•可信计算与信息安全•

DOI:10.15961/j.jsuese.201700627

基于量子BCH码的McEliece及Niederreiter公钥密码算法研究

韩海清[1,2], 张焕国[2], 赵　波[2], 王后珍[2]

(1.湖北理工学院 数理学院, 湖北 黄石 435003; 2.武汉大学 计算机学院, 湖北 武汉 430072)

摘　要:针对量子计算攻击对传统密码体制的安全威胁,设计出一类抗量子攻击的McEliece公钥密码体制,因为量子计算没有攻击McEliece公钥密码体制的多项式时间算法。给出了3类量子BCH码的生成算法,第1类是一般性量子BCH码生成算法,第2类是特殊的对称量子BCH码生成算法,第3类是特殊的非对称量子BCH码生成算法。以本文生成的非对称量子BCH码为基础,设计出量子McEliece公钥密码体制和量子Niederreiter公钥密码体制,详细给出这两种公钥体制的加密和解密过程。给出的密码体制既保留了抗量子计算优点,又能在量子态下加密和解密,其基本域为任意有限域。分析了这两种体制的计算复杂性理论、数据结构及算法模式,得到了时间复杂性和空间复杂性达到指数级,得到了抵抗Shor算法和Grover算法攻击的结果。最后,利用量子BCH码的结构特征,设计了一种经典Niederreiter体制数字签名,具有抗量子攻击能力。

关键词:CSS构造; 量子BCH码; 基于纠错码公钥密码体制; 抗量子攻击; 数字签名

中图分类号:TN918.2　　**文献标志码**:A　　**文章编号**:2096-3246(2018)05-0152-08

Research on McEliece and Niederreiter Public-key Cryptosystem Algorithm Based on Quantum BCH Codes

HAN Haiqing[1,2], *ZHANG Huanguo*[2], *ZHAO Bo*[2], *WANG Houzhen*[2]

(1.School of Mathematics and Physics, Hubei Polytechnic Univ., Huangshi 435003, China;
2.School of Computer, Wuhan Univ., Wuhan 430072, China)

Abstract: In order to resist the security threat of quantum computing attacks to the traditional cryptosystem, a class of McEliece public-key cryptosystems was designed in this paper, based on the fact that no quantum computing algorithm can attack the McEliece public-key cryptosystem within polynomial time. Three types of algorithms for generating quantum BCH codes were presented. The first one was general quantum BCH code generation algorithm, the second one was special symmetric quantum BCH code generation algorithm, and the third one was special asymmetric quantum BCH code generation algorithm. Based on the asymmetric quantum BCH codes generated in this paper, the quantum McEliece public-key cryptosystem and the quantum Niederreiter public-key cryptosystem were designed, and the encryption and decryption processes of the two public-key systems were given in detail. The proposed cryptosystems not only retained the advantages of the post-quantum computation, but also can encrypt and decrypt in quantum states. The basic field has been extended to the arbitrary finite field. The computational complexity theory, data structure and algorithm model of the two public-key cryptosystems were analyzed. The exponential time and space complexity were obtained, and the results of resisting the attacks of Shor and Grover algorithms were also obtained. Finally, with the structural characteristics of quantum BCH codes, a classical Niederreiter signature system was designed, which has the ability of resisting quantum attacks.

Key words: CSS construction; quantum BCH codes; public-key cryptosystem on error correcting codes; post-quantum attacks; digital signatures

量子计算机有天然的并行优势,计算速度可达指数级,量子计算的典型代表是Shor算法和Grover算法[1]。量子计算机的出现,使得电子计算机难于计算和求解的困难问题变得易于求解。这对基于数学难题的密码,构成极大威胁。例如,利用量子计算可以在较短时间内进行大整数的因子分解,可用于攻击

收稿日期:2017 – 08 – 05

基金项目:国家自然科学基金重点项目资助(2014CB340600); 湖北省教育厅重点项目资助(D20174502; B2014041); 湖北省科技厅项目资助(2018CFB550)

作者简介:韩海清(1979—),男,副教授,博士. 研究方向:信息安全. E-mail: hanhaiqing@whu.edu.cn

网络出版时间:2018 – 08 – 31 20 : 03 : 55　　**网络出版地址**:http://kns.cnki.net/kcms/detail/51.1773.tb.20180831.2003.001.html

RSA密码；利用量子计算易于求解离散对数，可对ELGamal密码和ECC密码进行攻击。美国Bell实验室提出的Grover算法和Shor算法，在量子计算机上，在多项式时间内攻破很多现有密码。尤其是Shor算法，利用量子Fourier变换具有计算加速功能这一优点，对能够规约为隐藏子群（HSP）的问题进行有效计算[2]。量子计算机的原理是利用量子并行、相干叠加和纠缠态等量子特性进行快速计算，但在实际应用中，相干叠加和纠缠态都很脆弱，难以保持，易与外部环境相互作用，产生量子消相干。量子纠错码是克服量子消相干的有效途径之一。

一些研究者们试图从经典数学纠错码着手，利用CSS构造思想构造量子纠错码，利用量子纠错码设计新的密码体制以对抗量子计算攻击。关于抗量子密码算法，国内外学者的研究主要集中在以下5个方面[3]：1）Merkle树签名方案，也被称为Hash函数方案；2）基于纠错码的密码方案，也被称为McEliece体制；3）基于格上困难问题的密码；4）MQ密码方案；5）研究现有安全强度高的对称密码，分析其抗量子计算能力。其中，McEliece体制是基于经典纠错码的纠错门陷设计出的密码，能较好地抗量子攻击。

关于量子编码与密码的研究报道有很多。例如，Jin[4–6]、Xu[7]等研究了量子纠错码，Chuang等[8]研究了量子数字签名，Ablayev等[9]研究了量子Hash函数，Bennett等[10]研究了量子秘钥分配问题，Zeng[11]研究了量子认证问题，Toyran[12]、Okamoto[13]、Wieschebrink[14]等提出了量子公钥密码问题。第1个McEliece公钥体制是1978提出的[15]，随后的多年研究表明，适当调整这种密码体制的参数后，量子计算也不能对其构成严重威胁，但这种体制的缺点是存储空间很大。1986年，Niederreiter提出了一种背包型的纠错码公钥体制，之后Li等[16]证明了其与McEliece公钥体制的安全性等价。有关McEliece和Niederreiter公钥密码体制的具体内容详见文献[3]。2011年，曹东等[17]利用QC-LDPC码设计二元McEliece公钥密码体制，并进行了仿真实验。

上述关于量子纠错码的研究，没有给出量子纠错码的生成算法。在设计抗量子计算攻击的公钥密码体制时，主要利用二元经典纠错码设计抗量子攻击的公钥体制。

作者先生成量子BCH码，利用量子BCH码设计量子McEliece公钥体制，且量子态包括二元和非二元情形。作者给出了3类典型的量子BCH码生成算法，第1类生成算法生成量子BCH码数目多，另外两类算法效率更高。相对于已有的一些抗量子计算加密算法，本文算法优势在于加解密时不需要经典态和量子态相互转换，提高了计算效率，同时，将量子态从二元推广到任意元。对加密算法从时间复杂性、空间复杂性、数据结构和算法模式上进行安全性分析，得到了抵抗Shor算法和Grover算法攻击的结果。利用生成的大量量子BCH码设计了抗量子计算的数字签名，给出了量子纠错码的一种应用。

