格上基于身份的增量签名方案

田苗苗，陈静，仲红
（安徽大学计算机科学与技术学院，安徽 合肥 230601）

摘 要：将基于身份的密码学思想应用于增量签名中，提出了基于身份的增量签名概念，并基于格上困难问题设计了一种基于身份的增量签名方案。在标准的小整数解困难假设下，所提方案在标准模型下满足适应性选择身份和选择消息攻击下的不可伪造性。理论分析和实验结果表明，所提增量签名算法比标准签名算法具有更高的计算效率。

关键词：增量签名；基于身份的密码学；格；标准模型；小整数解问题
中图分类号：TP309
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021037

Identity-based incremental signature scheme from lattices

TIAN Miaomiao, CHEN Jing, ZHONG Hong
School of Computer Science and Technology, Anhui University, Hefei 230601, China

Abstract: By taking ideas of identity-based cryptography into incremental signatures, the concept of identity-based incremental signature was proposed, and then a specific scheme from lattices was also constructed. The scheme was shown to be provably secure against adaptive chosen identity and chosen message attacks in the standard model, assuming the hardness of the small integer solution problem. Theoretical analysis and experimental results show that the computational overhead of the incremental signature algorithm is less than that of the standard signature algorithm.

Keywords: incremental signature, identity-based cryptography, lattice, standard model, small integer solution problem

1 引言

随着信息化的深入发展，数字信息在当今社会发挥着越来越重要的作用，保障数字信息的完整性和不可伪造性是现代社会健康发展的前提。数字签名[1]是一种基础的密码学原语，可以用来保证数字消息的完整性、发送者身份的不可抵赖性等，广泛应用于网上银行、电子政务、电子合同等诸多领域。传统的数字签名没有考虑消息之间的联系，每次签署消息所需的开销与消息的长度成正比，难以满足一些特定应用场景的需求。例如，在面向自然灾害预防或天气预报的环境传感网络中，分布于不同地理位置的一系列传感器需要监测环境数据并将其上传到上层收集设备保存[2]，为了保证这些监测数据的真实性，需要对其进行签名。由于要精准地进行自然灾害或天气预测，这些传感器需要持续监测并实时更新监测数据，而通常连续的监测数据，如温度和湿度数据等仅有微小的差异。随着监测任务的持续进行，数据不断增加，如果采用传统的数字签名方法，每次更新数据都必须重新计算签名，会导致传感器的开销很大。为了降低传感器的开销，延长传感器的使用寿命，可以采用增量签名[3]方案对这些监测数据进行签名。

增量签名的概念由 Bellare 等[3]于 1994 年提出，其基本出发点是，数字签名主要包括对消息进行哈希运算和对哈希结果进行签名两部分，如果哈希函

收稿日期：2020−07−16；**修回日期**：2020−10−26
基金项目：国家自然科学基金资助项目（No.61502443）
Foundation Item: The National Natural Science Foundation of China (No.61502443)

数具有增量性，那么当已知一个消息的哈希值时，用户可以快速得到另一个相似消息的哈希值，对该哈希值进行签名，即可得到新消息的签名。由于增量签名方案可以加快相似消息的签名过程，使签名生成时间与消息间的变化量成正比，因此对数据连续更新的场景或者存在大量相似数据的场景，采用增量签名方案而非传统签名方案，可以大大降低系统的整体开销。区块链是当前的一个研究热点，将一个交易加入区块链中的前提是确保该交易的完整性和不可伪造性，为此需对该交易签名并向全网广播，由其他用户检查签名的有效性，仅当签名有效时才将该交易加入区块链[4]。由于区块链中通常存在较多的相似数据，因此采用增量签名方案对交易进行签名有望大幅提高区块链系统的效率。最近，著名区块链公司 Kadena 已经在其企业级区块链上采用了增量签名算法。

增量签名这一概念被提出以来，许多增量签名方案[3,5-6]相继被提出，然而现有的增量签名方案都依赖于公钥基础设施（PKI, public key infrastructure），用户的公钥是一串随机字符，需要通过数字证书绑定用户的身份与其公钥的匹配关系，这会给系统带来额外的存储开销和计算开销。为了解决这个问题，本文借鉴基于身份的密码学思想[7]，提出了基于身份的增量签名概念，用户使用能唯一标识其身份的字符串（如电话号码、邮箱地址等）作为其公钥，相应的私钥由可信的私钥生成器（PKG, private key generator）根据系统主密钥和用户身份生成，从而消除了传统增量签名方案存在的证书管理问题。

此外，本文利用格上相关困难问题——标准的小整数解（SIS, small integer solution）问题[8-9]，设计了一种具体的基于身份的增量签名方案，该方案在标准模型下对适应性选择身份和选择消息攻击满足不可伪造性。基于格的密码学也是当前的一个研究热点，与基于离散对数和大数分解等传统困难问题的密码方案相比，基于格的密码方案有望抵抗量子计算机的攻击[10]，并且仅需要向量点乘、线性求和以及模运算等简单操作，计算效率较高。近年来，基于格的数字签名方案受到人们的广泛关注，格上基于身份的各类签名方案也被相继提出，如格上基于身份的（标准）签名方案[11-16]和环签名方案[17-18]等。然而，这些方案要么仅能在随机预言模型下证明是适应性安全的[13-14,16-17]，要么只能达到标准模型下的选择安全性（即仅能实现选择身份攻击下的不可伪造性）[11-12,18]。由于随机预言模型下证明安全的方案在实际应用中不一定安全[19]，因此构造标准模型下适应性安全的格上基于身份的签名方案具有重要的理论和现实意义。如果不考虑增量性，本文方案也可以看作一种在标准模型下对适应性选择身份和选择消息攻击满足不可伪造性的格上基于身份的签名方案。

具体地，本文的主要贡献包括以下 3 个方面。

1) 本文提出了基于身份的增量签名概念及模型，消除了以往增量签名中存在的证书管理问题，提高了增量签名方案的实际效率。

2) 本文利用格密码技术设计了一种基于身份的增量签名方案。首先，利用基于格的可编程哈希函数[20] $H_{\boldsymbol{K}}:\{0,1\}^n\to\mathbb{Z}_q^{n\times nt}$ 嵌入用户身份信息 $\mathrm{id}\in\{0,1\}^n$，得到 $H_{\boldsymbol{K}}(\mathrm{id})$，其中 $\boldsymbol{K}$ 是该哈希函数的密钥，n 和 t 均是正整数；其次，利用文献[21]提出的陷门概念及相关算法，为身份为 id 的用户生成私钥 $\boldsymbol{R}_{\mathrm{id}}\in\mathbb{Z}^{m\times nt}$，满足 $\boldsymbol{A}\boldsymbol{R}_{\mathrm{id}}=\boldsymbol{G}-H_{\boldsymbol{K}}(\mathrm{id})$，其中 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$、$\boldsymbol{G}\in\mathbb{Z}_q^{n\times nt}$ 是公开矩阵，m 是正整数；再次，利用文献 [22] 的编码方法，将消息 μ 编码为 $H(\mu)=\boldsymbol{C}_0+\sum_{i=1}^{\ell}(-1)^{\mu_i}\boldsymbol{C}_i$，其中，$(\boldsymbol{C}_0,\cdots,\boldsymbol{C}_\ell)\in(\mathbb{Z}_q^{n\times nt})^{\ell+1}$ 是公开参数，ℓ 是消息的比特长度，μ_i 是 μ 的第 i 位比特值，显然该编码方法具有增量性，即如果消息 μ' 与消息 μ 相似，不妨设 μ' 和 μ 仅第 j 位不同，则由 $H(\mu')=H(\mu)+((-1)^{\mu'_j}-(-1)^{\mu_j})\boldsymbol{C}_j$ 可知，当已知 $H(\mu)$ 时，易得 $H(\mu')$；最后，用户利用私钥 $\boldsymbol{R}_{\mathrm{id}}$ 可以得到短向量 $\sigma\in\mathbb{Z}^{m+2nt}$，满足 $[\boldsymbol{A}\,|\,H_{\boldsymbol{K}}(\mathrm{id})\,|\,H(\mu)]\sigma=\boldsymbol{u}\,(\mathrm{mod}\,q)$，并输出消息 μ 的签名 $\mathrm{sig}=(H(\mu),\sigma)$，其中 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 也是公开参数。

3) 本文证明了在标准的小整数解困难假设下，所提格上基于身份的增量签名方案在标准模型下满足适应性选择身份和选择消息攻击下的不可伪造性。

2　预备知识

2.1　符号定义

本文的安全参数为 n。令 $\mathbb{R}$ 和 $\mathbb{Z}$ 分别表示实数集和整数集。给定正整数 d，令 $[d]$ 表示集合 $\{0,\cdots,d-1\}$，令 $\mathrm{BitDecomp}_b(d)$ 表示 d 的 $\lceil\log b\rceil$ 维

