线性化方程方法破解TTM公钥加密体制

刘梦娟[1]，聂旭云[1,2]，胡 磊[2]，吴 劲[1]

(1. 电子科技大学计算机科学与工程学院 成都 610054; 2. 中国科学院研究生院信息安全国家重点实验室 北京 石景山区 100049)

【摘要】TTM是一类三角形多变量公钥密码体制。该文经过分析2004年的TTM实例发现，该实例中存在大量的一阶线性化方程，而且对于给定的公钥，这些线性化方程都可以通过预计算得到。对于给定的合法密文，可以利用一阶线性化方程攻击方法在2^{19}个2^8 域上的运算内找到了其相应的明文。该方法与二阶线性化方程攻击方法相比，恢复明文的复杂度降低了2^{12}倍。计算机实验证实了上述结果。

关 键 词 代数攻击; 线性化方程; 公钥密码学; 三角形体制; TTM

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.02.030

Linearization Equation Attack on TTM Public Key Cryptosystems

LIU Meng-juan[1], NIE Xu-yun[1,2], HU Lei[2], and WU Jing[1]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054;

2. State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences Shijingshan Beijing 100049)

Abstract TTM is a type of Multivariate public key cryptosystem. By analyzing the instance of TTM proposed in 2004, it can be found that there are many first order linearization equations satisfied by the cipher in this scheme. For a given public key, all first order linearization equations can be found through precomputation. For any given ciphertext, the corresponding plaintext can be found in less than 2^{19} operations over a finite field of size 2^8 by linearization equation attack. This attack reduced complexity of recovering plaintext from 2^{31} to 2^{19} compare to second order linearization equation attack. The results above are further confirmed by computer experiments.

Key words algebraic attack; linearization equation; public key cryptography; triangular cryptosystem; TTM

近年来，量子计算机的发展对传统公钥密码体制如RSA和ElGamal等基于数论困难问题造成了极大的威胁[1]。因此，有必要寻找更高效、安全的公钥密码系统来替代传统的公钥密码系统。

对寻找可替代的公钥密码系统已有一些研究，多变量公钥密码系统(MPKC)是其中一种。MPKC的密码函数一般由3个映射复合而成，$\overline{F} = L_1 \circ F \circ L_2$。其中，$L_1$、$L_2$为可逆仿射变换；$F$ 为一个二次映射，称为该体制的中心映射。MPKC的公钥为映射 $\overline{F}$ 的表达式，其形式一般为一组多变量二次多项式，私钥为映射 L_1、L_2、F 的表达式。多变量公钥密码体制的安全性基于解有限域上随机生成的多变量二次方程组是NP-困难问题。

三角形多变量公钥密码体制是效率最高的多变量公钥密码体制。现有的三角形加密体制有TTM[2]、MFE[3]和TRMC[4]等，但是它们都是不安全的。

文献[2]提出的TTM(tame transformation method)是一类三角形多变量公钥密码体制。TTM的设计思想来源于代数几何，其中心映射是驯顺变换。驯顺变换是代数几何中的一个核心概念，与Jacobian猜想紧密相关。

TTM加密体制自提出以来经历了几轮的攻击和防御。文献[5]利用最小秩方法完全破解了当时TTM的所有可能实例，并且以破解TTM发明者提出的挑战之一来进行证实。然而，文献[6]反驳了文献[5]的观点，并提出一个新的实例。但是这一新的体制和当时所有的实例都具有一个共同的弱点。文献[7]指出文献[6]中的实例的密文分量满足线性化方程，并且使用一种推广的线性化方程方法破解文献[6]中的实例[7]。为了抵挡这些攻击，文献[8]提出了一个新的实例[8]，可抵挡Goubin-Courtois攻击和Ding-Schmidt攻击。

然而，文献[9]指出文献[8]中的实例仍然存在缺

收稿日期：2008 – 06 – 16; 修回日期：2009 – 09 – 27

基金项目：国家自然科学基金(60803133、60973161)；高等学校博士学科点专项科研基金(200806140010)；信息安全国家重点实验室开放课题

作者简介：刘梦娟(1979 –)，女，博士，主要从事信息安全、密码学等方面的研究.

