



格上可编程哈希函数的环签名方案

葛炳辉, 赵宗渠, 何 铮, 秦攀科

(河南理工大学 计算机科学与技术学院, 河南 焦作 454000)

摘 要: 针对传统格上环签名方案的签名和密钥长度过长的问题, 建立一种改进的格上可编程哈希函数环签名模型。利用 MP12 陷门函数生成签名密钥, 通过可编程哈希函数模拟随机预言机的部分可编程性质, 运用格上的分区证明方法, 将其应用于环签名方案的构造, 从而得到验证密钥和签名。分析结果表明, 与其他采用随机矩阵与 G 矩阵的格上环签名方案相比, 该方案所得签名、验证密钥和签名密钥长度更短, 在标准模型下满足自适应选择消息攻击的存在不可伪造性 (EUF-CMA) 安全要求。

关键词: 格; 可编程哈希函数; 环签名; MP12 陷门函数; 标准模型

开放科学(资源服务)标志码(OSID):



中文引用格式: 葛炳辉, 赵宗渠, 何铮, 等. 格上可编程哈希函数的环签名方案[J]. 计算机工程, 2020, 46(10): 131-136.

英文引用格式: GE Binghui, ZHAO Zongqu, HE Zheng, et al. Ring signature scheme of programmable Hash function on lattices[J]. Computer Engineering, 2020, 46(10): 131-136.

Ring Signature Scheme of Programmable Hash Function on Lattices

GE Binghui, ZHAO Zongqu, HE Zheng, QIN Panke

(College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, Henan 454000, China)

[Abstract] To address the problem that the length of signature and key is too long in traditional ring signature schemes on lattices, this paper proposes an improved ring signature model of Programmable Hash Function (PHF) on lattices. The MP12 trapdoor function is used to generate the signature key. The PHF is used to simulate part of the programmable properties of the random oracle machine. The partition proof method on lattices is used for the construction of the ring signature scheme to obtain the verification key and signature. Analysis results show that compared with other lattice-based ring signature schemes using random matrix and G matrix, the proposed scheme reduces the length of the signature, verification key and signature key, and can meet Existential Unforgeability against Adaptive Chosen Messages Attack (EUF-CMA) security requirements in the standard model.

[Key words] lattice; Programmable Hash Function (PHF); ring signature; MP12 trapdoor function; standard model

DOI: 10.19678/j.issn.1000-3428.0056114

0 概述

随着现代科技的发展, 电子签名技术已广泛应用于人们的日常生活。环签名作为电子签名中的一种, 常用于电子现金、匿名电子投票、匿名举报和区块链应用等。环签名由密码学家 RIVEST 等人^[1]于 2001 年提出, 其与群签名一样, 都为签名者提供匿名性签名方案。在环签名中, 没有管理者只有环成员, 环成员之间彼此独立, 无需相互合作。在签名过程中, 签名者首先选定

1 个临时签名者集合, 签名者也包含在该集合中, 然后签名者利用自己的私钥和集合成员的公钥就可单独对消息进行签名。任何 1 位环成员都能代表集合对消息进行签名, 且验证签名只需集合成员的公钥、消息和签名, 无需签名者的私钥, 从而确保环签名的匿名性。研究人员采用不同安全模型提出多种环签名方案, 其安全性主要基于大整数因子化^[1-3]、离散对数^[4-5]和双线性配对^[6-8]等数论假设。随着量子计算机技术的进步, 大整数因子化和离散对数等问题可用 Shor 量子算

基金项目: 国家自然科学基金(61802117); “十三五”国家密码发展基金(MMJ20170122); 河南省科技厅项目(182102310923); 河南理工大学博士基金(B2016-39)。

作者简介: 葛炳辉(1995—), 男, 硕士研究生, 主研方向为密码学、信息安全; 赵宗渠(通信作者), 讲师、博士; 何 铮, 硕士研究生; 秦攀科, 讲师、博士。

收稿日期: 2019-09-25

修回日期: 2019-11-14

E-mail: zhaozong-qu@hpu.edu.cn

法在概率多项式时间 (Probabilistic Polynomial Time, PPT) 内求解, 这给密码设置带来新的挑战, 上述环签名方案等传统安全保护方法在量子计算环境下已不再安全^[9]。

