一种安全有效的(t, n)多秘密共享认证方案

谢 琪[*,***] 于秀源[**] 王继林[***]
[*](浙江大学数学系 杭州 310027)
[**](杭州师范学院 杭州 310012)
[***](浙江财经学院信息学院 杭州 310012)

摘 要：基于双子密钥的思想给出了一种安全有效的 (t, n) 多秘密共享认证方案，其优点是每个成员可以多次使用自己的子密钥来恢复庄家任意给定的用于共享的多个密钥，重构一个密钥只需公开 3 个参数，为抵抗成员的欺骗无须执行零知识证明协议。所给的方案与已有的方案相比在计算量和通信量方面有明显的优越性。

关键词： 多秘密分享，成员欺骗，认证
中图分类号：TP309， TN918.1 **文献标识码**：A **文章编号**：1009-5896(2005)09-1476-03

A secure and Efficient (t, n) Multisecret Sharing Authenticating Scheme

Xie Qi[*,***] Yu Xiu-yuan[**] Wang Ji-lin[***]
*(*Department of Mathematics, Zhejiang University, Hangzhou* 310027, *China*)
**(*Hangzhou Teachers College, Hangzhou* 310012, *China*)
***(*School of Information, Zhejiang University of Finance & Economics, Hangzhou* 310012, *China*)

Abstract A secure and efficient (t, n) multisecret sharing authenticating scheme based on double shadow is proposed. The main merits are that the participant can reuse his shadows to recover the sharing multiple secrets that the dealer given and it only needs three parameters to reconstruct one secret, and need not to perform a zero-knowledge protocol to prevent the participant cheating. The proposed scheme is clearly superior to the other existing schemes in terms of both computational costs and communication costs.

Key words Multisecret sharing, Participant cheating, Authenticating

1 引言

秘密分享是现代密码学的重要内容之一，在目前的信息化时代有重要的应用。1979 年 Shamir[1]和 Blakley[2]分别提出了(t, n)门限方案以解决秘密分享的问题，其基本思想是庄家(Dealer)选定主密钥 k，并将 k 分割成 n 份子密钥给 n 个成员，当子密钥的数目大于或等于门限值 t 时才可以导出主密钥 k，当子密钥的数目少于门限值时得不到主密钥。

自从(t, n)门限方案被提出来以后，秘密分享问题得到了广泛的研究，提出了许多方案。但这些方案大多存在一些问题，如无法抵抗庄家的欺骗和成员的欺骗，成员的子密钥只能使用一次等。针对以上不足，Harn[3]给出了可以抵抗庄家和成员欺骗的(t, n)门限多秘密共享认证方案，其缺点是为防止庄家和成员的欺骗需要执行在线的交互验证，而这必须进行大量的模幂乘运算，计算量和通信量都很大，而且只能共享预定或计算所得的密钥。1999 年，Lin 等人[4]提出了一种可以多次使用子密钥的多秘密共享方案，重构一个密钥只需公开 4 个参数，而且防止庄家和成员的欺骗的计算量低于 Harn 的方案。然而，He 等人[5]给出的一个攻击方案表明，Lin 等人的方案无法抵抗成员的欺骗，任何一个成员可以欺骗其他成员以便只有他自己才可以重构密钥。2002 年，He 等人[6]提出了一种多密钥共享认证方案，但为了抵抗成员的欺骗，必须执行零知识证明协议，而这会增加计算量和通信量。

本文基于双子密钥的的思想，给出了一个安全有效的多密钥共享认证方案，每个成员可以多次使用自己的子密钥，重构一个共享秘密只需公开 3 个参数，而且为抵抗成员的欺骗无须执行零知识证明协议，克服了 Lin 等人的方案的安全性缺陷，而计算量和通信量优于 He 等人的方案。

2004-05-17 收到，2004-08-23 改回
国家自然科学基金(10271037)资助课题

2　提出的新方案

2.1 实现的思想

提出的新方案采用了双子密钥的思想，就是庄家给每个成员生成一个子密钥，同时由该子密钥和庄家的私钥生成另一个子密钥，考虑到两个子密钥和庄家的私钥三者密切相关，可以抵抗庄家的欺骗；同时在秘密恢复阶段，每个成员必须使用两个子密钥，从而可以抵抗 He 等人[5]提出的成员的欺骗。

