# 利用三次剩余构造的基于身份的环签名方案

王 峰[1]，林昌露[2]

(1. 福建工程学院数理系 福州 350108; 2. 福建师范大学数学与计算机科学学院 福州 350108)

【摘要】基于身份的环签名不仅可以保护签名者的隐私，而且简化了密钥管理过程，在Ad-hoc网络等领域有着广泛的应用。而大部分基于身份的环签名方案都是利用计算代价昂贵的双线性对构造的。该文利用三次剩余构造了一个基于身份的环签名方案，并利用随机预言模型证明了该方案在大整数分解困难问题假设前提下是适应性选择身份和消息攻击下不可伪造的。该方法为构造基于身份的环签名提供了新的数学工具，扩展了研究空间。

关 键 词 三次剩余; 基于身份签名; 可证明安全; 随机预言模型; 环签名

中图分类号 O29 文献标志码 A doi:10.3969/j.issn.1001-0548.2013.05.026

# Identity-Based Ring Signature Scheme Based on Cubic Residues

WANG Feng[1] and LIN Chang-lu[2]

(1. Department of Mathematics and Physics, Fujian University of Technology Fuzhou 350108;
2. School of Mathematics and Computer Science, Fujian Normal University Fuzhou 350108)

**Abstract** Identity-based ring signature has wide applications such as ad-hoc networks etc., since it can protect the privacy of signer and simplify the process of key management. However, most of existing schemes are constructed from bilinear pairings. In this paper, we firstly propose a new identity-based ring signature scheme based on cubic residues. Our proposed scheme is secure against existential forgery on the adaptively chosen identity and message attacks under the random oracle model assuming the hardness of factoring. Our work extends the research field of identity-based ring signature due to the new mathematical tools.

**Key words** cubic residue; identity-based signature; provable security; random oracle; ring signature

环签名的概念是由文献[1]提出的，它可以实现签名者的无条件匿名性。环签名在匿名泄漏信息、电子现金或电子投票系统、保护知识产权、Ad-hoc和无线传感器网络、安全多方计算等方面有着广泛的应用[2]。

基于身份的公钥密码学概念是由文献[3]提出的。文献[4]第一次把环签名与基于身份的公钥密码有机的结合起来，利用双线性对构造了第一个基于身份的环签名方案。之后很多基于身份的环签名方案被构造出来，不过大都是利用双线性对构造的[5-6]。文献[7-8]分别提出了一个利用二次剩余构造的基于身份的签名方案和基于身份的环签名方案。文献[9]提出了利用三次剩余构造的基于身份的签名方案。

本文将文献[8]的方案推广到Eisenstein环 $\mathbb{Z}[\omega]$ 中，首次利用三次剩余理论构造出了基于身份的环签名方案，该方案避免了文献[8]的方案在签名和验证时计算是不可行的问题以及证明过程中的一些错误；并在大整数分解困难问题假设前提下，利用随机预言模型证明了所提出的方案是适应性选择消息和身份攻击下存在性不可伪造的。

## 1 三次剩余类

### 1.1 Eisenstein环

**定义 1**[10] 设 $\omega$ 是 $z^2+z+1=0$ 的复数根，集合 $\mathbb{Z}[\omega]=\{a+b\omega \mid a,b\in\mathbb{Z}\}$ 称为Eisenstein环。

**定义 2**[10] 设 $\alpha\in\mathbb{Z}[\omega]$，定义 $N(\alpha)=\alpha\bar{\alpha}$。

**定义 3**[10] $\varepsilon=\pm1,\pm\omega,\pm\omega^2\in\mathbb{Z}[\omega]$ 称为 $\mathbb{Z}[\omega]$ 的单位数；若 $\alpha,\beta\in\mathbb{Z}[\omega]$ 满足 $\alpha=\varepsilon\beta$，则称 $\alpha$、$\beta$ 为相伴数。

**定义 4**[10] 设 $\alpha\in\mathbb{Z}[\omega]$，$N(\alpha)>1$，任何分解式 $\alpha=\alpha_1\alpha_2$，都有 $N(\alpha_1)=1$ 或 $N(\alpha_2)=1$，则称 $\alpha$ 为不可分数。

**定义 5**[10] 设 $R\equiv1\pmod 3$，$R\in\mathbb{Z}$，$a\in\mathbb{Z}_R^*$，若存在 $X\in\mathbb{Z}_R^*$ 使得 $a\equiv X^3 \pmod R$ 成立，则称 $a$ 是

收稿日期：2012－08－25；修回日期：2013－04－16
基金项目：国家自然科学基金(61103247)；福建省教育厅基金(JB11120)；福建省自然科学基金(2011J05147)
作者简介：王峰(1978－)，男，主要从事信息安全方面的研究.

