No information flow using statistical fluctuations and quantum cryptography

Jan-Åke Larsson

Larsson, J., (2004), No information flow using statistical fluctuations and quantum cryptography, *Physical Review A: covering atomic, molecular, and optical physics and quantum information*, 69(4), 042317-1-042317-8. https://doi.org/10.1103/PhysRevA.69.042317

Original publication available at:
https://doi.org/10.1103/PhysRevA.69.042317

No information flow using statistical fluctuations, and quantum cryptography

Jan-Åke Larsson
Matematiska Institutionen, Linköpings Universitet, SE-581 83 Linköping, Sweden

The communication protocol of Home and Whitaker [Phys. Rev. A **67**, 022306 (2003)] is examined in some detail, and found to work equally well using a separable state. The protocol is in fact completely classical, based on simple post-selection of suitable experimental runs. The quantum cryptography protocol proposed in the same publication is also examined, and is found to indeed need *quantum* properties for the system to be secure. However, the security test proposed in the mentioned paper is found to be insufficient, and a modification is proposed here that will ensure security.

PACS numbers: 03.67.Hk, 03.65.Ud, 03.67.Dd

I. INTRODUCTION

Information transfer using quantum entanglement is a subject of great interest presently. Quantum teleportation [1, 2, 3, 4] is one of the more prominent applications, although it has caused some debate about what is teleported or not [5, 6], and on the relation to nonlocality and inseparability [7, 8, 9, 10, 11]. Since quantum entanglement is one of the important resources in quantum information theory, the interest in these issues is not surprising. One application is that of quantum computers which would have a big impact on our world when/if one is actually built. One more immediate application is quantum cryptography [12, 13, 14], and one proposal of a quantum-cryptographic protocol will be discussed below.

First we will look at a quantum communication setup presented in [15], that uses the experimental setup but not the communication protocol of the quantum teleportation experiment. The protocol of [15] (to be described briefly below) is intended to communicate apparatus settings from Alice to Bob without transmitting the settings on the classical channel that connects Alice and Bob. This procedure is then extended in [15] to make a quantum cryptography protocol. Here, these two will be critically examined in order.

The communication protocol is as follows: Alice and Bob share one half each of many copies of a maximally entangled 2-part spin-$\frac{1}{2}$ state indexed 2 and 3, and Alice has an additional particle at her disposal indexed 1, so that the total state is

$$|\Psi_{123}\rangle = \big(a\,|{\uparrow_1}\rangle + b\,|{\downarrow_1}\rangle\big)\tfrac{1}{\sqrt{2}}\big(|{\uparrow_2}{\downarrow_3}\rangle - |{\downarrow_2}{\uparrow_3}\rangle\big), \qquad (1)$$

using the obvious notation for eigenstates of s_{zn} (and we will denote the measurement results S_{zn} below). The coefficients a and b are chosen to be real here, so that $a^2+b^2=1$. Should one want to use complex coefficients, each occurrence of a^2 and b^2 below should be exchanged for $|a|^2$ and $|b|^2$, respectively. An alternative way to write the state is

$$\begin{aligned}|\Psi_{123}\rangle = \tfrac{1}{2}\Big\{ &\big|\Psi^+_{12}\big\rangle\big(-a\,|{\uparrow_3}\rangle + b\,|{\downarrow_3}\rangle\big)\\ &+\big|\Psi^-_{12}\big\rangle\big(-a\,|{\uparrow_3}\rangle - b\,|{\downarrow_3}\rangle\big)\\ &+\big|\Phi^+_{12}\big\rangle\big(-b\,|{\uparrow_3}\rangle + a\,|{\downarrow_3}\rangle\big)\\ &+\big|\Phi^-_{12}\big\rangle\big(+b\,|{\uparrow_3}\rangle + a\,|{\downarrow_3}\rangle\big)\Big\},\end{aligned} \qquad (2)$$

where we have used the Bell basis

$$\begin{aligned}\big|\Psi^+_{12}\big\rangle &= \tfrac{1}{\sqrt{2}}\big(|{\uparrow_1}{\downarrow_2}\rangle + |{\downarrow_1}{\uparrow_2}\rangle\big)\\ \big|\Psi^-_{12}\big\rangle &= \tfrac{1}{\sqrt{2}}\big(|{\uparrow_1}{\downarrow_2}\rangle - |{\downarrow_1}{\uparrow_2}\rangle\big)\\ \big|\Phi^+_{12}\big\rangle &= \tfrac{1}{\sqrt{2}}\big(|{\uparrow_1}{\uparrow_2}\rangle + |{\downarrow_1}{\downarrow_2}\rangle\big)\\ \big|\Phi^-_{12}\big\rangle &= \tfrac{1}{\sqrt{2}}\big(|{\uparrow_1}{\uparrow_2}\rangle - |{\downarrow_1}{\downarrow_2}\rangle\big).\end{aligned} \qquad (3)$$

Each run of the protocol uses four of these trios as follows.

Alice performs either (a) four Bell-state measurements on her two particles 1 and 2 or (b) four measurements of S_{z1} and S_{z2}. In either case, if Alice should happen to get *different* measurement results on her side in all four measurements [denoted "criterion Q" in Ref. [15]], she announces "OK" to Bob on the classical channel. Bob, on the other hand, always performs four measurements of S_{z3} and calculates the sum $S_{z3\mathrm{t}}$ of these results. If he received "OK" on the classical channel, the two possibilities of settings at Alice give different probability distributions of $S_{z3\mathrm{t}}$.

If Alice's setting was (a), Bob has the probability a^2 of getting $+\hbar$ for two of the four particles in the group, and the probability b^2 of getting $+\hbar$ for the other two particles. This is easily seen in Eq. (2), and implies the following for the probability distribution of the sum,

$$\begin{aligned}P(S_{z3\mathrm{t}}=2\hbar) = P(S_{z3\mathrm{t}}=-2\hbar) &= a^4b^4\\ P(S_{z3\mathrm{t}}=\hbar) = P(S_{z3\mathrm{t}}=-\hbar) &= 2a^2b^2(a^4+b^4)\\ P(S_{z3\mathrm{t}}=0) &= a^8+4a^4b^4+b^8.\end{aligned} \qquad (4)$$

Looking at expectation values, we see that

$$\langle S_{z3\mathrm{t}}\rangle = 0;\quad \langle S^2_{z3\mathrm{t}}\rangle = 4\hbar^2a^2b^2, \qquad (5)$$

where the latter is zero only if a or b is zero.

