TAIWANESE JOURNAL OF MATHEMATICS
Vol. 7, No. 4, pp. 615-629, December 2003
This paper is available online at http://www.math.nthu.edu.tw/tjm/

SQUARE-FREE Q_k COMPONENTS IN TTM

Lih-Chung Wang and Fei-Hwang Chang

Abstract. With tame transformation method (TTM), T. Moh invented a cryptosystem. The success of the system relies on the construction of the Q_k component. Some constructions of Q_k components are known but most of the Q_k components have square terms. There are some possible risks for square terms. In this paper, we give a systematic construction of square-free Q_k components to avoid the possible attacks.

1. Introduction

In 1997, T. Moh invented a cryptosystem using tame transformation method (TTM) [5]. This cryptosystem is much faster than other public key systems. The speed of the system even can match the speed of secret-key systems (DES etc.). However, the success of the system relies on the construction of the Q_k component. Some construction of Q_k components are known but most of the Q_k components have square terms. There are some potential risks for square terms. One potential risk is that many terms might vanish after differentiation. Thus the information of the tame automorphisms might release. Another possible risk is that a perfect-square Q_k component is 'linear' for the computational purpose. Such Q_k component might reduce the complexity of the whole system. The existence of Q_8 components with non-square terms was first shown in Moh's paper [6]. Chou, Guan and Chen found examples for square-free Q_8 components. (See [1], [3]) In this paper, we give a systematic construction of square-free Q_k components.

Let $\mathbb{K}$ be a field. An automorphism $\phi_i : \mathbb{K}^n \to \mathbb{K}^n$ is a tame automorphism if ϕ_i is an invertible affine transformation or, after a permutation of indices if necessary,

Received May 3, 2002; revised August 21, 2002.
Communicated by J. Yu.
2000 *Mathematics Subject Classification*: Primary 11T71, 14G50 and 94A60.
Key words and phrases: Tame transformation, TTM, cryptosystem, Q_k component, minimal generating polynomial.

of the following form

$$\phi_i \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \phi_{i,1} \\ \phi_{i,2} \\ \vdots \\ \phi_{i,j} \\ \vdots \\ \phi_{i,n} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 + f_2(x_1) \\ \vdots \\ x_j + f_j(x_1, x_2, \cdots, x_{j-1}) \\ \vdots \\ x_n + f_n(x_1, x_2, \cdots, x_{n-1}) \end{pmatrix}$$

where f_j is a polynomial of $(j-1)$ variables.

From now on, let $\mathbb{K}$ be a finite field of 2^8 elements, $\rho : \mathbb{K}^m \to \mathbb{K}^n$ $(m < n)$ be the embedding of the following form

$$\rho \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

and $\tau : \mathbb{K}^n \to \mathbb{K}^m$ be the projection such that $\tau \circ \rho = \mathrm{id}_{\mathbb{K}^m}$. Let $\pi = \phi_4 \circ \phi_3 \circ \phi_2 \circ \rho \circ \phi_1 : \mathbb{K}^m \to \mathbb{K}^n$, where ϕ_i's are tame automorphisms. We assume that ϕ_2 and ϕ_3 are non-affine, ϕ_1 and ϕ_4 are affine. The polynomial map of π and the finite field $\mathbb{K}$ will be announced as the public key. Let $(x_1, x_2, \cdots, x_m)$ be a plaintext. Then $\pi(x_1, x_2, \cdots, x_m)$ is the ciphertext. The legitimate receiver recover the plaintext by $\phi_1^{-1} \circ \tau \circ \phi_2^{-1} \circ \phi_3^{-1} \circ \phi_4^{-1}$. The private key is the set of ϕ_i's.

To implement the above TTM principle efficiently, Moh needs the following conditions.

- π send the zero vector of $\mathbb{K}^m$ to the zero vector of $\mathbb{K}^n$.
- The component $\phi_{2,j}$ of

$$\phi_2 \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 + f_2(x_1) \\ \vdots \\ x_j + f_j(x_1, x_2, \cdots, x_{j-1}) \\ \vdots \\ x_n + f_n(x_1, x_2, \cdots, x_{n-1}) \end{pmatrix}$$

  is of degree at most 2. (Note that this condition is not really necessary. See Examples of Implementation.)

