

基于编码的数字签名综述

宋永成^{1,2}, 黄欣沂¹, 伍玮³, 陈海霞¹

(1. 福建师范大学计算机与网络空间安全学院福建省网络安全与密码技术重点实验室, 福建 福州 350117;

2. 密码科学技术国家重点实验室, 北京 100878;

3. 福建师范大学数学与统计学院, 福建 福州 350117)

摘要: 量子计算理论和实践的快速发展导致基于传统数论困难问题的密码安全性存在很大不确定性。编码困难问题是公认的 NP 完全问题, 求解复杂度呈指数级增长, 且目前未发现量子计算对基于编码密码算法的威胁。因此, 基于编码的密码算法有望抵抗量子算法攻击, 是抗量子密码的主流方向之一。设计安全高效的基于编码的数字签名一直是公开问题。多年来, 国内外学者使用经典方法和新方法构造基于编码的数字签名, 但现存的构造存在安全性弱或性能差的不足。对当前基于编码的数字签名进行了综述, 分析和评价了各类基于编码的数字签名, 并指出未来的研究方向。

关键词: 抗量子密码; 基于编码的密码学; 数字签名; 身份认证

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021079

Survey of code-based digital signatures

SONG Yongcheng^{1,2}, HUANG Xinyi¹, WU Wei³, CHEN Haixia¹

1. Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China

2. State Key Laboratory of Cryptology, Beijing 100878, China

3. School of Mathematics and Statistics, Fujian Normal University, Fuzhou 350117, China

Abstract: The rapid development of quantum computing theory and practice brings great uncertainty to the security of cryptography based on hard problems in number theory. Code-based hard problem is recognized as NP-complete problem, the complexity increases exponentially, and there is currently no threat of quantum computing to code-based cryptographic algorithm. Therefore, code-based algorithm can resist the quantum algorithm attack, which is one of the main directions of quantum-resistant cryptography. It is still an open

收稿日期: 2021-03-01; 修回日期: 2021-06-10

通信作者: 黄欣沂, xyhuang@fjnu.edu.cn

基金项目: 国家自然科学基金(62032005, 61822202, 61872087, 61841701, 61902070, 61872089, 61972094); 福建省科学技术厅科学基金(2020J02016); 国家密码技术重点实验室项目(MMKFKT202008)

Foundation Items: The National Natural Science Foundation of China (62032005, 61822202, 61872087, 61841701, 61902070, 61872089, 61972094), Science Foundation of Fujian Provincial Science and Technology Agency (2020J02016), State Key Laboratory of Cryptology Research Fund (MMKFKT202008)

论文引用格式: 宋永成, 黄欣沂, 伍玮, 等. 基于编码的数字签名综述[J]. 网络与信息安全学报, 2021, 7(4): 1-17.

SONG Y C, HUANG X Y, WU W, et al. Survey of code-based digital signatures[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 1-17.

problem to design secure and efficient code-based signatures. For many years, international researchers use classical and new methods to construct code-based signatures, but existing constructions are weak in security or poor in performance. Code-based signatures were comprehensively summarized and analyzed, and future research directions were indicated.

Keywords: quantum-resistant cryptography, code-based cryptography, digital signatures, identification

1 引言

RSA、ECDSA 等经典密码算法的安全性主要基于分解大整数、求解离散对数等传统困难问题。但随着量子计算理论和实践的快速发展,基于传统困难问题密码算法的安全性存在很大不确定性。例如,Shor 量子算法^[1]可以有效求解离散对数问题和分解大整数问题。Grover 量子算法^[2]可以加速(最多二次方)求解困难问题。因此,研究安全高效的抗量子密码算法成为学术界和工业界的共识。

目前,设计抗量子密码算法基于的困难问题主要包括基于编码的困难问题^[3]、基于格的困难问题^[4]、基于多变量的困难问题^[5]、基于 LPN (learning parity with noise) 的困难问题^[6]、基于哈希函数的困难问题^[7]、基于同源的困难问题^[8]。本文主要研究基于编码的困难问题,设计的抗量子密码算法简称基于编码的密码算法或基于编码的密码学。

1978 年,Mc-Eliece^[9]开创了基于编码密码学,提出首个基于编码的公钥加密算法。经过长期的

研究,基于编码的加密算法和密钥交换协议取得积极进展,如美国国家标准技术研究所(NIST, National Institute of Standards and Technology)抗量子密码算法标准征集的第二、三轮竞选算法中,基于编码困难问题的构造主要是公钥加密算法和密钥交换协议^[10-14]。但是,基于编码的数字签名(CBDS, code-based digital signature)算法的研究相对滞后。

自 1978 年基于编码的密码学被正式提出以来,国内外学者从不同角度探索构造 CBDS 算法的方法。至今,CBDS 算法主要包括 5 类:Xinmei 型 CBDS 算法^[15]、Stern 型 CBDS 算法^[16]、KKS 型 CBDS 算法^[17]、Hash-Sign 型 CBDS 算法^[18]、Lyubashevsky 型 CBDS 算法^[19]。但这些 CBDS 算法存在签名和公钥长、效率低、安全性弱等不足。现有 CBDS 算法及其研究现状如图 1 所示,带下划线的 CBDS 算法是安全的或一次签名算法。

本文对 CBDS 算法进行综述,分析和评价各类 CBDS 算法,并指出每一类的研究状态和未来可能的研究方向。

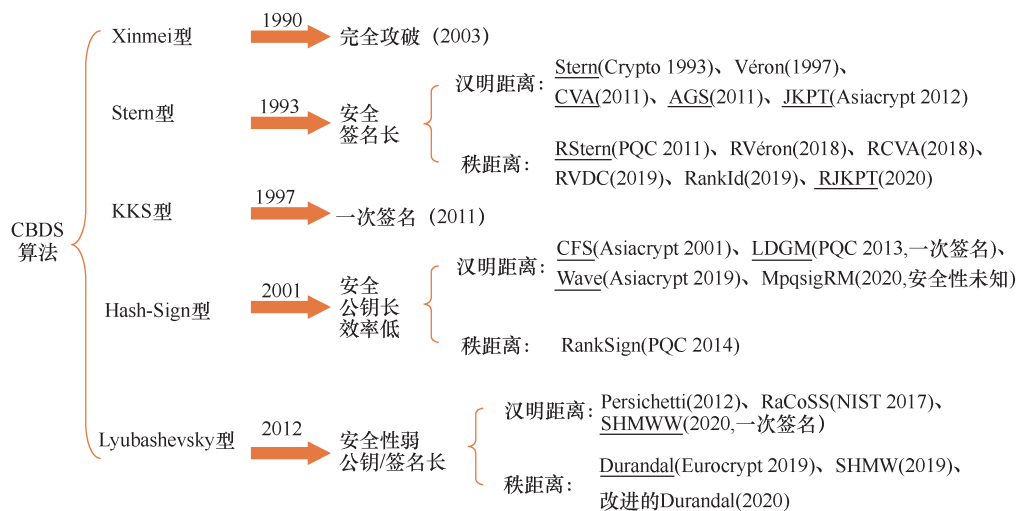


图 1 现有 CBDS 算法及其研究现状
Figure 1 Existing CBDS and its research status

2 基础知识

本节主要介绍数字签名算法、编码学（纠错码）基础、编码困难问题。

2.1 数字签名算法

Diffie 和 Hellman^[20]于 1976 年提出数字签名的概念。数字签名算法由如下 3 个多项式时间算法构成。

1) 密钥生成算法 $\text{KeyGen}(\lambda)$ ：该算法是概率多项式时间（PPT, probabilistic polynomial time）算法，它的输入为系统安全参数 λ ，输出为签名人的公钥/私钥(pk,sk)。

2) 签名生成算法 $\text{Sign}(M, \text{sk})$ ：该算法是 PPT 算法，它的输入为签名人的私钥 sk 和消息 M ，输出为消息 M 的签名 σ 。

3) 签名验证算法 $\text{Verify}(\text{pk}, (M, \sigma))$ ：该算法是确定多项式时间（DPT, deterministic polynomial time）算法，它的输入为签名人的公钥 pk 和消息/签名对 (M, σ) ，输出为一个比特 $b \in \{0, 1\}$ 。若 $b=1$ ，表明消息/签名对 (M, σ) 是有效的；若 $b=0$ ，表明消息/签名对 (M, σ) 是无效的。

数字签名算法的正确性要求：等式 $\text{Verify}(\text{pk}, (M, \text{Sign}(M, \text{sk}))) = 1$ 总是成立。这意味着，若签名人的公钥/私钥对(pk,sk)是由密钥生成算法 $\text{KeyGen}(\lambda)$ 正确生成的； M 的签名 σ 是由签名生成算法 $\text{Sign}(M, \text{sk})$ 正确生成的，那么消息/签名对 (M, σ) 一定使得验证算法 $\text{Verify}(\text{pk}, (M, \sigma)) = 1$ 的输出结果为 1。

数字签名算法的标准安全要求：在自适应选择消息攻击下满足存在不可伪造性（EUF-CMA, existential unforgeability under adaptive chosen message attacks）。对于 PPT 敌手，即使在获得他希望得到的有效消息/签名对后，其能为新消息计算有效签名的概率也是可忽略的。

2.2 编码学基础

本节给出汉明距离码和秩距离码、生成矩阵、校验矩阵的基本定义。

汉明距离码^[21]定义在 $\mathbb{F}_q$ 中。假设 $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ ， $\mathbf{x}$ 的汉明重量定义为 $\mathbf{x}$ 中非零元素的个数，记作 $\|\mathbf{x}\|_H \triangleq \#\{i \mid x_i \neq 0\}$ 。集合

$\{i \mid x_i \neq 0\}$ 被称为 $\mathbf{x}$ 的支集。假设 $\mathbf{x}' = (x'_1, x'_2, \dots, x'_n) \in \mathbb{F}_q^n$ ， $\mathbf{x}$ 与 $\mathbf{x}'$ 的汉明距离定义为向量 $\mathbf{x} - \mathbf{x}'$ 的汉明重量，即 $d_H(\mathbf{x} - \mathbf{x}') \triangleq \|\mathbf{x} - \mathbf{x}'\|_H$ 。

定义 1 汉明距离线性码。长度为 n 、维数为 k 的汉明距离线性码 $\mathcal{C}$ 是 $\mathbb{F}_q^n$ 的 k 维线性子空间，记作 $[n, k]_{\mathbb{F}_q}$ 。 $\mathcal{C}$ 的元素被称为码字， k/n 被称为码率。

