doi:10.3969/j.issn.1000-436x.2014.04.017

新扩展多变量公钥密码方案

乔帅庭[1,2]，李益发[1]，韩文报[1,2]
（1.信息工程大学 四院，河南 郑州 450002；2. 数学工程与先进计算国家重点实验室，江苏 无锡 214125）

摘 要：为了有效地抵抗线性攻击和差分攻击，基于“温顺变换”思想构造了一种非线性可逆变换，将此变换与Matsumoto-Imai (MI)方案结合，提出了一种新的扩展多变量公钥密码方案。接着，在扩展方案的基础上，设计出了新的多变量公钥加密方案和签名方案。分析结果表明：该方案继承了 MI 方案计算高效的优点，并且能够抵抗线性攻击、差分攻击和代数攻击。

关键词：温顺变换；新的扩展方案；线性攻击；差分攻击；代数攻击
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1000-436X(2014)04-0148-07

Novel extended multivariate public key cryptosystem

QIAO Shuai-ting[1,2], LI Yi-fa[1], HAN Wen-bao[1,2]
(1. The Fourth Institute Information Engineering University, Zhengzhou 450002, China;
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi 214125, China)

Abstract: To resist linearization attack and differential attack effectively, a nonlinear invertible transformation based on “tame transformation” was constructed. Incorporated with the Matsumoto-Imai (MI) scheme, a novel extended multivariate public key cryptosystem was proposed. Then, according to the proposed scheme, two practical applications including an encryption scheme and a signature scheme were designed respectively. Analysis results demonstrate that the extended cryptosystem inherits the merit of MI, i.e. efficient computation. Meanwhile, the novel extended scheme can also resist linearization attack, differential attack and algebraic attack.

Key words: tame transformation; the novel extended cryptosystem; linearization attack; differential attack; algebraic attack

1 引言

二十一世纪是信息的时代，继电子信息科学技术之后，量子和生物等新型信息科学正在建立和发展。量子计算机的产生将会对目前广泛使用的基于离散对数（包括椭圆曲线上的离散对数）和大数分解的公钥密码体制构成潜在的威胁[1~3]。为此，基于抗量子的公钥密码体制成为密码学中一个研究的热点和重点[4]。多变量公钥密码系统作为一种能有效抵抗未来的基于量子计算机攻击方法的密码体制，在近二十几年受到越来越多的关注。

多变量公钥密码体制的安全性是基于有限域上多元非线性方程组的难解性[5]和多项式同构问题[6]。1988 年，日本学者 Matsumoto 和 Imai 提出了第一个多变量公钥密码方案，即著名的 Matsumoto-Imai (MI)方案[7]。该方案将“小域—大域”思想引入了多变量公钥密码方案，有较高的计算效率，在当时被认为是安全的。然而，1995 年，Patarin 等提出了针对 MI 方案的线性攻击[8]，攻破了原始的 MI 体制。为了抵抗线性攻击，Patarin 等在 2001 年提出了 FLASH 方案[9]，Ding 等人于 2004 年提出了 PMI 方案[10]，但都受到差分攻击的影响[11,12]。到目前为止，多变量公钥密码体制主要有 5 类方案[5]：MI 方案、hidden field equation (HFE)方案、unbalanced oil and

收稿日期：2012-12-29；**修回日期**：2013-03-13
基金项目：国家高技术研究发展计划(“863”计划)基金资助项目(2009AA012201)；数学工程与先进计算国家重点实验开放课题基金资助项目(2013A03, 2013A10)
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2009AA012201); The Opening Projects of State Key Laboratory of Mathematical Engineering and Advanced Computing (2013A03, 2013A10)

vinegar (UOV)方案、stepwise triangular systems (STS)方案和 medium field equation (MFE)方案，但大部分不能同时用于加密和签名。近几年来，多变量公钥密码体制的研究一直是热点，相继出现了 CyclicRainbow 方案[13]、Double-Layer square 方案[14]、Enhenced STS 方案[15]等，它们在安全性上得到了不同程度的提高[16,17]。2011 年，Wang 等通过引入 Hash 认证技术、并结合传统 Multivariate Quadratic（MQ）公钥密码算法，提出了一种扩展 MQ 公钥密码体制[18]，同时具备加密和签名功能。但该方案的加密和签名算法的构造较为复杂，引入了较大的私钥空间。本文利用函数合成思想，构造了一种独特的基于温顺变换思想[19]的非线性可逆变换，并将此变换与 MI 方案结合起来，提出了一种新的扩展多变量公钥密码方案，且给出了新的扩展方案的加密和签名方案。分析结果显示：该方案继承了 MI 方案计算高效的特点，具有较小的私钥量；克服了 MI 方案不能抵抗线性攻击、差分攻击的缺陷，还能抵抗代数攻击。

