具有可追查性的抗合谋攻击门限签名方案①

周 萍[1,2]，何大可[1]

[1](西南交通大学 信息科学与技术学院，成都 610031)
[2](四川城市职业学院，成都 610101)

摘 要：好的门限签名方案应该具有很高的安全性，能够检测出任意不诚实成员的欺诈行为，同时能实现签名的匿名性和可追查性，并能抵抗合谋攻击和各种伪造性攻击。通过密码学分析和算法结构设计，首先讨论了实现门限签名匿名性和可追查性的一种有效方法，然后基于 Waters 基础签名方案，引入 Gennaro 分布式密钥生成协议、可验证秘密共享技术及部分签名验证协议，提出了一个具有匿名性和可追查性，抗合谋攻击及其他各种伪造性攻击，部分签名可验证的(t,n)门限签名方案，并在离散对数问题和双线性对逆运算问题两个困难问题假设下，给出了方案安全性的详细证明。

关键词：门限签名；合谋攻击；匿名性；可追查性；可验证

Threshold Signature Scheme with Traceability and Resisting Conspiracy Attack

ZHOU Ping[1,2], HE Da-Ke[1]

[1](College of Information Sciences & Technology, Southwest Jiaotong University, Chengdu 610031, China)
[2](Urban Vocational College of Sichuan, Chengdu 610110, China)

Abstract: The threshold signature schemes with better security cannot only detect any member's cheat behavior, provide anonymity and traceability simultaneously, but also resist conspiracy attack and every forgery attack. Through analysis for cryptography and algorithm design, it is discussed firstly of a method of the implementation of anonymity and traceability of threshold signature, then a partial signature verifiable (t, n) threshold signature scheme is proposed with anonymity and traceability simultaneously, resisting conspiracy attack and other forgery attacks. Based on the discrete logarithm difficulty and inverse bilinear pairing operation difficulty, certify has been given on security of the scheme in detail.

Key words: threshold signature; conspiracy attack; anonymity; traceability; verifiable

1 引言

门限签名是一种典型的数字签名技术，也是门限密码学研究的核心内容。自 1991 年 Desmedt 和 Frankel[1] 提出第一个门限签名方案以来，很多门限签名体制被相继提出[2-4]。门限签名中一个重要的研究课题是如何抵抗合谋攻击。所谓合谋攻击[5]是指当签名群中 t 个或更多成员合谋，可以获得其他成员的签名私钥和群签名私钥，进而伪造任何成员的部分签名或伪造群门限签名的现象。因此研究能够抵抗合谋攻击以及满足其他安全性要求的高效门限签名是很有意义的。本文给出一个具有可追查性和匿名性的，抗合谋攻击及其他各种伪造性攻击，可验证(t,n)门限签名方案，并给出方案的安全性证明。

2 匿名性和可追查性

一个优质的门限签名方案应该具有 8 个特性[6]：①群签名特性；②门限特性；③不可冒充性；④验证简单；⑤匿名性；⑥可追查性；⑦强壮性；⑧系统稳定性；匿名性是指任何人包括签名群内的任何成员，不管他是否参与签名，都不知道生成某个消息的签名的有哪些人；可追查性是指一旦发现有不诚实成员或

① 收稿时间:2011-08-24;收到修改稿时间:2011-10-30

成员子集伪造群内其他成员的签名，或其他不诚实事件发生时，可以追查到这些成员的身份。这就涉及到点 x_i 的选取(x_i 的用法见第 3 节)。由于在生成子密钥、子签名等诸多过程中要用到 x_i，若 x_i 表示真实身份则方案失去匿名性，若 x_i 和成员 P_i 毫无关联则方案不具备可追查性。因此方案要提供由 x_i 能够追查到成员 P_i 身份的方法。

为了使新方案同时具备匿名性和可追查性，我们设立一个仲裁机构 A。该机构的功能是赋予签名群内每个成员一个合法的身份，并在发生纠纷时能够进行合理的仲裁，提供不诚实成员的身份，也就是提供身份 ID 和点 x 之间的关系。当然 A 还可以有很多其他功能，以及为许多签名群服务。A 和签名群没有关系，它不是签名群内的成员或成员集合，也不参与任何消息的签名过程。

仲裁机构 A 通过以下过程为签名群($P_1,P_2,\cdots,P_n$)内所有成员提供身份：

1) A 为签名群选择两个互不相同的安全大素数 p,q，计算 N=pq 及 $\varphi(N)=(p-1)(q-1)$。A 再选择一个安全的 Hash 函数 $H:\{0,1\}^*\to Z^*_{\varphi(N)}$。

2) 签名群内的每个成员 P_i 将自己的身份信息 ID_i 发送给 A。

这里，成员的身份信息 ID_i 可以是成员的姓名，简称，群内代号或序号的函数(如 P_i 的 i 的函数 f(i))，也可以是成员的 IP 地址等能够唯一确定成员身份的信息。

