Global Analysis and Discrete Mathematics
Volume 1, Issue 2, pp. 93–100
ISSN: 2476-5341

Security Analysis of a Hash-Based Secret Sharing Scheme

M. Farhadi* · **H. Baypoor** ·
R. Mortazavi

Received: 28 December 2015 / Accepted: 5 September 2016

Abstract Secret sharing schemes perform an important role in protecting secret by sharing it among multiple participants. In 1979, (t, n) threshold secret sharing schemes were proposed by Shamir and Blakley independently. In a (t, n) threshold secret sharing scheme a secret can be shared among n participants such that t or more participants can reconstruct the secret, but it can not be reconstructed by $t - 1$ or fewer participants. The proposed schemes by Shamir and Blakley have some drawbacks. Multi-secret and verifiable schemes were invented to improve old schemes. We analysis the security of hash based secret sharing schemes, and show that the schemes have some drawbacks. In particular it is shown that the the schemes are not resistant against deceptive behavior by dealer and participants.

Keywords Secret sharing schemes · Minimal authorized subsets · cheating

Mathematics Subject Classification (2010) 94A60 · 94A62

*Corresponding author
M. Farhadi
School of Mathematics and Computer Science, Damghan University, Damghan, Iran
E-mail: farhadi@du.ac.ir

H. Baypoor
School of Mathematics and Computer Science, Damghan University, Damghan, Iran
E-mail: h.baypoor@std.du.ac.ir

R. Mortazavi
School of Engineering, Damghan University, Damghan, Iran
E-mail: r_mortazavi@du.ac.ir

1 Introduction

A secret sharing scheme is designed to safeguard a secret by splitting it into shares and distributing them among a group of participants. In 1979, (t, n) threshold secret sharing scheme were proposed by Shamir [12] and Blakley [1] independently. The Shamir scheme is based on Lagrange polynomial interpolation.

In a (t, n) threshold secret sharing scheme, a secret can be shared among n participants such that t or more participants can reconstruct the secret, but $t-1$ or fewer participants can not. Due to the special property of secret sharing scheme, it can be used in many applications, such as threshold access control [11], e-voting [9], anonymous token [8], and e-auction [2]. Also, secret sharing schemes have applications in the areas of security protocols, for example, database security and multiparty computation (MPC) [6].

A group of participants, which can recover the secret when they join together, is called an authorized subset. Any group of t or more participants forms an authorized subset in a (t, n) threshold scheme. The access structure Γ is the set of all authorized subsets.

Given any access structure Γ, the set $A \in \Gamma$ is called a minimal authorized subset if $\forall\ B \subset A$ then $B \notin \Gamma$. We use Γ_0 to denote the set of all minimal authorized subsets of Γ. More formally, in a (t, n) threshold scheme, let P denote the set of participants, then

$$\Gamma = \{A | A \subseteq P \ and\ |A| \geqslant t\}$$
$$\Gamma_0 = \{A | A \subseteq P \ and\ |A| = t\}$$

A dishonest dealer could distribute invalid shadows to the Participants. Furthermore, during the reconstruction phase there is no way to ascertain that the shadows provided by the participants of an authorized subset. We recognize the need to be able to confirm the consistency of shadows with the original secret. This is achieved by Verifiable Secret Sharing (VSS) schemes. The first interactive VSS scheme was proposed in 1985 by Chor, Goldwasser, Micali and Awerbuch [3]. Two commonly used examples are the computationally secure Feldman VSS [7] and the information-theoretically secure Pedersen VSS [10]. But these two schemes are not interactive.

In real applications, it is known that traditional secret sharing schemes like Shamir and Blakley can not solve the following problems. [13]

(1) only one secret can be shared during one secret sharing process, they can not be used to share multiple secrets simultaneously.

(2) The shadows of participants are not reusable. Once the secret has been reconstructed, all shadows will no longer be private.

(3) Deceptive behaviors of a dishonest dealer can not be detected. A dishonest dealer may distribute a fake shadow to a certain participant, and then that participant would subsequently never obtain the true secret.

