Cryptanalysis of an Improved One-Way Hash Chain Self-Healing Group Key Distribution Scheme

Yandong Zheng[1], Hua Guo[1] *

[1] State Key Laboratory of Software Development Environment, Beihang University

Beijing 100191, China

Email: hguo@buaa.edu.cn

Abstract

In 2014, Chen *et al.* proposed a one-way hash self-healing group key distribution scheme for resource-constrained wireless networks in Journal of Sensors (14(14):24358-24380, DOI: 10.3390/s141224358). They asserted that their scheme 2 has the constant storage overhead, low communication overhead, and is secure, i.e., achieves mt-revocation capability, mt-wise forward secrecy, any-wise backward secrecy and has mt-wise collusion attack resistance capability. Unfortunately, an attack method against Chen *et al.*'s scheme 2 is found in this paper, which contributes to some security flaws. More precisely, a revoked user can recover other legitimate users' personal secrets, which directly breaks the forward security, mt-revocation capability and mt-wise collusion attack resistance capability. Thus, Chen *et al.*'s scheme 2 is insecure.

Keywords: self-healing group key distribution, forward security, backward secrecy, collusion attack.

1 Introduction

In secure group communications, the group manager (GM) distributes a common cryptographic key to the group members. Therefore, key management including secure key distribution and key updating becomes a vital problem under unreliable networks. In an unreliable network, a user might not receive the session key distribution broadcast in some sessions. Each of such users will communicate with the GM and require GM to retransmit the lost broadcast messages, which would aggravate the burden of the traffic on the network. The group key distribution scheme with self-healing mechanism succeeds to solve the problem for an unreliable network, which is resistant to packet loss. Generally speaking, a user is able to recover session keys even if he doesn't receive the corresponding broadcast messages because of packet loss. More specifically, users are able to recover the lost session keys by combining a previous broadcast with a subsequent one without requesting anything to the GM if they lose some broadcast messages. Besides, the group key distribution scheme with self-healing property is fit for military environments. In case of users' location and some important information revealed, users only send some essential messages. In addition, in commercial content distribution applications, the

*Corresponding author: Hua Guo

self-healing mechanism may be useful to protect the highly sensitive information. The self-healing mechanism is that when the users receive the broadcast message, they can recover the session key by combining the broadcast with their own secret and can not recovery the session key by the broadcast or their own secret alone, and he can recovery the lost session keys by combining the previous with subsequent broadcast messages.

Staddon *et al.* first proposed the concept of self-healing and introduced a group key distribution scheme with self-healing property [1]. However, the scheme's storage and communication overhead is very high. Then, based on the work in [1], Blundo *et al.* [2] developed a new self-healing key distribution scheme which is more efficient and has less user memory storage. At the same time, they gave a lower bound on the resources required of such schemes [3]. Later, Liu *et al.* [4] introduced a new scheme to achieve the self-healing group key distribution, which is based on revocation polynomial rather than Lagrange interpolation. This scheme is more efficient and needs less storage. Then, some schemes based on hash chain were proposed [5, 6, 7, 8, 9, 10, 11, 12]. However, these hash chain-based schemes are not resistant to collusion attack. That is, if the revoked users collude with the new joined users, they can recover all of the session keys including. Obviously, this is not secure.

Recently, Chen et al.*et al.* [13] developed a scheme to realize the self-healing group key distribution based on one-way hash chain which can resist the collusion attack. In the new scheme, users are divided into the different groups according to the time they joined the group, and users can only recover the session keys from the session he joined in to the last session he is legitimate. They assert that their scheme is secure and satisfies all of the basic security properties, i.e., mt-wise forward secrecy, any-wise backward secrecy and resistance to mt-wise collusion attack. Unfortunately, we found a revoked user can recover other legitimate users' personal secrets which can be used to recover the current session's session key, this directly breaks the forward security, mt-revocation capability and mt-wise collusion attack resistance capability. Thus, Chen *et al.*'s scheme 2 is insecure.

We arrange the rest paper as follows. Chen *et al.*'s scheme 2 and corresponding security model are briefly introduced in section 2. An attack on Chen *et al.*'s scheme 2 are introduced and analyzed in section 3. In Section 4, we present the conclusion of this paper. For convenience, we adopt the same notations as Chen *et. al.*'s scheme and list notations in Table 1.

