INFORMATION-THEORETICALLY SECURE STRONG VERIFIABLE SECRET SHARING

Changlu Lin
State Key Lab. of Information Security, Graduate University of Chinese Academy of Sciences, China
Key Lab. of Network Security and Cryptology, Fujian Normal University, China
Key Lab. of Communication and Information System (Beijing Jiaotong University)
Beijing Municipal Commission of Education, China
lincl@is.ac.cn

Lein Harn
Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, U.S.A.
harnl@umkc.edu

Dingfeng Ye
State Key Lab. of Information Security, Graduate University of Chinese Academy of Sciences, China
ydf@is.ac.cn

Keywords: Secret sharing, Verifiable secret sharing, Secret sharing homomorphism, t-consistency, Information-theoretically secure.

Abstract: In a (t,n) secret sharing scheme, a mutually trusted dealer 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. When there is no mutually trusted dealer, a (n,t,n) secret sharing scheme can be used to set up a (t,n) secret sharing because each shareholder also acts as a dealer to decide a master secret jointly and divide each selected secret for others. A *verifiable secret sharing* (VSS) allows each shareholder to verify that all shares are t-consistent (*i.e.* every subset of t of the n shares defines the same secret). In this paper, we show that (t,n)-VSS and (n,t,n)-VSS proposed by Pedersen can only ensure that all shares are t-consistent; but shares may not satisfy the security requirements of secret sharing scheme. Then, we introduce a new notion of *strong* VSS. A strong VSS scheme can ensure that (a) all shares are t-consistent, and (b) all shares satisfy the security requirements of secret sharing scheme. We propose two simple ways to convert Pedersen's VSS schemes into strong VSS schemes, which are information-theoretically secure. We also prove that our proposed VSS schemes satisfy the strong verifiable property.

1 INTRODUCTIONS

Secret sharing schemes were introduced by both Blakley (Blakley, 1979) and Shamir (Shamir, 1979) independently in 1979 as a solution for safeguarding cryptographic keys and have been studied extensively in the literatures. In a secret sharing scheme, a secret s is divided into *n shares* and shared among n shareholders by a mutually trusted *dealer* 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 as (t,n)-SS.

In 1990, Ingemarsson and Simmon (Ingemarsson and Simmons, 1991) first considered the secret sharing scheme without the assistance of a mutually trusted third party. When there is no mutually trusted dealer, a (n,t,n) secret sharing scheme can be used to set up a (t,n) secret sharing because each shareholder also acts as a dealer to decide a master secret jointly and divide each selected secret for others.

Shamir's (t,n)-SS is based on the polynomial interpolation and is information-theoretically secure. However, since shareholders have no information about the secret, each shareholder must unconditionally trust that the received share is valid and the dealer has not made any fault in computing shares. In 1985, Chor *et al.* (Chor et al., 1985) extended the notion of the original secret sharing and presented a new notion of *verifiable secret sharing* (VSS). The property of verifiability allows shareholders to verify that all shares are t-consistent (*i.e.* every subset of t of the n shares defines the same secret). VSS(Benaloh, 1986; Feldman, 1987; Pedersen, 1992) is a fundamental tool for many research areas in cryptography, such as secure multi-party computation (Cramer et al., 2000) and Byzantine agreement (Cachin et al., 2005). Recent researches on VSS have studied asynchronous VSS (Cachin et al., 2002), multi-secrets VSS (Dehkordi and Mashhadi, 2008) and optimal round complexity of VSS (Katz et al., 2008), etc.

There are VSS schemes based on some computational assumptions. For example, Feldman's VSS scheme (Feldman, 1987) is based on the discrete logarithm assumption. Later, Pedersen (Pedersen, 1992) used a commitment scheme to remove the assumption in Feldman's VSS scheme to propose a VSS scheme which is information-theoretically secure. However, in Pedersen's VSS scheme the dealer can succeed in distributing incorrect shares if the dealer can solve the discrete logarithm problem.

