Journal of Computer Applications
计算机应用,2013,33(1):15-18
ISSN 1001-9081
CODEN JYIIDU
2013-01-01
http://www.joca.cn

文章编号:1001-9081(2013)01-0015-04
doi:10.3724/SP.J.1087.2013.00015

# 标准模型下高效的门限签名方案

石贤芝,林昌露*,张胜元,唐 飞
(福建师范大学 网络安全与密码技术福建省高校重点实验室,福州 350007)
(*通信作者电子邮箱 cllin@fjnu.edu.cn)

**摘 要**:为了提高门限签名方案的计算效率,结合 Gennaro 等(GENNARO R, JAREAKI S, KRAWCZYK H, *et al*. Secure distributed key generation for discrete-log based cryptosystem. Journal of Cryptology, 2007, 20(1): 51-83)的分布式密钥生成协议和谷科等(谷科,贾维嘉,姜春林. 高效安全的基于身份的签名方案. 软件学报,2011,22(6):1350-1360)的签名方案,在标准模型下利用双线性对技术构造了一个新的门限签名方案。所提方案没有可信的密钥份额分发中心,每个参与者都可以验证一些必要信息,从而避免了恶意私钥生成中心攻击和公钥份额代换攻击。通过与现有类似的两个门限签名方案对比表明,所提方案减少了双线性对运算,提高了计算效率。

**关键词**:门限签名;标准模型;无可信中心;基于身份签名
**中图分类号**:TP309.7 **文献标志码**:A

## Efficient threshold signature scheme in standard model

SHI Xianzhi, LIN Changlu*, ZHANG Shengyuan, TANG Fei
(*Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou Fujian* 350007, *China*)

**Abstract:** To improve the computational efficiency in the threshold signature scheme, the authors proposed a new threshold signature scheme based on bilinear pairing via combining Gennaro's (GENNARO R, JAREAKI S, KRAWCZYK H, *et al*. Secure distributed key generation for discrete-log based cryptosystem. Journal of Cryptology, 2007, 20(1): 51-83) distributed secret key generation solution and Gu's (GU K, JIA W J, JIANG C L. Efficient and secure identity-based signature scheme. Journal of Software, 2011, 22(6): 1350-1360) signature scheme in the standard model. There was no trusted dealer for secret key share distribution and each party could verify the validity of some important information, which guaranteed the proposed scheme can avoid the malicious private key generator attack and public key share replacing attack. The comparison results with two previous threshold signature schemes show that the proposed scheme needs less pairing computation and raises the computational efficiency.

**Key words:** threshold signature; standard model; non-trusted dealer; Identity-based Signature (IDS)

## 0 引言

门限签名[1]由于在现代社会中有很多应用而得到了人们普遍的研究;鉴于基于身份密码系统[2]所具有的优势,人们又提出了基于身份门限签名[3]的概念,基于身份的门限签名得到了广泛的关注[4-6]。随着标准模型下密码方案[7-8]的兴起,一些学者又开始研究标准模型下的门限签名,比如文献[9-10]。

文献[9-10]中的方案基于 Paterson 等[8]的方案;然而 Paterson 等的方案计算效率并不高,在生成私钥和签名时,所需要的群元素乘法运算太多,所以文献[9-10]中的门限签名方案计算效率也不会高。2011 年,谷科等[11]改进了 Paterson 等的方案,设计了一个高效、安全的基于身份的签名方案。与 Paterson 等的方案相比,计算效率有较大提高。

门限密码方案主要适用于各个参与者互不信任的场景,且在文献[3,10]中的一些门限签名方案大都是基于一个可信的密钥份额分发中心。然而,一方面参与者谁都不信任,一方面却又要求有一个可信中心的存在,这在一定程度上是矛盾的。研究高效的无可信中心门限密码方案具有一定的现实意义。

在谷科等[11]方案的基础上,本文提出一个无可信中心的门限签名方案,与文献[9-10]中的方案相比,计算效率有了较大的提高,特别是减少了双线性对运算的次数。本文还证明了所设计方案在标准模型下满足不可伪造性和健壮性。

## 1 预备知识

### 1.1 双线性映射

**定义 1** 设 $G,G_1$ 是两个循环群,$|G|=|G_1|=p$,$p$ 为素数,$g$ 是 $G$ 的生成元;双线性映射 $e:G\times G\rightarrow G_1$ 有如下 3 条性质。

1) 双线性性。对于任意的 $a,b\in \mathbf{Z}_p^*$,都有 $e(g^a,g^b)=e(g,g)^{ab}$。

2) 非退化性。即 $e(g,g)\neq 1$。

3) 可计算性。对于任意 $a,b\in \mathbf{Z}_p^*$,$e(g^a,g^b)$ 可有效计算。

### 1.2 计算 Diffie-Hellman 问题

**定义 2** $g$ 是群 $G$ 的生成元,$|G|=p$,$p$ 为素数,对于任意

**收稿日期**:2012-08-27。 **基金项目**:国家自然科学基金资助项目(61103247, 61102093);福建省自然科学基金资助项目(2011J05147);福建师范大学青年骨干教师资助项目(fjsdjk2012049)。

