), p. 231104. DOI: 10.1063/1.3597221.

[146] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov. “Controlling a Superconducting Nanowire Single-Photon Detector Using Tailored Bright Illumination”. *New Journal of Physics* 13.11 (2011), p. 113042. DOI: 10.1088/1367-2630/13/11/113042.

[147] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. "Avoiding the Blinding Attack in QKD". *Nat Photon* 4.12 (Dec. 2010), pp. 801–801. doi: 10.1038/nphoton.2010.278.

[148] Z. L. Yuan, J. F. Dynes, and A. J. Shields. "Avoiding the Blinding Attack in QKD". *Nature Photonics* 4.12 (Dec. 1, 2010), pp. 800–801. doi: 10.1038/nphoton.2010.269.

[149] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. "Controlling an Actively-Quenched Single Photon Detector with Bright Light". *Optics Express* 19.23 (Nov. 7, 2011), p. 23590. doi: 10.1364/OE.19.023590. arXiv: 0809.3408.

[150] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. "After-Gate Attack on a Quantum Cryptosystem". *New Journal of Physics* 13.1 (2011), p. 013043. doi: 10.1088/1367-2630/13/1/013043.

[151] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. "Thermal Blinding of Gated Detectors in Quantum Cryptography". *Optics Express* 18.26 (Dec. 20, 2010), pp. 27938–27954. doi: 10.1364/OE.18.027938.

[152] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov. "Attacks Exploiting Deviation of Mean Photon Number in Quantum Key Distribution and Coin Tossing". *Physical Review A* 91.3 (Mar. 26, 2015), p. 032326. doi: 10.1103/PhysRevA.91.032326.

[153] S. Braunstein and C. Caves. "Wringing out Better Bell Inequalities". *Annals of Physics* 202.1 (1990), pp. 22–56. doi: 10.1016/0003-4916(90)90339-P.

[154] J. F. Clauser and A. Shimony. "Bell's Theorem: Experimental Tests and Implications". *Reports on Progress in Physics* 41.12 (1978), p. 1881. doi: 10.1088/0034-4885/41/12/002.

[155] Y. Hasegawa, R. Loidl, G. Badurek, M. Baron, and H. Rauch. “Violation of a Bell-like Inequality in Single-Neutron Interferometry”. *Nature* 425.6953 (Sept. 4, 2003), pp. 45–48. DOI: 10.1038/nature01881.

[156] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao. “High-Visibility Interference in a Bell-Inequality Experiment for Energy and Time”. *Physical Review A* 47.4 (Apr. 1, 1993), R2472–R2475. DOI: 10.1103/PhysRevA.47.R2472.

[157] C. J. Broadbent, R. M. Camacho, R. Xin, and J. C. Howell. “Preservation of Energy-Time Entanglement in a Slow Light Medium”. *Physical Review Letters* 100.13 (Apr. 4, 2008), p. 133602. DOI: 10.1103/PhysRevLett.100.133602.

[158] T. R. Tan, Y. Wan, S. Erickson, P. Bierhorst, D. Kienzler, S. Glancy, E. Knill, D. Leibfried, and D. J. Wineland. “Chained Bell Inequality Experiment with High-Efficiency Measurements”. *Physical Review Letters* 118.13 (Mar. 2017), p. 130403. DOI: 10.1103/PhysRevLett.118.130403.

[159] A. Cabello, A. Rossi, G. Vallone, F. De Martini, and P. Mataloni. “Proposed Bell Experiment with Genuine Energy-Time Entanglement”. *Phys. Rev. Lett.* 102 (Jan. 2009), p. 040401. DOI: 10.1103/PhysRevLett.102.040401.

[160] A. Cuevas, G. Carvacho, G. Saavedra, J. Cariñe, W. a. T. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima, and G. B. Xavier. “Long-Distance Distribution of Genuine Energy-Time Entanglement”. *Nature Communications* 4 (Nov. 2013), p. 2871. DOI: 10.1038/ncomms3871.

[161] G. Carvacho, J. Cariñe, G. Saavedra, Á. Cuevas, J. Fuenzalida, F. Toledo, M. Figueroa, A. Cabello, J.-Å. Larsson, P. Mataloni, G. Lima, and G. B. Xavier. “Postselection-Loophole-Free Bell Test Over an Installed Optical Fiber Network”. *Physical Review Letters* 115.3 (July 14, 2015), p. 030503. DOI: 10.1103/PhysRevLett.115.030503.

[162] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. “Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication”. *Phys. Rev. Lett.* 82 (1999), pp. 2594–2597. doi: 10.1103/PhysRevLett.82.2594.

[163] S. Aaronson. *The No-Cloning Theorem and the Human Condition: My After-Dinner Talk at QCrypt 2016*. Sept. 15, 2016. url: https://www.scottaaronson.com/blog/?p=2903 (accessed Oct. 11, 2017).

[164] P. H. Salus. *Casting the Net: From ARPANET to Internet and Beyond...* Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1995. isbn: 978-0-201-87674-1.

[165] T.-y. Feng. “A Survey of Interconnection Networks”. *Computer* 14.12 (Dec. 1981), pp. 12–27. doi: 10.1109/C-M.1981.220290.

[166] J. Postel. “RFC 706: On the Junk Mail Problem”. *Network Working Group, Request for Comments* 706 (1975).

[167] P. J. Denning. “ACM President’s Letter: Electronic Junk”. *Commun. ACM* 25.3 (Mar. 1982), pp. 163–165. doi: 10.1145/358453.358454.

[168] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. “The Underground Economy of Spam: A Botmaster’s Perspective of Coordinating Large-Scale Spam Campaigns”. In: *Proceedings of the 4th USENIX Conference on Large-Scale Exploits and Emergent Threats*. LEET’11. Berkeley, CA, USA: USENIX Association, 2011, pp. 4–4.

[169] L. F. Cranor and B. A. LaMacchia. “Spam!” *Commun. ACM* 41.8 (Aug. 1998), pp. 74–83. doi: 10.1145/280324.280336.

[170] C. Dwork and M. Naor. “Pricing via Processing or Combatting Junk Mail”. In: *Advances in Cryptology — CRYPTO’ 92*. Annual International Cryptology Conference. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg,

Aug. 16, 1992, pp. 139–147. ISBN: 978-3-540-57340-1. DOI: 10.1007/3-540-48071-4_10.

[171] A. Back. “Hashcash, a Denial of Service Counter-Measure”. *Consulted* (Aug. 1, 2002).

[172] J. Douceur. “The Sybil Attack”. In: *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*. Jan. 2002.

[173] *FIPS 180-2: Secure Hash Standard (SHS)*. Information Technology Laboratory, National Institute of Standards and Technology, 2001.

[174] *Mining Hardware Comparison - Bitcoin Wiki*. URL: https://en.bitcoin.it/wiki/Mining_hardware_comparison (accessed July 25, 2017).

[175] *Bitcoin Energy Consumption Index*. 2017. URL: http://digiconomist.net/bitcoin-energy-consumption (accessed July 25, 2017).

[176] *Key World Energy Statistics 2016*. International Energy Agency, 2016.

[177] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin. “Storj: A Peer-to-Peer Cloud Storage Network”. *Consulted* (Dec. 15, 2014).

[178] M. Atzori. *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* SSRN Scholarly Paper ID 2709713. Rochester, NY: Social Science Research Network, Dec. 1, 2015.

[179] M. Pilkington. *Blockchain Technology: Principles and Applications*. SSRN Scholarly Paper ID 2662660. Rochester, NY: Social Science Research Network, Sept. 18, 2015.

[180] Y. Guo and C. Liang. “Blockchain Application and Outlook in the Banking Industry”. *Financial Innovation* 2.1 (Dec. 1, 2016), p. 24. DOI: 10.1186/s40854-016-0034-9.

[181] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov. "Quantum-Secured Blockchain" (May 25, 2017). arXiv: 1705.09258 [quant-ph].

[182] W. K. Wootters and W. H. Zurek. "A Single Quantum Cannot Be Cloned". *Nature* 299 (1982), pp. 802–803. DOI: 10.1038/299802a0.

[183] J. L. Park. "The Concept of Transition in Quantum Mechanics". *Foundations of Physics* 1.1 (Mar. 1, 1970), pp. 23–33. DOI: 10.1007/BF00708652.

[184] J. Ortigoso. "Twelve Years before the Quantum No-Cloning Theorem" (July 21, 2017). arXiv: 1707.06910 [physics, physics:quant-ph].

[185] S. Wiesner. "Conjugate Coding". *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. DOI: 10.1145/1008908.1008920.

[186] C. H. Bennett, G. Brassard, and S. Breidbart. "Quantum Cryptography II: How to Re-Use a One-Time Pad Safely Even If P=NP". *Natural Computing* 13.4 (Dec. 2014), pp. 453–458. DOI: 10.1007/s11047-014-9453-6.

[187] C. H. Bennett. "Quantum Cryptography: Uncertainty in the Service of Privacy". *Science* 257.5071 (Aug. 1992), pp. 752–753. DOI: 10.1126/science.257.5071.752.

[188] S. Aaronson and P. Christiano. "Quantum Money from Hidden Subspaces". *arXiv:1203.4740 [quant-ph]* (Mar. 2012). arXiv: 1203.4740 [quant-ph].

[189] S. Aaronson. "Quantum Copy-Protection and Quantum Money". In: *24th Annual IEEE Conference on Computational Complexity, 2009. CCC '09*. July 2009, pp. 229–242. DOI: 10.1109/CCC.2009.42.

[190] A. Lutomirski. "An Online Attack against Wiesner's Quantum Money". *arXiv:1010.0256 [quant-ph]* (Oct. 2010). arXiv: 1010.0256 [quant-ph].

[191] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. "Quantum Cryptography, or Unforgeable Subway Tokens". In: *Advances in Cryptology: Proceedings of CRYPTO '82*. Plenum, 1982, pp. 267–275. ISBN: 978-1-4757-0604-8. DOI: 10.1007/978-1-4757-0602-4_26.

[192] A. Brodutch, D. Nagaj, O. Sattath, and D. Unruh. "An Adaptive Attack on Wiesner's Quantum Money". *arXiv:1404.1507 [quant-ph]* (Apr. 2014). arXiv: 1404.1507 [quant-ph].

[193] M. Mosca and D. Stebila. "Quantum Coins". *arXiv:0911.1295 [quant-ph]* (Nov. 2009). arXiv: 0911.1295 [quant-ph].

[194] D. Gavinsky. "Quantum Money with Classical Verification". *AIP Conference Proceedings* 1633.1 (Dec. 2014), pp. 135–140. DOI: 10.1063/1.4903116.

[195] A. Molina, T. Vidick, and J. Watrous. "Optimal Counterfeiting Attacks and Generalizations for Wiesner's Quantum Money". In: *Theory of Quantum Computation, Communication, and Cryptography*. Ed. by K. Iwama, Y. Kawano, and M. Murao. Lecture Notes in Computer Science 7582. Springer Berlin Heidelberg, May 2012, pp. 45–64. ISBN: 978-3-642-35655-1.

[196] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac. "Unforgeable Noise-Tolerant Quantum Tokens". *Proceedings of the National Academy of Sciences* 109.40 (Oct. 2012), pp. 16079–16082. DOI: 10.1073/pnas.1203552109. arXiv: 1112.5456.

[197] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor. "Breaking and Making Quantum Money: Toward a New Quantum Cryptographic Protocol". *arXiv:0912.3825 [quant-ph]* (Dec. 2009). arXiv: 0912.3825 [quant-ph].

[198] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor. "Quantum Money from Knots". *arXiv:1004.5127 [quant-ph]* (Apr. 2010). arXiv: 1004.5127 [quant-ph].

[199] M. C. Pena, J.-C. Faugère, and L. Perret. "Algebraic Cryptanalysis of a Quantum Money Scheme The Noise-Free Case". In: IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15). Mar. 30, 2015.

[200] K. Ikeda. "qBitcoin". *arXiv:1708.04955 [quant-ph, q-fin]* (Aug. 2017). arXiv: 1708.04955 [quant-ph, q-fin].

[201] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell. "Generation of Fresh and Pure Random Numbers for Loophole-Free Bell Tests". *Physical Review Letters* 115.25 (Dec. 2015), p. 250403. doi: 10.1103/PhysRevLett.115.250403.

[202] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acın, J. Capmany, V. Pruneri, and M. W. Mitchell. "Ultra-Fast Quantum Randomness Generation by Accelerated Phase Diffusion in a Pulsed Laser Diode". *Optics Express* 22.2 (Jan. 2014), pp. 1645–1654. doi: 10.1364/OE.22.001645.

[203] K. S. Jakobsson. "Theory, Methods and Tools for Statistical Testing of Pseudo and Quantum Random Number Generators". Master Thesis. Linköping University, 2014.

[204] D. Hurley-Smith and J. Hernandez-Castro. "Quam Bene Non Quantum: Bias in a Family of Quantum Random Number Generators". *Cryptology ePrint Archive: Report 2017/842* (2017).

Publications

Publication A

Energy-Time Entanglement, Elements of Reality, and Local Realism

J. Jogenfors and J.-Å. Larsson. “Energy-Time Entanglement, Elements of Reality, and Local Realism”. *Journal of Physics A: Mathematical and Theoretical* 47.42 (Oct. 24, 2014), p. 424032. DOI: 10.1088/1751-8113/47/42/424032

This publication has been removed for copyright reasons. For more information, see http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-140912.

Publication B

Hacking the Bell Test Using Classical Light in Energy-Time Entanglement-Based Quantum Key Distribution

J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson. “Hacking the Bell Test Using Classical Light in Energy-Time Entanglement–based Quantum Key Distribution”. *Science Advances* 1.11 (Dec. 18, 2015), e1500793. DOI: 10.1126/sciadv.1500793.

Copyright © 2015 The Authors, some rights reserved; exclusive licensee American Association for the Advancement of Science. Distributed under a Creative Commons Attribution-NonCommercial License 4.0 (CC BY-NC 4.0). Reprinted with permission.

Raw experimental data published as J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson. *Data from: Hacking the Bell Test Using Classical Light in Energy-Time Entanglement–based Quantum Key Distribution*. 2015. DOI: 10.5061/dryad.81b74.

