ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.2, February 2009, pp.462−468
doi: 10.3724/SP.J.1001.2009.03177

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种高效的Long-Lived Self-Healing密钥分发机制*

李 徽[1,2+], 武传坤[1]

[1](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

[2](中国科学院 研究生院,北京 100049)

Efficient Long-Lived Self-Healing Key Distribution Scheme

LI Hui[1,2+], WU Chuan-Kun[1]

[1](State Key Laboratory of Information Security, Institution of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: E-mail: lihui@is.iscas.ac.cn

Li H, Wu CK. Efficient long-lived self-healing key distribution scheme. *Journal of Software*, 2009,20(2): 462−468. http://www.jos.org.cn/1000-9825/3177.htm

Abstract: Some improvements on three aspects have been made for the self-healing key distribution scheme proposed by Staddon *et al*. First, an efficient long-lived scheme which is unconditional secure instead of computational secure is proposed to lower the cost of computation and communication. Second, the capability of session key recovery of members is strengthened, which enables the members to recover some reasonable session keys in a certain special situation. Third, the number of broadcast messages and that of personal keys stored in users' memory are reduced.

Key words: self-healing; *t*-collusion resistant; polynomial; group communication; key management

摘 要: 对 Staddon 等人提出的 self-healing 密钥分发方案作了 3 个方面的改进:第一,提出了一种更高效的无条件安全的 long-lived 方案取代基于计算安全的 long-lived 方案,降低了计算复杂度和通信复杂度;第二,增强了用户恢复合理密钥的能力,使得在某个特殊场景中,用户可以恢复出合理密钥;第三,降低了广播消息的次数和存储在用户端的私人密钥数目.

关键词: self-healing;抗 *t*-合谋攻击;多项式;群组通信;密钥管理

中图法分类号: TP309 **文献标识码**: A

随着群组通信业务(例如视频点播)的展开,安全问题成为了一个关注焦点.为了防止非授权用户的非法访问,数据内容通过一个会话密钥进行加密,而此会话密钥仅由组内成员共享.同时,随着群组成员关系的动态变化,会话密钥必须随时保持更新.因此,如何安全地分发会话密钥以及实时地进行密钥更新成为群组通信中密钥管理的一大挑战.由于网络环境的不稳定,包含密钥材料的数据包容易丢失,一旦某成员未能接收到此类数据包,则不能对相应的数据流进行解密.为了减轻重传包含密钥材料的数据包所带来的网络阻塞,Staddon 等人提

* Supported by the National Basic Research Program of China under Grant No.2007CB807902 (国家重点基础研究发展计划(973)); the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z423 (国家高技术研究发展计划(863))

Received 2007-05-30; Accepted 2007-09-30

出了带成员撤销的 self-healing 密钥分发机制[1].此机制特点是在 m 轮会话过程(一轮通信)中,群组管理者(GM)可以动态地增加/删除群组成员,但一旦删除某成员后,此成员就不能再加入这轮通信剩余会话过程中,直到下一轮通信开始为止;群组成员在丢失某次会话的含密钥材料数据包后仍能恢复出此次会话密钥,如果他接收到此轮通信之前和之后的两次会话的包含密钥材料的数据包,而不用再和 GM 进行交互,以要求对丢失的含密钥材料数据包的重传;同时,这种方案可以抵抗一定程度上的合谋攻击.

Self-healing 密钥分发机制首先由 Staddon 等人[1]提出,为缩短广播消息长度,More 等人提出了滑动窗口的 self-healing 密钥发放机制[2].同时,Liu Donggang 等人在降低广播消息复杂度和用户所需存储私钥数目上给出了一种更为有效的方案[3].Blundo 等人以信息论的方法给出了 self-healing 密钥分发机制的下界条件,并提出一种新方案[4,5].在本文中,我们在以下 3 个方面作了改进,一是使 self-healing 机制可以运行地更高效,以前类似的机制大部分只考虑了 self-healing 属性,而机制可安全运行时间较短,即使提出的 long-lived 模型也是基于 DDH(decision Diffie-Hellman)问题,计算代价也比较高;二是我们增强了 Staddon 方案中的用户密钥恢复能力;三是相应降低了存储在用户端所必须的私钥数目和广播次数.

本文第 1 节回顾以前几种 self-healing 方案并指出其各自的弱点.第 2 节提出新方案的框架.第 3 节证明新方案的无条件安全性,并给出无条件安全的定义.第 4 节和第 5 节是对新机制的一些性能的增强和改进以及与以前的机制的比较.

1 以前的self-healing密钥分发机制

1.1 Staddon等人的方案

在 self-healing 密钥分发机制中,我们把整个通信过程分成若干轮,每一轮通信包含 m 次会话.所谓 long-lived 模型,是指此密钥分发机制能够在足够多轮的通信过程中安全运行,而无须改变存储在用户端的秘密参数.在我们回顾 Staddon 等人提出的基于 DDH 假设的 long-lived 模型(Construction 5)[1]之前,我们先回顾在一轮通信模型下的 self-healing 密钥分发机制.

