A GENERALIZED SECRET SHARING SCHEME REALIZING ORDERED ACCESS STRUCTURES

Tzong-Chen Wu[1], *Chih-Yin Lin*[2], *Tzuoh-Yi Lin*[3] *and Jing-Jang Hwang*[4]

[1,3] Department of Information Management,
National Taiwan University of Science and Technology, Taipei, Taiwan 106, R.O.C.
[1]Email: tcwu@cs.ntust.edu.tw; [3]Email: D8709001@mail.ntust.edu.tw
[2,4] Institute of Information Management,
National Chiao Tung University, Hsinchu, Taiwan 300, R.O.C.
[2]Email: lincy@iim.nctu.edu.tw; [4]Email: jjhwang@cc.nctu.edu.tw

ABSTRACT

The authors propose a novel generalized secret sharing scheme that realizes an ordered access structure, in which the participants of a qualified subset can reconstruct the shared secret only if they follow the sequence of share/ subshare presentation specified by the dealer. The security of the proposed scheme is based on the intractability of the discrete logarithm problem and the robustness of the one-way hash function. Besides, the cheating trick by presenting a fake subshare or the violation of the sequence of share/subshare presentation will be effectively identified during secret reconstruction.

1. INTRODUCTION

A secret sharing scheme is a very useful method for safeguarding a secret (for example, a sensitive document or a cryptographic key) among a set of suspicious participants [3, 13]. For doing this, the shared secret is usually divided into several pieces of shares and each participant is assigned a share. Meanwhile, each participant will be grouped into one or several qualified subsets, such that only the participants of a qualified subset can cooperatively reconstruct the shared secret by presenting their shares to each other. With all the qualified subsets regarding the shared secret they form an access structure and the secret sharing scheme that realizes a general access structure is referred to the generalized secret sharing scheme [2, 5, 9, 12].

Almost previously proposed generalized secret sharing schemes provide only the solution that the participants of a qualified subset have order-free sequence for the presentation of shares or subshares. Sometimes, it may require that these participants should follow a seriate order to present their shares or subshares for secret reconstruction. Such restriction for the presentation of shares or subshares could be in compliance the authorization strategy specified by the dealer. The access structure that achieves such requirement is called the ordered access structure. Note that, like previously proposed secret sharing schemes, the shared secret cannot be reconstructed if any one of the participants in the qualified subset is absent during the secret reconstruction phase.

Based on the intractability of the discrete logarithm problem [1, 8] and the robustness of the one-way hash function [7, 11], we shall propose a new generalized secret sharing scheme that can realize an ordered access structure. In the proposed scheme, each participant only holds one single share with fixed size. When the participants of a qualified subset want to reconstruct the shared secret, each of them should follow the predefined seriate order to present a publicly verifiable subshare (generated from his own share) to the subsequent one for secret reconstruction. Cheater identification for secret reconstruction, which has been intensively studied in the literature [4, 6, 10, 14-16], is also considered on the design of the proposed scheme.

2. THE PROPOSED SCHEME

Denote $G = \{u_1, u_2, ..., u_n\}$ as a set of n participants that want to share a secret k, and D as the dealer of k. Let Γ_k be the ordered access structure of k defined by D and Q_i be the i-th qualified subset in Γ_k. For preserving the property of the ordered access structure, any ordered qualified subset Q_i is represented as a sequence, i.e., $< u_{i1}, u_{i2}, ..., u_{im} >$, where each $u_{ij} \in G$. The shared secret k can be reconstructed only if all u_{ij}'s in Q_i honestly present their subshares (derived from their own shares) satisfying the sequence $< u_{i1}, u_{i2}, ..., u_{im} >$ specified by the dealer D.

The proposed scheme is divided into two phases: the preparation phase and the reconstruction phase. In the preparation phase, the dealer D defines system parameters, generates a share for each participant, and generates a check vector and a ticket for each qualified subset in the access structure. The main tasks in the reconstruction phase include generation/verification of subshares and secret reconstruction. Details of these two phases are described as follows.

2.1. Preparation Phase

Initially, the dealer D prepares a noticeboard that is publicly readable to all participants in the system, but only he has the access privilege to update the contents of the noticeboard. After that, D performs the following steps:

Step 1. Define system parameters:
- (1-1). Select two large primes p and q, such that $q \mid (p-1)$.
- (1-2). Select a generator g modulo p with order q.
- (1-3). Publish a one-way hash function h.
- (1-4). Put $\{p, q, g\}$ in the noticeboard.

