



文章编号:1001-9081(2019)07-1997-04

DOI:10.11772/j.issn.1001-9081.2018122429

基于改进版 Niederreiter 的双公钥密码方案

王 众^{*}, 韩益亮

(武警工程大学 密码工程学院, 西安 710086)

(* 通信作者电子邮箱 408632006@qq.com)

摘要: 基于编码的密码体制可以有效地抵抗量子计算攻击, 具有较好的可操作性以及数据压缩能力, 是后量子时代密码方案的可靠候选者之一。针对量子时代中计算机数据的安全保密问题, 对编码密码中的 Niederreiter 密码方案改进版进行深入研究, 提出了一种与双公钥加密方式相结合的密码方案。所提方案的安全性相比 Niederreiter 方案改进版以及基于准循环低密度奇偶校验码(QC-LDPC)的 Niederreiter 双公钥加密方案得到提升, 在密钥量方面相比传统 Niederreiter 密码方案的公钥量至少下降了 32%, 相比基于 QC-LDPC 码的 Niederreiter 双公钥加密方案也有效下降, 在量子时代保证计算机数据安全表现出较强的可靠性。

关键词: 编码密码; Niederreiter 密码体制; 系统码; 安全性分析; 效率分析

中图分类号: TP309.7 文献标志码:A

Dual public-key cryptographic scheme based on improved Niederreiter cryptosystem

WANG Zhong^{*}, HAN Yiliang

(College of Cryptology Engineering, Engineering University of PAP, Xi'an Shaanxi 710086, China)

Abstract: The code-based cryptosystem can effectively resist quantum computing attacks with good operability and data compression capability, and is one of the reliable candidates for the post-quantum era cryptographic scheme. Aiming at the security and confidentiality of computer data in the quantum era, the in-depth study of an improved Niederreiter cryptographic scheme in code-based cryptography was carried out, and a cryptographic scheme with combination of dual public-key encryption method was proposed. The security of the proposed scheme was improved compared with the improved Niederreiter scheme and the Niederreiter dual public-key cryptographic scheme based on Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) code. The amount of keys in the scheme is at least 32% lower than that of traditional Niederreiter scheme, and is also effectively reduced compared with that of the Niederreiter dual public-key cryptographic scheme based on QC-LDPC code, which shows the strong reliability for ensuring computer data security in the quantum age.

Key words: code-based cryptography; Niederreiter cryptosystem; system code; security analysis; efficiency analysis

0 引言

量子技术的概念近来越来越多地进入人们的视线, 量子技术的计算能力在给人们带来计算性能很强的并行计算、解决许多棘手问题的同时, 也构成了不容忽视的安全威胁。密码学中的传统公钥密码在量子计算机出现后不会再像现在那么安全可靠, 比如基于经典数论理论的 RSA(Rivest-Shamir-Adleman)公钥加密算法、椭圆曲线密码(Elliptic Curve Cryptography, ECC)、属性基密码等, 将会在量子计算机出现后不再可靠^[1]。目前可以较为有效地抵抗量子计算攻击的密码体制主要有以下四种: 基于编码的密码体制、基于格的密码体制 LWE(Learning With Errors)、基于 Hash 函数的密码体制以及基于多变量的密码体制。基于编码的密码体制具有较高的计算效率以及可操作性, 是量子时代一种可靠的安全选择。

基于编码的公钥密码体制是在有限域上多元多项式环上定义和运算的, 此类密码体制的算法核心是对一种纠错码 C 的应用, 主要的特征即为添加一个错误到码字中或根据码 C 的校验矩阵计算伴随式。1978 年, 美国科学家 McEliece^[2]第一个运用这种方法设计公钥密码算法, 提出首个基于编码理论的公钥加密方案, 其中私钥为一个二元不可约 Goppa 码, 公

钥为该码的生成矩阵被随机化处理之后的结果。1986 年, Niederreiter^[3]提出了著名的基于 Goppa 码的 Niederreiter 密码体制。该方案的安全性被证明是与 McEliece 体制是相同的, Niederreiter 体制的主要思想是从另一个角度利用随机线性码的译码困难问题, 该方案隐藏的是 Goppa 码的校验矩阵, Niederreiter 体制相比 McEliece 体制, 公钥存储量有所下降, 而且具有更高的传信率。2018 年, 刘相信等^[4]提出了一种对 Niederreiter 公钥密码系统的改进, 可以隐藏明文的汉明重量来有效抵抗信息集译码(Information Set Decoding, ISD)攻击等针对编码密码体制的攻击, 但是其安全性仍然可以在保障效率的前提下得到进一步提升。到目前的研究阶段, 基于编码理论的公钥密码学的研究重点主要放在了对码的选择上, 以保证安全性的同时, 提高实用性, 降低方案的密钥尺寸, 由最开始的 Goppa 码、Reed-Solomon 码^[5], 到现在的准循环中密度奇偶校验(Quasi-Cyclic Medium-Density Parity-Check, QC-MDPC)码^[6]、低密度奇偶校验(Low Density Parity Check, LDPC)码^[7]以及准循环低密度奇偶校验(Quasi-Cyclic Low-Density Parity-Check, QC-LDPC)码^[8]等, 通过不断优化码的选择, 编码密码的公钥量切实得到有效减少, 但是安全性并没有得到明显的提升。

