

基于纠错码的数字签名技术综述

任方^{1,2}, 郑东^{1,2}, 范九伦²

(1. 西安邮电大学无线网络安全技术国家工程实验室, 陕西 西安 710121;
2. 西安邮电大学通信与信息工程学院, 陕西 西安 710121)

摘要: 量子算法的出现对当前广泛使用的基于数论困难问题的数字签名算法造成了严重威胁, 而基于纠错码的数字签名算法可以抵抗已知的量子算法攻击, 近年来, 得到了众多研究者的关注, 成为最有发展潜力的数字签名技术之一。基于纠错码的数字签名算法具有较高的安全性和较快的运算速度, 其研究成果遍及普通签名、盲签名、环签名、群签名等多个领域。对基于纠错码的数字签名技术进行了综述, 分析和评价了当前的主流算法, 并指出未来可能的研究方向。

关键词: 纠错码; 数字签名; 校验子译码; 后量子密码

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00108

Survey of digital signature technology based on error correcting codes

REN Fang^{1,2}, ZHENG Dong^{1,2}, FAN Jiu-lun²

(1. National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China;
2. Department of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract: The emergence of quantum algorithms have threatened the security of digital signature algorithms widely used currently, most of which based on some hard problems in number theory. The digital signature algorithms based on error correcting codes, which can resist quantum attack, has been studied by many researchers in recent years and there have been many research results in different areas, such as normal digital signature, blind signature, ring signature, group signature. Because of the fast computation speed and high security, it has become one of the most promising digital signature technologies. A comprehensive introduction was given and digital signature technologies based on error correcting codes were summarized, the key technologies were analyzed and the possible research directions in the future were pointed out.

Key words: error correcting codes, digital signature, syndrome decoding, post quantum cryptography

1 引言

公钥密码与数字签名技术^[1~3]出现于 20 世纪

70 年代, 作为密码技术的重大突破, 公钥密码自问世以来已经在数据安全与保密通信等领域取得了大量重要的成果, 成为密码领域发展最为蓬勃

收稿日期: 2016-09-12; 修回日期: 2016-10-19。通信作者: 任方, renfang_81@163.com

基金项目: 国家自然科学基金资助项目 (No.61272037, No.61472472); 陕西省自然科学基金基础研究计划基金资助项目 (No.2015JQ6262); 陕西省教育厅专项科研计划基金资助项目 (No.15JK1669)

Foundation Items: The National Natural Science Foundation of China (No.61272037, No.61472472), The Natural Science Basic Research Plan of Shaanxi Province (No.2015JQ6262), Scientific Research Program Funded by Shaanxi Provincial Education Department (No.15JK1669)

的一个分支。经典的公钥数字签名算法都是基于数论中的经典难解问题,如 RSA 签名算法^[2]基于大整数分解的难解性、DSA 签名算法^[3]基于离散对数问题的难解性等。经典计算机不能有效求解这些数论难解问题,因此在此基础上建立的数字签名算法也不可能被有效攻击。但是量子算法^[4-6]的出现以及量子计算机的问世开始对这些问题提出了挑战。

目前,可用于密码算法破译的量子算法主要有 Shor 算法^[4]和 Grover 算法^[5]。Shor 算法可以对当前广泛使用的 RSA、ElGamal、ECC 公钥密码算法进行有效的攻击;而 Grover 算法可以将密钥的长度减半,极大提高攻击者攻击成功的概率。因此,一旦量子计算机在未来的几年到十几年内投入使用,这些基于数学难解问题的公钥密码算法都将寿终正寝,必须尽快寻求能够抵抗量子攻击的密码算法。目前,能够抵抗已知量子算法攻击的后量子密码体制^[6]包括基于纠错码问题的公钥密码体制^[7]、基于 Hash 函数的公钥密码体制^[8]、基于格问题的公钥密码体制^[9,10]、基于多变量问题的公钥密码体制^[11]。

基于纠错码的公钥密码算法最早由 McEliece 提出^[12],其基本思想是将待加密的明文看作一个合法码字,加密过程等价于给明文码字添加一个随机选择的错误向量,解密过程相当于译码。其后出现的 Niederreiter 加密算法^[13]基于校验子译码来实现加密与解密,其安全性与 McEliece 算法完全等价^[14]。第一个基于纠错码的数字签名算法是 1990 年的 Xinmei 方案^[15],但是该算法很快被攻击者攻破^[16-20],目前,基于纠错码的典型数字签名算法有 3 大类,分别以 CFS 算法^[21]、Stern 算法^[22]、KKS 算法^[23]为代表,在此基础上衍生出了众多的改进算法和实现特殊功能的数字签名算法,如盲签名、环签名、群签名。

作为公认的可以抵抗量子攻击的公钥密码技术,基于纠错码的数字签名技术是该领域未来发展的主流之一。除了具有较高的安全性之外,此类算法往往只需要进行一些简单的位运算,因此一般都具有很高的实现效率。本文对这一领域的主流算法进行介绍,分析算法的性能并展望未来的研究方向。

2 基础知识

2.1 纠错码基础

定义 1 线性分组码

给定有限域 F_q , 一个 (n, k) 线性分组码 C 定义为 n 维线性空间 F_q^n 的一个 k 维线性子空间。其中, F_q^n 中的向量称为字 (word), C 中的向量称为码字 (codeword), n 称为分组码的码长, k 称为分组码的维数。

定义 2 生成矩阵

一个 (n, k) 线性分组码 C 的生成矩阵是 $k \times n$ 的矩阵 G , 其中, G 的行向量构成了 C 的一组基。

由于 C 是一个子空间, 其基并不唯一, 因此其生成矩阵也不唯一, 但各个生成矩阵之间可以通过初等行变换相互转化, 即若 G 是 C 的一个生成矩阵, P 是一个初等矩阵, 则 PG 也是 C 的一个生成矩阵。

定义 3 校验矩阵

一个 (n, k) 线性分组码 C 的校验矩阵是一个 $(n-k) \times n$ 的矩阵 H , 其中, H 的任意行向量与 C 的生成矩阵 G 的任意行向量正交, 即 $HG^T = 0$ 。

