一种门限的基于身份无需随机预言的签名方案

蔡永泉, 张 可
(北京工业大学计算机学院, 北京 100022)

摘 要: 本文针对 Paterson 无需随机预言的签名方案, 提出了一种新的基于身份的无需随机预言的(t, n)门限签名方案, 并分析了新方案的正确性和安全性. 分析结果表明, 在离散对数难题下, 参与者能方便的产生个体签名, 公开验证者可通过验证公式, 决定是否接受个体签名和门限签名. 而任何攻击者不能伪造个体签名, 不能通过窃听个体签名、门限签名和其他公开信息得到系统秘密值, 即使已知所有参与者的秘密值, 也无法伪造门限签名. 该方案在各种可能的攻击下是安全的.

关键词: 基于身份门限签名; 分布式密钥产生协议; 双线性映射
中图分类号: TP393. 08 文献标识码: A 文章编号: 0372-2112 (2008) 10-1966-04

An ID-based Threshold Signature Scheme without Random Oracle

CAI Yong-quan, ZHANG Ke
(*College of Computer Science and Technology, Beijing University of Technology, Beijing* 100022, *China*)

Abstract: In a (t, n) threshold signature scheme, any sub set comprising at least t members is capable of signing any message, and incapable otherwise. The focuses of this paper are to propose a ID-based (t, n) threshold signature scheme without random oracle based on Paterson's signature scheme which is also without random oracle, and to analyze the validity and the security of the scheme as well. An important feature of our scheme, in which partial signatures can be expediently generated by participants under the discrete logarithm problem and any pubic verifier can check the validity of partial signatures and threshold signatures, is that any attacker, however, cannot obtain system secret value through the public information or by eavesdropping some partial signatures and threshold signatures, and neither can he forge partial signatures. Given the knowledge of all the participants' secret values, a threshold signature cannot be forged. This method is secure in various possible attacks.

Key words: identity-based threshold signature; distributed key generation protocol; bilinear pairing

1 引言

数字签名因防伪造、防抵赖、易于生成和传输等优点在信息安全中占有重要作用, 使得人们始终关注对它的研究. 此研究大体可分为两个时期, 即 1984 年前和 1984 年后. 前期研究的各种数字签名有非门限签名和门限签名. 门限签名由于采用(t, n)门限与非门限签名相比可以有多个签名者参加且更安全, 但无论是非门限签名或门限签名都必须借助于 CA 系统, 一旦 CA 系统被攻破, 就无法对签名进行验证. 后期研究以 Shamir[1] 于 1984 年提出的基于身份的签名方案为代表, 该签名允许任何用户使用签名者的标识符(如电子邮件地址等)来验证签名, 改变了数字签名对 CA 系统的依赖, 使得数字签名更便捷更可靠. 由于基于身份的数字签名具有众多的优点, 从而掀起了基于身份数字签名研究的热潮. 根据 Boneh[2], Cha、Cheon[3] 和 Hess[4] 提出的双线性配对技术构造的基于身份的加密方案, 提出了利用基于身份和双线性配对的签名方案. 随后, Paterson[5] 在 2006 年 ACISP 上提出了一种基于身份的无需随机预言的签名方案. 但他们的签名方案都只能用于单个签名人的签名, 不能用于多人签名, 且不具备门限功能.

本文针对 Paterson 签名方案, 结合 Gennaro[6] 分布式密钥产生协议, 提出了一种门限的基于身份无需随机预言的签名方案. 该方案不仅运算效率改善, 而且安全性提高, 以改变以上方案的不足.

2 理论背景

2.1 双线性映射

设 G 和 G_T 为阶同为素数 p 的乘法循环群, g 为 G 生成元, 双线性映射 $e: G \times G \rightarrow G_T$ 具有如下性质的映射:

收稿日期: 2007-09-17; 修回日期: 2008-04-28
基金项目: 国家 863 高技术研究发展计划(No. 2006AA01Z440)

(1) 线性性: 对于所有的 $u, v \in G, a, b \in Z_p$, 都有 $e(u^a, v^b) = e(u, v)^{ab}$.

(2) 非退化性: $e(g, g) \neq 1$.

(3) $e(u, v) = e(v, u)$.

