ELectronics EXpress

Self-healing key distribution scheme with long service time

Chanil Park[1a)], **Junbeom Hur**[2b)], **Kisuk Kweon**[1], **and Hyunsoo Yoon**[1]

[1] *Computer Science Department, KAIST, Republic of Korea*

[2] *Computer Science Department, UIUC, U.S.A.*

a) *chanil@nslab.kaist.ac.kr*

b) *jbhur@illinois.edu*

Abstract: Self-healing key distribution schemes for broadcast encryption are capable of recovering missed group keys and resisting a collusion attack of up to t revoked users. However, since previous schemes have been considered only m sessions, it does not suitable to support infinite sessions. In the paper, we propose an efficient δ-self healing key distribution scheme with revocation capability. The proposed scheme can support infinite sessions by updating the private key of users and supporting a partial revocation. The communication overhead of the proposed scheme is compared with several previous works.

Keywords: group communication, broadcast encryption, self healing key distribution

Classification: Science and engineering for electronics

References

[1] C. Blundo, P. D'Arco, A. De Santis, and M. Listo, "Design of Self-healing Key Distribution Schemes," *Design, Codes, and Cryptography*, vol. 32, pp. 15–44, 2004.

[2] R. Dutta and S. Mukhopadhyay, "Improved Self-Healing Key Distribution with Revocation in Wireless Sensor Network," *Proc. IEEE Wireless Commun. Netw. Conf.*, Hong Kong, China, 2007.

[3] D. Liu, P. Ning, and K. Sun, "Efficient Self-Healing Group Key Distribution with Revocation Capability," *Proc. 10th ACM Conf. Computer and Communications Security*, Washington, DC, USA, pp. 231–240, Oct. 2003.

[4] S. More, M. Malkin, J. Staddon, and D. Balfanz, "Sliding-Window Self-Healing Key Distribution," *Proc. ACM Workshop on Survivable and Self-Regenerative Systmes*, pp. 82–90, 2003.

[5] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, "Self-healing key distribution with revocation," *Proc. IEEE Symp. Security and Privacy*, pp. 241–257, 2002.

[6] V. Daza, J. Herranz, and G. Saez, "Flaws in some self-healing key distribution schemes with revocation," *Information Processing Letters*, vol. 109, no. 11, pp. 523–526, May 2009.

[7] D. Boneh, "The decision Diffie-Hellman problem," *Proc. 3th Conf. Algorithmic Number Theory Symposium, LNCS*, vol. 1432, pp. 48–63, 1998.

DOI: 10.1587/elex.7.913
Received April 12, 2010
Accepted June 07, 2010
Published July 10, 2010

1 Introduction

As multimedia broadcast technologies such as Pay-TV, Satellite Broadcasting, or Digital Multimedia Broadcasting (DMB) continue to develop, the security of broadcast contents became one of important challenges among researchers. Recently, self-healing key distribution schemes with revocation capability were proposed to provide an efficient solution for protecting broadcast contents [1, 3, 5]. Self-healing key distribution schemes with revocation capability enable legitimate members to recover secret keys, which are used to encrypt broadcast contents. We call the secret key a *group key* because all of the members in legitimate group can share it. In the self-healing key distribution schemes with revocation capability, the broadcast manager (we call it a group manager (GM) because it controls the group of legitimate members) divides the service time into m sessions and distributes a new secret key, which is a group key, to group members per each session through an encrypted key message. Then, each group member can obtain the group key by decrypting the key message with his private key. However, the revoked users cannot obtain the group key even if they can receive the key message.

2 Motivation

The previous self-healing key distribution schemes with revocation capability have problems in terms of service duration and member revocation. For the service duration, the previous schemes considered just m sessions. Hence, the GM had to update the private key of the members before starting a new session after m sessions had been expired. Thus, the GM had to reset the key distribution scheme again. We call this a *life-time extension* problem. Staddon et al. [5] suggested a solution to the problem by using Shamir secret sharing in the exponent. However, as mentioned in [1, 5], their solution has mainly two faults. First, if a member does not receive a private key update message, then there is no way for the member to update his private keys for future processes [1]. Second, new users who joined the group in the middle of sessions cannot update their private keys associated with the sessions to which they do not belong even if they receive the private key update message [1]. Dutta et al. proposed a self-healing key distribution scheme using encryption and decryption functions [2]. They tried to overcome the life-time extension problem by reusing the private keys. However, Daza et al. proved that Dutta et al.'s scheme are not secure at all [6].