模 $R$ 的三次剩余， $X$ 称为 $a$ 模 $R$ 的立方根。

### 1.2 三次剩余符号

**定义 6**[11] 设 $\alpha,\beta\in\mathbb{Z}[\omega]$，不可分数 $\pi$，$\pi_1,\cdots,\pi_t\in\mathbb{Z}[\omega]$，单位数 $\varepsilon\in\mathbb{Z}[\omega]$，如果映射 $(\cdot/\cdot)_3:\mathbb{Z}[\omega]\times(\mathbb{Z}[\omega]-(1-\omega)\mathbb{Z}[\omega])\to\{0,1,\omega,\omega^2\}$，满足：1) 若 $\pi$ 不是 $1-\omega$ 的相伴数，则 $(\alpha/\pi)_3\equiv\alpha^{(N(\pi)-1)/3}\pmod{\pi}$；2) 若 $\beta=\prod_{i=1}^{t}\pi_i^{k_i}$ (其中 $k_i\in\mathbb{Z}$) 且 $\beta$ 不能被 $(1-\omega)$ 整除，则 $(\alpha/\beta)_3\equiv\prod_{i=1}^{t}(\alpha/\pi_i)_3^{k_i}\pmod{\pi}$；3) $(\alpha/\varepsilon)_3=1$；则称 $(\cdot/\cdot)_3$ 为三次剩余符号。

### 1.3 $\mathbb{Z}[\omega]$ 中三次剩余根的计算

**定理 1**[9] 设 $m,l,R,\gamma,\delta\in\mathbb{N}_+$，$m=3^{\gamma}(3\delta+1)<3^l$，$\alpha$ 是模 $R$ 的三次剩余，若存在 $X\in\mathbb{Z}_R^*$ 满足 $\alpha^m\equiv X^{3^l}\pmod{R}$，则可以容易的计算出 $\alpha$ 模 $R$ 的立方根。

**定理 2**[9] 设素数 $p_1,p_2\in\mathbb{Z}$ 满足 $p_1\neq p_2$ 且 $p_1\equiv p_2\equiv 1(\bmod 3)$，$(p_1-1)(p_2-1)/9\equiv -1(\bmod 3)$，$R=p_1p_2$，$\alpha$ 是模 $R$ 的三次剩余，则 $\alpha$ 模 $R$ 的 $3^l$ 次根 $s\equiv\alpha^{d^l}\pmod{R}$，其中 $d=[(p_1-1)(p_2-1)/9+1]/3$。

### 1.4 因式分解困难性假设

**定义 7**[9] 设 $R=p_1p_2$，其中 $p_1,p_2$ 如定理2所述；$C\equiv -AB^{-1}\pmod{R}$，其中 $\pi_1,\pi_2\in\mathbb{Z}[\omega]$ 为不可分数，$A,B\in\mathbb{Z}$，且满足 $N(\pi_1)=p_1$，$N(\pi_2)=p_2$，$\pi_1\pi_2=A+B\omega$，$\gcd(B,R)=1$；则给定 $R$，$C$，计算 $p_1,p_2$ 满足 $R=p_1p_2$ 是困难的。

### 1.5 利用三次剩余根分解合数

**定理 3**[9] $R,C$ 如定义7所述，若有 $X,Y\in\mathbb{Z}$，$X^3\equiv Y^3\pmod{R}$，$(X/\pi_1\pi_2)_3\neq(Y/\pi_1\pi_2)_3$，则存在 $i\in\{0,1,2\}$ 使得 $\gcd(X-C^iY,R)=p_1$。

## 2 环签名定义及安全模型

### 2.1 环签名的概念

环签名是一种签名者模糊的数字签名。一个签名者要代表一个包含自己的集合(环)$L$对一个消息$m$的进行签名，并确保验证者相信这个消息的签名是环$L$的某个成员签署的有效签名，并可以实现签名者的无条件匿名性，即任何人都无法追踪到签名人的身份。

一个环签名必须满足如下几个安全性要求：

1) 正确性：如果签名者按照正确的环签名步骤对消息进行签名，那么验证者一定把它作为有效的签名接收。

2) 无条件匿名性：若一个环签名方案对任意的验证者$A$，即使他具有无限的计算能力，也不能以大于 $1/n$ 的概率猜出签名者所代表的$n$个环成员的身份；若验证者$A$是环成员，则该概率值不超过 $1/(n-1)$。

3) 不可伪造性：攻击者即使知道他所选择的消息$m$和环$L$的有效签名，他也不能以不可忽略的优势代表一个不包含自己的环成功伪造一个新消息的合法环签名。

### 2.2 环签名的Forking引理

对于一般的环签名方案，设$k$为安全参数，一个输出为 $l=l(k)$ 位的Hash函数$H$，由$n$个成员的环 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$ 生成的环签名为 $\mathrm{Sig}=\{L,m,R_1,R_2,\cdots,R_n,h_1,h_2,\cdots,h_n,\sigma\}$，其中，$R_i,i\in\{1,2,\cdots,n\}$，互不相同，并且 $R_i$ 在签名中出现的概率 $\leqslant 2/2^l$，m为消息，$h_i=H(L,m,R_i)$，$\sigma$ 的值由 $R_1$、$R_2$、…、$R_n$，$h_1$、$h_2$、…、$h_n$ 和$m$决定。

