计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20150887
54(2):305-312, 2017

新的基于格的可验证加密签名方案

张彦华　　胡予濮
(综合业务网理论与关键技术国家重点实验室(西安电子科技大学)　西安　710071)
(yhzhangxidian@163.com)

A New Verifiably Encrypted Signature Scheme from Lattices

Zhang Yanhua and Hu Yupu
(*State Key Laboratory of Integrated Service Networks* (*Xidian University*), *Xi'an* 710071)

Abstract　Verifiably encrypted signatures (VES) can ensure the fairness of the Internet exchange process effectively. In a VES system, a signer can generate an ordinary signature on a given message using the secret key of the signer and then encrypt it under the public key of the adjudicator. A verifier should be able to verify that this encrypted signature is indeed an encryption of the ordinary signature of the signer, but the verifier cannot be able to extract the ordinary signature. The ordinary signature can only be recovered by the adjudicator from this encrypted signature. Using the technique of basis delegation in fixed dimension suggested by Agrawal et al in CPYPTO 2010, the lattice-based preimage sampling algorithm and a non-interactive zero-knowledge proof for the learning with errors (LWE) problem, this paper constructs a new verifiably encrypted signature scheme from lattices, and based on the hardness of the short integer solution (SIS) problem and the LWE problem, this proposed construction is provably strong unforgeable in the random oracle model. Compared with current verifiably encrypted signature schemes, this scheme needs that the public-private key pair of the signer should be generated according to the public key of the adjudicator, and this scheme can resist quantum attacks and enjoy simpler constructions, shorter public-private keys, smaller signature size and higher efficiency.

Key words　verifiably encrypted signature (VES); fixed dimension; lattice; random oracle model; the learning with errors

摘　要　可验证加密签名(verifiably encrypted signature, VES)能够有效地保证互联网上交易过程的公平性.VES的核心思想是:签名者利用仲裁者的公钥对自己所签发的一个普通数字签名进行加密,随后证明密文中确实包含一个普通签名,任何验证者都可以利用仲裁者的公钥来验证其真实性,但在没有签名者或仲裁者的帮助下无法从中提取出普通签名;当争议发生时,验证者可以要求仲裁者从可验证加密签名中恢复出签名者的普通签名.利用Agrawal等人在美密2010上给出的固定维数的格基委派技术、格上原像抽样算法和差错学习问题的非交互零知识证明,该文构造出一个新的格上可验证加密签名方案,并在随机预言机模型下严格证明了其安全性.与已有的可验证加密签名方案相比,该方案要求签名者根据仲裁者公钥生成签名者公私钥对,构造简单,公私钥和签名尺寸更短,效率更高,并且能够抵抗量子攻击.

收稿日期:2015-09-30;**修回日期**:2016-05-16
基金项目:国家自然科学基金项目(61472309)
This work was supported by the National Natural Science Foundation of China (61472309).

关键词 可验证加密签名(VES);固定维数;格;随机预言机模型; 差错学习问题

中图法分类号 TP309

互联网在线交易已逐渐成为日常生活中比较重要的商品交换方式,如何在分布式网络中保证交换过程的公平性是电子商务安全亟待解决的关键问题之一. 1997 年,Asokan 等人[1]首次提出可验证加密签名(verifiably encrypted signature, VES)的概念. 可验证加密签名能够有效地保证互联网上交易过程的公平性. 一个可验证加密签名方案包含 3 个参与者:签名者(又称用户)、验证者和可信第三方(又称仲裁者). VES 的核心思想是:签名者利用仲裁者的公钥对自己所签发的一个普通数字签名进行加密,随后证明密文中确实包含一个普通签名,任何验证者都可以利用仲裁者的公钥来验证其真实性,但在没有签名者或仲裁者的帮助下无法从中提取出普通签名;当争议发生时,验证者可以要求仲裁者从可验证加密签名中恢复出签名者的普通签名.

基于双线性 Diffie-Hellman 假设,Boneh 等人[2]于 2003 年给出了第 1 个有效的非交互的 VES 方案. 签名验证过程不需要零知识证明,而且方案在随机预言机模型下是可证明安全的. 自此以后,VES 引起了众多学者的广泛关注,很多基于标准数论假设的 VES 方案相继被提出[3-7].

近年来,基于格构造新型密码系统因具有较高的渐进效率、运算简单和抗量子攻击等特点,成为后量子时代密码领域的研究热点,并取得了一系列研究成果[8-11]. 2010 年,Rückert 等人[12]构造出第 1 个基于格的标准模型下的 VES 方案,然而该方案是静态化的. 2011 年,Wang 等人[13]构造出第 1 个基于格的随机预言机模型下非静态化的 VES 方案,然而该方案不满足强不可伪造性. 2014 年,Kim 等人[14]构造出一个高效的基于格的 VES 方案,该方案不再额外需要梅克尔树(Merkle trees),但是签名者的公私钥尺寸和可验证加密签名的尺寸都明显较大.

本文增添仲裁者密钥生成阶段来生成仲裁者公私钥,并利用 Agrawal 等人[15]提出的固定维数的格基委派技术来生成签名者密钥,从而有效地减小签名者的公私钥尺寸;然后运用原像抽样算法和差错学习问题(learning with errors, LWE) 的非交互零知识证明构造出一个新的格上可验证加密签名方案,并在随机预言机模型下严格证明了其安全性. 与已有的基于格的可验证加密签名方案相比,该方案构造简单,公私钥和签名尺寸更短,效率更高.

1 基础知识

1.1 格

定义 1. 设 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 是 $\mathbb{R}^n$ 上 m 个线性无关的向量,格 Λ 定义为所有这些向量的整数线性组合构成的集合,即 $\Lambda=\mathcal{L}(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m)=\left\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i \mid x_i\in\mathbb{Z}\right\}$,其中向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 构成格 Λ 的一组基 $\boldsymbol{B}$.

定义 2. 设 q 是一个素数,$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$\boldsymbol{u}\in\mathbb{Z}_q^n$,则:

$$\Lambda_q^{\perp}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{x}=\boldsymbol{0} \bmod q\}, \tag{1}$$

$$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})=\{\boldsymbol{x}\in\mathbb{Z}^m \mid \boldsymbol{A}\boldsymbol{x}=\boldsymbol{u} \bmod q\}. \tag{2}$$

定义 3. 对任意 $s>0$,定义以向量 $\boldsymbol{c}$ 为中心,s 为参数的格 Λ 上的离散高斯分布为:

$$D_{\Lambda,s,\boldsymbol{c}}(\boldsymbol{x})=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\Lambda)}=\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\sum\limits_{\boldsymbol{x}\in\Lambda}\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}, \tag{3}$$

其中 $\boldsymbol{x}\in\Lambda$,$\rho_{s,\boldsymbol{c}}(\boldsymbol{x})=\exp(-\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2/s^2)$.