In this paper, we will show that (t,n)-VSS scheme and (n,t,n)-VSS scheme proposed by Pedersen can only ensure that all shares are generated by interpolated polynomial with degree *at most* $(t-1)$. This result only ensures that all shares are t-consistent, but shares may not satisfy the security requirements of secret sharing scheme. More specifically, Pedersen's VSSs cannot guarantee that at least t shares are needed to reconstruct the secret. Then, we introduce a new notion of *strong* VSS. A strong VSS scheme can ensure that (a) all shares are t-consistent, and (b) all shares satisfy the security requirements of secret sharing scheme. We propose two simple ways to convert Pedersen's VSS schemes into strong VSS schemes. We also prove that our proposed VSS schemes satisfy the strong verifiable property.

The Rest of this Paper is Organized as Follows. In the next section, we provide some preliminaries. In Section 3, we formally define and introduce the notion of strong VSS scheme. In Section 4, we propose two simple ways to convert Pedersen's VSSs into strong VSSs. We conclude in Section 5.

2 PRELIMINARIES

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

Scheme 1. Shamir's (t,n) threshold scheme.

1. Share generation: dealer D does as follows.
   - dealer D first picks a polynomial $f(x)$ of degree $(t-1)$ randomly: $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1}$, in which the secret $s = a_0 = f(0)$ and all coefficients $a_0, a_1, \dots, a_{t-1}$ are in a finite field $\mathbb{F}_p = GF(p)$ with p elements, where p is large prime.
   - D computes all shares:
   $$s_1 = f(1), s_2 = f(2), \dots, s_n = f(n).$$
   - Then, D outputs a list of n shares, $(s_1, s_2, \dots, s_n)$, and distributes each share s_i to corresponding shareholder P_i privately.
2. Secret reconstruction: with any t shares, $(s_{i_1},\dots,s_{i_t})$, where $A = \{i_1,\dots,i_t\} \subseteq \{1,2,\dots,n\}$ can reconstruct the secret s as follows.
$$s = f(0) = \sum_{i\in A} s_i\beta_i = \sum_{i\in A} s_i(\prod_{j\in A-\{i\}} \frac{x_j}{x_j - x_i}),$$
where β_i for $i \in A$ are Lagrange coefficients.

We note that the above scheme satisfies basic security requirements of secret sharing scheme as follows: 1) with knowledge of any t or more than t shares can reconstruct the secret s; and 2) with knowledge of any fewer than $(t-1)$ shares 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 can refer to the original paper (Shamir, 1979).

Secret Sharing Homomorphism. Benaloh (Benaloh, 1986) introduced the property of *homomorphism* in the secret sharing scheme to combine two shares of two different secrets by just adding these shares together.

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

$$s = F_I(s_{i_1},\dots,s_{i_t}), \text{ where } I = \{i_1,\dots,i_t\}.$$

Definition 1 (Homomorphism (Benaloh, 1986)). Let $\oplus$ and $\otimes$ be two binary functions on elements of the set S and T , respectively. We say that a (t,n)-SS has the $(\oplus,\otimes)$-homomorphic property if for any subset I, whenever

$$s = F_I(s_{i_1},\dots,s_{i_t}) \text{ and } s' = F_I(s'_{i_1},\dots,s'_{i_t}),$$

then

$$s \oplus s' = F_I(s_{i_1} \otimes s'_{i_1},\dots,s_{i_t} \otimes s'_{i_t}).$$

***t*-consistency.** Benaloh (Benaloh, 1986) presented a notion of *t-consistency* and proposed VSS to determine whether shares are t-consistent or not. We describe this notion as follows.

Definition 2 (*t*-consistency). A set of n shares $s_1, s_2, \dots, s_n$ is said to be t-consistent, if any subset of t of the n shares reconstructs the same secret.

Benaloh claimed that the shares $s_1, s_2, \dots, s_n$ in Shamir's (t,n)-SS are t-consistent if and only if the interpolation of the points $(1,s_1),(2,s_2),\dots,(n,s_n)$ yields a polynomial of degree *at most* $(t-1)$. This implies that if the interpolated 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 interpolated polynomial of n shares is with degree $(t-2)$, then all shares are $(t-1)$-consistent and also t-consistent. The polynomial with degree $(t-2)$, can be reconstructed with only $(t-1)$ (but *not* t) shares. This condition violates the security requirements of a (t,n)-SS that at least t shares are needed to reconstruct the secret.

