基于多项式秘密共享的前摄性门限 RSA 签名方案

徐 甫*
(解放军信息工程大学 郑州 450002)
(北京市信息技术研究所 北京 100094)

摘 要：现有可证明安全的前摄性门限 RSA 签名方案均依赖加性秘密共享方法，存在每次签名均需所有成员参与，易暴露合法成员的秘密份额，签名效率低下等问题。该文以 Shoup 门限签名为基础，提出一种基于多项式秘密共享的前摄性门限 RSA 签名方案，并对其进行了详细的安全性及实用性分析。结果表明，在静态移动攻击者模型中，该方案是不可伪造的和稳健的，与现有同类方案相比，其通信开销更低，运算效率更高。

关键词：门限签名；RSA；多项式秘密共享；前摄性
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2016)09-2280-07
DOI: 10.11999/JEIT151164

Proactive Threshold RSA Signature Scheme Based on Polynomial Secret Sharing

XU Fu
(*PLA Information Engineering University*, *Zhengzhou* 450002, *China*)
(*Information Technology Institute of Beijing City*, *Beijing* 100094, *China*)

Abstract: All the existing provable secure proactive threshold RSA signature schemes rely on additive secret sharing, in which all players have to cooperate to produce a signature, valid players' secret shares may be exposed, and the computing efficiency is too low. Based on Shoup's threshold RSA signature scheme, a proactive threshold RSA signature scheme is proposed by using polynomial secret sharing, and its security and practicability are analyzed. Results show that the proposed scheme is unforgeable and robust under the model of static mobile adversary, and compared with the existing comparable schemes, its communication overhead is lower and computing efficiency is higher.

Key words: Threshold signature; RSA; Polynomial secret sharing; Proactiveness

1 引言

近年来，门限签名方案获得了广泛的研究与应用[1−6]。在(l,k)门限签名方案中，群体的签名私钥(以下简称“私钥”)被所有l个成员通过秘密共享方案共同持有，任意k个以上(含k个)成员可以合作产生给定消息的群签名，而少于k个成员则不能产生合法的群签名。只要攻击者捕获的成员数量小于k，门限签名方案就是安全的。然而，当门限签名系统的生存期较长，攻击者有足够的时间和能力捕获k个以上成员时(称此类攻击者为移动攻击者，mobile adversary)，系统随即会被攻破。为了抵抗移动攻击者，文献[7]率先提出了前摄性(proactive)门限签名方案的概念，将签名系统的生存期划分为多个时间段，在每个时间段的起始阶段，所有l个成员共同对私钥进行重新共享(re-sharing)，即在不改变私钥的情况下，更新各成员所持有的私钥份额。这样，只要时间段划分得恰当，使得移动攻击者在每个时间段内捕获的成员数量小于k，就可以保证门限签名系统的安全。

文献[7]最初提出的前摄性门限签名方案是基于离散对数问题的。在为资源受限型网络提供安全服务时，签名方案的运算效率非常重要，而基于离散对数问题的签名方案在该方面并无优势，其签名的验证速度通常比 RSA 签名方案慢几个数量级[8]。同时，由于 RSA 签名方案广泛应用于各种场合，研究前摄性门限 RSA 签名方案具有较大的现实意义和较高的实用价值。自从前摄性门限签名方案的概念提出以来，已出现多种前摄性门限 RSA 签名方案[8−14]。其中大部分方案采用加性共享方法实现对

收稿日期：2015-10-21；改回日期：2016-06-06；网络出版：2016-07-19
*通信作者：徐甫 xuphou@163.com
基金项目：国家科技重大专项(2012ZX03002003)
Foundation Item: The National Science and Technology Major Project of China (2012ZX03002003)

私钥的共享[8−12]，在对给定的消息实施签名时，需要所有 l 个成员共同参与。当某一成员被攻击者捕获而不能产生正确的部分签名时，由其他成员合作恢复其私钥份额并生成合法的部分签名。然而，此类方案存在明显的不足：(1)签名请求者需要与所有 l 个成员通信，增加了网络的通信负担，降低了签名的效率；(2)当某一成员由于通信信道中断等问题而暂时无法响应签名请求时，其他成员会认为其已被攻击者捕获，进而恢复其私钥份额，造成其私钥份额泄露。文献[8]分析指出，对加性共享方法的依赖是目前前摄性门限 RSA 签名方案存在的主要问题之一。

为了摒弃加性共享方法，使得前摄性门限 RSA 签名方案能够在移动 Ad hoc 网络中得到应用，文献[13]引入了多项式共享方法。此外，文献[14]提出的方案虽涉及加性共享方法，但以多项式共享方法为主。然而，文献[13]的方案后来被证明是不安全的[15]；文献[14]的方案中，每次签名运算时，所有参与签名的 k 个成员需合作产生一个一次性的加性共享份额，增加了网络的通信负担和节点的运算负担。

本文以采用多项式共享方法的 Shoup 门限签名方案[16](不具备前摄性)为基础，将其中的加法、乘法和除法运算转移至整数环中，以便于私钥份额更新协议的设计，进而提出一种简单，高效，且可证明安全的前摄性门限 RSA 签名(Proactive Threshold RSA Signature, PTS-RSA)方案。文章第 2 节简要介绍了背景及相关工作；第 3 节详细描述 PTS-RSA 方案；第 4 节对提出的方案进行安全性和实用性分析；第 5 节为结束语。