3) A 按顺序 $P_1,P_2,\cdots,P_n$ 依次为每个成员 P_i (i=1,2,…,n)生成 x_i：

① 随机选取 e_i，满足 $1<e_i<\varphi(N)-1$，且 $\gcd(e_i,\varphi(N))=1$，计算 $d_i=e_i^{-1}\bmod\varphi(N)$。

② 计算 $x_i=H(ID_i)^{d_i}\bmod N$。

要求计算出的 $x_i\neq x_j(j=1,2,\cdots,i-1)$，若条件不成立则重新选取 e_i 进行①②过程。

③ A 将 xi 秘密发送给 Pi。

4) A 公布参数 N，Hash 函数 H()，同时安全删除 $p,q,\varphi(N)$，再将二元组(ID_i,e_i)秘密安全保存在表 LE (初始时为空)中。

当 P_i 伪造了其它成员的部分签名(或发生其他争执时)，签名合成者 D(或其他群内成员)找到 A 要求进行仲裁。D 将不诚实成员 P_i 的 x_i 发送给仲裁机构 A。A 遍历表 LE 并进行运算，找到符合条件 $x_i^{e_i}=H(ID_i)\bmod N$ 的二元组(ID_i,e_i)，将此(ID_i,e_i)发送给 D。D 验证 $x_i^{e_i}=H(ID_i)\bmod N$ 是否成立，若成立接受此 ID_i。如此 D 找到了不诚实成员 P_i 的身份 ID_i。这里规定，身份追查功能只向群内成员提供，若群外人向 A 发出要求，则 A 拒绝。

这是因为：

$$x_i^{e_i}=(H(ID_i)^{d_i}\bmod N)^{e_i}=H(ID_i)^{d_ie_i}=H(ID_i)\bmod N$$

有没有可能在表 LE 中找到两个符合条件的二元组，即出现 $x_i^{e_i}=H(ID_i)\bmod N$，$x_i^{e_k}=H(ID_k)\bmod N$，而 $i\neq k$ 的情况呢？这是不可能的。

因为：不失一般性，设：$x_1^{e_1}=H(ID_1)\bmod N$，$x_1^{e_2}=H(ID_2)\bmod N$，则：

$$x_1^{e_1}=H(ID_1)\ \mathrm{modN}\Rightarrow x_1=H(ID_1)^{d_1}\bmod N$$

且 $x_1^{e_2}=H(ID_2)\ \mathrm{modN}\Rightarrow x_1=H(ID_2)^{d_2}\bmod N=x_2$

由前述 x_i 的生成过程可知，不会出现 $x_1=x_2$，因此上述情况不会出现。

除了仲裁机构 A 外，任何人无法从 x_i 推测出用户的身份 ID_i。因为即使知道了参数 N 和 Hash 函数 H()，从 $x_i^{e_i}=H(ID_i)\bmod N$ 或 $x_i=H(ID_i)^{d_i}\bmod N$ 也无法计算出 ID_i，e_i 或 d_i，否则就是解决了离散对数难题及 Hash 函数逆运算难题。

3 新的具有可追查性的抗合谋攻击门限签名方案

在本节，基于 Waters 基础签名方案[7]，给出一个新的具有匿名性和可追查性的、抗合谋攻击和其他伪造性攻击、可验证(t,n)门限签名方案。该方案不需要可信中心，通过安全的 Gennaro 分布式密钥生成协议[8]实现群共享密钥的不可知性；采用可验证秘密共享技术（Verifiable Secret Sharing, VSS）实现对部分签名的验证；签名具有匿名性，在需要时可以追查出参与签名成员的真实身份；并且能够从根本上抵抗合谋攻击和各种伪造签名攻击。

方案由初始化阶段、门限密钥生成阶段、部分签名的生成和验证阶段、门限签名生成阶段、签名验证阶段和签名者身份追查阶段六部分组成。设签名消息均为 k 位二进制数(k 为一个固定的整数)，若消息不是 k 位的，则可以通过一个抗碰撞的 Hash 函数 $H_k:\{0,1\}^*\to\{0,1\}^k$ 将其映射为 k 位二进制数。

1) 初始化阶段

构造系统参数。n 个群成员($P_1,P_2,\cdots,P_n$)共同选取系统参数：两个乘法循环 GDH 群 G_1、G_2，他们的阶均为安全大素数 p，G_1 的生成元 g，随机选取一组 G_1 中不等于 g 的互不相同的元 $h,u',u_1,u_2,...,u_k$ (计算 $\log_g h$ 是不可行的)，选取双线性映射 e：$G_1\times G_1\rightarrow G_2$ 和抗碰撞的安全 hash 函数 $H:\{0,1\}^k\times G_1\times G_2\rightarrow Z_p^*$，计算 $g_1=e(g,g)$，$g_2=e(h,h)$。