(4) Deceptive behaviors of a malicious participant can not be prevented in the process of reconstruction. A malicious participant may provided a fake

shadow to cheat the other participants to prevent them from reconstructing the true secret.

(5) Private channels are required for the communications between the dealer and participants.

(6) The dealer knows all shadows of participants. The shares of participants are not reusable for different dealers.

Chum and Zhang proposed a simple secret sharing scheme by using cryptography hash function and herding hashes technique [5]. In this paper, we show that this scheme can not solve drawbacks of Shamir and Blakley schemes. The remainder of this paper is organized as follows. In section 2 we consider Chum and Zhang scheme. Verifiable scheme is considered in section 3. In section 4 Multi-Secret scheme is explained. In section 5 we check security analysis the functionalities of the three scheme. Finally, concludes our paper.

2 Chum and Zhang scheme

Setup and secret recovery phases of Chum and Zhang scheme [5] are as follow.

2.1 Setup

1. The scheme randomly generates n distinct shadows $s_1, s_2, \ldots, s_n$ for n participants $p_1, p_2, \ldots, p_n$, where the size of each shadow is the same as that of the secret. The scheme sends s_i to corresponding p_i through a secure private channel.
2. The scheme determines all the minimal authorized subsets. Suppose we have w minimal authorized subsets. Any participant recive a shadow, and combination of shadows of participants from these w authorized subsets will be a private message M_{priv}. For example, if p_1, p_2, p_3 are participants of an authorized subset then $M_{priv} = s_1||s_2||s_3$.
3. Calculate the M_{priv} hash for any authorized subset A_i as $H(M_{priv}) = h_i$, $i = 1, 2, \ldots, w$.
4. Suppose h be a secret and size of h same size of h_i. If we want random secret, we can generate this via same way as we perform for shadows, or secret h to be a predetermined fixed value.
5. We generate a control c_i for any authorized subset (all of the authorized subsets that contain all of the minimal authorized subsets) as $c_i = h_i \oplus h$, $i = 1, 2, \ldots, w$ (here, $\oplus$ is bitwise exclusive OR). A control c_i also used for determine wether a subset is authorized or not. (Control c_i determine for authorized subsets and the unauthorized subsets have not control c_i so can not recover secret h without control c_i).

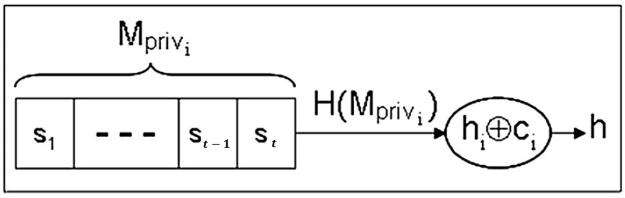

Fig. 1 Secret recovery by combination of private and public information

2.2 Secret recovery

Suppose an authorized subset A_i contains $p_1, p_2, \ldots, p_t$ participants. These participants can recover the secret h with combining their shadows (see Fig. 1).

1. Obtain the public information
2. $H(s_1||s_2||...||s_t) = h_i$ *and* $h_i \oplus c_i = h$

3 Set up a verifiable scheme for general access structure

Let f and g be cryptographic hash functions. The dealer generates shadows $s_1, s_2, ..., s_n$, and distributes the shadow to each participant and then publishes the hashes (by hash function g) of each shadow as commitments: $g_1, g_2, \ldots, g_n$. Participant i verifies his or her shadow by checking if $g(s_i) = g_i$ holds. If all participants confirm that taking his or her shadow as input to the hash function g, he or she gets the hash value equal to one of the commitments published by the dealer, we conclude the dealer sends out consistent shadows. Likewise, when the participants return their shadows, the dealer can verify the secret in the same way.

Hash function g is used to make the scheme verifiable. Hash function f is used as H in Chum and Zhang scheme. Partial information was given out here, however, if g is preimage resistant, it would be infeasible to find the original shadow s_i from g_i. Participant i can fool the party if he or she can find s'_i such that $g(s_i) = g(s'_i) = g_i$. However, this is also extremely difficult to achieve if g is second preimage resistant [5].