1.2 重要算法

引理 1[8]. 设 n 是正整数,$q\geqslant 2$,$m\geqslant 2n\operatorname{lb}q$,对于除了至多 $2q^{-n}$ 的部分之外所有的 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 以及任意 $s\geqslant\omega(\sqrt{\operatorname{lb}n})$,向量 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{e} \bmod q$ 的分布统计接近 $\mathbb{Z}_q^n$ 上的均匀分布,其中 $\boldsymbol{e}\in D_{\mathbb{Z}^m,s}$.

格上陷门抽样算法($TrapGen$)、离散高斯抽样算法($SampGau$)和原像抽样算法($SampPre$)由如下 2 个引理给出.

引理 2[9]. 设 n 是正整数,$q\geqslant 2$,$m>5n\operatorname{lb}q$,存在概率多项式时间(probabilistic polynomial time, PPT)算法 $TrapGen(q,n)$,输出 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$,其中 $\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times m}$ 上是统计均匀的,$\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基,且满足

$$\|\boldsymbol{T}_{\boldsymbol{A}}\|\leqslant O(n\operatorname{lb}q),\ \|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\leqslant O(\sqrt{n\operatorname{lb}q}).$$

引理 3[8]. 设 n 是正整数,素数 $q\geqslant 2$,$m>n$,矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$. $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基,高斯参数 $s\geqslant\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\times\omega(\sqrt{\operatorname{lb}m})$. 对于 $\boldsymbol{c}\in\mathbb{R}^m$ 和 $\boldsymbol{u}\in\mathbb{R}_q^n$,有:

1) $Pr[\|\boldsymbol{x}\|>s\sqrt{m} \mid \boldsymbol{x}\in D_{\Lambda_q^{\perp}(\boldsymbol{A}),s,\boldsymbol{c}}]\leqslant negl(n)$.

2) 存在 PPT 算法 $SampGau(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},s,\boldsymbol{c})$,输出一个统计接近 $D_{\Lambda_q^{\perp}(\boldsymbol{A}),s,\boldsymbol{c}}$ 的格向量 $\boldsymbol{x}\in\Lambda_q^{\perp}(\boldsymbol{A})$.

3) 存在 PPT 算法 $SampPre(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},\boldsymbol{u},s)$,输出一个统计接近 $D_{\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}),s}$ 的格向量 $\boldsymbol{x}\in\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A})$.

Gordon 等人[10]提出了一个变形的格基陷门抽样算法($OrthoSamp$),由如下引理给出.

引理 4[10]. 设 n 是正整数,素数 $q\geqslant 2$,正整数 $m\geqslant n+8n\operatorname{lb}q$,矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$ 的列向量的子集合构成 $\mathbb{Z}_q^n$. 存在 PPT 算法 $OrthoSamp(q,\boldsymbol{B})$,输出矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$,使得:

1) $\boldsymbol{A}\boldsymbol{B}^{\mathrm{T}}=\boldsymbol{0} \bmod q$,其中 $\boldsymbol{A}$ 的秩为 n,且在 $\mathbb{Z}_q^{n\times m}$ 上是统计均匀的.

2) $\boldsymbol{T}_{\boldsymbol{A}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基,即 $\boldsymbol{A}\boldsymbol{T}_{\boldsymbol{A}}=\boldsymbol{0} \bmod q$.

3) $\boldsymbol{T}_{\boldsymbol{A}}$ 的任一列向量 $\boldsymbol{t}_i\in\mathbb{Z}_q^m$ 统计接近 $D_{\Lambda_q^{\perp}(\boldsymbol{A}),s}$,其中 $s\geqslant O(\sqrt{n\operatorname{lb}q})\times\omega(\sqrt{\operatorname{lb}m})$.

定义 4. 对于矩阵 $\boldsymbol{A}\in\mathbb{Z}^{m\times m}$,如果 $\boldsymbol{A} \bmod q$ 作为 $\mathbb{Z}_q^{m\times m}$ 中的矩阵是可逆的,则称 $\boldsymbol{A}$ 是 $\mathbb{Z}_q$ 可逆的.

定义 5. 设 $\sigma_{\mathrm{R}}=\sqrt{n\operatorname{lb}q}\times\omega(\sqrt{\operatorname{lb}m})$,令 $D_{m\times m}$ 表示按照 $(D_{\boldsymbol{Z}^m,\sigma_{\mathrm{R}}})^m$ 来抽取的并且在 $\mathbb{Z}^{m\times m}$ 上 $\mathbb{Z}_q$ 可逆的矩阵分布.

Agrawal 等人[15]提出的格基委派技术($BasisDel$)能够生成固定维数的格基陷门,由如下引理给出.

引理 5[15]. 设 n 是正整数,$q>2$,$m>2n\operatorname{lb}q$,$\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基,可逆矩阵 $\boldsymbol{R}\in D_{m\times m}$,高斯参数 $s\geqslant\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|\times\sigma_{\mathrm{R}}\sqrt{m}\times\omega(\operatorname{lb}m)^3$. 存在 PPT 算法 $BasisDel(\boldsymbol{A},R,\boldsymbol{T}_{\boldsymbol{A}},s)$,输出 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$ 和 $T_{\boldsymbol{B}}\in\mathbb{Z}_q^{m\times m}$,其中 $\boldsymbol{B}=\boldsymbol{A}\boldsymbol{R}^{-1} \bmod q$,$\boldsymbol{T}_{\boldsymbol{B}}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的陷门基,且对于参数 s 的最小值满足 $\|\widetilde{\boldsymbol{T}}_{\boldsymbol{B}}\|\leqslant\|\widetilde{\boldsymbol{T}}_{\boldsymbol{A}}\|m^{1.5}\times\omega(\sqrt{\operatorname{lb}m})^4$.

引理 5 需要知道格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基 $\boldsymbol{T}_{\boldsymbol{A}}$ 和可逆矩阵 $\boldsymbol{R}$ 才能得到格 $\Lambda_q^{\perp}(\boldsymbol{A}\boldsymbol{R}^{-1})$ 的陷门基. 然而,如引理 6 指出,在选取可逆矩阵 $\boldsymbol{R}$ 的情况下,不用知道格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基就可以得到格 $\Lambda_q^{\perp}(\boldsymbol{A}\boldsymbol{R}^{-1})$ 的陷门基. 该性质对方案的安全性证明特别重要.

引理 6[15]. 设 n 是正整数,$q>2$,$m>2n\operatorname{lb}q$,矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 的列向量的子集合构成 $\mathbb{Z}_q^n$. 存在 PPT 算法 $SampRwith(\boldsymbol{A})$,输出矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$,$\boldsymbol{R}\in\mathbb{Z}_q^{m\times m}$ 和 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}_q^{m\times m}$,其中 $\boldsymbol{B}=\boldsymbol{A}\boldsymbol{R}^{-1} \bmod q$,其分布统计接近于 $D_{m\times m}$,矩阵 $\boldsymbol{T}_{\boldsymbol{B}}\in\mathbb{Z}_q^{m\times m}$ 是格 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的陷门基,且满足 $\|\widetilde{\boldsymbol{T}}_{\boldsymbol{B}}\|\leqslant O(\sqrt{n\operatorname{lb}q})$.