- 一轮通信模型下的 self-healing 密钥分发机制

1. (Initial set-up)群组管理者选择两个随机数 t,N,其中 t 是一个正整数,$N\in F_q$ 并且 $N\notin\{1,\ldots,n\}$(n 是预计用户总数).群组管理者在 $F_q[x,y]$中随机选择 m^2 个多项式 $s_{k,l}(x,y)=\sum_{i=0}^{t}a_{i,j}^{(k,l)}x^iy^j$ $(k,l\in\{1,\ldots,m\})$.每个用户 U_i 存储各自的密钥: $S_i=\{i,N,s_{1,1}(i,i),\ldots,s_{m,1}(i,i),s_{1,2}(i,i),\ldots,s_{m,m}(i,i)\}$. 接着,群组管理者在 $F_q[x]$中随机选择 m 个 t 次多项式 $p_1(x),p_2(x),\ldots,p_m(x)$ 以及此轮通信所使用的 m 个会话密钥 $K_1,\ldots,K_m\in F_q$, 定义多项式 $q_j(x)=K_j-p_j(x),(\forall j\in\{1,2,\ldots,m\})$.
2. (Broadcast) $L,R\subseteq\{1,2,\ldots,n\},|R|\leq t,L$ 表示合法的用户集合,R 表示撤销用户集合.同时,群组管理者选择 $W=\{w_1,w_2,\ldots,w_t\}\subseteq F_q$, 使得 $R\subseteq W,(W-R)\cap(L\cup\{N\})=\varnothing$. 于是,为第 j 次会话 ($j\in\{1,2,\ldots,m\}$) 的广播消息为 $B_j=B_j^1\cup B_j^2$:
$$B_j^1=\{p_{j'}(x)+s_{j',j}(N,x)\}_{j'=1,\ldots,j-1}\cup\{K_j+s_{j,j}(N,x)\}\cup\{q_{j'}(x)+s_{j',j}(N,x)\}_{j'=j+1,\ldots,m},$$
$$B_j^2=\{w_l,\{s_{j',j}(w_l,x)\}_{j'=1,\ldots,m}\}_{l=1,\ldots,t}.$$
3. (Session key recovery)设用户 U_i 是合法用户,当他接收到 B_j 后,根据 B_j^2 可以得到 t 个多项式插值 $s_{j,j}(w_l,x)(l=1,2,\ldots,t)$, 再结合其自身存储的私钥 $s_{j,j}(i,i)$ 可以恢复出多项式 $s_{j,j}(x,i)$, 所以用户 U_i 可以得到第 j 次会话密钥 $K_j=(K_j+s_{j,j}(N,x))|_{x=i}-s_{j,j}(N,i)$. 同理,$U_i$ 可以恢复一些多项式插值: $\{p_{j'}(i)\}_{j'=1,\ldots,j-1}$ 和 $\{q_{j'}(i)\}_{j'=j+1,\ldots,m}$.
4. (Key self-healing property)当用户 U_i 接收到不连续的两次广播消息 B_{j_1} 和 B_{j_2} ($j_1<j_2$)时,对任意的 $j(j_1<j<j_2)$,由于 $q_j(i)$由消息 B_{j_1} 可以恢复出来,而 $p_j(i)$由消息 B_{j_2} 可以恢复出来,则 $K_j=p_j(i)+q_j(i)$.

由此可见,此方案在一轮通信的过程中是可行的,但由于在此轮通信中,用户 U_i 已经得到 $s_{j',j}(N,i)$ ($j',j\in\{1,2,...,m\}$)中的某些值,所以在接下来的各轮通信过程中,无论用户 U_i 是否被撤销,他都能得到想恢复的密钥.为防止这种情况发生,一种方法是在每轮通信之前,群组管理者更新多项式 $s_{k,l}(x,y)$,并通知群组用户更换各自的私钥,但这种方法显然要求群组管理者和用户交互的次数增加,使通信复杂度增大.所以,Staddon 等人提出了一种 long-lived 模型.

