A Self-healing Key Distribution Scheme with Novel Properties

Biming Tian and Mingxing He
(Corresponding author: Biming Tian)

School of Mathematics & Computer Engineering, Xihua University
Chengdu, Sichuan, 610039, China (Email: bmt003@163.com)

(Received Sep. 28, 2006; revised and accepted Nov. 22, 2006 & Dec. 9, 2006)

Abstract

We improve a secret sharing scheme, which enables users select their personal keys by themselves instead of being distributed by group manager and users can reuse their personal keys no matter the shared secret is renewed or recovered. Then we apply it to design a self-healing key distribution scheme. The new scheme achieves good properties. Firstly, the scheme reduces storage overhead of personal key to a constant. Secondly, the scheme conceals the requirement of a secure channel in setup step. Finally, the long-lived scheme is much more efficient than those in previous schemes.

Keywords: Key distribution, self-healing, secret sharing

1 Introduction

The idea of self-healing key distribution schemes is that users, in a large and dynamic group communication over an unreliable network, can recover lost session keys on their own, even if lost some previous key distribution messages, without requesting additional transmissions from the group manager.

The problem of distributing keys over a reliable channel has received much attention in the past years [4, 5, 9]. A wireless network is an emerging trend in communication technology. It has many unique features. On the one hand, a node in a mobile wireless network may moves in and out of range frequently. On the other hand, devices in mobile wireless network are typically powered by batteries. Thus, traditional key distribution schemes used for reliable channel can not be applied to wireless network directly. Wireless network has widely application, such as military operations, rescue missions, and scientific explorations. Therefore, how to distribute and update the session key efficiently over an unreliable channel has been one of the hot research topics.

The first pioneering work of self-healing key distribution was introduced by Staddon et al. in [12] providing with formal definitions, lower bounds on the resources as well as some constructions. In [7], Liu et al. generalized the above definition and gave some constructions. By introducing a novel personal key distribution technique, Liu et al. reduced communication overhead and storage overhead. In addition, Liu et al. presented two techniques that allow trade-off between the broadcast size and the recoverability of lost session keys. These two methods further reduced broadcast message size in cases where there are frequent but short-term disruptions of communication and where there are long-term but infrequent disruptions of communication, respectively. Blundo et al. in [3] showed an attack that can be applied to the first construction in [12], presented a new mechanism for implementing the self-healing approach, extended the self-healing approach to key distribution, and proposed another key-recovery scheme which enabled a user to recover all lost session keys (for sessions in which he belongs to the group) by using only the current broadcast message. Blundo et al. in [2] started by analyzing definitions proposed in [7, 12] and showed that no protocol can achieve some of the security requirements stated in them. After the analysis, they presented a new definition of self-healing key distribution and concrete schemes. Subsequently, they gave some lower bounds on the resources required for implementing such schemes and proved that some of the bounds are tight. More et al. in [8] used a sliding window to correct the inconsistent robustness in [12]. Sa'ez in [10] first considered applying vector space secret sharing instead of Shamir's secret sharing schemes to self-healing key distribution scheme. All of these papers mainly focused on unconditionally secure schemes.

The rest of the paper is organized as follows. First of all, we introduce a secret sharing scheme and modify it to a simpler version in Section 2. Next, we present a concrete construction in Section 3. The construction follows in part ideas of [3] but considering the particular secret sharing scheme instead of a traditional one. As far as we know, this is the first time to consider this kind of self-healing key distribution schemes. We provide a detail analysis of the proposed scheme and give a brief introduction of long-lived scheme. We make a performance

comparison with some representative schemes in Section 4. Finally, we conclude this paper and point out some future research directions in Section 5.

2 Underlying Secret Sharing Scheme

Threshold secret sharing schemes were independently introduced by Shamir in [11] and Blakley in [1] in 1979. Many variants of them were proposed since then. Further works considered more concrete properties. Hwang and Chwang in [6] provided a method to realize a threshold secret sharing scheme with the novel property that users can select their personal key by themselves instead of being distributed by group manager. In this section, we introduce Hwang and Chwang's secret sharing scheme firstly and present our modification secondly.