It is easy to know that if all shares in Shamir's (t,n)-SS are generated by a polynomial with degree exactly $(t-1)$, then (a) all shares are t-consistent, and (b) all shares satisfy the security requirements of a (t,n)-SS.

Pedersen's VSS Scheme. We note that the disadvantage in Feldman's VSS scheme (Feldman, 1987) is that the committed value $c_0 = g^s$ is publicly known and the privacy of secret s depends on the difficulty of solving the discrete logarithm problem. In other words, Feldman's scheme is computationally secure. Pedersen (Pedersen, 1992) proposed a non-interactive and information-theoretically secure VSS scheme based on Feldman's VSS scheme.

Let p and q be two large primes such that $q|(p-1)$, and $g,h \in \mathbb{Z}_p^*$ are two elements of order q. There are n shareholders $\mathcal{P} = \{P_1,\dots,P_n\}$ and a dealer D who will divide a secret $s \in \mathbb{Z}_q$. We describe Pedersen's scheme in three steps.

Scheme 2. Pedersen's (t,n) VSS scheme.

1. Share generation: dealer D does as follows.
   - D first picks a polynomial $f(x)$ of degree at most $(t-1)$ randomly: $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1}$, in which the secret $s = a_0 = f(0)$ and all coefficients $a_0, a_1, \dots, a_{t-1}$ are in $\mathbb{Z}_q$.
   - D picks $b_0, b_1, \dots, b_{t-1} \in \mathbb{Z}_q$ at random. Let $k(x) = b_0 + b_1x + \cdots + b_{t-1}x^{t-1}$.
   - D computes shares (s_i,t_i) for $i = 1,\dots,n$ and each coefficient's commitment of added sum of polynomials of $f(x)$ and $k(x)$ as follows:
   $$(s_i,t_i) = (f(i),k(i)), \text{ for } i = 1,\dots,n, \text{ and}$$
   $$c_j = g^{a_j}h^{b_j} \pmod{p}, \text{ for } j = 0,1,\dots,t-1.$$
   - Then, D outputs a list of n shares $((s_1,t_1),\dots,(s_n,t_n))$ and distributes each share (s_i,t_i) to corresponding shareholder P_i privately. D also broadcasts $c_0, c_1, \dots, c_{t-1}$.
2. Share verification: each shareholder P_i, who has received the share (s_i,t_i) and all broadcasted information, can verify that share (s_i,t_i) defines a secret by testing that
$$g^{s_i}h^{t_i} = \prod_{j=0}^{t-1} c_j^{i^j} \pmod{p}. \tag{1}$$
3. Secret reconstruction: it is same as Shamir's scheme.

In Pedersen's scheme, the value g^s is not made publicly known, that is, the secret s is embedded in the commitment $c_0 = g^sh^{b_0} = g^{s+ub_0}$ where b_0 is a random number in $\mathbb{Z}_q$ and $u = \log_g h$. Thus, no information about the secret s is revealed even if an attacker with unlimited computing power can solve $u = \log_g h$, the attacker still gets no information about the secret s. It implies that Pedersen's scheme is information-theoretically secure.

3 DEFINITION OF STRONG VSS

We claim that the verification algorithm in Pedersen's scheme can only guarantee that the degree of interpolated polynomial $f(x)$ is at most $(t-1)$; but not exactly $(t-1)$. Let $u = \log_g h$. Then, we get the following result from equation 1.

$$g^{s_i+ut_i} = g^{f(i)+uk(i)}, \tag{2}$$

for $i = 0,1,\dots,n$. Thus, after successfully completing Pedersen's VSS, each shareholder can be convinced that the degree of the polynomial $d(x) = f(x) + uk(x)$ is exactly $(t-1)$. Since polynomial $d(x)$ is a combination of two polynomials, $f(x)$ and $k(x)$, each shareholder can conclude that the degree of polynomial $f(x)$ is at most $(t-1)$. However, this result does not guarantee that all shares satisfy the basic security requirements mentioned in previous section. More specifically, Pedersen's VSS cannot guarantee that at least t shares are needed to reconstruct the secret. For example, if polynomial $f(x)$ is with degree exactly $(t-2)$ and the polynomial $k(x)$ is with degree exactly $(t-1)$, then shares of $f(x)$ can be successfully verifiable according to Pedersen's VSS. Since the polynomial $f(x)$ is with degree exactly $(t-2)$, any $(t-1)$