APPLIED MATHEMATICS

Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution

2015 © The Authors, some rights reserved; exclusive licensee American Association for the Advancement of Science. Distributed under a Creative Commons Attribution NonCommercial License 4.0 (CC BY-NC).

10.1126/sciadv.1500793

Jonathan Jogenfors,[1]* Ashraf Mohamed Elhassan,[2]* Johan Ahrens,[2] Mohamed Bourennane,[2] Jan-Åke Larsson[1]†

Photonic systems based on energy-time entanglement have been proposed to test local realism using the Bell inequality. A violation of this inequality normally also certifies security of device-independent quantum key distribution (QKD) so that an attacker cannot eavesdrop or control the system. We show how this security test can be circumvented in energy-time entangled systems when using standard avalanche photodetectors, allowing an attacker to compromise the system without leaving a trace. We reach Bell values up to 3.63 at 97.6% faked detector efficiency using tailored pulses of classical light, which exceeds even the quantum prediction. This is the first demonstration of a violation-faking source that gives both tunable violation and high faked detector efficiency. The implications are severe: the standard Clauser-Horne-Shimony-Holt inequality cannot be used to show device-independent security for energy-time entanglement setups based on Franson's configuration. However, device-independent security can be reestablished, and we conclude by listing a number of improved tests and experimental setups that would protect against all current and future attacks of this type.

INTRODUCTION

A Bell experiment (*1*) is a bipartite experiment that can be used to test for preexisting properties that are independent of the measurement choice at each site. Formally speaking, the experiment tests if there is a "local realist" description of the experiment that contains these preexisting properties. Such a test can be used as the basis for security of quantum key distribution (QKD) (*2*, *3*). QKD uses a bipartite quantum system shared between two parties (Alice and Bob) that allows them to secretly share a cryptographic key. The first QKD protocol (BB84) (*2*) is based on quantum uncertainty (*4*) between noncommuting measurements, usually of photon polarization. The Ekert protocol (E91) (*3*) bases security on a Bell test instead of the uncertainty relation. Such a test indicates, through violation of the corresponding Bell inequality, a secure key distribution system. This requires quantum entanglement, and because of this, E91 is also called entanglement-based QKD.

To properly show that an E91 cryptographic system is secure or, alternatively, that no local realist description exists of an experiment, a proper violation of the associated Bell inequality is needed. As soon as a proper violation is achieved, the inner workings of the system is not important anymore, a fact known as device-independent security (*5*, *6*) or a loophole-free test of local realism (*7*). In the security context, the size of the violation is related to the amount of key that can be securely extracted from the system. However, a proper (loophole-free) violation is difficult to achieve. For long-distance experiments, photons are the system of choice and one particularly difficult problem is to detect enough of the photon pairs; this is known as the efficiency loophole (*8*–*10*).

If the violation is not good enough, there may be a local realist description of the experiment, giving an insecure QKD system. Even worse, an attacker could control the QKD system in this case. One particular example of this occurs when using avalanche photodetectors (APDs), which are the most commonly used detectors in commercial QKD systems: these detectors can be controlled by a process called "blinding" (*11*), which enables control via classical light pulses. When using photon polarization in the system, and if the efficiency is low enough in the Bell test, the quantum-mechanical prediction can be faked in such a controlled system (*12*, *13*). This means that the (apparent) Bell inequality violation can be faked, making a QKD system seem secure while it is not. Note that a proper (loophole-free) violation cannot be faked in this manner.

Here, we investigate energy-time entanglement–based systems in general and the Franson interferometer (*14*) in particular. Traditional polarization coding is sensitive to polarization effects caused by optical fibers (*15*), whereas energy-time entanglement is more robust against this type of disturbance. This property has led to an increased attention to systems based on energy-time entanglement because it allows a design without moving mechanical parts, which reduces complexity in practical implementations. A number of applications of energy-time entanglement, such as QKD, quantum teleportation, and quantum repeaters are described by Gisin and Thew (*16*). In particular, Franson-based QKD has been tested experimentally by a number of research groups (*17*–*22*).

It is already known that a proper Bell test is more demanding to achieve in energy-time entanglement systems with postselection (*23*, *24*), but certain assumptions on the properties of photons also reduce the demands to the same level as for a photon polarization–based test (*25*, *26*). The property in question is the particle-like behavior of the photon: it does not "jump" from one arm of an interferometer to the other. Clearly, classical light pulses cannot jump from one arm to the other, so the question arises: Is it at all possible to control the output of the detectors using classical light pulses to make them fake the quantum correlations? Below, we answer this question in the positive and give the details of such an attack and its experimental implementation.

Moreover, not only are faked quantum correlations possible to reach at a faked detector efficiency of 100%, but also, it is even possible to fake the extreme predictions of nonlocal Popescu-Rohrlich (PR) boxes (*27*) at this high detector efficiency. These predictions reach the algebraic

[1] Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden.
[2] Department of Physics, Stockholm University, 106 91 Stockholm, Sweden.
*These authors contributed equally to this work.
†Corresponding author. E-mail: jan-ake.larsson@liu.se

maximum 4 of the CHSH (Clauser-Horne-Shimony-Holt) inequality and would make a QKD system user suspicious; an attacker would, of course, not attempt to exceed the quantum bound $2\sqrt{2}$ (*28*). Finally, there are countermeasures that reestablish unconditional security, and we list a few examples, see the study of Jogenfors and Larsson (*24*) for a more complete list.

A Bell test of device-independent security, alternatively local realism, is always associated with a Bell inequality. The relevant part of the E91 QKD protocol up to and including the Bell test looks as follows. The general setup is a central source connected to two measurement sites, one at Alice and the other at Bob. The source prepares an entangled quantum state and distributes it to Alice and Bob, who each can choose between a number of measurement settings for their devices. The output can take the values −1, 0, or +1, denoting, for example, horizontal polarization, nondetection, and vertical polarization. Here, we are considering a pulsed source so that there are well-defined experimental runs and, therefore, also well-defined nondetection events. Alice selects a random integer $j \in \{1, 2, 3\}$ and performs the corresponding measurement A_j. Bob does the same with a random number $k \in \{2, 3, 4\}$ and measurement B_k. The quantum state and measurements are such that if $j = k$, then the outcomes are highly (anti-)correlated. This preparation and measurement process is performed over and over again until enough data have been gathered.

After a measurement batch has been completed, Alice and Bob publicly announce which settings j and k were used (but not the corresponding outcomes). They can then determine which measurements used the same settings $j = k$ and use the highly (anti-)correlated outcomes for key generation. The remaining outcomes corresponding to $j \neq k$ can be used for security testing in the Bell-CHSH (*1*, *29*) inequality

$$\begin{aligned} S_2 = {} & |E(A_1B_2) + E(A_3B_2)| + \\ & |E(A_3B_4) - E(A_1B_4)| \leq 2 \end{aligned} \tag{1}$$

where $E\,(A_jB_k)$ is the expected value of the product, often called "correlation" in this context. If the experimental S_2 is larger than 2, then there is a violation and the system is secure; there can be no local realist description of the experiment. The size of the violation is related to the output key rate; the maximal quantum prediction is $2\sqrt{2}$.

However, a proper violation is difficult to achieve. There are a number of ways that the test can give $S_2 > 2$ but still fail, known as loopholes (*7*). The most serious one is the detector efficiency loophole, wherein nondetections or zeros are not properly taken into account. If the zeros are ignored, conditioning on detection at both sites gives the conditional correlation $E(A_jB_k|\text{coinc.})$ and a modified bound (*9*, *10*)

$$\begin{aligned} S_{2,\mathrm{c}} = {} & |E(A_1B_2|\text{coinc.}) + E(A_3B_2|\text{coinc.})| + \\ & |E(A_3B_4|\text{coinc.}) - E(A_1B_4|\text{coinc.})| \leq \frac{4}{\eta} - 2 \end{aligned} \tag{2}$$

The efficiency η is the ratio of coincidences to local detections (*10*) and needs to be above 82% for the quantum value to give a violation. This is ignored in current experiments, with almost no exception (*30*–*32*). In the context of QKD, ignoring the zeros is allowed only if the attacker (Eve) cannot control the detectors to make no-detections depend on the local settings j and k. Unfortunately, the commonly used APDs can be controlled (*11*, *13*) unless extra precautions are taken.

For this study, we have investigated a quantum device based on energy-time entanglement with postselection. Although the results presented below are acquired from this particular device, the results apply to any such system. The Franson interferometer (*14*) is shown in Fig. 1 and is built around a source emitting time-correlated photons to both Alice and Bob. The unbalanced Mach-Zehnder interferometers have a time difference ΔT between the paths. In our pulsed setting, the time difference between a late and an early source emission is ΔT, giving rise to interference between the cases "early source emission, photons take the long path" and "late source emission, photons take the short path." There will be no interference if the photons "take different paths" through the analysis stations, and those events are discarded as noncoincident in a later step.

The analysis stations have variable phase modulators, and the setting choices are ϕ_j^A for measuring A_j at Alice and ϕ_k^B for measuring B_k at Bob. The quantum state is such that, given coincident detection, the correlation between A_j and B_k is high if $\phi_j^A + \phi_k^B = 0$. In the absence of noise, the correlation between Alice's and Bob's outcomes will be (*14*)

$$E(A_jB_k|\text{coinc.}) = \cos\,(\phi_j^A + \phi_k^B) \tag{3}$$

This again violates the CHSH inequality (*1*), but only if the postselection is ignored (*23*). When postselection is taken into account, one arrives at the inequality (*2*) with η = 50%, giving a bound of 6, which is no restriction. The question now is if Eve can control the system and fake the violation.

RESULTS

Using classical pulses of light as described in the Materials and Methods section, Alice and Bob measure a Bell value of

$$S_2 = 2.5615 \pm 0.0064 \tag{4}$$

which clearly violates the Bell bound 2. Figure 2 shows the variation of S_2 over 27 s as a solid black line. The stand-alone detectors have a faked efficiency of 100% when blinded; however, the detectors do not have identical optical and electrical properties. A slight adjustment of optical blinding power has therefore been used to avoid having both detectors

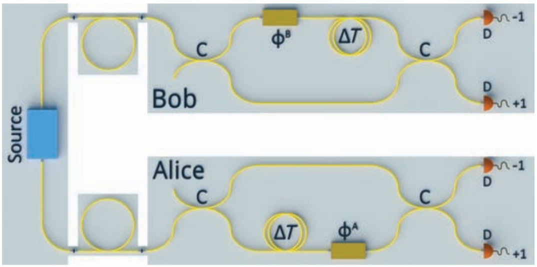


Fig. 1. Experimental setup of the Franson interferometer. The setup consists of a source, 2 × 2 couplers (C), delay loops (ΔT), phase modulators ϕ^A and ϕ^B, and detectors (D).

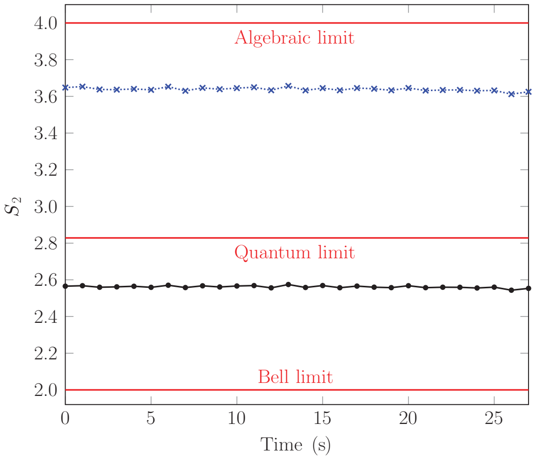


Fig. 2. The faked Bell value of our source is 2.5615 ± 0.0064 (solid black line), which clearly violates the CHSH inequality $S_2 \leq 2$. It is possible to increase the faked Bell value up to 3.6386 ± 0.0096 (dotted blue line, data for time slots where $p \leq r < 1/2 - p$ or $1/2 + p \leq r < 1 - p$). In both cases, the faked efficiency is 97.6%. Each point in the diagram corresponds to the S_2 value for 1 s worth of data.

click simultaneously. This gives a slight reduction in efficiency. Our source has a repetition rate of 5 kHz, and the average rate of clicks is 4.88 kHz, giving an average faked efficiency of 97.6%. The experimental Bell value is lower than the quantum prediction $2\sqrt{2}$ because of noise, most of which is due to unwanted clicks because pulses below the threshold are close to the threshold and are thus sensitive to small-intensity variations of the lasers.

Adjusting the source to produce fake nonlocal PR boxes (*27*) gives a faked Bell value of

$$S_2 = 3.6386 \pm 0.0096 \tag{5}$$

which is even beyond the quantum bound $2\sqrt{2}$. This is plotted in Fig. 2 as a dotted blue line. The faked efficiency remains at 97.6%, and noise still lowers the value from the ideal 4. As previously mentioned, Eve is free to combine pulses and phases at will to produce any Bell value between 0 and the above value 3.63. If the noise rate of the system is known, she can compensate by aiming for a higher Bell value and letting the noise bring it back down. This allows her to reach a faked Bell value that is indistinguishable from $2\sqrt{2}$.

DISCUSSION

Our faked Bell value seemingly violates the Bell-CHSH inequality, even though we are dealing with outcomes produced by classical light, that is, a local realist model. The more appropriate Bell inequality (2) for conditional correlations is clearly ineffective as a test of device-independent security with energy-time entanglement that uses postselection. The bound is too high. We need to improve the security tests in such a way that they unequivocally show security so that they can give a loophole-free violation of local realism.

An intuitive countermeasure to our attack is to add a power monitor to the analysis station that detects if the incoming light is too bright. If such an anomaly is detected, Alice and/or Bob are alerted and discard the relevant measurement outcomes. This modified Franson interferometer would not be vulnerable to the specific attack as described so far; however, it does not solve the postselection loophole, which is the actual issue at hand. Intuitive countermeasures such as power monitors were discussed by Lydersen *et al.* (*33*), who note that attacks can be adapted to such modifications ("a power meter at Bob's entrance…will not reveal the after-gate attack"). A similar argument already appears in the study of Lydersen *et al.* (*11*). In addition, Lydersen *et al.* (*34*) argue that loopholes should be countered by modifying the security proofs, and not by requiring manufacturers to make "frequent, possibly costly upgrades to their systems."