根据以上性质可得:

(1) 对任意的 $u \in G, v_1, v_2 \in G_T$, 满足 $e(u, v_1 v_2) = e(u, v_1) \cdot e(u, v_2)$.

(2) 对定义在 G 上的函数 Ψ, 和任意 $u, v \in G$, 满足 $e(u, \Psi(v)) = e(v, \Psi(u))$.

2.2 双线性 **Diffie-Hellman (Bilinear Diffie-Hellman)** 问题

给定 G 中元素 g, g^a, g^b, g^c, 计算 G_T 中的元素 $e(g, g)^{abc}$, 攻击者 A 在 G 中解 Bilinear Diffie-Hellman (简称 BDH) 问题的优势 ε 定义为: $\Pr[A(g, g^a, g^b, g^c) = e(g, g)^{abc}] \geqslant \varepsilon$.

2.3 Computational Diffie-Hellman 难题:

给定阶为素数 p、生成元为 g 的群 G, $g^a, g^b \in G$, 其中 a, b 是从 Z_p^* 中均匀随机选择的, 则 G 中的 Computational Diffie-Hellman (简称 CDH) 难题为计算 g^{ab}.

2.1 (ε, t)-**CDH** 假设:

如果没有能在运算时间 t 内以至少 ε 的概率解决 CDH 难题的算法, 则我们说 (ε, t)-CDH 假设成立.

3 基于身份的无需随机预言的门限签名方案

设该方案含有 1 个指定的合成者 (DS, Designated Synthesist) 和 n 个参与者, 其过程包括密钥的产生 (参数产生阶段无需可信中心)、签名和验证. 每个参与者利用他的私钥 $(\alpha, x_i, r_{ui}, r_{mi})$ 生成个体签名, 并发送给 DS, 而 DS 不知道任何参与者的秘密信息. 收到个体签名后, DS 把所有通过验证的个体签名合成为门限签名. 本方案中门限值为 t.

3.1 签名密钥和验证密钥的产生

我们以 Gennaro 协议为基础, 提出一个参数产生算法. 按照此算法, 所有参与的 n 方在无需存储密钥、重建密钥和可信第三方的情况下, 可以合作生成各自的秘密分享和公钥.

步骤 1　系统选择阶同为素数 p 的群 G, G_T 和秘密参数 α ($\alpha \in \boldsymbol{Z}_p$, 其中 $\boldsymbol{Z}_p$ 是以素数 p 为模的整数集合), 计算 $g_1 = g^\alpha$ (其中 g 是 G 的生成元), 随机选择 $g_2, u', m' \in G$. 并定义长度分别为 n_u 和 n_m 的向量 $\boldsymbol{U} = \{u_i\}$, $\boldsymbol{M} = \{m_i\}$, 向量的元素从 G 中随机选取. p_a 将 α 通过秘密信道传输给其他成员 $p_1, p_2, \ldots, p_n$, 将以上其他参数广播.

步骤 2　p_1 随机选择 $a_{1,k} \in_R \boldsymbol{Z}_p$, $(k = 0, 1, \ldots, t)$, 并选择属于他自己的 t 阶多项式 $f_1(X) = \sum_{k=0}^{t} a_{1,k} X^k \pmod p \in \boldsymbol{Z}_q[X]$, 得 $f_1(0) = a_{1,0}$; p_2 随机选择 $a_{2,k} \in_R \boldsymbol{Z}_q$, $(k = 0, 1, \ldots, t)$, 并选择属于他自己的 t 阶多项式 $f_2(X) = \sum_{k=0}^{t} a_{2,k} \cdot X^k \pmod p \in \boldsymbol{Z}_q[X]$, 得 $f_2(0) = a_{2,0}$, ……, p_n 随机选择 $a_{n,k} \in_R \boldsymbol{Z}_p$, $(k = 0, 1, \ldots, t)$, 并选择属于他自己的 t 阶多项式 $f_n(X) = \sum_{k=0}^{t} a_{n,k} X^k \pmod p \in \boldsymbol{Z}_q[X]$, 得 $f_n(0) = a_{n,0}$

