Journal of Information Hiding and Multimedia Signal Processing ©2009 ISSN 2073-4212
Ubiquitous International Volume **?**, Number **0?**, ?? **2013**

The Generalization of Harn-Lin's Scheme on Cheater Detection and Identification

Lein Harn

Department of Computer Science Electrical Engineering
University of Missouri-Kansas City
MO 64110-2499, USA
harnl@umkc.edu

Changlu Lin

Key Laboratory of Network Security and Cryptology
Fujian Normal University
Fujian, 350007, P.R.China
cllin@fjnu.edu.cn

Abstract. *Cheater detection and identification are important issues in the process of secret reconstruction. Most algorithms to detect and identify cheaters need the dealer to generate and distribute additional information to shareholders. In a recent paper, algorithms have been proposed to detect and identify cheaters based on shares only without needing any additional information. However, more than t (i.e. the threshold) shares are needed in the secret reconstruction. In this paper, we extend the algorithms to the situation when there are exact t shares in the secret reconstruction. We adopt the threshold changeable secret sharing which shareholders work together to change the threshold t into a new threshold t' (i.e., $t' < t$) and generate new shares of a (t', n) secret sharing; while at the same time, maintain the original secret. Since $t' < t$, there are redundant shares. We also include discussion on how to select the new threshold t' in order to detect and identify cheaters successfully.*

Keywords: Secret sharing; threshold changeable secret sharing; verifiable secret sharing; cheaters; redundant share.

1. Introduction.

In a (t, n) secret sharing scheme, a dealer divides the secret into shares in such a way that any t (i.e., the threshold) or more than t shares can reconstruct the secret; while any fewer than t shares cannot obtain any information about the secret. Shamir's (t, n) secret sharing scheme [16] is based on the linear polynomial. Secret reconstruction uses Lagrange interpolating polynomial.

When shareholders present their shares in the secret reconstruction, dishonest shareholders (i.e. cheaters) can always exclusively derive the secret by presenting fake shares and thus the other honest shareholders get nothing but a fake secret. It is easy to see that Shamir's (t, n) secret sharing scheme does not prevent dishonest shareholders in the secret reconstruction. Cheater detection and identification are important features in order to provide fair reconstruction of a secret.

There are many research papers in the literature to propose algorithms for cheater detection and identification. Most of these algorithms [17, 4, 15, 6, 5, 11, 9, 14, 13, 1] assume that there are exact t shareholders participated in the secret reconstruction. The dealer needs to provide additional information to enable shareholders to detect and identify cheaters. Some algorithms [12, 3] use error-correcting codes to detect and identify fake shares.

In a recent paper, Harn and Lin [7] proposed a new approach to detect and identify cheaters. The algorithm uses shares to detect and identify cheaters. When there are more than t (i.e., the threshold) shares in the secret reconstruction, the redundant shares can be used to detect and identify cheaters. In this approach, shares in a secret sharing scheme serve for two purposes; that are, (a) reconstructing the secret and (b) detecting and identifying cheaters. Since Harn and Lin's algorithm requires more than t shares in the secret reconstruction, the algorithm does not work if there are exact t shares. In this paper, we generalize Harn and Lin's algorithm to the situation when thee are exact t shares in the (t, n) secret reconstruction. We adopt the threshold changeable secret sharing (TCSS) which shareholders work together to change the threshold t into a new threshold t' and generate new shares of a (t', n) secret sharing; while at the same time, maintain the original secret. Since $t' < t$, there are redundant shares. The new shares can be verified without revealing the secret and new shares. We also include discussion on how to select the new threshold t' in cheater detection and identification.

The rest of this paper is organized as follows. In the next section, we briefly review Shamir's (t, n) secret sharing scheme [16] and Harn and Lin's algorithm [7]. In Section 3, we propose our generalized scheme. Section 4 presents the verifiable to support the proposed scheme. We conclude in Section 5.

