文章编号:1671 - 6833(2011)05 - 0077 - 03

# 可区分共享者角色的可验证的多秘密共享方案

刘 恒

(玉林师范学院 计算机科学与工程学院,广西 玉林 537000)

**摘 要**:针对前期研究中可区分秘密分享者角色的防欺诈秘密共享方案不能抵抗秘密分发者欺诈的缺点,提出一个改进的可区分共享者角色的可验证的多秘密共享方案.该方案不仅能抵抗共享者的欺骗,也能抵抗秘密分发者的欺诈;各共享者的秘密份额可以重复使用,每个共享者仅需维护一个秘密份额即可共享多个秘密;同时可以方便地实现数字签名,是一个可验证的多秘密共享方案.

**关键词**:多秘密共享;共享者角色;可验证;数字签名

**中图分类号**:TP309 **文献标志码**:A

## 0 引言

1979 年,Shamir[1] 和 Blakley[2] 独立地提出了秘密共享这一思想.此外,还有基于中国剩余定理的 Asmuth-Bloom 法[3] 和使用矩阵乘法的 Karnin-Greene-Hellman 法[4] 等.近 30 年来,学者们针对不同的应用问题,提出了各种各样的方案,例如可验证的秘密共享和多秘密共享,具体可参考文献[5 - 6].

笔者前期研究中提出的可区分秘密分享者角色的防欺诈秘密共享方案[7] 已假定秘密分发者诚实可信,在进行秘密共享方案的初始化过程中,一旦秘密分发者作弊,分发出来的是错误的或者虚假的数据,则秘密共享方案失败,该方案是单秘密共享方案,也就是说,秘密份额是一次性的,只能使用一次,这在现实应用中是很难让人满意.为了可以同时共享多个秘密,且达到防止秘密分发者的欺诈和共享者的欺骗,笔者在前期方案[7] 的基础上提出了一个可区分共享者角色的可验证的多秘密共享方案.

## 1 改进后的方案

在下面的描述中,$E(M,K)$ 表示用密钥 $K$ 对报文 $M$ 加密后得到的密文.为讨论方便,先假设分享秘密的共享者分别为 $A$、$B$ 和 $C$ 共 3 种角色,若有更多的角色类别可类推.

### 1.1 参数建立

方案有 1 个秘密分发者和 $n$ 个共享者.秘密分发者设为 $D$,$n$ 个共享者是 $P_1,P_2,\cdots,P_n$,担任 $A$、$B$、$C$ 共 3 种角色中的 1 种,$M_1,M_2,\cdots,M_m$ 是所要共享的 $m$ 个秘密.$D$ 利用密钥分配器分别向三类共享者分配密钥,密钥分配器是产生密钥和加密所产生密钥的中心源 $G$,事先为 $G$ 设置一个密钥 $K_G$.有一个系统公告牌,每个共享者均可读到公告牌上的内容,但无权向公告牌上写内容,只有 $D$ 可以在公告牌上修改或写入内容.$D$ 事先进行几项工作.

(1) 选定一个大素数 $p$ 和一个生成元 $g$,$g$ 为 $Z_p$ 的生成元,这两个数字公布在公告牌上.

(2) 选定一个素数 $q$,其中 $q|p-1$.

(3) 选 $h$ 是 $p$ 的一个素根,即 $h^n \equiv 1 \bmod p$.

(4) $D$ 的私钥,即要分割的密钥为 $S$.选择正整数 $a$、$b$、$c(a+b+c>=p)$,这 3 个数字保密,满足 $S=a+b+c \bmod p$,且将 $S$ 分解为 $n$ 个 $\{s_i\}$,将它的公开密钥 $T=g^S \bmod p$ 公布在公告牌上.