For member revocation, when a member joins the group in the previous schemes, he receives private keys for all sessions that he registered. Therefore, in order to revoke the members forever, the GM has to store identities, *ids*, of all revoked members in each session. We call it a *full revocation*. The full revocation causes short life-time of the self-healing key distribution.

In this paper, we propose an enhanced self-healing key distribution scheme with revocation capability that solves the life-time extension problem. The proposed scheme can support infinite sessions because GM updates private key of members per each session. The proposed scheme operates in the

DOI: 10.1587/elex.7.913
Received April 12, 2010
Accepted June 07, 2010
Published July 10, 2010

δ-sliding-window fashion and resists against a collusion attack of up to t revoked users. The proposed scheme requires a low storage cost in terms of the members and has a flexible user revocation property. In the proposed scheme, it is enough for the GM to consider revoked users in $\delta+1$ sessions. We call this a *partial revocation*. For the security of the proposed scheme, we prove that the scheme is secure under the hardness of Decisional Diffie-Hellman problem. We also show the practicality of proposed scheme through a simulation.

3 Notations

We describe some notations used in the paper. We assume that each group member has an unique identity i, where $i \in \{1, \cdots, n\}$. Let G_j be a communication group established by the GM in the j^{th} session and K_j be a group key for the j^{th} session. We use a notation $S_{i,j}$ for user's private key. $S_{i,j}$ is a private key of user U_i for the j^{th} session. We denote a set of users who are revoked in the j^{th} session by $\mathcal{R}_j$ and a set of users who join the group in the j^{th} session by $\mathcal{J}_j$. Hence, $G_j = (G_{j-1} \cup \mathcal{J}_j) \setminus \mathcal{R}_j$. We assume that once a user is revoked from the group, he is kept revoked for the forward sessions. When a user U_i joins the group $G_j(i.e,\ U_i \in G_j)$, he receives a private key $S_{i,j}$ from the GM. At any j^{th} session, member U_i in G_j can determine a group key K_j from the broadcast message B_j and the private key $S_{i,j}$.

4 δ-self healing key distribution with revocation capability

We present techniques for an efficient self-healing key distribution with revocation capability. In the techniques, a group member U_i receives a private key $S_{i,j}$ from the GM when he joins the group G_j while, in the previous schemes, a member U_i receives a set S_i of private keys when he joins the group in the j^{th} session, $i.e$ $S_i = \{S_{i,j}, \cdots, S_{i,m}\}$. In the proposed scheme, group members can update their private key $S_{i,j}$ to $S_{i,j+1}$ from the broadcast message B_j.

In the broadcast environment, members may miss the group key update messages. This can occur frequently in the mobile environments because members may not be on-line constantly. The proposed scheme can do the self-healing property for δ sessions. The construction is as follows:

Construction 1 *δ-self-healing key distribution with revocation capability*

1. **Setup:***Let $j, \delta \in \mathbb{N}$ denote a session index and a self-healing capability. Let g be a generator of a subgroup $G \subseteq F_q^*$ with a prime order p. For session $j \in \{1, \cdots, \delta\}$, the GM selects group keys $K_j = \mathrm{g}^{k_j}, 1 \le j \le \delta$, where k_j is a random value in F_p. The GM also selects t-degree polynomials $\alpha_j(x) \in F_p[x], 1 \le j \le \delta$ and defines $\beta_j(x) = \mathrm{g}^{k_j} - \alpha_j(x)$. The GM chooses two secret t-degree polynomials $p_1^a(x)$ and $p_1^b(x)$ from $F_p[x]$. The update of secret polynomials $p_j^a(x)$ and $p_j^b(x)$ in a session j is as follows:*

$$p_{j+1}^a(x) = p_j^a(x) + \mathrm{g}^{k_j}, \quad p_{j+1}^b(x) = p_j^b(x) + \mathrm{g}^{k_j}. \tag{1}$$

© IEICE 2010
DOI: 10.1587/elex.7.913
Received April 12, 2010
Accepted June 07, 2010
Published July 10, 2010

