新的标准模型下基于身份的环签名方案

刘振华[①②]　胡予濮[②]　牟宁波[②]　马　华[①]
[①](西安电子科技大学应用数学系　西安　710071)
[②](西安电子科技大学计算机网络与信息安全教育部重点实验室　西安　710071)

摘　要：该文提出了一种新的基于身份的环签名方案，并在标准模型下证明其能抵抗签名伪造攻击，且具有无条件匿名性。与现有标准模型下基于身份的环签名方案相比，新方案具有更短的公开参数，对于 n 个成员的环，签名长度只有 $n+1$ 个群元素，签名验证需要 $n+1$ 个双线性对运算，因此能更好的满足应用要求。

关键词：基于身份的密码；环签名；标准模型；双线性对
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)07-1727-05

New Identity-Based Ring Signature in the Standard Model

Liu Zhen-hua[①②]　Hu Yu-pu[②]　Mu Ning-bo[②]　Ma Hua[①]
[①](*Applied Mathematics Department, Xidian University, Xi'an* 710071, *China*)
[②](*Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an* 710071, *China*)

Abstarct: A new identity-based ring signature scheme is proposed. This scheme is existentially unforgeable in the standard model and unconditionally anonymous. Compared with the existing identity-based ring signature schemes in the standard model, this new scheme has shorter public parameter size, moreover, for n members of a ring, the signature only consists of $n+1$ group elements and needs $n+1$ pairings to verify, thus it can more satisfy the application requirements.

Key words: Identity-based cryptography; Ring signature; Standard model; Bilinear pairings

1　引言

大多数多用户电子商务应用中越来越关注匿名性。面向群体的签名方案使群组的一个成员代表群组产生一个签名。匿名面向群体签名方案有两个主要类型：群签名和环签名。在群签名方案中，群组是预先设定的，具有一个群组管理员，在必要的时候可以撤销签名者的匿名性，群管理员通过密钥分配创建群。环签名有相似的特点，但是不支持匿名撤销机制，不需要密钥分配。因此环签名能使任何一个实体自然地召集 $n-1$ 个任意实体，代表整个群组产生一个可公开验证的 $(1,\ n)$ 签名，同时实际签名人保持匿名。

Shamir提出了一种基于身份的公钥密码体制[1]，该体制中私钥生成器(PKG)把身份作为公钥并生成对应的私钥。PKG不需要维护所签发的证书列表，用户仅需要存储PKG的系统参数，而不是其他用户的证书数据库。因此基于身份的密码比传统公钥基础设施(PKI)提供更大的方便。2001年，Boneh等使用双线性对技术提出了第1个安全实用的基于身份的加密方案[2]，并在随机预言机模型下证明是安全的。

近年来，环签名[3]和基于身份的密码发展迅速，二者的结合——基于身份的环签名也得到了深入研究[4−9]。上述多数方案是基于双线性对的。不幸的是，基于身份的环签名理论仍遇到实际应用的两大问题，其一是现有多数方案是基于双线性对的，众所周知，双线性对的计算是相当昂贵的。其二是可证明安全问题，现有的多数基于身份的环签名方案在随机预言机模型下是安全的，然而，随机预言机模型把Hash函数作为一个完全随机的理想模型，是一个很强的要求。近年来有学者指出某些在随机预言机模型可证安全的方案在实际应用中并不安全[10]，因为真正的Hash函数与随机预言机的问答模式是有区别的。因此在不借助于随机预言机的标准模型下设计可证安全的方案，同时用尽可能少的双线性对运算，更有意义。

2006年Au等学者利用标准模型下基于身份的

2008-09-22 收到，2009-03-09 改回
国家自然科学基金(60473029, 60803149)和国家“973”规划项目(2007CB311201)资助课题

