一种安全的门限多秘密共享方案

黄东平, 刘 铎, 王道顺, 戴一奇
(清华大学计算机科学与技术系, 北京 100084)

摘 要: 提出了一种可认证的门限多秘密共享的新方案, 通过成员提供的子密钥的一个影子来恢复秘密, 由影子难以得到子密钥本身, 因此可以复用, 也即通过同一组子密钥共享多个秘密. 该方案可以对分发者发布的信息和参与者提供的子密钥影子进行认证, 从而可以抵御分发者欺骗和参与者欺骗. 方案的安全性基于 RSA 密码系统和 Shamir 的(k, n) 门限秘密共享方案. 另外, 本文还提出两种对这类门限多秘密共享方案的欺骗方法, 能不同程度的破坏几个已有方案的安全性, 但本文所提出的方案对这些欺骗有免疫能力. 该方案是计算安全的, 并且性能较现有诸方案更好.

关键词: 多秘密共享; 门限; 认证; 分发者欺骗; 参与者欺骗
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2006) 11-1937-04

A Secure Threshold Multi-Secret Sharing Scheme

HUANG Dong-ping, LIU Duo, WANG Dao-shun, DAI Yi-qi
(*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*)

Abstract: A verifiable threshold multi-secret sharing scheme is proposed in this paper. As the secret can be recovered with the shadows provided by participants and it is computationally difficult to get the sub-keys from the shadows, the sub-keys can be reused to share the multi-secret in this scheme. By verifying the information published by the dealer as well as the shadows of sub-keys provided by participants, this scheme can prevent both dealer and participant from cheating. The security of this scheme is the same as that of RSA cryptosystem and Shamir's (k , n)-threshold scheme. Two kinds of cheating methods against threshold multi-secret sharing scheme are also proposed, which can threaten the security of previous schemes more or less. But the scheme proposed in this paper provides efficient solutions against these cheatings and achieves the same computational security with a better performance compared with the previous schemes.

Key words: multi-secret sharing; threshold; authentication; dealer cheating; participant cheating

1 引言

有些情况下需要几个授权用户合作管理某个秘密, 如银行保险柜的密码, 公司的重要秘钥等. 秘密共享的基本问题即是如何给共享参与者集合中的每个成员子秘密, 使得每个授权子集里的参与者都拿出自己的子秘密时可以恢复秘密, 而非授权子集的成员则不可能得到秘密信息. 1979 年 Shamir[1] 和 Blakley[2] 首先分别基于 Lagrange 插值多项式和射影几何理论提出门限秘密共享方案, 又称作阈值秘密共享方案. 在(k, n) 门限秘密共享方案中, 一个秘密被分成 n 份, 分别给 n 个参与者, n 个参与者中的任意 k 个合作就可以得到秘密信息, 而少于 k 个却得不到. 文献[1]方案因为实现简单计算代价小而得到了广泛的研究和应用.

早期的方案存在一定问题: (1)无法验证分发者或者参与者提供的信息是否真实. 一些包括认证功能的共享方案相继被提出以解决成员欺骗问题[3,4]; (2) 成员的子密钥只能使用一次, 不太利于实际使用. 一些研究工作考虑了子秘密的复用问题, 使得同一组子秘密可以完成多重秘密的共享, 简化了密钥分配管理工作[5~8].

文[6~8]分别提出方案同时解决认证和子密钥的复用. 它们虽然一定程度上解决了认证问题和子密钥复用问题, 但由于对秘密分发者的认证不够, 可能导致不能成功检验其欺骗行为. 本文提出一种不同方案, 在解决这两个问题的同时, 在实现上比它们简单清晰, 计算量更小.

2 预备知识

为了描述方便, 在具体讨论方案之前先介绍一些文章将用到的定义与记号.

定义 1 共享参与者 是指拥有一份子秘密, 并且可以通过与足够多的其他共享参与者的合作得到共享的秘密的人或设备.

定义 2 秘密分发者 是指把子秘密分发给 n 个共享参与者的人或者设备. 他的任务还包括向公告牌上公布相应的辅助信息.

定义 3 公告牌 由秘密分发者发布辅助信息的媒介, 如 web 网站等. 公告牌只有秘密分发者可写, 而参与者只有阅读权限.