陷，即它的密文满足二阶线形化方程。对于给定公钥，从找到所有的这类方程张成的线性空间的一组基出发，结合给定的合法密文，可逐步解开锁多项式，最终找到合法密文相应的明文。在执行复杂度为 2^{39} 的预计算后，实际恢复密文的复杂度仅为 2^{31}。该攻击是惟密文攻击。

对文献[8]中的实例的中心映射作进一步的分析，可发现该实例的密文分量也满足一阶线性化方程。因此，可利用一阶线性化方程方法分析该实例。文献[10]提出线性化方程攻击方法，并利用该方法破解了多变量公钥加密体制——MI加密体制[11]。经过理论分析可得，对于给定的公钥，通过复杂度为 2^{38} 的运算可以找到所有的一阶线性化方程，其计算仅依赖于公钥，因此可以预计算。对于任意一个合法密文，恢复其相应明文的复杂度仅为 2^{19}，大大提高了攻击效率。文献[8]中的实例设计比以前的实例并没有多大的改善。同样，该攻击也是惟密文攻击。

目前，国内对TTM体制也有一些的研究。文献[12]利用内部扰动方法对TTM体制进行了改进，增强了改体制的安全性，可抵挡线性化方程攻击；但改进后的体制在解密速度上比原体制慢了 q^r 倍，q 为有限域的元素个数，r 未扰动维数。

本文介绍了线性化攻击方法及TTM加密体制的思想和实例，给出了以往攻击的回顾，对线性化方程攻击进行理论分析，并给出实际步骤和实验数据。

1 一阶线性化方程

一阶线性化方程为：

$$\sum a_{ij}x_i y_j + \sum b_i x_i + \sum c_j y_j + d = 0$$

式中 x_i 为明文分量；y_j 为密文分量，y_j 也可用其关于 x_i 的表达式来替代。如果给定合法密文，该方程就可转变为明文分量的线性方程。

对于分析一个多变量公钥加密体制，希望能仅利用公钥计算出合法密文相应的明文，即求解如下形式的方程组：

$$\begin{cases} y_1' = F_1(x_1, x_2, \cdots, x_n) \\ \quad\vdots \\ y_m' = F_m(x_1, x_2, \cdots, x_n) \end{cases} \tag{2}$$

式中 $y_1', y_2', \cdots, y_m'$ 为给定的合法密文；$F_1, F_2, \cdots, F_m$ 为公钥多项式；$x_1, x_2, \cdots, x_n$ 为明文变量。

解有限域上多变量非线性方程组是一个NP-困难问题。但是，如果方程数固定，那么未知数个数越少，解方程组的复杂度就越小。所以，应对该方程组进行消元。如果能得到一组线性独立的线性化方程，就可得到一个以明文分量为未知数的线性方程组。解该方程组即可将部分明文分量用其余分量线性表达。将这些线性表达式代入方程组(2)，就可消去一些未知数。对于消元后的方程组，如果解方程的复杂度太大，那么继续对消元后的方程组进行分析，判断是否满足一元线性化方程或其他类型的线性化方程。若可进一步消元，重复该过程直到不能再消元为止。

线性化方程攻击方法最早是由Paratin引入用于破解MI加密体制。目前，设计新的多变量公钥密码体制必须将线性化方程攻击方法考虑在内。利用线性化方程还可破解改进的MFE公钥加密体制[13]。

2 TTM加密体制

2.1 TTM加密体制的一般思想

令 $\boldsymbol{K}$ 是一个小的有限域，TTM加密函数 $F: \boldsymbol{K}^n \to \boldsymbol{K}^m$ 由 $\boldsymbol{K}$ 上的4个映射复合而成，即 $F = \phi_4 \circ \cdots \circ \phi_1$。TTM系统的公钥是 $F(x_0, x_1, \cdots, x_{n-1})$ 的表达式，私钥是所有的 ϕ_i 的表达式。$F: \boldsymbol{K}^n \to \boldsymbol{K}^m$ 是一组二次多项式。在所有的TTM设计实例中，ϕ_i 都是下列两种映射之一：