If we want keep the Franson interferometer unchanged, we need to use "fast switching" (*23*, *24*) and Pearle-Braunstein-Caves chained Bell inequalities (*8*, *35*) modified to apply under postselection. Fast switching refers to changing the phase setting so frequently that it is possible to have different phase settings for the two possible time delays, see Jogenfors and Larsson (*24*) for details. The chained inequalities are weakened but still produce a usable bound even after postselection on coincidence

$$\begin{aligned} S_{N,\mathrm{F}} = \; & |E(A_1B_2|\mathrm{coinc.}) + E(A_3B_2|\mathrm{coinc.})| + \\ & |E(A_3B_4|\mathrm{coinc.}) + E(A_5B_4|\mathrm{coinc.})| + \\ & \cdots + \\ & |E(A_{2N-1}B_{2N}|\mathrm{coinc.}) - E(A_1B_{2N}|\mathrm{coinc.})| \leq \\ & 2N-1. \end{aligned} \tag{6}$$

The standard inequalities do not condition on coincidence as is needed here, and they also have the bound $2N - 2$, which is more restrictive. Inequality (6) only gives the upper bound $S_{2,\mathrm{F}} \leq 3$ for the Bell-CHSH value, so the standard test is not useful even with fast switching. However, the quantum-mechanical prediction $S_{N,\mathrm{F}} = 2N \cos(\pi/2N)$ does violate this if $N \geq 3$, even though the violation is smaller than the standard Bell test. This reestablishes device-independent security for energy-time entangled QKD. In practice, though, the experimental requirements are high because the lowest acceptable visibility is 94.64% (*24*).

A better solution would be to eliminate the core problem: the postselection loophole. One alternative is the use of "hugging" interferometers (*24*, *36*) that gives an energy-time entangled interferometer with postselection, but without a postselection loophole. This setup is often referred to as "genuine energy-time entanglement." The drawback is the requirement of not one, but two fiber links each to Alice and Bob. A Bell violation has been shown experimentally (*37*), even with 1-km fiber length (*38*). Another alternative is to replace the first beam splitter of the analysis station with a movable mirror (*24*, *39*, *40*). This setup does not require postselection at all, and therefore, the original CHSH inequality is applicable.

In conclusion, we reiterate that Bell tests are a cornerstone of QKD and are necessary for device-independent security. Device-independent Bell inequality violation must be performed with care to avoid loopholes. Energy-time entanglement has the distinct advantage over polarization in that time and energy are more easily communicated over long distances than polarization. Therefore, energy-time entanglement may be preferable as a quantum resource to perform reliable key distribution.

Here, we have shown that QKD systems based on energy-time entanglement with postselection are vulnerable to attack if the corresponding security tests use the original CHSH inequality. Eve blinds the detectors and uses a local hidden variable (LHV) model to fool Alice and Bob into thinking that their system violates Bell's inequality even though there is no entanglement. Eve only needs access to the source device, not Alice's or Bob's measurement devices or laboratory equipment (including computers). Still, she fully controls the key output and breaks the security of the Franson system without Alice or Bob noticing.

Our attack has been performed with a faked detector efficiency of 97.6%, which is high enough to avoid the fair sampling assumption. It also shows that our Bell violation is not due to an artificially low detector efficiency apart from the inherent postselection. We can compare this to the study of Gerhardt *et al.* (*13*), where the faked detector efficiency was 50% when using active basis choice; that attack has an upper limit of 82.8% (*9*, *10*). Even if the faked detection efficiency in our experiment were 100%, our attack would work because the inherent postselection of the Franson interferometer removes half of the events.

In addition, our attack can produce a Bell value $S_2 = 4$ at any efficiency. Given the noise rate of a QKD device, Eve can fine-tune the attack to imitate the quantum prediction to any accuracy, therefore evading detection in a simple and effective way. It remains a fact that fast switching will restrict the Bell value to be below 3, but this fine-tuning ability shows the level of control an attacker can exert onto the system.

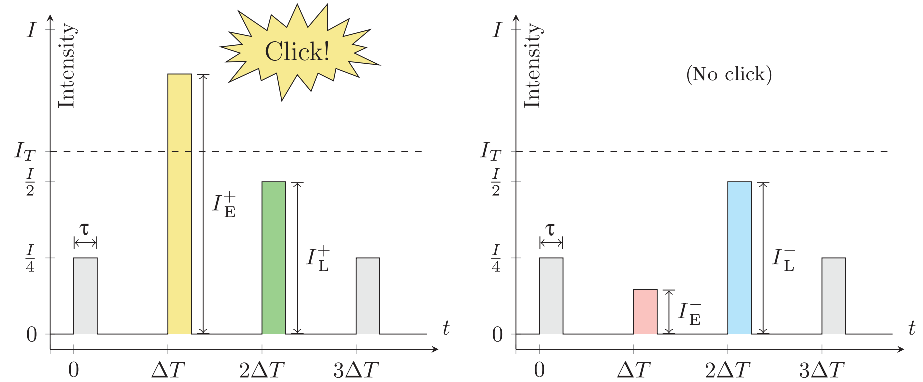
To build a device-independent QKD system based on energy-time entanglement, the designer will either have to use fast switching and replace the CHSH inequality with stronger tests such as modified Pearle-Braunstein-Caves inequalities, or use a system that does not exhibit the postselection loophole. These suggested improvements both have the essential property of establishing device independence without requiring additional assumptions and thereby maintain the powerful simplicity of device-independent QKD.

MATERIALS AND METHODS

Eve performs the attack by replacing the source with a faked-state generator that blinds the APDs (see Fig. 3) and makes them click at chosen instants in time. The blinding is accomplished using classical light pulses superimposed over continuous-wave (CW) illumination (*11*). In normal operation, an APD reacts to even a single incoming photon. A photon that enters the detector will create an avalanche of electrical current, which results in a signal, or "click," when the current crosses a certain threshold. The avalanche current is then quenched by lowering the APD bias voltage to below the breakdown voltage, making the detector ready for another photon and resulting in the so-called Geiger mode operation.

Under the influence of CW illumination, the quenching circuitry will make the current through the APDs proportional to the power of the incoming light. This will change the behavior of the APD into the so-called linear mode, more similar to a classical photodiode. It will no longer react to single photons, nor register clicks in the usual Geiger-like way and is therefore said to be "blind." The appropriate choice of CW illumination intensity will make the APD insensitive to single photons, yet still register a click when a bright pulse of classical light is superimposed over the CW illumination (*11*).

What remains is to construct classical light pulses that will give clicks in the way that Eve desires, violating the Bell inequality test for the Franson interferometer. Eve uses pulses with intensity I and pulse length $\tau \ll \Delta T$ intermingled with the CW light that blinds the APDs. A single pulse emitted by the source will be split when traveling through the interferometer, resulting in two pulses in each output port with intensity $I/4$ each. Alternatively, if two pulses are emitted, separated by ΔT and with phase difference ω, these two pulses will split to three. The middle pulse of the three is built up by two parts, so that the ±1 outputs show interference



A Constructive interference at the + output gives a large early time slot intensity and a corresponding click.

B Destructive interference at the − output gives a small early time slot intensity and no corresponding click.

Fig. 3. The blinding attack causes the detector to click only for pulses of greater intensity than I_T. If Eve sends three pulses of equal intensity I, they will arrive as four after the interferometer. By changing the phase shifts ω_E and ω_L between the pulses at the source, she can control the intensity of the early and late middle pulses at the ± output ports, giving clicks as desired. Here, $\phi = 0$, $\omega_E = \pi/8$, and $\omega_L = \pi/4$. The first and last pulses have a constant intensity of $I/4$.

$$
\begin{aligned}
I^{+}(\phi,\omega) &= I\,\cos^2\left(\frac{\phi+\omega}{2}\right)\\
I^{-}(\phi,\omega) &= I\,\sin^2\left(\frac{\phi+\omega}{2}\right)
\end{aligned}
\tag{7}
$$

where ϕ is the phase setting of the local analysis station. The chosen ω controls the ϕ dependence of the output. For example, if I is just less than $2I_T$ and ω = 0, there will be a +1 click for |ϕ| < π/2 and a −1 click otherwise.

However, this is not enough to fake the Bell violation, because the detection time needs to depend on the local setting (*23*). To enable this, Eve makes the source emit a group of three pulses separated by ΔT, with phase difference ω_E between the first and second pulse, and ω_L between the second and third pulse. When this pulse train passes through the interferometer, the output is four pulses, where the two center pulses have controllable intensity because of interference. The intensities for these two (early/late) pulses are

$$
\begin{aligned}
I_E^{+}(\phi\omega_E) &= I\,\cos^2\left(\frac{\phi+\omega_E}{2}\right)\\
I_E^{-}(\phi\omega_E) &= I\,\sin^2\left(\frac{\phi+\omega_E}{2}\right)\\
I_L^{+}(\phi\omega_L) &= I\,\cos^2\left(\frac{\phi+\omega_L}{2}\right)\\
I_L^{-}(\phi\omega_L) &= I\,\sin^2\left(\frac{\phi+\omega_L}{2}\right)
\end{aligned}
\tag{8}
$$

For example, with the same choice of I as above, $\omega_E = 0$, and $\omega_L = \pi/2$, there will be an early +1 click if ϕ = 0, and a late −1 click if ϕ = π/2. Note that the pulse trains to Alice and Bob can be chosen independently.

The last step of the attack is to use the LHV model in Fig. 4, which is a discretized version of an earlier known model (*23*). This LHV model prescribes the distribution of the sign and time slot of outcomes for Alice and Bob given local settings ϕ^A and ϕ^B. Single-particle outcomes obtained in this way follow the quantum predictions (*23*). The parameter p controls the desired level of violation, and θ and r are hidden variables that are chosen randomly for each experimental trial.

For the purposes of our attack, we choose to focus on the present Bell test: $\phi_1^A = 0, \phi_3^A = \pi/2, \phi_2^B = -\pi/4$, and $\phi_4^B = -3\pi/4$, so that the hidden variable θ is a multiple of π/4. Eve randomly chooses hidden variables r and θ as stated in Fig. 4, and reads off the desired results for the two settings at Alice.

If the results are in the same time slot, she uses two pulses and can directly calculate the needed phase difference. If the results are in different time slots (this only happens for Alice), Eve uses three pulses and calculates the two phase differences. The same r and θ are used to calculate the phase difference for Bob. Repeating this procedure will produce random outcomes (to Alice and Bob) that give exactly the quantum predictions for the mentioned settings, violating the Bell-CHSH inequality.

Joint Alice-Bob trials were performed with the pulse amplitudes as described in Eqs. 7 and 8 and depicted in Fig. 3. At the desired detector and time slot, a “click” will be forced (Fig. 3A) by constructive interference, whereas destructive interference causes “no click” (Fig. 3B). The sampling time used was 1 s, and each experiment was run for at least 27 s (see Fig. 2). At each point in time, the joint probabilities of Alice’s and Bob’s outcomes are computed from the detector counts, and these were then used to determine the Bell value. Note that the early and late time slots are measured in different experimental runs.

By adjusting the parameter p of the LHV model, we can go even further and produce Bell values up to and including the value 4 (see Fig. 4). Of course, Alice and Bob would be suspicious if they measured this value because their experiment does not contain nonlocal PR boxes (*27*). Eve would instead tune the Bell violation to compensate for inherent noise by raising the value just enough to reach $2\sqrt{2}$.

EXPERIMENTAL SETUP

The attack was experimentally implemented as shown in Fig. 5 and is built using standard fiber optic components. The CW is produced by a CW laser, whereas the pulses are created by a pulsed laser. These two light sources are combined at a fiber optic 2 × 2 coupler and then split into one beam for Alice and one for Bob. Each of these beams is then sent into a fiber optic 3 × 3 coupler (tritters) that equally divides them into three arms. The first arm consists of a ΔT delay loop and a phase modulator ω_E, the second arm has two ΔT delay loops and a phase modulator ω_M (so that $\omega_L = \omega_M - \omega_E$), whereas the third arm performs

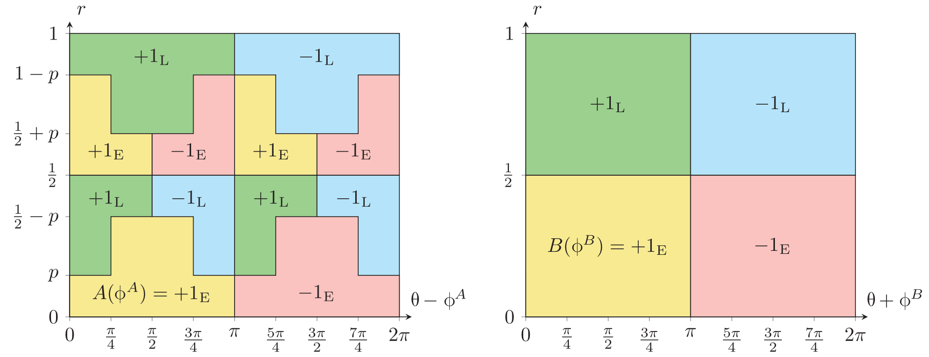


Fig. 4. Discretized LHV model (*23*) that can give any Bell value between 2 and 4. The hidden variables are $0 \le r < 1$ (a real number in the unit interval) and $\theta = n\frac{\pi}{4}$, where $0 \le n \le 7$ is an integer. The parameter $0 \le p \le 1/4$ can be chosen freely, and the output Bell value is $S_2 = 4 - 8p$, so that the “classical” $S_2 = 2$ is obtained with $p = 1/4$, the “quantum” $S_2 = 2\sqrt{2}$ is obtained with $p = (2-\sqrt{2})/4$ (as in the figure), and the “nonlocal box” $S_2 = 4$ is obtained with $p = 0$, all at 100% faked efficiency and 50% postselection.