**定理 4**[12] 对于一般的安全参数为$k$的环签名方案。设$A$是输入为群$L$中的每个成员的身份和公共参数，最多可以询问随机预言机$Q$次的多项式时间的图灵机。对于 $L^*\subset L$，假设$A$能够在时间$T$内以不可忽略的概率 $\varepsilon\geqslant 7A_n^Q/2^k$ 生成一个有效的签名 $\{L,m,R_1,R_2,\cdots,R_n,h_1,h_2,\cdots,h_n,\sigma\}$，那么，在时间 $T'\leqslant T$ 内以不可忽略的概率 $\varepsilon'\geqslant\varepsilon^2/66A_n^Q$ 利用$A$生成两个有效的签名 $\{L,m,R_1,R_2,\cdots,R_n,h_1,h_2,\cdots,h_n,\sigma\}$ 和 $\{L,m,R_1,R_2,\cdots,R_n,h_1',h_2',\cdots,h_n',\sigma'\}$，存在 $j\in\{1,2,\cdots,n\}$ 使得 $h_j\neq h_j'$，而对所有的 $i\notin\{1,2,\cdots,n\}\setminus\{j\}$ 都有 $h_i\neq h_i'$。

### 2.3 安全模型

假设攻击者是适应性选择身份和消息的，即攻击者可以对若干身份 $\mathrm{ID}_i$ 进行私钥询问之后，再选择目标身份，并且在攻击者输出伪造签名前，可以进行多次签名询问。攻击者$A$和挑战者$B$之间进行的交互游戏如下：

1) 挑战者$B$运行 $\mathrm{Setup}(k,l)$ 生成PKG的公开参数PM，然后将PM发送给$A$。

2) 攻击者$A$进行如下系列询问：

私钥询问：当收到关于 ID 的私钥询问时，挑战者$B$运行消息 $\mathrm{Extract}(\mathrm{ID}_U,\mathrm{MK},\mathrm{PM})$ 产生与 ID 相对应的私钥 $\mathrm{SK}_{\mathrm{ID}_U}$，然后发送给$A$。

签名询问：当收到关于 ID 在消息$m$的签名询问时，挑战者$B$运行消息 $\mathrm{sign}(m,L,\mathrm{SK}_{\mathrm{ID}_s})$ 得到签名 $\sigma$ 后，将签名 $\sigma$ 发送给$A$。

Hash询问：当收到关于任意输入的Hash询问时，

挑战者$B$计算相应的Hash值后，将该值发送给$A$。

3) $A$最后输出一个对于消息$m$和$n$个用户群的身份$L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$的签名$\sigma$，满足$A$并没有对$L$进行私钥询问且也没有对$(m,L)$进行签名询问。

若$A$输出的签名有效，那么认为$A$在游戏中获胜。$A$获胜的优势定义为$\mathrm{Adv}^{\mathrm{EF}}_{\mathrm{IDRSig},A}(k)=\Pr[$输出的签名有效$]$，EF是存在性伪造，IDRSig是基于身份的环签名方案，$k$是安全参数。

如果没有攻击者能够在至多$q_H$次Hash询问，$q_{sig}$次签名询问的前提下，在时间$t$内，以比$\varepsilon$更大的优势获得胜利，那么该基于身份的环签名方案就被定义为可抵抗选择消息和身份的存在性伪造攻击的$(t,q_H,q_{sig},\varepsilon)$安全方案。

## 3 方案的构造

利用三次剩余的理论构造一个基于身份的环签名方案IDRSig。该方案包括4个子算法：系统初始化算法、密钥生成算法、签名算法和验证算法，记作$\mathrm{IDRSig}=\{\mathrm{Setup},\mathrm{Extract},\mathrm{Sign},\mathrm{Verify}\}$。具体构造如下。

1) 系统初始化算法：$\mathrm{Setup}(k,l)\to\{\mathrm{MK},\mathrm{PM}\}$。

把$k$作为安全参数，$l=l(k)$，算法由私钥生成器PKG执行，具体步骤为：

① 随机生成两个大素数$p_1$、$p_2$，满足$p_1\equiv p_2\equiv 1\pmod 3$，$(p_1-1)(p_2-1)/9\equiv -1\pmod 3$，$2^{k-1}\leqslant(p_1-1)(p_2-1)$和$p_1p_2<2^k$，假设$(p_1-1)/3\equiv -1\pmod 3$，$(p_2-1)/3\equiv 1\pmod 3$；

② 选择两个随机数$\pi_1,\pi_2\in\mathbb{Z}[\omega]$，并且满足$N(\pi_1)=p_1$，$N(\pi_2)=p_2$；

③ 计算$R=p_1p_2$；

④ 令$A+B\omega=\pi_1\pi_2$，$A,B\in\mathbb{Z}$，计算$C\equiv -AB^{-1}\pmod R$，则$(C/p_1)_3=\omega^2$，$(C/p_2)_3=\omega$；

⑤ 随机选择$a\in\mathbb{Z}$，使得$(a/R)_3=\omega$；

⑥ 计算$d=[(p_1-1)(p_2-1)/9+1]/3$；

⑦ 选择两个单向Hash函数：$H_1:\{0,1\}^*\to\mathbb{Z}_R^*$，$H_2:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^l$；

⑧ 输出PKG的主密钥：$\mathrm{MK}=(p_1,p_2,\pi_1,\pi_2,d)$，公开参数$\mathrm{PM}=(R,H_1,H_2,a,C,l)$。

2) 密钥生成算法：$\mathrm{Extract}(\mathrm{ID}_U,\mathrm{MK},\mathrm{PM})\to\mathrm{SK}_{\mathrm{ID}_U}$。