(5) 设 $f(r,s)$ 是一个二元单向函数,具有如下性质:

a) 已知 $r$、$s$,容易计算出 $f(r,s)$;

b) 已知 $s$ 和 $f(r,s)$,不能求出 $r$;

c) 已知 $r$ 和 $f(r,s)$,不能求出 $s$;

收稿日期:2011 - 04 - 29;修订日期:2011 - 06 - 25

基金项目:广西省自然科学基金资助项目(0832286);广西教育科学"十一五"规划项目(2008B40);玉林师范学院青年科研资助项目(2009YJQN12)

作者简介:刘恒(1979 - ),女,广西梧州人,玉林师范学院讲师,主要从事信息安全和密码学、无线传感器网络研究,E-mail:jgxylh@126.com.

d)未知 $s$,对任意 $r$,难以计算 $f(r,s)$;

e)已知 $s$,找到不同的 $r_1$ 和 $r_2$ 满足 $f(r_1,s)=f(r_2,s)$ 在计算上是不可行的;

f)已知任意多的 $(r_i,f(r_i,s))$ 对,其中 $r\neq r_i$,求 $f(r,s)$ 是不可行的.

随机选择一个整数 $r$ 将其公布在公告牌上,$r\in Z_p$,计算出 $f(r,s_i)$ 和 $\sigma_i=g^{f(r,s_i)}\bmod p(i=1,\cdots,n)$.

(6) 在 $[m,p-1]$ 中选取 $n$ 个随机整数 $u_i(i=1,\cdots,n)$ 分别作为每个共享者 $P_i$ 的公开身份信息.

(7) 根据 $n+m$ 个数值对 $(0,M_1),(1,M_2),\cdots,(m-1,M_m)$ 以及 $(u_i,f(r,s_i)),i=1,\cdots,n$,构造 $n+m-1$ 次多项式:$h(x)=a_0+a_1x+a_2x^2+\cdots+a_{n+m-1}x^{n+m-1}$. 计算出 $\varepsilon_j\equiv g^{a_j}\bmod p(j=0.1,\cdots,n+m-1)$,并公布在公告牌上.

(8) 从集合 $[m,p-1]/Y\{u_i\}(i=1,\cdots,n)$ 中取出最小的 $n+m-t$ 个整数 $d_1,d_2,\cdots,d_{n+m-t}$,并计算出 $h(d_k)$ 和 $\tau_k=g^{h(d_k)}\bmod p$,其中 $k=1,\cdots,n+m-t$,并将 $\tau_k$ 公布在公告牌上.

### 1.2 秘密分发

密钥分配器对共享者进行身份鉴别后,先向 $A$ 类用户分配密钥,过程如下:密钥分配器随机产生大量密钥 $K_1,K_2,\cdots,K_i$,这些密钥都满足条件 $K_i\bmod p=a$,并用 $K_G$ 加密形成密钥流. 设某 $A$ 类共享者 $A_1$ 获得 $G$ 发来的一些经过 $K_G$ 加密的密钥后,选择其中一个,如 $E(K_{A_1},K_G)$. 这时,$A_1$ 在电脑终端输入一个密码 $K'_{A_1}$,用 $K'_{A_1}$ 来加密所选择的密钥,形成 $E(E(K_{A_1},K_G),K'_{A_1})$,并将这个经过两次加密的密钥回送给 $G$ 解密这一密钥,使之只处在 $K'_{A_1}$ 保护下,即 $E(E_{A_1},K'_{A_1})$,并将其发送给 $A_1$,$A_1$ 用 $K'_{A_1}$ 对之解密,则得到自己挑选的密钥 $K_{A_1}$,同时它在域中产生随机数 $a_{A_1}$,将 $a_{A_1}K_{A_1}$ 作为自己的私钥,然后将之代入到下面的式子中:$P_{A_1}=g^{K_{aA_1}}\bmod p$. 求出 $P_{A_1}$ 作为自己的公钥,并将 $P_{A_1}$ 发送给 $G$.

接下来密钥分配器向 $B$ 类共享者分配密钥,流程与前面所述的 $A$ 类共享者相似,唯一改变的是,密钥分配器随机产生的大量密钥都满足条件:$K_i\bmod p=b$;而对于 $C$ 类共享者,密钥分配器随机产生的大量密钥都满足条件:$K_i\bmod p=c$.