**作者简介**:石贤芝(1988-),男,山东菏泽人,硕士研究生,主要研究方向:密码学; 林昌露(1978-),男,福建三明人,博士,主要研究方向:密码学; 张胜元(1966-),男,福建龙岩人,教授,博士,主要研究方向:编码理论与密码学、组合数学; 唐飞(1986-),男,重庆垫江人,博士研究生,主要研究方向:密码学。

$a,b \in \mathbf{Z}_p^*$，已知 $g^a,g^b$，求 $g^{ab}$。

### 1.3 形式化定义与安全模型

**定义 3** IDTS-NTD 方案。一般地，一个无可信中心下基于身份的门限签名（Identity-based Threshold Signature with Non-Trusted Dealer, IDTS-NTD）方案由 5 个算法组成。

1）系统初始化。输入安全参数 $k$，生成系统公共参数 $params$。

2）生成门限密钥。$n$ 个签名参与者（以下简称参与者）通过合作生成各自的基于身份 $u$ 的私钥份额 $d_{u,i}$ 和能通过验证的公钥份额 $v_i(1 \leqslant i \leqslant n)$。

3）生成部分签名。每个参与者 $P_i(1 \leqslant i \leqslant n)$ 利用 $d_{u,i}$ 计算并公开消息 $m$ 的部分签名 $\sigma_i$。

4）合成整体签名。选择通过验证的任意 $t$ 个部分签名 $\sigma_i$，合成得到整体签名 $\sigma$。

5）验证整体签名。若 $\sigma$ 通过验证，输出 1；否则输出 0。

为了下面证明的需要，先来定义基于身份的签名（Identity-based Signature, IDS）方案的不可伪造性。

**定义 4** IDS 方案的不可伪造性。敌手 $A^{IDS}$ 是概率图灵机。考虑 $A^{IDS}$ 和挑战者 $C^{IDS}$ 之间的游戏 $G^{IDS}$。

阶段 1 $C^{IDS}$ 运行系统初始化算法，得到系统公共参数 $params$ 并发送给 $A^{IDS}$。

阶段 2 $A^{IDS}$ 询问身份 $u$ 的私钥。$C^{IDS}$ 运行 IDS 方案中的私钥提取算法，得到 $u$ 的私钥 $d_u$ 并发送给 $A^{IDS}$。$A^{IDS}$ 还询问包含 $(u,m)$ 的签名，这时 $C^{IDS}$ 首先运行私钥提取算法得到一个相关的私钥，然后利用这个私钥运行签名算法得到签名 $\sigma$，并把 $\sigma$ 发送给 $A^{IDS}$。

阶段 3 $A^{IDS}$ 输出有效的伪造签名 $(u^*,\tilde{m},\tilde{\sigma})$。这里要求在阶段 2 中 $A^{IDS}$ 不能询问目标身份 $u^*$ 的私钥，也不能询问包含 $(u^*,\tilde{m})$ 的签名。

定义 $A^{IDS}$ 成功的概率为：

$$Succ_{A^{IDS}}^{EUF\text{-}IDS}(k) = \Pr[Verify(params,u^*,\tilde{m},\tilde{\sigma}) = 1]$$

其中 $Verify(params,u^*,\tilde{m},\tilde{\sigma}) = 1$ 表示验证算法输出 1，下同。所有 $A^{IDS}$ 得到的 $Succ_{A^{IDS}}^{EUF\text{-}IDS}(k)$ 中的最大值记为 $Succ_{A^{IDS}}^{EUF\text{-}IDS}(t,q_e,q_s)$，其中每一个 $A^{IDS}$ 在 $t$ 的时间内，进行了至多 $q_e$ 次私钥询问，至多 $q_s$ 次签名询问。如果 $Succ_{A^{IDS}}^{EUF\text{-}IDS}(t,q_e,q_s)$ 是可以忽略的，就称 IDS 方案是可适应性选择身份攻击和选择消息攻击存在性不可伪造安全的，记为 $(t,q_e,q_s)$-EUF-IDS-CMA 安全的。

**定义 5** IDTS-NTD 方案的不可伪造性。敌手 $A^{IDTS}$ 是概率图灵机，考虑 $A^{IDTS}$ 和挑战者 $C^{IDTS}$ 之间的游戏 $G^{IDTS}$。

阶段 1 $C^{IDTS}$ 运行系统初始化算法，得到公共参数 $params$ 并发送给 $A^{IDTS}$。

阶段 2 $A^{IDTS}$ 腐蚀 $t-1$ 个参与者，不妨记为 $P_i(1 \leqslant i \leqslant t-1)$；游戏开始时，敌手就选择腐蚀哪些参与者，一旦选定，不能更改。