该算法由PKG执行。给定用户$\mathrm{ID}_U$，计算$\mathrm{SK}_{\mathrm{ID}_U}$：

① 计算

$$c_{U,1}=\begin{cases}0 & \text{当}\left(H_1(\mathrm{ID}_U)/R\right)_3=1\\ 1 & \text{当}\left(H_1(\mathrm{ID}_U)/R\right)_3=\omega^2\\ 2 & \text{当}\left(H_1(\mathrm{ID}_U)/R\right)_3=\omega\end{cases}$$

② 计算$PK_{ID_U}\equiv a^{c_{U,1}}\cdot H_1(ID_U)\pmod R$；

③ 计算：

$$c_{U,2}=\begin{cases}0 & \text{当}\left(\mathrm{PK}_{\mathrm{ID}_U}/p_1\right)_3=\left(\mathrm{PK}_{\mathrm{ID}_U}/p_2\right)_3=1\\ 1 & \text{当}\left(\mathrm{PK}_{\mathrm{ID}_U}/p_1\right)_3=\left(\mathrm{PK}_{\mathrm{ID}_U}/p_2\right)_3=\omega^2\\ 2 & \text{当}\left(\mathrm{PK}_{\mathrm{ID}_U}/p_1\right)_3=\left(\mathrm{PK}_{\mathrm{ID}_U}/p_2\right)_3=\omega\end{cases}$$

$H_3(\mathrm{ID}_U)\equiv a^{c_{U,1}}C^{c_{U,2}}H_1(\mathrm{ID}_U)\pmod R$；

④ $\mathrm{SK}_{\mathrm{ID}_U}\equiv(H_3(\mathrm{ID}_U))^{d'}\pmod R$，通过秘密通道将用户$\mathrm{ID}_U$的私钥$\mathrm{SK}_{\mathrm{ID}_U}$发送给用户$\mathrm{ID}_U$。

3) 签名算法：$\mathrm{sign}(m,L,SK_{ID_s})\to\sigma$。

① 令$L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$，对于$L$中每一个$\mathrm{ID}_i$，利用算法Extract中的函数计算$c_{U_i,1}$和$\mathrm{PK}_{\mathrm{ID}_i}$；

② 对于$\mathrm{ID}_i(i\in\{1,2,\cdots n\}\setminus\{s\})$，随机选取$r_i\in\mathbb{Z}_R^*$，计算$R_i\equiv r_i^{3^l}\pmod R$，$h_i=H_2(R_i,m,L)$；

③ 随机选取$r_s\in Z_R^*$，计算$R_s'\equiv r_s^{3^l}\pmod R$，$h_s'=H_2(R_s',m,L)$，$R_s=\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}\prod_{i\neq s}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})^{-1}$；

④ 计算$h_s=H_2(R_s,m,L)$，$V=(SK_{ID_s})^{h_s+h_s'}$；

⑤ 输出签名：$\sigma=(L,m,R_1,R_2,\cdots,R_n,V)$。

4) 验证算法：$\mathrm{Verify}(L,\sigma)\to\{0,1\}$。

① 对于$L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$中每一个$ID_i$，利用算法Extract中的函数计算$c_{U_i,1}$和$\mathrm{PK}_{\mathrm{ID}_i}$；

② 计算$h_i=H_2(R_i,m,L)$；

③ 验证$V^{3^l}=C^t\prod_{i=1}^n(R_i\cdot\mathrm{PK}_{\mathrm{ID}_i}^{h_i})$（其中$t\in\{0,1,2\}$）是否成立，若成立则输出1，即验证者认为签名有效，否则输出0，签名无效。

## 4 方案的正确性

根据下面的式子可以看出，如果签名者是诚实的，则他的签名可以通过验证算法。

$$V^{3^l}=((\mathrm{SK}_{\mathrm{ID}_s})^{h_s+h_s'})^{3^l}=$$

$$H_3(\mathrm{ID}_s)^{h_s}H_3(\mathrm{ID}_s)^{h_s'}=$$

$$C^{c_{s2}(h_s+h_s')}\mathrm{PK}_{\mathrm{ID}_s}^{h_s}\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}=$$

$$C^{c_{s2}(h_s+h_s')}\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}\prod_{i\neq s}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})^{-1}\times$$

$$\prod_{i\neq s}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})\mathrm{PK}_{\mathrm{ID}_s}^{h_s}=$$

$$C^{c_{s2}(h_s+h_s')}R_s\prod_{i\neq s}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})\mathrm{PK}_{\mathrm{ID}_s}^{h_s}=$$

$$C^{c_{s2}(h_s+h_s')}\prod_{i=1}^{n}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})=$$
$$C^{t}\prod_{i=1}^{n}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})$$

其中，$t\in\{0,1,2\}$。

由此可见，该验证算法是正确的。

## 5　方案的无条件匿名性

**定理 5**　方案 IDRSig 满足签名者无条件匿名性。

证明：由于 $r_1,r_2,\cdots,r_n$ 是随机生成，因而 $R_1,R_2,\cdots,R_n$ 是一致分布的，其中 $R_i=r_i^{3^l}\pmod R$，$(i\neq s)$；$R_s'=r_s^{3^l}\pmod R$，$h_s'=H_2(R_s',m,L)$，$R_s=\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}\prod_{i\neq s}(R_i\cdot\mathrm{PK}_{\mathrm{ID}_i}^{h_i})^{-1}$。

