Software Engineering and Applications 软件工程与应用, 2022, 11(5), 1064-1070
Published Online October 2022 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2022.115109

Hans汉斯

基于格上的一次群签名方案

侯　建，李子臣，张珍珍

北京印刷学院数字版权保护技术研究中心，北京

收稿日期：2022年7月21日；录用日期：2022年10月11日；发布日期：2022年10月20日

摘　要

传统的签名方案大多基于离散对数困难问题和大整数的素数分解问题，不能抵抗量子计算的攻击。针对此问题，本文基于格上ISIS困难问题，提出了一种新的一次群签名方案，并证明了方案的正确性、签名的不可伪造性、签名者的匿名性。新方案只需要密码杂凑算法的计算，具有更高的效率。

关键词

格，最小整数解问题，量子攻击，一次群签名

Lattice-Based Primary Group Signature Scheme

Jian Hou, Zichen Li, Zhenzhen Zhang

Digital Copyright Technology Research Center, Beijing Institute of Graphic Communication, Beijing

Received: Jul. 21st, 2022; accepted: Oct. 11th, 2022; published: Oct. 20th, 2022

Abstract

Traditional signature schemes are mostly based on discrete logarithmic hard problems and prime factorization problems of large integers, which cannot resist the attack of quantum computing. Aiming at this problem, this paper proposes a new primary group signature scheme based on the difficult problem of ISIS on the lattice, and proves the correctness of the scheme, the unforgeability of the signature and the anonymity of the signer. The new scheme only needs the calculation of the cryptographic hash algorithm and has higher efficiency.

Keywords

Lattice, SIS (Short Integer Solution), Quantum Attack, Primary Group Signature

文章引用: 侯建, 李子臣, 张珍珍. 基于格上的一次群签名方案[J]. 软件工程与应用, 2022, 11(5): 1064-1070.
DOI: 10.12677/sea.2022.115109

1. 引言

1991 年，Chaum 等人[1]提出了群签名方案。群签名方案允许群中的任一合法成员都可以代表群对消息进行匿名签名，在验证的过程中，只需要群公钥，同时签名不可伪造。如果需要进一步确定签名者身份，需要群管理员用追踪密钥找出签名者并核实其身份信息。群签名的这些特征，使得它在电子货币、电子商务、电子投票等领域得到很好地应用。一次性签名作为一种特殊的签名方式，其原理是基于无陷门单向密码杂凑函数对输入的消息进行签名。签名的安全性取决于密码杂凑函数安全。因此，一次签名方案具有较高的安全性和签名生成、验证的效率。本文一次群签名是在群签名的过程中暴露部分私钥。每签名一次更换一次密钥，来保证签名的绝对安全性。

随着量子计算的飞速发展，传统群签名方案的安全性受到了严重威胁，例如基于 RSA、ElGamal、ECC 等公钥密码体制的群签名方案[2] [3]。因此，急需研究设计能够抵御量子计算机攻击的群签名方案。基于格上的一次群签名算法方案具有效率高、抗量子计算机攻击等特点，成为当前后量子密码算法研究热点之一。

1979 年，Lamport [4]等人提出了一种基于单向函数的一次数字签名方案。由此引出了利用单向密码杂凑算法进行数字签名的研究，但由于该方案中需要存储大量的密钥，使得该方案在实际应用中受限。2010 年，Dov Gordon、Katz 和 Vaikuntanathan 在亚洲密码学会上第一次提出基于错误学习问题(LWE)设计的基于格的群签名方案[5] (简称 GKV 方案)。然而，GKV 方案在防止陷害攻击方面存在缺陷，其中，群管理员会盗用合法群成员进行签名，并且不能有效地管理群成员的加入和退出，使得签名的长度会随着群成员的增加而增长。2013 年，Laguillaumie、Langlois、Libert 和 Stehlé 在亚洲密码学会上对基于格的群签名方案进行了改进[6]，该方案解决了群签名长度随成员个数快速增长的问题，使得群成员个数与群签名长度满足对数关系。但是，该方案中采取加解密来设计追踪机制，使得签名效率大大降低，同时，还需要满足“加密方案”是安全的。2015 年，Nguyen、Jiang Zhang 和 Zhenfeng Zhang 为了使签名长度摆脱全成员的依赖，提出了基于 LWE 和小整数解问题(SIS)的格上群签名方案[7]，然而，该签名方案不能有效地管理群成员的加入和退出，在防止陷害攻击方面仍存在漏洞。2006 年，Zhou 等人提出了一种基于混沌的 Hash 函数，可以极大地提高数字签名的安全性能[8]。然而，该方案依赖 RSA 公钥密码体制，数字签名仍存在依赖大整数分解的困难性，在量子计算机的时代，无法抵抗后量子时代的量子攻击。在最近设计的基于格的群签名方案中[9] [10] [11] [12] [13]，仍然存在随着群成员的个数的增多，签名长度也在快速增加的问题。