汉明 GV 界^[22] (HGV) 是使 $\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i \geq q^{n-k}$ 成立的最小整数 d 。一般， $d_{\text{HGV}} \approx nH_q^{-1}(1-k/n) + o(n)$ ， $n \rightarrow \infty$ ，其中， $H_q(x) = -x \log_q x - (1-x) \log_q (1-x) + x \log_q (q-1)$ 是 q -进制熵函数。 $H_q^{-1}(\cdot)$ 是 $H_q(\cdot)$ 的反函数。

秩距离码^[23]定义在 $\mathbb{F}_{q^m}$ 中。假设 $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_{q^m}^n$ ($\mathbb{F}_{q^m}$ 可以视为 $\mathbb{F}_q$ 的 m 维空间)，且 $\boldsymbol{\beta} = (\beta_1, \beta_2, \dots, \beta_m) \in \mathbb{F}_{q^m}^m$ 是 $\mathbb{F}_{q^m}$ 的一组 $\mathbb{F}_q$ -基，那么在基 $\boldsymbol{\beta}$ 下，存在一个矩阵 $\mathbf{A}(\mathbf{x}) \in \mathbb{F}_q^{m \times n}$ ，使得 $\mathbf{x}$ 表示成 $\mathbf{x} = \boldsymbol{\beta} \mathbf{A}(\mathbf{x})$ 。 $\mathbf{x}$ 的秩重量定义为矩阵 $\mathbf{A}(\mathbf{x})$ 的秩，记作 $\|\mathbf{x}\|_R \triangleq \text{Rank}(\mathbf{A}(\mathbf{x}))$ 。

假设 $\mathbf{x}' = (x'_1, x'_2, \dots, x'_n) \in \mathbb{F}_{q^m}^n$ ， $\mathbf{x}$ 与 $\mathbf{x}'$ 的秩距离定义为向量 $\mathbf{x} - \mathbf{x}'$ 的秩重量，即 $d_R(\mathbf{x} - \mathbf{x}') \triangleq \|\mathbf{x} - \mathbf{x}'\|_R$ 。 $\mathbf{x}$ 的支集是由 $\mathbf{x}$ 的元素生成的 $\mathbb{F}_q$ -子空间，即 $E = \langle x_1, x_2, \dots, x_n \rangle_{\mathbb{F}_q}$ ，记作 $E = \text{Supp}(\mathbf{x})$ 。

定义 2 秩距离 $\mathbb{F}_{q^m}$ -线性码。长度为 n 、维数为 k 的秩距离 $\mathbb{F}_{q^m}$ -线性码 $\mathcal{C}$ 是 $\mathbb{F}_{q^m}^n$ 的 k 维线性子空间，记作 $[n, k]_{\mathbb{F}_{q^m}}$ 。 $\mathcal{C}$ 的元素被称为码字， k/n 被称为码率。

秩 GV 界^[23] (RGV) 是使 $V(q, m, n, r) \geq q^{(n-k)m}$ 成立的最小整数 r 。其中， $V(q, m, n, r)$ 是秩重量小于或等于 r 的码字个数，根据秩重量定义， $V(q, m, n, r) = \sum_{i=0}^r \prod_{j=0}^{i-1} \frac{(q^m - q^j)(q^n - q^j)}{q^i - q^j}$ 。一般，

$$d_{\text{RGV}}(m, n, k) \approx \frac{m+n-\sqrt{(m-n)^2+4km}}{2}。$$

根据线性空间的封闭性, 无论是汉明距离还是秩距离线性码, 最小距离等于所有码字的最小重量。

假设 $\mathcal{C}$ 是 $\mathbb{F}_q$ 上的 $[n, k]$ -线性码, 矩阵 $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ 是码 $\mathcal{C}$ 的生成矩阵当且仅当 $\mathcal{C} = \{\mathbf{m}\mathbf{G} \mid \mathbf{m} \in \mathbb{F}_q^k\}$; 矩阵 $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ 是码 $\mathcal{C}$ 的校验矩阵当且仅当 $\mathcal{C} = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{H}\mathbf{c} = \mathbf{0}\}$, 其中 $\mathbf{H}\mathbf{c}$ 称为 $\mathbf{c}$ 的校验子, 又称伴随式。

$\mathbf{G}$ (或 $\mathbf{H}$) 是系统形式的生成矩阵 (或校验矩阵), 当且仅当 $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{P}]$ (或 $\mathbf{H} = [\mathbf{I}_{n-k} \mid \mathbf{Q}]$)。

在编码密码学中, 通常使用准循环码^[24]和理想码^[13, 19]的系统生成矩阵和校验矩阵减少公钥的存储。

2.3 编码困难问题

编码困难问题^[25]是一类量子计算机无法有效求解的 NP 完全问题。因此, 基于编码困难问题设计抗量子密码算法是一个可靠的候选。本文涉及汉明距离码和秩距离码, 因此分别介绍在两种距离下编码困难问题。

问题 1 汉明校验子译码 (HSD, hamming syndrome decoding) 问题。假设 $\mathbf{H}$ 是随机 $[n, k]_{\mathbb{F}_q}$ -线性码的校验矩阵, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in \mathbb{N}^+$ 。给定 $(\mathbf{H}, \mathbf{s}, w)$, 要求计算出错误 $\mathbf{e} \in \mathbb{F}_q^n$, 使得 $\mathbf{H}\mathbf{e} = \mathbf{s}$ 且 $\|\mathbf{e}\|_H \leq w$ 。

问题 2 汉明一般译码 (HGD, hamming generic decoding) 问题。假设 $\mathbf{G}$ 是随机 $[n, k]_{\mathbb{F}_q}$ -线性码的生成矩阵, $\mathbf{y} \in \mathbb{F}_q^n$, $w \in \mathbb{N}^+$ 。给定 $(\mathbf{G}, \mathbf{y}, w)$, 要求计算出错误 $\mathbf{e} \in \mathbb{F}_q^n$ 和消息 $\mathbf{m} \in \mathbb{F}_q^k$, 使得 $\mathbf{y} = \mathbf{m}\mathbf{G} + \mathbf{e}$ 且 $\|\mathbf{e}\|_H \leq w$ 。

HSD 问题和 HGD 问题是等价的, 它们都是 NP 完全问题^[25]。1962 年, Prange^[26]首次使用信息集合译码 (ISD, information set decoding) 算法解 HGD 问题, 在此基础上大量 ISD 优化算法被提出, 如文献[27-30]的研究成果。

通过将 $\mathbb{F}_q$ 换成 $\mathbb{F}_{q^m}$ 并嵌入秩距离, 上述困难问题可以在秩距离下表达, 分别简称 RSD 问题、RGD 问题。RSD 问题可以归约到 HSD 问题。因此, 在秩距离下这些困难问题是可靠的。使

用秩距离码的最大优势是: 秩距离形式编码困难问题比汉明距离形式更可靠, 求解复杂度更高。1996 年, Chabaud 等^[31]首次研究解 RSD 问题的复杂度, 在此基础上国外学者提出大量解 RSD 问题算法, 如文献[32-36]的研究成果。

如果使用准循环矩阵或理想矩阵代替编码困难问题中 $\mathbf{H}$ 和 $\mathbf{G}$, 就称上述困难问题为准循环或理想形式的编码困难问题。至今, 没有求解该类型译码问题的高效方法。尽管存在一些求解准循环码形式译码问题的方法^[37-39], 但 these 方法仅仅是解一般形式的轻微加速, 约加速 $\mathcal{O}(\sqrt{n})$ 数量级, 其中 n 表示码长。文献[24]认为即使用系统准循环矩阵, 也不会对译码问题的复杂度造成很大影响。由于尚未存在解理想形式译码问题的方法, 所以目前解理想码形式译码问题的复杂度与解一般形式译码问题的复杂度是相当的。

问题 3 仿射秩校验子译码^[19] (ARSD, affine rank syndrome decoding) 问题。假设 $\mathbf{H}$ 是随机 $[n, k]_{\mathbb{F}_q}$ -线性码的校验矩阵, $\mathbf{H}'$ 是 $\mathbb{F}_{q^m}$ 中 $(n-k) \times n'$ 随机矩阵, $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$, F 是 $\mathbb{F}_{q^m}$ 的 r' 维子空间, $r \in \mathbb{N}^+$ 。给定 $(\mathbf{H}, \mathbf{H}', \mathbf{s}, r)$, 要求计算 $\mathbf{e} \in \mathbb{F}_{q^m}^n$ 和 $\mathbf{e}' \in \mathbb{F}_{q^m}^{n'}$, 使得 $\mathbf{H}\mathbf{e} + \mathbf{H}'\mathbf{e}' = \mathbf{s}$, $\|\mathbf{e}\|_R = r$ 且 $\text{Supp}(\mathbf{e}') \subseteq F$ 。

问题 4 秩支集学习^[23] (RSL, rank support learning) 问题。假设 $\mathbf{H}$ 是随机 $[n, k]_{\mathbb{F}_q}$ -线性码的校验矩阵, $\mathbf{H}\mathbf{e}_i$ ($i=1, 2, \dots, N$) 是 N 个校验子, 其中 $\mathbf{e}_i$ 拥有相同的 r 维支集 E , 即 $\mathbf{e}_i \in E^n$ 。给定 $(\mathbf{H}, \mathbf{H}\mathbf{e}_1, \dots, \mathbf{H}\mathbf{e}_N, r)$, 要求完全恢复 r 维支集 E 。

文献[23]表明解 RSL 问题的复杂度比解 RSD 问题的复杂度小。

问题 5 改进乘积空间子空间不可区分^[19] (PSSI⁺, advanced product spaces subspaces indistinguishability) 问题。假设 E 是固定 (敌手未知) 的 r 维 $\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$ -子空间。假设 F_i 、 W_i 分别是随机 d 、 w 维 $\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$ -子空间, 记为 $F_i \xleftarrow{\$} \text{Gr}(d, \mathbb{F}_{q^m})$ 、 $W_i \xleftarrow{\$} \text{Gr}(w, \mathbb{F}_{q^m})$ 。 EF_i 是子空间 E 和 F_i 的乘积空

间, $U_i \stackrel{s}{\leftarrow} \text{Gr}(dr - \lambda, EF_i)$ 且满足 $\{ef \mid \forall e \in E, \forall f \in F_i\} \cap U_i = \{0\}$, 即 U_i 不包含 ef 形式的非零元素。假设 H 是随机 $[n, k]_{\mathbb{F}_{q^m}}$ -线性码的校验矩阵, 则