(1) 形如 $\boldsymbol{f}(X) = \boldsymbol{A}\boldsymbol{X} + \boldsymbol{b}$ 的可逆仿射变换，其中，$\boldsymbol{X}$ 和 $\boldsymbol{b}$ 为 $\boldsymbol{K}^*$ 中的向量；$\boldsymbol{A}$ 为 $\boldsymbol{K}$ 上的可逆矩阵。

(2) 驯顺变换，它们的形式如下：

$$(y_0, y_1, \cdots, y_m) = J(x_0, x_1, \cdots, x_{n-1}) = (x_0, x_1 + q_1(x_0), \cdots, x_{n-1} + q_{n-1}(x_0, x_1, \cdots, x_{n-2}), q_n(x_0, x_1, \cdots, x_{n-1}), \cdots, q_{m-1}(x_0, x_1, \cdots, x_{n-1}))$$

驯顺变换的概念来自于代数几何，其逆变化也是驯顺变换，而且非常容易求出。

TTM体制构造的关键是构造锁多项式隐藏体制的三角形结构。在新的实例中构造了一组锁多项式 $G_j(x_0, x_1, \cdots, x_{n-1})$，$j = 0,1,\cdots,6$，使得该体制的中心映射变为：

$$(y_0, y_1, \cdots, y_m) = J(x_0, x_1, \cdots, x_{n-1}) = (x_0 + G_0, x_1 + q_1(x_0) + G_1, \cdots, x_6 + q_6(x_0, x_1, \cdots, x_5) + G_6, x_7 + q_7(x_0, x_1, \cdots, x_6), \cdots, x_{n-1} + q_{n-1}(x_0, x_1, \cdots, x_{n-2}), q_n(x_0, x_1, \cdots, x_{n-1}), \cdots, q_{m-1}(x_0, x_1, \cdots, x_{n-1}))$$

这一组锁多项式作为 y_j 的多项式是高次(≥ 2)，而作为 x_i 的多项式仅为2次。在解密过程中，需要使用锁多项式作为 y_j 的多项式来求值。

2.2 TTM加密体制描述

本文沿用文献[8]中的记号，取 $\boldsymbol{K}$ 为 F_{2^8}，$m=110$，$n=55$。映射 $F:\boldsymbol{K}^{55}\to\boldsymbol{K}^{110}$ 是4个映射 $\phi_1,\phi_2,\phi_3,\phi_4$ 的复合，即：

$$\overline{Y}=(\overline{y}_0,\overline{y}_1,\cdots,\overline{y}_{109})=F(\overline{X})=F(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{54})=\phi_4\circ\phi_3\circ\phi_2\circ\phi_1(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{54})$$

式中 $\overline{Y}$ 为密文；$\overline{X}$ 为明文；公钥为 $F(\overline{x}_0,\overline{x}_1,\cdots,\overline{x}_{54})$ 的表达式的每一个分量 $y_i=F_i(x_0,x_1,\cdots,x_{54})$ 都是二次多项式。$\phi_1,\phi_2,\phi_3,\phi_4$ 为其私钥，其中，ϕ_1,ϕ_4 为可逆仿射变换；ϕ_2 为二次驯顺变换；ϕ_3 为使用了锁多项式的8次映射；$\phi_3\circ\phi_2$ 称为TTM体制的中心映射。中心映射 $\phi_3\circ\phi_2$ 如下[8]：