2.1 Hwang and Chwang's Scheme

Let p be a large prime. α is a primitive element in $GF(p)$. A group manager is abbreviated to GM and n users $u_1, \ldots, u_n$.

Initialization:

1) $u_i (i = 1, \ldots, n)$ selects $s_i \in_R GF(p)$ as his personal key and computes $p_i = \alpha^{s_i} \bmod p$, sends p_i and his identity over public channel to GM. It is required that $s_i \neq s_j (1 \leq i, j \leq n, i \neq j)$ in the scheme. GM checks the values and requires the users reselect their personal keys if collision happened. The procedure ends when all the personal keys are qualified.

2) GM chooses a random $t-1$ degree polynomial $f(x) \in GF(p)[x]$ which satisfies that $f(0) = k$. k is the secret to be shared. GM randomly choose a point (x_i, y_i) for U_i. The point satisfies $x_i \neq x_j (i \neq j)$ and $y_i = f(x_i)$. GM chooses $r \in_R GF(p) (r \neq s_i)$ and computes $d_i = (y_i - p_i^r) \bmod p$ and $V = \alpha^r \bmod p$.

3) GM publishes the Table 1 and V on public bulletin board and keeps r and y_i secret.

Secret Recovery:
A qualified subset of t users who intend to recover the secret k. Without loss generality, suppose the subset is $\{u_1, \ldots, u_t\}$. $u_i (i - 1, \ldots, t)$ finds out d_i and v and computes $y_i = d_i + V^{s_i} \bmod p$. The t users gather ty_i and associate them with corresponding x_i on public bulletin board and obtain t different points (x_i, y_i) of polynomial $f(x)$. They can recover the $t-1$ degree polynomial $f(x)$ by using Lagrange's interpolation formula, and recover the secret $k = f(0)$.

Table 1: Information x_i and d_i of secret shares

ID_i	x_i	d_i
ID_1	x_1	d_1
$\vdots$	$\vdots$	$\vdots$
ID_n	x_n	d_n

Table 2: Information y_i of secret shares

ID_i	y_i
ID_1	y_1
$\vdots$	$\vdots$
ID_n	y_n

2.2 Improved Hwang and Chwang's Scheme

We reuse the parameters in the primary scheme and impress emphasis on the modifications. Let q be a large prime, $p = 2q + 1$ be a large prime, too. Other parameters are the same as those in the primary scheme Initialization.

1) It is required $p_i \neq p_j (i \leq i, j \leq n, i \neq j)$ in the improved scheme. In fact, GM detects if collision happens by comparing p_i with p_j in the primary scheme. Seen from this point, our constraint is more reasonable. We demand that other operations are the same as the primary scheme in this step.

2) GM chooses a random $t-1$ degree polynomial $f(x) \in GF(p)[x]$ which satisfies that $f(0) = k$. k is the secret to be shared. GM chooses $r \in_R GF(p) (r \neq s_i)$ and r is relatively prime to $p - 1$. Then, GM computes $y_i = f(p_i^r) \bmod p$ and $V = \alpha^r \bmod p$.

3) GM publishes the Table 2 and V on public bulletin board and keeps r secret.

Secret Recovery:
A qualified subset of t users who intend to recover the secret k. Without loss generality, suppose the subset is $\{u_1, \ldots, u_t\}$. $u_i (i = 1, \ldots, t)$ finds out V on public bulletin board and computes $x_i = V^{s_i} \bmod p = (\alpha^r)^{s_i} \bmod p = (\alpha^{s_i})^r \bmod p = p_i^r \bmod p$. The t users gather tx_i and associate them with corresponding y_i on public bulletin board and obtain t points (x_i, y_i) of polynomial $f(x)$. They can recover the $t - 1$ degree polynomial $f(x)$ by using Lagrange's formula, and recover the secret $k = f(0)$.