2.2 具体的方案

提出的新方案由系统初始化、子密钥的生成、秘密重构参数的生成、密钥的重构 4 个阶段组成。

(1) 系统初始化　庄家(Dealer)生成一个公告牌 NB 用于存放公开参数，并选择以下参数：

选定大素数 p' 和 q'，计算 $p=2p'+1$ 和 $q=2q'+1$，使得 p 和 q 也为素数，计算 $N=pq$ 和 $R=p'q'$，g 为 Z_N 中阶为 R 的生成元，(e, d)为密钥对，满足 $ed=1(\bmod R)$。庄家任取一个数 $x\in Z_n^*$ 作为自己的私钥，计算自己的公钥 $y=g^x \bmod N$。庄家在NB中公开$\{N, g, e, y\}$，而$\{d, R, x\}$保密。

(2) 子密钥的生成　设 $S=\{S_1,S_2,\cdots,S_m\}$ 是密钥集，$U=\{U_1,U_2,\cdots,U_n\}$ 是 n 个成员，其对应的身份为 ID_i $(i=1,2,\cdots,n)$。庄家随机生成一个 $t-1$ 阶的多项式 $f(x)=\sum_{i=0}^{t-1}a_ix^i \pmod R$，计算 $V=\{V_0,V_1,V_2,\cdots,V_{t-1}\}$，这里 $V_i=yx_i g^{a_i} \pmod N$，$a_i\in Z_R$，$i=0,1,2,\cdots,n$。

接着，庄家为每个成员 $U_i\in U$ 计算子密钥：$x_i=f(\mathrm{ID}_i)P_i^{-1} \pmod R$，其中，$P_i=\prod_{k=0,k\neq i}^{n}(\mathrm{ID}_i-\mathrm{ID}_k) \pmod R$，并计算另一个子密钥 $x_i'=xx_i \bmod R$。然后，庄家把$\{g^{P_i} \bmod N, x_i, x_i'\}$通过安全的信道发送给 U_i，同时为 U_i 计算公钥 $y_i=g^{x_i} \bmod N$，最后庄家把 V 和 y_i 放到NB中。U_i 收到 x_i 和 x_i' 后，可以通过 $(g^{P_i})^{x_i}=\prod_{k=0}^{t-1}(V_k)^{(\mathrm{ID}_i)^k} \bmod N$ 和 $y^{xi}=g^{x_i'} \bmod N$ 来验证 x_i 和 x_i' 的正确性。

(3) 秘密重构参数的生成　庄家针对 $S_i\in S$ 随机选择一个整数 $t_i\in Z_N$，$i=0,1,2,\cdots,n$，并计算：

$$C_i=(g^{1+x}t_i^x)^d \bmod N \tag{1}$$

从 $D_iC_i\equiv 1 \bmod R$ 中求得 D_i，然后计算：

$$T_i=(gt_i)^{D_id} \bmod N \tag{2}$$

$$h_i=(T_i^{xa_0}-S_i)C_i^{-a_0} \bmod N \tag{3}$$

最后，庄家把$\{T_i, C_i, h_i\}$放入 NB 中。

(4) 秘密的重构　设 w 是 U 中要重构密钥 S_i 的 t 个成员的集合。每个 $U_j\in w$ 从 NB 中获取$\{T_i, C_i, h_i\}$，计算 $A_{ij}=(T_i)^{x_j} \pmod N$和 $B_{ij}=(C_i)^{x_j} \pmod N$，并把$\{A_{ij}, B_{ij}\}$发送给 w 中的其他成员。

当收到所有的$\{A_{ij}, B_{ij}\}$后，w 中的每个成员验证下式是否成立：

$$(B_{ij})^e=y_jA_{ij}^{C_ie} \bmod N \tag{4}$$

验证式的正确性证明如下：

$$\begin{aligned}(B_{ij})^e=(C_i)^{ex_j}&=(g^{1+x}t_i^x)^{x_j}=y_jg^{xx_j}(t_i)^{xx_j}=y_j(gt_i)^{x_j'D_iC_ied}\\&=y_j(T_i)^{C_iex_j'}=y_jA_{ij}^{C_ie} \pmod N\end{aligned}$$