线性分组码的校验矩阵也不唯一且可以通过初等行变换相互转化, 实际上, H 的行构成了 C 的对偶空间的一组基。长为 n 的向量 c 是 C 的一个码字的充分必要条件是 $Hc^T = 0$ 。对于任意的字 c , 一般将 Hc^T 称为 c 的校验子。

定义 4 Hamming 距离与重量

线性分组码的 2 个码字 $u = (u_1, u_2, \dots, u_n)$ 和 $v = (v_1, v_2, \dots, v_n)$ 的 Hamming 距离 $d(u, v)$ 定义为 u 和 v 的不同分量的个数, 即 $d(u, v) = |\{i | u_i \neq v_i\}|$, 码字 u 的 Hamming 重量 $w(u)$ 定义为 u 与全零码字的距离, 即 $w(u) = d(u, 0)$, 码 C 中非零码字的最小 Hamming 重量称为 C 的最小距离, 一般记作 $d_{\min}$ 。

码的最小距离决定了码的纠错能力, 一般来说, 线性分组码的理论纠错能力 t 满足

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor。$$

基于纠错码的公钥加密与数字签名算法主要使用一种特殊的线性分组码: Goppa 码^[24]。典型

的二元 Goppa 码由 F_2 的某个扩域中的一个 n 元有序集合 $L = (\alpha_1, \alpha_2, \dots, \alpha_n)$ 和一个根不在 L 中的 t 次多项式 $g(x)$ 生成, 其参数具有以下形式: 码长 $n=2^m$, 维数 $k=n-mt$ 。利用 Goppa 码的生成集合 L 和生成多项式 $g(x)$ 可以进行有效的译码^[25], 这是构造基于纠错码的各类密码算法的基础。即将 Goppa 码的结构作为秘密的陷门信息或者签名的私钥, 可以方便地实现数字签名算法。

2.2 困难问题

基于纠错码的公钥加密与数字签名算法的理论安全性主要依赖于以下几个困难问题, 这些问题目前都被证明是 NP—完全问题^[26], 可以有效抵抗已知的量子算法攻击。

问题 1 校验子译码 (SD, syndrome decoding) 问题。

输入有限域 F_q 上的一个 $(n-k) \times n$ 的矩阵 H , 向量 $s \in F_q^{n-k}$, 整数 $l > 0$, 问是否存在一个字 $x \in F_q^n$, 其重量 $w(x) \leq l$, 使 $Hx^T = s$ 。

问题 2 寻找码字 (CF, codeword finding) 问题
输入有限域 F_q 上的一个 $(n-k) \times n$ 的矩阵 H , 整数 $l > 0$, 问是否存在一个非零的字 $x \in F_q^n$, 其重量 $w(x) \leq l$, 使 $Hx^T = 0$ 。

问题 3 完备译码 (CD, complete decoding) 问题

输入有限域 F_q 上的一个 $(n-k) \times n$ 的矩阵 H , 向量 $s \in F_q^{n-k}$, 问是否存在一个字 $x \in F_q^n$, 其重量 $w(x) \leq d_0$, 使 $Hx^T = s$ 。其中, d_0 表示以 H 为校验矩阵的线性分组码的 Gilbert-Varshamov 距离^[13]。

对于基于二元 Goppa 码构建的公钥加密与数字签名算法, 其安全性直接依赖于以下 2 个问题。

问题 4 Goppa 界译码 (GBD, goppa bounded decoding) 问题。

输入 F_2 上的一个 $(n-k) \times n$ 矩阵 H , 向量 $s \in F_2^{n-k}$, 寻找一个字 $x \in F_2^n$, 其重量 $w(x) \leq \frac{n-k}{\ln n}$, 使 $Hx^T = s$ 。

问题 5 Goppa 码的区分 (GD, goppa code distinguishing) 问题。

输入 F_2 上的一个 $(n-k) \times n$ 的矩阵 H , 判断 H 是一个 (n, k) Goppa 码的校验矩阵还是一个随机 (n, k) 码的校验矩阵。

GBD 问题作为 SD 问题的特例, 也被证明是 NP—困难的, 而 GD 问题虽然没有 NP 的证明, 但是学界普遍认为该问题也是困难问题。

2.3 基于纠错码的加密算法

McEliece 于 1978 年给出了第一个基于纠错码的加密算法^[12], 该算法至今未被攻破, 即使在计算能力已经很强大的今天, 只需修改算法的参数仍然可以达到想要的安全级别。原始的 McEliece 算法基于二元 Goppa 码构建, 后来也有很多人尝试使用其他的码类代替 Goppa 码, 但大多数都以失败而告终。

Niederreiter 给出了 McEliece 加密算法的一个重要变种^[13], 其安全性与 McEliece 算法等价^[14], 即如果能够攻破其中一个算法, 也就能够攻破另一个。Niederreiter 算法将明文消息看作一个具有固定重量的错误向量, 加密等价于计算校验子, 解密等价于校验子译码。

算法 1 Niederreiter 加密算法

参数生成

①选择 F_2 上的不可约 (n, k) Goppa 码 C , 码的纠错能力为 t , 校验矩阵为 H , 一个有效的校验子译码算法 γ 。

②选择 F_2 上的一个 $(n-k) \times (n-k)$ 的二元随机可逆矩阵 M , 一个 $n \times n$ 的二元随机置换矩阵 P 。

③系统公开参数为 $\langle t, H^{\text{pub}} = MHP \rangle$, 私钥为 $\langle M, H, P, \gamma \rangle$ 。

加密过程

发送者加密消息 m 的过程如下。

①将消息 m 表示为重量为 t 的向量 $e = \varphi_{n,t}(m) \in F_2^n$ 。

②计算密文 $s = H^{\text{pub}} e^T$ 。

解密过程

接收者解密密文 $s \in F_2^{n-k}$ 的过程如下。

首先, 计算 $M^{-1}s = HPe^T = H(Pe^T)$ 。

然后, 用译码算法对上述结果进行译码, 由于 Pe^T 仍然是一个重量为 t 的向量, 因此 $\gamma(M^{-1}s) = \gamma(HPe^T) = Pe^T$ 。

