Hindawi
Security and Communication Networks
Volume 2017, Article ID 5437403, 6 pages
https://doi.org/10.1155/2017/5437403

Research Article

How to Share Secret Efficiently over Networks

Lein Harn,[1] Ching-Fang Hsu,[2] Zhe Xia,[3,4] and Junwei Zhou[3,4]

[1]*Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO 64110, USA*
[2]*Computer School, Central China Normal University, Wuhan 430079, China*
[3]*Department of Computer Science, Wuhan University of Technology, Wuhan 430071, China*
[4]*Hubei Key Laboratory of Transportation Internet of Things, Wuhan University of Technology, Wuhan, China*

Correspondence should be addressed to Ching-Fang Hsu; cherryjingfang@gmail.com

Received 22 January 2017; Revised 22 July 2017; Accepted 9 August 2017; Published 27 September 2017

Academic Editor: Pedro Peris-Lopez

In a secret-sharing scheme, the secret is shared among a set of shareholders, and it can be reconstructed if a quorum of these shareholders work together by releasing their secret shares. However, in many applications, it is undesirable for nonshareholders to learn the secret. In these cases, pairwise secure channels are needed among shareholders to exchange the shares. In other words, a shared key needs to be established between every pair of shareholders. But employing an additional key establishment protocol may make the secret-sharing schemes significantly more complicated. To solve this problem, we introduce a new type of secret-sharing, called *protected secret-sharing* (PSS), in which the shares possessed by shareholders not only can be used to reconstruct the original secret but also can be used to establish the shared keys between every pair of shareholders. Therefore, in the secret reconstruction phase, the recovered secret is only available to shareholders but not to nonshareholders. In this paper, an information theoretically secure PSS scheme is proposed, its security properties are analyzed, and its computational complexity is evaluated. Moreover, our proposed PSS scheme also can be applied to threshold cryptosystems to prevent nonshareholders from learning the output of the protocols.

1. Introduction

Secret-sharing schemes, first introduced by Shamir [1] and Blakley [2] in 1979, are very important techniques to ensure secrecy and availability of sensitive information. Moreover, they are widely used as building blocks in various cryptographic protocols, such as threshold cryptosystems, attribute-based encryption, and multiparty computation. In a (t, n) threshold secret-sharing scheme, the secret is divided into n shares so that it can only be recovered with t or more than t shares, but fewer than t shares cannot reveal any information of the secret. In the past few decades, many secret-sharing schemes have been proposed in the literature, and three major approaches can be used to design them: Shamir's approach [1] based on the univariate polynomial, Blakely's approach [2] based on the hyperplane geometry, and Mignotte/Asmuth-Bloom approach [3, 4] based on the Chinese Remainder Theorem (CRT).

In the majority of existing secret-sharing schemes, it is simply assumed that shares are released by the shareholders in the secret reconstruction phase, and then anyone can reconstruct the secret using these revealed shares. But, in many cases, it is undesirable for nonshareholders to learn the secret. Considering the scenario where a famous billionaire sets up the will and shares it among his children using secret-sharing, the children are told that the will should not be read when the billionaire is alive and its contents should be kept strictly private among the family members. However, some paparazzi may want to learn the will after the billionaire passes away to make some head news. In this case, traditional secret-sharing schemes may not provide sufficient protection. To solve this problem, shareholders can use pairwise secure channels to exchange the shares so that the recovered secret is only available to shareholders but not to nonshareholders. If these secure channels are built using cryptographic methods, a shared key is required to be established between every pair of shareholders beforehand. However, employing an additional key establishment protocol may make the secret-sharing schemes significantly more complicated.

The same problem also arises if secret-sharing schemes are used as building blocks in some other cryptographic protocols. For example, threshold cryptography, first introduced by Desmedt [5], is the application of secret-sharing with public-key algorithms. Among various threshold cryptosystems, some are based on ElGamal [6, 7], some are based on RSA [8–11], some are based on Elliptic Curves [12, 13], and some are based on Pairing [14]. In these protocols, shares are either used to generate a digital signature or used to decrypt a ciphertext. To prevent any nonshareholder from learning the outputs of the protocol, a shared key is also needed between every pair of shareholders. Similarly, employing an additional key establishment protocol in threshold cryptosystems can complicate the process significantly.