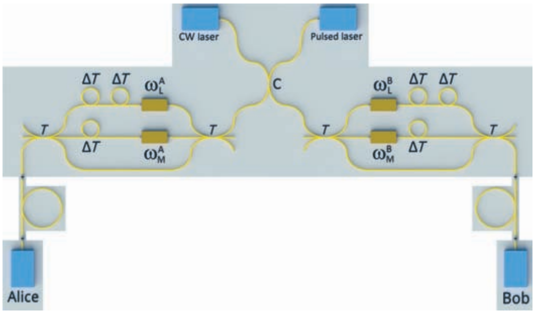


Fig. 5. Experimental setup of the attack on the Franson interferometer. The source consists of a CW laser for blinding the detectors, a pulsed laser for generating the bright classical light pulses, fiber optic couplers (C) delay loops (ΔT), phase modulators (ω and ϕ), and detectors (D). Alice and Bob have the same analysis stations as in Fig. 1.

no action. The three arms are then combined by a second 3×3 coupler into one output port that creates the output of the faked-state source generator.

The source sends bright light pulses with the setting and phase difference(s) to Alice's and Bob's analysis stations in the Franson interferometer. Each of the two analysis stations is constructed in a similar fashion: two fiber optic 2×2 couplers and one delay loop ΔT and a phase modulator ϕ^A (Alice's side) or ϕ^B (Bob's side).

The detectors used in the experiment are commercial products from Princeton Lightwave. These detectors are InGaAs avalanche photodiodes that use Geiger and biased pulse modes at the operating temperature 218 K. The detection wavelength range is 1300 to 1550 nm, giving a maximum detection efficiency of 20% at 1550 nm. The dark count rate is 5×10^{-5} ns^{-1}. Although the attack is demonstrated on this specific detector, other detector types using similar devices and circuitry are vulnerable as well.

Because the CW power becomes unevenly distributed between detectors, the efficiency of the blinding was affected. This imbalance was avoided by installing digital variable attenuators at the output ports. In addition, optical isolators were placed in front of the detectors to prevent crosstalk. The interferometers are passively stabilized and placed in a thermally and mechanically isolated environment in the form of a metal enclosure lined with styrofoam. This isolation has the effect of reducing phase drift, giving a 30-s time window in which measurements can be performed before a manual recalibration is required.

REFERENCES AND NOTES

1. J. S. Bell, On the Einstein-Podolsky-Rosen paradox. *Physics* **1**, 195–200 (1964).
2. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, paper published in the Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984.
3. A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
4. W. Heisenberg, Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik* **43**, 172–198 (1927).
5. A. Acín, N. Gisin, L. Masanes, From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
6. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
7. J.-Å. Larsson, Loopholes in Bell inequality tests of local realism. *J. Phys. A* **47**, 424003 (2014).
8. P. M. Pearle, Hidden-variable example based upon data rejection. *Phys. Rev. D* **2**, 1418–1425 (1970).
9. A. Garg, N. D. Mermin, Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Phys. Rev. D* **35**, 3831–3835 (1987).
10. J.-Å. Larsson, Bell's inequality and detector inefficiency. *Phys. Rev. A* **57**, 3304–3308 (1998).
11. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
12. J.-Å. Larsson, A practical Trojan Horse for Bell-inequality-based quantum cryptography. *Quantum Inf. Comput.* **2**, 434–442 (2002).
13. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, C. Kurtsiefer, Experimentally faking the violation of Bell's inequalities. *Phys. Rev. Lett.* **107**, 170404 (2011).
14. J. D. Franson, Bell inequality for position and time. *Phys. Rev. Lett.* **62**, 2205–2208 (1989).
15. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
16. N. Gisin, R. Thew, Quantum communication. *Nat. Photon.* **1**, 165–171, (2007).
17. Z. Y. Ou, X. Y. Zou, L. J. Wang, L. Mandel, Observation of nonlocal interference in separated photon channels. *Phys. Rev. Lett.* **65**, 321–324 (1990).
18. P. R. Tapster, J. G. Rarity, P. C. M. Owens, Violation of Bell's inequality over 4 km of optical fiber. *Phys. Rev. Lett.* **73**, 1923–1926 (1994).
19. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, Violation of Bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.* **81**, 3563–3566 (1998).
20. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, N. Gisin, Distribution of time-bin entangled qubits over 50 km of optical fiber. *Phys. Rev. Lett.* **93**, 180502 (2004).
21. T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, H. Takesue, Entanglement distribution over 300 km of fiber. *Opt. Express* **21**, 23241–23249 (2013).
22. D. Grassani, S. Azzini, M. Liscidini, M. Galli, M. J. Strain, M. Sorel, J. E. Sipe, D. Bajoni, Micrometer-scale integrated silicon source of time-energy entangled photons. *Optica* **2**, 88–94 (2015).
23. S. Aerts, P. Kwiat, J.-Å. Larsson, M. Zukowski, Two-photon Franson-type experiments and local realism. *Phys. Rev. Lett.* **83**, 2872–2875, (1999).
24. J. Jogenfors, J.-Å. Larsson, Energy-time entanglement, element of reality, and local realism. *J. Phys. A* **47**, 424032 (2014).
25. J. D. Franson, Inconsistency of local realistic descriptions of two-photon interferometer experiments. *Phys. Rev. A* **61**, 012105 (1999).
26. J. D. Franson, Nonclassical nature of dispersion cancellation and nonlocal interferometry. *Phys. Rev. A* **80**, 032119 (2009).
27. S. Popescu, D. Rohrlich, Quantum nonlocality as an axiom. *Found. Phys.* **24**, 379–385 (1994).
28. B. S. Cirel'son, Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4**, 93–100 (1980).
29. J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
30. M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, A. Zeilinger, Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497**, 227–230 (2013).
31. B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, P. G. Kwiat, Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111**, 130406 (2013).
32. J.-Å. Larsson, M. Giustina, J. Kofler, B. Wittmann, R. Ursin, S. Ramelow, Bell-inequality violation with entangled photons, free of the coincidence-time loophole. *Phys. Rev. A* **90**, 032107 (2014).
33. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 801 (2010).
34. L. Lydersen, V. Makarov, J. Skaar, Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography" [Appl. Phys. Lett. 98, 231104 (2011)]. *Appl. Phys. Lett.* **99**, 196101 (2011).
35. S. L. Braunstein, C. M. Caves, Wringing out better Bell inequalities. *Ann. Phys.* **202**, 22–56 (1990).
36. A. Cabello, A. Rossi, G. Vallone, F. De Martini, P. Mataloni, Proposed Bell experiment with genuine energy-time entanglement. *Phys. Rev. Lett.* **102**, 040401 (2009).
37. G. Lima, G. Vallone, A. Chiuri, A. Cabello, P. Mataloni, Experimental Bell-inequality violation without the postselection loophole. *Phys. Rev. A* **81**, 040101(R) (2010).
38. A. Cuevas, G. Carvacho, G. Saavedra, J. Cariñe, W. A. T. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima, G. B. Xavier, Long-distance distribution of genuine energy-time entanglement. *Nat. Commun.* **4**, 2871 (2013).
39. J. Brendel, N. Gisin, W. Tittel, H. Zbinden, Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.* **82**, 2594–2597 (1999).
40. W. Tittel, J. Brendel, N. Gisin, H. Zbinden, Long-distance Bell-type tests using energy-time entangled photons. *Phys. Rev. A* **59**, 4150–4163 (1999).

Funding: J.J. and J.-Å.L. were supported by Center for Industrial Information Technology (CENIIT) at Linköpings Universitet. M.B., J.A., and A.M.E. were supported by the Swedish

Research Council, Ideas Plus (Polish Ministry of Science and Higher Education grant IdP2011 000361), and ADOPT. **Author contributions:** J.-Å.L. conceived the idea. J.J. and J.-Å.L. developed the theory. M.B., J.A., J.J., and A.M.E. designed the experiment. A.M.E. performed the experiment. J.J. and A.M.E. analyzed the data. J.J., J.-Å.L., and M.B. wrote the research article. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data used to obtain the conclusions in this paper are available in Dryad or presented in the paper and/or the Supplementary Materials.

Submitted 15 June 2015
Accepted 29 September 2015
Published 18 December 2015
10.1126/sciadv.1500793

Citation: J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, J.-Å. Larsson, Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution. *Sci. Adv.* **1**, e1500793 (2015).

Publication C

Tight Bounds for the Pearle-Braunstein-Caves Chained Inequality Without the Fair-Coincidence Assumption

J. Jogenfors and J.-Å. Larsson. "Tight Bounds for the Pearle-Braunstein-Caves Chained Inequality without the Fair-Coincidence Assumption". *Physical Review A* 96.2 (Aug. 1, 2017), p. 022102. DOI: 10.1103/PhysRevA.96.022102.

This publication has been removed for copyright reasons. For more information, see http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-140912.

Publication D

High-Visibility Time-Bin Entanglement for Testing Chained Bell Inequalities

M. Tomasin, E. Mantoan, J. Jogenfors, G. Vallone, J.-Å. Larsson, and P. Villoresi. “High-Visibility Time-Bin Entanglement for Testing Chained Bell Inequalities”. *Physical Review A* 95.3 (Mar. 9, 2017), p. 032107. DOI: 10.1103/PhysRevA.95.032107.

This publication has been removed for copyright reasons. For more information, see http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-140912.

Publication E

Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics

J. Jogenfors. “Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics” (Apr. 5, 2016). arXiv: 1604.01383 [quant-ph].

Copyright © 2016 Jonathan Jogenfors.

Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No-Cloning Theorem of Quantum Mechanics

Jonathan Jogenfors*

April 5, 2016

Abstract

The digital currency Bitcoin has had remarkable growth since it was first proposed in 2008. Its distributed nature allows currency transactions without a central authority by using cryptographic methods and a data structure called the blockchain. Imagine that you could run the Bitcoin protocol on a quantum computer. What advantages can be had over classical Bitcoin? This is the question we answer here by introducing Quantum Bitcoin which, among other features, has immediate local verification of transactions. This is a major improvement over classical Bitcoin since we no longer need the computationally-intensive and time-consuming method of recording all transactions in the blockchain. Quantum Bitcoin is the first distributed quantum currency, and this paper introduces the necessary tools including a novel two-stage quantum mining process. In addition, Quantum Bitcoin resist counterfeiting, have fully anonymous and free transactions, and have a smaller footprint than classical Bitcoin.

1 Introduction

Modern society relies on money to function. Trade and commerce is performed using physical tokens (coins, banknotes) or electronically (credit cards, bank transfers, securities). Recently, cryptographic currencies such as Bitcoin has emerged as a new method to facilitate trade in a purely digital environment, without the need for a backing financial institution. Common to all functioning currencies is demand together with a controlled supply. Traditional, government-backed currencies mint currency according to rules decided by politics while Bitcoin works according to pre-defined mathematical rules. The currencies are then protected from counterfeiting either by physical copy-protection in the case of coins, banknotes and cashier's checks, or in Bitcoin by applying cryptography.

The laws of quantum mechanics have given rise to interesting applications in computer science. From the quadratic speedup of unstructured database search due to Grover [1] to the polynomial-time algorithm for integer factorization by Shor [2], some computing problems can be solved faster if a classical computer is replaced by a quantum one. In addition, quantum states are disturbed when measured, which has given rise to to quantum cryptography protocols such as BB84 [3] and E91 [4].

This begs the question: can quantum mechanics help us design new, improved money systems? The answer is yes. Starting with Wiesner [5], it has been shown that the no-cloning theorem [6] provides an effective basis for copy protection. See section 2.4 for a more detailed history of quantum money.

*Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden. Electronic address: jonathan.jogenfors@liu.se

Ideally we would like a payment system to have the following four properties (adapted from Mosca and Stebila [7]):

Anonymity. It should be difficult for any party to trace money, both where it came from and where it goes in the future.

Efficient local verification. There should be an efficient algorithm that can determine with high accuracy whether money is valid or not. This should be done without communicating to other peers.

Resistance against counterfeiting. It should be difficult for a counterfeiter to produce money that pass the verification procedure with non-negligible probability.

Transferable. Money should be unchanged by the verification procedure, and thus can be transferred and reused in a subsequent verification procedure.

We will make the formal definition of counterfeiting resistance in section 4.1.

In this paper, we construct Quantum Bitcoin, a novel currency that draws its inspiration from both Bitcoin and quantum mechanics. As we later show, our new currency fulfills all above requirements and has several advantages over existing payment systems, quantum or classical. The paper is organized as follows: Section 2 gives the background and concepts which are used in Quantum Bitcoin. In section 2.1 we discuss hash functions and digital signatures, section 2.3 introduces a model for the blockchain followed by a history of quantum money schemes in section 2.4.

Our main contribution is presented in section 3 where we give explicit protocols and algorithms for verifying and minting Quantum Bitcoin. Next, in section 4 we show that our protocol is secure and prevents counterfeiting.

2 Background

Quantum Bitcoin is for the most part based on existing technology, putting them together in a novel way to create the quantum currency.

2.1 Classical Cryptography

Hash functions, digital signatures.

Definition 1 *A classical public-key digital signature scheme $\mathcal{D}$ consists of three probabilistic polynomial-time classical algorithms [8]:*

1. $\mathsf{KeyGen}_{\mathcal{D}}$ *which takes as input a security parameter n and randomly generates a key pair $(k_{private}, k_{public})$.*

2. $\mathsf{Sign}_{\mathcal{D}}$ *which takes as input a private key $k_{private}$ and a message M and generates a (possibly randomized) signature* $\mathsf{Sign}_{\mathcal{D}}(k_{private}, M)$.

3. $\mathsf{Verify}_{\mathcal{D}}$*, which takes as input k_{public}, a message M, and a claimed signature ω, and either accepts or rejects.*

2.2 The Bitcoin protocol

The Bitcoin protocol was proposed in 2008 by Nakamoto [9]. The true identity behind that pseudonym still remains a mystery, but the concepts introduced in the original whitepaper have proven themselves by giving rise to a currency with a market cap exceeding 6 billion USD as of March 2016.

In order for a currency to function, there must be a finite amount in circulation as well as a controlled supply of new currency. Traditional currencies such as USD and EUR are controlled by a central organization, usually called the central bank. Bitcoin instead uses cryptography to distribute this task over a peer-to-peer network of users on the Internet.

Central to Bitcoin is the **blockchain**, which is a distributed ledger that records all transactions of every user. Using the blockchain, a user can compute his or her account balance by summing over all transactions to and from that account. A transaction is initiated by the sending party by digitally signing and then broadcasting a transaction message. The receiver of the transaction sees the transaction message, but is advised to wait until third parties, **miners** independently verify its validity. Otherwise, the sender could perform double-spending, where the same unit of currency is simultaneously and fraudulently sent to several receivers without them noticing.