本文针对上述问题，结合基于格上 ISIS 困难问题，提出了一个新的基于格上的一次群签名方案。该方案在整个算法的设计中用到了格的 One-Way Function (OWF)，在签名密钥和群公钥产生的过程中，通过哈希函数来计算，并将一次性签名融入其中，能够抵抗已知攻击，其安全性是利用哈希函数的单向性来保障，因为安全的哈希函数会有更多次扩散和混淆，原理是通过循环迭代一种特殊的结构使其更加安全，能抵抗量子计算的攻击。

2. 格上的困难问题

本文所设计的一次群签名方案是基于格上的困难问题，为便于理解，本节首先介绍格上的一些基本概念和安全模型。

设共有 m 个线性无关的向量 $v_1, v_2, \cdots, v_m \in R^n$，产生的集合：$\wedge(v_1, v_2, \cdots, v_m) = \left\{ \sum_{i=1}^{m} t_i v_i \mid t_i \in Z \right\}$ 称为格。

LWE (Learning With Error)问题：已知整数 $n, m \geq n, q > 2$，矩阵 $A \in Z_q^{n \times m}$，向量 $v \in Z_q^n$，概率分布 χm，向量 e 服从 Z_q^m 上的分布 χm，则可分为两类：

1) 搜索版本的 LWE：基于等式 $v^t = s^t A + e^t$，找到 s 的值。

2) 判定版本的 LWE：判定 v^t 是均匀选取的还是由公式 $v^t = s^t A + e^t$ 计算得出的。

SIS 问题(Small Integer Solutions Problem)：我们可以根据已知条件 $q \in Z, \beta \in R, A \in Z_q^{n \times m}$，找到一个向量(非 0) $v \in Z^m$，使得等式 $Av = 0 \bmod q$ 成立，并且满足条件 $\|v\| \leq \beta$。

ISIS 问题(Inhomogeneous Minimum Integer Solution Problem)：已知 $q \in Z, \beta \in R, A \in Z_q^{n \times m}$，向量 $u \in Z_q^n$，可以找到非零向量 $v \in Z^m$，使得 $Av = u \bmod q$，并且 $\|v\| \leq \beta$。

这个单向函数(OWF)的构造如下。首先，我们随机选取一个 $n \times m$ 阶的矩阵 $A \in \mathbb{Z}_q^{n \times m}$，然后，我们这个 OWF 的输入就是一个二进制向量 $x \in \{0,1\}^m$。这个 OWF 的输出则是：$f_A(x) = Ax \bmod q$。记 $H = f_A(x) = Ax \bmod q$。

2.1. 格上选择明文攻击(CPA)模型

现在的数字签名方案中，很多的学者利用 Chosen-Plaintext Attack (CPA)模型来证明其方案的安全性。

CPA 是一种典型的攻击模型。在限定的时间内，攻击者 F 会随机选择消息，通过询问随机预言机 O 来获得对消息的签名，并通过刚刚拿到的签名来构造一个合法的消息签名 $(M', \sigma^{M'})$。其中，图 1 展示了该过程。伪造者 F 给随机预言机 O 发送消息集合 $(M^1, M^2, \cdots, M^n)$，随机预言机将得到的签名集合 $(\sigma^1, \sigma^2, \cdots, \sigma^n)$ 再发送给 F。通过这些签名集合，F 可以伪造一个消息－签名对 $(M', \sigma^{M'})$。如果 $\sigma^{M'}$ 是合法的，并且消息 M' 不在询问的消息中，则 F 伪造成功。CPA-Secure-Model 模型原理是利用伪造者 F 成功的概率极小，并且这个概率可以忽略不计。

