一个可验证的门限多秘密分享方案

何明星[1,2], 范平志[1], 袁丁[1,3]
(1. 西南交通大学计算机与通信工程学院, 四川成都, 610031; 2. 四川工业学院计算机科学与工程系, 四川成都, 610039;
3. 四川大学电子信息学院, 四川成都, 610065)

摘 要: 基于离散对数计算和大整数分解的困难性, 利用 RSA 加密体制提出了一个新的门限多秘密分享方案. 该方案通过零知识证明等协议来防止秘密分发者和秘密分享者的欺诈行为, 因而是一个可验证的门限多秘密分享方案. 该方案还具有: 秘密影子可重复使用; 子秘密影子可离线验证; 供分享的秘密不须事先作预计算等特点. 该方案可用于会议密钥(秘密)分配、安全多方计算、门限数字签名等应用领域.

关键词: 秘密分享; 门限体制; 离散对数; RSA 加密体制; 零知识证明
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2002) 04-0540-04

A Verifiable Multiple Secrets Sharing Scheme

HE Ming-xing[1,2], FAN Ping-zhi[1], YUAN Ding[1,3]
(1. Southwest Jiaotong University, Chengdu, Sichuan 610031, China;
2. Sichuan University of Science and Technology, Chengdu, Sichuan 610039, China;
3. Sichuan University, Chengdu, Sichuan 610063, China)

Abstract: A new multiple secrets sharing scheme, based on the intractability of the discrete logarithm (DL) and the RSA encryption algorithm is presented, in which the participants' shadows remain secret and can be reused, even if all subshadows are made public. Meanwhile, by using a zero-knowledge proof protocol, the validity verification of shadow and subshadow is also provided to prevent both dealer cheating and other participant cheating, and any freely given secrets without pre-computation by dealer can be reconstructed. The scheme can be applied to many areas such as conference key distribution, secure multi-part computation, threshold signature etc.

Key words: multi-secret sharing; threshold scheme; discrete logarithm; RSA; zero-knowledge proof

1 引言

秘密分享在现代密码学中占有重要的地位. 秘密分享的基本问题是如何给参与者集合的每个参与者适当分配子秘密(秘密影子), 使得只要根据一定的授权存取结构汇集其中一部分参与者的子秘密经过计算就可恢复秘密. 在秘密分享方案中, 门限秘密分享方案是应用较广也是研究最早、成果最多的一种秘密分享方案. 具体地说, (k, n)门限秘密分享是分发者在 n 个参与者即所谓秘密分享者中把一个或多个秘密分拆成若干个子秘密, 分配给各个参与者, 使得这 n 个参与者中任何 k 个合作就可恢复秘密, 但任何少于 k 个的参与者都无法获得该秘密. 最早的秘密分享方案是在 1979 年由 Shamir 和 Blakley 分别基于 Lagrange 插值多项式和射影几何理论独立提出的[1]. 20 多年来, 门限秘密分享方案的研究与设计受到人们的广泛关注, 取得了长足的进步, 其应用涉及通信密钥管理、安全多方计算、金融网安全、电子商务等诸多领域[1,2]. 虽然 Shamir 和 Blakley 的方案奠定了门限方案的基础, 但 M Tompa 与 H Woll[3] 发现他们的方案不能防止秘密分发者与分享者的欺诈行为, 而且分享者所得到的秘密影子(Shadow)只能使用一次, 若有多个秘密则需多次分发秘密影子. 1985 年 Chor 等人提出了一个可防止分发者(Dealer)欺诈的秘密分享方案, 但这个方案不能防止分享者的欺诈[4]. 之后各种防欺诈秘密分享方案陆续提出[5~10], 其中大部分方案仅能防止分发者或分享者一方的欺诈, 而且这些方案只能一次分享一个秘密. Harn 1995 年提出了一个多秘密分享方案能同时防止分发者与分享者的欺诈[8]. 在 Harn 的方案中, 秘密分发者给每一个分享者一个秘密影子, 然后分享者再由此计算秘密子影子(Subshadow)分发给他的门限合作者, 这样即使公开子秘密影子, 秘密影子也可保密. 但 Harn 方案的缺点是对于每个供分享的秘密都须事先作预计算. 而且子秘密影子的认证都是各方在线合作的, 从而计算量和通信量均很大, 导致方案实施的困难.

