Information Sciences 180 (2010) 3059–3064

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Strong (n,t,n) verifiable secret sharing scheme

Lein Harn [a], Changlu Lin [b,*]

[a] Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, MO 64110, USA
[b] Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fujian 350007, PR China

ARTICLE INFO

Article history:
Received 15 December 2009
Received in revised form 14 April 2010
Accepted 17 April 2010

Keywords:
Secret sharing
Multiple dealers
t-Consistency
Verifiable secret sharing

ABSTRACT

A (t,n) secret sharing divides a secret into n shares in such a way that any t or more than t shares can reconstruct the secret; but fewer than t shares cannot reconstruct the secret. In this paper, we extend the idea of a (t,n) secret sharing scheme and give a formal definition on the (n,t,n) secret sharing scheme based on Pedersen's (t,n) secret sharing scheme. We will show that the (t,n) verifiable secret sharing (VSS) scheme proposed by Benaloh can only ensure that all shares are t-consistent (i.e. any subset of t shares defines the same secret); but shares may not satisfy the security requirements of a (t,n) secret sharing scheme. Then, we introduce new notions of *strong t*-consistency and *strong* VSS. A strong VSS can ensure that (a) all shares are t-consistent, and (b) all shares satisfy the security requirements of a secret sharing scheme. We propose a strong (n,t,n) VSS based on Benaloh's VSS. We also prove that our proposed (n,t,n) VSS satisfies the definition of a strong VSS.

© 2010 Elsevier Inc. All rights reserved.

1. Introduction

Secret sharing schemes were introduced by both Blakley [2] and Shamir [20] independently in 1979 as a solution for safeguarding cryptographic keys. Secret sharing schemes have been studied extensively in the literature. In a secret sharing scheme, a secret s is divided into n *shares* by a *dealer* and shared among n shareholders in such a way that any t or more than t shares can reconstruct this secret; but fewer than t shares cannot reconstruct the secret s. Such a scheme is called a (t,n) secret sharing, denoted it as (t,n) SS.

Shamir's (t,n) SS is based on the interpolating polynomial and is information-theoretically secure. In general, we assume that the dealer who divides the secret and distributes shares to shareholders without making any mistake. Any shareholder must unconditionally trust that the received share is valid. In 1985, Chor et al. [6] extended the notion of the original secret sharing and presented a notion of *verifiable secret sharing* (VSS). The property of verifiability means that shareholders are able to verify that their shares are consistent. VSS [1,9] is a fundamental tool for many researches in cryptography, such as secure multi-party computation [7,16,12] and Byzantine agreement [4]. There are papers to address the optimal round complexity of VSS [14,10,17], to propose multi-secrets VSS [5,21,8], and to use VSS and the Byzantine agreement protocol against the mobile adversary attack [3,22,19].

In 1990, Ingemarsson and Simmons [13] considered the secret sharing without the assistance of a mutually trusted third party. The basic idea of their proposed (t,n) SS is that there are n dealers (shareholders) who want to generate and share a master secret s jointly for some special applications. Each shareholder P_i first selects a random secret s_i and the master secret s is determined by $s=\sum_{i=1}^{n}s_i=s_1+\cdots+s_n$. Each shareholder shares his selected secret s_i with other shareholders using Shamir's $(t,n-1)$ SS. Thus, any shareholder has received $n-1$ shares from other shareholders. Any subset of t shareholders

[*] Corresponding author. Tel.: +86 1528 010 2192; fax: +86 591 83465174 0.
E-mail addresses: harnl@umkc.edu (L. Harn), cllin@fjnu.edu.cn (C. Lin).

0020-0255/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2010.04.016

know their own selected secrets (i.e. t secrets) and work together to reconstruct $n-t$ other secrets. Thus, any subset of t shareholders can reconstruct the master secret. In other words, this proposed secret sharing scheme enables mutually distrusted shareholders to set up a (t,n) SS. However, there is a potential problem in this scheme. Since the number of shares kept by each shareholder is proportional to the number of shareholders involved, the storage and management of shares becomes very complicated.