2　背景及相关工作

2.1 系统模型

(1)一般门限签名方案：一般门限签名方案(不具备前摄性)由密钥生成、签名和验证 3 个算法组成[2]。

定义 1　适应性选择消息攻击：敌手可以在看到签名方案的公钥之后进行任意次的签名查询，而且可以根据已经观察到的签名选择新的消息进行签名查询。

定义 2　不可伪造性：称 (l,k) 门限签名方案在适应性选择消息攻击下是不可伪造的，如果具备适应性选择消息攻击能力的敌手掌握了签名方案的所有公开参数，控制了 $k-1$ 个成员，且先后进行了 w 次群签名或部分签名查询(设使用的消息分别为 $\mathrm{msg}_1, \mathrm{msg}_2, \cdots, \mathrm{msg}_w$)，最终能够成功伪造一个新消息 $\mathrm{msg}(\mathrm{msg} \notin \{\mathrm{msg}_1, \mathrm{msg}_2, \cdots, \mathrm{msg}_w\})$ 的群签名的概率是可忽略的。

定义 3　稳健性：称 (l,k) 门限签名方案是稳健的，如果敌手最多可以攻破 $k-1$ 个成员，建立算法和签名算法仍然能够成功地运行。

显然，稳健性要求 $l \geq 2k-1$，在本文的剩余部分，假设这一条件始终成立。

定义 4　安全性：如果 (l,k) 门限签名方案满足不可伪造性和稳健性，则称该门限签名方案是安全的。

(2)前摄性门限签名方案：前摄性门限签名方案不仅包括密钥生成、签名和验证 3 个算法，还包括时间段的概念和私钥份额更新协议。前摄性门限签名系统的生存期被划分为多个时间段，在每个时间段的起始阶段，所有成员共同运行私钥份额更新协议，以获得新的私钥份额。前摄性门限签名方案的安全性同样由不可伪造性和稳健性组成。

(3)系统假设：本文假设前摄性门限签名协议在如下通信环境中执行：各成员间时间同步，各成员通过弱同步信道连接，任意两个成员之间具备安全信道，各成员可向所有其他成员发送广播消息。

本文假设前摄性门限签名协议面临静态移动攻击者的攻击：在每个时间段内，攻击者可实施适应性选择消息攻击，最多能够捕获任意不多于 $k-1$ 个成员，且攻击者在签名协议运行之前预先确定每个时间段内将要捕获的成员。

2.2 相关符号及含义

本文基本沿用文献[16]中的符号：

l 为持有私钥份额的成员个数；k 为门限值，至少需要 k 个成员合作，才能生成有效的群签名；n 为RSA模数，$n=pq$，其中，p，q 均为安全素数，即存在大素数 p'，q'，有 $p=2p'+1$，$q=2q'+1$ 成立；$L(n)$ 为 n 的长度(二进制位数)；Q_n 为由 Z_n^* 中所有模 n 二次剩余数组成的集合，即 $Q_n=\{u|u\in Z_n^*, \exists r\in Z_n^*, u=r^2 \bmod n\}$；$m$ 为 $p'q'$，Q_n 的阶。m 需严格保密，因为攻击者一旦掌握了 m，就可以由公开指数 e 直接求出私钥 d；e 为RSA公开指数，文献[16]方案及PTS-RSA方案中，可信中心选择大于 l 的素数作为 e，e 与 n 一起构成公钥；d 为PTS-RSA方案和文献[16]方案中的私钥，$ed\equiv 1 \bmod m$ (注：d 与标准RSA方案中的私钥不同)；S，Ω 为 $\{1,2,\cdots,l\}$ 中任意 k 个元素组成的集合，即 $S\subset\{1,2,\cdots,l\}$，$\Omega\subset\{1,2,\cdots,l\}$，且 $|S|=k$，$|\Omega|=k$。

2.3 离散对数恒等式协议

文献[16]中提出了一个离散对数恒等式协议。其具体细节如下：

设 $\alpha\in Z_m$ 为证明者 P 持有的一个秘密参数，v 为 Q_n 的生成元，$\tilde{v}=v^{\alpha} \bmod n$，且 v 和 $\tilde{v}$ 均为公开

值；协议的证明者 P 和验证者 V 都不知道 Q_n 的阶；$H'(\bullet)$ 是 Hash 函数，其输出为 L_1 比特(L_1 是一个安全参数，一般可取 128)。P 对 Q_n 中的某一元素 $\tilde{x}$ 实施了运算 $\hat{x}=\tilde{x}^{\alpha} \bmod n$ 后，想在不泄漏 α 的情况下向验证者 V 证明其拥有秘密参数 α，同时证明 $\hat{x}$ 的正确性。他们将进行如下协议：

(1)P 随机地选取 $r \in_R [0,2^{L(n)+2L_1}-1]$，计算 $v'=v^r \bmod n$，$x'=\tilde{x}^r \bmod n$，$c=H'(v,\tilde{x},\hat{v},\hat{x},v',x')$ 和 $z=\alpha c+r$。然后，P 公开 (z,c) 作为他拥有秘密参数 α，且 $\hat{x}=\tilde{x}^{\alpha} \bmod n$ 的证据。

(2)利用证据 (z,c)，验证者 V 通过判断 $c=H'(v,\tilde{x},\hat{v},\hat{x},v^z\hat{v}^{-c} \bmod n,\tilde{x}^z\hat{x}^{-c} \bmod n)$ 是否成立来决定是否相信 P 知道秘密参数 α 以及 $\hat{x}=\tilde{x}^{\alpha} \bmod n$ 是否成立。

2.4 整数环上的拉格朗日插值公式

设 $k-1$ 次多项式 $f(X)=\sum_{i=0}^{k-1}a_iX^i \in Z[X]$，令 ∂ 为 $\{0,1,\cdots,l\}$ 中任意 k 个整数组成的集合，即 $\partial \subset \{0,1,\cdots,l\}$，且 $|\partial|=k$。那么，如果已知 $\{f(i)|i\in\partial\}$，则在有理数域上，可通过拉格朗日插值法重构 $f(X)$：

$$f(X)=\sum_{j\in\partial} f(j)\prod_{j'\in\partial\backslash\{j\}}\frac{X-j'}{j-j'} \tag{1}$$