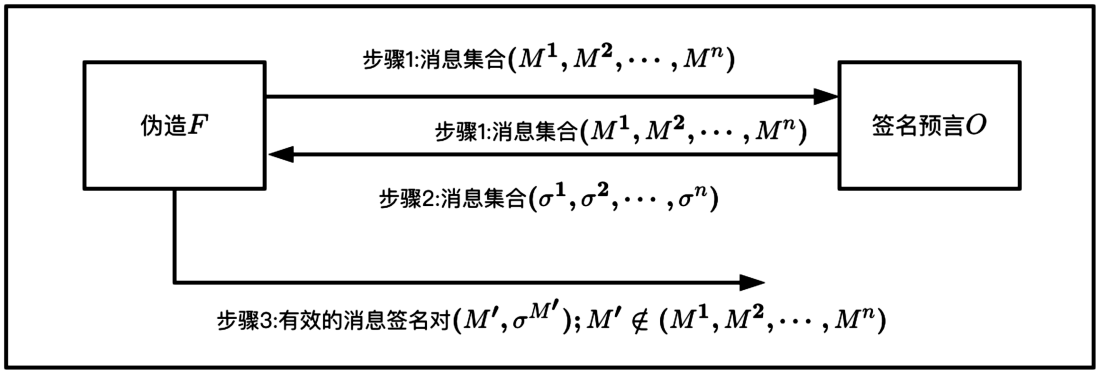

Figure 1. CPA model diagram
图 1. CPA 模型图

2.2. 格上非交互零知识证明

在 2013 年，基于 ISIS 问题的一个零知识证明被 Lauillaumie 等提出，只需要一个 Fiat-Shamir 转换，就能得到一个 ISIS 关系的非交互零知识证明(NIZKP)：$R_{ISIS} = \{(A, y, \beta, x) \mid \exists x \in Z_q^m, Ax = y \bmod q, \|x\| \leq \beta\}$，这里，$A \in Z_q^{n \times m}, y \in Z_q^m, \beta \in R$。

3. 基于 ISIS 群签名方案的设计

本文选取基于格上的哈希函数，提出了一种基于格上的一次群签名方案。该方案不仅在生成消息摘要的过程中使用哈希函数，而且在生成密钥算法、签名算法和验证算法中都是依赖此哈希函数。

3.1. 签名密钥的产生

假设群中有 m ($m \geq 2$)个群成员，群中每个成员选取 n 个二进制向量 $g_{ki} \in \{0,1\}^n$，$(1 \leq k \leq m, 1 \leq i \leq n)$，令 $X_k = \left(g_{k_1}, g_{k_2}, \cdots, g_{k_n}\right)$，那么， X_k 为成员 k 的签名私钥。

3.2. 群公钥产生

对于群中每个成员，计算 n 个二进制向量私钥的哈希值，并进行异或计算得到代表自己身份的 B_k，即 $B_k = H\left(g_{k_1}\right) \oplus H\left(g_{k_2}\right) \oplus \cdots \oplus H\left(g_{k_n}\right)(1 \leq k \leq m)$，其中，$H$ 为哈希运算。然后，这 m 个群成员分别将自己的 B_k 通过安全信道传输给可信第三方(TA)，这样，TA 将得到 m 个 n 维二进制向量 $B_1, B_2, \cdots, B_m$。TA 将收到的 $B_1, B_2, \cdots, B_m$ 进行异或并求哈希得到群公钥 $C_k = H\left(B_1 \oplus B_2 \oplus \cdots \oplus B_m\right)$。