A miner receives the broadcast transaction message and checks his or her local copy of the blockchain to check the transaction against the miner's local policy [10]. Usually, this means that the sender of the transaction must prove that he or she has knowledge of the private key corresponding to the public key of the originating account by using a signature. Also, the miner checks that the transferred bitcoin have not been spent. If the transaction is valid, the miner wants to append it to the blockchain.

Appending new data to the blockchain is the critical part of the Bitcoin protocol, and it requires some sort of authentication of the appended data. Otherwise, malicious miners could add invalid transactions to the blockchain, thereby defrauding users. Traditional authentication methods cannot be used for this purpose, as Bitcoin miners are loosely organized, anonymous and untrusted. Instead, Nakamoto [9] uses a **proof-of-work** puzzle, an idea introduced by Back [11]. Here, miners authenticate their verification by proving that they have spent computing power, and therefore energy. This prevents the Sybil attack [12], in which an attacker can flood a hypothetical voting mechanism. Such an attack becomes prohibitively expensive since each "vote" must be accompanied by a proof of spent energy.

The essentials of a proof-of-work puzzle is as follows: The data d is appended to a random nonce value r to produce $r + d$. This is fed to a cryptographically secure hash function f to produce the hash value $h = f(r + d)$. Next, the hash value is compared to a certain **threshold**. If h (interpreted as an integer on hexadecimal form) is smaller than the threshold value, the transaction is verified and d together with r is then broadcast to the network. The nonce value r can be seen as a solution to the proof-of-work puzzle d. The solution is easily verified, as it only requires one hashing operation f. If the nonce r is not a solution to the proof-of-work puzzle, the miner will have to try a new random nonce r and the process repeats. In fact, finding pre-images to secure hash functions is computationally difficult and requires a large number of trials.

Bitcoin implements the proof-of-work puzzle by packing a number of transactions into something called a **block**. Each block contains, among other things, a timestamp, the nonce, the hash value of the previous block, and the transactions [10]. The previous hash value fulfills an important function, as it prevents the data in previous blocks being modified. This imposes a chronological order of blocks, and the first Bitcoin block, called the **Genesis block** and was mined on January 3rd 2009.

Bitcoin miners are rewarded for their work by giving them newly minted Bitcoin. In fact, this is the only way in which new Bitcoin are added to the network. This is implemented as a special type of transaction, called a **coinbase** [10] which is added to the block by the miner. The reward size was originally 50 bitcoin, and is halved every 210000 transactions or approximately four years. At the time of writing this, the reward amounts to 12.5 bitcoin.

Further technical details such as forks, difficulty and confirmations are not discussed in this paper but are essential for the system to function. The end result is a system that rejects invalid data and adds correct data to an ever-growing list. The high level of data duplication makes attacks difficult as an attacker will have to compute hashes faster than the rest of the network combined.

According to Nakamoto [9] the probability for a malicious miner to succeed in verifying an invalid transaction is exponentially small in the number of confirmations as as long as a majority of miners (i.e. computing power) is used for benevolent purposes. This implies that the Bitcoin protocol is resistant to double-spending attacks. However, each confirmation takes 10 minutes to finish, so those six confirmations need one hour to finish, making transactions slow. In addition, Karame, Androulaki, and Capkun [13] found considerable variance in the time it takes to mine a block; they measured a standard deviation of mining time of almost 15 minutes. Bitcoin users must therefore make a decision between increased security and faster transaction times.

2.3 A Model of the Blockchain

For the purposes of Quantum Bitcoin, we model the blockchain as an random-access ordered array with timestamped dictionary entries. Blocks can be added to the end of the chain by solving a proof-of-work puzzle, and blocks in the chain can be read using a lookup function. In Quantum Bitcoin, the blocks do not contain standard transactions, only classical descriptors of the newly minted Quantum Bitcoin (and shards, discussed later). Therefore, blocks in the Quantum Bitcoin blockchain should be seen as general-purpose dictionaries that match serial numbers s to public keys[1] k_{public}.

We will use the following abstract definition:

Definition 2 *A classical distributed ledger scheme $\mathcal{L}$ consists of the following classical algorithms:*

- $\mathsf{Append}_{\mathcal{L}}$ *is an algorithm which takes (s, k_{public}) as input, where s is a classical serial number and k_{public} a classical public key. The algorithm fails if the serial number already exists in a block in the ledger. Otherwise, it begins to solve a proof-of-work puzzle by repeated trials of random nonce values. The algorithm succeeds if the puzzle is solved, at which time the ledger pair (s, k_{public}) is added as a new block.*
- $\mathsf{Lookup}_{\mathcal{L}}$ *is a polynomial-time algorithm that takes as input a serial number s and outputs the corresponding public key k_{public} if it is found in the ledger. Otherwise, the algorithm fails.*

Our formal definition is independent of the underlying block format and ruleset, so any secure blockchain implementation can be used. Note that $\mathsf{Append}_{\mathcal{L}}$ runs continuously until it succeeds – if another miner solves a proof-of-work puzzle it simply restarts the process transparently to the caller.

2.4 Previous Proposals for Quantum Money

As early as around 1970, Wiesner [5] and Broadbent and Schaffner [14] proposed a scheme that uses the no-cloning theorem to produce unforgeable quantum banknotes, however it took time for this result to be published. The paper was initially rejected [15] and according to Aaronson and Christiano [8] it took 13 years until it was finally published [5] in 1983. In the same year, BBBW [16] made improvements to Wiesner's scheme, such as an efficient way to keep track of every banknote in circulation. Another, more recent, extension by Pastawski et al. [17] increases the tolerance against noise. Even more recently, Brodutch et al. [18] presented an attack on the Wiesner and BBBW schemes.

After BBBW, quantum money received less attention due to the seminal 1984 paper by Bennett and Brassard [3] that created the field of quantum key distribution (QKD). Following two decades where virtually no work was done on quantum money, Mosca and Stebila [7, 19, 20]

[1] Do not confuse the public key k_{public} with the key of the dictionary

proposed *quantum coins* around ten years ago. In contrast to quantum banknotes (where each banknote is unique), quantum coins are all identical.

We distinguish between *private key* and *public-key* quantum money systems. In a private-key system, only the bank that minted the quantum money can verify it as genuine, while a public-key system allows anyone to perform this verification. The advantage of a public-key system over a private-key are obvious as long as it is just as secure. Until recently, all quantum money proposals were private-key, however in 2009 Aaronson [21] proposed the first public-key quantum money system. While this first public-key system was broken in a short time by Lutomirski et al. [22], it inspired others to re-establish security. A novel proposal by Farhi et al. [23] produced a public-key system using knot theory and superpositions of link diagrams, and this idea was further developed by Lutomirski [24].

In 2012, public-key quantum money based on hiding subspaces was introduced by Aaronson and Christiano [8]. The contribution consists first of an implicit scheme based on random oracles and then an explicit version based on multivariate polynomials. Further work by Pena, Faugère, and Perret [25] showed that this explicit scheme is insecure in the noiseless case, however the security of the noisy scheme remains unknown.

Another important distinction is between systems that are information-theoretically secure (ITS) and those secure under computational hardness assumptions. In an ITS quantum money scheme, no attacker can break the system even when given exponential computation time. For instance, Wiesner's scheme is ITS while BBBW is not. According to Farhi et al. [23], public-key quantum money cannot be ITS. Instead, the proposals by Aaronson and Christiano [8], Aaronson [21], and Farhi et al. [23] all rely on computational hardness assumptions, as will ours.

Common to all proposals discussed above is a centralized topology, with a number of users and one "bank" that issues (and possibly verifies) money. This requires all users to fully trust this bank, as a malevolent bank can perform fraud and revoke existing currency. This is true for both private-key and public-key schemes.

3 Our Contribution: Quantum Bitcoin

Our contribution is a modified quantum money scheme that removes trust from a central bank and instead uses an analogue to the Bitcoin miner. In our trust model we do not have to assume every single miner to be trustworthy, the system works as long as a certain percentage remains honest.

In this section we present the inner workings of Quantum Bitcoin. As with most quantum money schemes the central idea is the no-cloning theorem [6] which shows that it is impossible to copy an arbitrary quantum state $|\psi\rangle$. Quantum mechanics therefore provides an excellent basis on which to build a currency, as copy-protection is "built in". In section 4 we quantify the level of security the no-cloning theorem gives, and show that our Quantum Bitcoin are secure against counterfeiting.

We will use a quantum state as the unit of currency and endow it with classical information to facilitate verification. We then add a blockchain data structure which allows us to combine the quantum state with a distributed minting process, relinquishing trust in the central bank normally required by the security model in traditional quantum currencies.

In order to simplify the security analysis, we will construct a small "mini-scheme" [8, 23] which is then generalized to a full distributed Quantum Bitcoin scheme. The mini-scheme $\mathcal{M}$ does not use a blockchain and can only mint and verify one single Quantum Bitcoin. We then combine $\mathcal{M}$ with a digital signature scheme $\mathcal{D}$ and a distributed ledger scheme $\mathcal{L}$ to get the full-fledged Quantum Bitcoin description. In section 4 we will see that proving the security of $\mathcal{M}$ and $\mathcal{D}$ implies the security of the complete system $\mathcal{Q}$.

Intuitively we want the Quantum Bitcoin scheme $\mathcal{Q}$ to have the following properties:

1. a controlled method to feasibly generate an unlimited number of Quantum Bitcoin no faster than a given rate,
2. a verification procedure,
3. protection against forgery, so that the only way to map a polynomial number of Quantum Bitcoin to a larger number of Quantum Bitcoin with non-negligible success probability is the aforementioned generation process.

Here, we call a function $f(n)$ *negligible* if $f(n) = o(1/p(n))$ for every polynomial $p(n)$.

3.1 The Hidden Subspace Mini-Scheme

We adopt the Hidden Subspace mini-scheme system introduced by Aaronson and Christiano [8]. Let $\mathbb{F}_2^n$ be the space of binary sequences of length n, equipped with the standard inner product

$$\langle u, v\rangle = \sum (u)_i (v)_i \pmod 2. \tag{1}$$

We define A as a (secretly chosen) $n/2$-dimensional subspace of $\mathbb{F}_2^n$. In addition, let $A^\perp$ be the $n/2$-dimensional orthogonal complement to A, that is, the set of $y \in \mathbb{F}_2^n$ such that $\langle x, y\rangle = 0$ for all $x \in A$.

In the Mini-Scheme we create "quantum Bitcoin states" $|A\rangle$ in the following way:

$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x\in A} |x\rangle\,. \tag{2}$$

It is easy to prepare $\langle A\rangle$, a classical description of A which consists of $n/2$ generators. From this classical description one can create the quantum state in equation (2). Next, we define a public membership oracle U_A that is used to decide membership in A:

$$U_A |x\rangle = \begin{cases} -|x\rangle & \text{if } x \in A \\ |x\rangle & \text{otherwise,} \end{cases} \tag{3}$$

The membership oracle allows anybody to decide if a given, alleged quantum Bitcoin state corresponds to the subspace A. Note the parallel to classical digital signatures.

The unitary gate U_A is assumed to be a random oracle, but explicit methods are available, such as the (noisy) multivariate polynomial scheme by Aaronson and Christiano [8]. Using U_A, we can build a quantum circuit $\mathbb{P}_A$ that projects onto the basis states of $|A\rangle$ (figure 1).

1. Initiate a control qubit $|0\rangle$
2. Apply H to the control qubit
3. Apply U_A to $|x\rangle$ conditioned on the control qubit being in state $|1\rangle$
4. Apply H to the control qubit
5. Measure the control qubit and postselect on the outcome $|1\rangle$.

Note that the above algorithm maps $|x\rangle$ to $|1\rangle|x\rangle$ if $x \in A$ and $|0\rangle|x\rangle$ otherwise. Therefore, when measurement and postselection is performed, the algorithm returns 0 if and only if $|x\rangle \notin A$ and $|1\rangle|x\rangle$ otherwise.

We define $U_{A^\perp}$ and $\mathbb{P}_{A^\perp}$ in a similar way as above, except we instead operate on $A^\perp$. Together with the projectors $\mathbb{P}_A$ and $\mathbb{P}_{A^\perp}$ we can create a unitary operator

$$V_A = H_2^{\otimes n}\mathbb{P}_{A^\perp} H_2^{\otimes n}\mathbb{P}_A, \tag{4}$$

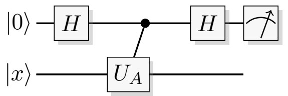


Figure 1: Quantum circuit $\mathbb{P}_A$.

where H denotes the Hadamard transform. We will use V_A to verify Quantum Bitcoin states, where we interpret $V_A |\psi\rangle = |A\rangle$ as passing and $V_A |\psi\rangle = 0$ as failing. Aaronson and Christiano [8, p. 28] show that V_A is a projector onto A, and that V_A accepts an arbitrary state $|\psi\rangle$ with probability $| \langle\psi|A\rangle |^2$.

Recall that a mini-scheme only mints and verifies one single Quantum Bitcoin. We can now give the formal definition:

Definition 3 *The Hidden Subspace mini-scheme $\mathcal{M}$ consist of two polynomial-time algorithms* $\mathsf{Mint}_{\mathcal{M}}$ *and* $\mathsf{Verify}_{\mathcal{M}}$.

Next, we set the requirements for the algorithm that generates the secret subspace A_r of $\mathbb{F}_2^n$.