1　量子BCH码的CSS构造算法

量子纠错码与经典纠错码相比在纠错方面有3点不同之处：一是，量子编码时，将单个量子比特态编成纠缠态，起冗余作用；二是，量子错误可以看成3种Pauli算子的线性组合，这3种算子对应3种量子错误，即量子比特翻转、量子相位翻转、量子比特和相位同时翻转；三是，量子纠错时，将错误对应到不同的正交Hilbert空间。下面将给出量子纠错码的定义。

1.1　量子纠错码

定义1　一个q元量子码Q记为$[[n,k,d]]_q$，是指Hilbert空间$C^{q^n}=C^q\otimes C^q\otimes\cdots\otimes C^q$（$n$个$C^q$的直积）的$q^k$维子空间成为量子纠错码$Q=C^q\otimes C^q\otimes\cdots\otimes C^q$（$k$个$C^q$的直积），能够纠正至多$t=\lfloor(d-1)/2\rfloor$个量子错误。

一个经典线性码是有限域上线性子空间，$C^{\perp}$表示Euclidean正交下码C的对偶码，$D^{\perp_H}$表示Hermitian内积下码D的对偶码。在构造量子码时，需要用到有限域F_q具有性质$C^{\perp}\subset C$的经典码，或有限域F_{q^2}上具有性质$D^{\perp_H}\subseteq D$的经典码，这两类码统称C和D为偶包含码。关于线性码的参数关系请参考文献[18]。

1.2　量子BCH码生成算法

作者主要利用量子BCH码实现McEliece加密体制，量子纠错码的生成算法主要基于CSS构造思想[19]。下面给出3类量子BCH码的构造方法。第1类生成算法主要指算法1和算法2，可以很全面地生成量子BCH码，由于分圆陪集选取较为复杂，所以该类算法效率不高；后两类生成算法生成的BCH码数量不多，但效率很高，其中，算法3生成的是对称的量子BCH码，算法4生成的是非对称的量子BCH码。

1.2.1　从分圆陪集角度构造量子BCH码

算法1　分圆陪集生成有限域F_q上的量子码

输入：n、q满足$\gcd(n,q)=1$。

输出：量子BCH码Q参数$[[n,k,d]]_q$。

Step1　计算分圆陪集C_i。令$m=ord_n(q)=\min\limits_{0\le i\le n}\{i\,|\,n|(q^i-1),\ i>0\}$，将$i$按$q$进制展开$i=i_0+i_1q+\cdots+i_{m-2}q^{m-2}+i_{m-1}q^{m-1}$，其中，$i_0,i_1,\cdots,i_{m-1}\in\{0,1,\cdots,q-1\}$，存在一一对应关系$i\leftrightarrow(i_0,i_1,\cdots,i_{m-1})$，分圆陪集$C_i$为$(i_0,i_1,\cdots,i_{m-1})$全体轮换圈所对应的数$i$。

Step2　任选若干个分圆陪集，计算它们的并集K，称K为定义集。

Step3 计算$K^{-1}=\{-a \bmod n | a\in K\}=\{(n-a) \bmod n | a\in K\}$。

Step4 判断$K\cap K^{-1}=A$, 若A为非空集, 转到Step2; 若A为空集转到Step5。

Step5 计算$k=n-|K|$, 设δ为K中连续数的个数, 输出量子码$[[n,n-2k,\geq d]]_q$, 最小距离满足$d\geq\delta+1$。

算法2 分圆陪集生成有限域F_{q^2}上量子码

输入: n、q^2满足$\gcd(n,q)=1$。

输出: 量子BCH码Q参数$[[n,k,d]]_{q^2}$。

Step1 计算分圆陪集C_i, 令$m=ord_n(q^2)=\min\limits_{0\leq i\leq n}\{i | n | (q^{2i}-1), i>0\}$, 将$i$按$q^2$进制展开为$i=i_0+i_1q^2+\cdots+i_{m-2}q^{2(m-2)}+i_{m-1}q^{2(m-1)}$, 其中, $i_0,i_1,\cdots,i_{m-1}\in\{0,1,\cdots,q^2-1\}$, 存在一一对应关系$i\leftrightarrow(i_0,i_1,\cdots,i_{m-1})$, 分圆陪集$C_i$为$(i_0,i_1,\cdots,i_{m-1})$的全体轮换圈所对应的数。

Step2 任选若干个分圆陪集, 计算其并集K, 称为定义集。

Step3 计算

$K^{-q}=\{-aq \bmod n | a\in K\}=\{(n-qa) \bmod n | a\in K\}$。

Step4 判断$K\cap K^{-q}=A$, 若A为非空集, 转到Step2; 若A为空集转到Step5。

Step5 计算$k=n-|K|$, 设δ为K中连续数的个数, 则存在量子码$[[n,2k-n,\geq d]]_{q^2}$, 满足$d\geq\delta+1$。

证明算法正确性: 算法1、算法2本质上基本是一致的, 不同之处在于算法1利用CSS法构造量子BCH码时使用了有限域F_q上的Euclidean内积; 算法2使用了有限域F_{q^2}上的Hermitian内积。下面先证明算法1中Step1计算结果能得到分圆陪集。

由定义知分圆陪集可写成$C_i=\{iq^x \bmod n | x\in Z\}$, 若$\forall a,b\in C_i$, 则$a=iq^x \bmod n, b=iq^y \bmod n$, 不妨设$y>x, a,b\in N=\{0,1,\cdots,n-1\}$, 注意到$m=ord_n(q)$, 那么, $b=aq^{y-x} \bmod n$, a按q进制展开有唯一表达式为$a=i_0+i_1q+\cdots+i_{m-2}q^{m-2}+i_{m-1}q^{m-1}$, 即存在一一对应关系$a\leftrightarrow(i_0,i_1,\cdots,i_{m-1})$, 但$q^m=1 \bmod n$, 所以, $aq=i_0q+i_1q^2+\cdots+i_{m-2}q^{m-1}+i_{m-1} (\bmod n)$存在一一对应关系$aq\leftrightarrow(i_{m-1},i_0,\cdots,i_{m-2})$。以此类推, aq^{y-x}与$(i_0,i_1,\cdots,i_{m-1})$的$(y-x)$次轮换对应, 从而证明了Step1是正确的。

取生成多项式$g(x)=\prod\limits_{k\in K}(x-\alpha^k)$构造BCH码$C$, 则对偶码$C^{\perp}\subset C\Leftrightarrow K\cap K^{-1}=\Phi$[18], 码$C$的参数为$[n,k,\geq\delta+1]$, 利用CSS构造法很快就可求出参数为$[[n,2k-n,\geq d]]_q$的量子码。 证毕

举 例 取$q^2=4, n=5, C_0=\{0\}, C_1=\{1,4\}, C_2=\{2,3\}$, $K=C_1=\{1,4\}$, $K^{-2}=\{-2\times1 \bmod 5,-2\times4 \bmod 5\}=\{3,2\}$, 有$K\cap K^{-2}=\Phi$, $k=n-|K|=3$, 所以, $[[n,2k-n,\geq d]]_{q^2}=[[5,2\cdot3-5,\geq d]]_{q^2}=[[5,1,\geq2]]_{q^2}$。