2 Overview of Chen *et. al.*'s Scheme

In this section, we briefly review the system model, security model and self-healing group key distribution scheme of Chen *et. al.*'s scheme 2.

2.1 System Model

In the model, a communication group in wireless networks includes a group manager (GM) and group users of $U = \{U_1, \cdots, U_n\}$ where n is the largest ID number. The group communication is set up and maintained by the GM's joining and revoking operations. Each group member U_i has uniquely identity i, where i ranges from 1 to N, and N is the largest. GM will distributes a personal secret $\mathcal{S}_i$ to user $U_i \in G_j$ when he joins the group. Let K_j denote the session key which is chosen by the GM. For each session, the GM distributes a broadcast message B_j to group members and legitimate users can compute K_j through the broadcast message B_j and his personal secret $\mathcal{S}_i$.

U_i	the i-th user
m	the maximum sessions
t	the maximum revoked users
F_q	a finite field of order q, and q is a prime
$\mathcal{S}(i)$	U_i's personal secret
B_j	the j-th broadcast message
$h(\cdot)$	hash function
$H(\cdot)$	the entropy function
$E_k(\cdot)/D_k(\cdot)$	a symmetric encryption/decryption function
ε_j	the session identifier
k_j^0	the seed of j-th key chain $k_j^0 \in F_q$
$k_j^{j'}$	the j' key in the j-th key chain
$R_j^{j'}$	the users joining the group in session j' and being revoked before or in session j and $j^{'} \leq j$
$\lvert R_j^{j'} \rvert$	the number of users in $R_j^{j'}$
R_j	the revoked users before and in session j, and $R_j = \{R_j^1, \cdots, R_j^j\}$
$\lvert R_j \rvert$	the number of users in R_j
$G_j^{j'}$	the group members who join the group in session j and are still legitimate in session j and $j' \leq j$
$\lvert G_j^{j'} \rvert$	the number of users in $G_j^{j'}$
G_j	all legitimate group members in session j, and $G_j = \{G_j^1, \cdots, G_j^j\}$
$\lvert G_j \rvert$	the number of users in G_j

Table 1: Notations

2.2 Security Model

The security model in Chen *et. al.*'s scheme 2 is introduced as follows.

Definition 1 *(Group key distribution with self-healing property and mt-revocation capability). The group key distribution scheme is self-healing and achieves mt-revocation capability if*

(1) For any user $U_i \in G_j^{j'}$, the session key K_j for session j is determined by the key updating broadcast packet B_j and the personal secret S_i. That is

$$H(K_j|B_j, S_j) = 0$$

(2) Only the broadcast messages or personal secrets alone can not obtain any information about K_j. That is

$$H(K_j|S_1, S_2, \cdots, S_N) = H(K_j|B_1, B_2, \cdots, B_m) = H(K_j)$$

(3) mt-revocation capability: If for a collusion of users in $\mathbf{R}_j$ can not compute K_j. However, it is easy for any legitimate user $U_i \notin \mathbf{R}_j$ to recover K_j. That is

$$H(K_j|B_j, S_i) = 0, H(K_j|B_j, \{S_r|U_r \in R_j\}) = H(K_j)$$

(4) Self-healing property: For any j, $j_1 < j \le j_2$, if a user U_i is legitimate both in session j_1 and in session j_2, he can recover the lost session key $K_j (j_1 \le j \le j_2)$ from broadcast packets B_{j_2}. That is

$$H(K_j | B_{j_2}, \{S_i | U_i \in G_j^{j_1}) = 0$$

Definition 2 *(mt-wise forward secrecy). The scheme achieves mt-wise forward secrecy if*

Even if any of users in R_j collude and they learn about session keys $K_{j'} (1 \le j' \le j)$, they cannot get any information about K_{j+1} where $R_j \subseteq U$ denotes the users who are revoked before session j and $|R_j| \le jt$, $j \in \{1, 2, \cdots, m\}$. That is

$$H(K_{j+1} | B_1, B_2, \cdots, B_m, \{S_r | U_r \in R_j\}, K_1, K_2, \cdots, K_j) = H(K_{j+1})$$