Definition 4 *A* ***Subspace Generator*** *$\mathcal{G}(r)$ takes a secret n-bit string r and returns $(s_r, \langle A_r\rangle)$, where s_r is a $3n$-bit string and $\langle A_r\rangle$ is a set of linearly independent secret generators $\{x_1, \ldots, x_{n/2}\}$ for a subspace $A_r \leq \mathbb{F}_2^n$. We require that the serial numbers are distinct for every r.*

The subspace generator is the first step in minting a Quantum Bitcoin as it generates the secret, random subspace necessary for state generation (A_r) as well as the public serial number s_r. In addition,

Definition 5 *A* ***Serial Number Verifier*** *$\mathcal{H}(s)$ takes a serial number s and passes if it is a valid serial number $s = s_r$ for some $\langle A_r\rangle$ and fails otherwise.*

The above definitions are mere skeletons and must be explicitly implemented. For the security analysis we will assume the subspace generator and serial number verifier to be random oracles, however explicit schemes are available such as the (noisy) multivariate polynomial scheme introduced by Aaronson and Christiano [8, pp. 32–38]. We now complete the mini-scheme with explicit minting and verification algorithms:

Definition 6 $\mathsf{Mint}_{\mathcal{M}}(n)$ *takes as input a security parameter n. It then randomly generates a secret n-bit key r which it passes to the Subspace Generator $\mathcal{G}(r)$ which returns the serial number s_r and a classical description $\langle A_r\rangle$ of the subspace A. Next, it prepares the quantum state $|A_r\rangle$ given in equation (2). The returned value is $(s_r, |A_r\rangle)$.*

Definition 7 $\mathsf{Verify}_{\mathcal{M}}(\not{c})$ *takes as input an alleged Quantum Bitcoin $\not{c}$ and performs the following checks, in order:*

1. *Form check: Accept if and only if $\not{c}$ has the form (s, ρ), where s is a classical serial number and ρ is a quantum state.*
2. *Serial number check: Accept if and only if the Serial Number Verifier $\mathcal{H}(s)$ accepts*
3. *Apply $V_{A_r} = H_2^{\otimes 2}\mathbb{P}_{A_r^\perp} H_2^{\otimes 2}\mathbb{P}_{A_r}$ to ρ and accept if and only if $V_{A_r}(\rho) \neq 0$*

Note that the verification procedure immediately terminates if any of the above steps fail.

3.2 The Standard Construction of Quantum Bitcoin

The mini-scheme $\mathcal{M}$ can only mint and verify one single Quantum Bitcoin, so to build a usable Quantum Bitcoin ecosystem we need to extend the model with a mechanism for minting any amount of currency. For this purpose we will define the full Quantum Bitcoin scheme, $\mathcal{Q}$, and implement it as an extension of the mini-scheme $\mathcal{M}$. The connection between $\mathcal{M}$ and $\mathcal{Q}$ is derived from the "standard construction" by Aaronson and Christiano [8], Lutomirski et al. [22], and Farhi et al. [23].

Definition 8 *A public-key distributed Quantum Bitcoin scheme $\mathcal{Q}$ consists of the following algorithms:*

- $\mathsf{KeyGen}_{\mathcal{Q}}$*, a polynomial-time algorithm which takes as input a security parameter n and randomly generates a key pair $(k_{private}, k_{public})$.*
- $\mathsf{Mint}_{\mathcal{Q}}$ *which takes a security parameter n and produces a quantum bitcoin \$.*
- $\mathsf{Verify}_{\mathcal{Q}}$*, a polynomial-time algorithm which takes as input an alleged quantum bitcoin ¢ and a corresponding public key k_{public} and either accepts or rejects.*

Given a mini-scheme $\mathcal{M} = (\mathsf{Mint}_{\mathcal{M}}, \mathsf{Verify}_{\mathcal{M}})$, a digital signature scheme $\mathcal{D} = (\mathsf{KeyGen}_{\mathcal{D}}, \mathsf{Sign}_{\mathcal{D}}, \mathsf{Verify}_{\mathcal{D}})$ and a distributed ledger scheme $\mathcal{D} = (\mathsf{KeyGen}_{\mathcal{L}}, \mathsf{Append}_{\mathcal{L}}, \mathsf{Lookup}_{\mathcal{L}})$, we will construct an initial, naive, version of the Quantum Bitcoin scheme $\mathcal{S} = (\mathsf{KeyGen}_{\mathcal{Q}}, \mathsf{Sign}_{\mathcal{Q}}, \mathsf{Verify}_{\mathcal{Q}})$. Later, we extend this standard construction to protect against a special type of attack.

First, $\mathsf{KeyGen}_{\mathcal{Q}}$ is $\mathsf{KeyGen}_{\mathcal{D}}$ from the digital signature scheme. Next, we define the algorithm for $\mathsf{Verify}_{\mathcal{Q}}$ for an alleged Quantum Bitcoin ¢:

1. Check that ¢ is on the form (s, ρ, σ), where the s is a classical serial number, ρ a quantum state, and σ a classical digital signature.
2. Call $\mathsf{Lookup}_{\mathcal{L}}(s)$ to retrieve the public key k_{public} associated with the serial number s.
3. Call $\mathsf{Verify}_{\mathcal{D}}(k_{public}, s, \sigma)$ to verify the digital signature of the Quantum Bitcoin.
4. Call $\mathsf{Verify}_{\mathcal{M}}(s, \rho)$ from the mini-scheme.

The main challenge of constructing Quantum Bitcoin is that the miners are untrusted which is in contrast to previous schemes where minting is done by a trusted entity such as a bank. In the same spirit as Bitcoin, the intention is to take individually untrusted miners and still be able to trust them as a group [9]. Our first, Bitcoin-inspired attempt at the $\mathsf{Mint}_{\mathcal{Q}}$ algorithm therefore becomes the following:

1. Call $\mathsf{KeyGen}_{\mathsf{D}}$ to randomly generate a key pair $(k_{private}, k_{public})$.
2. Generate a Quantum Bitcoin candidate by calling $\mathsf{Mint}_{\mathcal{M}}$, which returns (s, ρ), where s is a classical serial number and ρ is a quantum state.
3. Sign the serial number: $\sigma = \mathsf{Sign}_{\mathcal{D}}(k_{private}, s)$
4. Call $\mathsf{Append}_{\mathcal{L}}(s, k_{public})$ to attempt to append the serial number s and the public key k_{public} to the ledger.
5. If $\mathsf{Append}_{\mathcal{L}}$ failed, start again from step 2
6. If the serial number was successfully appended, put the serial number, quantum state and signature together to create the Quantum Bitcoin $\$ = (s, \rho, \sigma)$.

Here we identify the first major advantage of Quantum Bitcoin. Whereas Bitcoin requires each transaction to be recorded into the blockchain – a time-consuming process, Quantum Bitcoin transactions finalize immediately. Due to the no-cloning theorem of quantum mechanics, the underlying quantum state in the Quantum Bitcoin cannot be duplicated, thereby preventing counterfeiting in itself (see section 4). The only step of the protocol that uses $\mathsf{Append}_{\mathcal{L}}$ is minting, which "normal" users don't have to worry about and therefore reduces end-user complexity.

3.3 Preventing Quantum Double-Mining

Our naive attempt at algorithms for $\mathsf{Verify}_{\mathcal{Q}}$ and $\mathsf{Mint}_{\mathcal{Q}}$ seems to work, but there is a problem. In Quantum Bitcoin there is no implicit trust in the minters. This leads to a phenomena we call **quantum double-mining**. Ideally, $\mathsf{Mint}_{\mathcal{M}}$ should be an algorithm that generates unique quantum states every time it is called, similarly to a random oracle. However, a malicious miner could generate a Quantum Bitcoin, append it to the blockchain, and then covertly reuse $k_{private}$ to produce any number of identical Quantum Bitcoin. This is a serious problem, since it allows a miner to undermine the payment system at any time.

Compare this with classical Bitcoin. There, the blockchain records all transactions and a miner therefore relinquishes control over the mined bitcoin as soon as it is handed over to a recipient. In Quantum Bitcoin, however, there is no record of who owns what, so nobody would notice counterfeit, doubly-mined Quantum Bitcoin.

The incentives for the double-mining attack are huge. Reusing the private key allows them to duplicate the quantum bitcoin they just created, leading to an easy double-spend. Another more sinister strategy by the attacker is to mine a large number of quantum bitcoin, wait until these have circulated to other users, and then create a large amount of duplicate coins. Surely, such an attack would have detrimental effects on the currency as a whole.

The double-mining attack is prevented in a similar way as the double-spending problem is prevented in classical Bitcoin. However, while Bitcoin introduced the blockchain for all transactions, we only need to modify the minting end in the Quantum Bitcoin protocol. The advantage is that day-to-day use of the currency is only negligibly affected and in section 4.2 we show that this countermeasure is effective.

We add a secondary stage to the minting process where data is also appended to a new ledger $\mathcal{L}'$. For the secondary mining step, we introduce security parameters $m \geq 1$ and $T_{max} > 0$ and the algorithm is as follows:

1. A miner (this time called a **Quantum Shard Miner**) uses the above "naive" minting scheme, but the finished product (s, ρ, σ) is instead called a **Quantum Shard**.

2. Quantum Shard miners sell the Quantum Shards on a marketplace.

3. A miner (called a **Quantum Bitcoin Miner**) purchases m Quantum Shards $\{(s, \rho_i, \sigma_i)\}_{1 \leq i \leq m}$ on the marketplace that, for all $1 \leq i \leq m$, fulfill the following conditions:

   - $\mathsf{Verify}_{\mathcal{Q}}((s, \rho_i, \sigma_i))$ accepts
   - The timestamp T of the Quantum Shard in the Quantum Shard ledger $\mathcal{L}$ fulfills $t - T \leq T_{max}$, where t is the current time.

4. The Quantum Bitcoin miner calls $\mathsf{KeyGen}_{\mathcal{Q}}$ to randomly generate a key pair $(k_{private}, k_{public})$.

5. The Quantum Bitcoin miner takes the serial numbers of the m Quantum Shards and compiles the **classical descriptor** $s = (s_1, \ldots, s_m)$ and signs it as $\sigma_0 = \mathsf{Sign}_{\mathcal{D}}(k_{private}, s)$.

6. The Quantum Bitcoin miner takes the m Quantum Shards and, together with σ_0, produces a **Quantum Bitcoin Candidate**: $(s_1, \rho_1, \sigma_1, \ldots, s_m, \rho_m, \sigma_m, \sigma_0)$.

7. The Quantum Bitcoin miner calls $\mathsf{Append}_{\mathcal{L}'}(s, k_{public})$ to attempt to pair the Quantum Bitcoin Miner's public key k_{public} with the classical descriptor s in the ledger. Here, we require that Append fails if any of the m Quantum Shards already have been combined into a Quantum Bitcoin that exists in the ledger $\mathcal{L}'$.

This process is the complete quantum mining protocol, and it works because each participant is incentivized: Quantum Shard miners invest computing power to produce Quantum Shards, which Quantum Bitcoin Miners want for Quantum Bitcoin production. As there is only a finite number of Quantum Shards, they will have monetary value, thus rewarding the Quantum Shard miners. In turn, Quantum Bitcoin miners invest computing power to mint Quantum Bitcoin from Quantum Shards. The Quantum Bitcoin miners are rewarded with a valid Quantum Bitcoin, which, due to their limited supply, can be expected to have monetary value.

According to Nakamoto [9], such incentives "may help nodes to stay honest" and an attacker who has access to more computing power than the rest of the network combined finds that it is more rewarding to play by the rules than commit fraud. Also, quantum double-mining is prevented because two-stage mining makes it overwhelmingly difficult for a single entity to first produce m Quantum Shards and secondly combine them to a Quantum Bitcoin.

This construction assumes that a majority of miners are honest, i.e. discard private keys after mining (for details see section 4.2). Note the requirement that the quantum shards are less than T_{max} old. This is needed because the probability of successfully mining a single quantum shards approaches 1 as time goes by. Therefore, given enough time, a malicious miner can produce m valid quantum shards which it then could combine into a valid Quantum Bitcoin. The parameter T_{max} prevents this from happening by forcing expiry of old shards. An attacker must therefore compete against the rest of the network in a similar way way as in Bitcoin.

What remains is to slightly modify $\mathsf{Verify}_{\mathcal{Q}}$ to take two-stage mining into account:

1. Check that $¢$ is on the form $(s_1, \rho_1, \sigma_1, \ldots, s_m, \rho_m, \sigma_m, \sigma_0)$, where the s_i are classical serial numbers, ρ_i are quantum states, and σ_i (including σ_0) are digital signatures.

2. Call $\mathsf{Lookup}_{\mathcal{L}'}((s_1, \ldots, s_m))$ to retrieve the public key k_{public} of the Quantum Bitcoin Miner associated with the classical descriptor $(s_1, \ldots, s_m)$.

3. Call $\mathsf{Verify}_{\mathcal{D}}(k_{public}, (s_1, \ldots, s_m), \sigma_0)$ to verify the digital signature of the Quantum Bitcoin.

4. For each $1 \leq i \leq m$, call $\mathsf{Lookup}_{\mathcal{L}}(s_i)$ in order to retrieve the corresponding public keys $k_{public,i}$ from the Quantum Shard miners.

5. For each $1 \leq i \leq m$, call $\mathsf{Verify}_{\mathcal{D}}(k_{public,i}, s_i, \sigma_i)$ to verify the digital signatures of each of the Quantum Shards.

6. For $1 \leq i \leq m$, call $\mathsf{Verify}_{\mathcal{M}}(s_i, \rho_i)$.

The verification passes if and only if all of the above steps succeed. This method checks the digital signatures of both the Quantum Bitcoin and all its Quantum Shards before calling the verification procedure of the mini-scheme $\mathcal{M}$.

4 Security Analysis

In this section we perform the security analysis of Quantum Bitcoin and show that it is secure against counterfeiting. Here, we reap the benefits of the mini-scheme setup as the proof becomes relatively easy. We begin by quantifying the probability of false negatives and false positives in the verification process and then we show that the mini-scheme is secure, followed by the observation that a secure mini-scheme implies security of the full system $\mathcal{Q}$.

4.1 Counterfeiting

Our formal security analysis begins by modeling a counterfeiter, which is a quantum circuit that produces new, valid, Quantum Bitcoin outside of the normal minting procedure.