本文的贡献在于利用 RSA 加密体制以及零知识证明等

收稿日期: 2000-12-29; 修回日期: 2002-01-31
基金项目: 国家自然科学基金(No. 69825102)

协议, 设计了一个具有较好综合性能的多秘密门限分享方案, 主要有以下特点: (1)秘密影子可重复使用; (2) 子秘密影子可离线验证; (3)可检测秘密分发者与分享者的欺诈行为; (4) 不需事先对秘密进行预计算.

2　预备知识

在给出方案之前, 首先介绍本文用到的一些定义、记号与相关知识.

定义 1　秘密分发者(Dealer) 指把一个或多个秘密分发给 n 个秘密分享者的人或服务器. 比如网上会议的大会主席.

定义 2　公告栏(NB) 指存放公开参数或数据的媒介. 系统各方均可访问公告栏上的内容, 但只有秘密分发者才能修改或更新公告栏上的内容.

记秘密分发者为 P_d, $S=\{s_1, s_2, \ldots, s_m\}$为 m 个待分发秘密 s_j 的集合, $G=\{P_1, P_2, \ldots, P_n\}$是 n 个秘密分享者 P_j 的集合. 假设传送秘密影子的信道是安全可靠的. WA G 是G 中 t 个秘密分享者的集合, t 为门限值. I_j 表示 P_j 的身份标识号(比如, 1, 2, , , m).

对于秘密分发者 P_d 与秘密分享者集合 $G=\{P_1, P_2, \ldots, P_n\}$之间的一个可验证的秘密分享方案, 应满足以下要求:

(1) 如果秘密分发者遵循分发协议且各秘密分享者 P_j 遵循协议, 则 P_j 可正确收到 P_d 的秘密信息.

(2) 对于同一个秘密 s 的分配方案, 两个合法秘密分享者集合 W_1 A G 与 W_2 A G, (这里| W_1| = | W_2| = t)恢复出的秘密是相同的.

(3) 秘密分享者可检测秘密分发者的欺诈行为.

(4) 秘密分享者可检测其他分享者的欺诈行为.

零知识证明协议　所谓零知识证明, 是指一方(证明者)向另一方(验证方) 证明某个论断正确的一种协议, 同时要求在证明过程中不暴露证明方任何其它信息. 零知识证明在设计密码协议时是非常有用的. 在此, 先介绍本文中要用到的零知识证明协议[2]. 设 8 是一个循环群(设其阶为 m), g 是 8 的生成元, h 是 8 的一个元素. 该零知识证明协议可以满足以下要求: 证明者在已知 G、g、H、h 且$H=h^s$ 的条件下向验证者证明他知道 s, 而且有以 g 为底元素 G 的离散对数等于以 h 为底 H 的离散对数 s, 即 $G=g^s$, 同时证明者不会泄露 s 的信息. 协议描述如下: 设 A 是证明者, B 是验证者, 证明者 A 随机选取 r 并计算 $x=g^r$ 和 $xc=h^r$. 令 $c=Hc(g, h, G, H, x, xc)$, 其中 Hc 是一个 hash 函数. 他先计算 $y=r+cs$, 再把数据对(c, y)传给验证者 B 作为证据. 验证者收到(c, y)后验证 $c=Hc(g, h, G, H, g^y/G^c, h^y/H^c)$ 是否成立. 若是则 B 认为A 知道 s; 否则 B 认为A 不知道 s.

3　方案描述

基于第 2 节的准备, 本节提出多秘密分享方案. 设秘密分发者 P_d 有 m 个待分发的秘密 $S=\{s_1, s_2, \ldots, s_m\}$, P_d 需要将这 m 个秘密分发给 $G=\{P_1, P_2, \ldots, P_n\}$ 中的 t 个授权的秘密分享者, 这些分享者的集合为 W. 方案包含以下四个模块: 初始化; 秘密影子的生成算法; 秘密子影子的生成算法; 秘密恢复算法.