The *verifiability* is an important property in the secret sharing scheme. A verifiable secret sharing scheme enables all shareholders to work together to verify that their shares are t-consistent (i.e. any subset of t shares defines the same secret) without revealing the secret and the corresponding shares. In a secret sharing involving multiple dealers, the property of verifiability is more desirable since these dealers are mutually distrusted.

In this paper, we extend the basic idea of a (t,n) secret sharing scheme and give a formal definition on a secret sharing scheme with mutually distrusted dealers, denoted it as (n,t,n) SS, in which each shareholder also acts as a dealer. This scheme was originally proposed by Pedersen [18] in 1991. Our defined (n,t,n) SS is information-theoretically secure which is the same as Shamir's (t,n) SS. In addition, the size of each share of this scheme is the same as the size of the secret. Furthermore, we will show that the (t,n) VSS proposed by Benaloh can only ensure that all shares are t-consistent; but shares may not satisfy the security requirements of a (t,n) SS. More specifically, Benaloh's VSS cannot guarantee that at least t shares are needed to reconstruct the secret. We introduce new notions of *strong t*-consistency and *strong* VSS. A strong VSS can ensure that (a) all shares are t-consistent, and (b) all shares satisfy the security requirements of a secret sharing scheme. We propose a strong (n,t,n) verifiable secret sharing scheme, denoted it as strong (n,t,n) VSS, based on Benaloh's scheme. We prove that our proposed VSS satisfies the definition of a strong VSS.

The rest of this paper is organized as follows: In the next section, we review Shamir's (t,n) SS. In Section 3, we first review the scheme proposed by Pedersen [18] in 1991 and then we give a formal definition on this scheme as (n,t,n) SS. In Section 4, we define new notions of strong t-consistency and strong VSS. In Section 5, we propose a strong (n,t,n) VSS. We conclude in Section 6.

2. Review of Shamir's (t,n) SS

In Shamir's (t,n) SS based on the Lagrange interpolating polynomial, there are n shareholders $\mathcal{P}=\{P_1,\ldots,P_n\}$ and a mutually trusted dealer D. The scheme consists of two algorithms:

Scheme 1. Shamir's (t,n) SS

1. Share generation algorithm: The dealer D first selects a random polynomial $f(x)$ of degree $t-1$: $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$, such that $s=a_0$ and all coefficients $a_0,a_1,\ldots,a_{t-1}$ are in a finite field $\mathbb{F}_p=GF(p)$ with p elements. D computes n shares $(s_1,s_2,\ldots,s_n)$ as

$$s_1=f(1),s_2=f(2),\ldots,s_n=f(n).$$

The dealer distributes each share s_i to shareholder P_i secretly.

2. Secret reconstruction algorithm: For any t shares $(s_{i_1},\ldots,s_{i_t})$ where $\{i_1,\ldots,i_t\}\subset\{1,2,\ldots,n\}$, the secret s can be reconstructed using the Lagrange interpolating formula.

We note that the above algorithms satisfy the basic requirements of the secret sharing scheme, that are, (a) with knowledge of any t or more than t shares, shareholders can reconstruct the secret s; and (b) with knowledge of any $t-1$ or fewer than $t-1$ shares, shareholders cannot reconstruct the secret s. Shamir's scheme is information-theoretically secure since the scheme satisfies these two requirements without making any computational assumption. For more information on this scheme, readers are referred to the original paper [20].

3. Review of Pedersen's (n,t,n) SS

In this section, we give a formal definition on the (n,t,n) secret sharing scheme, denoted it as (n,t,n) SS, in which each shareholder also acts as a dealer. This scheme was originally proposed by Pedersen [18] in 1991.

Intuitively, each dealer (shareholder) in this model wants to participate to generate and share a *master secret*. Each dealer selects a random secret, called this secret as *sub-secret*. Each dealer can share this sub-secret with other dealers by generating *sub-shares* using Shamir's share generation algorithm. With the help of the homomorphism property [1], each shareholder can combine all sub-shares into a master share. Then, the master secret can be reconstructed based on any t or more than t master shares by using Shamir's secret reconstruction algorithm. We now describe the (n,t,n) SS below.

