第 39 卷 第 12 期
Vol.39 No.12

计 算 机 工 程
Computer Engineering

2013 年 12 月
December 2013

• 安全技术 •

文章编号：1000—3428(2013)12—0111—07 文献标识码：A 中图分类号：TP309.7

利用三次剩余构造的基于身份环签名方案

郭 浩，董晓蕾，曹珍富

(上海交通大学计算机科学与工程系，上海 200240)

摘 要：传统的基于身份环签名方案大多采用双线性配对实现，但配对方法的运算复杂度较高，会大幅降低签名方案的效率。为此，提出一种非配对的环签名方案。给出用于有效计算三次剩余 3^l 次根的算法，在该算法的基础上生成签名密钥，并结合三次剩余理论构造基于身份的环签名方案。分析结果表明，在大整数分解困难问题的假设前提下，该方案在随机预言模型下被证明是选择消息和身份安全的。同时，该方案也满足签名者无条件匿名性。

关键词：基于身份签名；环签名；三次剩余；大整数分解；随机预言模型；可证安全

Identity-based Ring Signature Scheme Constructed by Cubic Residues

GUO Hao, DONG Xiao-lei, CAO Zhen-fu

(Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

【Abstract】 Most identity-based schemes are based on the bilinear pairing, which has a high computational complexity and seriously reduces the efficiency of the cryptographic schemes. Aiming at this problem, this paper proposes a ring signature scheme without paring. By introducing a new technique of how to calculate the 3^lth root of a cubic residue in Eisenstein ring, which is applied to calculate ring signature keys as well, a new identity-based ring signature scheme is proposed based on cubic residues. This scheme is formally proved that it is chosen message and identity secure in the random oracle model, assuming the hardness of factoring. The proposed scheme is also been proved to meet the signer unconditional anonymity.

【Key words】 Identity-based Signature(IBS); ring signature; cubic residues; integer factorization; random oracle model; proven security

DOI: 10.3969/j.issn.1000-3428.2013.12.024

1 概述

环签名是 Rivest 等人于 2001 年提出的一种新型匿名签名技术[1]。在环签名的生成过程中，真正的签名者可以任意选取一组成员(包含他自身)作为可能的签名者，用自己的私有密钥和其他成员的公开密钥对文件签名。签名者选取的这组成员称作环，生成的签名称作环签名。签名接收者能证明签名者是来自环中的某一个人但无法确定是哪个。

一个环签名必须满足无条件匿名性和不可伪造性等安全性要求。

(1)无条件匿名性：攻击者即便非法获取了所有可能的签名者的私钥，他能确定出真正签名者的概率不超过 $1/n$，这里 n 为环中成员(可能的签名者)的个数。

(2)不可伪造性：外部攻击者在不知道任何成员的私钥的情况下，即使能从一个生成环签名的预言机得到任何消息 M 的签名，他也不能以不可忽略的优势成功伪造一个新消息的合法签名。

基于身份公钥密码学概念是 Shamir 于 1984 年提出的[2]。在基于身份密码学中，用户选择他们公开的身份信息(如 Email 等)作为公钥，由一个可信任的私钥分发中心(Private Key Generator, PKG)按照这些公开的身份信息为用户计算出相应的私钥，并通过安全渠道分发给用户。因此，在该密码体制下，通信一方只需要知道对方的 E-mail 等公开信息就可以进行加密和签名等密码学操作。但是直到 2001 年，基于身份的加密方案(Identity-based Encryption, IBE)才被实现[3-4]。之后，基于身份的密码体制成为密码学研究的热点，诸多方案被提出。

文献[5]提出了基于二次剩余的身份签名方案，并给出方案安全性的形式化证明；文献[6]给出了第一个基于身份的环签名方案；文献[7]给出了更有效的构造方案；文献[8]指出文献[6]和文献[7]中相冲突的地方；之后文献[9]给出了在匿名子集中构造基于身份环签名的方案；文献[10-11]利用常数配对运算实现环签名方案；文献[12]利用二次剩余构造了基于身份的环签名方案。但国内外在利用三次剩余构

基金项目：国家自然科学基金资助项目(60972034)

作者简介：郭 浩(1989－)，男，硕士研究生，主研方向：密码理论，信息安全；董晓蕾、曹珍富，教授、博士生导师

收稿日期：2012-11-29 **修回日期：**2013-01-01 **E-mail：**guo_hao@live.com

造基于身份的环签名方案方面的研究仍较少。

本文在三次剩余的基础上，设计一个环签名方案的具体方案，并利用环分叉引理和密码学相关证明技巧证明该方案满足相应的安全特性。

2 基本概念和工具

本节对一些数学基本概念、结论和工具进行介绍。

2.1 Eisenstein 环

整数 1 的三次根共有 3 个，分别是 1、$(-1+\sqrt{3}\mathrm{i})/2$ 和 $(-1-\sqrt{3}\mathrm{i})/2$。令 $\omega=(-1+\sqrt{3}\mathrm{i})/2$，复数 ω 满足以下性质：$\omega^3=1$，$\omega^2+\omega+1=0$，$\omega^2=\overline{\omega}$。

Eisenstein 环被定义为如下集合：

$\mathbb{Z}[\omega]=\{a+b\omega \mid a,b\in\mathbb{Z}\}$

(1)长度：对于 $\alpha\in\mathbb{Z}[\omega]$，定义 α 的值乘以其复数共轭，也等于其绝对值的平方，即：$N(\alpha)=\alpha\overline{\alpha}=a^2-ab+b^2, a,b\in\mathbb{Z}$。

用 $N(\alpha)$ 表示 α 的长度。给定一个素数 $p\equiv 1(\mathrm{mod}\,3), p\in\mathbb{Z}$，文献[13]提出了一个有效的算法去寻找不可分数 $\pi\in\mathbb{Z}[\omega]$，满足 $N(\pi)=p$。

(2)单位：$\mathbb{Z}[\omega]$ 中的单位定义为长度为 1 的元素，共有 6 个单位：±1，$\pm\omega$，$\pm\omega^2$。$\mathbb{Z}[\omega]$ 中 2 个元素 α 和 β 是相关的，如果存在单位 ε 使 $\alpha=\varepsilon\beta$ 成立。