$$\begin{aligned}
y_0&=x_0+G_0\\
y_i&=f_i+x_i+G_i\quad 1\leqslant i\leqslant 6\\
y_i&=f_i+x_i\quad 7\leqslant i\leqslant 21\\
&\vdots\\
y_{27}&=x_2x_9+x_{22}x_3+x_{27}\\
y_{28}&=x_6x_9+x_{22}x_7+x_{28}\\
y_{29}&=x_{10}x_7+x_8x_6+x_{29}\\
y_{30}&=x_{10}x_3+x_2x_8+x_{30}\\
y_{31}&=x_{11}x_{16}+x_{12}x_{15}+x_{19}+x_{31}\\
&\vdots\\
y_{95}&=x_3x_6+x_2x_7\\
y_{96}&=x_{10}x_{25}+x_{24}x_{22}+x_6\\
y_{97}&=x_0x_2+x_4x_6+x_{29}x_{22}+x_{28}x_{10}\\
y_{98}&=x_1x_3+x_5x_7+x_{30}x_9+x_{27}x_8\\
y_{99}&=x_1x_2+x_5x_6+x_{30}x_{22}+x_{27}x_{10}\\
y_{100}&=x_0x_3+x_4x_7+x_{29}x_9+x_{28}x_8\\
y_{101}&=x_0x_{30}+x_{29}x_1+x_6\\
y_{102}&=x_4x_{30}+x_{29}x_5+x_2\\
y_{103}&=x_{28}x_5+x_4x_{27}+x_3\\
y_{104}&=x_{28}x_{30}+x_{29}x_{27}\\
y_{105}&=x_{28}x_1+x_0x_{27}+x_7\\
y_{106}&=f_{106}\\
y_{107}&=f_{107}\\
y_{108}&=f_{108}\\
y_{109}&=f_{109}
\end{aligned}$$

式中 f_i 为随机选择的、以 $x_0,x_1,\cdots,x_{i-1}$ 为变量的二次多项式；G_i 为锁多项式，它们作为 y_j 的多项式是8次的，而作为 x_i 的多项式是2次的，分别用于解密过程和加密过程。解密时，计算 ϕ_3 的逆时需要求出锁多项式关于 y_j 的8次多项式的值。

本文给出的攻击方法与锁多项式的构造无关，因此不列出具体的锁多项式的表达式，详细的锁多项式表达式可参阅文献[8-9]。

3 以前的攻击

文献[9]利用二阶线性化方程攻击方法破解文献[8]中的实例，将TTM这个实例在锁多项式的构造中引入了二阶线性化方程。在利用公钥找到所有的二阶线性化方程后，对于给定的合法密文，可以找到明文空间的一个子空间。在该子空间上，所有的锁多项式都变为常数。因此，再利用顺序解密的方法，该攻击可以找到合法密文相应的明文。计算复杂度为：找到所有的二阶线性化方程的复杂度为 2^{39} 的预计算；恢复给定合法密文相应的明文复杂度仅为 2^{31}。该攻击是惟密文攻击。在奔IV、3 GHz、256 MB内存的PC机上可完全实现该攻击，其中预计算时间约为95 min，恢复明文的时间约为80 s。

4 线性化方程攻击

本文对TTM的中心映射进行了理论分析，发现该实例存在大量的一阶线性化方程。具体分析如下：根据中心映射的表达式，对不含随机选取的多项式的分量进行分析，即对 $y_{22},\cdots,y_{105}$ 的表达式进行分析。将 $y_{27},\cdots,y_{30}$ 和 $y_{94},\cdots,y_{100}$ 结合作如下计算：

$$\begin{aligned}
&x_{22}y_{29}+x_{10}y_{28}=\\
&x_7x_{10}x_{22}+x_6x_8x_{22}+x_{22}x_{29}+\\
&x_6x_9x_{10}+x_7x_{10}x_{22}+x_{10}x_{28}=\\
&x_6(x_8x_{22}+x_9x_{10})+x_{22}x_{29}+x_{10}x_{28}=\\
&x_6(y_{94}+x_1+x_4)+x_{22}x_{29}+x_{10}x_{28}=\\
&x_6y_{94}+x_6x_1+x_6x_4+x_{22}x_{29}+x_{10}x_{28}=\\
&x_6y_{94}+y_{97}+x_6x_1+x_2x_0
\end{aligned}$$

即有：

$$x_{22}y_{29}+x_{10}y_{28}+x_6y_{94}+y_{97}=x_6x_1+x_2x_0$$

类似地可以得到：

$$\begin{aligned}
x_{22}y_{30}+x_{10}y_{27}+x_2y_{94}+y_{99}&=x_6x_5+x_2x_4\\
x_9y_{29}+x_8y_{28}+x_7y_{94}+y_{100}&=x_7x_1+x_3x_0\\
x_9y_{30}+x_8y_{27}+x_3y_{94}+y_{98}&=x_7x_5+x_3x_4
\end{aligned}$$