2. Preliminaries.

2.1. Review of Shamir's secret sharing scheme [16].

In Shamir's (t, n) secret sharing scheme based on the polynomial, there are n shareholders and a mutually trusted dealer. The scheme consists of two algorithms:

Scheme 1: Shamir's (t, n) secret sharing scheme

1. Share generation algorithm: the dealer first picks a random polynomial of degree $t-1$, $f_i(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + a_0 \pmod p$, such that the secret s satisfies $f(0) = a_0 = s$ and all coefficients, $a_0, a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$, p is a prime with $p > s$. The dealer computes shares as, $f(x_i)$, for $i = 1, 2, \ldots, n$, and distributes each share $f(x_i)$ to shareholder U_i secretly.
2. Secret reconstruction algorithm: it takes any t or more than t shares, for example, with following t shares, $\{(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_t, f(x_t))\}$, as inputs, and outputs the secret s using the Lagrange interpolating formula as

$$s = \sum_{i=1}^{t} f(x_i) \prod_{r=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j} \pmod p.$$

We note that the above algorithms satisfy the basic requirements of the secret sharing scheme, that are, (1) with the knowledge of any t or more than t shares, shareholders can reconstruct the secret s; and (2) with the knowledge of any $t-1$ or fewer than $t-1$ shares, shareholders cannot obtain the secret s. Shamir's secret sharing scheme is unconditionally secure since the scheme satisfies these two requirements without making any computational assumption. For more information on this scheme, please refer to the original paper [16].

2.2. **Review of Harn and Lin's algorithm** [7]**.** We briefly review the algorithm [7] to detect and identify cheaters using the property of strong t-consistency and majority voting mechanism. The algorithm assumes that there are more than t shareholders participated in the secret reconstruction.

Benaloh [2] presented a notion of t-consistency to determine whether a set of n (i.e., $n > t$) shares are generated from a polynomial of degree $t - 1$ at most. Recently, Harn and Lin [8] proposed a new definition of strong t-consistency which is the extension of Benaloh's definition.

Definition 2.1 (Strong t-consistency [8])**.** *A set of n shares (i.e., $t < n$) is said to be strong t-consistent if (a) any subset of t or more than t shares can reconstruct the same secret, and (b) any subset of fewer than t shares cannot reconstruct the same secret.* □

It is obvious that if shares in Shamir's (t, n) secret sharing scheme are generated by a polynomial with degree $t - 1$ exactly, then shares are strong t-consistent. Checking strong t-consistency of n shares can be executed very efficiently by using the Lagrange interpolating formula. In fact, to check whether n shares are strong t-consistent or not, it only needs to check whether the interpolation of n shares yields a polynomial with degree $t - 1$ exactly. If this condition is satisfied, we can conclude that all shares are strong t-consistent. However, if there are some invalid shares, the degree of the interpolating polynomial of these n shares is more than $t - 1$ with very high probability. In other words, these n shares are most likely to be not strong t-consistent.

- Method for Detecting Cheaters: If there are more than t shares in Shamir's (t, n) secret sharing scheme and all shares are valid, all shares must be strong t-consistent. Cheater detection is determined by checking the property of strong t-consistency of all shares.
- Method for Identifying Cheaters: If there are n (i.e., $n > t$, the threshold) shares in the secret reconstruction and there have some invalid shares, the reconstructed secrets must be inconsistent. This is because any t shares can construct a secret and there are $\binom{n}{t}$ different combinations. Any t shares including some invalid shares is very likely to reconstruct a different secret from the true secret reconstruct based on all valid shares. After cheaters being detected, if the true secret is the majority of reconstructed secrets, we can use the majority voting mechanism to identify fake shares. The cheater identification method needs to figure out the majority of the reconstructed secrets first. A set, A, consisting of t valid shares is identified. Then, cheaters (i.e., having fake shares) can be identified one at a time by computing the reconstructed secret using shares in A and the testing share.

The primary advantage of Harn and Lin's algorithm is its simplicity. Shamir's (t, n) secret sharing scheme is capable to detect and identify cheaters without any modification. In [7], it also investigates the bounds of detection and identification which are functions of the threshold, the number of cheaters, and the number of redundant shares in the secret reconstruction. Interest readers can refer to the original paper.