如果取$K=C_2=\{2,3\}$, 则$K^{-2}=\{-2\times2 \bmod 5, -2\times3 \bmod 5\}=\{1,4\}$, 仍有判别式$K\cap K^{-2}=\Phi$, $k=n-|K|=3$, 但$K=C_2=\{2,3\}$中有2个连续数2、3, 则$d\geq\delta+1=3$, 根据量子码界可知: $2d\leq n-k+2\Rightarrow d\leq3$, 得到$d=3$, 所以存在$[[5,1,3]]_2$量子码。

注意1 根据算法1和算法2, 如果定义集K包含的数是连续的, 得到的量子码被称为RS量子码; 当参数$[[n,k,d]]_q$满足$2d=n-k+2$时被称为MDS量子码。RS量子码和MDS量子码是两类被广泛研究的特殊量子码。

注意2 有限域F_q上得Euclidean内积和有限域F_{q^2}的Hermitian内积, 很多性质都是相似的, 为避免啰嗦, 后续只讨论有限域F_q上Euclidean内积, 对于有限域F_{q^2}, 完全有类似的生成算法可求得。

1.2.2 从特殊分圆陪集角度构造量子码

第1类构造方法中, 需要搜索大量的分圆陪集, 计算效率会受到影响。由文献[19]可知, 如果存在F_q上线性码$C=[n,k,d]_q$满足$C^{\perp}\subseteq C$, 则存在参数为$[[n,2k-n,\geq d]]_q$的量子码, 如果$C^{\perp}$的最小距离超过d, 则量子码的最小距离就为d; 如果存在F_{q^2}上线性码$D=[n,k,d]_{q^2}$满足$D^{\perp_H}\subseteq D$, 则存在$[[n,2k-n,\geq d]]_{q^2}$的量子码。下面介绍利用特殊分圆陪集构造量子纠错码。其中, $[xodd]=x \bmod 2$, $[xeven]=(x-1) \bmod 2$, $\lceil x\rceil$为不小于x的最小整数。

算法3 特殊分圆陪集生成有限域F_q上的量子码

输入: $n=q^m-1$, 取$\delta_{\max}=q^{\lceil m/2\rceil}-1-(q-2)[modd]$, 令$\alpha$为$n$次本原单位根。

输出: 量子BCH码Q参数$[[q^m-1, q^m-1-2m\lceil(\delta-1)\cdot(1-1/q)\rceil, d_Q\geq\delta]]$。

Step1 设$N=\{0,1,2,\cdots,n-1\}$, 任取$\delta\leq\delta_{\max}$, 计算定义集$K=C_1\cup C_2\cup\cdots\cup C_{\delta-1}$, 其中, $C_x=\{xq^j \bmod n | j\in Z\}$为$F_q$上的分圆陪集。

Step2 选取多项式$g(x)=\prod\limits_{k\in K}(x-\alpha^k)$和$h(x)=\prod\limits_{k\in N\setminus K}(x-\alpha^{-k})$作为生成多项式, 生成狭义BCH码$C$和$C^{\perp}$, 且满足$C^{\perp}\subset C$。

Step3 根据C和$C^{\perp}$利用CSS构造法构造量子BCH码Q, 最小距离$d_Q\geq\delta$可根据需要进行设计。

算法3的证明可利用文献[20]中的定理34, 这里不再赘述。类似地, 还可生成F_{q^2}上的量子码Q, 其参数为$[[q^{2m}-1, q^{2m}-1-2m\lceil(\delta-1)(1-1/q^2)\rceil, d_Q\geq\delta]]$。此时有限域$F_{q^2}$的内积为Hermitian内积。算法3表明只需选取不同的δ, 就可得到不同的定义集, 生成一大批量子BCH码。

在经典BCH码中, 如果生成多项式的定义集为$K=C_b\cup C_{b+1}\cup\cdots\cup C_{b+\delta-2}$, 则最小距离$d\geq\delta$。当$n=$

q^m-1时其被称为本元BCH码，当$b=1$时被称为狭义BCH码。

1.2.3　非对称量子BCH码的构造

量子码Q能明确其纠正比特翻转错误和相位翻转错误的能力，则被称为非对称量子码。利用CSS构造可以得到非对称量子码。设C_1、C_2分别是F_q上的经典线性码，参数表达为$C_1=[n,k_1,d_1]$，$C_2=[n,k_2,d_2]$，并设$C_1^{\perp}\subseteq C_2$，从而$C_2^{\perp}\subseteq C_1$。且参数满足不等式$k_1+k_2-n\geq 0$，则存在量子码Q，其是参数为$[[n,k_1+k_2-n,d_z/d_x]]_q$的非对称量子纠错码。令$T=\{\mathrm{wt}(\boldsymbol{c})|\boldsymbol{c}\in(C_1\backslash C_2^{\perp})\cup(C_2\backslash C_1^{\perp})\}$，则$d_x=\min T$，$d_z=\max T$，该量子码可以纠正$\lfloor(d_x-1)/2\rfloor$个量子比特翻转，同时，可以纠正$\lfloor(d_z-1)/2\rfloor$个相位比特翻转。对于有限域$F_{q^2}$可利用$D_1^{\perp H}\subseteq D_2$类似地构造出非对称量子码。

算法4　有限域F_q上的非对称量子BCH码的生成

输入：$n=q^m-1$，取$\delta_{\max}=q^{\lceil m/2\rceil}-1-(q-2)[modd]$，$n$次本原单位根$\alpha$。

输出：量子BCH码Q参数$[[q^m-1,q^m-1-2m\lceil(\delta-1)\cdot(1-1/q)\rceil,d_z/d_x]]$。

Step1　设$N=\{0,1,2,\cdots,n-1\}$，任取$\delta\leq\delta_{\max}$计算定义集$K=C_1\cup C_2\cup\cdots\cup C_{\delta-1}$，其中，$C_x=\{xq^j \bmod n \mid j\in Z\}$为$F_q$上分圆陪集。

Step2　取多项式$g(x)=\prod_{k\in K}(x-\alpha^k)$作为生成多项式，生成狭义BCH码$C_1$。

Step3　任取$2\leq\delta'\leq\delta$，计算$K'=C_1\cup C_2\cup\cdots\cup C_{\delta'-1}$，由多项式$g(x)=\prod_{k\in K}(x-\alpha^k)$作为生成码$C_2$（也可以任意选取$C_1,C_2,\cdots,C_{\delta}$中下标连续的部分分圆陪集）。

Step4　根据C_1和C_2利用CSS构造法可以构造量子BCH码Q。令$T=\{\mathrm{wt}(c)|c\in(C_1\backslash C_2^{\perp})\cup(C_2\backslash C_1^{\perp})\}$，则$d_x=\min T$，$d_z=\max T$。

算法证明：从文献[20]知，Step2生成的码C_1包含其对偶码，且维数$k_1=q^m-1-m\lceil(\delta-1)(1-1/q)\rceil$，而Step3生成的码$C_2\supset C_1$，$C_2$的维数满足不等式$k_2>k_1$，则$k_2+k_1-n>2k_1-n=q^m-1-2m\lceil(\delta-1)(1-1/q)\rceil>0$，因此，可以得到非对称量子码。