The Analysis of Performance:

1) Feasibility. In the period of secret recovery, because α is a primitive element in $GF(p)$ and r is relatively prime to $p - 1$, for $i \neq j$, s_i and s_j are selected from $GF(p)$ and $p_i \neq p_j$, we know $x_i = p_i^r \bmod p = \alpha^{rs_i} \bmod p \neq \alpha^{rs_j} \bmod p = p_j^r \bmod p = x_j$, so they have t different points (x_i, y_i) of polynomial $f(x)$. By

using Lagrange's formula, they can recover the secret $k = f(0)$.

2) Security. In the period of initialization, because of the difficulty of solving discrete logarithm problem, anyone can neither get r from public information V and α with the knowledge $V = \alpha^r \bmod p$ nor further compute $x_i = p_i^r \bmod p$. In the period of secret recovery, u_i contributes $x_i = (p_i^r \bmod p) = (V^{s_i} \bmod p)$. Because of the difficulty of solving discrete logarithm problem, nobody can get s_i from public information V and x_i, which is u_i's personal key. That is, u_i's personal key is still secret even if the shared secret is recovered. In addition, p is a prime large enough to guarantee the infeasibility of exhaust searching x, which is relatively prime to $p-1$, and further finding out system parameter r, by comparing V with $\alpha^x \bmod p$.

3) System Updating. If system updating takes place before secret recovery, group manager reselects a $t-1$ degree polynomial $f'(x)$ which satisfies $f'(0) = k'$ and updating the public bulletin board according to $f'(x)$. k' is the secret to be shared. If system updating takes place after secret recovery, group manager should reselects a new parameter r' and computes $V' = \alpha^{r'} \bmod p$ besides the described operations in first situation.

All in all, the improved scheme reduces the public information without loss the security of primary scheme.

3 Self-healing Key Distribution Scheme

3.1 System Parameters

The model we consider in this paper is similar to the one given in [3] which is a slightly modified version of the model in [12].

Let $U = \{u_1, \ldots, u_n\}$ be the finite universe of users. A broadcast unreliable channel is available, and time is defined by a global clock. GM sets up and manages, by means of join and revoke operations, a communication group which is a dynamic subset of users of U. All of our operations take place in $GF(p)$, where both $p = 2q + 1$ and q are large primes. Suppose α is a primitive element in $GF(p)$. m denotes the number of sessions and t denotes the maximum number of user that can be revoked by GM. Let $G_j \subset U$ be the communication group established by the group manager in session j. Each user $U_i \in G_j$ holds a personal key $s_i \in GF(p)$. s_i is used to recover the session keys as long as user u_i is not removed by GM from the group. Different from the previous self-healing schemes, s_i is selected by user himself before or when joining G_j instead of being distributed by GM. Let $R_j \subset G_{j-1}$ denotes the set of revoked group users in session j and $J_j \subset U \setminus J_{j-1}$ denotes the set of users who join the group in session j with $R_j \cap J_j = \Phi$. Hence, $G_j = (G_{j-1} \cup J_j) \setminus R_j$ for $j \geq 2$ and by definition $G_1 = U$. $|G_j|$ denotes the number of user in session j. Moreover, for $j \in \{1, \ldots, m\}$, the session key K_j is randomly chosen by GM from $GF(p)$ and according to uniform distribution. For any non-revoked user $u_i \in G_j$, the j-th session key K_j is determined by broadcast information B_j and personal key s_i.

Given a subset of users $G = \{i_1, \ldots, i_g\} \subset U$, with $i_1 < \ldots < i_g$, we denote X_G as the random variables $X_{i_1}, \ldots, X_{i_g}$. For instance S_R denotes the personal keys of all users in $R \subset U$.

3.2 Concrete Construction

In this subsection, we apply improved secret sharing scheme to self-healing key distribution scheme.

Setup:

1) $u_i \in G_1$ selects $s_i \in_R GF(p)$ as his personal key and computes his masking key $p_i = \alpha^{s_i} \bmod p$, sends p_i and ID_i over public channel to GM. It is required that $p_i \neq P_j (1 \leq i, j \leq n, i \neq j)$ in the scheme. GM checks the validity of users and requires each user whose masking key is p_i reselect his personal key if collision happened (Because p is a large enough prime and s_i is selected randomly and independently in $GF(p)$, the probability of collision can be negligible, That is, the requirement is reasonable). The procedure ends when all the personal keys are qualified.