加密方案[11]，提出一个标准模型下可证安全的基于身份的环签名方案[12]。随后张跃宇等学者提出一个改进的方案[13]，具有更少的公开参数，减少了签名长度和双线性对的运算个数，但该方案是不安全的，即利用已知消息的签名能够伪造任何消息的有效环签名。本文提出了一个新的基于身份的环签名方案，并证明其在标准模型下是存在性不可伪造的，且具有无条件匿名性，同时保留了文献[12,13]的优点。

2 预备知识

2.1 安全模型

一个基于身份的$(1,\ n)$环签名方案由以下概率算法组成：

(1)系统建立(Setup)：该算法由PKG完成，输入安全参数k，输出主密钥s和系统参数Params。PKG保密s，公开Params。

(2)私钥生成(Extract)：给定一个用户的身份I，PKG计算用户私钥d，并通过安全方式发送给这个用户。

(3)签名(Sign)：输入公开参数Params，构成环的用户身份集合R，用户$I_\pi \in R$的私钥d_π和签名消息M，输出环R对M的基于身份的$(1,n)$环签名σ。

(4)验证(Verify)：输入公开参数Params，构成环的用户身份集合R，签名消息M和环签名σ，输出Valid 或Invalid。

下面介绍基于身份的环签名方案的安全模型，包括不可伪造性和匿名性。

定义1 如果不存在多项式时间内的敌手能以不可忽略的优势赢得以下游戏，则称一个基于身份的环签名方案具有适应性选择消息和选择身份攻击下的不可伪造性，该游戏在敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间进行。

(1)挑战者$\mathcal{C}$输入安全参数k，运行Setup算法得到系统参数Params和主密钥s，他发送系统参数给敌手$\mathcal{A}$并秘密保存主密钥。

(2)敌手$\mathcal{A}$进行多项式次数的适应性询问，即每次询问依赖于以前询问的结果，询问包括：

密钥提取询问：$\mathcal{A}$选择一个身份I，询问$\mathcal{C}$关于I的私钥，作为回答，$\mathcal{C}$运行Extract算法并把私钥d返回给$\mathcal{A}$。

签名询问：$\mathcal{A}$选择包含n个身份的集合$R=\{I_1,\ I_2,\ \cdots,\ I_n\}$和消息$M$，作为回答，$\mathcal{C}$运行Sign算法并把$(1,\ n)$环签名$\sigma$返回给$\mathcal{A}$。

(3)最后，敌手$\mathcal{A}$输出一个签名$(M^*,\ R^*,\ \sigma^*)$，要求：(1)$(M^*,\ R^*)$没有被询问过，(2)不能对R^*中任何成员进行密钥提取询问。如果$\mathrm{Verify}(M^*, R^*, \sigma^*)$是Valid，$\mathcal{A}$就赢得了游戏。

敌手$\mathcal{A}$的优势定义为它能赢得以上游戏的概率$Adv_{\mathcal{A}}=\Pr[\mathcal{A}\ \text{succeeds}]$。

定义2 如果任何包含n个用户的身份集合$R=\{I_1,\ I_2,\ \cdots,\ I_n\}$对消息$M$的$(1,\ n)$环签名$\sigma$，任何敌手$\mathcal{A}$能够识别实际签名人的优势不会大于随机猜测，亦即$\mathcal{A}$输出实际签名人的概率不会大于$1/n$，则称一个基于身份的环签名方案具有无条件匿名性。

2.2 双线性对

设G和G_T是阶为素数p的乘法循环群，g是G的一个生成元。双线性对是指满足下列性质的一个映射$e: G\times G\to G_T$：(1)双线性性 对任意的$a,\ b\in Z_p$，有$e(g^a,\ g^b)=e(g,\ g)^{ab}$；(2)非退化性 $e(g,\ g)\neq 1$；(3)可计算性对所有的$u,\ v\in G$，存在有效的算法计算$e(u,\ v)$。