基于格的密码构造能抵抗量子攻击, 且格中主要为线性运算和模运算, 相较传统密码指数运算速度更快, 因此其有望成为后量子传统公钥替代者之一, 基于格的密码方案设计也成为学者们的研究热点^[10-11]。由于格中问题在一般情况和最坏情况下困难性相同, 因此格上任意实例的安全性都相同, 该特性吸引众多密码学家对基于格的环签名方案进行研究^[12-13]。2010 年, CASH 等人^[14] 提出首个基于格的环签名方案, 并采用格基派生技术为环成员产生公私钥, 但是该方案签名长度较长, 计算费时不利于实施。2011 年, WANG 等人^[15] 提出基于格的环签名新方案, 但该方案缺少标准模型下的安全性证明。2012 年, 田苗苗等人^[16] 利用 GPV 格点筛选算法^[11] 提出一种基于格的环签名高效方案, 但如果将该方案中验证矩阵的 $l+2$ 个公钥和环签名向量代入签名验证公式, 则敌手最多试 $(l+2)^2$ 次就可找到满足签名验证公式的公钥从而找到签名者, 因此该方案不具备匿名性。2018 年, 热娜等人^[17] 针对文献^[15] 方案中不满足不可伪造性的问题进行优化后, 提出基于格的环签名改进方案, 该方案在随机预言模型下证明满足环签名中的匿名性和不可伪造性, 并使用 MPI2 陷门函数^[10] 生成陷门。虽然该方案已证明具有安全性, 但是在随机预言模型下证明安全的方案在实际应用中有可能不安全, 且该方案的签名密钥和签名长度较长。

2012 年, HOFHEINZ 等人^[18-19] 提出可编程哈希函数 (Programmable Hash Function, PHF), 该函数是一种可模拟随机预言机某些可编程性质的特殊哈希函数^[20], 并利用可编程哈希函数分别构造了基于双线性映射和基于 RSA 算法的签名方案, 这 2 种方案具有更短的签名长度, 且从理论上更容易证明其安全性。传统可编程哈希函数的定义与构造都存在特定于 DL 群之间的代数结构问题, 这也是几乎所有已知可编程哈希函数均由 DL 问题构造的原因。2016 年, ZHANG 等人^[21] 提出格上可编程哈希函数的概念, 利用格上可编程哈希函数重新构造了格上签名方案, 该方案继承了传统可编程哈希函数签名方案的优点, 改进了公钥过长的不足。虽然格和 DL 群之间代数结构差异较大, 传统可编程哈希函数定义看似不适合格, 且格上可编程哈希函数已超过传统可编程哈希函数的范围, 但由于格上可编程哈希函数继承了传统可编程哈希函数的概念, 并运用格上分区证明技巧^[21], 因此仍将其归类于可编程哈希函数。

文献^[21] 指出在非齐次小整数解 (Inhomogeneous Small Integer Solution, ISIS) 假设下, 任何基于格上的

可编程哈希函数均抗碰撞, 因此可直接应用于环签名方案。为缩短格上环签名方案的签名和密钥长度, 本文提出一种基于格上可编程哈希函数的环签名新方案, 利用可编程哈希函数的特殊性质和 MPI2 陷门函数生成陷门, 将可编程哈希函数嵌入环签名的构造中, 并对本文方案在标准模型下自适应选择消息攻击的存在不可伪造性 (Existential Unforgeability against Adaptive Chosen Messages Attack, EUF-CMA) 安全进行分析。

1 预备知识

1.1 格

格是由线性无关向量构成的整系数组合。假设向量 b_1, b_2, \dots, b_n 属于 \mathbb{R}^m 且线性无关, 则向量 b_1, b_2, \dots, b_n 是格的 1 组格基, 记作 $B = [b_1, b_2, \dots, b_n] \in \mathbb{R}^{m \times n}$, 该格表示为:

$$\mathcal{L}(b_1, b_2, \dots, b_n) = \left\{ \sum_{i=1}^n x_i b_i \mid x_i \in \mathbb{Z}, 1 \leq i \leq n \right\} \quad (1)$$

其中: 若 $m = n$, 则称格 $\mathcal{L}(b_1, b_2, \dots, b_n)$ 是满维的; 若 A 是 $n \times m$ 矩阵, 其列向量为 b_1, b_2, \dots, b_m , 则格由格基 B 生成, 表示为:

$$\mathcal{L}(B) = \mathcal{L}(b_1, b_2, \dots, b_m) = \{Bx \mid x \in \mathbb{Z}^m\} \quad (2)$$

1.2 格上的困难问题

本文基于格上的小整数解 (Small Integer Solution, SIS) 问题和非齐次小整数解问题这 2 种困难问题研究格上可编程哈希函数环签名方案的安全性。

定义 1 (SIS 问题) 若 q 为整数, $\beta(n)$ 为安全参数为 n 的函数, 则矩阵 $A \in \mathbb{Z}_q^{n \times m}$, 矩阵 A 中元素取自 \mathbb{Z}_q 的 $n \times m$ 矩阵中, $m = \text{poly}(n)$, $\text{SIS}_{q,\beta}$ 问题是找到非零向量 $v \in \mathbb{Z}^m$ 使得 $Av = 0 \pmod q$ 成立且满足 $\|v\| \leq \beta$ 。

定义 2 (ISIS 问题) 若 q 为整数, $\beta(n)$ 为安全参数为 n 的函数, 矩阵 $A \in \mathbb{Z}_q^{n \times m}$, $m = \text{poly}(n)$ 。向量 $y \in \mathbb{Z}_q^n$, $\text{ISIS}_{q,\beta}$ 问题是找到非零向量 $v \in \mathbb{Z}^m$ 使得 $Av = y \pmod q$ 成立且要满足 $\|v\| \leq \beta$ 。