1.3 格上困难问题

定义 6. 小整数解问题(small integer solution, SIS). 设 n 是正整数,q 为素数,给定随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和实数 $\beta=poly(n)$,找到非零向量 $\boldsymbol{e}$,使得 $\boldsymbol{A}\boldsymbol{e}=\boldsymbol{0} \bmod q$ 且 $\|\boldsymbol{e}\|\leqslant\beta$.

定义 7. 非齐次小整数解问题(inhomogeneous small integer solution, ISIS). 设 n 是正整数,q 为素数,给定矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和向量 $\boldsymbol{y}\in\mathbb{Z}_q^n$,实数 $\beta=poly(n)$,找到非零向量 $\boldsymbol{e}$,使得 $\boldsymbol{A}\boldsymbol{e}=\boldsymbol{y} \bmod q$ 且 $\|\boldsymbol{e}\|\leqslant\beta$.

引理 7[7]. 设 n 是正整数,$m,\beta=poly(n)$,对于任意素数 $q\geqslant\beta\times\omega(\sqrt{n\operatorname{lb}n})$,平均情况下的 SIS 和 ISIS 问题的困难性与最差情况下的近似最短独立向量问题(shortest independent vector problem, SIVP)的困难性是相同的,其近似因子为 $\gamma_1=\beta\times\widetilde{O}(\sqrt{n})$.

定义 8. 差错学习问题(learning with errors, LWE). 设 n 是正整数,q 为素数,对任意 $0<\alpha<1$,定义 ψ_α 为期望值为 0、标准差为 $\alpha/\sqrt{2\pi}$ 的 $[0,1)$ 上的正态分布,对应的 $\mathbb{Z}_q$ 上的离散分布为 $\bar{\psi}_\alpha$. 定义 $\boldsymbol{A}_{\boldsymbol{s},\bar{\psi}_\alpha}$ 为 $(\boldsymbol{u}_i,v_i)=(\boldsymbol{u}_i,\boldsymbol{u}_i^{\mathrm{T}}\boldsymbol{s}+x_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的分布,其中 $\boldsymbol{s},\boldsymbol{u}_i\in\mathbb{Z}_q^n$ 是随机选取的向量,$x_i\in\mathbb{Z}_q$ 依分布 $\bar{\psi}_\alpha$ 独立随机选取. LWE 问题是指给定 $\boldsymbol{A}_{\boldsymbol{s},\chi}$ 上多项式个样本量,找到向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$.

引理 8[16]. 设 n 是正整数,素数 $q>2\sqrt{n}/\alpha$,如果存在一个有效的量子算法解决 LWE 问题,那么就存在一个有效的量子算法解决最差情况下的近似 SIVP 问题,其近似因子为 $\gamma_2=\widetilde{O}(n/\alpha)$.

1.4 格上非交互零知识证明

2013 年,Laguillaumie 等人[17]给出了一个满足如下 ISIS 关系的非交互零知识证明协议,即

$$\begin{aligned}\mathrm{R}_{\mathrm{ISIS}}=\{&(\boldsymbol{A},\boldsymbol{y},\beta;\boldsymbol{x})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^n\times\mathbb{R}\times\mathbb{Z}^m;\\&\boldsymbol{A}\boldsymbol{x}=\boldsymbol{y} \bmod q,\|\boldsymbol{x}\|\leqslant\beta\}.\end{aligned}\tag{4}$$

利用 LWE 困难问题与 ISIS 困难问题的对偶性,Laguillaumie 等人同时给出了满足如下 LWE 关系的一个有效的零知识证明协议,即

$$\begin{aligned}R_{\mathrm{LWE}}=\{&(\boldsymbol{A},\boldsymbol{b},\alpha;\boldsymbol{s})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m\times\mathbb{R}\times\mathbb{Z}_q^n;\\&\|\boldsymbol{b}-\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}\|\leqslant\alpha q\sqrt{m}\}.\end{aligned}\tag{5}$$

2 可验证加密签名

2.1 定 义

可验证加密签名由如下 8 个 PPT 算法构成.

1) 系统建立($Setup$). 给定安全参数 λ,输出系统公开参数 PP.

2) 仲裁者密钥生成($Adj\text{-}KeyGen$). 给定公开参数 PP,输出仲裁者公私钥对(APK,ASK).

3) 签名者密钥生成($KeyGen$). 给定公开参数 PP、仲裁者公钥 APK,输出签名者公私钥对(PK,SK).

4) 普通签名生成($Sign$). 给定公开参数 PP、私钥 SK 和消息 M,输出普通签名 σ.

5) 普通签名验证($Verify$). 给定公开参数 PP、公钥 PK、签名 σ 和消息 M,输出接受或拒绝.

6) 可验证加密签名生成($VES\text{-}Sign$). 给定私钥 SK、消息 M 和仲裁者公钥 APK,输出可验证加密签名 ω.

7) 可验证加密签名验证($VES\text{-}Verify$). 给定公钥 PK、APK、签名 ω 和消息 M,输出接受或拒绝.

8) 仲裁(Adj). 给定公钥 PK、APK、仲裁者私钥 ASK、可验证加密签名 ω 和消息 M,输出普通签名 σ.

可验证加密签名方案的正确性需满足如下 2 点:

1) 运用 $VES\text{-}Sign$ 算法生成的可验证加密签名 ω 必须能通过 $VES\text{-}Verify$ 算法的验证;

2) 仲裁者运用 Adj 算法可以有效地从可验证加密签名 ω 中恢复出原始普通签名 σ,且 σ 必能通过 $Verify$ 算法的验证.

2.2 安全模型

可验证加密签名方案应满足强不可伪造性、强不透明性和可提取性 3 个安全属性. 可通过攻击者与挑战者的交互游戏来定义其安全性.

定义 9. 强不可伪造性. 若不存在多项式有界的敌手 $\mathcal{A}_1$ 能以不可忽略的优势赢得以下游戏,则称一个 VES 方案是强不可伪造的.

1) 系统建立. 挑战者 $\mathcal{C}_1$ 输入安全参数 λ,运行 $Setup$,$Adj\text{-}KeyGen$ 和 $KeyGen$ 算法生成 VES 方案的公开参数 PP 和所有公私钥对(APK,ASK),(PK,SK),并将(PP,APK,ASK,PK)发送给敌手 $\mathcal{A}_1$.

2) 询问阶段. $\mathcal{A}_1$ 适应性地进行多项式次如下询问.

① 普通签名生成询问. $\mathcal{C}_1$ 运行 $Sign$ 算法可获得任何消息 M 的普通签名 σ,并返回给 $\mathcal{A}_1$.

② 可验证加密签名生成询问. $\mathcal{C}_1$ 运行 $VES\text{-}Sign$ 算法获得任何消息 M 的 VES 签名 ω,并返回给 $\mathcal{A}_1$.

3) 伪造阶段. 最后,敌手 $\mathcal{A}_1$ 输出一个消息 M^* 及其 VES 签名 ω^*.

敌手 $\mathcal{A}_1$ 赢得上述游戏当且仅当:

1) ω^* 是消息 M^* 的一个合法 VES;

2) (M^*,ω^*)不是一个可验证加密签名生成的询问结果.

