Des. Codes Cryptogr. (2011) 60:63–66
DOI 10.1007/s10623-010-9416-6

Comments on Harn–Lin's cheating detection scheme

Hossein Ghodosi

Received: 22 April 2010 / Revised: 21 June 2010 / Accepted: 22 June 2010 /
Published online: 3 July 2010

Abstract Detection of cheating and identification of cheaters in threshold schemes has been well studied, and several solid solutions have been provided in the literature. This paper analyses Harn and Lin's recent work on cheating detection and identification of cheaters in Shamir's threshold scheme. We will show that, in a broad area, Harn–Lin's scheme fails to detect cheating and even if the cheating is detected cannot identify the cheaters. In particular, in a typical Shamir (t, n)-threshold scheme, where $n = 2t - 1$ and up to $t - 1$ of participants are corrupted, their scheme neither can detect nor can identify the cheaters. Moreover, for moderate size of groups their proposed cheaters identification scheme is not practical.

Keywords Threshold secret sharing schemes · Cheating detection · Cheaters identification

Mathematics Subject Classification (2000) 0804

1 Introduction

Since the invention of threshold secret sharing scheme in 1979 [2,6], it has been studied extensively, and several new structures have been introduced. The essential idea of these schemes is to protect the secrecy of sensitive information by distributing them among *n participants* in such a way that every set of at least t participants must cooperate in order to determine the secret. Secret sharing schemes of this type are called (t, n)-threshold schemes.

Since polynomial interpolation is possible over every field, Shamir suggests an elegant solution for constructing a (t, n)-threshold scheme. Unfortunately, the recovery of the secret can be easily corrupted by a dishonest participant who pools a modified share (instead of

Communicated by P. Wild.

H. Ghodosi (✉)
School of Business and Information Technology,
James Cook University, Townsville, QLD 4811, Australia
e-mail: hossein.ghodosi@jcu.edu.au

the original). The secret recovered is obviously different from the original, but the dishonest participant can compute the original secret, leaving other honest participants with an invalid secret. This way of cheating was discussed by Tompa and Woll [7]. Since then, detection of cheating and identification of cheaters in threshold schemes has been well studied, and several solid solutions have been provided in the literature.

Recently, Harn and Lin [4] have studied cheating problem in threshold schemes. This paper analyses Harn and Lin's recent work on cheating detection and identification of cheaters in Shamir's threshold scheme. We will show that, in a broad area, Harn–Lin's scheme fails to detect cheating and even if the cheating is detected cannot identify the cheaters. In particular, in a typical Shamir (t, n)-threshold scheme, where $n = 2t - 1$, and up to $t - 1$ of participants are corrupted, their scheme neither can detect nor can identify the cheaters. Moreover, for moderate size of groups their proposed cheaters identification scheme is not practical.

2 A brief review of Harn–Lin's work

Harn and Lin's cheating detection algorithm is based on the fact that in a Shamir (t, n)-threshold scheme any subset of $j\,(t \le j \le n)$ genuine shares are consistent, i.e., if j honest shareholders participate in the secret reconstruction protocol, the interpolated polynomial will be of degree at most $t - 1$. Thus, if the interpolated polynomial is of degree larger than $t - 1$, there exist cheaters in the system. They have proposed the following algorithms:

Algorithm 1 (Cheater Detection):

1. Compute an interpolated polynomial $f(x)$ of j points, where $(t < j \le n)$.
2. If $degree(f(x)) \le (t - 1)$, then there is no cheater, and the secret is $f(0)$. Otherwise there are cheaters in the system.

Algorithm 2 (Cheater Identification):

This algorithm is a bit lengthy (i.e., it has seven steps), and its running time is $O(j!)$. Since its description is not relevant to our discussion, we will not describe it here.

3 Analysis of Harn–Lin's work

3.1 Cheaters' attacks

Harn and Lin describe three types of cheaters' attacks.

1. *Type 1 attack*—Either honest shareholders accidentally contribute with wrong shares or dishonest shareholders contribute with random values (i.e., no strategy).
2. *Type 2 attack*—Assume that all shareholders release their shares synchronously (i.e., all shares must be revealed simultaneously). Under this assumption, only when the number of cheaters is larger than or equal to the threshold parameter t, the cheaters can implement a successful attack to fool honest shareholders.
3. *Type 3 attack*—Assume that shareholders release their shares one at a time. The optimum choice for cheaters is to release their shares after all honest shareholders releasing their shares. Thus, the cheaters can modify their shares based on the released shares.

4 Analysis of Harn–Lin's work

In democratic societies, a commonly accepted policy is that a majority rules. This is why Shamir suggests: by using a (t, n)-threshold scheme with $n = 2t - 1$ we get a very robust scheme. A silent assumption behind this model is that up to $t - 1$ shareholders may be corrupted. This model, which we refer to as a *typical Shamir (t, n)-threshold scheme*, has been extensively studied in the literature (see, e.g., [5]).

In the following we will show that, in a typical Shamir (t, n)-threshold scheme, Harn–Lin's scheme neither can detect nor can identify the cheaters. Moreover, for moderate size of groups their proposed cheaters identification algorithm is not practical.