签名群公布系统参数 $\{G_1,G_2,p,g,\ h,u',u_1,u_2,...,u_k,e,H,g_1,g_2\}$。

2) 门限密钥生成算法

① 如第 2 节所述，每个成员 P_i(i=1,⋯,n)在仲裁机构 A 的帮助下获得互不相同的整数 $x_i\in Z_p^*, x_i=x_i \bmod p$，这里 $x_i\neq x_j(1\le i,j\le n,i\neq j)$，将 x_i 作为自己的唯一标识，并在群内公布 x_i(此时注意不要泄露自己的身份)。

② 每个成员 P_i 都随机选择一个秘密分享 $\omega_i\in_R Z_p^*$，计算 ω_i 对应的公钥 $l_i=g_2^{\omega_i}$ 并在群内公布。其中，成员的公钥 l_i 须满足如下条件：任意 t 个成员所构成的成员子集 R 的 $L=\prod_{i\in R} l_i$ 均不相等。指定群内某成员将所有的共 C_n^t 个向量(L, $x_{i_1},x_{i_2},\cdots,x_{i_t}$)(这里 $i_1,i_2,\cdots,i_t\in\{1,2,\cdots,n\}$，且 C_n^t 个 L 互不相同)保存在一个表 TI 中并对外公布，做为签名群的系统参数之一。

③ 每个成员 P_i 随机选取一个系数在 Z_p 中、次数为 t-1 的多项式 $f_i(x)\in Z_p[x]$：$f_i(x)=a_{i0}+a_{i1}x+\cdots a_{i(t-1)}x^{t-1}$ ($a_{i0},a_{i(t-1)}\in Z_p^*$)

P_i 按如下步骤将 $f_i(x_j)$分发给其他成员：

a. 计算分享 $\lambda_{ij}=f_i(x_j)\bmod q$，并将 λ_{ij} 通过安全的信道秘密发送给成员 P_j ($j=1,2,\cdots,n,j\neq i$)，自己保留 λ_{ii}。

b. 将系数承诺 $g^{a_{i0}},g^{a_{i1}},\cdots,g^{a_{i(t-1)}}$ 在签名群中广播。

c. 每个成员 P_j 从其他成员 P_i 那里收到分享 λ_{ij} 后，用等式 $g^{\lambda_{ij}}=\prod_{k=0}^{t-1}(g^{a_{ik}})^{x_j^k}$ 是否成立来验证其有效性。如果未通过验证，P_j 拒绝该 λ_{ij}，并要求 P_i 重新发送 λ_{ij}。

当每个成员 P_i 所收到的 λ_{ij} 都通过验证等式后，P_i 计算 $\lambda_i=\sum_{j=1}^{n}\lambda_{ji}\bmod q$，并将($\omega_i$，$\lambda_i$)作为自己的签名私钥。

④ 输出公钥。为方便起见，定义 $F(x)=\sum_{i=1}^{n} f_i(x)$。当群中所有成员都成功地完成上述步骤后，各成员按如下方法计算群公钥 Y：

a. 每个成员 P_i 广播 $g_1^{a_{i0}},g_1^{a_{i1}},\cdots,g_1^{a_{i(t-1)}}$。

b. 每个成员 P_j 用下面的等式是否成立来验证所收到的广播值的有效性：

$$g_1^{\lambda_{ij}}=\prod_{k=0}^{t-1}(g_1^{a_{ik}})^{x_j^k}\quad (i,j=1,2,\cdots,n;i\neq j)$$

c. 每个成员 P_i 计算群公钥 Y 和子公钥 y_i：$Y=\prod_{j=1}^{n} g_1^{a_{j0}}$，$y_i=g_1^{\lambda_i}$，并公布群公钥 Y。

这里：$Y=\prod_{j=1}^{n} g_1^{a_{j0}}=g_1^{\sum_{j=1}^{n} f_j(0)}=g_1^{F(0)}\bmod p$，

$$y_i=g_1^{\lambda_i}=g_1^{\sum_{j=1}^{n} f_j(x_i)}=g_1^{F(x_i)}\bmod p$$

由此可知，相应的群私钥即为 $\lambda=F(0)=\sum_{i=1}^{n} f_i(0)$。

④ 每个成员 P_i 将(ω_i，λ_i)作为自己的子密钥，而将(l_i, y_i)作为自己的子公钥，并在群内部广播(x_i,l_i,y_i)。由于各成员的(x_i,l_i,y_i)仅在群内广播，因此群外的人并不知道群内任何成员的公钥。

3) 门限签名算法

设 m 为要签名的消息，m 的二进制串为 $(m_1,m_2,\cdots,m_k)\in\{0,1\}^k$。若 m 不是 k 位二进制串，则可通过一个安全的 hash 函数：$\{0,1\}^*\rightarrow\{0,1\}^k$,将映射为 k 位二进制串。设群中 t 个参与门限签名的成员构成集合 R。

① 每个签名成员 P_i ($P_i\in R$)任意选取随机数 $r_{i1},r_{i2}\in_R Z_p^*$，计算 $t_i=g^{r_{i1}}h^{r_{i2}}$，并将(x_i,l_i,t_i)秘密发送给 R 内的其他成员。