定义 10. 强不透明性. 若不存在多项式有界的敌手 $\mathcal{A}_2$ 能以不可忽略的优势赢得以下游戏,则称一个 VES 方案是强不透明的.

1) 系统建立. 挑战者 $\mathcal{C}_2$ 输入安全参数 λ,运行 $Setup$,$Adj\text{-}KeyGen$ 和 $KeyGen$ 算法生成 VES 方案的公开参数 PP 和所有公私钥对(APK,ASK),(PK,SK),并将(PP,APK,PK)发送给敌手 $\mathcal{A}_2$.

2) 询问阶段. $\mathcal{A}_2$ 适应性地进行多项式次如下询问.

① 普通签名生成询问. $\mathcal{C}_2$ 运行 $Sign$ 算法可获得任何消息 M 的普通签名 σ,并返回给 $\mathcal{A}_2$.

② 可验证加密签名生成询问. $\mathcal{C}_2$ 运行 $VES\text{-}Sign$ 算法可获得任何消息 M 的 VES 签名 ω,并返回给 $\mathcal{A}_2$.

③ 仲裁询问. $\mathcal{C}_2$ 运行 Adj 算法可获得消息 M 及其 VES 签名 ω 对应的普通签名 σ,并返回给 $\mathcal{A}_2$.

3) 伪造阶段. 最后,敌手 $\mathcal{A}_2$ 输出一个消息 M^* 及其普通签名 σ^*.

敌手 $\mathcal{A}_2$ 赢得上述游戏当且仅当:

1) σ^* 是消息 M^* 的一个合法普通签名;

2) (M^*,σ^*)不是一个仲裁询问结果.

定义 11. 可提取性. 若不存在多项式有界的敌手 $\mathcal{A}_3$ 能以不可忽略的优势赢得以下游戏,则称一个 VES 方案是可提取的.

1) 系统建立. 挑战者 $\mathcal{C}_3$ 输入安全参数 λ,运行 $Setup$ 和 $Adj\text{-}KeyGen$ 算法生成 VES 方案的公开参数 PP 和所有仲裁者公私钥对(APK,ASK),并将(PP,APK)发送给敌手 $\mathcal{A}_3$.

2) 询问阶段. $\mathcal{A}_3$ 适应性地进行多项式次如下询问.

仲裁询问:$\mathcal{C}_3$ 运行 Adj 算法可获得消息 M 及其 VES 签名 ω 对应的普通签名 σ,并返回给 $\mathcal{A}_3$.

3) 伪造阶段. 最后,敌手 $\mathcal{A}_3$ 输出一个消息 M^* 及其 VES 签名 ω^*,对应的签名者的公钥为 PK^*.

敌手 $\mathcal{A}_3$ 赢得上述游戏当且仅当:

1) ω^* 是消息 M^* 的一个合法 VES;

2)$\sigma^*=Adj(PP,ASK,APK,PK^*,\omega^*,M^*)$不是消息 M^* 的一个合法普通签名.

3 新的基于格的 VES 方案

3.1 方案构造

1) 系统建立. 输入安全参数 n,具体参数设置见 3.2 节. 选取 2 个安全的抗碰撞 Hash 函数 H_1:{0,

$1\}^{*}\rightarrow D_{m\times m}$,$H_2:\{0,1\}^{*}\times\mathbb{Z}_q^m\rightarrow\mathbb{Z}_q^n$;输出系统公开参数 $PP=(n,m,q,s_1,s_2,s_3,\alpha,H_1,H_2)$.

2) 仲裁者密钥生成. 输入公开参数 PP,运行算法 $TrapGen(q,n)$生成随机矩阵 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$和格 $\Lambda_q^{\perp}(\boldsymbol{B})$的陷门基 $T_{\boldsymbol{B}}\in\mathbb{Z}_q^{m\times m}$,且 $\|\tilde{\boldsymbol{T}}_{\boldsymbol{B}}\|\leqslant O(\sqrt{n\,\mathrm{lb}\,q})$;输出仲裁者公私钥对$(APK,ASK)=(\boldsymbol{B},\boldsymbol{T}_{\boldsymbol{B}})$.

3) 签名者密钥生成. 输入公开参数 PP 和仲裁者公钥 $APK=\boldsymbol{B}$;运行算法 $OrthoSamp(q,\boldsymbol{B})$生成随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和格 $\Lambda_q^{\perp}(\boldsymbol{A})$的陷门基 $\boldsymbol{T}_{\boldsymbol{A}}\in\mathbb{Z}_q^{m\times m}$,满足 $\boldsymbol{A}\boldsymbol{B}^{\mathrm{T}}=\boldsymbol{0}\bmod q$;输出公私钥对$(PK,SK)=(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}})$.

4) 普通签名. 输入公开参数 PP、私钥 $SK=\boldsymbol{T}_{\boldsymbol{A}}$ 和消息 M,签名者进行如下操作.

① 随机选取比特串 $\boldsymbol{r}\leftarrow\{0,1\}^n$ 和向量 $\boldsymbol{v}\in\mathbb{Z}_q^m$.

② 运行算法 $SampPre(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},H_2(M\|\boldsymbol{r}\|\boldsymbol{v}),s_1)$,生成向量 $\boldsymbol{d}\in\mathbb{Z}^m$.

③ 输出普通签名 $\sigma=(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{d})$.

5) 普通签名验证. 输入签名者公钥 $PK=\boldsymbol{A}$ 和签名 $\sigma=(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{d})$;如果 $\|\boldsymbol{d}\|\leqslant s_1\sqrt{m}$,$\boldsymbol{A}\boldsymbol{d}=H_2(M\|\boldsymbol{r}\|\boldsymbol{v})$,则接受 σ 为签名者对给定消息 M 的一个有效普通签名,否则,拒绝.

6) 可验证加密签名生成. 输入公开参数 PP、私钥 $SK=\boldsymbol{T}_{\boldsymbol{A}}$、仲裁者公钥 $APK=\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$和消息 M,签名者进行如下操作.

① 选取随机比特串 $\boldsymbol{r}\leftarrow\{0,1\}^n$,误差向量 $\boldsymbol{x}\in\bar{\psi}_{\alpha}^m$ 和随机向量 $\boldsymbol{s}\in\mathbb{Z}_q^m$.

② 令 $\boldsymbol{R}=H_1(M\|\boldsymbol{r})$,$\boldsymbol{B}'=\boldsymbol{B}\boldsymbol{R}^{-1}\in\mathbb{Z}_q^{n\times m}$.

③ 计算 $\boldsymbol{v}=\boldsymbol{B}'^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}\bmod q$,并构造对 $\boldsymbol{v}$ 的一个有效非交互零知识证明 π.

④ 运行 $SampPre(\boldsymbol{A},\boldsymbol{T}_{\boldsymbol{A}},H_2(M\|\boldsymbol{r}\|\boldsymbol{v})-\boldsymbol{A}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x},s_2)$生成向量 $\boldsymbol{e}\in\mathbb{Z}^m$.

⑤ 输出可验证加密签名 $\omega=(M,\boldsymbol{r},\boldsymbol{v},\pi,\boldsymbol{e})$.