- Long-lived 模型下的 self-healing 密钥分发机制

与一轮通信模型类似,但在进行第α轮通信时,GM 需要先广播一轮消息$\left\{g^{v_{1,1}^{(\alpha)}},g^{v_{1,2}^{(\alpha)}},...,g^{v_{m,m}^{(\alpha)}}\right\}$,其中,$g$ 是子群 $Z_p\subseteq F_q^*$ 的一个生成元,阶为 p(p 为一素数), $v_{1,1}^{(\alpha)},v_{1,2}^{(\alpha)},...,v_{m,m}^{(\alpha)}\subseteq Z_p^*$ 是一组随机数.然后,第 j 次会话密钥材料的广播消息为 $B_j=B_j^1\cup B_j^2$:

$$B_j^1=\{g^{p_{j'}^{(\alpha)}(x)+v_{j',j}^{(\alpha)}s_{j',j}^{(\alpha)}(N,x)}\}_{j'=1,...,j-1}\cup\{g^{K_j^{(\alpha)}+v_{j,j}^{(\alpha)}s_{j,j}^{(\alpha)}(N,x)}\}\cup\{g^{q_{j'}^{(\alpha)}(x)+v_{j',j}^{(\alpha)}s_{j',j}^{(\alpha)}(N,x)}\}_{j'=j+1,...,m},$$

$$B_j^2=\{w_l,\left\{g^{v_{j',j}^{(\alpha)}s_{j',j}^{(\alpha)}(w_l,x)}\right\}_{j'=1,...,m}\}_{l=1,...,t}.$$

而密钥恢复过程和 self-healing 过程也与前面的模型类似.最后,第 j 次会话密钥为 $g^{K_j^{(\alpha)}}$.此方案基于 DDH 问题假设,所以其安全性是计算安全的.

Staddon 等人的 long-lived 方案延长了机制安全运行时间,而无需用户和群组管理者协商在每轮通信开始时协商新的用户私钥.由于用到了指数运算,计算代价增大,同时,每轮通信过程中群组管理者需要多广播 1 次消息(需要广播$\left\{g^{v_{k,l}^{(\alpha)}}\right\}_{k,l\in\{1,...,m\}}$).所以,此方案中用户存储私钥的代价是 $O(m^2\log q)$,通信代价是 $O((mt(t+1)+m(t+1)+m^2)\log q)$(忽略存储或广播用户 ID 的代价).另外,此方案运行期间内,已被撤销和曾经被撤销的用户不超过 $2t$ 个成员,因为可能用户一旦被撤销,其私钥(秘密信息)会被泄露,而通过 $2t+1$ 个撤销成员的私钥,多项式 $s_{j',j}(x,x)(j',j\in\{1,2,...,m\})$就会被恢复出来,从而攻击者可以冒充合法用户得到会话密钥.Blundo 等人[4]也提出了类似的 long-lived 方案,其同样基于 DDH 问题,所花费的代价也类似于以上方案.同时,此方案是基于 DDH 困难假设,即它的安全性是计算安全的.Liu 等人提出了另外一种较为高效的方案[3].

1.2 Liu等人的方案

Liu 等人也提出了一种较为高效的方案,把通信代价降到 $O(mt\log q)$, 把每个用户的存储代价降到 $O(m\log q)$.它同样把通信过程分为若干轮,每轮有 m 次会话,但是广播密钥材料的消息中采用了遮罩函数,即 $B_j=\{R_i\}\cup\{P_i(x)=g_i(x)p_i(x)+h_i(x)\}_{i=1,...,j}\cup\{Q_i(x)=q_i(x)+f_i(x)\}_{i=j,...,m}$, 其中, $g_i(x)=(x-r_1)(x-r_2)...(x-r_{w_i})$, $R_i=\{r_1,r_2,...,r_{w_i}\}$是被撤销的用户集合;$\{h_j(i),f_j(i)\}_{j=1,...,m}$是用户私钥;$K_i=p_i(x)+q_i(x)$.

Liu 等人的方案在通信复杂度和存储复杂度上都有较大的改进,并且该方案可以在多轮通信安全运行.但是,此方案的缺陷在于泄露了一定量的用户秘密信息,由于 $P_i(x)=g_i(x)p_i(x)+h_i(x)$, 攻击者可以得到 $\{h_i(r_1),...,h_i(r_{w_i})\}$,即攻击者可以得到任何被撤销用户的一部分秘密信息,这将导致比较严重的后果,比如经过一定的信息积累,攻击者可能可以冒充某合法用户.

在本文中,我们提出了一种高效的 long-lived self-healing 密钥分发机制,并对它进行改进,使其通信代价和用户存储密钥代价都得到一定幅度的提高.但是,新机制用域上多项式运算取代了指数运算,使得计算代价大幅度减少.同时,新机制群组管理者和用户之间交互轮数比 Staddon 等人的 long-lived 方案少 1 次.并且其安全性是无条件安全的,新机制不会泄露用户的秘密信息.