比特分解，其中 b 为正整数。令矩阵 $\boldsymbol{A}$ 的格拉姆–施密特正交化为 $\tilde{\boldsymbol{A}}$，并且令其最大奇异值为 $s_1(\boldsymbol{A})=\max_{\boldsymbol{u}}\|\boldsymbol{A}\boldsymbol{u}\|$，其中，$\boldsymbol{u}$ 是任意的单位向量，$\|\cdot\|$ 是 ℓ_2 范数。

如果对任意的常数 c，存在整数 N，当 $n>N$ 时，$f(n)<n^{-c}$ 总成立，则称 f 为可忽略函数，并记为 $\mathrm{negl}(n)$。如果一个事件发生的概率不低于 $1-\mathrm{negl}(n)$，则称该事件以极大概率发生。令定义在有限集合 D 上的 2 个概率分布 X 和 Y 之间的统计距离为 $\Delta(X,Y)=\frac{1}{2}\sum_{x\in D}\left|\Pr[X=x]-\Pr[Y=x]\right|$。如果 $\Delta(X,Y)=\mathrm{negl}(n)$，则称 X 和 Y 统计接近。

2.2 基于身份的增量签名方案

本节介绍基于身份的增量签名方案的定义及安全模型。

定义 1 基于身份的增量签名方案由以下 5 个概率多项式时间算法组成，分别为系统建立算法 Setup、私钥提取算法 Extract、标准签名算法 Sign、增量签名算法 IncSig 以及签名验证算法 Verify。各算法的具体描述如下。

Setup。输入安全参数 n，输出系统主公钥 mpk 和主私钥 msk。

Extract。输入系统主公钥 mpk 和主私钥 msk，以及身份 id，输出该身份所对应的私钥 $\mathrm{sk}_{\mathrm{id}}$。

Sign。输入系统主公钥 mpk、身份 id 及其对应的私钥 $\mathrm{sk}_{\mathrm{id}}$，以及消息 μ，输出消息 μ 的签名 sig。

IncSig。输入系统主公钥 mpk、身份 id 及其对应的私钥 $\mathrm{sk}_{\mathrm{id}}$、一个有效的消息签名对 (μ,sig)，以及新消息 μ'，输出消息 μ' 的签名 sig'。

Verify。输入系统主公钥 mpk、身份 id 和一个消息签名对 (μ,sig)，如果 sig 是身份为 id 的用户对消息 μ 的有效签名，则输出 1；否则输出 0。

基于身份的增量签名方案首先要满足正确性，即对任意的身份 id 和消息 μ，如果算法 Setup(n)、Extract (mpk,msk,id) 以及 Sign (mpk,id,$\mathrm{sk}_{\mathrm{id}}$,$\mu$) 均正确执行，则：1) Verify (mpk,id,μ,sig) 应以极大概率输出 1；2) 对任意一个消息 μ' 以及一个有效的消息签名对 (μ,sig)，满足 Verify (mpk,id,μ,sig) =1，Verify(mpk,id,μ',IncSig(mpk,id,$\mathrm{sk}_{\mathrm{id}}$,$\mu$,sig,$\mu'$))应以极大概率输出 1。

根据传统增量签名的适应性选择消息安全模型[3]、基于身份签名的适应性选择身份和选择消息安全模型[14,23]，可定义基于身份的增量签名方案在适应性选择身份和选择消息攻击下的安全性。

定义 2 如果对任意的多项式时间敌手 $\mathcal{A}$，其赢得以下游戏的概率是可忽略的，则称该基于身份的增量签名方案满足适应性选择身份和选择消息攻击下的不可伪造性。游戏由敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 执行，包括以下 5 个阶段：系统建立阶段、私钥提取询问阶段、标准签名询问阶段、增量签名询问阶段和伪造阶段。

系统建立阶段。挑战者 $\mathcal{C}$ 运行算法 Setup(n)生成系统主公钥 mpk 和主私钥 msk，然后将主公钥 mpk 发送给敌手 $\mathcal{A}$，并初始化参数 α=0。

私钥提取询问阶段。敌手 $\mathcal{A}$ 可以适应性地向挑战者 $\mathcal{C}$ 询问身份 id 所对应的私钥，挑战者 $\mathcal{C}$ 运行算法 Extract (mpk,msk,id) 生成私钥 $\mathrm{sk}_{\mathrm{id}}$，并将其发送给敌手 $\mathcal{A}$。

标准签名询问阶段。敌手 $\mathcal{A}$ 可以适应性地向挑战者 $\mathcal{C}$ 进行标准签名询问。当敌手 $\mathcal{A}$ 询问身份为 id 的用户对消息 μ 的标准签名时，挑战者 $\mathcal{C}$ 运行算法 Sign (mpk,id,$\mathrm{sk}_{\mathrm{id}}$,$\mu$) 生成相应的签名 sig，并将其发送给敌手 $\mathcal{A}$。然后挑战者 $\mathcal{C}$ 保存 $(\mu_\alpha,\mathrm{sig}_\alpha)=(\mu,\mathrm{sig})$，并令 $\alpha=\alpha+1$。

增量签名询问阶段。敌手 $\mathcal{A}$ 也可以适应性地向挑战者 $\mathcal{C}$ 进行增量签名询问。不失一般性地，假设 2 个相似消息之间只相差 1 bit。当敌手 $\mathcal{A}$ 询问身份为 id 的用户对消息 μ' 的增量签名时，它需要发送 id 以及一个三元组 (i,j,v)，其中，$i\in[\alpha]$，表明 μ' 是 μ_i 的第 j 位被 v 代替所得的新消息。挑战者 $\mathcal{C}$ 首先找到有效的消息签名对 (μ_i,sig_i)，然后运行算法 IncSig(mpk,id,$\mathrm{sk}_{\mathrm{id}}$,$\mu_i$,$\mathrm{sig}_i$,$\mu'$) 生成相应的签名 sig'，并将其发送给敌手 $\mathcal{A}$，最后挑战者 $\mathcal{C}$ 保存 $(\mu_\alpha,\mathrm{sig}_\alpha)=(\mu',\mathrm{sig}')$，并令 $\alpha=\alpha+1$。

伪造阶段。敌手 $\mathcal{A}$ 伪造一个关于身份 id^* 的伪造消息签名对 (μ^*,sig^*)，若满足以下条件，则敌手 $\mathcal{A}$ 赢得游戏。

1) 敌手 $\mathcal{A}$ 没有对身份 id^* 进行过私钥提取询问，也没有对 μ^* 进行过标准签名询问或关于 μ^* 的增量签名询问，即 $\mu^*\notin\{\mu_0,\mu_1,\cdots,\mu_{\alpha-1}\}$。

2) 算法 Verify (mpk,id^*,μ^*,sig^*) =1。

2.3 格基础知识

定义 3 如果向量 $\boldsymbol{b}_1,\cdots,\boldsymbol{b}_m\in\mathbb{R}^m$ 是线性无关的，则以其为基构成的格 Λ 定义为

$\Lambda=\{\sum_{i=1}^{m}c_i\boldsymbol{b}_i:c_i\in\mathbb{Z}\}$。

给定矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$，其中 n,m,q 为正整数，易知 $\Lambda^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{x}=\boldsymbol{0}\ (\mathrm{mod}\ q)\}$ 是一个格，而集合 $\Lambda^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^m:\boldsymbol{A}\boldsymbol{x}=\boldsymbol{u}\ (\mathrm{mod}\ q)\}$ 是 $\Lambda^{\perp}(\boldsymbol{A})$ 的平移。

方案的安全性基于小整数解问题的困难性。文献[9]给出了小整数解问题的正式定义。

定义 4　给定正整数 n,m,q,β，以及随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，定义小整数解问题是求一个非零向量 $\boldsymbol{e}\in\mathbb{Z}^m$，满足 $\|\boldsymbol{e}\|\leqslant\beta$ 和 $\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0}\ (\mathrm{mod}\ q)$。

显然，小整数解问题可以看作求解格 $\Lambda^{\perp}(\boldsymbol{A})$ 上的一个非零短向量的问题。文献[9]已经证明，当 $q\geqslant\beta\omega(\sqrt{n\log n})$ 时，求解平均情况下的小整数解问题，其困难程度接近于求解最坏情况下格上的经典困难问题。

2.4　离散高斯分布

令以 $\boldsymbol{c}\in\mathbb{R}^m$ 为中心、$s>0$ 为参数的连续高斯函数为 $\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp\dfrac{-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}$，其中 $\boldsymbol{x}\in\mathbb{R}^m$。

定义 5　定义 m 维格 Λ 上，以 $\boldsymbol{c}\in\mathbb{R}^m$ 为中心、$s>0$ 为参数的离散高斯分布为

$$\forall\boldsymbol{x}\in\Lambda,\quad \mathcal{D}_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)}$$

其中，$\rho_{s,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{z}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{z})$。