4 Multi-secret scheme

In a multi-secret scheme [4], r secrets $h_1, h_2, \ldots, h_r$ are to be shared by the dealer among n participants $p_1, p_2, \ldots, p_n$ and any authorized subset can be reconstruct all secrets according to multiple public controls. Setup and secret recovery phases of this scheme are as follows:

4.1 Setup phase

Suppose dealer want to share the r secrets $h_1, h_2, \dots, h_r$ among n participant $p_1, p_2, \dots, p_n$. Dealer randomly generates n shadows $s_1, s_2, \dots, s_n$, then sends these shadows to $p_1, p_2, \dots, p_n$ participants through secure channel. After computing all minimal authorized subsets and computes values of
$hv_i = H(M_{priv_i})$, $i = 1, 2, ..., w$, $c_{ij} = hv_i \oplus h_j$, $i = 1, 2, \dots, w$, $j = 1, 2, \dots, r$.

4.2 Secret recovery phase

When the participants of a minimal authorized subset $A_i = \{p_1, p_2, \dots, p_t\}$ pool their shadows together, they can compute $hv_i = H(M_{priv_i})$ and achieve c_{ij} from public control area. Therefore, they can recover secrets $h_1, h_2, \dots, h_r$.

5 Security Analysis the functionalities of two schemes

In this section, we analyze 6 functionalities [13] of table 1 shows the results Chum and Zhang scheme and verifiable scheme.

functionality	Shamir scheme	Chum and Zhang scheme	Verifiable scheme	Multi-Secret scheme
1	No	No	No	No
2	No	No	Yes	No
3	No	No	No	No
4	No	No	No	Yes
5	No	No	No	No
6	No	No	No	No

Table 1 Performance features [13]

Functionality 1: Resist cheating by the dealer D
Functionality 2: Resist cheating by dishonest participants p_i
Functionality 3: Without secret channel
Functionality 4: Reconstruct multi-secrets parallelly
Functionality 5: Reuse of the secret shadows
Functionality 6: Reuse of the secret shadows for multiple rounds of sharing even with different dealers

5.1 Analysis of the Chum and Zhang scheme

1. Generate randomly the shadows by dealer and there is no control against this cheating in any phase. So, a dealer can first generate shadows and calculate
$H(M_{priv_i}) = h_i,\ i = 1, \dots, w,\ c_i = h_i \oplus h,\ i = 1, \dots, w,$

After this calculations, he or she can generates a fake shadow s'_i for participant p_i. Now, since there are no control for checking the equality of generated and sent shadows, the dealer can easily cheat without being detected.

2. In secret recovery phase, participant p_i can cheat by sending a fake shadow easily without being detected and main the secret would not recovered.
3. The randomly generated shadows by dealer in setup phase, sent for participant through secure channel.
4. In this scheme, only one secret can be reconstructed.
5. Whereas dealer generates shadows and knows all of the shadows of participant. Also in secret recovery phase, participants in an authorized subset pool their shadows together for secret recovery and leaked shadows of the authorized subset. So, the shadows are not reusable.
6. Whereas shadows and secret by dealer be generate, and according to explanations 5, the shadows is not reusable. Unless, in secret recovery phase the shadows still remain secret (hidden). In this case, shadows can be reused by changing the dealer. Because with fixed shadows and secret, public control also will remain fixed and similar to previous secret recovery phase, the secret be reconstructed (in this case, even by changing the main secret, shadows can be reused. For this, only the value of public control will be changed).

5.2 Analysis of the verifiable scheme

1. In this scheme, in final step, the dealer generates public controls using obtained hv_i from correct shadows and secret h. But, the dealer generates fake public controls to special minimal authorized subsets for publication. Now, since is no control for published values of public controls, the dealer can be cheat easily without detected.
2. In secret recovery phase, the participant(s) can be find a fake shadow s'_i such that $g(s'_i) = g_i$. So, he or she can cheat easily without being detected and the main secret would not recovered. Now, because g is preimage resistant, it would be infeasible to find a fake shadow s'_i such that $g(s_i) = g(s'_i) = g_i$.
3. In setup phase, the shadows generated by the dealer, must be sent for participants through a secure channel.
4. In this scheme, only one secret h can be reconstructed.
5. Like part 5 of Chum's and Zhang's scheme.
6. Like part 6 of Chum's and Zhang's scheme.

