第15卷 第2期 电子科学学刊 Vol. 15 No. 2
1993年3月 JOURNAL OF ELECTRONICS Mar., 1993

用 BCH 等线性分组码构造 McEliece 纠错码公钥密码体制*

李 元 兴
(北京邮电学院信息工程系,北京 100088)

摘要 McEliece 公钥密码体制是用线性纠错码中的一种特殊码类 Goppa 码构造的. 本文则表明采用 BCH 码或 RS 码等线性分组码也可构造安全的 McEliece 公钥密码体制 .

关键词 密码学; McEliece 公钥密码体制;纠错码

1. 引言

1978年, McEliece[1] 采用纠错码构造了一类公钥密码体制 (下简称 M 公钥体制). M公钥体制是最基本的一类纠错码密码体制, 它是解决加密与纠错相结合这一课题的基础,因而有着特别重要的意义. 迄今为止,已有许多学者对M公钥体制做了深入分析, 但这些分析主要集中在M公钥体制的安全性、提高码率和修改M公钥体制等方面,而关于M公钥体制的其它一些问题,如除 Goppa 码外, 如何用其它线性分组码构造安全的M公钥体制,则一直没有引起人们的注意,但这是一个很有现实意义的问题. 因为实际使用的纠错码大多是 BCH 码、RS 码和级联码,而不是 Goppa 码.

本文旨在表明如何采用 BCH 码和 RS 码等其它线性分组码构造安全的M公钥体制.

2. M 公钥体制简介

设码 C 是有限域 GF(2) 上的 (n,k,t) 即约 Goppa 码, 码长 $n=2^m$, 维数 $k \geqslant n-mt$, t 是 C 的纠错能力. 设 G 和 H 分别是 C 的 GF(2) 上的 $k \times n$ 阶生成矩阵和 $(n-k) \times n$ 阶一致校验矩阵. 令 S 和 P 分别代表 GF(2) 上的 $k \times k$ 阶随机满秩矩阵和 $n \times n$ 阶随机置换矩阵, 则 G,S 和 P 是秘密钥, G' 是公开密钥. 这里 $G'=SGP$.

设明文是 k 比特组. 令 $\underline{m}$ 是任意明文,则加密方程为

$$\underline{c}=\underline{m}G'+\underline{z} \tag{1}$$

(1)式中 $\underline{z}$ 是发方随机产生的重量为 t 的 n 比特矢量, $\underline{c}$ 是 $\underline{m}$ 的密文.

解密算法如下:

(1) 计算 $\underline{c}'$: $\underline{c}'=\underline{c}P^{-1}=\underline{m}SG+\underline{z}P^{-1}$.

(2) 计算 $\underline{c}'H^T$: $\underline{c}'H^T=\underline{z}P^{-1}H^T$. 对伴随式 $\underline{c}'H^T$ 做快速译码, 因 $\underline{z}P^{-1}$ 的重量为 t, 故译码得到 $\underline{m}S$.

1991.10.19 收到, 1992.03.06 定稿.
* 国家自然科学基金资助课题.
李元兴 男, 1966年生,博士后,现主要从事领域为信道编码、信息保密及其在数字移动通信等中的应用.

(3) 对 mS 右乘 S^{-1}，从而恢复明文 m.

目前主要有两种攻击M公钥体制的方法. 这两种方法均不能破译M公钥体制. 关于这两种攻击方法的介绍请参看文献[2].

3. 用 CBH 码等构造安全的 M 公钥体制

本节实际上就是要解决这样一个问题，即用其它线性分组码构造安全的M公钥体制. 首先讨论一下基于其它线性分组码的M公钥体制与基于 Goppa 码的M公钥体制有何实质上的区别. 当然应假定"其它线性分组码"是具有快速译码算法的码类，如 BCH 码，RS 码，否则即使是合法接收者也难以正确解密. BCH 码是实际中最常用的码类，因此下面以 BCH 码为例，分析用 BCH 码构造的M公钥体制与用 Goppa 码构造的有何不同.

定理 1　GF(2) 上相同参数的 (n,k,t) BCH 码的数目 $N_B < n^2$.