最终计算明文 $e^T = P^{-1}Pe^T$ 。

3 基于纠错码的数字签名

3.1 早期技术

第一个基于纠错码的数字签名方案由王新梅

于 1990 年给出^[15], 该方案同时还可以实现附加的加密功能, 被称为 Xinmei 方案。不久, Alabbadi 等^[16]对 Xinmei 方案提出了有效的选择明文攻击, 称为 AW 攻击, 该攻击的复杂度仅为多项式时间。随后他们给出了一种新的可以抵御 AW 攻击的数字签名方案, 称为 AW 方案^[17]。王新梅^[18]随后给出了 Xinmei 方案的一种修正, 可以抵御 AW 的攻击。2003 年, Xu^[19]和张振峰等^[20]分别对这一系列方案进行了分析和总结, 他们找到了从公钥计算私钥的有效方法, 并指出: 由于基于大矩阵分解的困难性构造出的这些数字签名均具有某种线性性质, 因此很难得到安全性高的数字签名方案, 从而为这一系列数字签名算法的研究画上了句号。

3.2 三大方向

目前, 公认可行的构造基于纠错码的数字签名算法有以下 3 条途径。

1) 从已有的基于纠错码的加密算法出发, 更改加解密次序, 实现数字签名。签名者将待签名的消息 (一般先进行 hash) 看作密文, 利用私钥对其进行解密作为签名, 而验证者利用公钥对签名进行加密实现验证签名。典型算法是 CFS 方案。

2) 从已有的零知识身份认证协议出发, 利用 Fiat-Shamir 给出的准则^[27]将其转换成数字签名算法。典型算法是 Stern 方案。

3) 构建校验子空间的一个特殊子集合, 使签名者能对其中的校验子进行有效地译码操作, 将译码结果作为签名值, 这是一种最一般的构造方法。典型算法是 KKS 方案。

3.2.1 CFS 方案

2001 年, Courtois 等^[21]利用校验子译码问题的困难性, 创造性地给出了第一个严格意义上的比较安全的基于纠错码的签名方案, 称为 CFS 方案。CFS 数字签名方案属于上述第一类构造方法, 它基于原始的 Niederreiter 加密算法, 将待签名消息 (的 hash 值) 看作 Niederreiter 加密算法的密文, 解密看作签名, 而加密则用来验证签名。

算法 2 CFS 签名算法

参数生成

①选择一个 F_2 上的不可约 (n, k) Goppa 码 C , 码的纠错能力为 t , 校验矩阵为 H , 以及一个有效的校验子译码算法 γ 。

②选择 F_2 上一个 $(n-k) \times (n-k)$ 的二元随机可逆

矩阵 M , 一个 $n \times n$ 二元随机置换矩阵 P 。

③选择一个公开的安全 hash 函数 $h: \{0,1\}^* \rightarrow F_2^{n-k}$ 。

④系统公开参数为 $\langle h, t, H^{\text{pub}} = MHP \rangle$, 私钥为 $\langle M, H, P, \gamma \rangle$ 。

签名过程

设签名者需要签署的消息为 m , 则签名过程如下。

①计算消息的 hash 值 $s=h(m)$ 。

②对于 $i=0,1,2,\dots$, 计算 $s_i = M^{-1}h(s \parallel i)$, 找到最小的 i_0 使 $\gamma(s_{i_0})$ 存在。

③记 $v = \gamma(s_{i_0})$, 则签名值为 $(i_0 \parallel vP)$ 。

验证过程

设验证者收到的消息签名对为 $\langle m, i \parallel u \rangle$, 则验证过程如下。

①计算 $a=h(h(m) \parallel i)$, 以及 $b = H^{\text{pub}} u^T$ 。

②若 $a=b$, 则签名正确, 否则签名验证失败。验证过程的正确性说明如下。

如果 $\langle m, i \parallel u \rangle$ 是根据签名过程得到的一对合法的消息—签名对, 则一定有

$$\begin{aligned} b &= H^{\text{pub}} u^T = MHP(vP)^T = MHPP^T v^T \\ &= MHv^T = Ms_{i'} = h(h(m) \parallel i') = a \end{aligned} \quad (1)$$

根据 CFS 算法给出的推荐参数, 其签名长度为 144 bit, 可以抵抗一般的生日攻击。对其稍加改动可以得到 3 个实用性更强的签名算法: 短签名 (签名长度为 81 bit)、快速签名 (签名长度为 132 bit) 以及折中的签名 (签名长度为 119 bit)。

CFS 算法的安全性证明由 Dallot 等^[28]给出, 在随机预言机模型^[29]下, CFS 算法的安全性可以归约到 SD 问题和 GD 问题上。然而, Faugere^[30]指出高码率的 Goppa 码可以与随机码区分开, 从而对上述证明的结果提出了挑战。尽管如此, 通过适当选择参数, CFS 还是普遍被认为能够达到较高的安全性, 10 余年来出现了各种改进算法, 如 mCFS^[28]、并行 CFS^[31]。目前, 大多数基于纠错码的签名方案以及特殊签名, 如盲签名、环签名等, 大都在 CFS 的基础上进行构造。所有这些签名算法的核心都与 CFS 一致, 即签名时对消息的 hash 值进行处理使其成为一个 Goppa 码的校验子, 签名过程是利用秘密的译码算法对校验子进行译码; 而验证签名时通过计算字的校验子并与消息的 hash 值进行对比来检验签名的有效性。

尽管 CFS 及其衍生出的一系列签名算法有较高的安全性，但其缺陷也是明显的，即签名的效率很低。以基本的 CFS 算法为例，签名时需要对消息的 hash 值进行变换后进行校验子译码，但由于 Goppa 码纠错能力的限制，只有一部分校验子是可以译码的，因此需要进行多次尝试（签名过程的计数器 i 标识了签名尝试的次数）。CFS 算法签名成功的概率可以做如下分析。

