Zhang *et al. EURASIP Journal on Wireless Communications and Networking* (2018) 2018:71
https://doi.org/10.1186/s13638-018-1086-5

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

(t, n) multi-secret sharing scheme extended from Harn-Hsu's scheme

Tong Zhang*, Xizheng Ke and Yanxiao Liu

Abstract

Multi-secret sharing scheme has been well studied in recent years. In most multi-secret sharing schemes, all secrets must be recovered synchronously; the shares cannot be reused any more. In 2017, Harn and Hsu proposed a novel and reasonable feature in multiple secret sharing, such that the multiple secrets should be reconstructed asynchronously and the recovering of previous secrets do not leak any information on unrecovered secrets. Harn and Hsu also proposed a (t, n) multi-secret sharing scheme that satisfies this feature. However, the analysis on Harn-Hsu's scheme is wrong, and their scheme fails to satisfy this feature. If one secret is reconstructed, all the other unrecovered secrets can be computed by any $t - 1$ shareholders illegitimately. Another problem in Harn-Hsu's work is that the parameters are unreasonable which will be shown as follows. In this paper, we prove the incorrectness of Harn-Hsu's scheme and propose a new (t, n) multi-secret sharing scheme which is extended from Harn-Hsu's scheme; our proposed scheme satisfies the feature introduced by Harn and Hsu.

Keywords: Secret sharing scheme, Multiple secrets, Asynchronous, Bivariate polynomial

1 Introduction

Secret sharing scheme [1, 2] is a useful fundamental cryptographic protocol that can protect information security among a group of participants. In traditional (t, n) secret sharing scheme, each of the n participants keep a share of secret s in such a way that any t or more participants can reconstruct the secret s; less than t participants cannot get any information on s. Secret sharing scheme is a useful fundamental to other cryptographic protocols [3, 4]. Due to the low efficiency in secret reconstruction of traditional (t, n) secret sharing scheme (shares are used to reconstruct only one secret), multiple secret sharing becomes more popular in recent years [5–7] which can improve the use efficiency of the shares.

In most multiple secret sharing schemes, all secrets are reconstructed synchronously. This characteristic would limit its applications in some asynchronous systems. In [8], Harn and Hsu introduced a new feature such that in multiple secret sharing, the multiple secrets should have the capability to be reconstructed asynchronously. Multiple secret sharing scheme with this new feature would adapt higher secure requirement in some asynchronous systems; it can expand application background of multi-secret sharing. In [8], a (t, n) multi-secret sharing based on bivariate polynomial was also proposed to fit the new feature (many verifiable secret sharing schemes were based on bivariate polynomial [9, 10]). However, their scheme does not satisfy the new feature. Their analysis is incomplete and ignores a wise attack from inside attackers. In addition, the parameters in their scheme are not reasonable either.

In this paper, we propose a wise attack from inside attackers and prove Harn-Hsu's scheme does not satisfy the new feature, and analysis why their parameters are unreasonable. Although their scheme does not work, the new feature of asynchronous secret reconstruction is worthwhile to be studied. Next, we introduce a new (t, n) multi-secret sharing scheme that can satisfy the new feature.

2 Review on Harn-Hsu's scheme

In [8], Harn and Hsu introduced a new secure requirement of multi-secret sharing scheme such that the secrets should be reconstructed asynchronously. The following definition concludes the secure model for this new feature:

*Correspondence: zhangtong@xaut.edu.cn
Department of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China

Definition 1 *In multiple-secret sharing scheme with asynchronous secret reconstruction, reconstructed secrets do not leak any information on the unrecovered secrets.*

The proposed (t, n) multi-secret sharing scheme based on bivariate polynomial in [8] is briefly described below.

2.1 *Harn-Hsu's scheme*

Share generation phase:

- A dealer selects a bivariate polynomial $F(x, y)$ over $GF(p)$, where the x has degree $t-1$ and y has degree $h-1$. The k multiple secrets are $s_1 = F(1,0), S_2 = F(2,0), ..., s_k = F(k,0)$. All the parameters satisfy $th > (t+h)(t-1) + (k-1)$.
- The dealer computes $f_i(x) = F(x, v_i), g_i(y) = F(v_i, y), i = 1, 2, ..., n$ and sends $f_i(x), g_i(y)$ to each shareholder P_i as their shares. v_i is the identity of shareholder P_i which is public information to all shareholders.