在本文中, 为描述的清晰和简洁, 还将使用如下记号:

D:	秘密分发者;
$P=\{P_1, P_2, \cdots, P_n\}$:	参与者的集合, 其基数 n 即为共享参与者个数;
k_i:	参与者 i 得到的子密钥;

投稿日期: 2005-10-27; 修回日期: 2006-08-11
基金项目: 国家自然科学基金(No. 90304014); 国家 863 高技术研究发展计划(No. 2005AA114160)

$\mathrm{ord}_m(a)$: 整数 a 模 m 的阶.

3 方案描述

在本节中将具体描述新的可验证多秘密门限共享方案, 该方案包括参数初始化, 秘密分发和秘密恢复等阶段. 该方案的一个重要特点是 n 个参与者中的任意 k 个通过其子秘密的影子, 就可以恢复秘密, 而子秘密本身不必公开, 可以复用. 并且这些影子可以验证, 以防止恶意用户的欺骗.

3.1 初始化

初始化阶段主要完成系统参数的选定, 为后续工作做准备. 秘密分发者选定两个强的大素数 p 和 q, 即 $p=2p'+1$, $q=2q'+1$, 其中 p', q' 也是大的素数, 计算乘积 $N'=p'q'$ 和 $N=pq$. 对它们的要求可以参考 RSA[9] 密码体制的安全性要求, 即攻击者在知道 N 的情况下想要得到 p 和 q 在计算上是困难的, 这是保证整个秘密共享体制安全性的关键. 在 Z_N 里随机选取一个满足 $\mathrm{ord}_N(g)=N'$ 的整数 g. 在公告牌上公布 N 和 g.

3.2 子密钥生成

分发者 D 随机生成一个 $k-1$ 次多项式 $f(x)=\sum_{i=0}^{k-1}a_ix^i \bmod N'$, 其中 $a_i\in Z_{N'}$, $a_0>1$. 计算检测向量 $\boldsymbol{V}=\{v_0, v_1, v_2, \cdots, v_{k-1}\}$, 其中

$$v_i=g^{a_i}\bmod N\ (i=0, 1, \cdots, k-1)$$

在公告牌上公布 $\boldsymbol{V}$. 取 $\{x_i\}_{1\leqslant i\leqslant n}\subset Z_N\setminus\{0\}$, 且满足: 对任意 $1\leqslant i<j\leqslant n$, $\gcd(x_i-x_j, N')=1$. 这些 x_i 就是参与者 P_i 的 ID, 计算

$$\lambda_i=\prod_{P_j\in P\setminus\{P_i\}}(x_i-x_j)\bmod N' \tag{1}$$

选择 x_i 的方式决定了能求解 $\lambda_i^{-1}\bmod N'$. 计算用户 P_i 的子秘密 $k_i=f(x_i)\lambda_i^{-1}\bmod N'$ 和认证信息 $s_i=g^{k_i}\bmod N$, 并在公告牌上公布 $\{x_i\}_{1\leqslant i\leqslant n}$ 和 $\{s_i\}_{1\leqslant i\leqslant n}$. 最后, 秘密分发者通过秘密通道发送 $\{g^{\lambda_i}\bmod N, k_i\}$ 给用户 P_i.

此时, 参与者 P_i 可以通过检测下面两式是否成立以检查 k_i 的真实性, 可以避免秘密分发者 D 的欺骗:

$$s_i=g^{k_i}\bmod N \tag{2a}$$

$$(g^{\lambda_i})^{k_i}\equiv\prod_{j=0}^{k-1}v_j^{x_i^j}\bmod N \tag{2b}$$

由文献[6]的定理 2, 真实的 k_i 能通过式(2b)的认证。

3.3 秘密的共享

为了共享任一秘密 S_j, 分发者 D 随机选取 $d_j\in Z_N$ 满足 $\gcd(d_j, N')=1$, 并计算 e_j 使得 $d_je_j\equiv 1(\bmod N')$. 计算 $h_j=g^{d_j}\bmod N$, $R_j=S_j-h_j^{a_0}\bmod N$, 在公告牌上公布 h_j, e_j 和 R_j.