- ϕ_3 is of the form

$$\phi_3 \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ x_{j+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 + f_1(x_2, x_3, \cdots, x_n) \\ \vdots \\ x_j + f_j(x_3, x_4, \cdots, x_n) \\ x_{j+1} \\ \vdots \\ x_n \end{pmatrix}$$

  such that the degrees of f_i's are big enough.

- The highest homogeneous parts of components of $\phi_3 \circ \phi_2 \circ \rho$ are linearly independent and of degree 2.

For security reason, Moh requires the following condition.

Choose ϕ_2 and j polynomials $l_1(x_1, x_2, \cdots, x_m), \ldots, l_j(x_1, x_2, \cdots, x_m)$ of degree 2 such that $f_1, \ldots, f_j$ in ϕ_3 are minimal generating polynomials of $l_1, \ldots, l_j$ with respect to $\phi_2 \circ \rho$. (For definition of minimal generating, see below.) If an f_i in ϕ_3 is of degree k and satisfy the above security condition, we will call such f_i a Q_k *component*. Our main result is a systematic construction of Q_k components such that $\phi_2 \circ \rho$, ϕ_3 and $\phi_3 \circ \phi_2 \circ \rho$ are square-free.

2. Construction of Square-Free Q_k Components

Let $\varphi : \mathbb{K}^m \to \mathbb{K}^n$ is a polynomial map. This map

$$\varphi \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} y_1(x_1, x_2, \cdots, x_m) \\ y_2(x_1, x_2, \cdots, x_m) \\ \vdots \\ y_n(x_1, x_2, \cdots, x_m) \end{pmatrix}$$

induces a ring homomorphism

$$\begin{array}{rccl} \varphi^\sharp : & \mathbb{K}[y_1, y_2, \cdots, y_n] & \longrightarrow & \mathbb{K}[x_1, x_2, \cdots, x_m] \\ & Q(y_1, y_2, \cdots, y_n) & \longmapsto & Q(y_1(x_1, x_2, \cdots, x_m), \cdots, y_n(x_1, x_2, \cdots, x_m)). \end{array}$$

Given a polynomial $l(x_1, x_2, \cdots, x_m) \in \mathbb{K}[x_1, x_2, \cdots, x_m]$, $Q\langle l \rangle$ is called a *generating polynomial* of l (over $y_1, y_2, \cdots, y_n$) if $\varphi^\sharp(Q) = l$. If Q is of the minimal degree among all possible generating polynomial of l, then it is called a *minimal generating polynomial* of l, and its degree is called the *generating degree* of l, in symbol $gen\deg(l)$. If l is not in the image of $\varphi^\sharp$, then we define $gen\deg(l) = \infty$.

Given $l(x_1, x_2, \cdots, x_m) \in \mathbb{K}[x_1, x_2, \cdots, x_m]$ and the generating degree $k > 1$, we want to choose appropriate

$$\begin{pmatrix} y_1(x_1) \\ y_2(x_1, x_2) \\ \vdots \\ y_m(x_1, x_2, \cdots, x_m) \\ \vdots \\ y_n(x_1, x_2, \cdots, x_m) \end{pmatrix} = \phi_2 \circ \rho \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}$$

such that we can construct a $Q_k\langle l\rangle$ which is a minimal generating polynomial of l over $y_1, y_2, \cdots, y_n$.

2.1. Basic Replacement Patterns

Let us start from that $k = 2$ and $l = x_\alpha x_\beta$. Let s_1, s_2, s_3, s_4, α and β be six different integers, consider the following eight polynomial expressions.

$$\begin{array}{ll} y_{65} = x_\alpha + x_{s_1} x_{s_3} & y_{69} = x_\alpha x_{s_3} \\ y_{66} = x_\beta + x_{s_2} x_{s_4} & y_{70} = x_\beta x_{s_4} \\ y_{67} = x_{s_1} + x_\alpha x_{s_4} & y_{71} = x_{s_1} x_{s_2} \\ y_{68} = x_{s_2} + x_\beta x_{s_3} & y_{72} = x_{s_3} x_{s_4}. \end{array}$$

It is easy to check that $Q_2\langle x_\alpha x_\beta\rangle = y_{65}y_{66} + y_{67}y_{68} + y_{69}y_{70} + y_{71} + y_{71}y_{72}$ is the minimal generating polynomial of l over $y_{65}, y_{66}, \cdots, y_{72}$. Then choose the other $y_i(x_1, x_2, \cdots)$ such that Q_2 is the minimal generating polynomial of l over $y_1, y_2, \cdots, y_{100}$. Note that y_{65} and y_{66} can be moved to y_α and y_β if s_i's are less than α and β.