Definition 1 (*(n,t,n) SS*). Suppose that there are n dealers (shareholders) $\mathcal{P}=\{P_1,\ldots,P_n\}$. A (n,t,n) SS consists of four algorithms (see Table 1):

Table 1
(n,t,n) SS.

S	S_1	$\cdots$	S_n	Master shares
P_1	s_{11}	$\cdots$	s_{n1}	$s_1 = \sum_{j=1}^{n} s_{j1}$
P_2	s_{12}	$\cdots$	s_{n2}	$s_2 = \sum_{j=1}^{n} s_{j2}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
P_n	s_{1n}	$\cdots$	s_{nn}	$s_n = \sum_{j=1}^{n} s_{jn}$

Scheme 2. (n,t,n) SS

1. Master secret generation algorithm: Each dealer P_i selects a random sub-secret S_i independently and the master secret can be determined as $S = \sum_{i=1}^{n} S_i = S_1 + \cdots + S_n$.
2. Sub-share generation algorithm: For each sub-secret S_i, dealer P_i selects a random polynomial $f_i(x)$ of degree $t-1$, such that $S_i = f_i(0)$ and uses Shamir's (t,n) SS to generates sub-shares, $s_{ij} = f_i(x_j)$, for $j = 1,2,\ldots,n$, for other dealers. P_i sends each s_{ij} to other dealer P_j secretly, for $j = 1,2,\ldots,n$, and $j \neq i$. Each dealer P_i will have n sub-shares, s_{ji}, for $j = 1,\ldots,n$.
3. Master share generation algorithm: Each shareholder (dealer) P_i with n sub-shares, s_{ji}, for $j = 1,\ldots,n$, computes the master share s_i as $s_i = \sum_{j=1}^{n} s_{ji} = \sum_{j=1}^{n} f_j(x_i)$.
4. Master secret reconstruction algorithm: With knowledge of any t or more than t master shares, the master secret $S = \sum_{j=1}^{n} f_j(0)$ can be reconstructed using the Lagrange interpolating formula.

In Ingemarsson–Simmons's proposal [13], each dealer needs to keep n sub-shares secretly. However, in Scheme 2, according to the property of additive homomorphism defined in [1], each dealer only needs to keep one master share secretly. Following theorem proves that the master secret can be reconstructed based on any t or more than t master shares according to the property of additive homomorphism.

Theorem 1. *With knowledge of any t or more than t master shares as we have described in master share generation algorithm, shareholders can reconstruct the master secret using Shamir's secret reconstruction algorithm.*

Let $\mathcal{S}$ be the domain of a secret and $\mathcal{T}$ be the domain of the shares corresponding to the secret. We say that the function $F_I : \mathcal{T}^t \to \mathcal{S}$ is an *induced* function of the (t,n) SS for each $I \subset \{1,2,\ldots,n\}$ with $|I| = t$. This function defines the secret s based on any subset of t shares $s_{i_1},\ldots,s_{i_t}$. $s = F_I(s_{i_1},\ldots,s_{i_t})$, where $I = \{i_1,\ldots,i_t\}$.

Proof. Let $I = \{i_1,\ldots,i_t\}$ be any subset in the set $\{1,\ldots,n\}$, then we obtain the following equations:

$$\begin{aligned}
S_1 &= F_I(s_{1i_1},\ldots,s_{1i_t}),\\
S_2 &= F_I(s_{2i_1},\ldots,s_{2i_t}),\\
&\vdots\\
S_n &= F_I(s_{ni_1},\ldots,s_{ni_t}).
\end{aligned}$$

Then, we have

$$\begin{aligned}
S = \sum_{i=1}^{n} S_i &= S_1 + S_2 + \cdots + S_n, && (1)\\
&= F_I(s_{1i_1},\ldots,s_{1i_t}) + F_I(s_{2i_1},\ldots,s_{2i_t}) + \cdots + F_I(s_{ni_1},\ldots,s_{ni_t}), && (2)\\
&= F_I((s_{1i_1} + s_{2i_1} + \cdots + s_{ni_1}),\ldots,(s_{1i_t} + s_{2i_t} + \cdots + s_{ni_t})), && (3)\\
&= F_I\left(\sum_{j=1}^{n} s_{ji_1},\ldots,\sum_{j=1}^{n} s_{ji_t}\right), && (4)\\
&= F_I(s_{i_1},\ldots,s_{i_t}). && (5)
\end{aligned}$$