2 新的long-lived self-healing密钥分发机制

这一节,我们先给出新机制的大体框架,然后在第 3 节对其进行优化改进.我们同样把整个通信过程分成若干轮,每轮包含 m 轮会话.具体步骤如下:

1. (Initial set-up)群组管理者选择两个随机数 t,N,其中 t 是一个正整数,$N\in F_q$ 并且 $N\notin\{1,\ldots,n\}$(n 是预计用户总数).群组管理者在 $F_q[x]$中随机选择 m^2 个多项式$A_{k,l}(x)=\sum_{i=0}^{2t}a_i^{(k,l)}x^i(k,l\in\{1,...,m\})$.每个用户 U_i 存储各自的私钥:$S_i=\{i,N,A_{1,1}(i),...,A_{m,1}(i),A_{1,2}(i),...,A_{m,m}(i)\}$.
2. (Set-Up for the αth round of m sessions)群组管理者为此轮通信构造出 m^2 个在 $F_q[x,y]$中的多项式 $s_{k,l}^{(\alpha)}(x,y)=\sum_{i=0}^{t}b_{i,j}^{(\alpha)(k,l)}x^iy^j(k,l\in\{1,...,m\})$. 且 $s_{k,l}^{(\alpha)}(x,y)$ 和 $A_{k,l}(x)$ 有如下关系:$\forall r\in\{0,1,2,...,2t\}$, $\sum_{\substack{0\le i\le t,0\le j\le t,\\ i+j=r}}b_{i,j}^{(\alpha)(k,l)}=a_r^{(k,l)}$.

   由此我们发现:

$$s_{k,l}^{(\alpha)}(i,i)=\sum_{r_1,r_2=0}^{t}b_{r_1,r_2}^{(\alpha)(k,l)}i^{r_1}\cdot i^{r_2}=\sum_{r_1,r_2=0}^{t}b_{r_1,r_2}^{(\alpha)(k,l)}i^{r_1+r_2}=\sum_{s=0}^{2t}\left(\sum_{\substack{0\le r_1\le t,0\le r_2\le t,\\ r_1+r_2=s}}b_{r_1,r_2}^{(\alpha)(k,l)}\right)\cdot i^s=\sum_{s=0}^{2t}a_s^{(k,l)}\cdot i^s=A_{k,l}(i).$$

   所以,即使用户所存储的私钥保持不变,每轮的函数 $s_{k,l}^{(\alpha)}(x,y)$ 也可以不同.此外,群组管理者在 $F_q[x]$中随机选择 m 个 t 次多项式 $p_1^{(\alpha)}(x),...,p_m^{(\alpha)}(x)$ 以及一轮通信所使用的 m 个随机数$K_1^{(\alpha)},...,K_m^{(\alpha)}\in Z_p$,定义多项式 $q_j^{(\alpha)}(x)=K_j^{(\alpha)}-p_j^{(\alpha)}(x)(\forall j\in\{1,2,...,m\})$.
3. (Broadcast)$L,R\subseteq\{1,2,...,n\},|R|\le t,L$ 表示合法的用户集合,R 表示撤销用户集合.同时,群组管理者选择 $W=\{w_1,w_2,...,w_t\}\subseteq F_q$,使得 $R\subseteq W,(W-R)\cap(L\cup\{N\})=\varnothing$,于是,第 j 次会话 ($j\in\{1,2,...,m\}$) 相应的广播消息是$B_j=B_j^1\cup B_j^2$:

$$B_j^1=\{p_{j'}^{(\alpha)}(x)+s_{j',j}^{(\alpha)}(N,x)\}_{j'=1,...,j-1}\cup\{K_j^{(\alpha)}+s_{j,j}^{(\alpha)}(N,x)\}\cup\{q_{j'}^{(\alpha)}(x)+s_{j',j}^{(\alpha)}(N,x)\}_{j'=j+1,...,m},$$