再考查 $V=(\mathrm{SK}_{\mathrm{ID}_s})^{h_s+h_s'}$ 是否会泄漏签名者的信息。由于 $\mathrm{SK}_{\mathrm{ID}_s}^{h_s'}=V(\mathrm{SK}_{\mathrm{ID}_s}^{h_s})^{-1}$，其中 $h_s=H_2(R_s,m,L)$，$\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}=R_s\prod_{i\neq s}(R_i\cdot\mathrm{PK}_{\mathrm{ID}_i}^{h_i})$ 可以公开计算，因而任何人都可以通过计算 $(\mathrm{SK}_{\mathrm{ID}_s}^{h_s'})^{3^l}=C^{c_{s2}h_s'}\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}=C^t\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}$ 把 $\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}$ 和 $\mathrm{SK}_{\mathrm{ID}_s}^{h_s'}$ 关联起来，其中 $t\in\{0,1,2\}$。利用等式 $R_j\prod_{i\neq j}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})=C^tV^{3^l}\ (H_{\mathrm{ID}_j}^{h_j})^{-1}$ 是否成立找出签名者是无效的。这是因为无论 $j=s$ 还是 $j\in\{1,2,\cdots,n\}\setminus\{s\}$，签名都是对称的，上述的等式实际上和验证算法一样。

$$R_j\prod_{i\neq j}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})=$$
$$\prod_{i\neq s}R_iR_s\prod_{i\neq j}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})=$$
$$\prod_{i\neq s}R_i\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}\prod_{i\neq s}(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})^{-1}\prod_{i\neq j}\mathrm{PK}_{\mathrm{ID}_i}^{h_i}=$$
$$\mathrm{PK}_{\mathrm{ID}_s}^{h_s'}\mathrm{PK}_{\mathrm{ID}_s}^{h_s}(\mathrm{PK}_{\mathrm{ID}_j}^{h_j})^{-1}=$$
$$C^{c_{s2}h_s'}(\mathrm{SK}_{\mathrm{ID}_s}^{3^l})^{h_s+h_s'}(\mathrm{PK}_{\mathrm{ID}_j}^{h_j})^{-1}=$$
$$C^{t}(\mathrm{SK}_{\mathrm{ID}_s}^{3^l})^{h_s+h_s'}(\mathrm{PK}_{\mathrm{ID}_j}^{h_j})^{-1}=$$
$$C^tV^{3^l}(\mathrm{PK}_{\mathrm{ID}_j}^{h_j})^{-1}$$

对任意的一个消息 $m$ 和环 $L$，分布 $R_1,R_2,\cdots,R_n$，无论谁是签名者，$V$ 都是独立的且均匀分布，因而对于任何即使有无限计算能力的敌手 $A$，都没有任何比猜测更高的优势判断出签名者。

## 6　方案的不可伪造性

**定理 6**　对于方案 IDRSig，在随机预言模型下，如果算法 $A$ 在多项式时间 $T_A$ 内，最多经过 $q_S$ 次签名询问，$q_{H_1}$ 次 $H_1$ 询问，$q_{H_2}$ 次 $H_2$ 询问，$q_E$ 次私钥询问，能够以不可忽略的概率 $\varepsilon_A$ 生成一个由 $n$ 个群成员的有效签名，那么因式分解问题可以在多项式时间 $2(T_A+T_{q_{H_1}}+T_{q_{H_2}}+nT_{q_S})$ 内以不可忽略的概率 $(1-\mu)^{2n+1}\varepsilon_A^2/2700A_n^{q_{H_2}}$ 解决，其中 $(1-\varepsilon_A/12)^{1/q_E}\leqslant\mu<1$。

证明：采用归约的方法证明。假设方案 IDRSig 不安全，即定义的攻击模型下，存在一个攻击者 $A$，可以以不可忽略的概率优势 $\varepsilon_A$ 攻击方案 IDRSig (假设 $\varepsilon_A\geqslant(12A_{q_{H_2}}^n+6(q_{H_2}+q_S)^2)/((1-\mu)^n2^k)$，其中 $k$ 是安全参数；否则，$\varepsilon_A$ 在安全参数 $k$ 下是可忽略的)，那么可以构造算法 $B$ 来有效地解决整数分解问题。然而这与定义7中整数分解困难相矛盾，所以假设不成立，即方案 IDRSig 是安全的。

算法 $B$ 的构造：$B$ 的任务是解决一个整数分解问题的实例，即给定一个输入 $R=p_1\cdot p_2$ ($B$ 不知道 $p_1$ 和 $p_2$) 和 $C$ (如定义7所述)，以不可忽略的概率优势输出 $p_1$、$p_2$。其中 $p_1,p_2$ 满足 $p_1\equiv p_2\equiv1(\mathrm{mod}\ 3)$，$(p_1-1)(p_2-1)/9\equiv-1(\mathrm{mod}\ 3)$，$2^{k-1}\leqslant(p_1-1)(p_2-1)$，$p_1p_2<2^k$，假设 $(p_1-1)/3\equiv-1(\mathrm{mod}\ 3)$，$(p_2-1)/3\equiv1(\mathrm{mod}\ 3)$。

