

Research note

# On-line multiple secret sharing based on a one-way function

Hung-Min Sun\*

*Department of Information Management, Chaoyang University of Technology, Wufeng, Taichung County 413, Taiwan*

Received 19 August 1998; accepted 25 January 1999

## Abstract

Based on a one-way function and the intractability of the Diffie–Hellman problem, Pinch proposed a on-line multiple secret sharing protocol which allows the shares to be reused. Ghodosi et al. showed that Pinch’s protocol is vulnerable to cheating. They also proposed a method to prevent the cheating problem in Pinch’s protocol. However, both Pinch’s and Ghodosi et al.’s protocols suffer from the disadvantages of high computation overhead and sequential reconstruction in the secret recovery phase. In this article, we propose a new on-line multiple secret sharing scheme. The security of the proposed scheme is only based on a one-way function, not on other intractable problems. Compared with other well-known schemes, our scheme has the advantages of lower computation overhead and parallel reconstruction in the secret recovery phase. © 1999 Elsevier Science B.V. All rights reserved.

*Keywords:* Secure system; Cryptography; Network security; Secret sharing; One-way function

## 1. Introduction

A secret sharing scheme is a method which allows a secret to be shared among a set of participants in such a way that only *qualified* subsets of participants can recover the secret [1,2]. The collection of subsets of participants that can reconstruct the secret in this way is called *access structure*, denoted by  $\Gamma$ . It is natural to require  $\Gamma$  to be monotone. The basis of  $\Gamma$ , denoted by  $\Gamma_0$ , is the family of all minimal qualified subsets. Based on one-way functions, Cahin [3] proposed a construction for on-line secret sharing with general access structures, with shares as short as the secret, and in which participants may be dynamically added or deleted without having to update the shares of the existing participants. Pinch [4] pointed out that Cachin’s scheme does not allow shares to be reused after the secret has been reconstructed without the help of a trusted computation device or a further distributed computation subprotocol such as that of Goldreich et al. [5]. Based on a one-way function and the intractability of the Diffie–Hellman problem [6], Pinch [4] proposed a modified protocol which allows the shares to be reused. Recently, Ghodosi et al. [7] showed that Pinch’s protocol is vulnerable to cheating. They also proposed a method to prevent cheating problem in Pinch’s protocol. As these both protocols include exponentiation computation, the computation overhead is high. Besides, the secret reconstruction of those must be sequential in the

secret recovery phase. It will be very time-consuming and inconvenient for secret reconstruction. In addition, because the security of both Pinch’s protocol and Ghodosi et al.’s protocol is based on the one-way function and the intractability of the Diffie–Hellman problem [6] (equivalent to the discrete logarithm problem [8]). If the discrete logarithm problem is solved, both these schemes will be insecure.

In this article, we propose a new on-line multiple secret sharing protocol which is only based on a one-way function, not on other intractable problems. Compared with other well-known schemes, our scheme has the advantages of lower computation overhead and parallel reconstruction in the secret recovery phase. This article is organized as follows. In Section 2, we introduce both Pinch’s protocol and Ghodosi et al.’s protocol. In Section 3, we propose and analyze our on-line secret sharing protocol. Finally, we conclude this article in Section 4.

## 2. Review of Pinch’s protocol and Ghodosi et al.’s protocol

In this section, we first introduce both Pinch’s protocol and Ghodosi et al.’s protocol and then propose the disadvantages of these both protocols.

### 2.1. Pinch’s protocol

Let  $f$  be a one-way function with domain  $M$  and range  $G$ , where  $M = \langle M, \cdot \rangle$  is a multiplicative group and  $G = \langle G, + \rangle$

\* Tel.: 886-4-3323000 ext. 7122; fax: 886-4-3742337.  
E-mail address: hmsun@mail.cyut.edu.tw (H.-M. Sun)

is an additive group. For simplicity, we assume that  $G$  is the additive group modulo  $p$ , where  $p$  is a prime number and  $M$  is the multiplicative group to the same modulus. The following protocol is used to share  $m$  secrets  $K^{[h]}$  with access structures  $\Gamma^{[h]}$  for  $h = 1, \dots, m$ .

