基于最大 F 距离码的 McEliece 公钥密码体制

韩 牟[1] 张 宏[1] 叶有培[1] 许春根[2]

(南京理工大学计算机学院 南京 210094)[1] (南京理工大学理学院 南京 210094)[2]

摘 要 基于 F 度量,构造了最大 F 距离码,提出了基于最大 F 距离码的新 McEliece 公钥密码系统。合法接收者通过引入一个随机矩阵 X 作为附加私钥,并把 X 加入到原始公钥中,从而产生了一个新的公钥,使该密码系统能够有效抗击敌手通过已知的公钥获得私钥的攻击。同时 F 度量的引入,提高了攻击密钥体积较小的公钥密码系统的复杂度和难度。通过对现有可行攻击方法的分析,说明了基于最大 F 距离码的新 McEliece 公钥密码系统是安全可行的。

关键词 F 度量,最大 F 距离码,新 McEliece 公钥密码系统,安全性

中图法分类号 TP309 **文献标识码** A

McEliece Public-key Cryptosystem Based on the Maximum *F*-distance Code

HAN Mu[1] ZHANG Hong[1] YE You-pei[1] XU Chun-geng[2]

(School of Computer Science and Technology, NUST, Nanjing 210094, China)[1] (Science of Mathematics, NUST, Nanjing 210094, China)[2]

Abstract In terms of F-metric, the maximum F-distance code was constructed, a new modification of the McEliece public key cryptosystem based on maximum F-distance codes was proposed. The legal party chooses a random matrix as an extra secret key and adds it to the original public key to produce a new modified public key. It makes such cryptosystem effective for resisting the attack based on getting private keys from known public keys. Moreover, using F-metric increases the complexity of the system, making it harder to attack allowing for smaller key sizes. Attacks on such a system were also investigated. It is shown that the McEliece public key cryptosystem based on maximum F-distance codes is security and feasibility.

Keywords F-metric, Maximum F-distance code, New McEliece public key cryptosystem, Security

随着纠错码与密码理论的深入研究,基于汉明度量和基于秩度量的线性码在密码学中得到广泛应用。McEliece 根据一般线性码的译码问题是一个 NPC 问题和 Goppa 码具有快速译码算法的特点,最早提出了一个基于纠错码的公钥密码体制[1]。随后 Niederreiter 提出了另一个基于纠错码的公钥密码体制,该体制隐藏了具有快速译码算法的广义 RS 码的校验矩阵[2]。1985 年,俄国学者 Gabidulin 首先提出了秩距离码[3],至今利用秩距离码构造的各种密码系统已经被广泛研究[4-6],但文献[7]中的研究结果表明基于秩距离码的公钥密码系统是不安全的。

1998 年,俄国学者 Gabidulin 在文献[8]中介绍了一类新的度量,即 F 度量。随后基于 F 度量的纠错码开始得到国内外一些学者的关注,但迄今为止深入的研究还不多。本文基于 F 度量构造了最大 F 距离码,提出了基于最大 F 距离码的新的 McEliece 公钥密码系统。说明该系统能够有效抗击敌手想通过已知的公钥获取私钥的攻击。由于 F 度量及基于 F 度量码的特点,使得该密码系统可以抵抗对密钥体积较小的公钥密码系统的攻击。本文最后通过对现有可行的攻击方法的分析,证明了新的 McEliece 公钥密码系统的可行性与安全性。

1 基本概念

1.1 McEliece 公钥密码体制

1978 年,McEliece 根据一般线性码的译码问题是一个 NPC 问题,最早提出了一个基于纠错码的公钥密码体制[1]。McEliece 公钥密码体制的对偶体制,即 Niederreiter 公钥密码体制[2],是基于寻找一般线性码陪集中的陪集首的困难性而提出的。

对于一个给定的码 C,McEliece 公钥密码体制与 Niederreiter 公钥密码体制是等价的。这两个密码体制都使用了具有快速译码算法且通过快速译码算法可纠正 t 个错误的[n, k]线性码。

McEliece 公钥密码体制与 RSA 公钥密码体制相比的主要优点是,用 McEliece 公钥密码体制加密(解密)每信息比特所需的二元运算数小于 RSA 公钥密码体制。

与 RSA 公钥密码体制相比,McEliece 公钥密码体制的主要缺点是,其公钥体积过大,需要占用较大的存储空间。表 1 列出了 McEliece 公钥密码体制与 RSA 公钥密码体制的特点。