阶段 3 $A^{IDTS}$ 询问包含身份 $u$ 的私钥，$C^{IDTS}$ 运行基本签名方案中的私钥提取算法，得到私钥 $d_u$ 并发送给 $A^{IDTS}$。$A^{IDTS}$ 还询问包含 $(u,m)$ 的签名，这时 $C^{IDTS}$ 首先运行基本签名方案中的私钥提取算法得到一个相关的私钥，然后利用这个私钥运行签名算法得到签名 $\sigma$，并把 $\sigma$ 发送给 $A^{IDTS}$。

阶段 4 $A^{IDTS}$ 递交目标身份 $u^*$。$A^{IDTS}$ 代表被腐蚀 $P_i(1 \leqslant i \leqslant t-1)$，$C^{IDTS}$ 代表诚实 $P_i(t \leqslant i \leqslant n)$，合作运行生成门限密钥算法，得到各个参与者基于身份 $u^*$ 的私钥份额 $d_{u^*,i}$ 和公钥份额 $v_i^*$。

阶段 5 $A^{IDTS}$ 询问包含 $(u^*,m)$ 的签名。以 $m$ 和 $d_{u^*,i}(t \leqslant i \leqslant n)$ 作为输入，$C^{IDTS}$ 运行生成部分签名算法和合成整体签名算法，得到基于身份 $u^*$ 的消息 $m$ 的签名 $\sigma$，并发送给 $A^{IDTS}$。注意，$A^{IDTS}$ 还可以询问部分签名 $\sigma_i(t \leqslant i \leqslant n)$。

阶段 6 $A^{IDTS}$ 输出有效的伪造签名 $(u^*,\tilde{m},\tilde{\sigma})$。这里要求 $A^{IDTS}$ 不能询问基于身份 $u^*$ 的私钥 $d_{u^*}$，也不能询问包含 $(u^*,\tilde{m})$ 的签名。

定义 $A^{IDTS}$ 成功的概率为：

$$Succ_{A^{IDTS}}^{EUF\text{-}IDTS}(k) = \Pr[Verify(params,u^*,\tilde{m},\tilde{\sigma}) = 1]$$

把所有 $A^{IDTS}$ 得到的 $Succ_{A^{IDTS}}^{EUF\text{-}IDTS}(k)$ 中的最大值记为 $Succ_{A^{IDTS}}^{EUF\text{-}IDTS}(t,q_e,q_s)$，其中每一个 $A^{IDTS}$ 在 $t$ 的时间内，询问了至多 $q_e$ 次私钥，询问至多 $q_s$ 次签名。如果 $Succ_{A^{IDTS}}^{EUF\text{-}IDTS}(t,q_e,q_s)$ 可忽略，则就称 IDTS-NTD 方案是可适应性选择身份攻击和选择消息攻击存在性不可伪造安全的，记为 $(t,q_e,q_s)$-EUF-IDTS-CMA 安全的。

**定义 6** IDTS-NTD 方案的健壮性。在 IDTS-NTD 方案中，若在敌手最多可腐蚀 $t-1$ 个参与者的情况下，算法仍能产生正确的输出和有效的签名，则就称 IDTS-NTD 方案是健壮的。

## 2 IDTS-NTD 方案的构造

本文方案中，所有的参与者都可以验证公钥份额的有效性，生成部分签名时所需要的乘法运算较少，验证签名只需要一次双线性对运算。该方案由 5 个算法构成，如下。

1）系统初始化。$G,G_1$ 是两个大素数 $p$ 阶的循环群，$g$ 和 $h$ 是 $G$ 的两个生成元，$\log_g h$ 未知，$g_2 \leftarrow_R G$（$G$ 中随机选取 $g_2$），$u' \leftarrow_R G,m' \leftarrow_R G,n_u$ 维向量 $\boldsymbol{U} = (u_k)_{n_u}$，$\boldsymbol{M} = (m_k)_{n_m}$，$u_k \leftarrow_R G,m_k \leftarrow_R G,n_u,n_m$ 是正整数。双线性映射 $e:G \times G \rightarrow G_1$。系统公共参数为 $params = (G,G_1,e,g,h,g_2,u',m',\boldsymbol{U},\boldsymbol{M})$。

2）生成门限密钥。设 $u$ 表示一个身份的 $n_u$ 长比特串，$u[k]$ 为 $u$ 的第 $k$ 个比特位，集合 $U' \subset \{1,\cdots,n_u\}$ 为满足 $u[k]=1$ 的所有指标 $k$ 的集合。