对于一个纠错能力为 t ，参数为 $n = 2^m$ ， $k = n - mt$ 的 (n, k) Goppa 码，可以计算出可译码的校验子个数为

$$N_D = \sum_{i=1}^t \binom{n}{i} \approx \binom{n}{t} \approx \frac{n^t}{t!} \quad (2)$$

而总的校验子个数为

$$N_T = 2^{n-k} = 2^{mt} = n^t \quad (3)$$

二者之比即为随机选取一个校验子可译码的概率

$$P_D = \frac{N_D}{N_T} \approx \frac{\binom{n}{t}}{n^t} = \frac{1}{t!} \quad (4)$$

因此，CFS 算法签名成功的概率为 $P_s = \frac{N_D}{N_T} \approx$

$\frac{n^t}{t!} = \frac{1}{t!}$ ，即平均需要尝试 $t!$ 次才能够得到一个可以译码的校验子，如 $t=10$ 时，平均需要尝试 $10! = 3\,628\,800$ 次才能得到一个签名。最初的文献中作者建议取 $t=9$ 。但是在文献[32]给出的 Bleichenbacher 攻击下这一参数已经不再安全，建议参数至少取 $m=15$ ， $t=12$ 或 $m=16$ ， $t=10$ 。随着新的攻击方法的出现， t 的取值要求必然越来越大，这就使签名成功的次数呈指数增长，签名速度会越来越低，算法的实现效率也会越来越差。Finiasz^[31]给出的并行 CFS 在保持参数较小的情况下可以达到较高的签名安全性，在一定程度上提升了签名效率。Barreto^[33]给出的算法使用 QD Goppa 码代替 Goppa 码，可以降低公钥尺寸，但是却又增加了签名时间消耗。

目前，这一方向主要的研究目标和发展方向如下。

①提升 CFS 类算法的签名速度，寻找可译码的校验子稠密的 Goppa 码的子类，同时研究不依

赖于码的纠错能力 t 的签名过程。

②使用其他码类构造 CFS 类的签名算法，在保证较高安全性的前提下降低公钥的尺寸。

3.2.2 Stern 方案

Stern^[22]给出了基于纠错码的零知识身份认证协议，使用 Fiat-Shamir 给出的方法^[27]可以将 Stern 的身份认证协议转换成标准的数字签名方案，这种方式属于上述第 2 种构造方法。

Stern 身份认证协议与 Niederreiter 加密算法密切相关，其安全性基于校验子译码的困难性。用户私钥是一个低重量字 e ，将其校验子 He^T 作为公钥发给验证者。算法采用 3 轮零知识证明协议来证明用户拥有 e ，从而实现身份认证。Stern 身份认证方案如算法 3 所示。

算法 3 Stern 身份认证方案

参数生成

①系统参数：随机选择一个 F_2 上的 (n, k) 码 C ，其校验矩阵为 $(n-k) \times n$ 的矩阵 H ，选择一个公开的抗碰撞 hash 函数 h 。

②用户设置私钥 $e \in F_2^n$ ，满足条件 $w(e) = p$ 。

③计算公钥 $s = He^T$ ，系统公开参数为 $\langle p, h, H \rangle$ 。

认证过程

①证明者选择随机向量 $y \in F_2^n$ ，以及集合 $\{1, 2, \dots, n\}$ 上的一个随机置换 σ ，计算 $c_1 = h(\sigma | Hy^T)$ ， $c_2 = h(\sigma(y))$ ， $c_3 = h(\sigma(y + e))$ ，将三元组 $\langle c_1, c_2, c_3 \rangle$ 发送给验证者。

②验证者发送随机请求 $b \in \{1, 2, 3\}$ 。

③证明者根据 b 的值给验证者公开一定的信息：如果 $b=0$ ，公开 $\langle y, \sigma \rangle$ ；如果 $b=1$ ，公开 $\langle y + e, \sigma \rangle$ ；如果 $b=2$ ，公开 $\langle \sigma(y), \sigma(e) \rangle$ 。

④验证者检验消息：如果 $b=0$ ，检验 c_1 和 c_2 ，可直接验证；如果 $b=1$ ，检验 c_1 和 c_3 ，其中 c_3 可以直接验证，验证 c_1 时需要用到 $Hy^T = H(y + e)^T + He^T = H(y + e)^T + s$ ；如果 $b=2$ ，检验 c_2 和 c_3 以及是否有 $w(\sigma(e)) = p$ ，可直接验证。

在上述认证协议的一次执行过程中，一个不诚实的攻击者伪装成合法用户欺骗验证者成功的概率为 $\frac{2}{3}$ ^[22]。如果想要减小这一概率，需要多次执行协议。

Stern 方案的缺陷包括：①协议执行的次数往往过多，当需要攻击者的欺骗概率小于 2^{-16} 时，

Stern 方案需要执行 28 次才可以；②公钥尺寸过大，典型值为 150 000 bit。为了缩短公钥尺寸，Gaborit 利用双循环矩阵给出了一个轻量级的身份认证方案^[34]，大大降低了公钥尺寸，甚至可以达到比 RSA 的公钥大小还要小，典型值为 347 bit。方案的安全性可以归结为双循环线性码的校验子译码问题，其困难性是否与原始的 SD 问题等价还不清楚。Cayrel 等^[35]在此基础上构造出了一个 5 轮的 q 元双循环码的身份认证方案，其中不诚实的攻击者每轮能够欺骗成功的概率下降为 $\frac{1}{2}$ ，从而实现相同的欺骗概率，该方案比 Stern 方案减少了协议执行的次数。

理论上讲，任何一种零知识身份认证协议均可按 Fiat-Shamir 方法转换成数字签名方案，而且普遍认为以这种模式得到的数字签名在随机预言机模型下的安全性等价于身份认证方案的安全性，然而 Goldwasser 等^[36]却给出了一种反例，即存在一种安全的身份认证方案，经 Fiat-Shamir 方法转换生成的数字签名方案却是不安全的。尽管如此，这一模式并未被摒弃，主要是因为它实现简单，不需要专门设计签名方案。

