Comments on "New Results on Frame-Proof Codes and Traceability Schemes"

Jacob Löfvenberg and Jan-Åke Larsson

Jacob Löfvenberg and Jan-Åke Larsson, Comments on "New Results on Frame-Proof Codes and Traceability Schemes" in IEEE TRANSACTIONS ON INFORMATION THEORY, 2010, (56), 11,5888-5889.
http://dx.doi.org/10.1109/TIT.2010.2070632

(or more precisely, the seed) is used in the Join protocol. As a result, there exists an adversary $\mathcal{A}$ that can easily win in the adversarial model (i.e., guess correctly the value of b). The adversary $\mathcal{A}$ works as follows:

1) The adversary $\mathcal{A}$ asks an `Execute` query to form a group $\mathcal{G}$ with group key $\mathtt{sk}_{\mathcal{G}}$.
2) $\mathcal{A}$ issues a `Test` query and obtains a response K which is either $\mathtt{sk}_{\mathcal{G}}$ or a random key.
3) $\mathcal{A}$ also issues a `Join` query to add a new user into the group $\mathcal{G}$, and obtains the communication transcript of the join protocol.
4) $\mathcal{A}$ then computes $\hat{x}_2' = H(K)$, $\hat{X}_2' = g^{\hat{x}_2'}$ and compares $\hat{X}_2'$ with $\hat{X}_2$ in the transcript of the join protocol. If they are equal, $\mathcal{A}$ returns 1, indicating that $K = \mathtt{sk}_{\mathcal{G}}$. Otherwise, $\mathcal{A}$ returns 0.

It is easy to see that with a overwhelming probability $H(K) \neq H(\mathtt{sk}_{\mathcal{G}})$ for a random K. Hence, the (*passive*) adversary $\mathcal{A}$ has a overwhelming probability to guess correctly the value of b and win the game. It is worth noting that the adversary even doesn't perform any `Reveal` or `Corrupt` queries.

5) Flaws in the Security Proof: Since the attack above can be simulated in the model, there must be some mistakes in the security proof of [2]. When carefully reading the proof, one can find that the security proof in [2] fails to analyze the winning probability of the adversary in some attacking scenarios, such as a join or leave query is performed to the test session.

6) Conclusion: In this letter, we revisited the Dutta-Barua dynamic group key agreement protocol [2] and showed a flaw inside the protocol. Different from the existing attacks against the protocol, our attack is based on adversarial model defined by Dutta and Barua in [2]. It would be an interesting task to design a more complete security model as well as a secure and practical protocol for group key agreement in the dynamic setting.

References

[1] R. Dutta and R. Barua, "Constant round dynamic group key agreement," in *Proc. ISC 2005*, 2005, vol. 3650, Lecture Notes in Computer Science, pp. 74–88.

[2] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," *IEEE Trans. Inform. Theory*, vol. 54, no. 5, pp. 2007–2025, May 2008.

[3] C. M. Teo Joseph, C. H. Tan, and J. M. Ng, "Security analysis of provably secure constant round dynamic group key agreement," *IEICE Trans.*, vol. E89-A, no. 11, pp. 3348–3350, Nov. 2006.

Comments on "New Results on Frame-Proof Codes and Traceability Schemes"

Jacob Löfvenberg and Jan-Åke Larsson

The paper "New Results on Frame-Proof Codes and Traceability Schemes" [1] claims to give results for two code classes, frame-proof codes and traceability schemes, in the form of lower bounds on the maximum code size, and explicit code constructions. We will here briefly review the four claims of [1], noting that the proofs and constructions presented in [1] fail, and that the claims also contradict previously published upper bounds [2], [3].

We apologize for being terse here; details can be found in our three-page paper [4] originally submitted in 2005. We have been asked by IEEE IT to keep this letter to only one page, but are grateful for this opportunity to voice our concerns about [1].

We use the same setting and notation as [1]: binary constant-weight codes of length l, weight w, minimum Hamming distance 2δ, and a number c of cooperating copy-distributing users. The binary entropy function is denoted $H(x)$, and logarithms are in base 2. We first consider [1, Theor. 6] that reads as follows.