①$P_i$ 生成自己的秘密值份额 $(\alpha_i,\gamma_i)$。

a）每个 $P_i$ 随机选择 $\mathbf{Z}_p$ 上的两个 $t-1$ 次多项式：

$$f_i(x) = a_{i0} + a_{i1}x + a_{i2}x^2 + \cdots + a_{i(t-1)}x^{t-1}$$

$$f'_i(x) = b_{i0} + b_{i1}x + b_{i2}x^2 + \cdots + b_{i(t-1)}x^{t-1}$$

$P_i$ 广播 $C_{ik} = g^{a_{ik}}h^{b_{ik}},0 \leqslant k \leqslant t-1$。记 $z_i = a_{i0},z'_i = b_{i0}$，$P_i$ 计算共享值 $s_{ij} = f_i(j),s'_{ij} = f'_i(j),1 \leqslant j \leqslant n$，然后把共享值 $(s_{ij},s'_{ij})$ 通过安全信道发给参与者 $P_j$。

b）$P_j(j \neq i)$ 通过判定

$$g^{s_{ij}}h^{s'_{ij}} = \prod_{k=0}^{t-1}(C_{ik})^{j^k};\quad 1 \leqslant i \leqslant n \tag{1}$$

是否成立，来验证他收到的 $(s_{ij},s'_{ij})$ 的有效性。若不成立，$P_j$ 对 $P_i$ 进行公开投诉。

c）若对 $P_i$ 的投诉大于 $t-1$ 个，$P_i$ 就是不合格的；当对 $P_i$ 的投诉大于 0 且小于 $t$ 个时，$P_i$ 要公开与式（1）匹配的 $(s_{ij},s'_{ij})$，若公开的 $(s_{ij},s'_{ij})$ 中至少有一个仍不满足式（1），此时 $P_i$ 也是不合格的。所有合格的参与者集合记为 $QUAL$。秘密值 $\alpha = \sum_{i \in QUAL} z_i \pmod p$，$P_i$ 的秘密值份额 $\alpha_i$ 为 $\alpha_i = \sum_{j \in QUAL} s_{ji} \pmod p$；秘密值 $\gamma = \sum_{i \in QUAL} z'_i \pmod p$，$P_i$ 的秘密值份额 $\gamma_i$ 为 $\gamma_i = \sum_{j \in QUAL} s'_{ji} \pmod p$。

②$P_i$ 生成自己的私钥份额 $d_{u,i}$。

每个 $p_i$ 计算自己的私钥份额 $d_{u,i} = \left(g_2^{\alpha_i} \cdot (g_2)^{\gamma_i \cdot (u' + \sum_{j \in U'} u_j)},e(g_2,g)^{\gamma_i}\right)$。基于身份 $u$ 的私钥 $d_u$ 为 $d_u =$

$\left(g_2^{\alpha}\cdot(g_2)^{\gamma\cdot(u'+\sum_{j\in U'}u_i)},e(g_2,g)^{\gamma}\right)$。易知 $d_u$ 不能由任何单独一方计算出来。

③$P_i$ 生成自己的公钥份额 $v_i$。

a) 每个 $P_i(1\leqslant i\leqslant n)$ 广播各自的公钥份额 $v_i=e(g_2,g)^{\alpha_i}$。

b) $QUAL$ 中的每个 $P_i$ 广播 $A_{ik}=e(g_2,g)^{a_{ik}},0\leqslant k\leqslant t-1$。对于每个 $i\in QUAL,P_j(1\leqslant j\leqslant n)$ 验证式(2)是否成立:

$$e(g_2,g^{s_{ij}})=\prod_{k=0}^{t-1}(A_{ik})^{j^k} \tag{2}$$

若不成立,$P_j$ 对 $P_i$ 进行公开投诉。当 $P_i$ 收到了投诉之后,除 $P_i$ 之外的其他 $n-1$ 个参与者合作重构出 $P_i$ 的两个多项式,从而广播正确的 $A_{ik},k=0,1,\cdots,t-1$。

c) 验证 $v_i=e(g_2,g)^{\alpha_i}$ 的有效性。每个参与者通过计算式(3)是否成立来验证 $v_i$ 的有效性:

$$e(g_2,g)^{\alpha_i}=\prod_{j\in QUAL}\prod_{k=0}^{t-1}(A_{jk})^{i^k} \tag{3}$$

若不成立,验证者要对 $P_i$ 进行公开投诉,并广播 $P_i$ 有效的公钥份额 $v_i=\prod_{j\in QUAL}\prod_{k=0}^{t-1}(A_{jk})^{i^k}$。公钥为 $v=e(g_2,g)^{\alpha}$。易知每一方都可以通过公开的 $v_i$ 计算出 $v_o$。