Definition 3 *(any-wise backward secrecy). The scheme guarantees any-wise backward secrecy if*

Even if any of users in D_j collude and they learn about session keys $K_{j'} (j' \ge j)$, they cannot get any information about K_j where $D_j \subseteq U$ denotes the users who join the group after session j. That is

$$H(K_j | B_1, B_2, \cdots, B_m, \{S_v | U_v \in D_j\}, K_{j+1}, K_{j+2}, \cdots, K_m) = H(K_j)$$

Definition 4 *(resistance to mt-wise collusion attack). The scheme is resistant to mt-wise collusion attack if*

Even if any of users in R_{j_1} and D_{j_2} collude and they learn about $\{B_1, B_2, \cdots, B_m, \{S_i | U_i \in R_{j_1}\}\} \bigcup \{B_1, B_2, \cdots, B_m, \{S_i | U_i \in R_{j_2}\}\}$, they cannot get any information about K_j. That is

$$H(K_j | B_1, B_2, \cdots, B_m, \{S_i | U_i \in R_{j_1} \cup D_{j_2}\}) = H(K_j)$$

2.3 Chen *et. al.*'s Self-Healing Group Key Distribution Scheme 2

Chen *et. al.*'s self-healing group key distribution scheme 2 includes five parts: Set up, Broadcast in session j, Group session key recovery and self-healing, Group member addition and Group member revocation.

- Set up

  The GM selects a random $2t$-degree polynomial $s_1(x) = a_0 + a_1 x + \cdots + a_{2t} x^{2t}$ and a random t-degree polynomial $s_2(x) = b_0 + b_1 x + \cdots + b_t x^t$ from $F_q[x]$. Then, the GM chooses a number ε_1 at random from F_q. The GM sends the user's personal secret $\mathcal{S}_i = \{\varepsilon_1 \cdot s_1(i), \varepsilon_1 \cdot s_2(i)\}$ to a user via a secure channel.

- Broadcast in session j (for $1 \le j \le m$)

  Let $\mathbf{R}_j = \{R_j^1, R_j^2, \cdots, R_j^{j'}, \cdots, R_j^j\}$ be the set of revoked users before and in session j, where $R_j^{j'}$ is the set of users who join the group in session j' and are revoked before and in session j. $R_j^{j'} = \{U_{r_1^{j'}}, U_{r_2^{j'}}, \cdots, U_{r_{w_{j'}}^{j'}}\}$ and $|R_j^{j'}| = w_{j'} \le t$. $r_1^{j'}, r_2^{j'}, \cdots, r_{w_{j'}}^{j'}$ are the IDs of users in $R_j^{j'}$. $R_j^{j'} = \emptyset$ if no users joined the group in session j'.

– The GM chooses a random value $k_j^0 \in F_q$ and a one-way hash function $h(\cdot)$. Note that $h^i(\cdot)$ denotes applying i times hash operation. Then GM constructs the j-th key chain for session j: $\{k_j^1, k_j^2, \cdots, k_j^j\}$, where

$$\begin{aligned} k_j^1 &= h(k_j^0), \\ k_j^2 &= h(k_j^1) = h(h(k_j^0)) = h^2(k_j^0), \\ &\cdots, \\ k_j^j &= h(k_j^{j-1}) = h(h(k_j^{j-2})) = \cdots = h^j(k_j^0), \end{aligned}$$

For security, $k_j^0 (1 \le j \le m)$ is different from each other.

The GM splits the $k_j^{j'}$ into two t-degree polynomials, $U_j^{j'}(x)$ and $V_j^{j'}(x)$, where

$$k_j^{j'} = U_j^{j'}(x) + V_j^{j'}(x), j' = 1, 2, \cdots, j.$$

– To construct the revocation polynomials for session j, the GM firstly chooses number sets $\overline{R}_j^{j'}$, where $\overline{R}_j^{j'} = \{\overline{r}_1^{j'}, \overline{r}_2^{j'}, \cdots, \overline{r}_{t-w_{j'}}^{j'}\}$ are random numbers which are not used as a user ID and different from each other. Then, the GM computes

$$A_j^{j'}(x) = \Pi_{z=1}^{|R_j^{j'}|}(x - r_z^{j'})\Pi_{z'=1}^{t-|R_j^{j'}|}(x - \overline{r}_{z'}^{j'}), j' = 1, 2, \cdots, j$$

