Wireless Pers Commun (2017) 97:3943–3950
DOI 10.1007/s11277-017-4708-z

A Novel Threshold Cryptography with Membership Authentication and Key Establishment

Lein Harn[1] · **Ching-Fang Hsu**[1,2]

Published online: 31 July 2017

Abstract Threshold cryptography has become one of most important tools in providing secure applications such as password protection, cloud computing, etc. Threshold cryptography splits a secret into multiple pieces in such a way that only with enough number (i.e., threshold) of pieces of secret can recover the secret and therefore enable the application; but with fewer than the threshold cannot recover the secret. Shamir's (t, n) threshold scheme based on a univariate polynomial is the most popular secret sharing scheme so far. The public-key based threshold cryptography which incorporates a public-key algorithm, such as digital signature or encryption scheme, with a secret sharing, called *threshold signature/decryption* scheme, has become an active research area. While implementing threshold cryptographic schemes over networks, it involves multiple users. All secure multi-user network applications need to have membership authentication and key establishment in prior of applications; otherwise attackers can participated in the threshold cryptographic applications without being detected. Membership authentication is used to ensure that all users are legitimate members. Key establishment is used to establish session keys among members and the session keys are used to protect exchange information in application. In this paper, we propose a novel design which embeds the function of membership authentication and key establishment in threshold cryptographic schemes. Tokens of members obtained during registration can be used for (a) membership authentication; (b) key establishment and (c) threshold cryptographic applications. However, all

Lein Harn and Ching-Fang Hsu contributed equally to this work

✉ Ching-Fang Hsu
cherryjingfang@gmail.com

Lein Harn
harnl@umkc.edu

[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

existing threshold cryptographic solutions need additional membership authentication and key establishment.

Keywords Threshold cryptography · Threshold secret sharing · Membership authentication · Key establishment

1 Introduction

As the use of cloud computing becomes widespread, security of the cloud computing becomes an important research topic. Secret sharing (SS) is one of most important cryptographic primitives for data outsourcing [1, 2]. In Shamir's (*t, n*) threshold SS [3], the user of an outsourced data file, F, splits F into n sub-files, $f_1, f_2, \ldots, f_n$, such that each sub-file f_i, is padded with some redundant information to make it having the same size as that of F. The file F can be retrieved if t out of n sub-files are available. Nirmala et al. [4] provided a comparative study of SSs in cloud computing.

Threshold cryptography has become one of most important tools in providing secure applications such as password protection [5], cloud computing [1, 2, 4], etc. Threshold cryptography splits a secret into multiple pieces in such a way that only with enough number (i.e., threshold) of pieces of the secret can recover the secret and therefore enable the application; but with fewer than the threshold cannot recover the secret. Shamir's (t, n) threshold SS [3] based on a univariate polynomial is the most popular SS so far. There are other approaches used to design SSs. For example, Azimuth-Bloom's SS [6] is based on the Chinese Remainder Theorem (CRT), and Blakely's SS [7] is based on hyperplane geometry.

The public-key based threshold cryptography which incorporates a public-key algorithm, such as digital signature or encryption scheme, with a SS, called *threshold signature/decryption* scheme [8–11], has become one active research area. The threshold signature scheme in which a signature can only be generated if there are enough number of signers working together has become a commercial application [12]. The threshold decryption in which a ciphertext can only be decrypted successfully if there are enough number of receivers working together. The public-key threshold cryptographic schemes have become popular tools to provide security solutions.

While implementing threshold cryptographic scheme over networks, it involves multiple users. Any secure multi-user application needs membership authentication and key establishment in prior of the application; otherwise attackers can participated in the threshold cryptographic applications without being detected. Membership authentication is used to ensure that all users are legitimate members. Most user authentication protocols [13, 14] are one-to-one interactions which involve one prover and one verifier. In a recent paper [15], a new type of authentication, called *group authentication*, has been proposed based on the SS which authenticates all users at once. But the group authentication can only determine whether all users are members or not. If there are non-members, the group authentication cannot identify non-members. The key establishment enables secret session keys shared among all members in a communication. The session keys will be used to protect exchange information in the application. Key establishment is an active research area. Various key establishment schemes have been proposed. In general, there are two types of key establishment schemes: the centralized [16, 17] and the distributed schemes [18, 19]. The centralized key establishment uses a key generation center (KGC) to

distribute keys for members and the distributed key establishment requires members to generate the keys.

