基于中国剩余定理的门限RSA签名方案的改进

徐 甫*①② 马静谨②
①(解放军信息工程大学 郑州 450002)
②(北京市信息技术研究所 北京 100094)

摘 要：针对基于中国剩余定理的门限RSA签名方案无法签署某些消息，以及部分签名合成阶段运算量大的问题，论文提出一种基于虚拟群成员的改进方法，使得改进后的方案能够签署所有消息，同时能够极大地减少部分签名合成阶段的运算量，当门限值为10时，可以将部分签名合成阶段的运算量减少为原来的1/6。对改进方案进行了详细的安全性和实用性分析。结果表明，改进方案在适应性选择消息攻击下是不可伪造的，且其运算效率较其他门限RSA签名方案更高。

关键词：门限签名；RSA签名方案；Asmuth-Bloom秘密共享；中国剩余定理
中图分类号： TP309 **文献标识码**： A **文章编号**：1009-5896(2015)10-2495-06
DOI: 10.11999/JEIT150067

Improvement of Threshold RSA Signature Scheme Based on Chinese Remainder Theorem

Xu Fu①② Ma Jing-jin②
①(*PLA Information Engineering University*, *Zhengzhou* 450002, *China*)
②(*Information Technology Institute of Beijing City*, *Beijing* 100094, *China*)

Abstract: To slove the problems that Chinese Remainder Theorem (CRT) based threshold RSA signature scheme can not be used to sign some messages and the amount of computation in partial signatures combining phase is large, an improving method is proposed, in which a virtual group member is introduced, making the scheme can be used to sign all messages and significantly reducing the amount of computation in partial signatures combining phase, e.g. when the threshold value is 10, the amount of computation in partial signatures combining phase can be reduced to 1/6 of the original. The security and practicability of the improved scheme are analyzed. Results show that it is non-forgeable against an adaptive chosen message attack and more efficient than other threshold RSA signatures.

Key words: Threshold signature; RSA signature scheme; Asmuth-Bloom secret sharing; Chinese Remainder Theorem (CRT)

1 引言

随着分布式系统的广泛使用，以及对用户身份认证、密钥管理等手段的需求越来越强烈，门限签名方案逐渐成为了该领域的一个研究热点[1–3]，并获得了广泛应用[4]。作为门限密码学的重要组成部分，门限签名由秘密共享与数字签名相结合而产生。在(t,n)门限签名方案中，群体的签名密钥被所有n个成员共同持有，使得群体中任意不少于t个成员的子集可以代表群体对给定消息进行签名，而任意少于t个成员的子集则不能产生有效的群签名。同时，门限签名不改变签名的验证方法，验证者只需要知道群体的唯一公开密钥，就可以简单而方便地验证群签名是否有效。

秘密共享方案(Secret Sharing Scheme, SSS)是门限签名的基础。已有的许多门限签名方案，包括门限RSA签名方案[5–8]，ElGamal类门限签名方案[9,10]等，都使用基于拉格朗日插值方法的Shamir SSS[11]实现对签名私钥的共享。2007年，Kaya和Selçuk首次将基于中国剩余定理(Chinese Remainder Theorem, CRT)的Asmuth-Bloom SSS[12]引入了门限密码学，并利用该方案构造了门限RSA签名方案[13](以下简称“Kaya-Selçuk方案”)。

由于Asmuth-Bloom SSS自身的特性，将其应用于门限RSA签名方案时，在部分签名合成阶段，直接用各部分签名进行模乘运算只能生成一个不完

收稿日期：2015-01-12；改回日期：2015-05-28；网络出版：2015-07-17
*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)

整的群签名，需要经过矫正运算后，才能够得到正确的群签名。Kaya-Selçuk 方案中，对于经过 Hash 函数处理的消息 w，矫正运算过程中需产生矫正因子 $\kappa = w^{-M_\psi} \bmod N$，为元素 $w^{M_\psi} \bmod N$ 在 Z_N 中的逆元。但是，由于 $N = pq$ 不是素数，Z_N 是交换环而不是域，$w^{M_\psi} \bmod N$ 在 Z_N 中的逆元未必存在。因此，Kaya-Selçuk 方案并不是对所有消息都适用的。同时，矫正运算过程中，平均需要进行 $t+1$ 次模指数运算，以及一些辅助运算，增大了签名合成者的运算负担。