上述共享秘密的方法也决定了选择不同的 d_j 就可以共享不同的秘密.

3.4 秘密的恢复

秘密共享参与者集合里的任意 k 个成员合作, 利用他们掌握的子秘密和公告牌上的公告信息, 就可以恢复秘密. 恢复过程中, 每个参与者提供的不是自己的子秘密, 而是根据子秘密和公告信息计算出的影子信息. 而且影子信息是可验证的, 从而防止了参与者欺骗. 反过来, 由影子信息得到子秘密在计算上是不可行的, 从而子秘密可以复用. 为了描述方便, 我们不妨设参与恢复的 k 个参与者为: $Q=\{P_1, P_2, \cdots, P_k\}$. 恢复过程如下:

(1)每个参与者从公告牌下载 h_j, e_j 和 N.

(2)每个参与者 P_i 计算并出示 $X_{j,i}=h_j^{k_i}\bmod N$. 这个 $X_{j,i}$ 就是 P_i 的影子信息.

(3)每个参与者可以验证其他人是否有欺骗行为. 比如要验证 P_i 给的 $X_{j,i}$ 是否属实, 只需要验证 $X_{j,i}^{e_j}\bmod N$ 与 s_i 是否一致. 事实上, 在参与者诚实的情况下, 由下式可知, 这二者是相等的:

$$X_{j,i}^{e_j}\equiv(h_j^{k_i})^{e_j}\equiv g^{d_jk_ie_j}\equiv g^{k_i}\bmod N=s_i \tag{3}$$

(4)恢复秘密的操作者计算

$$\begin{aligned}&\alpha_i=\prod_{P_l\in Q\setminus\{P_i\}}(-x_l)\cdot\prod_{P_l\in P\setminus Q}(x_i-x_l);\\&\beta_j=\prod_{P_i\in Q}X_{j,i}^{\alpha_i}\bmod N;\\&S_j=\beta_j+R_j\bmod N\end{aligned} \tag{4}$$

S_j 即为共享的秘密.

3.5 方案正确性证明

定理 1 在方案的所有参与者都诚实而正确地执行协议的前提下, 以上所述方案得到的 S_j 确实是秘密分发者所共享的秘密.

证明:

$$\begin{aligned}\beta_j&=\prod_{P_i\in Q}X_{j,i}^{\alpha_i}\bmod N=\prod_{P_i\in Q}(h_j^{k_i})^{\alpha_i}\bmod N\\&=h_j^{\sum_{P_i\in Q}k_i\alpha_i}\bmod N=h_j^{a_0}\bmod N\end{aligned} \tag{5}$$

因此, $\beta_j+R_j\bmod N=h_j^{a_0}+S_j-h_j^{a_0}\bmod N=S_j\bmod N$, 此即共享的秘密, 证毕.

其间, 参与者通过验证

$$\beta_j^{e_j}\equiv g^{a_0}\bmod N \tag{6}$$

检查 $h_j^{a_0}$ 的真实性, 以防止分发者的欺骗.

4 方案分析

接下来从安全性和计算复杂性两个方面来分析该方案.

4.1 安全性分析

下面结合可能遭到的攻击分析该方案的安全性.

(1)本方案可避免秘密分发者选用低阶的 g 对秘密共享参与者的欺骗

欺骗的方法是分发者选用一个阶低于 $p'q'$ 的 g, 不妨设 $\mathrm{ord}_N(g)=q'$, 他给 P_i 的不是 $k_i=f(x_i)\lambda_i^{-1}\bmod N'$, 而是 $k'_i=(f(x_i)+zq')\lambda_i^{-1}\bmod N'$, 其中 z 是任一满足 $\gcd(z, N')=1$ 的整数. 这样的 g 总能取得到, 实际上, 当 $t>1$ 且 $t\mid 2p'q'$ 时, 有下面命题保证总能取到模 N 阶为 t 的元素.

命题 2 $\exists\, G\in Z_N$ 使得 $\mathrm{ord}_N(G)=2p'q'$.