收稿日期:2018-12-10;修回日期:2019-02-06;录用日期:2019-03-21。基金项目:国家自然科学基金资助项目(61572521)。

作者简介:王众(1995—),男,山东泰安人,硕士研究生,主要研究方向:抗量子密码; 韩益亮(1977—),男,甘肃会宁人,教授,博士生导师,博士,主要研究方向:抗量子密码。



双公钥的思想是对明文进行二次加密,这种方法可以很好地提高公钥密码体制的安全性。2008年,张颖等^[9]就曾利用双公钥对 McEliece 体制进行改进,使安全性有较好的提升,但是毕竟使用了双公钥的方式加密,会使得密钥量增加,实用性不强。2016年,李冲等^[10]提出了基于 QC-LDPC 码的双公钥 Niederreiter 密码方案,由于 QC-LDPC 码的采用,能够使得双公钥方案的密钥量有所下降,安全性有较高提升,但是,密钥量和安全性仍有较大的提升空间。本文尝试将 Niederreiter 体制的改进版与双公钥的加密方式相结合,并采用系统码,在增加方案安全性的同时,保证有效的实用性。

1 相关工作

1.1 SDP 问题

校验子译码问题(Syndrome Decoding Problem, SDP) 给定一个 (n, k) 的线性码,它的最小汉明距离为 d ,该码的校验矩阵为 $\mathbf{H} \in F_2^{(n-k) \times n}$,它的纠错能力为 t 且 t 满足方程 $d = 2t + 1$ 。当给定一个向量 $\mathbf{v} \in F_2^{(n-k) \times n}$ 时,寻找一个错误向量 $\mathbf{e} \in F_2^n$,它的汉明重量要小于等于 t ,且与向量 \mathbf{v} 以及矩阵 \mathbf{H} 满足方程 $\mathbf{v} = \mathbf{e}\mathbf{H}^T$,寻找错误向量 \mathbf{e} 这个问题已被证明为 NP 困难问题^[11]。

1.2 Niederreiter 密码方案改进版

2018年,刘相信等^[4]提出的 Niederreiter 密码方案改进版,对错误向量 \mathbf{e} 的重量进行了隐藏,使得方案可以较好地抵抗 ISD 攻击,为使改进版方案与双公钥加密方法易于结合,对改进版方案中的随机可逆矩阵的选择变为可逆置换矩阵 \mathbf{T} ,具体方案描述如下。

1) 密钥生成。选择二元 (n, k, t) Goppa 码,纠错能力为 t ,其校验矩阵 \mathbf{H} 为 $(n - k) \times n$ 维,快速译码算法 $\beta_{\mathbf{H}, t}(\cdot)$,将 \mathbf{H} 随机拆分成两个矩阵 $\mathbf{H}_1, \mathbf{H}_2$ 且 $\mathbf{H} = \mathbf{H}_1 + \mathbf{H}_2$,随机选取三个维度为 $(n - k) \times (n - k)$ 可逆矩阵 $\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3$,随机选取一个 $n \times n$ 维的可逆置换矩阵 \mathbf{T} ,分别计算 $\mathbf{H}' = \mathbf{S}_1 \mathbf{H}_1 \mathbf{T}, \mathbf{H}'' = \mathbf{S}_2 \mathbf{H}_2 \mathbf{T}, \mathbf{H}''' = \mathbf{S}_3 \mathbf{H} \mathbf{T}$,将 $(\mathbf{H}', \mathbf{H}'', \mathbf{H}''', t)$ 作为公钥,而 $(\mathbf{S}_1, \mathbf{S}_2, \mathbf{S}_3, \mathbf{T}, \beta_{\mathbf{H}, t}(\cdot))$ 作为私钥。

2) 加密过程。首先将明文 \mathbf{m} 编码成 $GF(2)$ 上的汉明重量 t 的 n 维向量 \mathbf{e} ,并将 \mathbf{e} 拆分为两个向量 $\mathbf{e}_1, \mathbf{e}_2$,且 $\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2$, $wt(\mathbf{e}_1) = t_1, wt(\mathbf{e}_2) = t_2 (t \neq t_1 \neq t_2)$ 。进行运算可得三个密文, $\mathbf{c}_1 = \mathbf{e}_1 \mathbf{H}'^T, \mathbf{c}_2 = \mathbf{e}_1 \mathbf{H}''^T, \mathbf{c}_3 = \mathbf{e}_2 \mathbf{H}'''^T$,将 $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ 作为最后的密文发送给接收者。