证明　由代数编码理论可知，一个设计纠 t 个错误的二元 BCH 码，其生成多项式 $g(x)$ 包含有 $2t$ 个接连根. 设 $2t$ 个接连根是 $\alpha^b, \alpha^{b+1}, \alpha^{b+2}, \cdots, \alpha^{b+2t-1}$. 这里 b 是正整数，α 是 GF(2^m) 中的 n 次单位元，m 是满足 $n/(2^m-1)$ 的最小正整数. GF(2^m) 中以 n 次单位元表示的任何 $2t$ 个接连根均可作为 $g(x)$ 的根，用来设计产生 (n,k,t) BCH 码. 因为 GF(2^m) 中 n 次单位元共有 $\varphi(n)$ 个，且对每一个单位元，b 可取 $0,1,\cdots,n-1$，因此以 n 次单位元表示的 $2t$ 个接连根的可能数目就为 $n\varphi(n)$，故可能的 (n,k,t) BCH 码的数目 N_B 等于 $n\varphi(n)$ (其中包括有完全相同的 BCH 码). 因为 $\varphi(n) \leqslant n-1$，故 $N_B < n^2$.　证毕

若是二元本原 BCH 码，则 $n = 2^m - 1$，$k \geqslant n - mt$. 这与二元即约 Goppa 码相似. 译 BCH 码的计算复杂度为 $O(n\log n)$[3].

我们知道，相同参数的 (n,k,t) 即约 Goppa 码的数目 $N_G \approx 2^{mt}/t$. 译 Goppa 码的计算复杂度为 $O(n\log^2 n)$.

上述结果表明，尽管 Goppa 码、BCH 码的译码均存在快速算法，但它们相同参数的码的数目却大不一样. 对 Goppa 码，当 $n = 1024$，$t = 50$ 时，$N_G \approx 2^{500}$. 因此密码分析者要猜出体制设计者随机选用的秘密钥 G 是没有希望的. 但对 BCH 码，当 $n = 1024$ 时，N_B 小于 2^{20}，因此密码分析者很容易猜出体制设计者随机选定的秘密钥 G. 可见，用 BCH 码构造的M公钥体制很容易泄露体制选用的秘密钥 G，而用 Goppa 码构造的体制则不会泄露秘密钥 G.

那么泄露 G 对体制的安全性有无影响呢？这里不妨假设下面的 M 公钥体制是用 BCH 码构造的.

显然，用 BCH 码构造的M公钥体制与用 Goppa 码构造的M公钥体制具有完全相同的加密、解密算法. 此处省略体制加密、解密的具体步骤. 令 G 是 (n,k,t) BCH 码的 $k \times n$ 阶生成矩阵，S 和 P 分别与本文第二节中的相同，则 $G' = SGP$. 体制秘密钥为 S，G，P，公开密钥为 G'. 对 k 长明文 m，密文 $c = mG' + z$. z 仍是二元、重量为 t 的 n 长随机矢量.

下面分析这种体制的安全性.

类似于 Goppa 码M公钥体制的安全性分析，这里也有两种攻击体制安全性的方法，即方法 1 与方法 2.

因为 G' 组合等价于 BCH 码的生成矩阵 G，且代表的是一个一般线性分组码的生成矩阵，因此已知 G' 和 c，解方程 $c = mG' + z$，求 m，所需的最低工作因子为 $W = k^3\binom{n}{k}\Big/\binom{n-t}{k}$，是指数时间算法，不能破译体制．这就是方法 2.

下面重点讨论方法 1，即从 G' 中分解出 S, G 与 P.

定理 2 设 S, G 分别是 GF(2) 上的 $k \times k$ 阶满秩矩阵和 $k \times n$ 阶秩为 k 的矩阵．令 $G_1 = SG$，当 G 固定，而 S 取遍所有 $k \times k$ 阶满秩矩阵时，可能的 G_1 的数目与可能的 S 的数目相同，都为 $N_S = 2^{k^2}\prod_{i=1}^{k}(1-2^{-i})$.

证明 设 S_1 和 S_2 是 GF(2) 上的任意两个 $k \times k$ 阶满秩矩阵，且 $S_1 \neq S_2$．若 $S_1G = S_2G$，则 $(S_1 - S_2)G = 0$．因 G 是秩为 k 的矩阵，因而 G 中 k 行线性独立，故必有 $S_1 - S_2 = 0$．这与条件相矛盾．因此当 $S_1 \neq S_2$ 时，有 $S_1G \neq S_2G$．所以可能的 G_1 的数目就等于可能的 S 的数目，都为 N_S．而 $N_S = 2^{k^2}\prod_{i=1}^{k}(1-2^{-i})$[2]． 证毕

定理 3 设 G, P 分别是 GF(2) 上的 $k \times n$ 阶秩为 k 的矩阵和 $n \times n$ 阶置换矩阵．令 $G_2 = GP$，当 G 固定，P 取遍 $n!$ 种可能的置换矩阵时，可能的 G_2 的数目至少为 $k!$.