In this paper, we propose a novel design which embeds the function of membership authentication and key establishment in threshold cryptographic schemes. We propose a membership authentication and key establishment based on polynomial-based SS. During registration, each member will receive a "token" from the membership registration center (MRC). Tokens are generated by a multivariate polynomial and each share is a univariate polynomial. Each member uses the token for membership authentication, key establishment and threshold cryptographic applications. We propose an efficient way to implement threshold cryptography in network applications. In other words, our design does not need separate membership and key establishment for threshold cryptography. In summary, we list the contributions of this paper below.

- Instead of using a univariate polynomial in all existing threshold cryptographic schemes, we propose to use a bivariate polynomial in the cryptographic applications.
- Tokens generated by a bivariate polynomial initially can be used for (a) membership authentication; (b) key establishment and (c) threshold cryptographic applications.
- Our proposed approach is very efficient since there is no need for additional membership authentication and key establishment.

The rest of this paper is organized as follows: In the next section, we review some preliminaries. Our proposed scheme is given in Sect. 3. In Sect. 4, we analyze our proposed scheme. We conclude in Sect. 5.

2 Preliminaries

In Shamir's (t, n) threshold SS [3], the dealer selects a univariate polynomial, $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1} nod\, p$, to generate shares for shareholders. In a bivariate polynomial, $F(x, y) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{2,0}x^2 + a_{1,1}xy + a_{0,2}y^2 + \cdots + a_{t-1,0}x^{t-1} + a_{t-2,1}x^{t-2}y + \cdots + a_{t-1,t-1}x^{t-1}y^{t-1} nod\, p$, where $a_{i,j} \in GF(p)$, if the coefficients satisfy, $a_{i,j} = a_{j,i}, \quad \forall i, j$, it is a symmetric bivariate polynomial. There are many (t, n) verifiable SSs (VSSs) in the literature [20–22] use symmetric bivariate polynomials to generate shares. In these schemes, the dealer select a symmetric bivariate polynomial to generate shares. $F(x_i, y)$, $i = 1, 2, \ldots, n$, where x_i is a public information of shareholder, U_i. Each share, $F(x_i, y)$, is a univariate polynomial. Since $F(x_i, x_j) = F(x_j, x_i)$, $\forall i, j \in [0, t-1]$, a pairwise key, can be shared between any pair of shareholders, U_i and U_j. Harn and Xu [24] used a symmetric bivariate polynomial to design a dynamic threshold secret reconstruction scheme. Blundo et al. [23] have proposed a non-interactive k-secure m-conference protocol based on a multivariate polynomial, $F(x_1, x_2 \ldots, x_m)$. Because each share, $F(x_i, x_2 \ldots, x_m)$, is a polynomial involving $m-1$ variables with degree k, each user needs to store $(k+1)^{m-1}$ coefficients. The storage space of each user is exponentially proportional to the size of conference. This makes their protocol impractical. Recently, Harn and Gong [25] proposed a conference key establishment scheme using a special type of multivariate polynomial to overcome the storage problem of each user.

In this paper, we propose a novel design of threshold cryptographic schemes. Our design integrates solutions of both threshold cryptography and secure network together. In other words, we propose to use a multivariate polynomial to generate tokens. The tokens

can be used to provide (a) membership authentication; (b) key establishment and (c) threshold applications.

3 Proposed Scheme

In the following discussion, we demonstrate our proposed design using a bivariate polynomial for a (*t, n*) threshold SS. The similar design can be applied to other threshold cryptographic algorithms [8–11] such as threshold signature/decryption.

3.1 Phase 1: Registration Phase

The MRC selects a $l-1$ degree symmetric polynomial, $F(x,y) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{2,0}x^2 + a_{1,1}xy + a_{0,2}y^2 + \cdots + a_{t-1,0}x^{l-1} + a_{t-2,1}x^{t-2}y + \cdots + a_{t-1,t-1}x^{t-1}y^{l-1} mod\ p$, with $F(0,0) = a_{0,0} = s$, where s is the secret. The MRC computes tokens, $s_i(y) = F(x_i, y) \mod p$ for members, $U_i, i = 1, 2, \ldots, n$, where $x_i \notin \{0, 1\}$ is the public information associated with each member, U_i. The MRC sends each token, $s_i(y)$, to member U_i secretly.