Remark 2.1. *As pointed out in* [7]*, the computational complexity of method to detect cheaters is $O(1)$ and the complexity to identify cheaters is $O(j!)$, where j is the number of shares in the secret reconstruction. The method of cheater identification only works properly when there is small number of shares in the secret reconstruction.*

3. **Proposed algorithm.**

From now on, we assume that there are t, where $t \leq n$, shareholders with their shares $\{(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_t, f(x_t))\}$, obtained from a trusted dealer in Shamir's (t, n) secret sharing scheme want to reconstruct the secret.

The basic idea of our approach is to adopt the threshold changeable secret sharing (TCSS) which shareholders work together to change the threshold t into a new threshold t' and generate new shares of a (t', n) secret sharing; while at the same time, maintain the original secret. Since $t' < t$, there has enough redundant shares in the secret reconstruction to detect and identify cheaters; while at the same time, keep the same secret. The new shares of the (t', t') secret sharing scheme are generated and are used to reconstruct the secret. In our proposed algorithm, each shareholder M_i acts like a dealer to select a random $(t' - 1)$-th degree polynomial $f_i(x)$ with the constant term $f_i(0) = f(x_i) \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j}$ (mod p). Then, each shareholder M_i computes sub-shares $f_i(x)$ for other shareholders. After receiving all shares from other shareholders, each shareholder releases the sum of all sub-shares which is the share of sum of polynomials as $F(x) = \sum_{r=1}^{t} f_r(x) \pmod p$. The interpolation of all released sums can construct the polynomial $F(x)$ with constant term $F(0) = s$. The TCSS scheme in this algorithm is similar to the strong (n, t, n) verifiable secret sharing scheme proposed in [8]. However, in current application, there are t shareholders working together to change the threshold t into a new threshold t' and generate new shares. Thus, it is a (t, t', t) verifiable secret sharing scheme. In addition, these new shares can be verified without revealing the secret and new shares. We will give detail discussions in Section 4.

3.1. **Secret reconstruction algorithm.** We describe the secret reconstruction algorithm as following steps.

Algorithm: Secret reconstruction algorithm

Step 1.: For each shareholder M_i, uses his share $f(x_i)$ obtained from the dealer to compute $y_i' = f(x_i) \prod_{j=1, j\neq i}^{t} \frac{-x_i}{x_i - x_j}$ (mod p) and selects a random polynomial $f_i(x)$ with $(t' - 1)$-th degree satisfying $f_i(0) = y_i'$. Then, shareholder M_i computes sub-shares, $f_i(x_j)$, for all other shareholders, M_j, for $j = 1, 2, \ldots, t$, $j \neq i$, and sends each sub-share $f_i(x_j)$ to shareholder M_j secretly. Shareholder M_i computes and keeps a self-generated sub-share $f_i(x_i)$. By the end of this step, every shareholder receives $t - 1$ sub-shares from other shareholders.

Step 2.: For each shareholder M_i, after receiving all sub-shares, $f_r(x_i)$, for $r = 1, 2, \ldots, t$, computes

$$z_i = \sum_{j=1}^{t} f_j(x_i) \pmod p.$$

z_i is the new share. In Theorem 1, we will prove that the threshold of z_i, for $i = 1, 2, \ldots, j$, is t'. z_i is t'. In Section 4, we will describe complete procedures to verify these new shares.

Step 3.: With knowledge of z_i, for $i = 1, 2, \ldots, t$, shareholders can follow Harn and Lin's algorithm [7] to detect and identify cheaters. If there is no cheater, the secret s can be computed following Lagrange interpolating formula.

Theorem 3.1. *If shareholders act honestly and present valid shares in above algorithm, the threshold of z_i is t', and the secret s can be recovered successfully following Lagrange interpolating formula.*

Proof. If shareholders act honestly in the algorithm, each new share z_i is the additive sum of sub-shares of random polynomials $f_i(x)$, for $i = 1, 2, \ldots, t$, selected by shareholders.

