山西大学学报(自然科学版)48(5):880—887,2025
Journal of Shanxi University(Nat. Sci. Ed.)

DOI:10.13451/j.sxu.ns.2025082

基于格的高效环签名方案

任燕[1*],徐秋霞[2]

(1.运城学院 数学与信息技术学院, 山西 运城 044000;
2.广东技术师范大学 数学与系统科学学院, 广东 广州 510000)

摘　要:基于格的环签名方案不仅能抵抗量子计算机的攻击,还具有完全的匿名性,因此在电子投票、电子货币等方面有着广泛的应用。现有的基于格的环签名主要利用零知识证明和拒绝抽样技术两种方式实现。针对这些方案通信开销和成本较高、效率较低的问题,本文利用不可区分分布替代拒绝抽样、次高位比特替代原始数值相结合的方法,提出了一个基于格的高效环签名方案(Lattice-based Ring Signature Scheme with Near-high-bits Technique, NHB-LRS)。该方案无须像拒绝抽样技术一样重复多次,可一次成功生成签名,并有效减小密钥大小和签名尺寸。安全性分析表明,该方案具备环签名应有的不可伪造性和匿名性。效率分析结果进一步显示,在相同安全级别下,该方案展现出更高的运行效率、更低的通信代价以及更紧凑的签名结构,签名尺寸为同类型方案的10%。

关键词:基于格;环签名;数字签名
中图分类号:TP309.7　　**文献标志码**:A　　**文章编号**:0253-2395(2025)05-0880-08

An Efficient Lattice-based Ring Signature Scheme

REN Yan[1*], XU Qiuxia[2]

(1. *School of Mathematics and Information Technology, Yuncheng University, Yuncheng* 044000*, China;*
2. *School of Mathematics and Systems Science, Guangdong Polytechnic Normal University, Guangzhou* 510000*, China*)

Abstract: The lattice-based ring signature scheme not only resists attacks from quantum computers, but also has complete anonymity, making it widely used in electronic voting, electronic currency, and other fields. The existing lattice-based ring signatures are mainly implemented using two methods: zero knowledge proof and rejection sampling techniques. To address the issues of high communication overhead and cost, as well as low efficiency in these schemes, this paper proposes an efficient lattice-based ring signature scheme (Lattice-based Ring Signature Scheme with Near-high-bits Technique, NHB-LRS) by combining the methods of using indistinguishable distribution to replace rejection sampling and the Near-high-bits to replace the original numerical value. This method can successfully generate signatures in one go without the need for repeated operations, like the rejection sampling technique, and can effectively reduce the size of key and signature. Security analysis shows that this scheme possesses the unforgeability and anonymity that ring signatures should have. Furthermore, efficiency analysis results further show that the scheme achieves higher operational efficiency, lower communication costs, and a more compact signature structure under the same security level. The signature size is 10% of the same type of scheme.

Key words: lattice-based; ring signature; digital signature

收稿日期:2025-04-14;**接受日期**:2025-06-06
基金项目:国家自然科学基金(12201133);山西省回国留学人员科研资助项目(2023-169);山西省高校科技创新项目(2021L467);全国统计科学研究项目(2021LY047);广州市科技计划项(2023A04J0365);广东技术师范大学科研启动基金(2021SDKYA029)
* **通信作者**:任燕(1982—),女,山西运城人,博士,副教授,研究方向为密码学、信息安全。E-mail: renyan-2000@163.com
引文格式:任燕,徐秋霞.基于格的高效环签名方案[J].山西大学学报(自然科学版),2025,48(5):880-887. DOI:10.13451/j.sxu.ns.2025082.

0 引言

环签名是由Rivest等[1]于2001年提出的一种可以实现完全匿名的数字签名技术。在环签名方案中,签名者通过选择一个临时的集合,使用自己的私钥和集合中其他成员的公钥生成签名,验证者通过使用环中成员的公钥来验证签名的有效性。这个过程不需要经过其他成员的同意,验证者只能确认签名来自这个环集合,但是不能确定是环中哪个成员生成的签名,即验证者不能跟踪签名者的真实身份,保证了用户的匿名性,因此环签名方案在电子投票[2]、电子现金[3]、车联网[4]等领域具有广泛的应用。