3.3. 签名过程

群中的所有成员都可以对消息进行签名，若由第 k 个成员进行签名，则签名过程如下：

假设消息为 $M \in \{0,1\}^*$，计算消息 M 的摘要 $d = (d_1, d_2, \cdots, d_n)$，其中， $d_i \in \{0,1\}^n$。

第 k 个成员将表示自己身份的 B_k 发送给 TA，TA 通过群成员的身份集 $\left(B_1, B_2, \cdots, B_m\right)$ 验证他是否为合法的群成员里的一员。如果未通过，直接丢弃该请求；若验证通过，被判定为群内一员，TA 计算 $Y_k = \sum_{j \neq k} \oplus B_j$ 并将 Y_k 发送给该成员 k。该群成员根据自己的签名密钥和可信第三方发送过来的 Y_k 对消息进行签名。

具体签名过程如下：

当 d_i 向量中的 0 的个数大于 $n-m$ 的时候，记 $d_i = \{0\}^n$，此时 g_{k_i} 保持不变；否则 $d_i = \{1\}^n$，求出 g_{k_i} 对应的 Hash 值 $H\left(g_{k_i}\right)$。在 $n+1$ 的位置将 Y_k 添加到签名中。

那么，对消息 M 的签名 $S = \left\{s_1, s_2, \cdots, s_n, Y_k\right\} \in^{\{n+1,m\}}$，其中：

$$s_i = \begin{cases} g_{k_i} & d_i = \{0\}^n \\ H\left(g_{k_i}\right) & d_i = \{1\}^n \end{cases} \quad (1 \leq i \leq n)。$$

3.4. 验证过程

验证者收到群签名后，首先计算消息 M 的摘要 $d = (d_1, d_2, \cdots, d_n)$。然后利用群公钥 C_k 对收到的签名 $S = \left\{s_1, s_2, \cdots, s_n, Y_k\right\}$ 进行验证。

首先，计算 $P = \left(P_1 \oplus P_2 \oplus \cdots \oplus P_n \oplus Y_k\right)$，其中：

$$p_i = \begin{cases} H\left(s_i\right) & d_i = \{0\} \\ s_i & d_i = \{1\} \end{cases} \quad (1 \leq i \leq n)。$$