If Alice's setting was (b) instead, inspection in Eq. (1) shows that Bob will get two each of "up" and "down", or in other words that

$$\begin{aligned}P(S_{z3\mathrm{t}}=2\hbar) = P(S_{z3\mathrm{t}}=\hbar) &= P(S_{z3\mathrm{t}}=-\hbar)\\ &= P(S_{z3\mathrm{t}}=-2\hbar) = 0;\quad P(S_{z3\mathrm{t}}=0)=1,\end{aligned} \qquad (6)$$

so

$$\langle S_{z3\mathrm{t}}\rangle = 0;\quad \langle S^2_{z3\mathrm{t}}\rangle = 0. \qquad (7)$$

Bob now checks if the value of S_{z3t} he received is zero or nonzero. In the case his measured sum is nonzero he knows with certainty that Alice's setting was (a), in the ideal case, since it is obvious in Eq. (6) that nonzero values only occur for setting (a). If the measured sum is zero, the situation is different. We have

$$P\Big(S_{z3t}=0\,\Big|\,\text{setting (b)}\Big)=1, \tag{8}$$

while

$$P\Big(S_{z3t}=0\,\Big|\,\text{setting (a)}\Big)=a^8+4a^4b^4+b^8. \tag{9}$$

To distinguish the setting (a) from the setting (b), one wants the error probability in Eq. (9) to be as small as possible. It is minimized if $a=b=1/\sqrt{2}$, for which it is $3/8=0.375$. If the protocol is modified to use $4N$ triads rather than four, this probability can be made arbitrarily small. The protocol will indeed indicate to Bob which setting Alice has used, even though the "OK" that Alice sent on the classical channel seems to have nothing to do with the setting she chose.

II. A SEPARABLE-STATE IMPLEMENTATION

It is noted in Ref. [15] that maximal entanglement is not necessary for this scheme, but it is argued that entanglement does play a role. Let us look at this claim closer. Suppose that the state used is not that of Eq. (1)) but the separable mixed state

$$\begin{aligned}\rho_{123}=&\big(a^2\left|\uparrow_1\right\rangle\left\langle\uparrow_1\right|+b^2\left|\downarrow_1\right\rangle\left\langle\downarrow_1\right|\big)\\&\otimes\tfrac{1}{2}\big(\left|\uparrow_2\downarrow_3\right\rangle\left\langle\uparrow_2\downarrow_3\right|+\left|\downarrow_2\uparrow_3\right\rangle\left\langle\downarrow_2\uparrow_3\right|\big).\end{aligned} \tag{10}$$

Rewriting this in the Bell basis yields the expression

$$\begin{aligned}\rho_{123}=&\tfrac{1}{4}\Big[\big(\left|\Psi^+_{12}\right\rangle\left\langle\Psi^+_{12}\right|+\left|\Psi^-_{12}\right\rangle\left\langle\Psi^-_{12}\right|\big)\\&\quad\otimes\big(a^2\left|\uparrow_3\right\rangle\left\langle\uparrow_3\right|+b^2\left|\downarrow_3\right\rangle\left\langle\downarrow_3\right|\big)\\&+\big(\left|\Phi^+_{12}\right\rangle\left\langle\Phi^+_{12}\right|+\left|\Phi^-_{12}\right\rangle\left\langle\Phi^-_{12}\right|\big)\\&\quad\otimes\big(b^2\left|\uparrow_3\right\rangle\left\langle\uparrow_3\right|+a^2\left|\downarrow_3\right\rangle\left\langle\downarrow_3\right|\big)\Big]\\&+\tfrac{1}{4}\Big[\big(\left|\Psi^+_{12}\right\rangle\left\langle\Psi^-_{12}\right|+\left|\Psi^-_{12}\right\rangle\left\langle\Psi^+_{12}\right|\big)\\&\quad\otimes\big(a^2\left|\uparrow_3\right\rangle\left\langle\uparrow_3\right|-b^2\left|\downarrow_3\right\rangle\left\langle\downarrow_3\right|\big)\\&-\big(\left|\Phi^+_{12}\right\rangle\left\langle\Phi^-_{12}\right|+\left|\Phi^-_{12}\right\rangle\left\langle\Phi^+_{12}\right|\big)\\&\quad\otimes\big(b^2\left|\uparrow_3\right\rangle\left\langle\uparrow_3\right|-a^2\left|\downarrow_3\right\rangle\left\langle\downarrow_3\right|\big)\Big],\end{aligned} \tag{11}$$

where the first parenthesis contains the diagonal elements. The question now is what happens when using the above protocol on ρ_{123}. Let us assume that Alice has received four different measurement results [criterion Q] and announced "OK" on the classical channel.

If Alice's setting was (a), Bob has the probability a^2 of getting $+\hbar$ for two of the four particles in the group, and the probability b^2 of getting $+\hbar$ for the other two particles. This is easily seen in Eq. (11), from this follows that the probability distribution of the sum is

$$\begin{aligned}P(S_{z3t}=2\hbar)=P(S_{z3t}=-2\hbar)&=a^4b^4\\P(S_{z3t}=\hbar)=P(S_{z3t}=-\hbar)&=2a^2b^2(a^4+b^4)\\P(S_{z3t}=0)&=a^8+4a^4b^4+b^8.\end{aligned} \tag{12}$$

Looking at expectation values, we see that

$$\langle S_{z3t}\rangle=0;\quad\langle S_{z3t}^2\rangle=4\hbar^2a^2b^2, \tag{13}$$

where the latter is zero only if a or b is zero.

If Alice's setting was (b) instead, inspection in Eq. (10) shows that

$$\begin{aligned}P(S_{z3t}=2\hbar)&=P(S_{z3t}=\hbar)=P(S_{z3t}=-\hbar)\\&=P(S_{z3t}=-2\hbar)=0;\quad P(S_{z3t}=0)=1,\end{aligned} \tag{14}$$

so

$$\langle S_{z3t}\rangle=0;\quad\langle S_{z3t}^2\rangle=0. \tag{15}$$

This is exactly the same as Eqs. (4)–(7), so the conclusion is the same. There is another way to see this because, with a and b possibly complex,

$$\begin{aligned}\left|\Psi_{123}\right\rangle\left\langle\Psi_{123}\right|=&\big(a\left|\uparrow_1\right\rangle+b\left|\downarrow_1\right\rangle\big)\big(\bar{a}\left\langle\uparrow_1\right|+\bar{b}\left\langle\downarrow_1\right|\big)\\&\otimes\tfrac{1}{2}\big(\left|\uparrow_2\downarrow_3\right\rangle-\left|\downarrow_2\uparrow_3\right\rangle\big)\big(\left\langle\uparrow_2\downarrow_3\right|-\left\langle\downarrow_2\uparrow_3\right|\big)\\=&\rho_{123}-\big(a\left|\uparrow_1\right\rangle+b\left|\downarrow_1\right\rangle\big)\big(\bar{a}\left\langle\uparrow_1\right|+\bar{b}\left\langle\downarrow_1\right|\big)\\&\otimes\tfrac{1}{2}\big(\left|\uparrow_2\downarrow_3\right\rangle\left\langle\downarrow_2\uparrow_3\right|+\left|\downarrow_2\uparrow_3\right\rangle\left\langle\uparrow_2\downarrow_3\right|\big)\\&+\big(a\bar{b}\left|\uparrow_1\right\rangle\left\langle\downarrow_1\right|+\bar{a}b\left|\downarrow_1\right\rangle\left\langle\uparrow_1\right|\big)\\&\otimes\tfrac{1}{2}\big(\left|\uparrow_2\downarrow_3\right\rangle\left\langle\uparrow_2\downarrow_3\right|-\left|\downarrow_2\uparrow_3\right\rangle\left\langle\downarrow_2\uparrow_3\right|\big).\end{aligned} \tag{16}$$