4.1 A wise cheating attack

Consider a typical Shamir scheme and let $\{P_{i1}, \ldots, P_{iq}\}$ be the group of q cheaters ($q \geq 1$). No matter whether the secret reconstruction protocol is *synchronous* or *asynchronous* (i.e., type 2 or type 3 attack), the cheaters generate a random $t - 1$ degree polynomial $g(x)$, such that for all honest shareholders, P_i, participating in the secret reconstruction protocol, it satisfies $g(i) = 0$. Then cheaters compute $g(i1), \ldots, g(iq)$ for all cheaters in the protocol. The honest shareholders contribute with their genuine shares, while each cheater contributes with their modified share, which is the sum of their genuine share and their share from $g(x)$ polynomial. The idea behind this attack is that, honest participants have, indeed, added their shares from the $g(x)$ polynomial to their genuine shares—their share from $g(x)$ are zero. Hence, due to *(+, +)-homomorphism* property [1] of Shamir's threshold scheme, the shares submitted by participants are associated with $h(x)$ polynomial, where $h(x) = f(x) + g(x)$. Therefore, after obtaining the modified secret, $h(0)$, the cheaters easily compute the correct secret $f(0)$, since they know $f(0) = h(0) - g(0)$, but the honest shareholders learn a wrong secret.

This attack clearly shows that, in Harn–Lin's work, the requirement of having at least t cheaters, in order to perform type 2 attack, is not correct. Note that as long as the number of honest participants in the secret reconstruction protocol is smaller than the threshold parameter (no matter how many cheaters exist in the protocol), the attack is always successful.

4.2 Comments on cheating detection

Let us recall the wise attack of previous section, where the secret reconstruction protocol is performed in the presence of $H < t$ honest shareholders and $C < t$ cheaters, such that $j = (H + C)$, and $j > t$. Obviously, Algorithm 1 (i.e., the cheater detection algorithm of Harn–Lin's scheme) accepts the shares, since the resulting polynomial $h(x) = f(x) + g(x)$ is of degree at most $t - 1$. That is, the algorithm cannot detect the cheating.

It is worth mentioning that, in the secret reconstruction algorithm, although a set of inconsistent shares indicates there is a cheating, a set of consistent shares does not guarantee that there is no cheating. That is, Algorithm 1 always fails to detect successful cheating (i.e., where the shares are consistent). In order to amend Harn–Lin's work, we suggest replacing Theorems 1, 2, and 3 of Harn–Lin's work with the following theorem, which is independent from the type of attack.

Theorem 1 *If (j-C) > (t–1), Algorithm 1 always detects cheating.*

4.3 Comments on identification of cheaters

We have three comments on cheater identification algorithm of Harn–Lin's scheme.

1. Since Algorithm 1 fails to properly detect cheating, Algorithm 2 cannot identify cheaters. That is, Algorithm 2 at most can identify the cheaters when the submitted shares to secret reconstruction protocol are not consistent.
2. Even if the cheating is detected, cheater identification is not guaranteed. This is because, Harn–Lin's cheater identification algorithm accepts shares as genuine, if they have majority in generating the same secret. This mechanism works if $H > (C + t - 1)$—see Harn–Lin's work. Thus, in a (t, n)-threshold scheme, if up to $t - 1$ participants are corrupted, the number of honest shareholders must be larger than $2(t - 1)$, which implies $n > 3(t-1)$. That is, in a (t, n)-threshold schemes, if $n \leq 3(t-1)$, always $t-1$ participants can prevent the secret reconstruction. This is because the algorithm cannot identify the cheaters, although it detects cheating. In particular, Harn–Lin's cheater identification algorithm cannot identify cheaters in a typical Shamir scheme.
3. The running time of Algorithm 2 is $O(j!)$. Although it can be executed for small values of j, for groups of moderate size it is totally impractical. For example, if $t = 6$, the cheaters identification protocol implies $j \geq 16$, and thus Algorithm 2 requires 16! runs of Shamir's secret reconstruction protocol. Since $lg(n!) = \theta(nlgn)$ [3], we will have $lg(16!) = 16lg(16) = 64$. That is, it requires 2^{64} runs of Shamir's secret reconstruction protocol, which is not practical.

References

1. Benaloh J.: Secret sharing homomorphisms: keeping shares of a secret secret. In: Odlyzko A. (ed.) Advances in Cryptology—Proceedings of CRYPTO'86. Lecture Notes in Computer Science, vol. 263, pp. 251–260. Springer-Verlag, Heidleberg (1987).
2. Blakley G.: Safeguarding cryptographic keys. In: Proceedings of AFIPS 1979 National Computer Conference, vol. 48, pp. 313–317 (1979).
3. Cormen T., Leiserson C.E., Rivest R., Stein C.: Introduction to Algorithms, Second edn. MIT Press, USA (2001).
4. Harn L., Lin C.: Detection and identification of cheaters in (t, n) secret sharing scheme. In: Designs, Codes and Cryptography, vol. 52, pp. 15–24 (2009).
5. Rabin T.: Robust sharing of secrets when the dealer is honest or cheating. J. ACM **41**(6), 1089–1109 (1994).
6. Shamir A.: How to share a secret. Commun. ACM **22**, 612–613 (November) (1979).
7. Tompa M., Woll H.: How to share a secret with cheaters. J. Cryptol. **1**(2), 133–138 (1988).