For $k = 2$ and $l = x_\gamma$, the construction is similar. Let $y_{73} = x_\gamma + x_\alpha x_\beta$.

$$Q_2\langle x_\gamma\rangle = y_{73} + Q_2\langle x_\alpha x_\beta\rangle.$$

2.2. Construction of Q_k

To create a $Q_3\langle x_\alpha x_\beta\rangle$, consider the above first pattern

$$\begin{array}{ll} y_{65} = x_\alpha + x_{s_1} x_{s_3} & y_{69} = x_\alpha x_{s_3} \\ y_{66} = x_\beta + x_{s_2} x_{s_4} & y_{70} = x_\beta x_{s_4} \\ y_{67} = x_{s_1} + x_\alpha x_{s_4} & y_{71} = x_{s_1} x_{s_2} \\ y_{68} = x_{s_2} + x_\beta x_{s_3} & y_{72} = x_{s_3} x_{s_4}. \end{array}$$

Then replace y_{72} with a $Q_2\langle x_{s_3} x_{s_4}\rangle$. Hence

$$Q_3\langle x_\alpha x_\beta\rangle = y_{65}y_{66} + y_{67}y_{68} + y_{69}y_{70} + y_{71} + y_{71}Q_2\langle x_{s_3} x_{s_4}\rangle.$$

That is, consider

$$\begin{aligned}
y_{65} &= x_\alpha + x_{s_1}x_{s_3} & y_{69} &= x_\alpha x_{s_3}\\
y_{66} &= x_\beta + x_{s_2}x_{s_4} & y_{70} &= x_\beta x_{s_4}\\
y_{67} &= x_{s_1} + x_\alpha x_{s_4} & y_{71} &= x_{s_1}x_{s_2}\\
y_{68} &= x_{s_2} + x_\beta x_{s_3}
\end{aligned}$$

$$\begin{aligned}
y_{72} &= x_{s_3} + x_{t_1}x_{t_3} & y_{76} &= x_{s_3}x_{t_3}\\
y_{73} &= x_{s_4} + x_{t_2}x_{t_4} & y_{77} &= x_{s_4}x_{t_4}\\
y_{74} &= x_{t_1} + x_{s_3}x_{t_4} & y_{78} &= x_{t_1}x_{t_2}\\
y_{75} &= x_{t_2} + x_{s_4}x_{t_3} & y_{79} &= x_{t_3}x_{t_4}
\end{aligned}$$

where t_i's are another 4 different integers. Then

$$\begin{aligned}
Q_3\langle x_\alpha x_\beta\rangle &= y_{65}y_{66} + y_{67}y_{68} + y_{69}y_{70} + y_{71} + y_{71}Q_2\langle x_{s_3}x_{s_4}\rangle\\
&= y_{65}y_{66} + y_{67}y_{68} + y_{69}y_{70} + y_{71} + y_{71}(y_{72}y_{73} + y_{74}y_{75} + y_{76}y_{77} + y_{78} + y_{78}y_{79})
\end{aligned}$$

Similarly, we can construct

$$Q_3\langle x_\gamma\rangle = y_{80} + Q_3\langle x_\alpha x_\beta\rangle$$

where $y_{80} = x_\gamma + x_\alpha x_\beta$.

To create a $Q_4\langle x_\alpha x_\beta\rangle$, you can have two choices. One is by induction

$$Q_4\langle x_\alpha x_\beta\rangle = y_{65}y_{66} + y_{67}y_{68} + y_{69}y_{70} + y_{71}Q_3\langle x_{s_3}x_{s_4}\rangle.$$

The other is

$$Q_4\langle x_\alpha x_\beta\rangle = Q_2\langle x_\alpha\rangle Q_2\langle x_\beta\rangle.$$

By induction on k, you can get a bunch of choices to construct Q_k.

