doi:10.11959/j.issn.1000-436x.2015182

新扩展多变量公钥密码方案的安全性分析

聂旭云[1,2]，刘波[1]，鲁刚[3]，钟婷[1]

（1. 电子科技大学 信息与软件工程学院，四川 成都 611731；
2. 中国科学院信息工程研究所 信息安全国家重点实验室，北京 100093；
3. 电子科技大学 计算机科学与工程学院，四川 成都 611731）

摘 要：新扩展多变量公钥密码方案是乔等提出的一种多变量公钥密码体制的安全性增强方案。该方案引入了一个非线性“温顺变换”，试图隐藏原始方案的弱点，如线性化方程。然而，分析表明，若原始方案满足线性化方程，则改进方案必然满足二次化方程。给定公钥，在找到所有的二次化方程之后，将要破解的合法密文代入到二次化方程中，可以得到关于明文变量的二次方程。这降低了要求解的方程组的次数。结合 Groebner 基方法，可以快速地恢复合法密文相应的明文。

关键词：多变量公钥密码系统；二次化方程；线性化方程；温顺变换；代数攻击

中图分类号：TN918.1 **文献标识码**：A

Cryptanalysis of novel extended multivariate public key cryptosystem

NIE Xu-yun[1,2], LIU Bo[1], LU Gang[3], ZHONG Ting[1]

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China;
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
3. School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract: The novel extended multivariate public key cryptosystem is a new security enhancement method on multivariate public key cryptosystems, which is proposed by Qiao, *et al*. A nonlinear invertible transformation was used, named “tame transformation”, on the original multivariate public key cryptosystem to hide its weakness such as linearization equation. However, it is found that if there are many linearization equations satisfied by the original MPKC, there would be many quadratization equations (QE) satisfied by the improved scheme. Given a public key, after finding all QE, a valid cipheretext can be substituted into the QE to derive a set of quadratic equations on the plaintext variable. This exactly reduce the degree of the system wanted to solve. Then the corresponding plaintext can be recovered for a given valid ciphertext combining with Groebner basis method.

Key words: multivariate public key cryptosystems; quadratic equations; linear equations; tame transformation; algebraic attack

1 引言

多变量公钥密码系统（MPKC，multivariate public key cryptosystem）被认为是有希望抵挡未来量子计算机攻击的公钥密码系统之一。其安全性基于求解有限域上随机生成的多变量多项式方程组问题（MQ, multivariate quadratic）的困难性[1]。

线性化方程分析方法是一种常用的 MPKC 安全性分析方法。该分析方法成功的关键在于多变量密码体制是否满足如下形式的关系式。

$$\sum_{i=1}^{n} a_i x_i g_i(y_1,\cdots,y_m) + h(y_1,\cdots,y_m) + c = 0$$

收稿日期：2014-10-09；**修回日期**：2014-11-15

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目(2013CB834203)；国家自然科学基金资助项目（61370026,61472064）

Foundation Items: The National Natural Basic Research Program of China (973 Program)(2013CB834203)；The National Natural Science Foundation of China (61370026,61472064)

其中，n 是明文变量的个数，m 是密文变量的个数，$x_i(1\leqslant i\leqslant n)$ 和 $y_j(1\leqslant j\leqslant m)$ 分别为明文变量和密文变量，$g_i(1\leqslant i\leqslant n)$ 和 h 是密文变量的多项式函数。

线性化方程分析方法是 Patarin[2]在 1995 年提出来破解 MI 体制[3]的。Ding 等对该方法进行了推广，提出了高阶线性化方程分析方法[4]，并破解了 MFE 体制[5]。为了抵挡对 MFE 体制的二阶线性化方程攻击，Wang 等改进了 MFE 的中心映射，将 MFE 的公钥从二次多项式提升到了四次多项式[6]。但遗憾的是，Cao 等发现改进后的 MFE 满足二次化方程[7]，并利用该方法成功地破解了改进的 MFE 公钥加密体制。二次化方程方法与线性化方程方法不同之处在于要破解的多变量密码体制满足如下形式的关系式。

$$\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=1}^{m}a_{ijk}x_ix_jy_k+\sum_{i=1}^{n}\sum_{j=i}^{n}b_{ij}x_ix_j+\sum_{i=1}^{n}\sum_{j=1}^{m}c_{ij}x_iy_j+\sum_{i=1}^{n}d_ix_i+\sum_{i=1}^{m}e_iy_i+f=0$$