(but *not* t) shares can reconstructed the secret. This condition violates the basic security requirements that at least t shares are needed to reconstruct the secret. In summary, Pedersen's VSS can only guarantee that all shares are t-consistent; but shares may not satisfy the security requirements of a secret sharing scheme. In this section, we propose a new notion of strong verifiable secret sharing that ensures all shares are generated by a polynomial with degree exactly $(t-1)$. We give the definition.

Definition 3 (Strong VSS). In a strong (t,n) verifiable secret sharing scheme, all shares are generated by a polynomial with degree exactly $(t-1)$.

It is easy to understand that if all shares are generated by a polynomial with degree exactly $(t-1)$, then (a) all shares are t-consistent, and (b) all shares satisfy the basic security requirements.

Remark 1. Feldman's VSS scheme satisfies the definition of a strong VSS scheme.

4 OUR PROPOSED SCHEMES

4.1 Strong (t,n)-VSS

We use a *public* polynomial $f'(x)$ and a secret polynomial $f(x)$ to generate real shares. This public polynomial will play an important role to ensure all shares are generated by a polynomial with degree exactly $(t-1)$ in our proposed scheme. The secret sharing homomorphism ensures that the secret $s = F(0) = f'(0) + f(0)$ can be reconstructed by shares with the form as

$$s_i = f'(i) + f(i).$$

Also, each share s_i still remains to be a secret even $f'(i)$ is made publicly known.

There are n shareholders, $\mathcal{P} = \{P_1, \dots, P_n\}$, and a dealer D who will divide a secret $s \in \mathbb{Z}_q$. We describe our (t,n)-VSS as follows.

Scheme 3. Our strong (t,n)-VSS scheme.

1. Share generation: dealer D does the following procedures.
   - D first picks two polynomial $f'(x)$ and $f(x)$ of degree with exactly $(t-1)$ randomly: $f'(x) = a'_0 + a'_1 x + \cdots + a'_{t-1} x^{t-1}$ and $f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$, where all coefficients a'_i and a_i for $i = 0, 1, \dots, t-1$ are in $\mathbb{Z}_q$. We note that $f(x)$ is kept secret by the dealer and $f'(x)$ is made publicly known. Set $F(x) = f'(x) + f(x)$, thus the secret $S = F(0) = f'(0) + f(0) = a'_0 + a_0$ and $F_i = a'_i + a_i$ for $i = 0, 1, \dots, t-1$.
   - D picks $b_0, b_1, \dots, b_{t-1} \in \mathbb{Z}_q$ at random. Let $k(x) = b_0 + b_1 x + \cdots + b_{t-1} x^{t-1}$.
   - D computes shares (s_i, t_i) and each coefficient's commitment of added sum of polynomials of $F(x)$ and $k(x)$as follows:
   $$(s_i, t_i) = (f(i), g(i)), \text{ for } i = 1, \dots, n, \text{ and}$$
   $$c_j = g^{F_j} h^{b_j} \pmod{p}, \text{ for } j = 0, 1, \dots, t-1.$$
   - Then, D outputs a list of n shares, $((s_1, t_1), \dots, (s_n, t_n))$, and distributes each share (s_i, t_i) to corresponding shareholder P_i privately. D also broadcasts $c_0, c_1, \dots, c_{t-1}$.
   - Each shareholder P_i computes the real share $S_i = s_i + f'(i)$.
2. Share verification: each shareholder P_i, who has share (S_i, t_i) and all broadcasted information, can verify that the real share S_i defines a secret by testing that
$$g^{S_i} h^{t_i} = \prod_{j=0}^{t-1} c_j^{i^j} \pmod{p}. \qquad (3)$$
3. Secret reconstruction: it is the same as Shamir's scheme.