2.3. More Complicated Replacement Patterns

We should point out that there are more complicated replacement patterns. Here we give two patterns.

(1) For

$$\begin{aligned}
y_{65} &= x_\alpha + x_{s_5} + x_{s_2}x_{s_4}\\
y_{66} &= x_\beta + x_{s_1}x_{s_3}\\
y_{67} &= x_{s_1} + x_\beta x_{s_4}\\
y_{68} &= x_{s_2} + x_\alpha x_{s_3} + x_{s_3}x_{s_5}\\
y_{69} &= x_\alpha x_{s_4}\\
y_{70} &= x_\beta x_{s_3}\\
y_{71} &= x_\beta x_{s_5}\\
y_{72} &= x_{s_1}x_{s_2}\\
y_{73} &= x_{s_3}x_{s_4}
\end{aligned}$$

we have $Q_2\langle x_\alpha x_\beta\rangle = y_{71} + y_{72} + y_{65}y_{66} + y_{67}y_{68} + y_{69}y_{70} + y_{71}y_{73} + y_{72}y_{73}$.

(2) For

$$\begin{array}{ll}
y_{65} = x_\alpha + x_{s_1}x_{s_3} & y_{71} = x_{s_1}x_{s_5} \\
y_{66} = x_\beta + x_{s_2}x_{s_4} & y_{72} = x_\beta x_{s_7} \\
y_{67} = x_\beta x_{s_1} & y_{73} = x_{s_2}x_{s_6} \\
y_{68} = x_{s_3} + x_{s_5}x_{s_7} & y_{74} = x_\alpha x_{s_8} \\
y_{69} = x_\alpha x_{s_2} & y_{75} = x_{s_1}x_{s_2} \\
y_{70} = x_{s_4} + x_{s_6}x_{s_8} & y_{76} = x_{s_3}x_{s_4}
\end{array}$$

we have $Q_2\langle x_\alpha x_\beta\rangle = y_{65}y_{66} + y_{67}y_{68} + y_{69}y_{70} + y_{71}y_{72} + y_{73}y_{74} + y_{75}y_{76}$.

3. Demonstration of Q_8

Here we give three examples to demonstrate how different Q_8's are and how easy to create Q_8's systematically. For the convenience of readers, we let l to be a monomial of degree 2. Note that it is easy to make l complicated.

Example 1

$$\begin{array}{lll}
y_{27} = x_{27} + x_{11}x_{12} & y_{40} = x_{40} + x_{37}x_{38} & y_{53} = x_{19} + x_{22}x_{31} \\
y_{28} = x_{28} + x_{13}x_{14} & y_{41} = x_{11} + x_{14}x_{27} & y_{54} = x_{21} + x_{20}x_{32} \\
y_{29} = x_{29} + x_{15}x_{16} & y_{42} = x_{13} + x_{12}x_{28} & y_{55} = x_{19}x_{21} \\
y_{30} = x_{30} + x_{17}x_{18} & y_{43} = x_{11}x_{13} & y_{56} = x_{20}x_{22} \\
y_{31} = x_{31} + x_{19}x_{20} & y_{44} = x_{12}x_{14} & y_{57} = x_{20}x_{31} \\
y_{32} = x_{32} + x_{21}x_{22} & y_{45} = x_{12}x_{27} & y_{58} = x_{22}x_{32} \\
y_{33} = x_{33} + x_{23}x_{24} & y_{46} = x_{14}x_{28} & y_{59} = x_{23} + x_{26}x_{33} \\
y_{34} = x_{34} + x_{25}x_{26} & y_{47} = x_{15} + x_{18}x_{29} & y_{60} = x_{25} + x_{24}x_{34} \\
y_{35} = x_{35} + x_{27}x_{28} & y_{48} = x_{17} + x_{16}x_{30} & y_{61} = x_{23}x_{25} \\
y_{36} = x_{36} + x_{29}x_{30} & y_{49} = x_{15}x_{17} & y_{62} = x_{24}x_{26} \\
y_{37} = x_{37} + x_{31}x_{32} & y_{50} = x_{16}x_{18} & y_{63} = x_{24}x_{33} \\
y_{38} = x_{38} + x_{33}x_{34} & y_{51} = x_{16}x_{29} & y_{64} = x_{26}x_{34} \\
y_{39} = x_{39} + x_{35}x_{36} & y_{52} = x_{18}x_{30} &
\end{array}$$