② 每个成员 P_i 得到 R 中所有其他成员的(x_i,l_i,t_i)后，首先计算：

$$T=\prod_{P_i\in R} t_i,\quad L=\prod_{P_i\in R} l_i,\quad H_1=H(m,T,L),$$

$$C_i=\prod_{P_j\in R,j\neq i}\frac{-x_j}{x_i-x_j}\ \bmod p$$

这里 C_i 是 R 集合中对应于成员 P_i 的 Lagrange 插值系数。

③ 每个成员 P_i 计算

$$\sigma_{i1}=g^{C_i\lambda_i}\bullet(u'\prod_{j=1}^{k}u_j^{m_j})^{r_{i1}},\quad \sigma_{i2}=h^{\omega_i H_1}\bullet(u'\prod_{j=1}^{k}u_j^{m_j})^{r_{i2}}\qquad(1)$$

并将部分签名 $\sigma_i=(\sigma_{i1},\sigma_{i2},t_i,x_i,l_i,y_i)$ 和中间参数(T,L)秘密发送给合成者。

④ 合成门限签名。合成门限签名的工作可由群内任何成员或成员组成的集合完成(合成者不一定是参与签名的成员)。简化起见，假定由指定成员 D 来完成。

D 收到所有成员的部分签名 $\sigma_i=(\sigma_{i1},\sigma_{i2},t_i,x_i,l_i,y_i)$ 和中间变量(T,L)后，按如下顺序工作：

① 验证(x_i,l_i,y_i)是成员 P_i 的身份标识 x_i 和子公钥(l_i,y_i)，即将该(x_i,l_i,y_i)和第 2 步门限密钥生成算法的第(4)步中的(x_i,l_i,y_i)相比较，如不符，要求 P_i 重新发送；

② 计算 $T=\prod_{P_i\in R}t_i$， $L=\prod_{P_i\in R}l_i$， $H_1=H(m,T,L)$ 和 t 个成员的 C_i： $C_i=\prod_{P_i\in R,j\neq i}\frac{-x_j}{x_i-x_j}\mod p$。检查自己计算的(T,L)及 t 个成员发来的共 t+1 个(T,L)是否完全相同。如不相同，说明有成员发送有误或不诚实。要求所有签名成员重新发送 σ_i 和(T,L)；

③ 用下式检验部分签名 σ_i 的有效性：

$$e(\sigma_{i1},g)e(\sigma_{i2},h)\bullet[e(t_i,u'\prod_{j=1}^{k}u_j^{m_j})]^{-1}=y_i^{C_i}l_i^{H_1} \quad (2)$$

若上式不成立，则 D 可认为该成员 P_i 是不诚实的，要求其重新生成部分签名。

④假定每个成员的部分签名都通过验证，D 计算 $\sigma=(\sigma_1,\sigma_2,T,L)$，其中：

$$\sigma_1=\prod_{P_i\in R}\sigma_{i1}，\quad \sigma_2=\prod_{P_i\in R}\sigma_{i2} \quad (3)$$

则 $\sigma=(\sigma_1,\sigma_2,T,L)$ 就是最终的门限签名。

4) 签名验证算法

给定公钥 Y，消息 $m=(m_1,m_2,\cdots,m_k)\in\{0,1\}^k$ 和 m 的签名 $\sigma=(\sigma_1,\sigma_2,T,L)$，首先验证 L 在表 TI 中存在，然后再验证等式：

$$e(\sigma_1,g)e(\sigma_2,h)\bullet[e(T,u'\prod_{j=1}^{k}u_j^{m_j})]^{-1}=YL^{H(m,T,L)} \quad (4)$$

是否成立。如果上述两个条件都满足，则签名有效，否则签名无效。

5) 签名成员身份追查

当发生纠纷时，群中的任何人都可以通过以下方法追查出生成某有效门限签名 $\sigma=(\sigma_1,\sigma_2,T,L)$ 的 t 个成员的身份，而群外的人无法追查到参与签名的具体成员。

首先，从表 TI 中查到和签名 $\sigma=(\sigma_1,\sigma_2,T,L)$ 中的 L 相对应的 $x_{i_1},x_{i_2},\cdots,x_{i_t}$，然后在仲裁机构 A 的帮助下，追查出参与门限签名的 t 个人的身份。则参加签名的成员即为这 t 个人。由第 2 节可知，身份追查功能只向群内成员提供，所以群外人不能追查出参与签名的具体成员。

4 正确性证明和安全性分析

4.1 正确性证明

方案的正确性由下面两个定理给出。

定理 1 若签名成员 P_i 诚实地生成了部分签名 $\sigma_i=(\sigma_{i1},\sigma_{i2},t_i,x_i,l_i,y_i)$，即其签名 σ_i 是由(1)计算而得，则 σ_i 满足部分签名验证等式(2)。