$$B_j^2=\{w_l,\{s_{j',j}^{(\alpha)}(w_l,x)\}_{j'=1,...,m}\}_{l=1,...,t}.$$

4. (Session key recovery)设用户 U_i 是合法用户,当他接收到 B_j 以后,根据 B_j^2 可以得到 t 个多项式插值 $s_{j,j}^{(\alpha)}(w_l,i)(l=1,2,...,t)$, 再结合其自身存储的私钥 $A_{j,j}(i)(A_{j,j}(i)=s_{j,j}^{(\alpha)}(i,i))$ 可以恢复出多项式$s_{j,j}^{(\alpha)}(x,i)$, 所以,用户 U_i 可以得到第 j 次会话密钥 $K_j^{(\alpha)}=(K_j^{(\alpha)}+s_{j,j}^{(\alpha)}(N,x))|_{x=i}-s_{j,j}^{(\alpha)}(N,i)$. 同理,$U_i$ 可以恢复一些多项式插值:$\{p_{j'}^{(\alpha)}(i)\}_{j'=1,...,j-1}$ 和 $\{q_{j'}^{(\alpha)}(i)\}_{j'=j+1,...,m}$.
5. (Key self-healing property)当用户 U_i 接收到不连续的两次广播消息 B_{j_1} 和 $B_{j_2}(j_1<j_2)$时,对任意的 $j(j_1<j<j_2)$, 由于 $q_j^{(\alpha)}(i)$ 由消息 B_{j_1} 可以恢复出来,而 $p_j^{(\alpha)}(i)$ 由消息 B_{j_2} 可以恢复出来,则 $K_j^{(\alpha)}=p_j^{(\alpha)}(i)+q_j^{(\alpha)}(i)$.
6. (Join)当在第 α 轮通信的第 j' 次会话时加入成员 U_c 时,只需给此用户分配私钥:$S_c=\{c,N,\{A_{j,l}(i)\}_{j,l\in\{j',...,m\}}\}$.
7. (Revocation)当要撤销某个用户 U_c 时,只需把此成员序号 c 加入到撤销集 R 和集合 W 中,但要使集合 R 和 W 满足第 3 步(Broadcast)中所述的关系式 $R\subseteq W,(W-R)\cap(L\cup\{N\})=\varnothing$. 同时,和以前各种同类型机制一样,一旦某用户被撤销,其在此轮通信过程的剩余会话中就不能再被加入进来.

另外,我们注意到,新机制和原有的各种 self-healing 机制一样,在整个通信过程中,被撤销过的用户(包括已撤销和曾经被撤销的用户)不能超过 $2t$ 个,因为被撤销过的用户的私钥很可能被泄露,而通过 $2t+1$ 个用户的私钥可以恢复出任何一个合法用户的私钥,所以机制将不能继续安全运行.

3 安全性分析

首先,我们给出具有 t 成员撤销能力的 self-healing 密钥分发机制无条件安全定义[1,4].定义中的各种符号与本文第 2 节使用的符号一致.

定义 1. 令 $t,i\in\{1,2,...,n\}$,并且 $j\in\{1,2,...,m\}$.若 D 是一个无条件安全的密钥分发机制,则必须满足如下条件 ($H(\cdot)$ 表示信息的熵):

1) 对任意的合法成员 U_i,记由 S_i 和 B_j 一起推导获得的秘密信息为 $z_{i,j}(z_{i,j}=\{p_1^{(\alpha)}(i),...,p_{j-1}^{(\alpha)}(i),K_j^{(\alpha)},q_{j+1}^{(\alpha)}(i),...,q_m^{(\alpha)}(i)\})$,即 $H(z_{i,j}\mid B_j,S_i)=0$,则会话密钥 $K_j^{(\alpha)}$ 可以由 $z_{i,j}$ 确定,即 $H(K_j^{(\alpha)}\mid z_{i,j})=0$.
2) 对任意的用户集合 $B\subseteq\{U_1,U_2,...,U_n\}, B\leqslant t$,并且 $U_i\notin B$ 且用户 U_i 未被撤销,则集合 B 中用户获取不到任何有关 S_i 的信息,即 $H(S_i\mid\{S_{i'}\}_{U_{i'}\in B},B_1,B_2,...,B_m)=H(S_i)$,也就是说,即使 t-成员合谋攻击也不能获得其他成员的秘密信息.
3) 所有用户 $U_1,U_2,\ldots,U_n$ 都不能只从所有广播消息或个人私钥获得广播消息 B_j 中含的秘密信息 $z_{i,j}$,即 $H(z_{i,j}\mid B_1,B_2,...,B_m)=H(z_{i,j})=H(z_{i,j}\mid S_1,...,S_n)$.

定义 2. D 具有 t 成员撤销能力是指,对于任意集合 $R\subseteq\{U_1,...,U_n\}$,且 $|R|\leqslant t$,则对于任意一次广播消息 B_j,若 $U_i\notin R$, U_i 能够恢复密钥 $K_j^{(\alpha)}$,即 $H(K_j^{(\alpha)}\mid B_j,S_i)=0$;但若 $U_i\in R$,他便不能恢复相应密钥,即 $H(K_j^{(\alpha)}\mid B_j,\{S_{i'}\}_{U_{i'}\in R})=H(K_j^{(\alpha)})$. 也就是说,即使 t 个被撤销的成员进行合谋攻击也不能恢复会话密钥,只有合法成员才能恢复会话密钥.