2. **Registration:** *In the j^{th} session, when a new member subscribes to the group, the GM first assigns a new id $u \in F_p$ to the member and the GM sends to the member a group key g^{k_j} for the current session and private key $S_{u,j+1} = (p^a_{j+1}(u), p^b_{j+1}(u))$ for the next session via secure channels.*
3. **Broadcast:** *In the j^{th} session, let a set $\mathcal{R}_j = \cup_{j'=j-\delta}^{j} Rev_{j'}$, $|\mathcal{R}_j| \le t$, where $Rev_{j'}$ is a set of newly revoked members in the j'^{th} session. The GM generates a group key $g^{k_{j+\delta}}$ by randomly selecting $k_{j+\delta} \in F_p$. The GM also generates a t-degree polynomial $\alpha_{j+\delta}(x) \in F_p[x]$ and sets $\beta_{j+\delta}(x) = g^{k_{j+\delta}} - \alpha_{j+\delta}(x)$. The GM chooses random t-degree polynomials $f_j(x), g_j(y) \in F_p[x]$, which are used to hide the security data. The GM broadcasts message B_j, which consists of $\mathcal{R}_j$ and the following messages:*

$$\{f_j(x)\cdot\Lambda_j(x) + g^{k_{v-1}}\cdot p^a_v(x)\}_{\max(j-\delta,1)\le v\le j}, \tag{2}$$

$$\{g_j(x)\cdot\Lambda_j(x) + g^{k_{v-1}}\cdot p^b_v(x)\}_{\max(j-\delta,1)\le v\le j}, \tag{3}$$

$$\{g^{k_j+f_j(x)\cdot g_j(x)}\}, \tag{4}$$

$$\{g^{v\cdot k_j}\cdot\alpha_v(x)\cdot\Lambda_j(x) + f_j(x)\}_{\max(j-\delta,1)\le v\le j-1}, \tag{5}$$

$$\{g^{v\cdot k_j}\cdot\beta_v(x)\cdot\Lambda_j(x) + g_j(x)\}_{j+1\le v\le j+\delta}, \tag{6}$$

where $\Lambda_j(x) = \prod_{r\in\mathcal{R}_j}(x-r)$.

4. **Key recovery:** *The member U_i in the j^{th} session can compute a group key g^{k_j} from the broadcast message B_j. After received B_j, U_i checks his private key $S_{i,v} = (p^a_v(i), p^b_v(i))$ and the group key $g^{k_{v-1}}$. U_i gets $f_j(i)$ and $g_j(i)$ by evaluating (2) and (3) at $x = i$, respectively. Then U_i computes the group session key g^{k_j} from (4) as follows:*

$$f_j(i) = \frac{\{f_j(x)\cdot\Lambda_j(x) + g^{k_{v-1}}\cdot p^a_v(x)\}\Big|_{x=i} - g^{k_{v-1}}\cdot p^a_v(i)}{\Lambda_j(i)} \tag{7}$$

$$g_j(i) = \frac{\{g_j(x)\cdot\Lambda_j(x) + g^{k_{v-1}}\cdot p^b_v(x)\}\Big|_{x=i} - g^{k_{v-1}}\cdot p^b_v(i)}{\Lambda_j(i)} \tag{8}$$

$$g^{k_j} = \left(\frac{\{g^{k_j+f_j(x)\cdot g_j(x)}\}\Big|_{x=i}}{g^{f_j(i)\cdot g_j(i)}}\right). \tag{9}$$

After received the group key g^{k_j}, U_i computes the equation (6) and gets values $\beta_{j+1}(i), \cdots, \beta_{j+\delta}(i)$, which are used in cases that broadcast message is missed. U_i stores these values securely.

5. **δ-self-healing and private key update:** *The member U_i from the r^{th} session to the s^{th} sessions s.t. $|s-r| \le \delta+1$, i.e. $U_i \in \bigcap_{\ell=r}^{s} G_\ell$, can recover group keys g^{k_ℓ}, $r < \ell < s$, from the broadcast messages B_r and B_s. Then U_i can update his private key. Recall from Step (4), U_i can get $\beta_{r+1}(i), \cdots, \beta_{s-1}(i)$ from the broadcast message B_r. U_i can also get $\alpha_{r+1}(i), \cdots, \alpha_{s-1}(i)$ from the broadcast message B_s. Then U_i obtains $g^{k_\ell} = \alpha_\ell(i) + \beta_\ell(i), r < \ell < s$, and updates his private key,*

$$p^a_{s+1}(i) = p^a_r(i) + \sum_{\ell=r}^{s} g^{k_\ell}, \quad p^b_{s+1}(i) = p^b_r(i) + \sum_{\ell=r}^{s} g^{k_\ell}. \tag{10}$$

DOI: 10.1587/elex.7.913
Received April 12, 2010
Accepted June 07, 2010
Published July 10, 2010

5 Security analysis

We discuss the security proof for the δ-self-healing key distribution scheme with revocation capability. The proof is conducted under the hardness of Decisional Diffie-Hellman (DDH) problem with respect to revoked users.