可以注意到，该方程中明文变量的次数是二次的，而线性化方程中，明文变量的次数是一次的。若把一个合法密文代入二次化方程，将得到明文变量的二次多项式方程。因此这类方程被称为“二次化方程”。这有助于结合 Groebner 基方法来恢复合法密文相应的明文。

2013 年，乔帅庭等应用“温顺变化”的思想提出了一种 MPKC 的安全性增强方案[8]。该方案的核心思想是在密钥生成阶段，先对明文变量做二次温顺变化，然后再用原始的 MPKC 进行加密，即用原始的 MPKC 密码函数复合一个二次温顺变化。这样做的优点是能够隐藏原始的 MPKC 体制的一些弱点，比如说消除原始体制的线性化方程。这样做的缺点是，经过函数的复合，公钥多项式由二次提升到了 4 次。在变量个数和方程个数相同的情形下，这增大了体制的公钥量。

本文主要工作是对乔等提出的基于温顺变换的多变量公钥安全增强方案进行安全分析。若原始的 MPKC 方案满足线性化方程，则该增强方案可以消除线性化方程，但是该增强方案必然满足二次化方程。这是由于该增强方案的关键思想是仅仅对明文变量用温顺变换从一次提高到了二次，然后再用原始的多变量公钥密码体制进行加密运算。

利用该增强方案的公钥，可以找到所有的二次化方程。在找到所有的二次化方程后，代入要破解的合法密文，可以得到一组明文变量的二次多项式方程组。结合给定合法密文与公钥构成的多变量多项式方程组，采用 Groebner 基方法可恢复相应的明文。注意，找到所有的二次化方程与要破解的合法密文无关，因此可以预计算。本文给出了详细的理论分析，并采用计算机实验证实了分析结果。实验结果表明，采用了二次化方程方法后，求解密文的时间远远小于直接利用 Groebner 基方法求解密文的时间。

2　预备知识

2.1　多变量公钥密码系统

多变量公钥密码系统具有如下一般形式。

令 k 是一个有限域，n 和 m 为 2 个正整数。要构造一个 MPKC 体制，首先选取一个非线性可逆映射 $F:k^n\to k^m$，即 MPKC 的中心映射。为了在公钥中隐藏 F 的结构，将 F 复合上 k^n、k^m 上的 2 个可逆仿射变换 L_1 和 L_2。因此，MPKC 公钥具有如下形式。

$$\begin{aligned}y=(y_1,\cdots,y_m)&=\bar{F}(x)=\bar{F}(x_1,\cdots,x_n)\\&=L_2\circ F\circ L_1(x_1,\cdots,x_n)\end{aligned}$$

公钥 $\bar{F}$ 总是可以表示有限域 k 上的 m 个 n 元多项式

$$\begin{cases}y_1=f_1(x_1,\cdots,x_n)\\\quad\vdots\\y_m=f_m(x_1,\cdots,x_n)\end{cases}$$

MPKC 的私钥为 L_1、L_2 和中心映射 F。本文中关注多变量公钥加密体制，其加密、解密过程如下所示。

加密：给定公钥 $\bar{F}$，明文 $x'=(x_1',\cdots,x_n')$，计算密文

$$(y_1',\cdots,y_m')=\bar{F}(x_1',\cdots,x_n')$$

解密：给定合法密文 $y'=(y_1',\cdots,y_m')$，私钥 L_1、L_2 和中心映射 F，依次计算 L_2^{-1},F^{-1},L_1^{-1}，得到相应的明文

$$\begin{aligned}x'=(x_1',\cdots,x_n')&=\bar{F}^{-1}(y_1',\cdots,y_m')\\&=L_1^{-1}\circ F^{-1}\circ L_2^{-1}(y_1',\cdots,y_m')\end{aligned}$$