证明：若记 $U=u'\prod_{j=1}^{k}u_j^{m_j}$，则由部分签名的生成公式(1)可知：

$$\sigma_{i1}=g^{C_i\lambda_i}U^{r_{i1}}，\quad \sigma_{i2}=h^{\omega_iH_1}U^{r_{i2}}$$

因此，可得：

$$\begin{aligned}&e(\sigma_{i1},g)e(\sigma_{i2},h)\bullet[e(t_i,u'\prod_{j=1}^{k}u_j^{m_j})]^{-1}\\&=e(g^{C_i\lambda_i}U^{r_{i1}},g)e(h^{\omega_iH_1}U^{r_{i2}},h)\bullet[e(t_i,U)]^{-1}\\&=\frac{e(g^{C_i\lambda_i}U^{r_{i1}},g)e(h^{\omega_iH_1}U^{r_{i2}},h)}{e(g^{r_{i1}}h^{r_{i2}},U)}\\&=\frac{e(g^{C_i\lambda_i},g)e(U^{r_{i1}},g)e(h^{\omega_iH_1},h)e(U^{r_{i2}},h)}{e(g^{r_{i1}},U)e(h^{r_{i2}},U)}\\&=e(g,g)^{C_i\lambda_i}e(h,h)^{\omega_iH_1}=y_i^{C_i}l_i^{H_1}\end{aligned}$$

因此，验证等式(2)成立。

定理 2 如果方案中的 t 个成员都是诚实的，即都产生了合法的部分签名 $\sigma_i=(\sigma_{i1},\sigma_{i2},t_i,x_i,l_i,y_i)$，则由式(3)计算出来的门限签名 S 满足签名验证等式(4)。

证明：同上，若记 $U=u'\prod_{j=1}^{k}u_j^{m_j}$，则由部分签名的生成公式(1)可知： $\sigma_{i1}=g^{C_i\lambda_i}U^{r_{i1}}$， $\sigma_{i2}=h^{\omega_iH_1}U^{r_{i2}}$

再由(3)式可知：

$$\sigma_1=\prod_{P_i\in R}\sigma_{i1}=\prod_{P_i\in R}g^{C_i\lambda_i}U^{r_{i1}}=g^{\sum_{P_i\in R}C_i\lambda_i}U^{\sum_{P_i\in R}r_{i1}}=g^{\lambda}U^{r_1}，$$

$$(\text{记 } r_1=\sum_{P_i\in R}r_{i1}) \quad (5)$$

$$\sigma_2=\prod_{P_i\in R}\sigma_{i2}=\prod_{P_i\in R}h^{\omega_iH_1}U^{r_{i2}}=h^{\sum_{P_i\in R}\omega_iH_1}U^{\sum_{P_i\in R}r_{i2}}=h^{\sum_{P_i\in R}\omega_iH_1}U^{r_2}$$

$$(\text{记 } r_2=\sum_{P_i\in R}r_{i2}) \quad (6)$$

$$T=\prod_{P_i\in R}t_i=\prod_{P_i\in R}g^{r_{i1}}h^{r_{i2}}=g^{r_1}h^{r_2}，\quad L=\prod_{P_i\in R}l_i=\prod_{P_i\in R}g_2^{\omega_i}=g_2^{\sum_{P_i\in R}\omega_i}$$

因此，有：

$$e(\sigma_1,g)e(\sigma_2,h)\bullet[e(T,u'\prod_{j=1}^{k}u_j^{m_j})]^{-1}$$

$$=\frac{e(g^{\lambda}U^{r_1},g)e(h^{\sum_{P_i\in R}\omega_i H_1}U^{r_2},h)}{e(g^{r_1}h^{r_2},U)}$$

$$=\frac{e(g^{\lambda},g)e(U^{r_1},g)e(h^{\sum_{P_i\in R}\omega_i H_1},h)e(U^{r_2},h)}{e(g^{r_1},U)e(h^{r_2},U)}$$

$$=Yg_2^{\sum_{P_i\in R}\omega_i H_1}=YL^{H(m,T,L)}$$

因此，由式(3)计算出来的门限签名 S 满足签名验证等式(4)。证毕。

4.2 安全性分析

方案的安全性基于如下两个困难问题：

定义 1 离散对数问题(DLP)：假设 G 为一个生成元为 g，阶为 q 的乘法循环群。任给 $y\in G$，求 $x\in Z_q$，使得 $g^x=y$。

定义 2 双线性对逆运算问题(IBPOP)[9]：设 G_1、G_2 是两个乘法循环群，他们的阶均为大素数 q，G_1 的生成元 P，$e: G_1\times G_1\rightarrow G_2$ 为一个双线性映射。任给一个 $y\in RG_2$，求 $X\in G_1$，使 e(X,P)=y 成立。

文献[9]中证明了求解 IBPOP 的困难度，不小于在双线性对所基于的群 G_1,G_2 上求解 CDHP 的困难度，且不大于在 G_1,G_2 上求解离散对数问题的困难度。