本文对 Kaya-Selçuk 方案进行了改进，通过引入一个虚拟群成员，在不需要矫正运算的情况下，保证了签名方案的正确性。在改进的 Kaya-Selçuk 方案中，不再需要对 $w^{M_\psi} \bmod N$ 求逆，确保其对所有消息都适用。同时，由于不再需要矫正运算，减少了部分签名合成阶段的运算量，提高了签名的效率。

文章第 2 节简要介绍了背景及相关工作；第 3 节对 Kaya-Selçuk 方案进行改进；第 4 节对提出的改进方案进行正确性、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 门限签名方案及其安全性

定义 1 (t,n) 门限签名方案由 3 部分组成：建立(setup)、签名(signing)和验证(verification)。

建立：可信中心根据系统参数 I 生成公钥和私钥，采用 SSS 对私钥进行共享，并将其份额通过安全信道发送给各成员。

签名：t 个以上(含 t 个)成员通过计算产生待签署消息 m 的部分签名，并发送给签名合成者(通常为参与签名的某一成员)，然后由签名合成者将所有部分签名合成为群签名。

验证：验证群签名是否正确。

定义 2 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 3 称 (t,n) 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 $t-1$ 个成员，且先后进行了 k 次群签名或部分签名查询(设使用的消息分别为 $\mathrm{msg}_1, \mathrm{msg}_2, \cdots, \mathrm{msg}_k$)，最终能够成功伪造一个新消息 $\mathrm{msg}(\mathrm{msg} \notin \{\mathrm{msg}_1, \mathrm{msg}_2, \cdots, \mathrm{msg}_k\})$ 的群签名的概率是可忽略的。

2.2 Asmuth-Bloom SSS

Asmuth 和 Bloom 于 1983 年以 CRT 为理论基础，提出了一种新的 SSS[12]：为了在 n 个成员中共享秘密 d，秘密分发者首先需执行如下步骤：

(1)选择 $n+1$ 个两两互素，且满足如下条件的正整数 $m_0, m_1, \cdots, m_n$。

(a) $m_0 > d$，且 m_0 为素数；

(b) $m_0 < m_1 < m_2 < \cdots < m_n$；

$$\text{(c)} \prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1} \tag{1}$$

(2)令 $M = \prod_{i=1}^{t} m_i$，分发者计算 $y = d + Am_0$，其中，A 为随机产生的，且能够使得 $0 \le y < M$ 成立的正整数。

(3)计算第 i 个成员的秘密份额 $y_i = y \bmod m_i$，$1 \le i \le n$，并分发至第 i 个成员。

如果获得秘密份额的 t 个成员想重构秘密值 d，他们可进行如下步骤：

(1)令该 t 个成员组成的集合为 ψ，$M_\psi = \prod_{i\in\psi} m_i$，$M_{\psi\setminus\{i\}} = \prod_{j\in\psi, j\ne i} m_j$，$M'_{\psi,i}$ 为 $M_{\psi\setminus\{i\}}$ 的在 Z_{m_i} 中的乘法逆元，即 $M_{\psi\setminus\{i\}} M'_{\psi,i} \equiv 1 (\bmod m_i)$。那么，由 $y \equiv y_i (\bmod m_i), i \in \psi$，可根据 CRT[14]求得唯一的 $y = \sum_{i\in\psi} u_i \bmod M_\psi$，其中，$u_i = y_i M'_{\psi,i} M_{\psi\setminus\{i\}} \bmod M_\psi$ 由第 i 个成员计算；

(2)计算秘密值 $d = y \bmod m_0$。

2.3 Kaya-Selçuk 方案

为了满足 Kaya-Selçuk 方案将 m_0 设定为 $\phi(N)$ 的要求，以及提高门限 RSA 签名方案安全性，Kaya 和 Selçuk 对 Asmuh-Bloom SSS 进行了修改，不再要求 m_0 为素数，且将式(1)所确定的条件修改为

$$\prod_{i=1}^{t} m_i > m_0^2 \prod_{i=1}^{t-1} m_{n-i+1}$$

定义 4 称成员个数为 n，门限值为 t 的 Kaya-Selçuk 方案为 (t,n)-Kaya-Selçuk 方案。

(t,n)-Kaya-Selçuk 方案包括建立、签名和验证 3 个阶段。

(1)建立： 可信中心选择 RSA 素数 $p = 2p'+1$ 和 $q = 2q'+1$，其中，p' 和 q' 也为大素数。计算 $N = pq$ 和 $\phi(N) = 4p'q'$。从 $Z^*_{\phi(N)}$ 中选择满足条件 $ed \equiv 1 \bmod \phi(N)$ 的 e 和 d，分别作为公钥和私钥。将改进后的 Asmuh-Bloom SSS 中的 m_0 设定为 $\phi(N) = 4p'q'$，并用该 SSS 对私钥 d 进行共享。