7) 可验证加密签名验证. 输入签名者公钥 $PK=\boldsymbol{A}$、仲裁者公钥 $APK=\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$和签名 $\omega=(M,\boldsymbol{r},\boldsymbol{v},\pi,\boldsymbol{e})$;首先验证非交互零知识证明 π 的有效性,计算 $\boldsymbol{R}=H_1(M\|\boldsymbol{r})$,如果 π 是有效的,$\boldsymbol{A}\boldsymbol{B}^{\mathrm{T}}=\boldsymbol{0}\bmod q$,$\|\boldsymbol{e}\|\leqslant s_2\sqrt{m}$,$\boldsymbol{A}(\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{v})=H_2(M\|\boldsymbol{r}\|\boldsymbol{v})\bmod q$,则接受 ω 为签名者对消息 M 的一个有效的可验证加密签名;否则,拒绝.

8) 仲裁. 输入签名者公钥 $PK=\boldsymbol{A}$,仲裁者私钥 $ASK=\boldsymbol{T}_{\boldsymbol{B}}$ 和签名 $\omega=(M,\boldsymbol{r},\boldsymbol{v},\pi,\boldsymbol{e})$,仲裁者进行如下操作.

① 计算 $\boldsymbol{R}=H_1(M\|\boldsymbol{r})$.

② 运行算法 $BasisDel(\boldsymbol{B},\boldsymbol{R},\boldsymbol{T}_{\boldsymbol{B}},s_3)$生成随机矩阵 $\boldsymbol{B}'=\boldsymbol{B}\boldsymbol{R}^{-1}\in\mathbb{Z}_q^{n\times m}$和 $\Lambda_q^{\perp}(\boldsymbol{B}')$的陷门基 $\boldsymbol{T}_{\boldsymbol{B}'}\in\mathbb{Z}_q^{m\times m}$.

③ 利用 $\boldsymbol{T}_{\boldsymbol{B}'}$从 $\boldsymbol{v}=\boldsymbol{B}'^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x}\bmod q$ 中解出$(\boldsymbol{s},\boldsymbol{x})$.

④ 计算 $\boldsymbol{d}=\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}\in\mathbb{Z}_q^m$.

⑤ 输出普通签名 $\sigma=(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{d})$.

3.2 参数设置

为保证仲裁过程中可以从 $\boldsymbol{v}$ 中有效解出$(\boldsymbol{s},\boldsymbol{x})$和系统的安全运行,给定安全参数为 n,设置其他参数如下:

$$m=n+8n^{1+\delta},\tag{6}$$

$$q=80m^{1.5}\sqrt{n}\times\omega\sqrt{\mathrm{lb}\,m},\tag{7}$$

$$\alpha=1/40m^{1.5}\omega\sqrt{\mathrm{lb}\,m},\tag{8}$$

$$s_1=2m^{1.5}\sqrt{n}\times\omega(\mathrm{lb}\,m)+\sqrt{m}\times\omega\sqrt{\mathrm{lb}\,m},\tag{9}$$

$$s_2=\sqrt{m}\times\omega\sqrt{\mathrm{lb}\,m},\tag{10}$$

$$s_3=m^{1.5}\times\omega(\sqrt{\mathrm{lb}\,m})^4,\tag{11}$$

$$n^{\delta}>|b(q)|=O(\mathrm{lb}\,n).\tag{12}$$

3.3 安全性证明

3.3.1 正确性

令 $\omega=(M,\boldsymbol{r},\boldsymbol{v},\pi,\boldsymbol{e})$是可验证加密签名生成算法的一个输出,方案的正确性分析如下:

1) 由于签名者选取随机向量 $\boldsymbol{s}$,从而签名者可以构造出一个有效的非交互零知识证明 π.

2) 仲裁者计算 $\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}\boldsymbol{v}\bmod q=\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}(\boldsymbol{B}'^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x})\bmod q=(\boldsymbol{B}'\boldsymbol{T}_{\boldsymbol{B}'})^{\mathrm{T}}+\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}\boldsymbol{x}\bmod q=\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}\boldsymbol{x}\bmod q$,由于 $\boldsymbol{T}_{\boldsymbol{B}'}$ 和 $\boldsymbol{x}$ 的分量元素都比较小,向量 $\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}\boldsymbol{x}$ 的每一个分量都远小于 q,从而 $\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}\boldsymbol{x}\bmod q=\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}\boldsymbol{x}$,容易计算$(\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}})^{-1}(\boldsymbol{T}_{\boldsymbol{B}'}^{\mathrm{T}}\boldsymbol{x})=\boldsymbol{x}$.

3) 容易计算 $\boldsymbol{A}\sigma=\boldsymbol{A}(\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x})=\boldsymbol{A}\boldsymbol{e}+\boldsymbol{A}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}=H_2(M\|\boldsymbol{r}\|\boldsymbol{v})\bmod q$.

4) 在可验证加密签名验证算法中,我们有:

$$\boldsymbol{A}(\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{v})=\boldsymbol{A}\boldsymbol{e}+\boldsymbol{A}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{v}=\boldsymbol{A}\boldsymbol{e}+\boldsymbol{A}\boldsymbol{R}^{\mathrm{T}}(\boldsymbol{B}'^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x})=$$
$$\boldsymbol{A}\boldsymbol{e}+\boldsymbol{A}(\boldsymbol{B}'\boldsymbol{R})^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{A}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}=\boldsymbol{A}\boldsymbol{e}+\boldsymbol{A}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{A}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}=$$
$$\boldsymbol{A}(\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x})=H_2(M\|\boldsymbol{r}\|\boldsymbol{v})\bmod q.$$

3.3.2 强不可伪造性

定理 1. 如果存在敌手 $\mathcal{A}_1$ 以不可忽略的优势 ε_1 攻破方案的强不可伪造性,则可构造算法 $\mathcal{B}_1$ 以概率 ε_1/q_{H_2} 求解 ISIS 问题,其中 q_{H_2} 表示敌手可进行 H_2 询问的最大次数.

证明. 假设 $\mathcal{B}_1$ 获得了一个 ISIS 问题实例($\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$,$\boldsymbol{y}\in\mathbb{Z}_q^n$,$n,m,q,s$),要求 $\mathcal{B}_1$ 通过模拟游戏利用 $\mathcal{A}_1$ 求解出一个非零向量 $\boldsymbol{e}$,使得 $\boldsymbol{A}\boldsymbol{e}=\boldsymbol{y}\bmod q$ 且 $\|\boldsymbol{e}\|\leqslant s\sqrt{m}$.