计算 $H(P) \oplus C_k$ 的值是否等于 $0 \in \{0\}^n$。若相等，则认为得到的签名消息有效，否则无效，说明该签名为非法签名。

具体的签名和验证过程如图 2 所示。

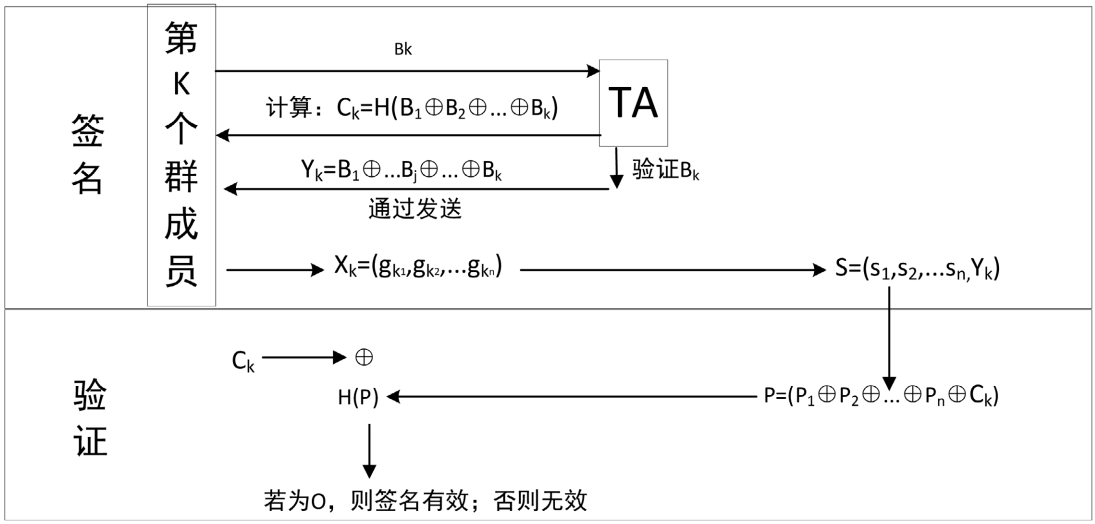

Figure 2. Signing and verification process
图 2. 签名和验证过程

下面对上述签名方案的正确性进行证明。

事实上，由上述签名过程知，当 $d_i=\{0\}^n$ 时，$p_i=H(s_i)=H(g_{k_i})$；当 $d_i=\{1\}^n$ 时，$p_i=s_i=H(g_{k_i})$。所以，

$$H(P)=H(P_1\oplus P_2\oplus\cdots\oplus P_n\oplus Y_k)=H\left(H(g_{k_1})\oplus H(g_{k_2})\oplus\cdots\oplus H(g_{k_n})\right)。$$

又因为，群公钥为 $C_k=H(B_1\oplus B_2\oplus\cdots\oplus B_m)=H\left(H(g_{k_1})\oplus H(g_{k_2})\oplus\cdots\oplus H(g_{k_n})\right)$。

所以，可以得出 $H(P)\oplus C_k=0$。明显，上述签名验证是正确的。

4. 安全性分析

4.1. 不可否认性

在得到对消息 M 的群签名 $S=\{s_1,s_2,\cdots,s_n,Y_k\}$ 后，如果想知道群中谁完成了此次签名，只需要可信第三方 TA 计算 $p_i=\begin{cases}H(s_i) & d_i=\{0\}^n\\ s_i & d_i=\{1\}^n\end{cases}(1\le i\le n)$，从而计算 $B_k=P_1\oplus P_2\oplus\cdots\oplus P_n$，TA 通过 B_k 和存储的每个群成员的签名密钥的哈希值，就能确定该签名人员，因此，本方案具有不可否认性。

4.2. 不可伪造性

在第 2.1 节中我们介绍了 CPA 安全模型，在此基础上，本节将描述本文方案具备不可伪造性。本文首先，假设存在一个伪造者 F，假设伪造者 F 只知道公钥 C_k，并且只能对一条消息的签名进行询问。

定理 1 在 CPA 安全模型下，该方案具有不可伪造性。令 t_{ow}，ε_{ow} 为正实数，让 $G=\left\{H:\{0,1\}^n\to\{0,1\}^n\right\}$ 是 $(t_{ow},\varepsilon_{ow})$ 个单向函数族。在使用 G 的 CPA 模型和 $(t_{OTS},\varepsilon_{OTS},1)$ 参数下，满足 $\varepsilon_{OTS}\le 4n\varepsilon_{OW}$ 和 $t_{OTS}=t_{OW}-t_{SIG}-t_{GEN}$，其中，$t_{GEN}$ 和 t_{SIG} 分别为密钥生成和签名时间。

本节只需证明底层哈希函数是一个单向哈希函数，即本文在 CPA 模型下存在不可伪造性，即将证明安全性规约为底层哈希函数的安全性。

在伪造者 F 只知道公钥 C_k，随机预言机(O)能够获取新的密钥对 (sk,pk) 的前提下，伪造者 F 会向 O 询问消息 M 的合法签名，当收到来自随机预言机返回的签名 s_i^M 时，F 再将试图构造一个合法的消息－签

名对$\left(M',s_i^{M'}\right)$，必须满足签名$s_i^{M'}$合法，且$M\neq M'$。如果在有限时间t内，伪造者F能成功构建消息－签名对的概率不大于ε，则说明我们的签名方案在CPA安全模型下不可伪造，记为$(t,\varepsilon,1)-EU$。