① $e_i \stackrel{s}{\leftarrow} E^n$ 和 $e'_j \stackrel{s}{\leftarrow} E^n$, 即 e_i 和 e'_j 是长度为 n 且有相同支集 E 的向量, 其中 $i=1, 2, \dots, l$, $j=1, 2, \dots, l'$ 。 l 个 e_i 和 l' 个 e'_j 分别构成 $n \times l$ 矩阵 E 和 $n \times l'$ 矩阵 E' 。

② 计算 $S = HE$ 和 $S' = HE'$, PSSI⁺问题是给定 H 、 S 和 S' , 区分分布 $\{(z_i, F_i) \mid z_i \stackrel{s}{\leftarrow} \mathbb{F}_{q^m}^n, \text{Supp}(z_i) = W_i + U_i\}$ 和分布 $\{(z'_i, F_i) \mid z'_i \stackrel{s}{\leftarrow} \mathbb{F}_{q^m}^n, \|z'_i\|_R = dr - \lambda + w\}$ 。

问题 6 汉明支集学习^[40] (HSL, hamming support learning) 问题。假设 H 是随机 $[n, k]_{\mathbb{F}_q}$ -线性码的校验矩阵, 集合 $J \subset \{1, 2, \dots, n\}$ 。 $(He_1, \dots, He_N)$ 是 N 个校验子, 其中 $\text{Supp}(e_i) \subset J$ 。 给定 $(H, He_1, \dots, He_N)$, HSL(q, m, n, k, N) 问题要求完全恢复 J 。

3 基于编码的数字签名

本节分别分析和评价 5 类基于编码的数字签名 (CBDS) 算法: Xinmei 型 CBDS 算法^[15]、Stern 型 CBDS 算法^[16]、KKS 型 CBDS 算法^[17]、Hash-Sign 型 CBDS 算法^[18]、Lyubashevsky 型 CBDS 算法^[19]。

3.1 Xinmei 型 CBDS 算法

王新梅^[15]于 1990 年提出第一个 CBDS 算法, 简称 Xinmei 算法。1992 年, Alabbadi 和 Wicker^[41]对 Xinmei 算法提出有效的选择消息攻击, 简称 AW 攻击, 随后给出一种可以抵抗 AW 攻击的新算法, 简称 AW 算法^[42-43]。同时王新梅对 Xinmei 算法作出修正^[44], 该算法可以抵抗 AW 攻击。但是, 在 2001—2003 年, 文献^[45-48]分别对这一系列算法进行了分析总结, 找到了有效攻击方法, 表明 Xinmei 型的设计很难构造出安全有效的 CBDS 算法, 该类型 CBDS 算法的研究至此终止。

3.2 Stern 型 CBDS 算法

身份认证协议^[49]是允许一方向另一方证明

自己身份的交互式协议。Fiat-Shamir 变换^[50]可以把任何 (交互式) 身份认证协议转化成 (非交互式) 数字签名算法。因此, 采用 “身份认证协议 $\rightarrow$ Fiat-Shamir 变换 $\rightarrow$ 数字签名算法” 的研究思路, 设计基于编码身份认证 (CBID, code-based identification) 协议也是构造 CBDS 算法的途径。

1993 年, Stern^[16]首次提出安全的 CBID 协议, 简称 Stern 协议, 如图 2 所示。Stern 协议需运行三轮, 欺骗概率 (2/3) 不可忽略。本文称欺骗概率不可忽略的 CBID 协议为 Stern 型 CBID 协议或 Stern 型协议; 称使用 Fiat-Shamir 变换将 Stern 型 CBID 协议转化成的数字签名算法为 Stern 型 CBDS 算法。

Stern 协议的安全性依赖于解 HSD 问题的困难性, 它的目的是: 允许证明者向验证者证明他拥有 HSD 问题的解。证明者的私钥是一个重量为 t 的错误 $e \in \mathbb{F}_2^n$, 公开随机线性码的一个校验矩阵 $H \in \mathbb{F}_2^{(n-k) \times n}$ 和私钥对应的校验子 $s = He$ 。通过承诺、挑战、回应三轮交互, 验证者确定证明者拥有错误 e 。在图 2 中, $\mathcal{H}$ 是一个安全的哈希函数, S_n 是 n 阶对称群。

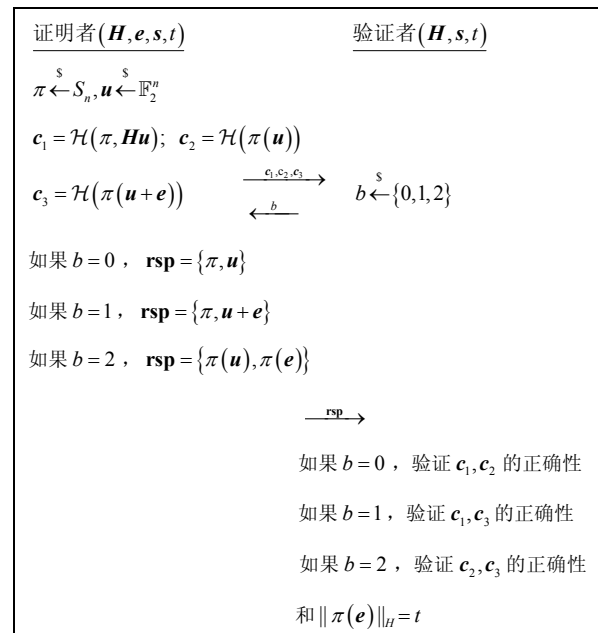


图 2 Stern 身份认证协议
Figure 2 Stern identification protocol

但是, Stern 协议的欺骗概率是 2/3, 即执行一次 Stern 协议, 不诚实证明者成功地欺骗验证

者的概率是 $2/3$ 。这意味着达到某个安全级别，必须重复执行协议多次，从而导致通信开销很大。例如，达到 128 bit 安全级别（解 HSD 问题复杂度 $\geq 2^{128}$ 且欺骗概率 $\leq 2^{-128}$ ），需运行协议 219 次（ $(2/3)^{219} \leq 2^{-128}$ ），此时通信开销（均指平均通信开销，下同）为 81 kB。如果使用 Fiat-Shamir 变换把 Stern 协议转化成签名算法，则签名长度等于通信开销。因此，Stern 型 CBDS 算法签名太大，实用性差。构造高效 Stern 型 CBDS 算法的难点是：减少 Stern 协议的通信开销（减小单次通信开销和欺骗概率）。

在减少单次通信开销方面，Véron^[51]于 1996 年提出一个欺骗概率 $2/3$ 三轮 CBID 协议，简称 Véron 协议，如图 3 所示。Véron 协议的安全性依赖于解 HGD 问题的困难性，它的目的是：允许证明者向验证者证明他拥有 HGD 问题的解。证明者的私钥是一个待编码消息 $m \in \mathbb{F}_2^k$ 和一个重量为 t 的错误 $e \in \mathbb{F}_2^n$ ，公开一个随机线性码的生成矩阵 $G \in \mathbb{F}_2^{k \times n}$ 和 $y = mG + e$ 。通过承诺、挑战、回应三轮交互，验证者确定证明者拥有 m 和 e 。Véron 协议的优势是单次通信开销比 Stern 协议更小。但文献[52]表明， G 是公开的， $\pi((u+m)G)$ 会泄露置换 π 的信息，从而 e 的信息被泄露，进而 Véron 协议不满足零知识性。同时 Jain 等^[52]提出一个基于 HGD 问题的身份认证协议，简称 JKPT 协议，如图 4 所示。 $\mathcal{C}_G$ 是由生成矩阵 G 决定的码。JKPT 协议和 Véron 协议类型相同，但 JKPT 协议比 Stern 协议的通信开销更大（128 bit 安全级别，为 109 kB）。

在减小欺骗概率方面，CVA 身份认证协议^[53]（简称 CVA 协议，如图 5 所示）和 AGS 身份认证协议^[54]（简称 AGS 协议，如图 6 所示）增大协议的轮数（5 轮），实现更小的欺骗概率（ $1/2$ ）。这使相同安全级别重复运行协议的次数更少，从而减小通信开销。例如，达到 128 bit 安全级别，需运行协议 128 次。CVA 协议的安全性依赖于解 q -进制 HSD 问题的困难性，它的目的是：允许证明者向验证者证明他拥有 q -进制 HSD 问题的解。对于 128 bit 安全级别，CVA 协议的通信开销为 60 kB。AGS 协议的安全性依赖于解 HGD 问题的困难性，它的目的是：允许证明者向验证

者证明他拥有 HGD 问题的解。对于 128 bit 安全级别，AGS 协议的通信开销为 45 kB。另外，AGS 协议仅仅适用于循环码（ $n=2k$ ），而循环结构容易受到攻击的影响^[37-39]。为避免这些攻击的影响，码的维数 k 应为素数，且满足 $(X^k - 1)/(X - 1)$ 是既约多项式。这样的 k 值是稀疏的，要增大协议的性能，通常选择更大的值。对于 Stern、JKPT、CVA 协议，如果使用循环结构减少公钥长度，则 k 应满足上述条件。