模拟过程如下：

1) $\mathcal{B}_1$ 运行算法 $OrthoSamp(q,\boldsymbol{A})$ 生成 $\boldsymbol{B}\in\mathbb{Z}_q^{n\times m}$ 和 $\Lambda_q^{\perp}(\boldsymbol{B})$ 的陷门基 $\boldsymbol{T_B}\in\mathbb{Z}_q^{m\times m}$，$\boldsymbol{BA}^{\mathrm{T}}=\boldsymbol{0} \bmod q$；令仲裁者公私钥对 $(APK,ASK)=(\boldsymbol{B},\boldsymbol{T_B})$，并将 $\boldsymbol{A},\boldsymbol{B}$ 和 $\boldsymbol{T_B}$ 发送给 $\mathcal{A}_1$，$\mathcal{B}_1$ 随机选取 $i^*\in\{1,2,\cdots,q_{H_2}\}$. $\mathcal{B}_1$ 维护 2 个列表 l_1 和 l_2 分别存储对 H_1 和 H_2 询问的应答.

2) 虽然 $\mathcal{B}_1$ 没有对应于格 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基，但是 $\mathcal{B}_1$ 仍可以正确回答 $\mathcal{A}_1$ 的询问，具体过程如下.

① $H_1(M\|\boldsymbol{r}\|)$ 询问. $\mathcal{B}_1$ 首先检查列表 l_1 中是否存在对该询问的应答，若存在，直接返回；否则，$\mathcal{B}_1$ 随机选取矩阵 $\boldsymbol{R}\in D_{m\times m}$ 并将 $(M,\boldsymbol{r},\boldsymbol{R})$ 存储在列表 l_1 中，然后将 $\boldsymbol{R}$ 返回给 $\mathcal{A}_1$.

② $H_2(M\|\boldsymbol{r}\|\boldsymbol{v})$ 询问. $\mathcal{B}_1$ 首先进行 $H_1(M\|\boldsymbol{r})$ 询问并获得矩阵 $\boldsymbol{R}$. 如果此次询问恰好是第 i^* 次询问，$\mathcal{B}_1$ 计算 $\boldsymbol{h}_2=\boldsymbol{AR}^{\mathrm{T}}\boldsymbol{v}+\boldsymbol{y} \bmod q$，并将 $(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{h}_2,\perp)$ 存储在列表 l_2 中，然后将 $\boldsymbol{h}_2$ 返回给 $\mathcal{A}_1$；如果不是第 i^* 询问，$\mathcal{B}_1$ 计算 $\boldsymbol{h}_2=\boldsymbol{A}(\boldsymbol{R}^{\mathrm{T}}\boldsymbol{v}+\boldsymbol{e}) \bmod q$，其中 $\boldsymbol{e}\in D_{\boldsymbol{Z}^m,s}$，并将 $(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{h}_2,\boldsymbol{e})$ 存储在列表 l_2 中，然后将 $\boldsymbol{h}_2$ 返回给 $\mathcal{A}_1$.

③ 可验证加密签名询问. 不失一般性，假设 $\mathcal{A}_1$ 在进行可验证加密签名询问之前已进行过 H_1 和 H_2 询问. $\mathcal{B}_1$ 在列表 l_2 中找到 $(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{h}_2,\boldsymbol{e})$，如果 $\boldsymbol{e}=\perp$，则 $\mathcal{B}_1$ 直接放弃模拟，否则，返回 $\boldsymbol{e}$ 作为签名应答.

3) 最终，$\mathcal{A}_1$ 输出一个伪造的可验证加密签名 $\omega^*=(M^*,\boldsymbol{r}^*,\boldsymbol{v}^*,\pi^*,\boldsymbol{e}^*)$. 不失一般性，假设 $\mathcal{A}_1$ 在输出伪造的可验证加密签名之前已经进行过 H_1 和 H_2 询问. $\mathcal{B}_1$ 在列表 l_2 中找到 $(M^*,\boldsymbol{r}^*,\boldsymbol{v}^*,\boldsymbol{h},\boldsymbol{e})$，如果 $\boldsymbol{e}\neq\perp$，则 $\mathcal{B}_1$ 直接放弃，否则，$\mathcal{B}_1$ 直接返回 $\boldsymbol{e}^*$ 作为 ISIS 实例的应答.

由上可知，$\boldsymbol{A}(\boldsymbol{R}^{*\mathrm{T}}\boldsymbol{v}^*+\boldsymbol{e}^*) \bmod q=H_2(M^*\|\boldsymbol{r}^*\|\boldsymbol{v}^*)=\boldsymbol{AR}^{*\mathrm{T}}\boldsymbol{v}^*+\boldsymbol{y} \bmod q$，其中 $\boldsymbol{R}^*=H_1(M^*\|\boldsymbol{r}^*)$. 从而可得 $\boldsymbol{Ae}^*=\boldsymbol{y} \bmod q$，$\|\boldsymbol{e}^*\|\leqslant s\sqrt{m}$. 因而只要 $\mathcal{A}_1$ 成功攻破上述方案的强不可伪造性，算法 $\mathcal{B}_1$ 就可以以概率 $1/q_{H_2}$ 求解 ISIS 问题，从而我们易知算法 $\mathcal{B}_1$ 成功求解 ISIS 问题的概率为 ε_1/q_{H_2}. 证毕.

3.3.3 强不透明性

定理 2. 如果存在敌手 $\mathcal{A}_2$ 以不可忽略的优势 ε_2 攻破方案的强不透明性，则可构造算法 $\mathcal{B}_2$ 以概率 ε_2/q_{H_1} 求解 LWE 问题，其中 q_{H_1} 表示敌手可进行 H_1 询问的最大次数.

证明. 假设 $\mathcal{B}_2$ 获得了一组 LWE 问题实例 $(\boldsymbol{u}_i\in\mathbb{Z}_q^n,v_i=\boldsymbol{u}_i^{\mathrm{T}}\boldsymbol{s}^*+x_i\in\mathbb{Z}_q)$，$i\in\{1,2,\cdots,m\}$，要求 $\mathcal{B}_2$ 通过模拟游戏利用 $\mathcal{A}_2$ 求解出向量 $\boldsymbol{s}^*\in\mathbb{Z}_q^n$.

模拟过程如下：

1) $\mathcal{B}_2$ 首先构造矩阵 $\boldsymbol{B}'\in\mathbb{Z}_q^{n\times m}$，其中第 i 列恰好是向量 $\boldsymbol{u}_i$；构造向量 $\boldsymbol{v}'\in\mathbb{Z}_q^m$，其中第 i 个分量元素恰好是 v_i；$\mathcal{B}_2$ 选取随机矩阵 $\boldsymbol{R}'\in D_{m\times m}$，然后运行算法 $OrthoSamp(q,\boldsymbol{B}'\boldsymbol{R}')$ 生成随机矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 和 $\Lambda_q^{\perp}(\boldsymbol{A})$ 的陷门基 $\boldsymbol{T_A}\in\mathbb{Z}_q^{m\times m}$，$\boldsymbol{B}'\boldsymbol{R}'\boldsymbol{A}^{\mathrm{T}}=\boldsymbol{0} \bmod q$；令仲裁者公钥 $APK=\boldsymbol{B}'\boldsymbol{R}'$，签名者公私钥对 $(PK,SK)=(\boldsymbol{A},\boldsymbol{T_A})$，并将 APK,PK 发送给敌手 $\mathcal{A}_2$，同时 $\mathcal{B}_2$ 随机选取 $i^*\in\{1,2,\cdots,q_{H_1}\}$. $\mathcal{B}$ 维护 3 个列表 l_1,l_2,l_3 分别存储对 H_1 询问、H_2 询问和可验证加密签名询问的应答.