(3)原数：如果 $\alpha\in\mathbb{Z}[\omega],\exists\beta\in\mathbb{Z}[\omega]:\alpha=1+3\beta$，则称 $\alpha\in\mathbb{Z}[\omega]$ 为原数或原形式数[14]。

(4)不可分数：Eisenstein 环中的不可分数必然是以下形式之一[15]：

1) $1-\omega$；

2)整数环中满足 $p\equiv 2(\mathrm{mod}\,3)$ 的素数 p；

3) $a+b\omega$ 形式的数，其中，$a\equiv 2(\mathrm{mod}\,3), 3\mid b$，并且 $N(a+b\omega)$ 是整数环中满足 $p\equiv 1(\mathrm{mod}\,3)$ 的素数。

(5)唯一分解：$\forall\beta\in\mathbb{Z}[\omega]:\beta=\varepsilon\prod_{i=1}^{t}\pi_i^{\kappa_i}$。其中，$\pi_i$ $(i=1,2,\cdots,t)$ 是 $\mathbb{Z}[\omega]$ 中的不可分数；ε 是单位[15]。不考虑不可分数 π_i 的顺序，β 的分解是唯一的。

(6)三次剩余：给定满足 $N\equiv 1(\mathrm{mod}\,3)$ 的正整数 N，称正整数 $a\in\mathbb{Z}_N^*$ 是模 N 的三次剩余，当且仅当存在整数 x，使得 $a\equiv x^3(\mathrm{mod}\,N)$。

2.2 三次剩余符号

如果 $\alpha\in\mathbb{Z}[\omega]$，$\pi$ 是 $\mathbb{Z}[\omega]$ 中的不可分数，那么 $\alpha^{(N(\pi)-1)/3}\equiv\omega^{\lambda}(\mathrm{mod}\,\pi)$，其中，$\lambda\in\{0,1,2\}$[13]。

Eisenstein 环上的三次剩余符号定义为：

$$\left(\frac{\bullet}{\bullet}\right)_3:\mathbb{Z}[\omega]\times(\mathbb{Z}[\omega]-(1-\omega)\mathbb{Z}[\omega])\to\{0,1,\omega,\omega^2\}$$

其含义见文献[13]。

若 π 为 $\mathbb{Z}[\omega]$ 中的不可分数且不被 $1-\omega$ 整除，那么 $\left(\frac{\alpha}{\pi}\right)_3=\alpha^{(N(\pi)-1)/3}$。若 $\beta=\prod_{i=1}^{t}\pi_i^{\kappa_i}\in\mathbb{Z}[\omega]$，且 $\pi_1,\pi_2,\cdots,\pi_t$ 是 $\mathbb{Z}[\omega]$ 中的不可分数且不被 $1-\omega$ 整除，那么 $\left(\frac{\alpha}{\beta}\right)_3=\prod_{i=1}^{t}\left(\frac{\alpha}{\pi_i}\right)_3^{\kappa_i}$。

如果 ε 的长度是 1，那么 $\left(\frac{\alpha}{\varepsilon}\right)_3=1$。如果 $\gcd(\alpha,\beta)\neq 1$，那么 $\left(\frac{\alpha}{\beta}\right)_3=0$。

三次剩余运算符号满足以下更多的规则[13]：

(1)如果 $\alpha\equiv\alpha'(\mathrm{mod}\,\beta)$，那么 $\left(\frac{\alpha}{\beta}\right)_3=\left(\frac{\alpha'}{\beta}\right)_3$；

(2)相乘率成立，即 $\left(\frac{\alpha\cdot\alpha'}{\beta}\right)_3=\left(\frac{\alpha}{\beta}\right)_3\cdot\left(\frac{\alpha'}{\beta}\right)_3$；

(3)如果 α 与 β 都是原形式，那么 $\left(\frac{\alpha}{\beta}\right)_3=\left(\frac{\beta}{\alpha}\right)_3$；

(4)如果 β 是原形式，$\beta=1+3(m+n\omega)$，$m\in\mathbb{Z}$，$n\in\mathbb{Z}$ 那么 $\left(\frac{1-\omega}{\beta}\right)_3=\omega^m$，$\left(\frac{\omega}{\beta}\right)_3=\omega^{-(m+n)}$，$\left(\frac{-1}{\beta}\right)_3=1$。文献[13]提供了一个有效的算法，在不需要分解 β 的情况下求出 $\left(\frac{\alpha}{\beta}\right)_3$ 的值。

2.3 求三次剩余符号值的有效算法

本节利用定理 1 来计算 $\mathbb{Z}[\omega]$ 中三次剩余的立方根，利用定理 5 来计算 $\mathbb{Z}[\omega]$ 三次剩余的 3^l 次方根。

定理 1 如果 m、l、R 都是正整数，$m<3^l$，且存在正整数 γ 和 δ 满足 $m=3^{\gamma}(3\delta+1)$。如果 a 是模 N 的三次剩余，$X\in\mathbb{Z}_N^*$ 且 $a^m\equiv X^{3^l}(\mathrm{mod}\,N)$，则 $y\equiv\frac{X^{3^{l-\gamma-1}}}{a^{\delta}}(\mathrm{mod}\,N)$，满足 $y^3\equiv a(\mathrm{mod}\,N)$，也就是说 y 是 a 的立方根。

定理 2[13] 如果 p 和 q 是整数环中的素数，并且 $p\equiv q\equiv 1(\mathrm{mod}\,3)$。令 $N=p\cdot q$，而 π_1,π_2 是 $\mathbb{Z}[\omega]$ 中的不可分数，满足 $N(\pi_1)=p$，$N(\pi_2)=q$，整数 A 和 B 满足，$A+B\omega=\pi_1\cdot\pi_2$，且 B 与 N 互素。令 $C=-A\cdot B^{-1}(\mathrm{mod}\,N)$，则 $C\equiv\omega(\mathrm{mod}\,\pi_1\pi_2)$，$C^3\equiv 1(\mathrm{mod}\,N)$。

上述定理可以通过直接演算来证明。

定理 3 p,q,π_1,π_2,C 的定义与定理 2 中相同。当 $\frac{(p-1)(q-1)}{9}\equiv 2(\mathrm{mod}\,3)$ 时，则：

$$\left(\frac{C}{\pi_1\cdot\pi_2}\right)_3=\left(\frac{\omega}{\pi_1}\right)_3\cdot\left(\frac{\omega}{\pi_2}\right)_3=1$$