$B$ 按照如下的操作模拟攻击模型中的游戏与 $A$ 交互。

1) $B$ 随机选取 $a\in\mathbb{Z}_R^*$ 满足 $(a/R)_3=\omega$，选择安全参数 $k\in\mathbb{Z}$，$l=l(k)$，把 $(R,a,C,l)$ 作为公开参数发送给 $A$。

2) 然后 $B$ 回答 $A$ 的一系列询问如下：

$H_1$-询问：不失一般性，假设 $A$ 在进行密钥询问之前先进行 $H_1$-询问。为了响应 $A$ 的 $H_1$-询问，$B$ 维护了一个 $H_1$ 列表 $\mathrm{TAB}_{H_1}$，表中的每项为六元组 $<\mathrm{ID}_i,H_1(\mathrm{ID}_i),s_i,c_{i1},c_{i2},W>$，其中 $\mathrm{ID}_i$ 是被询问的身份，$H_1(\mathrm{ID}_i)$ 是 $B$ 的回答，$s_i,c_{i1},c_{i2},W$ 是内部参数。当 $A$ 对身份 $\mathrm{ID}_i$ 进行询问时，如果列表 $\mathrm{TAB}_{H_1}$ 中已含有项 $<\mathrm{ID}_i,H_1(\mathrm{ID}_i),s_i,c_{i1},c_{i2},W>$，那么 $B$ 将 $H_1(\mathrm{ID}_i)$ 作为值返回。否则 $B$ 随机选择 $s_i\in\mathbb{Z}_R^*$ 且 $s_i$ 不在列表 $\mathrm{TAB}_{H_1}$ 中；随机选择 $(c_{i1},c_{i2})\in\{0,1,2\}^2$；选择 $W\in\{0,1\}$ 满足 $\Pr\{W=0\}=\mu$，$\Pr\{W=1\}=1-\mu$；若 $W=0$ 则 $H_1(ID_i)=s_i^{3^l}/(a^{c_{i1}}C^{c_{i2}})$，否则 $H_1(ID_i)$ 取随机数值，然后在表中加入新的项 $<ID_i,H_1(ID_i),s_i,c_{i1},c_{i2},W>$，返回 $H_1(ID_i)$。

私钥询问：当收到 **A** 关于 $ID_i$ 的私钥询问时，$B$ 首先在列表 $\mathrm{TAB}_{H_1}$ 中搜索 $\mathrm{ID}_i$。如果 $W=0$，则返回 $\mathrm{SK}_{\mathrm{ID}_i}=s_i$ 给 $A$，否则 $B$ 不回答并停止。显然 $B$ 停止的概率不超过 $1-\mu^{q_E}\leqslant\varepsilon_A/12$。

$H_2$-询问：为了响应 $A$ 的 $H_2$-询问，$B$ 维护了一

个 $H_2$ 列表 $\mathrm{TAB}_{H_2}$。表中的每项是四元组 $<R_i,m,L,H_2>$，其中 $(R_i,m,L)$ 是被询问的信息，$H_2$ 是$B$的回答。当$A$对 $(R_i,m,L)$ 进行询问时，如果列表 $\mathrm{TAB}_{H_2}$ 中已含有项 $<R_i,m,L,H_2>$，那么$B$将 $H_2$ 的值返回，否则，$B$选择一个随机数 $H_2\in\{0,1\}^l$，并将 $H_2$ 的值返回，然后在列表 $TAB_{H_2}$ 中加入新的项 $<R_i,m,L,H_2>$。

签名询问：当$B$收到$A$要求 $m$ 在$n$个用户群的身份 $L=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$ 的签名询问时(不妨假设$A$没有对 $L$ 的任一成员进行私钥询问，否则，$A$可以自己生成一个有效的签名)，$B$执行如下操作：

① $B$首先在列表 $\mathrm{TAB}_{H_1}$ 中找到包含 $\mathrm{ID}_i$ 项，并计算 $\mathrm{PK}_{ID_i}\equiv a^{c_{i1}}\cdot H_1(\mathrm{ID}_i)(\mathrm{mod}\ R)$，若在列表 $\mathrm{TAB}_{H_1}$ 中找不到包含 $\mathrm{ID}_i$ 项，则按照 $\mathrm{TAB}_{H_1}$ 的构造方法可得到包含 $\mathrm{ID}_i$ 的项，然后计算 $\mathrm{PK}_{\mathrm{ID}_i}\equiv a^{c_{i1}}\cdot H_1(ID_i)\times(\mathrm{mod}\ R)$；

② 随机选择 $s\in\{1,2,\cdots,n\}$，对于 $\mathrm{ID}_i(i\in\{1,2,\cdots,n\}\backslash\{s\})$，随机选取 $r_i\in\mathbb{Z}_R^*$，计算 $R_i\equiv r_i^{3^l}(\mathrm{mod}\ R)$，在列表 $\mathrm{TAB}_{H_2}$ 中询问 $h_i=H_2(R_i,m,L)$，若在列表 $\mathrm{TAB}_{H_2}$ 中找不到包含 $h_i=H_2(R_i,m,L)$ 项，则按照 $\mathrm{TAB}_{H_2}$ 的构造方法可得包含 $h_i=H_2(R_i,m,L)$ 的项；