这种构造方式的另一个缺陷在于数字签名算法生成的签名长度依赖于身份认证方案交互的轮数，这往往导致签名长度过长，如 Stern 方案产生的签名长度大约为 120 000 bit，远大于同类型的数字签名。因此该方向的一个主要研究目标是缩短身份认证协议的交互轮数以及降低数字签名的长度。

目前，这一方向主要的研究目标和发展方向如下。

①研究不同于 Stern 方案的基于纠错码的身份认证协议，降低每一轮的攻击者欺骗成功概率，缩短协议的交互轮数，以降低最终的签名长度。

②寻找根据 Fiat-Shamir 方法将身份认证协议转换得到数字签名这一模式的严格安全证明。

3.2.3 KKS 方案

KKS 签名方案由 Kabatianskii、Krouk 和 Smeets 于 1997 提出^[23]。该方案属于上述第 3 种构造方法，是一种直接构造的数字签名算法。因为 KKS 方案对一个消息进行签名时不需要执行译码操作，这一特点使其可以适用于任意纠错码，同时达到很高的签名速度。KKS 签名方案的主要思想是利用给定线性码的可译码的校验子的子集

合构成一个较大维数的子空间，据此建立一个公钥矩阵，矩阵的若干列之和对应一个校验子，从而使每一个消息都是可以进行译码的。原始文献^[23]提出了 KKS 的 4 种变形：KKS-1、KKS-2、KKS-3 和 KKS-4，当公钥参数不泄露任何信息的时候，签名算法的安全性等价于 Niederreiter 加密方案。

KKS 方案存在 2 个缺点：其一是公钥的尺寸相对较大；其二是安全性不高，即 KKS 方案是一个一次签名方案。KKS 方案的安全性讨论由 Cayrel 等^[37]于 2007 年给出，证明了攻击者只需要 2^{77} 个二进制运算和不超过 20 对签名（依赖于签名参数，20 是典型值），就能成功攻破 KKS-3 方案，因此 KKS 方案产生的每一个签名都会泄露有关私钥的一些信息，从而不能抵抗已知明文攻击，只能用于一次性签名。Otmani 等^[38]对 KKS 方案中的所有参数均进行了攻击，证明如果参数选择不当，即使没有已知的签名，也能够从公开参数中完全恢复出私钥。这种攻击对于早期 KKS 型签名方案均有效，也是目前对 KKS 方案最强大的攻击。

Barreto^[39]提出了一个 KKS 方案的“噪声”变异，该方案增加了一个额外的 hash 函数和一个错误向量，并且在随机预言机模型下证明了算法是 EUF-CMA 安全的。和 KKS 方案相似，这个方案也可以使用任意的线性码且其安全性也依赖于校验子译码问题。

目前，这一方向主要的研究目标和发展方向为：在保持 KKS 方案良好的签名效率的前提下，寻求更安全的变种，突破一次性签名的限制，实现标准的数字签名功能。

4 基于纠错码的特殊数字签名

4.1 盲签名

盲签名 (BS, blind signature) 由 Chaum^[40]于 1982 年首次提出，主要用于电子投票和电子支付系统等需要匿名性的场合。Chaum^[41]给出了一个用于电子支付的盲签名方案；Stadler^[42]给出了公平的盲签名方案；Okamoto^[43]给出了基于大整数分解和离散对数的认证方案的盲签名方案；Pointcheval^[44]基于 Schnorr 的协议^[45]给出了可证明安全的盲签名方案。目前，多种成熟的盲签名方案主要应用在同时需要匿名性和认证性的场合中，如在电子现金中实现不可跟踪的电子现金、

在电子选举中实现无记名选举。

盲签名是一种交互式协议, 结果是使持有某个消息 m 的用户 User 获得签名人 Signer 对消息 m 的数字签名 s ; 但是 Signer 却不知道消息 m 的内容; 即使以后将消息—签名对 (m, s) 公开, Signer 也无法追踪消息与自己执行签名过程之间的相互关系。其基本安全需求如下。

1) 盲性: 除请求签名的消息拥有者外, 消息内容对任何人 (包括签名人) 均不可见。

2) 不可伪造性: 任何不知道签名人私钥的人都无法有效地计算出一个能够通过签名验证方程的消息—签名对 (m, s) 。

3) 不可抵赖性: 只要证明消息的签名是合法的, 那么签名人无论如何都无法否认他签过这个消息。

4) 不可追踪性: 签名消息公开以后, 签名人不知道何时签的, 而且即使留有当时的签名信息, 也无法追踪到消息的内容。

第一个基于纠错码的盲签名方案是 Overbeck 于 2009 年提出的 QC 盲签名方案^[46]。该方案基于零知识证明协议与 CFS 签名算法, 作者并未给出严格的安全性证明, 但是声称方案的安全性可以归结为某些 PKP^[47]实例和 SD 问题的困难性。该方案给出的签名长度较长, 典型值达到几 M 的大小, 因此实用性不高。王倩等^[48]基于 CFS 给出了一种新的盲签名方案, 其实现效率接近于 CFS 算法, 但尚未给出安全性证明。目前没有被广泛承认的其他方案。

4.2 群签名

群签名 (GS, group signature) 由 Chaum 等^[49]于 1991 年提出, 指的是以群组的名义进行数字签名。群组成员包括一个管理员与若干群成员, 任意群成员拥有自己的私钥和群组公钥, 均可以代表群进行签名。而当对签名结果产生争执的时候, 管理员可以追踪签名的群成员身份, 由此实现有效的追责。

群签名可以看作一种“群成员匿名身份认证”, 即成员可以证明他属于哪个群组, 但却不泄露其身份。其安全需求如下。

1) 不可伪造性: 群签名不可被群成员之外的任何人伪造。

2) 匿名性: 签名的群成员不可被管理员之外的人识别。

3) 可追踪性: 管理员可有效追踪签名的群成员。

4) 抗合谋攻击: 群成员合谋不能伪造其他群成员的签名。

Boneh 等^[50]给出了短群签名方案。Lysyanskaya 等^[51]给出了群盲签名的概念, 并将其有效用于电子现金。民主群签名是一种特殊的群签名, 民主群签名体制中的群组成员地位都是平等的, 任何成员都可以代表该群组产生群签名。而群组内任何成员都可以从给定的有效群签名中恢复出产生该签名的群成员的身份。Zheng 等^[52]使用公开可验证秘密分享技术设计了门限可追踪的民主群签名。