D1. The dealer randomly chooses  $n$  ‘shares’  $S_1, \dots, S_n$  which are relatively prime to  $p - 1$  and transmits  $S_i$  over a secret channel to the corresponding  $P_i$  for all  $i = 1, \dots, n$ .

D2. For every shared secret  $K^{[h]}$  and for every minimal qualified subset  $X \in I_0^{[h]}$ , the dealer randomly chooses  $g_X^{[h]}$  to be a generator of  $\text{GF}(p)$  and computes  $T_X^{[h]} = K^{[h]} - f((g_X^{[h]})^{\prod_{x:P_x \in X} S_x})$  and publishes  $\mathbf{H}^{[h]} = \{(g_X^{[h]}, T_X^{[h]}) | X \in I_0^{[h]}\}$  on the notice board.

To recover the shared secret  $K^{[h]}$ , a set of participants  $Y \in \Gamma^{[h]}$  proceed as follows:

R1. The members of  $Y$  agree on a minimal qualified subset  $X \subseteq Y$ . Assume that  $X = \{P_1, \dots, P_t\}$ .

R2. Member  $P_1$  reads  $g_X^{[h]}$  from the notice board, computes  $(g_X^{[h]})^{S_1}$  and passes the result to  $P_2$ .

R3. Each subsequent member  $P_i$ , for  $1 < i < t$ , receives  $(g_X^{[h]})^{S_1 \dots S_{i-1}}$ , computes  $(g_X^{[h]})^{S_1 \dots S_i}$  and passes the result to  $P_{i+1}$ .

R4. The final participant  $P_t$  receives  $(g_X^{[h]})^{S_1 \dots S_{t-1}}$  and computes  $V_X^{[h]} = (g_X^{[h]})^{S_1 \dots S_t} = (g_X^{[h]})^{\prod_{x:P_x \in X} S_x}$ .

R5. On behalf of the group  $Y$ , member  $P_t$ , reads  $T_X^{[h]}$  from the notice board and then reconstructs the secret

$$K^{[h]} = T_X^{[h]} + f(V_X^{[h]}).$$

## 2.2. Ghodosi et al.’s protocol

Basically, Ghodosi et al.’s protocol is the same as *Pinch’s protocol*. Ghodosi et al. [7] showed that Pinch’s scheme is vulnerable to cheating as follows. If a dishonest participant  $P_i \in X$  contributes his fake share  $S'_i = \alpha \cdot S_i$ , where  $\alpha$  is a random integer modulo  $(p - 1)$ , only the participant  $P_i$  can calculate the correct value  $V_X^{[h]}$  by  $[(g_X^{[h]})^{S_1 \dots \alpha S_i \dots S_t}]^{\alpha^{-1}} = (g_X^{[h]})^{S_1 \dots S_t} = V_X^{[h]}$  and hence the correct secret as in Pinch’s scheme, while the other participants cannot. Therefore, Ghodosi et al. suggested that the dealer publishes the information  $(g_X^{[h]}, V_X^{[h]})$  (corresponding to every shared secret and every authorized set  $X$ ) on the notice board. Let  $V_X^{[h]*}$  be the final result in Step R4 of the reconstruction phase. Every participant can verify whether  $(g_X^{[h]}, V_X^{[h]}) \stackrel{?}{=} (g_X^{[h]}, V_X^{[h]*})$ . If the verification fails, then cheating has occurred in the protocol and thus the computed secret is not correct.

It is clear that the security of both Pinch’s protocol and Ghodosi et al.’s protocol is based on the one-way function and the intractibility of the Diffie–Hellman problem [6] (equivalent to the discrete logarithm problem [8]). In general, the existence of one-way function is believed.

However, if the discrete logarithm problem is solved, both these schemes will be insecure. Besides, because these protocols include exponentiation computation, the computation overhead is high. In addition, the secret reconstruction in step R3 must be sequential. It will be very time-consuming and inconvenient for secret reconstruction.

## 3. New on-line secret sharing scheme

In this section, we propose and analyze our new on-line secret sharing scheme which is only based on a one-way function, not on other intractable problems.

### 3.1. New on-line secret sharing protocol

We assume that there exists a one-way function,  $f$ , with both domain and range  $G$ . The following protocol is used to share  $m$  secrets  $K^{[h]}$  with access structures  $\Gamma^{[h]}$  for  $h = 1, \dots, m$ .