In this paper, we use bivariate polynomials to propose a new type of secret-sharing scheme, called *protected secret-sharing* (PSS), in which shareholders can use their shares to achieve two purposes simultaneously: one is to reconstruct the original secret and the other is to establish a shared key between every pair of shareholders. Using these shared keys, shareholders can build pairwise secure channels among them to exchange the shares in the secret reconstruction phase. Therefore, PSS provides an efficient solution to protect the original secret from nonshareholders. Our proposed scheme is information theoretically secure, and it can be easily extended to threshold cryptosystems for the same purpose.

Note that although bivariate polynomials have been used to design many different types of secret-sharing schemes in the literature, for example, verifiable secret-sharing (VSS) [15–17], pairwise key distribution [18–21], and dynamic secret-sharing [22], the purpose of this work is different from the previous ones, and the types of employed bivariate polynomials are different as well.

The rest of paper is organized as follows. In Section 2, we review some secret-sharing schemes based on polynomials. In Section 3, we present the models for PSS, including the system model, the adversary model, and the security goals. Our proposed (t, n) PSS scheme based on bivariate polynomials is introduced in Section 4. Its security and complexity analysis is described in Section 5. Finally, we conclude the paper in Section 6.

2. Review of Secret-Sharing Schemes Based on Polynomials

Shamir's (t, n) secret-sharing scheme [1] is based on univariate polynomials. The dealer first randomly selects a polynomial $f(x)$ over $\mathbb{Z}_p$ with degree at most $t-1$, where $s = f(0)$ is the secret. Then the dealer evaluates the polynomial $f(x)$ at different points w_i to generate the shares $f(w_i)$ for $i = 1, 2, \ldots, n$. Here, p is a large prime with $p > s$, and w_i is some public information associated with each shareholder. In what follows in this paper, we assume that all computations are modulo p unless otherwise stated.

In 1985, Chor et al. [23] have extended the notion of secret-sharing and they have proposed the first verifiable secret-sharing (VSS) scheme. The verifiability property allows shareholders to verify the validity of their received shares. If invalid shares were found, shareholders can request the dealer to regenerate new shares. In the literature, several (t, n) VSS schemes [15, 16, 24–27] are designed using bivariate polynomials. A bivariate polynomial with degree at most $t-1$ can be represented as

$$F(x, y) = a_{0,0} + a_{1,0}x + a_{0,1}y + \cdots + a_{t-1,t-1}x^{t-1}y^{t-1}, \quad (1)$$

where $a_{i,j} \in \mathbb{Z}_p, \forall i, j \in [0, t-1]$. If the coefficients satisfy $a_{i,j} = a_{j,i}, \forall i, j \in [0, t-1]$, such a polynomial is called a symmetric bivariate polynomial. Otherwise, it is called an asymmetric bivariate polynomial. In these VSS schemes, the dealer uses a symmetric bivariate polynomial $F(x, y)$ to generate shares $F(w_i, y)$ for the shareholders, where $i = 1, 2, \ldots, n$. Each share $F(w_i, y)$ is a univariate polynomial with degree at most $t-1$. Note that since $F(w_i, w_j) = F(w_j, w_i), \forall i, j \in [1, n]$, a pairwise key $k_{ij} = F(w_i, w_j) = F(w_j, w_i)$ can be established between the shareholders U_i and U_j. Therefore, a symmetric bivariate polynomial can enable two shareholders to establish a pairwise shared key.

3. Models for Protected Secret-Sharing

3.1. System Model

Definition 1 (protected secret-sharing (PSS)). In a PSS, the received shares by shareholders can be used to serve two purposes simultaneously: (a) reconstruct the original secret and (b) establish pairwise shared keys among shareholders (note that these pairwise shared keys are used to build a secure channel between every pair of shareholders in order to exchange the shares in the secret reconstruction phase. Therefore, the reconstructed secret can be protected from any nonshareholder).

The players in our proposed scheme include a trusted dealer $\mathcal{D}$, n shareholders $\{U_1, U_2, \ldots, U_n\}$, and some insider or outsider adversaries. We assume that all these players have unlimited computational power. Among the n shareholders, at least a portion ϵ of them are assumed to be honest.