(2)签名： 设 m 为待签署信息，$h(\bullet)$ 为值域为 Z^*_N 的 Hash 函数，$w = h(m)$，包含 t 个成员的团体 ψ 希望生成对 m 的有效签名。他们的签名过程分为 3 个步骤：

(a)生成部分签名：每个签名参与者 $i \in \psi$ 计算

$u_i = y_i M'_{\psi,i} M_{\psi\setminus\{i\}} \bmod M_\psi$ 和 $s_i = w^{u_i} \bmod N$。

(b)合成部分签名：签名合成者计算 $\bar{s} = \prod_{i\in\psi} s_i \bmod N$。

(c)矫正：令 $\kappa = w^{-M_\psi} \bmod N$ 为矫正因子，签名合成者通过计算寻找满足 $(\bar{s}\kappa^j)^e \equiv w(\bmod N),\ 0 \le j < t$ 的 j，令 δ 表示该合适的 j 值，那么，计算群签名 $s = \bar{s}\kappa^\delta$。

(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 $h(m) = s^e \bmod N$ 是否成立，如成立则认为群签名有效。

3　改进的 Kaya-Selçuk 方案

改进的 Kaya-Selçuk 方案(以下简称“改进方案”)同样包括建立、签名和验证 3 个阶段。

定义 5　称成员个数为 n，门限值为 t 的改进方案为 (t,n)-改进方案。

(t,n)-改进方案的各阶段运行过程如下：

(1)建立：　可信中心选择既为安全素数，又为 Sophie Germain 素数的两个大数 p' 和 q'，计算 $p = 2p'+1$ 及 $q = 2q'+1$，那么 p 和 q 也为大素数。计算 $N = pq$，$\lambda(N) = \mathrm{lcm}(p-1, q-1) = 2p'q'$，从 $Z^*_{\lambda(N)}$ 中选择满足条件 $ed \equiv 1 \bmod \lambda(N)$ 的 e 和 d，分别作为公钥和私钥。用 Kaya 和 Selçuk 改进后的 Asmuh-Bloom SSS 对私钥 d 进行共享，具体过程如下：

令 $m_0 = \lambda(N)$，选择满足以下条件的整数 $m_1, m_2, \cdots, m_r, \cdots, m_{n+1}$。

(a) $m_r = m_0 z$，其中，z 为安全素数；

(b) $m_1, m_2, \cdots, m_r, \cdots, m_{n+1}$ 两两互素(由于 $m_0 | m_r$，其中隐含了 m_0 与除 m_r 之外的数互素)，且 $m_0 < m_1 < \cdots < m_r < \cdots m_{n+1}$；

(c) $\prod_{i=1}^{t+1} m_i > m_0^2 \prod_{i=1}^{t+1} m_{n-i+2}$。

令 $M = \prod_{i=1}^{t+1} m_i$，可信中心计算 $y = d + Am_0$，其中 A 为使得 $0 \le y < M$ 成立的正整数。第 i 个成员关于 d 的秘密份额为 $y_i = y \bmod m_i, 1 \le i \le n+1$。

需要指出的是，$y_i, i = 1,2,\cdots,r-1,r+1,\cdots,n+1$ 由可信中心通过安全信道发送至第 i 个成员，但 y_r 由可信中心向所有成员广播。第 r 个成员为虚拟群成员，在部分签名生成阶段，其角色由签名合成者承担。

(2)签名：设 m 为待签署信息，$h(\bullet)$ 为值域为 Z_N^* 的 Hash 函数，$w = h(m)$，包含 t 个签名参与者的团体 ψ 希望生成对 m 的有效签名。他们的签名过程分为两个步骤：

(a)生成部分签名：令 $\overline{\psi} = \psi \cup \{r\}$，每个签名参与者 $i \in \psi$ 计算 $u_i = y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod M_{\overline{\psi}}$ 和 $s_i = w^{u_i} \bmod N$。