第一个基于纠错码的群签名方案由 Ezerman 等^[53]于 2015 年提出, 实现了 CPA 匿名和可追溯性要求, 其安全性在随机预言机模型下归约为 McEliece 问题和 SD 问题的一个变种。该方案的密钥尺寸和签名长度均比同类型其他后量子密码技术构造的群签名方案小。

4.3 环签名

环签名 (RS, ring signature) 由 Rivest 等^[54]于 2001 年提出。环签名允许一个签名者代表一个成员集合进行匿名的签名。签名者在签名时不需要其他成员的帮助, 只需利用自己的私钥和其他成员的公钥即可生成合法的签名。验证时只能确定签名是来自于群组中的某个成员而无法追踪其真实身份。

环签名可看作没有管理员的群签名, 为生成一个环签名, 真实的签名者宣布一个任意的包含自己在内的身份集合, 称为“可能的签名者”。计算签名使用自己的私钥和可能的签名者的公钥。

环签名的安全需求如下。

1) 匿名性: 给定一个环签名, 除了签名人外, 任何人无法获知产生该签名的签名人身份。

2) 不可伪造性: 任何不在环 L 中的人没有能力伪造一份声称是 L 中成员生成的环签名。

Zheng 等^[55]在 2007 年第一次提出了基于纠错码的环签名方案, 该方案相当于是对基本 CFS 方案的一种扩展, 其安全性可以归结到 SD 问题和 GD 问题, 目前, 尚未发现有效的攻击方法。方案给出的签名长度为 $144+126l$ bit (l 表示环中的成员数目), 这是在保持安全性的前提下所能达到的较短的签名长度。

4.4 门限环签名

门限环签名 (TRS, threshold ring signature) 是一种将门限思想与环签名结合起来的签名方案。在一个 (l, N) 的门限环签名方案中, 签名私钥以分布式的形式由 N 个成员进行保管, 至少 l 个成员参与才能生成一个有效的门限环签名。第一个门限环签名由 Bresson、Stern 和 Szyldo 于 2002 年提出^[56], 称为 BSS 方案。Wong 等^[57]使用多方陷门变换给出了一种使用串联结构的门限环签名方案。Liu 等^[58]同时基于 RSA 和 DL 公钥密码算法给出了可分离门限环签名的概念, 这些方案的安全性都是基于传统的数论困难问题。

第一个基于纠错码的高效可证明安全的门限环签名方案由 Melchor 给出^[59], 该方案推广了 Stern 身份认证方案, 并利用 Fiat-Shamir 方法将其转换为门限环签名方案。该方案的安全性依赖于 SD 问题, 其签名长度和计算复杂性都是 Stern 方案的 N 倍, 其中, N 为环成员个数, 典型签名长度为 $20N \times 10^3$ bit。建议使用 Gaborit^[60]的双循环矩阵, 可以大幅度减少公钥尺寸, 典型值为 $347N$ bit。

Dallot 等^[61]基于 CFS 方案给出了另一个可证明安全的基于纠错码的门限环签名方案。该方案是将 CFS 签名算法和 Bresson^[62]给出的门限环签名构造方法进行结合而得到, 满足一致性、匿名性和不可伪造性。典型的签名长度为 $675N-228l$ bit, 其中, N 为环成员数, l 为签名门限数。其安全性依赖于 2 个困难问题: Goppa 界译码 (GBD) 问题和 Goppa 码区分 (GD) 问题。

4.5 基于身份签名

Shamir^[63]于 1984 年提出的基于身份密码将用户的公开身份信息 (如 E-mail、名字、IP 地址) 作为用户公钥, 用户的私钥由可信的私钥生成中心 (PKG, private key generator) 根据秘密的系统主密钥和用户公钥生成。基于身份密码体制近年来发展非常迅速^[64-67], 并且促进了基于属性密码体制^[68-70]的诞生, 在自组织网、云计算、大数据等环境下有广泛的应用。Shamir 利用大整数分解问题给出了第一个基于身份的数字签名 (IBS, identity based signature) 算法。Bellare^[71]对一大类基于身份的加密与签名的安全性进行了证明; Galindo^[72]证明了一大类在标准模型下可证明安全的基于身份签名体制的可行性。

Cayrel 等^[73]于 2007 年提出了第一个基于纠错码的 IBS 方案, 其主要思想是将 mCFS 算法和改进后的 Stern 身份认证方案进行结合, 利用 mCFS 对给定的用户身份 hash 值进行 SD 译码, 而 Stern 方案用来实现身份认证。方案的安全性依赖于 SD 和 GD 问题的求解。该方案中用户的身份公钥高达 1×10^6 bit, 且需要进行多轮信息交互, 实用性不强。

基于纠错码的特殊数字签名的研究还处于起步阶段, 目前, 该领域的主要研究目标和发展方向如下。

1) 现有的几个算法的安全性讨论还远远不够, 需要进行更严格的安全性证明。

2) 现有算法的构造大都是简单地将 CFS、Stern 等算法与特殊目的相结合而得到, 而 CFS 算法的实现效率较低、Stern 算法的公钥太大, 因此, 需要研究专门的特殊数字签名算法, 以尽可能避免普通数字签名算法的这些缺陷。

3) 更多特殊类型的数字签名, 如门限签名、代理签名、多重签名、同态签名等尚未出现基于纠错码构建的算法, 需要在这方面进行深入研究。

5 结束语

基于纠错码的公钥密码体制能够抵抗现有的量子算法攻击, 具有较高的安全性与较快的实现效率, 是未来密码学发展的主流方向之一。本文综述了基于纠错码的数字签名技术, 首先, 详细描述了几类基于纠错码的主流数字签名算法; 然后, 介绍了几种特殊类型的数字签名体制以及利用纠错码加以实现的研究进展。在对基于纠错码的典型数字签名算法的细节进行介绍的基础上, 对算法的安全性和实现效率进行了分析和评价, 同时指出了基于纠错码的数字签名技术每一分支未来的研究目标和发展方向。