进一步，如果 $(p-1)/3\equiv 2(\mathrm{mod}\,3),(q-1)/3\equiv 1(\mathrm{mod}\,3)$，则：

$$\left(\frac{C}{\pi_1}\right)_3=\left(\frac{\omega}{\pi_1}\right)_3=\omega^{\frac{p-1}{3}}=\omega^2$$

$$\left(\frac{C}{\pi_2}\right)_3=\left(\frac{\omega}{\pi_2}\right)_3=\omega^{\frac{q-1}{3}}=\omega$$

定理 4 相关变量定义同定理 2。当 $\frac{(p-1)(q-1)}{9}\equiv 2(\mathrm{mod}\,3)$ 时，正整数 $d=\frac{1}{3}[\frac{1}{9}(p-1)(q-1)+1]$ 是良定义的。给定三次剩余整数 a，如果存在 X 满足 $X\in\mathbb{Z}[\omega]$，$\left(\frac{X}{\pi_1\cdot\pi_2}\right)_3=1$，那么 a^d 是 a 模 N 的立方根，即 $(a^d)^3\equiv a(\mathrm{mod}\,N)$。该定理可以通过直接演算来证明。

定理 5 相关参数定义同定理 2。如果 α 是模 N 的三次剩余，那么 α 的 3^l 次方根 s 可以按下式计算 $s\equiv\alpha^{d^l}\ \mathrm{mod}\,N$。这里 l 是一个正整数。

证明：$s^{3^l}\equiv\alpha^{d^l\cdot 3^l}\equiv\alpha^{(3d)^l}(\mathrm{mod}\,N)$。

从定理 4 可以得到：

$$\alpha^{(3d)^l}\equiv\alpha^{\overbrace{3d\bullet\cdots\bullet 3d}^{l次}}\equiv\alpha(\mathrm{mod}\,N)$$

2.4 大整数分解困难问题

设 k 为安全参数，N 是 2 个大素数 p 和 q 的乘积。标准的大整数分解问题是：给定合数 N，输出 p 或 q。

令 N' 为 2 个大素数 p' 和 q' 的乘积，这里：

$$p'\equiv q'\equiv 1(\mathrm{mod}\,3),\frac{(p'-1)(q'-1)}{9}\equiv 2(\mathrm{mod}\,3)$$

C 的定义同定理 2，并且满足 $C\equiv\omega(\mathrm{mod}\,\pi_1\pi_2)$，$C^3\equiv 1(\mathrm{mod}\,N')$。

定义另外一个大整数分解问题如下：给定 N' 和 C，怎样输出 p' 或 q'。事实上，这个大整数分解问题的困难程度和标准大整数分解问题一样，因为 C 是 1 的立方根，C 不能帮助攻击者分解 N'。

设 $\mathcal{A}'$ 代表一个多项式时间概率算法，在 $\mathcal{A}'$ 中给定 $N'=p'\cdot q'$ 和 C，$\mathcal{A}'$ 输出 p' 或 q'。$Fac_{A',N',C}(k)$ 是一个函数，如果 $p'\cdot q'=N'$ 或 $p'\cdot q'=0$，$Fac_{A',N',C}(k)=1$。这个分解问题的困难假设是在算法 $\mathcal{A}'$ 运行时间不超过 t 的时间内满足 $\Pr[Fac_{A',N',C}(k)=1]\leqslant\varepsilon$。这里 ε 为一个不可忽略的概率。

2.5 基于立方根的合数分解

设 $N=pq$，这里 p 和 q 是大素数，$p\equiv q\equiv 1(\mathrm{mod}\,3)$，$\frac{(p-1)(q-1)}{9}\equiv 2(\mathrm{mod}\,3)$。$\pi_1,\pi_2,C$ 的定义同定理 2，a 为模 N 的三次剩余。若 $X\in\mathbb{Z},Y\in\mathbb{Z}$ 为 a 的 2 个立方根，并且满足 $\left(\frac{X}{\pi_1\cdot\pi_2}\right)_3\neq\left(\frac{Y}{\pi_1\cdot\pi_2}\right)_3$，那么 N 能够被分解，因为 p 等于 $\gcd(X-Y,N)$、$\gcd(X-CY,N)$ 或 $\gcd(X-C^2Y,N)$。该结论可由如下定理得出[13]：

定理 6 如果存在 $X,Y\in\mathbb{Z}$，$X^3\equiv Y^3(\mathrm{mod}N)$，并且 $\left(\frac{X}{\pi_1\cdot\pi_2}\right)_3\neq\left(\frac{Y}{\pi_1\cdot\pi_2}\right)_3$，那么 $p=\gcd(X-C^iY,N)$，$i\in\{0,1,2\}$。

证明：由于 $X^3\equiv Y^3(\mathrm{mod}\,N)$，有：

$(X-Y)(X-CY)(X-C^2Y)\equiv 0(\mathrm{mod}\,pq)$

如果 $pq\,|\,(X-C^iY)$，那么 $X\equiv C^iY(\mathrm{mod}\,\pi_1\pi_2)$，这样可以得到 $\left(\frac{X}{\pi_1\cdot\pi_2}\right)_3=\left(\frac{C^iY}{\pi_1\cdot\pi_2}\right)_3$。

而本文已经证明 $C\equiv\omega(\mathrm{mod}\,\pi_1\pi_2)$，由 $\frac{(p-1)(q-1)}{9}\equiv 2(\mathrm{mod}\,3)$ 得到 $\left(\frac{\omega}{\pi_1\cdot\pi_2}\right)_3=1$。这样 $\left(\frac{X}{\pi_1\cdot\pi_2}\right)_3=\left(\frac{C^iY}{\pi_1\cdot\pi_2}\right)_3=\left(\frac{Y}{\pi_1\cdot\pi_2}\right)_3$，这与假设矛盾。这就证明了 $\exists i\in\{0,1,2\}$ 使 $p\,|\,(X-C^iY)$ 且 $q\nmid(X-C^iY)$。这样可以得到：

$p=\gcd(X-C^iY,N),i\in\{0,1,2\}$

2.6 环签名方案的分叉引理

文献[16]给出了签名体制安全性证明的一些分叉引理，随后文献[17]给出了在随机预言模型下证明环签名的分叉引理。本文将用此引理来证明基于身份的环签名方案的不可伪造性。