2.3 困难假设

计算性Diffie-Hellman假设：给定$(g,\ g^a,\ g^b)\in G$，其中$a,\ b\in Z_p$是未知的整数，无多项式时间算法$\mathcal{C}$至少以概率ε计算g^{ab}。若概率$\Pr[\mathcal{C}(g,\ g^a,\ g^b)=g^{ab}]\geq\varepsilon$，则称$\mathcal{C}$具有优势$\varepsilon$。

3 新的基于身份的环签名方案

本节给出的新的标准模型下基于身份的环签名方案。

系统建立(Setup)：(G,G_T)表示双线性乘法循环群，其中$|G|=|G_T|=p$，p是一个大素数，g是群G的一个生成元。双线性对$e:\ G\times G\to G_T$，Hash函数$H_m:\{0,\ 1\}^*\to Z_p^*$。选择一个秘密值$\alpha\in Z_p$，计算$g_1=g^\alpha$。随机选择$g_2,\ u'\in G$和长度为n_u的一个向量$\boldsymbol{U}=(u_i)$，向量中的元素都是从群G中随机选取。系统公共参数 Params 设置为$(G,\ G_T,\ e,\ g,\ g_1,\ g_2,\ u',\boldsymbol{U})$，系统主私钥为$g_2^\alpha$。

私钥生成(Extract)：令I是长度为n_u的比特串，也表示用户I的身份，记$\mathcal{U}\subseteq\{1,\ 2,\ \cdots,\ n_u\}$是满足$I[i]=1$的下标$i$的集合。相应于身份$I$的私钥$d_I$的生成方式如下：随机选择$r_I'\in Z_p$，令$U=u'\prod_{i\in\mathcal{U}}u_i$，计算$d_I=(d_{I,1},\ d_{I,2})=(g_2^\alpha(U)^{r_I'},\ g^{r_I'})$。

签名(Sign)：令$R=\{I_1,\ I_2,\ \cdots,\ I_n\}$为环签名中所包含的$n$个身份的列表，实际的签名者身份$I_\pi\in R$($\pi\in\{1,\ 2,\ \cdots,\ n\}$)，对消息$M$进行签名，计算$m=H_m(R,\ M)$。相应的环签名生成如下：随机选取$r_1,\ r_2,\ \cdots,\ r_n\in Z_p$，计算

$$\sigma=\left(d_{\pi,1}^{m}\prod_{j=1}^{n}(U_j)^{r_j},g^{r_1},g^{r_2},\cdots,g^{r_{\pi-1}},d_{\pi,2}^{m}g^{r_\pi},\cdots,g^{r_n}\right)$$
$$=\left((g_2^{\alpha})^m(U_\pi)^{mr'_\pi}\prod_{j=1}^{n}(U_j)^{r_j},\ g^{r_1},\ g^{r_2},\cdots,g^{r_{\pi-1}},\right.$$
$$\left.g^{r_\pi+mr'_\pi},\cdots,g^{r_n}\right)\tag{1}$$

签名验证(Verify)：给定身份列表 R 在消息 M 上的签名 $\sigma=(S,\ R_1,\ R_2,\ \cdots,\ R_n)$，验证者计算 $m=H_m(R,\ M)$，$U_j=u'\prod_{i\in\mathcal{U}_j}u_i$，其中 $j=1,\ 2,\ \cdots,\ n$，检查等式 $e(S,\ g)=e(g_1,\ g_2)^m\prod_{j=1}^{n}e(U_j,\ R_j)$ 是否成立，如果成立，输出 Valid，否则输出 Invalid。

正确性：从下面的推导中很容易得出改进的方案是正确的。

$$e(S,\ g)=e\left((g_2^{\alpha})^m(U_\pi)^{mr'_\pi}\prod_{j=1}^{n}(U_j)^{r_j},\ g\right)$$
$$=e((g_2^{\alpha})^m,\ g)e\left((U_\pi)^{mr'_\pi+r_\pi}\prod_{j=1,j\neq\pi}^{n}(U_j)^{r_j},\ g\right)$$
$$=e(g_1,\ g_2)^m\prod_{j=1}^{n}e(U_j,\ R_j)$$
$$=e(g_1,\ g_2)^m\prod_{j=1}^{n}e(U_j,\ R_j)\tag{2}$$