还可以生成F_{q^2}上的量子码Q，其参数为$[[q^{2m}-1,q^{2m}-1-2m\lceil(\delta-1)(1-1/q^2)\rceil,d_z/d_x]]$，此时有限域$F_{q^2}$的内积为Hermitian内积。利用常循环码也可以构造非对称量子纠错码，详情参见文献[21]。

2　基于量子BCH码设计量子McEliece和量子Niederreiter公钥密码体制

在解密过程中，基于量子BCH码设计的量子McEliece公钥密码体制和量子Niederreiter公钥密码体制需要使用BCH码的译码算法。主要采用BCH码的Berlekamp-Massey译码算法，简称BM译码算法。量子McEliece公钥密码体制的思想如下：

1）将量子BCH码Q，通过隐藏得到等价的量子BCH码Q'。

2）量子BCH码Q'将明文消息编码成量子纠缠态。

3）加密：在已编码的量子纠缠态中，故意加入量子错误（比特翻转或相位翻转），从而得到错误污染后的量子态，即是密文。

4）解密：由Q'的纠错功能消除量子错误，得到消息的量子态，由编码原则恢复明文。

根据第1节给出的非对称量子BCH码构造方法，经典BCH码满足$C_1^{\perp}\subset C_1\subset C_2$，由CSS构造出量子码$Q$。设$C_2$的生成矩阵为$\boldsymbol{G}_2$，任意选取可逆方阵$\boldsymbol{U}$和置换矩阵$\boldsymbol{P}$，使得$\boldsymbol{G}_2'=\boldsymbol{U}\boldsymbol{G}_2\boldsymbol{P}$，相应地，隐藏$C_1^{\perp}$、$C_1$的生成矩阵和校验矩阵。隐藏后的生成矩阵和校验矩阵，仍记为$\boldsymbol{G}_2$、$\boldsymbol{H}_2$、$\boldsymbol{G}_1$、$\boldsymbol{H}_1$。量子码的比特翻转和相位翻转纠错能力记为t_x、t_z。当$C_1=C_2=C$时处理方法类似。对于有限域F_{q^2}需考虑Hermitian正交即可。设F_q为特征为p的有限域，则$\forall\boldsymbol{x}\cdot\boldsymbol{y}\in F_q^n$，$\boldsymbol{x}\cdot\boldsymbol{y}$为Euclidean内积，$\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y})$表示内积$\boldsymbol{x}\cdot\boldsymbol{y}$的迹。量子态表示为$|\boldsymbol{x}\rangle$，常用的量子变换大都采用酉变换，其逆变换和原变换几乎相同。作者采用的酉变换大致为：

1）广义Hadamard门变换

$$|\boldsymbol{x}\rangle\xrightarrow{H^{\otimes n}}\frac{1}{\sqrt{q^n}}\sum_{\boldsymbol{y}\in F_q^n}\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y})}|\boldsymbol{y}\rangle。$$

当$F_q=F_2$时，

$$|\boldsymbol{x}\rangle\xrightarrow{H^{\otimes n}}\frac{1}{\sqrt{2^n}}\sum_{\boldsymbol{y}\in F_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{y}\rangle。$$

2）有限域F_2^n上的Fourier变换

$$|\boldsymbol{x}\rangle\xrightarrow{F}\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{2^n}\boldsymbol{x}\cdot\boldsymbol{y}}|\boldsymbol{y}\rangle。$$

3）任意函数f的U_f黑盒变换

$$|\boldsymbol{x}\rangle|\boldsymbol{y}\rangle\xrightarrow{U_f}|\boldsymbol{x}\rangle|\boldsymbol{y}\oplus f(\boldsymbol{x})\rangle。$$

2.1　密钥生成

1）给出隐藏量子码Q及纠错能力t_x、t_z。

2）公钥：$\boldsymbol{G}_1$、$\boldsymbol{G}_2$和t_x、t_z。

3）私钥：$\boldsymbol{U}$、$\boldsymbol{P}$及相应的BM译码算法。

2.2　加密过程

1）任选明文$\boldsymbol{m}\in GF(2^{k_2})$和$\boldsymbol{x}=\boldsymbol{m}\boldsymbol{G}_2$，编码成量子纠缠态为：

$$|\boldsymbol{x}+C_1\rangle=\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}|\boldsymbol{x}+\boldsymbol{y}\rangle。$$

2）随机选择比特翻转向量和相位翻转错误$\boldsymbol{e}_x$、$\boldsymbol{e}_z$，量子Hamming重量满足：

$$W_{\text{quantum}}(\boldsymbol{e}_x)\le t_x, W_{\text{quantum}}(\boldsymbol{e}_z)\le t_z。$$

3）加密得到密文为：

$$|cip\rangle=\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\mathrm{Tr}[(\boldsymbol{y}+\boldsymbol{x})\cdot\boldsymbol{e}_z]}|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x\rangle。$$

2.3 解密过程

利用量子纠错码检出错误$\boldsymbol{e}_x$、$\boldsymbol{e}_z$，去掉错误得到量子态：$|\boldsymbol{x}+C_1\rangle=\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}|\boldsymbol{x}+\boldsymbol{y}\rangle$，由此恢复出明文$\boldsymbol{m}$。为了说明量子纠错过程，有如下引理。

引　理　设F_q的特征为p，C为F_q上的线性码，$C^{\perp}$为C的对偶码，$\forall\boldsymbol{x}\in F_q^n$，则$\sum_{\boldsymbol{y}\in C}\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\cdot\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y})}=\begin{cases}|C|, \boldsymbol{x}\in C^{\perp};\\ 0, \boldsymbol{x}\notin C^{\perp}。\end{cases}$

证明：线性码C是一个加法群，U_p表示复数域上全体p次单位根组成的集合。取定$\boldsymbol{x}\in F_q^n$，定义映射：

$$\chi_x: C\to U_p\text{即}\chi_x:\boldsymbol{y}\mapsto\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\cdot\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y})},$$

满足下列性质：

1）$\chi_x(\boldsymbol{y}_1+\boldsymbol{y}_2)=\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\cdot\mathrm{Tr}(\boldsymbol{x}\cdot(\boldsymbol{y}_1+\boldsymbol{y}_2))}=\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}(\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y}_1)+\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y}_2))}=\chi_x(\boldsymbol{y}_1)\cdot\chi_x(\boldsymbol{y}_2)$；

2）$\chi_x(\boldsymbol{0})=\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\mathrm{Tr}(\boldsymbol{0})}=1$。