With the above y_i's, we can construct the following two Q_8 components.

$$\begin{aligned}
Q_8\langle x_{39}x_{40}\rangle = {}&[y_{39} + (y_{35} + y_{43} + y_{27}y_{28} + y_{41}y_{42} + y_{43}y_{44} + y_{45}y_{46}) \\
&\qquad (y_{36} + y_{49} + y_{29}y_{30} + y_{47}y_{48} + y_{49}y_{50} + y_{51}y_{52})] \\
&[y_{40} + (y_{37} + y_{55} + y_{31}y_{32} + y_{53}y_{54} + y_{55}y_{56} + y_{57}y_{58}) \\
&\qquad (y_{38} + y_{61} + y_{33}y_{34} + y_{59}y_{60} + y_{61}y_{62} + y_{63}y_{64})].
\end{aligned}$$

Example 2

$$
\begin{array}{lll}
y_{41} = x_{41} + x_{40}x_1 & y_{61} = x_{61} + x_{58}x_{60} & y_{81} = x_{25}x_{51} \\
y_{42} = x_{42} + x_{37}x_{39} & y_{62} = x_{62} + x_{58}x_{59} & y_{82} = x_{29}x_{48} \\
y_{43} = x_{43} + x_{41} + x_{38}x_{40} & y_{63} = x_{63} + x_{56}x_{59} & y_{83} = x_{33}x_{45} \\
y_{44} = x_{44} + x_{20}x_{41} & y_{64} = x_{64} + x_{57}x_{60} & y_{84} = x_{37}x_{42} \\
y_{45} = x_{45} + x_{33}x_{35} & y_{65} = x_{24} + x_{21}x_{53} + x_{21}x_{55} & y_{85} = x_{53}x_{54} \\
y_{46} = x_{46} + x_{44} + x_{34}x_{36} & y_{66} = x_{28} + x_{25}x_{50} + x_{25}x_{52} & y_{86} = x_{50}x_{51} \\
y_{47} = x_{47} + x_{19}x_{41} & y_{67} = x_{32} + x_{29}x_{47} + x_{29}x_{49} & y_{87} = x_{47}x_{48} \\
y_{48} = x_{48} + x_{29}x_{31} & y_{68} = x_{36} + x_{33}x_{44} + x_{33}x_{46} & y_{88} = x_{44}x_{45} \\
y_{49} = x_{49} + x_{47} + x_{30}x_{32} & y_{69} = x_{40} + x_{37}x_{41} + x_{37}x_{43} & y_{89} = x_{41}x_{42} \\
y_{50} = x_{50} + x_{18}x_{41} & y_{70} = x_{23} + x_{22}x_{54} & y_{90} = x_{23}x_{24} \\
y_{51} = x_{51} + x_{25}x_{27} & y_{71} = x_{27} + x_{26}x_{51} & y_{91} = x_{27}x_{28} \\
y_{52} = x_{52} + x_{50} + x_{26}x_{28} & y_{72} = x_{31} + x_{30}x_{48} & y_{92} = x_{31}x_{32} \\
y_{53} = x_{53} + x_{17}x_{41} & y_{73} = x_{35} + x_{34}x_{45} & y_{93} = x_{35}x_{36} \\
y_{54} = x_{54} + x_{21}x_{23} & y_{74} = x_{39} + x_{38}x_{42} & y_{94} = x_{39}x_{40} \\
y_{55} = x_{55} + x_{53} + x_{22}x_{24} & y_{75} = x_{22}x_{55} & y_{95} = x_{21}x_{22} \\
y_{56} = x_{56} + x_{42}x_{43} & y_{76} = x_{26}x_{52} & y_{96} = x_{25}x_{26} \\
y_{57} = x_{57} + x_{45}x_{46} & y_{77} = x_{30}x_{49} & y_{97} = x_{29}x_{30} \\
y_{58} = x_{58} + x_{48}x_{49} & y_{78} = x_{34}x_{46} & y_{98} = x_{33}x_{34} \\
y_{59} = x_{59} + x_{51}x_{52} & y_{79} = x_{38}x_{43} & y_{99} = x_{37}x_{38} \\
y_{60} = x_{60} + x_{54}x_{55} & y_{80} = x_{21}x_{54} & y_{100} = x_{16}x_{41}
\end{array}
$$

