MQ 公钥密码体制等价密钥分析

王 鑫[1]，孙 晨[2]，王新梅[1]

(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 空军工程大学 导弹学院，陕西 三原 713800)

摘要：MQ 公钥密码体制存在多个私钥对应同一个公钥的问题. 应用高斯不变算子对私钥空间进行等价分类，给出了任一私钥的等价类中所含元素的个数与明密文分量之间的关系式. 该式表明，对任一公钥有指数级个私钥与之对应，从而使私钥(进而公钥)空间大量减少. 同时，还给出了私钥的仿射结构的标准形，该形式具有稀疏性，从而能够有效地减少计算量，提高存储效率. 最后，以 R-SE(2)签名体制为例，分析了分层结构对体制安全性的影响.

关键词：多变量公钥密码；代数分析；等价密钥；高斯不变算子；R-SE(2)

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1001-2400(2009)03-0428-05

Equivalent keys of multivariate quadratic public key cryptosystem

WANG Xin[1], *SUN Chen*[2], *WANG Xin-mei*[1]

(1. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China;
2. Missile Inst. of Airforce Eng. Univ., Sanyuan 713800, China)

Abstract: The multivariate quandratic cryptosystem has the problem that many superflous private keys correspond to the same public key. By applying the Gauss Sustainer, the private key space is partitioned into equivalence classes. And then, a relationship between the number of elements in any equivalence private key class and plaintext (ciphertext) is established. This formula shows the number of private keys corresponding to any given public key is exponential. Hence, the private (further the public) key space is reduced greatly. Moreover, the normal form of affine transformations of the private key is derived. It has the sparse characteristic, which will reduce computing complexity and improve the storage efficiency. Finally, the R-SE(2) public key signature scheme is taken for an example, and the security performance of this scheme affected by the step-structure is analyzed.

Key Words: multivariate public key cryptosystem; algebraic cryptanalysis; equivalent keys; Gauss sustainer; R-SE(2)

1997 年美国科学家 Peter Shor 提出了量子分解算法[1]，该算法是迄今量子计算领域最著名的算法，它利用量子计算的并行性，可以在多项式时间内解决大整数分解或离散对数问题. 日前，中国科技大学潘建伟教授等与英国牛津大学的研究人员合作，已利用光量子计算机实现了 Shor 量子分解算法. 因此两大公钥密码体制 RSA 和 ECC(椭圆曲线密码体制)的安全受到严重威胁.

基于 MQ(Multivariate Quadratic)问题的多变量二次公钥密码体制被认为是能抵御未来基于量子计算机攻击的几种公钥密码体制之一. 其安全性在于有限域上求解多变量二次多项式方程组是一个 NP-C 问题[2-3]. 该体制具有较高的效率和安全性，且易于硬件实现，是量子计算机时代的一种安全的密码体制和数字签名备选方案[4-6].

设 F 为有限域，MQ 密码体制的公钥 $P = T \circ P' \circ S$(符号 $\circ$ 表示映射的合成)，其中 $S \in \mathrm{Aff}^{-1}(F^n)$，

收稿日期：2008-05-20

基金项目：国家自然科学基金资助(90604009，60503010)

作者简介：王 鑫(1979-)，女，西安电子科技大学博士研究生，E-mail：wangxin@mail.xidian.edu.cn.

$T \in \mathrm{Aff}^{-1}(F^m)$(即有限域 F 上的仿射变换).核方程是由 n 个变量 m 个二次方程所构成的方程组:

$$p_i(x_1,\cdots,x_n) := \sum_{1\leqslant j\leqslant k\leqslant n} \gamma_{i,j,k}x_jx_k + \sum_{i=1}^{n} \beta_{i,j}x_j + \alpha_i \quad ,$$

其中 $1\leqslant i\leqslant m$,系数 $\gamma_{i,j,k},\beta_{i,j},\alpha_i \in F$.记上述 m 个方程为 $\mathrm{MQ}(F^n,F^m)$.多项式向量 $\boldsymbol{P}(x) := (p_1(x_1,\cdots,x_n),\cdots,p_m(x_1,\cdots,x_n)) \in \mathrm{MQ}(F^n,F^m)$ 为公钥,三元组 $(T,P',S) \in \mathrm{Aff}^{-1}(F^m)\times\mathrm{MQ}(F^n,F^m)\times\mathrm{Aff}^{-1}(F^n)$ 为私钥.本文中对私钥的核方程用符号′加以标识.