参考文献:

- [1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [2] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
- [3] KATZ J, LINDELL Y. Introduction to modern cryptography[M]. Boca Raton: CRC Press, 2014.
- [4] SHOR P W. Algorithms for quantum computation: discrete loga-

- rithms and factoring[C]//The 35th Annual Symposium on Foundations of Computer Science, IEEE. 1994: 124-134.
- [5] GROVER L K. A fast quantum mechanical algorithm for database search[C]//The 28th Annual ACM Symposium on Theory of Computing. 1996: 212-219.
 - [6] Post-quantum cryptography[M]. Springer Science & Business Media, 2009.
 - [7] OVERBECK R, SENDRIER N. Code-based cryptography[C]//Post-quantum Cryptography. Berlin Heidelberg: 2009: 95-145.
 - [8] MERKLE R C. A certified digital signature[C]//Advances in Cryptology--CRYPTO'89, Springer New York. 1990: 218-238.
 - [9] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: a ring-based public key cryptosystem[M]//Algorithmic Number Theory. Berlin Heidelberg, 1998: 267-288.
 - [10] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 34.
 - [11] MATSUMOTO T, IMAI H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption[C]//Advances in Cryptology-EUROCRYPT'88, Berlin Heidelberg. 1988: 419-453.
 - [12] MCELIECE R J. A public-key cryptosystem based on algebraic coding theory [J]. DSN Progress Report, 1978, 42(44): 114-116.
 - [13] NIEDERREITER H. Knapsack-type cryptosystems and algebraic coding theory[J]. Problems of Control and Information Theory, 1986, 15(2): 159-166.
 - [14] LI Y X, DENG R H, WANG X M. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems[J]. IEEE Transactions on Information Theory, 1994, 40(1): 271-273.
 - [15] WANG X M. Digital signature scheme based on error-correcting codes[J]. Electronics Letters, 1990, 26(13):898-899.
 - [16] ALABBADI M, WICKER S B. Security of Xinmei digital signature scheme[J]. Electronics Letters, 1992, 28(9):890-891.
 - [17] ALABBADI M, WICKER S B. Digital signature schemes based on error-correcting codes[C]//IEEE International Symposium on Information Theory. 1993: 199-199.
 - [18] 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. Correction of digital signature scheme for error correcting codes[J]. Journal of Electronics, 2000, 28(2): 110-112.
 - [19] XU S B, DOUMEN J, TILBORG H V. On the security of digital signature schemes based on error-correcting codes[J]. Designs Codes & Cryptography, 2003, 28(2):187-199.
 - [20] 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 D. Analysis of AW digital signature scheme based on error correcting codes [J]. Chinese Journal of Science, 2003, 33 (2): 164-167.
 - [21] COURTOIS N T, FINIASZ M, SENDRIER N. How to achieve a McEliece-based digital signature scheme[C]//Advances in Cryptology-ASIACRYPT 2001. 2001:157-174.
 - [22] STERN J. A new identification scheme based on syndrome decoding[C]//Advances in Cryptology—CRYPTO'93, Berlin Heidelberg. 1994: 13-21.
 - [23] KABATIANSKII G, KROUK E, SMEETS B. A digital signature scheme based on random error-correcting codes[C]//Cryptography and Coding, Berlin Heidelberg. 1997: 161-167.
 - [24] MACWILLIAMS F J, SLOANE N J A. The theory of error correcting codes[M]. Elsevier, 1977.
 - [25] PATTERSON N. The algebraic decoding of Goppa codes[J]. IEEE Transactions on Information Theory, 1975, 21(2): 203-207.
 - [26] BERLEKAMP E R, MCELIECE R J, VANTILBORG H C A. On the inherent intractability of certain coding problems[J]. IEEE Transactions on Information Theory, 1978, 24(3): 384-386.
 - [27] FIAT A, SHAMIR A. How to prove yourself: Practical solutions to identification and signature problems[C]//Advances in Cryptology-CRYPTO'86, Berlin Heidelberg. 1987: 186-194.
 - [28] DALLOT L. Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme[M]//Research in Cryptology. Berlin Heidelberg: Springer, 2008: 65-77.
 - [29] BELLARE M, ROGAWAY P. Random oracles are practical: a paradigm for designing efficient protocols[C]//The 1st ACM Conference on Computer and Communication Security, Association for Computing Machinery. 1993:62-73.
 - [30] FAUGERE J C, 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.
 - [31] FINIASZ M. Parallel-CFS[C]//Selected Areas in Cryptography. Berlin Heidelberg: Springer, 2011:159-170.
 - [32] FINIASZ M, SENDRIER N. Security bounds for the design of code-based cryptosystems[C]//Advances in Cryptology- ASIA-CRYPT 2009. 2009: 88-105.
 - [33] BARRETO P S L M, CAYREL P L, MISOCZKI R, et al. Quasi-dyadic CFS signatures[C]//Information Security and Cryptology, Berlin Heidelberg. 2011: 336-349.
 - [34] GABORIT P, GIRAULT M. Lightweight code-based identification and signature[C]//IEEE International Symposium on Information Theory. 2007: 191-195.
 - [35] CAYREL P L, VÉRON P, ALAOUI S M E Y. A zero-knowledge identification scheme based on the qary syndrome decoding problem[C]//Selected Areas in Cryptography. 2011: 171-186.
 - [36] GOLDWASSER S, KALAI Y T. On the (in) security of the Fiat-Shamir paradigm[C]//The Annual Symposium on Foundations of Computer Science. 2003:102-113.
 - [37] CAYREL P L, OTMANI A, VERGNAUD D. On kabatian-skii-krouk-smeets signatures[C]//Arithmetic of Finite Fields. Berlin Heidelberg, 2007: 237-251.
 - [38] OTMANI A, TILLICH J P. An efficient attack on all concrete KKS proposals[C]//Post-quantum Cryptography. Berlin Heidelberg, 2011: 98-116.
 - [39] BARRETO P S L M, MISOCZKI R, SIMPLICIO M A. One-time signature scheme from syndrome decoding over generic error-correcting codes[J]. Journal of Systems & Software, 2011, 84(2):198-204.
 - [40] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology. Springer US, 1983: 199-203.
 - [41] CHAUM D, FIAT A, NAOR M. Untraceable electronic cash[C]//Advances in Cryptology. 1990: 319-327.
 - [42] STADLER M, PIVETEAU J M, CAMENISCH J. Fair blind signatures[C]//Advances in Cryptology—Eurocrypt'95. 1995: 209-219.
 - [43] OKAMOTO T. Provably secure and practical identification schemes and corresponding signature schemes[C]//Advances in Cryptology-CRYPTO'92. 1993: 31-53.
 - [44] POINTCHEVAL D, STERN J. Provably secure blind signature schemes[C]//Advances in Cryptology—ASIACRYPT'96. 1996: 252-265.
 - [45] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.
 - [46] OVERBECK R. A step towards QC blind signatures[J]. IACR Cryptology ePrint Archive, 2009: 102.
 - [47] SHAMIR A. An efficient identification scheme based on permuted kernels[C]//Advances in Cryptology-CRYPTO'89. 1990: 606-609.
 - [48] 王倩, 郑东, 任方. 基于编码的盲签名方案[J]. 计算机应用,