3.2 Phase 2: Membership Authentication and Key Establishment

We assume that r (i.e., $t < r \leq n$) members, for example $\{U_{v_1}, U_{v_2}, \ldots, U_{v_r}\}$, want to engage in a threshold cryptographic application.

Step 1. Each member U_{v_i} broadcasts a random integer, $r_i \in GF(p)$, to all other members.

Step 2. Each member U_{v_i} uses his token, $s_{v_i}(y)$, to compute pairwise shared keys, $k_{i,j} = s_{v_i}(x_{v_j}) = F(x_{v_i}, x_{v_j})$, $j = 1, 2, \ldots, r, \quad j \neq i$, where $k_{i,j}$ is the secret key shared between shareholders, U_{v_i} and U_{v_j}.

Step 3. Each member U_{v_i} computes authentication responses, $Auth_{i,j} = h(k_{i,j}\|r_j), j = 1, 2, \ldots, r, \quad j \neq i$, where $h(k_{i,j}\|r_j)$ is a one-way hash output with $k_{i,j}$ and r_j as inputs. Each $Auth_{i,j}$ is sent to member U_{v_j} publicly for authentication.

Step 4. After receiving $Auth_{i,j} = h(k_{i,j}\|r_j)$, from member U_{v_i}, member U_{v_j} uses his computed pairwise shared key, $k_{j,i} = s_{v_j}(x_{v_i}) = F(x_{v_j}, x_{i_j})$, in Step 2 to check whether $Auth_{i,j} \stackrel{?}{=} h(k_{j,i}\|r_j)$. If the checking is successful, member U_{v_i} has been authenticated; otherwise, member U_{v_i} has not been authenticated. Repeat this process for all other members U_{v_i}, $i = 1, 2, \ldots, r, \quad i \neq j$.

3.3 Phase 3: Threshold Cryptographic Application

In this phase, members follow a threshold cryptographic algorithm to complete the process. However, all exchange information among members is encrypted under the pairwise shared keys, $k_{i,j}$, $j = 1, 2, \ldots, r, \quad j \neq i$, in Step 2.

In the following discussion, we demonstrate the secret reconstruction in a threshold SS. We assume that all members in $\{U_{v_1}, U_{v_2}, \ldots, U_{v_j}\}$ have been successfully authenticated in Phase 2.

3.3.1 Secret Reconstruction

Step 1. Each member U_{v_i} uses his token, $s_{v_i}(y)$, to compute $q_{v_i} = s_{v_i}(0)\prod_{k=1,k\neq j}^{r}\frac{-x_{v_k}}{x_{v_j}-x_{v_k}} \bmod p$.
Step 2. Each member U_{v_i} uses his computed pairwise shared keys, $k_{i,j}, j = 1,2,\ldots,r, \quad j \neq i$, in Phase 2, Step 2 to encrypt q_{v_i} as $u_{i,j} = E_{k_{i,j}}(q_{v_i}), j = 1,2,\ldots,r, \quad j \neq i$. Member U_{v_i} sends each $u_{i,j}$ to member U_{v_j}.
Step 3. After receiving $u_{j,i}$, from other member, member U_{v_i} uses his computed pairwise shared key, $k_{i,j}$, in Phase 2, Step 2 to decrypt as $q_{v_j} = E_{k_{i,j}}(u_{j,i})$. Repeat this process for all $u_{j,i}, i = 1,2,\ldots,r, \quad i \neq j$.
Step 4. After obtaining $q_{v_j}. j = 1,2,\ldots,r, \quad j \neq i$, from all other members, member U_{v_i} computes $\sum_{j=1}^{r} q_{v_j} \bmod p = \sum_{j=1}^{r} s_{j_i}(0)\prod_{k=1,k\neq j}^{r}\frac{-x_{v_k}}{x_{v_j}-x_{v_k}} \bmod p = s$.

4 Analysis

4.1 Correctness

In Step 4 of the secret reconstruction, we have $\sum_{j=1}^{r} q_{v_j} \bmod p = \sum_{j=1}^{r} s_{j_i}(0)\prod_{k=1,k\neq j}^{r}\frac{-x_{v_k}}{x_{v_j}-x_{v_k}} \bmod p = \sum_{j=1}^{r} F(x_j,0)\prod_{k=1,k\neq j}^{r}\frac{-x_{v_k}}{x_{v_j}-x_{v_k}} \bmod p = F(0,0) = s$.