为了表示方便，当 $\boldsymbol{c}=\boldsymbol{0}$ 时，将其省略。

关于离散高斯分布，有如下重要结论成立[22,24-25]。

引理 1　给定基为 $\boldsymbol{B}\in\mathbb{R}^{m\times m}$ 的 m 维格 Λ，中心 $\boldsymbol{c}\in\mathbb{R}^m$，实数 $\varepsilon>0$ 以及参数 $s>s_1(\tilde{\boldsymbol{B}})\omega(\sqrt{\log m})$，则对于任意的 $\boldsymbol{x}\in\Lambda$，有

$$\Pr_{\boldsymbol{x}\leftarrow\mathcal{D}_{\Lambda,s,\boldsymbol{c}}}[\|\boldsymbol{x}-\boldsymbol{c}\|>s\sqrt{m}]\leqslant\frac{1+\varepsilon}{1-\varepsilon}2^{-m}$$

引理 2　给定正整数 $n,q,m\geqslant 2n\log q$，实数 $\varepsilon\in(0,1)$ 以及高斯参数 $s\geqslant\omega(\sqrt{\log m})$。如果 $\boldsymbol{x}$ 服从离散高斯分布 $\mathcal{D}_{\mathbb{Z}^m,s}$ 且 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，则事件“$\boldsymbol{A}\boldsymbol{x}$ 的概率分布与 $\mathbb{Z}_q^n$ 上的均匀分布的统计距离不超过 2ε”，将以不低于 $1-q^{-n}$ 的概率成立。

2.5　格陷门函数

基于格的陷门函数是格密码学的重要工具之一，传统的格陷门是格的一个短基。本文提出的格上基于身份的增量签名方案采用文献[21]的 $\boldsymbol{G}$ −陷门概念及其相关算法，分别为陷门生成算法 TrapGen、原像采样算法 SampleD 和陷门委派算法 DelTrap。这种陷门函数的参数较小，计算和存储开销也较少。

令 $\boldsymbol{g}^{\mathrm{T}}=[1,2,\cdots,2^{t-1}]$，则定义矩阵 $\boldsymbol{G}=\boldsymbol{I}_n\otimes\boldsymbol{g}^{\mathrm{T}}$，其中 $\otimes$ 代表张量积。文献[21]给出了格 $\Lambda^{\perp}(\boldsymbol{G})$ 的一个公开短基 $\boldsymbol{S}\in\mathbb{Z}^{nt\times nt}$，使对任意的 $\boldsymbol{u}\in\mathbb{Z}_q^n$，利用 $\boldsymbol{S}$ 可求得短向量 $\boldsymbol{x}\in\mathbb{Z}_q^{nt}$ 满足 $\boldsymbol{G}\boldsymbol{x}=\boldsymbol{u}\ (\mathrm{mod}\ q)$。

下面给出 $\boldsymbol{G}$ −陷门的正式定义。

定义 6　令整数 $n\geqslant 1$，$q\geqslant 2$，$t=\lceil\log q\rceil$ 以及 $m>nt$。定义 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 的 $\boldsymbol{G}$ −陷门为 $\boldsymbol{R}\in\mathbb{Z}^{(m-nt)\times nt}$，满足 $\boldsymbol{A}\begin{bmatrix}\boldsymbol{R}\\ \boldsymbol{I}_{nt}\end{bmatrix}=\boldsymbol{H}\boldsymbol{G}$，其中 $\boldsymbol{H}\in\mathbb{Z}_q^{n\times n}$ 是可逆矩阵，称为 $\boldsymbol{R}$ 的标签。

为了表示方便，如无特殊说明，下文将 $\boldsymbol{H}\in\mathbb{Z}_q^{n\times n}$ 统一设定为单位矩阵 $\boldsymbol{I}_n\in\mathbb{Z}_q^{n\times n}$。

文献[21]展示了如何生成随机矩阵的 $\boldsymbol{G}$ −陷门。

引理 3　给定整数 $n\geqslant 1$，$q\geqslant 2$，$t=\lceil\log q\rceil$ 以及 $m>nt$，存在一个多项式时间算法 TrapGen，输入安全参数 n，输出矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 及其 $\boldsymbol{G}$ −陷门 $\boldsymbol{R}\in\mathbb{Z}^{(m-nt)\times nt}$，使矩阵 $\boldsymbol{A}$ 的概率分布与 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布统计接近，且 $s_1(\boldsymbol{R})\leqslant s'O(\sqrt{nt})$ 以极大概率成立，其中 $s'>\omega(\sqrt{\log n})$。此外，对任意矩阵 $\boldsymbol{A}_1\in\mathbb{Z}_q^{n\times nt}$，存在一个多项式时间算法 DelTrap，输入矩阵 $\boldsymbol{A}'=[\boldsymbol{A}\,|\,\boldsymbol{A}_1]\in\mathbb{Z}_q^{n\times(m+nt)}$、$\boldsymbol{A}$ 的 $\boldsymbol{G}$ −陷门 $\boldsymbol{R}$ 和高斯参数 $s\geqslant\sqrt{7(s_1(\boldsymbol{R})^2+1)}\omega(\sqrt{\log n})$，输出矩阵 $\boldsymbol{A}'$ 的 $\boldsymbol{G}$ −陷门 $\boldsymbol{R}'\in\mathbb{Z}^{m\times nt}$，使 $s_1(\boldsymbol{R}')\leqslant sO(\sqrt{nt})$ 以极大概率成立。

文献[21]给出了利用矩阵 $\boldsymbol{A}$ 的 $\boldsymbol{G}$ −陷门生成 $\Lambda^{\boldsymbol{u}}(\boldsymbol{A})$ 中短向量的方法。

引理 4　给定整数 $n\geqslant 1$，$q\geqslant 2$，$t=\lceil\log q\rceil$ 以及 $m>nt$，存在一个多项式时间算法 SampleD，输入矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 及其 $\boldsymbol{G}$ −陷门 $\boldsymbol{R}\in\mathbb{Z}^{(m-nt)\times nt}$，向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 和高斯参数 $\tilde{s}\geqslant\sqrt{7(s_1(\boldsymbol{R})^2+1)}\omega(\sqrt{\log n})$，输出概率分布统计接近于 $\mathcal{D}_{\Lambda^{\boldsymbol{u}}(\boldsymbol{A}),\tilde{s}}$ 的向量 $\boldsymbol{e}\in\mathbb{Z}^m$。

2.6　可编程哈希函数

可编程哈希函数（PHF, programmable hash function）的概念最初由 Hofheinz 等[26]提出，可以用来构造标准模型下安全的密码方案。简单来说，

可编程哈希函数有 2 种工作模式，即正常模式和陷门模式。正常模式包含 H.Gen 和 H.Eval 这 2 种算法，而陷门模式包含 H.TrapGen 和 H.TrapEval 这 2 种算法。在拥有陷门信息的情况下，这 2 种模式是不可区分的，因此可以在安全性证明中使用陷门模式模拟正常模式。本文采用 Zhang 等[20]提出的基于格的高效可编程哈希函数来嵌入身份信息。下面给出无覆盖集合族的概念。

定义 7 给定整数 $v,L,\kappa\geqslant 0$，如果集合族 $\mathrm{CF}=\{\mathrm{CF}_X\}_{X\in[L]}$ 满足对任意最多包含 v 个元素的集合 $S\subseteq[L]$ 以及任意的元素 $Y\in[L]\setminus S$，至少存在一个元素 $z\in\mathrm{CF}_Y\subseteq[\kappa]$ 且 $z\notin\bigcup_{X\in S}\mathrm{CF}_X$，并且所有子集 CF_X 的元素个数均为 $\eta\in\mathbb{Z}$，则称 CF 为集合 $[\kappa]$ 上的 η 均匀 v −无覆盖集族。

给定整数 n，$v=\omega(\log n)$，$\kappa\leqslant 16v^2n$，$L=2^n$，$\eta=\dfrac{\kappa}{4v}$，$q,t=\lceil\log q\rceil$ 以及 η 均匀 v −无覆盖集族 $\mathrm{CF}=\{\mathrm{CF}_X\}_{X\in[L]}$，Zhang 等[20]构造的基于格的高效可编程哈希函数 $H\colon[L]\to\mathbb{Z}_q^{n\times nt}$ 简要描述如下。

1) $H.\mathrm{Gen}(n)\to\boldsymbol{K}$。输入安全参数 n，输出 $\boldsymbol{K}=(\hat{\boldsymbol{A}},\boldsymbol{A}_0,\cdots,\boldsymbol{A}_{w-1})$，其中，$\hat{\boldsymbol{A}}$ 和 $\boldsymbol{A}_0,\cdots,\boldsymbol{A}_{w-1}$ 均为 $\mathbb{Z}_q^{n\times nt}$ 上的随机矩阵，$w=\lceil\log\kappa\rceil$。