We note that Eq. (1) follows from the master secret generation algorithm; Eq. (2) follows from the sub-secret reconstruction using Shamir's secret reconstruction algorithm; Eq. (3) follows from the additive homomorphism property; and Eq. (5) implies that the master secret can be reconstructed using Shamir's secret reconstruction algorithm with t master shares $s_{i_1},\ldots,s_{i_t}$. □

Remark 1. It is easy to observe that the above (n,t,n) SS uses Shamir's (t,n) SS as building block and is based on the additive homomorphism property. Since Shamir's (t,n) SS is information-theoretically secure, this (n,t,n) SS is also information-theoretically secure. In addition, the size of each master share is identical to the size of each share in Shamir's (t,n) SS. The same approach can be applied on any linear (t,n) SS [15] to convert any (t,n) SS into an efficient (n,t,n) SS.

4. Definitions of strong t-consistency and strong VSS

A verifiable secret sharing scheme enables all shareholders to work together to verify that their shares are t-consistent. In other words, without revealing the secret and the corresponding shares, all shareholders can work together to verify that any subset of t shares defines the same secret. In a secret sharing scheme involving multiple dealers, the property of verifiability is more desirable since these dealers are mutually distrusted. In the (n,t,n) SS, the master share of each shareholder is a combination of n sub-shares generated by n mutually distrusted dealers. Thus, verifiability of these master shares is very important.

Benaloh [1] presented a notion of t-consistency to determine whether a secret sharing scheme is t-consistent or not. We describe this notion below.

Definition 2 (*t-consistency*). A set of n shares $s_1,\ldots,s_n$ is said to be t-consistent, if any subset of t shares reconstructs the same secret.

Benaloh [1] observed that the shares $s_1,\ldots,s_n$ in Shamir's (t,n) SS are t-consistent if and only if the interpolation of the points $(1,s_1),\ldots,(n,s_n)$ yields a polynomial of degree *at most* $t-1$. This implies that if the interpolating polynomial of n shares is with degree at most $t-1$, then all shares are t-consistent. However, the property of t-consistency does not guarantee that all shares satisfy the security requirements of a (t,n) SS. For example, if the interpolating polynomial of n shares is with degree $t-2$, then all shares are both $(t-1)$-consistent and t-consistent. The polynomial with degree $t-2$ can be reconstructed with only $t-1$ (which is less than the threshold, t) shares. This condition violates the security requirement of a (t,n) SS, that is, at least t shares are needed to reconstruct the secret. Benaloh's VSS [1] can only verify that all shares are generated by a polynomial with degree at most $t-1$. Thus, shares may not satisfy the security requirement of a (t,n) SS.

Remark 2. Ghodosi et al. [11] have shown that, in Shamir's (t,n) SS, if the coefficient of highest term, a_{t-1}, of a $(t-1)$th degree polynomial is non-zero, it can increase the probability of successfully guessing the secret $s \in \mathbb{F}_p$ from $1/p$ to $1/(p-1)$ when $t-1$ shareholders collude. In other words, Shamir's (t,n) SS scheme is not information-theoretically secure if the degree of the polynomial is $t-1$ exactly.

We propose new notions of *t-consistency* and *strong verifiable secret sharing* that ensures all shares are generated by a polynomial with degree $t-1$ exactly.

Definition 3 (*Strong t-consistency*). A set of n shares are 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 $t-1$ or fewer than $t-1$ shares cannot reconstruct the same secret (i.e. $t \leqslant n$).

Definition 4 (*Strong VSS*). All shares in a strong verifiable secret sharing scheme can be verified to satisfy the strong t-consistency.

In a strong (t,n) VSS or (n,t,n) VSS, if shares are generated by a linear polynomial, then the polynomial is with degree $t-1$ exactly. It is obvious that if all shares in Shamir's (t,n) SS are generated by a polynomial with degree $t-1$ exactly, then (a) all shares are t-consistent, and (b) all shares satisfy the security requirements of a (t,n) SS. On the other hand, if all shares in Shamir's (t,n) SS are generated by a polynomial with degree at most $t-1$, then this can only guarantee that all shares are t-consistent.