1.3 格上可编程哈希函数

哈希函数 $\mathcal{H}: \mathcal{X} \rightarrow \mathbb{Z}_q^{n \times m}$ 为可编程哈希函数 ($u, v, \beta, \gamma, \delta$) - PHF, 如果存在 PPT 内的陷门密钥生成 H. TrapGen 算法和陷门计算 H. TrapEval 算法, 则给出均匀随机矩阵 $A \in \mathbb{Z}_q^{n \times m}$ 和公开的陷门矩阵 $B \in \mathbb{Z}_q^{n \times m}$, 其具有以下性质:

1) 句法。在 PPT 内算法 $(K', \text{td}) \leftarrow \text{H. TrapGen}(1^k, A, B)$ 输出密钥 K' 和陷门 td 。对于任意输入的 $X \in \mathcal{X}$, 由陷门算法 $(R_X, S_X) = \text{H. TrapEval}(\text{td}, K', X)$ 得到 $R_X \in \mathbb{Z}_q^{m \times m}$ 和 $S_X \in \mathbb{Z}_q^{n \times n}$, 则 $s_1(R_X) \leq \beta$ 和 $S_X \in I_n \cup \{0\}$ 在陷门 td 上且大概率生成密钥 K' 。

2) 正确性。对于 $(K', \text{td}) \leftarrow \text{H.TrapGen}(1^k, A, B)$, 所有 $X \in \mathcal{X}$ 及与其相关的 $(R_X, S_X) = \text{H.TrapEval}(\text{td}, K', X)$ 存在 $H_{K'}(X) = \text{H.Eval}(K', X) = AR_X + S_X B$ 。

3) 统计上更接近陷门密钥。对于全部密钥 $(K', \text{td}) \leftarrow \text{H.TrapGen}(1^k, A, B)$ 和 $K \leftarrow \text{H.Gen}(1^k)$, (A, K') 和 (A, K) 之间的统计距离最大为 γ 。

4) 分布均匀的隐藏矩阵。对于所有 $(K', \text{td}) \leftarrow \text{H.TrapGen}(1^k, A, B)$, 任意输入 $X_1, X_2, \dots, X_u, Y_1, Y_2, \dots, Y_v \in \mathcal{X}$ 对于任意 i, j 有 $X_i \neq Y_j$, 使得 $(R_{X_i}, S_{X_i}) = \text{H.TrapEval}(\text{td}, K', X_i)$ 和 $(R_{Y_j}, S_{Y_j}) = \text{H.TrapEval}(\text{td}, K', Y_j)$, 进而得到 $\Pr[S_{X_1} = S_{X_2} = \dots = S_{X_u} = 0 \wedge S_{Y_1}, S_{Y_2}, \dots, S_{Y_v} \in I_n] \geq \delta$, 其中概率超过与 K' 同时产生的陷门 td 。

若 γ 可忽略而 δ 不可忽略, 则称该哈希函数为 (u, v, β) -PHF; 若 u 为 k 中随机选取的多项式, 则称该哈希函数为 (poly, v, β) -PHF。

1.4 环签名

环签名方案由 KeyGen、Sign 和 Verify 3 个概率多项式时间算法组成^[3]。

1) KeyGen(1^n) 算法。输入系统安全参数 n , KeyGen 算法为每位环成员生成其签名密钥 sk_i 和验证密钥 vk_i 。

2) Sign($\text{sk}_i, \mathbb{R}, M$) 算法。输入环成员集合 \mathbb{R} 、消息 M 以及签名者的签名密钥 sk_i , Sign 算法得到的输出是环成员集合 \mathbb{R} 对消息 M 的签名 σ 。

3) Verify(\mathbb{R}, M, v) 算法。输入环成员集合 \mathbb{R} 、消息 M 以及签名 σ , 若验证满足签名条件, 则 Verify 算法输出为 1, 否则输出为 0。

1.5 环签名安全模型

若环签名方案满足匿名性和不可伪造性 2 个条件, 则该环签名方案为安全的签名方案。

1) 匿名性。假设 PPT 内敌手 A 以优势 $P_{\text{adv}} = P_{\text{suc}} - 1/2$ 赢得游戏, P_{suc} 为敌手 A 赢得此游戏的概率, 若得到的 P_{adv} 可忽略, 则该环签名方案满足匿名性。

(1) 输入系统安全参数 k , 挑战者 C 运用陷门生成 $\text{TrapGen}(1^n, 1^{\bar{m}}, q, I_n)$ 算法, 挑战者 C 将系统参数发送给敌手 A。

(2) 敌手 A 对签名进行询问, 挑战者 C 将所得签名结果返回给敌手 A, 挑战者 C 向敌手 A 提交消息 $M \in \{0, 1\}^n$ 、环成员集合 \mathbb{R} 和用户 i_0, i_1 的身份, 挑战者 C 随机选取 $b \in \{0, 1\}$, 最终敌手 A 得到签名 σ_b 。