2　多变量公钥密码体制及 MI 方案简介

本文方案是在多变量公钥密码体制基础上，与 MI 方案结合而成的，下面从多变量公钥密码体制的一般结构、加解密及签名和 MI 方案三方面对相关研究工作展开论述。

2.1　多变量公钥密码的一般结构

多变量公钥密码的门限函数形式为有限域上一类多元二次方程组

$$P=(p_1(x_1,\cdots,x_n),\cdots,p_n(x_1,\cdots,x_n)) \quad (1)$$

每个 p_i 为一个关于 $x=(x_1,\cdots,x_n)$ 的非线性二次方程

$$y_k=p_k(x):\sum_i P_{ik}x_i+\sum_i Q_{ik}x_i^{\,2}+\sum_{i>j}P_{ijk}x_ix_j \quad (2)$$

所有的系数和变量都在域 $K=F_q$ 中，q 为域 K 的阶。多变量公钥体制的构造主要基于 multivariate quadratic (MQ)问题及 isomorphism of polynomials (IP)问题的难解性。

定义 1　给定有限域 F_q 上的 n 个变元 m 个方程组成的非线性方程组

$$\begin{cases} p_1(x_1,\cdots,x_n)=y_1 \\ p_2(x_1,\cdots,x_n)=y_2 \\ \quad\vdots \\ p_m(x_1,\cdots,x_n)=y_m \end{cases}$$

其中，p_i 的系数和变量均取自有限域 $K=F_q$，通常 q>2，每个多项式的形式为

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

求解该方程组的问题称为 MQ 问题。已经证明 MQ 问题为 NP 难问题，即使是在最小的域 F_2 上。

定义 2　设(*P*)和(*Q*)为有限域 F_q 上随机的 n 元 m 个方程的多变量方程组，且(*P*)和(*Q*)同构，则有 $P=T\circ Q\circ S$，T 和 S 分别为 2 个可逆的仿射变换。称寻找从(*Q*)到(*P*)同构的(*T*, *S*)的问题为 IP 问题，即多项式同构问题。

一般地，设 $(Q)\in(F_q[a_1,\cdots,a_n])^m$ 为 F_q 上 m 个多项式集合，集合中每个多项式都是 n 元二次多项式，其形式如下

$$b_i=\sum_{1\leqslant j\leqslant k\leqslant n}\gamma_{i,jk}a_ja_k+\sum_{1\leqslant j\leqslant n}\beta_{i,j}a_j+\alpha_i,1\leqslant i\leqslant m$$

S，T 分别为 $F_q^{\,n}$ 和 $F_q^{\,m}$ 上 2 个可逆的仿射变换，记 $S(x_1,\cdots,x_n)=(a_1,\cdots,a_n)$，$T(b_1,\cdots,b_m)=(y_1,\cdots,y_m)$，则由 $P=T\circ Q\circ S$ 可从(*Q*)得到另一个 n 元 m 个方程的多变量方程组(*P*)，形式如下所示

$$y_i=\sum_{1\leqslant j\leqslant k\leqslant n}\gamma'_{i,jk}a_ja_k+\sum_{1\leqslant j\leqslant n}\beta'_{i,j}a_j+\alpha'_i,1\leqslant i\leqslant m$$

2.2　加解密及签名

多变量公钥密码的加解密方法如下所示

$$u=(u_1,\cdots,u_n)\underset{S^{-1}}{\overset{S}{\rightleftarrows}}x=(x_1,\cdots,x_n)\underset{Q^{-1}}{\overset{Q}{\rightleftarrows}}$$

$$y=(y_1,\cdots,y_m)\underset{T^{-1}}{\overset{T}{\rightleftarrows}}v=(v_1,\cdots,v_m)$$

这里，S 和 T 分别为 $F_q^{\,n}$ 和 $F_q^{\,m}$ 上的可逆仿射变换，中心映射为 $Q:F_q^{\,n}\to F_q^{\,m}$，公钥为 $P=T\circ Q\circ S$，S 和 T 共同“隐藏”中心映射 Q 的结构，是私钥的重要组成部分。

1) 加密

给定明文 $(u_1,\cdots,u_n)$，利用公钥 $P=T\circ Q\circ S$ 对其进行运算，得到密文 $(v_1,\cdots,v_n)=P(u_1,\cdots,u_n)$。

2) 解密

给定密文 $(v_1,\cdots,v_n)$，利用私钥 $\{T^{-1},Q^{-1},S^{-1}\}$ 对密文依次进行 T^{-1}、Q^{-1} 和 S^{-1} 运算，得到明文 $(u_1,\cdots,u_n)=S^{-1}(Q^{-1}(T^{-1}(v_1,\cdots,v_n)))$。

3) 签名

给定消息 M，得到消息摘要 $(v_1,\cdots,v_m)=\mathrm{Hash}(M)$，利用私钥 $\{T^{-1},Q^{-1},S^{-1}\}$ 对其依次进行

T^{-1}、Q^{-1} 和 S^{-1} 运算，得到签名 $(u_1,\cdots,u_n)=S^{-1}(Q^{-1}(T^{-1}(v_1,\cdots,v_n)))$。