3) 生成部分签名。设 $m$ 表示一个消息的 $n_m$ 长比特串,$m[k]$ 表示 $m$ 的第 $k$ 个比特位,集合 $\mathbb{M}'\subset\{1,\cdots,n_m\}$ 为满足 $m[k]=1$ 的所有指标 $k$ 的集合。$P_i$ 随机选择 $r_{m,i}\in\mathbf{Z}_p$,计算并广播消息 $m$ 的部分签名如下:

$$\sigma_i=(\sigma_i[1],\sigma_i[2],\sigma_i[3])=\left(g_2^{\alpha_i}\cdot(g_2)^{\gamma_i\cdot(u'+\sum_{j\in U'}u_i)},(g_2)^{r_{m,i}\cdot(m'+\sum_{j\in\mathbb{M}'}m_i)},e(g_2,g)^{r_{m,i}},e(g_2,g)^{\gamma_i}\right)$$

4) 合成整体签名。对于每个 $\sigma_i$,签名合成者检验式(4)是否成立:

$$e(\sigma_i[1],g)=v_i\cdot(\sigma_i[2])^{m'+\sum_{j\in\mathbb{M}'}m_i}\cdot(\sigma_i[3])^{u'+\sum_{j\in U'}u_i} \tag{4}$$

若成立,$\sigma_i$ 就是有效的;否则 $\sigma_i$ 是无效的。合成者选出通过式(4)验证的任意 $t$ 个部分签名,记 $\mathbb{R}=\{i\mid\sigma_i$ 通过验证$\}$,$|\mathbb{R}|=t$,则关于消息 $m$ 的整体签名如下:

$$\sigma=(\sigma[1],\sigma[2],\sigma[3])$$

其中:$\sigma[1]=\prod_{i\in\mathbb{R}}(\sigma_i[1])^{\lambda_i}$,$\sigma[2]=\prod_{i\in\mathbb{R}}(\sigma_i[2])^{\lambda_i}$,$\sigma[3]=\prod_{i\in\mathbb{R}}(\sigma_i[3])^{\lambda_i}$;$\lambda_i=\prod_{j\in\mathbb{R},j\neq i}\frac{-j}{i-j}$ 为 Lagrange 插值系数。

5) 验证整体签名。签名验证者计算式(5)是否成立:

$$e(\sigma[1],g)=v\cdot(\sigma[2])^{m'+\sum_{j\in\mathbb{M}'}m_i}\cdot(\sigma[3])^{u'+\sum_{j\in U'}u_i} \tag{5}$$

若成立,$\sigma$ 有效,输出 1;否则输出 0。

## 3　方案分析

### 3.1　方案的正确性分析

**定理 1**　正确的公钥份额 $v_i$ 能通过式(3)的验证。

证明　事实上,

$$e(g_2,g)^{\alpha_i}=e(g_2,g)^{\sum_{j\in QUAL}s_{ji}}=\prod_{j\in QUAL}e(g_2,g)^{s_{ji}}=\prod_{j\in QUAL}e(g_2,g)^{f_j(i)}=\prod_{j\in QUAL}e(g_2,g)^{\sum_{k=0}^{t-1}a_{jk}\cdot i^k}=\prod_{j\in QUAL}\prod_{k=0}^{t-1}(e(g_2,g)^{a_{jk}})^{i^k}=\prod_{j\in QUAL}\prod_{k=0}^{t-1}(A_{jk})^{i^k}$$

**定理 2**　正确的部分签名 $\sigma_i$ 能通过式(4)的验证。

证明　事实上,

$$e(\sigma_i[1],g)=e\left(g_2^{\alpha_i}\cdot(g_2)^{\gamma_i\cdot(u'+\sum_{j\in U'}u_i)}\cdot(g_2)^{r_{m,i}\cdot(m'+\sum_{j\in\mathbb{M}'}m_i)},g\right)=e(g_2^{\alpha_i},g)\cdot e\left((g_2)^{\gamma_i\cdot(u'+\sum_{j\in U'}u_i)},g\right)\cdot e\left((g_2)^{r_{m,i}\cdot(m'+\sum_{j\in\mathbb{M}'}m_i)},g\right)=e(g_2,g)^{\alpha_i}\cdot e(g_2,g)^{r_{m,i}\cdot(m'+\sum_{j\in\mathbb{M}'}m_i)}\cdot e(g_2,g)^{\gamma_i\cdot(u'+\sum_{j\in U'}u_i)}=v_i\cdot(\sigma_i[2])^{m'+\sum_{j\in\mathbb{M}'}m_i}\cdot(\sigma_i[3])^{u'+\sum_{j\in U'}u_i}$$