令 $\Delta=l!$，在式(1)两端同时乘以 Δ，可得

$$\Delta f(X)=\sum_{j\in\partial}\lambda_{X,j}^{\partial}f(j) \tag{2}$$

其中，$\lambda_{X,j}^{\partial}=\Delta\prod_{j'\in\partial\backslash\{j\}}\frac{X-j'}{j-j'}$。

由于 $\left(\prod_{j'\in\partial\backslash\{j\}}(j-j')\right)\Big|\Delta$，式(2)中的运算均可以在整数环 Z 中进行，因此，我们称式(2)为整数环上的拉格朗日插值公式。

3 PTS-RSA 签名方案

本文提出的 PTS-RSA 方案包括密钥生成、签名、验证和私钥份额更新 4 个阶段。

(1)密钥生成：可信中心选择并计算初始参数 (n,m,e,d)(各符号含义及相互关系见 2.2 节)。令 $a_0=d$，随机选择 $a_i\in Z$，$i=1,2,\cdots,k-1$，构成多项式 $f(X)=\sum_{i=0}^{k-1}a_iX^i \in Z[X]$。可信中心计算秘密份额

$$s_i=f(i),\ i=1,2,\cdots,l$$

并将 s_i 通过安全信道发送给用户 i。

可信中心随机选择 Q_n 的生成元 v，并计算 $v_i=v^{s_i} \bmod n, i=1,2,\cdots,l$，并将 (v,v_i) 作为验证密钥公开。

(2)签名：设 M 为待签署信息，$H(\bullet)$ 为值域为 Z_n^* 的 Hash 函数，$x=H(M)$，包含 k 个成员的团体 S 希望生成对 M 的有效签名。他们的签名过程如下：

步骤 1 生成部分签名及正确性证据：每个签名参与者 $i\in S$ 计算部分签名

$$x_i=x^{2\Delta s_i} \bmod n \tag{3}$$

令 $\tilde{x}=x^{4\Delta} \bmod n$，那么 $x_i^2\equiv\tilde{x}^{s_i}(\bmod n)$ 成立，参与者 i 为了证明 x_i 的正确性，按照 2.3 节所述计算 $c=H'(v,\tilde{x},v_i,x_i^2 \bmod n,v',x')$ 和 $z=s_ic+r$，并将 (z,c) 作为 x_i 的正确性证据。

步骤 2 验证并合成部分签名：签名合成者首先验证 $c=H'(v,\tilde{x},v_i,x_i^2 \bmod n,v^zv_i^{-c} \bmod n,\tilde{x}^zx_i^{-2c} \bmod n)$ 对每个成员 $i\in S$ 是否成立。如果都成立，则计算 $w=\prod_{i\in S}x_i^{2\lambda_{0,i}^S} \bmod n$。令 $e'=4\Delta^2$，由于 $(e',e)=1$，可使用扩展欧几里得算法得到满足 $e'a+eb=1$ 的 a 和 b，然后计算 $y=w^ax^b \bmod n$，y 即为信息 M 的标准 RSA 签名。

(3)验证：验证过程与标准 RSA 签名方案的验证过程相同，即验证 $H(M)=y^e \bmod n$ 是否成立，如成立则认为群签名有效。

(4)私钥份额更新：在进行私钥份额更新时，采用“零共享”技术[17]：设成员 j 在第 t 时间段内的私钥份额为 $s_j^{(t)}$，则在第 t 次私钥份额更新时，首先，Ω (任一由 k 个成员组成的集合)中的每一成员 i 随机生成常数项为 0 的 $k-1$ 次多项式 $g_i(X)\in Z[X]$，计算 $g_i(j), j=1,2,\cdots,l$，并将 $g_i(j)$ 通过安全信道发送给成员 j，如图 1 所示；然后，每一成员 $j\in\{1,2,\cdots,l\}$ 计算 $s_j^{(t+1)}=s_j^{(t)}+\sum_{i\in\Omega}g_i(j)$，作为其 $t+1$ 时刻的秘密份额。

在实际运行中，私钥份额更新协议还需要验证各种信息的真实性，具体步骤如下：

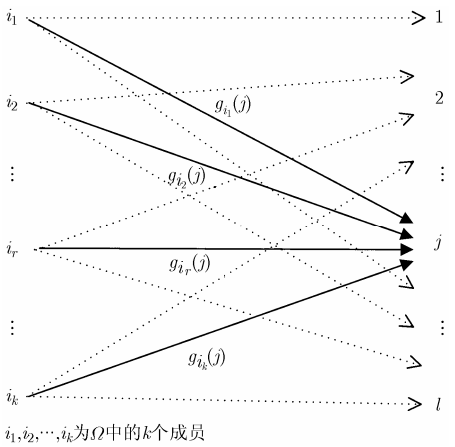

图 1 “零共享”技术

步骤 1　Ω (任一由 k 个成员组成的集合)中的每个成员 i 均随机生成常数项为 0 的 $k-1$ 次多项式 $g_i(X)=g_{i,1}X+g_{i,2}X^2+\cdots+g_{i,k-1}X^{k-1}\in Z[X]$，计算 $g_i(j)$ 和 $G_{i,j}=v^{g_i(j)} \bmod n,\ j=1,2,\cdots,l$，并公开 $G_{i,j}$。然后将 $g_i(j), j\in\{1,2,\cdots,l\}\setminus\{i\}$ 通过安全信道发送给成员 j，将 $g_i(i)$ 保存起来。

步骤 2　每个成员 $j\in\{1,2,\cdots,l\}$ 在接收到所有的 $g_i(j), i\in\Omega\setminus\{j\}$ 后，执行如下步骤：