4) 验证

给定签名 $(u_1,\cdots,u_n)$，利用公钥 $P=T\circ Q\circ S$ 对其进行运算，得到消息摘要 $(v_1',\cdots,v_m')$，然后判断 $(v_1',\cdots,v_m')=\mathrm{Hash}(M)$ 是否成立，若成立，则签名有效，否则，签名无效。

2.3 MI 方案

1988 年，Matsumoto 和 Imai 提出了第一个多变量公钥方案——MI 方案[7]。

令 k 为一有限域，$k=F_q$，特征为 2，可设 $q=2^w$。K 为 k 的 n 次扩域，$K=F_{q^n}$。定义 K 同构 $\phi:K\to k^n$，$\phi(a_0+a_1x+\cdots+a_{n-1}x^{n-1})=(a_0,\cdots,a_{n-1})$。正整数 θ 满足 $gcd(1+q^\theta,\ q^n-1)=1$，此时定义 F：$K\to K$，$F(X)=X^{1+q^\theta}$，则 F 为可逆的，$F^{-1}(X)=X^t$，这里 t 满足 $t(1+q^\theta)\equiv 1 \bmod (q^n-1)$。

定义映射 $\bar{F}:k^n\to k^n$：

$$\begin{aligned}\bar{F}(x_1,\cdots,x_n)&=\phi\circ F\circ\phi^{-1}(x_1,\cdots,x_n)\\&=(\bar{F}_1(x_1,\cdots,x_n),\cdots,\bar{F}_n(x_1,\cdots,x_n))\end{aligned}$$

此时，$\bar{F}_i(x_1,\cdots,x_n)$ 为关于 $x_1,\cdots,x_n$ 的二次多项式。

最后，随机选择 2 个 k^n 上的可逆的仿射变换 L_1 和 L_2，定义

$$\begin{aligned}\hat{F}(x_1,\cdots,x_n)&=L_1\circ\bar{F}\circ L_2(x_1,\cdots,x_n)\\&=(\hat{F}_1(x_1,\cdots,x_n),\cdots,\hat{F}_n(x_1,\cdots,x_n))\end{aligned}\tag{3}$$

则 MI 方案的公钥为 $\hat{F}$，私钥为 L_1、L_2、θ。

3 新的扩展多变量公钥密码方案

多变量公钥密码体制根据不同的中心映射的构造方法主要可分为：MI 体制、隐藏域方程体制、不平衡油醋体制、三角形体制以及中间域方程体制。这些算法大多不能同时用于加密和签名，而且，大部分受到不同程度地攻击[19]，例如线性攻击、差分攻击、代数攻击等。如何构造一种安全高效且同时具备加密和签名功能的多变量方案仍是一个值得研究的难题和热点。

本文利用温顺变换(tame transformation)思想，构造出非线性可逆变换 $L_3:F_q^{\,n}\to F_q^{\,n}$，即 $L_3(x_1,\cdots,x_n)=(t_1,\cdots,t_n)$。然后，将 MI 方案 $\hat{F}=L_1\circ\phi\circ F\circ\phi^{-1}\circ L_2$ 与基于温顺变换思想的非线性可逆变换结合起来，提出了一种新的扩展多变量公钥密码方案

$$\begin{aligned}\hat{F}(x_1,\cdots,x_n)&=L_1\circ\phi\circ F\circ\phi^{-1}\circ L_2\circ L_3(x_1,\cdots,x_n)\\&=(p_1'(x_1,\cdots,x_n),\cdots,p_n'(x_1,\cdots,x_n))\end{aligned}\tag{4}$$

3.1 L_3 的构造

L_3 的构造用到一类特殊的映射 $G:GF(q)^n\to GF(q)^n$，其形式为

$$\begin{pmatrix}t_1\\t_2\\\vdots\\t_{n-1}\\t_n\end{pmatrix}=\begin{pmatrix}x_1\\x_2+g_1(x_1)\\\vdots\\x_{n-1}+g_{n-2}(x_1,\cdots,x_{n-2})\\x_n+g_{n-1}(x_1,\cdots,x_{n-2},x_{n-1})\end{pmatrix}$$

其中，g_i 为任意二次多项式。此变换结构特殊，容易求逆，也称温顺变换[19]。

取正整数 n，d，且满足 $n>2d$，构造基于温顺变换的可逆变换 $L_3(x_1,\cdots,x_n)=(t_1,\cdots,t_n)$，其形式如下

$$\begin{cases}t_1=x_1+c_1x_{d+1}x_n\\t_2=x_2+c_2x_{d+2}x_{n-1}\\\quad\vdots\\t_d=x_d+c_dx_{2d}x_{n-d+1}\\t_{d+1}=x_{d+1}\\\quad\vdots\\t_n=x_n\end{cases}\tag{5}$$

$L_3^{-1}(t_1,\cdots,t_n)=(x_1,\cdots,x_n)$ 形式如下

$$\begin{cases}x_1=t_1-c_1t_{d+1}t_n\\x_2=t_2-c_2t_{d+2}t_{n-1}\\\quad\vdots\\x_d=t_d-c_dt_{2d}t_{n-d+1}\\x_{d+1}=t_{d+1}\\\quad\vdots\\x_n=t_n\end{cases}\tag{6}$$