初始化　秘密分发者 P_d 创建公告栏并定义如下参数:

p, q 为 P_d 秘密选择的两个不同的强大素数, 即 $p=2pc+1$, $q=2qc+1$, 且 pc, qc 仍为大素数; $N=pq$ 发布在公告栏上; $Nc=pc\,qc$, 由 P_d 保密; e, d 为秘密分发者 P_d 的 RSA 公钥和私钥, 满足 $ed=1 \bmod U(N)$, 其中 U 是 Euler 函数. 即 d 由P_d 保密, 而 e 发布在公告栏上; g 为 Z_N 中阶为Nc 的生成元, 发布在公告栏上. Hc 是一个公开的 hash 算法.

秘密影子的生成算法　首先, P_d 随机生成(t- 1) 次多项式 $f(x)=a_0+a_1x+\ ,\ +a_{t-1}x^{t-1} \bmod Nc$, $a_k \in Z_{Nc}$, $0<a_k<Nc-1$, 然后计算检测向量 $V=(v_0, v_1, \ldots, v_{t-1})$, 其中

$$v_k=g^{a_k} \bmod N \quad (k=0, 1, \ldots, t-1) \tag{1}$$

并在公告栏 NB 上公开 V. 令

$$k_j=\prod_{P_k \in G\setminus\{P_j\}} (I_j-I_k) \bmod Nc \tag{2}$$

这里 I_j 表示分享者 P_j 的身份标识号. 注意到 pc、qc 是两个大素数, 应有$|I_j-I_k|<pc$, $|I_j-I_k|<qc$ 于是 I_j-I_k 与 pc、qc 分别互素, 而 pc、qc 也互素, 因而 k_j 与 $Nc=pc\,qc$ 互素, 从而 $k_j^{-1} \bmod Nc$ 存在. 于是对于秘密分享者 $P_j \in G$, P_d 可按如下定义为其计算秘密影子

$$x_j=f(I_j) \# k_j^{-1} \bmod Nc \tag{3}$$

并通过安全信道给 P_j 发送$\{g^{k_j} \bmod N, x_j\}$, P_d 同时为 P_j 计算公钥

$$y_j=g^{x_j} \bmod N \tag{4}$$

将其发布在 NB 上. 当 $P_j \in G$ 收到 P_d 发来的秘密影子后, 通过下式对 x_j 的有效性进行验证

$$(g^{k_j})^{x_j}=\prod_{k=0}^{t-1} (v_k)^{I_j^k} \pmod N \tag{5a}$$

若式(5a)不成立, 则可检测到秘密分发者 P_d 有对 P_j 的欺诈行为(P_d 传递的秘密影子不满足式(4) 或者式(3)). 事实上, 任何一个参与者也可通过验证下式是否成立

$$(y_j)^{P_k \in G\setminus\{P_j\}^{(I_j-I_k)}}=\prod_{k=0}^{t-1} (v_k)^{I_j^k} \pmod N \tag{5b}$$

来对 P_d 的公钥发布是否存在欺诈行为进行检测.

秘密子影子的生成算法　首先, 对任意待分配的秘密 s_i ($i=1, 2, \ldots, m$), P_d 随机选取相应的整数 $r_i \in Z_{Nc}$, 再随机选取 $g_i \in Z_{Nc}$, 计算

$$c_i=(gg_i)^d \bmod N \tag{6}$$

$$h_i=g_i^{a_i} r_i - s_i \pmod N \tag{7}$$

然后 P_d 在NB 上发布四元组(c_i, r_i, g_i, h_i).

为了恢复秘密 s_i, 每个秘密分享者 P_j 须为秘密 s_i 计算子影子 k_{ij}:

$$k_{ij}=g_i^{x_j} \bmod N \tag{8}$$

$$c_{ij}=c_i^{x_j} \bmod N \tag{9}$$

P_j 再随机选取整数 $r_{ij} \in [1, N]$ 并计算 $c_{ij}=Hc(g, g_i, y_j, k_{ij}, g^{r_{ij}}, g_i^{r_{ij}})$, $y_{ij}=r_{ij}+c_{ij}x_j$. 最后, 将四元组$(k_{ij}, c_{ij}, c_i, y_{ij})$传给 W 中的其他所有合作者, 作为向合作者证明秘密子影子 k_{ij} 计

算正确的证据.