(b)合成部分签名：签名合成者按照步骤(a)的方法，为虚拟群成员计算部分签名 s_r，然后合成所有 $t+1$ 个部分签名，生成群签名

$$s = \prod_{i\in\overline{\psi}} s_i \bmod N \tag{2}$$

(3)验证：验证过程与 Kaya-Selçuk 方案的验证过程相同。

4　对改进方案的分析

4.1　正确性分析

引理 1[14]　设 p 和 q 是两个不同的素数，$N = pq$，则 $\forall m \in Z_N$ 以及任意非负整数 k，有 $m^k \bmod N = m^{k \bmod \lambda(N)} \bmod N$ 成立。

引理 2　在改进方案中，有 $d = \sum_{i\in\overline{\psi}} y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod m_0$ 成立。

证明　根据 CRT[14]，有 $y = \sum_{i\in\overline{\psi}} y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod M_{\overline{\psi}}$ 成立，因此，

$$d = y \bmod m_0 = \left(\sum_{i\in\overline{\psi}} y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod M_{\overline{\psi}} \right) \bmod m_0 \tag{3}$$

由 $m_r | M_{\overline{\psi}}$，以及 $m_0 | m_r$ 可知，$m_0 | M_{\overline{\psi}}$。那么，根据式(3)可得，$d = \sum_{i\in\overline{\psi}} y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod m_0$。证毕

定理 1　改进方案是正确的，即 $s = w^d \bmod N$ 成立。

证明　$s = \prod_{i\in\overline{\psi}} s_i \bmod N = \prod_{i\in\overline{\psi}} w^{u_i} \bmod N = \prod_{i\in\overline{\psi}} w^{y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod M_{\overline{\psi}}} \bmod N = w^{\sum_{i\in\overline{\psi}} \left(y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod M_{\overline{\psi}} \right)} \bmod N$。

根据引理 1 以及 $m_0 | M_{\overline{\psi}}$，可得

$$s = w^{\sum_{i\in\overline{\psi}} \left(y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod M_{\overline{\psi}} \right) \bmod m_0} \bmod N$$

$$= w^{\sum_{i\in\overline{\psi}} y_i M'_{\overline{\psi},i} M_{\overline{\psi}\setminus\{i\}} \bmod m_0} \bmod N$$

根据引理 2，可得 $s = w^d \bmod N$。　证毕

4.2　安全性分析

本节对改进方案进行安全性证明，证明过程中参考了 Kaya-Selçuk 方案安全性证明中的方法[13]。

定理 2　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，则改进方案也是适应性选择消息攻击下不可伪造的。

证明　为了将改进方案的安全性归约为标准 RSA 签名方案的安全性，我们将构建模拟器 SIM，其输入为改进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)的角度看，与改进方案在运行过程中的输出信息是不可区分的。

令 ψ' 表示被敌手 E 控制的成员集合，$|\psi'|=t-1$，$M_{\psi'}=\prod_{j\in\psi'}m_j$。在模拟密钥分发过程时，SIM 随机选择 $y_j^{'}\in Z_{m_j}, j\in\psi'$ 作为受控成员 j 的密钥份额，则根据广义 CRT[15]及 $y_r\equiv d(\bmod(m_r,m_0))$，包含 $t+1$ 个方程的同余方程组

$$\left.\begin{aligned} x&\equiv y_j^{'}\left(\bmod m_j\right),\ \ j\in\psi'\\ x&\equiv y_r\left(\bmod m_r\right)\\ x&\equiv d\left(\bmod m_0\right)\end{aligned}\right\} \tag{4}$$

在 $Z_{m_rM_{\psi'}}$ 中有唯一解 y'。由于 $d=y'\bmod m_0$，可令 $y'=d+A'm_0$，则受控成员 j 的密钥份额 $y_j^{'}=y'\bmod m_j$。在改进方案中，密钥份额 $y_j=y\bmod m_j$，其中 $y=d+Am_0$。因此，模拟器输出的密钥份额 $y_j^{'}$ 可以认为是在改进方案中重新选择 A 后产生的。由此可以得出，敌手 E 无法判断 $\{y_j^{'}|j\in\psi'\}$ 是由改进方案产生还是由 SIM 产生。