Note that the last two terms are off-diagonal only. Writing $\left|\Psi_{123}\right\rangle\left\langle\Psi_{123}\right|$ in the Bell basis on particles 1 and 2 will yield a full matrix in the density representation, consisting of 64 elements. Let us not write that large expression here, but simply note that

$$\begin{aligned}\left|\Psi_{123}\right\rangle\left\langle\Psi_{123}\right|=&\tfrac{1}{4}\Big[\big(\left|\Psi^+_{12}\right\rangle\left\langle\Psi^+_{12}\right|+\left|\Psi^-_{12}\right\rangle\left\langle\Psi^-_{12}\right|\big)\\&\quad\otimes\big(a^2\left|\uparrow_3\right\rangle\left\langle\uparrow_3\right|+b^2\left|\downarrow_3\right\rangle\left\langle\downarrow_3\right|\big)\\&+\big(\left|\Phi^+_{12}\right\rangle\left\langle\Phi^+_{12}\right|+\left|\Phi^-_{12}\right\rangle\left\langle\Phi^-_{12}\right|\big)\\&\quad\otimes\big(a^2\left|\downarrow_3\right\rangle\left\langle\downarrow_3\right|+b^2\left|\uparrow_3\right\rangle\left\langle\uparrow_3\right|\big)\Big]\\&+\Big[\text{off-diagonal terms}\Big]\\=&\rho_{123}+\Big[\text{off-diagonal terms}\Big].\end{aligned} \tag{17}$$

So, it is clear from Eq. (17) that for (a) Bell-state measurements at Alice and S_{z3} measurements at Bob, the two states will yield the same statistics. Similarly, it is clear from Eq. (16) that for (b) measurements of S_{zn} at Alice and Bob, the two states will yield the same statistics. The densities have equal diagonal elements *in both expansions*, and are therefore impossible to distinguish if Alice and Bob are only allowed to use measurements (a) or (b), and measurement of S_{z3}, respectively. A discussion of the role of the off-diagonal elements in regular quantum teleportation can be found in Ref. [5]. Of course, the off-diagonal elements will play a role if Alice and Bob are allowed other measurements than the ones singled out above. Especially, only allowing Bob measurements of S_{z3} is a severe restriction, but we will investigate this further in Section IV below.

However, for the proposed protocol, the *separable* mixed state ρ_{123} will produce the same results as $|\Psi_{123}\rangle\langle\Psi_{123}|$. In fact, the protocol does not use any specifically *quantum* properties of the system, it uses classical postselection to obtain the desired statistics. Postselection *is* known to sometimes give unexpected results (see, e.g., [16]).

III. A COIN-TOSS IMPLEMENTATION

It is not difficult to implement this protocol using a number of classical unbiased and biased coin tosses. To make it look like the above setup, we will use three coins c_1, c_2 and c_3 that are divided so that Alice can read off the results from coins c_1 and c_2 while Bob can read the result of coin c_3.

Coin c_1 is biased so that

$$P(c_1 = +1) = a^2; \quad P(c_1 = -1) = b^2, \tag{18}$$

where we have used $+1$ to denote "heads" and -1 to denote "tails". Coin c_2 is fair, i.e.,

$$P(c_2 = +1) = \tfrac{1}{2}; \quad P(c_2 = -1) = \tfrac{1}{2}, \tag{19}$$

and coin c_3 always gives the opposite result to coin c_2. This can be implemented using *one* coin toss at the "source of the c_2-c_3 pair," communicating the result to Alice, and the opposite result to Bob, both on a classical channel. In addition, we will need a fair coin c_4 that Alice will use in case (a) below. An important comment to make is that the coins c_1, c_2, and c_4 should be independent.

The protocol proceeds as above, with groups of four tosses of the coins c_1–c_4. A "measurement" consists of reading off the result of a coin toss. Alice reads either (a) four results of c_4 and the product c_1c_2 [which, in a way, corresponds to the Bell-state measurement used previously], or (b) four results of c_1 and c_2. In either case, if Alice should happen to get four *different* results on her side [criterion Q], she announces "OK" to Bob on the classical channel. Bob, on the other hand, always reads off c_3, and calculates the sum $c_{3\mathrm{t}}$ of the results. If he received "OK" on the classical channel, the two possibilities of settings at Alice give different conditional probability distributions of $c_{3\mathrm{t}}$.

The case when Alice used setting (b) is trivial, since Bob will receive two each of $+1$ and -1, so the probability distribution reads

$$\begin{aligned} P(c_{3\mathrm{t}} = 2) &= P(c_{3\mathrm{t}} = 1) = P(c_{3\mathrm{t}} = -1) \\ &= P(c_{3\mathrm{t}} = -2) = 0; \quad P(c_{3\mathrm{t}} = 0) = 1, \end{aligned} \tag{20}$$

and the classical expectations are

$$E(c_{3\mathrm{t}}) = 0; \quad E(c_{3\mathrm{t}}^2) = 0. \tag{21}$$

The case when Alice's setting was (a) is a more complicated and, for clarity, let us do the calculation explicitly. Since the coins c_1 and c_2 are independent and c_2 is fair,

$$P(c_1c_2 = -1) = \tfrac{1}{2}, \tag{22}$$

and since $c_3 = -c_2$ we have

$$\begin{aligned} P(c_3 = -1 \cap c_1c_2 = -1) &= P(c_2 = +1 \cap c_1 = -1) \\ &= P(c_2 = +1)P(c_1 = -1) = \tfrac{1}{2}b^2. \end{aligned} \tag{23}$$