如果式(4)成立，则每个成员可以利用下式来构造出秘密 S_i：

$$S_i=\prod_{U_j\in w}(A_{ij})^{\Delta_j}-h_i\left(\prod_{U_j\in w}(B_{ij})^{\Delta_j}\right) \bmod N \tag{5}$$

其中

$$\Delta_j=\prod_{U_k\in w-\{U_j\}}(-\mathrm{ID}_k)\prod_{U_k\in U-w}(\mathrm{ID}_j-\mathrm{ID}_k)$$

w 中的每个成员都可以从式(5)重构出秘密 $S_i\in S$，其重构的过程如下：

因为

$$\begin{aligned}&\sum_{U_j\in w}(x_j\Delta_j)\\&=\sum_{U_j\in w}(f(\mathrm{ID}_j)P_j^{-1}\Delta_j)\\&=\sum_{U_j\in w}f(\mathrm{ID}_j)\prod_{U_k\in U-\{U_j\}}(\mathrm{ID}_j-\mathrm{ID}_k)^{-1}\\&\quad\times\prod_{U_k\in w-\{U_j\}}(-\mathrm{ID}_k)\prod_{U_k\in U-w}(\mathrm{ID}_j-\mathrm{ID}_k)\\&=\sum_{U_j\in w}f(\mathrm{ID}_j)\\&\quad\times\prod_{U_k\in w-\{U_j\}}((-\mathrm{ID}_k)(\mathrm{ID}_j-\mathrm{ID}_k)^{-1})\\&=f(0)=a_0(\bmod R)\end{aligned}$$

所以

$$\begin{aligned}&\prod_{U_j\in w}(A_{ij})^{\Delta_j}-h_i(\prod_{U_j\in w}(B_{ij})^{\Delta_j})\\&=(\prod_{U_j\in w}(A_{ij})^{\Delta_j})-(T_i^{xa_0}-S_i)C_i^{-a_0}(\prod_{U_j\in w}(B_{ij})^{\Delta_j})\\&=(T_i)^{x\sum_{U_j\in w}(x_j\Delta_j)}-(T_i^{xa_0}-S_i)C_i^{-a_0}(C_i)^{\sum_{U_j\in w}(x_j\Delta_j)}\\&=T_i^{xa_0}-(T_i^{xa_0}-S_i)C_i^{-a_0}C_i^{a_0}=S_i(\bmod N)\end{aligned}$$

3　安全性分析

下面讨论对提出的方案的几种可能的攻击，分析表明这些攻击方案是无效的。

攻击 1 不诚实的成员试图伪造满足式(4)的$\{A_{ij}, B_{ij}\}$，以便只有他自己可以重构真正的秘密S_i。如果他随机给出伪造的A_{ij}或B_{ij}，直接从式(4)计算$B_{ij}=y_j^{d}A_{ij}^{C_i} \bmod N$或$A_{ij}=B_{ij}^{D_i}y_j^{-D_i d} \bmod N$是困难的，因为他不知道$d$和$D_i$；如果他试图利用 He 等人攻击 Lin 等人的方案的方法来伪造A_{ij}和B_{ij}也是困难的。例如他伪造$A_{ij}^{'}\neq A_{ij}$，然后计算满足式(4)的$B_{ij}^{'}$，这需要他知道D_i和x，而他必须解因子分解问题或离散对数问题。

攻击 2 庄家试图给每个成员分发伪造的子密钥x_i和秘密值$x_i^{'}$。如果庄稼分发给每个成员的x_i和$x_i^{'}$是假的，则他们的子密钥x_i和秘密值$x_i^{'}$无法通过$(g^{P_i})^{x_i}=\prod_{k=0}^{t-1}(V_k)^{(\mathrm{ID}_i)^k} \cdot(\bmod\ N)$和$y^{x_i}=g^{x_i} \bmod N$的验证。