A1. The dealer randomly chooses  $n$  secret ‘shares’  $S_1, \dots, S_n$  from  $G$  and transmits  $S_i$  over a secret channel to the corresponding  $P_i$  for all  $i = 1, \dots, n$ .

A2. For every shared secret  $K^{[h]}$  and for every minimal qualified subset  $X \in I_0^{[h]}$ , the dealer randomly chooses  $R_X^{[h]}$  in  $G$ , computes

$$T_X^{[h]} = K^{[h]} - \sum_{x:P_x \in X} f(R_X^{[h]} + S_x),$$

and publishes  $\mathbf{H}^{[h]} = \{(R_X^{[h]}, T_X^{[h]}) | X \in I_0^{[h]}\}$  on the notice board.

To recover the shared secret  $K^{[h]}$ , a set of participants  $Y \in \Gamma^{[h]}$  proceed as follows:

B1. The members of  $Y$  agree on a minimal qualified subset  $X \subseteq Y$ . Assume that  $X = \{P_1, \dots, P_t\}$ .

B2. Each member  $P_i$ , for  $1 \leq i \leq t - 1$ , reads  $R_X^{[h]}$  from the notice board, computes  $f(R_X^{[h]} + S_i)$  and sends this result to  $P_t$ . Note that  $P_t$  is the unique member who is responsible for reconstructing the secret.

B3.  $P_t$  reads  $R_X^{[h]}$  and  $T_X^{[h]}$  from the notice board and computes  $f(R_X^{[h]} + S_t)$ .

B4. On behalf of the group  $Y$ , member  $P_t$ , receives  $f(R_X^{[h]} + S_i)$ , for  $1 \leq i \leq t - 1$ , and reconstructs the secret  $K^{[h]} = T_X^{[h]} + \sum_{i=1}^t f(R_X^{[h]} + S_i) = T_X^{[h]} + \sum_{x:P_x \in X} f(R_X^{[h]} + S_x)$ .

Note that once a shared secret is recovered, the secret is assumed to be public and will not be reconstructed again because  $P_t$  has known the secret.

### 3.2. Security analysis of the new protocol

For an adversary who attempts to get the correct secret, he can collect  $f(R_X^{[h]} + S_i)$ , for  $1 \leq i \leq t - 1$ , from the network by Step B2. However, the information is useless to compute  $K^{[h]}$  because  $f(R_X^{[h]} + S_t)$  is unknown. In addition, he cannot

recover any share  $S_i$  from the public information  $R_X^{[h]}$  and  $f(R_X^{[h]} + S_i)$  because  $f$  is a one-way function. Now we consider the case when some secrets have been released. We assume the secret  $K^{[h]}$  is publicly known. Therefore, one can get all  $f(R_X^{[h]} + S_i)$  for  $1 \leq i \leq t$ . However, the information,  $f(R_X^{[h]} + S_i)$ , presented to recover the secret by participant  $P_i$ , is not the same for each shared secret  $K^{[h]}$  and for each minimal qualified subset  $X$ . That is, the information  $f(R_X^{[h]} + S_i)$  is only useful for the specific secret  $K^{[h]}$  and the specific subset  $X$ . Though two different secrets have the same minimal qualified subset  $X$ , the information  $f(R_X^{[h]} + S_i)$  will not be the same one. Thus the information  $f(R_X^{[h]} + S_i)$  is only useful for the secret  $K^{[h]}$ , not for other secrets. It is remarked that the information  $f(R_X^{[h]} + S_i)$  is used only once because a shared secret is reconstructed only once.

### 3.3. Computation overhead

Our protocol is based on a one-way function. There were many one-way functions designed in the past, e.g., LFSR [9], MD5 [10], SHA [11], etc. Most of them are based on some simple operations such as permutation, substitution, and XOR. Therefore, the computation of a one-way function is much faster than the exponentiation computation. Hence our protocol is more efficient than other protocols based on the Diffie–Hellman problem.

### 3.4. Parallel reconstruction

In our protocol, the Step B2 can be parallelly proceeded while the Step R3 of Pinch's protocol needs to be proceeded sequentially.