2) GM chooses, independently and uniformly, m polynomials of degree t, say $f_1(x), \ldots, f_m(x) \subset GF(p)[x]$, and m session keys $K_1, \ldots, K_m \subset GF(p)$. For each session $j = 1, \ldots, m$, defines $z_j = K_j + f_j(0)$.

Broadcast:

1) Let P_{G_j} denote the masking keys of the users in G_j. In session j, GM randomly chooses $r_j \in GF(p)$, r_j is relatively prime to $p-1$ and $(\alpha^{r_j} \bmod p) \notin P_{G_1}, \ldots, P_{G_j}$. For $i = 1, \ldots, |G_j|$, GM computes: $y_i^j = f_j(P_i^{r_j}) \bmod p$ and $V_j = \alpha^{r_j} \bmod p$, then publish Table 3 and V_j on public bulletin board.

2) GM chooses a set of values(different from 0)$W_j = \{\omega_1^j, \ldots, \omega_t^j\}$, such that the masking keys of the users in R, denoted by the set P_R, are contained in W, i.e.,$P_R \subseteq W_j$ and $P_{G_j} \cap W_j = \Phi$. GM publishes Table 4 on public bulletin board and broadcasts a message $B_j =< z_1, \ldots, z_j >$.

Key computation:

1) According to V_j and his secret key, user u_i computes $P_i^{r_j} \bmod p = V_j^{s_i} \bmod p$ and associates it with information on public bulletin board, he owns $t+1$ points, $< ((\omega_1^j)^{r_j}, f_j((\omega_1^j)^{r_j} \bmod p), \ldots, ((\omega_t^j)^{r_j}, f_j((\omega_t^j)^{r_j}) \bmod p), (p_i^{r_j}, y_i^j) >$ of $f_j(x)$.

Table 3: Personal keys information of users in session j

ID_i	y_i^j
ID_1	y_1^j
$\vdots$	$\vdots$
$ID_{\lvert G_j\rvert}$	$y_{\lvert G_j\rvert}^j$

Table 4: Information of revoked users

$(\omega_i^j)^{r_j}$	$f_j((\omega_i^j)^{r_j}) \bmod p$
$(\omega_1^j)^{r_j}$	$f_j((\omega_1^j)^{r_j}) \bmod p$
$\vdots$	$\vdots$
$(\omega_t^j)^{r_j}$	$f_j((\omega_t^j)^{r_j}) \bmod p$

2) User recovers polynomial $f_j(x)$ by applying Lagrange's interpolation formula to $t+1$ different points, further recover the secret $f_j(0)$.

3) User computes K_j by subtracts $f_j(0)$ from z_j.

Add and revoke group members:

1) A new user u_i can join the communication group starting from session j, he selects $s_i \in_R GF(p)$ as his secret key and computes $p_i = \alpha^{s_i}$, sends p_i and ID_i over public channel to GM. GM checks the validity of ID_i an requires each user whose masking key is p_i reselects his personal key if collision happened. Note that GM adds p_i to P_R in the following sessions for the sake of security. Otherwise, u_i can be accepted as a qualified group user if no collision happens.

2) If a user is revoked in session j, the pair $(p_i^{r_j}, f_j(p_i^{r_j}) \bmod p)$ must be published on public bulletin board in the following sessions. If a revoked user wants to rejoin the later session, he must submit a new identity and personal key to GM. That is, one user can be seen as two in this situation. The scheme allows for revoking up to t users from the group.

3.3 Analysis of Security

This section we show that our construction realizes a self-healing key distribution scheme with revocation capability.

1) a. Session key recovery by a user is described in Key computation step of the construction.

   b. On the one hand, since the session keys are chosen according to the uniform distribution and independent of the personal keys, it is straightforward to see that the personal keys alone do not give any information about any session key. On the other hand, it is not difficult to see that every z, for $j = 1, \ldots, m$, perfectly hides key K_j because $z_j = K_j + f_j(0)$.The set of session keys can not be determined by broadcast messages alone.