定义 3. D 具有 self-healing 属性是指,对任意的 $1\leqslant j_1<j<j_2\leqslant m$:

1) 若任意的用户 U_i 在第 j_1 和 j_2 次会话期间都是合法用户,则第 j 次会话密钥 $K_j^{(\alpha)}$ 可以由 $\{z_{i,j_1},z_{i,j_2}\}$ 确定,即 $H(K_j^{(\alpha)}\mid z_{i,j_1},z_{i,j_2})=0$.
2) 对于任意两个没有交集的集合 $B,C\subseteq\{U_1,...,U_n\}$,且 $|B\cup C|\leqslant t$,其中 B 集合是在第 j_1 次会话前被撤销的用户集合(不能再加入此轮剩余会话过程),C 集合是在第 j_2 次会话开始加入系统的用户集合,则秘密信息 $K_j^{(\alpha)}$ 不能由信息 $\{z_{i',l}\}_{U_{i'}\in B,1\leqslant l\leqslant j_1}\cup\{z_{i',l}\}_{U_{i'}\in C,\ j_2\leqslant l\leqslant m}$ 推出,即 $H(K_j^{(\alpha)}\mid\{z_{i',l}\}_{U_{i'}\in B,1\leqslant l\leqslant j_1}\cup\{z_{i',l}\}_{U_{i'}\in C,\ j_2\leqslant l\leqslant m})=H(K_j^{(\alpha)})$.

我们先给出如下的定理:

定理 1. 我们构造的具有每轮 t 次撤销能力的 self-healing 密钥分发机制是无条件安全的.

证明:我们的构造与 Staddon 等人的构造 3(一轮通信模型)区别在于对多项式 $s_{k,l}^{(\alpha)}(x,y)$ $(k,l\in\{1,...,m\})$ 的选取.我们首先简要说明每轮多项式 $s_{k,l}^{(\alpha)}(x,y)$ 各项系数的选取方法.在 $F_q[x]$ 随机选择完多项式 $A_{k,l}(x)$ 之后,多项式 $s_{k,l}^{(\alpha)}(x,y)$ 系数的选择根据第 2 节的描述,我们有如下关系式:

$$\begin{cases}
\boxed{b_{t,t}^{(\alpha)(k,l)}} & = a_{2t}^{(k,l)}\\
b_{t-1,t}^{(\alpha)(k,l)}+\boxed{b_{t,t-1}^{(\alpha)(k,l)}} & = a_{2t-1}^{(k,l)}\\
\cdots & \cdots\\
b_{1,t}^{(\alpha)(k,l)}+b_{2,t-1}^{(\alpha)(k,l)}+...+\boxed{b_{t,1}^{(\alpha)(k,l)}} & = a_{t+1}^{(k,l)}\\
\boxed{b_{0,t}^{(\alpha)(k,l)}}+b_{1,t-1}^{(\alpha)(k,l)}+b_{2,t-2}^{(\alpha)(k,l)}+...+b_{t,0}^{(\alpha)(k,l)} & = a_t^{(k,l)}\\
\boxed{b_{0,t-1}^{(\alpha)(k,l)}}+b_{1,t-2}^{(\alpha)(k,l)}+b_{2,t-3}^{(\alpha)(k,l)}+...+b_{t-1,0}^{(\alpha)(k,l)} & = a_{t-1}^{(k,l)}\\
\cdots & \cdots\\
\boxed{b_{0,2}^{(\alpha)(k,l)}}+b_{1,1}^{(\alpha)(k,l)}+b_{2,0}^{(\alpha)(k,l)} & = a_2^{(k,l)}\\
b_{0,1}^{(\alpha)(k,l)}+\boxed{b_{1,0}^{(\alpha)(k,l)}} & = a_1^{(k,l)}\\
\boxed{b_{0,0}^{(\alpha)(k,l)}} & = a_0^{(k,l)}
\end{cases}\tag{1}$$

则在上面的关系式左边的所有项中,先选择除了带方框项以外的其余各项,这些项均可以在 $F_q[x]$ 上随机且独立地选择,然后由多项式 $A_{k,l}(x)$ 的系数得到相应的带方框的项(注意,$A_{k,l}(x)$ 的各项系数也是非公开的).这样就构

造出了所需要的多项式$s_{k,l}^{(\alpha)}(x,y)$.而多项式$s_{k,l}^{(\alpha)}(N,x)=\sum_{r_2=0}^{t}\left(\sum_{r_1=0}^{t}b_{r_1,r_2}^{(\alpha)(k,l)}N^{r_1}\right)\cdot x^{r_2}$,所以,根据式(1)中系数的选取方法,$s_{k,l}^{(\alpha)}(N,x)$ 中各项系数在用户看来是在 $F_q[x]$上随机且独立选择的.同理,$s_{k,l}^{(\alpha)}(w_i,x),s_{k,l}^{(\alpha)}(x,i)$ 中各项系数在用户看来也是在 $F_q[x]$上随机且独立选择的.因此,新方案中的广播消息与 Staddon 等人一轮通信模型中的广播消息所含有的信息量相同,所以与旧方案一致,我们的方案符合上述安全性的 3 个定义(证明方法是 t 次一元多项式的确定至少需要 t+1 个该多项式的插值,否则,该多项式的选取在攻击者看来是在 $F_q[x]$上均匀分布的). □