We assume that there exists a secure channel between the dealer and every shareholder, so that the shares can be securely distributed to shareholders. Moreover, we assume that every player is connected to a common authenticated broadcast channel $\mathcal{C}$, so that any message sent through $\mathcal{C}$ can be heard by the other players. The adversaries cannot modify messages sent by an honest player through $\mathcal{C}$, and they cannot prevent honest players from receiving messages from $\mathcal{C}$. Note that these assumptions are widely used in existing secret-sharing schemes. With these assumptions, we can focus our discussion on the key aspects of PSS without digging into the low level of technical details. Our purpose is to provide an efficient way to establish additional pairwise secret channels among shareholders without invoking a separate key establishment protocol.

Our proposed PSS scheme consists of two phases: (i) share generation and distribution by the dealer and (ii) secret reconstruction by shareholders. During the share generation and distribution phase, the dealer selects a random asymmetric bivariate polynomial to generate the shares for each shareholder, and every share consists of two univariate

polynomials. These shares are sent to shareholders through the secure channels. During the secret reconstruction phase, each shareholder first uses her share to compute pairwise shared keys with the other shareholders. With these shared keys, pairwise secure channels can be established among the shareholders. After receiving the shares from the other shareholders through these secure channels, each shareholder can recover the original secret without leaking it to any nonshareholder.

3.2. Adversary Model. We consider two types of adversaries in the proposed PSS scheme.

(i) Insider Adversary. The insider adversary is a legitimate shareholder who owns a share generated by the dealer. An insider adversary may work alone or collude with some other insider adversaries to learn the secret before it is supposed to be reconstructed or to recover invalid secret using fake shares. Note that when the secret is reconstructed, we assume that the insider adversaries can learn the secret, but they will not leak the secret to nonshareholders, for example, the outsider adversaries.

(ii) Outsider Adversary. The outsider adversary is an attacker who does not own any share generated by the dealer, but she may try to learn the secret that she is unauthorized to access. Note that this attack is possible in many existing secret-sharing schemes when the shares are exchanged in an insecure fashion during the secret reconstruction phase.

3.3. Security Goals. In the security analysis, we demonstrate that the following security goals are satisfied in the proposed PSS scheme based on our assumptions.

Definition 2 (correctness). If there exist a portion $\epsilon > 2/3$ of honest shareholders, the correct secret can always be reconstructed. And any insider adversary who uses fake share in the share reconstruction phase can be identified.

Definition 3 (secrecy). If there exist a portion $\epsilon > 1/2$ of honest shareholders, the insider adversaries cannot learn any information of the secret before the secret is supposed to be reconstructed. Moreover, in the secret reconstruction phase, the traffic flows over the broadcast channel $\mathscr{C}$ reveal no information of the secret to the outsider adversary.

Note that the proposed PSS scheme aims to achieve information theoretical security. Hence, both of the above security goals do not rely on any computational assumption.

4. The Proposed PSS Scheme

In this section, we propose a (t, n) PSS scheme using asymmetric bivariate polynomials. There are two major differences between shares generated by a univariate polynomial and by a bivariate polynomial: (1) the shares generated by a univariate polynomial are integers in $\mathbb{Z}_p$, but shares generated by a bivariate polynomial are univariate polynomials over $\mathbb{Z}_p$; (2) the shares generated by a univariate polynomial can only be used to reconstruct the secret, but the shares generated by a bivariate polynomial not only can be used to reconstruct the secret but also can be used to establish pairwise keys among shareholders.

4.1. Share Generation and Distribution Phase. At first, the dealer $\mathscr{D}$ selects a random asymmetric polynomial:

$$F(x, y) = a_{0,0} + a_{1,0}x + a_{0,1}y + \cdots + a_{t-1,h-1}x^{t-1}y^{h-1}, \quad (2)$$

where $F(x, y)$ is with degree at most $t - 1$ in x and with degree at most $h - 1$ in y (i.e., $h > t(t - 1)$; we will explain this condition in the security analysis), where $s = F(0, 0)$ is the secret, $a_{i,j} \in \mathbb{Z}_p$, and p is a large prime integer with $p > s$. The dealer $\mathscr{D}$ computes a pair of shares $s_i^1(y) = F(w_i, y)$ and $s_i^2(x) = F(x, w_i)$ for each shareholder U_i, where w_i is the public information associated with the corresponding shareholder U_i. The dealer sends the pair of shares $\{s_i^1(y), s_i^2(x)\}$ to each shareholder U_i through the secure channel.