According to the property of secret sharing homomorphisms, z_i is the share of polynomial $F(x) = \sum_{r=1}^{t} f_r(x) \pmod{p}$. It is obvious that the degree of polynomial $F(x)$ is $t' - 1$. Thus, the threshold of z_i, for $i = 1, 2, \ldots, t$, is t'. In addition, if each shareholder owns a valid share in Step 1, the random polynomial $f_i(x)$ selected by shareholder M_i satisfies $f_i(0) = y'_i = f(x_i) \prod_{j=1, j\neq i}^{i} \frac{-x_i}{x_i - x_j} \pmod{p}$. Knowing z_i, for $i = 1, 2, \ldots, t$, the secret s can be recovered since the polynomial $F(x)$ satisfies $F(0) = \sum_{i=1}^{t} f_j(0) \pmod{p} = \sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{-x_i}{x_i - x_j} \pmod{p} = s$. However, if there are some invalid shares, the secret s cannot be computed from the released new shares. □

Remark 3.1. *Since the threshold of the new shares z_i is t', there are $t - t'$ redundant shares in above algorithm. In the following, we will discuss how to choose the new threshold t' in order to detect and identify cheaters in our proposed secret reconstruction algorithm.*

3.2. **Selecting t' in Our Design.** Harn and Lin [7] have classified three types of attack according to the behavior of attackers; that are, (a) Type 1 attack - attackers present fake shares without any collaboration; (b) Type 2 attack - shares are released synchronously and colluded attackers modify their shares to fool honest shareholders; and (c) Type 3 attack - shares are released asynchronously and colluded attackers modify their shares to fool honest shareholders. The bounds of detection and identification of cheaters are functions of the threshold, the number of cheaters, and the number of shares in the secret reconstruction. In a recent paper, Ghosting [10] has proposed a *wise cheating attack* on the cheater detection method based on the property of strong t-consistency. New bounds of detection of cheaters can be found. In the following, we list the bounds of detection and identification of cheaters incorporating the attack proposed by Ghosting [10].

Theorem 3.2. *Under Type 1 attack, Harn-Lin's scheme can successfully detect cheaters if $j \geq t + 1$, and identify cheaters if $j - c > t$, where j is the number of shares, t is the threshold and c is the number of cheaters in the secret reconstruction.*

Theorem 3.3. *Under Type 2 attack, Harn-Lin's scheme can successfully detect cheaters if $j - c \geq t$, and identify cheaters if $\{(c < t) \cap (j - c \geq t + 1)\} \cup \{(c \geq t) \cap (j - c > c + t - 1)\}$, where j is the number of shares, t is the threshold and c is the number of cheaters in the secret reconstruction.*

Theorem 3.4. *Under Type 3 attack, Harn-Lin's scheme can successfully detect cheaters if $j - c \geq t$, and identify cheaters if $\{j \geq t + 1\} \cap \{j - c > c + t - 1\}$, where j is the number of shares, t is the threshold and c is the number of cheaters in the secret reconstruction.*

In this paper, we consider the situation when there are exact t shares in the secret reconstruction. In order to create redundant shares to detect and identify cheaters, the proposed secret reconstruction algorithm enables shareholders to work together to change the threshold from its original value t to a new value t' such that there are $t - t'$ redundant shares in the secret reconstruction. New shares of the (t', t') secret sharing scheme are generated and are used in the secret reconstruction.

Let us re-evaluate the upper and lower bounds in terms of the new threshold t'. In above theorems, the symbols, j is the number of participated shares, t is the threshold, and c is the number of cheaters in the secret reconstruction. In our proposed algorithm, the number of participated shares is t and the threshold is t'. From Theorems 3.2, 3.3 and 3.4, we can obtain the following results: (1) Under Type 1 attack, the proposed algorithm can successfully detect cheaters if $t' \leq t - 1$, and identify cheaters if $t' \leq t - c - 1$; (2) Under Type 2 attack, the proposed algorithm can successfully detect cheaters if $t' \leq t - c$, and identify cheaters if $\{c + 1 \leq t' \leq t - c - 1\} \cup \{t' \leq \min\{c, t - 2c\}\}$; (3) Under Type 3 attack, the proposed algorithm can successfully detect cheaters if $t' \leq t - c$, and identify cheaters if $t' \leq \min\{t-1, t-2c\}$. We summarize this result in Table 1.

TABLE 1. Bounds of the threshold t' when t and c are given.