4 增强合法用户恢复密钥能力

现在我们考虑以下情形:当合法用户 U_i 接收到第 j_1 次会话广播消息后,在第 j_2 次会话时被撤销,当他接收到第 j_2 次会话广播消息后,上面给出的方案不能提供 U_i 恢复第 j_1 次到第 j_2 次期间所有会话密钥(用户 U_i 在此段时间内是合法用户)的能力.为此,我们修改新机制中 Initial set-up 和 Broadcast 的过程如下:

1. (Initial set-up)此阶段群组管理者除了要完成第 2 节中描述的过程以外,还要选择有序集合 $\overline{W}=\{\overline{w}_1,\overline{w}_2,...,\overline{w}_t\}\subseteq F_q$,使得 $\overline{W}\cap(U\cup\{N\})=\varnothing$($U$ 表示所有可能的用户集合,N 是一个在第 2 节中所选的整数),并且公开集合 $\overline{W}$.
2. (Broadcast) $L,R\subseteq\{1,2,...,n\},|R|\le t$, L 表示合法的用户集合,R 表示已撤销用户的有序集合(按照用户的序号排列).在进行第 j 次会话($j\in\{1,2,...,m\}$)时,令$|R|=r_j,R=\{r_1,r_2,...,r_{r_j}\}$,群组管理者构造有序集合 W_j,$W_j=\{w_{j,1},w_{j,2},...,w_{j,t}\}=\{r_1,r_2,...,r_{r_j},\overline{w}_1,\overline{w}_2,...,\overline{w}_{t-r_j}\}$(注意,$R\subseteq W_j,(W_j-R)\cap(L\cup\{N\})=\varnothing$).对任意 $i\in\{1,2,...,r_j\}$,令 r_i 在第 x_i 次会话期间被撤销(一旦某成员被撤销,其在此轮通信剩余过程中就都被撤销,故 $x_i\le j$),于是,第 j 次会话($j\in\{1,2,...,m\}$)相应的广播消息是 $B_j=B_j^1\cup B_j^2$:

$$B_j^1=\{p_{j'}^{(\alpha)}(x)+s_{j',j'}^{(\alpha)}(N,x)\}_{j'=1,...,j-1}\cup\{K_j^{(\alpha)}+s_{j,j}^{(\alpha)}(N,x)\}\cup\{q_{j'}^{(\alpha)}(x)+s_{j',j}^{(\alpha)}(N,x)\}_{j'=j+1,...,m},$$

$$B_j^2=\{\langle r_i,x_i\rangle\}_{i=1,2,...,r_j}\cup\{\{s_{j',j'}^{(\alpha)}(w_{j',l},x)\}_{l=1,...,t}\}_{j'=1,...,j-1}\cup\{\{s_{j',j}^{(\alpha)}(w_{j,l},x)\}_{l=1,...,t}\}_{j'=j,...,m}.$$

现在我们分析此方案的正确性.当用户 U_i 接收到消息 B_j 后,他能够恢复有序集合 $W_{j'}$ ($1\le j'\le j$),$W_{j'}=\{r_{i_1},r_{i_2},...,r_{i_k},\overline{w}_1,\overline{w}_2,...,\overline{w}_{t-k}\}$,其中,$\{r_{i_1},r_{i_2},...,r_{i_k}\}$是符合以下条件的最大的集合:$\{r_{i_1},r_{i_2},...,r_{i_k}\}\subseteq R$,且 $i_1<i_2<...<i_k,\forall l\in\{1,2,...,k\},x_{i_l}\le j'$.因此,当 U_i 接收到第 j_1 次会话广播消息和第 j_2 次会话广播消息后,并在第 j_2 次会话时被撤销,他依旧能够恢复第 $j(j_1<j<j_2)$次会话密钥,因为通过 B_{j_1} 可以恢复出多项式$s_{j,j_1}^{(\alpha)}(x,i)$,从而得到$q_j^{(\alpha)}(i)=(q_j^{(\alpha)}(x)+s_{j,j_1}^{(\alpha)}(N,x))|_{x=i}-s_{j,j_1}^{(\alpha)}(N,i)$,然后通过 B_{j_2} 恢复出多项式$s_{j,j}^{(\alpha)}(x,i)$,从而得到值$p_j^{(\alpha)}(i)$,最后由$K_j^{(\alpha)}=p_j^{(\alpha)}(i)+q_j^{(\alpha)}(i)$ 得到第 j 次会话的密钥.

以上对第 2 节所描述机制(记为机制 1)的改进(记为机制 2)对安全性没有影响,因为机制 2 中用户端存储的私钥信息和群组管理者广播的消息所包含的信息是机制 1 所包含信息的子集,其公开的信息量少于机制 1 公开的信息量,所以优化后的机制仍然是无条件安全的.