2) $H.\mathrm{Eval}(\boldsymbol{K},X)\to\boldsymbol{Z}$。输入 $\boldsymbol{K}=(\hat{\boldsymbol{A}},\boldsymbol{A}_0,\cdots,\boldsymbol{A}_{w-1})$ 和整数 $X\in[L]$，输出 $\boldsymbol{Z}=H_{\boldsymbol{K}}(X)$。

哈希值 $\boldsymbol{Z}$ 的具体计算方法如下。首先，令 $\boldsymbol{Z}=\hat{\boldsymbol{A}}$；然后，对所有的元素 $z\in\mathrm{CF}_X$，分别计算 $(b_0,\cdots,b_{w-1})=\mathrm{BitDecomp}_\kappa(z)$ 和 $\boldsymbol{B}_z=\boldsymbol{A}_{w-1}-b_{w-1}\boldsymbol{G}$，令 $i=w-2,\cdots,0$，迭代计算 $\boldsymbol{B}_z=(\boldsymbol{A}_i-b_i\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{B}_z)$，其中 $\boldsymbol{G}^{-1}(\boldsymbol{B}_z)$ 表示满足 $\boldsymbol{GY}=\boldsymbol{B}_z$ 的小解 $\boldsymbol{Y}$；最后，令 $\boldsymbol{Z}=\boldsymbol{Z}+\boldsymbol{B}_z$ 并输出 $\boldsymbol{Z}$。

上述可编程哈希函数具有如下性质[20]。

引理 5 给定安全参数 n，矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times 2nt}$ 和 $\boldsymbol{G}\in\mathbb{Z}_q^{n\times nt}$，存在多项式时间算法 $H.\mathrm{TrapGen}(n,\boldsymbol{A},\boldsymbol{G})\to(\boldsymbol{K}',\mathrm{td})$ 和 $H.\mathrm{TrapEval}(\mathrm{td},\boldsymbol{K}',X)\to(\boldsymbol{D}_X,\boldsymbol{S}_X)$，其中 $X\in[L]$，$\boldsymbol{D}_X$ 服从高斯分布 $\mathcal{D}_{\mathbb{Z}^{2nt\times nt},s}$，高斯参数 $s\geqslant O(n^2t\log n)\omega(\log n\sqrt{\log nt})$，$\boldsymbol{S}_X$ 是 $\mathbb{Z}_q^{n\times n}$ 中的可逆矩阵或 $\boldsymbol{0}$，并满足 $H.\mathrm{Eval}(\boldsymbol{K}',X)=\boldsymbol{AD}_X+\boldsymbol{S}_X\boldsymbol{G}$。此外，如果令 $H.\mathrm{Gen}(n)\to\boldsymbol{K}$，则 $(\boldsymbol{A},\boldsymbol{K}')$ 和 $(\boldsymbol{A},\boldsymbol{K})$ 的概率分布统计接近。

上述引理表明，该可编程哈希函数存在较好的模拟方法，可以在安全性证明中模拟该函数。

3 具体方案

3.1 方案描述

本文方案各算法的具体实现过程如下。

1) 系统建立算法

Setup(n)。输入安全参数 n，执行以下步骤。

① 运行算法 TrapGen(n) 生成矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 及其 $\boldsymbol{G}$ −陷门 $\boldsymbol{R}\in\mathbb{Z}^{nt\times nt}$。

② 运行算法 H.Gen(n) 生成 $\boldsymbol{K}$。

③ 选择 ℓ+1 个随机矩阵 $\boldsymbol{C}_0,\cdots,\boldsymbol{C}_\ell\in\mathbb{Z}_q^{n\times nt}$ 以及一个随机向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$。

④ 输出系统主私钥 $\mathrm{msk}=\boldsymbol{R}$ 和主公钥 $\mathrm{mpk}=(\boldsymbol{A},\boldsymbol{K},\boldsymbol{C}_0,\cdots,\boldsymbol{C}_\ell,\boldsymbol{u})$。

2) 私钥提取算法

Extract(mpk,msk,id)。输入系统主公钥 mpk、主私钥 msk 以及身份 $\mathrm{id}\in\{0,1\}^n$，执行以下步骤。

① 利用可编程哈希函数计算 $H_{\boldsymbol{K}}(\mathrm{id})\in\mathbb{Z}_q^{n\times nt}$ 并构造矩阵 $\boldsymbol{A}_{\mathrm{id}}=[\boldsymbol{A}\,|\,H_{\boldsymbol{K}}(\mathrm{id})]$。

② 运行算法 DelTrap($\boldsymbol{A}_{\mathrm{id}},\boldsymbol{R},s$) 生成矩阵 $\boldsymbol{A}_{\mathrm{id}}$ 的 $\boldsymbol{G}$ −陷门 $\boldsymbol{R}_{\mathrm{id}}\in\mathbb{Z}^{m\times nt}$。

③ 输出私钥 $\mathrm{sk}_{\mathrm{id}}=\boldsymbol{R}_{\mathrm{id}}$。

3) 标准签名算法

Sign(mpk,id,$\mathrm{sk}_{\mathrm{id}}$,$\mu$)。输入系统主公钥 mpk、身份 id 及其对应的私钥 $\mathrm{sk}_{\mathrm{id}}$，消息 $\mu\in\{0,1\}^\ell$，执行以下步骤。

① 计算 $H(\mu)=\boldsymbol{C}_0+\sum_{i=1}^{\ell}(-1)^{\mu_i}\boldsymbol{C}_i$ 并构造矩阵 $\boldsymbol{A}_\mu=[\boldsymbol{A}_{\mathrm{id}}\,|\,H(\mu)]$。

② 运行算法 SampleD($\boldsymbol{A}_\mu,\boldsymbol{R}_{\mathrm{id}},\boldsymbol{u},\tilde{s}$) 生成 σ。

③ 输出签名 $\mathrm{sig}=(H(\mu),\sigma)$。

4) 增量签名算法

IncSig(mpk,id,$\mathrm{sk}_{\mathrm{id}}$,$\mu$,sig,$\mu'$)。输入系统主公钥 mpk、身份 id 及其对应的私钥 $\mathrm{sk}_{\mathrm{id}}$、一个有效的消息签名对 (μ,sig)，以及新消息 $\mu'\in\{0,1\}^\ell$。不失一般性地，假设 μ' 与 μ 仅第 j 位不同，执行以下步骤。

① 计算 $H(\mu')=H(\mu)+((-1)^{\mu'_j}-(-1)^{\mu_j})\boldsymbol{C}_j$ 并构造矩阵 $\boldsymbol{A}_{\mu'}=[\boldsymbol{A}_{\mathrm{id}}\,|\,H(\mu')]$。

② 运行算法 SampleD($\boldsymbol{A}_{\mu'},\boldsymbol{R}_{\mathrm{id}},\boldsymbol{u},\tilde{s}$) 生成 σ'。

③ 输出签名 $\mathrm{sig}'=(H(\mu'),\sigma')$。

5) 签名验证算法

Verify(mpk,id,μ,sig)。输入系统主公钥 mpk、

身份 id 和一个消息签名对 (μ,sig)，执行以下步骤。

① 利用可编程哈希函数计算 $H_{\boldsymbol{K}}(\mathrm{id})$ 并构造矩阵 $\boldsymbol{A}_{\mathrm{id}}=[\boldsymbol{A}\,|\,H_{\boldsymbol{K}}(\mathrm{id})]$。

② 计算 $\boldsymbol{A}_{\mu}=[\boldsymbol{A}_{\mathrm{id}}\,|\,\boldsymbol{C}_0+\sum_{i=1}^{\ell}(-1)^{\mu_i}\boldsymbol{C}_i]$。

③ 验证 $\boldsymbol{A}_{\mu}\sigma=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 和 $\|\sigma\|\leqslant\tilde{s}\sqrt{m+2nt}$ 是否均成立，若是，输出 1；否则输出 0。

3.2 参数设置

令安全参数 n 为 2 的幂次，$t=\lceil\log q\rceil$，$m\geqslant 2nt$。根据文献[9]，令 $q\geqslant\beta\omega(\sqrt{n\log n})$，其中 $\beta\geqslant O(n^{3.5}t^{2.5}\log n)\omega(\log^{2.5}n\sqrt{\log nt})$。由引理 3 可知，算法 TrapGen 输出的 $\boldsymbol{R}$ 将以极大概率满足 $s_1(\boldsymbol{R})\leqslant\omega(\sqrt{\log n})O(\sqrt{nt})$。当算法 DelTrap 的高斯参数 $s\geqslant\sqrt{7(s_1(\boldsymbol{R})^2+1)}\omega(\sqrt{\log n})$ 时，该算法输出的 $\boldsymbol{R}_{\mathrm{id}}$，将以极大概率满足 $s_1(\boldsymbol{R}_{\mathrm{id}})\leqslant sO(\sqrt{nt})$。根据引理 4，令算法 SampleD 的高斯参数 $\tilde{s}\geqslant\sqrt{7(s_1(\boldsymbol{R}_{\mathrm{id}})^2+1)}\omega(\sqrt{\log n})$。