Thus

$$P(c_3 = -1 | c_1c_2 = -1) = \frac{P(c_3 = -1 \cap c_1c_2 = -1)}{P(c_1c_2 = -1)} = b^2, \tag{24a}$$

and from that follows

$$P(c_3 = +1 | c_1c_2 = -1) = a^2. \tag{24b}$$

From a similar calculation we obtain

$$\begin{aligned} P(c_3 = -1 | c_1c_2 = +1) &= a^2, \\ P(c_3 = +1 | c_1c_2 = +1) &= b^2. \end{aligned} \tag{25}$$

An "OK" from Alice means that the result of c_1c_2 was $+1$ twice and -1 twice. This implies that the probability distribution of the sum $c_{3\mathrm{t}}$ must be

$$\begin{aligned} P(c_{3\mathrm{t}} = 2) = P(c_{3\mathrm{t}} = -2) &= a^4b^4 \\ P(c_{3\mathrm{t}} = 1) = P(c_{3\mathrm{t}} = -1) &= 2a^2b^2(a^4 + b^4) \\ P(c_{3\mathrm{t}} = 0) &= a^8 + 4a^4b^4 + b^8. \end{aligned} \tag{26}$$

Looking at expectation values, we see that

$$E(c_{3\mathrm{t}}) = 0; \quad E(c_{3\mathrm{t}}^2) = 4a^2b^2, \tag{27}$$

where the latter is zero only if a or b is zero.

This is the same statistics as obtained before (modulo the measurement-result labels $\pm\hbar$), so this completely classical scheme implements the protocol just as well as the previous two quantum systems.

IV. QUANTUM CRYPTOGRAPHY

The second issue in [15] is to provide a quantum cryptography protocol based on the above procedure. As is usual, Alice and Bob are assumed to have an open but unjammable classical channel to communicate on, and a quantum channel that in this case consists of the common source emitting particles 2 and 3. Alice has two random sequences of bits, one that provides the *raw key* to be transmitted to Bob over the quantum channel, and another that decides the *encoding* to be used. Bob has a third random bit sequence that decides the *decoding* he will use.

Note that the described use of three different random bit sequences is very similar to the BB84 [12] protocol. The difference is that the present setup uses a source of entangled pairs of qubits, much as in Ekert quantum cryptography [13] but, as we will see shortly, without the Bell inequality test. Another difference is the usage of several pairs of qubits for transmission of a bit in the key, as described below.

For each bit with the value 1 in the raw key Alice makes (a) $4N$ Bell-state measurements, and for each bit with the value 0 she uses the encoding bit-sequence to determine which to perform of (b) $4N$ measurements of S_{z1} and S_{z2}, or (c) $4N$ measurements of S_{x1} and S_{x2}. Bob, who knows nothing of Alice's two bit sequences, uses his decoding bit sequence to determine which to perform of (b') $4N$ measurements of S_{z3} or (c') $4N$ measurements of S_{x3}.

Given that Alice receives the four possible results N times each [criterion Q], she announces the encoding to Bob (but not the key bit), i.e., which setting of (b) or (c) she used. If she happened to use setting (a), the encoding bit will make her announce one of (b) or (c) to Bob, randomly with equal probability. This means that Alice transmits the encoding bit to Bob, but not the raw key bit; she does not transmit any information about the raw key over the classical channel.

Bob discards data where his setting was (b') and Alice announced (c), and where his setting was (c') and Alice announced (b). For the remaining runs, when he used setting (b') he can determine whether Alice's setting was (a) or (b) by the earlier protocol, and similarly when he used setting (c') he can determine whether Alice's setting was (a) or (c). He can now determine the bits of the raw key for the experimental runs that remain after the above filtering. He also communicates which runs he is using to Alice, but neither the settings nor the resulting bit. The remaining bit sequence (the sifted key) will now be equal at Alice and Bob, or at least as equal as possible, see below. They have established a key to use in their cryptographic scheme.

There will be some noise in the sifted key even in the ideal case, because Bob cannot with certainty say, for example, whether Alice used (a) or (b). If Bob receives a nonzero result in his measurement of $S_{z3\mathrm{t}}$, he knows that Alice's setting was (a) but if Bob receives a zero result, the probability that Alice used setting (b) is larger than $\frac{1}{2}$ but there is a nonzero probability that the setting was (a). This probability will depend on a, b and N and tend to zero as N tends to infinity. In a real implementation one has to choose N finite, otherwise the key rate will be zero. For example, when $a = b$ and $N = 1$,

Table 1
Normal operation: $P(\mathrm{OK}) = \frac{6}{64}$

Alice's bit	Bob's bit	Probability
0	0	1
0	1	0
1	0	$\frac{3}{8}$
1	1	$\frac{5}{8}$

The visible effect will be that some ones in Alice's bit-sequence will arrive as the value zero at Bob. In the ideal case, no zeros will become one, so evidently, Bob's copy of the sifted key will have slightly more zeros than Alice's copy.

Comparing this cryptographic scheme with the previously described communication scheme, the set of possible measurement setups is extended so that the off-diagonal terms in the expansion of $|\Psi_{123}\rangle\langle\Psi_{123}|$ come into play, making that particular state or another entangled state a requirement for the quantum cryptography scheme. And the whole idea of quantum cryptography is to use specifically *quantum* properties of a system in such a way that eavesdropping always will be detectable. It is noted in Ref. [15] that if $|\Psi_{123}\rangle\langle\Psi_{123}|$ is used, and the eavesdropper Eve makes $4N$ measurements of either S_{z3} or S_{x3} at random, she will be detected. In the case $a = b$ and $N = 1$, we have

Table 2
Eve is listening: $P(\mathrm{OK}) = \frac{6}{64}$

Alice's bit	Eve's basis	Bob's bit	Probability
0	correct	0	1
0	correct	1	0
0	incorrect	0	$\frac{3}{8}$
0	incorrect	1	$\frac{5}{8}$
0	(mean)	0	$\frac{11}{16}$
0	(mean)	1	$\frac{5}{16}$
1	either	0	$\frac{3}{8}$
1	either	1	$\frac{5}{8}$

Apparently, there will be extra noise, but only in the zeros. In comparison to the BB84 protocol, the situation is as follows:

Table 3

		BB84	HW[15]
Alice's bit	Eve is	$P(\mathrm{error})$	$P(\mathrm{error})$
0	absent	0	0
1	absent	0	$\frac{3}{8}$
0	present	$\frac{1}{4}$	$\frac{5}{16}$
1	present	$\frac{1}{4}$	$\frac{3}{8}$

The performance of BB84 is better than the protocol of Home and Whitaker [15] when Eve is absent, while the figures are comparable when Eve is present. Of course, the protocol of [15] uses more qubits per sifted key bit than BB84. Both protocols will reject half the data outright (when the "settings" disagree at Alice and Bob), but in addition, the protocol of [15] uses four qubits for each raw key bit and of these only 6/64 will yield a bit in the sifted key, that is, when Alice announces "OK" on the classical channel. Also there is another problem, which we will turn to now.