采用以下的记号：

$$\begin{cases}
w_1:=x_{22}y_{29}+x_{10}y_{28}+x_6y_{94}+y_{97}\\
w_2:=x_{22}y_{30}+x_{10}y_{27}+x_2y_{94}+y_{99}\\
w_3:=x_9y_{29}+x_8y_{28}+x_7y_{94}+y_{100}\\
w_4:=x_9y_{30}+x_8y_{27}+x_3y_{94}+y_{98}
\end{cases}\tag{3}$$

则有：

$$w_1 = x_6x_1 + x_2x_0$$
$$w_2 = x_6x_5 + x_2x_4$$
$$w_1 = x_7x_1 + x_3x_0$$
$$w_1 = x_7x_5 + x_3x_4$$

用一个矩阵方程来表示上述4个方程，即有：

$$\begin{pmatrix} w_1 & w_2 \\ w_3 & w_4 \end{pmatrix} = \begin{pmatrix} x_6 & x_2 \\ x_7 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_5 \\ x_0 & x_4 \end{pmatrix} \tag{5}$$

用 $\boldsymbol{A}^*$ 表示矩阵 $\boldsymbol{A}$ 的伴随矩阵，而且在特征2的有限域上，矩阵 $\boldsymbol{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 的伴随矩阵 $\boldsymbol{A}^* = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$。因此，可将式(4)化为：

$$\begin{pmatrix} x_6 & x_2 \\ x_7 & x_3 \end{pmatrix}^* \begin{pmatrix} w_1 & w_2 \\ w_3 & w_4 \end{pmatrix} = \begin{pmatrix} x_6 & x_2 \\ x_7 & x_3 \end{pmatrix}^* \begin{pmatrix} x_6 & x_2 \\ x_7 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_5 \\ x_0 & x_4 \end{pmatrix}$$

即有：

$$\begin{pmatrix} x_6 & x_2 \\ x_7 & x_3 \end{pmatrix}^* \begin{pmatrix} w_1 & w_2 \\ w_3 & w_4 \end{pmatrix} = (x_6x_3 + x_2x_7) \begin{pmatrix} x_1 & x_5 \\ x_0 & x_4 \end{pmatrix} \tag{6}$$

由中心映射的表达式可知，$y_{95} = x_6x_3 + x_2x_7$。将式(3)代入式(6)，并展开可得:

$$\begin{cases} y_{27}y_{29} + y_{28}y_{30} + y_{94}y_{95} + x_1y_{95} + x_{27}y_{29} \\ +x_{30}y_{28} + x_3y_{97} + x_2y_{100} = 0 \\ x_{27}y_{30} + x_{30}y_{27} + x_3y_{99} + x_2y_{98} + x_5y_{95} = 0 \\ x_{28}y_{29} + x_{29}y_{28} + x_6y_{100} + x_0y_{95} + x_7y_{97} = 0 \\ y_{27}y_{29} + y_{28}y_{30} + y_{94}y_{95} + x_4y_{95} + x_{28}y_{30} \\ +x_{29}y_{27} + x_7y_{99} + x_6y_{98} = 0 \end{cases}$$

式中　第2个和第3个方程正是一阶线性化方程；第1个和第4个方程是二阶线性化方程，而且这两个二阶线性化方程的和恰巧是一个一阶线性化方程。从表达式可看出，这些线性化方程是线性无关的。

由于 F 是由 $\phi_3 \circ \phi_2$ 内外复合可逆仿射变换所得，所有这些一阶线性化方程都可确定一个以下形式的一阶线性化方程：

$$\sum_{i=0,\,j=0}^{54\;109} a_{ij}\overline{x}_i F_j + \sum_{i=0}^{54} b_i\overline{x}_i + \sum_{j=0}^{109} c_j F_j + d = 0 \tag{7}$$