3) 解密过程。收到 $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$ 后,进行如下操作:

$$\mathbf{c}_1 \mathbf{S}_1^{-1T} = \mathbf{e}_1 \mathbf{H}'^T \mathbf{S}_1^{-1T} = \mathbf{e}_1 \mathbf{T}^T \mathbf{H}_1^T \quad (1)$$

$$\mathbf{c}_2 \mathbf{S}_2^{-1T} = \mathbf{e}_1 \mathbf{H}''^T \mathbf{S}_2^{-1T} = \mathbf{e}_1 \mathbf{T}^T \mathbf{H}_2^T \quad (2)$$

$$\mathbf{c}_3 \mathbf{S}_3^{-1T} = \mathbf{e}_2 \mathbf{H}'''^T \mathbf{S}_3^{-1T} = \mathbf{e}_2 \mathbf{T}^T \mathbf{H}^T \quad (3)$$

由上述两个过程可知, $\mathbf{H} = \mathbf{H}_1 + \mathbf{H}_2, \mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2$,因此, $\mathbf{c}_1 \mathbf{S}_1^{-1T} + \mathbf{c}_2 \mathbf{S}_2^{-1T} + \mathbf{c}_3 \mathbf{S}_3^{-1T} = \mathbf{e} \mathbf{T}^T \mathbf{H}^T$,利用译码算法 $\beta_{\mathbf{H}, t}(\cdot)$ 进行译码可得 $\mathbf{e} \mathbf{T}^T$,再利用私钥 \mathbf{T} ,即可得到密文 $\mathbf{e} = \mathbf{e} \mathbf{T}^T \mathbf{T}^{T-1}$ 。

通过上述对 Niederreiter 密码方案改进版的阐述,可以发现许多针对 Niederreiter 方案的攻击方法例如像 ISD 攻击等的代价由于对重量 t 进行隐藏后变得较大,正是由于 t 的选择变得灵活后,那么在选码时便可选择适当的维度来避免密钥量过大,具体分析请参考文献[4],但文献[4]若采用双公钥的加密方法能进一步加强方案的安全性,并通过选取系统码来进行构造,避免方案的密钥量过大,增加方案的实用性。

2 基于改进版 Niederreiter 的双公钥密码方案

2.1 参数生成

选取两个二元即约系统码 G_1, G_2 维度分别为 (n, k) 和 $(n - k, k)$,纠错能力分别为 t_1, t_2 ,两个码对应的校验矩阵为

$(n - k) \times n$ 维的 \mathbf{H}_1 和 $(n - k) \times (n - k)$ 维的 \mathbf{H}_2 ,且 \mathbf{H}_2 可以拆分为 $\mathbf{H}_2 = \mathbf{H}_3 + \mathbf{H}_4$,其中矩阵 $\mathbf{H}_3, \mathbf{H}_4$ 为随机拆分得到的。两个码的译码算法为 $\beta_{1, H_1}(\cdot)$ 和 $\beta_{2, H_2}(\cdot)$ 。随机选取一个 $(n - k) \times (n - k)$ 维可逆矩阵 \mathbf{S} ,与一个 $n \times n$ 的置换矩阵 \mathbf{T} ,并计算 $\bar{\mathbf{H}} = \mathbf{S} \mathbf{H}_1 \mathbf{T}$ 。再随机选择三个 $(n - 2k) \times (n - 2k)$ 的可逆矩阵 $\mathbf{A}, \mathbf{B}, \mathbf{C}$,以及 $(n - k) \times (n - k)$ 维的置换矩阵 \mathbf{Q} ,并计算 $\mathbf{H}' = \mathbf{A} \mathbf{H}_3 \mathbf{Q}, \mathbf{H}'' = \mathbf{B} \mathbf{H}_4 \mathbf{Q}, \mathbf{H}''' = \mathbf{C} \mathbf{H}_2 \mathbf{Q}$ 。公开密钥即为 $(\bar{\mathbf{H}}, \mathbf{H}', \mathbf{H}'', \mathbf{H}''', t_1, t_2)$,私钥即为 $(\mathbf{S}, \mathbf{T}, \mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{Q}, \beta_{1, H_1}(\cdot), \beta_{2, H_2}(\cdot))$ 。

2.2 加密过程

首先利用系统码 G_1 所产生的公钥 $\bar{\mathbf{H}}$ 对 n 维明文 \mathbf{m} 进行第一步加密,产生密文 $\mathbf{c}_1, \mathbf{c}_1 = \mathbf{m} \bar{\mathbf{H}}^T$ 。此处注意,在对 G_2 进行选择时,它的纠错能力 t_2 需要满足 $t_2 > wt(\mathbf{c}_1)$,以方便后面的译码解密,且这一点在选码时易于实现。