4.2. Secret Reconstruction Phase. Without loss of generality, assume that u (i.e., $t \le u \le n$) shareholders $\{U_1, U_2, \ldots, U_u\}$ are participating in the secret reconstruction phase:

(1) Between every pair of shareholders, they compute two shared keys. For example, the shareholders U_i and U_j (i.e., we assume that $i < j$) can compute the shared keys as $k_{i,j} = s_i^1(w_j) = s_j^2(w_i) = F(w_i, w_j)$ and $k_{j,i} = s_i^2(w_j) = s_j^1(w_i) = F(w_j, w_i)$.

(2) Each shareholder U_i then uses her share $s_i^1(y)$ to compute a *Lagrange Component* δ_i as

$$\delta_i = s_i^1(0) \prod_{j=1, j\neq i}^{u} \frac{-w_j}{w_i - w_j} \pmod{p}. \quad (3)$$

(3) For each pair of shareholders, they use their shared keys to build a secure channel and then use this channel to exchange their Lagrange Components. For example, the shareholder U_i computes $c_{i,j} = E_{k_{i,j}}(\delta_i)$, where $E_{k_{i,j}}(\delta_i)$ denotes the one-time pad encryption of δ_i using the key $k_{i,j}$, and sends $c_{i,j}$ to the shareholder U_j through the authenticated broadcast channel $\mathscr{C}$. Similarly, U_j encrypts her share δ_j by one-time pad using the shared key $k_{j,i}$ and sends $c_{j,i}$ to U_i using the authenticated channel $\mathscr{C}$.

(4) After receiving the ciphertexts $c_{j,i}$ for $j \in \{1, 2, \ldots, u\} \setminus \{i\}$, the shareholder U_i can decrypt them individually as $D_{k_{j,i}}(c_{j,i}) = \delta_j$, where $D_{k_{j,i}}(c_{j,i})$ denotes the decryption of $c_{j,i}$ using the key $k_{j,i}$.

(5) Finally, each shareholder U_i computes the secret as $s = \sum_{j=1}^{u} \delta_j$.

5. Security and Complexity Analysis

In this section, we first prove the correctness and secrecy of the proposed scheme; that is, neither type of adversaries can achieve its objectives based on our assumptions. Then, we briefly analyze the complexity of the proposed scheme.

5.1. Security Analysis

Theorem 4. *The proposed scheme achieves the correctness property. That is, if there exist a portion $\epsilon > 2/3$ of honest shareholders, the correct secret can always be reconstructed. And any dishonest shareholder who uses fake share in the share reconstruction phase can be identified.*

Proof. To prove this theorem, we first consider the situation that there are no dishonest shareholders. Then we justify why less than a portion of 1/3 dishonest shareholders cannot prevent the correct secret from being reconstructed. In step 2 of the secret reconstruction phase, each shareholder U_i uses her share $s_i^1(y)$ to compute the Lagrange Component of the secret s as

$$\delta_i = s_i^1(0) \prod_{j=1, j\neq i}^{u} \frac{-w_j}{w_i - w_j} = F(w_i, 0) \prod_{j=1, j\neq i}^{u} \frac{-w_j}{w_i - w_j}. \quad (4)$$

Since $F(x, 0)$ is a univariate polynomial with degree at most $t-1$, the secret s can be obtained in step 5 through Lagrange Interpolation as

$$s = F(0,0) = \sum_{i=1}^{u} F(w_i, 0) \prod_{j=1, j\neq i}^{u} \frac{-w_j}{w_i - w_j}. \quad (5)$$

Therefore, if all shareholders are honest, the correct secret can be reconstructed. However, if there exist some dishonest shareholders, they may use fake shares in the secret reconstruction phase. In the proposed PSS scheme, the secret can be reconstructed by any subset of t or more than t shareholders. Hence, we assume that there are at most $t-1$ dishonest shareholders. Otherwise, the dishonest shareholders working together will have the ability to reconstruct the secret. In this case, any polynomial $F(x, 0)$ that passes n points agrees at most $t-1$ points and it disagrees at least $n-t+1$ points. In other words, these polynomials have a Hamming distance $n-t+1$, and this distance can correct any number of errors that is less than $(n-t+1)/2$ according to Coding Theory. Therefore, if $t-1 < (n-t+1)/2$, the correct secret can always be reconstructed. Note that $t-1 < n/3$ is another form of this inequality. To speed up the decoding process, either the Euclidean decoder or the Berlekamp-Massey decoder can be used. Moreover, if the correct secret is determined, the invalid shares can be identified as well. This is because any subset that contains invalid shares will interpolate into an incorrect secret. □