我们从以下几个方面展开对方案的安全性分析。

1) 方案同时具有匿名性和可追查性。

由第 3 节的签名方案可知，方案能够在隐藏签名成员身份的同时，实现签名的可追查性。

定理 3 方案具有匿名性和可追查性。

证明：首先，在方案的门限密钥生成阶段和门限签名阶段，每个成员都是以 x_i 做为自己的唯一标识，参与密钥(公钥和私钥)生成的每个阶段，并在群内公布 (x_i,l_i,y_i)，同样签名时也是以 x_i 为标识参与签名，因此在这两个阶段中都没有泄露自己的身份 ID_i；其次，签名生成后，由门限签名 $\sigma=(\sigma_1,\sigma_2,T,L)$ 中的必要参数 L，可以通过查表 TI 的方法追查出参与签名的 t 个成员的标识 $x_{i_1},x_{i_2},\cdots,x_{i_t}$，然后在仲裁机构 A 的帮助下，确认出这 t 个成员的真实身份。因为 L 实际上是 t 个签名成员的公钥 l_i 之积，而群中任意 t 个成员的公钥之积 L 均不相等(参见第 3 节第(2)点第②小点中的定义)，且在表 TI 中(如果 L 不在表中则不能通过签名验证，签名无效)，因此可以在表 TI 中由 L 唯一地追查到 t 个成员的标识 $x_{i_1},x_{i_2},\cdots,x_{i_t}$；第三，因为所有成员的部分公钥($l_i$，$y_i$)仅在群内部公布，群外的任何人(包括门限签名的验证者、仲裁机构等)不能从 L 中获得签名成员的部分公钥。第四，如果参与签名的 t 个成员生成签名 (σ_1,σ_2,T,L) 后，想假冒成其他 t 个成员生成的，用那 t 个成员的标识 $x'_{i_1},x'_{i_2},\cdots,x'_{i_t}$ 查表 TI 得到的 L' 替换出自己的 L，则假冒签名 (σ_1,σ_2,T,L') 不能通过验证等式(4)，签名无效。

2) 方案能够抵抗各种伪造性攻击，包括群内成员的合谋攻击。

定理 4 攻击者不能伪造任意成员的合法部分签名。

证明：设攻击者 F 试图假冒合法成员 P_i 完成对消息 m 的部分签名。这时可分为两种情况：1. F 是群内某个恶意成员，2. F 是群外某个攻击者。若 F 是群内成员，则可在方案的门限密钥生成阶段得到 Pi 公布的公钥(x_i,l_i,y_i)，若不是群内成员，则不能得到(x_i,l_i,y_i)。无论哪种情况，由部分签名生成公式(1)可知，只知道(x_i,l_i,y_i)，不知道 P_i 的私钥 ω_i 和 λ_i，无法伪造出满足部分签名验证方程(2)的合法部分签名。而要想得到 ω_i 和 λ_i，他将面临求解离散对数难题。因此，F 不能伪造任意成员 P_i 的合法部分签名。

定理5 攻击者不能伪造签名群对某一消息m的合法的门限签名。

证明：假设攻击者 F 试图伪造签名群对消息 m 的门限签名。由式(5)(6)可知：

$$\sigma_1=g^{\lambda}U^{r_1}\ (\text{记}\ r_1=\sum_{P_i\in R}r_{i1}),\ \sigma_2=h^{\sum_{P_i\in R}\omega_i H_1}U^{r_2}\ \ (\text{记}\ r_2=\sum_{P_i\in R}r_{i2})$$

这里，记消息 m 的二进制串为

$(m_1,m_2,\cdots,m_k)\in\{0,1\}^k$，上式中：$U=(u'\prod_{j=1}^{k}u_j^{m_j})$，

$H_1=H(m,T,L)$。且：$T=\prod_{P_i\in R}t_i=\prod_{P_i\in R}g^{r_{i1}}h^{r_{i2}}=g^{r_1}h^{r_2}$，

$$L=\prod_{P_i\in R}l_i=\prod_{P_i\in R}g_2^{\omega_i}=g_2^{\sum_{P_i\in R}\omega_i}$$

设 F 首先随机选取整数 $r_1,r_2\in_R Z_p^*$，计算 $T=g^{r_1}h^{r_2}$。由上述(5)(6)可知，不知道群私钥 λ =F(0)和 $\sum_{P_i\in R}\omega_i$，无法构造满足验证方程(4)的合法的门限签名。而 F 并不知道 $\sum_{P_i\in R}\omega_i$ (事实上群内任何成员均不知道 $\sum_{P_i\in R}\omega_i$)。因此，一方面如果 F 想要得到 λ 和 $\sum_{P_i\in R}\omega_i$，F 将面临求解离散

