关于 McEliece 公钥体制的安全性*

隆永红

（中国科学院软件研究所，北京 100080）

（湘潭大学计算机科学系，湘潭 411105）

摘要　本文证明了 McEliece 公钥体制中的公开钥矩阵实际上就是一个 Goppa 码生成矩阵，指出 Adams 和 Meijer 对 McEliece 公钥体制安全性分析的不合理之处. 本文的结果对 Korzhik_Turkin 攻击是一种理论上的支持，并与一类基于纠错码的公钥体制的安全性密切相关.

关键词　公钥体制，纠错码，Goppa 码，密码分析.

1978 年 McEliece[1]基于纠错码理论提出了一种双钥密码体制. 在该体制中，一个 k 位明文消息 m 被加密成 $c=mG'+e$，其中“+”表示模 2 加法. $k\times n$ 矩阵 $G'=SGP$，其中 S 为 $k\times k$ 二元非奇异阵，P 为 $n\times n$ 置换矩阵，G 为某最小距离为 d 的 Goppa 码的生成矩阵. 与背包体制和 RSA 体制相比，McEliece 体制是有其独特之处的. 从 Brickell 和 Odlyzko 在其综述性文章[2]中把它列为单独的一类体制这一点，不难看出 McEliece 体制的代表意义. 关于该体制的安全性分析，1991 年以前的结论都是肯定的[2-5]，即认为 McEliece 体制是相当安全的，因此不断地有一些新的基于纠错码的单钥或双钥体制提出[4]. 尤其是 Adams 和 Meijer[5]的分析结果，更是激发了不少学者对纠错码体制的兴趣. 文献[6－8]就先后提出了基于纠错码的签名、加密和融签名加密纠错为一体的公钥体制，其中文献[6,7]中的数字签名方案已被笔者攻破[9].

在 1991 年的欧洲密码学会议论文集里，有两篇关于 McEliece 体制安全性分析的文章. 一篇是 Korzhik 和 Turkin 的文章[10]，提出了一种基于迭代优化算法[11]的对 McEliece 体制的实际上有效的攻击方法，并对 Adams 和 Meijer[5]的分析结果提出了质疑. 另一篇是 Gibson 的文章[12]，证明了与文献[5]截然相反的结论，指出每一个 McEliece 体制的实例都有许多陷门. 但从这些文献的内容来看，其作者似乎都把 G' 当成一个一般的满秩阵来对待. 笔者在此证明，McEliece 体制中的公开钥矩阵 G' 实际上就是一个 Goppa 码的生成矩阵，从而解释了文献[5]中得出的结论与实际情况相反的原因，对 Korzhik_Turkin 攻击也是一种理论上的支持.

本文的结果与一类基于纠错码的公钥体制的安全性密切相关.

---

* 本文 1993－11－12 收到，1994－06－20 定稿

作者隆永红，1964 年生，在读博士，主要研究领域为分布式数据库，计算机软件，密码学，自动机理论.

本文通讯联系人：隆永红，北京 100080，中国科学院软件研究所

1 有关 Goppa 码的一个平凡性质

用 $V_n(q)$ 表示 $GF(q)$ 上 n 维向量空间,S_n 表示 $\{1,2,\cdots,n\}$ 上所有置换的集合.

定义 1.[13]设 $g(z)$ 是 $GF(q^m)$ 上 t 次首一多项式,$L=\{\alpha_1,\cdots,\alpha_n\}\subset GF(q^m)$,使得 $|L|=n$ 而且 $g(\alpha_i)\neq 0$,对 $1\leqslant i\leqslant n$. 定义 Goppa 多项式为 $g(z)$ 的 Goppa 码 $\Gamma(L,g)$ 为字母表 $GF(q)$ 上所有满足下式的码字 $c=(c_1,c_2,\cdots,c_n)$ 的集合

$$\sum_{i=1}^{n}(c_i/(z-\alpha_i))\equiv 0 \pmod{g(z)}.$$

定义 2. 设 C' 和 C 为两个 (n,k) 线性码,称 C 和 C' 等价如果 C' 中所有码字都能通过对 C 中码字的坐标施以一固定置换而得到.

显然,C 和 C' 是等价的当且仅当存在置换 $\sigma\in S_n$ 使得 $c=(c_1,\cdots,c_n)\in C$ 当且仅当 $c'=(c'_1,\cdots,c'_n)=(c_{\sigma(1)},\cdots,c_{\sigma(n)})\in C'$.