步骤 3　p_1 对 $j = 1, 2, \ldots, n$ 且 $j \neq 1$ 和 $k = 0, 1, \ldots, t$, 计算 $s_{1j} = f_1(j)$, $A_{1,k} = e(g_2, g)^{\alpha_{1,k}} \pmod p$, $y_{1,j} = e(g_2, g)^{\alpha s_{1,j}} \pmod p$. 然后将 s_{1j} 秘密的发送给其他成员 p_j ($j = 1, 2, \ldots, n$ 且 $j \neq 1$), 并广播 $A_{1,k}$ 和 $y_{1,j}$; p_2 对 $j = 1, 2, \ldots, n$ 且 $j \neq 2$ 和 $k = 0, 1, \ldots, t$, 计算 $s_{2j} = f_2(j)$, $A_{2,k} = e(g_2, g)^{\alpha a_{2,k}} \pmod p$, $y_{2,j} = e(g_2, g)^{\alpha s_{2,j}} \pmod p$. 然后将 S_{2j} 秘密的发送给其他成员 p_j ($j = 1, 2, \ldots, n$ 且 $j \neq 2$), 并广播 $A_{2,k}$ 和 $y_{2,j}$; ……; p_n 对 $j = 1, 2, \ldots, n$ 且 $j \neq n$ 和 $k = 0, 1, \ldots, t$, 计算 $s_{nj} = f_n(j)$, $A_{n,k} = e(g_2, g)^{\alpha_{n,k}} \pmod p$, $y_{n,j} = e(g_2, g)^{\alpha s_{n,j}} \pmod p$. 然后将 $s_{n,j}$ 秘密的发送给其他成员 p_j ($j = 1, 2, \ldots, n$ 且 $j \neq n$), 并广播 $A_{n,k}$ 和 $y_{n,j}$.

参与者收到 $A_{1,k}, A_{2,k}, \ldots, A_{n,k}, y_{1,j}, y_{2,j}, \ldots, y_{n,j}$ 后, 结合以前收到的系统参数后执行步骤 4.

步骤 4　p_1 对于 $i = 1, 2, \ldots, n$, 验证: $y_{i,1} = \prod_{k=0}^{t} A_{i,k}^{1^k}$ 是否成立; p_2 对于 $i = 1, 2, \ldots, n$, 验证: $y_{i,2} = \prod_{k=0}^{t} A_{i,k}^{2^k}$ 是否成立; ……; p_n 对于 $i = 1, 2, \ldots, n$, 验证: $y_{i,n} = \prod_{k=0}^{t} A_{i,k}^{n^k}$ 是否成立.

$$Q \prod_{k=0}^{t} A_{i,k}^{1^k} = \prod_{k=0}^{t} [e(g_2, g)^{\alpha \cdot a_{j,k}}]^{1^k} = e(g_2, g)^{\alpha \cdot \sum_{k=0}^{t} (a_{j,k} \cdot 1^k)} = e(g_2, g)^{\alpha \cdot f_i(1)} \pmod p,$$

又 $y_{i,1} = e(g_2, g)^{\alpha s_{i,1}} = e(g_2, g)^{\alpha f_i(1)}$,

$$\prod_{k=0}^{t} A_{i,k}^{2^k} = \prod_{k=0}^{t} [e(g_2, g)^{\alpha \cdot a_{j,k}}]^{2^k} = e(g_2, g)^{\alpha \cdot \sum_{k=0}^{t} (a_{i,k} \cdot 2^k)} = e(g_2, g)^{\alpha \cdot f_i(2)} \pmod p,$$

又 $y_{i,2} = e(g_2, g)^{\alpha s_{i,2}} = e(g_2, g)^{\alpha f_i(2)}$,

……,

$$\prod_{k=0}^{t} A_{i,k}^{n^k} = \prod_{k=0}^{t} [e(g_2, g)^{\alpha \cdot a_{i,k}}]^{n^k} = e(g_2, g)^{\alpha \cdot \sum_{k=0}^{t} (a_{i,k} \cdot n^k)} = e(g_2, g)^{\alpha \cdot f_i(n)} \pmod p,$$

又 $y_{i,n} = e(g_2, g)^{\alpha \cdot s_{i,n}} = e(g_2, g)^{\alpha f_i(n)}$,

所以我们可以通过检查 $\prod_{k=0}^{t} A_{i,k}^{1^k}$ 是否等于 $y_{i,1}$, $\prod_{k=0}^{t} A_{i,k}^{2^k}$ 是否等于 $y_{i,2}$, ……, $\prod_{k=0}^{t} A_{i,k}^{n^k}$ 是否等于 $y_{i,n}$ 来验证分发的正确性.