Secret reconstruction phase:

- Let $P_1, P_2, ..., P_t$ be involved in this phase. Any pair of (P_i, P_j) computes a common pairwise key $K_{i,j} = F(v_i, v_j)$ $(v_i < v_j)$ using their shares.
- For a secret $s_r \in [s_1, s_2, ..., s_k]$, each one of these t shareholders computes his Lagrange component on s_r respectively.
- Each shareholder $P_i, i = 1, 2, ..., k$ sends share information on s_r to other $k-1$ shareholders $P_j, j = 1, 2, ..., k, j \neq i$ using the secure channel which is built up by $K_{i,j}$.
- Each shareholder can reconstruct the secret s_r using the Lagrange formula.

There are two main contributions of the above scheme.

Contribution 1 *The shares of shareholders cannot be only used to reconstruct secrets, but also to generate pairwise keys for each pair of shareholders. By transferring information using a secure channel which is built up by pairwise key, the scheme can resist attack from outsiders.*

Contribution 2 *In* [8]*, it is also claimed that their scheme satisfies Definition* 1*. It is proved that even* $k-1$ *secrets have been reconstructed; any* $t-1$ *shareholders still cannot get any information on the last secret.*

3 Results and discussion

3.1 Proof of security in Harn-Hsu's work

In [8], Contribution 2 is proved by the following theorem:

Theorem 1 *In* [8]*, all* k *multiple secrets can be reconstructed asynchronously such that* $t-1$ *shareholders get no information of unrecovered secrets from reconstructed secrets.*

Proof The bivariate polynomial $F(x, y)$ has th coefficients in total. On the other hand, each shareholder can establish $t + h$ independent equations on those th coefficients from their shares; therefore, any $t-1$ shareholder can build up $(t-1)(t+h)$ equations. Suppose $k-1$ secrets have been recovered which means that $k-1$ additional equations are built. Since the parameters t, h, k satisfy $th > (t+h)(t-1) + (k-1)$, this means $t-1$ shareholders cannot get enough independent equations on those th coefficients to recover $F(x, y)$. As a result, the last secret cannot be reconstructed. □

3.2 Comments on Harn-Hsu's work

In this part, we will show that the conclusion of above Theorem 1 is not correct. $t-1$ shareholders do not need to reconstruct $F(x, y)$ to compute unrecovered secrets; there exists a wise attack from these $t-1$ shareholders.

Theorem 2 *In Harn-Hsu's work, any* $t-1$ *shareholder can recover all* $k-1$ *secrets with only one reconstructed secret.*

Proof The k multiple secrets in Harn-Hsu's work is $s_1 = F(1,0), s_2 = F(2,0), ..., s_k = F(k,0)$. Let $f(x) = F(x, 0)$, then the k secrets are k points on the $f(x)$ $(s_i = f(i))$ which is of degree $t-1$. On the other hand, each shareholder receives a share $g_i(y) = F(v_i, y)$ from a dealer; he can compute a value $g_i(0) = F(v_i, 0) = f(v_i)$ which is also a point on $f(x)$; $t-1$ shareholders would have $t-1$ points on $f(x)$. Therefore, once a secret s_r is reconstructed, any $t-1$ shareholder can obtain $t-1+1 = t$ points on a $t-1$ degree polynomial $f(x)$, then $f(x)$ can be reconstructed by the Lagrange formula; all the other secrets $s_i, i = 1, 2, ..., k, i \neq r$ are recovered by these $t-1$ shareholders. □

In addition, Harn-Hsu's scheme requires that $th > (t+h)(t-1) + (k-1)$, which means the parameter h would be as large as t^2. In this case, the size of share $g_i(y) = F(v_i, y)$ for each shareholder is expanded too much comparing with other multi-secret sharing schemes which is also unreasonable in practical applications.

3.3 Proposed scheme

Although Harn-Hsu's work fails to satisfy the feature of asynchronous secret reconstruction, this new feature is still reasonable and practical. In this part, we propose a new (t, n) multi-secret sharing scheme which is fit for the new feature. Our scheme is also based on a bivariate polynomial which is inspired by Harn-Hsu's work.