随着量子计算机的提出,基于传统经典数论难解问题的密码体制变得不再安全,学者们开始积极寻找能够抵抗量子计算机攻击的新的密码算法。目前,抗量子安全的密码体制主要有基于哈希(Hash-based)、基于编码(Code-based)、基于多变量(Multivariate-based)、基于格(Lattice-based)4种。而其中基于格的密码体制的困难问题存在一般情况到最坏情况下的规约,且具有较高的算法效率和并行性,具有独特的优势,所以受到更多关注。

在基于格的环签名方案研究中,Brakerski和Kalai[5]首先在标准模型中提出了一种基于格的具有环陷门功能的通用环签名方案,主要基于非齐次的最短整数解问题(Inhomogeneous Short Integer Solution,ISIS)实现。但是,该方案仅在比较弱的安全定义下才是安全的,要达到完全的安全性,则需要进行低效的转换。Melchor等[6]将Lyubashevsky在文献[7]中提出的基于格的签名转换为环签名,但是这个方案并不实用。2016年,Libert等在文献[8]中提出了一种基于格的累加器,借助累加器和格理论中的零知识证明系统,构建了具有对数签名尺寸的环签名方案,但是,累加器中应用的零知识参数效率很低。Esgin等[9]采用文献[10-11]中提出的多对一零知识证明构造了一个基于格的环签名方案,与文献[8]相同,文献[9]中的方案也是对数大小,并且在随机预言模型中是安全的。此外,还有很多基于格的环签名方案被提出[12-16],但是这些方案均采用了拒绝抽样技术,需要不断重复,直至生成符合要求的签名。

总体来说,现有的基于格的环签名方案,要么使用了零知识证明,要么使用了拒绝抽样技术,具有花销大且签名尺寸大的问题。为解决这些问题,本文采用不可区分分布替代拒绝抽样,次高位比特代替原始数值相结合的方法,提出了一种基于格的高效环签名方案(Lattice-based Ring Signature Scheme with Near-high-bits Technique, NHB-LRS)。该方法可以不重复成功地生成签名,而且可减小签名尺寸。

1 预备知识

1.1 符号说明

本文中使用的符号定义见表1。

表1 符号及含义

Table1 Symbols and meanings

符号	含义
Z	整数集合
q	一个奇素数
Z_q	整数模q取在区间$\left[-\frac{q}{2},\frac{q}{2}\right]$的余数
R	实数集合
$[N]$	集合$\{1,2,\cdots,N\}$
R_q	一个商环$R_q=Z_q[x]/<x^n+1>$
$\boldsymbol{R}_q^{h\times v}$	h与v分别表示矩阵的行数与列数
$\boldsymbol{R}_q^{v}$	v表示向量的维数

1.2 困难问题

公钥密码学中,密码方案的安全性一方面依赖于私钥的安全性,另一方面依赖于求解密码方案底层数学假设的困难程度,基于格的密码学也不例外。Albrecht和Bos等[17-18]的研究表明,秩大的具有模运算的格比理想格能抵抗更多的攻击,同时,模运算的格假设仍然可以保留格的结构来构建大量的短而可逆的元素,因此,本方案主要基于模格上的小整数解(Module Short Integer Solution,MSIS)、搜索模格上的容错学习(Search Module Learning with Errors,S-MLWE)、判定模格上的容错学习(Decision Module Learning with Errors,D-MLWE)三个格上的困难问题及其变体,具体给出下面的困难假设:

定义1 MSIS 问题:给定一个随机矩阵 $\boldsymbol{A}\in\boldsymbol{R}_q^{h\times v}$,找到一个向量 $\boldsymbol{r}\in\boldsymbol{R}_q^v$,使得 $\boldsymbol{Ar}=0$,其中 $\boldsymbol{r}\neq\vec{0}$ 且 $\|\boldsymbol{r}\|_2\leqslant t$,是困难的。

定义2 S-MLWE 问题:均匀随机地选择一个向量 $\boldsymbol{r}\in\boldsymbol{S}_\beta^v$,给定 $\boldsymbol{A},\boldsymbol{s}$,其中 $\boldsymbol{A}\in\boldsymbol{R}_q^{h\times v}$ 为一个随机矩阵,$\boldsymbol{s}=\boldsymbol{Ar}$,找到一个向量 $\boldsymbol{r}'\in\boldsymbol{S}_\beta^v$,使得 $\boldsymbol{s}=\boldsymbol{Ar}'$,其中 $0\leqslant\|\boldsymbol{r}'\|_\infty\leqslant\beta$,是困难的。