4　安全分析

本节从匿名性和存在不可伪造性两个方面分析新环签名的安全性，同时给出性能分析。

4.1 匿名性

定理 1　新方案是无条件匿名的。

证明　在新方案的签名 $\sigma=(S,R_1,R_2,\cdots,R_n)$ 中，$\{R_j\}\ (j=1,\cdots,\pi-1,\pi+1,\cdots,n)$ 是随机生成的，没有提供实际签名者的任何信息。另外 $R_\pi=g^{mr'_\pi+r_\pi}$，其中 r'_π 是由私钥生成中心(与实际签名人独立的)随机生成的，r_π 由实际签名者随机选择的，因此 R_π 的分布是随机的。最后我们考虑 $S=d_{\pi,1}^{m}\prod_{j=1}^{n}(U_j)^{r_j}=(g_2^{\alpha})^m(U_\pi)^{mr'_\pi+r_\pi}\prod_{j=1,j\neq\pi}^{n}(U_j)^{r_j}$，其中指数部分是随机的，$g_2^{\alpha}$ 是主私钥，m 是身份列表 R 和消息 M 的无碰撞 Hash 值。所有这些都没有提供任何有关实际签名人的信息。对于敌手来说就等同于暴力猜测。因此新的环签名方案是无条件匿名的。

证毕

4.2 存在不可伪造性

定理 2　在经过至多 q_E 次密钥提取询问，q_S 次签名询问以后，假设存在一个敌手 $\mathcal{A}$ 能够按照定义 1 在时间 t 内，能以优势 ε 伪造签名，那么存在一个算法 $\mathcal{C}$ 在时间 $t'=t+(4q_E+(2n+3)q_S)\tau+((n_u+2)q_E+((n_u+1)n+2)q_S)\rho$ 内，以概率 $\varepsilon'\geq\frac{\varepsilon}{2^{n+1}(q_E+q_S)^n(n_u+1)^n}$ 解决计算性 Diffie-Hellman 问题的一个实例，其中 ρ 和 τ 分别为群 G 中的乘法和指数运算时间。

证明　设挑战者 $\mathcal{C}$ 收到一个随机 CDH 问题实例$(g,\ A=g^a,\ B=g^b)$，他的目标是计算 g^{ab}，$\mathcal{C}$ 把 $\mathcal{A}$ 作为子程序调用并回答 $\mathcal{A}$ 的询问，方案的证明基于 Waters 的思想[13]。

建立：$\mathcal{C}$ 设置 $l=2(q_E+q_S)$，并随机选择一个整数 $k\ (0\leq k\leq n_u)$。设对于给定的 q_E，q_S 和 n_u，有 $l(n_u+1)<p$。然后随机选择一个整数 $x'\in Z_l$ 和一个 n_u 维的向量 $\boldsymbol{X}=(x_i)\ (x_i\in Z_l)$。最后随机选择一个整数 $y'\in Z_p$ 和一个 n_u 维的向量 $\boldsymbol{Y}=(y_i)\ \ (y_i\in Z_p)$。为了方便，对于身份 I 定义如下两个函数：$F(I)=(p-lk)+x'+\sum_{i\in\mathcal{U}}x_i$，$J(I)=y'+\sum_{i\in\mathcal{U}}y_i$，其中 $\mathcal{U}\subseteq\{1,2,\cdots,n_u\}$ 为身份 $I[i]=1$ 的所有下标 i 的集合。然后挑战者 $\mathcal{C}$ 指定参数如下：

$$g_1=g^a,\ g_2=g^b,\ u'=g_2^{(p-lk)+x'}g^{y'},$$
$$u_i=g_2^{x_i}g^{y_i}(1\leq i\leq n_u)\tag{3}$$