Theorem 1. Our proposed (t,n)-VSS satisfies the definition of a strong VSS scheme.

Proof 1. *Following above (t,n)-VSS scheme successfully, each shareholder can be convinced that the degrees of polynomials $G(x) = F(x) + k(x)$ is exactly $(t-1)$. Thus, each shareholder can conclude that the degree of polynomial $F(x) = f'(x) + f(x)$ is at most $(t-1)$. This conclusion is similar to the conclusion of Pedersen's scheme that ensures each shareholder that the interpolated polynomial of all shares is with degree at most $(t-1)$. Since the degree of the public polynomial $f'(x)$ is exactly $(t-1)$, each shareholder can finally conclude that the degree of polynomial $F(x)$ is exactly $(t-1)$.* □

4.2 Strong (n,t,n)-VSS

In (t,n)-SS, there is a mutually trusted party who divides the secret and distributes shares to shareholders. For some applications, it is impossible to identify such a mutually trusted dealer. In 1990, Ingemarsson and Simmon (Ingemarsson and Simmons, 1991) first considered the secret sharing scheme without the assistance of a mutually trusted third party. The basic idea of their proposed (t,n)-SS is that there are n dealers (or shareholders) who want to generate a master secret s jointly for some special application. Each shareholder i first chooses a secret s_i randomly and the master secret s is determined by $s = \sum_{i=1}^{n} s_i = s_1 + \cdots + s_n$. Each shareholder shares his chosen secret s_i with other shareholders using the Shamir's $(t, n-1)$-SS. Then, any shareholder has received $(n-1)$ shares from other shareholders. Any subset of t of the n shareholders know their own chosen secrets (*i.e.* t secrets) and work together to reconstruct $(n-t)$ other secrets. Thus, any subset of t of the n shareholders can generate the master secret. Their proposed secret scheme enables n users to set up a (t,n)-SS without the assistance of a mutually trusted dealer. This approach can be denoted as the model of a (n,t,n)-SS, where n refers to the number of dealers and shareholders.

In a (n,t,n)-SS, each shareholder also acts as a dealer to generate master secret and sub-shares for all other shareholders. This kind of secret sharing is very difficult to set up especially when it involves a large number of shareholders. In addition, since the number of shares kept by each shareholder is proportional to the number of shareholders involved in (Ingemarsson and Simmons, 1991), the storage and management of shares of each shareholder becomes very complicated. When the number of shareholders becomes very large, the reasonable approach is to divide shareholders into several groups. Each group will then elect a mutually trusted dealer to represent this group to join other dealers from other groups to set up the secret sharing. The dealers are not mutually trusted. In fact, the number of shareholders n can be much larger than the number of dealers d (*i.e.* $d << n$). This approach to manage a large number of users can be found in many practical applications, for example in Public-Key Infrastructure (PKI) (Housley et al., 2002) for issuing public-key digital certificates by Certificate Authorities (CA), and in ad-hoc networks (Zhou and Haas, 1999; Ma and Cheng, 2008) for managing user registration by distributed registration centers, etc. This approach can be denoted as the model of (d,t,n)-SS, where d is the number of dealers, t is the threshold value and n is the number of shareholders. Specially, when $d = 1$, $(1,t,n)$-SS becomes the original Shamir's (t,n)-SS. This indicates that (d,t,n)-SS is a generalization of (t,n)-SS.

In (n,t,n)-SS involving multiple dealers, the verifiability is more desirable than in (t,n)-SS since these dealers are mutually distrusted. Pedersen (Pedersen, 1992) presented a (n,t,n)-VSS. However, Pedersen's (n,t,n)-VSS, is not a strong VSS. In other words, Pedersen's scheme only ensures each shareholder that the interpolated polynomial of all shares is with degree at most $(t-1)$.

In this section, we propose a strong (n,t,n)-VSS based on Pedersen's (n,t,n)-VSS. We note that the main difference between our proposed scheme and the Pedersen's scheme is that it requires each dealer (shareholder) must pick a random polynomial with degree exactly $(t-1)$ in our scheme. We will proof that our proposed scheme is a strong VSS.