Definition 9 *A* ***counterfeiter*** *C is a quantum circuit of polynomial size (in n) which maps a polynomial (in n) number of valid Quantum Bitcoin to a polynomial number (in n) of new, possibly entangled alleged Quantum Bitcoin.*

We next need to quantify the probability of a counterfeit Quantum Bitcoin to be accepted by the verification procedure. This is the probability of a false positive:

Definition 10 *A Quantum Bitcoin scheme $\mathcal{Q}$ has* ***soundness error*** *δ if, given any counterfeiter C and a collection of q valid Quantum Bitcoin $\$_1, \ldots, \$_q$ we have*

$$Pr(\mathsf{Count}(C(\$_1, \ldots, \$_q)) > q) \leq \delta, \tag{5}$$

where Count *is a* ***counter*** *that takes as input a collection of (possibly-entangled) alleged Quantum Bitcoin $\$_1, \ldots, \$_r$ and outpts the number of indices $0 \leq i \leq r$ such that* $\mathsf{Verify}(\$_i)$ *accepts*

Conversely, we quantify the probability of false negative, i.e. the probability that a valid Quantum Bitcoin is rejected by the verification procedure:

Definition 11 *A Quantum Bitcoin scheme $\mathcal{Q}$ has* ***completeness error*** *ε if* $\mathsf{Verify}(\$)$ *accepts with probability at least $1 - \varepsilon$ for all valid Quantum Bitcoin \$. If $\varepsilon = 0$ then $\mathcal{Q}$ has* ***perfect completeness****.*

We call a Quantum Bitcoin scheme $\mathcal{Q}$ **secure** if it has completeness error $\varepsilon \leq 1/3$ and negligible soundness error. Next, we continue with analyzing the mini-scheme. Recall that a mini-scheme only mints and verifies one single Quantum Bitcoin, so that a mini-scheme counterfeiter only takes the single valid Quantum Bitcoin as input. To perform this analysis, we need a technical tool, the double verifier:

Definition 12 *For a mini-scheme $\mathcal{M}$, we define the* ***double verifier*** Verify_2 *as a polynomial-time algorithm that takes as input a single serial number s and two (possibly-entangled) quantum states ρ_1 and ρ_2 and accepts if and only if* $\mathsf{Verify}_{\mathcal{M}}(s, \sigma_1)$ *and* $\mathsf{Verify}_{\mathcal{M}}(s, \sigma_2)$ *both accept.*

Now, we define the soundness and completeness error for the mini-scheme:

Definition 13 *A mini-scheme $\mathcal{M}$ has* ***soundness error*** *δ if, given any quantum circuit C (the* ***counterfeiter****),* $\mathsf{Verify}_2(s, C(\$))$ *accepts with probability at most δ. Here the probability is over the Quantum Bitcoin \$ output by* $\mathsf{Mint}_{\mathcal{M}}$ *as well as the behavior of* Verify_2 *and C.*

Definition 14 *A mini-scheme $\mathcal{M}$ has* ***completeness error*** *ε if* $\mathsf{Verify}(\$)$ *accepts with probability at least $1 - \varepsilon$ for all valid Quantum Bitcoin or Quantum Shards \$. If $\varepsilon = 0$ then $\mathcal{Q}$ has* ***perfect completeness****.*

As for the Quantum Bitcoin scheme $\mathcal{Q}$, we call a mini-scheme $\mathcal{M}$ **secure** if it has completeness error $\varepsilon \leq 1/3$ and negligible soundness error. While 1/3 sounds like a high error probability, Aaronson and Christiano [8, pp. 42–43] show that the completeness error ε of a secure system can be made exponentially small in n at the cost of only a modest increase in the soundness error δ.

What remains is to show that the Quantum Bitcoin system $\mathcal{Q}$ is, in fact, secure. This would be difficult had we not used the mini-scheme model, but now we can do this in a single step. The following theorem is adapted from Aaronson and Christiano [8, p. 20]:

Theorem 1 *If there exists a secure mini-scheme $\mathcal{M}$, then there also exists a secure Quantum Bitcoin scheme $\mathcal{Q}$.*

Proof *We use the Subspace Generator $\mathcal{G}(r)$ from definition 4 as a one-way function: given a n-bit string r, $\mathcal{G}(r)$ outputs (among others) an unique $3n$-bit serial number s_r. If there exists a polynomial-time quantum algorithm to recover r from s_r it would be possible for a counterfeiter to copy Quantum Bitcoin, which is a contradicts the security of the mini-scheme. Therefore, $\mathcal{G}(r)$ is a one-way function secure against quantum attack. Since such one-way functions are necessary and sufficient for secure digital signature schemes [26], we immediately get a digital signature scheme $\mathcal{D}$ secure against quantum chosen-plaintext attacks. The final step is to show that $\mathcal{M}$ and $\mathcal{D}$ together produce a secure Quantum Bitcoin system $\mathcal{Q}$, which is done in Aaronson and Christiano [8, p. 20].*

This is the elegance of the mini-scheme model, where a secure mini-scheme immediately gives us the full, secure system. Therefore, a counterfeiter who wants to break $\mathcal{Q}$ is forced to break the security of $\mathcal{M}$. Therefore, if we show that $\mathcal{M}$ is indeed secure we are finished:

Theorem 2 *The mini-scheme $\mathcal{M} = (\mathsf{Mint}_{\mathcal{M}}, \mathsf{Verify}_{\mathcal{M}})$, which is defined relative to the classical oracle U, has zero completeness and $1/\exp(n)$ soundness error.*

Proof *The Inner-Product Adversary Method by Aaronson and Christiano [8, p. 31] gives an upper bound to the information gained by a single oracle query. Theorem 1 then shows that the mini-scheme $\mathcal{M}$ is secure since a valid Quantum Bitcoin always passes verification (zero completeness error), and counterfeit Quantum Bitcoin pass with only an exponentially small probability (negligible soundness error).*

This ties together the security of the mini-scheme $\mathcal{M}$ and the Quantum Bitcoin scheme $\mathcal{Q}$. Theorem 2 shows that $\mathcal{M}$ is secure, and from theorem 1 it then follows that $\mathcal{Q}$ is secure. Explicitly, any counterfeiter must make $\Omega(2^{n/4})$ queries to successfully copy a Quantum Bitcoin. For large enough n, this is computationally infeasible. Specifically, $n = 512$ requires at least 2^{128} oracle queries.

Note that Quantum Bitcoin are not information-theoretically secure. Therefore, it is conjectured that a hypothetical attacker without access to an exponentially fast computer cannot perform the exponential number of queries required to perform counterfeiting. Recall from section 2.4 that public-key quantum money cannot be information-theoretically secure as shown by Farhi et al. [23], so this should not come as a surprise.

4.2 Quantum Double-Mining

Now we analyze the effect of the security parameters m and T_{max} on the probability of quantum double-mining. Quantum double-mining is when the same entity first mines a number of Quantum Shards, then combines them into a Quantum Bitcoin. The security parameter m controls the number of Quantum Shards required per Quantum Bitcoin, and T_{max} is the maximum age of the Quantum Shards.

For an attacker to perform quantum double-mining, he or she must therefore mine $m - 1$ Quantum Shards in T_{max} seconds after a first quantum shard has been mined. Remember that Quantum Shards expire after T_{max} seconds. In reality the attacker must both mint Quantum Shards and combine them into Quantum Bitcoin before T_{max} runs out. We simplify the analysis, however, by making it easier for the attacker and allow T_{max} time to mine Quantum Shards, and then again T_{max} time to mine Quantum Bitcoin.

We model our attack by assigning the probability p to the probability of an attacker mining the next block in either the Quantum Shard or Quantum Bitcoin blockchain. p can be understood as the proportion of the world's computing power controlled by the attacker. We define $k := \lfloor T_{max}/T_{block} \rfloor \geq 2$ as the average number of blocks mined before T_{max} runs out, where T_{block} is the average time between mined blocks. Bitcoin uses $T_{block} = 600\,\mathrm{s}$, although empirical research by Karame, Androulaki, and Capkun [13] suggests that the distribution of mining times corresponds to a shifted geometric distribution with parameter 0.19. The probability of the attacker mining mining $m-1$ of these k Quantum Shards is then

$$\eta_1 = \binom{k}{m-1} p^{m-1}(1-p)^{k-m+1}. \tag{6}$$

Next, the attacker must combine these Quantum Shards into a Quantum Bitcoin before another T_{max} runs out. The probability for this is the probability of mining a single block:

$$\eta_2 = \binom{k}{1} p(1-p)^{k-1} = kp(1-p)^{k-1}. \tag{7}$$

The total probability of quantum double-mining η is then

$$\eta = \eta_1\eta_2 = \binom{k}{m-1} k \left(\frac{p}{1-p}\right)^m (1-p)^{2k}. \tag{8}$$

We bound the binomial coefficient by above using the formula

$$\binom{n}{k} < \left(\frac{ne}{k}\right)^k \text{ for } 1 \leq k \leq n, \tag{9}$$

which gives

$$\eta < \left(\frac{ke}{m-1}\right)^{m-1} k \left(\frac{p}{1-p}\right)^m (1-p)^{2k} \text{ for } 2 \leq m \leq k+1. \tag{10}$$

We set $m-1 = \gamma k$ which for $1/k < \gamma < 1$ gives

$$\eta < k\left(\frac{e}{\gamma}\cdot\frac{p}{1-p}\right)^{\gamma k}\left(\frac{p}{1-p}\right)(1-p)^{2k}. \tag{11}$$

We note that

$$\frac{e}{\gamma}\cdot\frac{p}{1-p} < \frac{1}{2} \Leftrightarrow 0 \leq p < \frac{\gamma}{2e+\gamma}, \tag{12}$$

where the upper bound of p approaches $1/(2e+1) \approx 15.5\,\%$ as γ goes to 1. Under those constraints we get $\sup p/(1-p) = 1/2e$ and $(1-p)^{2k} \leq 1$. Plugging in all this in equation (11) we get the following worst-case upper limit for the double-mining probability:

$$\eta < \frac{k}{2e} 2^{-\gamma k}. \tag{13}$$

In other words, the probability of quantum double-mining is exponentially small in k as long as the attacker controls less than 15 % of the computing power. Note that equation (13) is the worst-case approximation and we should expect a much lower probability in a real scenario. What remains is to determine the parameter γ. Too large, and it will be difficult for *any* Quantum Bitcoin to be mined as every single Quantum Shard must be sold to a Quantum Bitcoin miner before T_{max} runs out. Too small, and the bound in equation (13) is weakened, making it easier for a malicious miner to perform double-mining. The smaller we make γ, the larger we must make k to achieve the required security.

4.3 Quantum Bitcoin Longevity

What remains is to show that a Quantum Bitcoin does not wear out too quickly, i.e. that they can be verified enough number of time and can be considered *money*. We will make use of the "Almost As Good As New Lemma" [8, 27] which is as follows:

Lemma 1 *Suppose a measurement on a mixed state ρ yields a particular outcome with probability $1-\varepsilon$. Then after the measurement, one can recover a state $\widetilde{\rho}$ such that $\|\widetilde{\rho}-\rho\|_{tr} \leq \sqrt{\varepsilon}$*

Since we can make the completeness error exponentially small in n, this means we can make $\mathsf{Verify}(\$)$ accept a valid Quantum Bitcoin with exponentially large probability in n. Lemma 1 therefore says that we can reconstruct a Quantum Bitcoin $\widetilde{\$}$ such that $\left\|\widetilde{\$}-\$\right\|_{tr}$ is exponentially small in n as well. In other words, a Quantum Bitcoin \$ can be verified $\exp n$ times.

This exponential number of verifications before "wearing out" means that our Quantum Bitcoin will be usable for a long enough time to be considered "money". This is directly analogous to traditional, physical banknotes which are expected to last for a large enough number of transactions before wearing out.

5 Comparison to Classical Bitcoin

We will now compare Quantum Bitcoin to the classical Bitcoin protocol by Nakamoto [9] and show that Quantum Bitcoin has several advantages. Bitcoin transactions must be verified by third-party miners which, on average, takes 60 minutes but has considerable variance [13]. Bitcoin transactions are therefore slow. In contrast, Quantum Bitcoin transactions are immediate and only requires the receiver to have read-only access to a reasonably recent copy of the blockchain. In addition, the transactions are local, so that no blockchain must be updated, nor does it require a third party to know of the transaction.

Local transactions are also independent of network access. Bitcoin requires two-way communication with the Internet, while Quantum Bitcoin transactions can be performed in remote areas, including in space. The read-only blockchain access requirement makes it possible to store a local offline blockchain copy in, for example, a book. A user only needs to consult this book to perform transactions, given that the Quantum Bitcoin in question were minted before the book was printed.

Another performance advantage is scalability. According to Garzik [28], Bitcoin as originally proposed by Nakamoto [9] has an estimated global limit of seven transactions per second. In comparison, the local transactions of Quantum Bitcoin implies that there is no upper limit to the transaction rate. It should be noted, however, that the minting rate is limited by the capacity of the Quantum Shard and Quantum Bitcoin blockchains. By placing the performance restriction only in the minting procedure, the bottleneck should be much less noticeable than if it were in the transaction rate as well.

Local transactions also mean anonymity, since only the sender and receiver are aware of the transaction even occurring. No record, and therefore no paper trail, is created. In essence, a Quantum Bitcoin transaction is similar to that of ordinary banknotes and coins, except no central point of authority has to be trusted. Classical Bitcoin, on the other hand, records all transactions in the blockchain which allows anybody with a copy to trace transaction flows, even well after the fact. This has been used by several authors [29–34] to de-anonymize Bitcoin users.

Another advantage of Quantum Bitcoin is that transactions are free. Classical Bitcoin transactions usually require a small fee [9] to be paid to miners in order to prevent transaction spam and provide additional incentive. It is also envisioned [9, 35] that fees will allow mining to continue past the year 2140, when the last new bitcoin is expected to be mined. In Bitcoin, mining is required for transactions to work. None of this is needed in Quantum Bitcoin as local transactions require no fees. Even a hypothetical inflation control scheme, similar to that of Bitcoin, will make mining stop completely as it no longer will be necessary at all.

Compared to Bitcoin, the blockchain of Quantum Bitcoin is smaller and grows at a more predictable rate. By nature, data added to a blockchain can never be removed, and as of March 2016 the size of the Bitcoin blockchain exceeds 60 GB. Quantum Bitcoin also has a growing blockchain, however it only grows when minting currency, not due to transactions.

Per the discussion in the previous paragraph, Quantum Bitcoin mining could become superfluous so that the Quantum Bitcoin blockchain only grows to a given size. For example, if we limit the number of Quantum Bitcoin to 21 million (just like in Bitcoin) and choose 512-bit serial numbers and a 256-bit digital signature scheme $\mathcal{D}$, the Quantum Bitcoin blockchain will only ever grow to roughly 2 GB in size plus some overhead.