到稿日期:2009-06-22 返修日期:2009-09-01 本文受某部委十一五重点预研项目,国家自然科学基金重大研究计划(90718021)资助。

韩 牟(1980—),女,博士生,主要研究方向为信息安全,E-mail:hanmu8098@126.com;张 宏(1956—),男,教授,博士生导师,主要研究方向为信息安全、数据挖掘,E-mail:zhhong@mail.njust.edu.cn(通信作者)。

表 1　McEliece 与 RAS 的特点

特征 \ 密码体制	McEliece 公钥密码体制 [1024,524,101] 二元不可约 Goppa 码	RSA 公钥密码体制模为 1024-bit,公钥指数为 17
公钥体积	67072 bytes	256 bytes
加密每信息比特所需的二元运算数	514	2402
解密每信息比特所需的二元运算数	5140	738112

1.2　F 度量

设 Ω 表示有限域 F_q 上的一个 n 维向量空间，若 X 为 Ω 的一个非空子集，则称包含 X 的 Ω 的最小线性子空间 F_X 为 X 的张成，记为 $span\langle X\rangle$。

设 F 由 Ω 的一类子空间 F_i 组成，记 $F=\{F_1,F_2,\cdots,F_N\}$，其中 $F_i\subset\Omega$ 且 $span\langle\bigcup_{i=1}^{N}F_i\rangle=\Omega$。

定义 1　设 $\vec{x}=(x_1,x_2,\cdots,x_n)$ 和 $\vec{y}=(y_1,y_2,\cdots,y_n)$ 为 Ω 中的两个向量，则向量 $\vec{x}$ 的 F 范数或 F 权定义为最小子集 I 的基数，其中 $I\subset\{1,2,\cdots,N\}$ 且 $x\in\langle\bigcup_{i\in I}F_i\rangle$。$F$ 范数记为 $N_F(x)$。而向量 $\vec{x}$ 和 $\vec{y}$ 之间的 F 距离是指它们差的范数，表示成 $d_F(x,y)$，即 $d_F(x,y)=N_F(x-y)$。

定义 2　Ω 的非空子集合 C 叫做码，C 中的向量叫做码字。

定义 3　定义码 C 的最小距离为不同码字之间 F 距离的最小值，可表示成 $d_F(C)$，即 $d=d_F(C)=\min\{d_F(x,y)\mid x,y\in C,x\neq y\}$。

定义 4　如果组成类 $F=\{F_1,F_2,\cdots,F_N\}$ 的所有元素为 ${F_q}^N$ 上的向量，那么由这个类生成的度量称之为射影 F 度量。可将类 F 中的所有元素记为 f_i，即 $F=\{f_1,f_2,\cdots,f_N\}$。

命题 1(广义 Singleton 界)　如果存在 q 元(n,k,d_F)码，则 $d_F\leqslant n-k+1$。

1.3　Parent 码

设 φ 为从 F_q^N 到 Ω 的一个映射，$\varphi:F_q^N\to\Omega$，使得 $\varphi(e_i)=f_i$ $(i=1,\cdots,N)$ 成立。其中 $\{e_1,e_2,\cdots,e_N\}$ 为 F_q^N 的标准基，且 $f_i\in F$。

定义 5　φ 的核 $P:=ker\varphi\subset F_q^N$ 称为 Parent 码。若 $\forall x\in\Omega$，则有 F_q^N 中的 Parent 码 P 的一个陪集 D 存在，$D=\varphi^{-1}(x)$。设 $F_q^N\backslash P$ 表示 P 的陪集的集合，则由纠错码理论知，$D\in F_q^N\backslash P$ 的陪集首为 D 中具有最小汉明重量的元素，并且陪集首的汉明重量即为陪集 D 的汉明重量，记为 $w(D)$。

下面两个命题给出了 F 度量与汉明度量的关系。

命题 2　$\forall x\in\Omega$，则有 $N_F(x)=w(\varphi^{-1}(x))$。

命题 3　$d_H(\varphi^{-1}(D))=\min(d_F(D))$。

$P:=ker\varphi\subset F_q^N$ 为 Parent 码，$\forall X\in ker\varphi$，存在 F_q^n 中的矩阵 F，使得 $FX=0$。矩阵 F 列向量即为向量 $\varphi(e_i)=f_i$，$i=1,2,\cdots,N$。由此可知 Parent 码 P 为一个以 F 为校验矩阵的 $[N,N-n]$码。