(a)验证 $G_{i,j}, j=1,2,\cdots,l$ 的合法性，即对 Ω 中的每个成员 i，验证 $G_{i,j}$ 以 v 为底，模 n 时的离散对数值是否为同一个常数项为 0 的 $k-1$ 次多项式函数在点 j, j=1,2,$\cdots$,l 处的函数值：令 $\Re=\{1,2,\cdots,k-1\}$，$G_i(X)=\prod_{j\in\Re}G_{i,j}^{\lambda_{X,j}^{\Re\cup\{0\}}} \bmod n$。对每个 $j\in\{k,k+1,\cdots,l\}$，验证 $G_{i,j}^{\Delta} \bmod n=G_i(j)$ 是否成立，如果都成立，则认为所有 $G_{i,j}$, j=1,2,$\cdots$,l 都合法，否则，认为成员 i 为恶意成员(实际上，如果 $G_{i,j}$ 都合法，则 $G_i(X)=\prod_{j\in\Re}G_{i,j}^{\lambda_{X,j}^{\Re\cup\{0\}}} \bmod n=\prod_{j\in\Re}v^{g_i(j)\lambda_{X,j}^{\Re\cup\{0\}}} \bmod n=v^{\sum_{j\in\Re}g_i(j)\lambda_{X,j}^{\Re\cup\{0\}}} \bmod n=v^{\Delta g_i(X)} \bmod n$，因此 $\forall j\in\{k,k+1,\cdots,l\}$, $G_{i,j}^{\Delta} \bmod n=G_i(j)$ 一定成立)。

(b)对每个成员 $i\in\Omega$，验证 $v^{g_i(j)} \bmod n=G_{i,j}$ 是否都成立，如果都成立，则计算新的私钥份额 $s_j^{(t+1)}=s_j^{(t)}+g(j)$，其中，$g(X)=\sum_{i\in\Omega}g_i(X)$。否则，认为成员 i 发送了虚假的 $g_i(j)$，生成投诉信息并广播。

以第 1 次私钥份额更新，即 $t=1$ 为例，由于 $s_j^{(1)}=f(j)$，令 $f'(X)=f(X)+g(X)$，那么，$s_j^{(2)}=f'(j)$ 成立。由 $g_i(X), i\in\Omega$ 的常数项均为 0 可知，$f'(j)$ 的常数项为 $a_0=d$。因此，$s_j^{(2)}, j=1,2,\cdots,l$ 对私钥 d 构成了有效的 (k,l) 共享。这样就实现了在不改变私钥的情况下私钥份额的更新。

步骤 3　私钥份额由 $s_j^{(t)}$ 更新为 $s_j^{(t+1)}$ 后，每个成员 $j\in\{1,2,\cdots,l\}$ 将部分签名的正确性验证密钥更新为 $v_j^{(t+1)}=v^{s_j^{(t+1)}} \bmod n$，并将其向其他成员广播，以便于后续签名过程中对部分签名进行正确性验证。

步骤 4　为防止恶意成员使用虚假的私钥份额产生 $v_j^{(t+1)}$，任一成员 $i\in\{1,2,\cdots,l\}$ 均可通过验证 $v_j^{(t+1)}=v_j^{(t)}\cdot\prod_{i\in\Omega}G_{i,j} \bmod n$ 是否成立来判断 $v_j^{(t+1)}$, $j\in\{1,2,\cdots,l\}\setminus\{i\}$ 的正确性。

4　对方案的分析

4.1 安全性分析

定理 1 (正确性)　PTS-RSA 方案是正确的。

证明　要证明签名方案的正确性，只要证明签名过程中产生的群签名 y 为标准 RSA 签名，即 $y^e \bmod n=x$ 即可。

由于 $w=\prod_{i\in S}x_i^{2\lambda_{0,i}^S} \bmod n$，$w^e=\left(\prod_{i\in S}x_i^{2\lambda_{0,i}^S}\right)^e \bmod n=\left(\prod_{i\in S}x^{2\Delta s_i\cdot 2\lambda_{0,i}^S}\right)^e \bmod n=x^{4e\Delta\sum_{i\in S}s_i\lambda_{0,i}^S} \bmod n$ 成立。而根据式(2)，令 $X=0$，有 $\Delta d=\Delta f(0)=\sum_{i\in S}\lambda_{0,i}^S f(i)=\sum_{i\in S}\lambda_{0,i}^S s_i$，因此，$w^e=x^{4\Delta^2 ed} \bmod n=x^{4\Delta^2} \bmod n=x^{e'} \bmod n$。由 $y=w^a x^b \bmod n$ 及 $e'a+eb=1$ 可知，$y^e \bmod n=w^{ea}x^{eb} \bmod n=x^{e'a}x^{eb} \bmod n=x^{e'a+eb} \bmod n=x$。　证毕

定理 2 (不可伪造性)　如果标准 RSA 签名方案是适应性选择消息攻击下不可伪造的，那么，面对静态移动攻击者实施适应性选择消息攻击时，PTS-RSA 方案是不可伪造的。

证明　为了将 PTS-RSA 方案的不可伪造性归约至标准 RSA 签名方案的不可伪造性，我们将构建模拟器 SIM，其输入为 PTS-RSA 方案的所有公开参数。其输出满足：从敌手 E(具备适应性选择消息攻击能力的静态移动攻击者)的角度看，与 PTS-RSA 方案在运行过程中的输出信息是不可区分的。

令 $S^{(t)}, t=1,2,\cdots$ 表示第 t 个时间段内被敌手 E 捕获的成员组成的集合，$|S^{(t)}|=k-1$。SIM 对 PTS-RSA 方案的模拟包括对密钥生成、签名及私钥份额更新过程的模拟。