完成第一步后,进行第二步加密。将 \mathbf{c}_1 看作新的明文,用 G_2 所产生的一系列公钥对其进行加密。首先将进行拆分, $\mathbf{c}_1 = \mathbf{c}_2 + \mathbf{c}_3$,计算 $\mathbf{x}_1 = \mathbf{c}_2 \mathbf{H}'^T, \mathbf{x}_2 = \mathbf{c}_2 \mathbf{H}''^T, \mathbf{x}_3 = \mathbf{c}_3 \mathbf{H}'''^T$,将 $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ 作为密文,发送给接收者。

2.3 解密过程

当接收者收到密文 $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3)$ 后,进行以下解密操作。

1) 运用私钥 $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{Q}$ 以及译码算法 $\beta_{2, H_2}(\cdot)$,进行第一步解密。

$$\mathbf{x}_1 \mathbf{A}^{-1T} = \mathbf{c}_2 \mathbf{H}'^T \mathbf{A}^{-1T} = \mathbf{c}_2 \mathbf{Q}^T \mathbf{H}_3^T \quad (4)$$

$$\mathbf{x}_2 \mathbf{B}^{-1T} = \mathbf{c}_2 \mathbf{H}''^T \mathbf{B}^{-1T} = \mathbf{c}_2 \mathbf{Q}^T \mathbf{H}_4^T \quad (5)$$

$$\mathbf{x}_3 \mathbf{C}^{-1T} = \mathbf{c}_3 \mathbf{H}'''^T \mathbf{C}^{-1T} = \mathbf{c}_3 \mathbf{Q}^T \mathbf{H}_2^T \quad (6)$$

计算 $\mathbf{x}_1 \mathbf{A}^{-1T} + \mathbf{x}_2 \mathbf{B}^{-1T} + \mathbf{x}_3 \mathbf{C}^{-1T} = \mathbf{c}_1 \mathbf{Q}^T \mathbf{H}_2^T$,利用译码算法 $\beta_{1, H_1}(\cdot)$ 对 $\mathbf{c}_1 \mathbf{Q}^T \mathbf{H}_2^T$ 进行译码得到 $\mathbf{c}_1 \mathbf{Q}^T$,再利用私钥 \mathbf{Q} 进行运算得到 $\mathbf{c}_1 = \mathbf{c}_1 \mathbf{Q}^T \mathbf{Q}^{T-1}$ 。

2) 完成第一步解密得到 \mathbf{c}_1 后,第二步解密就是普通的 Niederreiter 密码体制的译码解密。运用私钥 \mathbf{S}, \mathbf{T} 和码 G_1 的译码算法 $\beta_{1, H_1}(\cdot)$ 进行解密,具体如下:

$$\mathbf{c}_1 \mathbf{S}^{-1T} = \mathbf{m} \bar{\mathbf{H}}^T \mathbf{S}^{-1T} = \mathbf{m} \mathbf{T}^T \mathbf{H}_1^T \quad (7)$$

利用译码算法 $\beta_{1, H_1}(\cdot)$ 对 $\mathbf{m} \mathbf{T}^T \mathbf{H}_1^T$ 译码即可得到 $\mathbf{m} \mathbf{T}^T$,利用私钥 \mathbf{T} 进行运算得到 $\mathbf{m} = \mathbf{m} \mathbf{T}^T \mathbf{T}^{T-1}$ 。

从上述的加解密过程可以看出,加密时,先对明文进行传统的 Niederreiter 加密,得到密文后,采用改进版 Niederreiter 再进行加密。解密时,先对改进版 Niederreiter 解密得到第一次加密的密文,再利用传统的 Niederreiter 解密方式进行解密得到最后的明文即可。

3 安全性分析

3.1 直接攻击

所谓直接攻击,是指在拥有密文 \mathbf{c} 和公钥 $\bar{\mathbf{H}}$ 后,通过直接求解方程 $\mathbf{c} = \mathbf{m} \bar{\mathbf{H}}^T$ 来求得明文的攻击方法,但是 Niederreiter 密码体制所依赖的是 SDP 校验子译码问题,该问题为 NP 困难问题,因此直接通过方程来求解明文 \mathbf{m} 是十分困难的。本文方案采用了双公钥的加密方法,使得破解的工作量至少翻倍,又由于第二次加密采用了改进的 Niederreiter 密码体制,使得安全性又有了新的提升。