多变量公钥密码体制中存在多个私钥对应同一个公钥的问题,该思想由 Kipnis 和 Shamir 在对 Balance Oil Vinegar scheme 进行密钥恢复攻击时首先提出[7].其后 Wolf 等人对 HFE,MIA,UOV 及 STS4 类具体的 MQ 密码体制的密钥[8-9]进行了分析,但没有对一般形式的 MQ 体制的密钥进行研究.同时,由于在 MQ 体制中密钥以高阶矩阵的形式存储和运算,若采用全阶矩阵,则会导致高计算量.笔者对 GF(2)上无常数项的一般形式 MQ 密码体制的密钥进行了分析.通过应用高斯不变算子,将私钥的仿射部分化为具有稀疏特性的矩阵,选该形式作为等价类的代表元,可以有效地节省存储空间、缩短操作时间.同时,还证明了对同一个公钥总存在 $\prod_{i=0}^{n-1}(2^n-2^i)\prod_{i=0}^{m-1}(2^m-2^i)$ 个私钥与之对应,从而使私钥(进而公钥)空间大量减少.最后,以 R-SE(2)公钥密码体制[10]为例进行密钥分析,给出了分层结构的层数对密钥及体制安全性的影响.

1　等价私钥与高斯不变算子

定义 1　设 $\boldsymbol{M}_S \in F^{n\times n}$ 是 $n\times n$ 矩阵,$\boldsymbol{v}_s \in F^n$ 是一向量,定义 $\boldsymbol{S}(\boldsymbol{x}) := \boldsymbol{M}_S\boldsymbol{x} + \boldsymbol{v}_s$ 为仿射变换 $\boldsymbol{S}$ 的矩阵表示.

定义 2　由文献[8-9],两个私钥 (T_1,P_1',S_1) 和 $(T_2,P_2',S_2) \in \mathrm{Aff}^{-1}(F^m)\times\mathrm{MQ}(F^n,F^m)\times\mathrm{Aff}^{-1}(F^n)$ 等价,是指对应公钥相同,即 $T_1\circ P_1'\circ S_1 = P = T_2\circ P_2'\circ S_2$.易证该二元关系为一等价关系.因而可以对私钥空间划分等价类.

定义 3　设 $(T,P',S) \in \mathrm{Aff}^{-1}(F^m)\times\mathrm{MQ}(F^n,F^m)\times\mathrm{Aff}^{-1}(F^n)$,对任意的 $\sigma\in\mathrm{Aff}^{-1}(F^n)$,$\tau\in\mathrm{Aff}^{-1}(F^m)$,有 $P = T\circ\tau^{-1}\circ\tau\circ P'\circ\sigma\circ\sigma^{-1}\circ S$ 成立.若 $\tau\circ P'\circ\sigma$ 保持 P' 的形状不变,则称 (σ,τ) 为一个不变算子[8-9].

上述定义中的"形状"是概指,不同的陷门构造有不同的核方程形式.例如,后面的 R-SE(2)公钥密码体制,"形状"为分层下的一一映射结构.

定理 1　两个私钥 (T,P',S) 和 $(T_1,P_1',S_1) \in \mathrm{Aff}^{-1}(F^m)\times\mathrm{MQ}(F^n,F^m)\times\mathrm{Aff}^{-1}(F^n)$ 等价,当且仅当存在不变算子 (σ,τ).从而对给定私钥 $(T,P',S) \in \mathrm{Aff}^{-1}(F^m)\times\mathrm{MQ}(F^n,F^m)\times\mathrm{Aff}^{-1}(F^n)$,其所在等价类元素的个数等于不变算子 (σ,τ) 的个数.