With the above y_i's, we can construct the following two Q_8 components.

$$
\begin{aligned}
Q_8\langle x_{62}x_{64}\rangle = & [y_{64} + (y_{60} + y_{85} + y_{90} + y_{54}y_{55} + y_{65}y_{70} + y_{75}y_{80} + y_{85}y_{95} + y_{90}y_{95}) \\
& \quad (y_{57} + y_{88} + y_{93} + y_{45}y_{46} + y_{68}y_{73} + y_{78}y_{83} + y_{88}y_{98} + y_{93}y_{98})] \\
& [y_{62} + (y_{59} + y_{86} + y_{91} + y_{51}y_{52} + y_{66}y_{71} + y_{76}y_{81} + y_{86}y_{96} + y_{91}y_{96}) \\
& \quad (y_{58} + y_{87} + y_{92} + y_{48}y_{49} + y_{67}y_{72} + y_{77}y_{82} + y_{87}y_{97} + y_{92}y_{97})].
\end{aligned}
$$

$$
\begin{aligned}
Q_8\langle x_{61}x_{63}\rangle = & [y_{63} + (y_{59} + y_{86} + y_{91} + y_{51}y_{52} + y_{66}y_{71} + y_{76}y_{81} + y_{86}y_{96} + y_{91}y_{96}) \\
& \quad (y_{56} + y_{89} + y_{94} + y_{42}y_{43} + y_{69}y_{74} + y_{79}y_{84} + y_{89}y_{99} + y_{94}y_{99})] \\
& [y_{61} + (y_{60} + y_{85} + y_{90} + y_{54}y_{55} + y_{65}y_{70} + y_{75}y_{80} + y_{85}y_{95} + y_{90}y_{95}) \\
& \quad (y_{58} + y_{87} + y_{92} + y_{48}y_{49} + y_{67}y_{72} + y_{77}y_{82} + y_{87}y_{97} + y_{92}y_{97})].
\end{aligned}
$$

Example 3

$$
\begin{array}{lll}
y_{41} = x_{41} + x_{17}x_{18} & y_{61} = x_{55} + x_{39}x_{40} & y_{81} = x_{23}x_{44} \\
y_{42} = x_{42} + x_{19}x_{20} & y_{62} = x_{53} + x_{37}x_{38} & y_{82} = x_{19}x_{42} \\
y_{43} = x_{43} + x_{21}x_{22} & y_{63} = x_{54}x_{58} & y_{83} = x_{37}x_{53} \\
y_{44} = x_{44} + x_{23}x_{24} & y_{64} = x_{56}x_{57} & y_{84} = x_{33}x_{51} \\
y_{45} = x_{45} + x_{25}x_{26} & y_{65} = x_{40} + x_{37}x_{55} & y_{85} = x_{29}x_{49}
\end{array}
$$