There are n dealers (shareholders), $\mathcal{P} = \{P_1, \ldots, P_n\}$, who want to define a secret $s \in \mathbb{Z}_q$ and distribute it among themselves. We describe our (n,t,n)-VSS as follows.

Scheme 4. Our strong (n,t,n)-VSS scheme.

1. Share generation: dealer (shareholder) P_w does as follows.
   - P_w first picks a sub-polynomial $f_w(x)$ of degree exactly $(t-1)$ randomly: $f_w(x) = a_{w0} + a_{w1}x + \cdots + a_{w(t-1)}x^{t-1}$, in which the sub-secret $s_w = a_{w0} = f_w(0)$ and all coefficients $w_{w0}, a_{w1}, \ldots, a_{wt-1}$ are in $\mathbb{Z}_q$. We note that the master secret is $s = s_1 + s_2 + \cdots + s_n$ corresponding to the master polynomial $F(x) = \sum_{w=1}^{n} f_w(x)$.
   - P_w picks $b_{w0}, b_{w1}, \ldots, b_{w(t-1)} \in \mathbb{Z}_q$ at random. Let $k_w(x) = b_{w0} + b_{w1}x + \cdots + b_{w(t-1)}x^{t-1}$.
   - P_w compute all sub-shares (s_{wi}, t_{wi}) and coefficient's commitment of $f_w(x)$ and $k_w(x)$ as follows:
     $$(s_{wi}, t_{wi}) = (f_w(i), k_w(i)), \text{ for } i = 1, \ldots, n, \text{ and}$$
     $$c_{wj} = g^{a_{wj}} h^{b_{wj}} \pmod p, \text{ for } j = 0, 1, \ldots, t-1.$$
   - Then, P_w distributes each sub-share (s_{wi}, t_{wi}) to corresponding shareholder P_i privately and broadcasts $c_{w0}, c_{w1}, \ldots, c_{w(t-1)}$.
   - After P_w has received all sub-shares and broadcasted information from others, P_w computes the master share (s_w, t_w) where $s_w = s_{1w} + s_{2w} + \cdots + s_{nw} \pmod q$ and $t_w = t_{1w} + t_{2w} + \cdots + t_{nw} \pmod q$. P_w also computes $c_j = c_{1j} c_{2j} \cdots c_{nj} \pmod p$ for $j = 0, 1, \ldots, t-1$.
2. Share verification: each shareholder P_w who has obtained the master share (s_w, t_w) and all commitment values c_j for $j = 0, 1, \ldots, t-1$, can verify that all master shares s_i really define a secret by testing that
   $$g^{s_w} h^{t_w} = \prod_{j=0}^{t-1} c_j^{w^j} \pmod p. \tag{4}$$
3. Secret reconstruction: it is same as Shamir's scheme.

Remark 2. The property of secret sharing homomorphisms ensures that all master shares (s_w, t_w) for $w = 1, 2, \ldots, n$ of the master polynomials, $F(x) = \sum_{w=1}^{n} f_w(x)$ and $K(x) = \sum_{w=1}^{n} k_w(x)$, are the additive sum of all shares corresponding to sub-polynomials, $f_w(x)$ and $k_w(x)$. In addition, it ensures that the size of each master share is the same as the size of the master secret.

Theorem 2. Our proposed (n,t,n)-VSS satisfies the definition of a strong VSS scheme.

Proof 2. *According to our discussion presented in section 4.1, each shareholder can conclude that the degree of master polynomial $F(x) = \sum_{w=1}^{n} f_w(x)$ is at most $(t-1)$ if our proposed (n,t,n)-VSS is successfully completed. This result is the same as Pedersen's (t,n)-VSS. As long as the degree of the subpolynomial selected by the shareholder is exactly $(t-1)$, this shareholder can therefore be convinced that, the degree of the master polynomial $F(x)$ must be exactly $(t-1)$ due to linear property of polynomials.* □

Remark 3. Our proposed (n,t,n)-VSS is almost the same as Pedersen's (n,t,n)-VSS. However, the main difference between our proposed scheme and the Pedersen's scheme is that it requires each dealer (shareholder) must pick random polynomials with degree exactly $(t-1)$ in our scheme; but polynomials with degree at most $(t-1)$ in Pedersen's scheme. With this difference, our scheme is a strong (n,t,n)-VSS; but Pedersen's scheme is not a strong (n,t,n)-VSS. Pedersen's scheme can only ensure that all shares are t-consistent; but all shares may not satisfy the security requirements of a secret sharing scheme. Our proposed (n,t,n)-VSS can ensure that (a) all shares are t-consistent, and (b) all shares satisfy the security requirements of a secret sharing scheme.