证明. 由 $p=2p'+1$, $q=2q'+1$, 取 g_1 满足 $\mathrm{ord}_p(g_1)=2p'$, g_2 满足 $\mathrm{ord}_q(g_2)=2q'$. 由于 $\gcd(p, q)=1$, 通过中国剩余定理可求出 $G\in Z_N$ 使得 $G\equiv g_1\bmod p$, $G\equiv g_2\bmod q$. 由于 $\gcd(G, N)=1$, 存在 $t\in[1, \varphi(N)]$, 使得 $G^t\equiv 1\bmod N$, 于是有 $G^t\equiv 1\bmod p$ 且 $G^t\equiv 1\bmod q$. 从 $G\equiv g_1\bmod p$, $G\equiv g_2\bmod q$ 可看出 $2p'\mid t$, $2q'\mid t$, 故而 $2p'q'\mid t$; 另一方面, 由数论的知识可知

N 不存在原根, 故而必然有 $t=2p'q'$, 也即 $\mathrm{ord}_N(G)=2p'q'$.

而后 P_i 在对分发者的认证中无法识别出该伪子秘密,

$$g^{k'_i}\equiv g^{(f(x_i)+zq')\lambda_i^{-1}}\equiv g^{f(x_i)\lambda_i^{-1}}g^{q'z\lambda_i^{-1}}\equiv g^{k_i}\bmod N=s_i$$

式(2a)成立, 显然式(2b)也成立. 在恢复秘密的过程中, 因为

$$(X'_{j,i})^{e_j}\equiv(h_j^{k'_i})^{e_j}\equiv g^{d_jk'_ie_j}\equiv g^{k'_i}\equiv g^{k_i}g^{zq'\lambda_i^{-1}}\bmod N=s_i$$

同样能通过式(3)对 P_i 的认证.

但是, 这对于共享的秘密没有什么影响; 事实上, 由下式可见

$$(X'_{j,i})^{\alpha_i}\equiv(h_j^{k'_i})^{\alpha_i}\equiv(g^{k'_i})^{d_j\alpha_i}\equiv(g^{k_i+zq'\lambda_i^{-1}})^{d_j\alpha_i}\equiv(g^{k_i})^{d_j\alpha_i}$$
$$\equiv(X_{j,i})^{\alpha_i}\bmod N,$$

也即恢复出的秘密仍是正确的. 因此在我们提出的方案中, 这种欺骗方法是没有实际意义的.

而在已有的方案[6, 7]中, 这种欺骗却是有效的, 其结果是参与者拿到一个伪子秘密但无法成功检测出欺骗, 当他诚实地参与到恢复过程中时, 他能通过认证, 但最终恢复得到的是一个错误的秘密. 限于篇幅, 相关讨论见附录 A.

(2) 分发者不能用给参与者伪 k_i 的方法进行欺骗

注意到这类方法中认证的是 k_i 和 λ_i 的乘积, 相应地, 另一种欺骗方式即是分发者给参与者 P_i 伪子秘密, 令 $\lambda'_i=z\lambda_i\bmod N'$, $k'_i=z^{-1}k_i\bmod N'$, $s'_i=g^{z^{-1}k_i}\bmod N$, 其中 z 是任一满足 $\gcd(z,\varphi(N))=1$ 的整数.

P_i 认证分发者的式(2a)与式(2b)显然能通过认证. 在有 P_i 参与的恢复过程中, 这种欺骗也能通过式(3)的认证, 因为:

$$X'^{e_j}_{j,i}\equiv(h_j^{k'_i})^{e_j}\equiv g^{d_jk'_ie_j}\equiv g^{k'_i}\bmod N=s'_i$$

这样, 由式(4)恢复出的 β_j 不正确:

$$\beta'_j=\left(\prod_{P_i\in Q}g^{d_jk_i\alpha_i}\right)g^{d_j\alpha_i(z^{-1}-1)k_i}\bmod N=g^{a_0d_j}g^{d_jk_i\alpha_i(z^{-1}-1)}\bmod N$$

但是, 此时 β'_j 无法通过式(6)的验证, 欺骗被成功检测出来.

而这种欺骗对文献[7, 8]中所描述的方案却是有效的, 参与者将无法检测出其获得的子秘密的真伪, 在他诚实的情况下, 他虽然能通过恢复秘密时的认证, 但最终恢复得到却的是一个错误的秘密. 相关讨论见附录 B.