(3) 敌手 A 输出身份猜测 b' 。

2) 不可伪造性。假设 PPT 内敌手 A 赢得游戏的概率 P_{suc} 可忽略, 则称该环签名方案在选择子环和适应性选择消息攻击下具有不可伪造性。

(1) 建立系统 (KeyGen(1^k))。输入系统安全参数 k , 挑战者 C 采用陷门生成算法 $\text{TrapGen}(1^n, 1^{\bar{m}},$

$q, I_n)$ 将公钥集合 $\mathbb{R} = \{\text{vk}_1, \text{vk}_2, \dots, \text{vk}_l\}$ 发送给敌手 A, 而将其私钥 sk_i 保密。

(2) 签名询问 (Sign Queries)。敌手 A 适应性选择子环 $\mathbb{R} = \{\text{vk}_1, \text{vk}_2, \dots, \text{vk}_l\}$ 和消息 $M \in \{0, 1\}^n$, 挑战者 C 运行 Sign 算法将结果 σ 返回给敌手 A。

(3) 伪造签名 (Forgery)。敌手 A 输出环签名 $(\mathbb{R}', M', \sigma')$, 若验证 $(\mathbb{R}', M', \sigma')$ 为有效且未在签名询问中被询问, 则敌手 A 赢得该游戏, 伪造成功。

2 方案描述

本文方案中系统参数的生成: $1, n, m', v, q \in \mathbb{Z}$, $\beta \in \mathbb{R}$ 为安全参数 $k = \lceil \lg q \rceil$ 中的多项式, 假设 $H = (\text{H.Gen}, \text{H.Eval})$ 为从 $\{0, 1\}^1$ 到 $\mathbb{Z}_q^{n \times m}$ 的任意 $(1, v, \beta)$ -PHF, 系统参数 $\bar{m} = O(n \lg n)$, $m = \bar{m} + m'$ 且 $s > \max(\beta, \sqrt{m}) \cdot \omega(\sqrt{\lg n}) \in \mathbb{R}$, 环签名方案 SIG = (KeyGen, Sign, Verify) 具体步骤如下:

1) KeyGen(1^k)。输入安全参数 k , 用 MP12 陷门生成算法^[10] 计算得到 $(A_i, T_i) \leftarrow \text{TrapGen}(1^n, 1^{\bar{m}}, q, I_n)$, 其中 $A_i \in \mathbb{Z}_q^{n \times \bar{m}}$, $T_i \in \mathbb{Z}_q^{(\bar{m} - nk) \times nk}$ 。随机选择 $A_0 \leftarrow \mathbb{Z}_q^{n \times nk}$ 和 $u \leftarrow \mathbb{Z}_q^n$, 计算 $K \leftarrow \text{H.Gen}(1^k)$, 最终得到 $(\text{vk}_i, \text{sk}_i) = ((A_i, A_0, u, K), T_i)$ 。

2) Sign(sk_i, K, M)。假设 $\mathbb{R} = \{\text{vk}_1, \text{vk}_2, \dots, \text{vk}_l\}$ 为环成员集合, 给出私钥 sk_i 和消息 $M \in \{0, 1\}^n$, 随机选择 $t \leftarrow \{0, 1\}^1$, 计算 $A_{\mathbb{R}, M, t} = (A_{\mathbb{R}} \parallel (A_0 + H(0 \parallel t)G) + H_K(M)) \in \mathbb{Z}_q^{n \times m}$ 以及 $H_K(M) = \text{H.Eval}(K, M) \in \mathbb{Z}_q^{n \times nk}$, 其中 $A_{\mathbb{R}} = [A_1 \parallel A_2 \parallel \dots \parallel A_l]$ 为环成员集合 \mathbb{R} 中有序串联的矩阵, 然后计算 $e \leftarrow \text{Sample}(T_i, A_{\mathbb{R}, M, t}, I_n, u, s)$, 最终得到签名 $\sigma = (e, t)$ 。

3) Verify(K, M, σ)。给出环成员集合 \mathbb{R} 、消息 M 和签名 $\sigma = (e, t)$, 计算 $A_{\mathbb{R}, M, t} = (A_{\mathbb{R}} \parallel (A_0 + H(0 \parallel t)G + H_K(M))) \in \mathbb{Z}_q^{n \times m}$, 其中 $H_K(M) = \text{H.Eval}(K, M) \in \mathbb{Z}_q^{n \times nk}$ 。如果满足 $\|e\| \leq s \cdot \sqrt{m}$ 和 $A_{\mathbb{R}, M, t}e = u$, 则输出为 1, 否则输出为 0。

T_i 为敌手 A 的 1 个 G 陷门, 其通过零行填充可扩展到 $A_{\mathbb{R}, M, t}$ 的 1 个 G 陷门, 且 $s_1(T_i) \leq \sqrt{m} \cdot \omega(\sqrt{\lg n})$ 。由于 $s = \tilde{O}(n^{2.5}) > s_1(T_i) \cdot \omega(\sqrt{\lg n})$, 向量 e 的输出通过 SampleD 得到, 而 SampleD 遵循满足 $A_{\mathbb{R}, M, t}e = u$ 的 $D_{\mathbb{Z}^m, s}$ 分布, 因此, $\|e\| \leq s \cdot \sqrt{m}$ 以极大概率成立, 说明本文环签名方案具有正确性。