如果 $p_1, p_2, \ldots, p_n$ 都通过了验证, 我们称通过验证后的参与者集合为 Q.

步骤 5. 对 $j \in Q$, 参与者 p_1 计算属于他的秘密分享 $x_1 = \sum_{j \in Q} s_{j,1}$; 参与者 p_2 计算属于他的秘密分享 $x_2 =$

$\sum_{j\in Q}s_{j,2}$; …; 参与者 p_n 计算属于他的秘密分享 $x_n=\sum_{j\in Q}s_{j,n}$. 那么所有参与者隐式的共同享有秘密值 $x=\sum_{i=0}^{n}a_{i,0}$.

执行以上步骤以后, 可得公共参数$(G, G_T, e, g, g_1, g_2, u', U, m', m, M)$, p_i 的公钥 $C_i=e(g_2, g_1)^{x_i}$和系统公钥$S=\prod_{i\in Q}A_{i,0}=e(g_2, g_1)^{\sum_{i\in Q}f_i(0)}(\mathrm{mod}\ p)$. 这样, 以上参数和参与者集合 Q 形成公钥为$(S, C_1, C_2, \cdots, C_n)$和秘密分享为$(x_1, \cdots, x_n)$的门限系统.

3.2 签名和验证

(1)为了对消息 m 进行有效的签名, 首先对 m 的二进制串进行统计, 令所有为 1 的位的序号的集合为 Γ. 类似的, 参与者 p_i 的身份可表示为二进制串, 其所有为 1 的位的序号的集合为 Ω. p_i 随机选择 $r_{ui}, r_{mi}\in\mathbf{Z}_p$. 则 p_i 的个体签名为 $\sigma_i=(V_i, R_{ui}, R_{mi}, i)$, 其中 $V_i=g_2^{\alpha x_i}(u'\prod_{k\in\Omega}u_k)^{r_{ui}}(m'\prod_{j\in\Gamma}m_j)^{r_{mi}}$, $R_{ui}=g^{r_{ui}}$, $R_{mi}=g^{r_{mi}}$.

(2) Q 中每一个参与者 p_i 将 σ_i 发送给任意指定合成者(DS), DS 对每个个体签名进行验证.

定理 1 若等式 $e(V_i, g)\cdot e(u'\prod_{k\in\Omega}u_k, R_{ui})^{-1}\cdot e(m'\prod_{j\in\Gamma}m_j, R_{mi})^{-1}=C_i$ 成立, 则 σ_i 为有效个体签名.

证明 将 $e(V_i, g)\cdot e(u'\prod_{k\in\Omega}u_k, R_{ui})^{-1}\cdot e(m'\prod_{j\in\Gamma}m_j, R_{mi})^{-1}$写成如下形式:

$$e(V_i, g)=e[g_2^{\alpha x_i}(u'\prod_{k\in\Omega}u_k)^{r_{ui}}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}}, g] \quad (1)$$

$$e(u'\prod_{k\in\Omega}u_k, R_{ui})^{-1}=e(u'\prod_{k\in\Omega}u_k, g^{r_{ui}})^{-1}=e[(u'\prod_{k\in\Omega}u_k)^{-r_{ui}}, g] \quad (2)$$

$$e(m'\prod_{j\in\Gamma}m_j, R_{mi})^{-1}=e(m'\prod_{j\in\Gamma}m_j, g^{r_{mi}})^{-1}=e[(m'\prod_{j\in\Gamma}m_j)^{-r_{mi}}, g] \quad (3)$$