4 方案分析

4.1 正确性分析

定理 1　本文提出的格上基于身份的增量签名方案满足正确性。

证明　考虑标准签名和增量签名 2 种情况。

1) 设消息 $\mu=[\mu_1,\cdots,\mu_\ell]$ 关于身份 id 的标准签名是 $\mathrm{sig}=(H(\mu),\sigma)$。由参数设置以及方案构造可知，$\boldsymbol{A}_{\mu}=[\boldsymbol{A}_{\mathrm{id}}\,|\,\boldsymbol{C}_0+\sum_{i=1}^{\ell}(-1)^{\mu_i}\boldsymbol{C}_i]$。根据引理 4 和引理 1，$\boldsymbol{A}_{\mu}\sigma=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 和 $\|\sigma\|\leqslant\tilde{s}\sqrt{m+2nt}$ 以极大概率成立。

2) 设消息 $\mu=[\mu_1,\cdots,\mu_\ell]$ 关于身份 id 的增量签名是 $\mathrm{sig}=(H(\mu),\sigma)$，原消息 $\mu'=[\mu'_1,\cdots,\mu'_\ell]$ 的签名是 $\mathrm{sig}'=(H(\mu'),\sigma')$。设消息 μ 与 μ' 仅第 j 位不同，则 $H(\mu)=H(\mu')+((-1)^{\mu_j}-(-1)^{\mu'_j})\boldsymbol{C}_j=\boldsymbol{C}_0+\sum_{i=1}^{\ell}(-1)^{\mu_i}\boldsymbol{C}_j$ 并且 $\boldsymbol{A}_{\mu}=[\boldsymbol{A}_{\mathrm{id}}\,|\,\boldsymbol{C}_0+\sum_{i=1}^{\ell}(-1)^{\mu_i}\boldsymbol{C}_i]$。同样，由引理 4 和引理 1 可知，$\boldsymbol{A}_{\mu}\sigma=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 和 $\|\sigma\|\leqslant\tilde{s}\sqrt{m+2nt}$ 将以极大概率成立。

综上，本文提出的增量签名方案是正确的。证毕。

4.2 安全性分析

定理 2　如果小整数解问题是困难的，则本文提出的格上基于身份的增量签名方案对适应性选择身份和选择消息攻击是不可伪造的。

证明　假设存在多项式时间的敌手 $\mathcal{A}$ 在进行了 Q_1 次私钥提取询问、Q_2 次标准签名询问和 Q_3 次增量签名询问后（其中 $Q_1\leqslant\omega(\log n)$，$Q_2$ 和 Q_3 满足 $Q_2+Q_3<q$），能以不可忽略的概率 ε 伪造一个有效的签名，则存在一个多项式时间的算法 $\mathcal{B}$ 能够以概率 ε' 解决标准的小整数解问题，其中 $\varepsilon'\geqslant\frac{\varepsilon}{\omega(n\log^2 n)q}\left(1-\frac{Q_2+Q_3}{q}\right)$。算法 $\mathcal{B}$ 的工作过程如下。

1) 系统建立阶段。给定小整数解问题的实例 $\boldsymbol{A}=[\bar{\boldsymbol{A}}\,|\,\boldsymbol{u}]\in\mathbb{Z}_q^{n\times(m+n)}$，其中 $\bar{\boldsymbol{A}}$ 和 $\boldsymbol{u}$ 分别是从 $\mathbb{Z}_q^{n\times m}$ 和 $\mathbb{Z}_q^{n}$ 中均匀随机选取的。算法 $\mathcal{B}$ 执行以下步骤。

① 运行算法 $H.\mathrm{TrapGen}(n,\bar{\boldsymbol{A}},\boldsymbol{G})\rightarrow(\boldsymbol{K}',\mathrm{td})$。

② 选择 $\ell+1$ 个矩阵 $\boldsymbol{R}_i\in\mathbb{Z}^{m\times nt}$，其中 $\boldsymbol{R}_i$ 服从高斯分布 $\mathcal{D}_{\mathbb{Z}^{m\times nt},s'}$，高斯参数 $s'\geqslant\omega(\sqrt{\log nt})$。

③ 选择 ℓ 个标量 $h_i\in\mathbb{Z}_q$，并设 $h_0=1$。

④ 令 $\boldsymbol{C}_i=\bar{\boldsymbol{A}}\boldsymbol{R}_i+h_i\boldsymbol{G}\in\mathbb{Z}_q^{n\times nt}(i\in[\ell+1])$，并将系统主公钥 $\mathrm{mpk}=(\bar{\boldsymbol{A}},\boldsymbol{K}',\boldsymbol{C}_0,\cdots,\boldsymbol{C}_\ell,\boldsymbol{u})$ 发送给敌手 $\mathcal{A}$。

根据引理 2 可知，$\{\boldsymbol{C}_i\}_{i=[\ell+1]}$ 统计接近于 $\mathbb{Z}_q^{n\times nt}$ 上的均匀分布；同时，由引理 5 以及文献[20]的定理 3 可知，$H.\mathrm{TrapGen}$ 算法生成 $\boldsymbol{K}'=(\hat{\boldsymbol{A}},\{\boldsymbol{A}_i\}_{i\in[w]})$，其中，$\hat{\boldsymbol{A}}$ 和 $\boldsymbol{A}_0,\cdots,\boldsymbol{A}_{w-1}$ 的分布均统计接近于 $\mathbb{Z}_q^{n\times nt}$ 上的均匀分布，因此与方案中 $\boldsymbol{K}$ 的分布是统计接近的。该算法的具体过程如下。首先选择一个随机矩阵 $\bar{\boldsymbol{A}}\in\mathbb{Z}_q^{n\times m}$、$w$+1 个矩阵 $\hat{\boldsymbol{D}}$ 和 $\{\boldsymbol{D}_i\}_{i\in[w]}$，其中 $\hat{\boldsymbol{D}}$ 和 $\boldsymbol{D}_i$ 服从高斯分布 $\mathcal{D}_{\mathbb{Z}^{m\times nt},s'}$，高斯参数 $s'\geqslant\omega(\sqrt{\log nt})$；然后，从集合 $[\kappa]$ 中随机选择一个正整数 z' 并计算 $(b'_0,\cdots,b'_{w-1})=\mathrm{BitDecomp}_{\kappa}(z')$，令 c 表示 $(b'_0,\cdots,b'_{w-1})$ 中 1 的个数；最后计算 $\hat{\boldsymbol{A}}=\bar{\boldsymbol{A}}\hat{\boldsymbol{D}}-(-1)^c\boldsymbol{G}$ 以及 $\boldsymbol{A}_i=\bar{\boldsymbol{A}}\boldsymbol{D}_i+(1-b'_i)\boldsymbol{G}$。算法输出 $\boldsymbol{K}'=(\hat{\boldsymbol{A}},\{\boldsymbol{A}_i\}_{i\in[w]})$ 和 $\mathrm{td}=(\hat{\boldsymbol{D}},\{\boldsymbol{D}_i\}_{i\in[w]},z')$。

2) 私钥提取询问阶段。敌手 $\mathcal{A}$ 可以适应性地进行私钥提取询问。当算法 $\mathcal{B}$ 接收到敌手 $\mathcal{A}$ 对某个身份 $\{\mathrm{id}_i\}_{i\in[Q_1]}$ 的私钥提取询问时，执行以下步骤。

① 运行算法 $H.\mathrm{TrapEval}(\mathrm{td},\boldsymbol{K}',\mathrm{id}_i)$ 得到 $(\boldsymbol{D}_{\mathrm{id}_i},\boldsymbol{S}_{\mathrm{id}_i})$。