2　最大 F 距离码的构造

2.1　Vandermonde F 度量

设 F 为 F_q 上的一个广义 Vandermonde 矩阵，即

$$F=\begin{pmatrix}u_1 & u_2 & \cdots & u_N\\ u_1x_1 & u_2x_2 & \cdots & u_Nx_N\\ \cdots & \cdots & \cdots & \cdots\\ u_1x_1^{n-1} & u_2x_2^{n-1} & \cdots & u_N^{n-1}x_N^{n-1}\end{pmatrix}\quad(n\leqslant N)$$

其中，x_i 为 F_q 中互不相同的元素，u_i 为 F_q 中的非零元素。

设 f_i 为矩阵 F 的列向量，则有 $f_i\subset\Omega\langle\bigcup_{i=1}^{N}f_i\rangle=\Omega(i=1,2,\cdots,N)$，那么由 F 度量的概念可知，向量 $f_1,f_2,\cdots,f_N$ 定义了一个 F 度量，即 $F=\{f_1,f_2,\cdots,f_N\}$，称为 Vandermonde F 度量。以 F 为校验矩阵的 Parent 码 P 为一个广义 RS 码。

2.2　最大 F 距离码

定义 6　设 C 是 q 元$[n,k,d_F]$码，如果 $d_F(C)=n-k+1$，则 C 叫做最大 F 距离码。

设 C 是参数为$[n,k]$的 q 元线性码，取 C 的一组 q-基$\{v_1,v_2,\cdots,v_k\}$，$v_i=(g_{i1},\cdots,g_{in})(1\leqslant i\leqslant n)$，其中 $g_{ij}\in F_q(1\leqslant j\leqslant n,1\leqslant i\leqslant k)$，则每个码字可唯一地表示成 $c=b_1v_1+b_2v_2+\cdots+b_kv_k=(b_1,b_2,\cdots,b_k)G,(b_1,b_2,\cdots,b_k\in F_q)$，$G$ 是 F_q 上秩为 k 的 $k\times n$ 矩阵，

$$G^T=(v_1,v_2,\cdots,v_k)=\begin{pmatrix}g_{11} & \cdots & g_{k1}\\ g_{12} & \cdots & g_{k2}\\ \vdots & \cdots & \vdots\\ g_{1n} & \cdots & g_{kn}\end{pmatrix}$$

则 G 叫做线性码 C 的一个生成矩阵。可以先把 $K=q^k$ 个信息编成 F_q^k 中的向量 $b=(b_1,b_2,\cdots,b_k)^T$(共 q^k 个)，为了纠错，再把它们编成 C 中的码字 $c=G^Tb$ 。

设 $G^T=\begin{pmatrix}v_1 & v_2 & \cdots & v_k\\ v_1y_1 & v_2y_2 & \cdots & v_ky_k\\ \vdots & \vdots & \cdots & \vdots\\ v_1y_1^{n-1} & v_2y_2^{n-1} & \cdots & v_ky_k^{n-1}\end{pmatrix}$，其中 v_i 为 F_q 上的非零元素，y_i 为 F_q 上两两互不相同的元素。令 $x_i\neq y_i$，则$(F|G^T)$为广义 Vandermonde 矩阵，

$$(F|G^T)=\begin{pmatrix}u_1 & u_2 & \cdots & u_N & v_1 & v_2 & \cdots & v_k\\ u_1x_1 & u_2x_2 & \cdots & u_Nx_N & v_1y_1 & v_2y_2 & \cdots & v_ky_k\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ u_1x_1^{n-1} & u_2x_2^{n-1} & \cdots & u_N^{n-1}x_N^{n-1} & v_1y_1^{n-1} & v_2y_2^{n-1} & \cdots & v_ky_k^{n-1}\end{pmatrix}$$