③ 随机选择 $h_s\in\{0,1\}^l$，$V\in\mathbb{Z}_R^*$，$t\in\{0,1\ \ ,2\}$，计算 $R_s=V^{3^l}\cdot C^{-t}\cdot\prod_{i\neq s}(R_i\cdot\mathrm{PK}_{\mathrm{ID}_i}^{h_i})^{-1}\cdot(\mathrm{PK}_{\mathrm{ID}_s}^{h_s})^{-1}$；

④ 如果 $R_s$ 已经在列表 $\mathrm{TAB}_{H_2}$ 中出现，$B$终止游戏，否则，$B$返回 $\sigma=(L,m,\bigcup_{i=1}^n R_i,V)$ 作为签名，并将 $<R_s,m,L,h_s>$ 添加到列表 $\mathrm{TAB}_{H_2}$ 中。

由于本文假设 $R_i$ 在签名中出现的概率 $\leqslant 2/2^l$，故$B$终止游戏的概率 $\leqslant q_{H_2}\cdot q_S\cdot(2/2^l)\leqslant\varepsilon_A/6$；而第二次模拟环签名由于与前次模拟具有相同的输出 $(R_s,m,L)$ 造成$B$终止游戏的概率 $\leqslant(q_s^2/2)\cdot(2/2^l)\leqslant\varepsilon_A/6$；因而$B$在签名询问中终止游戏的概率 $\leqslant\varepsilon_A/3$。加上$B$在私钥询问时终止游戏的概率 $\leqslant\varepsilon_A/12$，$B$终止游戏的概率 $\leqslant 5\varepsilon_A/12$。$B$得到一个有效的环签名的概率 $\tilde{\varepsilon}_B=\Pr[$ $B$得到一个有效的签名]=Pr[$B$没有终止游戏并且$A$成功] $\geqslant\Pr[$ $A$成功|$B$没有终止游戏] $-\Pr[$ $B$终止游戏] $\geqslant\varepsilon_A-5\varepsilon_A/12=7\varepsilon_A/12$。

假定$A$在$B$不知 $L$ 的任何成员的私钥情况下(否则，$B$可以自己伪造签名)提供给 $(L,m)$ 一个有效签名，该情况发生的概率是 $(1-\mu)^n$。因而$B$在不知 $L$ 的任何成员的私钥情况下，在时间 $T_B\leqslant T_A+T_{q_{H_1}}+T_{q_{H_2}}+nT_{q_S}$ 内，以概率 $\varepsilon_B=(1-\mu)^n\tilde{\varepsilon}_B\geqslant(1-\mu)^n 7\varepsilon_A/12\geqslant 7A_n^{q_{H_2}}/2^k$ 伪造 $(L,m)$ 一个有效签名。

应用定理4，$B$可以在时间 $T'\leqslant 2T_B$ 内以不可忽略的概率 $\tilde{\varepsilon}'\geqslant\varepsilon_B^2/66A_n^Q$ 通过执行两次$A$生成两个有效的签名 $\{L,m,R_1,R_2,\cdots,R_n,h_1,h_2,\cdots,h_n,\sigma\}$ 和 $\{L,m,R_1,R_2,\cdots,R_n,h_1',h_2',\cdots,h_n',\sigma'\}$，其中存在 $j\in\{1,2,\cdots,n\}$ 使得 $h_j\neq h_j'$ 而对所有的 $i\notin\{1,2,\cdots,n\}\backslash\{j\}$ 都有 $h_i\neq h_i'$。则有 $V^{3^l}=C^t\prod_{i=1}^n(R_i\mathrm{PK}_{\mathrm{ID}_i}^{h_i})$，$V'^{3^l}=C^{t'}\prod_{i=1}^n(R_i\ \mathrm{PK}_{\mathrm{ID}_i}^{h_i'})$，故有 $(V/V')^{3^l}\equiv C^{t-t'}\cdot\mathrm{PK}_{\mathrm{ID}_j}^{h_j-h_j'}(\mathrm{mod}\ R)$，其中，$t,t'\in\{0,1,2\}$。

$B$ 询问列表 $\mathrm{TAB}_{H_1}$ 找到 $<\mathrm{ID}_j,H_1(\mathrm{ID}_j),s_j,c_{j1},c_{j2},W>$，$W$ 以概率 $1-\mu$ 使得 $H_1(\mathrm{ID}_i)=s_i^{3^l}/(a^{c_{i1}}C^{c_{i2}})$，才有 $C^{c_{i2}}\cdot\mathrm{PK}_{\mathrm{ID}_i}\equiv SK_{ID_i}^{3^l}(\mathrm{mod}\ R)$。

当 $t=t'$ 时，若 $\exists\gamma,\delta\in\mathbb{N}_+$，使得 $h_j-h_{j'}=3^\gamma(3\delta+1)$，则利用定理1可以容易地计算 $\mathrm{PK}_{\mathrm{ID}_j}$ 模 $R$ 的立方根 $s_j'$，否则，计算失败。由于 $h_j$ 都是随机选取的，故 $\Pr[t=t']=1/3$，$\Pr[\exists\gamma,\delta\in\mathbb{N}_+$，使得 $h_j-h_{j'}=3^\gamma(3\delta+1)]=1/3$。