对数难题；另一方面，如果 F 选择随机数 $r_1,r_2 \in_R Z_p^*$ 和 $\lambda',l \in_R Z_p^*$ (用来代替 λ 和 $\sum_{P_i \in R}\omega_i$)，计算出 $T=g^{r_1}h^{r_2}$ 和 $L=g_2^l$，然后计算 $H_1=H(m,T,L)$，$\sigma_1=g^{\lambda'}U^{r_1}$，$\sigma_2=h^{lH_1}U^{r_2}$，则验证方程(4)不能成立(因为 $Y \neq g^{\lambda'}$)，且该 L 不在表 TI 内因此也不能通过验证；若只选择随机数 $r_1,r_2 \in_R Z_p^*$，不选择 $\lambda',l \in_R Z_p^*$，而从验证方程(4)中直接求出门限签名(σ_1,σ_2)，也将面临求解双线性对逆运算问题。因此，攻击者不能伪造出签名群对消息 m 的能够通过验证的合法门限签名。

下面讨论新方案的抗合谋攻击能力。

定理 6 方案中，即使 t 个或更多恶意成员合谋，也无法伪造任意成员的合法部分签名。

证明：若签名群内的 t 个或更多恶意成员合谋，则他们可以利用自己手中的私钥 $\lambda_j=F(x_j) \bmod p$，用 Lagrange 插值公式重构出 t-1 次多项式 F(x)，然后计算出欲伪造成员 P_i 的私钥 $\lambda_i=F(x_i) \bmod p$。但是他们无法获取该成员的另一个私钥 ω_i。如果想要从 $l_i=g_2^{\omega_i}$ 推算出 ω_i，将面临求解离散对数难题；如果任意选择一个整数 $\omega_i' \in_R Z_p^*$，计算出 $l_i'=g_2^{\omega_i'}$ 来代替 l_i，则无法通过部分签名验证公式(2)和(x_i,l_i,y_i)身份验证；如果采用真实的，想要从部分签名验证公式(2)推算出部分签名 $\sigma_i=(\sigma_{i1},\sigma_{i2},t_i,x_i,l_i,y_i)$ 中的 σ_{i2} (这时 $\sigma_{il}=g^{C_i\lambda_i}U^{r_{i1}}$ 可以计算出来)，将面临求解双线性对逆运算问题。总之，只知道私钥 λ_i，不知道私钥 ω_i，无法合成能够通过部分签名验证公式(2)的有效部分签名。即使 t 个或更多恶意成员合谋也无法伪造任意成员的合法部分签名。

类似于定理 6 的证明，可以得到下面的定理 7。

定理 7 方案中，即使 t 个或更多恶意成员合谋，也无法伪造出其他 t 人签名子群代表签名群的对任意消息 m 的合法门限签名。

3) 方案利用可验证秘密共享技术，实现了对分享 λ_{ij} 的可验证性。

方案基本采用了 Gennaro[8]的分布式密钥生成协议。在分发 λ_{ij} 时，通过引入可验证秘密共享技术来验证 λ_{ij} 的有效性，防止秘密分发者的不诚实行为。新方案在生成部分私钥阶段，各成员 P_i 在秘密发送 λij 的同时广播该多项式各系数的承诺 $g^{a_{i0}},g^{a_{i1}},\cdots,g^{a_{i(t-1)}}$，使接收者可以利用这些承诺值及验证等式：

$$g^{\lambda_{ij}}=\prod_{k=0}^{t-1}(g^{a_{ik}})^{x_j^k}$$

验证收到的 λ_{ij} 是否正确，同时在输出公钥时，各成员 P_i 公布 $g_1^{a_{i0}},g_1^{a_{i1}},\cdots,g_1^{a_{i(t-1)}}$，接收者可以利用验证等式：$g_1^{\lambda_{ij}}=\prod_{k=0}^{t-1}(g_1^{a_{ik}})^{x_j^k}$ 再次验证收到的 λ_{ij} 是否正确，及 $g_1^{a_{i0}},g_1^{a_{i1}},\cdots,g_1^{a_{i(t-1)}}$ 是否正确。而在这两次验证过程中，由离散对数问题的难解性，接收者并不能得到关于多项式 f(x)及系数 $a_{i0},a_{i1},\cdots,a_{i(t-1)}$ 的任何信息。这样就保证了秘密分发者的诚实性，实现了分享 λ_{ij} 的可验证性。

4.3 和其他方案的比较

一个实用的门限签名方案应该具有很高的安全性能，包括能够检测出任意不诚实成员在生成密钥阶段和生成部分签名阶段的欺诈行为；能够同时实现签名的匿名性和可追查性；能够抵抗合谋攻击和各种伪造性攻击。本文方案具有上述多种安全性，同时在分发分享 λ_{ij} 时每个接收成员都必须验证 λ_{ij} 的正确性，因此可以防止秘密分发者的欺诈行为。

在文献[3]的方案中，部分签名可验证，可以抵抗合谋攻击，签名具备可追踪性，但不具备匿名性。同时因为每个成员的私钥 x_i 都是由密钥分配中心 SDC 生成，SDC 知道所有成员的签名密钥。方案因此无法抵抗不可信 SDC 对任意消息的伪造性攻击。