所以，χ_x是码C到U_p的一个群同态，也被称为线性特征标。

当$\boldsymbol{x}\notin C^{\perp}$时，$\chi_x\ne 1$，那么，存在$\bar{\boldsymbol{y}}\in F_q^n\backslash\{\boldsymbol{0}\}$，$\chi_x(\bar{\boldsymbol{y}})\in U_p$，满足$\chi_x(\bar{\boldsymbol{y}})\ne 1,0$。从而有：

$$\chi_x(\bar{\boldsymbol{y}})\sum_{\boldsymbol{y}\in C}\chi_x(\boldsymbol{y})=\sum_{\boldsymbol{y}\in C}\chi_x(\bar{\boldsymbol{y}})\chi_x(\boldsymbol{y})=\sum_{\boldsymbol{y}\in C}\chi_x(\boldsymbol{y}+\bar{\boldsymbol{y}})\underline{\underline{\boldsymbol{t}=\boldsymbol{y}+\bar{\boldsymbol{y}}}}\sum_{\boldsymbol{t}\in C}\chi_x(\boldsymbol{t})=\sum_{\boldsymbol{y}\in C}\chi_x(\boldsymbol{y}),$$

$$(\chi_x(\bar{\boldsymbol{y}})-1)\sum_{\boldsymbol{y}\in C}\chi_x(\boldsymbol{y})=0,$$

但$\chi_x(\bar{\boldsymbol{y}})-1\ne 0$，故

$$\sum_{\boldsymbol{y}\in C}\chi_x(\boldsymbol{y})=0=\sum_{\boldsymbol{y}\in C}\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y})}。$$

所以，$\sum_{\boldsymbol{y}\in C}\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\cdot\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y})}=\begin{cases}|C|, \boldsymbol{x}\in C^{\perp};\\ 0, \boldsymbol{x}\notin C^{\perp}。\end{cases}$

证毕

当$F_q=F_2$时，则$\sum_{\boldsymbol{y}\in C}(-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}=\begin{cases}0, \boldsymbol{x}\notin C^{\perp};\\ |C|, \boldsymbol{x}\in C^{\perp}。\end{cases}$ 3类量子错误可以分别看成比特翻转和相位翻转的线性组合。设量子状态为$|\boldsymbol{x}+C_1\rangle=\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}|\boldsymbol{x}+\boldsymbol{y}\rangle$。在加密过程中，选取比特翻转错误为$\boldsymbol{e}_x$，相位翻转错误为$\boldsymbol{e}_z$。下面以$F_q=F_2$为例说明解密过程。对于一般有限域，只需将$(-1)^{\boldsymbol{x}\cdot\boldsymbol{y}}$改成$\mathrm{e}^{\frac{2\pi\mathrm{i}}{p}\mathrm{Tr}(\boldsymbol{x}\cdot\boldsymbol{y})}$，且使用广义Hadamard门变换，引理1的结果依然成立。于是将量子密文设为$\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{e}_z}|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x\rangle$。

纠错过程如下：

定理1　$\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{e}_x}|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x\rangle$可用$\boldsymbol{H}_1$纠正比特翻转。

证明：利用计算

$$|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x\rangle|0\rangle\xrightarrow{U_f}|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x\rangle|0+f(\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x)\rangle。$$

取$f(\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x)=\boldsymbol{H}_1(\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x)=\boldsymbol{H}_1\boldsymbol{e}_x$，$\boldsymbol{H}_1$为$C_1$的校验矩阵，可以算出$\boldsymbol{e}_x$。

同理，可将

$$\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{e}_z}|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x\rangle|0\rangle\to\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{e}_z}|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{e}_x\rangle|\boldsymbol{H}_1\boldsymbol{e}_x\rangle。$$

利用错误算子去掉$\boldsymbol{e}_x$，得到：

$$\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{e}_z}|\boldsymbol{x}+\boldsymbol{y}\rangle。$$

证毕

定理2　相位翻转错误$\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{e}_z}|\boldsymbol{x}+\boldsymbol{y}\rangle$可以转化为比特翻转错误。

证明：应用Hadamard门作用为：

$$\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{e}_z}|\boldsymbol{x}+\boldsymbol{y}\rangle\to\frac{1}{\sqrt{|C_1|}}\frac{1}{\sqrt{2^n}}\sum_{\boldsymbol{u}\in F_2^n}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})(\boldsymbol{e}_z+\boldsymbol{v})}|\boldsymbol{v}\rangle\underline{\underline{\boldsymbol{u}'=\boldsymbol{u}+\boldsymbol{e}_z}}\frac{1}{\sqrt{|C_1|2^n}}\sum_{\boldsymbol{u}'\in F_2^n}\sum_{\boldsymbol{y}\in C_1}(-1)^{(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{u}'}|\boldsymbol{u}'+\boldsymbol{e}_z\rangle=\frac{1}{\sqrt{|C_1|2^n}}\sum_{\boldsymbol{u}'\in F_2^n}(\sum_{\boldsymbol{y}\in C_1}(-1)^{\boldsymbol{y}\cdot\boldsymbol{u}'})(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}'}|\boldsymbol{u}'+\boldsymbol{e}_z\rangle。$$

由引理可知，

$$\frac{1}{\sqrt{|C_1|2^n}}\sum_{\boldsymbol{u}'\in F_2^n}(\sum_{\boldsymbol{y}\in C_1}(-1)^{\boldsymbol{y}\cdot\boldsymbol{u}'})(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}'}|\boldsymbol{u}'+\boldsymbol{e}_z\rangle=\sqrt{\frac{|C_1|}{2^n}}\sum_{\boldsymbol{u}'\in C_1^{\perp}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}'}|\boldsymbol{u}'+\boldsymbol{e}_z\rangle。$$

再利用$C_1^{\perp}$的检验矩阵$\boldsymbol{G}_1$可以计算出$\boldsymbol{e}_z$，与定理1中类

似，错误算子可以去掉$\boldsymbol{e}_z$。

于是得到量子态：

$$\sqrt{\frac{|C_1|}{2^n}}\sum_{\boldsymbol{u}'\in C_1^{\perp}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}'}|\boldsymbol{u}'\rangle\underline{\underline{\boldsymbol{u}=\boldsymbol{u}'}}\sqrt{\frac{|C_1|}{2^n}}\sum_{\boldsymbol{u}\in C_1^{\perp}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}|\boldsymbol{u}\rangle,$$

再次应用量子Hadamard变换，上述状态变为：

$$\sqrt{\frac{|C_1|}{2^n}}\sum_{\boldsymbol{u}\in C_1^{\perp}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}|\boldsymbol{u}\rangle\to\frac{\sqrt{|C_1|}}{2^n}\sum_{\boldsymbol{v}\in F_2^n}\sum_{\boldsymbol{u}\in C_1^{\perp}}(-1)^{(\boldsymbol{x}+\boldsymbol{v})\cdot\boldsymbol{u}}|\boldsymbol{v}\rangle\underline{\underline{\boldsymbol{v}'=\boldsymbol{x}+\boldsymbol{v}}}$$

$$\frac{\sqrt{|C_1|}}{2^n}\sum_{\boldsymbol{v}'\in F_2^n}\sum_{\boldsymbol{u}\in C_1^{\perp}}(-1)^{\boldsymbol{v}'\cdot\boldsymbol{u}}|\boldsymbol{v}'+\boldsymbol{x}\rangle。$$