任意的 $(\overline{x}_0, \overline{x}_1, \cdots, \overline{x}_{54}) \in \boldsymbol{K}^{55}$ 都满足式(7)。

对于给定的公钥和由该公钥加密的任意合法密文，攻击由找到所有的一阶线性化方程出发。

要找到所有的一阶线性化方程，等价于找到所有的未知向量 $(a_{0,0}, \cdots, a_{54,109}, b_0, b_1, \cdots, b_{54}, c_0, c_1, \cdots, c_{109}, d)$ 张成的$\boldsymbol{K}$-线性空间的一组基。令D为该线性空间维数。

式(7)中的未知系数的个数为：55×110+55+110+1=6 216。因此本文选取比6 216略多，如6 500个明文 $(\overline{x}_0, \overline{x}_1, \cdots, \overline{x}_{54})$，将它们代入式(7)，可以得到以未知系数为未知数的线性方程组。解该方程组，就可得到D个线性无关的向量，记为$\{(a_{ij}^{(k)}, b_i^{(k)}, c_j^{(k)}, d^{(k)}), 1 \leqslant k \leqslant D\}$，也就是得到了$D$个线性无关的一阶线性化方程。记该组方程为：

$$\sum_{i=0,\,j=0}^{54\;109} a_{ij}^{(k)}\overline{x}_i F_j + \sum_{i=0}^{54} b_i^{(k)}\overline{x}_i + \sum_{j=0}^{109} c_j^{(k)} F_j + d^{(k)} = 0 \tag{8}$$

其计算复杂度为 $(6\ 216)^3 \leqslant 2^{38}$。计算机实验表明，该计算所需的时间为90 min，且 $D = 92$。

上述步骤仅依赖于任意给定的公钥，因此在公钥给定后，该步骤可以预计算。

给定一个合法密文 $\overline{y}' = (\overline{y}'_0, \overline{y}'_1, \cdots, \overline{y}'_{109})$，目标是找到其相应明文 $\overline{x}' = (\overline{x}'_0, \overline{x}'_1, \cdots, \overline{x}'_{54})$。将 $(F_0, F_1, \cdots, F_{109}) = (\overline{y}'_0, \overline{y}'_1, \cdots, \overline{y}'_{109})$ 代入方程组(8)，即可得到 $x_0, x_1, \cdots, x_{54}$ 的线性方程组。设该方程组的解空间的维数为 l。解该方程，可将 $(\overline{x}_0, \overline{x}_1, \cdots, \overline{x}_{54})$ 中的 l 用其余 $55-l$ 个变量线性表达出来。用 $(\overline{x}_{u_1}, \overline{x}_{u_2}, \cdots, \overline{x}_{55-l})$ 表示这 $55-l$ 个变量，然后将这 l 个线性表达式代入原公钥多项式，可得到新的仅有 $55-l$ 个变量的二次多项式，记为 $\overline{F}_j(x_{u_1}, x_{u_2}, \cdots, x_{u_{55-l}})$，$0 \leqslant j \leqslant 109$。实验结果表明，$l = 50$。因此可得到仅有5个变量的二次方程组，即：

$$\overline{F}_j(\overline{x}_{u_1}, \overline{x}_{u_2}, \cdots, \overline{x}_{u_{55-l}}) = \overline{y}'_j \qquad 0 \leqslant j \leqslant 109$$

可以很容易地利用线性化方法解上述方程组，得到剩余的5个变量的值。将所求出的值代入 l 个线性表达式，就可以得到合法密文 $\overline{y}' = (\overline{y}'_0, \overline{y}'_1, \cdots, \overline{y}'_{109})$ 相应的明文 $\overline{x}' = (\overline{x}'_0, \overline{x}'_1, \cdots, \overline{x}'_{54})$。上述步骤的计算复杂度仅为 2^{19}。实验表明，这些步骤所需时间不到1 s。

上述攻击方法预计算复杂度与文献[9]中提出的攻击方法相差不大，但是恢复明文的复杂度由 2^{31} 降到了 2^{19}，大大提高了攻击效率。计算机实验也表明，恢复给定密文的相应明文的时间也由80 s降到了1 s以内。