② 若 $\boldsymbol{S}_{\mathrm{id}_i}=\boldsymbol{0}$，则 $\mathcal{B}$ 终止，否则执行下一步。

③ 输出 $\mathrm{sk}_{\mathrm{id}_i}=\boldsymbol{D}_{\mathrm{id}_i}$。

由引理 5 以及文献[20]的定理 3 可知，$\boldsymbol{D}_{\mathrm{id}_i}$ 的分布统计接近于 $\mathbb{Z}^{m\times nt}$ 上的均匀分布，与方案中私钥 $\boldsymbol{R}_{\mathrm{id}_i}$ 的分布是统计接近的。$\boldsymbol{D}_{\mathrm{id}_i}$ 的具体生成过程如下。首先，令 $\boldsymbol{D}_{\mathrm{id}_i}=\hat{\boldsymbol{D}}$，$\boldsymbol{S}_{\mathrm{id}_i}=-(-1)^c\boldsymbol{I}_n$，并对所有的 $z\in\mathrm{CF}_{\mathrm{id}_i}$，计算 $(b_0,\cdots,b_{w-1})=\mathrm{BitDecomp}_\kappa(z)$，令 $\boldsymbol{B}_z=\boldsymbol{A}_{w-1}-b_{w-1}\boldsymbol{G}$, $\boldsymbol{D}_z=\boldsymbol{D}_{w-1}$，$\boldsymbol{S}_z=(1-b'_{w-1}-b_{w-1})\boldsymbol{I}_n$；然后，对所有的 $i=w-2,\cdots,0$，迭代计算 $\boldsymbol{B}_z=(\boldsymbol{A}_i-b_i\boldsymbol{G})\boldsymbol{G}^{-1}(\boldsymbol{B}_z)$，$\boldsymbol{S}_z=(1-b'_i-b_i)\boldsymbol{S}_z$ 以及 $\boldsymbol{D}_z=\boldsymbol{D}_i\boldsymbol{G}^{-1}(\boldsymbol{B}_z)+(1-b'_i-b_i)\boldsymbol{D}_z$；最后，算法输出 $\boldsymbol{D}_{\mathrm{id}_i}=\hat{\boldsymbol{D}}+\boldsymbol{D}_z\in\mathbb{Z}^{m\times nt}$ 和 $\boldsymbol{S}_{\mathrm{id}_i}=-(-1)^c\boldsymbol{I}_n+\boldsymbol{S}_z$。

3) 标准签名询问阶段。敌手 $\mathcal{A}$ 可以适应性地进行标准签名询问。算法 $\mathcal{B}$ 接收到敌手 $\mathcal{A}$ 对身份 id_i 和消息 $\{\mu_i\}_{i\in[Q_2]}$ 的标准签名询问时，执行以下步骤。

① 计算 $\boldsymbol{R}_{\mu_i}=\boldsymbol{R}_0+\sum_{j=1}^{\ell}(-1)^{\mu_{ij}}\boldsymbol{R}_j$，$h_{\mu_i}=h_0+\sum_{j=1}^{\ell}(-1)^{\mu_{ij}}h_j$。

② 若 $\boldsymbol{S}_{\mathrm{id}_i}\neq\boldsymbol{0}$，则算法 $\mathcal{B}$ 有 $[\bar{\boldsymbol{A}}\,|\,H_{\boldsymbol{K}}(\mathrm{id}_i)]$ 的 $\boldsymbol{G}$–陷门 $\boldsymbol{D}_{\mathrm{id}_i}$。由于 $\boldsymbol{D}_{\mathrm{id}_i}$ 也是 $[\bar{\boldsymbol{A}}\,|\,H_{\boldsymbol{K}}(\mathrm{id}_i)\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu_i}+h_{\mu_i}\boldsymbol{G}]$ 的 $\boldsymbol{G}$–陷门，因此对消息 $\{\mu_i\}_{i\in[Q_2]}$ 的签名询问，算法 $\mathcal{B}$ 可以直接调用算法 SampleD 获得非零短向量 σ_i，满足 $[\bar{\boldsymbol{A}}\,|\,H_{\boldsymbol{K}}(\mathrm{id}_i)\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu_i}+h_{\mu_i}\boldsymbol{G}]\sigma_i=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 以及 $\|\sigma_i\|\leqslant\tilde{s}\sqrt{m+2nt}$。

③ 若 $\boldsymbol{S}_{\mathrm{id}_i}=\boldsymbol{0}$，则算法 $\mathcal{B}$ 执行以下步骤。

a. 若 $h_{\mu_i}=0$，则 $\mathcal{B}$ 终止。

b. 若 $h_{\mu_i}\neq0$，则算法 $\mathcal{B}$ 有 $[\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu_i}+h_{\mu_i}\boldsymbol{G}]$ 的 $\boldsymbol{G}$–陷门 $\boldsymbol{R}_{\mu_i}$。由于 $\boldsymbol{R}_{\mu_i}$ 也是 $[\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{D}_{\mathrm{id}_i}\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu_i}+h_{\mu_i}\boldsymbol{G}]$ 的 $\boldsymbol{G}$–陷门，因此对消息 $\{\mu_i\}_{i\in[Q_2]}$ 的标准签名询问时，算法 $\mathcal{B}$ 可以直接调用算法 SampleD 获得非零短向量 σ_i，满足 $[\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{D}_{\mathrm{id}_i}\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu_i}+h_{\mu_i}\boldsymbol{G}]\sigma_i=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 以及 $\|\sigma_i\|\leqslant\tilde{s}\sqrt{m+2nt}$。

4) 增量签名询问阶段。敌手 $\mathcal{A}$ 也可以适应性地进行增量签名询问。当敌手 $\mathcal{A}$ 询问身份为 id_i 的用户对消息 $\{\mu'_i\}_{i\in[Q_3]}$ 的增量签名时，它需要发送身份 id_i、一个有效的消息签名对 (μ_i,σ_i)，以及新消息 μ'_i 给算法 $\mathcal{B}$，然后算法 $\mathcal{B}$ 执行以下步骤。

① 计算 $\boldsymbol{R}_{\mu'_i}=\boldsymbol{R}_{\mu_i}+((-1)^{\mu'_{ij}}-(-1)^{\mu_{ij}})\boldsymbol{R}_j$ 以及 $h_{\mu'_i}=h_{\mu_i}+((-1)^{\mu'_{ij}}-(-1)^{\mu_{ij}})h_j$。

② 若 $\boldsymbol{S}_{\mathrm{id}_i}\neq\boldsymbol{0}$，则算法 $\mathcal{B}$ 有 $[\bar{\boldsymbol{A}}\,|\,H_{\boldsymbol{K}}(\mathrm{id}_i)]$ 的 G–陷门 $\boldsymbol{D}_{\mathrm{id}_i}$。由于 $\boldsymbol{D}_{\mathrm{id}_i}$ 也是 $[\bar{\boldsymbol{A}}\,|\,H_{\boldsymbol{K}}(\mathrm{id}_i)\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu'_i}+h_{\mu'_i}\boldsymbol{G}]$ 的 G–陷门，因此对消息 $\{\mu'_i\}_{i\in[Q_3]}$ 的增量签名询问，算法 $\mathcal{B}$ 可以直接调用算法 SampleD 获得非零短向量 σ'_i，满足 $[\bar{\boldsymbol{A}}\,|\,H_{\boldsymbol{K}}(\mathrm{id}_i)\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu'_i}+h_{\mu'_i}\boldsymbol{G}]\sigma'_i=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 以及 $\|\sigma'_i\|\leqslant\tilde{s}\sqrt{m+2nt}$。

③ 若 $\boldsymbol{S}_{\mathrm{id}_i}=\boldsymbol{0}$，则算法 $\mathcal{B}$ 执行以下步骤。

a. 若 $h_{\mu'_i}=0$，则 $\mathcal{B}$ 终止。

b. 若 $h_{\mu'_i}\neq0$，则算法 $\mathcal{B}$ 有 $[\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu'_i}+h_{\mu'_i}\boldsymbol{G}]$ 的 $\boldsymbol{G}$–陷门 $\boldsymbol{R}_{\mu'_i}$。由于 $\boldsymbol{R}_{\mu'_i}$ 也是 $[\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{D}_{\mathrm{id}_i}\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu'_i}+h_{\mu'_i}\boldsymbol{G}]$ 的 $\boldsymbol{G}$–陷门，因此对消息 $\{\mu'_i\}_{i\in[Q_3]}$ 的增量签名询问，算法 $\mathcal{B}$ 可以直接调用算法 SampleD 获得非零短向量 σ'_i，满足 $[\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{D}_{\mathrm{id}_i}\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\mu'_i}+h_{\mu'_i}\boldsymbol{G}]\sigma'_i=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 以及 $\|\sigma'_i\|\leqslant\tilde{s}\sqrt{m+2nt}$。

5) 伪造阶段。敌手 $\mathcal{A}$ 以概率 ε 输出新消息 $\hat{\mu}$ 关于身份 $\hat{\mathrm{id}}$ 的签名 $(H(\hat{\mu}),\hat{\sigma})$，算法 $\mathcal{B}$ 执行以下步骤。

① 计算 $\boldsymbol{R}_{\hat{\mu}}=\boldsymbol{R}_0+\sum_{i=0}^{\ell}(-1)^{\hat{\mu}_i}\boldsymbol{R}_i$ 和 $h_{\hat{\mu}}=h_0+\sum_{i=0}^{\ell}(-1)^{\hat{\mu}_i}h_i$。

② 如果 $\boldsymbol{S}_{\hat{\mathrm{id}}}\neq\boldsymbol{0}$ 或 $h_{\hat{\mu}}\neq0$，则 $\mathcal{B}$ 终止。