(1)在模拟密钥生成过程时，SIM 随机选择整数 $\overline{s}_j^{(1)}$ 作为受控成员 $j\in S^{(1)}$ 的私钥份额。那么，由拉格朗日插值方法可知：必定存在 $k-1$ 次多项式 $f^{(1)}(X)$，满足 $f^{(1)}(0)=d$，以及 $f^{(1)}(j)=\overline{s}_j^{(1)}$ 对任一 $j\in S^{(1)}$ 成立。虽然 SIM 不知道 d，无法通过拉格朗日插值方法重构 $f^{(1)}(X)$，但 SIM 输出的密钥份额 $\{\overline{s}_j^{(1)}\mid j\in S^{(1)}\}$ 可以认为是在 PTS-RSA 方案中使用 $f^{(1)}(X)$ 代替 $f(X)$ 后产生的。因此，对于敌手 E 来说，无法判断 $S^{(1)}$ 中 $k-1$ 个成员的私钥份额是由 PTS-RSA 方案产生，还是由 SIM 产生。

为生成验证密钥 $(\overline{v}^{(1)},\overline{v}_i^{(1)})$，SIM 可随机选择消息 $\overline{M}$，并对原始 RSA 签名方案进行签名查询获得 $\overline{M}$ 的签名 $\overline{y}$。令 $H(\overline{M})=u$，那么，$\forall i\in\{1,2,\cdots,l\}$，可以采用下述步骤(2)中求部分签名 $\overline{x}_i^{(1)}$ 的方法求出 $u_i=u^{2\Delta\overline{s}_i} \bmod n$。令 $\overline{v}^{(1)}=u^{2\Delta}$，$\overline{v}_i^{(1)}=u_i$，则 $\overline{v}_i^{(1)}=(\overline{v}^{(1)})^{\overline{s}_i} \bmod n$ 成立。将 $(\overline{v}^{(1)},\ \overline{v}_i^{(1)})$ 作为验证密钥公开。

(2)在模拟第 1 时间段内的签名过程时，对于受控成员 $j\in S^{(1)}$, SIM 使用 $\overline{s}_j^{(1)}$ 生成其部分签名 $\overline{x}_j^{(1)}$。对于成员 $i\notin S^{(1)}$，在获得合法签名对 (y,M) (可通过

对原始RSA签名方案进行签名查询获得)的情况下，根据式(2)，可得

$$\Delta f^{(1)}(X)=\lambda_{X,0}^{S^{(1)}\cup\{0\}}d+\sum_{j\in S^{(1)}}\lambda_{X,j}^{S^{(1)}\cup\{0\}}f^{(1)}(j)$$

那么，SIM 可以为成员 i 计算部分签名

$$\overline{x}_i^{(1)}=\overline{x}^{2\Delta\overline{s}_i^{(1)}}\bmod n=y^{2\left(\lambda_{i,0}^{S^{(1)}\cup\{0\}}+e\sum\limits_{j\in S^{(1)}}\lambda_{i,j}^{S^{(1)}\cup\{0\}}\overline{s}_j^{(1)}\right)}\bmod n \tag{4}$$

其中，$\overline{x}=H(M)$。

由于$\left\{\overline{s}_j^{(1)}\middle|j\in S^{(1)}\right\}$的不可区分性，导致敌手 E 无法区分$\left\{\overline{x}_j^{(1)}\middle|j\in S^{(1)}\right\}$，而由式(4)可知，任一$\overline{x}_i^{(1)},i\notin S^{(1)}$与$\left\{\overline{x}_j^{(1)}\middle|j\in S^{(1)}\right\}$都能够合成为合法的群签名。因此，$\left\{\overline{x}_i^{(1)}\middle|i\notin S^{(1)}\right\}$对于敌手 E 来说也是不可区分的。

关于部分签名的正确性证据$(\overline{z},\overline{c})$的产生方法，请参阅文献[16]方案中的相关部分。

(3)在模拟第 1 次私钥份额更新过程时，SIM 首先随机选择集合Ω，并明确Ω与$S^{(1)}$，$S^{(2)}$的关系，假设如图 2 所示。根据系统模型，对于$S^{(1)}\cap S^{(2)}$中的任一成员 j，攻击者能够掌握其私钥份额增量$g(j)=s_j^{(2)}-s_j^{(1)}$；对于$(S^{(1)}\setminus S^{(2)})\cup(S^{(2)}\setminus S^{(1)})$中的任一成员 i，攻击者无法掌握其私钥份额增量$g(i)=s_i^{(2)}-s_i^{(1)}$，否则将导致攻击者在同一时刻掌握大于$k-1$个成员的私钥份额，与系统模型不符。

SIM 选择随机整数$\overline{s}_j^{(2)}$作为成员$j\in S^{(2)}$在第 2 时间段内的私钥份额，同时使用步骤(1)中求$\overline{v}_j^{(1)}$的方法求出$\overline{v}_j^{(2)}$(使用相同的底数$\overline{v}$)。随机选择成员$i'\in\Omega\setminus S^{(1)}$，$\forall i\in\Omega\setminus\{i'\}$，随机选择常数项为 0 的$k-1$次多项式$\overline{g}_i(X)\in Z[X]$，计算$\overline{g}_i(j)$和$\overline{G}_{i,j}=\overline{v}^{\overline{g}_i(j)}\bmod n$，$j=1,2,\cdots,l$，然后计算$\overline{G}_{i',j}=\overline{v}_j^{(2)}\Big/\left(\overline{v}_j^{(1)}\prod_{i\in\Omega\setminus\{i'\}}\overline{G}_{i,j}\right)\bmod n$，$j=1,2,\cdots,l$；对任一$j\in S^{(1)}\cap S^{(2)}$，计算$g_{i',j}=\overline{s}_j^{(2)}-\overline{s}_j^{(1)}-\sum_{i\in\Omega\setminus\{i'\}}\overline{g}_i(j)$作为$i'$发送给$j$的数值。

下面分析不可区分性，主要包括$\overline{s}_j^{(2)}$，$\overline{v}_i^{(2)}$，$\overline{G}_{i,j}$，$\overline{g}_i(j)$等的不可区分性。