In the next section, we propose a strong (n,t,n) VSS that enables all shareholders to work together to verify that their shares are generated from a polynomial with degree $t-1$ exactly.

Remark 3. If dealer generates shares of a (t,n) SS using a polynomial with degree at most $t-1$ and all shareholders do not know the degree of the polynomial, the security can still be maintained if the probability of needing fewer than t shares to reconstruct the secret is low. However, the probability of needing fewer than t shares to reconstruct the secret depends on how the dealer to select polynomial with degree at most $t-1$ in share generation process. If the dealer selects a random polynomial with degree less than or equal to $t-1$, the probability of needing fewer than t shares to reconstruct the secret is $(t-1)/t$. On the other hand, if the dealer selects a polynomial with random coefficient a_{t-1}, the probability of needing fewer than t shares to reconstruct the secret is $1/p$, where p is the modulus. No matter how the dealer selects a polynomial, in VSS, shareholders still need to verify that the dealer follows the right procedures to select polynomial since shareholders do not trust the dealer. Benaloh's VSS cannot provide this type of verifiability.

5. Strong (n,t,n) VSS

Our strong (n,t,n) VSS is based on Benaloh's (t,n) VSS. Note that Benaloh's (t,n) VSS cannot provide strong VSS. Our scheme includes following steps:

Scheme 3. Strong (n,t,n) VSS

1. Each dealer (shareholder) P_i follows (n,t,n) SS as described in Section 3 to select a random *primary sub-polynomial* $f_i(x)$ (corresponding to the primary sub-secret) with degree $t-1$ exactly such that $S_i = f_i(0)$. Then, each dealer P_i uses Shamir's (t,n) SS to compute and distribute the sub-shares = $f_i(x_j)$, for $j = 1,\ldots,n$, of the primary sub-secret to all other dealers. After receiving all sub-shares from other dealers, each dealer P_i computes the primary master share as $s_i = \sum_{j=1}^{n} s_{ji}$.
2. Each dealer (shareholder) P_i selects k (say $k = 100$) random secondary sub-polynomials with degree $t-1$ exactly. Then, each dealer P_i computes and distributes sub-shares r_{ij}^{l} of each secondary sub-secret to all other dealers using Shamir's share generation algorithm, where $j = 1,\ldots,n$, $l = 1,\ldots,100$. At the end of this step, each shareholder P_i has the primary master share s_i corresponding to the primary master secret and 100 secondary master shares $R = \{r_i^l\}$, for $l = 1,\ldots,100$, corresponding to 100 secondary master secrets, where $r_i^l = \sum_{j=1}^{n} r_{ji}^{l} = r_{1i}^{l} + \cdots + r_{ni}^{l}$.
3. All shareholders work together to determine to open any subset A (say $|A| = 50$) of secondary master shares corresponding to secondary master secrets. Each shareholder needs to reveal secondary master shares in subset A to the public.
4. All shareholders can verify whether their revealed secondary master shares are generated from polynomials with degree $t-1$ exactly and consistently. If this verification is passed for all secondary master shares in subset A, all shareholders (dealers) can be convinced that the degree of all "unopened" secondary polynomials is $t-1$ exactly with very high probability.
5. All shareholders (dealers) work together again to reveal the additive sum of the primary master share and each secondary master share in the subset $R-A$. For example, shareholder P_i reveals $s_i + r_i^l$, for every $r_i^l \in R-A$. All shareholders can verify whether revealed values are generated from polynomials with degree $t-1$ exactly and consistently. If this verification is passed for all master shares and each secondary master share in subset $R-A$, all shareholders (dealers) can be convinced that the degree of polynomial corresponding to the primary master secret is $t-1$ exactly.

Theorem 2. *The proposed (n,t,n) VSS satisfies the definition of a strong VSS.*

Proof. In Step 3, all shareholders select a random subset A and reveal corresponding secondary master shares. These public information will be used to verify whether their secondary master shares are generated from polynomials with degree $t-1$ exactly. Since the subset A is selected randomly, if all opened secondary polynomials are with degree $t-1$ exactly in Step 4, it ensures that the remaining 50 unopened secondary sub-polynomials are with degree $t-1$ exactly with very high probability.