2) 虽然 $\mathcal{B}_2$ 没有对应于格 $\Lambda_q^{\perp}(\boldsymbol{B}'\boldsymbol{R}')$ 的陷门基，但是 $\mathcal{B}_2$ 仍可以正确回答敌手 $\mathcal{A}_2$ 的询问，具体过程如下.

① $H_1(M\|\boldsymbol{r}\|)$ 询问. 如果此次询问恰好是第 i^* 次询问，$\mathcal{B}_2$ 将 $(M,\boldsymbol{r},\perp,\boldsymbol{R}')$ 存储在列表 l_1 中并将 $\boldsymbol{R}'$ 返回给 $\mathcal{A}_2$；如果此次询问不是第 i^* 次询问，$\mathcal{B}_2$ 运行算法 $SampRwith(\boldsymbol{B})$ 生成可逆矩阵 $\boldsymbol{R}\in\mathbb{Z}_q^{m\times m}$，$\boldsymbol{BR}^{-1}\in\mathbb{Z}_q^{n\times m}$ 和 $\boldsymbol{T}_{\boldsymbol{BR}^{-1}}\in\mathbb{Z}_q^{m\times m}$，$\mathcal{B}_2$ 将 $(M,\boldsymbol{r},\boldsymbol{T}_{\boldsymbol{BR}^{-1}},\boldsymbol{R})$ 存储在列表 l_1 中并将 $\boldsymbol{R}$ 返回给 $\mathcal{A}_2$.

② $H_2(M\|\boldsymbol{r}\|\boldsymbol{v})$ 询问. $\mathcal{B}_2$ 首先检查列表 l_2 中是否存在对该询问的应答，若存在，直接返回；否则，$\mathcal{B}_2$ 随机选取向量 $\boldsymbol{h}_2\in\mathbb{Z}_q^n$ 并将 $(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{h}_2)$ 存储在列表 l_2 中，然后将 $\boldsymbol{h}_2$ 返回给 $\mathcal{A}_2$.

③ 可验证加密签名询问. 不失一般性，假设敌手 $\mathcal{A}_2$ 在进行可验证加密签名询问之前已经进行过 H_1 和 H_2 询问. $\mathcal{B}_2$ 在列表 l_1 中找到 $(M,\boldsymbol{r},\boldsymbol{T}_{\boldsymbol{BR}^{-1}},\boldsymbol{R})$，如果 $\boldsymbol{T}_{\boldsymbol{BR}^{-1}}\neq\perp$，则 $\mathcal{B}_2$ 按照算法步骤进行可验证加密签名生成，否则，令 $\boldsymbol{v}=\boldsymbol{v}'$，$\mathcal{B}_2$ 利用陷门基 $\boldsymbol{T_A}$ 运行算法 $SampPre(\boldsymbol{A},\boldsymbol{T_A},H_2(M\|\boldsymbol{r}\|\boldsymbol{v})-\boldsymbol{AR}'^{\mathrm{T}}\boldsymbol{x},s_2)$ 生成向量 $\boldsymbol{e}$，并构造对 $\boldsymbol{v}$ 的一个有效非交互零知识证明 π. $\mathcal{B}_2$ 将 $(M,\boldsymbol{r},\boldsymbol{v},\pi,\boldsymbol{e})$ 存储在列表 l_3 中，返回 $\boldsymbol{e}$ 作为签名应答.

④ 仲裁询问. 不失一般性，假设 $\mathcal{A}_2$ 在进行仲裁询问之前已经进行过 H_1 询问，当收到 $\mathcal{A}_2$ 对可验证加密签名 $\omega=(M,\boldsymbol{r},\boldsymbol{v},\pi,\boldsymbol{e})$ 的仲裁询问，$\mathcal{B}_2$ 在列表 l_1 中找到 $(M,\boldsymbol{r},\boldsymbol{T}_{\boldsymbol{BR}^{-1}},\boldsymbol{R})$，如果 $\boldsymbol{T}_{\boldsymbol{BR}^{-1}}=\perp$，则 $\mathcal{B}_2$ 直接放弃；否则，$\mathcal{B}_2$ 利用 $\boldsymbol{T}_{\boldsymbol{BR}^{-1}}$ 对 $\boldsymbol{v}=(\boldsymbol{BR}^{-1})^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x} \bmod q$ 进行求解得 $\boldsymbol{x}$，并返回普通签名 $\sigma=(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{d}=\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x})$ 给 $\mathcal{A}_2$，其中 $\boldsymbol{R}=H_1(M\|\boldsymbol{r}\|)$.

3) 最终,敌手 $\mathcal{A}_2$ 输出一个有效的普通数字签名 $\sigma^*=(M^*,\boldsymbol{r}^*,\boldsymbol{v}^*,\boldsymbol{d}^*)$. 在这里,假设 σ^* 是 $\mathcal{A}_2$ 从可验证加密签名询问结果中提取出来的. 不失一般性,假设敌手 $\mathcal{A}_2$ 在输出伪造的可验证加密签名之前已经进行过 H_1 询问、H_2 询问和可验证加密签名询问. $\mathcal{B}_2$ 首先在列表 l_1 中找到$(M^*,\boldsymbol{r}^*,\boldsymbol{T}_{\boldsymbol{BR}^{-1}},\boldsymbol{R})$,在列表 l_3 中找到$(M^*,\boldsymbol{r}^*,\boldsymbol{v},\pi,\boldsymbol{e})$;如果 $\boldsymbol{T}_{\boldsymbol{BR}^{-1}}\neq\perp$,则 $\mathcal{B}_2$ 直接放弃,否则,我们易知 $\boldsymbol{v}=\boldsymbol{v}'$,$\boldsymbol{R}=\boldsymbol{R}'$,$\mathcal{B}_2$ 利用 $\boldsymbol{R}$ 和 $\boldsymbol{e}$ 可以由向量 $\boldsymbol{d}^*=\boldsymbol{e}+\boldsymbol{R}'^{\mathrm{T}}\boldsymbol{x}$ 求得 $\boldsymbol{x}$,从而可以由 $\boldsymbol{v}'=\boldsymbol{B}'^{\mathrm{T}}\boldsymbol{s}^*+\boldsymbol{x} \bmod q$ 求解出 $\boldsymbol{s}^*$.

因而只要 $\mathcal{A}_2$ 成功攻破上述方案的强不透明性,算法 $\mathcal{B}_2$ 就可以有效求解 LWE 问题,从而我们易知算法 $\mathcal{B}_2$ 成功求解 LWE 问题的概率为 ε_2/q_{H_1}.

证毕.

3.3.4 可提取性

定理 3. 上述可验证加密签名方案满足可提取性.