每个秘密分享者 P 在收到其他所有合作者 P_j 传来的四元组(k_{ij}, c_{ij}, c'_{ij}, y_{ij})后可首先按下式离线检测秘密子影子 k_{ij} 的正确性:

$$c_{ij}^{e} = y_j k_{ij} \pmod N \tag{10}$$

若式(10)不成立,则可断定秘密分享者 P_j 伪造秘密 s_i 的子影子 k_{ij}. 若式(10)满足,则可认为秘密子影子 k_{ij} 是正确的. 在安全性要求更高的情况下,为了进一步加强安全性(以防对式(10)的其它攻击), P 可以利用第 2 节中描述的零知识证明协议再次检测 P_j 所传子影子的(k_{ij}, c_{ij})的合法性. 例如, P_j 想欺骗接收者 P 以使接收方 P 不能恢复正确的秘密,他可能用虚假秘密影子 x'_j 代替自己的真秘密影子 x_j,计算虚假秘密子影子: $kc_{ij} = g_i^{x'_j} \bmod N$,也即 P 可能收到信息 $kc_{ij} = g_i^{x'_j} \bmod N$. 但注意到 P_j 的公钥 $y_j = g^{x_j} \bmod N$ 是发布在 NB 上的,于是 P 可以利用第 2 节中介绍的零知识证明协议来检验是否有 $x'_j = x_j$,而不会泄露 P_j 的秘密影子 x_j,这只需将协议中的(g, h, G, H)替换为(g, g_i, y_j, k_{ij})即可. 这时根据 P_j 的证据(c'_{ij}, y_{ij}), P 可以检验下式是否成立:

$$c'_{ij} = Hc(g, g_i, y_j, k_{ij}, g^{y_{ij}}/y_j^{c'_{ij}}, g_i^{y_{ij}}/k_{ij}^{c'_{ij}}) \tag{11}$$

若成立,则确认子影子的合法性. 否则,则认为 P_j 有欺诈行为.

秘密恢复算法 W 中的每个秘密分享者 P 现在可以从 NB 上获得$\{r_i, h_i\}$,从 W 中的其他分享者 P_j 处收到 k_{ij}. 于是 P 可以离线独立计算

$$s_i = \Big(\sum_{P_j \in W} k_{ij}^{\$_j}\Big) r_i - h_i \bmod N \tag{12}$$

其中

$$\$_j = \sum_{P_j \in W \setminus \{P_j\}} (-I_k) \Big/ \sum_{P_k \in G \setminus W} (I_j - I_k) \tag{13}$$

因为由下面定理 1 即可保证:如果秘密分发者遵循分发协议且秘密分享者遵循协议,则 P 可正确恢复 P_d 发送的秘密信息 s_i.

定理 1 W 中的每个秘密分享者可通过式(12)恢复秘密 $s_i \in S$.

证明 有了 t 个秘密子影子 k_{ij},与 $\$_j$($j = 1, 2, \cdots, t$),由 Lagrange 插值公式易知

$$\begin{aligned} a_0 &= f(0) = \sum_{P_j \in W} f(I_j) \prod_{P_k \in W \setminus \{P_j\}} (-I_k)(I_j - I_k)^{-1} \\ &= \sum_{P_j \in W} f(I_j) \prod_{P_k \in G \setminus \{P_j\}} (I_j - I_k)^{-1} \prod_{P_k \in G \setminus W} (I_j - I_k) \prod_{P_k \in W \setminus \{P_j\}} (-I_k) \\ &= \sum_{P_j \in W} f(I_j) k_j^{-1} \$_j = \sum_{P_j \in W} (x_j \$_j) \pmod{Nc} \end{aligned}$$