证明　令 $S = \sigma\circ S_1$,$T = T_1\circ\tau$,则 $\sigma = S\circ S_1^{-1} \in \mathrm{Aff}^{-1}(F^n)$,$\tau = T_1^{-1}\circ T \in \mathrm{Aff}^{-1}(F^m)$.由仿射变换定义可知 (σ,τ) 存在.因 (T_1,P_1',S_1) 和 (T,P',S) 等价,故 $P_1' = \tau\circ P'\circ\sigma$.对给定的陷门构造,核方程 P_1' 与 P' 形式一致,因此 (σ,τ) 为一不变算子.反之,若对私钥 (T,P',S) 存在一个不变算子 (σ,τ),易见 $(T\circ\tau^{-1},\tau\circ P'\circ\sigma,\sigma^{-1}\circ S)$ 与之等价.因此私钥 (T,P',S) 和 (T_1,P_1',S_1) 等价,当且仅当存在不变算子 (σ,τ) 与之对应.从而等价类 $\overline{(T,P',S)} = \{(T\circ\tau^{-1},\ \tau\circ P'\circ\sigma,\ \sigma^{-1}\circ S)\colon (\sigma,\tau)$ 为不变算子$\}$,即等价类中元素的个数 $|\overline{(T,P',S)}|$ 等于不变算子 (σ,τ) 的个数.

定义 4　高斯不变算子.选用对矩阵的高斯变换,即行(列)对换,域 F 中元素对行(列)的乘法,以及行(列)相加,所对应的矩阵分别为对换阵,数乘阵和倍加阵.由定义及定理 2 的证明可知高斯变换构成一不变算子,故称之为高斯不变算子.同时,它们构成仿射变换的子群,从而可以对仿射空间进行等价分类.

2　MQ 体制的密钥问题

对于 GF(2)上的多项式,由于常数项(取值仅为 0,1)的存在对体制的安全性没有显著增益,同时对等价类个数的影响微乎其微,因而,文中所讨论的 MQ 方程均为不含常数项.又因对所有的 x,有 $x^2 = x$,因此 n

个自变量,m 个方程的形式如下:

$$\begin{cases} y'_1 = p'_1(x'_1,\cdots,x'_n) = \sum\limits_{1\leqslant j\leqslant k\leqslant n} \gamma_{1,j,k}x'_jx'_k = (x'_1,\cdots,x'_n)\,\boldsymbol{\Gamma}_1\,(x'_1,\cdots,x'_n)^{\mathrm{T}} \quad , \\ y'_2 = p'_2(x'_1,\cdots,x'_n) = \sum\limits_{1\leqslant j\leqslant k\leqslant n} \gamma_{2,j,k}x'_jx'_k = (x'_1,\cdots,x'_n)\,\boldsymbol{\Gamma}_2\,(x'_1,\cdots,x'_n)^{\mathrm{T}} \quad , \\ \vdots \\ y'_m = p'_m(x'_1,\cdots,x'_n) = \sum\limits_{1\leqslant j\leqslant k\leqslant n} \gamma_{m,j,k}x'_jx'_k = (x'_1,\cdots,x'_n)\,\boldsymbol{\Gamma}_m\,(x'_1,\cdots,x'_n)^{\mathrm{T}} \quad , \end{cases}$$

其中,$\boldsymbol{\Gamma}_i$ $(i=1,\cdots,m)$ 为方程组的系数矩阵,T 表示转置.

引理 1 设 F 是 q 个元素的有限域,则 F 上$(n\times n)$ 的可逆矩阵有 $\prod\limits_{i=0}^{n-1}(q^n-q^i)$ 个.

证明 首行的 n 维向量共有 q^n-1 种选择(除去零向量);接下来的每个行向量均是从所有 n 维向量中去掉与该行之前所有行线性相关的向量,因此第 i 行可选的向量数即为 q^n-q^{i-1}.

定理 2 设 F 是 q 个元素的有限域. 已知 GF(2)上无常数项的 MQ 系统的一个私钥 $(T,P',S)\in \mathrm{Aff}^{-1}(F^m)\times \mathrm{MQ}(F^n,F^m)\times \mathrm{Aff}^{-1}(F^n)$,则有 $\prod\limits_{i=0}^{n-1}(2^n-2^i)\prod\limits_{i=0}^{m-1}(2^m-2^i)$ 个等价私钥. 从而,对每一个公钥都有上述数目的私钥与之对应.