### 3.5. Detection of cheating

Similar to Ghodosi et al.'s protocol, our scheme can also detect the occurrence of cheating by putting some additional authentic information on the notice board. For every shared secret  $K^{[h]}$ , we put  $D^{[h]} = f(K^{[h]})$  on the notice board. Anyone can verify its correctness of the computed secret,  $\bar{K}^{[h]}$ , by testing  $f(\bar{K}^{[h]}) \stackrel{?}{=} D^{[h]}$ .

### 3.6. Detection of cheaters

In addition to detecting cheating, our scheme can also detect the cheaters accurately. For every shared secret  $K^{[h]}$ , for every minimal qualified subset  $X \in \Gamma_0^{[h]}$ , and for every participant  $P_i \in X$ , we put  $C_{X,i}^{[h]} = f(f(R_X^{[h]} + S_i))$  on the notice board. Once the computed secret is not correct, anyone can verify its correctness of the information  $f(R_X^{[h]} + S_i)$  which is presented by  $P_i$ , by testing  $f(f(R_X^{[h]} + S_i)) \stackrel{?}{=} C_{X,i}^{[h]}$ . Thus, cheaters can be identified.

### 3.7. On-line property

Here, we consider how to add participants, to delete participants, to update access structures, and to renew the shared

secrets in our protocol. In many situations, the participants of a secret sharing scheme will not remain the same during the entire life-time of the secret. The access structure itself may change, too, if it is adapted to the new configuration of participants. Similar to the monotonicity of the access structure, we assume that the changes to the access structure are monotone, i.e. participants are only added and qualified subsets remain qualified. We assume that some participants and some access structures need to be added. The dealer needs only to distribute the shares to the new participants and update the information of bulletin board as in Steps A1 and A2 of our protocol. The previously issued shares are still valid and no shares have to be transmitted. When some participants or some access structures need to be deleted, the shared secrets should be renewed for the reason of security. Therefore the dealer only needs to update the information of bulletin board as in Step A2 of our protocol. The shares remain unchanged.

## 4. Conclusions

In this article, we propose an efficient protocol for on-line multiple secret sharing which is only based on the one-way function, not on other intractable problems. Our scheme is able to detect cheating and, moreover, to detect cheaters correctly. Compared with other well-known schemes, our scheme provides the advantages of lower computation overhead and parallel reconstruction in the secret recovery phase.

## Acknowledgements

This work was supported in part by the National Science Council, Taiwan, under contract NSC-87-2213-E-324-003.

## References

- [1] M. Ito, A. Saito, T. Nishizeki, Secret sharing scheme realizing general access structure, Proc. IEEE Globecom'87, Tokyo, 1987, pp. 99–102.
- [2] E.F. Brickell, D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, Journal of Cryptology 5 (1992) 153–166.
- [3] C. Cachin, On-line secret sharing, in: C. Boyd (Ed.), Cryptography and Coding, Lecture Notes in Computer Science, 1025 (1995) 190–198.
- [4] R.G.E. Pinch, Online multiple secret sharing, Electronics Letters 32 (12) (1996) 1087–1088.
- [5] O. Goldreich, S. Micali, A. Wigderson, How to play any mental game or a completeness theorem for protocols with honest majority, Proc. 19th Annual Symp. Theory of Computing (STOC), 1987, pp. 218–229.
- [6] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Info. Theory IT-22 (1976) 644–654.
- [7] H. Ghodosi, J. Pieprzyk, G.R. Chaudhry, J. Seberry, How to prevent

- cheating in Pinch's scheme, *Electronics Letters* 33 (17) (1997) 1453–1454.
- [8] U.M. Maurer, Towards the equivalence of breaking the Diffie–Hellman protocol and discrete logarithms, in: Y.G. Desmedt (Ed.), *Advances in Cryptography—Crypto'94*, Lecture Notes in Computer Science, 839 (1994) 271–281.
- [9] S.W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, CA, 1967.
- [10] B. Chneier, One-way hash functions, *Dr. Dobbs's Journal* 16 (9) (1991) 148–151.
- [11] National Institute of Standards and Technology, NIST FIPS PUB 186, Digital signature standard, U.S. Department of Commerce, May, 1994.