3.2 新扩展方案

利用函数合成思想将 MI 方案与基于温顺变换思想构造的 L_3 结合，得到新扩展多变量公钥密码方案的公钥多项式为

$$\hat{F}(x_1,\cdots,x_n)=L_1\circ\phi\circ F\circ\phi^{-1}\circ L_2\circ L_3(x_1,\cdots,x_n)$$

其中，L_1、L_2、ϕ、ϕ^{-1} 的定义同 MI 方案中的定义一致，L_3 的定义如 3.1 节所述。正整数 θ 满足条件

$gcd(1+q^{\theta},q^n-1)=1$，此时定义 F：$K\to K$，$F(X)=X^{1+q\theta}$，则 F 为可逆的，且当 $t(1+q^{\theta})\equiv 1 \bmod (q^n-1)$时 $F^{-1}(X)=X^t$。

对应地，$(L_1^{-1},L_2^{-1},L_3^{-1},\theta)$作为私钥。

3.3 基于新扩展体制的加密方案

基于新体制的加密方案的私钥 $D=\{L_1^{-1},F^{-1},L_2^{-1},L_3^{-1}\}$，其中 L_3^{-1} 的形式如 3.1 节所述。

加密过程：加密者用公钥 $\hat{F}$ 对明文 $(x_1,\cdots,x_n)$ 进行加密，得到密文：

$$(y_1,\cdots,y_n)=\hat{F}(x_1,\cdots,x_n)$$

解密过程：解密者收到密文 $(y_1,\cdots,y_n)$ 后，做如下计算。

1) 用私钥 L_1^{-1} 计算可得 $(y_1',\cdots,y_n')=L_1^{-1}(y_1,\cdots,y_n)$。

2) 用中心映射 $\bar{F}=\phi\circ F\circ\phi^{-1}$ 的逆变换 $\bar{F}^{-1}$ 计算 $(x_1',\cdots,x_n')=\bar{F}^{-1}(y_1',\cdots,y_n')$。

3) 用私钥 L_2^{-1} 计算得到 $(t_1,\cdots,t_n)=L_2^{-1}(x_1',\cdots,x_n')$。

4) 用私钥 L_3^{-1} 计算便可得到相应的明文 $(x_1,\cdots,x_n)=L_3^{-1}(t_1,\cdots,t_n)$。

由解密的过程，可得明文 $(x_1,\cdots,x_n)$ 与密文 $(y_1,\cdots,y_n)$ 满足如下关系式：

$$\begin{aligned}(x_1,\cdots,x_n)&=L_3^{-1}(L_2^{-1}(\bar{F}^{-1}(L_1^{-1}(y_1,\cdots,y_n))))\\&=(L_1\circ\bar{F}\circ L_2\circ L_3)^{-1}(y_1,\cdots,y_n)\\&=\hat{F}^{-1}(y_1,\cdots,y_n)\end{aligned}\tag{7}$$

从而可得，$\hat{F}(x_1,\cdots,x_n)=(y_1,\cdots,y_n)$。由此可知解密过程的正确性。

3.4 基于新扩展体制的签名方案

签名：设 M 为待签名文件，用公开的散列函数 Hash 计算 $(y_1,\cdots,y_n)=\mathrm{Hash}(M)$。签名体制的私钥和上述加密方案的私钥一致，计算签名 $(x_1,\cdots,x_n)$ 的步骤和 3.3 中解密步骤相同，不再详述。

验证：验证者收到消息 M 和签名 $(x_1,\cdots,x_n)$ 后，验证如下。

1) 计算 $\mathrm{Hash}(M)=(y_1,\cdots,y_n)$；

2) 然后验证下列方程组

$$\begin{cases}p_1'(x_1,\cdots,x_n)-y_1=0\\p_2'(x_1,\cdots,x_n)-y_2=0\\\quad\vdots\\p_n'(x_1,\cdots,x_n)-y_n=0\end{cases}$$

是否成立。若成立，则签名有效；否则，签名无效。

4 新方案的性能分析和安全性分析

下面将对新方案进行性能分析和安全性分析。性能分析主要包括公私钥大小和扩展体制的运算效率。安全性分析则从针对多变量公钥密码体制的结构攻击和直接攻击着手。

4.1 性能分析

4.1.1 公私钥大小

1) 基于“温顺变换”思想的扩展方案的公钥的一般形式为

$$\begin{aligned}p_i(x_1,\cdots,x_n)&=p_i(t_1,\cdots,t_n)\\&=\sum_{1\leqslant j\leqslant k\leqslant n}a'_{ijk}t_jt_k+\sum_{j=1}^{n}b'_{ij}t_j+e_i\end{aligned}$$

由 3.1 节中 t_i 的构造可得

$$\begin{aligned}p_i(x_1,\cdots,x_n)=&\sum a_{ijklo}x_jx_kx_lx_o+\\&\sum b_{ijkl}x_jx_kx_l+\sum c_{ijk}x_jx_k+\sum d_{ij}x_j+e_i\end{aligned}$$