证明 对仿射变换 S 和 T 分别应用高斯算子 σ 和 τ,由于 $\boldsymbol{M}_S$ 和 $\boldsymbol{M}_T$ 均为可逆矩阵,故通过高斯变换均可将其化为单位阵 $\boldsymbol{E}$,称为仿射变换 S 和 T 的标准形式.

下面分析 σ 和 τ 对核方程的影响. 设

$$\sigma(\boldsymbol{x}) = \boldsymbol{x}\boldsymbol{C} = \boldsymbol{x}' \quad , \quad \tau(\boldsymbol{y}') = \boldsymbol{y}'\boldsymbol{D} = \boldsymbol{y} \quad ,$$

其中 $\boldsymbol{D}=(d_{i,j})_{m\times m}$,代入公钥方程

$$\boldsymbol{y} = (y_1,\cdots,y_n) = \tau\circ P'\circ\sigma(\boldsymbol{x}) = (\boldsymbol{x}'\boldsymbol{\Gamma}_1(\boldsymbol{x}')^{\mathrm{T}},\cdots,\boldsymbol{x}'\boldsymbol{\Gamma}_m(\boldsymbol{x}')^{\mathrm{T}})\,\boldsymbol{D} \quad ,$$

得变换后输出

$$y_i = \boldsymbol{x}\left(\sum_{j=1}^{m} d_{ji}\boldsymbol{C}\boldsymbol{\Gamma}_j\boldsymbol{C}^{\mathrm{T}}\right)\boldsymbol{x}^{\mathrm{T}} \quad ,$$

其中 $1\leqslant i\leqslant m$.

要保持 y_i 的系数矩阵 $\boldsymbol{\Gamma}_i$ 形状不变,$\boldsymbol{C}$ 和 $\boldsymbol{D}$ 可取任一可逆矩阵. 由引理 1,可逆矩阵 $\boldsymbol{C}$ 和 $\boldsymbol{D}$ 的个数分别为 $\prod\limits_{i=0}^{n-1}(2^n-2^i)$ 和 $\prod\limits_{i=0}^{n-1}(2^m-2^i)$,也即 σ 和 τ 的个数. 故由定理 1,与已知私钥等价的私钥有 $\prod\limits_{i=0}^{n-1}(2^n-2^i)\prod\limits_{i=0}^{m-1}(2^m-2^i)$ 个,从而每一个公钥都有此数目的私钥与之对应.

结论分析:

(1) 通过应用高斯不变算子 σ 和 τ,将仿射变换 S 和 T 对应的矩阵 $\boldsymbol{M}_S$ 和 $\boldsymbol{M}_T$ 均化为了标准形. 该形式简化了矩阵结构,具有"稀疏"性,因此在存储空间和运算时间受限的场合,如智能卡上,选标准形作为等价类的代表元,可以有效地节省存储空间、缩短操作时间.

(2) 当 $m=n=100$ bit 时,一个私钥约有 $2^{19\,996}$ 个等价的私钥. 通过计算,私钥由原来的525.2 kbit减为505.2 kbit. 大量等价私钥的存在使得实际安全参数空间的规模大为减少,为保持私钥空间势必加大密钥空间,这将导致密钥规模增大,从而降低存储和运算效率. 因此,从设计角度而言应避免大量密钥等价,使一个等价类中只有少数(甚至一个)私钥.

(3) 需指出等价类的划分,不变算子并不惟一.

3 R-SE(2)PKC 的密钥问题

R-SE(2)公钥密码体制(于 2004 年提出,见文[10])为上述所研究的一般 MQ 体制的一种具体构造. 首先 m 个方程被分为 L 层,设 r_l 表示每层中新变量的个数,m_l 表示每层中方程的个数,满足 $r_l=m_l$,即若取公

共参数 r,则有 $m=n=Lr$. 在第 l $(1\leqslant l\leqslant L)$ 层中,方程所含有的变量为 $x'_k, k\leqslant \sum_{j=1}^{l} r_j$,即之前所有层中的变量加上本层的新变量. 核方程(即第 l 层中的第 t $(1\leqslant t\leqslant r)$ 个方程)形式如下:

$$p'_{(l-1)r+t}(\boldsymbol{x}')=\psi_{l,t}(x'_1,\cdots,x'_{(l-1)r})+\phi_{l,t}(x'_{(l-1)r+1},\cdots,x'_{lr}) \quad ,$$

其中 $\psi_{l,t},\phi_{l,t}$ 分别为 $GF(2)$ 上不含常数项的 $(l-1)r$ 和 r 个变量的二次多项式. 并且对任意的 $l\in\{1,\cdots,L\}$,函数 $(\phi_{l,1},\cdots,\phi_{l,r})$: $F_2^r\to F_2^r$ 均为一一映射.