文献[4]的方案没有可信中心，所有成员运行交互式协议共同生成签名私钥和公钥。部分签名可验证，可以抵抗合谋攻击和各种伪造性攻击，签名不具备可追踪性和匿名性。同时分享 λ_{ij} 没有进行正确性验证，无法防止不诚实成员在生成密钥阶段的欺诈行为。

5 总结

本文给出一个新的具有匿名性和可追查性的、抗合谋攻击和其他伪造性攻击、可验证(t,n)门限签名方案。该方案不需要可信中心，通过安全的分布式密钥生成协议实现群共享密钥的不可知性，并可防止不诚实成员在分发分享时的欺诈行为；采用可验证秘密共享技术实现对部分签名的验证；签名具有匿名性，在需要时可以追查出参与签名成员的真实身份；并且能够从根本上抵抗合谋攻击和各种伪造签名攻击。相比于其他门限签名，本方案具有更强的系统安全可靠性，将在电子商务及其他领域发挥更大的作用。

(下转第 81 页)

基于状态图的测试主要有以下 5 种覆盖准则：(1)状态覆盖(2)转移覆盖(3)转移对覆盖(4)ZOT 循环覆盖准则(5)全 ZOT 路径覆盖准则[4]。限于篇幅，在这里采用转移覆盖准则。依据状态转换图以及引入的具体状态，得到如下的分枝树。

取分枝树的每一条分枝，即是满足转移覆盖准则的测试序列：

1--2′ --3--4

1--2′ --3--2

1--2″ --4′ --5′ --4

1--2″ --4′ --5′ --6

1--2″ --4--2

1--2″ --4″ --6--4

1--2″ --4″ --6--5″ --6

3.3 结果分析

一般运用状态转换图进行问题的分析通常需要考虑状态爆炸的问题。本例在只有 3 个进程的假设前提下对非确定的状态转换，通过引入具体状态而进行确定化，以生成有效的测试序列。事实上，在具体执行的过程中，所有的状态均为具体状态，状态转换图也可以作为测试结果的验证依据。

4 结语

本文对基于形式化 B 规格进行测试用例自动生成的研究，给出了效用谓词的生成过程与其充分性分析，同时对基于集合的状态模型转换为状态转换图，并对非确定的状态图进行确定性转换，按照转移覆盖原则生成测试序列。下一步的研究工作是结合测试脚本，真正实现测试过程自动化。

参考文献

1 Legeard B, Peureux F, Utting M. Automated Boundary Testing from Z and B. Proc. of the International Conference on Formal Methods Europe (FME'02). Copenhagen, Denmark, July 2002. LNCS 2391, Springer-Verlag, 2002: 21–40.

2 Dick J, Faivre A. Automating the generation and sequencing of test cases from model-based specifications. FME'93: Industrial-Strength Formal Methods. LNCS 670, Springer-Verlag, April 1993: 268–284.

3 van Aertryck L, Benveniste M, Le Metayer D. CASTING: a formally based software test generation method. 1st IEEE International Conference on Formal Engineering Methods (ICFEM'97). 1997: 99–112.

4 李鹏,彭祥伟,周喜,等.基于状态图的测试路径自动生成.计算机工程,2011,37(2):25–29.

5 马亮,张刚.测试用例自动生成方法的现状及研究.现代电子技术,2008.

6 Abrial JR.裘宗燕译.B 方法.北京:电子工业出版社,2004.

7 Legeard B, Peureux F. Generation of functional test sequences from B formal specifications-presentation and industrial case-study. 16th IEEE International Conference on ASE2001. 2001: 377–381.

(上接第 76 页)

参考文献

1 Desmedt Y, Frankel Y. Shared Generation of Authenticators and Signatures. In: Feigenbaum J, ed, Advances in Cryptology-Crypto'91 Proc. LNCS 576, Berlin: Springer-Verlag, 1992:457–469.

2 Xie Q. Cryptanalysis and improvement of two threshold signature schemes. Journal of Communications, 2005,26(7): 123–128.

3 徐光宝,姜东焕.抗合谋攻击的门限签名方案分析与改进.计算工程,2010,36(20):155–156,166.

4 高炜,于晓冬.对一个无可信中心的(t,n)门限签名方案的改进,2010,46(1):84–86.

5 Li CM, Hwang T, Lee NY. Remark on the threshold RSA signature scheme. In: Stinson DR, ed, Advances in Cryptology-Crypto'93 Proc. LNCS773, Berlin: Springer-Verlag, 1994: 413-420.

6 王贵林,卿斯汉.几个门限群签名方案的弱点.软件学报,2000,11(10):1326–1332.

7 Waters B. Efficient identity-based encryption without random oracles. Advances in Cryptology-Eurocrypt 2005. LNCS 3494, Berlin: Springer-Verlag, 2005: 114–127.

8 Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems. Advances in Cryptology -EUROCRYPT 1999. LNCS 1592, Berlin: Springer-Verlag, 1999, 295–310.

9 辛向军,肖国镇.几种具有附加性质的数字签名体制的研究[博士学位论文].西安:西安电子科技大学,2007.