给定安全参数 k，Hash 函数输出 k bit 的元素，环 $L=\{ID_1,ID_2,\cdots,ID_n\}$。给定消息 M，一般的环签名方案输出的环签名格式为 $\{L,M,R_1,\cdots,R_n,h_1,\cdots,h_n,\sigma\}$。这里 $R_i,i\in\{1,2,\cdots,n\}$ 是互不相同的，且在一个签名中 R_i 出现的概率不超过 $2/2^k$。h_i 为 Hash 函数输出的值，σ 的值和所有的 $\cup\{R_i\}$、$\cup\{h_i\}$、M 均相关。

定理 7 给定安全参数 k，$\mathcal{A}$ 为概率多项式时间图灵机，$\mathcal{A}$ 接收各种公开参数和对随机预言机进行至多 Q 次询问的回答。如果 $\mathcal{A}$ 能在时间 T 内以不可忽略的概率 $\varepsilon\geqslant\frac{7C_{Q,n}}{2^k}$ 产生一个有效的签名 $\{L,M,R_1,\cdots,R_n,h_1,\cdots,h_n,\sigma\}$。这里 $C_{Q,n}$ 定义为 Q 个元素的 n-排列，即 $C_{Q,n}=Q(Q-1)\cdots(Q-n+1)$。那么可以通过图灵机重放攻击在时间 $T'\leqslant T$ 内以概率 $\varepsilon'\geqslant\frac{\varepsilon^2}{66C_{Q,n}}$ 得到 2 个有效的环签名：

$\{L,M,R_1,\cdots,R_n,h_1,\cdots,h_n,\sigma\}$

$\{L,M,R_1,\cdots,R_n,h_1',\cdots,h_n',\sigma'\}$

这里有某个 $j\in\{1,2,\cdots,n\}$，$h_j\neq h_j'$，$i\in\{1,2,\cdots,n\}\backslash\{j\}$，$h_i=h_i'$[12]。

3 方案的构造

本节利用三次剩余理论构造出一个基于身份的环签名方案 IDRSig。IDRSig 包含 4 个子算法，*IDRSig*=(*Setup, Extract, Sign, Verify*)，各个算法构造如下：

(1)*Setup*(*k*, l)：接收输入安全参数(*k*, l)，该初始化算法由 PKG 按如下步骤执行：

1)生成 2 个随机大素数 p、q，满足 $p\equiv q\equiv 1(\mathrm{mod}\,3)$，$\frac{(p-1)(q-1)}{9}\equiv 2(\mathrm{mod}\,3)$，且 $2^{k-1}\leqslant (p-1)(q-1), pq<2^k$。不失一般性，假设 $\frac{p-1}{3}\equiv 2(\mathrm{mod}\,3)$，$\frac{q-1}{3}\equiv 2(\mathrm{mod}\,3)$。

2)生成 2 个不可分数 $\pi_1,\pi_2\in\mathbb{Z}[\omega]$，使得 $N(\pi_1)=p$，$N(\pi_2)=q$。

3)计算 $N=pq$。

4)令 $A+B\omega=\pi_1\pi_2, A,B\in\mathbb{Z}$，计算 $C=-A\cdot B^{-1}(\mathrm{mod}N)$。由定理 3 可得：$\left(\frac{C}{p}\right)_3=\omega^2,\left(\frac{C}{q}\right)_3=\omega$。

5)随机选择 $a\in\mathbb{Z}$，使得 $\left(\frac{a}{N}\right)_3=\omega$。

6)计算 $d=\frac{1}{3}[\frac{1}{9}(p-1)(q-1)+1]$。

7)选择 2 个单向哈希函数 $h_1(\bullet):\{0,1\}^*\to\mathbb{Z}_N^*$，$h_2(\bullet,\bullet):\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^l$。该算法执行完后，PKG 的主密钥为 $MSK=\{p,q,\pi_1,\pi_2,d\}$，公开参数为 $PP=\{N,h_1,h_2,a,C,l\}$。

(2)*Extract*(*ID, MSK, PP*)：该算法也由 PKG 执行。给定用户的身份 ID，这个算法按如下步骤计算用户的私钥：

1)计算 $c_1=\begin{cases}0 & \text{if}\left(\frac{h_1(ID)}{N}\right)_3=1\\ 1 & \text{if}\left(\frac{h_1(ID)}{N}\right)_3=\omega^2\\ 2 & \text{if}\left(\frac{h_1(ID)}{N}\right)_3=\omega\end{cases}$。

2)计算 $h\equiv a^{c_1}h_1(ID)(\mathrm{mod}\,N)$，注意 $\left(\frac{h}{N}\right)_3=1$。

3)计算 $c_2=\begin{cases}0 & \text{if}\left(\frac{h}{p}\right)_3=\left(\frac{h}{q}\right)_3=1\\ 1 & \text{if}\left(\frac{h}{p}\right)_3=\omega,\left(\frac{h}{q}\right)_3=\omega^2\\ 2 & \text{if}\left(\frac{h}{p}\right)_3=\omega^2,\left(\frac{h}{q}\right)_3=\omega\end{cases}$。

4)计算公钥 $PK_{ID}=H(ID)\equiv a^{c_1}C^{c_2}h_1(ID)(\mathrm{mod}\,N)$，$\left(\frac{H(ID)}{p}\right)_3=\left(\frac{H(ID)}{q}\right)_3=1$，这样 $H(ID)$是模 N 的三次剩余。

5)计算私钥 SK_{ID} 为 $H(ID)$的 3^l 次方根：

$$SK_{ID}\equiv H(ID)^{d^l}(\mathrm{mod}\,N)$$

注意 ${SK_{ID}}^{3^l}\equiv H(ID)(\mathrm{mod}\,N)$。用户的私钥为 $\{SK_{ID}, c_1, c_2\}$。

(3)*Sign*(M, c_1, c_2, PP, L)：$L=\{ID_1, ID_2, \cdots, ID_n\}$ 为所有 n 个用户的身份集合；M 为待签名的消息，实际的签名者被索引为 s(如他的公钥为 $PK_{ID_s}=H(ID_s)$)，按如下的步骤给出代表这个群组 L 基于身份的环签名：