- 2015, 35(10): 2867-2871.
- WANG Q, ZHENG D, REN F. A blind signature scheme based on coding [J]. Computer Application, 2015, 35 (10): 2867-2871.
- [49] CHAUM D, VAN HEYST E. Group signatures[C]//Advances in Cryptology- EUROCRYPT'91. 1991: 257-265.
- [50] BONEHD, BOYEN X, SHACHAM H. Short group signatures[C]//Advances in Cryptology-CRYPTO. 2004: 41-55.
- [51] LYSYANSKAYA A, RAMZAN Z. Group blind digital signatures: a scalable solution to electronic cash[C]//Financial Cryptography. 1998:184-197.
- [52] ZHENG D, LI X, MA C, et al. Democratic group signatures with threshold traceability[J]. IACR Cryptology ePrint Archive, 2008: 112.
- [53] EZERMAN M F, LEE H T, LING S, et al. A provably secure group signature scheme from code-based assumptions[J]. IACR Cryptology ePrint Archive, 2015: 479.
- [54] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//Advances in Cryptology—ASIACRYPT 2001. 2001: 552-565.
- [55] ZHENG D, LI X, CHEN K. Code-based ring signature scheme[J]. IJ Network Security, 2007, 5(2): 154-157.
- [56] BRESSION E, STERN J, SZYDLO M. Threshold ring signatures and applications to ad-hoc groups[C]//Advances in Cryptology-CRYPTO 2002. 2002:465-480.
- [57] WONG D S, FUNG K, LIU J K, et al. On the RS-code construction of ring signature schemes and a threshold setting of RST[C]//Information and Communications Security. 2003:34-46.
- [58] LIU J K, WEI V K, WONG D S. A separable threshold ring signature scheme[J]. Lecture Notes in Computer Science, 2003, 2971: 12-26.
- [59] MELCHOR C A, CAYREL P L, GABORIT P, et al. A new efficient threshold ring signature scheme based on coding theory[J]. IEEE Transactions on Information Theory, 2011, 57(7): 4833-4842.
- [60] GABORIT P, GIRAULT M. Lightweight code-based identification and signature[C]//IEEE International Symposium on Information Theory. 2007:191-195.
- [61] DALLOT L, VERGNAUD D. Provably secure code-based threshold ring signatures[C]//Cryptography and Coding. 2009: 222-235.
- [62] BRESSION E, STERN J, SZYDLO M. Threshold ring signatures and applications to ad-hoc groups[C]//Advances in Cryptology-CRYPTO 2002. 2002:465-480.
- [63] SHAMIR A. Identity-based cryptosystems and signature schemes[J]. Lecture Notes in Computer Science, 1985, 21(2):47-53.
- [64] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]//Advances in Cryptology-CRYPTO 2001.2001: 213-229.
- [65] BAEK J, ZHENG Y. Identity-based threshold decryption[C]//Public Key Cryptography-PKC 2004. 2004: 262-276.
- [66] ZHAO S, AGGARWAL A, FROST R, et al. A survey of applications of identity-based cryptography in mobile ad-hoc networks[J]. Communications Surveys & Tutorials, IEEE, 2012, 14(2): 380-400.
- [67] SILVA D E, PESSOA A L C. Towards a fully self-organized identity-based key management system for MANETs[C]//2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). 2013: 717-723.
- [68] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology-EUROCRYPT 2005. 2005: 457-473.
- [69] CHASE M. Multi-authority attribute based encryption[M]//Theory of Cryptography, Berlin Heidelberg. 2007: 515-534.
- [70] LI J, REN K, KIM K. A2BE: accountable attribute-based encryption for abuse free access control[J]. IACR Cryptology ePrint Archive, 2009, 2009: 118.
- [71] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and signature schemes[J]. Journal of Cryptology, 2009, 22(1): 1-61.
- [72] GALINDO D, HERRANZ J, KILTZ E. On the generic construction of identity-based signatures with additional properties[C]//Advances in Cryptology-ASIACRYPT 2006. 2006: 178-193.
- [73] CAYREL P L, GABORIT P, GIRAULT M. Identity-based identification and signature schemes using correcting codes[C]//WCC. 2007: 69-78.

作者简介:



任方 (1981-), 男, 陕西西安人, 博士, 西安邮电大学副教授, 主要研究方向为密码学与信息安全。



郑东 (1964-), 男, 山西翼城人, 博士, 西安邮电大学教授、博士生导师, 主要研究方向为后量子密码及云计算安全技术。



范九伦 (1964-), 男, 河南焦作人, 博士, 西安邮电大学教授、博士生导师, 主要研究方向为信号与信息处理、信息安全。