于是由下面的推导可得 $s'_i = s_i$

$$\begin{aligned} s'_i &= \Big(\sum_{P_j \in W} k_{ij}^{\$_j}\Big) r_i - h_i = \Big(\sum_{P_j \in W} (g_{ij}^{x_j})^{\$_j}\Big) r_i - h_i \\ &= g_i^{\sum_{P_j \in W} x_j \$_j} r_i - h_i = g_i^{a_0} r_i - h_i = s_i \pmod N \end{aligned}$$

4 安全性分析

上述方案的安全性是基于离散对数计算和大数分解的困难性的,因而是计算安全的. 尽管子影子 k_{ij} 在恢复秘密 s_i 的计算中在门限组 W 中是公开的,但 P_j 的秘密影子 x_j 仍可保密. 因为由式(8),若已知 k_{ij}, g_i 求解 x_j 等价于离散对数的计算. 同样,知道秘密 s_i 也不会影响其余的秘密 s_t 的安全性,因为不同的秘密 s_i 有不同的 g_i, r_i 来对其进行随机化,因此每个秘密分享者可以利用同一个秘密影子重复产生不同的子影子来恢复不同的秘密,而系统的安全性不会受到影响.

欺诈检测 一个可验证的秘密分享方案应该为每个秘密分享者提供验证的能力,比如验证:(a)秘密分发者所提供的秘密影子是属实的;(b)一个秘密分享者发送给另一个秘密分享者的秘密子影子是属实的[4,5,7,8,10]. 事实上,在实际通信中,秘密分发者可能给分享者提供虚假的秘密影子;一个秘密分享者也可能给另一个秘密分享者发送虚假的秘密子影子. 下面的定理可保证本方案所提供的检测方法的正确性.

定理 2 秘密分发者对秘密影子的伪造可由每个分享者根据式(5a)识别.

证明 因为 $x_j = f(I_j) k_j^{-1} \bmod Nc$,有

$$(g^{k_j})^{x_j} = g^{k_j f(I_j) k_j^{-1}} = g^{f(I_j)} = g^{\sum_{k=0}^{t-1} a_k I_j^k} = \prod_{k=0}^{t-1} (v_k)^{(I_j)^k} \pmod N$$

定理 3 (子影子离线检测)若子影子 k_{ij} 真,则式(10)即 $c_{ij}^{e} = y_j k_{ij} \pmod N$ 成立. 亦即若等式 $c_{ij}^{e} = y_j k_{ij} \pmod N$ 不成立,则 P_j 必有欺诈.

证明 显然有

$$c_{ij}^{e} = (c_{ij}^{x_j})^{c} = ((gg_i)^{d})^{x_j e} = (g^{x_j})^{de} g_i^{x_j} = y_j k_{ij} \bmod N$$

由此可知,若秘密分享者企图伪造子影子 k_{ij} 而逃过检测必须知道 RSA 加密体制的私钥,这又等价于破译 RSA 因而是困难的.

定理 4 第 2 节中的零知识证明是正确的. 因而若式(11)成立,则可确认 P_j 所传子影子的合法性. 否则可确认 P_j 有欺骗行为.

证明 (1)假设(c, y)是有效证据,显然有 $c = Hc(g, h, G, H, g^{y}/G^{c}, h^{y}/H^{c})$.

(2)反之,若 $c = Hc(g, h, G, H, g^{y}/G^{c}, h^{y}/H^{c})$,令 $x = g^{y}/G$, $xc = h^{y}/H^{c}$,由于 8 是循环群,生成元为 g,因而 8 中任何一个元素可用 g 的幂来表示,于是设有整数 A, B, C, D 使得 $h = g^{A}$, $H = g^{B}$, $x = g^{C}$, $xc = g^{D}$,根据 x, xc 的定义,可得 $x = g^{y}/G = g^{C}$, $xc = h^{y}/H^{c} = g^{D}$,即 $g^{y-sc} = g^{C}$, $g^{Ay-Bc} = g^{D}$,从而 $y - sc = C \bmod m$, $Ay - Bc = D \bmod m$,因此可得 $CA - D = c(B - sA) \bmod m$,注意到 c 为由 hash 函数得到的随机值,所以 $B - sA = 0 \bmod m$,故 $H = g^{B} = g^{sA} = h^{s}$,由已知 $G = g^{s}$,这说明 G 与 H 相对于底数 g, h 有共同的离散对数.