1)对于每个 ID_i，计算 (c_{i1}, c_{i2}) 和 $PK_{ID_i}=H(ID_i)$。

2)随机选择 $r_i\in\mathbb{Z}_N^*$，计算 $R_i\equiv r_i^{3^l}(\mathrm{mod}\,N)$ 和 $h_i=h_2(R_i, M, L), \forall i\in\{1,2,\cdots,n\}\setminus\{s\}$。

3)随机选择 $r_s\in\mathbb{Z}_N^*$，计算 $R_s'\equiv r_s^{3^l}(\mathrm{mod}\,N)$，$h_s'=h_2(R_s', M, L)$ 和 $R_s=PK_{ID_s}^{h_s'}\cdot\prod_{i\neq s}(R_i\cdot PK_{ID_i}^{h_i})^{-1}$。

4)计算 $h_s=h_2(R_s, M, L)$ 和 $V\equiv(SK_{ID_s})^{h_s+h_s'}(\mathrm{mod}\,N)$。输出的签名为 $\sigma=\{L, M, \bigcup_{i=1}^n R_i, \bigcup_{i=1}^n(c_{i1}, c_{i2}), V\}$。

(4)*Verify*(*PP, M, σ*)：给一个消息 M 和签名 σ，任何用户能用如下算法验证签名的有效性：

1)对 ID_i，计算公钥 $PK_{ID_i}=H(ID_i), \forall i\in\{1,2,\cdots,n\}$。

2)计算 $h_i=h_2(R_i, M, L), \forall i\in\{1,2,\cdots,n\}$。

3)检验 $V^{3^l}=\prod_{i=1}^n(R_i\cdot PK_{ID_i}^{h_i})$ 是否成立，如果成立，输出“签名有效”；否则输出“签名无效”。

签名方案 IDRSig 的正确性验证如下：

$$\begin{aligned}V^{3^l}&\equiv((SK_{ID_s})^{h_s+h_s'})^{3^l}\equiv PK_{ID_s}^{h_s}\cdot PK_{ID_s}^{h_s'}\equiv\\ &PK_{ID_s}^{h_s'}\cdot\prod_{i\neq s}(R_i\cdot PK_{ID_i}^{h_i})^{-1}\cdot\prod_{i\neq s}(R_i\cdot PK_{ID_i}^{h_i})\cdot PK_{ID_s}^{h_s}\equiv\\ &R_s\cdot\prod_{i\neq s}(R_i\cdot PK_{ID_i}^{h_i})\cdot PK_{ID_s}^{h_s}=\prod(R_i\cdot PK_{ID_i}^{h_i})\end{aligned}$$

4 安全性证明

本节在基于大整数分解困难问题的基础上证明方案 IDRSig 的安全性。

4.1 攻击模型

为了定义合理的攻击模型，应假设攻击者拥有最大的自由度，即适应性选择消息和身份攻击。在本文模型中，攻击者可以在对若干身份 $ID_i(i=1,2,\cdots,n)$ 进行私钥查询后，再选择目标身份(不能包含已查询过私钥的 ID_i)，并且攻击者在输出伪造签名前，可以进行多次签名查询(不能包含目标身份环和消息)。

定义 1 为了定义安全性，本文考虑在攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间进行的交互游戏如下：

(1)挑战者 $\mathcal{C}$ 首先生成 PKG 公开参数 *PP*，然后将 *PP* 公开给 $\mathcal{A}$。

(2)攻击者 $\mathcal{A}$ 进行一系列的查询：

1)私钥查询：当收到关于 ID 的私钥查询时，挑战者 $\mathcal{C}$ 运行 $Extract()$ 产生与 ID 对应的私钥 SK_{ID} 以及标签 (c_1,c_2) 然后发送给 $\mathcal{A}$。

2)签名查询：$\mathcal{A}$ 首先选择 n 个用户身份的群组 $\bigcup\{ID_i\}(1\leqslant i\leqslant n)$ 和消息 M，$\mathcal{C}$ 输出基于身份的环签名 σ。

3)Hash 查询：当收到 Hash 函数的查询时，$\mathcal{C}$ 计算相应的 Hash 值后，将该值返还给 $\mathcal{A}$。

(3) $\mathcal{A}$ 最后输出一个对消息 M 的签名 σ 和 n 个用户的身份 $\bigcup\{ID_i\}(1\leqslant i\leqslant n)$，满足 $\mathcal{A}$ 并没有对 $\bigcup\{ID_i\}(1\leqslant i\leqslant n)$ 进行私钥查询，且也没有对 M 和 $\bigcup\{ID_i\}(1\leqslant i\leqslant n)$ 进行签名查询。

若 $\mathcal{A}$ 输出的签名被 $\mathcal{C}$ 判定为有效，那么 $\mathcal{A}$ 在游戏中获胜。$\mathcal{A}$ 输出的签名有效的概率即为 $\mathcal{A}$ 在游戏中获胜的优势。

定义 2 签名方案 IDRSig 是选择消息和身份安全的，如果没有攻击者能够以不可忽略的优势在上述游戏中胜出。

定义 3 签名方案 IDRSig 是具有无条件匿名性，如果任何验证者，即使有无穷的计算资源，都无法以大于 $1/n$ 的概率猜出代表 n 个用户的环的真正签名者的身份。如果签名者是环中不同于真正签名者的成员，那么他能猜出真正签名者的身份不大于 $1/(n-1)$。

4.2　存在性、不可伪造性和签名者匿名性

本文将签名方案 IDRSig 的安全性总结为如下定理：

定理 8 在随机预言机模型(签名方案 IDRSig 中 Hash 函数被建模为随机预言机)下，如果存在算法 $\mathcal{A}$ (也为攻击者)随机选择一个含有 n 个用户的身份环，在多项式时间 T_A 内至多进行 q_s 签名查询，q_{h_1} 次 h_1 查询，q_{h_2} 次 h_2 查询，q_e 次私钥查询，能以不可忽略的概率 ε_A 输出有效签名，那么大整数分解问题能以不可忽略的概率 $\dfrac{(1-\mu)^{2n+1}}{873C_{q_{h_2},n}}\varepsilon_A^2$ 在多项式时间 $2(T_A+T_{q_{h_1}}+T_{q_{h_2}}+nT_{q_s})$ 内解决。