– The GM chooses a random session key K_j from F_q. Then, the GM computes

$$M_j^{j'}(x) = A_j^{j'}(x) \cdot U_j^{j'}(x) + \varepsilon_{j'} \cdot s_1(x)$$

and

$$N_j^{j'}(x) = V_j^{j'}(x) + \varepsilon_{j'} \cdot s_2(x).$$

After that, the GM broadcasts the message

$$\begin{aligned} B_j \;=\; & \mathbf{R}_j \cup \overline{\mathbf{R}}_j \cup \{M_j^{j'}(x) | j' = 1, 2, \cdots, j\} \cup \{N_j^{j'}(x) | j' = 1, 2, \cdots, j\} \\ & \cup \{E_{k_j^{j'}}(K_{j'}) | j' = 1, 2, \cdots, j\} \end{aligned}$$

where $\overline{\mathbf{R}}_j = \{\overline{R}_j^1, \overline{R}_j^2, \cdots, \overline{R}_j^j\}$ and $E_k(\cdot)$ is a symmetric encryption function.

- Group session key recovery and self-healing

  Any legitimate user $U_i \in G_j^{j'}$ can recover the j-th session key when he receives the broadcast message B_j as follows.

– U_i uses his personal secret $\varepsilon_{j'} \cdot s_1(i)$ and $\varepsilon_{j'} \cdot s_2(i)$ to compute

$$U_j^{j'}(i) = \frac{M_j^{j'}(i) - \varepsilon_{j'} \cdot s_1(i)}{A_j^{j'}(i)}$$

and

$$V_j^{j'}(i) = N_j^{j'}(i) - \varepsilon_{j'} \cdot s_2(i)$$

respectively.

Thus, $k_j^{j'} = U_j^{j'}(i) + V_j^{j'}(i)$.

– U_i uses the hash function $h(\cdot)$ to compute all $\{k_j^{j''}\}$ for $j' < j'' \leq j$ in the j-th key chain.
– U_i recovers the session keys $\{K_{j''}\}(j' < j'' \leq j)$ by decrypting $E_{k_j^{j''}}(K_{j''})$ $(j' < j'' \leq j)$ with corresponding keys $\{k_j^{j''}\}(j' < j'' \leq j)$.

- Group member addition

  When a new user U_i joins the group in session j, the GM sends him a personal key $\mathcal{S}_i = \{\varepsilon_{j+1} \cdot s_1(i), \varepsilon_j \cdot s_2(i)\}$ through a secure channel. For keeping backward secrecy, the GM starts a new session.

- Group member revocation

  When a user U_i who joins the group in session j' is revoked in session j, the GM includes $(x - r_j^{j'})$ into $A_{j''}^{j'}(x)(j \leq j'' \leq m)$. For keeping forward secrecy, the GM starts a new session.

3 Cryptanalysis of Chen *et. al.*'s Scheme 2

We now show that Chen *et.al.*'s scheme 2 can not keep the forward security and can not resist collusion attack.

Let $G_{j_1}^{j'}$ denote the users who join the group in session j' and are still legitimate in session j_1 where $j' < j_1$. Suppose that $U_i \in G_{j_1}^{j'}$ and U_i is revoked in session $j_2 (j' < j_1 < j_2)$. Now we are ready to show how U_i, who is revoked in session j_2, recovers other user's personal secret who is legitimate in session j_2, furthermore uses this personal secret to compute the session key K_{j_2} which should be kept secret from U_i.

Step 1. U_i computes $k_{j'}^{j'}$ and $k_{j_1}^{j'}$ with his personal key $\mathcal{S}_i$ and the broadcast messages $M_{j'}^{j'}(x)$, $N_{j'}^{j'}(x)$ and $M_{j_1}^{j'}(x)$, $N_{j_1}^{j'}(x)$.