3 安全性分析

3.1 匿名性分析

定理 1 本文格上可编程哈希函数的环签名方案满足完全匿名性。

证明 对本文方案匿名性的证明过程如下:

1) 假设存在 PPT 内的敌手 A 和挑战者 C, 挑战者 C 运用方案中的陷门生成 $\text{TrapGen}(1^n, 1^{\bar{m}}, q, I_n)$ 算法, 输出公开验证密钥 $\text{vk}_i = (A_i, A_0, u, K)$ 和签名私钥 $\text{sk}_i = T_i$, 挑战者 C 将系统参数发送给敌手 A。

2) 敌手 A 向挑战者 C 提出环成员集合 \mathbb{R} 和消息 $M \in \{0, 1\}^n$ 的签名询问, 挑战者 C 执行签名方案的签名步骤, 即执行 $\text{Sign}(\text{sk}_i, \mathbb{R}, M)$, 挑战者 C 将得到的签名结果返回给敌手 A。

3) 敌手 A 适应性选择询问用户 $i < l$ 的相应私钥, 挑战者 C 返回 B_i 。

4) 挑战者 C 向敌手 A 提交消息 $M \in \{0, 1\}^n$ 、环成员集合 \mathbb{R} 和用户 i_0, i_1 的身份, 挑战者 C 随机选取 $b \in \{0, 1\}$, 输入 i_b 对应的私钥 T_b , 并执行 $\text{Sample}(T_i, A_{\mathbb{R}, M, i}, I_n, u, s)$ 算法得到签名 σ_b 返回给敌手 A。

5) 敌手 A 输出身份猜测 b' 。

上述匿名性证明过程中用户 i_0, i_1 的签名分别为 σ_1, σ_2 , 由于 σ_1 和 σ_2 为从 $D_{A_u^\perp(A_{\mathbb{R}, M, i}, s)}$ 中利用高斯抽样算法得到, 具有相同分布且两者之间的统计距离可忽略不计, σ_1 和 σ_2 不可区分, 敌手 A 赢得该游戏的优势可忽略, 因此本文方案满足完全匿名性。

3.2 不可伪造性分析

对本文方案进行不可伪造性分析, 将系统参数设置为: $1, \bar{m}, n, q, v \in \mathbb{Z}$ 为安全参数 k 的多项式, 适应地选择 $1 = O(\text{lb } n)$ 和 $v = \omega(\text{lb } n)$, 如果存在概率多项式时间内的伪造者 F 以不可忽略的概率 ε 进行 $Q = \text{poly}(n)$ 次签名查询, 则会打破本文格上可编程哈希函数的环签名方案的 EUF-CMA 安全性。采用算法 B 解决上述 $\text{ISIS}_{q, \bar{m}, \beta}$ 问题, 其中概率至少为 $\varepsilon' \geq \frac{\varepsilon}{16 \cdot 2^{1/nv^2} - \text{negl}(k)} = \frac{\varepsilon}{Q \cdot \tilde{O}(n)}$ 。

证明 对本文方案不可伪造性的证明过程如下:

给出算法 B 的结构并模拟伪造者 F 的攻击环境, 有至少 $\frac{\varepsilon}{\tilde{O}(n^2)}$ 的概率解决 $\text{ISIS}_{q, \bar{m}, \beta}$ 问题。首先采用算法 B 随机选择向量 $t' \leftarrow_r \{0, 1\}^1$, 伪造者 F 输出带标签的伪造签名 $t^* = t'$, 然后模拟 EUF-CMA 游戏如下:

1) 密钥生成 (KeyGen)。给出 $\text{ISIS}_{q, \bar{m}, \beta}$ 问题的挑战实例 $(A_i, u) \in \mathbb{Z}_q^{n \times \bar{m}} \times \mathbb{Z}_q^n$, 计算环成员集合 \mathbb{R} 中有序串联的矩阵 $A_{\mathbb{R}} = [A_1 \parallel A_2 \parallel \cdots \parallel A_l]$, $(K', \text{td}) \leftarrow \text{H.TrapGen}(1^k, A_{\mathbb{R}}, G)$ 。采用算法 B 随机选取 $T_0 \leftarrow_r (D_{\mathbb{Z}_q^{\bar{m}}, \omega(\sqrt{\text{lb } n})})^{nk}$, 计算 $A_0 = A_{\mathbb{R}} T_0 - H(0 \parallel t')G$, 并输出 $\text{vk} = (A_i, A_0, u, K')$, 保密 (T_0, td) 。

2) 签名过程 (Signing)。给出消息 M , 通过算法 B 随机地选取标签 $t \leftarrow_r \{0, 1\}^1$, 如果 t 被用来回答超过 v 个消息的签名, 则算法 B 中止, 否则计算 $(T_M, S_M) = \text{H.TrapEval}(\text{td}, K', M)$, 得到 $A_{\mathbb{R}, M, t} = (A_{\mathbb{R}} \parallel (A_0 +$