定义3 D-MLWE 问题:随机给定 $\boldsymbol{A}\leftarrow\boldsymbol{R}_q^{h\times v},\boldsymbol{u}\leftarrow\boldsymbol{R}_q^h$ 及 $\boldsymbol{r}\in\boldsymbol{S}_\beta^v$,$(\boldsymbol{A},\boldsymbol{Ar})$ 与 $(\boldsymbol{A},\boldsymbol{u})$ 的分布是不可区分的,其中 $\leftarrow$ 表示从集合中随机选取。

1.3 数学工具

1.3.1 范数

对于 $f=\sum_i f_i X_i\in R$,给出 f 的范数定义如下:

$$l_1:\|f\|_1=\sum_i|f_i|;\ l_2:\|f\|_2=\Big(\sum_i|f_i|^2\Big)^{\frac{1}{2}};\ l_\infty:\|f\|_\infty=\max|f_i|。$$

1.3.2 次高比特

假设 $2^t<q<2^{t+1}$,且 $2\leqslant\mu<t$,令 $D_q=\left\lfloor\frac{q}{2}\right\rfloor$,对每个

$$a=\pm b \bmod q, a\in Z, 0\leqslant b<\frac{q}{2},$$

将 b 的前 μ 比特记作 a_1,则

$$a\equiv\sigma\left(a_1 2^{t-\mu}+a_0\right)\bmod q,\sigma\in\{-1,1\},0\leqslant a_1<2^\mu \text{ 且 } 0\leqslant a_1 2^{t-\mu}+a_0\leqslant\frac{q}{2},$$

此时 a_1 为 $a \bmod q$ 的次于最高 μ 比特的数值,称为次高比特,记作

$$a_1=\text{Near}-\text{high}-\text{bits}(a,\mu,q)。$$

当 $a=\sum_{i=0}^{n-1}a[i]x^i\in R^n$ 为一个多项式时,对每个系数做如下处理:

$a_1[i]=\text{Near}-\text{high}-\text{bits}(a[i],\mu,q)$,这里 $a_1[i]$ 即为 $a[i]$ 的次高比特,$a_1=\sum_{i=0}^{n-1}a_1[i]x^i$ 称为多项式的次高比特。

次高比特具有如下性质:

对任意的 $a,\varepsilon\in Z,\mu\geqslant 1$,$a_1=\text{Near}-\text{high}-\text{bits}(a,\mu,q)$,$\tilde{a}_1=\text{Near}-\text{high}-\text{bits}(a+\varepsilon,\mu,q)$,如果 $|\varepsilon|\leqslant 2^{t-\mu-1}$,则 $-1\leqslant|\tilde{a}_1-a|\leqslant 2$。

这个性质说明,对给定的 a,有唯一的 a_1 与之对应,且 a 发生细微改变的同时,a_1 会发生较大改变,所以可以用次高比特来代替 a,作为密钥,从而减少密钥和签名尺寸,提高方案的效率。

1.4 环签名

环签名是一种可以用来保护签名者隐私的特殊数字签名。其基本原理是,在签名过程中将签名者组成一个环,在环上生成一个临时公私钥对,并利用临时公钥对进行签名。其他人可以验证签名的有效性,但无法确定签名者的身份。一个环签名方案由以下四种算法组成:

初始化Setup:该算法的输入是一个安全参数,输出为公共参数。

密钥生成KeyGen:该算法的输入是公共参数,输出为环中每位用户的公钥和私钥。

签名生成Sign:该算法的输入是公共参数、要签名的消息m、签名者的私钥、环成员的公钥列表,输出为签名。

验证算法Verify:该算法的输入是消息m上的签名,输出为$b\in\{0,1\}$,其中1表示签名有效,0表示签名无效。

1.5 安全模型

一个好的环签名方案必须具有正确性、不可伪造性、匿名性等特性。

令$L=\{pk_i|i\in\{1,2,\cdots,N\}\}$表示签名方案中用户的公钥列表,$O_K$表示密钥生成预言机、$O_S$表示签名预言机、$O_H$哈希预言机,功能分别如下:

O_K:基于输入的pk_i,输出相应的sk_i。

O_S:基于输入的一个公钥集$L=\{pk_1,pk_2,\cdots,pk_N\}$(其中$pk_i$是由$O_K$生成的),一个消息$m$,输出一个有效的签名$\sigma'$。

O_H:输出一个哈希值。

定义4 正确性。如果合法签名者通过签名算法生成的签名正确,验证算法输出1的概率为1。

定义5 不可伪造性。对于多项式时间的敌手C和模拟器S,赢得以下游戏的优势记为Adv_C^{unf}。如果该优势可以忽略不计,则称环签名是不可伪造的。游戏过程如下:

(1)C可以获得S生成的公钥列表L。

(2)S获得环签名$\sigma_L(m)$。

(3)C调用Verify算法输出b。

(4)当下列条件满足时,就说敌手C赢得游戏:

— 输出的b为1;

— 敌手C只查询$pk\notin L$;

—(L,m)没有要求被签名。

(5)$Adv_C^{unf}=\Pr[b=1]$。

定义6 匿名性。对于多项式时间的敌手C和模拟器S,赢得以下游戏的优势记为Adv_C^{ano},如果该优势可以忽略不计,则称环签名具有匿名性。游戏过程如下:

(1)C发送L,m给S,其中$L=\{pk_0,pk_1\}$,m是消息。

(2)S在$b=\{0,1\}$中随机选择一个b。

(3)S调用Sign算法计算σ_b。

(4)S将σ_b发送给C。

(5)C输出$b'=\{0,1\}$。

(6)当下列条件满足时,就说敌手C赢得游戏:

— pk_0,pk_1不能使用O_K与O_S;

— $b=b'$的概率为$\frac{1}{2}$。

2 NHB-LRS方案的构造

本文所构造的方案,主要利用不可区分的分布来代替拒绝样本,次高位比特代替原始数相结合的方法,该方法成功生成签名的概率为1。本方案包含一个签名者和一组其他成员的公钥,有初始化Setup,密钥生成算法KeyGen,签名算法Sign,验证算法Verify四个算法,下面给出具体描述。

2.1 **初始化阶段**Setup

该算法的输入为1^{λ},输出为$\boldsymbol{A}' \leftarrow \boldsymbol{R}_q^{h\times v}$、$Z_\beta = \left\{x \in Z, \|x\|_\infty \leqslant \beta\right\}$,$H$是一个映射到$Z_1{}^v$的哈希函数。

2.2 **密钥生成算法**KeyGen

KeyGen算法的输入是$\boldsymbol{A}'$,对于第i个用户,按照如下过程生成公私钥对:

(1)计算$\boldsymbol{A} = \text{Near} - \text{high} - \text{bits}(\boldsymbol{A}', \mu, q)$;

(2)均匀随机地选取$\boldsymbol{r}_i \leftarrow Z_\beta{}^v$;

(3)计算$\boldsymbol{PK}_i = \boldsymbol{A}\boldsymbol{r}_i$,私钥$\boldsymbol{SK}_i = \boldsymbol{r}_i$。

$(\boldsymbol{PK}_i, \boldsymbol{SK}_i)$即为算法输出的密钥对,其中$\boldsymbol{PK}_i$是公钥,$\boldsymbol{SK}_i$是私钥。

2.3 **签名算法**Sign

签名者为$\pi \in [1, N]$,其选择的环成员集合为$S = [1, N]$,此时环成员的公钥形成一个环,签名者使用自己的私钥对消息进行签名,因此Sign算法的输入是签名者的私钥r_π、消息m、各用户的公钥列表$L = \{\boldsymbol{PK}_i | i = 1, 2, \cdots, N\}$和公共参数$\boldsymbol{A}$,其输出是签名$\sigma$。签名的细节如下:

(1)计算$\boldsymbol{d}_{\pi+1} = H(L, m, \boldsymbol{A})$;

(2)当$i = \pi + 1, \pi + 2, \cdots, N, 1, \cdots, \pi - 1$时:

随机选择$\boldsymbol{r}_{z,i} \leftarrow Z_\beta^v$,计算$\boldsymbol{d}_{i+1} = H(L, m, \boldsymbol{t}_i)$,其中$\boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_{z,i} - \boldsymbol{d}_i\boldsymbol{PK}_i - \boldsymbol{A}$;

