

Short Paper

New Multistage Secret Sharing Scheme Based on the Factorization Problem

NARN-YIH LEE AND TZONELIH HWANG*

*Applied English Department
Southern Taiwan University of Technology
Tainan, Taiwan 710, R.O.C.*

**Institute of Information Engineering
National Cheng-Kung University
Tainan, Taiwan 701, R.O.C.*

E-mail: hwangtl@server2.iie.ncku.edu.tw

An efficient multistage (t, n) secret sharing scheme is proposed. The scheme allows a group of users to share multiple secrets, and only one secret share needs to be kept by each user. Knowing the exposed secrets will not affect the security of the other secrets not yet revealed. Moreover, only one public value is needed in the proposed scheme.

Keywords: cryptography, data privacy, secret sharing, factorization problem, Lagrange interpolation polynomial

1. INTRODUCTION

A (t, n) secret sharing scheme [1, 2] allows a secret to be shared among n users in such a way that only t or more users can reconstruct the secret, but any $t - 1$ or less users have absolutely no information about the secret. One common drawback of almost all known secret sharing schemes is that they are one-time schemes. That is, once any t or more users reconstruct the secret by pooling their shares, both the secret and all shares become known to everyone within the group and everyone else. Thus, each share kept by each user can be used to reconstruct only one secret. However, if many different secrets have to be shared among the group of users, a straightforward method is to apply the secret sharing scheme repeatedly. In this case, each user has to keep many secret shares, which is very inefficient.

In 1994, He and Dawson proposed a multistage (t, n) secret sharing (MSS) scheme [3] based on a one-way function to solve this problem. For k secrets to be shared among n users, only one secret share has to be kept by each user. The share is the same size as any single secret. These k secrets can be reconstructed one by one in a predetermined order, and revelation of the secrets at earlier stages will not compromise the security of

Received October 14, 1998; revised February 9, 1999; accepted May 21, 1999.
Communicated by Chi Sung Laih.

the remaining secrets. However, kn public values are required in the He-Dawson scheme. Recently, Harn [4] proposed an alternative scheme for solving the same problem with only $k(n-t)$ public values.

In this paper, a new multistage (t, n) secret sharing scheme based on the factoring problem will be proposed. With the new scheme, each user has to keep only one secret share, and only one public value is required in the system. In the following, we will briefly review Harn's scheme [4] first. Then, the proposed scheme will be presented in Section 3. Finally, a concluding remark will be given in Section 4.

2. REVIEW OF HARN'S SCHEME

Let $H: Z_p \rightarrow Z_p$ be a one-way function, where P is a fixed odd prime. $H^j(x)$ denotes j successive applications of $H()$ to x , i.e., $H^0(x) = x$ and $H^j(x) = H(H^{j-1}(x))$. A share distribution center (SDC) randomly chooses some integers, x_i and y_i for $i = 1, 2, \dots, n$ as the users' public values and secret values, respectively. Then, SDC performs the following steps, for $j = 0, 1, \dots, k-1$.

1. Compute $H^j(y_i)$, for $i = 1, 2, \dots, n$.
2. Reconstruct an $(n-1)$ th degree Lagrange interpolation polynomial $f_j(x)$ which passes through $(x_i, H^j(y_i))$ for $i = 1, 2, \dots, n$, and $f_j(0) = s_j$ is the j th stage secret to be shared among users.
3. Compute $(n-t)$ public values as $f_j(m)$, for $m = 1, 2, \dots, n-t$.

SDC sends y_i privately to user i , for $i = 1, 2, \dots, n$, and publishes all the public values. The k secrets should be reconstructed in the following order: $s_{k-1}, s_{k-2}, \dots, s_1, s_0$. When trying to reconstruct the secret s_j , the user i should submit his/her $(j+1)$ th secret share $H^j(y_i)$. With the knowledge of t secret shares and $(n-t)$ additional public shares, $f_j(m)$, for $m = 1, 2, \dots, n-t$, a unique Lagrange interpolation polynomial $f_j(x)$ can be determined, and the secret $f_j(0) = s_j$ can be obtained.

3. THE PROPOSED SCHEME

Harn [7], in 1995, proposed a new multiple secrets sharing scheme based on the difficulty of solving the discrete logarithm problem. Our scheme uses a similar concept to develop a new multistage secret sharing scheme, but the security of our scheme is based on the factorization problem. The new multistage secrets sharing scheme is described below. SDC is assumed to determine the parameters of the system and to distribute secret shares to each user.