本文关注对多变量公钥加密体制的恢复密文攻击，即给定公钥 $y=\bar{F}(x)$ 及合法密文 $y'=(y_1',\cdots,y_m')$，求解方程组

$$\begin{cases} y'_1 = f_1(x_1,\cdots,x_n) \\ \quad\vdots \\ y'_m = f_m(x_1,\cdots,x_n) \end{cases} \tag{1}$$

2.2 线性化方程

对于 MPKC，线性化方程指的是如下形式的方程

$$\sum_{i=1}^{n} a_i x_i g_i(y_1,\cdots,y_m) + h(y_1,\cdots,y_m) + c = 0$$

其中，$g_i(1\leqslant i\leqslant n)$ 和 h 是密文变量的多项式函数。$g_i(1\leqslant i\leqslant n)$ 和 h 中的最高次数称为线性化方程的阶。

例如，一阶线性化方程形式如下

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_i y_j + \sum_{i}^{n} b_i x_i + \sum_{i}^{m} c_i y_i + d = 0$$

二阶线性化方程的形式如下

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=j}^{m} a_{ijk}x_i y_j y_k + \sum_{i=1}^{n}\sum_{j=1}^{m} b_i x_i y_j + \sum_{i=1}^{m}\sum_{j=i}^{m} c_{ij} y_i y_j + \sum_{i=1}^{n} d_i x_i + \sum_{i=1}^{m} e_i y_i + f = 0$$

给定合法密文 $y' = (y'_1,\cdots,y'_m)$，将其代入上述线性化方程，这些线性化方程将变为明文变量的一次多项式方程。如果可以找到足够多的线性化方程，代入要破解的合法密文，攻击者就可以得到明文变量的线性方程组。求解这个线性方程组，可以得到明文变量之间的线性关系式，从而可以对方程组（1）进行消元，降低求解方程组（1）的难度，快速地恢复出给定密文相应的明文。关于线性化方程的详细描述可参见文献[9]。

2.3 二次化方程

对于 MPKC，二次化方程是指如下形式的方程

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i x_j g_{ij}(y_1,\cdots,y_m) + \sum_{i=1}^{n} b_i x_i h_i(y_1,\cdots,y_m) + r(y_1,\cdots,y_m) + c = 0$$

其中，$g_{ij}(1\leqslant i\leqslant n, 1\leqslant j\leqslant n)$，$h_i(1\leqslant i\leqslant n)$ 和 r 是密文变量的多项式函数。g_{ij}、h_i 和 r 中的最高次数称为二次化方程的阶。

例如，一阶二次化方程具有如下形式

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=j}^{m} a_{ijk}x_i x_j y_k + \sum_{i=1}^{n}\sum_{j=1}^{m} b_i x_i y_j + \sum_{i=1}^{n}\sum_{j=i}^{n} c_{ij}x_i x_j + \sum_{i=1}^{n} d_i x_i + \sum_{i=1}^{m} e_i y_i + f = 0$$

给定合法密文 $y' = (y'_1,\cdots,y'_m)$，将其代入上述二次化方程，这些二次化方程将变为明文变量的二次多项式方程。如果可以找到足够多的二次化方程，代入要破解的合法密文，攻击者就可以得到明文变量的二次多项式方程组。将所有得到的二次多项式方程与方程组（1）组成新的方程组，再用 Groebner 基方法进行求解，将大大缩减求解明文的时间。