(3) 攻击者试图通过 $g^{a_0}\bmod N$ 恢复 $h_j^{a_0}$

假设 RSA 密码系统是安全的. 如果攻击者能得到 $h_j^{a_0}$, 由于 $(g^{a_0})^{d_j}\equiv h_j^{a_0}\bmod N$, 这可以看作 RSA 密码系统的解密运算, 其中 g^{a_0}是密文, d_j 是私钥, $h_j^{a_0}$是明文. 根据 a_0 以及 d_j 的取法, $h_j^{a_0}$可以是任意合法的明文. 这表明该攻击者具有根据一个 RSA 密码系统的密文得到其明文的能力, 与假设矛盾.

(4) 攻击者试图从公告牌上的 s_i 得到 k_i

假设攻击者能通过 s_i 得到 k_i, 由于 $g^{k_i}\equiv s_i\bmod N$, 那么有 $g^{k_i}\equiv s_i\bmod p$ 和 $g^{k_i}\equiv s_i\bmod q$. 这表明攻击者具有求解有限域上的离散对数问题的能力, 但事实上这个问题在计算上是困难的, 因此该假设不能成立.

(5) 假设 $k-1$ 个参与者试图恢复秘密

他们拥有秘密的 $k-1$ 次多项式上的 $k-1$ 个点, 不足以确定该多项式. 这 $k-1$ 个点可以看作一个 k 元线性方程组里的 $k-1$ 个相容的方程式, 但这个方程组里面约束的数目少于未知数的数目, 不足以唯一确定方程的一组解. 设 P_l 是其余 $n-k+1$ 个参与者中的任意一个, 那么, 对于任意 $k_l\in\{0,1,\cdots,N'-1\}$, (x_l,k_l) 与他们的秘密信息, 结合公告牌上的秘密信息, 都能确定一个 $k-1$ 次多项式, 这样的多项式共有 N' 个. 以他们拥有的信息, 他们无法区分这 N' 个多项式. 也就是说, $k-1$ 个参与者合作, 得不到秘密.

4.2 时间复杂度分析

设计算一次 $g^a\bmod N$ 需要的时间量为 T_e, 其中 $g\in Z_N$, $a\in Z_N$, 而如式(4)这样的指数运算, 由于指数是 Z_N 中多个元素的乘积, 在分析中算做多次运算. 下表列出了为防止可能发生的各种欺骗而进行的认证涉及的运算次数, 以及每共享一个秘密需要公布的参数数目.

	文[6]方案	文[7]方案	文[8]方案	本方案
P_i 防止 D 欺骗	$(k^2+2n+k+4)T_e/2$	$(k^2+k+4)T_e/2$	$(k^2+k+4)T_e/2$	$(k^2+k+4)T_e/2$
P_i 防止 P_j 欺骗	$(k-1)T_e$	$3(k-1)T_e$	$2(k-1)T_e$	$(k-1)T_e$
D 防止 P_i 欺骗	$2T_e$	$4T_e$	$2T_e$	$2T_e$
公布信息数目	4	4	3	3
能否对抗欺骗 1	否	否	是	是
能否对抗欺骗 2	是	否	否	是

其中在本方案中, P_i 为防止 D 欺骗, 需要验证式(2a)和(2b), 分别需要 T_e 次和 $(1+(k-1)+(k-1)k/2)T_e$ 次; 在恢复秘密过程中需要验证式(6), 需要 T_e 次运算; P_i 为防止 P_j 欺骗, 需要验证式(3), 共需要 $(k-1)T_e$ 次; D 为防止 P_i 欺骗, 需要计算 h_j 和 R_j, 共 $2T_e$ 次.

文献[7, 8]中所提出的方案通过修改亦可防止文中所述的分发者给参与者伪 k_i 的第二种欺骗方式, 只要参与者放弃式(2b)这样的验证方式, 而改用文[6]中的(5b)方案, 其代价是多用 nT_e 次运算.

由此可见, 本方案比文献[6~8]更安全, 需要的运算次数更少, 同时, 需要发布在公告牌上的信息也比文献[6, 7]要少.