$$\begin{array}{lll}
y_{46} = x_{46} + x_{27}x_{28} & y_{66} = x_{36} + x_{33}x_{52} & y_{86} = x_{25}x_{45} \\
y_{47} = x_{47} + x_{41}x_{42} & y_{67} = x_{32} + x_{29}x_{50} & y_{87} = x_{21}x_{43} \\
y_{48} = x_{48} + x_{43}x_{44} & y_{68} = x_{28} + x_{25}x_{46} & y_{88} = x_{17}x_{41} \\
y_{49} = x_{49} + x_{29}x_{30} & y_{69} = x_{24} + x_{21}x_{44} & y_{89} = x_{38}x_{40} \\
y_{50} = x_{50} + x_{31}x_{32} & y_{70} = x_{20} + x_{17}y_{42} & y_{90} = x_{34}x_{36} \\
y_{51} = x_{51} + x_{33}x_{34} & y_{71} = x_{38} + x_{39}x_{53} & y_{91} = x_{30}x_{32} \\
y_{52} = x_{52} + x_{35}x_{36} & y_{72} = x_{34} + x_{35}x_{51} & y_{92} = x_{26}x_{28} \\
y_{53} = x_{53} + x_{49}x_{50} & y_{73} = x_{30} + x_{31}x_{49} & y_{93} = x_{22}x_{24} \\
y_{54} = x_{54} + x_{45}x_{46} & y_{74} = x_{26} + x_{27}x_{45} & y_{94} = x_{18}x_{20} \\
y_{55} = x_{55} + x_{51}x_{52} & y_{75} = x_{22} + x_{23}x_{43} & y_{95} = x_{37}x_{39} \\
y_{56} = x_{56} + x_{47}x_{48} & y_{76} = x_{18} + x_{19}x_{41} & y_{96} = x_{33}x_{35} \\
y_{57} = x_{57} + x_{53}x_{54} & y_{77} = x_{39}x_{55} & y_{97} = x_{29}x_{31} \\
y_{58} = x_{58} + x_{55}x_{56} & y_{78} = x_{35}x_{52} & y_{98} = x_{25}x_{27} \\
y_{59} = x_{59} + x_{53}x_{55} & y_{79} = x_{31}x_{50} & y_{99} = x_{21}x_{23} \\
y_{60} = x_{60} + x_{54}x_{56} & y_{80} = x_{27}x_{46} & y_{100} = x_{17}x_{19}
\end{array}$$

With the above y_i's, we can construct the following two Q_8 components.

$$\begin{aligned}
Q_8\langle x_{58}x_{57}\rangle = &[y_{56} + (y_{48} + y_{93} + y_{43}y_{44} + y_{69}y_{75} + y_{81}y_{87} + y_{93}y_{99}) \\
&\quad (y_{47} + y_{94} + y_{41}y_{42} + y_{70}y_{76} + y_{82}y_{88} + y_{94}y_{100})] \\
&[(y_{54} + y_{92} + y_{45}y_{46} + y_{68}y_{74} + y_{80}y_{86} + y_{92}y_{98}) \\
&\quad (y_{89} + y_{61}y_{62} + y_{65}y_{71} + y_{77}y_{83} + y_{89}y_{95})] \\
&\quad + y_{64}(y_{55} + y_{90} + y_{51}y_{52} + y_{66}y_{72} + y_{78}y_{84} + y_{90}y_{96}) \\
&\quad + y_{63}(y_{53} + y_{91} + y_{49}y_{50} + y_{67}y_{73} + y_{79}y_{85} + y_{91}y_{97}) + y_{57}y_{58}.
\end{aligned}$$

$$\begin{aligned}
Q_8\langle x_{59}x_{60}\rangle = &\{y_{60} + [y_{56} + (y_{48} + y_{93} + y_{43}y_{44} + y_{69}y_{75} + y_{81}y_{87} + y_{93}y_{99}) \\
&\quad (y_{47} + y_{94} + y_{41}y_{42} + y_{70}y_{76} + y_{82}y_{88} + y_{94}y_{100})] \\
&\quad (y_{54} + y_{92} + y_{45}y_{46} + y_{68}y_{74} + y_{80}y_{86} + y_{92}y_{98})\} \\
&(y_{59} + y_{89} + y_{61}y_{62} + y_{65}y_{71} + y_{77}y_{83} + y_{89}y_{95}).
\end{aligned}$$

4. Further Discussion on Implementation

The following **implementation example 1** gives more complicated Moh's implementation, which ϕ_3 has eight Q_k-components. The following **implementation example 2** demonstrates another possibility that we can make some entries of ϕ_2 become of degree 8 and the public key is still of degree 2. In fact, it is not hard to create ϕ_2 and ϕ_3 of high degrees such that the public key is still of degree 2. Note that these two implementations have been routinely checked to avoid the attack of XL method [7].