再者,若有必要,子影子的合法性检测可通过式(10)与式(11)两次验证,更进一步加强了本方案的安全性.

5 结论

文中提出的多秘密门限分享方案,具有比较满意的特性,可用于会议秘密分配、安全分布式计算、电子商务等应用领域. 若考虑把本方案作适当的改进还可用于具有不同权限(如大会不同密级的文件分发)的秘密分享解决方案. 同时,由于它是基于离散对数计算和大数分解的困难性的,所以总体上是计算安全的. 当然,本方案是在假定安全信道已存在的情况

下着重讨论如何检测秘密分发者与秘密分享者的欺诈行为的. 若考虑秘密分发者与秘密分享者之间所传信息的认证功能, 以避免中间截获攻击, 可以采取签名或签密的办法[9] 对方案进行加强.

感谢　Ericsson 研究院 Rolf. J. Blum, Andras Mahes, Gorlan Selander 博士对本文初稿的建设性评论.

参考文献:

[1] E F Brickell, D M Daveport. On the classification of idea secret sharing scheme [J]. J Cryptology, 1991, 4(2): 123- 134.

[2] P A Fouque, G Poupard, J Stern. Sharing decryption in the context of voting or lotteries [A]. Proceedings of Financial Cryptography 2000 [C]. Berlin: Springer Verlag, 2000. 90- 104.

[3] M Tompa, H Woll. How to share a secret with cheaters [J]. Journal of Cryptology, 1988, 1(2): 133- 138.

[4] B Chor, S Goldwasser, S Micali, B Awerbuch. Veriable secret sharing and achieving simultaneity in the presence of faults[A]. Proceedings of 26th FOCS[C]. 1985. 251- 260.

[5] M Stadler. Publicly verifiable secret sharing [A]. Advances in cryptology—Eurocrypte96 [C]. Berlin: Springer Verlag, 1996. 190- 199.

[6] R G E Pinch. Online multiple secret sharing [J]. Electronics Letters, 1996, 32(12): 1087- 1088.

[7] R Gennaro, S Micali. Verifiable secret sharing as secure computation [A]. Advances in cryptology—Cryptoe 94 [C]. Berlin: Springer Verlag, 1995. 168- 182.

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

[9] 张福泰, 王育民, 郑东. 用签密构造可验证秘密分享方案 [A]. CCICS. 2001 论文集 [C]. 北京: 科学出版社, 2001. 244- 248.

[10] F Boudot, J Traore. 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.

作者简介:

何明星　男, 1964 年生于四川省南江县, 1990 年获重庆大学应用数学专业硕士学位, 现为四川工业学院计算机科学与工程系副教授, 西南交通大学计算机与通信工程学院通信与信息系统专业博士生, 主要研究兴趣为网络与信息安全、电子商务.

范平志　男, 1994 年获英国 Hull 大学通信工程专业博士学位, 现为西南交通大学计算机与通信工程学院教授, 博士生导师, IEEE 高级会员, 国家杰出青年基金获得者, 主要研究兴趣为移动通信、无线 IP、网络与信息安全.

(上接第 535 页)

参考文献:

[1] U M Maurer. Secret key agreement by public discussion from common information [J]. IEEE Trans IT, 1993, 39(3): 733- 742.

[2] M J Gander, U M Maurer. On the secret key rate of binary random variables [A]. Proc. of the 1994 IEEE Symp on Information Theory [C]. 1994. 351.

[3] U M Maurer. Protocols for secret key agreement based on common information [A]. Advances in Cryptology—CRYPTO. 92, Lecture Notes in Computer Science [C]. Berlin: Springer—Verlag, 1993. 740: 461- 470.

[4] Christian Cachin. Enropy measures and unconditional security in cryptography [D]. ETH, 1997.

[5] Stefan Wolf. Information—theoretically and computationally secure key agreement in sryptography [D]. ETH, 1999.