Phase 1: Group secrets and secret share generation phase.

SDC selects $N = p \cdot q$, $p = 2p' + 1$ and $q = 2q' + 1$, where p, q, p', q' are large primes, and defines $\lambda(N) = 2p'q'$. Let α be a primitive element in both $GF(p)$ and $GF(q)$, and let $L (\approx 10^{50})$ be a random number with $GCD(L, \lambda(N)) = 1$. Both N and L are public, while $p,$

q, p', q' and $\lambda(N)$ are kept secret.

Theorem 1. Let α be a primitive element modulo V , where V is an integer, $V > 1$. Then, α^L is a primitive element modulo V if and only if $GCD(L, \phi(V)) = 1$ [5].

By Theorem 1, if α is a primitive element in both $GF(p)$ and $GF(q)$, then $\alpha^L, \alpha^{L^2}, \alpha^{L^3}, \dots, \alpha^{L^{k-1}}$ are primitive elements, too. These k secrets, to be shared by the users, are determined by

$$S_i = \alpha^{dL^i} \text{ mod } N, \text{ for } i = 0, 1, \dots, k - 1,$$

where d is a random number such that $GCD(d, \lambda(N)) = 1$ (so d is odd).

Let $A(|A| = n)$ be the set of all users in the system. SDC randomly chooses a secret polynomial $f(x)$ modulo $\lambda(N)$ of degree $t - 1$ and $f(0) = d$. SDC distributes to each user $i, i \in A$, a public odd integer x_i with an even $f(x_i)$ (See [6] for a more detailed description), and a secret value $K_i = \alpha^{S_i} \text{ mod } N$, where

$$s_i = \frac{f(x_i)/2}{\prod_{\substack{j \in A \\ j \neq i}} (x_i - x_j)/2} \text{ (mod } p'q').$$

These k secrets will be reconstructed one by one in the following order: $S_{k-1}, S_{k-2}, \dots, S_0$. SDC can be revoked after issuing these secrets.

Phase 2: Group secret reconstruction phase.

Let B be any subset of size t in A . To reconstruct the $(l + 1)$ th secret $S_l, l \in [0, k-1]$, each user $i, i \in B$, has to compute

$$K_{i,l} = K_i^{L^l \cdot \prod_{\substack{j \in A \\ j \in B \\ j \neq i}} (x_i - x_j) \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j)} \text{ mod } N.$$

Then, S_l can be derived as

$$\begin{aligned} \prod_{i \in B} K_{i,l} &= \prod_{i \in B} K_i^{L^l \cdot \prod_{\substack{j \in A \\ j \in B \\ j \neq i}} (x_i - x_j) \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j)} \text{ mod } N \\ &= \alpha^{\sum_{i \in B} s_i \cdot L^l \cdot \prod_{\substack{j \in A \\ j \in B \\ j \neq i}} (x_i - x_j) \prod_{\substack{j \in B \\ j \neq i}} (0 - x_j)} \text{ mod } N \\ &= \alpha^{f(0) \cdot L^l} \text{ mod } N \\ &= \alpha^{d \cdot L^l} \text{ mod } N \\ &= S_l \text{ mod } N. \end{aligned}$$

Discussion:

1. According to the property of the secret sharing scheme [1], it is impossible to recon-

struct the secret without the knowledge of at least t secret shares. Thus, it is very difficult for only $t - 1$ or less users to reconstruct these k secrets.

2. Exposure of the secrets $S_{k-1}, \dots, S_{t+1}, S_t$ will not harm the security of the other secrets, S_{t-1}, \dots, S_1, S_0 , unless one can solve the factoring problem. Since $S_t = S_{t-1}^L \pmod N$, an attacker has to compute $L^{-1} \pmod{\lambda(N)}$ in order to obtain S_{t-1} . However, it is cryptographically infeasible to obtain $L^{-1} \pmod{\lambda(N)}$ if the factors of N are unknown to the attacker.
3. If user i 's secret share $K_{i,t}$,

$$K_{i,t} = K_i^{L^t} \prod_{\substack{j \in A \\ j \in B}}^{(x_i - x_j)} \prod_{\substack{j \in B \\ j \neq i}}^{(0 - x_j)} \pmod N,$$

is revealed to an attacker where the secret S_t is reconstructed, then the attacker may try to determine user i 's secret key K_i or the next secret share $K_{i,t-1}$,

$$K_{i,t-1} = K_i^{L^{t-1}} \prod_{\substack{j \in A \\ j \in B}}^{(x_i - x_j)} \prod_{\substack{j \in B \\ j \neq i}}^{(0 - x_j)} \pmod N.$$

Again, in both cases, the attacker has to factorize N .