除此之外,此方案还有一个优点就是用户 U_i 只需存储私钥$\{i,N,\{A_{k,l}(i)\}_{k,l\in\{1,2,...,m\},k\ge l}\}$,节省了用户的存储空间.现在,我们来分析机制 2 用户端存储代价和通信代价.因为用户 ID 可以从一个很小的域中选择,而每轮通信过程中撤销用户最多为 t 个,故我们可以忽略存储或者广播用户 ID 的代价.由于用户不需要存储$\{A_{k,l}(i)\}_{k,l\in\{1,2,...,m\},k<l}$,所以其存储代价是$O\left(\frac{m(m+1)}{2}\log q\right)$;而广播消息 B_j^1 包含 m 个 t 次多项式,广播消息 B_j^2 包含 mt 个 t 次多项式和最多 t 个撤销用户的信息,所以通信代价是$O((mt(t+1)+m(t+1))\log q)$.

5 与原有方案的比较

在本文第 1 节,我们回顾了一些原有的 self-healing 机制,并指出了它们各自的缺点.Staddon 等人在文献[1]中以及 Blundo 等人在文献[4]中各自提出的 long-lived 方案均采用了指数运算,计算代价较大;在每次会话密钥

分发过程中,群组管理者需要多广播1次消息;并且这两种方案由于都是基于DDH困难问题假设,所以安全性都是计算安全的.Liu 等人的方案[3]虽然在效率上比前两个方案有较大提高,但攻击者可以轻易地获得一些用户的一部分秘密信息,当这些秘密信息积累到一定程度时,self-healing 密钥分发机制将不再安全,攻击者可以获得其想要的会话密钥(具体攻击方法参见本文第 1.2 节).

在新方案中,我们弥补了上述的各种缺陷,并且使花费的代价尽可能地最优,其中用户端存储私钥的代价是$O\left(\frac{m(m+1)}{2}\log q\right)$,而通信代价为$O((mt(t+1)+m(t+1))\log q)$.其优势在于:

1. 我们避免了使用指数运算,而只是域上多项式的相关运算,降低了计算复杂度.
2. 群组管理者广播消息次数比 Staddon 等人和 Blundo 等人的方案少 1 次.
3. 用户端存储私钥数目比 Staddon 等人的方案少将近一半.
4. 与 Liu 等人的方案相比,新方案没有泄露用户秘密信息.且其安全性为无条件安全,而不再像 Staddon 等人和 Blundo 等人的机制那样建立在 DDH 困难问题假设的基础上.

6 结 论

在本文中,我们提出了一种高效的 long-lived self-healing 密钥分发机制,存储代价是$O\left(\frac{m(m+1)}{2}\log q\right)$,而通信代价是$O((mt(t+1)+m(t+1))\log q)$.新机制避免了使用指数运算使得计算效率大幅度提高,并且由于不再基于 DDH 假设,所以安全性不再是计算安全,而是无条件安全.另外,我们增强了用户恢复合理密钥的能力,使得在某些比较特殊的情况下仍能恢复出密钥,同时,用户所存储的私钥数目是 Staddon 等人的机制的一半,从而节省了用户端的存储空间,并且广播消息次数减少了 1 次.

在对 self-healing 密钥分发机制的研究中,一个仍然有趣且具挑战性的问题在于,如何在用户的私钥存储量和广播消息长度两者之间取得更好的优化关系.新机制中仍旧存在一个弊端,即和原有各种机制一样,在整个通信过程中,撤销过的用户数(包括已撤销和曾撤销的用户)不能超过 $2t$,因为撤销的用户容易泄露其私钥,而通过 $2t+1$ 个用户的私钥可以恢复出任何一个合法用户的私钥.

References:

[1] Staddon J, Miner S, Franklin M, Balfanz D, Malkin M, Dean D. Self-Healing key distribution with revocation. In: Abadi M, Bellovin S, eds. Proc. of the IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2002. 224−240.

[2] Miner S, Malkin M, Staddon J, Balfanz D. Sliding-Window self-healing key distribution. In: Liu P, Pal P, eds. Proc. of the 2003 ACM Workshop on Survivable and Self-Regenerative Systems. Fairfax: ACM Press, 2003. 82−90.

[3] Liu D, Ning P, Sun K. Efficient self-healing group key distribution with revocation capability. In: Atluri V, Jaeger T, eds. Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington: ACM Press, 2003. 231−240.

[4] Blundo C, D'Arco P, Santis A, Listo M. Design of self-healing key distribution schemes. Design Codes and Cryptography, 2004,32(1-3):15−44.

[5] Blundo C, D'Arco, de Santis A. On self-healing key distribution schemes. IEEE Trans. on Information Theory, 2006,52(12): 5455−5467.

李徽(1983－),男,江西南昌人,博士生,主要研究领域为密码学,信息安全.

武传坤(1964－),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全.