在模拟部分签名的过程时，对于受控成员 $j\in\psi'$，SIM 使用 $y_j^{'}$ 生成其部分签名 s_j，使用 y_r 生成虚拟群成员 r 的部分签名 s_r，对于成员 $i\notin\psi'$，在获得合法签名对 (s,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

$$s_i=s\left(\prod_{j\in\psi'\cup\{r\}}s_j\right)^{-1}\bmod N \tag{5}$$

其中，$s_j=\left(h(m)\right)^{u_j}\bmod N=\left(h(m)\right)^{y_jM_{\bar{\psi},j}^{'}M_{\bar{\psi}\backslash\{j\}}\bmod M_{\bar{\psi}}}\bmod N$，$\bar{\psi}=\psi'\cup\{r\}\cup\{i\}$。由于 $\{y_j^{'}|j\in\psi'\}$ 的不可区分性，导致敌手 E 无法区分 $\{s_j|j\in\psi'\}$，而任一 s_i 与 $\{s_j|j\in\psi'\}$ 及 s_r 都能够合成为合法的群签名。因此，$\{s_i|i\notin\psi'\}$ 对于敌手 E 来说也是不可区分的。

现在，假设敌手 E 能够伪造改进方案的群签名，那么，对于改进方案所依托的原始 RSA 签名方案，敌手 E′ 在不知道密钥 d 的情况下，可通过向原始 RSA 签名方案进行签名查询获得合法签名对，然后使用 SIM 模拟出改进方案的输出，并调用敌手 E 攻击改进方案的算法来产生消息 m' 的合法群签名 s'，这样，敌手 E′ 就成功伪造了 m' 在原始 RSA 签名方案中的签名 s'。

令 $\mathrm{Pr_{TH}}$ 表示敌手 E 成功伪造改进方案的一个群签名的概率，$\mathrm{Pr_{RSA}}$ 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 $\mathrm{Pr_{TH}}\le\mathrm{Pr_{RSA}}$。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 $\mathrm{Pr_{RSA}}$ 可忽略。那么，$\mathrm{Pr_{TH}}$ 也可以忽略，根据定义 3 可知，改进方案在适应性选择消息攻击下也是不可伪造的。 证毕

4.3 实用性分析

4.3.1 对签名合成效率的影响分析 与 Kaya-Selçuk 方案相比，改进方案在运算量方面的变化主要在于签名合成阶段，合成者需要为虚拟群成员计算一个部分签名，而不再需要进行矫正运算。本节对两种方案中合成部分签名的运算量进行比较。

在 (t,n)-Kaya-Selçuk 方案的部分签名合成阶段，签名合成者需要合成 t 个部分签名，以及进行矫正运算，所需操作及运算如表 1 所示。

表 1 (t,n)-Kaya-Selçuk方案中部分签名合成阶段需要的运算

操作	所需运算
合成 t 个部分签名	$t-1$ 次模 N 乘法运算
计算 $\kappa=w^{-M_\psi}\bmod N$	1 次模 N 指数运算和 1 次模 N 逆运算
计算 $(\bar{s}\kappa^j)^e\bmod N$, $j=0,1,\cdots,t-1$	平均需要 t 次模 N 指数运算和 $0.5t$ 次模 N 乘法运算

在 (t,n)-改进方案的部分签名合成阶段，签名合成者需要为虚拟群成员计算部分签名 s_r，并合成 $t+1$ 个部分签名，所需操作及运算如表 2 所示。

表2 (t,n)-改进方案中部分签名合成阶段需要的运算

操作	所需运算
计算 $M_{\bar{\psi},r}^{'}$	1 次模 m_r 逆运算
计算 u_r	2 次模 $M_{\bar{\psi}}$ 乘法运算
计算 s_r	1 次模 N 指数运算
合成 $t+1$ 个部分签名	t 次模 N 乘法运算