3.2 直接译码攻击

直接译码攻击是指通过公钥 $\bar{\mathbf{H}}, \mathbf{H}', \mathbf{H}'', \mathbf{H}'''$ 得到 $\mathbf{S}, \mathbf{H}_1, \mathbf{T}$ 和 \mathbf{A}, \mathbf{H}_3 与 \mathbf{B}, \mathbf{H}_4 以及 \mathbf{C}, \mathbf{H}_2 和 \mathbf{Q} ,然后通过码的快速译码算法得到明文 \mathbf{m} 来攻破该体制。由矩阵的相关理论可以得知,矩阵的分解不是唯一的,比如像从矩阵 \mathbf{H} 中分解出 $\mathbf{S}, \mathbf{H}_1, \mathbf{T}$,它们各自可能的个数分别为 $2^{(n-2k)^2} \prod_{i=1}^{n-2k} (1 - 2^{-i})$ 、 $\frac{1}{t^2} n^{t^2}$ 和 $(n - k)!$,由此可见,当 n 和 t 的取值比较大时,矩阵可能的数



目十分巨大,这导致敌手在多项式时间内是难以通过公钥分解出私钥的,而本文方案有4个公钥矩阵,工作量会变为4倍,相比 Niederreiter 方案改进版^[4]的三个公钥矩阵和基于 QC-LDPC 码的 Niederreiter 双公钥加密方案^[11]的两个矩阵,工作量加倍,安全性增强。

3.3 信息集译码(ISD)攻击

李元兴等^[12]指出,可以通过解线性方程组的方法来攻破 Niederreiter 密码体制。所谓信息集译码攻击即 ISD 攻击是指:给定明文 $\mathbf{m} = (m_1, m_2, \dots, m_n)$,以及加密方程 $\mathbf{c} = \mathbf{m}\mathbf{H}^T$,任意选择明文 $\mathbf{m} = (m_1, m_2, \dots, m_n)$ 中的 k 个分量,并将其删除,并相应删除公钥矩阵 \mathbf{H} 中的 k 列,那么可得到新的方程即为 $\mathbf{c} = \mathbf{m}_{1 \times (n-k)} \mathbf{H}_{(n-k) \times (n-k)}^T$,此时,若矩阵 $\mathbf{H}_{(n-k) \times (n-k)}^T$ 可逆,那么可求得 $\mathbf{m}_{1 \times (n-k)} = \mathbf{c} \times \mathbf{H}_{(n-k) \times (n-k)}^{T^{-1}}$,然后查看 $wt(\mathbf{m}_{1 \times (n-k)})$ 是否为公开的汉明重量 t ,若为 t ,则在相应的 k 个位置上补零即可得到最后的明文 \mathbf{m} 。当矩阵 $\mathbf{H}_{(n-k) \times (n-k)}^T$ 不可逆或者最后求得的 $\mathbf{m}_{1 \times (n-k)}$ 的汉明重量不符合要求时,需要重新选择矩阵 $\mathbf{H}_{(n-k) \times (n-k)}^T$ 进行以上运算。ISD 攻击对于编码密码来说是一种较为强力的攻击方法,并且还被不断深化与研究^[13-17]。在文献[18]中,已经证明采用双公钥方式进行两次普通 Niederreiter 加密的方法可以有效抵抗此类攻击,攻击成功的工作因子为 $W = [(n-k)^3 C_{n-k-t_2}^k / C_n^k] \cdot [(n-2k)^3 C_{n-t_1}^k / C_{n-t_1}^k]$,因此当 n, t 选取较大时攻击者在多项式时间内难以攻破双公钥的 Niederreiter 密码体制。

本文采用双公钥的 Niederreiter 加密方式,在第一次加密时是采用的普通的 Niederreiter 密码方案,第二次加密时则是采用的改进的 Niederreiter 密码方案。改进的 Niederreiter 密码体制的最大特点就是对加密的消息 \mathbf{c}_1 的汉明重量进行了隐藏,将其进行了拆分,成为了两部分 $\mathbf{c}_1 = \mathbf{c}_2 + \mathbf{c}_3$,并相应地将校验矩阵 \mathbf{H}_2 进行了拆分 $\mathbf{H}_2 = \mathbf{H}_3 + \mathbf{H}_4$,与拆分后的明文进行加密运算。采用 ISD 攻击的一个关键所在就是要掌握明文的汉明重量,这样才能确认是否攻击成功。改进的 Niederreiter 密码体制加密后的密文为 $\mathbf{x}_i = \mathbf{c}_i \mathbf{H}^T$ 的形式,并非 \mathbf{c}_i ,那么 \mathbf{c}_i 的汉明重量也就更加灵活,取值范围从 0 到 $n-k$,那么攻击者也就不能判断 $wt(\mathbf{x}_i \mathbf{H}_{(n-2k) \times (n-2k)}^{T^{-1}})$ 是否符合要求,因此,对于一个汉明重量为 t_i 的加密信息 $\mathbf{c}_i = (\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_{n-k})$,右乘一个 $(n-k) \times (n-2k)$ 的矩阵 \mathbf{H}^T ,相当于在 \mathbf{H}^T 中选取相应的 t_i 行,而 $0 \leq t_i \leq n-k$,因此,采用解线性方程组攻击第二次加密的代价为 $C_{n-k}^0 + C_{n-k}^1 + C_{n-k}^2 + \dots + C_{n-k}^{n-k-1} + C_{n-k}^{n-k} = 2^{n-k}$ 。综上可知,ISD 攻击针对基于改进版 Niederreiter 的双公钥密码方案的工作因子为 $W = 2^{n-k} \cdot [(n-k)^3 C_{n-k-t_2}^k / C_n^k]$,相比于基于 QC-LDPC 码的双公钥 Niederreiter 密码方案^[11]有较大提升。Niederreiter 改进版^[4]只有一次加密的过程,它的工作因子为 $C_{n-k}^0 + C_{n-k}^1 + C_{n-k}^2 + \dots + C_{n-k}^{n-k-1} + C_{n-k}^{n-k} = 2^{n-k}$,从上面对本文方案工作因子的分析可以看出,二次加密的信息为第一次加密的密文,因此安全性较其有较大的提升。