V. A COHERENT ATTACK

If the source is in an insecure location, or if Eve has access to both the quantum channel going from the source to Alice and that going to Bob, she can replace the source with her own. Eve can of course replace the source emitting the entangled state with a source randomly emitting either $4N$ copies of the mixed state

$$\frac{1}{2}\big(|\uparrow_{z2}\downarrow_{z3}\rangle\langle\uparrow_{z2}\downarrow_{z3}| + |\downarrow_{z2}\uparrow_{z3}\rangle\langle\downarrow_{z2}\uparrow_{z3}|\big), \tag{28a}$$

or $4N$ copies of

$$\tfrac{1}{2}\left(|\uparrow_{x2}\downarrow_{x3}\rangle\langle\uparrow_{x2}\downarrow_{x3}| + |\downarrow_{x2}\uparrow_{x3}\rangle\langle\downarrow_{x2}\uparrow_{x3}|\right), \tag{28b}$$

but that would yield the same statistics as that obtained when Eve is simply eavesdropping on (one of) the quantum channels. And then, Alice and Bob can use a statistical test to detect Eve's precense.

Eve can do something more clever than transmitting $4N$ copies of a mixed state, but let us now restrict ourselves to the case $N = 1$ and $a = b$ for simplicity. Note that Eve has complete freedom of choosing what state to send to Alice and Bob, including what *sequence* of states to send. She can for instance choose to send the sequence

$$\begin{aligned}&|\uparrow_{z2}\downarrow_{z3}\rangle\langle\uparrow_{z2}\downarrow_{z3}|,\ |\uparrow_{z2}\downarrow_{z3}\rangle\langle\uparrow_{z2}\downarrow_{z3}|,\\ &|\downarrow_{z2}\uparrow_{z3}\rangle\langle\downarrow_{z2}\uparrow_{z3}|,\ |\downarrow_{z2}\uparrow_{z3}\rangle\langle\downarrow_{z2}\uparrow_{z3}|,\end{aligned} \tag{29}$$

which would yield a key bit of zero at Bob if Bob uses the (b') setting: measurement of $S_{z3\mathrm{tot}}$; in the above sequence, the sum of the received spins is zero. At Alice, the sequence will yield "OK" if Alice uses the (b) setting. In a different notation, Eve will have sent the state

$$|\mathrm{C}_{z2}\rangle = |\uparrow^1_{z2}\uparrow^2_{z2}\downarrow^3_{z2}\downarrow^4_{z2}\rangle \tag{30}$$

to Alice (the upper index on the right-hand side denotes the timeslot, and in hexadecimal $\mathrm{C}_{16} = 1100_2$ perhaps with the name "qunybble" [17]), and

$$|3_{z3}\rangle = |\downarrow^1_{z3}\downarrow^2_{z3}\uparrow^3_{z3}\uparrow^4_{z3}\rangle \tag{31}$$

to Bob. Obviously, this state is only good if Alice and Bob do not use (c) and (c'). If they do, the probability of "OK" at Alice is 6/64 since the results will be random at Alice, and there will be some noise in the "transmitted" key bit at Bob, since the measurement results will be random there as well. But Eve has one more ace up her sleeve: entanglement.

Note that

$$\begin{aligned}|3_{z3}\rangle + |\mathrm{C}_{z3}\rangle =& \frac{1}{2}\Big[\Big(|0_{x3}\rangle + |\mathrm{F}_{x3}\rangle\Big) + \Big(|3_{x3}\rangle + |\mathrm{C}_{x3}\rangle\Big)\\ &- \Big(|5_{x3}\rangle + |\mathrm{A}_{x3}\rangle\Big) - \Big(|9_{x3}\rangle + |6_{x3}\rangle\Big)\Big],\end{aligned} \tag{32a}$$

$$\begin{aligned}|5_{z3}\rangle + |\mathrm{A}_{z3}\rangle =& \frac{1}{2}\Big[\Big(|0_{x3}\rangle + |\mathrm{F}_{x3}\rangle\Big) - \Big(|3_{x3}\rangle + |\mathrm{C}_{x3}\rangle\Big)\\ &+ \Big(|5_{x3}\rangle + |\mathrm{A}_{x3}\rangle\Big) - \Big(|9_{x3}\rangle + |6_{x3}\rangle\Big)\Big],\end{aligned} \tag{32b}$$

and

$$\begin{aligned}|9_{z3}\rangle + |6_{z3}\rangle =& \frac{1}{2}\Big[\Big(|0_{x3}\rangle + |\mathrm{F}_{x3}\rangle\Big) - \Big(|3_{x3}\rangle + |\mathrm{C}_{x3}\rangle\Big)\\ &- \Big(|5_{x3}\rangle + |\mathrm{A}_{x3}\rangle\Big) + \Big(|9_{x3}\rangle + |6_{x3}\rangle\Big)\Big].\end{aligned} \tag{32c}$$

Letting $q = \exp(2i\pi/3)$, Eve can choose to transmit the state $|\psi_{3,00}\rangle$, given by

$$\begin{aligned}&\sqrt{6}|\psi_{3,00}\rangle\\ &= \Big(|3_{z3}\rangle + |\mathrm{C}_{z3}\rangle\Big) + q\Big(|5_{z3}\rangle + |\mathrm{A}_{z3}\rangle\Big) + q^2\Big(|9_{z3}\rangle + |6_{z3}\rangle\Big)\\ &= \Big(|3_{x3}\rangle + |\mathrm{C}_{x3}\rangle\Big) + q\Big(|5_{x3}\rangle + |\mathrm{A}_{x3}\rangle\Big) + q^2\Big(|9_{x3}\rangle + |6_{x3}\rangle\Big),\end{aligned} \tag{33}$$

for which the result of measuring *either of* the sum $S_{z3\mathrm{tot}}$ and the sum $S_{x3\mathrm{tot}}$ is zero. The above is an entangled state, but the entanglement is in the sequence of particles emitted to Bob instead of the pairwise entanglement between particles 2 and 3 in the original source. Bob will always receive the measurement result zero, irrespective if his setting is (b') or (c'); this particular source is "tuned" for zeros. In addition, if Eve transmits the same state to Alice, or rather the corresponding $|\psi_{2,00}\rangle$, Alice will have a higher chance of getting "OK" if she uses the setting (b) or (c), since the results at particle 2 will be two of "up" and two "down". The probability of getting "OK" is then $\frac{1}{4}$ (or 16/64) rather than the usual $6/64$. We have