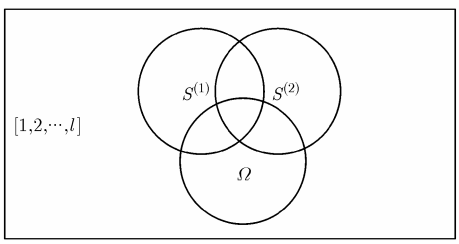

图 2 集合关系

(a)由拉格朗日插值方法知，对任一$j\in S^{(2)}$，$f^{(2)}(j)=\overline{s}_j^{(2)}$，以及$f^{(2)}(0)=d$可唯一确定$k-1$次多项式$f^{(2)}(X)\in Z[X]$。由$\overline{s}_j^{(1)}$和$\overline{v}_j^{(1)}$的不可区分性直接可以得出$\overline{s}_j^{(2)}$和$\overline{v}_j^{(2)}$的不可区分性；

(b)$\forall i\in\Omega\setminus\{i'\}$，由于$\overline{g}_i(X)$由随机选择产生，$\overline{g}_i(j)$和$\overline{G}_{i,j}$的不可区分性是显然的。令$\overline{g}(X)=f^{(2)}(X)-f^{(1)}(X)$，$\overline{g}_{i'}(j)=\overline{g}(j)-\sum_{i\in\Omega\setminus\{i'\}}\overline{g}_i(j)$。那么，$\forall j\in S^{(1)}\cap S^{(2)}$，$g_{i',j}=\overline{s}_j^{(2)}-\overline{s}_j^{(1)}-\sum_{i\in\Omega\setminus\{i'\}}\overline{g}_i(j)=\overline{g}_{i'}(j)$成立。$\forall j\in\{1,2,\cdots,l\}$，$\overline{G}_{i',j}=\overline{v}_j^{(2)}\Big/\left(\overline{v}_j^{(1)}\cdot\prod_{i\in\Omega\setminus\{i'\}}\overline{G}_{i,j}\right)\bmod n=\overline{v}^{\overline{s}_j^{(2)}-\overline{s}_j^{(1)}}\Big/\prod_{i\in\Omega\setminus\{i'\}}\overline{v}^{\overline{g}_i(j)}\bmod n=\overline{v}^{\overline{g}(j)}-\sum_{i\in\Omega\setminus\{i'\}}\overline{g}_i(j)\bmod n=\overline{v}^{\overline{g}_{i'}(j)}\bmod n$。显然，这与 PTS-RSA 方案是一致的。

(4)第t($t=2,3,\cdots$)时间段内的签名过程，及第t次私钥份额更新过程的模拟方法与步骤(2)，步骤(3)类似，不再赘述。

现在，假设敌手 E 能够伪造 PTS-RSA 方案的群签名，那么，对于 PTS-RSA 方案所依托的原始 RSA 签名方案，敌手E′在不知道其私钥的情况下，可通过向该 RSA 签名方案进行签名查询获得合法签名对，然后使用 SIM 模拟出 PTS-RSA 方案的输出，并调用敌手E攻击 PTS-RSA 方案的算法来产生新消息M'的合法群签名y'，这样，敌手E′就成功伪造了M'在原始 RSA 签名方案中的签名y'。

令$\mathrm{Pr}_{\mathrm{PTS}}$表示敌手E成功伪造PTS-RSA方案的一个群签名的概率，$\mathrm{Pr}_{\mathrm{RSA}}$表示敌手E′成功伪造原始 RSA 签名方案的一个签名的概率，那么，由以上分析可知$\mathrm{Pr}_{\mathrm{PTS}}\le\mathrm{Pr}_{\mathrm{RSA}}$。如果标准 RSA 签名方案在适应性选择消息攻击下是不可伪造的，即$\mathrm{Pr}_{\mathrm{RSA}}$可忽略。那么，$\mathrm{Pr}_{\mathrm{PTS}}$也可以忽略，即 PTS-RSA 方案在适应性选择消息攻击下也是不可伪造的。 证毕

定理 3(稳健性) 当$l\ge 2k-1$时，即使攻击者控制了多达$k-1$个成员，剩余的成员仍能够合作产生合法的群签名。

证明 为了证明 PTS-RSA 方案的稳健性，只需证明当恶意成员发送虚假信息时，能够被合理检测出来即可。这主要包括签名阶段对部分签名x_i，以及私钥份额更新阶段对$G_{i,j}$，$g_i(j)$和$v_j^{(t+1)}$进行正确性验证。其中，对部分签名x_i进行正确性验证的合理性可参阅文献[16]方案中的相关部分。

(1)假设恶意成员i选择$g_{i,j}$来计算得到$G_{i,j}$，即$G_{i,j}=v^{g_{i,j}}\bmod n$，且$g_{i,j}$不是同一个常数项为 0 的$k-1$次多项式函数在点$j$，$j=1,2,\cdots,l$处的函数值，仍能够通过 PTS-RSA 方案私钥份额更新阶段步骤