5 结　论

本文给出了2004年TTM的发明者提出的一个实例的又一攻击方法，即一阶线性化方程攻击方法。这一攻击比以前的攻击效率有了大幅的提高。而且文献[8]中的TTM的实例与以前的实例一样具有一个共同的缺陷，即它们的密文都满足一阶线性化方程。

线性化方程攻击是分析多变量公钥密码体制有效的方法。今后继续尝试将线性化方程攻击方法用于分析文献[13-14]中提出的多变量公钥密码体制。

参 考 文 献

[1] SHOR P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[2] MOH T T. A fast public key system with signature and master key functions[J]. Comm in Algebra, 1999, 27: 2207-2222.

[3] WANG Lih-chung, YANG Bo-yin, HU Yuh-hua, et al. A Medium-field multivariate public key encryption scheme[C]//CT-RSA 2006: Proceedings of the Cryptographers' Track at the RSA Conference 2006. Heidelberg: Springer, 2006, LNCS 3860: 132-149.

[4] WANG Lih-chung, CHANG Fei-hwang. Tractable rational map cryptosystem[DB/OL]. [2006-02-03]. http://eprint.iacr.org/2004/046.

[5] GOUBIN L, COURTOIS N T. Cryptanalysis of the TTM cryptosystem[C]//ASIACRYPT 2000: Proceedings of 6th International Conference on the Theory and Application of Cryptology and Information Security 2000. Heidelberg: Springer, 2000, LNCS 1976: 44-57.

[6] CHEN Jiun-ming, MOH T T. On the goubin-courtois attack on TTM[DB/OL]. [2001-07-21]. http://eprint.iacr.org/2001/072.

[7] DING Jin-tai, SCHMIDT D. The new TTM implementation is not secure[J]. Progress in Computer Science and Applied Logic, 2003, 23: 113-128.

[8] MOH T T, CHEN Jiun-ming, YANG Bo-yin. Building instances of TTM immune to the goubin-courtois attack and the ding-schmidt[DB/OL]. [2004-07-21]. http://eprint.iacr.org/2004/168.

[9] NIE Xu-yun, HU Lei, LI Jian-yu, et al. Breaking a new instance of ttm cryptosystem[C]//ACNS 2006: Proceedings of Third International Conference Applied Cryptography and Network Security. Heidelberg: Springer, 2006, LNCS 3989: 210-225.

[10] PATARIN J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88[C]//Crypto'95: Proceedings of 15th Annual International Cryptology Conference. Heidelberg: Springer, 1995, LNCS 963: 248-261.

[11] MATSUMOTO T, IMAI H. Public quadratic polynomial-tuples for efficient signature verification and message encryption[C]// EUROCRYPT'88: Proceedings of International Conference on the Theory and Application of Cryptographic Techniques 1988. Heidelberg: Springer, LNCS 330: 419-453.

[12] 巫治平, 叶顶锋, 马卫局. TTM密码系统的扰动变形[J]. 计算机研究与发展, 2006, 43(12): 2082-2087.
WU Zhi-ping, YE Ding-feng, MA Wei-ju. Perturbed variant of TTM cryptosystem[J]. Journal of Computer Research and Development, 2006, 43(12): 2082-2087.

[13] 王志伟, 郑世惠, 杨义先, 等. 改进的Medium-Field多变量公钥加密方案[J]. 电子科技大学学报, 2007, 36(6): 1152-1154.
WANG Zhi-wei, ZHENG Shi-hui, YANG Yi-xian, et al. Improved medium-field multivariate public key encryption scheme[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(6): 1152-1154.

[14] 王志伟，郑世惠，杨义先，等. 概率多变量签名方案的新构造[J]. 北京邮电大学学报, 2008, 31(6): 26-29.
WANG Zhi-wei, ZHENG Shi-hui, YANG Yi-xian, et al. A new construction of probabilistic multivariate signature scheme[J]. Journal of Beijing University of Posts and Telecommunication, 2008, 31(6): 26-29.

编 辑 黄 莘