类似地,可以证明,正确的 $\sigma$ 也可以通过式(5)的验证。

### 3.2　方案的安全性分析

**定理 3**　健壮性。在有至多 $t-1(n\geqslant 2t-1)$ 个被腐蚀参与者的情况下,本文中的 IDTS-NTD 方案是健壮的。

证明　一个被敌手腐蚀参与者的表现形式有两种:一是终止正常行为,什么也不做;二是广播错误的信息。

首先,证明生成门限密钥算法的健壮性。在生成私钥份额时,参考了 Gennaro 等[12] 的分布式秘密生成协议,里面对这部分的健壮性已经证明。在生成公钥份额时,若被腐蚀参与者 $P_i(1\leqslant i\leqslant t-1)$ 什么也不做,其他诚实的签名参与者 $P_j(t\leqslant j\leqslant n,n\geqslant 2t-1)$ 由于拥有 $s_{ij}$,就能通过合作重构出 $P_i$ 的两个多项式,从而计算出正确的公钥份额 $v_i=e(g_2,g)^{\alpha_i}$。若 $P_i$ 广播错误的 $A_{ik},A_{ik}$ 不能通过式(2)的验证,$P_j$ 通过合作重构出正确的 $A_{ik}$。若 $P_i$ 广播错误的 $v_i=e(g_2,g)^{\alpha_i},v_i$ 不能通过式(3)的验证,$P_j$ 照样通过合作得到 $v_i=\prod_{j\in QUAL}\prod_{k=0}^{t-1}(A_{jk})^{i^k}$。所以,无论被腐蚀参与者表现形式如何,生成门限密钥算法都能产生正确的输出结果。

其次,证明生成部分签名算法的健壮性。若被腐蚀 $P_i$ 不公开部分签名,由于诚实参与者的人数为 $n-(t-1)\geqslant 2t-1-t+1=t$,所以签名合成者可以得到不少于 $t$ 个有效的部分签名,从而合成有效的整体签名。若 $P_i$ 公开错误的部分签名,由定理 2 知,这种部分签名是无效的,在合成整体签名时就不会用到,从而合成者也可以得到有效的整体签名。

对于其他的两个算法,被腐蚀参与者无需参与,故健壮性无需证明。

下面证明 IDTS-NTD 方案的不可伪造性。定理 5 是主要结果,由定理 4 和引理 1 可直接得到。

**定理 4**　若文献[11]中的 IDS 方案是 $(t_1,q_e,q_s)$-EUF-IDS-CMA 安全的,则 IDTS-NTD 方案是 $(t_2,q_e,q_s)$-EUF-IDTS-CMA 安全的。

证明　通过定义 4 和定义 5 中的游戏 $G^{\mathrm{IDS}}$ 与 $G^{\mathrm{IDTS}}$ 证明:若 $A^{\mathrm{IDTS}}$ 能攻击 IDTS-NTD 方案的不可伪造性,则 $A^{\mathrm{IDS}}$ 就能攻击 IDS 方案的不可伪造性。

阶段 1　$A^{\mathrm{IDTS}}$ 从 $C^{\mathrm{IDTS}}$ 处得到公共参数 $params=(G,G_1,e,g,h,g_2,u',m',\boldsymbol{U},\boldsymbol{M})$,$params$ 也作为游戏 $G^{\mathrm{IDS}}$ 的公共参数。

阶段 2　$A^{\mathrm{IDTS}}$ 腐蚀 $t-1$ 个签名参与者 $P_i(1\leqslant i\leqslant t-1)$。这样,在 $A^{\mathrm{IDTS}}$ 询问目标身份 $u^*$ 的相关信息时,$A^{\mathrm{IDTS}}$ 代表 $P_i(1\leqslant i\leqslant t-1)$ 进行游戏,$C^{\mathrm{IDTS}}$ 代表 $P_i(t\leqslant i\leqslant n)$ 进行游戏。

阶段 3　$A^{\mathrm{IDTS}}$ 询问包含身份 $u$ 的私钥。$A^{\mathrm{IDS}}$ 从 $C^{\mathrm{IDS}}$ 处得到私钥 $d_u$ 并发送给 $A^{\mathrm{IDTS}}$。$A^{\mathrm{IDS}}$ 与 $A^{\mathrm{IDTS}}$ 还可以询问包含 $(u,m)$ 的签名。

阶段 4　$A^{\mathrm{IDTS}}$ 递交目标身份 $u^*$,$A^{\mathrm{IDTS}}$ 代表 $P_i(1\leqslant i\leqslant t-1)$,$C^{\mathrm{IDTS}}$ 代表 $P_i(t\leqslant i\leqslant n)$,二者合作运行生成门限密钥算