2-(1)的验证，即 $\forall j \in \{k,k+1,\cdots,l\}$, $G_{i,j}^{\Delta} \bmod n = G_i(j)$ 成立。令 $g_i^{'}(X) = \left(\sum_{j\in\Re} g_{i,j}\lambda_{X,j}^{\Re\cup\{0\}}\right)\Big/\Delta$，显然，$g_i'(X)$ 为常数项为 0 的 $k-1$ 次多项式函数。由 $G_i(X)$ 的构造过程知，$G_i(X) = v^{\Delta g_i'(X)} \bmod n$。根据假设，必定存在 $j' \in \{k,k+1,\cdots,l\}$，满足 $g_{i,j'} \neq g_i^{'}(j')$，且 $v^{\Delta g_{i,j'}} \bmod n = G_{i,j'}^{\Delta} \bmod n = G_i(j') = v^{\Delta g_i^{'}(j')} \bmod n$，令 $\delta = g_{i,j'} - g_i^{'}(j')$，则 $\delta \neq 0$ 且 $v^{\Delta\delta} \equiv 1(\bmod n)$ 成立。由 v 是 Q_n 的生成元，v 的阶 $\mathrm{ord}(v) = m$，以及 m 不能整除 Δ 可知，$m|\delta$。由于 e 为素数，$(e,\delta)=1$，$(e,2)=1$ 成立，可由扩展欧几里得算法求出 α，β，α' 和 β'，满足 $\alpha e+\beta\delta=1$ 和 $\alpha' e+\beta' 2=1$。对任意消息 M，令 $x=H(M)$，则 $y=x^{2\beta'\alpha+\alpha'} \bmod n$ 即为 M 的标准 RSA 签名。这是因为 $y^e \bmod n = x^{2\beta'\alpha e} x^{\alpha' e} \bmod n = (x^2)^{\beta'(1-\beta\delta)} x^{\alpha' e} \bmod n$，由于 x^2 的阶 $\mathrm{ord}(x^2)|m$，$m|\delta$，因此，$y^e \bmod n = x^{2\beta'} x^{\alpha' e} \bmod n = x^{2\beta'+\alpha' e} \bmod n = x$。

上述分析说明，如果恶意成员 i 公开的 $G_{i,j}$ 以 v 为底，模 n 时的离散对数值不是同一个常数项为 0 的 $k-1$ 次多项式函数在点 j, $j=1,2,\cdots,l$ 处的函数值，仍能够通过验证，则他可以成功伪造任意消息 M 的标准 RSA 签名。而后者的概率是可忽略的，因此，前者的概率也是可忽略的。

(2)如果恶意成员 i 能够产生 $r \neq g_i(j)$，满足 $v^r \bmod n = G_{i,j}$，则 $v^r \equiv v^{g_i(j)}(\bmod n)$，由此可得 $v^{r-g_i(j)} \equiv 1(\bmod n)$ 成立。令 $\delta = r - g_i(j)$，可以采用与证明过程(1)类似的方法来证明 r 通过验证的概率是可忽略的。

(3)同理可证，在将部分签名的正确性验证密钥更新为 $v_j^{(t+1)} = v^{s_j^{(t+1)}} \bmod n$ 时，恶意成员 j 使用虚假的 $s_j^{(t+1)}$ 生成 $v_j^{(t+1)}$ 并通过验证的概率也是可以忽略的。　　证毕

4.2 实用性分析

表 1 列出了现有的前摄性门限 RSA 签名方案的安全性和使用的秘密共享方法。其中，静态安全表示能够抵抗静态移动攻击者，动态安全表示能够抵抗动态移动攻击者。

正如引言部分所述，基于加性共享方法的前摄性门限 RSA 签名方案存在诸多问题。文献[13]方案虽然使用多项式共享方法，但已经被证明是不安全的。文献[14]方案在签名时需要所有签名参与者合作生成一个临时的加性共享份额，增加了通信次数，延长了节点入网认证时间。由表 1 可知，PTS-RSA 方案是目前唯一不依赖加性共享方法、可证明安全的前摄性门限 RSA 签名方案，由于其签名方法简单，仅需要签名请求者向 k 个成员分别申请部分签名即可，而 k 个成员之间无需任何信息交互，因而非常适合资源受限型网络。下面我们通过 PTS-RSA 方案与文献[14]方案在通信量和计算量方面的比较来说明 PTS-RSA 方案在该方面的优势。由于门限签名的密钥生成过程不会频繁进行，该过程所需的运算量及通信量对方案的实用性影响不大，因此，我们主要针对签名阶段和私钥份额更新阶段对两种方案进行对比。同时由于签名和私钥份额更新协议运行的频率也不相同，我们将对这二者进行分别对比。

表 1 前摄性门限RSA签名方案的安全性和使用的秘密共享方法

前摄性门限 RSA 签名方案	安全性	使用的秘密共享方法
文献[8]方案	静态安全	加性共享
文献[9]方案	静态安全	加性共享
文献[10]方案	静态安全	加性共享
文献[11]方案	动态安全	加性共享
文献[12]方案	动态安全	加性共享
文献[13]方案	已被证明不安全	多项式共享
文献[14]方案	静态安全	多项式共享为主，加性共享为辅
PTS-RSA 方案	静态安全	多项式共享

两种方案的通信次数见表 2。当 $l=20$，$k=10$ 时，文献[14]方案在签名和私钥份额更新阶段的通信次数分别为 265 和 415，而 PTS-RSA 方案中相应的数值分别为 10 和 190。由此可见，PTS-RSA 方案在降低通信开销方面的性能远远优于文献[14]方案。

表 2 两种方案通信次数

签名方案	签名阶段	私钥份额更新阶段
文献[14]案	$2.5k^2+1.5k$	$2.5k^2-3.5k+kl$
PTS-RSA 方案	k	$k(l-1)$

与模指数运算相比，模乘法、模加法和模逆运算的计算量几乎可以忽略，因此，我们通过比较签名方案所需进行的模指数运算次数来比较两种方案的签名效率。表 3 列出了文献[14]方案、PTS-RSA 方案各阶段所需进行的模指数运算次数。当 $l=20$，$k=10$，$h=10$ 时（h 为文献[14]方案中的安全参数），文献[14]方案在签名和私钥份额更新阶段的所需的模指数运算次数分别为 2365 和 2375，而 PTS-RSA 方案中相应的数值分别为 82 和 1520。因此，PTS-RSA 方案的运算效率高于文献[14]方案，签名效率的优势尤其明显。

表 3 两种方案模指数运算次数

签名方案	签名阶段	私钥份额更新阶段
文献[14]方案	$k(k-1)(1.5h+7.5)$ $+k(3h+4)$	$k(k-1)(1.5h+8.5)$ $+(k+3)l$
PTS-RSA 方案	$8k+2$	$l(k+1)^2-k^3+k^2$