5 结论

本文提出一种新的门限多秘密共享方案. 由于利用了离散对数问题和大数分解问题的难解性以及 Shamir 共享方案[1]的安全性, 本方案是计算安全的. 本文还提出了两种新的欺骗攻击方式, 并分析论证了这两种攻击方式对已有诸方案安全性的影响, 且指出本文所提出的新方案是能够抵抗或检测这两种攻击的. 另外, 新方案执行和验证所需要的运算次数也不同程度地少于已有诸方案. 因此, 本文所提出的方案无论从安全性还是执行的效率上都优于已有诸方案[6~8].

附录

A. 秘密分发者选用低阶的 g 对秘密共享参与者的欺骗

本部分以文[6]中提出的方案为例说明. 先简要介绍其方案: 分发者选择 d 和 e 使得 $de\equiv1\bmod\varphi(N)$, 公布 e 而保密 d.

用(2a)和(2b)或

$$\left(s_i\right)^{\prod_{P_t\in Q,t\neq j}(x_i-x_t)}=\prod_{j=0}^{k-1}(v_j)^{x_i^j}\bmod N \qquad (a1)$$

来验证子秘密. 共享一个秘密 S_j 时, 分发者选取 $g_j\in Z_{N'}$ 和 $r_j\in Z_{N'}$, 计算 $c_j=(gg_j)^d \bmod N$ 和 $h_j=g_j^{a_0}r_j-S_j$, 在公告牌上发布$\{c_j, r_j, g_j, h_j\}$. 恢复秘密时, P_i 计算并公布

$$k_{ji}=g_j^{k_i}\bmod N \qquad (a2)$$

$$c_{ji}=c_j^{k_i}\bmod N \qquad (a3)$$

其他参与者通过 $c_{ji}^e=s_ik_{ji}\bmod N$ (a4)

认证 P_i. 最后用 $S_j=\left(\prod_{P_i\in Q}k_{ji}^{\alpha_i}\right)r_j-h_j\bmod N$ (a5)

恢复秘密.

现在讨论在分发者用低阶参数 g 欺骗 P_i 时情况: 设分发者选用阶为 q' 的 g, 给参与者 x_i 分发的 $k'_i=(f(x_i)+zq')\lambda_i^{-1}\bmod N'$, 那么

$$g^{k'_i}\equiv g^{(f(x_i)+zq')\lambda_i^{-1}}\equiv g^{f(x_i)\lambda_i^{-1}}g^{q'z\lambda_i^{-1}}\equiv g^{f(x_i)\lambda_i^{-1}}\equiv g^{k_i}\bmod N=s_i$$

式(2a)成立, 显然式(a1)也成立. P_i 无法识别出该伪子秘密. 设在共享一个秘密的时候, 分发者选取 g_j 使得 $\mathrm{ord}_N(g_j)=p'q'$ 并继续后续操作. 设 P_i 参与恢复该秘密, 由于

$$(c'_{ji})^e\equiv(gg_j)^{dk'_ie}\equiv(gg_j)^{k'_i}\equiv s_ik'_{ji}\bmod N$$

只要参与者 P_i 诚实, 他能通过式(a4)的检测. 这样, 在其式(a5)的计算中,

$$S'_j=g^{\sum_{P_t\in Q}k_t\alpha_t+zq'\lambda_i^{-1}\alpha_i}r_j-h_j\bmod N=g_j^{a_0+zq'\lambda_i^{-1}\alpha_i}r_j-h_j\bmod N$$

由于 g_j 阶数为 $p'q'$, 上式只有在 $p'\mid z\lambda_i^{-1}\alpha_i$ 的情况下才可能等于 S_j, 对于随机选取的 z 这个可能性极小. 可见, 分发者可以给参与者 P_i 分发一个伪子秘密, 使得该伪子秘密能通过一切认证, 但最终恢复出的却是一个错误的秘密. 对于这种攻击方式, 文[7]方案同样无法幸免.