分配结束后,每个共享者都得到了个人的私钥,而密钥分配器 $G$ 上则有每个共享者的公钥. $D$ 可以把这些公钥整理成共享者的公钥表公布在公告牌上,以后可以用于验证共享者的数字签名.

在新方案中,$a$、$b$、$c$ 是秘密片段,是共享秘密的影子,而每个共享者的私钥可以认为是 $a$、$b$、$c$ 的影子,正因为有这种影子的扩展,每种角色的人员都可以有无数个. 密钥分配器可以同时分配多个密钥,达到多秘密共享,则有:

(1) $a_1a_2,\cdots,a_x;b_1,b_2,\cdots,b_y;c_1,c_2,\cdots,c_z,x+y+z=m$.

(2) $P_{A_1},P_{A_2},\cdots,P_{A_{n1}};P_{B_1},P_{B_2},\cdots,P_{B_{n2}};P_{C_1},P_{C_2},\cdots,P_{C_{n3}},n1+n2+n3=n$.

### 1.3 密钥使用

当需要获得共享的秘密时,只要每种角色中各有一人合作即可恢复. 但有时并不需要恢复秘密,而只需要确认某 3 个人分别持有 3 个角色的秘密片段,且他们都认可某个消息. 假设一个消息 $M$ 要求必须经过上述 3 种角色中各一人的认可才能生效,设 $A$ 角色中某个 $A_i$ 看过消息 $M$ 后认可此消息,则他需要用到他的私钥进行以下操作:

①求出 $a=K_{A_i}\bmod p$;②计算 $T_1=g^a\bmod p$;③用私钥对消息 $M$ 与 $T_1$ 进行签名,并发送给验证者.

同时,如果 $B$ 角色中的某个 $B_i$ 看过消息 $M$ 后也认可此消息,则他也进行类似的计算并签名. 在经过最后一个人签名后,验证者可利用 $D$ 的公钥验证:$T=(T_1\times T_2\times T_3)\bmod p$. 如果该式成立,则可确认:

(1) 这 3 个人分别是 $A$、$B$、$C$ 共 3 个角色的成员;(2) 这 3 个人都认可消息 $M$,则 $T_1$、$T_2$、$T_3$ 是这 3 个人的认证片段.

如果该式不成立,则可以对 $T_1$、$T_2$、$T_3$ 分别验证 $T_1=g^a\bmod p$,$T_2=g^b\bmod p$,$T_3=g^c\bmod p$,哪个式子不成立则说明哪个人是非法的共享者.

更进一步,如果要区分某种角色中不同人员的权限,则先要对该角色的秘密片段进行进一步的切割,比如,对 $A$ 角色中的高级共享者,向其分配秘密片段 $a$;对 $A$ 角色的普通共享者,向其分配的秘密片段为 $\frac{a}{2}$,这样,两个普通共享者认可消息 $M$ 就相当于一个高级共享者认可消息 $M$,从而区别其权限. 对各角色的秘密片段做更精细的切割,可以实现更精细的权限管理.

## 2 安全性论证

(1) 识别秘密分发者的欺诈. 根据公告牌上的相关参数,每一个共享者都可以通过

$$g^{f(r,s_i)} = \prod_{j=0}^{n+m-1} \varepsilon_j^{u_i^j} \bmod p \qquad \text{(等式 1)}$$

和

$$\tau_k = \prod_{j=0}^{n+m-1} \varepsilon_j^{d_k^j} \bmod p \qquad \text{(等式 2)}$$

来验证消息的正确性,从而识别出恶意的秘密分发者.

可以证明:$g^{f(r,s_i)} = g^{h(u_i)} = g^{a_0+a_1u_i+\cdots+a_{n+m-1}u_i^{n+m-1}} = \prod_{j=0}^{n+m-1} \varepsilon_j^{u_i^j} \bmod p$. 可见,当 $D$ 无欺诈行为时,等式(1)是成立的. 等式(2)的证明类似等式(1).