证明. 对于消息 M 的 VES $\omega=(M,\boldsymbol{r},\boldsymbol{v},\pi,\boldsymbol{e})$,我们证明如果该签名是有效的,那么总可以由 ω 提取出一个普通签名 $\sigma=(M,\boldsymbol{r},\boldsymbol{v},\boldsymbol{d}=\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x})$. 非交互零知识证明 π 可以有效确保 $\boldsymbol{v}=(\boldsymbol{BR}^{-1})^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{x} \bmod q$ 中的 $\boldsymbol{x}$ 是一个短向量. 由仲裁过程可知,可以以极大概率从 $\boldsymbol{v}$ 中提取出 $\boldsymbol{x}$,从而可以构造出短向量 $\boldsymbol{d}=\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}$.

由可验证加密签名验证过程可知,

$$H_2(M\|\boldsymbol{r}\|\boldsymbol{v})=\boldsymbol{A}(\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{v})=$$
$$\boldsymbol{A}[\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}(\boldsymbol{BR}^{-1})^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}]=$$
$$\boldsymbol{A}[\boldsymbol{e}+\boldsymbol{B}^{\mathrm{T}}\boldsymbol{s}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}]=\boldsymbol{A}(\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x}).$$

因而只要可验证加密签名 ω 是有效的,那么 $\boldsymbol{v}$ 中肯定含有短向量 $\boldsymbol{x}$,使得

$$\boldsymbol{A}(\boldsymbol{e}+\boldsymbol{R}^{\mathrm{T}}\boldsymbol{x})=H_2(M\|\boldsymbol{r}\|\boldsymbol{v}).$$

证毕.

3.4 效率比较

表 1 给出了该文方案与已有的基于格的可验证加密签名方案的比较结果. 文献[13]的方案仅满足存在性不可伪造性,文献[14]的方案虽满足强不可伪造性(strong unfrogeability),但签名者的公私钥和可验证加密签名尺寸都明显较大. 该文方案虽然要求签名者公私钥对需根据仲裁者公钥生成,但是其构造简单,不仅满足强不可伪造性和强不透明性,而且签名者公私钥和可验证加密签名更短,效率更高,实用性更强.

Table 1 Efficiency Comparison of Schemes

表 1 方案的效率对比

Scheme	‖PK‖	‖SK‖	‖VES‖	Strong Unforgeability
Ref[13]	$nm\,\mathrm{lb}\,q$	$m^2\,\mathrm{lb}\,q$	$(2m+n)\,\mathrm{lb}\,q+n+l$	No
Ref[14]	$2nm\,\mathrm{lb}\,q$	$2m^2\,\mathrm{lb}\,q$	$(2m+m^2)\,\mathrm{lb}\,q+n+l$	Yes
Ours	$nm\,\mathrm{lb}\,q$	$m^2\,\mathrm{lb}\,q$	$2m\,\mathrm{lb}\,q+n+l$	Yes

4 结束语

本文利用 Agrawal 等人提出的固定维数的格基委派技术,构造出一个新的格上可验证加密签名方案. 在随机预言机模型下证明了方案的安全性是基于格上 ISIS 和 LWE 问题,保证了其在量子环境下的安全性. 与已有的基于格的可验证加密签名方案相比,该方案构造简单,公私钥和签名尺寸更短,效率更高.

参 考 文 献

[1] Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange [C] //Proc of the 4th ACM Conf on Information Security and Privacy. New York: ACM, 1997: 7-17

[2] Boneh D, Gentry C, Lynn B, et al.. Aggregate and verifiably encrypted signatures from bilinear maps [G] // LNCS 2656: Proc of Eurocrypt 2003. Berlin: Springer, 2003: 416-432

[3] Zhou Yousheng, Sun Yanbin, Qing Sihan, et al. An efficient id-based verifiably encrypted signature scheme [J]. Journal of Computer Research and Development, 2011, 48(8): 1350-1356 (in Chinese)
(周由胜,孙艳宾,卿斯汉,等. 一种高效的基于身份的可验证加密签名方案[J]. 计算机研究与发展, 2011, 48(8): 1350-1356)

[4] Shen Jian, Wang Jin, Zheng Yuhui, et al. A novel verifiably encrypted signature from weil pairing [C] //Proc of HumanCom and EMC 2013. Berlin: Springer, 2014: 603-607

[5] Calderon T, Meiklejohn S, Shacham H, et al. Rethinking verifiably encrypted signatures: A gap in functionality and potential solutions [G] //LNCS 8366: Proc of CT-RSA 2014. Berlin: Springer, 2014: 349-366

[6] Shim K A. On the security of verifiably encrypted signature schemes in a multi-user setting [J]. Annals of Telecommunications, 2014, 69(11): 585-591

[7] Nishimaki R, Xagawa K. Verifiably encrypted signatures with short keys based on the decisional linear problem and obfuscation for encrypted VES [J]. Designs, Codes and Cryptography, 2015, 77(1): 61-98

[8] Gentry C, Peikert C, Vaikuntanathan V. How to use a short basis: Trapdoors for hard lattice and new cryptographic constructions [C] //Proc of the 40th Annual Symp on Theory of Computing. New York: ACM, 2008: 197-206

[9] Alwen J, Peikert C. Generating shorter bases for hard random lattices [J]. Theory of Computing Systems, 2011, 48(3): 535-553

[10] Gordon S D, Katz J, Vaikuntanathan V. A group signature scheme from lattice assumptions [G] //LNCS 6477: Proc of Asiacrypt 2010, Berlin: Springer, 2010: 395-412

[11] Nguyen P Q, Zhang J, Zhang Z F. Simpler efficient group signatures from lattices [G] //LNCS 9020: Proc of PKC 2015. Berlin: Springer, 2015: 401-426

[12] Rückert M, Schneider M, Schröoder D. Generic constructions for verifiably encrypted signatures without random oracles or NIZKs [G] //LNCS 6123: Proc of ACNS 2010. Berlin: Springer, 2010: 22-25

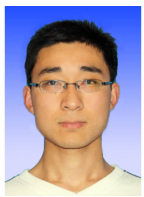
[13] Wang Fenghe, Hu Yupu, Wang Chunxiao. A verifiably encrypted signature scheme from lattice assumption [J]. Journal of Information and Computational Science, 2011, 8(8): 1431-1438

[14] Kim K S, Jeong I R. Efficient verifiably encrypted signatures from lattices [J]. International Journal of Information Security, 2014, 13(4): 305-314

[15] Agrawal S, Boneh D, Boyen X. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE [G] //LNCS 6223: Proc of Crypto 2010. Berlin: Springer, 2010: 98-115

[16] Regev O. On lattices, learning with errors, random linear codes, and cryptography [C] //Proc of the 37th Annual Symp on Theory of Computing. New York: ACM, 2005: 84-93

[17] Laguillaumie F, Langois A, Libert B, et al. Lattice-based group signature scheme with logarithmic signature size [G] //LNCS 6477: Proc of Asiacrypt 2013. Berlin: Springer, 2013: 41-61



Zhang Yanhua, born in 1989. PhD candidate in Xidian University. His research interests include public key cryptography based on lattice and provable security.

Hu Yupu, born in 1955. Professor and PhD supervisor. His main research interests include multilinear map, public key cryptography based on lattice, witness encryption and fully homomorphic encryption.