Step 2. In session j', U_i receives the broadcast messages $M_{j'}^{j'}(x), N_{j'}^{j'}(x)$, where

$$M_j^{j'}(x) = A_j^{j'}(x) \cdot U_j^{j'}(x) + \varepsilon_{j'} \cdot s_1(x), \tag{1}$$

and

$$N_j^{j'}(x) = V_j^{j'}(x) + \varepsilon_{j'} \cdot s_2(x). \tag{2}$$

Note that

$$k_{j'}^{j'} = U_{j'}^{j'}(x) + V_{j'}^{j'}(x),$$

Equation (2) can be converted to

$$N_j^{j'}(x) = k_{j'}^{j'} - U_j^{j'}(x) + \varepsilon_{j'} \cdot s_2(x). \tag{3}$$

Let (1)+$A_j^{j'}(x) \cdot$ (3), U_i can obtain

$$M_{j'}^{j'}(x) + A_{j'}^{j'}(x) \cdot N_{j'}^{j'}(x) = k_{j'}^{j'} \cdot A_{j'}^{j'}(x) + \varepsilon_{j'} \cdot s_1(x) + A_{j'}^{j'}(x) \cdot \varepsilon_{j'} \cdot s_2(x) \tag{4}$$

With the values of $k_{j'}^{j'}$ which is computed from step (1), U_i can obtain

$$M_{j'}^{j'}(x) + A_{j'}^{j'}(x) \cdot N_{j'}^{j'}(x) - A_{j'}^{j'}(x) \cdot k_{j'}^{j'} = \varepsilon_{j'} \cdot s_1(x) + A_{j'}^{j'}(x) \cdot \varepsilon_{j'} \cdot s_2(x) \tag{5}$$

Step 3. Since U_i is also legitimate in session j_1, U_i can obtain the similar result in the same way:

$$M_{j_1}^{j'}(x) + A_{j_1}^{j'}(x) \cdot N_{j_1}^{j'}(x) - A_{j_1}^{j'}(x) \cdot k_{j_1}^{j'} = \varepsilon_{j'} \cdot s_1(x) + A_{j_1}^{j'}(x) \cdot \varepsilon_{j'} \cdot s_2(x) \tag{6}$$

Let (3)-(4), user U_i can obtain

$$\begin{aligned} & M_{j'}^{j'}(x) + A_{j'}^{j'}(x) \cdot N_{j'}^{j'}(x) - A_{j'}^{j'}(x) \cdot k_{j'}^{j'} - M_{j_1}^{j'}(x) - A_{j_1}^{j'}(x) \cdot N_{j_1}^{j'}(x) + A_{j_1}^{j'}(x) \cdot k_{j_1}^{j'} \\ =& (A_{j'}^{j'}(x) - A_{j_1}^{j'}(x)) \cdot \varepsilon_{j'} \cdot s_2(x) \end{aligned} \tag{7}$$

Step 4. U_i computes $\varepsilon_{j'} \cdot s_2(x)$ as

$$\begin{aligned} & \varepsilon_{j'} \cdot s_2(x) \\ =& \frac{M_{j'}^{j'}(x) + A_{j'}^{j'}(x) \cdot N_{j'}^{j'}(x) - A_{j'}^{j'}(x) \cdot k_{j'}^{j'} - M_{j_1}^{j'}(x) - A_{j_1}^{j'}(x) \cdot N_{j_1}^{j'}(x) + A_{j_1}^{j'}(x) \cdot k_{j_1}^{j'}}{(A_{j'}^{j'}(x) - A_{j_1}^{j'}(x))} \end{aligned} \tag{8}$$

Take $\varepsilon_{j'} \cdot s_2(x)$ to (3), U_i computes $\varepsilon_{j'} \cdot s_1(x)$ as

$$\varepsilon_{j'} \cdot s_1(x) = M_{j'}^{j'}(x) + A_{j'}^{j'}(x) \cdot N_{j'}^{j'}(x) - A_{j'}^{j'}(x) \cdot k_{j'}^{j'} - A_{j'}^{j'}(x) \cdot \varepsilon_{j'} \cdot s_2(x) \tag{9}$$

Step 5. U_i gets a legitimate user's identity, v, in session j_2 by observing $R_j^{j'}$ where $j > j_2$.

Step 6. U_i computes $\varepsilon_{j'} \cdot s_1(v)$ and $\varepsilon_{j'} \cdot s_2(v)$ through $\varepsilon_{j'} \cdot s_1(x)$ and $\varepsilon_{j'} \cdot s_2(x)$. Then, U_i pretends U_v to compute the session key K_{j_2} using $\varepsilon_{j'} \cdot s_1(v), \varepsilon_{j'} \cdot s_2(v)$ and $M_{j_2}^{j'}(x), N_{j_2}^{j'}(x)$ from the broadcast message B_{j_2}.