法,得到参与者各自的基于身份 $u^*$ 的私钥份额 $d_{u^*,i}$ 和公钥份额 $v_i^*$。具体如下,对于 $P_i(1 \leqslant i \leqslant t-1)$,$A^{\text{IDTS}}$ 随机选取多项式 $f_i(x)$ 和 $f'_i(x)$,计算 $s_{ij} = f_i(j)$,$s'_{ij} = f'_i(j)$,$C_{ik} = g^{a_{ik}}h^{b_{ik}}$,$0 \leqslant k \leqslant t-1$;把 $s_{ij}$,$s'_{ij}(t \leqslant j \leqslant n)$ 秘密地发送给 $C^{\text{IDTS}}$,$C_{ik}$ 公开。对于 $P_i(t \leqslant i \leqslant n)$,$C^{\text{IDTS}}$ 也随机选取多项式 $f_i(x)$ 和 $f'_i(x)$,计算 $s_{ij} = f_i(j)$,$s'_{ij} = f'_i(j)$,$C_{ik} = g^{a_{ik}}h^{b_{ik}}$,$0 \leqslant k \leqslant t-1$;$s_{ij}$,$s'_{ij}(1 \leqslant j \leqslant t-1)$ 秘密地发送给 $A^{\text{IDTS}}$,$C_{ik}$ 公开。$A^{\text{IDTS}}$ 和 $C^{\text{IDTS}}$ 通过公开的 $C_{ik}$ 来验证各自收到的 $s_{ij}$,$s'_{ij}$,从而确定出诚实参与者集合 $QUAL$。这样,$A^{\text{IDTS}}$ 得到秘密值份额 $(\alpha_i, r_i)(1 \leqslant i \leqslant t-1)$;$C^{\text{IDTS}}$ 也得到秘密值份额 $(\alpha_i, r_i)(t \leqslant i \leqslant n)$,从而得到参与者各自的私钥份额 $d_{u^*,i}$ 和公钥份额 $v_i^*$。显然,此时,$C^{\text{IDTS}}$ 掌握了所有的 $s_{ij}$,$s'_{ij}(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)$,故 $C^{\text{IDTS}}$ 可以得到秘密值 $(\alpha, r)$;而 $A^{\text{IDTS}}$ 只掌握了一部分的 $s_{ij}$,$s'_{ij}$,不能得到 $(\alpha, r)$。所以 $C^{\text{IDTS}}$ 可以得到整体私钥 $d_{u^*} = \left(g_2^{\alpha} \cdot (g_2)^{r\cdot(u'+\sum_{j\in\mathcal{U}} u_j)}, e(g_2,g)^r\right)$,而 $A^{\text{IDTS}}$ 不能得到 $d_{u^*}$。

阶段 5 $A^{\text{IDS}}$ 和 $A^{\text{IDTS}}$ 询问包含 $(u^*, m)$ 的签名。由于 $C^{\text{IDTS}}$ 掌握了私钥 $d_{u^*}$ 和密钥份额 $d_{u^*,i}(t \leqslant i \leqslant n)$,$C^{\text{IDTS}}$ 有签名的能力,所以 $A^{\text{IDTS}}$ 可以从 $C^{\text{IDTS}}$ 处得到包含 $(u^*, m)$ 的签名 $\sigma$ 以及部分签名 $\sigma_i(t \leqslant i \leqslant n)$,然后 $A^{\text{IDTS}}$ 把 $\sigma$ 发送给 $A^{\text{IDS}}$。

阶段 6 $A^{\text{IDTS}}$ 输出伪造签名 $(u^*, \tilde{m}, \tilde{\sigma})$,其中 $\tilde{\sigma}$ 是基于身份 $u^*$ 消息 $\tilde{m}$ 的有效签名。$A^{\text{IDS}}$ 也把 $(u^*, \tilde{m}, \tilde{\sigma})$ 作为输出的伪造签名。

也就是说,若 $A^{\text{IDTS}}$ 能构造出满足定义 5 中的 $(u^*, \tilde{m}, \tilde{\sigma})$,则 $A^{\text{IDS}}$ 就能构造出满足定义 4 中的 $(u^*, \tilde{m}, \tilde{\sigma})$。所以有:

$$Succ_{A^{\text{IDTS}}}^{\text{EUF-IDTS}}(t_2, q_e, q_s) < Succ_{A^{\text{IDS}}}^{\text{EUF-IDS}}(t_1, q_e, q_s)$$

反之,若文献[11]中的 IDS 方案是 $(t_1, q_e, q_s)$-EUF-IDS-CMA 安全的,则本文的 IDTS-NTD 方案就是 $(t_2, q_e, q_s)$-EUF-IDTS-CMA 安全的。

**引理 1**[11] 如果计算 Diffie-Hellman(Computational Diffie-Hellman, CDH)问题是 $(t', \varepsilon')$ 困难的,那么 IDS 方案是标准模型下可适应性选择身份攻击和选择消息攻击 $(t, q_e, q_s, \varepsilon)$ 不可伪造安全的。其中:

$$\varepsilon' = \frac{\varepsilon}{16(q_e+q_s)q_s(n_u+1)(n_m+1)}$$

$$t' = t + O\left\{(4q_e+5q_s)C_e + (q_e+q_s)C_p + q_s\left(\frac{n_m+1}{2}\right) + q_e\left(\frac{n_u+1}{2}\right)\right\}$$