证明：k 为安全参数，$N=pq$ 为大整数困难问题输入，其中，p 和 q 为 2 个大素数，$p\equiv q\equiv 1(\mathrm{mod}\,3)$，$\dfrac{p-1}{3}\equiv 2(\mathrm{mod}\,3)$，$\dfrac{q-1}{3}\equiv 1(\mathrm{mod}\,3)$，假设有攻击者 $\mathcal{A}$ 通过攻击签名方案 IDRSig 来解决这个难题。

按假设，攻击者 $\mathcal{A}$ 能以不可忽略的概率 ε_A 伪造环签名。本文引入一个概率多项式时间图灵机 $\mathcal{C}$ (挑战者)来应用分叉引理的结论。$\mathcal{C}$ 能有效地模拟与攻击者 $\mathcal{A}$ 进行交互游戏的环境。实际上 $\mathcal{C}$ 通过与 $\mathcal{A}$ 进行模拟游戏，试图以 $\mathcal{A}$ 为子程序去获得对同一消息的 2 个合法的环签名。

图灵机 $\mathcal{C}$ 收到 $N=pq$ 后，计算出 C，C 的定义同第 2 节定理 2。选择 $a\in\mathbb{Z}_N^*$ 满足雅可比符号 $\left(\dfrac{a}{N}\right)=\omega$ 和安全参数 $l\geqslant 160$，然后将 $\{N,a,C,l\}$ 作为公共参数发送给 $\mathcal{A}$。

$\mathcal{A}$ 开始攻击签名方案 IDRSig，并向 $\mathcal{C}$ 发起如下询问：

(1) h_1 询问：假设 $\mathcal{A}$ 在对标识 ID 进行私钥询问前进行 h_1 询问。为响应 $\mathcal{A}$ 的 h_1 查询，$\mathcal{C}$ 维护了一个 h_1 列表 TAB_{h_1} 来代表随机预言机模型 H_1，当 $\mathcal{A}$ 询问一个标识 ID_i 的 Hash 值时，$\mathcal{C}$ 随机选择一个值 $s_i\in\mathbb{Z}_N^*$ 然后重复上述过程直到 s_i 不在 TAB_{h_1} 中。此时，$\mathcal{C}$ 随机选择 $W\in\{0,1\}$，假设 $\Pr(W=0)=\mu$。如果 W=0，定义 $h_1(ID_i)\equiv\dfrac{s_i^{3^l}}{C^{c_{i2}}a^{c_{i1}}}(\mathrm{mod}\,N)$，$\{c_{i1},c_{i2}\}\in\{0,1,2\}^2$；如果 W=1，$\mathcal{C}$ 随机产生一个值 $r\in\mathbb{Z}_N^*$ 作为 $h_1(ID_i)$ 的值。然后 $\mathcal{C}$ 将 $<ID_i,h_1(ID_i),s_i,c_{i1},c_{i2},W>$ 存入表 TAB_{h_1} 中。

(2) h_2 询问：为响应 $\mathcal{A}$ 的 h_2 查询，$\mathcal{C}$ 维护了一个 h_2 列表 TAB_{h_2} 作为随机预言机模型 H_2，当 $\mathcal{A}$ 询问 H_2 Hash 值时，$\mathcal{C}$ 查询表 TAB_{h_2}，如果找到相同的记录，将结果返回给 $\mathcal{A}$，否则 $\mathcal{C}$ 将生成一个随机值返还给 $\mathcal{A}$，并将该记录存在表 TAB_{h_2} 中。

(3)私钥询问：每次 $\mathcal{A}$ 询问标识 ID_i 的私钥时，$\mathcal{C}$ 在表 TAB_{h_1} 中查询 ID_i 的记录，如果 W=0，$\mathcal{C}$ 返回 $<s_i,c_{i1},c_{i2}>$ 给 $\mathcal{A}$；如果 W=1，$\mathcal{C}$ 无法回答并且停机。注意 $\mathcal{C}$ 在这个过程中停机的概率小于 $1-\mu^{q_e}$。

(4)签名询问：$\mathcal{A}$ 选择一个 n 个身份标识的群组 $L=\bigcup\{ID_i\}(1\leqslant i\leqslant n)$ 和任意的消息 M。假设 $\mathcal{A}$ 没有查询环 L 中任何成员的私钥。作为对 $\mathcal{A}$ 的应答，$\mathcal{C}$ 产生如下过程：

1)对每个身份标识 ID_i，计算 $\{c_{i1},c_{i2}\}$ 和 $PK_{ID_i}=H(ID_i)\equiv a^{c_{i1}}C^{c_{i2}}h_1(ID_i)(\mathrm{mod}\,N)$。

2)随机选择索引 $s\in\{1,2,\cdots,n\}$。

3)选择 $r_i\in\mathbb{Z}_N^*$，计算 $R_i\equiv r_i^{3^l}(\mathrm{mod}N)$ 和 $h_i=h_2(R_i,M,L)$，$\forall i\in\{1,2,\cdots,n\}\setminus\{s\}$。可以确定 $\mathcal{A}$ 在进行签名查询后肯定会对这些输入进行 h_2 询问来验证签名的正确性。

4)选择 $h_s\in\{0,1\}^l$。

5)选择 $V\in\mathbb{Z}_N^*$。

6)计算 $R_s=V^{3^l}\cdot\prod_{i\neq s}(R_i\cdot PK_{ID_i}{}^{h_i})^{-1}\cdot\left(PK_{ID_s}{}^{h_s}\right)^{-1}$。

7)令 $h_2(R_s,M,L)=h_s$，当 $\mathcal{A}$ 对这个输入进行 h_2 询问时，$\mathcal{C}$ 返回 h_s。

8)返回多元项 $\{L,M,\bigcup_{i=1}^{n}R_i,V\}$。

在签名模拟中，可能存在一些“碰撞”。在加密方案 IDRSig 中，假定没有 R_i 在环签名中出现的概率大于 $2/2^k$。发生的碰撞可能有以下 2 种：

(1)在签名模拟中，$\mathcal{C}$ 输出的多元组 $<R_s,M,L>$ 和 $\mathcal{A}$ 以前询问随机预言机 H_2 返回的值相同。这种碰撞发生的概率为 $q_{h_2}\cdot q_s\cdot\frac{2}{2^k}$。

(2) $\mathcal{C}$ 在 2 次签名模拟中输出的多元组 $<R_s, M, L>$ 相同。这种碰撞发生的概率为 $\frac{{q_s}^2}{2}\cdot\frac{2}{2^k}$。