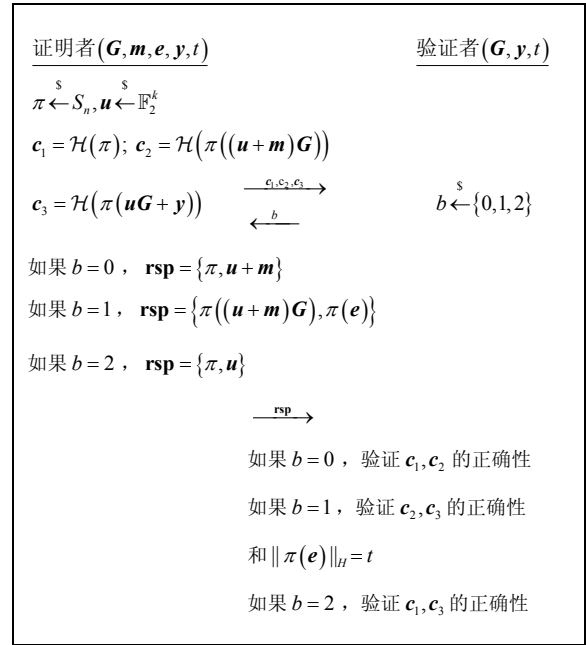


图 3 Véron 身份认证协议
Figure 3 Véron identification protocol

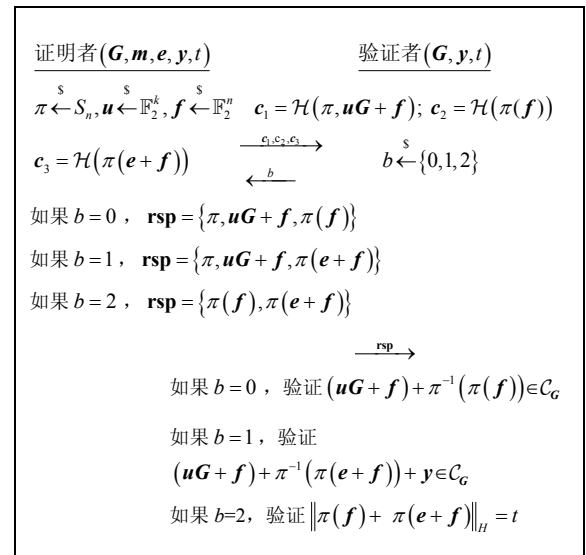


图 4 JKPT 身份认证协议
Figure 4 JKPT identification protocol

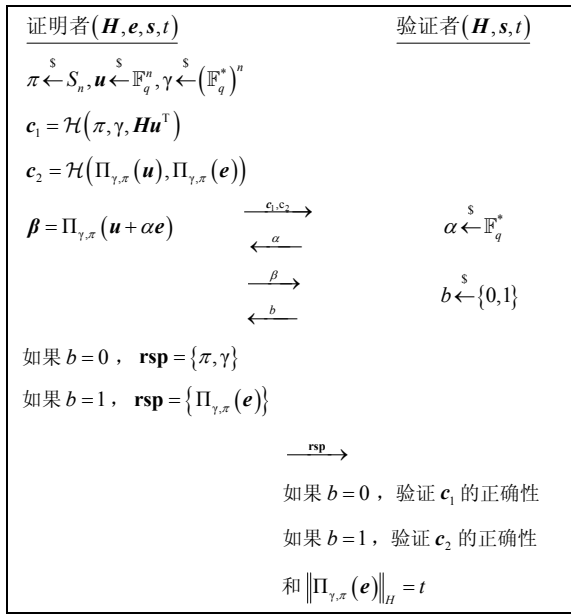


图 5 CVA 身份认证协议
Figure 5 CVA identification protocol

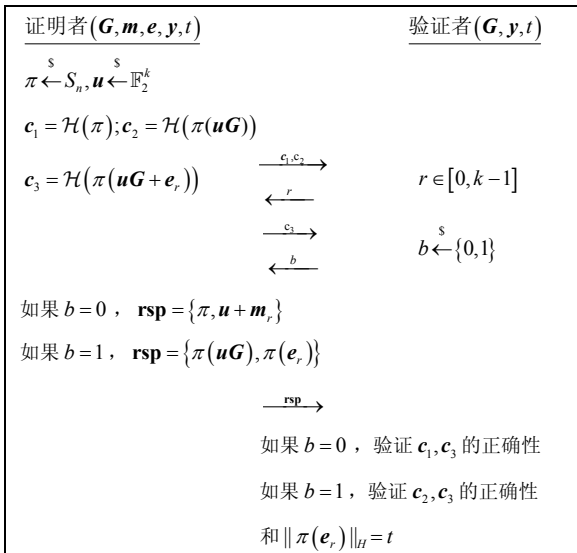


图 6 AGS 身份认证协议
Figure 6 AGS identification protocol

上述所有 CBID 协议 (Stern、CVA、AGS、JKPT) 都使用汉明距离码。构造编码密码算法的另一方向是使用秩距离码, 目前的研究表明: 解秩距离形式译码问题复杂度比汉明距离形式增长更快。尽管文献[44-45]提出两个解秩距离译码问题的新代数方法, 但这两个方法对满足 $m = \Theta(n)$, $k = \Theta(n)$, $t = \Theta(\sqrt{n}) \approx d_{\text{RGV}} / 3$ 的参数更加有效。对于全距离译码情况 ($t \approx d_{\text{RGV}}$, 码率 $\approx 1/2$), 与汉明距离译码问题相比, 秩距离译码问题可以以更小的安全参数, 实现标准的安全级别。由于 CBID 协议均依赖于全距离译码问题, 所以使用秩距离码可以进一步减小密钥长度和通信开销。

目前, 秩距离 CBID 协议都是 Stern、Véron、AGS、CVA、JKPT 协议的秩距离变体^[55-59]。但这些秩距离变体存在通信开销大、不满足完备性、不满足零知识性等, 具体如下。

① 尽管 Stern 和 JKPT 协议的秩距离变体^[55,59] (分别简称 RStern 和 RJKPT 协议) 是安全的 CBID 协议, 但它们的通信开销仍然很大 (128 bit 安全级别, 分别为 61 kB 和 79 kB)。

② 文献[60]表明 Véron 协议的秩距离变体^[56]不满足零知识性。CVA 协议的秩距离变体^[56]通信开销更大 (128 bit 安全级别, 为 3 MB)。

③ AGS 和 CVA 协议的秩距离变体^[56-58]不满足完备性。AGS 协议的两个秩距离变体^[57-58]使用秩距离循环码, 受叠码攻击^[61]的影响。为避免叠码攻击的影响, 需选择更大的安全参数实现标准的安全级别, 这会降低协议的性能。

表 1 统计了安全 CBID 协议的性能 (128 bit 安全级别)。该方向需要研究的问题是: ① 构造单次通信开销或欺骗概率更小的 Stern 型 CBID 协议; ② 在

表 1 安全 CBID 协议的性能 (128 bit 安全级别)
Table 1 The performance of secure CBID protocols (128-bit security level)

距离	协议	公钥长度/bit	执行一次通信开销/bit	欺骗概率	通信开销 (或签名长度) /kB
秩距离	RStern ^[55]	816	2 298	2/3	61
	RTKPT ^[59]	1 309	2 955	2/3	79
汉明距离	Stern ^[16]	1 100	3 044	2/3	81
	JKPT ^[52]	1 873	4 075	2/3	109
	AGS ^[54]	1 873	2 871	1/2	45
	CVA ^[53]	1 374	3 825	1/2	60

秩距离下, 构造安全高效的 Stern 型 CBID 协议。

3.3 KKS 型 CBDS 算法

1997 年, Kabatianskii 等^[17]基于 HSL 问题提出 KKS 签名算法 (算法 1)。KKS 算法的核心思想是: 把给定线性码的可译校验子构成一个集合, 用给定线性码的校验矩阵 (公钥) 和另一个随机码的生成矩阵 (私钥) 构造新公钥, 使得公钥和消息的乘积属于上述集合中的校验子, 该校验子对应的错误 (签名值) 是消息和生成矩阵的乘积。KKS 型 CBDS 算法不需要译码操作。

算法 1 KKS 签名算法

密钥生成 签名者进行下面步骤。

- ① 根据安全级别 λ , 选择安全参数 N, K, n, k, t_1, t_2 。
- ② 随机选择 $[N, K]$ -码的校验矩阵 $H \in \mathbb{F}_2^{(N-K) \times N}$ 。
- ③ 随机选择集合 $\{1, \dots, N\}$ 一个基数为 n 的子集 J ;
- ④ 随机选择 $[n, k]$ -线性码的生成矩阵 $G \in \mathbb{F}_2^{k \times n}$ (所决定的线性码记为 C_{hidden}), 使得码 C_{hidden} 的码字重量高概率地集中在 $[t_1, t_2]$ 内。
- ⑤ 计算 $F \triangleq H_J G^T$, 其中, H_J 表示以集合 J 为索引的列构成的矩阵。
- ⑥ 输出私钥 J 、 G 和公钥 F 、 H 。

签名生成 签名者生成消息 $m \in \mathbb{F}_2^N$ 的签名 $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_N) \in \mathbb{F}_2^N$ 定义如下:

- ① $\sigma_J = mG$;
- ② $\sigma_i = 0, i \notin J$

签名验证 签名接收者进行如下步骤验证消息/签名对 (m, σ) 的有效性:

- ① $t_1 \leq \|\sigma\|_H \leq t_2$;
- ② $H\sigma^T = Fm^T$ 。

2007 年, Cayrel 等^[62]分析了 KKS 签名算法的安全性, 结论表明, KKS 签名算法生成的签名会泄露私钥 J 的信息, 攻击者最多需要 20 个签名, 就能攻破 KKS 签名算法。因此, KKS 签名算法不能抵抗已知消息攻击, 只能用于一次签名。

Barreto 等^[63]提出了 KKS 签名算法的修正, 通过给 KKS 签名算法添加额外的哈希函数和错误向量, 构造 KKS 签名算法的变体 (算法 2)。

文献[63]在随机谰言模型下证明 KKS 签名算法变体是 EUF-ICMA 安全的, 这个算法和原始的 KKS 签名算法相似, 可以使用任何纠错码且安全性依赖于 HSL 问题。Otmani 等^[40]对 KKS 签名算法及其变体中的所有参数进行了攻击, 结论表明: 如果由校验矩阵 H 所决定线性码码率 (k/n) 小于或等于生成矩阵 G 所决定线性码码率的 2 倍 $(2k/n)$, 攻击更容易成功。即使攻击者不获得签名, 也能利用公开参数和 Stern 译码算法的变体^[64]恢复出私钥。如果攻击者能够获得消息签名对, 则能加速攻击成功时间。

算法 2 KKS 签名算法变体

密钥生成 签名者进行下面步骤。

- ① 根据安全级别 λ , 选择安全参数 N, K, n, k, t_1, t_2 。
- ② 选择安全哈希函数 $\mathcal{H}: \{0, 1\}^* \times \mathbb{F}_2^{N-K} \rightarrow \mathbb{F}_2^k$ 。
- ③ 随机选择 $[N, K]$ -随机线性码的校验矩阵 $H \in \mathbb{F}_2^{(N-K) \times N}$ 。
- ④ 随机选择集合 $\{1, \dots, N\}$ 一个基数为 n 的子集 J 。
- ⑤ 随机选择 $[n, k]$ -线性码的生成矩阵 $G \in \mathbb{F}_2^{k \times n}$ (所决定的线性码记为 C_{hidden}), 使得码 C_{hidden} 的码字重量高概率地集中在 $[t_1, t_2]$ 内。
- ⑥ 计算 $F \triangleq H_J G^T$, 其中, H_J 表示以集合 J 为索引的列构成的矩阵
- ⑦ 输出私钥 J 、 G 和公钥 F 、 H 。

签名生成 签名者生成消息 $M \in \{0, 1\}^*$ 的签名 (h, σ) 步骤如下。

- ① 随机选择一个重量为 n 的错误向量 $e \in \mathbb{F}_2^N$, 计算 $h \triangleq \mathcal{H}(M, He^T)$ 。
- ② 计算 $y = (y_1, y_2, \dots, y_N) \in \mathbb{F}_2^N$:
 - a. $y_J = hG$;
 - b. $i \notin J; y_i = 0$;
- ③ 计算 $\sigma \triangleq y + e$ 。