表 1 和表 2 中的运算包括模指数、模乘法、模逆等运算。其中，模指数运算中通常需要进行多次模平方运算和模乘法运算，以平方-乘算法为例[14]，设 e 的长度为 l bit，重量为 h_e，则计算 $X^e\bmod N$（X 为 Z_N^* 中的任意值)共需要 l 次模 N 平方运算和 h_e 次模 N 乘法运算[14]。如果将模 N 平方运算和模 N 乘法运算的计算复杂性看作同一量级，并以 h_e 取平均值 $0.5l$ 来计算，计算 $X^e\bmod N$ 的运算量大约相当于 $1.5l$ 次模 N 乘法运算。由于 N 通常取 1024 bit 以上的大数，$\lambda(N)$ 的长度仅比 N 略小，而 $e\in Z_{\lambda(N)}^*$，其长度 l 通常也较大，可能在 512 bit 以上。因此，与计算 $(\bar{s}\kappa^j)^e\bmod N, j=0,1,\cdots,t-1$ 所需的运算量相比，表 1 中的模乘法运算的运算量可以忽略，模逆运算可使用减法和移位实现[16]，其运算量同样可以忽略。同理，与计算 $w^{M_\psi}\bmod N$ 所需的运算量相比，表 1 中的模乘法和模逆运算的运算量也可以忽略；与计算 $s_r=w^{u_r}\bmod N$ 所需的运算量相比，表 2 中的模乘法和模逆运算的运算量也可以忽略。那么，(t,n)-Kaya-Selçuk 方案中部分签名合成的运算量约

相当于计算 $(\bar{s}\kappa^j)^e \bmod N, j=0,1,\cdots,t-1$ 和 $w^{M_\psi} \bmod N$ 所需的运算量，约为 $1.5l\times(0.5t+1)$ 次模 N 乘法运算(由于 j 较小，计算 $\kappa^j \bmod N$ 的运算量可忽略)；而 (t,n)-改进方案中部分签名合成的运算量约相当计算 $s_r = w^{u_r} \bmod N$ 所需的运算量，约为 $1.5l$ 次模 N 乘法运算。因此，改进方案的部分签名合成的运算量减少为原来的 $1/(0.5t+1)$。当 t 较大，比如 $t=10$ 时，改进方案的部分签名合成的运算量减少为原来的 1/6，极大地提高了部分签名合成的效率。

4.3.2 与其他门限 RSA 签名方案的对比分析　由于门限签名的建立过程不会频繁进行，建立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(包括部分签名产生和合成)和验证阶段对本文改进方案与现有的其他门限 RSA 方案进行对比。

除基于 CRT 的门限 RSA 门限签名方案之外，效率较高，具有代表性的门限 RSA 门限签名方案包括 Shoup 方案[5]和徐秋亮方案[6](以下简称“Xu 方案”)。Kaya 和 Selçuk 选择了 Shoup 方案作为签名效率的比较对象[13]，但王贵林等人[17]提出了一种针对 Shoup 方案的改进方案(以下简称“Wang 方案”)，简化了其签名方程。因此，我们选择 Wang 方案和 Xu 方案作为本文改进方案的比较对象。表 3 列出了 3 种方案的部分签名产生、合成阶段和验证阶段的运算量(与上一节相同，仅考虑了模指数运算)。

由表 3 可知，本文改进方案在部分签名合成阶段运算量为其他两种方案的 $1/t$；3 种方案在部分签名产生阶段的运算量相同；验证阶段的运算量方面，改进方案与 Shoup 方案相同，为 Xu 方案的 1/2。总体来讲，与其他两种门限 RSA 签名方案相比，改进方案在运算效率方面具有较大的优势。

在签名方案的通信开销方面，3 种方案的部分签名都是通过模 N 指数运算产生的，平均长度相同；3 种方案的部分签名最终都是通过模 N 乘法运算合成为群签名的，因而群签名的平均长度也相同。从签名请求者发起申请开始至其收到群签名的全部过程中，3 种方案都需要经历如下通信过程：

(1)签名请求者将待签署信息 m 发送给 t 个以上成员；

(2)收到 m 的各成员(即签名参与者)生成部分签名后将其发送给签名合成者；

(3)签名合成者生成群签名后将其发送给签名请求者。

因此，改进方案的通信开销与其他两种方案基本相同。

5　结束语

本文针对 Kaya 和 Selçuk 提出的基于 CRT 的门限 RSA 签名方案的部分签名合成阶段需要进行 Z_N 中的求逆运算和复杂的矫正运算，导致该方案无法对某些消息进行签署，以及部分签名合成效率低下的问题，提出了一种改进方法，通过设置一个虚拟群成员，在部分签名合成阶段无需求逆运算和矫正运算的情况下，能够保证签名的正确性，使得改进后的方案能够签署所有消息。同时，由于不再需要矫正运算，使得部分签名合成的运算量大大减少，极大地提高了部分签名合成的效率，并合理选择了大素数，使得方案的安全性不受影响。