4. Since α^{L^l} is a primitive element in both $GF(p)$ and $GF(q)$ and d is a random number, α^{dL^l} could be any element in the reduced residue set modulo N , for $0 \leq l \leq k - 1$. Thus, the probability of deriving d from α^{L^l} and α^{dL^l} is extremely low and can be neglected. (The primitive element α does not need to be published.)
5. Compared with the number of public values in [3] and [4], the new scheme needs only one public value, L .
6. The security of [3] and [4] is based on the difficulty of breaking a one way function; however, the security of the proposed scheme is based on the factorization problem.

Complexity:

Table 1 shows the number of secret values and public values which need to be kept by each user and the system's public values in He-Dawson's scheme, Harn's scheme and our scheme. It can be seen that the proposed scheme outperforms He-Dawson's scheme and Harn's scheme. However, if the threshold value t is equivalent to n in Harn's scheme, then the number of public values in the system in Harn's scheme is less than that in our scheme.

Table 1. The number of user and system parameters.

	User I's secret share	User I's public value	System's public values
He-Dawson [3]	1	1	kn
Harn [4]	1	1	$k(n - t)$
Our scheme	1	1	1

On the other hand, compared to He-Dawson's and Harn's schemes, our scheme requires that more computational work be done in reconstructing the group secrets. This is because none of the users knows the factors, p and q , of N . When the users cooperate to reconstruct the group secrets, they have to deal with large exponent computation on the modular N .

4. CONCLUSIONS

A new multistage (t, n) secret sharing scheme based on the factoring problem has been proposed. Only one secret share needs to be kept by each user, and there is only one public value in our scheme. Compared with the previously proposed schemes [3, 4], the number of public values in the new scheme is reduced. However, the question of how to reduce the computational work required by the newly proposed scheme must be answered future research, and NSC88-2213-E-218-001.

ACKNOWLEDGEMENT

The authors would like to thank the referees for their valuable comments. This work was supported by the National Science Council of Republic of China under contract number NSC85-2213-E006-059.

REFERENCES

1. A. Shamir, "How to share a secret," *Communications of ACM*, Vol. 22, No. 11, 1979, pp. 612-613.
2. G. R. Blakley, "Safeguarding cryptographic keys," in *FIPS Proceedings*, Vol. 48, 1979, pp. 313-317.
3. J. He and E. Dawson, "Multistage secret sharing based on one-way function," *Electronics Letters*, Vol. 30, No. 19, 1994, pp. 1591-1592.
4. L. Harn, "Comment on the multistage secret sharing based on one-way function," *Electronics Letters*, Vol. 31, No. 4, 1995, pp. 262.
5. Kenneth H. Rosen, *Elementary Number Theory and its Applications*, 2nd ed., Addison-Wesley Publishing Company, 1987, pp. 249-298.
6. Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," *Advances in Cryptology – Crypto '91, Proceedings*, Springer Verlag, 1991, pp. 457-469.
7. L. Harn, "Efficient sharing (broadcasting) of multiple secrets," *IEE Proceedings Computers and Digital Techniques*, Vol. 142, No. 3, 1995, pp. 237-240.

Narn-Yih Lee (李南逸) was born in Chiayi, Taiwan, in 1967. He received the B.S. degree in Information Science from Tunghai University in 1990, the M.S. degree in applied mathematics from Chung-Hsing University in 1992 and the Ph.D. degree in Information Engineering from National Cheng-Kung University, Taiwan, in 1996. He is currently an associate professor in the Department of Applied Foreign Languages, Nan-Tai Institute of Technology, Tainan, Taiwan.

Tzonelih Hwang (黃宗立) is currently a professor in the Institute of Information Engineering, National Cheng-Kung University, Tainan, Taiwan. His research interests include coding theory, cryptography and network security. He is a member of IEEE and IACR (International Association for Cryptologic Research).