6 Conclusion

Quantum Bitcoin is a tangible application of quantum mechanics where we construct the ideal distributed, publicly-verifiable payment system. The no-cloning theorem provides the foundation of an unforgeable item, and the addition of a blockchain allows us to produce currency without trusting a central entity. Quantum Bitcoin is the first example of a secure, distributed payment system with local transactions.

Two parties can transfer Quantum Bitcoin by transferring a quantum state over a suitable channel and reading off a publicly-available blockchain. Transactions are settled immediately without having to wait for confirmation from miners, and the Quantum Bitcoin can be used and re-constructed an exponential number of times before they wear out. There is no transaction fee, yet the system can scale to allow an unlimited rate of transactions.

In section 1, we set up four goals that our distributed money scheme should fulfill. Let's see how well Quantum Bitcoin does:

Anonymity. Transactions are local and there is no paper trail for a transaction.

Resistance against counterfeiting. We showed in section 4 that it is computationally unfeasible for any quantum counterfeiter to forge Quantum Bitcoin.

Efficient local verification. The verification algorithms are polynomial-time and do not require communication with third parties.

Transferable. Quantum Bitcoin can be transferred through quantum channels, and after verification they can be reconstructed to its original state with high probability.

Note that while Quantum Bitcoin is secure against a counterfeiter with access to a quantum computer, the protocol is not information-theoretically secure. The corresponding security proofs must therefore place the standard complexity assumptions on the attacker.

We invite further study of our proposal, including security aspects related to counterfeiting and two-stage mining. In addition, there are a few issues that should be addressed. First, there is an issue of atomicity, as there is no obvious way to Quantum Bitcoin into smaller units like the change mechanism in Bitcoin.

References

[1] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing.* STOC '96. New York, NY, USA: ACM, 1996, pp. 212–219. ISBN: 978-0-89791-785-8. DOI: 10.1145/237814.237866.

[2] Peter W. Shor. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science.* Santa Fe, NM: IEEE Computer Society Press, Nov. 1994, pp. 124–134.

[3] C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Proc. of the IEEE Int. Conf. on Computers, Systems, and Signal Processing.* 175textendash179. Bangalore, India: IEEE New York, 1984.

[4] Artur K. Ekert. “Quantum cryptography based on Bell’s theorem”. *Phys. Rev. Lett.* 67 (1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661.

[5] Stephen Wiesner. “Conjugate Coding”. *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. ISSN: 0163-5700. DOI: 10.1145/1008908.1008920.

[6] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. *Nature* 299.5886 (Oct. 28, 1982), pp. 802–803. DOI: 10.1038/299802a0.

[7] Michele Mosca and Douglas Stebila. “Quantum Coins” (Nov. 6, 2009). arXiv: 0911.1295.

[8] Scott Aaronson and Paul Christiano. “Quantum Money from Hidden Subspaces” (Mar. 21, 2012). arXiv: 1203.4740.

[9] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. *Consulted* 1.2012 (2008), p. 28.

[10] Krzysztof Okupski. “Bitcoin Developer Reference” (2015).

[11] Adam Back. “Hashcash, a denial of service counter-measure” (Aug. 1, 2002).

[12] John R Douceur. “The Sybil Attack”. In: *Peer-to-peer Systems.* Springer, 2002, pp. 251–260.

[13] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. “Double-spending Fast Payments in Bitcoin”. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security.* CCS ’12. New York, NY, USA: ACM, 2012, pp. 906–917. ISBN: 978-1-4503-1651-4. DOI: 10.1145/2382196.2382292.

[14] Anne Broadbent and Christian Schaffner. “Quantum cryptography beyond quantum key distribution”. *Designs, Codes and Cryptography* 78.1 (Dec. 21, 2015), pp. 351–382. ISSN: 0925-1022, 1573-7586. DOI: 10.1007/s10623-015-0157-4.

[15] Gilles Brassard. “Brief history of quantum cryptography: A personal perspective”. In: *Theory and Practice in Information-Theoretic Security, 2005. IEEE Information Theory Workshop on.* IEEE, 2005, pp. 19–23.

[16] Charles H. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. “Quantum Cryptography, or Unforgeable Subway Tokens”. In: *Advances in Cryptology.* Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Boston, MA: Springer US, 1983, pp. 267–275. ISBN: 978-1-4757-0604-8. DOI: 10.1007/978-1-4757-0602-4_26.

[17] Fernando Pastawski, Norman Y. Yao, Liang Jiang, Mikhail D. Lukin, and J. Ignacio Cirac. “Unforgeable Noise-Tolerant Quantum Tokens”. *Proceedings of the National Academy of Sciences* 109.40 (Oct. 2, 2012), pp. 16079–16082. ISSN: 0027-8424, 1091-6490. DOI: 10.1073/pnas.1203552109. arXiv: 1112.5456.

[18] Aharon Brodutch, Daniel Nagaj, Or Sattath, and Dominique Unruh. “An adaptive attack on Wiesner’s quantum money” (Apr. 5, 2014). arXiv: 1404.1507.

[19] Michele Mosca and Douglas Stebila. “Uncloneable quantum money”. In: Canadian Quantum Information Students’ Conference (CQISC). 2006.

[20] Michele Mosca and Douglas Stebila. “A framework for quantum money”. In: Quantum Information Processing (QIP). Brisbane, Australia, 2007.

[21] S. Aaronson. "Quantum Copy-Protection and Quantum Money". In: *24th Annual IEEE Conference on Computational Complexity, 2009. CCC '09.* 24th Annual IEEE Conference on Computational Complexity, 2009. CCC '09. July 2009, pp. 229–242. DOI: 10.1109/CCC.2009.42.

[22] Andrew Lutomirski, Scott Aaronson, Edward Farhi, David Gosset, Avinatan Hassidim, Jonathan Kelner, and Peter Shor. "Breaking and making quantum money: toward a new quantum cryptographic protocol" (Dec. 20, 2009). arXiv: 0912.3825.

[23] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor. "Quantum money from knots" (Apr. 28, 2010). arXiv: 1004.5127.

[24] Andrew Lutomirski. "Component mixers and a hardness result for counterfeiting quantum money" (July 1, 2011). arXiv: 1107.0321.

[25] Marta Conde Pena, Jean-Charles Faugère, and Ludovic Perret. "Algebraic Cryptanalysis of a Quantum Money Scheme The Noise-Free Case". In: IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'15). Mar. 30, 2015.

[26] J. Rompel. "One-way Functions Are Necessary and Sufficient for Secure Signatures". In: *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing.* STOC '90. New York, NY, USA: ACM, 1990, pp. 387–394. ISBN: 978-0-89791-361-4. DOI: 10.1145/100216.100269.

[27] Scott Aaronson. "Limitations of Quantum Advice and One-Way Communication" (Feb. 14, 2004). arXiv: quant-ph/0402095.

[28] Jeff Garzik. *Making Decentralized Economic Policy.* BIP 100 - Theory and Discussion, v0.8.1. June 15, 2015.

[29] Fergal Reid and Martin Harrigan. "An Analysis of Anonymity in the Bitcoin System". In: *Security and Privacy in Social Networks.* Ed. by Yaniv Altshuler, Yuval Elovici, Armin B. Cremers, Nadav Aharony, and Alex Pentland. New York, NY: Springer New York, 2013, pp. 197–223. ISBN: 978-1-4614-4138-0.

[30] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names". In: *Proceedings of the 2013 Conference on Internet Measurement Conference.* IMC '13. New York, NY, USA: ACM, 2013, pp. 127–140. ISBN: 978-1-4503-1953-9. DOI: 10.1145/2504730.2504747.

[31] Malte Moser, Rainer Bohme, and Dominic Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem". In: IEEE, Sept. 2013, pp. 1–14. ISBN: 978-1-4799-1158-5. DOI: 10.1109/eCRS.2013.6805780.

[32] "BitIodine: Extracting Intelligence from the Bitcoin Network". PhD thesis. Aug. 2013.

[33] Dániel Kondor, Márton Pósfai, István Csabai, and Gábor Vattay. "Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network". *PLoS ONE* 9.2 (Feb. 2014). Ed. by Matjaž Perc, e86197. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0086197.

[34] Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. "Evaluating User Privacy in Bitcoin". In: *Financial Cryptography and Data Security.* Ed. by Ahmad-Reza Sadeghi. Lecture Notes in Computer Science 7859. Springer Berlin Heidelberg, Apr. 2013, pp. 34–51. ISBN: 978-3-642-39883-4. DOI: 10.1007/978-3-642-39884-1_4.

[35] Kerem Kaskaloglu. "Near Zero Bitcoin Transaction Fees Cannot Last Forever" (2014).

Publication F

Comment on “Franson Interference Generated by a Two-Level System”

J. Jogenfors, A. Cabello, and J.-Å. Larsson. “Comment on ”Franson Interference Generated by a Two-Level System”” (Mar. 15, 2017). arXiv: 1703.05055 [quant-ph].

This is a comment on M. Peiris, K. Konthasinghe, and A. Muller. “Franson Interference Generated by a Two-Level System”. *Physical Review Letters* 118.3 (Jan. 19, 2017), p. 030501. DOI: 10.1103/PhysRevLett.118.030501.

An erratum referencing our comment was published as M. Peiris, K. Konthasinghe, and A. Muller. “Franson Interference Generated by a Two-Level System”. *Physical Review Letters* 118.3 (Jan. 19, 2017), p. 030501. DOI: 10.1103/PhysRevLett.118.030501.

Copyright © 2017 Jonathan Jogenfors, Adán Cabello, and Jan-Åke Larsson.

Comment on “Franson Interference Generated by a Two-Level System”

Jonathan Jogenfors,[1] Adán Cabello,[2] and Jan-Åke Larsson[1]

[1] *Institutionen för systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden*
[2] *Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*

In a recent Letter [Phys. Rev. Lett. **118**, 030501 (2017)], Peiris, Konthasinghe, and Muller report a Franson interferometry experiment using pairs of photons generated from a two-level semiconductor quantum dot. The authors report a visibility of 66% and claim that this visibility “goes beyond the classical limit of 50% and approaches the limit of violation of Bell’s inequalities (70.7%).” We explain why we do not agree with this last statement and how to fix the problem.

In a recent Letter [1], Peiris, Konthasinghe, and Muller report a Franson interferometry experiment using pairs of photons generated via frequency-filtered scattered light from a two-level semiconductor quantum dot. The authors report a visibility of 66% and claim that this visibility “goes beyond the classical limit of 50% and approaches the limit of violation of Bell’s inequalities (70.7%).” In the following we explain why we do not agree with this last statement.

A violation of the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [2] without supplementary assumptions (so that it is loophole-free and therefore potentially usable for device-independent applications) is only possible in a very small region of values of the overall detection efficiency η and the visibility V. Specifically, it must occur that $V \geq (2/\eta - 1)/\sqrt{2}$ [3]. Therefore, the 70.7% visibility bound mentioned by Peiris, Konthasinghe, and Muller only holds under the assumption that $\eta = 1$.

The problem is that this value is impossible to achieve in the Franson interferometer, even ideally. As the authors correctly point out, in the Franson interferometer there is a crucial post-selection step which requires discarding, on average, 50% of the recorded photons. Therefore, *even in the ideal case that the detectors and couplings were perfect*, the effective η falls to 50%. This implies that it is possible to produce a classical local hidden variable models while retaining the same output statistics as predicted by quantum theory [4–6].

In fact, the above problem has recently been exploited to experimentally show that the security proof in Franson-based quantum key distribution schemes can be circumvented, exposing its users to eavesdropping [7]. In these attacks, tailored pulses of classical light are used, which indicates that the 50% “classical limit” can be beat even in a purely classical setting.

However, as described in [4], there is a possibility of detecting a genuine violation of a Bell inequality in the setting of Peiris, Konthasinghe, and Muller. It requires using a *different* Bell inequality, namely, a three-setting chained Bell inequality introduced by Pearle [8]. This modification allows for a genuine violation of local realism, but requires a higher visibility: At least, 94.63% [4, 6]. Although demanding, a recent work [9] shows that such an experiment is feasible.

In conclusion, while the setup in [1] is promising, the experimental data does not rule out all classical descriptions. A test of the three-setting chained Bell inequality could be a more suitable application for this correlated photon pair source. However, the corresponding experiment would be much more challenging as it requires a visibility of, at least, 94.63%.

This work was supported by the project “Photonic Quantum Information” (Knut and Alice Wallenberg Foundation, Sweden) and Project No. FIS2014-60843-P, “Advanced Quantum Information” (MINECO, Spain), with FEDER funds.

[1] M. Peiris, K. Konthasinghe, and A. Muller, Franson Interference Generated by a Two-Level System, Phys. Rev. Lett. **118**, 030501 (2017).

[2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories Phys. Rev. Lett. **23**, 880 (1969).

[3] J.-Å. Larsson, Modeling the singlet state with local variables, Phys. Lett. A **256**, 245 (1999).

[4] S. Aerts, P. Kwiat, J.-Å. Larsson, and M. Żukowski, Two-Photon Franson-Type Experiments and Local Realism, Phys. Rev. Lett. **83**, 2872 (1999).

[5] A. Cabello, A. Rossi, G. Vallone, F. De Martini, and P. Mataloni Proposed Bell Experiment with Genuine Energy-Time Entanglement, Phys. Rev. Lett. **102**, 040401 (2009).

[6] J. Jogenfors and J.-Å. Larsson, Energy-time entanglement, elements of reality, and local realism, J. Phys. A: Math. Theor. **47**, 424032 (2014).

[7] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, Hacking the Bell test using classical light in energy-time entanglementbased quantum key distribution, Science Advances **1**, e1500793 (2015).

[8] P. Pearle, Hidden-variable example based upon data rejection, Phys. Rev. D **2**, 1418 (1970).

[9] M. Tomasin, E. Mantoan, J. Jogenfors, G. Vallone, J.-Å. Larsson, and P. Villoresi, High-visibility time-bin entanglement for testing chained Bell inequalities, Phys. Rev. A **95**, 032107 (2017).