B. 秘密分发者选用伪子秘密对秘密共享参与者的欺骗

本部分以文[8]所描述的方案为例说明. 该方案中分发者选择 d 和 e 使得 $de\equiv 1\bmod \varphi(N)$, 公布 e 而保密 d, 其余准备工作——包括对秘密分发者的认证——与本文方案相同. 当共享一个秘密 S_j 时, 秘密分发者选取 $r_j\in Z_{N'}$, 并计算 $C_j=g^{r_jd}\bmod N$ 和 $h_j=(g^{a_0r_jd}\bmod N)\oplus S_j$, 而后将$\{r_j, C_j, h_j\}$发布到公告牌上. 恢复秘密时, P_i 计算并公布

$$A_{ij}=(C_j)^{k_i}\bmod N \qquad (b1)$$

其余参与者通过 $(A_{ij})^e=(s_i)^{r_j}\bmod N$ (b2)

认证 P_i. 用 $S_j=h_j\oplus\left(\prod_{P_i\in Q}A_{ji}^{\alpha_i}\bmod N\right)$ (b3)

得到秘密.

现在讨论在分发者用伪子秘密欺骗参与者的情况. 分发者给参与者 P_i 伪子秘密, 令 $p'_i=zp_i$, 相应的 $k'_i=z^{-1}k_i$, $s'_i=g^{z^{-1}k_i}$. 式(2b)只能验证 k_i 和 p_i 的乘积, P_i 无法发现该欺骗. 设 P_i 参与秘密 S_j 的恢复, 如果他诚实, 可以通过式式(b2)的验证, 因为

$$(A'_{ij})^e\equiv(C_j)^{k'_ie}\equiv g_j^{r_jdk'_ie}\equiv g_j^{r_jk'_i}\equiv(s'_i)^{r_j}\bmod N$$

但是他们恢复得到的秘密:

$$S'_j=(g^{a_0r_jd}\bmod N)\oplus S_j\oplus(g^{a_0r_jd+(z^{-1}-1)k_i\alpha_ir_jd})\bmod N$$

等于 S_j 当且仅当 $\mathrm{ord}_N(g)\mid(z^{-1}-1)k_i\alpha_ir_jd$, 对于随机选取的 z, 这个可能性极小.

参考文献:

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

[2] Blakley G R. Safeguarding cryptographic keys[A]. Proceedings of National Computer Conference[C]. Montvale, NJ: AFIPS Press, 1979. 48: 313–317.

[3] Stadler M. Publicly verifiable secret sharing[A]. Advances in Cryptology-Eurocrypt'96[C]. Berlin: Springer Verlag, 1996. 190–199.

[4] Fabrice Boudot, Jacques Traoré. Efficient publicly verifiable secret sharing schemes with fast or delayed recovery[A]. Lecture Notes in Computer Science 1726[C]. Berlin: Springer Verlag, 1999. 87–102.

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

[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.
He M X, Fan P Z, Yuan D. A verifiable multiple secrets sharing scheme[J]. Acta Electronica Sinica, 2002, 30(4): 540–543. (in Chinese)

[7] 施荣华. 一种多密钥共享认证方案[J]. 计算机学报, 2003, 26(5): 552–556.
Si R H. A multisecret sharing authenticating scheme[J]. Chinese Journal of Computers, 2003, 26(5): 552–556. (in Chinese)

[8] Chang T Y, Hwang M S, Yang W P. An improvement on the Lin-Wu (t, n) threshold verifiable multi-secret sharing scheme[J]. Applied Mathematics and Computation, 2005, 163(1): 169–178.

[9] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystem[J]. Communication of ACM, 1978, 21: 120–126.

作者简介:

黄东平 男, 1977 年生于四川巴中, 清华大学计算机科学与技术系博士研究生, 主要研究领域为信息安全, 算法设计与分析.
E-mail: hdp01@mails.tsinghua.edu.cn

刘 铎 男, 1978 年生于北京, 清华大学计算机科学与技术系博士研究生, 主要研究领域为密码学, 组合算法的设计与分析.

王道顺 男, 1964 年生于四川苍溪, 博士, 清华大学计算机科学与技术系副教授, 研究领域为图像加密, 数字水印和密码算法.

戴一奇 男, 1946 年生于浙江, 清华大学计算机科学与技术系教授, 博导, 研究领域为信息安全, 算法设计与分析.