对应的公钥空间为 $n(C_d^2+d+2C_d^2+2d+(n-d)d+C_n^2+n+d+n+1)$，即 $n\cdot\dfrac{n^2+3n+2+(d^2+(2n+5)d)}{2}$，而 MI 方案的公钥为 $n\cdot(n^2+3n+2)/2$，$n\cdot[n^2+3n+2+(d^2+(2n+5)d)]/2$ 关于正整数 d 是递增函数，由于 $n>2d$，当 d=1 时，公钥大小基本不变，当 $d=\lfloor n/2\rfloor$ 时，扩展体制的公钥大小约为 MI 方案公钥的 2.25 倍。若选取合适的 d 值（比如 $d=\lfloor n/4\rfloor$，约为 MI 方案的 1.56 倍），可适当降低公钥大小。经分析，可取参数 w=8，n=32，$d\geqslant 6$，当 d=6 即 $d=\dfrac{3}{16}n$ 时，扩展体制的公钥大小为 MI 方案公钥的 1.41 倍。而 MI 方案的公钥空间大小约为 $\dfrac{1}{2}wn^3$ bit，所以在推荐参数 w=8，n=32，d=6 下，扩展方案的公钥空间约为 22.56 KB，与其他的多变量公钥密码体制相比，该体制的公钥空间是比较理想的。

对于私钥而言，如 3.1 节定义，L_3 的私钥为 $c_1,\cdots,c_d$，由于 $d=6$，相对于 L_1、L_2 的私钥量，L_3 的私钥量极小，而 MI 方案的私钥量大小约为 $2wn^2$ bit，Wang 等人的方案私钥量约为 $3wn^2$ bit，新扩展方案的私钥量大小约为 $w(2n^2+6)$ bit，在推荐参数 w=8，n=32 下，MI 方案私钥量大约为 2 KB，Wang 等人的私钥量约为 3 KB，新扩展方案的私钥量约为 2 KB，与 MI 方案相比，对应的扩展体制私钥量基

本不发生变化；与 Wang 等人的方案相比，本文新的扩展方案缩小了约 1/3 私钥量。

4.1.2 运算效率

由 L_3，L_3^{-1} 构造可知，它们的运算仅仅多出了 d 个乘法和加法，在推荐参数 w=8，n=32，d=6 下，相对于 MI 体制的加解密和签名效率，运算 L_3 和 L_3^{-1} 可忽略不计，不影响全局运算效率，因此，新的扩展体制保持了 MI 方案的高效性。

可见，本文提出的新的扩展方案具备较小的公钥量和私钥量，保持了 MI 方案的优势，具有较高的加解密和签名效率。

4.2 安全性分析

多变量体制的安全性分析分为结构攻击和直接攻击 2 类。结构攻击是针对多变量体制特殊的结构特征，主要包括线性攻击和差分攻击。直接攻击是从多变量体制的公钥多项式入手，常用的攻击方法为 Gröbner 基算法和 XL 算法。通常认为只要攻击方案的复杂度超过 $O(2^{80})$，则称该方案可抗此种攻击。下面进行本文方案的安全性分析。

4.2.1 抗线性攻击

1998 年 Patarin 提出的一种线性攻击[8]，在 w=8，n=32 的情况下，经过 $O(2^{32})$ 次运算就可以求解。

根据 MI 方案特殊的中心映射 $F: X \mapsto X^{q^\theta+1}$，存在如下特殊的代数关系式

$$Y^{q^\theta-1} = X^{q^{2\theta}-1} \tag{8}$$

两边分别乘以 XY，得到关系式

$$XY^{q^\theta} = YX^{q^{2\theta}} \tag{9}$$

进一步，通过同构映射 ϕ 的作用，定义 $X = \phi^{-1} \circ L_2(x_1, \cdots, x_n)$，$Y = \phi^{-1} \circ T^{-1}(y_1, \cdots, y_n)$，可以得到 n 个 F_q 上的多元二次方程式，每个方程式具有如下的形式

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij} x_i y_j + \sum_{i=1}^{n} b_i x_i + \sum_{i=1}^{n} c_i y_i + d = 0 \tag{10}$$

其中，a_{ij}、b_i、c_i、d 为方程式的$(n+1)^2$ 个系数。

在给出 $O((n+1)^2)$个明密文对 $(x_1, \cdots, x_n, y_1, \cdots, y_n)$ 时，可以求解上述方程组的系数。一旦所有的系数均被求解得到，那么在给定密文 $y=(y_1, \cdots, y_n)$ 的情况下，就可得到关于明文 $x=(x_1, \cdots, x_n)$ 的 n 个线性方程组。