下面计算 $\mathcal{C}$ 得到一个有效签名的概率:

$\tilde{\varepsilon}_C$ =Pr($\mathcal{C}$ 获得一个有效签名)=Pr($\mathcal{C}$ 没有停机&&在线模拟中无碰撞发生&& $\mathcal{A}$ 在游戏中胜出)≥Pr($\mathcal{A}$ 在游戏中胜出|$\mathcal{C}$ 没有停机&&在线签名模拟中无碰撞发生)−Pr($\mathcal{C}$ 停机|在线模拟中有碰撞发生)≥ $\varepsilon_A-(1-\mu^{q_e})-q_{h_2}\cdot q_s\cdot\frac{2}{2^k}-\frac{{q_s}^2}{2}\cdot\frac{2}{2^k}\geqslant\frac{7\varepsilon_A}{12}$。

假设 $\mathcal{A}$ 提交给 $\mathcal{C}$ 对(L, M)的有效的签名，环 L 有 n 个成员，必须确定 $\mathcal{C}$ 不知道任意一个成员的私钥(否则 $\mathcal{C}$ 能自己生成伪造的环签名)。这种可能性的概率为 $(1-\mu)^n$。这样，$\mathcal{C}$ 在不知道环成员私钥的情况下获得有效签名的概率为 $\varepsilon_C=(1-\mu)^n\tilde{\varepsilon}_C\geqslant\frac{7C_{Q,n}}{2^k}$。总的执行时间 $T_C\leqslant T_A+T_{q_{h_1}}+T_{q_{h_2}}+nT_{q_s}$。

对图灵机 $\mathcal{C}$ 应用环签名的分叉引理让 $\mathcal{A}$ 执行 2 遍对签名方案 IDRSig 的攻击过程，在总的运行时间 $T'\leqslant 2T_C$ 内，$\mathcal{C}$ 以概率 $\tilde{\varepsilon}'\geqslant\frac{\varepsilon_C^2}{66C_{q_{h_2},n}}$ 获得 2 个有效的签名:

$\{L, M, R_1,\cdots,R_n, h_1,\cdots,h_n, V\}$

$\{L, M, R_1,\cdots,R_n, h_1',\cdots,h_n', V'\}$

其中，$j\in\{1,2,\cdots,n\}$, $h_j\neq h_j'$, $i\in\{1,2,\cdots,n\}\setminus\{j\}$, $h_i=h_i'$。那么可以得到:

$$V^{3^l}=\prod_{i=1}^{n}(R_i\cdot PK_{ID_i}{}^{h_i}),\ V'^{3^l}=\prod_{i=1}^{n}(R_i\cdot PK_{ID_i}{}^{h_i'})$$

从而可以得到: $(V/V')^{3^l}\equiv PK_{ID_j}{}^{(h_j-h_j')}(\bmod N)$。

假设不存在正整数 γ,δ 使得 $h_j-h_j'=3^\gamma(3\delta+1)$，那么模拟失败。由于 h_j, h_j' 是随机选取的，因此存在上述条件的 γ,δ 的概率为 1/3。利用定理 5，$\mathcal{C}$ 能计算出 PK_{ID_j} 的 3^l 次根 s'。$\mathcal{C}$ 在表 TAB_{h_1} 中查找项 $<ID_j, h_1(ID_j), s_j, c_{j1}, c_{j2}, W>$，如果 $s'\neq\pm s_j(\bmod N)$，由定理 6，N 能被分解；否认 $\mathcal{C}$ 报告出错。值得说明的是，s_j 是由 $\mathcal{C}$ 独立于 $\mathcal{A}$ 选取的 PK_{ID_j} 的 3^l 次根，因此，事件 $s'\neq\pm s_j(\bmod N)$ 的概率为 2/3。这样，则能以概率:

$$\varepsilon'=\frac{2}{9}(1-\mu)\tilde{\varepsilon}'\geqslant\frac{2}{9}(1-\mu)\frac{\varepsilon_C^2}{66C_{q_{h_2},n}}\geqslant$$

$$\frac{2}{9}(1-\mu)\frac{((1-\mu)^n\frac{7\varepsilon_A}{12})^2}{66C_{q_{h_2},n}}\geqslant\frac{(1-\mu)^{2n+1}}{873C_{q_{h_2},n}}\varepsilon_A^2$$

在多项式时间 $2(T_A+T_{q_{h_1}}+T_{q_{h_2}}+nT_{q_s})$ 内解决大整数分解问题。

定理 9 签名方案 IDRSig 具有签名者无条件匿名性。

证明: 由于 $\bigcup_{i\neq s}\{R_i\}$ 和 h_s' 都是随机生成的，因此 $\prod_{i=1}^{n}\{R_i\}$ 是均匀分布的。

接下来看 $V\equiv(SK_{ID_s})^{h_s+h_s'}(\bmod N)$ 是否会泄露实际签名者的信息。由于 h_s 能公开计算出，主要考察 $V\cdot(SK_{ID_s}{}^{h_s})^{-1}\equiv SK_{ID_s}{}^{h_s'}(\bmod N)$。由于任何验证者都可以通过计算 $R_s\cdot\prod_{i\neq s}(R_i\cdot PK_{ID_i}{}^{h_i})$ 来计算 $PK_{ID_s}{}^{h_s'}$。

下面通过检验 $\left(SK_{ID_s}{}^{h_s'}\right)^{3^l}=PK_{ID_s}{}^{h_s'}$ 是否成立来确定 ID_j 是否是实际签名者 ID_s 的身份。最终要验证等式 $R_j\cdot\prod_{i\neq j}(R_i\cdot PK_{ID_i}{}^{h_i})\equiv\ V^{3^l}\cdot(PK_{ID_j}{}^{h_j})^{-1}$ 是否成立。实际上，上式在 $j=s$ 和 $j\in\{1,2,\cdots,n\}\setminus\{s\}$ 时都是成立的，证明如下:

$$R_j\cdot\prod_{i\neq j}(R_i\cdot PK_{ID_i}{}^{h_i})\equiv R_s\cdot\prod_{i\neq s}R_i\cdot\prod_{i\neq j}PK_{ID_i}{}^{h_i}\equiv$$

$$PK_{ID_s}{}^{h_s'}\cdot\prod_{i\neq s}\left(R_i\cdot PK_{ID_i}{}^{h_i}\right)^{-1}\cdot\prod_{i\neq s}R_i\cdot\prod_{i\neq j}PK_{ID_i}{}^{h_i}\equiv$$

$$PK_{ID_s}{}^{h_s'}\cdot PK_{ID_s}{}^{h_s}\cdot\left(PK_{ID_j}{}^{h_j}\right)^{-1}\equiv$$

$$\left(SK_{ID_s}{}^{3^l}\right)^{h_s+h_s'}\cdot\left(PK_{ID_j}{}^{h_j}\right)^{-1}\equiv$$

$$V^{3^l}\cdot(PK_{ID_j}{}^{h_j})^{-1}$$

这样可以得出结论对于给定的消息 M 和身份标识集合 L，$\bigcup_{i\neq s}\{R_i\}$，V 是独立均匀分布的，因此，敌手即使在得到环 L 中所有成员私钥和拥有无穷计算资源，仍然无法以大于 1/n 的概率猜出实际的签名者。