定理 3　设 F 是 q 元有限域,那么对 R-SE(2)PKC 的一个私钥 $(T,P',S)\in \mathrm{Aff}^{-1}(F^m)\times \mathrm{MQ}(F^n,F^m)\times \mathrm{Aff}^{-1}(F^n)$,有 $(Lr!)^2\left(1+\sum_{j=1}^{r-1}\sum_{i=1}^{r-j} C_r^j C_{r-j}^i\right)2^{r\sum_{i=1}^{L}(n-ir)}$ 等价私钥. 从而,每一个公钥都有上述数目的私钥与之对应.

证明　应用高斯算子 σ 和 τ,得输出方程

$$y_i=\boldsymbol{x}\left(\sum_{j=1}^{n} d_{ji}\boldsymbol{C}\boldsymbol{\Gamma}_j\boldsymbol{C}^{\mathrm{T}}\right)\boldsymbol{x}^{\mathrm{T}} \quad ,\quad 1\leqslant i\leqslant n \quad ,$$

由核方程 $p'_{(l-1)r+t}$ 形式,可知第 l 层方程所对应的矩阵具有相同结构

$$\begin{pmatrix} (*)_{(l-1)r*(l-1)r} & 0 & 0 \\ 0 & (*)_{r*r} & 0 \\ 0 & 0 & 0_{(n-lr)*(n-lr)} \end{pmatrix} \quad ,$$

其中主对角线上 $(r\times r)$ 分块矩阵对应于方程的双射部分.

要保证 P' 结构形式不变,即维持双射 $(\phi_{l,1},\cdots,\phi_{l,r})$: $F_2^r\to F_2^r$ 结构不变. 取

$$C:=\begin{pmatrix} I_1 & 0 & \cdots & 0 \\ 0 & I_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & I_L \end{pmatrix} \quad ,$$

其中 I_l 为单位阵或其对换阵,实现每层 $\boldsymbol{x}$ 全排列,$\boldsymbol{C}$ 的个数为 $Lr!$. 取

$$\boldsymbol{D}:=\begin{pmatrix} \boldsymbol{E}_1 & * & * & \cdots & * & * \\ 0 & \boldsymbol{E}_2 & * & \cdots & * & * \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \boldsymbol{E}_{L-1} & * \\ 0 & 0 & 0 & \cdots & 0 & \boldsymbol{E}_L \end{pmatrix} \quad ,$$

$\boldsymbol{E}_l$ 为单位阵,对换阵或倍加阵,实现双射结构内部变换. 可以证明,上述取法均保持变换后的核方程双射结构不变. 其中倍加矩阵个数为

$$Lr!\cdot\left(1+\sum_{j=1}^{r-1}\sum_{i=1}^{r-j} C_r^j C_{r-j}^i\right) \quad .$$

因此等价的私钥个数为　　$(Lr!)^2\cdot\left(1+\sum_{j=1}^{r-1}\sum_{i=1}^{r-j} C_r^j C_{r-j}^i\right)\cdot 2^{r\sum_{i=1}^{L}(n-ir)}$.

从而,每一个公钥都有上述数目的私钥与之对应.

取 $n=100$ bit, (L,r) 分别取(25,4),(20,5)(原作者建议参数)和(10,10),则在高斯不变算子的作用下层数对密钥的影响如表 1.

表 1　分层结构对密钥数影响

层数 L	25	20	10
等价的私钥数	$2^{19\,212}$	$2^{23\,764}$	$2^{45\,025}$

如上所述,层数越少,等价私钥越多,密钥减少量越多,从而密钥空间越小. 因此,对相同大小的私钥,分层越多,安全性越高.