2.4 Matsumoto-Imai 公钥加密体制

MI 密码体制（又叫 C^*）作为第一种真正意义上的多变量公钥密码体制，是由 Matsumoto 和 Imai 在 1988 年提出的。

MI 体制的中心映射选取的是 q 元有限域 k 的 n 次扩域 K 上的一个单变量映射 $\tilde{F}$，形式如下

$$\tilde{F}(X) = X^{q^\theta+1}$$

其中，$1\leqslant\theta<n$，满足

$$\gcd(q^\theta+1, q^n-1) = 1$$

令 $(\alpha_1,\cdots,\alpha_n)$ 是大域 K 在小域 k 上的一组基，$\phi: K\to k^n$ 是域 K 到 k^n 的线性同构

$$\phi(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) = (a_1, a_2, \cdots, a_n)$$

利用该同构映射，可将映射 $\tilde{F}$ 变为小域 k 上的二次多项式映射

$$F: k^n \to k^n, (y_1,\cdots,y_n) = F(x_1,\cdots,x_n) = \phi\circ\tilde{F}\circ\phi^{-1}(x_1,\cdots,x_n)$$

关于 MI 体制的详细介绍，参见文献[3]。

Patarin 发现 MI 体制满足一阶线性化方程，并利用一阶线性化方程方法将 MI 体制破解[2]。Diene 等[10]详细地分析了 MI 体制中满足的线性化方程张成的线性空间的维数。

3 新扩展多变量公钥密码方案

乔等引入了温顺变换的思想来增强多变量公钥密码体制的安全性。具体的思想是在密钥生成的过程中，先将其构造的可逆二次温顺变换 $L_3: k^n\to k^n$ 作用于明文变量，然后再用原始的公钥加密体制作用于温顺变换的结果，也就是说，其公钥是由 L_1、中心映射 F、L_2 和 L_3 这 4 个映射复合而成，即

$$y = (y_1,\cdots,y_m) = \bar{F}(x) = \bar{F}(x_1,\cdots,x_n) = L_2\circ F\circ L_1\circ L_3(x_1,\cdots,x_n)$$

3.1 L_3 的构造

取正整数 n，d，且满足 $n>2d$，$L_3: k^n\to k^n$ 的

形式如下

$$\begin{cases} t_1 = x_1 + c_1 x_{d+1} x_n \\ t_2 = x_2 + c_2 x_{d+2} x_{n-1} \\ \quad \vdots \\ t_d = x_d + c_d x_{2d} x_{n-d+1} \\ t_{d+1} = x_{d+1} \\ \quad \vdots \\ t_n = x_n \end{cases}$$

从 L_3 的形式容易看出，该映射是可逆的。$L_3^{-1}(t_1,\cdots,t_n)=(x_1,\cdots,x_n)$ 形式如下

$$\begin{cases} x_1 = t_1 - c_1 t_{d+1} t_n \\ x_2 = t_2 - c_2 t_{d+2} t_{n-1} \\ \quad \vdots \\ x_d = t_d - c_d t_{2d} t_{n-d+1} \\ x_{d+1} = t_{d+1} \\ \quad \vdots \\ x_n = t_n \end{cases}$$

通过原始的 MPKC 体制和 L_3 的复合，其公钥多项式变成了多变量四次多项式。具体的方案介绍详见文献[8]。

3.2　新扩展方案的实例

文献[8]中选择使用 MI 体制作为原始的 MPKC，给出了扩展方案的性能分析和参数选择，并指出当 k=2^8，n=32，$d \geqslant 6$ 时，该扩展方案可以抵挡现有攻击。

该扩展方案未对 θ 选取做出要求，在实验中发现，当 k=2^8，n 为 2 的方幂时，满足条件的 θ 并不存在。因此，在实验当中，最大选取 n=33。

4　安全性分析

文献[8]指出，尽管 MI 体制满足线性化方程，但是在复合上 L_3 之后，新的扩展方案不再满足线性化方程，并且适当选择参数下，该扩展方案可以抵挡 Groebner 基方法的攻击。但经过分析可发现，该扩展方案满足二次化方程，这对求解给定合法密文相应的明文提供了帮助。