签名验证 签名接收者进行如下步骤验证消息/签名对 $(M, (h, \sigma))$ 的有效性。

- ① $\|\sigma\|_H \leq 2n$ 。
- ② $h = \mathcal{H}(M, H\sigma^T + Fh^T)$ 。

2012 年, Gaborit 和 Schrek^[64]提出 GS 一次签

名算法（算法3）。GS算法被视为是KKS签名算法的准循环形式变体，比KKS签名算法性能更好，能进一步限制现有攻击^[62,40]的影响。对于80 bit安全级别，安全参数选择为 $(\lambda, r, k, l, t, w) = (80, 3, 6299, 12, 263, 2714)$ ，公钥为18 kB，签名为2 kB。

算法3 GS签名算法

密钥生成 签名者进行下面步骤

- ① 根据安全级别 λ ，选择安全参数 r, k, l, t, w 。
- ② 选择安全的哈希函数 $\mathcal{H}: \{0, 1\}^* \rightarrow \mathbb{F}_2^{\log k}$ 。
- ③ 随机选择 $[rk, rk - k]$ -准循环线性码的系统校验矩阵 $\mathbf{H} \in \mathbb{F}_2^{k \times rk}$ 。
- ④ 随机选择 l 个重量为 t 、长度为 rk 的错误 $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_l$ 。
- ⑤ 计算 $\mathbf{s}_i \triangleq \mathbf{H} \mathbf{e}_i^T$ ， $i = 1, 2, \dots, l$ 。
- ⑥ 输出私钥 $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_l$ 、公钥 $\mathbf{H}$ 和 $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_l$ 。

签名生成 签名者生成消息 $\mathbf{M} \in \{0, 1\}^*$ 的签名 σ 的步骤如下。

- ① 随机选择一个正整数 $j \in [0, 2^k]$ ，计算哈希值 $\mathcal{H}(\mathbf{M}, j)$ ，并将其分成 l 组，每组对应 $[0, k-1]$ 的整数 i ，进而定义一个 i 位循环移位运算 π_i ， $i = 1, 2, \dots, l$ 。

- ② 计算 $\mathbf{e} = \sum_{i=1}^l \pi_i(\mathbf{e}_i)$ ，直到 $\|\mathbf{e}\|_H \leq w$ ，否则返回到第①步。

- ③ 签名 $\sigma \triangleq (\mathbf{e}, j)$ 。

签名验证 签名接收者进行如下步骤验证消息\签名对 $(\mathbf{M}, \sigma)$ 的有效性

- ① $\|\mathbf{e}\|_H \leq w$ ；
- ② 计算 $\mathcal{H}(\mathbf{M}, j)$ ，恢复 π_i ，验证 $\mathbf{H} \mathbf{e}^T = \pi_i(\mathbf{s}_i)$ 。

因此，KKS型CBDS算法的主要不足是安全性不高，被认为是一次签名算法。这一方向需要研究的问题是：在保持签名算法良好签名效率的前提下，减小公钥长度，寻求更安全的变体，突破一次签名的限制，实现标准数字签名的功能。

3.4 Hash-Sign型CBDS算法

基于编码困难问题设计 Hash-Sign型CBDS

算法的主要困难在于：相对整个字空间，可译校验子的数量很少。具体地说，给定 $\mathbb{F}_q$ 上 $[n, k, t]$ -线性纠错码，该码最多可纠正 t 位错误（ $t \leq d_{\text{HGV}}/2$ ），但 $\sum_{i=0}^t \binom{n}{i} (q-1)^i \ll 2^{n-k}$ ，即错误

空间的基数与校验子空间的基数差距很大。这表明错误空间与校验子空间无法实现一一对应，而且很难通过有效方法找到可译的校验子。

2001年，Courtois等^[18]提出第一个Hash-Sign型CBDS算法，简称CFS签名算法。CFS签名算法使用二进制Goppa码，对于给定的正整数 m 和 t ，Goppa码的码长为 $n = 2^m$ ，维数为 $k = n - mt$ ，最小距离为 $d \geq 2t + 1$ ，至多纠正 t 位错误。在随机谰言模型下，CFS签名算法的安全性被归约到SD问题和区分Goppa码问题。文献[18]提供了两种实现签名的方法：①使用完备译码；②添加计数指针。两种CFS框架如图7所示。

第一种方法（使用完备译码）的核心思想是：首先把消息 $\mathbf{M}$ 哈希到校验子空间 $\mathcal{H}(\mathbf{M}) \in \mathbb{F}_2^{n-k}$ ，然后随机选择重量为 δ 的错误向量 $\mathbf{e}_1^\delta$ ，计算 $\mathbf{h} (= \mathbf{Q}^{-1} \mathcal{H}(\mathbf{M}))$ 与 $\mathbf{Q}^{-1} \mathbf{H} \mathbf{e}_1^\delta$ 的和，并检查值 $\mathbf{h} + \mathbf{Q}^{-1} \mathbf{H} \mathbf{e}_1^\delta$ 是否可以译码。如果可以译码，就把译出错误的 $\mathbf{P}^{-1}$ 置换和 $\mathbf{H} \mathbf{e}_1^\delta$ 作为消息 $\mathbf{M}$ 的签名；否则不断尝试重量为 δ 的随机错误向量，直到找到一个可译的 $\mathbf{h} + \mathbf{Q}^{-1} \mathbf{H} \mathbf{e}_N^\delta$ （译出的错误定义为 $\mathbf{e} + \mathbf{e}_N^\delta$ ），最后把 $\mathbf{P}^{-1}(\mathbf{e} + \mathbf{e}_N^\delta)$ 和 $\mathbf{H} \mathbf{e}_N^\delta$ 作为消息的签名。验证签名时，首先使用公钥计算 $\mathbf{H} \mathbf{P}^{-1}(\mathbf{e} + \mathbf{e}_N^\delta)$ ，然后比较 $\mathbf{H} \mathbf{P}^{-1}(\mathbf{e} + \mathbf{e}_N^\delta)$ 与 $\mathcal{H}(\mathbf{M}) + \mathbf{H} \mathbf{e}_N^\delta$ 是否相等，从而检验签名的有效性。该方法生成一个签名平均需要尝试 $\binom{n}{\delta}$ 次。

第二种方法（添加计数指针）的核心思想是：首先把消息 $\mathbf{M}$ 和计数指针0哈希到校验子空间 $\mathcal{H}(\mathbf{M}, 0) \in \mathbb{F}_2^{n-k}$ ，然后检查值 $\mathbf{h}_0 (= \mathbf{Q}^{-1} \mathcal{H}(\mathbf{M}, 0))$ 是否可以译码。如果可以译码，就把译出错误的 $\mathbf{P}^{-1}$ 置换和计数指针0作为消息的 $\mathbf{M}$ 签名；否则更新计数指针，继续和消息进行哈希，直到找到一个可译的 $\mathbf{Q}^{-1} \mathcal{H}(\mathbf{M}, N)$ （译出的错误定义为 $\mathbf{e}$ ），

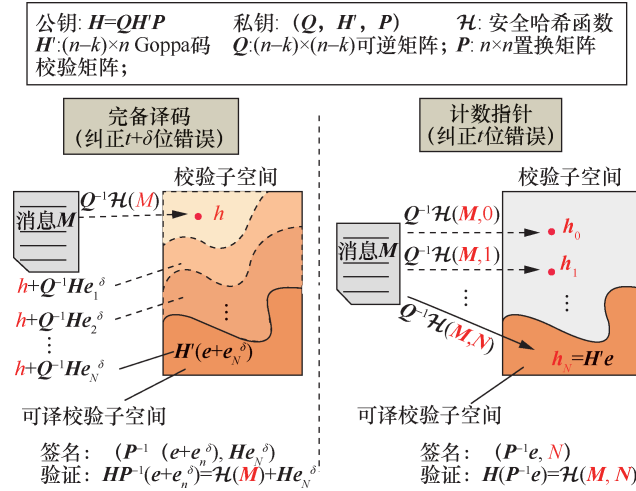


图 7 两种 CFS 框架

Figure 7 Two frameworks of CFS

最后把 $P^{-1}e$ 和计数指针 N 作为消息的签名。验证签名时, 首先使用公钥计算 $HP^{-1}e$, 比较 $HP^{-1}e$ 与哈希值 $\mathcal{H}(M, N)$ 是否相等, 从而检验签名的有效性。该方法生成一个签名平均需要哈希 $t!$ 次,

$$\sum_{i=0}^t \binom{n}{i} / 2^{n-k} \approx t!.$$

对于添加计数指针的 CFS 算法 (算法 4), 它的签名长度为 $(t-1)m + \log t$, 公钥长度为 $tm2^m$, 安全级别为 $2^{mt/2}$ 。CFS 签名算法最大的优势是签名很短。根据文献[65]的分析, 对于 80 bit 安全级别, 建议选择 $m=21, t=10$; $m=19, t=11$ 或者 $m=15, t=12$ 。文献[66]指出存在有效方法区分高码率 Goppa 码和随机码, 这就要求 m 和 t 更大才能抵抗这种区分攻击。随着解译码问题复杂度的改进, 为了达到标准安全级别, 要么增大 m 值, 要么增大 t 值, 这分别导致更大的公钥长度和更长的签名时间。根据以上所述, CFS 签名算法存在公钥太长、签名效率低的不足。近 20 年来, 针对 CFS 算法效率低的问题, 国外学者提出众多改进算法^[67-72], 主要使用其他码类代替 Gopp 码, 涉及的码类包括 Quasi-Dyadic 码、LDGM 码、LRPC 码、 $(U|U+V)$ 码。但这些算法改进并不明显, 要么安全性弱, 要么生成签名慢、公钥长。

算法 4 CFS 签名算法

密钥生成 签名者进行下面步骤。

- ① 根据安全级别 λ , 选择安全参数 n, k, t 。
- ② 选择安全的哈希函数 $\mathcal{H}: \{0, 1\}^* \rightarrow \mathbb{F}_2^{n-k}$ 。
- ③ 随机选择二进制 $[n, k, 2t+1]$ -Goppa 码的校验矩阵 $H \in \mathbb{F}_2^{(n-k) \times n}$, 其译码算法记为 γ 。

④ 随机选择可逆矩阵 $Q \in \mathbb{F}_2^{(n-k) \times (n-k)}$, 置换矩阵 $P \in \mathbb{F}_2^{n \times n}$ 。