$C_i=e(g_2, g)^{\alpha\cdot x_i}$

$$\begin{aligned}&e(V_i, g)\cdot e(u'\prod_{k\in\Omega}u_k, R_{ui})^{-1}\cdot e(m'\prod_{j\in\Gamma}m_j, R_{mi})^{-1}\\&=e\{[g_2^{\alpha x_i}(u'\prod_{k\in\Omega}u_k)^{r_{ui}}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}}]\\&\quad\cdot[(u'\prod_{k\in\Omega}u_k)^{-r_{ui}}][(m'\prod_{j\in\Gamma}m_j)^{-r_{mi}}], g\}\\&=e[g_2^{\alpha x_i}, g]\\&=e[g_2, g]^{\alpha x_i}\\&=C_i\end{aligned}$$

(3)如果所有个体签名通过了 DS 的验证, 那么 DS 计算 $V=\prod_{i\in Q}V_i^{L_i}$, $R_u=\prod_{i\in Q}R_{ui}^{L_i}$, $R_m=\prod_{i\in Q}R_{mi}^{L_i}$, 其中 L_i 为拉格朗日插值系数, $L_i=\prod_{j\in Q, j\neq i}\left(\frac{-j}{i-j}\right)$. 最后, DS 发布门限签名 $\sigma=(V, R_u, R_m)$.

(4)公开的验证者可通过系统公钥 $S=\prod_{i\in Q}A_{i,0}$来验证门限签名 σ.

定理 2 若等式 $e(V, g)\cdot e(u'\prod_{k\in\Omega}u_k, R_u)^{-1}\cdot e(m'\prod_{j\in\Gamma}m_j, R_m)^{-1}=S$ 成立, 则 σ 为有效的门限签名, 否则无效.

证明 同样将此验证公式等号左边三项分别展开:

$$\begin{aligned}e(V, g)&=e(\prod_{i\in Q}V_i^{L_i}, g)\\&=e\{\prod_{i\in Q}[g_2^{\alpha x_i}\cdot(u'\prod_{k\in\Omega}u_k)^{r_{ui}}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}}]^{L_i}, g\}\\&=\prod_{i\in Q}e\{[g_2^{\alpha x_i}\cdot(u'\prod_{k\in\Omega}u_k)^{r_{ui}}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}}]^{L_i}, g\} \quad (4)\end{aligned}$$

$$\begin{aligned}e(u'\prod_{k\in\Omega}u_k, R_u)&=e(u'\prod_{k\in\Omega}u_k, \prod_{i\in Q}R_{ui}^{L_i})\\&=e[u'\prod_{k\in\Omega}u_k, \prod_{i\in Q}(g^{r_{ui}})^{L_i}]\\&=\prod_{i\in Q}e[u'\prod_{k\in\Omega}u_k, (g^{r_u})^{L_i}] \quad (5)\end{aligned}$$

$$\begin{aligned}e(m'\prod_{j\in\Gamma}m_j, R_m)&=e(m'\prod_{j\in\Gamma}m_j, \prod_{i\in Q}R_{mi}^{L_i})\\&=e[m'\prod_{j\in\Gamma}m_j, \prod_{i\in Q}(g^{r_{mi}})^{L_i}]\\&=\prod_{i\in Q}e[m'\prod_{j\in\Gamma}m_j, (g^{r_{mi}})^{L_i}] \quad (6)\end{aligned}$$

则 $e(V, g)\cdot e(u'\prod_{k\in\Omega}u_k, R_u)^{-1}\cdot e(m'\prod_{j\in\Gamma}m_j, R_m)^{-1}$

$$\begin{aligned}&=\{\prod_{i\in Q}e[[g_2^{\alpha x_i}\cdot(u'\prod_{k\in\Omega}u_k)^{r_u}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}}]^{L_i}, g]\}\\&\quad\cdot\{\prod_{i\in Q}e[u'\prod_{k\in\Omega}u_k, (g^{r_u})^{L_i}]\}^{-1}\cdot\{\prod_{i\in Q}e[m'\prod_{j\in\Gamma}m_j, (g^{r_{mi}})^{L_i}]\}^{-1}\\&=\prod_{i\in Q}e\{[g_2^{\alpha x_i}\cdot(u'\prod_{k\in\Omega}u_k)^{r_{ui}}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}}]^{L_i}, g\}\\&\quad\cdot\prod_{i\in Q}e[(u'\cdot\prod_{k\in\Omega}u_k)^{r_{ui}L_i}, g]^{-1}\cdot\prod_{i\in Q}e[(m'\prod_{j\in\Gamma}m_j)^{r_{mi}L_i}, g]^{-1}\\&=\prod_{i\in Q}e\{g_2^{\alpha x_i L_i}, g\}=e(g_2^{\alpha}, g)^{\sum_{i\in Q}L_i x_i}=e(g_2^{\alpha}, g)^{x}\end{aligned}$$