容易证明下面的性质成立.

性质 1. 设 G 是 (n,k) 线性码 C 的生成矩阵,P 是 $n\times n$ 置换阵,则有由 $G'=GP$ 生成的线性码 C' 与 C 等价.

证明:设 $P=(p_{ij})_{1\leqslant i,j\leqslant n}$. 令 $\sigma\in S_n$,$\sigma(i)=j$ 当且仅当 $p_{ij}=1$. 容易验证 $c=(c_1,c_2,\cdots,c_n)\in C$ 当且仅当 $(c_{\sigma(1)},\cdots,c_{\sigma(n)})\in C'$.

性质 2. 设 C 为 $\Gamma(L,g)$Goppa 码,线性码 C' 与 C 等价,则 C' 也是 Goppa 码. L 和 g 的含义同定义 1.

证明:根据定义 2,存在一个 $\sigma\in S_n$,使得对任何 $c'=(c'_1,\cdots,c'_n)\in C'$,有 $c=(c_1,\cdots,c_n)=(c'_{\sigma(1)},\cdots,c'_{\sigma(n)})\in C$. 令 $\alpha'_i=\alpha_{\sigma^{-1}(i)}$,则有

$$\sum_{i=1}^{n}(c'_i/(z-\alpha'_i))=\sum_{i=1}^{n}(c'_{\sigma(i)}/(z-\alpha'_{\sigma(i)}))=\sum_{i=1}^{n}(c_i/(z-\alpha_i))\equiv 0 \pmod{g(z)}$$

注意到 $L'=\{\alpha'_1,\alpha'_2,\cdots,\alpha'_n\}=\{\alpha_{\sigma^{-1}(1)},\cdots,\alpha_{\sigma^{-1}(n)}\}=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}=L$,
再由定义 1,不难得出 C' 也是 Goppa 码. 证毕.

由性质 1 和性质 2,得

定理. 若 (n,k) 线性码 C 为 Goppa 码,G 是其生成矩阵,则由 $G'=GP$ 生成的线性码 C' 也是 Goppa 码. 其中 P 是 $n\times n$ 置换阵.

由于当 S 是 $k\times k$ 非奇异阵,SG 与 G 生成相同的线性码,所以有下面的推论成立.

推论. 若 (n,k) 线性码 C 为 Goppa 码,G 是其生成矩阵,则由 $G'=SGP$ 生成的线性码 C' 也是 Goppa 码. 其中 S 是 $k\times k$ 非奇异阵,P 是 $n\times n$ 置换阵.

2 关于 Adams 和 Meijer 对 McEliece 体制的分析

Adams 和 Meijer[5]计算了使得 $G_i=S_iG'P_i$ 成为 Goppa 码的 P_i 和 S_i 对偶的期望数 EXP,其中 P_i 是置换阵,S_i 非奇异. 结果是 $EXP\ll 1$. 即几乎只有原秘密钥 S^{-1} 和 P^{-1} 才能使得 $S^{-1}G'P^{-1}$ 成为某 Goppa 码的生成矩阵. 因此,Adams 和 Meijer 断言 McEliece 体制是相当安全的,因为其中的陷门多于一个的可能性极小,类似于 Brickell[14]的攻击不会成功.

他们使用的分析方法是，先定义二元 $k\times n$ 满秩矩阵集合上的等价关系 R 如：$A\ R\ B$ 当且仅当存在一个 $k\times k$ 可逆阵 S 和一个 $n\times n$ 置换阵 P 使得 $A=SBP$.
然后，使用纯组合的方法计算

$$EXP'=\#G/\#C,$$

其中 $\#G$ 是给定 n 和 k 之后可能的 Goppa 码生成矩阵的数目，$\#C$ 是 R 等价类的数目.

其分析结果与实际情况相反，原因有两个：一是在整个分析过程中，他们都把 G' 看成一个一般的满秩阵，忽略了本文上一节所述的 Goppa 码生成矩阵的代数性质；另外他们在假设 Goppa 码生成矩阵均匀分布于所有 $k\times n$ 满秩阵集合上之后，把 EXP' 等同于 EXP.