命题 4　若 G^T 为 q 元线性码 C 生成矩阵的转置矩阵，则码 C 为最大 F 距离码，且可纠正 $t_k=[\frac{n-k}{2}]$位错。

证明：设 g 为一个码向量，$g^T=a^TG$，其中 $a=(a_1,a_2,\cdots,a_k)^T$，$W_H(a)=s\neq0$，则 $g=a_{j1}g_{j1}+a_{j2}g_{j2}+\cdots+a_{js}g_{js}$。设 $N_F(g)=l$，由 F 范数的定义可知 $g=b_1f_{i1}+b_2f_{i2}+\cdots+b_lf_{il}$，其中 b_i 为非零元素。由 $g=b_1f_{i1}+b_2f_{i2}+\cdots+b_lf_{il}=a_{j1}g_{j1}+a_{j2}g_{j2}+\cdots+a_{js}g_{js}$ 可知广义 Vandermonde 矩阵(F|G^T)中的 $l+s$ 个互不相同的列 $f_{i1},f_{i2},\cdots,f_{il},g_{j1},g_{j2},\cdots,g_{js}$ 为线性相关的，所以有 $l+s\geqslant n+1$，即 $N_F(g)\geqslant n-s+1$。因此 $d_F\geqslant n-k+1$，又由 Singleton 界可知 $d_F=n-k+1$。

设 c 为接收到的信息，则由纠错码理论知 $c=g+e$，其中 g 为一个码向量而 e 为差错向量。设 t 为差错向量 e 的 F 权，即 $t=N_F(e)$，若 $t\leqslant t_k$，则可以使用广义 RS 码的快速译码算法对基于最大 F 距离码进行快速译码。

3　基于最大 F 距离码的公钥密码体制

3.1　方案构造

设 C 为 $GF(q)$上的一线性最大 F 距离码，在 F 度量下，码 C 具有快速译码算法，$G^T=(v_iy_i^j)$ $(i=1,\cdots,k;j=0,\cdots,n-1)$为码 C 生成矩阵的转置矩阵，S 为有限域 $GF(q)$ 上 $k\times$

k 非奇异矩阵。

• 私钥：X,S,G^T。

• 公钥：$G_{pub}^T=G^TS+X$，其中 X 为秩为 1 的矩阵，矩阵 X 的选择遵循如下条件。

(1)在给定的最大 F 距离码任意陪集中选择 F 范数为 $d_F-1=n-k=2t_k=r$ 的陪集首，记为 $x=(x_1,x_2,\cdots,x_n)$，$x_i\in GF(q)$。

(2)计算 $X=x^Ta$，$a=(a_1,a_2,\cdots,a_k)$ 为随机选取的向量，a_i 为 $GF(q)$ 中的非零元素。

• 加密：$c=G_{pub}^Tm+e$，其中 $m=(m_1,m_2,\cdots,m_k)^T$ 为由 k 个信息位组成的明文消息，$e=(e_1,e_2,\cdots,e_n)^T$ 为随即选取的向量，且 $N_F(e)\leqslant t_k-1$。

• 解密：由 $c=G_{pub}^Tm+e$ 有 $c=(G^TS+X)m+e=G^TSm+Xm+e$。消息的合法接收者知道 $Xm=x^T\lambda$，其中 λ 仅取决于明文 m，x 对于合法的接收者来说是已知的。消息的合法接收者需要进行两次解密才能得到明文消息 m。

3.2 安全性分析

对基于线性码的公钥密码系统有两种攻击方法，即直接攻击方法与结构攻击方法。

直接攻击，即敌手将密文看作是在有限域 F_q 上随机选取的码，使用一般线性码的译码算法进行译码，但随着密钥体积的增加使用直接攻击方法攻击基于纠错码的密码体制已经是不可行的，因此结构攻击方法引起了广泛的关注。结构攻击分为由公钥获得私钥的攻击方法和敌手通过截获的密文获得明文的攻击方法。下面通过对结构攻击方法的分析来说明基于最大 F 距离码的 McEliece 公钥密码系统是安全可行的。

攻击方法 1(由公钥获得私钥)　1992 年，Sidelnikov 与 Shestakov 给出了一个可以在多项式时间内恢复广义 Reed-Solomon 码结构的算法，使用这个攻击方法可以完全攻破基于广义 Reed -Solomon 码的公钥密码体制[11]。本文所给出的最大 F 距离码的生成矩阵为广义 Vandermonde 矩阵，在基于 F 度量的 McEliece 公钥密码体制中，合法接收者通过引入一个随机矩阵 X 作为附加私钥，并把 X 加入到原始公钥中，产生了一个新的公钥 $G_{pub}^T=G^TS+X$，从而使敌手很难通过公钥 G_{pub}^T 来获得私钥 G^T，使得基于最大 F 距离码的 McEliece 公钥密码体制能够有效抗击该攻击方法。