$H(0 \parallel t)G) + H_K'(M)) = (A_{\mathbb{R}} \parallel A_{\mathbb{R}}(T_0 + T_M) + (H(0 \parallel t) - H(0 \parallel t') + S_M)G)$ 。由于 $S_M = bI_n = H(b \parallel 0)$, 其中 $b \in \{-1, 0, 1\}$, 因此存在 $\hat{S} = H(0 \parallel t) - H(0 \parallel t') + S_M = H(b \parallel (t - t'))$ 。算法 B 需区分以下情况:

(1) $t \neq t'$ 或者 $t = t' \wedge b \neq 0$ 。在该情况下, \hat{S} 可逆, $\hat{T} = T_0 + T_M$ 对于 $A_{\mathbb{R}, M, t}$ 是 1 个 G 陷门。由于 $s_1(T_0) \leq \sqrt{m} \cdot \omega(\sqrt{\text{lb } n})$ 且 $s_1(T_M) \leq \tilde{O}(n^{2.5})$, 因此 $s_1(\hat{T}) \leq \tilde{O}(n^{2.5})$, 计算 $e \leftarrow \text{SampleD}(\hat{T}, A_{\mathbb{R}, M, t}, \hat{S}, u, s)$, 最终得到签名 $\sigma = (e, t)$ 。若设置合适的 $s = \tilde{O}(n^{2.5}) \geq s_1(\hat{T}) \cdot \omega(\sqrt{\text{lb } n})$, 则算法 B 以不可忽略的概率生成消息 M 的有效签名。

(2) $t = t' \wedge b = 0$: 算法 B 停止。

3) 伪造 (Forge)。在进行最多 Q 次签名询问后, 伪造者 F 输出消息 $M^* \in \{0, 1\}^n$ 的伪造签名 $\sigma^* = (e^*, t^*)$, 从而有 $\|e^*\| \leq s\sqrt{m}$ 和 $A_{\mathbb{R}, M^*, t^*} e^* = u$, 其中 $A_{\mathbb{R}, M^*, t^*} = (A_{\mathbb{R}} \parallel (A_0 + H(0 \parallel t^*)G) + H_K(M^*)) \in \mathbb{Z}_q^{n \times m}$ 。通过算法 B 计算 $(T_{M^*}, S_{M^*}) = \text{H.TrapEval}(\text{td}, K', M^*)$, 如果 $t^* \neq t'$ 或者 $S_{M^*} \neq 0$, 则算法 B 中止模拟。此外, 存在 $A_{\mathbb{R}, M^*, t^*} = (A_{\mathbb{R}} \parallel A_{\mathbb{R}}(T_0 + T_{M^*})) = (A_{\mathbb{R}} \parallel A_{\mathbb{R}} \hat{T})$, 其中 $\hat{T} = T_0 + T_{M^*}$, 最终算法 B 输出 $\hat{e} = (I_m \parallel \hat{T})e^*$ 作为解决方案。

由 $\text{ISIS}_{q, \bar{m}, \beta}$ 问题的定义可知 (A_i, u) 均匀分布于 $\mathbb{Z}_q^{n \times \bar{m}} \times \mathbb{Z}_q^n$ 。由于 $T_0 \leftarrow_r (D_{\mathbb{Z}_q^{\bar{m}}, \omega(\sqrt{\text{lb } n})})^{nk}$, 因此得到 $A_0 \in \mathbb{Z}_q^{n \times nk}$ 在统计上接近 $\mathbb{Z}_q^{n \times nk}$ 。此外, 模拟密钥 K' 在统计上接近真实密钥 K , 因此, 模拟验证密钥 vk 的分布在统计上接近真实验证密钥。

假设全部消息 M_1, M_2, \dots, M_u 在回答签名查询时, 通过算法 B 使用相同标签 $t = t'$, 对于 $i \in \{1, 2, \dots, u\}$ 使得 $(T_{M_i}, S_{M_i}) = \text{H.TrapEval}(\text{td}, K', M_i)$, 给出 2 个条件: 1) 某些标签 t 用于回答超过 v 个消息的签名; 2) S_{M_i} 对于某些 $i \in \{1, 2, \dots, u\}$ 不可逆, 当 $S_{M^*} \neq 0$ 或者 $t^* \neq t$ 成立时, 模拟过程中止。