2) Suppose that a collection R of t revoked group members in session j collude. The coalition of R can count on at most t points on $f_j(x)$. In order to recover the session key K_j from the broadcast, revoked users in R must compute $f_j(0)$. Combine an arbitrary point with the t points on $f_j(x)$, they can interpolate a different polynomial. Thus, K_j is completely safe.

3) a. For any u_i that is a member in session r and $s(1 \le r < s \le m)$, he can recover $< f_r(0), \ldots, f_s(0) >$. By the method of key computation step in previous construction, u_i can subsequently recover the whole sequence of session keys $K_r, \ldots, K_s$. In fact, in our construction, a qualified user can recover the all the session key before session s. This is a stronger self-healing scheme.

   b. Because the coalition of $C \cup D$ can count on at most t points on $f_j(x)$, for any $r < j \le s$. Hence, session keys K_j are completely safe with respect to joint coalition of size at most t of new and revoked users.

3.4 Long-lived Scheme

After a set of sessions has expired in Construction 3 and Construction 4 in [12], some rekeying of the users is necessary before distributing new session keys. The reason is that the state of the system has changed as a result of the broadcasts. A straightforward method is distributing a new personal key to each user over a reliable channel, and proceeding as before. It is too trivial and expensive to realize. Another solution was described in [12]. Staddon et al. set up computationally secure long-lived protocols by moving all interpolations to the exponent. However, the construction has two problems. Scheme 4 given in [3], along the same lines of [12], modifies the construction to solve one of problems, while the other seems to be an interesting open problem.

The problem lies in the join operation in presence of new users. It seems difficult to slightly modify Construction 5 given in [12] and Scheme 4 given in [3] in order to enable a secure join. Furthermore, the cost of modular exponentiations involved may be prohibitive. It is expectant to look for other alternatives.

In our scheme, because of the randomness of $r_j (j = 1, \ldots, m)$, personal key can be used repeatedly. Before the starting of the next m sessions, only user, who revoked in previous m sessions and will join the next m sessions, reselects his personal key and submit it to the group manager to verify its validity. There are no requirements of secure channels between users and the group manager and interpolations in the exponent. As far as we know, this is the best way to extend the lifetime of personal key. The operations what the group manager should do the same as before in broadcast period. Comparing with previous schemes, our long-lived scheme is more feasible and more efficient.

Table 5: Performance comparison

methods	Storage	communication	security
S3 of [3]	$(m-j+1)\log p$	$(tj+j)\log p$	Unconditionally
Our scheme	$\log p$	$(tj+j)\log p$	Computationally
S4 of [3]	$m\log p$	$(m+2tj+j)\log p$	Computationally
long-lived scheme	$\log p$	$(tj+j)\log p$	Computationally

4 Efficiency Comparison with Previous Schemes

The most prominent property of our scheme is that storage complexity reduces to a constant. In previous schemes, storage overhead comes from the personal key that each group user has to keep, which is determined by the number of masking polynomials [7]. In an unconditionally secure self-healing key distribution scheme, with respect to Theorem 5.2 in [3], every user who belongs to G_j has to store a personal key of at least $(m-j+1)\log p$ bits. In our scheme, every user stores a personal key of size $\log p$ bits. Another remarkable property is that personal key can be reused to next m sessions with out any alternation. We should point out that the efficiency improvements are obtained by relaxing the security slightly. One shortcoming of our construction is that a user should do a little more computation than the former schemes. Fortunately, as far as the computation ability of current wireless networks is concerned, the little more increase is acceptable.

We make a performance comparison of our scheme and some schemes in [3]. See Table 5 for detail information.