5 结束语

本文提出的环签名方案符合文献[17]中一般环签名方案的条件，因此，在安全性证明过程中能引用该文献中的相关结果，并形式化地证明该方案为可抵抗选择消息和身份的存在性伪造攻击的安全方案。此外，根据文献[18]的结论，一次配对运算至少需要 11 110 次域 $F_{3^{163}}$ 上的乘法操作，而一次标量点乘大约需几百次该域上的乘法操作，文中提出的环签名方案没有采用配对操作，因而实现的效率要高于采用双线性配对运算构造的方案。

下一步将构造其他基于三次剩余的身份基签名方案，并同时研究如何不借助随机预言模型来证明该类方案的安全性。

参考文献

[1] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret[C]// Proc. of the 7th International Conference on the Theory and Application of Cryptology and Information Security. London, UK: [s. n.], 2001.

[2] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Proc. of CRYPTO'84. Santa Barbara, USA: [s. n.], 1985.

[3] Boneh D, Franklin M. Identity Based Encryption from the Weil Pairing[C]//Proc. of CRYPTO'01. Santa Barbara, USA: [s. n.], 2001.

[4] Cocks C. An Identity Based Encryption Scheme Based on Quadratic Residues[C]//Proc. of the 8th IMA International Conference on Cryptography and Coding Cryptography and Coding. Berlin, Germany: Springer-Verlag, 2001.

[5] 柴震川, 董晓蕾, 曹珍富. 利用二次剩余构造基于身份的数字签名方案[J]. 中国科学 F 辑: 信息科学, 2009, 39(2): 199-204.

[6] Zhang Fangguo, Kim K. ID-based Blind Signature and Ring Signature from Pairings[C]//Proc. of ASIACRYPT'02. Berlin, Germany: Springer-Verlag, 2002.

[7] Lin Chih-Yin, Wu Tzong-Chen. An Identity-based Ring Signature Scheme from Bilinear Pairings[EB/OL]. (2003-08-10). http://eprint.iacr.org/2003/117.

[8] Awasthi A, Lai S. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings[EB/OL]. (2004-04-21). http://eprint.iacr.org/2004/184.

[9] Javier H, Saez G. New Identity-based Ring Signature Schemes[C]//Proc. of ICICS'04. Berlin, Germany: Springer-Verlag.

[10] Chow S S M, Yiu S, Hui L C K. Efficient Identity Based Ring Signature[C]//Proc. of ACNS'05. Berlin, Germany: Springer-Verlag, 2005.

[11] Nguyen L. Accumulators from Bilinear Pairings and Applications to ID-based Ring Signatures and Group Membership Revocation[C]//Proc. of CT-RSA'05. Berlin, Germany: Springer-Verlag, 2005.

[12] Hu Xiong, Qin Zhiguang, Li Fagen. Identity-based Ring Signature Scheme Based on Quadratic Residues[J]. High Technology Letters, 2009, 15(1): 94-100.

[13] Willliams H C. An M3 Public-key Encryption Scheme[C]// Proc. of Crypto'85. Berlin, Germany: Springer-Verlag, 1985.

[14] Damg 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(6): 643-652.

[15] 柯 召, 孙 琦. 数论讲义[M]. 2 版. 北京: 高等教育出版社, 2001.

[16] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures[J]. Journal of Cryptology, 2000, 13(3): 361-369.

[17] Herranz J, Saez G. Forking Lemmas for Ring Signature Schemes[C]//Proc. of INDOCRYPT'03. Berlin, Germany: Springer-Verlag, 2003.

[18] Barreto S L M, Lynn B, Scott M. On the Selection of Pairing-friendly Groups[C]//Proc. of SAC'04. Berlin, Germany: Springer-Verlag, 2004.

编辑 金胡考

(上接第 110 页)

[7] Incel O D, van Hoesel L, Jansen P, et al. MC-LMAC: A Multi-channel MAC Protocol for Wireless Sensor Networks[J]. Ad Hoc Networks, 2011, 9(1): 73-94.

[8] Ahn G S, Hong S G, Miluzzo E, et al. Funneling-MAC: A Localized, Sink-oriented MAC for Boosting Fidelity in Sensor Networks[C]//Proc. of the 4th International Conference on Embedded Networked Sensor Systems. [S. l.]: ACM Press, 2006: 293-306.

[9] Incel O D. A Survey on Multi-channel Communication in Wireless Sensor Networks[J]. Computer Networks, 2011, 55(13): 3081-3099.

[10] Durmaz I O, Ghosh A, Krishnamachari B, et al. Fast Data Collection in Tree-based Wireless Sensor Networks[J]. IEEE Transactions on Mobile Computing, 2012, 11(1): 86-99.

[11] Ortiz J, Culler D. Multichannel Reliability Assessment in Real World WSNs[C]//Proc. of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks. New York, USA: ACM Press, 2010: 162-173.

[12] Le Hieu-Khac, Henriksson D, Abdelzaher T. A Practical Multi-channel Media Access Control Protocol for Wireless Sensor Networks[C]//Proc. of the 7th International Conference on Information Processing in Sensor Networks. [S. l.]: IEEE Computer Society, 2008: 70-81.

[13] Le Long, Rhee I. Implementation and Experimental Evaluation of Multi-channel MAC Protocols for 802.11 Networks[J]. Ad Hoc Networks, 2010, 8(6): 626-639.

编辑 陆燕菲