- ⑤ 计算 $H' \triangleq QHP$ 。

- ⑥ 输出私钥 Q, P, H' 和公钥 H' 。

签名生成 签名者生成消息 $M \in \{0, 1\}^*$ 的签名 σ 的步骤如下。

- ① 将计数指针 i 从 0 开始赋值, 计算 $s \triangleq Q^{-1}\mathcal{H}(M, i)$, 直到 s 可以由译码算法 γ 译码。将译码结果记为 e' , 即 $H'e'^T = s$ 。

- ② 签名 $\sigma \triangleq (e'P, i)$ 。

签名验证 签名接收者进行如下步骤验证消息\签名对 (M, σ) 的有效性。

- ① $\|e'P\|_H = t$ 。
- ② $H'(e'P)^T = \mathcal{H}(M, i)$ 。

2010 年, Finiasz^[67]提出并行 CFS 算法。新算法在安全参数较小的情况下可以达到标准的安全级别, 但签名变长, 签名效率更低。

2010 年, Barreto 等^[68]基于 Quasi-Dyadic 码改进 CFS 签名算法。改进的签名算法虽然能减小公钥长度, 但降低了签名效率。

2013 年, Baldi 等^[69]基于 LDGM 码改进 CFS

算法, 简称 LDGM。由于改进的算法生成的签名具有某种相关性, 敌手可以利用多个签名获得的信息, 为新消息伪造签名^[73]。因此, LDGM 算法被视为一次签名算法。

2014 年, Gabori 等^[70]提出基于秩距离 LRPC 码的 Hash-Sign 型 CBDS 算法, 简称 RankSign 算法。但是, Debris-Alazard 等^[74]利用扩张 LRPC 码秩重量很小的特点, 攻破了 RankSign 算法和 NIST 中的改进版^[75]。

2019 年, Debris-Alazard 等^[71]提出基于 $(U|U+V)$ 码的 CFS 签名算法, 简称 Wave 签名算法。Wave 签名算法的安全性基于三进制高错误率 HSD 问题^[76]和 $(U|U+V)$ 码区分问题。虽然目前没有发现安全漏洞, 但公钥依然很长, 且生成签名的效率低 (128 bit 安全级别, 每生成一个签名需要几秒)。

2020 年, Yongwoo 等^[72]基于修改的 RM 码改进了 CFS 算法, 简称 MpqsigRM 算法。MpqsigRM 算法是 NIST 第一轮中 pqsigRM 算法^[77]的修正, 它的安全性被归约到 SD 问题和修改的 RM 码区分问题。在能抵抗现有攻击的条件下, MpqsigRM 算法的性能比 CFS 算法更优, 具有公钥短、生成签名快的优点, 但该算法的安全性存疑。

上述改进的 CFS 算法都无法满足实际需求。目前, 构造 Hash-Sign 型 CBDS 算法需要进一步研究的问题是: ① 探索可译校验子稠密的 Goppa 码类或其他码类代替 Goppa 码, 在保证标准安全级别的前提下, 提高签名的效率, 减小公钥长度; ② 提高 Wave 签名算法的签名效率和公钥长度; ③ 研究不依赖纠错能力的 Hash-Sign 型 CBDS 算法。

3.5 Lyubashevsky 型 CBDS 算法

2012 年, Lyubashevsky^[78]提出基于格的无陷门签名算法, 该签名算法可视为由身份认证协议结合 Fiat-Shamir 变换转化而来。Lyubashevsky 签名算法包含的身份认证协议称为 Lyubashevsky 身份认证协议。根据 Lyubashevsky 身份认证协议的设计思路, 基于编码困难问题设计的身份认证协议被称为 Lyubashevsky (也称 Schnorr- Lyubashevsky) 型

CBID 协议; 使用 Fiat-Shamir 变换将 Lyubashevsky 型 CBID 协议转化成的数字签名算法称为 Lyubashevsky 型 CBDS 算法。

Lyubashevsky 型 CBID 协议^[19]的设计思路如图 8 所示。将有限域中两个矩阵 H 和 T 作为公钥, 证明者证明他拥有小重量向量构成的私钥矩阵 S 满足 $T = HS^T$ 。证明者首先随机选择一个小重量承诺向量 y 并计算 $x \triangleq Hy^T$, 将 x 发送给验证者。验证者随机选择一个小重量向量 c 作为挑战发送给证明者。在收到挑战 c 之后, 证明者计算 $z = y + cS$, 将 z 发送给验证者。最后验证者验证 z 是小重量且满足等式 $H_z^T - Tc^T = x$ 。

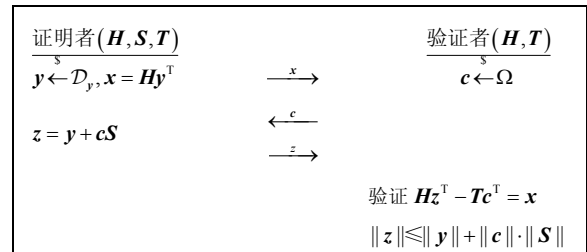


图 8 Lyubashevsky 型 CBID 协议
Figure 8 CBID in Lyubashevsky framework

Lyubashevsky 型 CBID 协议的特点是: 欺骗概率可忽略, 执行一次就能满足安全要求; 不依赖陷门和译码算法。因此, Lyubashevsky 型 CBDS 算法可以克服 Hash-Sign 型和 Stern 型 CBDS 算法的不足。Stern 型 CBID 协议欺骗概率大 (2/3 或 1/2), 必须重复多次, 才能满足安全要求, 这导致 Stern 型 CBDS 算法签名太长, 实用性差。Hash-Sign 型 CBDS 算法使用陷门和译码算法, 极大限制了安全参数的选择, 这导致公钥太长、效率太低, 实用性差。

近年来国内外学者采用 “Lyubashevsky 型 CBID 协议 $\rightarrow$ Fiat-Shamir 变换 $\rightarrow$ Lyubashevsky 型 CBDS 算法” 的思路, 构造一系列 CBDS 算法^[19,79-80,82,84,86,88-89]。但这些 CBDS 算法大多要求 y 、 c 、 S 、 z 小重量, 这很难使 z 隐藏私钥 S , 从而导致签名算法不安全。

2012 年, Persichetti^[79]使用 Lyubashevsky 型 CBID 协议的简单形式构造 CBDS 算法。在 Persichetti 算法中, 挑战是有限域的元素, 而不是

向量, 签名人首先计算挑战和私钥(小重量向量)的乘积, 然后加上随机小重量错误。但根据 Persichetti 的分析, 在汉明距离下, 可以通过统计分析恢复私钥; 在秩距离下, 可以通过代数攻击恢复私钥。换句话说, 这种简单构造不能很好地隐藏私钥。

另一个类似的工作是 NIST 第一轮中的 RaCoSS 签名算法^[80]。该算法使用很大的 Chernoff 界限限制签名的重量, 而且安全参数小, 这使得敌手仅利用公钥就能伪造签名^[81]。之后, 文献[82]通过减小生成签名的重量, 选择大安全参数修正该算法。但由于重量限制一直很宽松, 大于 HGV 界, 所以改进的算法再一次被攻破^[83]。

2018 年, Persichetti^[84]提出改进算法, 并声称新算法可以实现一次签名。在该算法中, 私钥是由小重量向量生成的循环矩阵, 承诺向量和挑战向量都是小重量的, 签名的重量接近 GV 界。由于签名的重量接近 GV 界, 所以它克服了 RaCoSS 算法的弱点, 但签名重量很小带来另一个不足。文献[22, 85]分别利用签名重量很小的性质, 提出代数和统计攻击。Deneuville 等^[22]将挑战转化成 LDPC 码的校验矩阵, 生成的签名作为 LDPC 码的校验子。由于要求生成签名的重量接近 GV 界, 导致私钥、承诺向量、挑战向量的重量都很小且达到相应 LDPC 码的译码能力, 所以使用 LDPC 码的译码算法可解出私钥和承诺向量。Santini 等^[85]提出的统计攻击表明, 仅通过一个签名就可以恢复出私钥。该统计攻击利用小重量承诺的特性, 由于私钥向量循环移位后与承诺向量几乎没有交集, 所以通过对挑战向量进行重量次循环后, 可以很大概率决定私钥的支集。Deneuville 等^[22]提出进一步的改进, 新改进算法使用一系列固定重量的向量构成私钥矩阵(不是循环矩阵), 挑战依然是小重量向量。但是, 这个构造生成的签名会泄露私钥信息, 仅对有限数量的签名是安全的。

2019 年, Song 等^[86]根据 Lyubashevsky 架构提出一个秩距离 CBDS 算法, 简称 SHMW 算法。该算法的不足类似 Persichetti 算法^[84](要求承诺小重量, 签名的重量接近 GV 界)。因此, Aragon 等^[87]利用该不足提出一个有效攻

击: 首先用挑战向量构造 LRPC 码的校验矩阵, 然后用 LRPC 码译码算法解出小重量承诺向量和私钥。

2019 年, Aragon 等^[19]根据 Lyubashevsky 型 CBID 协议的变体(如图 9 所示)提出秩距离 Durandal 签名算法, 该算法是目前安全的秩距离 CBDS 算法。Lyubashevsky 型 CBID 协议的变体主要不同点在于: 证明者添加额外的项 pS 到 $y + cS'$ 获得形式为 $z = y + cS' + pS$ 签名。通过这种方式获得的 z 具有很好的随机性, 敌手无法有效地从 z 中获得私钥的信息。Durandal 算法满足 EUF-CMA 安全性要求, 安全性归约到 PSSI⁺问题、判定形式 RSL 问题、ARSD 问题。但 Durandal 算法依赖的困难问题可靠性弱, 需进一步优化所依赖困难问题的可靠性、公钥长度、签名长度、签名效率。

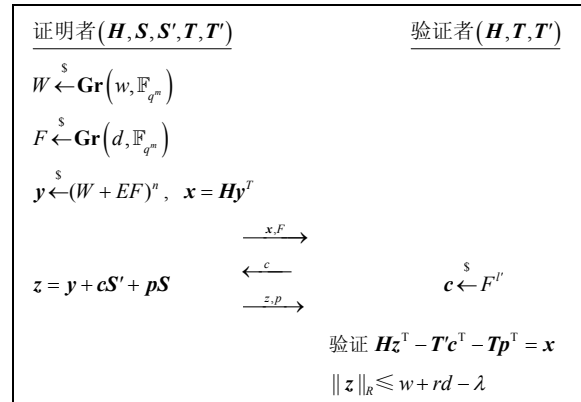


图 9 Durandal 算法的身份认证形式
Figure 9 Durandal algorithm in the identification form

2020 年, Song 等^[88]在理想码情形下, 利用多项式乘积可以表达成向量-矩阵乘积的性质, 改进了 Durandal 算法。在改进算法中, 签名人仅仅选择两个相同小支集向量作为私钥, 不必选择元素来自同一支集的矩阵作为私钥。改进的 Durandal 算法依赖可靠的 RSD 问题, 不再依赖 RSL 问题。对于 128 bit 安全级别, 在签名效率和密钥长度方面, 改进算法都有明显改进。