Theorem 1 *If there exists an algorithm $\mathcal{A}$ which can break Construction 1 with non-negligible probability ϵ, then we can solve the decisional Diffie-Hellman problem with the same probability ϵ.*

Proof 1 *Before describing the proof, we are briefly describing the DDH-problem. The DDH-problem says that given a group G with prime order p and a generator g, it is computationally infeasible to distinguish if a triple $< \mathrm{g}^a, \mathrm{g}^b, \lambda >$ is of the form $< \mathrm{g}^a, \mathrm{g}^b, \mathrm{g}^{ab} >$ or $< \mathrm{g}^a, \mathrm{g}^b, \mathrm{g}^c >$, where a, b, c are chosen uniformly at random in $\mathbb{Z}_p^*$. For details the reader is referred to [7].*

We can say that the coalition of up to t revoked users can success in breaking Construction 1 if there exists an efficient algorithm $\mathcal{A}$ that can determine the polynomials $f_j(x)$ and $g_j(x)$ with non-negligible probability ϵ from given broadcast message B_j. We show that the algorithm $\mathcal{A}$ can be used to construct an efficient algorithm $\mathcal{A}'$ for solving the DDH-problem with the same probability ϵ. We assume that $\mathcal{A}'$ is allowed to control the external network for the j^{th} session. $\mathcal{A}'$ takes as input DDH challenge $< \mathrm{g}^a, \mathrm{g}^b, \lambda >$, where $a, b \in \mathbb{Z}_p^*$ are random values and g is a generator of group G. $\mathcal{A}'$ sets up Construction 1. Let $\mathcal{R}_j = \{U_1, \cdots, U_t\}$ be a set of revoked users at the j^{th} session. After choosen a random group key g^{k_j}, $\mathcal{A}'$ generates a broadcast message B'_j for the j^{th} session as follow:

- *$\mathcal{A}'$ chooses random polynomials $f'_j(x), g'_j(x) \in F_p[x]$ and computes*

$$\lambda \cdot \mathrm{g}^{k_j + bf'_j(x) + ag'_j(x) + f'_j(x)g'_j(x)}.$$

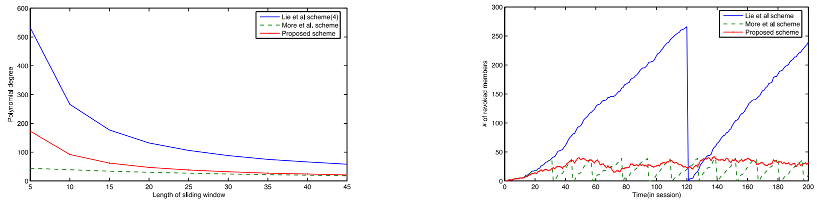
- *$\mathcal{A}'$ computes other parameters with the same way of original construction.*
- *$\mathcal{A}'$ broadcasts message B'_j, which consists of*

$$\begin{aligned}
&\{f'_j(x)\cdot\Lambda_j(x) + \mathrm{g}^{k_{j-1}}\cdot p^a_j(x)\}, \{g'_j(x)\cdot\Lambda_j(x) + \mathrm{g}^{k_{j-1}}\cdot p^b_j(x)\},\\
&\{\lambda \cdot \mathrm{g}^{k_j + bf'_j(x) + ag'_j(x) + f'_j(x)g'_j(x)}\},\\
&\{\mathrm{g}^{v\cdot k_j}\cdot\alpha_v(x)\cdot\Lambda_j(x) + f'_j(x)\}_{\max(j-\delta,1)\le v\le j-1},\\
&\{\mathrm{g}^{v\cdot k_j}\cdot\beta_v(x)\cdot\Lambda_j(x) + g'_j(x)\}_{j+1\le v\le j+\delta}
\end{aligned}$$

where $\Lambda_j(x) = \prod_{r\in\mathcal{R}_j}(x - r)$.