Table 4

Eve tunes the source for zeros

Alice's bit	$P(\mathrm{OK})$	Bob's bit	Probability
0	$\frac{16}{64}$	0	1
0	$\frac{16}{64}$	1	0
1	$\frac{6}{64}$	0	1
1	$\frac{6}{64}$	1	0

Eve cannot use this source only, since only zeros would be transmitted (correctly) to Bob. But Eve can also tune the source to produce ones; note that

$$\begin{aligned}|0_{z3}\rangle - |\mathrm{F}_{z3}\rangle =& \frac{1}{2}\Big[\Big(|1_{x3}\rangle + |\mathrm{E}_{x3}\rangle\Big) + \Big(|2_{x3}\rangle + |\mathrm{D}_{x3}\rangle\Big)\\ &+ \Big(|4_{x3}\rangle + |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle + |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{34}$$

while

$$\begin{aligned}|1_{z3}\rangle - |\mathrm{E}_{z3}\rangle =& \frac{1}{2}\Big[-\Big(|1_{x3}\rangle - |\mathrm{E}_{x3}\rangle\Big) + \Big(|2_{x3}\rangle - |\mathrm{D}_{x3}\rangle\Big)\\ &+ \Big(|4_{x3}\rangle - |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{35a}$$

$$\begin{aligned}|2_{z3}\rangle - |\mathrm{D}_{z3}\rangle =& \frac{1}{2}\Big[\Big(|1_{x3}\rangle - |\mathrm{E}_{x3}\rangle\Big) - \Big(|2_{x3}\rangle - |\mathrm{D}_{x3}\rangle\Big)\\ &+ \Big(|4_{x3}\rangle - |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{35b}$$

$$\begin{aligned}|4_{z3}\rangle - |\mathrm{B}_{z3}\rangle =& \frac{1}{2}\Big[\Big(|1_{x3}\rangle - |\mathrm{E}_{x3}\rangle\Big) + \Big(|2_{x3}\rangle - |\mathrm{D}_{x3}\rangle\Big)\\ &- \Big(|4_{x3}\rangle - |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{35c}$$

and

$$|8_{z3}\rangle - |7_{z3}\rangle = \frac{1}{2}\Big[\Big(|1_{x3}\rangle - |E_{x3}\rangle\Big) + \Big(|2_{x3}\rangle - |D_{x3}\rangle\Big) + \Big(|4_{x3}\rangle - |B_{x3}\rangle\Big) - \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big]. \tag{35d}$$

So Eve could use the state $|\psi_{3,11}\rangle$, where

$$\begin{aligned}\sqrt{10}|\psi_{3,11}\rangle =& \Big(|0_{z3}\rangle - |F_{z3}\rangle\Big) \\ &+ q\Big(|1_{z3}\rangle + |2_{z3}\rangle + |4_{z3}\rangle + |8_{z3}\rangle\Big) \\ &+ q^2\Big(|E_{z3}\rangle + |D_{z3}\rangle + |B_{z3}\rangle + |6_{z3}\rangle\Big) \\ =& \Big(|0_{z2}\rangle - |F_{z2}\rangle\Big) \\ &+ q\Big(|1_{z2}\rangle + |2_{z2}\rangle + |4_{z2}\rangle + |8_{z2}\rangle\Big) \\ &+ q^2\Big(|E_{z2}\rangle + |D_{z2}\rangle + |B_{z2}\rangle + |6_{z2}\rangle\Big),\end{aligned} \tag{36}$$

for which the relevant probabilities are

Table 5
Eve tunes the source for ones

Alice's bit	$P(\text{OK})$	Bob's bit	Probability
0	0	0	0
0	0	1	1
1	$\frac{6}{64}$	0	0
1	$\frac{6}{64}$	1	1

Eve does not want to change the ratio of ones to zeros in the transmitted key from that of the raw key, since that would enable a statistical test for her presence. The rate of OK's should be $6/64$ irrespective of whether Alice has a 0 or a 1 in her raw key. This will be achieved by letting Eve's source be tuned for zeros with a probability of $6/16$, and be tuned for ones with a probability of $10/16$. In quantum language, Eve would tune the source to send

$$\tfrac{3}{8}\big|\psi_{2,00}\psi_{3,00}\big\rangle\big\langle\psi_{2,00}\psi_{3,00}\big| + \tfrac{5}{8}\big|\psi_{2,11}\psi_{3,11}\big\rangle\big\langle\psi_{2,11}\psi_{3,11}\big|. \tag{37}$$

Remarkably, this is the same ratio as is required to make the 16 different bit combinations of the four particles equally probable, something also desired by Eve, because otherwise, e.g., Bob could test the statistical properties of his unfiltered data to detect Eve. With this ratio, the probability of "OK" is

$$P\Big(\text{OK}\Big|\text{Raw key bit is 0}\Big) = \tfrac{6}{16}\cdot\tfrac{16}{64} + \tfrac{10}{16}\cdot 0 = \tfrac{6}{64} \tag{38a}$$

and

$$P\Big(\text{OK}\Big|\text{Raw key bit is 1}\Big) = \tfrac{6}{16}\cdot\tfrac{6}{64} + \tfrac{10}{16}\cdot\tfrac{6}{64} = \tfrac{6}{64} \tag{38b}$$

Zeros are transferred only when the source is tuned for zeros, which also means that there will be no errors in the zeros, in the ideal case. However, ones will be "transferred" both when the source is tuned for ones (no errors in the ideal case) and when the source is tuned for zeros (all errors in the ideal case). With the above weighting, the rate of errors in the ones will be

$$P\Big(\text{Bob gets a 0}\Big|\text{OK, Raw key bit is 1}\Big) = \tfrac{6}{16}\cdot 1 + \tfrac{10}{16}\cdot 0 = \tfrac{3}{8} \tag{39}$$

We arrive at

Table 6
Eve tunes the source: $P(\text{OK}) = \frac{6}{64}$

Alice's bit	Bob's bit	Probability
0	0	1
0	1	0
1	0	$\frac{3}{8}$
1	1	$\frac{5}{8}$

This table is identical to Table 1, "Normal operation." Eve is controlling the source, and she knows what values Bob will recieve when Alice announces "OK" on the classical channel. She has, quite surprisingly, used entanglement to her benefit for a coherent attack on the four qubits making up a single key bit value. The errors occur exactly like in the case Eve is absent.

VI. THE PERFECT ILLUSION?

So Eve has a way to eavesdrop unnoticed on Alice and Bob, at least if the security test used is the one proposed in Section IV, estimating the error rate in the sifted key. But note that with the above tuned source, if Alice receives a spin sum is equal to zero, Bob will also receive a spin sum equal to zero, *regardless of the setting they use*. And (provided they have read this paper) Alice and Bob will by now know to test this in their system. Is this then enough?