如果 $\boldsymbol{S}_{\hat{\mathrm{id}}}=\boldsymbol{0}$ 且 $h_{\hat{\mu}}=0$，则根据定义 2 可知，签名 $(H(\hat{\mu}),\hat{\sigma})$ 满足 $[\bar{\boldsymbol{A}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{D}_{\hat{\mathrm{id}}}\,|\,\bar{\boldsymbol{A}}\boldsymbol{R}_{\hat{\mu}}]\hat{\sigma}=\boldsymbol{u}\,(\mathrm{mod}\,q)$ 和 $\|\hat{\sigma}\|\leqslant\tilde{s}\sqrt{m+2nt}$。令 $\boldsymbol{e}=[\boldsymbol{I}_m\,|\,\boldsymbol{D}_{\hat{\mathrm{id}}}\,|\,\boldsymbol{R}_{\hat{\mu}}]\hat{\sigma}$，上式变形为 $\bar{\boldsymbol{A}}\boldsymbol{e}=\boldsymbol{u}\,(\mathrm{mod}\,q)$。将等式右侧的 $\boldsymbol{u}$ 移到左边，得到 $\boldsymbol{A}\hat{\boldsymbol{e}}=\boldsymbol{0}\,(\mathrm{mod}\,q)$, 其中 $\hat{\boldsymbol{e}}=\begin{bmatrix}\boldsymbol{e}\\-1\end{bmatrix}\neq\boldsymbol{0}$ 且 $\|\hat{\boldsymbol{e}}\|<\|\boldsymbol{e}\|+1$。由于 $\|\boldsymbol{e}\|<\left(1+\|\boldsymbol{D}_{\hat{\mathrm{id}}}\|+\|\boldsymbol{R}_{\hat{\mu}}\|\right)\|\hat{\sigma}\|$，$\|\boldsymbol{D}_{\hat{\mathrm{id}}}\|\leqslant s_1(\boldsymbol{D}_{\hat{\mathrm{id}}})$，$\|\boldsymbol{R}_{\hat{\mu}}\|\leqslant s_1(\boldsymbol{R}_{\hat{\mu}})$，并且根据文献[20-21]可知，$s_1(\boldsymbol{D}_{\hat{\mathrm{id}}})\leqslant O(n^{2.5}t^{1.5}\log n)\omega(\log n\sqrt{\log nt})$ 以及 $s_1(\boldsymbol{R}_{\hat{\mu}})\leqslant\sqrt{\ell+1}O(\sqrt{nt})\omega(\sqrt{\log nt})$ 均以极大概率成立，因此 $\|\hat{\boldsymbol{e}}\|<O(n^{3.5}t^{2.5}\log n)\omega(\log^{2.5}n\sqrt{\log nt})$。因此，$\hat{\boldsymbol{e}}$ 是小整数解问题实例 $\boldsymbol{A}=[\bar{\boldsymbol{A}}\,|\,\boldsymbol{u}]$ 的一个解。

最后，计算算法 $\mathcal{B}$ 完整地破解上述小整数解问题的概率 ε'。由于算法 $\mathcal{B}$ 成功破解上述小整数解问题需要私钥提取询问阶段、标准签名询问阶段和增量签名询问阶段都不终止且伪造阶段成功输出 $\hat{\boldsymbol{e}}$，而算法 $\mathcal{B}$ 在私钥提取询问阶段、标准签名询问阶段、增量签名询问阶段以及伪造阶段都不终止，需要满足私钥提取询问阶段所有的 $\boldsymbol{S}_{\mathrm{id}_i}\neq\boldsymbol{0}$、标准签名

询问阶段 $\boldsymbol{S}_{\mathrm{id}_i} \neq \boldsymbol{0}$ 或 $h_{\mu_i} \neq 0$ 以及伪造阶段 $\boldsymbol{S}_{\mathrm{id}^*} = \boldsymbol{0}$ 且 $h_{\hat{\mu}} = 0$ 均成立，而该事件发生的概率不低于 $\boldsymbol{S}_{\mathrm{id}_i} \neq \boldsymbol{0}$ 且 $\boldsymbol{S}_{\mathrm{id}^*} = \boldsymbol{0}$ 和 $h_{\mu_i} \neq 0$ 且 $h_{\hat{\mu}} = 0$ 同时发生的概率，根据文献[20]的定理 3 和文献[22]的引理 27 可知，此概率不低于 $\frac{1}{\kappa q}\left(1-\frac{Q_2+Q_3}{q}\right)=\frac{1}{\omega\left(n\log^2 n\right)q}\left(1-\frac{Q_2+Q_3}{q}\right)$，因此算法 $\mathcal{B}$ 完整地破解上述小整数解问题的概率为 $\varepsilon' \geqslant \frac{\varepsilon}{\omega\left(n\log^2 n\right)q}\left(1-\frac{Q_2+Q_3}{q}\right)$。证毕。

4.3　对比分析

本节将本文方案与基于 PKI 的增量签名方案和基于身份的签名方案分别进行比较。

1) 与基于 PKI 的增量签名方案对比

表 1 给出了本文方案与几种增量签名方案的特征比较。文献[3]和文献[6]的方案都是基于 PKI 的，存在证书管理问题。文献[3]的方案基于离散对数（DL, discrete logarithm）问题的困难性，在随机预言模型下对适应性选择消息攻击是安全的。文献[6]的方案基于格上 k 次小整数解（k-SIS, k-small integer solutions）问题的困难性[27]，在标准模型下对适应性选择消息攻击是安全的。然而由于将 k-SIS 问题规约到标准 SIS 问题会增加乘法因子 $k!$，其中 k 与签名次数有关，因此文献[6]中方案的签名次数较有限。与这 2 种方案相比，本文方案不仅消除了证书管理问题，而且在标准模型下基于标准的 SIS 问题证明了方案满足适应性选择身份和选择消息攻击下的不可伪造性。

表 1　　3 种增量签名方案对比

方案	基于身份	标准模型	困难假设	适应性安全
文献[3]方案	否	否	DL	是
文献[6]方案	否	是	k-SIS	是
本文方案	是	是	SIS	是

2) 与格上基于身份的签名方案对比

表 2 给出了本文方案与几种格上基于身份的签名方案的比较结果，其中 n 表示安全参数，$t=\lceil \log q \rceil$。从表 2 可以看出，虽然本文方案相比文献[11-15]中的方案而言，在公开参数大小、签名密钥大小和签名长度等方面优势不明显，但本文方案的安全性较高。具体地，文献[13-14]中的方案仅在随机预言模型下达到适应性选择身份和选择消息攻击下的不可伪造性，文献[15]中的方案在随机预言机模型下仅对选择身份攻击是安全的，而文献[11-12]中的方案虽然是在标准模型下可证明安全的，但这些方案只对选择身份攻击是安全的。

此外，本文方案还具有增量性。假设 2 个消息仅相差 1 bit，则当已知一个消息的哈希值时，采用本文方案计算新消息的哈希值仅需一次矩阵加法运算即可，而完整的哈希计算则需要计算 $\ell+1$ 次矩阵加法。由于 ℓ 通常较大，因此本文方案可以加快标准签名算法的签名过程。

4.4　性能评估

本节将通过具体实验来展示增量签名算法相对于标准签名算法的性能提升情况。

根据 3.1 节的方案描述可知，标准签名算法与增量签名算法都需要运行 SampleD 和计算消息的哈希值（由于矩阵 $\boldsymbol{A}_{\mathrm{id}}$ 具有一定的稳定性，因此这里忽略其计算开销），然而标准签名算法的消息编码方式为 $H(\mu)=\boldsymbol{C}_0+\sum_{i=1}^{\ell}(-1)^{\mu_i}\boldsymbol{C}_i$，其计算时间与整个消息 μ 的长度成正比，增量签名算法的消息编码方式为 $H(\mu')=H(\mu)+((-1)^{\mu'_j}-(-1)^{\mu_j})\boldsymbol{C}_j$，其计算时间仅与消息的改变量（$\mu'$ 和 μ 之间的比特差异数）成正比。因此，当需要对 d 个连续变化的数据进行签名时，用增量签名方案仅需执行一次标准签名算法和 d–1 次增量签名算法，而采用标准签名方案需执行 d 次标准签名算法。直观上看，增量签名算法的运行时间要比标准签名算法的少，因此增量签名方案

表 2　　本文方案与几种格上基于身份的签名方案对比

方案	公开参数大小	签名密钥大小	签名长度	标准模型	适应性安全
文献[11]方案	$O(n^2t^2)$	$O(n^2t^2)$	$O(nt)$	是	否
文献[12]方案	$O(n^2t)$	$O(n^2t^2)$	$O(nt)$	是	否
文献[13-14]方案	$O(n^2t)$	$O(nt^2)$	$O(nt)$	否	是
文献[15]方案	$O(n^2t)$	$O(n^2t^2)$	$O(n^2t)$	否	否
本文方案	$O(n^2t)$	$O(n^2t^2)$	$O(n^2t)$	是	是