(2) 识别共享者的欺骗. 当需要恢复共享的秘密信息 $M$ 时,$n$ 个共享者中可能存在内部欺骗者或外部欺骗者,其中,内部欺骗者出示假的片段以阻止共享的秘密信息的正确恢复,外部欺骗者则设法参与共享的秘密信息的恢复以获得 $M$.

检测内部或外部欺骗者,一是可以根据对 $T_1$、$T_2$、$T_3$ 分别验证 $T_1 = g^a \bmod p$, $T_2 = g^b \bmod p$, $T_3 = g^c \bmod p$ 识别;二是即使欺骗者窃取了秘密片段 $a$ 或 $b$ 或 $c$,并由此得出了合法的认证片段,但是由于合法的共享者的私钥是由 $a$ 或 $b$ 或 $c$ 随机生成的,欺骗者很难由其得到某个合法共享者的私钥,这样秘密分发者在利用公钥表验证共享者的签名时就可识别出欺骗者,因为欺骗者的签名是用假私钥冒充某个合法共享者签的.

## 3　结论

笔者在前题研究的基础上提出了一个可区分共享者角色的可验证的多秘密共享方案,除了保留原方案的优良特性外,还能有效地防止恶意的秘密分发者分发伪信息. 同时,根据二元单向函数的特性,在秘密恢复过程中,使用子秘密 $s_i$ 的伪份额为 $f(r,s_i)$,可知任何参与者的子秘密都不会被泄露,因为尽管秘密恢复了,但是子秘密仍然是安全的,可以在下次秘密共享中继续使用,只要重新选择一个随机数 $r$ 即可,从而达到了多秘密共享. 数字签名可继续沿用原方案[7]中的签名算法,共享者完成签名后,别人无论何时要验证其签名,只要从秘密分发者原来制作的公钥列表上读取其公钥,对其运用 DSS 数字签名的验证算法即可. 该方案具有广阔的应用前景,如何产生 $f(r,s)$ 的表达式和增强密钥使用的安全性,将是笔者下一步的研究方向.

## 参考文献:


[1] SHAMIR A. How to share a secret[J]. Comm of ACM, 1979, 22(1): 612 - 613.

[2] BLAKLEY G R. Safeguarding cryptographic keys[C] // Proc NCC, AFIPS Press, Montvale, 1979, 48: 313 - 317.

[3] ASMUTH C, BLOOM J. A Modular approach to key safegrarding[J]. IEEE Transactions On Information Theory, 1983, 29(2): 208 - 210.

[4] KARNIN E D, GREEN J W, HELLMAN M E. On sharing secret systems[J]. IEEE Transactions On Information Theory, 1983, 29(1): 35 - 41.

[5] 庞辽军,李慧贤,李志洁,等. 一个可验证的门限多秘密共享方案[J]. 哈尔滨工业大学学报,2008, 40(9): 1462 - 1465.

[6] 周洪伟, 郭渊博, 李沁. 门限多重秘密共享方案[J]. 计算机工程与设计,2008, 29(8): 1946 - 1951.

[7] LIU Heng, WU Hua-jian. A cheating-proof secret-sharing scheme capable of differentiating the roles of the secret sharers[J]. Journal of zhengzhou: Natural science,2006,38(3): 35 - 38.


## A Verifiable Multi-Secret Sharing Scheme Differentiating the Roles of the Sharers


LIU Heng

(School of Computer Science and Engineering, Yulin Normal University, Yulin 537000, China)



**Abstract**: In view of the shortcomings in resisting the secret dealer's fraud in the anti-fraud secret-sharing scheme differentiating the roles of the secret sharers put forwarded in early time, the author proposed an improved verifiable multi-secret sharing scheme differentiating the roles of the secret sharers. This scheme is able to resist the fraud from sharers and share dealers, and it can only one reusable secret shadow is required to be kept by each sharer for sharing multiple secrets, and it can easily realize the implementation of digital signature.



**Key words**: multi-secret sharing; role of the secret sharers; verifiable; digital signature