伪造者 F 最多进行 $Q = \text{poly}(n)$ 次签名询问, 选择 $1 = O(\text{lb } n)$ 得到 $\frac{Q}{2^1} \leq \frac{1}{2}$ 。对于每个签名消息, 算法 B 会随机选择标签 $t \leftarrow_r \{0, 1\}^1$, 且用任何标签 t 回答超过 v 个消息的签名概率小于 $Q^2 \cdot \left(\frac{Q}{2^1}\right)^v$, 设置的 $v = \omega(\text{lb } n)$ 可忽略不计, 且算法 B 用相同标签 $t = t'$ 回答 $u \geq v$ 消息的签名概率可忽略。在 $u \leq v$ 的条件下, 对于 $i \in \{1, 2, \dots, u\}$ 和 $S_{M^*} = 0, S_{M_i}$ 为可逆且概率至少为 $\delta = \frac{1}{16nv^2} - \text{negl}(k)$ 。 t' 为随机选择且隐藏于伪造者 F 中, $\Pr[t^* = t']$ 的概率至少为 $\frac{1}{2^1} - \text{negl}(k)$ 。因此, 若伪造者

F 能在真实游戏中以 ε 概率成功攻击本文方案的 EUF-CMA 安全,则伪造者 F 会以至少 $(\varepsilon - Q^2 \left(\frac{Q}{2^l}\right)^v) \cdot \delta \cdot$

$$\left(\frac{1}{2^l} - \text{negl}(k)\right) = \frac{\varepsilon}{2^l \cdot 16nv^2} - \text{negl}(k) = \frac{\varepsilon}{Q \cdot \tilde{O}(n)}$$

的概率在模拟游戏中输出伪造的 (M^*, e^*) 。

证明 $\hat{e} = (I_m \parallel \mathbb{R}) e^*$ 能有效解决 $\text{ISIS}_{q, \bar{m}, \bar{\beta}}$ 问题的例证 (A, u) 如下:通过签名方案中验证算法的条件得到 $A_{\mathbb{R}, M^*, I^*} e^* = u$ 和 $\|e^*\| \leq s \sqrt{m}$, 由于 $s_1(T_0) \leq \sqrt{m} \cdot \omega(\sqrt{\text{lb } n})$ 和 $s_1(T_{M^*}) \leq \beta = \tilde{O}(n^{2.5})$,

因此 $\|\hat{e}\| \leq \tilde{O}(n^{2.5}) \cdot s \sqrt{m} = \tilde{O}(n^{5.5}) = \bar{\beta}$, 证明完毕。

4 效率分析

本文利用格上可编程哈希函数的特殊性质设计出一种在标准模型下可证明安全性的环签名方案,并以验证密钥长度、签名密钥长度、签名长度以及基于格上的困难问题作为方案效率评价指标,将本文方案与文献[15-17]中格上同类型环签名方案进行对比,结果如表 1 所示。

表 1 4 种格上环签名方案评价指标比较结果
Table 1 Evaluation index comparison results of four ring signature schemes on lattices

方案	验证密钥长度	签名密钥长度	签名长度	困难问题
文献[15]方案	\hat{nm}	\hat{m}^2	$(l+1)\hat{m}+1$	SIS
文献[16]方案	\hat{nm}	\hat{m}^2	$(l+2)\hat{m}$	SIS
文献[17]方案	nm	$(m-\omega) \cdot \omega$	lm	SIS
本文方案	$n(\bar{m}+1) + (n^2+1)k$	$(\bar{m}-nk) \cdot nk$	$nk+1$	ISIS

在计算验证密钥长度、签名密钥长度和签名长度时,文献[15]方案和文献[16]方案采用随机矩阵陷门函数^[11],而本文方案和文献[17]方案采用 G 矩阵陷门函数^[10],该陷门函数在生成过程中不涉及代价较高的矩阵求逆操作,计算复杂度相当于 2 个随机矩阵的 1 次乘运算,陷门生成过程较简单。此外,由于陷门采用原像采样算法,该算法支持并行运算且输入项为小整数,对离散空间需求较低,因此本文方案的验证密钥长度、签名密钥长度、签名长度均小于文献[15]方案和文献[16]方案。此外,文献[15]方案和文献[16]方案的陷门参数 $\hat{m} \geq 5n \text{lb } q$,而本文方案由于安全参数 $k = \lceil \text{lb } q \rceil$ 取值很小, m' 为 k 中的整数且 $\bar{m} = O(n \text{lb } q)$,其中 $m = \bar{m} + m'$,对比发现本文方案的 m 小于文献[15]方案和文献[16]方案的 \hat{m} ,因此本文方案具有更短的验证密钥、签名密钥和签名。本文方案将可编程哈希函数应用到环签名的签名构造中,存在 $m \geq \omega \geq n$,因此本文方案的验证密钥比文献[17]方案更长,但其签名密钥长度和签名长度均短于文献[17]方案。对于方案安全性基于格上的困难问题,由表 1 可知,文献[15-17]方案的安全性取决于格上的 SIS 问题,而本文方案的安全性取决于 ISIS 问题,SIS 和 ISIS 问题的困难性分别基于格中最短矢量问题(SVP)和最近矢量问题(CVP),SVP 和 CVP 是非确定性多项式(Nondeterministic Polynomial, NP)难问题,且在 PPT 内为归约关系。由上述分析可知,本文方案的效率高于文献[15-17]方案。