5 CONCLUSIONS

In this paper, we first show that VSS schemes proposed by Pedersen can only ensure that shares are t-consistent, but shares may not satisfy the security requirements of secret sharing scheme. Then, we introduce a new notion of strong VSS. A strong VSS scheme can ensure that (a) all shares are t-consistent and (b) all shares satisfy the security requirements of secret sharing scheme. Based on Pedersen's VSS schemes, we propose two VSS schemes, (t,n)-VSS and (n,t,n)-VSS, which are information-theoretically secure. We also prove that our proposed VSS schemes satisfy the strong verifiable property.

REFERENCES

Benaloh, J. C. (1986). Secret sharing homomorphisms: Keeping shares of a secret secret. In *Proc. Crypto'86*, volume 263 of *LNCS*, pages 251–260. Springer-Verlag.

Blakley, G. R. (1979). Safeguarding cryptographic keys. In *Proc. Nat. Computer Conf.*, volume 48, pages 313–317. AFIPS Press.

Cachin, C., Kursawe, K., Lysyanskaya, A., and Strobl, R. (2002). Asynchronous verifiable secret sharing and proactive cryptosystems. In *Proc. 9th ACM Conf. Computer and Communications Security*, pages 88–97. ACM Press.

Cachin, C., Kursawe, K., and Shoup, V. (2005). Random oracles in constantinople: practical asynchronous byzantine agreement using cryptography. *J. Cryptology*, 8(3):219–246.

Chor, B., Goldwasser, S., Micali, S., and Awerbuch, B. (1985). Verifiable secret sharing and achieving simultaneously in the presence of faults. In *Proc. 26th IEEE Symp. on Foundations of Computer Science*, pages 383–395. IEEE Society.

Cramer, R., Damgård, I., and Maurer, U. (2000). Verifiable secret sharing and achieving simultaneously in the presence of faults. In *Proc. Eurocrypt'00*, volume 1807 of *LNCS*, pages 316–334. Springer-Verlag.

Dehkordi, M. H. and Mashhadi, S. (2008). New efficient and practical verifiable multi-secret sharing schemes. *Information Sciences*, 178(9):2262–2274.

Feldman, P. (1987). A practical scheme for non-interactive verifiable secret sharing. In *Proc. 28th IEEE Symp. on Foundations of Computer Science*, pages 427–437. IEEE Society.

Housley, R., Polk, W., Ford, W., and Solo, D. (2002). Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. rfc3280, ietf. Available: http://www.ipa.go.jp/security/rfc/RFC3280-00EN.html.

Ingemarsson, I. and Simmons, G. J. (1991). A protocol to set up shared secret schemes without the assistance of a mutualy trusted party. In *Proc. Eurocrypt'90*, volume 472 of *LNCS*, pages 266–282. Springer-Verlag.

Katz, J., Koo, C., and Kumaresan, R. (2008). Improved the round complexity of vss in point-to-point networks. In *Proc. ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 499–510. Springer-Verlag.

Ma, C. and Cheng, R. (2008). Key management based on hierarchical secret sharing in ad-hoc networks. In *Proc. Inscrypt 2007*, volume 4990 of *LNCS*, pages 182–191. Springer-Verlag.

Pedersen, T. P. (1992). Non-interactive and information-theoretic secure verfiable secret sharing. In *Proc. Crypto'91*, volume 576 of *LNCS*, pages 129–140. Springer-Verlag.

Shamir, A. (1979). How to share a secret. *Commun. ACM*, 22(11):612–613.

Zhou, L. and Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Networks Magazine*, 13(6):24–30.