(3)计算$\boldsymbol{r}_{z,\pi} = \boldsymbol{d}_\pi \boldsymbol{r}_\pi$。

签名为$\sigma = (\boldsymbol{d}_1, \boldsymbol{r}_{z,i})(i = 1, 2, \cdots, N)$。

2.4 **验证算法**Verify

此算法的输入是消息m、签名σ、公钥$\boldsymbol{PK}$和公共参数$\boldsymbol{A}$,输出是0或1,0表示签名是无效的,1表示签名是有效的。验证者通过如下过程验证签名的正确性:

当$i = 1, 2, \cdots, N$计算:

(1)$\boldsymbol{t}' = \boldsymbol{A}\boldsymbol{r}_{z,i} - \boldsymbol{d}_i\boldsymbol{PK}_i - \boldsymbol{A}$;

(2)$\boldsymbol{d}'_{i+1} = H(L, m, \boldsymbol{t}'_i)$。

如果$\boldsymbol{d}'_1 = \boldsymbol{d}_1$输出1,否则输出0。

3 方案的正确性和安全性分析

下面将证明我们方案的验证算法是正确的。

定理1 算法的验证过程是正确的。

证明 验证算法的流程如下:

如果$i \neq \pi$, $\boldsymbol{d}'_{i+1}$可由Sign算法求得;

如果$i = \pi$,则

$$\boldsymbol{t}' = \boldsymbol{A}\boldsymbol{r}_{z,i} - \boldsymbol{d}_\pi \boldsymbol{PK}_\pi - \boldsymbol{A} = \boldsymbol{A}\boldsymbol{d}_\pi \boldsymbol{r}_\pi - \boldsymbol{d}_\pi \boldsymbol{A}\boldsymbol{r}_\pi - \boldsymbol{A} = \boldsymbol{A},$$

所以,在这种情况下有$\boldsymbol{d}'_{i+1} = \boldsymbol{d}_{i+1}$,综上,验证过程是正确的。

方案的安全性证明由如下两个定理给出。

定理2 在MSIS假设下,本文提出的方案是不可伪造的。

证明 假设敌手C可以伪造环签名,我们将证明存在一个多项式算法能以不可忽略的概率解决MSIS问题。

假设有一个模拟器S,在随机预言机模式下,它可以在不知道用户的私钥的情况下输出签名者的签名。

模拟器S的工作原理如下所示。

Setup

(1)选择一个$pk_\pi \in L$;

(2)制造一个密钥生成预言机O_K,通过它获得pk_π相应的私钥sk_π。

Hashquery

假设敌手C可以在O_H中进行查询,H的响应为$(\boldsymbol{d}_1,\boldsymbol{d}_2,\cdots,\boldsymbol{d}_w)$,将被敌手保存在$H$-list中。

Signature

在这个过程中,敌手C使用Hashquery的结果,执行以下操作:

选择$\boldsymbol{d}_{\pi+1}\in\boldsymbol{Z}_1^v$;

当$i=\pi+1,\pi+2,\cdots,N,1,\cdots,\pi-1$时,

(1)随机选择$\boldsymbol{r}_{z,i}\leftarrow\boldsymbol{Z}_\beta^v$;

(2)计算$\boldsymbol{t}_i=\boldsymbol{A}\boldsymbol{r}_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A}$;

(3)计算$\boldsymbol{d}_{i+1}=H(L,m,\boldsymbol{t}_i)$。

设置$\boldsymbol{d}_{\pi+1}=H(L,m,\boldsymbol{A})$;

返回$(\boldsymbol{d}_1,\boldsymbol{r}_{z,i})$。

如果签名可以通过验证算法,那么我们认为$\boldsymbol{d}_{i+1}$是在C进行Hashquery之后获得的。

现在,我们比较伪造签名和合法签名,我们可以看到

$$\mathrm{d}'_{i+1}=H(L,m',\boldsymbol{t}'_i)=H(L,m',\boldsymbol{A}\boldsymbol{r}'_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A})=H(L,m,\boldsymbol{A}\boldsymbol{r}_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A})=\boldsymbol{d}_{i+1}$$

如果$m\neq m',\boldsymbol{A}\boldsymbol{r}'_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A}\neq\boldsymbol{A}\boldsymbol{r}_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A}$,可以找另外一个$\boldsymbol{d}_j$。