In Step 5, if the interpolating polynomial of the additive sum of the primary master share and each unopened secondary master share is with degree $t-1$ exactly, all shareholders can be convinced that the interpolation of the primary master shares yields a polynomial, denoted it as $f(x) = \sum_{i=1}^{n} f_i(x)$, with degree at most $t-1$. In (n,t,n) VSS, a shareholder also acts as a dealer who has contributed a random primary sub-polynomial in $f(x)$. The additive sum of all primary sub-polynomials forms the polynomial $f(x)$. As long as the degree of the polynomial $f(x)$ is at most $t-1$ and the degree of the primary sub-polynomial selected by the shareholder is $t-1$ exactly, the shareholder can conclude that the degree of the polynomial $f(x)$ must be $t-1$ exactly.

We now consider the situation when there are c colluded shareholders to fail our proposed VSS protocol. In the following analysis, we restrict the parameter c in a (n,t,n) SS to satisfy $c < t$ and $t \leqslant n-c$. The first condition, $c < t$, is to limit colluded shareholders to reconstruct the secret by themselves. The second condition, $t \leqslant n-c$, is to guarantee that the honest shareholders can always reconstruct the secret. We consider two possible attacks from colluded shareholders. The first attack is that each colluded shareholder selects a *primary sub-polynomial* with degree less than $t-1$ in Step 1. Then, the primary polynomial of the master secret is still with degree $t-1$ exactly since the primary polynomial is the additive sum of all sub-polynomials selected by shareholders. This attack cannot affect our proposed VSS. The second attack is that some colluded shareholders select *primary sub-polynomials* with degree larger than $t-1$ in Step 1. Then, the primary polynomial of the master secret is with degree larger than $t-1$. Our proposed VSS protocol can detect this attack since the secondary polynomials in Step 5 are determined by all shareholders and colluded shareholders cannot influence the outcome of the VSS protocol by themselves completely. In other words, in Step 5, honest shareholders can verify that the revealed values are generated from polynomials with degree larger than $t-1$.We want to point out that if the degree of the primary sub-polynomial selected by each shareholder is $t-1$ exactly, the highest coefficient of the additive sum of all primary sub-polynomials can still be zero. This will result a polynomial with degree $t-2$. However, the probability of this case is $1/p$ which can be ignored.

In Step 5, by revealing the additive sum of the primary master share and each secondary master share does not leak any information of the primary master share. Thus, all primary shares and the master secret are unconditionally protected. □

6. Conclusions

In this paper, we extend the basic definition of a (t,n) secret sharing scheme and give a formal definition of the (n,t,n) secret sharing scheme with multiple dealers. We show that the (t,n) VSS proposed by Benaloh can only ensure that all shares are t-consistent; but shares may not satisfy the security requirements of a (t,n) secret sharing scheme. We introduce new notions of strong t-consistency and strong VSS. We also propose a strong (n,t,n) VSS based on Benaloh's VSS, and prove that our proposed VSS satisfies the definition of a strong VSS.

References

[1] J.C. Benaloh, Secret sharing homomorphisms: keeping shares of a secret, in: Advances in Cryptology, Proceedings of the Crypto'86, 11–15 August, Santa Barbara, California, USA, LNCS, vol. 263, Springer-Verlag, Berlin, 1987, pp. 251–260.

[2] G.R. Blakley, Safeguarding cryptographic keys, Proceedings of the AFIPS'79 National Computer Conference, vol. 48, AFIPS Press, 1979, pp. 313–317.

[3] C. Cachin, K. Kursawe, A. Lysyanskaya, R. Strobl, Asynchronous verifiable secret sharing and proactive cryptosystems, in: Proceedings of the Ninth ACM Conference Computer and Communications Security, 18–22 November, Washington, DC, USA, ACM Press, New York, 2002, pp. 88–97.

[4] C. Cachin, K. Kursawe, V. Shoup, Random oracles in constantinople: practical asynchronous Byzantine agreement using cryptography, Journal of Cryptology 18 (3) (2005) 219–246.