	Detectability	Identifiability
Type 1	$t' \leq t-1$	$t' \leq t-c-1$
Type 2	$t' \leq t-c$	$\{c+1 \leq t' \leq t-c-1\} \cup \{t' \leq \min\{t-1, t-2c\}\}$
Type 3	$t' \leq t-c$	$t' \leq \min\{t-1, t-2c\}$

We use the following example to explain how to choose the new threshold t' in our proposed algorithm to meet the requirements of cheater detection and identification. Assume that in Shamir's $(7, 15)$ secret sharing scheme, our proposed secret reconstruction algorithm needs to detect and identify at most two cheaters. From Table 1, we can compute the maximal values of the new threshold t'. We list the threshold values in Table 2.

TABLE 2. Maximum values of t' for $t = 7, n = 15$ and $c = 2$.

	$t'_{\max}$for detectability	$t'_{\max}$for identifiability
Type 1	6	4
Type 2	5	4
Type 3	5	3

4. **Verifiable Secret Sharing (VSS) Scheme.** After shares being refreshed, all shareholders need to work together to verify that the refreshing process is performed by legitimate shareholders and all new shares are consistent (i.e., any t' or more than t' new shares can recover the secret). In a conventional VSS, shareholders are able to verify that their shares are consistent without revealing their shares or the secret. In this paper, we propose a VSS which can also authenticate the refreshing process. Our proposed VSS is based on the VSS model proposed by Benaloh [2] in which all shareholders work together to verify their new shares. Only after new shares being successfully verified, shareholders upload their new shares to replace old shares.

Scheme 2: Verifiable secret sharing scheme

Step 1.: For each shareholder U_i, for $i = 1, \ldots, t$, acts as a verifier to use his new share z_i and old share $f(x_i)$ to compute $v_i = z_i - f(x_i) \pmod q$.

Step 2.: Each shareholder U_i, for $i = 1, \ldots, t$, who acts as a verifier, randomly select to randomly select a polynomial $g_i(x)$ with $(t'-1)$ exact degree, and then U_i computes sub-shares $u_{ij} = g_i(x_j)$ and sends u_{ij} to the shareholder U_j, for $j = 1, \ldots, t$.

Step 3.: After receiving all information u_{ji} from other shareholders, U_i computes $u_i = \prod_{l=1}^{t} u_{ji}$ and $w_i = z_i + u_i$, for $i = 1, \ldots, t$, and then v_i and w_i are made publicly known.

Step 4.: From the released values, $\{v_i \text{ and } w_i \mid i = 1, 2, \ldots, t\}$, each shareholder can construct the interpolating polynomial $V(x)$ and $W(x) = F(x) + G(x)$, where $G(x) = \prod_{i=1}^{t} g_i(x)$. If $V(0) = 0$, the degree of $V(x)$ and $W(x)$ are $t'-1$ exact, then the refreshing process is authenticated and all new shares have been verified successfully, that are, the refreshing process is performed by all legitimate shareholders and new shares are generated by a polynomial with degree $t' - 1$ exact. Thus, new shares can be uploaded to replace the old shares. However, if the verification fails, it needs to restart a new refreshing process.

Theorem 4.1. *If $V(0) = 0$ and the degree of $V(x)$ and $W(x)$ is $t' - 1$, the refreshing process is authenticated and all new shares are generated by a $(t'-1)$-th degree polynomial.*

Proof. If the refreshing process is performed by legitimate shareholders and all shareholders (also verifiers) act honestly, the Lagrange interpolating polynomial of these t released values, v_i, for $i = 1, 2, \ldots, t$, is $V(x) = F(x) - f(x)$, where the polynomial $F(x) = \sum_{r=1}^{t} f_r(x) \pmod p$ of degree $t' - 1$ with $F(0) = s$ is defined in Theorem 3.1 and the polynomial $f(x)$ of degree $t' - 1$ with $f(0) = s$ is selected by the dealer. Thus, we have $V(0) = 0$ and the degree of the polynomial $V(x) = F(x) - f(x)$ is $t' - 1$ exact. Furthermore, if they check the degree of $W(x)$ is $t' - 1$ exact, since each verifier contributes a sub-polynomial with degree $t' - 1$ exact, so the degree of $F(x)$ is at most $t' - 1$. However, each verifier also contributes one sub-polynomial in $F(x)$ in refreshing new shares, the degree of $F(x)$ must be also $t' - 1$ exact. In a word, the refreshing process is authenticated since $V(0) = 0$ and the degree of the polynomial $V(x)$ is $t' - 1$ exact, and all new shares are generated by a $(t' - 1)$-th degree polynomial of $F(x)$. □