4.2 Threshold of the Secret

There are two major differences between shares generated by a $t-1$ degree univariate polynomial and by a $t-1$ degree symmetric bivariate polynomial, (a) there are t different coefficients in a $t-1$ degree univariate polynomial but there are $\frac{t(t+1)}{2}$ different coefficients in a $t-1$ degree symmetric bivariate polynomial, and (b) shares by a $t-1$ degree univariate polynomial are integers in $GF(p)$; but shares by a $t-1$ degree symmetric bivariate polynomial is a univariate polynomial having $t-1$ degree. We give the definition of the threshold of a threshold SS.

Definition 1 (*Threshold of a threshold SS*) The threshold, *th*, of a threshold SS specifies the minimal number of shares needed to reconstruct the secret.

It is well-known that the threshold of shares generated by a $t-1$ degree univariate polynomial is t. The following theorem states the threshold of shares generated by a $t-1$ degree symmetric bivariate polynomial.

Theorem 1 *The threshold of shares generated by a* $t-1$ *degree symmetric bivariate polynomial is* $th = \left\lceil\frac{t+1}{2}\right\rceil$.

Proof In a $t-1$ degree symmetric bivariate polynomial, there are $\frac{t(t+1)}{2}$ different coefficients, In addition, each share is a univariate polynomial having $t-1$ degree. In other words, it can establish t linearly independent equations in terms of coefficients of the bivariate polynomial from each share. Having enough number of shares (i.e., *th*), the total number of linearly independent equations, $th \cdot t$, needs to satisfy $th \cdot t \geq \left\lceil\frac{t(t+1)}{2}\right\rceil$ in order to

recover the bivariate polynomial and therefore to reconstruct the secret. This implies that $th = \lceil \frac{t+1}{2} \rceil$. □

4.3 Possible Attacks

4.3.1 Insider Attackers

Inside attackers are legitimate members who own valid tokens from the MRC during registration. From Theorem 1, we obtain that the threshold of shares generated by a $t-1$ degree symmetric bivariate polynomial is $\lceil \frac{t+1}{2} \rceil$. Thus, it needs at least $\lceil \frac{t+1}{2} \rceil$ insider attackers to work together to reconstruct the secret.

4.3.2 Outside Attackers

Outside attackers are illegitimate users who do not own any valid tokens from MRC. The outside attackers may try to impersonate members in the secret reconstruction to obtain the secret. However, since in the secret reconstruction, all exchange information of legitimate members are encrypted using pairwise shared keys and outside attackers do not own any valid token to recover any pairwise shared key, so the outside attacker cannot obtain the reconstructed secret.

4.4 Performance

The proposed scheme does not need any additional key establishment and authentication. Membership authentication and pairwise shared keys in the secret reconstruction are based on the same tokens used to reconstruct the secret. Thus, our proposed solution is very efficient in comparing with all existing threshold cryptographic solutions which need additional membership and key establishment schemes to prevent outside attackers.

5 Conclusion

Threshold cryptography is an active research area in network security. We propose a novel design to integrate solutions of both threshold cryptography and network security. Users can use their tokens obtained during registration to provide (a) membership authentication, (b) key establishment and (c) threshold applications.

References

1. Bessani, A., Correia, M., Quaresma, B., Andre, F., & Sousa, P. (2011). DEPSKY: Dependable and secure storage in a cloud-of clouds. In *Proceedings of the sixth conference on computer systems (Eurosys'11)*, pp. 31–46.
2. Agudo, I., Nuñez, D., Giammatteo, G., Rizomiliotis, P., & Lambrinoudakis, C. (2011) Cryptography goes to the cloud. In *Proceedings of STA 2011 workshops*, CCIS 187 (pp. 190–197). Berlin: Springer.
3. Shamir, A. (1979). How to share a secret. *Communications of the Association for Computing Machinery, 22*(11), 612–613.