攻击方法 2(检验可能的明文消息)　1988 年，Lee 和 Brickell 给出了一种用信息集译码的方法攻击基于二元不可约 Goppa 码的 McEliece 公钥密码体制[12]，但这种攻击方法不适用于基于 F 度量的 McEliece 公钥密码体制。

敌手可以通过检验每一个可能的明文消息来攻击基于最大 F 距离码的 McEliece 公钥密码体制。

设 m^{test} 为待检验的明文消息，敌手首先计算 $G_{pub}^Tm^{test}$，接着计算截获的密文 c 与 $G_{pub}^Tm^{test}$ 差的 F 范数，若 $N_F(c-G_{pub}^Tm^{test})<t_k-1$，则 m^{test} 为原始的明文消息。使用这种攻击方法所需的计算量为：$(q-1)^k$。

例 1　$q=2^8$，$n=60$，$k=20$，$t_k=\left[\frac{n-k}{2}\right]=20$，则可知公钥 G_{pub}^T 的体积为 9600bytes，使用攻击方法 2 的计算量为 $(q-1)^k\approx2^{159}$。

通过对攻击方法 2 的分析及例 1 说明了，对基于最大 F 距离码的新 McEliece 公钥密码系统可以选取较小的参数获得比较大的工作因子，从而提高了攻击密钥体积较小的公钥密码系统的复杂度和难度，同时还可以减少密钥的存储空间。

由上述安全性分析可知，现有可行的攻击方法不适于新的 McEliece 公钥密码系统，因此该公钥密码体制是安全可行的。

结束语　本文基于 F 度量，提出了基于最大 F 距离码的新 McEliece 公钥密码体制，并说明了它的可行性与安全性。但随着基于 F 度量码的新译码算法的提出，它的安全性还需要进一步研究。

参 考 文 献

[1] McEliece R J. A Public-key Cryptosystem Based on Algebraic Coding Theory[R]. Jet Propulsion Lab. DSN Progress Reprot. 1978

[2] Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory[J]. Probl. Control Inform. Theory, 1986, 15(2): 159-166

[3] Gabidulin E M. Theory of Code with Maximum Rank Distance [J]. Problem of Information Tarnsmission, 1985, 21(1): 1-12

[4] Gabidulin E M, Paramonov A V, Tretjakov O V. Ideals over a Non-Commutative Ring and their Application in Cryptology[A]// Proceeding of EUROCRYPT'91, Lecture Notes in Computer Science [C]. Springer-Verlag, 1991: 482-489

[5] 杜伟章，王新梅. 基于最大秩距离码的 Stern 方案[J]. 软件学报，2001，12(10)：1552-1554

[6] 杜伟章，王新梅. 基于最大秩距离码的两种 Rao-Nam 方案[J]. 通信学报，2002，23(10)：1-5

[7] Overbeck R. Structural Attack for Public key Cryptosystems based on Gabidulin Codes [J]. Journal of Cryptology, 2008, 21: 280-301

[8] Gabidulin E M, Simonis J. Metrics Generated by Families of Subspace[J]. IEEE Trans. Inf. Theory, 1998, 44(5): 1336-1341

[9] Li X Y, Deng R H, Wang X M. On the equivalence of McEliece's and Niederreiter's Public-key Cryptosystems[J]. IEEE Transacions on Information Theory, 1994, 40(1): 271-273

[10] Canteaut A, Sendrier N. Cryptanalysis of the original McEliece cryptosystem [A]// Proceeding of ASIACRYPT'98 Lecture Notes in Computer Science[C]. Springer-Verlag, 1998: 187-199

[11] Sidelnikov V M, Shetakov S O. On the Cryptosystem Based on Generalized Reed-Solomon Codes [J]. Discrete Math, 1992, 3(3)

[12] Lee P J, Brickell E F. An observation on the secutity of McEliece's public-key Cryptosystem [A]// Proceeding of EUROCRYPT'88, Lecture Notes in Computer Science [C]. Springer-Verlag, 1988: 275-280

[13] 李元兴. 纠错码在现代密码学中的应用[J]. 通信学报，1991，9(4)：102-106

[14] 王新梅，李元兴，武传坤. McEliece 公钥体制修正[J]. 电子学报，1994，22(4)：90-92