Theorem 5. *The proposed scheme satisfies the secrecy property. That is, the outsider adversaries cannot obtain any information of the secret. Moreover, if there exist a portion $\epsilon > 1/2$ of honest shareholders and the condition $h > t(t-1)$ holds, then t or more than t shares can recover the secret, but fewer than t shares cannot reveal any information of the secret.*

Proof. Although the shareholders exchange information through the authenticated broadcast channel $\mathscr{C}$ in the secret reconstruction phase, all messages are encrypted. Based on the assumption that the asymmetric polynomial is randomly selected over $\mathbb{Z}_p$ by the dealer $\mathscr{D}$, the messages and the shared keys are all randomly distributed within the same space $\mathbb{Z}_p$. Moreover, since the messages are exchanged only once, one-time pad can be used here to encrypt these messages. Therefore, even if the outsider adversary has unlimited computational power, she cannot obtain any information of the secret. Next, we prove that if $\epsilon > 1/2$ and $h > t(t-1)$, the insider adversaries cannot learn the secret before it is reconstructed. Regarding the first inequality, it just simply states that there should be a majority of honest shareholders. Otherwise, the dishonest shareholders will have all the abilities that the honest ones have, that is, reconstruct the secret. Note that this requirement is widely used in most of the existing secret-sharing schemes. Regarding the second inequality, recall that the polynomial $F(x, y)$ is an asymmetric polynomial of degree $t-1$ in x and degree $h-1$ in y. It contains th different coefficient. In the proposed scheme, each share $\{s_i^1(y), s_i^2(x)\}$ contains two univariate polynomials with degree $h-1$ in y and degree $t-1$ in x, respectively. In other words, each shareholder can use her share to establish at most $t+h$ linearly independent equations in terms of the coefficients of the bivariate polynomial $F(x, y)$. When there are $t-1$ colluded shareholders with their shares together, they can establish a total of $(t+h)(t-1)$ linearly independent equations. If the number of coefficients of the bivariate polynomial $F(x, y)$ is larger than the number of equations available to the colluded shareholders, that is, $th > (t+h)(t-1)$, the $t-1$ dishonest shareholders cannot recover $F(x, y)$. Hence, they cannot learn any information of the secret. Therefore, these two inequalities together ensure that fewer than t shares cannot reveal any information of the secret. □

5.2. Complexity Analysis. In this section, we analyze the complexity of our proposed scheme and compare it with the one in Shamir's secret-sharing scheme. Regarding the share generation and distribution phase, in our proposed PSS scheme, each share $\{s_i^1(y), s_i^2(x)\}$ consists of two univariate polynomials: one is $t-1$ degree in x and the other is $h-1$ degree in y. Therefore, $t+h$ coefficients in $\mathbb{Z}_p$ need to be transmitted from the dealer to each shareholder, and each shareholder needs to store these coefficients. The storage requirement for each shareholder is $(t+h)\log_2 p$ bits, where p is the modulus. In Shamir's secret-sharing scheme, each share is a single value in $\mathbb{Z}_p$. Therefore, only one value in $\mathbb{Z}_p$ needs to be transmitted from the dealer to each shareholder, and the storage requirement for each shareholder is $\log_2 p$ bits. Note that, when evaluating the polynomials, Horner's algorithm can be used to reduce the computational cost in both our proposed scheme and in Shamir's secret-sharing scheme.

Regarding the secret reconstruction phase, in step 1, each shareholder needs to compute pairwise shared keys with the other shareholders. Note that this step does not involve any interaction. Using Horner's algorithm, evaluating the polynomials of degree $h-1$ and degree $t-1$ requires h steps and t steps, respectively, where each step consists of one multiplication and one addition. In step 2, each

shareholder needs to compute $\delta_i = s_i^1(0)\prod_{j=1,j\neq i}^{u}(-w_j/(w_i - w_j))$. Since $s_i^1(0)$ is the constant coefficient of the polynomial $s_i^1(y)$, there is no need to compute this value. Therefore, the computational cost of evaluating δ_i is identical to that in Shamir's secret-sharing scheme. Finally, there are $u - 1$ one-time pad encryptions in step 3 and $u - 1$ one-time pad decryptions in step 4.