Let us see if Eve can construct a system that obeys the following:

(i) Eve can eavesdrop, or alternatively, control the source so that she knows in advance what the results should be for both measurement settings

(ii) if Alice gets spin-sum zero at one setting, then Bob also should get spin-sum zero at the same setting

(iii) the spin-sum at one setting at Bob is statistically independent of the spin-sum at the other setting at Alice, and vice versa

(iv) the 16 different local results are equally probable at either setting

It takes some calculation to determine a state with these desired properties (desired by Eve, that is), but one such state is

$$\tfrac{9}{64}\big|\psi_{2,00}\psi_{3,00}\big\rangle\big\langle\psi_{2,00}\psi_{3,00}\big| + \tfrac{5}{64}\big|\alpha_{2,01}\alpha_{3,01}\big\rangle\big\langle\alpha_{2,01}\alpha_{3,01}\big| + \tfrac{5}{64}\big|\alpha'_{2,10}\alpha'_{3,10}\big\rangle\big\langle\alpha'_{2,10}\alpha'_{3,10}\big| + \tfrac{5}{64}\big|\beta_{2,01}\beta_{3,01}\big\rangle\big\langle\beta_{2,01}\beta_{3,01}\big| + \tfrac{5}{64}\big|\beta'_{2,10}\beta'_{3,10}\big\rangle\big\langle\beta'_{2,10}\beta'_{3,10}\big| + \tfrac{5}{64}\big|\gamma_{2,01}\gamma_{3,01}\big\rangle\big\langle\gamma_{2,01}\gamma_{3,01}\big| + \tfrac{5}{64}\big|\gamma'_{2,10}\gamma'_{3,10}\big\rangle\big\langle\gamma'_{2,10}\gamma'_{3,10}\big| + \tfrac{8}{64}\big|\chi_{2,11}\chi_{3,11}\big\rangle\big\langle\chi_{2,11}\chi_{3,11}\big| + \tfrac{8}{64}\big|\chi'_{2,11}\chi'_{3,11}\big\rangle\big\langle\chi'_{2,11}\chi'_{3,11}\big| + \tfrac{9}{64}\big|\phi_{2,11}\phi_{3,11}\big\rangle\big\langle\phi_{2,11}\phi_{3,11}\big|. \tag{40}$$

Here, the first index of the pure states in the pure-state expansion is the particle index as used before, and the later two indices indicate which bit value the particular state is tuned for, in the bases (b) and (c), in order. The included states are $\big|\psi_{3,00}\big\rangle$ as defined in Eq. (33), and

$$\begin{aligned}|\alpha_{3,01}\rangle &= \frac{1}{\sqrt{2}}\Big(|3_{z3}\rangle - |\mathrm{C}_{z3}\rangle\Big)\\ &= \frac{1}{2\sqrt{2}}\Big[-\Big(|1_{x3}\rangle - |\mathrm{E}_{x3}\rangle\Big) - \Big(|2_{x3}\rangle - |\mathrm{D}_{x3}\rangle\Big)\\ &\qquad + \Big(|4_{x3}\rangle - |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{41a}$$

$$\begin{aligned}|\beta_{3,01}\rangle &= \frac{1}{\sqrt{2}}\Big(|5_{z3}\rangle - |\mathrm{A}_{z3}\rangle\Big)\\ &= \frac{1}{2\sqrt{2}}\Big[-\Big(|1_{x3}\rangle - |\mathrm{E}_{x3}\rangle\Big) + \Big(|2_{x3}\rangle - |\mathrm{D}_{x3}\rangle\Big)\\ &\qquad - \Big(|4_{x3}\rangle - |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{41b}$$

$$\begin{aligned}|\gamma_{3,01}\rangle &= \frac{1}{\sqrt{2}}\Big(|9_{z3}\rangle - |6_{z3}\rangle\Big)\\ &= \frac{1}{2\sqrt{2}}\Big[-\Big(|1_{x3}\rangle - |\mathrm{E}_{x3}\rangle\Big) + \Big(|2_{x3}\rangle - |\mathrm{D}_{x3}\rangle\Big)\\ &\qquad + \Big(|4_{x3}\rangle - |\mathrm{B}_{x3}\rangle\Big) - \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{41c}$$

together with their "mirrored" counterparts

$$\begin{aligned}|\alpha'_{3,10}\rangle &= \frac{1}{2\sqrt{2}}\Big[-\Big(|1_{z3}\rangle - |\mathrm{E}_{z3}\rangle\Big) - \Big(|2_{z3}\rangle - |\mathrm{D}_{z3}\rangle\Big)\\ &\qquad + \Big(|4_{z3}\rangle - |\mathrm{B}_{z3}\rangle\Big) + \Big(|8_{z3}\rangle - |7_{z3}\rangle\Big)\Big]\\ &= \frac{1}{\sqrt{2}}\Big(|3_{x3}\rangle - |\mathrm{C}_{x3}\rangle\Big),\end{aligned} \tag{42a}$$

$$\vdots \quad .$$

We also need the state

$$\begin{aligned}|\chi_{3,01}\rangle &= \frac{1}{\sqrt{2}}\Big(|0_{z3}\rangle - |\mathrm{F}_{z3}\rangle\Big)\\ &= \frac{1}{2\sqrt{2}}\Big[\Big(|1_{x3}\rangle + |\mathrm{E}_{x3}\rangle\Big) + \Big(|2_{x3}\rangle + |\mathrm{D}_{x3}\rangle\Big)\\ &\qquad + \Big(|4_{x3}\rangle + |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle + |7_{x3}\rangle\Big)\Big],\end{aligned} \tag{43}$$

mirrored in the same way, and finally,

$$\begin{aligned}|\phi_{3,11}\rangle &= \frac{1}{2\sqrt{2}}\Big[\Big(|1_{z3}\rangle - |\mathrm{E}_{z3}\rangle\Big) + \Big(|2_{z3}\rangle - |\mathrm{D}_{z3}\rangle\Big)\\ &\qquad + \Big(|4_{z3}\rangle - |\mathrm{B}_{z3}\rangle\Big) + \Big(|8_{z3}\rangle - |7_{z3}\rangle\Big)\Big]\\ &= \frac{1}{2\sqrt{2}}\Big[\Big(|1_{x3}\rangle - |\mathrm{E}_{x3}\rangle\Big) + \Big(|2_{x3}\rangle - |\mathrm{D}_{x3}\rangle\Big)\\ &\qquad + \Big(|4_{x3}\rangle - |\mathrm{B}_{x3}\rangle\Big) + \Big(|8_{x3}\rangle - |7_{x3}\rangle\Big)\Big].\end{aligned} \tag{44}$$

Each of these states show the same properties as the states that were used in Section V, given that Alice and Bob use the same settings, but show different behaviour when they use different settings. For example, if Eve sends $|\beta_{2,01}\beta_{3,01}\rangle$ and Alice and Bob both use the (b) setting (or Alice (a) and Bob (b)), the results will follow Table 4 because this state is tuned for zeros in this basis. If Alice and Bob both use the (c) setting (or Alice (a) and Bob (c)), the results will follow Table 5 because this state is tuned for ones in this basis. If they use different settings, the spin sum will differ at the two sites.