2020 年, Song 等^[89]根据 Lyubashevsky 型 CBID 协议的架构提出汉明距离 CBDS 算法, 简称 SNMWW 算法。在 SNMWW 算法中, 私钥由一些高码率随机线性码的系统生成矩阵构成, 挑

战是小重量向量，要求签名重量接近 GV 界。之后，Aragon 等^[90]提出一个新统计攻击，对于 80 bit 安全级别，通过 10 个签名， 2^{40} 的计算代价可恢复私钥。但仅知一个签名无法成功攻击。该签名算法签名很短（80 bit 安全级别，签名长度为 4 990 bit），公开矩阵 H 可由 320 bit 长的种子生成。因此，该算法被视为目前最优的编码一次签名算法。

Lyubashevsky 型 CBDS 算法需要研究的问题是：① 优化 Durandal 签名算法的公钥长度和签名长度，提高该算法的可用性；② 提高 Durandal 签名算法依赖困难问题的可靠性。

综上所述，CBDS 算法的研究情况总结如下。

① 存在性能差、安全性弱等不足，具体如表 2 所示。性能差主要体现在公钥长、签名长、签名效率低。签名效率低主要体现在 Hash-Sign 型 CBDS 算法生成签名时间较长，文献[71,91-92]测试了 Wave 和 CFS 的签名时间，每生成一个签名平均需要几秒。需要优化 Stern 型 CBDS 算法的签名长度、Hash-Sign 型 CBDS 算法的公钥长度和签名效率、Lyubashevsky 型 CBDS 算法的签名和公钥长度。

② 构造安全 CBDS 算法的方法少，有待进一步研究探索。目前 CBDS 算法的类型主要有 Xinmei 型、KKS 型、Stern 型、Hash-Sign 型、Lyubashevsky 型。仅最后三类存在安全的 CBDS 算法，且有待进一步改进安全性和性能。

4 结束语

基于编码的密码算法能够抵抗量子算法攻击，是抗量子密码的主流方向之一。设计安全高效的基于编码的数字签名是待解决的难题。本文综述了基于编码的数字签名技术，介绍了现有构造基于编码的数字签名的方法及其研究进展；分析了算法安全性和性能，同时指出了基于编码的数字签名未来可能的研究目标和发展方向。

参考文献：

- [1] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//The 35th Annual Symposium on Foundations of Computer Science. 1994: 124-134.
- [2] GROVER L K. A fast quantum mechanical algorithm for database search[C]//The 28th Annual ACM Symposium on the Theory of Computing. 1996: 212-219.
- [3] SENDRIER N. Code-based cryptography: state of the art and perspectives[J]. IEEE Security & Privacy, 2017, 15(4): 44-50.
- [4] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[C]//The 3rd International Algorithmic Number Theory Symposium. 1998: 267-288.
- [5] PETZOLDT A, CHEN M S, YANG B Y, et al. Design principles for HFEv-based multivariate signature schemes[C]//The 21st International Conference on the Theory and Application of Cryptology and Information Security(ASIACRYPT). 2015: 311-334.
- [6] KILTZ E, PIETRZAK K, VENTURI D, et al. Efficient authentication from hard learning problems[J]. Journal of Cryptology, 2017, 30(4): 1238-1275.

表 2 现存安全 CBDS 算法的性能（128 bit 安全级别）
Table 2 The performance of existing secure CBDS (128-bit security level)

类型	算法	公钥长度	签名长度	不足之处
Stern 型	Stern ^[16]	1 100 bit	81 kB	签名长
	JKPT ^[52]	1 873 bit	109 kB	
	AGS ^[54]	1 873 bit	45 kB	
	CVA ^[53]	1 374 bit	60 kB	
	RStern ^[55]	816 bit	61 kB	
	RJKPT ^[59]	1 309 bit	79 kB	
Hash-Sign 型	Wave ^[71]	3.2 MB	8 312 bit	公钥长签名效率低
	CFS ^[18]	2 GB	306 bit	
Lyubashevsky 型	Durandal ^[19]	15 kB	4 kB	签名和公钥长度待优化
	改进的 Durandal ^[88]	5 kB	3 kB	

- [7] MERKLE R C. A certified digital signature[C]// The 9th Annual International Cryptology Conference (CRYPTO). 1990: 218-238.
- [8] JALALI A, AZARDERAKHSH R, KERMANI M M, et al. ARMv8 SIKE: optimized supersingular isogeny key encapsulation on ARMv8 processors[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2019, 66-I(11): 4209-4218.
- [9] MC-ELIECE R J. A public-key cryptosystem based on algebraic coding theory[R]. Te DSN Progress Report, 1978, 4244: 114-116.
- [10] BERNSTEIN D J, CHOU T, LANGE T, et al. Classic McEliece[R]. Third Round Submission to the NIST Post-quantum Cryptography Call, 2020.
- [11] ARAGON N, BARRETO P, BETTAIEB S, et al. Bike[R]. Third Round Submission to the NIST Post-quantum Cryptography Call, 2020.
- [12] MELCHOR C A, ARAGON N, BETTAIEB S, et al. Hamming quasi-cyclic (HQC)[R]. Third Round Submission to the NIST Post-quantum Cryptography Call, 2020.
- [13] MELCHOR C A, ARAGON N, BETTAIEB S, et al. Rank quasi-cyclic(RQC)[R]. Second Round Submission to the NIST Post-quantum Cryptography Call, 2019.
- [14] ARAGON N, BLAZY O, DENEUVILLE J D, et al. Rollo[R]. Second Round Submission to the NIST Post-quantum Cryptography Call, 2019.
- [15] WANG X M. Digital signature scheme based on error-correcting codes[J]. Electronics Letters, 1990, 26(13): 898-899.
- [16] STERN J. A new identification scheme based on syndrome decoding[C]//The 13th Annual International Cryptology Conference (CRYPTO). 1993: 13-21.
- [17] KABATIANSKII G, KROUK E, SMEETS B. A digital signature scheme based on random error-correcting codes[C]//The 6th IMA International Conference on Cryptography and Coding. 1997: 161-167.
- [18] COURTOIS N T, FINIASZ M, SENDRIER N. How to achieve a McEliece-based digital signature scheme[C]//The 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). 2001: 157-174.
- [19] ARAGON N, BLAZY O, GABORIT P, et al. Durandal: a rank metric based signature scheme[C]//The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). 2019: 728-758.
- [20] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [21] MACWILLIAMS F J, SLOANE N J A. The theory of error-correcting codes[M]. North-Holland: North-Holland Publishing Company, 1977.
- [22] DENEUVILLE J, GABORIT P. Cryptanalysis of a code-based one-time signature[J]. Designs, Codes and Cryptography, 2020, 88(9): 1857-1866.
- [23] GABORIT P, HAUTEVILLE A, PHAN D H, et al. Identity-based encryption from codes with rank metric[C]//The 37th Annual International Cryptology Conference (CRYPTO). 2017: 194-224.
- [24] AGUILAR-MELCHOR C, BLAZY O, DENEUVILLE J C, et al. Efficient encryption from random quasi-cyclic codes[J]. IEEE Transactions on Information Theory, 2018, 64(5): 3927-3943.
- [25] BERLEKAMP E R, MCELIECE R J, VAN TILBORG H C A. On the inherent intractability of certain coding problems[J]. IEEE Transactions on Information Theory, 1978, 24: 384-386.
- [26] PRANGE E. The use of information sets in decoding cyclic codes[J]. IRE Transactions on Information Theory, 1962, 8(5): 5-9.
- [27] MAY A, OZEROV I. On computing nearest neighbors with applications to decoding of binary linear codes[C]//The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). 2015: 203-228.
- [28] TORRES R C, SENDRIER N. Analysis of information set decoding for a sub-linear error weight[C]//The 7th International Conference on Post-Quantum Cryptography (PQCrypto). 2016: 144-161.
- [29] BOTH L, MAY A. Decoding linear codes with high error rate and its impact for LPN security[C]//The 9th International Conference on Post-Quantum Cryptography (PQCrypto). 2018: 25-46.
- [30] NIEBUHR R, PERSICHETTI E, CAYREL P, et al. On lower bounds for information set decoding over F_q and on the effect of partial knowledge[J]. International Journal of Information and Coding Theory (IJICOT). 2017, 4(1): 47-78.
- [31] CHABAUD F, STERN J. The cryptographic security of the syndrome decoding problem for rank distance codes[C]//The 3rd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). 1996: 368-381.
- [32] GABORIT P, ZEMOR G. On the hardness of the decoding and the minimum distance problems for rank codes[J]. IEEE Transactions on Information Theory, 2016, 62: 7245-7252.
- [33] GABORIT P, RUATTA O, SCHREK J. On the complexity of the rank syndrome decoding problem[J]. IEEE Transactions on Information Theory, 2016, 62(2): 1006-1019.
- [34] ARAGON N, GABORIT P, HAUTEVILLE A, et al. A new algorithm for solving the rank syndrome decoding problem[C]//IEEE International Symposium on Information Theory (ISIT). 2018: 2421-2425.
- [35] BARDET M, BROS M, CABARCAS D, et al. Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems[C]//The 26th International Conference on the Theory and