[5] T.Y. Chang, M.S. Hwang, W.P. Yang, An improvement on the Lin–Wu (t,n) threshold verifiable multi-secret sharing scheme, Applied Mathematics and Computation 163 (1) (2005) 169–178.

[6] B. Chor, S. Goldwasser, S. Micali, B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, 21–23 October, Oregon, Portland, IEEE Computer Society, 1985, pp. 383–395.

[7] R. Cramer, I. Damgård, U. Maurer, General secure multi-party computation from any linear secret sharing scheme, in: Advances in Cryptology, Proceedings of the Eurocrypt'00, 14–18 May, Bruges, Belgium, LNCS, vol. 1807, Springer-Verlag, Berlin, 2000, pp. 316–334.

[8] M.H. Dehkordi, S. Mashhadi, New efficient and practical verifiable multi-secret sharing schemes, Information Sciences 178 (2008) 2262–2274.

[9] P. Feldman, A practical scheme for non-interactive verifiable secret sharing, in: Proceedings of the 28th IEEE Symposium on Foundations of Computer Science, 27–29 October, Los Angeles, California, IEEE Computer Society, 1987, pp. 427–437.

[10] M. Fitzi, J. Garay, S. Gollakota, C.P. Rangan, K. Srinathan, Round-optimal and efficient verifiable secret sharing, in: Proceedings of the Third Theory of Cryptography Conference – TCC'06, 4–7 March, New York, NY, USA, LNCS, vol. 3876, Springer-Verlag, Berlin, 2006, pp. 329–342.

[11] H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, Remarks on the multiple assignment secret sharing scheme, in: Proceedings of the ICICS'97, 11–14 November, Beijing, China, LNCS, vol. 1334, Springer-Verlag, Berlin, 1997, pp. 72–80.

[12] O. Goldreich, Secure multiparty computation, <http://www.wisdom.weizman.ac.il/oded/pp.html>, 2007.

[13] I. Ingemarsson, G.J. Simmons, A protocol to set up shared secret schemes without the assistance of a mutually trusted party, in: Advances in Cryptology, Proceedings of the Eurocrypt'90, 21–24 May, Aarhus, Denmark, LNCS, vol. 473, Springer-Verlag, Berlin, 1991, pp. 266–282.

[14] J. Katz, C. Koo, R. Kumaresan, Improved the round complexity of VSS in point-to-point networks, in: Proceedings of the ICALP 2008, Part II, 7–11 July, Reykjavik, Iceland, LNCS, vol. 5126, Springer-Verlag, Berlin, 2008, pp. 499–510.

[15] S.C. Kothari, Generalized linear threshold scheme, in: Advances in Cryptology, Proceedings of the Crypto'84, 19–22 August, Santa Barbara, California, USA, LNCS, vol. 196, Springer-Verlag, Berlin, 1984, pp. 231–241.

[16] U. Maurer, Secure multi-party computation made simple, Discrete Applied Mathematics 154 (2) (2006) 370–381.

[17] A. Patra, A. Choudhary, T. Rabin, C.P. Rangan, The round complexity of verifiable secret sharing revisited, in: Advances in Cryptology, Proceedings of the Crypto'09, 16–20 August, Santa Barbara, California, USA, LNCS, vol. 5677, Springer-Verlag, Berlin, 2009, pp. 487–504.

[18] T.P. Pedersen, A threshold cryptosystem without a trusted party, in: Advances in Cryptology, Proceedings of the Eurocrypt'91, 8–11 April, Brighton, UK, LNCS, vol. 547, Springer-Verlag, Berlin, 1991, pp. 522–526.

[19] D. Schultz, B. Liskov, M. Liskov, Brief announcement: mobile proactive secret sharing, in: PODC'08, 18–21 August, Toronto, Canada, 2008, p. 458.

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

[21] J. Shao, Z. Cao, A new efficient (t,n) verifiable multi-secret sharing (VMSS) based on YCH scheme, Applied Mathematics and Computation 168 (1) (2005) 135–140.

[22] L. Zhou, APSS: proactive secret sharing in asynchronous systems, ACM Transactions on Information and System Security 8 (3) (2005) 259–286.