定理 1 新扩展方案利用函数合成思想，将非线性可逆变换 L_3 与 MI 方案结合起来，从而可抗线性攻击。

证明 根据中心映射的构造可得

$$XY^{q^\theta} = YX^{q^{2\theta}}$$

由新体制的构造得 $X = \phi^{-1} \circ L_2 \circ L_3(x_1, \cdots, x_n) = \phi^{-1} \circ L_2(t_1, \cdots, t_n)$，$Y = \phi^{-1} \circ L_1^{-1}(y_1, \cdots, y_n)$，通过同构映射 ϕ 的作用，可以得到 n 个 F_q 上的多元二次方程式，每个方程式具有如下的形式

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}' t_i y_j + \sum_{i=1}^{n} b_i' t_i + \sum_{i=1}^{n} c_i' y_i + d = 0 \tag{11}$$

在给出 $O((n+1)^2)$个 $(t_1, \cdots, t_n, y_1, \cdots, y_n)$ 时，可以求解上述方程组的系数。而密文 $(y_1, \cdots, y_n)$ 已知，中间量 $(t_1, \cdots, t_n)$ 未知，所以代入密文后仍然无法解出方程组的系数；但当 $d=1, \cdots, 5$ 时，含有二次非线性项较少，此时若对 $t_1, \cdots, t_5$ 进行穷举，可以在 $O(2^{80})$时间以内攻破。以 d=1 为例，此时 $t_1 = x_1 - c_1 x_{d+1} x_n$，$t_i = x_i$ $(i=2, \cdots, n)$ 得到如下的关系式

$$\sum_{i=2}^{n}\sum_{j=1}^{n} a_{ij}' x_i y_j + \sum_{i=2}^{n} b_i' x_i + \sum_{i=1}^{n} c_i' y_i + t_1 \sum_{j=1}^{n} a_{1j}' y_j + b_1' t_1 + d = 0 \tag{12}$$

若对 t_1 进行穷举，可得

$$\sum_{i=2}^{n}\sum_{j=1}^{n} a_{ij}' x_i y_j + \sum_{i=2}^{n} b_i' x_i + \sum_{i=1}^{n} c_i'' y_i + d' = 0 \tag{13}$$

而在参数 w=8，n=32，d=1 时，假设出现最好的情况：攻击者知道 $t_i = x_i$ $(i=2, \cdots, n)$。在已知足够多的明密文对 $(t_1, x_2, \cdots, x_n, y_1, \cdots, y_n)$ 时，可求解出系数，在给定密文 $y=(y_1, \cdots, y_n)$ 时，可依次给出 $t_1, x_2, \cdots, x_n$，此过程的复杂度为 $O(2^{32})$。再对 c_1 穷举，可得到明文 $x_1, \cdots, x_n$，所以在 d=1 时，线性攻击成功的复杂度约为 $O(2^{40})$，当 d=2 时，线性攻击成功的复杂度约为 $O(2^{48})$，依次类推，d=5 时，线性攻击成功的复杂度约为 $O(2^{72})$。所以当 $d \geqslant 6$ 时，线性攻击成功的复杂度为 $O(2^{80})$，即安全级别为 $O(2^{80})$。

综上所述，新的扩展方案可抵抗线性攻击。

4.2.2 抗差分攻击

MI 体制是公钥密码发展的一个里程碑，它为该领域带来了一种全新的设计思想。在此基础上，相继提出了 PMI 方案、SFLASH 方案等。但是 PMI 方案、SFLASH 方案均受到差分攻击。SFLASH 方案其实就是 MI-Minus 方案即 C^{*-} 体制，可通过差分

分析恢复出 r 个被去掉的多项式的等价多项式，再加上已知的 $n-r$ 个公钥多项式，从而构成了一个完整的 MI 方案的公钥多项式，这样就可重新利用线性攻击去伪造签名。

首先，给出差分的定义：对于函数 $F(x)$，定义其在 a 点处的差分为

$$DF(a,x)=F(x+a)-F(x)-F(a)+F(0)$$

在 MI 方案中，中心函数为 $\bar{F}(x)=x^{1+q^\theta}$，所以 $D\bar{F}(a,x)=a^{q^\theta}x+ax^{q^\theta}$。显然 $D\bar{F}(a,x)$ 是一个关于变量 x 和 a 的双线性对称函数。对于 $\forall\xi\in GF(q^n)$，差分函数 $D\bar{F}$ 有一个特殊的性质（即乘法特性）

$$D\bar{F}(a,\xi\cdot x)+D\bar{F}(\xi\cdot a,x)=(\xi+\xi^{q^\theta})D\bar{F}(a,x) \tag{14}$$

同理，MI 体制的公钥函数 $\hat{F}=L_1\circ\bar{F}\circ L_2$ 的差分函数 $D\hat{F}$ 满足如下关系式

$$\begin{aligned}&D\hat{F}(\xi a,x)+D\hat{F}(a,\xi x)\\&=L_1\circ D\bar{F}(\xi\cdot L_2(a),L_2(x))+L_1\circ D\bar{F}(L_2(a),\xi\cdot L_2(x))\\&=L_1\circ(\xi+\xi^{q^\theta})\circ L_1^{-1}\circ D\hat{F}(a,x)\end{aligned} \tag{15}$$