- Application of Cryptology and Information Security (ASIACRYPT). 2020: 507-536.
- [36] BARDET M, BRIAUD P, BROS M, et al. An algebraic attack on rank metric code-based cryptosystems[C]//The 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). 2020: 64-93.
- [37] SENDRIER N. Decoding one out of many[C]//The 4th International Conference on Post-Quantum Cryptography (PQCrypto). 2011: 51-67.
- [38] GUO Q, JOHANSSON T, LÖNDAHL C. A new algorithm for solving ring-LPN with a reducible polynomial[J]. IEEE Transactions on Information Theory. 2015, 61(11): 6204-6212.
- [39] LÖNDAHL C, JOHANSSON T, SHOOSHTARI M K, et al. Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension[J]. Designs, Codes and Cryptography. 2016, 80(2): 359-377.
- [40] OTMANI A, TILLICH J P. An efficient attack on all concrete KKS proposals[C]//The 4th International Conference on Post-Quantum Cryptography (PQCrypto). 2011: 98-116.
- [41] ALABBADI M, WICKER S B. Security of Xinmei digital signature scheme[J]. Electronics Letters, 1992, 28(9): 890-891.
- [42] ALABBADI M, WICKER S B. Digital signature schemes based on error-correcting codes[C]//IEEE International Symposium on Information Theory (ISIT). 1993: 199-199.
- [43] ALABBADI M, WICKER S B. A digital signature scheme based on linear error-correcting block codes[C]//The 4th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). 1993: 238-248.
- [44] 王新梅. 纠错码数字签名方案的修正[J]. 电子学报, 2000, 28(2): 110-112.
- WANG X M. Modification of error-correcting code digital signature scheme[J]. Acta Electronica Sinica, 2000, 28(2): 110-112.
- [45] YE D, YANG J, DAI Z, et al. Attacks on two digital signature schemes based on error correcting codes[C]//International Conference on Information and Communications Security. 2001: 84-89.
- [46] ZHANG Z, FENG D, DAI Z. Cryptanalysis on AW digital signature scheme based on error-correcting codes[J]. Science in China Series F Information Sciences, 2002, 45(5): 397-400.
- [47] XU S B, DOUMEN J, VAN TILBORG H. On the security of digital signature schemes based on error-correcting codes[J]. Designs, Codes and Cryptography, 2003, 28(2): 187-199.
- [48] 张振峰, 冯登国, 戴宗铎. 基于纠错码的 AW 数字签名方案的分析[J]. 中国科学, 2003, 33(2): 164-167.
- ZHANG Z F, FENG D G, DAI Z Z. Analysis of AW digital signature scheme based on error-correcting code[J]. Science China. 2003, 33(2): 164-167.
- [49] KATZ J, LINDELL Y. Introduction to modern cryptography[M]. Taylor & Francis: CRC Press, 2014.
- [50] FIAT A, SHAMIR A. How to prove yourself: practical solutions to identification and signature problems[C]//The 6th Annual International Cryptology Conference (CRYPTO). 1986. 186-194
- [51] VÉRON P. Improved identification schemes based on error-correcting codes[J]. Applicable Algebra in Engineering, Communication and Computing, 1996, 8(1): 57-69.
- [52] JAIN A, KRENN S, PIETRZAK K, et al. Commitments and efficient zero-knowledge proofs from learning parity with noise[C]//The 18th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). 2012: 663-680.
- [53] CAYREL P, VÉRON P, ALAOUI S M E Y. A zero-knowledge identification scheme based on the q -ary syndrome decoding problem[C]//The 17th International Conference on Selected Areas in Cryptography (SAC). 2010: 171-186.
- [54] AGUILAR C, GABORIT P, SCHREK J. A new zero-knowledge code based identification scheme with reduced communication[C]//IEEE Information Theory Workshop (ITW). 2012: 648-652.
- [55] GABORIT P, SCHREK J, ZÉMOR G. Full cryptanalysis of the Chen identification protocol[C]//The 4th International Conference on Post-Quantum Cryptography (PQCrypto). 2011: 35-50.
- [56] BELLINI E, CAULLERY F, HASIKOS A, et al. Code-based signature schemes from identification protocols in the rank metric[C]//The 17th International Conference on Cryptology and Network Security (CANS). 2018: 277-298.
- [57] BELLINI E, CAULLERY F, GABORIT P, et al. Improved Véron identification and signature schemes in the rank metric[C]//International Symposium on Information Theory (ISIT). 2019: 1872-1876.
- [58] AYEIBIE E B, ASSIDI H, SOUIDI E M. An efficient identification scheme based on rank metric[C]//The 12th International Symposium on Foundations and Practice of Security (FPS). 2019: 273-289.
- [59] BELLINI E, GABORIT P, HASIKOS A, et al. Enhancing code based zero-knowledge proofs using rank metric[C]//The 19th International Conference on Cryptology and Network Security (CANS). 2020: 570-592.
- [60] LAU T S C, TAN C H, PRABOWO T F. Key recovery attacks on some rank metric code-based signatures[C]//The 17th IMA International Conference on Cryptography and Coding (IMACC). 2019: 215-235.
- [61] HAUTEVILLE A, TILLICH J. New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem[C]//IEEE International Symposium on Information Theory (ISIT). 2015:

- 2747-2751.
- [62] CAYREL P L, OTMANI A, VERGNAUD D. On Kabatianskii-Krouk-Smeets signatures[C]//The 1st International Workshop on Arithmetic of Finite Fields (WAIFI). 2007: 237-251.
- [63] BARRETO P S L M, MISOCZKI R, SIMPLICIO JR M A. One-time signature scheme from syndrome decoding over generic error-correcting codes[J]. *Journal of Systems and Software*, 2011, 84(2): 198-204.
- [64] GABORIT P, SCHREK J. Efficient code-based one-time signature from automorphism groups with syndrome compatibility[C]//IEEE International Symposium on Information Theory (ISIT). 2012: 1982-1986.
- [65] FINIASZ M, SENDRIER N. Security bounds for the design of code-based cryptosystems[C]//The 15th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). 2009: 88-105.
- [66] FAUGERE J, GAUTHIER-UMANA V, OTMANI A, et al. A distinguisher for high-rate McEliece cryptosystems[J]. *IEEE Transactions on Information Theory*, 2013, 59(10): 6830-6844.
- [67] FINIASZ M. Parallel-CFS strengthening the CFS McEliece-based signature scheme[C]//The 17th International Conference on Selected Areas in Cryptography (SAC). 2010: 159-170.
- [68] BARRETO P S L M, CAYREL P L, MISOCZKI R, et al. Quasi-Dyadic CFS signatures[C]//The 6th International Conference on Information Security and Cryptology (Inscrypt). 2010: 336-349.
- [69] BALDI M, BIANCHI M, CHIARALUCE F, et al. Using LDGM codes and sparse syndromes to achieve digital signatures[C]//The 5th International Conference on Post-Quantum Cryptography (PQCrypto). 2013: 1-15.
- [70] GABORIT P, RUATTA O, SCHREK J, et al. RankSign: An efficient signature algorithm based on the rank metric[C]//The 6th International Conference on Post-Quantum Cryptography (PQCrypto). 2014: 88-107.
- [71] DEBRIS-ALAZARD T, SENDRIER N, TILLICH J P. Wave: A new family of trapdoor one-way preimage sampleable functions based on codes[C]//The 25th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). 2019: 21-51.
- [72] LEE Y, LEE W, KIM Y S, et al. Modified pqsigRM: RM code-based signature scheme[J]. *IEEE Access*, 2020, 8: 177506-177518.
- [73] PHESSO A, TILLICH J P. An efficient attack on a code-based signature scheme[C]//The 7th International Conference on Post-Quantum Cryptography (PQCrypto). 2016: 86-103.
- [74] DEBRIS-ALAZARD T, TILLICH J P. Two attacks on rank metric code-based schemes: RankSign and an IBE scheme[C]//The 24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). 2018: 62-92.
- [75] ARAGON N, GABORIT P, HAUTEVILLE A, et al. RankSign-a signature proposal for the NIST's call[R]. First Round Submission to the NIST Post-Quantum Cryptography Call, 2017.
- [76] BRICOUT R, CHAILLOUX A, DEBRIS-ALAZARD T, et al. Ternary syndrome decoding with large weight[C]//The 26th International Conference on Selected Areas in Cryptography (SAC). 2019: 437-466.
- [77] LEE W, KIM Y S, NO J S. A new signature scheme based on punctured reed-muller code with random insertion[J]. *Computer Research Repository (CoRR)*, 2016.
- [78] LYUBASHEVSKY V. Lattice signatures without trapdoors[C]//The 31th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2012: 738-755.
- [79] PERSICHETTI E. Improving the efficiency of code-based cryptography[D]. Auckland: University of Auckland, 2012: 111-115.
- [80] FUKUSHIMA K, ROY P S, XU R, et al. Random code-based signature scheme (RaCoSS)[R]. First Round Submission to the NIST Post-quantum Cryptography Call. 2017.
- [81] BERNSTEIN D J, HAJLSING A, LANGE T, et al. Comments on RaCoSS. A submission to NIST's PQC Competition[EB]. 2018.
- [82] ROY P S, MOROZOV K, FUKUSHIMA K, et al. Code-based signature scheme without trapdoors[R]. IEICE Technical Report, 2018, 118: 17-22.
- [83] XAGAWA K. Practical attack on RaCoSS-R[J]. *IACR Cryptology ePrint Archive*, 2018: 831.
- [84] PERSICHETTI E. Efficient one-time signatures from quasi-cyclic codes: A full treatment [J]. *Cryptography*, 2018, 2(4): 30.
- [85] SANTINI P, BALDI M, CHIARALUCE F. Cryptanalysis of a one-time code-based digital signature scheme[C]//IEEE International Symposium on Information Theory (ISIT). 2019: 2594-2598.
- [86] SONG Y, HUANG X, MU Y, et al. A new code-based signature scheme with shorter public key[J]. *IACR Cryptology ePrint Archive*, 2019: 53.
- [87] ARAGON N, BLAZY O, DENEUVILLE J C, et al. Cryptanalysis of a rank-based signature with short public keys[J]. *Designs, Codes and Cryptography*, 2020: 88(4): 643-653.
- [88] SONG Y, HUANG X, MU Y, et al. An improved durandal signature scheme[J]. *SCIENCE CHINA Information Sciences*, 2020, 63(3): 132103:1-132103:16.

- [89] SONG Y, HUANG X, MU Y, et al. A code-based signature scheme from the Lyubashevsky framework[J]. Theoretical Computer Science, 2020, 835: 15-30.
- [90] ARAGON N, BALDI M, DENEUVILLE J C, et al. Cryptanalysis of a code-based full-time signature[J]. Designs, Codes and Cryptography, 2021.
- [91] BERNSTEIN D J, CHOU T, SCHWABE P. McBits: fast constant-time code-based cryptography[C]//The 15th International Workshop on Cryptographic Hardware and Embedded Systems (CHES). 2013: 250-272.
- [92] LANDAIS G, SENDRIER N. Implementing CFS[C]//The 13th International Conference on Cryptology in India (INDOCRYPT). 2012: 474-488.



黄欣沂（1981- ），男，江苏仪征人，福建师范大学教授、博士生导师，主要研究方向为密码学与信息安全。



伍玮（1981- ），女，江苏南京人，福建师范大学教授，主要研究方向为密码学与信息安全。

[作者简介]



宋永成（1993- ），男，安徽亳州人，博士，主要研究方向为基于编码的密码学、数字签名与身份认证。



陈海霞（1982- ），女，江苏南通人，福建师范大学博士生，主要研究方向为图像认证、图像取证、网络安全与密码学等。