再根据引理可知，

$$\frac{\sqrt{|C_1|}}{2^n}\sum_{\boldsymbol{v}'\in F_2^n}\sum_{\boldsymbol{u}\in C_1^{\perp}}(-1)^{\boldsymbol{v}'\cdot\boldsymbol{u}}|\boldsymbol{v}'+\boldsymbol{x}\rangle=$$

$$\frac{\sqrt{|C_1|}}{2^n}\left|C_1^{\perp}\right|\sum_{\boldsymbol{v}'\in C_1}|\boldsymbol{v}'+\boldsymbol{x}\rangle=\frac{\sqrt{|C_1|}}{2^n}\frac{2^n}{|C_1|}\sum_{\boldsymbol{v}'\in C_1}|\boldsymbol{v}'+\boldsymbol{x}\rangle=$$

$$\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{v}'\in C_1}|\boldsymbol{v}'+\boldsymbol{x}\rangle=\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}|\boldsymbol{x}+\boldsymbol{y}\rangle。$$

这就是初始量子态$|\boldsymbol{x}+C_1\rangle=\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}|\boldsymbol{x}+\boldsymbol{y}\rangle$，从而得到$\boldsymbol{x}$可以恢复消息$\boldsymbol{m}$。如果$F_q\neq F_2$，将得到$|-\boldsymbol{x}+C_1\rangle=\frac{1}{\sqrt{|C_1|}}\sum_{\boldsymbol{y}\in C_1}|-\boldsymbol{x}+\boldsymbol{y}\rangle$，依然可以恢复消息$\boldsymbol{m}$。

证毕

基于量子BCH码的量子Niederreiter公钥密码体制，给出如下算法：

算法5　基于量子BCH码的量子Niederreiter公钥密码体制

1）给定量子BCH码Q，隐藏得到等价的量子BCH码Q'。

2）将明文消息对应到量子错误。

3）公钥：量子BCH码Q'校验矩阵$\boldsymbol{H}^{\text{puk}}$、$t_x/t_z$。

4）私钥：BM译码算法和对应伴随式译码算法，隐藏变换。

5）加密：将量子错误算子作用在一个由量子BCH码Q'编码的纠缠态上。

6）解密：利用Q'的纠错功，检测出量子错误，恢复得到明文消息。

此算法证明过程与量子McEliece公钥密码体制完全相似，在此省略。

3　安全性分析

文献[16]证明了经典Niederreiter公钥密码体制的安全性等价于经典McEliece公钥体制，在量子状态下，可能会有很多变化。文献[22]中引进了数据复杂性分析量子计算的安全性。下面从计算复杂度和数据复杂度的角度重点分析量子BCH码的McEliece公钥体制的安全性。

1）首先，未知其译码算法，利用接收向量直接译码，这是一个NPC问题。这说明无法从密文猜测译码算法，进而，猜测错误为$\boldsymbol{e}_x$、$\boldsymbol{e}_z$。且加密过程需要选择量子错误$\boldsymbol{e}_x$、$\boldsymbol{e}_z$，量子Hamming重量满足$W_{\text{quantum}}(\boldsymbol{e}_x)\le t_x$，$W_{\text{quantum}}(\boldsymbol{e}_z)\le t_x$，两类错误组合满足下列组合公式：

$$\binom{n}{t_x}\binom{n}{t_z}\ge\binom{n}{t_x+t_z}=\binom{n}{t},$$

一般地，t比较小，所以$\binom{n}{t}\approx O(n!)$，$\lim\limits_{n\to\infty}\frac{n!}{2^n}=\infty$，说明错误$\boldsymbol{e}_x$、$\boldsymbol{e}_z$的数据复杂度也很大。

2）在经典情形下，参数相同时，BCH码数目远没有Goppa多，作者利用的是量子BCH码，有2个优点：① 一个量子BCH码由两个具有偶包含的经典BCH组成，使得量子BCH码数目成组合增加；② 由于量子BCH码在应用前被隐藏，如果穷举出隐藏变换，需要知道可逆矩阵$\boldsymbol{U}$和置换矩阵$\boldsymbol{P}$，F_q上k阶可逆矩阵数目为$(q^k-1)(q^k-q)(q^k-q^2)\cdots(q^k-q^{k-1})=q^{k^2}\prod_{i=1}^{k}(1-q^{-i})>q^{k(k-1)}$。而$n$阶置换矩阵$\boldsymbol{P}$的数目大约为$n!$，还可以将置换矩阵每行为1的元素换成$F_q$中的非零元素，即具有不改变码字Hamming重量的特性，这样符合条件的置换矩阵数目为$n!(q-1)^n$。采用CSS构造量子BCH码时，要求$k_1+k_2>n\Rightarrow k>\frac{n}{2}$，搜索隐藏变换计算复杂度为$O((\sqrt[4]{q})^{n^2}(q-1)^n n!)$，当$q>2^4$时，$\lim\limits_{n\to\infty}\frac{(\sqrt[4]{q})^{n^2}(q-1)^n n!}{2^n}=\infty$。

3）利用矩阵分解的方法，从量子BCH码的隐藏中得到量子码的生成矩阵，涉及到矩阵分解和矩阵乘法，是非交换群中的运算，即量子算法所不擅长的。

4）文献[17]利用数值仿真分析了量子McEliece体制有很高的计算复杂度，可以抵抗Grove量子搜索计算。文献[23]分析了McEliece体制可以抵抗量子Fourier采样攻击。

基于量子BCH码的McEliece体制存在存储空间大的弱点。除了上述安全分析外，还需考虑空间复杂度。当没有参与运算时，认为空间复杂度为$O(1)$。具体分析如下：

1）为了得到量子BCH码，需要存储线性码$C_1\subset C_2$，及其对偶码$C_1^{\perp}$、$C_2^{\perp}$。需要存储生成矩阵和校验矩阵，并进行相应的运算，故空间复杂度为$O(n)$。

2）存储量子态$|\boldsymbol{x}+C_1\ge\sum_{\boldsymbol{y}\in C_1}|\boldsymbol{x}+\boldsymbol{y}\rangle$，采用$U_f$及Hadamard门变换，存储空间为$O(q^{k_1})$。

3）存在$C_1^{\perp}$、C_2的效验矩阵$\boldsymbol{H}_1$、$\boldsymbol{H}_2$，矩阵乘法运算

存储复杂度为$O(n^3)$。对$\sqrt{\frac{|C_1|}{2^n}}\sum_{\boldsymbol{u}\in C_1^{\perp}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{u}}|\boldsymbol{u}\rangle$做量子Hadamard门变换，存储空间为$O(q^{n-k_1})$。

存储空间没有顺序，最大空间复杂度为$O(q^{n-k_1})\approx O(q^{n/2})(k_1+k_2>n)$，但$q=p^m\Rightarrow O(q^{n/2})\approx O(p^{nm/2})$，$\lim\limits_{n\to\infty}\frac{p^{nm/2}}{2^n}=\infty(m>2)$。

4）经典BCH的译码算法中，较通用的译码算法为BM算法，需要存储大量的伴随式，伴随式个数为$\binom{n}{t}\approx n!(t\ll n)$空间复杂度为$O(n!)$。

5）量子纠错实质上是先经典码纠错，再转换成量子态，需要很大中间转换存储空间，空间复杂度$O(q^{k_2-k_1}n!)>O(n!)$。

从空间复杂性分析的2）~5）知，作者提出的密码算法空间复杂性和时间复杂性都很大，进而数据复杂性也很大，具有很好的抗Shor算法和Grover算法攻击能力。

4 利用一类量子BCH构造时的偶包含码设计抗量子计算数字签名

文献[24]提出了CFS数字签名，作者在构造量子BCH码时，需要用到具有偶包含（偶码被包含在码内）特性的经典码。这种经典码可用于设计数字签名，类似CFS方案而具有抗量子攻击能力。