注意到主私钥 $g_2^a=g^{ab}$ 和等式 $U=u'\prod_{i\in\mathcal{U}}u_i=g_2^{F(I)}\cdot g^{J(I)}$。

预言机模拟：$\mathcal{C}$ 应答私钥提取询问和签名询问如下：

私钥提取询问：当敌手 $\mathcal{A}$ 询问相应于身份 I 的私钥时，挑战者 $\mathcal{C}$ 检查 $F(I)=0\bmod l$ 是否成立，若成立，$\mathcal{C}$ 放弃游戏；否则 $\mathcal{C}$ 随机选取 $r\in Z_p$，并把模拟的私钥 d_I 发送给敌手 $\mathcal{A}$，其中：$d_I=(d_{I,1},d_{I,2})=\left(g_1^{-\frac{J(I)}{F(I)}}\left(u'\prod_{i\in\mathcal{U}}u_i\right)^r,\ g_1^{-\frac{1}{F(I)}}g^r\right)$。挑战者 $\mathcal{C}$ 能模拟这样一个私钥，当且仅当 $F(I)\neq0\bmod l$，如同 Waters 的证明[11]，只考虑一个充分条件 $F(I)\neq0\bmod p$。d_I 是身份 I 的一个有效私钥，令 $r'=r-\frac{a}{F(I)}$，则有 $d_{I,2}=g_1^{-\frac{1}{F(I)}}g^r=g^{r'}$ 和

$$d_{I,1}=g_1^{-\frac{J(I)}{F(I)}}(g_2^{F(I)}g^{J(I)})^r$$
$$=g_2^a(g_2^{F(I)}g^{J(I)})^{\frac{-a}{F(I)}}(g_2^{F(I)}g^{J(I)})^r$$
$$=g_2^a(g_2^{F(I)}g^{J(I)})^{r-\frac{a}{F(I)}}=g_2^a(g_2^{F(I)}g^{J(I)})^{r'}\tag{4}$$

签名询问：对于身份列表 $R=\{I_1,I_2,\cdots,I_n\}$ 中的身份 I_j 关于消息 M 的签名询问，$\mathcal{C}$ 计算 $m=H_m(R,\ M)$。记 $K=\{k\mid F(I_k)\neq 0 \bmod l\}$，$\mathcal{C}$ 随机选择 $\pi\in K$，则 $\mathcal{C}$ 执行 I_π 私钥提取询问构造私钥，然后运行签名算法生成 R 对 M 的签名。如果 $K=\phi$，$\mathcal{C}$ 放弃游戏。

伪造：如果上述询问中，$\mathcal{C}$ 未放弃游戏，则 $\mathcal{A}$ 以至少 ε 的概率返回身份列表 $R^*=\{I_1^*,\ I_2^*,\ \cdots,\ I_n^*\}$，消息 M^* 和伪造签名 $\sigma^*=(S^*,\ R_1^*,\ R_2^*,\ \cdots,\ R_n^*)$。如果 $F(I_j^*)\neq 0 \bmod p\ (j=1,\ 2,\ \cdots,\ n)$，$\mathcal{C}$ 放弃游戏，否则 $\mathcal{C}$ 计算：

$$\frac{S^*}{(R_1^*)^{J(I_1^*)}\cdots(R_n^*)^{J(I_n^*)}}=\frac{\left(g_2^a\left(u'\prod_{i\in\mathcal{U}_\pi^*}u_i\right)^{r_\pi'}\right)^{m^*}\prod_{j=1}^{n}\left(u'\prod_{i\in\mathcal{U}_j^*}u_i\right)^{r_j}}{g^{J(I_1^*)r_1}\cdots g^{J(I_\pi^*)(r_\pi'm^*+r_\pi)}\cdots g^{J(I_n^*)r_n}}=(g^{ab})^{m^*}\quad(5)$$