4 效率分析

4.1 系统码优势

采用双公钥的加密方式,可以有效地提高系统的安全性;但是也会存在一个较为明显的弊端,就是密钥量的增加,而密钥量对于基于编码的密码体制而言,本身就是一个缺陷。Niederreiter 密码体制在相同的安全性下相比 McEliece 体制的密钥量有所减少;但是相对传统的公钥密码像背包密码等,它的密钥量还是很大。如何有效提高编码密码体制的效率,减小公钥量是个至关重要的问题。目前基于编码理论的公钥密码学研究的重点主要放在了对码的选择上,由最开始的

Coppa 码、Reed-Solomon 码,到现在的 QC-MDPC 码、LDPC 码以及 QC-LDPC 码等,来减少编码密码的公钥量。本文方案就采用系统码来有效减少密钥量。

系统码的生成矩阵或者校验矩阵,可以通过一系列行列变换变换为 $\mathbf{G} = (\mathbf{I}_k | \mathbf{Q})$ 或 $\mathbf{H} = (-\mathbf{Q}^T | \mathbf{I}_{n-k})$,其中 \mathbf{Q} 为一个 $k \times (n-k)$ 阶的矩阵,那么它的转置即为 $(n-k) \times k$ 阶矩阵,而矩阵 \mathbf{I}_k 与 \mathbf{I}_{n-k} 均为单位矩阵,由此,可以看出,系统码在存储时,只需对 $k \times (n-k)$ 阶的矩阵 \mathbf{Q} 或 $(n-k) \times k$ 阶矩阵 $-\mathbf{Q}^T$ (负号代表矩阵中的元素为其逆元)进行存储即可,若不采用系统码构造,则需对 $k \times n$ 阶矩阵或 $(n-k) \times n$ 阶矩阵进行存储。在本文方案中,有四个公开的密钥矩阵 $\bar{\mathbf{H}}, \mathbf{H}', \mathbf{H}'', \mathbf{H}'''$,除了矩阵 \mathbf{H} 的维度为 $(n-k) \times n$ 阶,其余三个矩阵均为 $(n-2k) \times (n-k)$ 阶,在采用系统码后,对 \mathbf{H} 进行存储的维度为 $(n-k) \times k$ 阶,对 \mathbf{H}''' 进行存储的维度为 $(n-2k) \times k$ 阶,而对 $\mathbf{H}', \mathbf{H}''$ 进行存储的维度与 \mathbf{H}''' 的维度不同,是因为 \mathbf{H}''' 由系统码 G_2 的校验矩阵 \mathbf{H}_2 通过行列变换得到的,可以节约存储,而 $\mathbf{H}', \mathbf{H}''$ 是由系统码 G_2 的校验矩阵 \mathbf{H}_2 进行拆分得到的 \mathbf{H}_3 、 \mathbf{H}_4 通过行列变换得到, $\mathbf{H}_3, \mathbf{H}_4$ 未必满足系统码的性质,因此 $\mathbf{H}', \mathbf{H}''$ 的维度仍为 $(n-2k) \times (n-k)$ 阶。以 $n = 1024, k = 1024 - 10t, t = 55$ 为例,普通 Niederreiter 密码体制所存储公钥矩阵的尺寸为 $p_1 = (n-k) \times n = 56.32 \times 10^4$,而本文的双公钥 Niederreiter 密码方案的公钥尺寸为 $p_2 = (n-k) \times k + (n-2k) \times k + 2 \times (n-2k) \times (n-k) = 38.03 \times 10^4$ 。由该例子可以看出,本文的双公钥 Niederreiter 密码方案由于系统码的采用不仅保证了安全性的提升,并有效降低了 32% 的公钥量。表 1 为本文方案密钥尺寸与改进版 Niederreiter 密码方案进行比较。