攻击者以均匀分布随机选择索引$a\in\{1,\cdots,n\}$和$b\in\{0,1\}^m$。他将矩阵$y_a[b]$替换为目标矩阵y。接下来，Adv_{OTS}使用修改后的公钥运行伪造F。如果伪造者要求其预言机签署消息M的摘要$d=(d_1,d_2,\cdots,d_n)$，并且如果$d_a=1-b$，则攻击者扮演预言机的角色，签署消息并返回签名。攻击者可以签署这条消息，因为他知道原始密钥对，并且由于$d_a=1-b$，公钥中修改后的向量没有被使用。但是，如果$d_a=b$，则对手无法签署M。所以他对预言机查询的回答是失败，这也导致伪造者中止。如果伪造者的预言机查询成功，或者伪造者根本没有询问预言机，伪造者可能会产生伪造消息M'和签名$s_i^{M'}$。如果$d'_a=b$，则$s_a^{M'}$是攻击者返回y的原像。否则，对手返回失败。正是描述如算法1：

算法1：Adv_{OTS}

输入：$y=H(x)$，$x\in\{0,1\}^m$

输出：y的前像x'，使得$y=H(x)$；否则失败

1) 生成新的密钥对(sk,pk)
2) 选取$a\in\{1,\cdots,n\}$，$b\in\{0,1\}^m$
3) 用验证密钥C_k将$y_a[b]$替换为y
4) 执行F
5) 当F使用消息M请求其唯一的预言机查询：
a) 如果$d_a=1-b$，则对消息M签名，并用签名s_i^M回应伪造的F
b) 否则返回失败
6) 当F对消息M'输出一个有效的签名$s_i^{M'}$
a) 如果$d'_a=b$，则返回作$s_a^{M'}$为y的原像
b) 否则返回失败

我们现在计算攻击者Adv_{OTS}的成功概率。我们用ε表示伪造者成功的概率，用t表示它的运行时间，通过t_{GEN}和t_{SIG}，我们分别表示方案中生成密钥和签名所需的时间。当且仅当F使用消息M和$d_a=1-b$查询预言机时，对手Adv_{OTS}可以成功地找到y的原像，或者如果他根本不查询预言机，如果伪造者返回消息M'的有效签名，其中$d'_a=b$。由于b是均匀分布的随机选择，因此，$d_a=1-b$的概率为$\frac{1}{2}$。由于M'必须与查询的消息M不同，因此，至少存在一个索引c使得$d'_c=1-d_c$。如果c=a，Adv_{OTS}成功的概率至少为$\frac{1}{2n}$。因此，攻击者在时间$t_{OW}=t+t_{SIG}+t_{GEN}$中找到原像的成功概率至少为$\frac{\varepsilon}{4n}$。证毕。

因此，Adv_{OTS}在时间t_{OTS}内能成功构建消息－签名对$\left(M',s_i^{M'}\right)$的概率不大于ε_{OTS}，这也能看出该方案的安全性可规约为底层哈希函数的单向性。

4.3. 匿名性

定理2 在随机预言机模型下，本方案在LWE假设下是CPA-匿名的。

证明：通过游戏G_0、G_1证明。

G_0：挑战者依据本方案得到群公钥$C_k=H(B_1\oplus B_2\oplus\cdots\oplus B_m)$、成员私钥$X_k$，并将$(X_k,C_k)$发送给敌手，从$\{1,\cdots,m\}$中随机选择两个身份标识$i_1,i_2$，并记$i_0\leftarrow\{i_1,i_2\}$，并以身份$i_0$按照本方案对消息$M$进

行签名，得到 $S'=\{s_1',s_2',\cdots,s_nY_k\}$，并将该签名发送给敌手。

G_1：与 G_0 一样，除了用 NIZKP 生成。依据 NIZKP 性质可知，G_0 和 G_1 在计算上不可取分。

综上所述，在随机预言机模型下，本方案在 LWE 假设下是 CPA-匿名的。

5. 结束语

在当代密码学研究中，量子发展迅速，后量子时代数字签名算法已经变得不可或缺。本文基于格上的哈希函数设计了一种一次群签名方案，相比较于传统的 RSA、ECC 等公约密码体制建立的数字签名，可以有效地抵抗量子攻击。与已有的签名方案相比，本文是基于格上的一次性签名方案，可以获得更高的效率。相信在未来，随着后量子计算机的发展，传统的签名算法将逐步被淘汰，而抗量子的这些签名算法将会成为主流，尤其今年 NIST 将后量子数字签名算法 SPHINCS$^+$推荐进入第四轮行业标准的评估，抗量子的算法进一步得到发展。下一步将基于格的一次性环签名，进一步解决密钥太大的问题。