5.3 Analysis of the multi-secret scheme

1. Whereas dealer generates shadows $s_1, s_2, \ldots, s_n$, he can generate a fake shadow s'_i and send it for participant p_i after the calculation $H(M_{priv_i}) =$

$h_i,\ i = 1, \ldots, w$ and $c_{ij} = h_i \oplus h,\ i = 1, \ldots, w,\ j = 1, \ldots, r$. In this case, in secret recovery phase, computed h_is will be incorrect. Additionally, indirectly obtained secrets by authorized subset A_i from an another authorized subset A_k, will be incorrect and the secrets indirectly obtained are different for A_i and A_k. So, cheating in the secret sharing can be detected, but it is not clear who is participants or the dealer.

2. In secret recovery phase, a participant can be cheated by presentation a fake shadow, without being detected.
3. In setup phase, the randomly generated shadows by dealer have to be sent to participants through a secure channel.
4. In this scheme, r secrets $h_1, h_2, \ldots, h_r$ can be reconstructed.
5. Similar to part 5 of Chum's and Zhang's scheme.
6. Similar to part 6 of Chum's and Zhang's scheme.

6 Conclusion

The proposed scheme by Shamir and Blakley have drawbacks that the most important of them is cheating by dealer and participant in secret sharing. In this paper, we analyzed proposals of Chum and Zhang based on cryptography hash function and herding hashes technique, verifiable scheme and Multi-Secret scheme, and we investigated 6 functionalities for these schemes. Then we observed these schemes can not eliminate drawbacks in Shamir and Blakley scheme, which in this case also cheating by dealer and participant is not detectable.

References

1. G. Blakley, Safe guarding cryptographic keys, In: Proceedings of the AFIPS 1979 Nalt Conf, AFIPS Press, New York, 313-317 (1979).
2. F. Brandt and T. Sandholm, On the existence of unconditionally privacy-preserving auction protocols, ACM Transactions on Information and System Security (TISSEC), 11(2), Article No. 6, 1-21 (2008).
3. B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, Verifiable secret sharing and achieving simultaneity in the presence of faults, In Foundations of Computer Science, 26th Annual Symposium, 383-395 (1985).
4. C. Chum, and X. Zhang, Implementations of a Hash Function Based Secret Sharing Scheme, Journal of Applied Security Research, 10(4), 525-542 (2015).
5. C. Chum, and X. Zhang, Hash function-based secret sharing scheme designs, Security and Communication Networks, 6(5), 584-592 (2013).
6. R. Cramer, I. Damgård and J.B. Nielsen, Multiparty Computation, an Introduction, In Lecture Notes, 1-83 (2009).
7. P. Feldman, A practical scheme for non-interactive verifiable secret sharing, IEEE Computer Society, In Proceedings of the 28th Annual Symposium on Foundations of Computer Science, Washington, DC, USA.SFCS '87, 427-438 (1987).
8. H. Ge and S. Tate, A direct anonymous attestation scheme for embedded devices, PKC, 4450, LNCS, 16-30 (2007).
9. A. Kiayias and M. Yung, Tree-homomorphic encryption and scalable hierarchical secret-ballot elections, FC 2010, 6052, LNCS, pp. 257-271. (2010).

10. T.P. Pedersen, Non-interactive and information-theoretic secure verifiable secret sharing, In Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '91, London, UK, 129-140 (1992).
11. N. Saxena, G. Tsudik and J. Yic, Threshold cryptography in P2P and MANETs: The case of access control, Computer Networks, 51(12), 3632-3649 (2007).
12. A. Shamir, How to share a secret, Communications of the ACM, 22(11), 612-613 (1979).
13. L. Yanhong, F. Zhang and J. Zhang, Attacks to some verifiable multi-secret sharing schemes and two improved schemes, Information Sciences, 329, 524-539 (2016).