改进版 Niederreiter 由于可对重量 t 进行隐藏,因此只需选取一个维度较小的码字,而本文方案第二步采用的是改进版 Niederreiter,因此可以选择维度较小的系统码,第一步选择一个符合第 2 章描述的系统码即可,因此相比改进版 Niederreiter,密钥量只多在一个系统码上。由表 1 可以看出,本文方案由于采用的是系统码,因此选择两个码后,密钥尺寸会有一定增加,但是在合理范围内,并获得更高的安全性。具体的安全性优势已在第 3 章中进行了分析。

表 1 两种方案的代价和密钥尺寸对比

Tab. 1 Cost and key size comparison of two schemes

方案	参数选取	ISD 攻击方案代价	密钥尺寸/b
改进版 Niederreiter	(80, 40)	2^{80}	9 600
本文方案	(120, 40) 和 (80, 40)	$> 2^{80}$	11 200

4.2 重量 t 优势

本文的双公钥 Niederreiter 密码方案另一个优势特点就是在第二步加密时采用的改进版 Niederreiter 密码方案,如 3.3 节所述,它可以很好地将加密信息的汉明重量进行隐藏,所达到的效果就是使得 ISD 攻击的代价对于 (n, k, t) 维的码为 $C_n^0 + C_n^1 + C_n^2 + \dots + C_n^{n-1} + C_n^n = 2^n$,这相比传统 Niederreiter 密码方案在安全性方面有很大的提升。为了提高方案的使用效率,就可以考虑在选码时降低汉明重量 t 的选择,没有必要再去选择 t 过大的码,而可以达到同样的安全性要求,这就相比基于 QC-LDPC 码的双公钥 Niederreiter 密码方案^[10]在选择码时可以减小码的维度,以达到降低公钥尺寸的目的。将第二步加密时的选码与基于 QC-LDPC 码的双公钥 Niederreiter 密码方案^[10]的第二步选码进行比较,结果如表 2 所示。

由表 2 可以看出,本文方案相比 QC-LDPC 码方案可以选择较小维度的码字以达到同 QC-LDPC 码方案同样的安全级



别,使得公钥的尺寸有很大幅度的下降,如表1中在80 b安全级下,本文方案密钥尺寸为5 040 b而QC-LDPC码方案为28 408 b。

表2 两种方案的第二步加密密钥尺寸对比

Tab. 2 Comparison of the second-step encryption key size of two schemes

参数选取(n, k, t)		ISD 攻击代价		QC-LDPC 方案密钥尺寸	本文方案密钥尺寸
QC-LDPC 方案	本文方案	QC-LDPC 方案	本文方案	$(n-k) \times k/b$	$3(n-k) \times k/b$
(346, 212, 48)	(82, 42, 20)	2^{80}	2^{82}	28 408	5 040
(546, 396, 59)	(128, 68, 30)	2^{130}	2^{128}	59 400	12 240

由于最后的密文是由 G_2 码的公钥产生,因此 G_1 码在选择时也可以选择较小的汉明重量 t ,而不会影响到整个双公钥体系的安全,但是 G_1 、 G_2 码的选择由于解密时还要考虑译码问题,如2.2节所述,需要结合实际情况进行选择。结合4.1节的分析,可以看出本文的双公钥Niederreiter密码方案不仅安全性得到较大的提升,而且公钥尺寸相比基于QC-LDPC码的双公钥Niederreiter密码方案有效下降,相比传统的Niederreiter密码方案至少下降了32%,能够在更多的场景中有效运用。

5 结语

基于编码的密码体制是抗量子计算时代的优良候选者之一,双公钥的加密方式旨在增加密码方案的安全性。本文对改进版Niederreiter密码方案以及双公钥加密方式进行深入研究,将二者进行结合,并采用系统码,提出了一个双公钥Niederreiter密码方案。本文方案在安全性方面相比改进版Niederreiter得到显著提升,可以良好地抵抗ISD等针对编码密码体制的攻击。本文方案在公钥量方面,相比Niederreiter密码方案至少下降了32%,而相比基于QC-LDPC码的双公钥Niederreiter密码方案也有效降低。优良的性质使得本文方案在今后的抗量子密码时代能够为计算机安全提供可靠的安全保障,但是需要注意的一点便是在选择系统码时要结合实际情况以及应用场景选择合适的参数,以保证方案的正确性。

参考文献 (References)