Step 2. Generate a share $S_j = (s1_j, s2_j)$ for each $u_j \in G$, where $s1_j, s2_j \in Z_q^*$ are randomly chosen, and then send S_j to u_j via a secure channel.

Step 3. For each qualified subset Q_i in Γ_k, generate a check vector V_i and a ticket T_i as follows:
- (3-1). Randomly select an integer $w_{i0} \in Z_q^*$.
- (3-2). Let $(s1_{ij}, s2_{ij})$ be the share for $u_{ij} \in Q_i$. For $j = 1,2,\ldots,m$, compute
$$w_{ij} = w_{i(j-1)} \cdot s1_{ij} + s2_{ij} \bmod q, \quad (1)$$
$$v_{ij} = h(g^{w_{ij}}) \bmod p.$$
- (3-3). Compute $t1_i$ and $t2_i$ as $t1_i = g^{w_{i0}} \bmod p$ and $t2_i = k - g^{w_{im}} \bmod p$.
- (3-4). Denote V_i and T_i by $V_i = (v_{i1}, v_{i2}, \ldots, v_{im})$ and $T_i = (t1_i, t2_i)$, and put V_i and T_i in the noticeboard.

2.2. Secret Reconstruction Phase

Suppose that the participants of the qualified subset $Q_i = < u_{i1}, u_{i2}, \ldots, u_{im} >$ want to reconstruct the secret k and the communication channels among them are noise-free. These participants cooperatively perform the following steps:

Step 1. The first participant u_{i1} gets $t1_i$ from the noticeboard, computes the subshare A_{i1} by $A_{i1} = t1_i^{s1_{i1}} \cdot g^{s2_{i1}} \bmod p$ and then presents it to the subsequent participant u_{i2}.

Step 2. The subsequent participants u_{ij}'s (for $j = 2,3,\ldots, m-1$) do the following tasks in accordance with the sequence $< u_{i2}, \ldots, u_{i(m-1)} >$:
- (2-1). Get $v_{i(j-1)}$ from the noticeboard and verify $A_{i(j-1)}$ by testing if
$$h(A_{i(j-1)}) = v_{i(j-1)} (\bmod p). \quad (2)$$
If the equality fails, then identify $u_{i(j-1)}$ as a cheater and stop this phase.
- (2-2). Compute a subshare
$$A_{ij} = A_{i(j-1)}^{s1_{ij}} \cdot g^{s2_{ij}} \bmod p. \quad (3)$$
Then, present it to the next participant $u_{i(j+1)}$.

Step 3. The last participant u_{im} first verifies $A_{i(m-1)}$ as in Step (2-1), and then computes $A_{im} = A_{i(m-1)}^{s1_{im}} \cdot g^{s2_{im}} \bmod p$ and presents it all the other participants in Q_i.

Step 4. Every participant $u_{ij} \in Q_i - < u_{im} >$ gets v_{im} from the noticeboard and verifies A_{im} as in Step (2-1).

Step 5. Every participant $u_{ij} \in Q_i$ gets $t2_i$ from the noticeboard and reconstructs the shared secret k by computing $k = t2_i + A_{im} \bmod p$.

Note that from Steps 2 to 3, the violation of subshare presentation will be effectively identified, because the subshares A_{ij}'s sequentially presented by the participants of the qualified subset are publicly verifiable. Once the shared secret k has been reconstructed, all these subshares are useless.

Here, we will give a brief sketch to show that the proposed scheme works correctly. By raising both sides of Equation 1 to exponents with base g, it yields the result of Equation 3. Based on the fact that $A_{ij} = g^{w_{ij}} (\bmod p)$, one can easily deduce the correctness of the proposed scheme from Equation 3.

3. SECURITY ANALYSIS

It is believed that solving the discrete logarithm problem (DLP) over GF(p) is computationally infeasible when p is large (e.g., more than 512 bits) [8]. On the other hand, a one-way hash function h is considered robust enough if it produces a large enough output (e.g. at least 128 bits [11]) and has the following properties [7]:

(i) h can be applied to an argument of any size and produces a fixed-size output.
(ii) Given x, it is easy to compute $h(x)$.
(iii) Given $h(x)$, it is computationally infeasible to deter mine x.
(iv) $h(x)$ is collision free, i.e. it is computationally infeasible to find distinct x and y with $h(x) = h(y)$.