Given the broadcast message B'_j, $\mathcal{A}$ can not distinguish it from the real B_j because B'_j have exactly the same distribution of broadcast messages by a real execution of Construction 1. Hence, if λ=g^{ab} then $\mathcal{A}$ returns that the polynomials $f_j(x) = f'_j(x) + a$ and $g_j(x) = g'_j(x) + b$; otherwise, $\mathcal{A}$ returns random $f_j(x)$ and $g_j(x)$. Then $\mathcal{A}'$ computes a value $\lambda' = \frac{\mathrm{g}^{f_j(x)g_j(x)}}{\mathrm{g}^{bf'_j(x)+ag'_j(x)+f'_j(x)g'_j(x)}}$. If $\lambda' = \lambda$ then $\mathcal{A}'$ outputs that $< \mathrm{g}^a, \mathrm{g}^b, \lambda >$ is of the form $< \mathrm{g}^a, \mathrm{g}^b, \mathrm{g}^{ab} >$; and otherwise, outputs that $< \mathrm{g}^a, \mathrm{g}^b, \lambda >$ is a random triple $< \mathrm{g}^a, \mathrm{g}^b, \mathrm{g}^c >$.

DOI: 10.1587/elex.7.913
Received April 12, 2010
Accepted June 07, 2010
Published July 10, 2010



(a) Trade-off between sliding windows and polynomial degree (packet size:64 KB, base field: 64 bit)

(b) Possible service time for the revocation models (sliding window: 10, sessions:200)

Fig. 1. Service time between several schemes

Hence, it follows that $\mathcal{A}'$ can solve the DDH problem with the same probability ϵ which $\mathcal{A}$ can retrieve the polynomials $f_j(x)$ and $g_j(x)$ from the broadcast message B'_j.

6 Performance analysis

We compare the proposed scheme with the previous schemes [3, 4]. If we assume that the users maintain membership during m sessions from the $1st$ session, [3] needs $2m + 2\delta - 1$ storage capacity and [4] needs $3m$ storage capacity in terms of group members. However, in the proposed scheme, the members need $2 + \delta$ storage capacity to store private keys over $p^a_j(x), p^b_j(x)$ in the j^{th} session and points over $\beta_{j+1}(x), \cdots, \beta_{j+\delta}(x)$. In terms of communication, [3] and [4] need $(3t + 2)\delta$ and $3t^2 + 4t + (8t + 4)\delta$ communication capacity, respectively. But, we need $(8t+4)\delta+6t+3$ communication capacity. Although the proposed scheme costs more communication overhead than [3], we can see that the proposed scheme has longer lifetime than the other schemes. Fig. 1 (a) shows the trade-off between the sliding window size and possible polynomial degree. Hence, if we set the sliding window $\delta = 10$, then [3] and [4] can allow 266 and 39 revoked members in its communication capacity, respectively. However, the proposed scheme can allow approximately 100 revoked members. Fig. 1 shows the possible service time for the revocation models (full revocation and partial revocation) in the previous schemes and the proposed scheme. We simulated it with the sliding window $\delta = 10$ and the sessions $m = 200$. We can see that [3] is reset at the 120^{th} session and [4] is reset frequently. It is due to that the previous schemes follow the full revocation model. However, since the proposed scheme follows the partial revocation, it can provides the key distribution service without the reset. Hence, the proposed scheme can support long service time.

7 Conclusion

In this paper, we proposed the efficient δ-self-healing key distribution scheme with revocation capability. In the protocol, we showed that the secure transmission of some private keys can solve the life-time extension problem. Furthermore, we showed that the proposed scheme supports long service time

DOI: 10.1587/elex.7.913
Received April 12, 2010
Accepted June 07, 2010
Published July 10, 2010

by performing the simulation. Concerning the security, we proved that the scheme is computationally secure under the hardness of DDH-problem.

Acknowledgment

This research is supported by the Ubiquitous Computing and Network(UCN) Project, Knowledge and Economy Frontier R&D Program of the Ministry of Knowledge Economy(MKE) in Korea as a result of UCN's subproject 10C1-T1-20S.

DOI: 10.1587/elex.7.913
Received April 12, 2010
Accepted June 07, 2010
Published July 10, 2010