4.1　二次化方程

因为 MI 体制满足一阶线性化方程，由新扩展方案的构造可知，中间变量 $t_1,\cdots,t_n$ 与密文变量满足如下形式的一阶线性化方程

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \tilde{a}_{ij} t_i y_j + \sum_{i=1}^{n} \tilde{b}_i t_j + \sum_{i=1}^{n} \tilde{c}_i y_i + \tilde{d} = 0 \qquad (2)$$

而

$$\begin{cases} t_1 = x_1 + c_1 x_{d+1} x_n \\ t_2 = x_2 + c_2 x_{d+2} x_{n-1} \\ \quad \vdots \\ t_d = x_d + c_d x_{2d} x_{n-d+1} \\ t_{d+1} = x_{d+1} \\ \quad \vdots \\ t_n = x_n \end{cases} \qquad (3)$$

将式(3)代入式(2)可知新扩展方案满足如下形式的方程

$$\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=1}^{n} a_{ijk} x_i x_j y_k + \sum_{i=1}^{n}\sum_{j=i}^{n} b_{ij} x_i x_j + \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij} x_i y_j + \sum_{i=1}^{n} d_i x_i + \sum_{i=1}^{n} e_i y_i + f = 0 \qquad (4)$$

这正是二次化方程。给定公钥，对于所有的明文/密文对都满足该二次化方程。

为了实现攻击，需要找到所有的二次化方程。找到一个二次化方程意味着找到它的所有系数。显然，所有的二次化方程的系数向量构成了有限域 k 上的一个线性空间，记为这个线性空间为 V，其维数为 D。因此，找到所有的二次化方程等价于找到 V 的一组基。利用公钥随机生成一个明文/密文对代入式(4)可以得到一个以方程系数 a_{ijk}，b_{ij}，c_{ij}，d_i，e_i 和 f 为变量的线性方程。式(4)中的系数个数等于不同的单项式的个数，其个数为

$$\Gamma = n^2(n+1)/2 + n(n+1)/2 + n^2 + 2n + 1 = (n+1)^2(n+2)/2$$

为了找到 V 的一组基，可利用公钥生成比 Γ 略多的明文/密文对，并将这些明密对代入式(4)，这样就得到了关于二次化方程系数的线性方程组。求解该方程组，即可得到 V 的一组基，也就得到了 D 个线性无关的二次化方程。用 $E_\rho (1 \leqslant \rho \leqslant D)$ 表示这些方程

$$\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=1}^{n} a_{ijk}^{(\rho)} x_i x_j y_k + \sum_{i=1}^{n}\sum_{j=i}^{n} b_{ij}^{(\rho)} x_i x_j + \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}^{(\rho)} x_i y_j + \sum_{i=1}^{n} d_i^{(\rho)} x_i + \sum_{i=1}^{n} e_i^{(\rho)} y_i + f^{(\rho)} = 0 \qquad (5)$$

注意到，上述工作只依赖于给定的公钥，而独立于要破解的密文。因此，对于给定公钥，寻找所有的二次化方程可以预计算，而且仅需要计算一次。

4.2 唯密文攻击

给定合法密文 $y'=(y'_1,\cdots,y'_m)$，将其代入方程组(5)，再对其系数矩阵做高斯消元，可得到一组（不妨设为 D' 个）线性无关的以明文变量为未知量的二次多项式方程组

$$\begin{cases}\sum\limits_{j=i}^{n}\sum\limits_{k=1}^{n}\tilde{a}_{ij}^{(\rho)}x_ix_j+\sum\limits_{i=1}^{n}\tilde{b}_i^{(\rho)}x_i+\tilde{c}=0\\ 1\leqslant\rho\leqslant D'\end{cases}\tag{6}$$

将方程组(6)与方程组(1)合并，可得到 $D'+n$ 个以明文变量为未知量的二次多项式方程组。此时，可用 Groenber 基方法求解该方程组得到合法密文相应的明文。实验结果表明，这部分计算过程所耗费的时间比直接使用 Groenber 基方法求解方程组(1)所耗费的时间要小得多。