若 $(X/\pi_1\pi_2)_3\neq(Y/\pi_1\pi_2)_3$，$B$可以利用定理3分解 $R$。由于列表 $\mathrm{TAB}_{H_1}$ 中 $s_j$ 是随机选取的，故 $\Pr[(X/\pi_1\pi_2)_3\neq(Y/\pi_1\pi_2)_3]=2/3$。

总之，本文可以在多项式时间 $T'\leqslant 2T_B\leqslant 2(T_A+T_{q_{H_1}}+T_{q_{H_2}}+nT_{q_S})$ 内以概率

$$\varepsilon'\geqslant(1/3)\cdot(1/3)\cdot(2/3)(1-\mu)\tilde{\varepsilon}'\geqslant$$
$$(2/27)(1-\mu)\varepsilon_B^2/66A_n^Q\geqslant$$
$$(2/27)(1-\mu)((1-\mu)^n 7\varepsilon_A/12)^2/66A_n^Q\geqslant$$
$$(1-\mu)^{2n+1}\varepsilon_A^2/2\ 700A_n^{q_{H_2}}$$

解决因式分解问题。

## 7 性能分析

表1为几种方案的性能比较。这几种方案的安全性都是在随机预言模型下被证明是安全的。本文的方案首次提出了利用三次剩余构造的基于身份的环签名方案，与文献[6]相比，避免了双线性对的较为复杂的运算，提高了签名验证的效率。同时，该方案将文献[8]中的方案推广到Eisenstein环 $\mathbb{Z}[\omega]$ 中。由于文献[8]的方案在签名和验证算法中都要用到在不知$N$的分解的情况下判定模$N$的二次剩余问题，在计

算上不可行，本文提出的方案避免了该问题，也避免了文献[8]方案中存在性不可伪造证明中的一些错误。

**表1　几种方案的性能分析**

| 方案 | 安全性 | 数学问题 | 困难性假设 |
|---|---|---|---|
| 本文的方案 | 随机预言模型下可证明安全 | 三次剩余 | 大整数分解问题 |
| 文献[6]的方案 | 随机预言模型下可证明安全 | 双线性对 | 计算Diffle-Hellman问题 |
| 文献[8]的方案 | 随机预言模型下可证明安全 | 二次剩余 | 大整数分解问题 |

## 8　总　结

本文利用三次剩余构造了一个无需双线性对实现的基于身份的环签名方案。在大整数分解困难问题假设前提下，该方案在随机预言模型下被证明是适应性选择身份和消息攻击下不可伪造的。如何构造在标准模型下利用三次剩余构造安全的基于身份的环签名仍是一个公开问题。

## 参　考　文　献


[1] RIVEST R, SHAMIR A, TAUMAN Y. How to leak a secret[C]//Advances in Cryptology - ASIACRYPT ’01, LNCS 2248. Berlin: Springer-Verlag, 2001: 552-565.

[2] 吴磊. 基于身份环签名的研究[D]. 济南: 山东大学, 2009．
WU Lei. Research on ID-based ring signature[D]. Jinan: Shandong University, 2009.

[3] SHAMIR A. Identity based cryptosystems and signature schemes[C]//Advances in Cryptology-CRYPTO ’84, LNCS 196. Berlin: Springer-Verlag, 1984: 47-53.

[4] ZHANG Fang-guo, KIM K. ID-based blind signature and ring signature from pairings[C]//Advances in Cryptology-ASIACRYPT’02, LNCS 2501. Berlin: Springer-Verlag, 2002: 533-547.

[5] HERRANZ J, SAEZ G. New identity based ring signature schemes[C]//Proceedings of the 6th International Conference-ICICS’04 LNCS 3269. Berlin: Springer-Verlag, 2004: 27-39.

[6] ZHUN Li-jun, ZHANG Fu-tai. Efficient ID-based ring signature and ring signcryption schemes[C]//International Conference on Computational Intelligence and Security, CIS'08. [S.l.]: [s.n.], 2008.

[7] 柴震川, 董晓蕾, 曹珍富. 利用二次剩余构造的基于身份的数字签名方案[J]. 中国科学F辑, 2009, 39(2): 199-204.
CAI Zhen-chuan, DONG Xiao-lei, CAO Zhen-fu. Identity based signature scheme based on quadratic residues[J]. Science in China Series F: Information Sciences, 2009, 39(2): 199-204.

[8] XIONG Hu, QIN Zhi-guang, LI Fa-gen. Identity-based ring signature scheme based on quadratic residues[J]. High Technology Letters, 2009, 15(1): 94-100.

[9] XING Dong-sheng, CAO Zhen-fu, DONG Xiao-lei. Identity based signature scheme based on cubic residues[J]. Science in China Series F: Information Sciences, 2011, 54(10): 2001-2012.

[10] 柯召, 孙琦. 数论讲义[M]. 第2版. 北京: 高等教育出版社, 2001．
KE Shao, SUN Qi. Lectures on number theory[M]. 2nd ed. Beijin: Higher Education Press, 2001.

[11] DAMGARD I B, FRANDSEN G S. Efficient algorithms for GCD and cubic residuosity in the ring of eisenstein integers[J]. Journal of Symbolic Computation, 2005(39): 643-652.

[12] HERRANZ J, SAEZ G. Forking lemmas for ring signature schemes[C]//Proceedings of INDOCRYPT’03, LNCS 2904. Berlin: Springer-Verlag, 2003: 266-279.


编　辑　税　红