表 3 改进方案与其他门限RSA签名方案的运算量

签名方案	部分签名产生阶段的模指数运算次数	部分签名合成阶段的模指数运算次数	验证阶段的模指数运算次数
Wang 方案[17]	1	t	1(忽略次数较小的模指数运算)
Xu 方案[6]	1	t	2
本文改进方案	1	1	1

参 考 文 献

[1] 马春光, 石岚, 周长利, 等. 属性基门限签名方案及其安全性研究[J]. 电子学报, 2013, 41(5): 1012-1015.
Ma Chun-guang, Shi Lan, Zhou Chang-li, *et al*.. Threshold attribute-based signature and its security[J]. *Acta Electronica Sinica*, 2013, 41(5): 1012-1015.

[2] 杨小东, 李春梅, 徐婷, 等. 无双线性对的基于身份的在线/离线门限签名方案[J]. 通信学报, 2013, 34(8): 185-190.
Yang Xiao-dong, Li Chun-mei, Xu Ting, *et al*.. ID-based on-line/off-line threshold signature scheme without bilinear pairing[J]. *Journal on Communications*, 2013, 34(8): 185-190.

[3] 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 Pei-yu, 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.

[4] 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.

Zhang Wen-fang, Wang Xiao-min, 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.

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

[6] 徐秋亮. 改进门限 RSA 数字签名体制[J]. 计算机学报, 2000, 23(5): 449–453.
Xu Qiu-liang. A modified threshold RSA digital signature scheme[J]. *Chinese Journal of Computers*, 2000, 23(5): 449–453.

[7] 张文芳, 何大可, 王小敏, 等. 基于新型秘密共享方法的高效 RSA 门限签名方案[J]. 电子与信息学报, 2005, 27(11): 1745–1749.
Zhang Wen-fang, He Da-ke, Wang Xiao-min, *et al*.. A new RSA threshold group signature scheme based on modified Shamir's secret sharing solution[J]. *Journal of Electronic & Information Technology*, 2005, 27(11): 1745–1749.

[8] Aboud S J, Yousef S, and Cole M. Undeniable threshold proxy signature scheme[C]. Proceedings of 5th International Conference on Computer Science and Information Technology, Amman, Jordan, 2013: 150–153.

[9] Gennaro R, Jarecki S, Krawczyk H, *et al*.. Robust threshold DSS signatures[J]. *Information and Computation*, 2001, 164(1): 54–84.

[10] Kim S, Kim J, Cheon J H, *et al*.. Threshold signature schemes for ElGamal variants[J]. *Computer Standards & Interfaces*, 2011, 33(4): 432–437.

[11] Shamir A. How to share a secret?[J]. *Communications of the ACM*, 1979, 22(11): 612–613.

[12] Asmuth C and Bloom J. A modular approach to key safeguarding[J]. *IEEE Transactions on Information Theory*, 1983, 29(2): 208–210.

[13] Kaya K and Selçuk A A. Threshold cryptography based on Asmuth-Bloom secret sharing[J]. *Information Sciences*, 2007, 177(19): 4148–4160.

[14] 金晨辉, 郑浩然, 张少武, 等. 密码学[M]. 北京: 高等教育出版社, 2009: 244–367.
Jin Chen-hui, Zheng Hao-ran, Zhang Shao-wu, *et al*.. Cryptography[M]. Beijing: Higher Education Press, 2009: 244–367.

[15] Iftene S and Grindei M. Weighted threshold RSA based on the Chinese remainder theorem[C]. Proceedings of Ninth International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, 2007: 175–181.

[16] 谭丽娟, 陈运. 模逆算法的分析、改进及测试[J]. 电子科技大学学报, 2004, 33(4): 383–386.
Tan Li-juan and Chen Yun. Analysis and improvement of modular inverse algorithm[J]. *Journal of UEST of China*, 2004, 33(4): 383–386.

[17] 王贵林, 卿斯汉, 王明生. Shoup 门限 RSA 签名方案的改进[J]. 计算机研究与发展, 2002, 39(9): 1046–1050.
Wang Gui-lin, Qing Si-han, and Wang Ming-sheng. Improvement of Shoup's threshold RSA signature scheme[J]. *Journal of Computer Research and Development*, 2002, 39(9): 1046–1050.

徐 甫： 男，1983 年生，博士生，研究方向为信息安全.
马静谨： 男，1981 年生，工程师，研究方向为数据链安全.