3.3.1 Proposed scheme

Share generation phase:

- A dealer selects a bivariate polynomial $F(x, y)$ over $GF(p)$, where both x and y have degree $t-1$. The t multiple secrets are $s_1 = F(1,0), S_2 = F(2,0), ..., s_t = F(t,0)$.
- The dealer computes $f_i(x) = F(x, v_i), i = 1, 2, ..., n$ and sends $f_i(x)$ to each shareholder P_i as their shares. v_i is the identity of shareholder P_i which is public information to all shareholders.

Secret reconstruction phase:

- Let $P_1, P_2, ..., P_t$ be involved in this phase. For a secret $s_r \in [s_1, s_2, ..., s_k]$, each shareholder P_i computes and discloses a value $e_i = f_i(r)$.
- The secret s_r can be reconstructed from $e_1, e_2, ..., e_t$ using the Lagrange formula: $s_r = \sum_{i=1}^{t} \left(e_i \prod_{j=1, j\neq i}^{t} \frac{-v_j}{v_i - v_j} \right)$

Theorem 3 *Our proposed scheme satisfies the feature of asynchronous secret reconstruction.*

Proof First we prove the correctness of our scheme. Each shareholder computes $e_i = f_i(r) = F(r, v_i)$, $i = 1, 2, ..., t$. Let $g_r(y) = F(r, y)$ ($g_r(y)$ is of degree $t-1$), then each e_i is a point on $g_r(y)$ since $e_i = g_r(v_i)$. Therefore $g_r(y)$ can be reconstructed by these t points using the Lagrange formula. The secret $s_r = F(r,0) = g_r(0)$ is computed by $s_r = \sum_{i=1}^{t} \left(e_i \prod_{j=1, j\neq i}^{t} \frac{-v_j}{v_i - v_j} \right)$.

Suppose $t-1$ secrets $s_1, s_2, ..., s_{t-1}$ have been recovered. In this case, any $t-1$ shareholder obtains $t-1$ points on polynomial $f_s(x) = F(x, 0)$. In order to recover secret s_t, these $t-1$ shareholders need to obtain one more point on $f_s(x)$. However, these $t-1$ shareholders can build no more linear equation on the t coefficients of $f_s(x)$ at all based on the property of asymmetric bivariate polynomial [5, 6]. In other word, with $t-1$ recovered secrets $s_1, s_2, ..., s_{t-1}$, any $t-1$ shareholders will find that each value $u \in GF(p)$ could be the last legal secret s_t, and they have equal probability such that $\left\{ Pr(u = s_t) = \frac{1}{p} \mid u \in GF(p) \right\}$. Therefore, $t-1$ shareholders cannot reconstruct the secret s_t with all previous reconstructed secrets. □

In [8], each pair of shareholders computes a common pairwise key using their shares which can be used to build up a secure channel between any two shareholders. This secure channel can protect information from attack of outsiders. In the above scheme, no pairwise key exists and all t shareholders can share a common key to build up a secure platform. The security level from one common key is weaker than pairwise keys between any two shareholders. Therefore, we can improve our proposed scheme which is shown in the revised scheme below.

3.3.2 Revised scheme

Share generation phase:

- A dealer selects an asymmetric bivariate polynomial $F(x, y)$ over $GF(p)$, where both x and y have degree $t-1$. The t multiple secrets are $s_1 = F(1,0), S_2 = F(2,0), ..., s_t = F(t,0)$.
- The dealer selects a symmetric bivariate polynomial $G(x, y)$ over $GF(p)$, where both x and y have degree $t-1$.
- The dealer computes $f_i(x) = F(x, v_i), i = 1, 2, ..., n$ and sends $f_i(x)$ to each shareholder P_i as their shares. v_i is the identity of shareholder P_i which is public information to all shareholders.
- The dealer computes $u_i(x) = G(x, v_i), i = 1, 2, ..., n$ and sends $u_i(x)$ to each shareholder P_i

Secret reconstruction phase:

- Let $P_1, P_2, ..., P_t$ be involved in this phase. Each pair of (P_i, P_j) computes a common key $K_{i,j} = G(v_i, v_j)$. (P_i can compute $K_{i,j}$ by $K_{i,j} = u_i(v_j)$; P_j computes $K_{i,j}$ by $K_{i,j} = u_j(v_i)$.) Then they build up a secure channel using $K_{i,j}$.
- Same as in the proposed scheme, but transmits information using secure channels.