5 结束语

本文针对现有可证明安全的前摄性门限 RSA 签名方案均依赖加性共享方法，不能满足资源受限型网络的应用需求这一问题，以文献[16]提出的门限 RSA 签名方案为基础，将其中的加法、乘法和除法运算均转移至整数环中，结合“零共享”技术，设计了合理的私钥份额更新协议，进而形成一种在通信开销和计算效率方面均优于现有方案的前摄性门限 RSA 签名方案。在静态移动攻击者模型中对方案的安全性进行了详细的证明。后续工作将集中于研究如何抵抗动态移动攻击者(此类攻击者可根据已掌握的私钥份额和签名来选择新的捕获对象，具有更强的攻击能力)，进一步提高签名系统的安全性。

参 考 文 献

[1] 徐甫, 马静谨. 基于中国剩余定理的门限 RSA 签名方案的改进[J]. 电子与信息学报, 2015, 37(10): 2495–2500. doi: 10.11999/JEIT150067.
XU Fu and MA Jingjin. Improvement of threshold RSA signature scheme based on Chinese remainder theorem[J]. *Jouranl of Electronic & Information Technology*, 2015, 37(10): 2495–2500. doi: 10.11999/JEIT150067.

[2] 王洁, 蔡永泉, 田有亮. 基于博弈论的门限签名体制分析与构造[J]. 通信学报, 2015, 36(5): 1–8. doi:10.11959/j.issn.1000-436x.2015189.
WANG Jie, CAI Yongquan, and TIAN Youliang. Analysis and construction for threshold signature scheme based on game theory[J]. *Journal on Communications*, 2015, 36(5): 1–8. doi: 10.11959/j.issn.1000-436x.2015189

[3] 曹阳. 基于秘密共享的数字签名方案[J]. 重庆邮电大学学报(自然科学版), 2015, 27(3): 418–421. doi: 10.3979 /j.issn.1673-825X.2015.03.021.
CAO Yang. Digital signature scheme based on secret sharing[J]. *Journal of Chongqing University of Posts and Telecommunications* (*Natural Science Edition*), 2015, 27(3): 418–421. doi: 10.3979/j.issn.1673-825X.2015.03.021.

[4] KAYA K and SELÇUK A A. Sharing DSS by the Chinese remainder theorem[J]. *Journal of Computational and Applied Mathematics*, 2014, 259: 495–502. doi: 10.1016/j.cam. 2013. 05.023.

[5] 崔涛, 刘培玉, 王珍. 前向安全的指定验证者(t, n)门限代理签名方案[J]. 小型微型计算机系统, 2014, 35(5): 1061–1064.
CUI Tao, LIU Peiyu, and WANG Zhen. Forward secure (t,n) threshold proxy signature scheme with designated verifier[J]. *Journal of Chinese Computer Systems*, 2014, 35(5): 1061–1064.

[6] 张文芳, 王小敏, 郭伟, 等. 基于椭圆曲线密码体制的高效虚拟企业跨域认证方案[J]. 电子学报, 2014, 42(6): 1095–1102. doi: 10.3969 /j.issn.0372-2112.2014.06.010.
ZHANG Wenfang, WANG Xiaomin, GUO Wei, *et al*. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem[J]. *Acta Electronica Sinica*, 2014, 42(6): 1095–1102. doi: 10.3969/j.issn.0372-2112.2014.06.010.

[7] HERZBERG A, JAKOBSSON M S, JARECKI H, *et al*. Proactive public key and signature systems[C]. Proceedings of the 4th ACM Conference on Computers and Communication Security, Zurich, Switzerland, 1997: 100–110.

[8] JARECKI S and SAXENA N. Further simplifications in proactive RSA signature schemes[C]. Proceedings of TCC'05, Massachusetts, USA, 2005: 510–528.

[9] FRANKEL Y, GEMMELL P, MACKENZIE P D, *et al*. Proactive RSA[C]. Proceedings of CRYPTO'97, California, USA, 1997: 440–454.

[10] RABIN T. A simplified approach to threshold and proactive RSA[C]. Proceedings of CRYPTO'98, California, USA, 1998: 89–104.

[11] FRANKEL Y, MACKENZIE P D, and YUNG M. Adaptive security for the additive-sharing based proactive RSA[C]. Proceedings of PKC'01, Cheju Island, Korea, 2001: 240–263.

[12] ALMANSA J F, DAMGARD I, and NIELSEN J B. Simplified threshold RSA with adaptive and proactive security[C]. Proceedings of EUROCRYPT 2006, Saint Petersburg, Russia, 2006: 593–611.

[13] LUO H, KONG J, ZERFOS P, *et al*. URSA: Ubiquitous and robust access control for mobile ad hoc networks[J]. *IEEE/ACM Transactions on Networking*, 2004, 12(6): 1049–1063. doi: 10.1109/TNET.2004.838598.

[14] FRANKEL Y, GEMMELL P, MACKENZIE P D, *et al*. Optimal-resilience proactive public-key cryptosystems[C]. Proceedings of the 38th Symposium on Foundations of Computer Science (FOCS), Miami Beach, USA, 1997: 384–393.

[15] JARECKI S and SAXENA N. On the insecurity of proactive RSA in the URSA mobile ad hoc network access control protocol[J]. *IEEE Transactions on Information Forensics and Security*, 2010, 5(4): 739–749. doi: 10.1109/TIFS.2010. 2058104.

[16] SHOUP V. Practical threshold signatures[C]. Proceedings of EUROCRYPT 2000, Bruges, Belgium, 2000: 207–220.

[17] ZHOU L and HAAS Z J. Securing Ad hoc networks[J]. *IEEE Network*, 1999, 13(6): 24–30.

徐 甫： 男，1983 年生，博士生，研究方向为信息安全.