5 Conclusions

In this paper, we made a brief introduction of Hwang and Chwang's secret sharing scheme in [6] firstly and gave a modification version of it secondly. The most prominent property of the original scheme is that user can select his personal key by himself instead of being distributed by group manager. The improved scheme kept the properties of the original paper all the same and decreased storage overhead greatly. By introducing the novel secret sharing scheme, we developed an efficient computationally secure self-healing group key distribution scheme. New scheme reduced the storage overhead to a constant. To the best of our knowledge, this is the first time to realize constant length of personal key storage overhead. Comparing with the previous schemes, there was slightly decrease in communication overhead in the proposed scheme and threshold scheme in [10] can be adopted to further reduce communication overhead. In addition, after a set of sessions have expired, the construction of extending lifetime is much more efficient than those in previous schemes. We should point out that the efficiency improvements are obtained by relaxing the security slightly. We will explore other ways to realize unconditionally secure self-healing key distribution scheme with the novel properties of our scheme. In addition, we will devote to develop a model that characterizes failures in large and highly mobile wireless networks and further investigate the performance of the proposed schemes in this model.

Acknowledgments

This work is support by the National Natural Science Foundation of China under Grant no. 60473030 and the Foundation of Science & Technology Agency of Sichuan Province under Grant no. 05JY029-131.

References

[1] G. Blakley, "Safeguarding cryptographic keys," in *Proceedings of AFIPS 1979 National Computer Conference*, vol. 48, pp. 313-317, 1979.

[2] C. Blundo, P. D'Arco, A. D. Santis, and M. Listo, "Definitions and Bounds for Self-Healing Key Distribution," in *Proceedings of the 31st International Colloquium on Automata, Languages and Programming (ICALP'04)*, LNCS 3142, pp. 234-245, Springer-Verlag, 2004.

[3] C. Blundo, P. D'Arco, A. Santis, and M. Listo, "Design of self-healing key distribution schemes," *Design Codes and Cryptography*, no. 32, pp. 15-44, 2004.

[4] C. Blundo, L. F. Mattos, and D. Stinson, "Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution," in *Crypto'96*, LNCS 1109, pp. 387-400, 1996.

[5] R. Canetti, T. Malkin, and K. Nissim, "Efficient communication-storage tradeoffs for multicast encryption," in *Eurocrypt'99*, LNCS 1592, pp. 459-474, 1999.

[6] S. J. Hwang, C. C. Chang, and W. P. Yang, "An Efficient Dynamic Threshold Scheme," *IEICE Transactions Information System*, vol. E79-D, no. 7, pp. 936-941, 1996.

[7] D. Liu, P. Ning, and K. Sun, "Efficient self-healing key distribution with revocation capability," in *Proceedings of the 10th ACM Conference on Computer and Communication Security*, pp. 231-240, Washington, DC, USA, 2003.

[8] S. M. More, M. Malkin, J. Staddon, and D.Balfanz, "Sliding window self-healing key distribution with revocation," in *ACM Workshop on Survivable and Self-*

Regenerative Systems, pp. 82-90, New York, USA, 2003.

[9] A. Perrig, D. Song, and J. D. Tygar, "ELK, a new protocol for efficient large-group key distribution," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 247-262, 2001.

[10] G. Sa'ez, "On threshold self-healing key distribution schemes," in *Cryptography and Coding*, LNCS 3796, pp. 340-354, 2005.

[11] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.

[12] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, "Self-healing key distribution with revocation," in *Proceedings IEEE Symposium on Security and Privacy*, pp. 224-240, 2002.

Biming Tian is currently working toward the MS degree in the School of Mathematics & Computer Engineering, Xihua University. She received her B.S degree in computer science from Henan University in 2004. Her current research interest is key management.

Mingxing He received his M. S. degree in applied mathematics from Chongqing University in 1990 and Ph. D. degree in information engineering from Southwest Jiaotong University in 1993, respectively. From 2002 to 2003 he was a research staff at the Department of Information and Communication Systems of Hagen University, Germany. He is now a professor and vice dean with the School of Mathematics and Computer Engineering, Xihua University, P. R. China. His current research interests include cryptography and network security. He is a member of the International Association for Cryptologic Research (IACR). He has served on the program committees of numerous conferences and workshops.