因为已知 $m^*=H_m(R^*,\ M^*)$，所以 $\mathcal{C}$ 计算得出 $g^{ab}=(g^{abm^*})^{1/m^*}$。

概率分析：通过分析 $\mathcal{C}$ 不放弃游戏的概率来评估 $\mathcal{C}$ 模拟成功的概率。模拟不中断需要满足 3 个条件：(1)在私钥提取询问中 $F(I)\neq 0 \bmod l$；(2)在签名询问中 $F(I_k)\neq 0 \bmod l$；(3) $F(I_j^*)=0 \bmod p\ (j=1,2,\cdots,n)$。与文献[12, 13]相似，如果敌手 $\mathcal{A}$ 攻击伪造的概率为 ε，则 $\mathcal{C}$ 解决计算性 Diffie-Hellman 问题的概率为 $\varepsilon'\geq\dfrac{\varepsilon}{2^{n+1}(q_E+q_S)^n(n_u+1)^n}$。

时间复杂度计算：算法 $\mathcal{C}$ 的运行时间是敌手 $\mathcal{A}$ 的时间加上应答 q_E 次私钥提取询问和 q_S 次签名询问的时间。每次私钥提取询问需要执行 4 次指数运算和至多 n_u+2 次乘法运算，每次签名询问需要执行至多 $2n+3$ 次指数运算和至多 $(n_u+1)n+2$ 乘法运算。所以 $\mathcal{C}$ 的时间复杂度为 $t+(4q_E+(2n+3)q_S)\tau+((n_u+2)q_E+((n_u+1)n+2)q_S)\rho$。 证毕

4.3 性能分析

新方案的签名长度与环的成员数 n 成线性关系，为 $n+1$ 个群 G 元素，签名验证需要 $n+1$ 个双线性对运算($e(g_1,\ g_2)$ 可以预计算)和群 G_T 上的 1 个指数运算，公开参数包含 n_u+4 个群 G 元素。n_u 表示身份的比特数，是抗碰撞 Hash 函数的输出，一般至少是 160。椭圆曲线上一个群元素的长度至少是 1024 bit，才能等同 1024 bit RSA 的安全级别。因此每个参与者至少存储公开参数为 164 kbyte。

文献[12]中方案的签名长度为 $n+2$ 个群元素，签名验证需要 $n+2$ 个双线性对运算，公开参数包含 n_u+n_m+5 个群 G 元素(n_m 表示消息的比特数)，亦即每个参与者至少存储公开参数 325 kbyte。

与文献[13]方案相比，虽然增加了一个指数运算，但是文献[13]方案不能够抵抗伪造攻击，即利用已知消息的签名能够伪造任何消息的有效环签名。设已知身份列表 R 在消息 M 上的签名 $\sigma=(S,R_1,R_2,\cdots,R_n)$，不妨设实际签名者为 I_π，私钥 $d_\pi=(g_2^\alpha(U_\pi)^{r_\pi'},\ g^{r_\pi'})$(当然敌手不知道)。现在可以对任何消息伪造签名，并且能通过验证，方法如下：消息 $M'\neq M$，身份列表 R，计算 $m'=H_m(R,M')$，随机选取 $t'\in Z_p$，计算

$$\begin{aligned}\sigma'&=\left(S(U_\pi)^{\frac{1}{t'+m'}},R_1,R_2,\cdots,R_\pi g^{\frac{1}{t'+m'}},\cdots,R_n\right)\\&=\left(g_2^\alpha(U_\pi)^{r_\pi'+\frac{1}{t+m}+\frac{1}{t'+m'}}\prod_{j=1}^{n}(U_j)^{r_j},\ g^{r_1},g^{r_2},\cdots,g^{r_{\pi-1}},\right.\\&\qquad\left.g^{r_\pi+r_\pi'+\frac{1}{t+m}+\frac{1}{t'+m'}},\cdots,g^{r_n}\right)\end{aligned}\quad(6)$$