这样,我们有

$$m=m',\boldsymbol{A}\boldsymbol{r}'_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A}=\boldsymbol{A}\boldsymbol{r}_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A},$$

即

$$\boldsymbol{A}(\boldsymbol{r}'_{z,i}-\boldsymbol{r}_{z,i})=0。$$

我们假设$\boldsymbol{r}'_{z,i}\neq\boldsymbol{r}_{z,i}$,所以$C$可以通过两个方程找到一个非零向量$\boldsymbol{r}=\boldsymbol{r}'_{z,i}-\boldsymbol{r}_{z,i}$使$\boldsymbol{A}\boldsymbol{r}=0$,这意味着$C$可以解决MSIS问题。

定理3 本文提出的方案在D-MLWE假设下满足匿名性。

证明 假设模拟器S可以在不知道l的私钥$\boldsymbol{r}_l$的情况下输出签名者l的签名。输出的签名与真实签名不可区分。模拟器S的操作如下:

Setup

假设m是要签名的消息,L是公钥列表,用D_t表示任意$0<t<N$的集合。选择一个$\boldsymbol{pk}_i\in L,\boldsymbol{sk}_i\in D_t$,$(\boldsymbol{pk}_i,\boldsymbol{sk}_i)$不是由KeyGen生成的。

Hashquery

假设模拟器S可以在H中进行查询,H的响应为$(\boldsymbol{d}_1,\boldsymbol{d}_2,\cdots,\boldsymbol{d}_w)$,将被模拟器保存在$H$-list中。

Signature

在这个过程中,模拟器S使用Hashquery的结果,做以下操作。

选择$\boldsymbol{d}_1\in\boldsymbol{Z}_1{}^v$;

当$i\in\{1,2,\cdots,N\}$时

随机选择$\boldsymbol{r}_{z,i}\leftarrow\boldsymbol{Z}_\beta^v$,计算$\boldsymbol{t}_i=\boldsymbol{A}\boldsymbol{r}_{z,i}-\boldsymbol{d}_i\boldsymbol{PK}_i-\boldsymbol{A}$,$\boldsymbol{d}_{i+1}=H(L,m,\boldsymbol{t}_i)$;

设置$\boldsymbol{d}_1=H(L,m,\boldsymbol{t}_1)$;

返回$(\boldsymbol{d}_1,(\boldsymbol{r}_{z,i})_{i\in[N]})$。

该签名可以通过验证算法,然后考虑$\boldsymbol{d}_1$。在真实签名中,$\boldsymbol{d}_1$来自哈希函数的值,是均匀随机分布的,在模拟过程中,$\boldsymbol{d}_1$从D中选择。

现在,我们比较伪造签名和合法签名,我们可以看到$\boldsymbol{r}_{z,i}$是从$\boldsymbol{Z}_\beta^v$中随机选择的。但是,敌手可以正确地区分$\boldsymbol{d}_1$和生成的签名。也就是说$(\boldsymbol{A},\boldsymbol{A}\boldsymbol{r}_{z,\pi})$和$(\boldsymbol{A},\boldsymbol{r}_{z,i})$是可区分的,其中$\boldsymbol{r}_{z,i}$是随机的,从而解决了D-MLWE问题。

4 安全参数

基于格的签名方案的实用性很大程度上取决于通信和存储开销,特别是签名的尺寸。本节主要讨论我们方案的参数选择和签名尺寸分析。

我们方案的签名形式为$(\boldsymbol{d}_1,\boldsymbol{r}_{z,i})$,有两部分组成,其中:

$\boldsymbol{d}_1$由3个多项式组成,每个系数的取值范围为$\{-1,0,1\}$,每个系数需要2比特;

对于每个$\boldsymbol{r}_{z,i}$,它由3个多项式组成,每个系数的取值范围为$\{-(\beta+1),\beta+1\}$,其中$\beta=1$,每个系数需要3比特,因此共需要:

$$(1\times 3\times n+N\times 3\times 3\times n)\text{bits}=\frac{(0.375+1.125N)n}{1\,024}\text{KiB}$$