事实上，由本文上一节所述的 Goppa 码的性质可知，对于 McEliece 体制中的 G'，$EXP\gg1$，G' 的 R 等价类中所有矩阵都是 Goppa 码生成矩阵. 对任何 $k\times k$ 非奇异阵 S_i 和 $n\times n$ 置换阵 P_i，$G_i=S_iG'P_i$ 都是 Goppa 码生成矩阵. 显然是不符合均匀分布假设的.

3 结束语

Korzhik 和 Turkin[10]已经提出了一种基于迭代优化算法[11]的对 McEliece 体制的有效攻击方法，文献[12]也证明了与 Adams_Meijer 分析相矛盾的结果. 但是他们都没有指出 McEliece 体制中的公开钥矩阵实际上就是一个 Goppa 码生成矩阵. 而且，近两年依然有不少与 McEliece 体制类似的体制及肯定性的安全性分析见诸于文献. 本文所证明的 Goppa 码生成矩阵的代数性质从编码理论的角度来看虽然是平凡的，但与一类基于纠错码的公钥体制的安全性却密切相关，从密码分析的角度来看是有意义的.

致谢 本文的成文得益于同鲍丰和高翔同志的讨论，谨在此表示感谢.

参考文献

1 McEliece R J. A public key cryptosystem based on algebraic coding theory. JPL DSN Progress Rep., 1978(**42**—44):114—116.

2 Brickell E F, Odlyzko A M. Cryptanalysis: a survey of resent results. Proceeding of the IEEE, 1988,**76**(**5**):578—593.

3 Wang Yumin, Zhang Hailin, Zhang Kan. Performance analysis and parameter optimization on m—public—key cryptosystem. Acta Electronics Sinica, 1992,**20**(**4**):32—36.

4 Li Yuanxin, Wang Xinmei. The application of error—correcting codes to modern cryptology. Journal of China Institute of Communications, 1991,**12**(**4**):92—96.

5 Adams C M, Meijer H. Security—related comments regarding the McEliece public key cryptosystem. Advances in Cryptology—Proc. Crypto 87, Santa Barbara, CA, Aug. 17—20, 1987. 224—228.

6 Wang Xinmei. Digital signature scheme based on error—correcting codes. Electron. Lett., 1990,**26**(**13**):898—899.

7 王新梅. 纠错码数字签名、加密纠错公钥体制. 电子学报. 1991,**19**(**5**):48—54.

8 Li Yuanxin, Cheng Jian, Wang Xinmei. A joint signature encryption and error—correction public—key cryptosystem based on algebraic coding theory. Journal of Electronics, 1991,**13**(**4**):359—364.

9 隆永红. W 签名方案与 ECPS2 中的签名都是不可信赖的. 见:陶仁骥等编:密码学进展—CHINACRIPT'92,北京:科学出版社,1992.

10 Korzhik V I, Turkin A I. Cryptanalysis of McEliece's public—key cryptosystem. Advance in Cryptology: Proceedings of EUROCRYPT'91, Springer—Verlag, 1991.

11 Turkin A I, Korzhik V I. The practically—optimal decoding algorithm for arbitrary linear codes over a BSC with polynomial time complexity. Presented at the IEEE Intl. Symp. Info. Th., Budapest, 1991.

12 Gibson J K. Equivalent Goppa codes and trapdoors to McEliece's public key cryptosystem. Advance in Cryptology: Proceedings of EUROCRYPT'91, Springer—Verlag, 1991.

13 Van Lint J H. Introduction to coding theory. Springer—Verlag, New York, 1982.

14 Brickell E F. Breaking iterated knapsacks. Advance in Cryptology: Proceedings of EUROCRYPT'84, Springer—Verlag, 1985. 342—358.

ON THE SECURITY OF THE MCELIECE'S PUBLIC KEY CRYPTOSYSTEM

Long Yonghong

(*Institute of Software, The Chinese Academy of Science, Beijing* 100080)

(*Department of Computer Science, Xiangtan University, Xiangtan* 411105)

Abstract Contrary to the Adams_Meijer analysis, in this paper it is proved that the public matrix G' in the McEliece's cryptosystem and all other matrices in the R_equivalence class of G' are still generator matrices of Goppa codes. This result may be a theoretical support to the Korzhik_Turkin attack while explaining why the Adams—Meijer analysis to the McEliece's cryptosystem conflicts with the real situation.

Key words Public key cryptosystem, error correcting code, Goppa code, crypanalysis.