$Qx=\prod_{i\in Q}a_{i,0}=\prod_{i\in Q}f_i(0)$

$\therefore$ 上式 $e(g_2^{\alpha}, g)^{x}=e(g_2, g^{\alpha})^{\sum_{i\in Q}f_i(0)}=\prod_{i\in Q}A_{i,0}=S$

显然, 如果仅有 $k(k<t)$ 个参与者合谋生成门限签名, 那么 $x=\sum_{i\in Q}L_i x_i$ 必然不能成立[6], 其最终签名也无法通过验证公式.

4 安全性分析

1. 签名密钥和验证密钥产生阶段中, 对参与者 $p_1, p_2, \cdots, p_n$ 的验证是公开有效的, 可以排除居心不良的假冒者. 任意 $t+1$ 个诚实参与者可以重构秘密值.

2. 攻击者由 C_i 和S 的值不能得到参与者秘密分享(私钥)x_i 或系统秘密值x, 因为要解离散对数难题.

3. 攻击者不能试图由个体签名 σ_i 或门限签名 σ 来推导秘密参数 α, 这是因为:

(1)在由 k 个不同签名者对同一消息 m 的个体签名过程中, σ_i 含 α 的分量为 $V_i=g_2^{\alpha\cdot x_i}\cdot(u'\prod_{k\in\Omega}u_k)^{r_{ui}}\cdot(m'$

$\prod_{j\in\Gamma} m_j)^{r_{mi}}$. 设 g_2, u', $U=\{u_i\}$, m', $M=\{m_i\}$ 都已知, 集合 Γ 不变化且公开, 另有集合 Ω 对攻击者也已知, x_i, r_{ui}, r_{mi} 都未知, 则这 k 个 V_i 及其值形成一个关于 α 和另外 $3k$ 个未知数的方程组, 攻击者不能得出方程组的正确解.

(2) 在各参与者对 k 个不同消息的 k 轮门限签名过程中, 我们取极端的例子, 假设攻击者在某 k 轮门限签名中共获得 k 个来自同一签名者的个体签名. 仍设 Γ 和 Ω 已知, 然而在对不同消息的签名过程中, r_{ui} 和 r_{mi} 每次都不相同, 方程组中将有至少 $2k$ 个未知数. 另外 α 和 x_i 在 g_2 的指数中是不可区分的, 故无法解出 α 值.

(3) 类似地, 由定理 2 的证明过程可知, 从已知的门限签名 σ 出发, 求解 α 将归结为离散对数难题和 α、x 的不可区分性上.

4. 攻击者不能试图伪造参与者 p_i 的个体签名 σ_i. 假设一个攻击者随机选择 α', x_i', r_{ui}', $r_{mi}' \in Z_p$ 来伪造 p_i 的签名 $\sigma_i' = [g^{\alpha'\cdot x_i'}\cdot(u'\prod_{k\in\Omega}u_k)^{r_{ui}'}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}'}, g^{r_{ui}'}, g^{r_{mi}'}, i]$. 而定理 1 中验证公式右边的值为: $e(g_2, g)^{\alpha\cdot x_i}$, 显然难以通过验证. 可见, 在未知秘密参数 α 和秘密分享 x_i 的情况下, 成功伪造有效个体签名在计算上是不可行的.

5. 攻击者不能试图伪造一个满足该式的门限签名 σ, 因为:

(1) 假设一个伪造者随机选择了 α', x'_1, r'_{u1}, r'_{m1}, x_2', r'_{u2}, r'_{m2}, …, x'_n, r'_{un}, r'_{mn}, x'_n, r'_{un}, $r'_{mn} \in Z_p$ 来伪造门限签名 $\sigma' = (V', R_u', R_m') = \{\prod_{i\in Q}[g_2^{\alpha'\cdot x_i'}\cdot(u'\prod_{k\in\Omega}u_k)^{r_{ui}'}\cdot(m'\prod_{j\in\Gamma}m_j)^{r_{mi}'}]^{L_i}, (g^{r_{ui}'})^{L_i}, (g^{r_{mi}'})^{L_i}\}, (i=1, 2, \ldots, n)$. 则定理 2 中验证公式左边结果为 $\prod_{i\in Q}e(g_2^{\alpha'\cdot x_i'\cdot L_i}, g) = e(g_2, g)^{\sum_{i\in Q}\alpha'\cdot x_i'\cdot L_i}$, 显然无法使验证公式成立.