Note that U_i is revoked in session j_2, thus he should not have computed K_{j_2}. Therefore the scheme cannot achieve the forward security. When the revoked user U_i obtains the session key K_{j_2}, he of course can give this session key to a new user who joins the group after session j_2 thus should not know K_{j_2}. Hence, the scheme can not resist the collusion attack. Similarly, the scheme does not have the *mt*-revocation capability.

4 Conclusion

Chen *et. al* claimed that their self-healing group key distribution scheme 2 achieves a perfect performance on storage overhead which is constant, and a better tradeoff between the storage overhead and the total communication overhead, thus is practical for resource-constrained wireless networks in bad environments. Unfortunately, we found that Chen *et al.*'s scheme 2 is insecure. Some security flaws are pointed out in this paper, i.e., the scheme 2 can not hold some basic security properties, say, the forward security, *mt*-revocation capability and *mt*-wise collusion attack resistance capability.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61300172), the Research Fund for the Doctoral Program of Higher Education (No. 20121102120017) and the Fund of the State Key Laboratory of Software Development Environment (No. SKLSDE-2014ZX-14).

References

[1] Staddon, J.; et al. Self-healing key distribution with revocation. IEEE Symposium on Security and Privacy, 2002, 241-257.

[2] Blundo, C.; et al. Design of Self-Healing Key Distribution Schemes. Designs Codes and Cryptography. 2004, 32,13:15-44.

[3] Blundo, C.; P. D'Arco; A. De Santis. On Self-Healing Key Distribution Schemes. IEEE Transactions on Information Theory. 2006, 52,12:5455-5467.

[4] Liu, D.; P. Ning; K. Sun. Efficient Self-Healing Group Key Distribution with Revocation Capability. In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS03 (2003):231-240.

[5] Dutta, R., Y. D. Wu, and S. Mukhopadhyay. Constant storage selfhealing key distribution with revocation in wireless sensor network. In IEEE International Conference on Communications (ICC07), 2007: 1323-1328.

[6] Dutta, R.; S. Mukhopadhyay. Improved Self-Healing Key Distribution with Revocation in Wireless Sensor Network. Wireless Communications and Networking Conference. WCNC,2007: 2963-2968.

[7] Ratna D.; Sourav Mukhopadhyay. Designing Scalable Self-healing Key Distribution Schemes with Revocation Capability. Parallel and Distributed Processing and Applications. 2007, 419-430.

[8] Dutta, R.; Mukhopadhyay, S.; Emmanuel, S. Low bandwidth self-healing key distribution for broadcast encryption. In Proceedings of the 2nd Asia International Conference on Modeling and Simulation (ICOMS-2008), Kuala Lum pur, Malaysia, 13C15 May 2008, 867-872.

[9] Dutta, R.; E C. Chang; S. Mukhopadhyay. Efficient Self-healing Key Distribution with Revocation for Wireless Sensor Networks Using One Way Key Chains. International Conference on Applied Cryptography and Network Security Springer Berlin Heidelberg 2007: 385-400.

[10] Han, S.; et al. Efficient threshold self-healing key distribution with sponsorization for infrastructureless wireless networks. IEEE Transactions on Wireless Communications. 2009, 8,4:1876-1887.

[11] Kausar, F.; Hussain, S.; P. A. Masood. Secure group communication with self-healing and rekeying in wireless sensor networks. Proceedings of the 3rd international conference on Mobile ad-hoc and sensor networks Springer-Verlag 2007, 4864, 737-748.

[12] Yang, Y.; et al. Computationally Secure Hierarchical Self-healing Key Distribution for Heterogeneous Wireless Sensor Networks. Lecture Notes in Computer Science, 2009: 135-149.

[13] Chen, H.; Xie, L.; Wang, Q. Improved One-Way Hash Chain and Revocation Polynomial-Based Self-Healing Group Key Distribution Schemes in Resource-Constrained Wireless Networks. Sensors. 2014, 14.12: 24358-80.