4. Nirmala, S. J., Bhanu, S. M. S., & Patel, A. A. (2012). A comparative study of the secret sharing algorithms for secure data in the cloud. *International Journal on Cloud Computing: Services and Architecture, 2*(4), 63–71.
5. Simonite, T. (2012). To keep passwords safe from hackers, just break them into bits. *Technology Review.*
6. Asmuth, C., & Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transactions on Information Theory, 29*(2), 208–210.
7. Blakley, G. R. (1979). Safeguarding cryptographic keys. In *Proceedings of American federation of information processing societies national computer conference*, Vol. 48, pp. 313–317, New York.
8. Boldyreva, A. (2003) Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. In *6th international workshop on practice and theory in public key cryptography,* pp. 31–46, Miami, FL, January 6–8, 2003.
9. Harn, L. (1994). Group-oriented (t, n) threshold signature and multisignature. *IEE Proceedings-Computers and Digital Techniques, 141*(5), 307–313.
10. Canetti, R., & Goldwasser, S. (1999). An efficient threshold public key cryptosystem secure against adaptive chosen ciphertext attack. *Proceedings of Eurocrypt, 1999,* 90–106.
11. Desmedt, Y., & Frankel, Y. (1989). Threshold cryptosystems. *Proceedings of Crypto, 1989,* 307–315.
12. Prisco, G. (2015) Threshold signatures: The new standard for wallet security? *Bitcoin Magzine,* March 2015.
13. Das, M. L. (2009). Two-Factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications, 8*(3), 1086–1090.
14. Harn, L., & Ren, J. (2011). Generalized digital certificate for user authentication and key establishment for Secure Communications. *IEEE Transactions on Wireless Communications, 10*(7), 2372–2379.
15. Harn, L. (2013). Group authentication. *IEEE Transactions on Computers, 62*(9), 1893–1898.
16. IEEE Standard 802.16-2004 (2004) *Part 16: Air Interface for Fixed Broadband Wireless Access Systems.* IEEE.
17. Harn, L., & Lin, C. (2010). Authenticated group key transfer protocol based on secret sharing. *IEEE Transactions on Computers, 59*(6), 842–846.
18. Bresson, E., Chevassut, O., & Pointcheval, D. (2007). Provably-secure authenticated group Diffie–Hellman key exchange. *ACM Transactions Information and System Security, 10*(3), 255–264.
19. Katz, J., & Yung, M. (2007). Scalable protocols for authenticated group key exchange. *Journal of Cryptology, 20,* 85–113.
20. Katz, J., Koo, C., Kumaresan, R. (2008) Improved the round complexity of VSS in point-to point networks. In *Proceedings of ICALP '08*, Part II, in: LNCS, Vol. 5126 (pp. 499–510). Berlin: Springer.
21. Kumaresan, R., Patra, A., Rangan, C. P. (2010) The round complexity of verifiable secret sharing: the statistical case. In *Advances in cryptology—ASIACRYPT 2010*, LNCS, Vol. 6477 (pp. 431–447). Berlin: Springer.
22. Patra, A., Choudhary, A., Rabin, T., Rangan, C. P. (2009). The round complexity of verifiable secret sharing revisited. In *Advances in cryptology, proceedings of the Crypto'09*, 16–20 August, Santa Barbara, CA, LNCS, Vol. 5677 (pp. 487–504). Berlin: Springer.
23. Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., Yung, M. (1993). Perfectly-secure key distribution for dynamic conferences. In *Advances in cryptology-Crypto'92*, Vol. 740 (pp. 471–486). Berlin: Springer.
24. Harn, L., & Xu, C. F. (2015). Dynamic threshold secret reconstruction and its application to the threshold cryptography. *Information Processing Letters, 115,* 851–857.
25. Harn, L., & Gong, G. (2015). Conference key establishment protocol using a multivariate polynomial and its applications. *Security and Communication Networks, 8,* 1794–1800.

Lein Harn received the B.S. degree in electrical engineering from the National Taiwan University in 1977, the M.S. degree in electrical engineering from the State University of New York-Stony Brook in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota in 1984. He is currently a Professor at the Department of Electrical and Computer Engineering, University of Missouri, Kansas City (UMKC). He is currently investigating new ways of using secret sharing in various applications.

Ching-Fang Hsu received the M.Eng. and the Ph.D. degrees in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2010 respectively. From Sep. 2010 to Mar. 2013, she was a Research Fellow at the Huazhong University of Science and Technology. She is currently an Assistant Professor at Central China Normal University, Wuhan, China. Her research interests are in cryptography and network security, especially in secret sharing and its applications.