(2) 如果攻击者随机选择了 R_u' 和 R_m'. 由定理 2 的证明过程可知, 他可以省去对 r_{ui} 和 r_{mi} 的考虑. 但是为了求出满足验证公式的 V' 值, α 和 x_i 仍是必需的. 根据 2 和 3 的分析我们知道, 适合 R_u' 和 R_m' 的 V' 是无法求出的. 另外, 即使攻击者知道秘密 x 和所有参与者的秘密分享 x_1, x_2, …, x_n 并随机选择了一个 V' 值, 那么他试图确定一个合适 α' 的使得等式成立, 仍至少是离散对数问题和双线性映射求逆问题. 因此门限签名是安全的.

5 结论

本文利用 Gennaro 基于离散对数难题的分布式密钥产生协议和 Paterson 无需随机预言的数字签名方案, 构造了一种新的门限签名方案, 即基于身份的无需随机预言 (t, n) 的门限签名方案. 和 Boneh[7] 的基于 $q-$ SDH 假设的签名方案相比, 本方案是基于安全性更高的 CDH 假设; 且最终签名阶段仅包含了 3 个群元素, 约是前者的一半, 在门限签名生成阶段无需配对运算, 签名验证阶段仅需 3 次配对运算, 使得运算效率得到改善.

每个参与者被隐式的分配一个不同的秘密分享(私钥向量的分量), 他能方便的产生个体签名. 验证者可以通过验证公式验证个体签名和门限签名的合法性. 该方案在离散对数难题假设下, 能防止攻击者从个体签名和门限签名中得到秘密参数 α 和共享秘密 x. 假冒参与者不能产生有效的个体签名, 因此无法参与到门限签名的生成过程. 伪造者在非法获知所有 $(t=n)$ 参与者秘密分享的情况下仍不能伪造门限签名, 比起其他基于身份的门限签名方案, 本方案具有更强的抗伪造性.

参考文献:

[1] Shamir. Identity-based Cryptosystems and signature schemes [A]. Proc. of CRYPTO ‘84, LNCS 196[C]. Springer-Verlag, 1984. 47– 53.

[2] D Boneh, M Franklin. Identity-based encryption from the weil pairing[A]. Proc. of CRYPTO 2001, LNCS 2139[C]. Springer-Verlag, 2001. 213– 229.

[3] J Cha, J Cheon. An Identity-based signature from gap diffid-hellman groups[A]. Proc. of PKC 2003, LNCS 2567[C]. Springer-Verlag, 2003. 18– 30.

[4] F Hess. Efficient identity based signature schemes based on pairings[A]. Proc. of SAC 2002, LNCS 2595[C]. Springer-Verlag, 2002. 310– 324.

[5] Kenneth G Paterson, Jacob C N Schuldt. Efficient identity-based signatures secure in the standard model [A]. ACISP 2006, LNCS 4058[C]. Springer-Verlag Berlin Heidelberg 2006, 2006. 207– 222.

[6] R Gennaro, S Jarecki, H Krawczyk, T Rabin. Secure distributed key generation for discrete-log based cryptosystems[A]. EUROCRYPT 1999, LNCS 1592[C]. Berlin: Springer-Verlag, 1999. 295– 310.

[7] D Boneh, X Boyen. Short signatures without random oracles [A]. EUROCRYPT‘2004, LNCS 3027[C]. Springer-Verlag, 2004. 56– 73.

作者简介:

蔡永泉　男, 1956 年出生, 教授、博导, 主要从事计算机网络协议开发、网络安全及其算法的研究. E-mail: cyq@bjut.edu.cn

张可　男, 1984 年出生, 在读研究生, 感兴趣的领域: 通信网络、数字签名.