其中:$C_e$ 表示一次指数运算时间,$C_p$ 表示一次双线性对计算时间。

结合定理 4 和引理 1,就能得到如下定理。

**定理 5** 不可伪造性。标准模型下,若 CDH 问题是困难的,则本文所构造的 IDTS-NTD 方案是可适应性选择身份攻击和选择消息攻击存在性不可伪造安全的。

### 3.3 计算效率比较

文献[9-10]中,分别设计了一个 IDTS(Identity-based Threshold Signature)方案,这两个 IDTS 方案都基于 Paterson 等的签名方案。下面分别以生成和验证一个部分签名所花费的时间作标准,把本文方案和这两个方案在计算效率上作比较,其中省略了可以预计算的参数。具体如表 1 所示。

表 1 中:$C_m$,$C_e$,$C_p$ 分别表示作一次乘法运算、指数运算、双线性对运算所花费的时间;$n_m$ 和 $n_u$ 分别表示一个消息 $m$ 或身份 $u$ 的比特位数,一般为几十或几百比特。从表 1 可以看出,本文方案在计算时间上有明显的降低,特别是双线性对运算只需要一次。

**表 1 3 种方案在计算效率上的比较**

| 方案 | 生成一个部分签名所需时间 | 验证一个部分签名所需时间 |
|---|---|---|
| 文献[9]方案 | $\left(\frac{n_m}{2}+1\right)C_m + 2C_e$ | $\left(\frac{n_m+n_u}{2}+2\right)C_m + 3C_p$ |
| 文献[10]方案 | $\left(\frac{n_m+n_u}{2}+1\right)C_m + 3C_e$ | $\left(\frac{n_m}{2}+1\right)C_m + 2C_p$ |
| 本文方案 | $C_m + 2C_e$ | $2(C_m + C_e) + C_p$ |

## 4 结语

本文提出了一个标准模型下高效的无可信中心门限签名方案,该方案避免了恶意私钥生成中心攻击,同时一些必要的参数也可以正确地得到验证;与其他两个类似的 IDTS 方案相比,本文方案的计算效率有较大提高。

**参考文献:**


[1] DESMEDT Y. Society and group oriented cryptography: a new concept [C]// CRYPTO'87: A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, LNCS 293. Berlin: Springer-Verlag, 1988: 120-127.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 1984 on Advances in Cryptology, LNCS 196. Berlin: Springer-Verlag, 1984: 47-53.

[3] BAEK J, ZHENG Y L. Identity-based threshold signature scheme from the bilinear pairings [C]// Proceedings of the International Conference on Information Technology: Coding and Computing. Washington, DC: IEEE Computer Society, 2004: 124-128.

[4] XU F, LYU X. A new identity-based threshold ring signature scheme [C]// Proceedings of the 2011 IEEE International Conference on Systems, Man and Cybernetics. Piscataway: IEEE Press, 2011: 2646-2651.

[5] LIU J, HUANG S. Identity-based threshold proxy signature scheme from bilinear pairings [J]. Informatica, 2010, 21(1): 41-56.

[6] YANG T, XIONG H, HU J B, *et al.* A traceable certificateless threshold proxy signature scheme from bilinear pairings [C]// APWeb'11: Proceedings of the 13th Asia-Pacific Web Conference on Web Technologies and Applications, LNCS 6612. Berlin: Springer-Verlag, 2011: 376-381.

[7] WATERS B. Efficient identity-based encryption without random oracles [C]// EUROCRYPT'2005: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 3494. Berlin: Springer-Verlag, 2005: 114-127.

[8] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model [C]// ACISP 2006: Proceedings of the 11th Australasian Conference on Information Security and Privacy, LNCS 4058. Berlin: Springer-Verlag, 2006: 207-222.

[9] XIONG H, QIN Z G, LI F G. Identity-based threshold signature in the standard model [J]. International Journal of Network Security, 2010, 10(1): 75-85.

[10] GAO W, WANG G L, WANG X L, *et al.* Efficient identity-based threshold signature scheme from bilinear in the standard model [EB/OL]. [2012-02-19]. http://eprint.iacr.org/2012/073.pdf.

[11] 谷科,贾维嘉,姜春林. 高效安全的基于身份的签名方案[J]. 软件学报,2011,22(6):1350-1360.

[12] GENNARO R, JAREAKI S, KRAWCZYK H, *et al.* Secure distributed key generation for discrete-log based cryptosystem [J]. Journal of Cryptology, 2007, 20(1): 51-83.