若使用“减方法”后 MI 体制的公钥为 $\hat{F}'=L_1^-\circ\bar{F}\circ L_2$，则可根据公钥 $\hat{F}'$ 并结合式(15)的特殊性质，可求出非平凡映射 N_ξ 使之满足

$$\hat{F}''=\hat{F}'\circ N_\xi=L_1^-\circ M_\xi\circ\bar{F}\circ L_2 \tag{16}$$

其中，N_ξ和M_ξ均表示关于ξ的线性映射。

于是可从 $\hat{F}''$ 中随机选出 r 个方程，与公钥中的 $n-r$ 个方程一起构成新的 MI 算法的公钥，其成功的概率为 $1-1/q$。然后再用上述线性化方程攻击方法来伪造签名。

定理 2　新扩展方案在 MI 方案的基础上，引入了非线性可逆变换 L_3，打破了 MI 体制的乘法反对称性，能很好地抵抗差分攻击。

证明　对于新方案而言，由于在 MI 方案外层增加了可逆非线性变换 L_3，此时公钥函数 $\hat{F}$ 变为 $\hat{F}$

$$\hat{F}=L_1\circ\bar{F}\circ L_2\circ L_3\xrightarrow{\text{定义}L_2'=L_2\circ L_3}L_1\circ\bar{F}\circ L_2' \tag{17}$$

由于 L_3 变换是一个非线性变换，对应地，式(17)中 L_2' 也是一个非线性变换，因此对于 $\forall x,\xi\in GF(q^n)$，显然有

$$\xi\circ L_2'(x)\neq L_2'(\xi x) \tag{18}$$

故对于新体制公钥函数 $\hat{F}=L_1\circ\bar{F}\circ L_2'$ 的差分函数为 $D\hat{F}$ 有

$$\begin{aligned}&D\hat{F}(\xi a,x)+D\hat{F}(a,\xi x)\\&=L_1\circ D\bar{F}(\xi\cdot L_2'(a),L_2'(x))+\\&\quad L_1\circ D\bar{F}(L_2'(a),\xi\cdot L_2'(x))\\&\neq L_1\circ(\xi+\xi^{q^\theta})\circ L_1^{-1}\circ(D\hat{F}(a,x))\end{aligned} \tag{19}$$

式(19)表明非线性变换 L_3 的引入破坏了 MI 体制公钥的乘法反对称性。

所以新扩展方案能抵抗差分攻击。

4.2.3　抗代数攻击

代数攻击常用的工具包括 Gröbner 基算法和 XL 算法[17]。目前，计算 Gröbner 基最有效的算法为 F4 和 F5 算法。

定理 3　新的扩展方案是将 MI 方案与非线性可逆变换 $L_3:F_q^n\to F_q^n$ 结合而成，公钥多项式为 $P(x_1,\cdots,x_n)=(y_1,\cdots,y_n)$，在推荐的参数 n=32 下，可以抵抗代数攻击。

证明　根据方程的个数 m 和变量的个数 n 之间的大小关系，分 3 种情况讨论。

1) 当 m=n 时，多元二次方程组为置换方程组，当 $k=GF(q)\neq GF(2)$ 时，求解方程组的复杂度为 $O(2^{3m})$[19]。

2) 当 m>n 时，多元二次方程组为超定方程组，此时用 XL 算法。当 $m\geqslant\varepsilon n^2$，$0<\varepsilon\leqslant 1/2$ 时，XL 算法都可以在 $n^{O(1/\sqrt{\varepsilon})}$ 的多项式时间内运行成功[20]。

3) 当 m<n 时，多元二次方程组为不定方程组[21]，求解的复杂度约等于穷尽搜索的复杂度 $O(q^m)$。

在新方案中，公钥多项式为 $P(x_1,\cdots,x_n)=(p_1(x_1,\cdots,x_n),\cdots,p_n(x_1,\cdots,x_n))$，对应的方程组为

$$\begin{cases}p_1(x_1,\cdots,x_n)=0\\\quad\vdots\\p_n(x_1,\cdots,x_n)=0\end{cases} \tag{20}$$

此时，方程组的个数和变量的个数相等，都为 n，但由 4.1.1 节知 $p_i(x_1,\cdots,x_n)$ 为多元四次多项式，求解方程组(20)的复杂度远大于求解多元二次方程组。在给定的参数 n=32 下，由情况 1)可得，求解多元二次方程组的复杂度为 $O(2^{96})$，可见求解新体制公钥多项式的复杂度在 $O(2^{96})$之上。

所以新扩展方案在特定参数下可以抵抗代数攻击。

目前，针对多变量体制的攻击主要包括线性攻击、差分攻击和代数攻击。由定理 1~定理 3 可知，新的扩展方案能同时抵抗线性化攻击、差分攻击和代数攻击，所以新扩展方案是安全的。

5 结束语

针对 MI 方案不能抵抗线性攻击和差分攻击，本文基于温顺变换思想构造了一种的独特的非线性可逆变换，并将此非线性变换与 MI 方案结合，提出一种新的扩展多变量公钥密码方案。对应地，构造了新的扩展方案的加密方案和签名方案。新的扩展方案保持了 MI 方案计算高效的优点，具有较小的公私钥空间；同时能抵抗线性化攻击、差分攻击和代数攻击，在安全性上得到了提高。是否存在一个新的攻击方法有待进一步研究。

参考文献：

[1] SHOR P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Rev, 1999, 41(2): 303–332.