4.1 预备工作

设Alice选择量子BCH码Q_{A}由一对偶包含码$D^{\perp}\subset D$通过CSS构成，Bob选择量子BCH码Q_{B}是一对偶包含码$C^{\perp}\subset C$通过CSS构成的。取$\boldsymbol{G}_{\mathrm{A}}$为码$D$的生成矩阵，$\boldsymbol{G}_{\mathrm{B}}$为码$C$的生成矩阵，$\boldsymbol{H}_{\mathrm{A}}$为$D$的校验矩阵，$\boldsymbol{H}_{\mathrm{B}}$为$C$的校验矩阵，$\overline{\boldsymbol{G}}_{\mathrm{A}}$为$\boldsymbol{G}_{\mathrm{A}}$的右逆$\boldsymbol{G}_{\mathrm{A}}\overline{\boldsymbol{G}}_{\mathrm{A}}=\boldsymbol{I}_K$。设$\boldsymbol{P}_{\mathrm{A}}$、$\boldsymbol{P}_{\mathrm{B}}$为置换矩阵，$\boldsymbol{U}$为任意可逆矩阵，则$\boldsymbol{G}'_{\mathrm{A}}=\boldsymbol{P}_{\mathrm{A}}^{-1}\overline{\boldsymbol{G}}_{\mathrm{A}}$，$\boldsymbol{H}'_{\mathrm{B}}=\boldsymbol{U}\boldsymbol{H}_{\mathrm{B}}\boldsymbol{P}_{\mathrm{B}}$。$t$为码$C$的最大纠错能力。

公钥：$\boldsymbol{G}'_{\mathrm{A}}$、$\boldsymbol{G}_{\mathrm{B}}$、$\boldsymbol{H}'_{\mathrm{B}}$、$t$存入PKDB中，公开的Hash函数$h_1$、$h_2$。

私钥：Alice的私钥$\boldsymbol{H}_{\mathrm{A}}$、$\boldsymbol{P}_{\mathrm{A}}$、$\boldsymbol{G}_{\mathrm{A}}$、$\overline{\boldsymbol{G}}_{\mathrm{A}}$及Bob的私钥$\boldsymbol{H}_{\mathrm{B}}$、$\boldsymbol{P}_{\mathrm{B}}$、$\boldsymbol{U}$。

4.2 签名过程（设$\boldsymbol{M}$为签名信息）

1）Alice随机选取一个汉明权重$W_{\mathrm{H}}(\boldsymbol{e})\le t$的$n$维向量$\boldsymbol{e}$，在PKDB中查找到$\boldsymbol{H}'_{\mathrm{B}}$。计算$\boldsymbol{e}(\boldsymbol{H}'_{\mathrm{B}})^{\mathrm{T}}=\boldsymbol{S}_{\mathrm{A}}$，相当于计算$\boldsymbol{e}$的伴随式，$\boldsymbol{S}_{\mathrm{A}}$为$(n-k)$维向量，$\boldsymbol{H}'_{\mathrm{B}}$可看成$C$的对偶码$C^{\perp}$的生成矩阵。$\boldsymbol{R}_{\mathrm{A}}=\boldsymbol{S}_{\mathrm{A}}\boldsymbol{H}'_{\mathrm{B}}$看成$C^{\perp}$中编码得到的码字。

2）Alice对$\boldsymbol{M}$进行如下处理：

$$\boldsymbol{J}=sig(\boldsymbol{M})=\{\boldsymbol{e}+[(h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e}))-\boldsymbol{e}\overline{\boldsymbol{G}}_{\mathrm{A}}]\boldsymbol{G}_{\mathrm{A}}\}\boldsymbol{P}_{\mathrm{A}},$$

Alice将$(\boldsymbol{M},\boldsymbol{J},\boldsymbol{R}_{\mathrm{A}})$当成签名消息发给Bob。

4.3 验证签名过程

1）Bob收到$(\boldsymbol{M},\boldsymbol{J},\boldsymbol{R}_{\mathrm{A}})$后，利用$\boldsymbol{R}_{\mathrm{A}}=\boldsymbol{S}_{\mathrm{A}}\boldsymbol{H}'_{\mathrm{B}}$是$C^{\perp}$中码字，因为$C^{\perp}$的最小距离比$C$大，由$C^{\perp}$的译码算法得到$\boldsymbol{S}_{\mathrm{A}}$，$\boldsymbol{S}_{\mathrm{A}}(\boldsymbol{U}^{-1})^{\mathrm{T}}=\boldsymbol{e}(\boldsymbol{H}'_{\mathrm{B}})^{\mathrm{T}}(\boldsymbol{U}^{-1})^{\mathrm{T}}=\boldsymbol{e}(\boldsymbol{P}_{\mathrm{B}})^{\mathrm{T}}\boldsymbol{H}_{\mathrm{B}}^{\mathrm{T}}$且$\boldsymbol{W}_{\mathrm{H}}(\boldsymbol{e}(\boldsymbol{P}_{\mathrm{B}})^{\mathrm{T}})\le t$，利用$C$进行译码得差错向量$\boldsymbol{e}(\boldsymbol{P}_{\mathrm{B}})^{\mathrm{T}}$，Bob由私钥$\boldsymbol{P}_{\mathrm{B}}$得到$\boldsymbol{e}$。

2）Bob计算

$$\begin{aligned}\boldsymbol{S}_1=\boldsymbol{J}\boldsymbol{G}'_{\mathrm{A}}&=\{[(h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e})-\boldsymbol{e}\overline{\boldsymbol{G}}_{\mathrm{A}}]\boldsymbol{G}_{\mathrm{A}}\}\boldsymbol{P}_{\mathrm{A}}\boldsymbol{G}'_{\mathrm{A}}=\\&\{\boldsymbol{e}+[h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e})-\boldsymbol{e}\overline{\boldsymbol{G}}_{\mathrm{A}}]\boldsymbol{G}_{\mathrm{A}}\}\boldsymbol{P}_{\mathrm{A}}\boldsymbol{P}_{\mathrm{A}}^{-1}\overline{\boldsymbol{G}}_{\mathrm{A}}=\\&\boldsymbol{e}\overline{\boldsymbol{G}}_{\mathrm{A}}+[h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e})-\boldsymbol{e}\overline{\boldsymbol{G}}_{\mathrm{A}}]\boldsymbol{G}_{A}\overline{\boldsymbol{G}}_{A}=\\&\boldsymbol{e}\overline{\boldsymbol{G}}_{\mathrm{A}}+h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e})-\boldsymbol{e}\overline{\boldsymbol{G}}_{\mathrm{A}}=\\&h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e})。\end{aligned}$$

3）Bob在1）中得到$\boldsymbol{e}$，从签名中得到$\boldsymbol{M}$，计算$\boldsymbol{S}_2=h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e})$。