4.3 实验结果及复杂度估计

本文所有计算机实验均采用 Magma 软件在普通 PC 机上实现。PC 机的配置为: Intel Core i5-3470 CPU，3.2 GHz，4 GB 内存。

4.3.1 实验步骤

步骤 1 给定公钥，找出所有二次化方程的系数向量 $(a_{ijk},b_{ij},c_{ij},d_i,e_i,f)$ 所张成的线性空间的一组基。

正如 4.1 节所述，为了找到所有的二次化方程组，这里需要计算足够多的明文/密文对代入方程(4)，来得到关于系数的线性方程组。该方程组的变量个数为 $(n+1)^2(n+2)/2$ 个。一般来说，选择略多于 $(n+1)^2(n+2)/2$ 个明密对，就可以完全找到该线性方程组的解空间。若使用一般的高斯消元，解该方程的计算复杂度为 $((n+1)^2(n+2)/2)^3$ 次域 k 上的运算。当 $k=2^8$，$n=33$ 时，计算复杂度约为 2^{43} 次 2^8 域上的运算，解空间的维数为 $D=32$。

步骤 2 获得以明文变量为未知量的二次多项式方程组。

将要破解的合法密文代入步骤 1 中所得的二次化方程组，合并同类项，即可获得 D' 个以明文变量为未知量的二次多项式方程组。这部分的计算量较小，可忽略不计。实验结果表明，总有 $D'=D$。

步骤 3 恢复合法密文相应的明文。

将步骤 2 中得到的以明文变量为未知量的二次多项式方程组与方程组(1)合并，然后用 Groebner 基方法进行求解。在所有的实验中，都成功地恢复了合法密文相应的明文。

4.3.2 实验结果

在实验中，选择 $k=\mathrm{GF}(2^8)$，选取了不同的 n，d，θ 来进行实验。对于所有的实验，都成功地恢复了合法密文相应的明文。对实验各个环节的时间进行了统计，如表 1 所示。

通过表 1 可以看出，随着 n 的增长，得到二次化方程的时间增长较大，但是 Groebner 基求解的时间却相差无几。在多数情况下，$D=n-\gcd(n,\theta)$ 这与文献[10]中给出的 MI 体制满足的线性化方程的维数结果不小于 $2n/3$ 是一致的，但是还存在着一些例外，如表 1 中的 $n=20$，$d=5$，$\theta=4$，而 $D=15$。

另外，在实验中，将本文的破解方法与直接使用 Groebner 基求解方程组进行了比较，如表 2 所示。

表 1 不同参数下二次化方程破解时间比较

n	d	θ	D	D'	$T1$/s	$T2$/s	$T3$/s	合计/s
17	5	4	16	16	6.6	18.8	0.015	38.4
17	8	4	16	16	6.5	19.2	0	39.0
17	8	16	16	16	6.4	19.1	0	38.5
20	5	4	15	15	16.7	73.6	0.016	120.6
20	10	4	16	16	15.9	73.8	0.015	122.8
20	10	16	16	16	16.6	73.7	0.016	122.9
23	5	4	22	22	37.1	240.4	0.015	375.3
23	11	4	22	22	37.6	240.3	0.016	375.5
23	11	22	22	22	37.5	240.5	0.031	375.6
26	5	4	24	24	73.5	700.0	0.015	993.5
26	12	4	24	24	77.5	702.2	0.047	1 001.6
26	12	24	24	24	78.3	699.9	0.016	999.4
33	7	4	32	32	313.3	5 232.1	0.016	6 655.3
33	16	4	32	32	318.2	5 391.5	0.047	6 855.3
33	16	32	32	32	320.0	5 332.0	0.016	6 802.4

注：$T1$：生成明密对时间；$T2$：得到二次化方程的时间；$T3$：Groebner 基求解时间。

表 2　二次化方程方法与 Groebner 基直接求解比较

n	d	θ	$T1$/s	$T2$/s
14	5	4	0.015	0.234
15	5	5	0.078	0.266
17	5	4	0.015	103.015
18	5	4	0.016	442.391