- [1] 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.
- [2] McELIECE R J. A public-key cryptosystem based on algebraic coding theory [J]. DSN Progress Report, 1978, 42(44): 114–116.
- [3] NIEDERREITER H. Knapsack-type cryptosystems and algebraic coding theory [J]. Problems of Control and Information Theory, 1986, 15(2): 159–166.
- [4] 刘相信,杨晓元. Niederreiter公钥密码方案的改进[J]. 计算机应用, 2018, 38(7): 1956–1959. (LIU X X, YANG X Y. Improvement of the Niederreiter public key system [J]. Journal of Computer Applications, 2018, 38(7): 1956–1959.)
- [5] 张俊. 编码的构造与译码问题及其在密码学中的应用[D]. 天津: 南开大学, 2014: 23–39. (ZHANG J. The problem of coding construction and decoding and its application in cryptography [D]. Tianjin: Nankai University, 2014: 23–39.)
- [6] 李泽慧, 杨亚涛, 李子臣. 基于QC-MDPC码的公钥密码方案设计[J]. 计算机应用研究, 2015, 32(3): 881–884. (LI Z H, YANG Y T, LI Z C. Design of public key cryptography based on QC-MDPC code [J]. Application Research of Computers, 2015, 32(3): 881–884.)
- [7] 曹东, 赵生妹, 宋耀良. 一种基于量子准循环LDPC码的McEliece公钥密码算法[J]. 南京邮电大学学报(自然科学版), 2011, 31(2): 64–68. (CAO D, ZHAO S M, SONG Y L. A McEliece public key cryptography algorithm based on quantum quasi-cyclic LDPC Code [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2011, 31(2): 64–68.)
- [8] 王延丽. 基于QC-LDPC码的McEliece公钥密码体制研究[D]. 西安: 西安电子科技大学, 2013: 1–5. (WANG Y L. Research on McEliece public key cryptosystem based on QC-LDPC code [D]. Xi'an: Xidian University, 2013: 1–5.)
- [9] 张颖, 岳殿武. 基于代数几何码的公钥密码体制[J]. 通信学报, 2008, 29(6): 75–81. (ZHANG Y, YUE D W. Public key crypto-system based on algebraic geometry codes [J]. Journal on Communications, 2008, 29(6): 75–81.)
- [10] 李冲, 韩益亮. 基于QC-LDPC码的双公钥Niederreiter密码方案[J]. 计算机应用研究, 2016, 33(11): 3446–3449. (LI C, HAN Y L. Double public key Niederreiter cryptography scheme based on QC-LDPC code [J]. Application Research of Computers, 2016, 33(11): 3446–3449.)
- [11] 范武英, 任方. 基于校验子译码问题的伪随机序列研究综述[J]. 西安邮电大学学报, 2017, 22(2): 1–6. (FAN W Y, REN F. Review of pseudo-random sequence based on syndrome decoding problem [J]. Journal of Xi'an University of Posts and Telecommunications, 2017, 22(2): 1–6.)
- [12] 李元兴, 王新梅. 关于代数码Niederreiter公钥密码体制的安全性及参数优化[J]. 电子学报, 1993, 21(7): 33–36. (LI Y X, WANG X M. On the security and parameter optimization of algebraic Niederreiter public key cryptography [J]. Acta Electronica Sinica, 1993, 21(7): 33–36.)
- [13] PRANGE E. The use of information sets in decoding cyclic codes [J]. IRE Transactions on Information Theory, 1962, 8(5): 5–9.
- [14] MAY A, OZEROV I. On computing nearest neighbors with applications to decoding of binary linear codes [C]// EUROCRYPT 2015: Proceedings of the 2015 Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 203–228.
- [15] 李梦东, 蔡坤锦, 邵玉芳. 信息集攻击算法的改进[J]. 密码学报, 2016, 3(5): 505–515. (LI M D, CAI K J, SHAO Y F. An improved algorithm of information set decoding [J]. Journal of Cryptologic Research, 2016, 3(5): 505–515.)
- [16] TORRES R C, SENDRIER N. Analysis of information set decoding for a sub-linear error weight [C]// PQCrypto2016: Proceedings of the 2016 International Workshop on Post-Quantum Cryptography. Berlin: Springer, 2016: 144–161.
- [17] KACHIGAR G, TILLICH J P. Quantum information set decoding algorithms [C]// PQCrypto 2017: Proceedings of the 2017 International Workshop on Post-Quantum Cryptography. Berlin: Springer, 2017: 69–89.
- [18] 杨磊鑫, 杜伟章. 利用双公钥的Niederreiter公钥密码体制的改进[J]. 长沙理工大学学报(自然科学版), 2010, 7(4): 74–77. (YANG L X, DU W Z. Improvement of Niederreiter public key cryptosystem using double public key [J]. Journal of Changsha University of Science and Technology (Natural Science), 2010, 7(4): 74–77.)

This work is partially supported by the National Natural Science Foundation of China (61572521).

WANG Zhong, born in 1995, M. S. candidate. His research interests include anti-quantum cryptography.

HAN Yiliang, born in 1977, Ph. D., professor. His research interests include anti-quantum cryptography.