4）判断：若$\boldsymbol{S}_1=\boldsymbol{S}_2$，则签名有效；否则，签名无效。

注意3 由于篇幅过长，本签名协议的安全性分析与文献[25]类似，只不过本签名涉及的纠错码都是量子BCH码；另外，在本签名中用到两个hash函数h_1、h_2，设$h_1(\boldsymbol{M})$的取值定长为r，$h_2(\boldsymbol{e})$取值长为$n-r$，$(h_1(\boldsymbol{M})\,\|\,h_2(\boldsymbol{e}))$正好看成一个长为$n$的向量。

5 结 论

矩阵乘法运算没有交换性，不能规约到HSP问题（hidden subgroup problem）。量子Fourier 变换不擅长处理该类问题[2]，具有良好的抗量子计算攻击。但是，量子McEliece和Niederreiter公钥密码体制也存在存储量大，效率低的弱点。作者利用量子BCH码易于编码成量子纠缠态、纠错能力可设计、译码算法多（如Peterson-Gorenstein-Zierler译码算法、Berlekamp-Massey译码算法、Su Giyama译码算法等）等优点设计了基于量子BCH码的McEliece和Niederreiter公钥密码算法，重点研究量子BCH码的量子MCEliece公钥体制。在此过程中，作者先给出了3类典型的量子BCH码生成算法，其中，算法1和算法2是第1类，算法3是第2类对称量子BCH码生成算法，算法4是第3类非对称量子BCH码生成算法。然后，利用量子BCH码设计量子McEliece公钥密码体制和量子Niederreiter公钥密码体制，并分析了安全性。本文方法完全可以推广到任意有限域上的量子BCH码的MCEliece公钥体制。

作者所提出的量子McEliece和Niederreiter公钥密码体制，在纠错过程中，仍是经典码的纠错方式，应进一步研究更方便的q元量子码的纠错方式，结合量子力学，从物理纠错方面加以研究；需要对量子McEliece体制进行更完善的安全分析，需要借鉴已有的

安全分析方法，给出更加充分的安全分析；另外，量子McEliece体制和量子Niederreiter体制的安全性证明和可应用性等方面有待进一步研究。

参考文献：

[1] Zhang Huanguo,Wang Houzhen.Anti-cryptography quantum computing research[J].Netinfo Security,2011(6):56–59.

[2] Grigni M,Schulman L,Vazirani M,et al.Quantum mechanical algorithms for the nonabelian hidden subgroup problem[J].Combinatorica,2004,24(1):137–154.

[3] Bernstein D J,Buchmann J,Dahmen E,等.抗量子计算密码[M].张焕国,王后珍,杨昌,译.北京:清华大学出版社,2015.

[4] Jin Lingfei,Xing Chaoping.A construction of new quantum MDS codes[J].IEEE Transactions on Information Theory,2014,60(5):2921–2925.

[5] Jin Lingfei,Xing Chaoping.New MDS self-dual codes from generalized reed—olomon codes[J].IEEE Transactions on Information Theory,2017,63(3):1434–1438.

[6] Jin Lingfei.Quantum stabilizer codes from maximal curves[J].IEEE Transactions on Information Theory,2014,60(1):313–316.

[7] Xu Gen,Li Ruihu,Guo Luobin,et al.New quantum codes constructed from quaternary BCH codes[J].Quantum Information Processing,2016,15(10):4099–4116.

[8] Chuang I,Gottesman D.Quantum digital signatures:US 7246240[P].2007-07-17.

[9] Ablayev F M,Vasiliev A V.Cryptographic quantum hashing[J].Laser Physics Letters,2014,11(2):025202.

[10] Bennett C H,Brassard G.Quantum cryptography:Public key distribution and coin tossing[J].Theoretical Computer Science,2014,560(1):7–11.

[11] Zeng Guihua.Quantum authentication[M]//Quantum Private Communication.Heidelberg:Springer,2010:167–215.

[12] Toyran M.Quantum cryptography[C]//Proceedings of the 2007 IEEE 15th Signal Processing and Communications Applications.Eskisehir:IEEE,2007:1–4.

[13] Okamoto T,Tanaka K,Uchiyama S.Quantum public-key cryptosystems[M]//Advances in Cryptology — CRYPTO 2000.Heidelberg:Springer,2000:147–165.

[14] Wieschebrink C.Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes[C]//Proceedings of the Third International Conference on Post-Quantum Cryptography.Heidelberg:Springer-Verlag,2010:61–72.

[15] McEliece R J.A public-key cryptosystem based on algebraic coding theory[R].Pasadena:California Institute of Technology,1978:114–116

[16] Li Yuanxing,Deng R H,Wang Xinmei.On the equivalence of McEliece's and Niederreiter's public-key cryptosystems[J].IEEE Transactions on Information Theory,1994,40(1):271–273.

[17] Cao Dong,Zhao Shengmei,Song Yaoliang,et al.Quantum McEliece public-key cryptosystem based on quantum QC-LDPC codes[J].Journal of Nanjing University of Posts and Telecommunications (Natural Science),2011,31(2):64–68.[曹东,赵生妹,宋耀良,等.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.]

[18] Huffman W C,Pless V.Fundamentals of error-correcting codes[M].Cambridge:Cambridge University Press,2003.

[19] Calderbank A R,Rains E M,Shor P W,et al.Quantum error correction via codes over GF(4)[J].IEEE Transactions on Information Theory,1998,44(4):1369–1387.

[20] Aly S A,Klappenecker A,Sarvepalli P K.On quantum and classical BCH codes[J].IEEE Transactions on Information Theory,2007,53(3):1183–1188.

[21] Wang Liqi,Zhu Shixin.On the construction of optimal asymmetric quantum codes[J].International Journal of Quantum Information,2014,12(3):1450017.

[22] Zhang Huanguo,Mao Shaowu,Wu Wanqing,et al.Overview of quantum computation complexity theory[J].Chinese Journal of Computers,2016,39(12):2403–2428.[张焕国,毛少武,吴万青,等.量子计算复杂性理论综述[J].计算机学报,2016,39(12):2403–2428.]

[23] Dinh H,Moore C,Russell A.McEliece and Niederreiter cryptosystems that resist quantum fourier sampling attacks[M]//Advances in Cryptology—CRYPTO 2011.Heidelberg:Springer-Verlag,2011:761–779.

[24] Courtois N T,Finiasz M,Sendrier N.How to achieve a McEliece-based digital signature scheme[M]//Advances in Cryptology ASIACRYPT 2001.Heidelberg:Springer-Verlag,2001:157–174.

[25] Liu Jinhui,Jia Jianwei,Zhang Huanguo,et al.Digital signature protocol based on error-correcting code[J].Journal of Huazhong University of Science and Technology (Natural Science Edition),2014,42(11):97–101.[刘金会,贾建卫,张焕国,等.一种基于纠错码的数字签名协议[J].华中科技大学学报(自然科学版),2014,42(11):97–101.]

（编辑　赵　婧）

引用格式：Han Haiqing,Zhang Huanguo,Zhao Bo,et al.Research on McEliece and Niederreiter public-key cryptosystem algorithm based on quantum BCH codes[J].Advanced Engineering Sciences,2018,50(5):152–159.[韩海清,张焕国,赵波,等.基于量子BCH码的McEliece及Niederreiter公钥密码算法研究[J].工程科学与技术,2018,50(5):152–159.]