注：$T1$：二次化方程方法中求解方程组的时间；$T2$：直接采用 Groebner 基求解方程组的时间。

由于当 $n>18$ 时，采用普通的 PC 机进行 Groebner 基求解方程组过程中，程序报错，显示内存不够。因此，表 2 中仅选取了较小的 n 进行比较。通过表 2 可发现，当 n=18，$T2$ 是 $T1$ 的约 30 000 倍，可见二次化方程能够非常有效地缩短 Groebner 基求解方程组的时间。

5　结束语

本文给出了乔等提出的 MPKC 的安全性增强方案的安全性分析。通过分析发现，若原始体制满足一阶线性化方程，则乔等的改进方案必然满足一阶二次化方程。本文利用二次化方程方法成功地破解了乔等改进方案的一个实例。从实验中可知，二次化方程的存在将有助于利用 Groebner 基恢复合法密文相应的明文。因此，在设计多变量公钥密码体制的时候，要尽量避免二次化方程的出现。

参考文献：

[1] DING J T, GOWER J, SCHMIDT D. Multivariate Public Key Cryptosystems [M]. Berlin: Springer-Verlag, 2006.

[2] PATARIN J. Cryptanalysis of the Matsumoto and Imai public key scheme of eurocrypt 1988[A]. Proceedings of Advances in Cryptology, Crypto 1995[C]. Santa Barbara, California, USA, 1995. 248-261.

[3] MATSUMOTO T, IMAI H. Public quadratic polynomial-tuples for efficient signature verification and message encryption [A]. Proceedings of Advances in Cryptology- Eurocrypt'88[C]. Davos, Switzerland, 1988. 419-453.

[4] DING J T, HU L, NIE X Y, LI J Y, WAGNERJ. High order linearization equation (HOLE) attack on multivariate public key cryptosystems [A]. Proceedings of Public key Cryptography—PKC 2007[C]. Beijing, China, 2007. 233-248.

[5] WANG L C, YANG B Y, HU Y H, LAI F. A medium-field multivariate public-key encryption scheme [A]. Proceedings of Topics in Cryptology, CT-RSA 2006[C]. San Jose, CA, USA, 2006. 132-149.

[6] WANG X, FENG F, WANG X, WANG Q. A more secure MFE multivariate public key encryption scheme[J]. International Journal of Computer Science and Applications, 2009, 6(3): 1-9.

[7] CAO W W, NIE X Y, HU L, TANG X L, DING J T. Cryptanalysis of two quartic encryption schemes and one improved MFE scheme[A]. Proceedings of Cryptology, PQCrypto 2010[C]. Darmstadt, Germany, 2010. 41-60.

[8] 乔帅庭, 李益发, 韩文报. 新扩展多变量公钥密码方案[J]. 通信学报, 2014, 35(4): 148-154.
QIAO S T, LI Y F, HAN W B. Novel extended multivariate public key cryptosystem[J]. Journal on Communications, 2014, 35(4): 148-154.

[9] NIE X Y, PETZOLDT A, BUCHMANN J, LI F G. Linearization equation attack on 2-layer nonlinear piece in hand method[J]. IEICE Transactions , 2014, 97(9): 1952-1961 .

[10] DIENE A, DING J T, GOWER J E, HODGES T J, YIN Z J. Dimension of the linearization equations of the Matsumoto-Imai cryptosystems[A]. Proceedings of Code and Cryptography—WCC 2005[C]. Bergen, Norway, 2005. 242-251.

作者简介：

聂旭云（1975-），男，江西樟树人，电子科技大学副教授、硕士生导师，主要研究方向为多变量公钥密码、代数攻击等。

刘波（1990-），男，重庆人，电子科技大学硕士生，主要研究方向为多变量公钥密码。

鲁刚（1976-），男，四川成都人，电子科技大学博士生，主要研究方向为多变量公钥密码。

钟婷（1977-），女，四川成都人，电子科技大学副教授、硕士生导师，主要研究方向为云计算安全。