The security of the proposed scheme depends on the achievement of the following two issues:

Security issue 1: Under the cryptographic assumption the DLP, any adversary cannot reveal the share held by the participant from its derived subshare.
Analysis:

From Equations 1 and 3, it can be seen that the share $S_{ij} = (s1_{ij}, s2_{ij})$ for $u_{ij} \in Q_i$ is protected by the secret parameters w_{ij}'s chosen by *D*. However, it is computationally infeasible to solve w_{ij}'s form the public check vector V_i or the ticket T_i under the cryptographic assumption of the DLP.

Security issue 2: Under the robustness of a one-way hash function, the cheating trick by pooling a fake subshare will be effectively identified.

Analysis:

From Step (2-1) of the reconstruction phase, it is to see that a fake subshare will be regarded as valid if it can pass the verification check, i.e., Equation 2, performed by the subsequent participant. However, under the assumption of a robust one-way hash function, it is computationally infeasible for an adversary or a malicious participant to find the input value corresponding to a specific output (i.e. the check value v_{ij} in the check vector V_i) from the one-way hash function *h*.

4. CONCLUSIONS

We have addressed a new application for a generalized secret sharing scheme that realizes an ordered access structure, in which the participants of a qualified subset can reconstruct the shared secret only if they present their subshares in a seriate order specified by the dealer in advance. The security of the proposed scheme is based on the intractability of the discrete logarithm problem and the robustness of the one-way hash function. Besides, the proposed scheme provides the solution for identifying the cheating trick by presenting a fake subshare or violating the seriate order of subshare presentation during the secret reconstruction phase.

5. ACKNOWLEDGEMENT

Part of this work is supported by the National Science Council, Republic of China, under the contract number NSC 89-2416-H011-014.

6. REFERENCES

[1] L.M. Adleman and K.S. McCurley, "Open problems in number-theoretic complexity, II", *Proceedings of First Algorithmic Number Theory Symposium (ANTS-I)*, Springer-Verlag, 1994, pp. 291-322

[2] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions", *Advances in Cryptology - CRYPTO '88*, Springer-Verlag, 1988, pp. 27-35.

[3] G.R. Blakley, "Safeguarding cryptographic keys", *Proceedings of American Federation of Information Processing Societies (AFIPS) 1979 National Computer Conference*, Vol. 48, 1979, pp. 313-317.

[4] E.F. Brickell and D.R. Stinson, "The detection of cheaters in threshold schemes", *Advances in Cryptology - CRYPTO '88*, Springer-Verlag, 1988, pp. 564-577.

[5] C. Cachin, "On-line secret sharing", *Proceedings of Cryptography and Coding: 5-th IMA (the Institute of Mathematics and its Applications) Conference*, Springer- Verlag, 1994, pp.190-198.

[6] C.C. Chang and R.J. Hwang, "Efficient cheater identification method for threshold schemes", *IEE Proceedings Computers and Digital Techniques*, Vol. 144, No. 1, 1997, pp. 23-27.

[7] D.W. David and W.L. Price, *Security for computer networks*, Wiley, 1984.

[8] W. Diffie and M.E. Hellman "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, 1976, pp. 644-654.

[9] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure", *Proceedings of IEEE Global Telecommunications Conference: Globecom'87*, IEEE, 1987, pp. 99-102.

[10] H.Y. Lin and L. Ham, "A generalized secret sharing scheme with cheater detection", *Advances in Cryptology - ASIACRYPT'91*, Springer-Verlag, 1991, pp. 22-26.

[11] R.C. Merkle, "One-way hash functions and DES", *Advances in Cryptology: CRYOTO' 88*, Springer-Verleg, 1988, pp. 564-577.

[12] R.G.E. Pinch, "Online multiple secret sharing", *Electronics Letters*, Vol.32, No.12, 1996, pp. 1087-1088.

[13] A. Shamir, "How to share a secret", *Communications of the ACM*, Vol.22, No.11, 1979, pp. 612-613.

[14] K.J. Tan, H.W. Zhu and S.J. Gu, "Cheating identification in (*t*, *n*) threshold scheme", *Computer Communications*, Vol. 22, No. 8, 1999, pp. 762-765.

[15] M. Tompa and H. Woll, "How to share a secret with cheaters", *Journal of Cryptology*, Vol.1. No.1, 1988, pp. 133-138.

[16] T.C. Wu and T.S. Wu, "Cheating detection and cheater identification in secret sharing schemes", *IEE Proceedings Computers and Digital Techniques*, Vol. 142, No. 5, 1995, pp. 367-369.