The statistics obtained from the state in Eq. (40) follows the behaviour of the original state exactly, as far as the spin sums are concerned, and Table 6 gives the key-transmission errors. The existence of this state shows that only checking the key bits, or indeed, checking statistical properties of the spin sums at the two sites at *any* combination of the two settings, will not provide any security.

Is the illusion perfect, then? Not at all. For example, if the spin sum is one of the extreme values at one site, e.g., a result of 0_{z2} or F_{z2}, there will be no occurrences of spin sum zero at the other site at the other setting, i.e., none of 3_{x3}, 5_{x3}, 6_{x3}, 9_{x3}, A_{x3}, and C_{x3} will occur. Simply put, this is because there is no possibility to make

$$\begin{aligned}|0_{z3}\rangle + |\mathrm{F}_{z3}\rangle &= c_1\Big(|3_{x3}\rangle + |\mathrm{C}_{x3}\rangle\Big)\\ &\quad + c_2\Big(|5_{x3}\rangle + |\mathrm{A}_{x3}\rangle\Big) + c_3\Big(|9_{x3}\rangle + |6_{x3}\rangle\Big)\end{aligned} \tag{45}$$

in fact,

$$\begin{aligned}|0_{z3}\rangle + |\mathrm{F}_{z3}\rangle &= \frac{1}{2}\Big[\Big(|0_{x3}\rangle + |\mathrm{F}_{x3}\rangle\Big) + \Big(|3_{x3}\rangle + |\mathrm{C}_{x3}\rangle\Big)\\ &\qquad + \Big(|5_{x3}\rangle + |\mathrm{A}_{x3}\rangle\Big) + \Big(|9_{x3}\rangle + |6_{x3}\rangle\Big)\Big].\end{aligned} \tag{46}$$

In other words, there is no possibility to combine the value 0 or F in one basis (and no spin sum zero results there) with *only* spin sum zero in the other. And this property of the quantum state space together with requirements (i)–(iv) makes it impossible for Eve to combine an extreme spin sum result at one site at one setting with a spin sum zero at the other site at the other setting.

Thus, Alice and Bob *absolutely must* augment their test for noise in the key with a

> Test to see whether the full local results at one setting is independent of the spin sum at the remote site at the other setting.

Testing independence of *the spin sums* at different settings is *not enough*. I would perhaps go so far as conjecturing that the protocol would be secure given the mentioned two tests (and a test that the local results occur with equal probability), but I would not really recommend using them as tests of security of the protocol. There are two reasons for this: they would provide a relatively weak statistical test, since the test cases occur quite rarely; but a more important reason is that the tests are complicated to motivate, and it would perhaps be difficult to convince a potential user that it ensures security, even if it may be possible to present a formal security proof. The lesson from this is instead that one needs to analyze *the full local data set* together with *information from the remote site*. Since this is necessary, one may as well choose a much simpler and more easily motivated security test that does respect this structure:

> Test the individual qubits at the two sites. That is, test whether the local results at one setting is the same as the remote results at the same setting.

This test would provide the kind of security intended in [15], and would fail if Eve uses the kind of source described above.

VII. CONCLUSIONS

The communication protocol proposed in [15] does clearly not use any specifically *quantum* properties of the quantum teleportation setup. In particular it does not need an entangled state since a separable state performs equally well. The system is using classical postselection of appropriate experimental runs to transfer the data. One could have hoped that the *quantum* properties of the quantum system of either Section I or II would enhance Bob's chance of distinguishing Alice's setting (a) from (b), but this is not the case, since the protocol shows the same performance using the purely classical system of Section III.

As to the quantum-cryptographic protocol of [15], the usage of several qubits to transmit a single key bit is problematic. Simply testing for noise in the sifted key is not sufficient in this quantum-cryptographic scheme, because Eve can use entanglement to her benefit, to eavesdrop without being noticed. In Section VI we noted that an additional test was needed; a test for independence of the remote spin sum with the full local result. But a simpler test was also suggested; to test whether the remote qubit results are identical to the local qubit results if the same setting is used at the two sites.

Of course, Eve will have a difficult time establishing the entangled mixed state needed for eavesdropping when Alice and Bob use the originally proposed test. But this is more a technological issue; the above reasoning is talking about the protocol as being (in)secure *in principle*, just as [15] is talking about the protocol as being usable *in principle*.

Since it is necessary to test the individual qubits to obtain a secure system, the protocol does seem wasteful because it only uses entanglement present in groups of $4N$ qubits for key transmission. Also, when Alice's raw key bit is 1, no entanglement at all is used, since the behaviour of the protocol in this situation is derived from the fact that Bob's results are statistically independent from Alice's. Many runs will also be discarded because Alice will send "OK" quite seldom, since criterion Q (see Section IV) will be fulfilled with probability only $\frac{6}{64}$.

In all, little of the available entanglement is put to good use, even when the qubits are individually tested, since the sifted key is derived from a joint result of several qubit measurements. Entanglement is a valuable resource, and should be used with care. In conlusion, while these protocols are theoretically interesting, they are probably not very useful in practice.

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[2] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).

[3] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[4] M. A. Nielsen, E. Knill, and R. Laflamme, Nature (London) **396**, 52 (1998).

[5] M. Koniorczyk, T. Kiss, and J. Janzky, J. Phys. A: Math. Gen. **34**, 6949 (2001).

[6] A. Peres, quant-ph/0304158.

[7] S. Popescu, Phys. Rev. Lett. **72**, 797 (1994).

[8] N. Gisin, Physics Letters A **210**, 157 (1996).

[9] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).

[10] M. Żukowski, Phys. Rev. A **62**, 032101 (2000).

[11] R. Clifton and D. Pope, Physics Letters A **292**, 1 (2001).

[12] C. H. Bennett and G. Brassard, in *Proc. of the IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[13] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[15] D. Home and M. A. B. Whitaker, Phys. Rev. A **67**, 022306 (2003).

[16] S. Aerts, P. Kwiat, J.-Å. Larsson, and M. Żukowski, Phys. Rev. Lett. **83**, 2872 (1999).

[17] In computer science a "nybble" is half a byte, or four bits. Four qubits would then constitute a qunybble.