证明 因为 G 的秩为 k，所以 G 中一定存在 k 个线性独立的列向量，且它们互不相同．当对 G 实施 $n!$ 种可能的列置换时，则至少有 $k!$ 种置换，其置换结果互不相同，因而可能的 G_2 的数目就至少为 $k!$． 证毕

定理 4 在M公钥体制中，公钥 $G' = SGP$．若已知 G' 和 G，仍难以求得 S 和 P.

证明 (1) 令 $G_1 = SG$，则 $G' = G_1P$．由定理 2 可知，可能的 G_1 的数目为 $N_S > 2^{k^2}\prod_{i=1}^{k}(1-2^{-i})$，而可能的 P 的数目为 $n!$．因此从 G' 中恰好分解出 G_1 和 P 是很难的．G_1 难以获得，则 S 也难以求得．所以 S 和 P 均难以获得．(2) 令 $G' = SG_2$，$G_2 = GP$．由定理 3 可知，可能的 G_2 的数目至少为 $k!$，又因可能的 S 的数目为 $N_S > 2^{k^2}\prod_{i=1}^{k}(1-2^{-i})$，所以从 G' 中恰好分解出 S 和 G_2 是难以实现的．由于难以求得 G_2，当然也难求得 P．故 S 和 P 均难以求得．(3) 因 $G' = SGP$，故 $(G')^T = P^TG^TS^T = P^{-1}G^TS^T$．所以 $G'(G')^T = SGPP^{-1}G^TS^T = SGG^TS^T$．令 $\tilde{G}' = G'(G')^T$，$\tilde{G} = GG^T$，则

$$\tilde{G}' = S\tilde{G}S^T \tag{2}$$

已知 G' 和 G，求 S 和 P，转化为已知 $\tilde{G}'$ 和 $\tilde{G}$，求满足(2)式的 S．一旦 S 求得，则 P 也可求得．

展开(2)式，得到 nk 个联立的 k^2 元二次非线性方程组．从目前已有的结果看，尚没有求解二次非线性方程组的有效算法，所以求解(2)式是很难的．因 S 难以求，故 P 也就难以得到．

综上分析表明，在M公钥体制中，即使已知秘密钥 G，仍难以求得另外两个秘密钥 S 和 P． 证毕

由文献[4]的结论知，若得不到 S 和 P，则很难在 G' 和 G 之间找到映射关系，因而不能破译M公钥体制.

定理 5　GF(2) 上的 BCH 码可用于构造安全的M公钥体制.

定理 5 对 RS 码或其它具有快速译码算法的线性分组码也同样适用.

我们的分析表明，M公钥体制的构造，可不局限于 Goppa 码，这是很有实际意义的.

必须指出，定理 4 和定理 5 是基于求解难题，即求解二次非线性方程组. 若找到了解二次非线性方程组的有效算法，则定理 4 和定理 5 就不再成立了. 这时安全的M公钥体制就必须采用 Goppa 码构造.

参　考　文　献

[1] R. J. McEliece, DSN Propress Report, Jet Propulsion Laboratory, Pasadema, Jan./Feb., (1978), pp. 114—116.

[2] T. R. N. Rao, K. H. Nam, *IEEE Trans. on IT*, **IT-35**(1989)4, 829—833.

[3] F. J. Macwilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, Part I, North-Holland, Oxford, (1977), Ch. 12.

[4] C. M. Adams, H. Meijer, *IEEE Trans. on IT*, **IT-35**(1989)2, 454—455.

USING BCH OR OTHER LINEAR BLOCK CODES TO CONSTRUCT MCELIECE'S PUBLIC-KEY CRYPTOSYSTEM

Li Yuanxing

(Beijing University of Posts and Telecommunications, Beijing 100088)

Abstract　McEliece's public-key cryptosystem was constructed with the Goppa codes. This paper shows other linear block codes, i.e., BCH codes or RS codes, can also be used to construct secure McEliece's cryptosystem.

Key words　Cryptology; McEliece's public-key Cryptosystem; Error-correcting codes