,其中N为环中用户数量,n为多项式的次数。

当多项式的次数取1 024时,方案的参数设置和签名尺寸如表2所示。

我们提出的NHB-LRS方案与文献[19]中提出的基于格的环签名和文献[20]中提出的L2RS方案在不同用户数量下的签名尺寸对比如图1所示。

结果表明,本方案的签名长度与用户数量呈线性关系,且尺寸仅为上述两种方案的十分之一,综合比较,本方案的存储空间要求更低,通信开销更小,实用性更强。

表2 方案的参数设置与签名尺寸

Table 2 Parameter settings and signature sizes for scheme

参数	尺寸
q	2^{32}
n(多项式的次数)	1 024
λ(安全参数)	100
h	1
v	3
S_β中的β	1
次高比特的位数μ	2^{30}
公钥	1.125 KiB
N=1	1.5 KiB
N=8	9.375 KiB
N=32	36.375 KiB
N=128	144.375 MiB

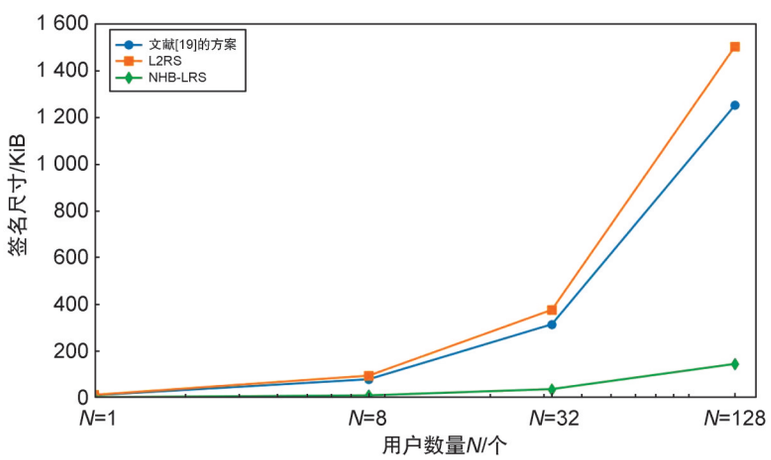

图1 签名尺寸对比

Fig. 1 Comparison of signature sizes

5 结论

基于格的环签名方案作为一类抗量子安全的数字签名技术,在后量子时代有着广泛的应用前景,但现有的方案效率较低、通信代价较高。本文以不可区分分布替代拒绝抽样、次高位比特代替原始数值相结合的方法,构造了一个更高效的基于格的环签名方案,并证明了方案的安全性。因该方法能够一次性成功生成签名,不需重复操作,提高效率的同时,还可有效减小签名尺寸,实用性更强。后续的工作,可采用相同的思想构造具有其他功能的抗量子安全数字签名方案。

参考文献:

[1] RIVEST R L, SHAMIR A, TAUMAN Y. How to Leak a Secret[C]//Advances in Cryptology-ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia: Springer, 2001: 552-565. DOI: 10.1007/3-540-45682-1_32.

[2] RODRÍGUEZ-HENRÍQUEZ F, ORTIZ-ARROYO D, GARCÍA-ZAMORA C. Yet Another Improvement over the Mu-Varadharajan E-voting Protocol[J]. *Comput Stand Interfaces*, 2007, **29**(4): 471-480. DOI: 10.1016/j.

csi.2006.11.003.

[3] LIBERT B, LING S, NGUYEN K, *et al*. Zero-knowledge Arguments for Lattice-based PRFS and Applications to E-cash[C]//Advances in Cryptology – ASIACRYPT 2017. Cham: Springer, 2017: 304−335. DOI: 10.1007/978-3-319-70700-6_11.

[4] PRIYA J C, PRAVEEN R, NIVITHA K, *et al*. Improved Blockchain-based User Authentication Protocol with Ring Signature for Internet of Medical Things[J]. *Peer Peer Netw Appl*, 2024, **17**(4): 2415−2434. DOI: 10.1007/s12083-024-01716-9.

[5] BRAKERSKI Z, KALAI Y T. A Framework for Efficient Signatures, Ring Signatures and Identity Based Encryption in the Standard Model[J/OL]. *IACR Cryptology ePrint Archive*, 2010: 086. https://eprint.iacr.org/2010/086.pdf

[6] MELCHOR A C, BETTAIEB S, BOYEN X, *et al*. Adapting Lyubashevsky's Signature Schemes to the Ring Signature Setting[M]//Progress in Cryptology-AFRICACRYPT 2013. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013: 1−25. DOI: 10.1007/978-3-642-38553-7_1.