[2] 付向群, 鲍皖苏, 周淳. Shor 整数分解量子算法的加速实现[J]. 科学通报, 2010, 4: 322-327.
FU X Q, BAO W S, ZHOU C. Speeding up implementation for Shor's factorization quantum[J]. Chinese Sci Bull, 2010, 4: 322-327.

[3] MYASNIKOV A D, USHAKOV A. Quantum algorithm for the discrete logarithm problem for matrices over finite group rings[EB/OL]. https://eprint.iacr.org/2012/574.pdf, 2012.

[4] BERNSTEIN D J, BUCHMANN J, DAHMEN E. Post-Quantum Cryptography[M]. Berlin: Springer-Verlag, 2009.

[5] DING J T, YANG B Y. Multivariate Public Key Cryptography[M]. Berlin: Springer-Verlag, 2009.

[6] TANG S, XU L. Proxy signature scheme based on isomorphisms of polynomials[A]. NSS 2012[C]. Fujian, China, 2012. 113-125.

[7] MATSUMOTO T, IMAI H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption[A]. Advances in Cryptology—EUROCRYPT'88[C]. Switzerland, 1988. 419-453.

[8] PATARIN J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88[A]. Advances in Cryptology—CRYPT0'95[C]. Santa Barbara, California, USA, 1995. 248-261.

[9] PATARIN J, COURTOIS N, GOUBIN L. Flash, a fast multivariate signature algorithm[A]. Topics in Cryptology—CT-RSA 2001[C]. San Francisco, CA, USA, 2001. 298-307.

[10] DING J. A new variant of the Matsumoto-Imai cryptosystem through perturbation[A]. Public Key Cryptography–PKC 2004[C]. Singapore, 2004. 305-318.

[11] DUBOIS V, FOUQUE P A, STERN J. Cryptanalysis of SFLASH with slightly modified parameters[A]. Advances in Cryptology-EUROCRYPT 2007[C]. Barcelona, Spain, 2007. 264-275.

[12] DING J, GOWER J E. Inoculating multivariate schemes against differential attacks[A]. Public Key Cryptography-PKC 2006[C]. New York, USA, 2006. 290-301.

[13] PETZOLDT A, BULYGIN S, BUCHMANN J. CyclicRainbow–a multivariate signature scheme with a partially cyclic public key[A]. Progress in Cryptology-INDOCRYPT 2010[C]. Hyderabad, India, 2010. 33-48.

[14] CLOUGH C L, DING J. Secure variants of the square encryption scheme[A]. Post-Quantum Cryptography[C]. Darmstadt, Germany, 2010. 153-164.

[15] TSUJII S, GOTAISHI M, TADAKI K, *et al*. Proposal of a signature scheme based on STS trapdoor[A]. Post-quantum cryptography[C]. Darmstadt, Germany, 2010. 201-217.

[16] THOMAE E, WOLF C. Roots of square: cryptanalysis of double-layer square and square+[A]. Post-Quantum Cryptography[C]. Taipei, China, 2011. 83-97.

[17] THOMAE E, WOLF C. Cryptanalysis of enhanced TTS, STS and all its variants, or: why cross-terms are important[A]. Progress in Cryptology-AFRICACRYPT 2012[C]. Ifrance, Morocco, 2012. 188-202.

[18] WANG H Z, ZHANG H G. Extended multivariate public key cryptosystems with secure encryption function[J]. Science China Information Sciences, 2011, 54(6): 1161- 1171.

[19] 王后珍, 张焕国, 管海明等. 多变量代数理论及其在密码学中的应用[J]. 北京工业大学学报, 2010 , 5: 627-634.
WANG H Z, ZHANG H G, GUAN H M, *et al*. Multivariate algebra theory and its application in cryptography[J]. Journal of Beijing University of Technology, 2010, 5: 627-634.

[20] ALBRECHT M R, CID C, FAUGÈRE J C, *et al*. On the relation between the MXL family of algorithms and Gröbner basis algorithms[J]. Journal of Symbolic Computation, 2012, 47(8): 926-941.

[21] THOMAE E, WOLF C. Solving underdetermined systems of multivariate quadratic equations revisited[A]. PKC 2012[C]. Darmstadt, Germany, 2012. 156-171.

作者简介：

乔帅庭（1987-），男，河南洛阳人，信息工程大学硕士生，主要研究方向为多变量公钥密码。

李益发（1964-），男，安徽芜湖人，博士，信息工程大学副教授、硕士生导师，主要研究方向为信息安全。

韩文报（1963-），男，河北广平人，博士，信息工程大学教授、博士生导师，主要研究方向为信息安全。