Based on the above analysis, the computational complexities are similar in both schemes. But, compared with Shamir's secret-sharing scheme, more information needs to be transmitted and stored by each shareholder in our proposed scheme. The price is paid to achieve an additional property that the recovered secret is not revealed to nonshareholders. This property is desirable in many applications and our proposed scheme achieves it even if the adversaries have unlimited computational power. Although including a pairwise key establishment protocol [18, 28] with Shamir's secret-sharing scheme can protect the secret from nonshareholders as well, most pairwise key establishment protocols are computationally secure (not information theoretically secure) and the complexity of key establishment protocol will have a quadratic relationship with the number of shareholders participating in the secret reconstruction phase.

5.3. Some Future Works. In the last three decades, many fascinating works about secret-sharing have been proposed in the literature, and different types of secret-sharing schemes can provide different properties. For example, verifiable secret-sharing (VSS) scheme [15–17] not only allows the shareholders to verify the validity of their received shares in the share generation and distribution phase but also allows the verification of the revealed shares in the secret reconstruction phase. In proactive secret-sharing schemes [29–31], shareholders can refresh their shares periodically without the dealer being involved, so that the shares obtained by the adversaries will become obsolete after the shares are updated. Moreover, the threshold can be dynamically adjusted when some shareholders join in or leave. In multiple secret-sharing schemes [32–34], each shareholder can use her share to recover multiple secrets at different stages. In this paper, we have not considered these additional properties, and the existing secret-sharing schemes have not considered the issue of protecting the secret(s) from nonshareholders. Therefore, incorporating the ideas presented in this paper with these different types of secret-sharing schemes will be interesting, and we consider these further investigations as our future works.

6. Conclusion

A new type of secret-sharing, called protected secret-sharing (PSS), has been introduced in this paper. In a PSS scheme, the shareholders' shares not only can be used to recover the secret but also can be used to protect the shares against nonshareholders in the secret reconstruction phase. A (t, n) PSS scheme using a bivariate polynomial is proposed, and we provide security and complexity analysis of the proposed scheme. Some possible future works are also discussed in the paper. Note that our method is generic enough to be directly applied with threshold cryptosystems for the same purpose.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Authors' Contributions

The authors have equal contribution to this paper.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China (Grants nos. 61772224, 61601337, 61672398, and 61503289), the Key Natural Science Foundation of Hubei Province (Grant no. 2015CFA069), the Science and Technology Support Program of Hubei Province (Grants nos. 2015BAA120 and 2015BCE068), the Applied Fundamental Research of Wuhan (Grant no. 20160101010004), the Humanity and Social Science Youth Foundation of Ministry of Education of China (no. 15YJC870029), and the Research Planning Project of National Language Committee (no. YB135-40).

References

[1] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612-613, 1979.

[2] R. Blakley, "Safeguarding cryptographic keys," *Proceedings of the National Computer Conference*, vol. 48, pp. 313–317, 1979.

[3] M. Mignotte, "How to share a secret," in *Proceedings of the Advances in Cryptology–EUROCRYPT '82*, T. Beth, Ed., Lecture Notes in Computer Science, pp. 371–375, 1982.

[4] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.

[5] Y. Desmedt, "Society and group oriented cryptography: a new concept," in *Proceedings of the Advances in Cryptology–CRYPTO '87*, vol. 1987, pp. 120–127.

[6] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Proceedings of the Advances in CRYPTO '89*, vol. 435 of *Lecture Notes in Computer Science*, pp. 307–315, 1989.

[7] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEE Proceedings: Computers and Digital Techniques*, vol. 141, no. 5, pp. 307–313, 1994.

[8] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," in *Proceedings of the Advances in CRYPTO '91*, vol. 576 of *Lecture Notes in Computer Science*, pp. 457–469, 1991.

[9] A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung, "How to share a function securely," in *Proceedings of the 26th Annual ACM Symposium on the Theory of Computing*, pp. 522–533, May 1994.

[10] R. Gennaro, S. a. Jarecki, H. Krawczyk, and T. Rabin, "Robust and efficient sharing of RSA functions," in *Proceedings of the Advances in CRYPTO '96*, vol. 1109 of *Lecture Notes in Comput. Sci.*, pp. 157–172, 1996.

[11] V. Shoup, "Practical threshold signature," in *Proceedings of the Advances in EUROCRYPT '00*, Lecture Notes in Computer Science, pp. 207–220, 2000.

[12] L. Ertaul and W. Lu, "Ecc based threshold cryptography for secure data forwarding and secure key exchange in manet," in *Proceedings of the International Conference on Research in Networking*, 2005.