非常适用于处理数据仅有细微差别的大数据系统。

下面给出各算法的实验运行结果，具体包括标准签名算法、增量签名算法以及签名验证算法的计算开销。

本文方案的实验代码采用 C++11 编写、g++5.4.0 编译。实验由配置了 Ubuntu 16.04 LTS 系统、Intel Core i5-7500 CPU 和 16 GB 内存的 PC 运行。本文实验选取 2 组数据，分别是 n=128 和 n=256。消息长度分别为 256 bit、384 bit 和 512 bit，增量签名的消息改变量为原消息长度的一半。在本文实验中，令 $\omega(\sqrt{\log n})=\sqrt{\dfrac{\ln\left(2n\left(1+\dfrac{1}{\varepsilon}\right)\right)}{\pi}}$，其中 $\varepsilon=2^{-80}$，其他相关参数如表 3 所示。所有实验结果均为运行 10 次实验的平均值。

表 3　　实验参数的具体设置

符号	值	
	n=128	n=256
q	$\approx 2^{56}$	$\approx 2^{61}$
β	$\approx 9\times10^{14}$	$\approx 2\times10^{16}$
$s_1(\boldsymbol{R})$	≈ 211	≈ 312
s	$\approx 2\,454$	$\approx 3\,663$
$s_1(\boldsymbol{R}_{\mathrm{id}})$	$\approx 10^5$	$\approx 3\times10^5$
$\tilde{s}$	$\approx 2\times10^6$	$\approx 4\times10^6$

图 1 和图 2 分别展示了当 n=128 和 n=256 时，标准签名算法和增量签名算法的计算时间比较。标准签名算法的计算时间包括计算消息哈希值以及执行 SampleD 的时间，而增量签名算法的计算时间包括计算消息增量哈希值以及执行 SampleD 的时间，其中 Hash 表示计算消息哈希值的时间，IncHash 表示计算消息增量哈希值的时间，SampleD 表示执行 SampleD 的时间。从图 1 和图 2 可以看出，随着消息长度的不断增加，Hash 和 IncHash 都会增长，但 IncHash 的值更小。具体地，当 n=128 时，增量签名算法的整体计算效率相比标准签名算法提高了 41.9%～50.2%；当 n=256 时，增量签名算法的整体计算效率相比标准签名算法提高了 39.9%～48.3%。

表 4 为不同参数下签名验证算法 Verify 的计算时间对比。由于该算法的执行时间对标准签名算法和增量签名算法都是相同的，因此表 4 列出了在不同的 n 和消息长度的情况下，Verify 算法的执行时间变化情况。从表 4 中可以看出，随着 n 和消息长度的增加，Verify 算法所需的时间也会增加，但其绝对值仍较小。

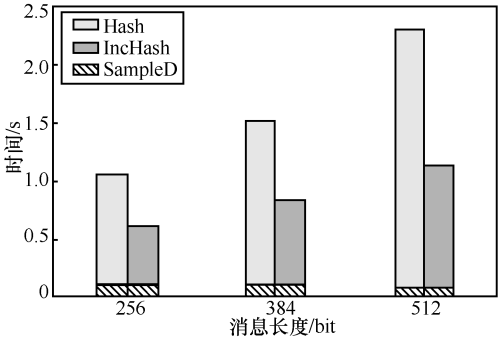

图 1　当 n=128 时，2 种签名算法的计算时间对比

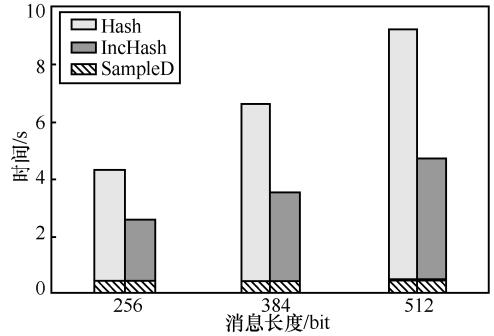

图 2　当 n=256 时，2 种签名算法的计算时间对比

表 4　不同参数下验证算法的计算时间对比

消息长度/bit	计算时间/s	
	n=128	n=256
256	0.96	3.86
384	1.42	6.22
512	2.18	8.81

5　结束语

本文提出了基于身份的增量签名概念，并基于格上困难问题设计了一种具体方案。在标准的小整数解困难假设下，本文方案在标准模型下对适应性选择身份和选择消息攻击是不可伪造的。与基于 PKI 的增量签名方案相比，本文方案消除了公钥证书的管理问题，提高了方案的实际使用效率。此外，与格上基于身份的签名方案相比，本文方案不仅具有增量性和更好的计算效率，而且安全性也较高。

参考文献：

[1] GOLDWASSER S, MICALI S, RIVEST R. A digital signature scheme secure against adaptive chosen-message attacks[J]. SIAM Journal on computing, 1988, 17(2): 281-308.

[2] KHATI L, VERGNAUD D. Analysis and improvement of an authentication scheme in incremental cryptography[C]//International Conference on Selected Areas in Cryptography. Berlin: Springer, 2018: 50-70.

[3] BELLARE M, GOLDREICH O, GOLDWASSER S. Incremental

cryptography: the case of hashing and signing[C]//Annual International Cryptology Conference. Berlin: Springer, 1994: 216-233.

[4] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[5] ATIGHEHCHI K. On the incremental digital signatures[C]//IEEE International Conference on Trust, Security and Privacy in Computing and Communications/IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). Piscataway: IEEE Press, 2018: 1605-1609.

[6] CHEN J, TIAN M, GAO C, et al. A lattice-based incremental signature scheme[J]. IEEE Access, 2019, 7: 21201-21210.

[7] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1984: 47-53.

[8] AJTAI M. Generating hard instances of lattice problems[C]//ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 99-108.

[9] MICCIANCIO D, REGEV O. Worst-case to average-case reductions based on Gaussian measures[J]. SIAM Journal on Computing, 2007, 37(1): 267-302.

[10] REGEV O. Lattice-based cryptography[C]//Annual International Cryptology Conference. Berlin: Springer, 2006: 131-141.

[11] TIAN M, HUANG L, WEI Y. A new hierarchical identity-based signature scheme from lattices in the standard model[J]. International Journal of Network Security, 2012, 14(6): 310-315.

[12] LIU Z, HU Y, ZHANG X, et al. Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model[J]. Security and Communication Networks, 2013, 6(1): 69-77.

[13] TIAN M, HUANG L. Efficient identity-based signature from lattices[C]//IFIP International Information Security Conference. Berlin: Springer, 2014: 321-329.

[14] TIAN M, HUANG L. Identity-based signatures from lattices: simpler, faster, shorter[J]. Fundamenta Informaticae, 2016, 145(2): 171-187.

[15] YANG Z, DUONG D, et al. Hierarchical identity-based signature in polynomial rings[J]. The Computer Journal, 2020, 63(10): 1490-1499.

[16] XIE J, HU Y, GAO J, et al. Efficient identity-based signature over NTRU lattice[J]. Frontiers of Information Technology & Electronic Engineering, 2016, 17(2): 135-142.

[17] ZHAO G, TIAN M. A simpler construction of identity-based ring signatures from lattices[C]//International Conference on Provable Security. Berlin: Springer, 2018: 277-291.

[18] 孙意如, 梁向前, 商玉芳. 理想格上基于身份的环签名方案[J]. 计算机应用, 2016, 36(7): 1861-1865.
SUN Y R, LIANG X Q, SHANG Y F. Identity based ring signature scheme in ideal lattice[J]. Journal of Computer Applications, 2016, 36(7): 1861-1865.

[19] CANETTI R, GOLDREICH O, HALEVI S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4): 557-594.

[20] ZHANG J, CHEN Y, ZHANG Z. Programmable hash functions from lattices: short signatures and IBEs with small key sizes[C]//Annual International Cryptology Conference. Berlin: Springer, 2016: 303-332.

[21] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 700-718.

[22] BOYEN X. Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2010: 499-517.

[23] CHOON J, CHEON J. An identity-based signature from gap Diffie-Hellman groups[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2003: 18-30.

[24] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//ACM Symposium on Theory of Computing. New York: ACM Press, 2005: 84-93.

[25] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]//ACM Symposium on Theory of Computing. New York: ACM Press, 2008: 197-206.

[26] HOFHEINZ D, KILTZ E. Programmable hash functions and their applications[C]//Annual International Cryptology Conference. Berlin: Springer, 2008: 21-38.

[27] BONEH D, FREEMAN D. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2011: 1-16.

[作者简介]

田苗苗（1987− ），男，安徽阜阳人，博士，安徽大学副教授、硕士生导师，主要研究方向为密码学与信息安全。

陈静（1996− ），女，安徽池州人，安徽大学硕士生，主要研究方向为密码学与信息安全。

仲红（1965− ），女，安徽固镇人，博士，安徽大学教授、博士生导师，主要研究方向为网络与信息安全。