记 $\sigma'=(S',R_1',R_2',\cdots,R_n')$，显然等式 $e(S',g)=e(g_1,g_2)\cdot\prod_{j=1}^{n}e(U_j,\ R_j')$ 成立，即身份列表 R 对 M' 的有效环签名是 $\sigma'=(S',R_1',R_2',\cdots,R_n')$。实际上，攻击身份 I_π 可以是任选的。所以文献[13]方案是不安全的。

综上所述，考虑签名的计算代价和通信代价均与环成员数成线性关系，而且双线性对自身相对较大的运算量，新方案在计算量和通信量上优于文献[12]方案，在安全上优于文献[13]方案，是有一定意义的。

5 结论

本文提出了一个新的基于身份的环签名方案，在标准模型下基于计算性 Diffie-Hellman 困难假设是存在性不可伪造的，且具有无条件匿名性。与现有标准模型下基于身份的环签名方案相比，新方案无论在计算量上，还是在安全性上都有较大改善，具有一定优势。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes[C]. Crypto1984, 1984, LNCS 196: 47–53.

[2] Boneh D and Franklin M. Identity-based encryption from the Weil pairings[C]. Crypto2001, 2001, LNCS 2139: 213–229.

[3] Wang L L, Zhang G Y, and Ma C G. A survey of ring signature[J]. *Frontiers of Electrical and Electronic Engineering in China*, 2008, 3(1): 10–19.

[4] Zhang F and Kim K. ID-based blind signature and ring

signature from pairings[C]. Asiacrypt2002, 2002, LNCS 2501: 533–547.

[5] Xu J, Zhang Z F, and Feng D G. A ring signature scheme using bilinear pairings[C]. WISA2004, 2004, LNCS 3325: 163–172.

[6] Chow S S M, Yiu S M, and Hui L C K. Efficient identity based ring signature[C]. ACNS2005, 2005, LNCS 3531: 499–512.

[7] Chow S S M, Lui R W C, and Hui L C K, *et al.*. Identity based ring signature: why, how and what next[C]. EuroPKI2005, 2005, LNCS 3545: 144–161.

[8] 王玲玲, 张国印, 马春光. 一种签名长度固定的基于身份的环签名方案[J]. 电子与信息学报, 2007, 29(11): 2645–2648.
Wang L L, Zhang G Y, and Ma C G. An identity-based ring signature scheme with constant-size signature[J]. *Journal of Electronics & Information Technology*, 2007, 29(11): 2465–2468.

[9] 王化群, 张力军, 赵君喜. 两种环签名方案的安全性分析及其改进[J]. 电子与信息学报, 2007, 29(1): 201–204.
Wang Hua-qun, Zhang Li-jun, and Zhao Jun-xi. Cryptanalysis and improvement of two ring signature schemes[J]. *Journal of Electronics & Information Technology*, 2007, 29(1): 201–204.

[10] Canetti R, Goldreich O, and Halevi S. The random oracle methodology, revisited[J]. *Journal of the ACM*, 2004, 51(4): 557–594.

[11] Waters B. Efficient identity-based encryption without random oracles[C]. Eurocrypt2005, 2005, LNCS 3494: 114–127.

[12] Au M H, Liu J K, and Yuen T H, *et al.*. ID-based ring signature scheme secure in the standard model[C]. IWSEC 2006, 2006, LNCS 4266: 1–16.

[13] 张跃宇, 李晖, 王育民. 标准模型下基于身份的环签名方案[J]. 通信学报, 2008, 29(4): 40–44.
Zhang Yue-yu, Li Hui, and Wang Yu-min. Identity-based ring signature scheme under standard model[J]. *Journal of Communications*, 2008, 29(4): 40–44.

刘振华：男，1978 年生，博士生，研究方向为现代密码学、信息安全.

胡予濮：男，1955 年生，博士，教授，博士生导师，研究方向为密码学、网络与信息安全.

牟宁波：男，1982 年生，博士生，研究方向为现代密码学、信息安全.