[7] LYUBASHEVSKY V. Lattice Signatures Without Trapdoors[C]//Advances in Cryptology−EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques. Cambridge, USA: Springer, 2012: 738−755. DOI: 10.1007/978-3-642-29011-4_43.

[8] LIBERT B, LING S, NGUYEN K, *et al*. Zero-knowledge Arguments for Lattice-based Accumulators: Logarithmic-size Ring Signatures and Group Signatures without Trapdoors[M]//Advances in Cryptology-EUROCRYPT 2016. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 1−31. DOI: 10.1007/978-3-662-49896-5_1.

[9] ESGIN M F, STEINFELD R, SAKZAD A, *et al*. Short Lattice-based One-out-of-many Proofs and Applications to Ring Signatures[M]//Applied Cryptography and Network Security. Cham: Springer International Publishing, 2019: 67−88. DOI: 10.1007/978-3-030-21568-2_4.

[10] GROTH J, KOHLWEISS M. One-out-of-many Proofs: Or how to Leak a Secret and Spend a Coin[M]//Advances in Cryptology-EUROCRYPT 2015. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015: 253−280. DOI: 10.1007/978-3-662-46803-6_9.

[11] BOOTLE J, CERULLI A, CHAIDOS P, *et al*. Short Accountable Ring Signatures Based on DDH[M]//Computer Security-ESORICS 2015. Cham: Springer International Publishing, 2015: 243−265. DOI: 10.1007/978-3-319-24174-6_13.

[12] WANG J, SUN B. Ring Signature Schemes from Lattice Basis Delegation[M]//Information and Communications Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 15−28. DOI: 10.1007/978-3-642-25243-3_2.

[13] 贾小英, 何德彪, 许芷岩, 等. 格上高效的基于身份的环签名体制[J]. 密码学报, 2017, **4**(4): 392−404. DOI: 10.13868/j.cnki.jcr.000191.
JIA X Y, HE D B, XU Z Y, *et al*. An Efficient Identity-based Ring Signature Scheme over a Lattice[J]. *J Cryptologic Res*, 2017, **4**(4): 392−404. DOI: 10.13868/j.cnki.jcr.000191.

[14] 汤永利, 夏菲菲, 叶青, 等. 格上基于身份的可链接环签名[J]. 密码学报, 2021, **8**(2): 232−247. DOI: 10.13868/j.cnki.jcr.000433.
TANG Y L, XIA F F, YE Q, *et al*. Identity-based Linkable Ring Signature on Lattice[J]. *J Cryptologic Res*, 2021, **8**(2): 232−247. DOI: 10.13868/j.cnki.jcr.000433.

[15] KUMAR R, PADHYE S. A Lattice-based Ring Signature Scheme with Gradual Revelation of Non-signers [J]. *Int J Inf Technol*, 2025, **17**(1): 567−574. DOI: 10.1007/s41870-024-02275-1.

[16] GAO W, HU Y P, WANG B C, *et al*. Improved Lattice-based Ring Signature Schemes from Basis Delegation [J]. *J China Univ Posts Telecommun*, 2016, **23**(3): 11−28. DOI: 10.1016/S1005-8885(16)60027-4.

[17] ALBRECHT M R, DEO A. Large Modulus Ring-LWE ≥ Module-LWE[C]//International Conference on the Theory and Applica− tion of Cryptology and Information Security. Cham, Switzerland: Springer, 2017: 267−296. DOI: 10.1007/978-3-319-70694-8_10.

[18] BOS J, DUCAS L, KILTZ E, *et al*. CRYSTALS - Kyber: A CCA-secure Module-lattice-based KEM[C]//2018 IEEE European Symposium on Security and Privacy (EuroS&P). New York: IEEE, 2018: 353−367. DOI: 10.1109/EuroSP.2018.00032.

[19] BAUM C, LIN H, OECHSNER S. Towards Practical Lattice-based One-time Linkable Ring Signatures[M]//Information and Communications Security. Cham: Springer International Publishing, 2018: 303−322. DOI: 10.1007/978-3-030-01950-1_18.

[20] TORRES W A, STEINFELD R, SAKZAD A, *et al*. Post-quantum One-time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT V1.0) [M]//Information Security and Privacy. Cham: Springer International Publishing, 2018: 558−576. DOI: 10.1007/978-3-319-93638-3_32.