攻击 3 不诚实的成员试图利用其他成员以前的A_{ij}和B_{ij}、不与其他$(t-1)$个成员合作来重构新的秘密。不妨设他想利用$\{A_{ij}^{a}, A_{ij}^{b}, B_{ij}^{a}, B_{ij}^{b}\}$来重构新的秘密$S_k$，则$A_{kj}=A_{ij}^{a}A_{ij}^{b}=(g^2(t_a t_b))^{D_i dx_j} \bmod N$，$B_{kj}=B_{ij}^{a}B_{ij}^{b}=(g^2(g^2 t_a \cdot t_b)^x)^{x_j} \bmod N$，即使随机选取的$t_c$满足$t_c=t_a t_b \bmod N$，但$A_{kj}$和$B_{kj}$也不能满足式(4)，所以攻击失败。

攻击 4 不诚实的成员试图利用其他成员的A_{ij}和B_{ij}获取他们的子密钥x_i和秘密值$x_i^{'}$，而这是困难的，因为他面临解离散对数问题。

所以，提出的新方案是安全的。

4 计算复杂性分析

由于 He 等人[6]的方案是已有方案中较好的、而且本文实现了与 He 等人[6]的方案一样的优点，所以本节只给出本文提出的方案在计算量与通信量方面与 He 等人的方案的比较。

为方便起见，不妨设$|N|$表示N的长度，T_e表示一个模幂乘运算所需的计算量，T_h表示执行一次单向 Hash 函数所需的计算量。由于数的一次加、减、乘、除的计算量远小于T_e或T_h的计算量，所以忽略不计。

在 He 等人[6]的方案中，一个成员为抵抗管理者的欺骗所需要的计算量为$(2t+1)T_e$，在恢复共享秘密时，每个成员为了抵抗其他成员的欺骗，必须执行零知识证明，否则会遭到 He 等人[5]提出的方法的攻击，所以为执行零知识证明每个成员所需的传输量为$4(t-1)|N|$，每个成员执行一次零知识证明所需的计算量为$9(t-1)T_e+2(t-1)T_h$，每恢复一个共享秘密庄家需要公开 4 个参数。而本文提出的方案中一个成员为抵抗管理者的欺骗所需要的计算量为$(2t+3)T_e$，在恢复共享秘密时，每个成员的传输量为$2(t-1)|N|$，每个成员为了抵抗其他成员的欺骗所需的计算量为$4(t-1)T_e$，每恢复一个共享秘密庄家只需要公开 3 个参数。

所以，本文提出的方案在计算量与通信量方面优于 He 等人的方案。

5 结束语

本文基于双子密钥的思想给出了一种安全有效的(t, n)多秘密共享认证方案，每个成员可以多次使用自己的子密钥来恢复庄家任意给定的用于共享的多个秘密，重构一个秘密只需公开 3 个参数，而且为抵抗成员的欺骗无须执行零知识证明协议。所给的方案与已有的方案相比有明显的优越性，克服了 Lin 等人的方案的安全性缺陷而计算量和通信量优于 He 等人的方案，可以应用于会议密钥分配、安全分布式计算、电子商务等领域。

参 考 文 献

[1] Shamir A. How to share a secret[J]. *Commun. ACM*, 1979, 22(11): 612 – 613.

[2] Blackly G R. Safeguarding cryptographic keys[A]. Proc. Nat. Computer Conf. AFIPS Conf. Proc., New York, USA,1979: 313 – 317.

[3] Harn L. Efficient sharing of multiple secrets[J]. *IEE Proc. Comput. and Digit. Tech.*, 1995, 142(3): 237 – 240.

[4] Lin T Y. Wu T C. (t, n)-threshold verifiable multisecret sharing scheme based on the factorization and the discrete logarithm modulo a composite problems [J]. *IEE Proc. Comput. Digit. Tech.*, 1999. 146(5): 264 – 268.

[5] He W H, Wu T S. Comment on Lin-Wu (t, n)-threshold verifiable multisecret sharing scheme [J]. *IEE Proc. Comput. Digit. Tech.*, 2001, 148(3): 139.

[6] 何明星, 范平志, 袁丁. 一个可验证的门限多秘密共享方案[J]. 电子学报, 2002, 30(4): 540 – 543.

谢 琪： 男，1968 年生，副教授，博士生，研究方向为密码学和信息安全.

于秀源： 男，1942 年生，教授，博士生导师，研究方向为数论及其应用、密码学和信息安全.

王继林： 男，1965 年生，副教授，博士，研究方向为网络安全和电子商务.