4 结 束 语

MQ 公钥体制中存在多个私钥对应同一个公钥的问题,笔者首先分析了 GF(2)上一般形式 MQ 密码体制的私钥等价问题.通过应用高斯不变算子,首先给出了私钥仿射结构具有稀疏性的标准形式,从而能够有效减少运算量,提高存储空间的利用率,适用于存储效率和实时性要求较高的场合.同时,还得出对任一私钥存在大量私钥与之等价的结论,导致实际安全参数空间的规模由于等价类的存在而大量减少.最后,对 R-SE(2)公钥密码体制进行了类似的密钥分析.该分析方法不仅揭示了私钥间的内在联系,而且有助于产生新的攻击方法.

参考文献:

[1] Shor P. Polynomial-time Algorithms for Pime Factorization and Discrete Logarithms on A Quantum Computer [J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[2] Garay M, Johnson D. Computers and Intractability —a Guide to the Theory of NP-Completeness [M]. San Francisco: W H Freeman and Company, 1979: 250-251.

[3] Patarin J, Goubin L. Trapdoor One-way Permutations and Multivariate Polynomials [C]//International Conference on Information Security and Cryptology 1997, LNCS: 1334. Berlin: Springer, 1999: 356-368.

[4] European IST. NESSIE Project [EB/OL]. [2000-12-12]. http://www.cryptonessie.org.

[5] Akkar M, Courtois N T, Duteuil R, et al. A Fast and Secure Implementation of Sflash [C]//PKC 2003, LNCS: 2567. Berlin: Springer, 2003: 267-278.

[6] 韦宝典, 刘景伟, 王新梅. NESSIE 分组密码及其安全性分析[J]. 西安电子科技大学学报, 2004, 31(3): 377-382.
Wei Baodian, Liu Jingwei, Wang Xinmei. The NESSIE Block Ciphers and Their Security [J]. Journal of Xidian University, 2004, 31(3): 377-382.

[7] Kipnis A, Shamir A. Cryptanalysis of the Oil and Vinegar Signature Scheme [C]//Advances in Cryptology—CRYPTO 1998, LNCS: 1462. Berlin: Springer, 1998: 257-267.

[8] Wolf C, Preneel B. Equivalent Keys in HFE, C*, and Variations [C]//Proceedings of Mycrypt 2005, LNCS: 3725. Berlin: Springer, 2005: 33-49.

[9] Wolf C, Preneel B. Superfluous Keys in Multivariate Quadratic Asymmetric Systems [C]//PKC 2005, LNCS 3386. Berlin: Springer, 2005: 275-287.

[10] Kasahara M, Sakai R. A Construction of Public Key Cryptosystem for Realizing Ciphertext of Size 100 Bit and Digital Signature Scheme [J]. IEICE Trans on Fundamentals, 2004: E87-A(1): 102-109.

(编辑: 高西全)

(上接第 405 页)

[5] Karhunen J, Joutsensalo J. Representation and Separation of Signal Using Nonlinear PCA Type Learning[J]. Neural Networks, 1994, 7(1): 113-121.

[6] Zhu Xiaolong, Zhang Xianda, Ding Zizhe, et al. Adaptive Nonlinear PCA Algorithms for Blind Source Separation without Prewhitening[J]. IEEE Trans on Circuits and Systems, 2006, 53(3): 745-753.

[7] 何昭水, 谢胜利, 傅予力. 稀疏表示与病态混叠盲分离[J]. 中国科学 E 辑·信息科学, 2006, 36(8): 864-879.
He Zhaoshui, Xie Shengli, Fu Yuli. Sparse Representations and Blind Source Separation of Morbidity Mixtures[J]. Science in China Ser E Information Sciences, 2006, 36(8): 864-879.

[8] 冶继民, 张贤达, 金海红. 超定盲信号分离的半参数统计方法[J]. 电波科学学报, 2006, 21(3): 331-336.
Ye Jimin, Zhang Xianda, Jin Haihong. Semi-parametric Statistical Approach for Overdetermined Blind Source Separation [J]. Chinese Joural of Radio Science, 2006, 21(3): 331-336.

[9] 张贤达. 矩阵分析与应用[M]. 北京: 清华大学出版社, 2004.

(编辑: 郭 华)