5 结束语

格上可编程哈希函数能模拟随机预言机部分可编程性质,通过格上分区证明方式直接应用于签名构造和安全性验证。本文提出一种新的格上可编程哈希函数环签名方案,利用 MP12 陷门函数生成陷门,将可编程哈希函数应用到环签名构造中,进而形成验证密钥、签名密钥和签名。分析结果表明,该方案所得签名和密钥较其他格上环签名方案更短,且在标准模型下满足 EUF-CMA 安全要求。后续将研究如何在保持签名密钥和签名长度不变的情况下,缩短验证密钥长度并提高效率,同时考虑将本文方案推广到基于身份的环签名方案中,以得到更短的签名和密钥。

参考文献

- [1] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//Proceedings of the 7th International Conference on Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2001:21-28.
- [2] DODIS Y, KIAYIAS A, NICOLOSI A, et al. Anonymous identification in ad-hoc groups [C]//Proceedings of EUROCRYPT'04. Berlin, Germany: Springer, 2004: 609-626.
- [3] BENDER A, KATZ J, MORSELLI R. Ring signatures: stronger definitions, and constructions without random oracles[EB/OL]. [2019-08-10]. <https://www.iacr.org/cryptodb/data/paper.php?pubkey=12638>.
- [4] ABE M, OHKUBO M, SUZUKI K. L-out-of-n signatures from a variety of keys[C]//Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2002:65-73.

- [5] HERRANZ J, GERMAN S. Forking lemmas for ring signature schemes[J]. Journal of Management Studies, 2003, 2904(2): 266-279.
- [6] ZHANG F, SAFAVINAINI R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications [C]//Proceedings of PKC'04. Berlin, Germany: Springer, 2004: 277-290.
- [7] SHACHAM H, WATERS B. Efficient ring signatures without random oracles[J]. Public Key Cryptography, 2007, 3352(2): 166-180.
- [8] NGUYEN L. Accumulators from bilinear pairings and applications[C]//Proceedings of CT-RSA'05. Berlin, Germany: Springer, 2005: 275-292.
- [9] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303-332.
- [10] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: simpler, tighter, faster, smaller [C]//Proceedings of EUROCRYPT'12. Berlin, Germany: Springer, 2012: 700-718.
- [11] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions [C]//Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York, USA: ACM Press, 2008: 32-37.
- [12] LI Zichen, LIANG Lan, SUN Yafei. Digital certificate scheme based on lattice signature algorithm[J]. Journal of Cryptologic Research, 2018, 5(1): 13-20. (in Chinese)
李子臣, 梁斓, 孙亚飞. 一种基于格签名算法的数字证书方案[J]. 密码学报, 2018, 5(1): 13-20.
- [13] JIA Xiaoying, HE Debiao, XU Zhiyan, et al. An efficient identity-based ring signature scheme over a lattice[J]. Journal of Cryptologic Research, 2007, 4(4): 392-404. (in Chinese)
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.
- [14] CASH D, HOFHEINZ D, KILTZ E, et al. Bonsai trees, or how to delegate a lattice basis[C]//Proceedings of 2010 International Conference on Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2010: 62-68.
- [15] WANG Jin, SUN Bo. Ring signature schemes from lattice basis delegation [C]//Proceedings of the 13th Conference on Information and Communications Security. Berlin, Germany: Springer, 2011: 15-28.
- [16] TIAN Miaomiao, HUANG Liusheng, YANG Wei. Efficient lattice-based ring signature scheme[J]. Chinese Journal of Computers, 2012, 35(4): 712-718. (in Chinese)
田苗苗, 黄刘生, 杨威. 高效的基于格的环签名方案[J]. 计算机学报, 2012, 35(4): 712-718.
- [17] Rena Ehmet, ZHANG Juan, LI Wei, et al. An improvement of a ring signature scheme based on lattices[J]. Journal of Xiamen University (Natural Science Edition), 2018, 57(2): 238-242. (in Chinese)
热娜·艾合买提, 张娟, 李伟, 等. 一个基于格的环签名方案的改进[J]. 厦门大学学报(自然科学版), 2018, 57(2): 238-242.
- [18] HOFHEINZ D, KILTZ E. Programmable Hash functions and their applications[EB/OL]. [2019-08-10]. <https://link.springer.com/article/10.1007/s00145-011-9102-5>.
- [19] HOFHEINZ D, JAGER T, KILTZ E. Short signatures from weaker assumptions[C]//Proceedings of ASIACRYPT'11. Berlin, Germany: Springer, 2011: 647-666.
- [20] WANG Zhiwei. Short signature based on programmable Hash functions[J]. SCIENTIA SINICA Informationis, 2013, 43(3): 335-342. (in Chinese)
王志伟. 基于可编程 Hash 函数的短签名[J]. 中国科学(信息科学), 2013, 43(3): 335-342.
- [21] ZHANG Jiang, CHEN Yu, ZHANG Zhenfeng. Programmable Hash functions from lattices; short signatures and IBES with small key sizes[C]//Proceedings of CRYPTO'16. Berlin, Germany: Springer, 2016: 303-332.

编辑 宋 圆