基金项目

国家自然科学基金(61370188)；北京市教委科研计划(KM202010015009)；北京市教委科研计划资助(No. KM202110015004)；北京印刷学院博士启动金项目(27170120003/020)；北京印刷学院科研创新团队项目(Eb202101)；北京印刷学院校内学科建设项目(21090121021)；北京印刷学院重点教改项目(22150121033/009)；北京印刷学院科研基础研究一般项目(Ec202201)。

参考文献

[1] Chaum, D. and Van Heyst, E. (1991) Group Signatures. *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques*, Brighton, April 8-11 1991, 257-265. https://doi.org/10.1007/3-540-46416-6_22

[2] Fang, D.J., Wang, N. and Liu, C.L. (2010) An Enhanced RSA-Based Partially Blind Signature. *Proceedings of* 2010 *International Conference on Computer and Communication Technologies in Agriculture Engineering*, Chengdu, 12-13 June 2010, 565-567.

[3] Wang, X.M. and Dong, Y.R. (2010) Threshold Group Signature Scheme with Privilege Subjects Based on ECC. *Proceedings of International Conference on Communications and Intelligence Information Security*, Xi'an, 13-14 October 2010, 84-87. https://doi.org/10.1109/ICCIIS.2010.64

[4] Lamport, L. (1979) Constructing Digital Signatures from a One Way Function. SRI-CSL-98, SRI International Computer Science Laboratory.

[5] Dov Gordon, S., Katz, J. and Vaikuntanathan, V. (2010) A Group Signature Scheme from Lattice Assumptions. *Proceedings of* 16*th International Conference on the Theory and Application of Cryptology and Information Security*, Singapore, 5-9 December 2010, 395-412. https://doi.org/10.1007/978-3-642-17373-8_23

[6] Laguillaumie, F., Langlois, A., Libert, B. and Stehlé, D. (2013) Lattice-Based Group Signatures with Logarithmic Signature Size. *Proceedings of* 19*th International Conference on the Theory and Application of Cryptology and Information*, Bengaluru, 1-5 December 2013, 41-61. https://doi.org/10.1007/978-3-642-42045-0_3

[7] Nguney, P., Zhang, J. and Zhang, Z. (2015) Simpler Efficient Group Signatures from Lattices. *Proceedings of* 18*th IACR International Conference on Practice and Theory in Public-Key Cryptography*, Gaithersburg, MD, 30 March-1 April 2015, 401-426. https://doi.org/10.1007/978-3-662-46447-2_18

[8] Zhou, C.H., Zhu, G.M., Zhao, B.H. and Wei, W. (2006) Study of One-Way Hash Function to Digital Signature Technology. *Proceedings of* 2006 *International Conference on Computational Intelligence and Security*, Guangzhou, 3-6 November 2006, 1503-1506. https://doi.org/10.1109/ICCIAS.2006.295310

[9] 汤永利, 李元鸿, 张晓航, 等. 格上基于身份的群签名方案[EB/OL]. 计算机研究与发展: 1-11. http://kns.cnki.net/kcms/detail/11.1777.TP.20220303.1757.002.html, 2022-10-13.

[10] 韩涛. 基于格的高效群签名体制的设计与应用[D]: [硕士学位论文]. 济南: 山东大学, 2021.

[11] 李子臣, 张玉龙, 王誉晓, 等. 改进的基于格的动态群签名方案[J]. 武汉大学学报(理学版), 2016, 62(2): 135-140.

[12] 梁丽琴. 基于格的群签名研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2014.

[13] 李静. 格上基于身份的群签名方案研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2012.