The revised scheme satisfies both Contributions 1 and **2** in Harn-Hsu's work, and the size of share is much smaller than their scheme. Comparisons between Harn-Hsu's work and our schemes are shown in Table 1.

Both our proposed scheme and its revised version are reasonable and practical. In a system that requires high secure level, the revised version is more practical; otherwise, our proposed scheme has advantage in a system that requires higher computational efficiency and speed.

Table 1 Comparisons between Harn-Hsu's work and our schemes

Schemes	Contribution 1	Contribution 2	Number of secrets	Size of share
Harn-Hsu's scheme	Yes	No	k	More than t^2
Scheme 1	No	Yes	t	t
Revised scheme	Yes	Yes	t	$2t$

Contribution 1 pairwise keys, *Contribution 2* asynchronous secret reconstruction, *Size of share* the number of coefficients in share

4 Conclusions

Asynchronous secret reconstruction is a reasonable and practical feature in (t, n) multi-secret sharing scheme which is first introduced by Harn-Hsu's work [8] recently. However, in this paper, we prove that Harn-Hsu's scheme does not satisfy this new feature. Once a secret is recovered by t shareholders, any $t - 1$ shareholder can reconstruct all the rest of the secrets illegitimately. Next, we propose a new (t, n) multi-secret sharing scheme which satisfies this new feature. In revised version, each pair of shareholders can compute a common pairwise key to build up a secure channel which is consistent with Harn-Hsu's work.

5 Method

In this work, we aim to point out the mistake of Harn-Hsu's scheme and give a modification of their work to overcome the problem. The security analysis of Harn-Hsu' work is only based on the property of interpolation polynomial.

Funding

The research presented in this paper is supported in part by the China National Natural Science Foundation (No. 61502384), Xi'an Science and Technology Project (No. 2017080CG/RC043(XALG004)), Industrial Science and Technology Project of Shaanxi Province (No. 2016GY-140), and Science Research Project of the Key Laboratory of Shaanxi Provincial Department of Education (No. 15JS078).

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Authors' contributions

TZ contributed in algorithm designing; XK was responsible for security analysis; YL carried out the writing. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 7 March 2018 Accepted: 21 March 2018
Published online: 02 April 2018

References

1. GR Blakley, in *AFIPS1979 national computer conference*. Safeguarding cryptographic keys. vol.48, (1979), pp. 313–317
2. A Shamir, How to share a secret. Commun. ACM. **22**(11), 612–613 (1979)
3. CM Tang, SH Gao, CL Zhang, The optimal linear secret sharing scheme for any given access structure. J. Syst. Sci. Complex. **26**(4), 634–649 (2013)
4. CM Tang, CL Cai, Verifiable mobile online social network privacy-preserving location sharing scheme. Concurr. Comput. Pract. Experience. **29**(24), 1–10 (2017)
5. L Harn, Secure secret reconstruction and multi-secret sharing schemes with unconditional secure. Secur. Commun. Netw. **7**(3), 567–573 (2014)
6. J Herranz, A Ruiz, G Saez, New results and applications for multi-secret sharing schemes. Des. Codes Cryptography. **73**(3), 841–864 (2014)
7. YX Liu, Efficient (n, t, n) secret sharing schemes. J. Syst. Softw. **85**(6), 1325–1332 (2012)
8. L Harn, CF Hsu, (t, n) multi-secret sharing scheme based on bivariate polynomial. Wireless Pers. Commun. **95**(2), 1–10 (2017)
9. J Katz, CY Koo, R Kumaresa, Improving the round complexity of VSS in point-to-point networks. Inf. Comput. **207**(8), 889–899 (2009)
10. R Kumaresan, A Patra, CP Rangan, in *ASIACRYPT2010, LNCS*. The round complexity of verifiable secret sharing: the statistical case. vol. 6477 (Springer, Heidelberg, 2010), pp. 431–447