[13] Y. Shang, X. Wang, Y. Li, and Y. Zhang, "A general threshold signature scheme based on elliptic curve," *Advanced Materials Research*, 2013.

[14] W. Gao, G. Wang, X. Wang, and Z. Yang, "One-round ID-based threshold signature scheme from bilinear pairings," *Informatica*, vol. 20, no. 4, pp. 461–476, 2009.

[15] M. Fitzi, J. Garay, S. Gollakota, C. P. Rangan, and K. Srinathan, "Round-optimal and efficient verifiable secret sharing," in *Proceedings of the 3rd Theory of Cryptography Conference, TCC '06*, Lecture Notes in Comput. Sci., pp. 329–342, Springer, 2006.

[16] R. Kumaresan, A. Patra, and C. P. Rangan, "The round complexity of verifiable secret sharing: The statistical case," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6477, pp. 431–447, 2010.

[17] A. Patra, A. Choudhary, T. Rabin, and C. Pandu Rangan, "The round complexity of verifiable secret sharing revisited," in *Proceedings of the Advances in Cryptology-CRYPTO '09*, Lecture Notes in Comput. Sci., pp. 487–504, Springer, Berlin, 2009.

[18] D. Liu, P. Ning, and L. I. Rongfang, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, 2005.

[19] H. Liang and C. Wang, "An energy efficient dynamic key management scheme based on polynomial and cluster in wireless sensor netwoks," *Journal of Convergence Information Technology*, vol. 6, no. 5, pp. 321–328, 2011.

[20] S. Guo and V. Leung, "A compromise-resilient group rekeying scheme for hierarchical wireless sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference 2010, WCNC '10*, 2010.

[21] N. Saxena, G. Tsudik, and J. H. Yi, "Efficient node admission and certificateless secure communication in short-lived MANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 2, pp. 158–170, 2009.

[22] L. Harn and C.-F. Hsu, "Dynamic threshold secret reconstruction and its application to the threshold cryptography," *Information Processing Letters*, vol. 115, no. 11, pp. 851–857, 2015.

[23] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," *Foundations of Computer Science*, pp. 383–395, 1985.

[24] R. Cramer, I. Damgård, S. Dziembowski, M. Hirt, and T. Rabin, "Efficient multiparty computations secure against an adaptive adversary," in *Proceedings of the Conference on the Theory and Applications of Cryptographic Techniques*, vol. 1999, pp. 311–326.

[25] R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin, "The round complexity of verifiable secret sharing and secure multicast," in *Proceedings of the Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pp. 580–589, 2001.

[26] J. Katz, C.-Y. Koo, and R. Kumaresan, "Improving the round complexity of vss in point-to-point networks," in *International Colloquium on Automata, Languages, and Programming*, pp. 499–510, 2008.

[27] V. Nikov and S. Nikova, "On proactive secret sharing schemes," in *Proceedings of the International Workshop on Selected Areas in Cryptography*, Lecture Notes in Comput. Sci., pp. 308–325, Springer, Berlin, New York, NY, USA.

[28] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in cryptology—EUROCRYPT*, pp. 453–474, 2001.

[29] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive secret sharing or: how to cope with perpetual leakage," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 963, pp. 339–352, 1995.

[30] Y. Frankel, P. Gemmell, P. D. MacKenzie, and M. Yung, "Optimal-resilience proactive public-key cryptosystems," in *Proceedings of the 1997 38th IEEE Annual Symposium on Foundations of Computer Science*, pp. 384–393, October 1997.

[31] T. Rabin, "A simplified approach to threshold and proactive RSA," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1462, pp. 89–104, 1998.

[32] T.-Y. Wu and Y.-M. Tseng, "Publicly verifiable multi-secret sharing scheme from bilinear pairings," *IET Information Security*, vol. 7, no. 3, pp. 239–246, 2013.

[33] A. Endurthi, O. B. Chanu, A. N. Tentu, and V. C. Venkaiah, "Reusable multi-stage multi-secret sharing schemes based on CRT," *Journal of Communications Software and Systems*, vol. 11, no. 1, pp. 15–24, 2015.

[34] J. Herranz, A. Ruiz, and G. Sáez, "New results and applications for multi-secret sharing schemes," *Designs, Codes and Cryptography*, vol. 73, no. 3, pp. 841–864, 2014.