Theorem 6: Let q be a prime power. Suppose there exists a c-frame-proof code with length $l \leq q$, constant weight w, and $c = l/w$. Then, for any $\sigma > 0$ and l satisfying

$$\frac{\log l}{l} < \sigma \quad \text{and} \quad l > \left(13 + \sqrt{13^2 + 48\sigma}\right)/12\sigma \qquad \text{[1]:6}$$

the maximum number of codewords n satisfies

$$n > \frac{1}{q^{\delta-1}} 2^{(H(\frac{1}{c})-\sigma)l}. \qquad \text{[1]:13}$$

There is no proof of [1, Theor. 6]; the chain of lemmas preceding Theorem 6 is (we believe) intended as a proof, but the implication in [1, Lemma 3] is needed in the reverse direction, and Lemma 3 is not an equivalence [4]. Also, Theorem 6 contradicts a previously published upper bound [2]

$$n \leq c\left(2^{\lceil \frac{l}{c} \rceil} - 1\right). \qquad (1)$$

To see this, let $q = 2^6$ and note that a 2-frame-proof code exists with $l = 64$, $w = 32$, and $\delta = 3$, see [4]. With $\sigma = 7/64$, the above inequalities read $n > 2^{-12} 2^{(1-7/64)64} = 2^{45}$ and $n \leq 2(2^{32} - 1)$, a clear contradiction.

Even if Theorem 6 does not hold, there is an explicit construction underlying [1, Theor. 10], also providing lower bounds for the number of codewords n:

Manuscript received March 05, 2010; revised May 17, 2010. Date of current version October 20, 2010.

J. Löfvenberg was with the Department of Electrical Engineering, Linköping University, SE-581 83 Linköping, Sweden. He is now with the FOI: Swedish Defence Research Agency, Division of Information Systems, SE-581 11 Linköping, Sweden (e-mail: jaclof@foi.se).

J.-Å. Larsson was with the Department of Mathematics, Linköping University, SE-581 83 Linköping, Sweden. He is now with the Department of Electrical Engineering, Linköping University, SE-581 83 Linköping, Sweden (e-mail: jan-ake.larsson@liu.se).

Communicated by R. Safavi-Naini, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2010.2070632

Theorem 10: For a given integer $c > 1$, there exists a c-frame-proof code with constant weight w and length $l = cw$, restricted by ([1]:6) with $\sigma = \frac{1}{2}\left(H\left(\frac{1}{c}\right) - \frac{1}{c}\right)$ and

$$\log l < \frac{1}{2} \cdot \frac{c^2}{c-1}\sigma \qquad [1]{:}20$$

that has $n > 2^{l/c}$ codewords.

Unfortunately, with the given parameter relations it is not possible to choose the parameters so that ([1]:20) is satisfied. Inserting l and σ into ([1]:20) we obtain

$$\log cw < \frac{1}{4} \cdot \frac{c^2}{c-1}\left(H\left(\frac{1}{c}\right) - \frac{1}{c}\right) \qquad (2)$$

and using the inequality $\ln x \leq x - 1$ it can be shown that this enforces weight $w < 1$, see [4]. Furthermore, even the underlying construction scheme fails, which can be verified with the same technique and some patience [4]. The construction used in [1] establishes two parameter regions, one where the c-frame-proof property holds and another that ensures a large number of codewords; the problem is that the intersection is empty, except for codes with weight $w = 1$. The constructed codes can *either* be made c-frame-proof *or* be given a number of codewords $n > 2^{l/c}$, but are *never* guaranteed *both* properties.

There are also two claims for c-traceability schemes in [1]. Theorem 7 claims a lower bound for the maximum number of codewords, but the intended proof of Theorem 7 needs the implication in Lemma 5 in in the reverse direction [4], and the claim violates another previously published upper bound [3]. Similarly as above, an explicit construction underlies Theorem 11 that claims existence of a c-traceability scheme with a large number of codewords. Also here, unless $w = 1$, the given parameter relations cannot be satisfied, and the construction scheme can either ensure c-traceability or a large number of codewords, never both [4].

References

[1] R. Safavi-Naini and Y. Wang, "New results on frame-proof codes and traceability schemes," *IEEE Trans. Inform. Theory*, vol. 47, no. 11, pp. 3029–3033, Nov. 2001.

[2] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1042–1049, Mar. 2001.

[3] D. R. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes," *SIAM J. Discrete Math.*, vol. 11, pp. 41–53, Feb. 1998.

[4] J.-Å. Larsson and J. Löfvenberg, Comment on "New Results on Frame-Proof Codes and Traceability Schemes" 2009 [Online]. Available: http://arxiv.org/abs/0912.1440