5. **Conclusion.** We propose a generalized cheater detection and identification algorithm for Shamir's (t, n) secret sharing scheme. Our scheme allows shareholders to detect and identify cheaters using their shares only without needing any additional information. When t shareholders need to reconstruct the secret, shareholders work together to change the threshold to a new threshold so redundant shares can be used to detect and identify cheaters. New shares are generated and used in the secret reconstruction. We include discussion on how to choose the new threshold to meet the requirements of cheater detection and identification.

Acknowledgment. This research is supported by the National Natural Science Foundation of China under Grant No. 61103247/61102093 and the Natural Science Foundation of Fujian Province under Grant No. 2011J05147.

REFERENCES

[1] T. Araki, Efficient (k, n) threshold secret sharing schemes secure against cheating from $n-1$ cheaters, in: Proceedings of ACISP'07, LNCS **4586**, pp. 13–142. Springer-Verlag (2007).

[2] J. C. Benaloh, Secret sharing homomorphisms: keeping shares of a secret secret, in: Proceedings of CRYPTO '86, LNCS **263**, pp. 251–260, Springer-Verlag (1987).

[3] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, Secret sharing schemes with veto capabilities, in: Proceedings of the First French-Israeli Workshop on Algebraic Coding, LNCS **781**, pp. 82–89. Springer-Verlag (1993).

[4] E. F. Brickell, and D. R. Stinson, The detection of cheaters in threshold schemes, in: Proceedings of Crypto'88, LNCS **403**, pp. 564–577. Springer-Verlag (1990).

[5] M. Carpentieri, A perfect threshold secret sharing scheme to identify cheaters, Designs, Codes and Cryptography **5**(3): 183–187 (1995).

[6] M. Carpentieri, A. De Santis, and U. Vaccaro, Size of shares and probability of cheating in threshold schemes. In: Proceedings of Eurocrypt'93, LNCS **765**, pp. 118–125. Springer-Verlag (1994).

[7] L. Harn, and C. Lin, Detection and identification of cheaters in (t, n) secret sharing scheme, Designs, Codes and Cryptography **52**(1): 15–24 (2009).

[8] L. Harn, and C. Lin, Strong (n, t, n) verifiable secret sharing scheme, Information Sciences, **180** (16): 3059–3064, (2010).

[9] J. He, and E. Dawson, Shared secret reconstruction, Designs, Codes and Cryptography **14**(3): 221–237 (1998).

[10] H. Ghosting, Comments on Harn-Lin's cheating detection scheme, Designs, Codes and Cryptography, **60**(1): 63–66 (2011).

[11] K. Kurosawa, S. Obana, and W. Ogata, t-cheater identifiable (k, n) secret sharing schemes, in: Proceedings of CRYPTO'95, LNCS **963**, pp. 410–423. Springer-Verlag (1995).

[12] R. J. McEliece, and D. V. Sarwate, On sharing secrets and Reed-Solomon codes, Communications of the ACM **24**(9): 583–584 (1981).

[13] W. Ogata, K. Kurosawa, D.R. Stinson, Optimum secret sharing scheme secure against cheating, SIAM Journal on Discrete Mathematics **20**(1), 79–95 (2006).

[14] J. Pieprzyk, and X. M. Zhang, Cheating prevention in linear secret sharing, in: Proceedings of ACISP'02, LNCS **2384**, pp. 121–135. Springer-Verlag (2002).

[15] T. Rabin, and M. Ben-Or, Verifiable secret sharing and multiparty protocols with honest majority, in: Proceedings of the 21st Annual ACM Symposium on the Theory of Computing, pp. 73–85 (1989).

[16] A. Shamir, How to share a secret, Communications of the ACM **22**(11): 612–613 (1979).

[17] M. Tompa, and H. Woll, How to share a secret with cheaters, Journal of Cryptology **1**(3): 133–138 (1989).