Implementation Example 1

In this example, let n = 100 and m = 49. Define

$$
\begin{array}{lll}
y_1 = x_1 & y_{35} = x_{35} + x_{19}x_{33} & y_{68} = x_{42}x_{44} \\
y_2 = x_2 & y_{36} = x_{36} + x_{20}x_{34} & y_{69} = x_{43}x_{45} \\
y_3 = x_3 + x_1x_2 & y_{37} = x_{37} + x_{21}x_{35} & y_{70} = x_{40}x_{42} \\
y_4 = x_4 + x_2x_3 & y_{38} = x_{38} + x_{22}x_{36} & y_{71} = x_{41}x_{43} \\
y_5 = x_5 + x_1x_3 & y_{39} = x_{39} + x_{23}x_{37} & y_{72} = x_{38}x_{40} \\
y_6 = x_6 + x_3x_5 & y_{40} = x_{40} + x_{24}x_{38} & y_{73} = x_{39}x_{41} \\
y_7 = x_7 + x_2x_5 & y_{41} = x_{41} + x_{25}x_{39} & y_{74} = x_{36}x_{38} \\
y_8 = x_8 + x_1x_5 & y_{42} = x_{42} + x_{26}x_{40} & y_{75} = x_{37}x_{39} \\
y_9 = x_9 + x_5x_8 & y_{43} = x_{43} + x_{27}x_{41} & y_{76} = x_{34}x_{36} \\
y_{10} = x_{10} + x_3x_8 & y_{44} = x_{44} + x_{28}x_{42} & y_{77} = x_{35}x_{37} \\
y_{11} = x_{11} + x_9x_{10} & y_{45} = x_{45} + x_{29}x_{43} & y_{78} = x_{32}x_{34} \\
y_{12} = x_{12} + x_8x_{10} & y_{46} = x_{46} + x_{30}x_{44} & y_{79} = x_{33}x_{35} \\
y_{13} = x_{13} + x_9x_{11} & y_{47} = x_{47} + x_{31}x_{45} & y_{80} = x_{14}x_{32} \\
y_{14} = x_{14} + x_5x_{13} & y_{48} = x_{48} + x_{12}x_{13} & y_{81} = x_{15}x_{33} \\
y_{15} = x_{15} + x_9x_{14} & y_{49} = x_{49} + x_{46}x_{47} & y_{82} = x_{10} + x_9x_{12} \\
y_{16} = x_{16} + x_{10}x_{15} & y_{50} = x_{30} + x_{45}x_{46} & y_{83} = x_{11} + x_8x_{13} \\
y_{17} = x_{17} + x_{11}x_{16} & y_{51} = x_{31} + x_{44}x_{47} & y_{84} = x_{30}x_{31} \\
y_{18} = x_{18} + x_{12}x_{17} & y_{52} = x_{28} + x_{43}x_{44} & y_{85} = x_{28}x_{29} \\
y_{19} = x_{19} + x_{13}x_{18} & y_{53} = x_{29} + x_{42}x_{45} & y_{86} = x_{26}x_{27} \\
y_{20} = x_{20} + x_{14}x_{19} & y_{54} = x_{26} + x_{41}x_{42} & y_{87} = x_{24}x_{25} \\
y_{21} = x_{21} + x_{15}x_{20} & y_{55} = x_{27} + x_{40}x_{43} & y_{88} = x_{22}x_{23} \\
y_{22} = x_{22} + x_{16}x_{21} & y_{56} = x_{24} + x_{39}x_{40} & y_{89} = x_{20}x_{21} \\
y_{23} = x_{23} + x_{17}x_{22} & y_{57} = x_{25} + x_{38}x_{41} & y_{90} = x_{18}x_{19} \\
y_{24} = x_{24} + x_{18}x_{23} & y_{58} = x_{22} + x_{37}x_{38} & y_{91} = x_{16}x_{17} \\
y_{25} = x_{25} + x_{19}x_{24} & y_{59} = x_{23} + x_{36}x_{39} & y_{92} = x_{14}x_{15} \\
y_{26} = x_{26} + x_{20}x_{25} & y_{60} = x_{20} + x_{35}x_{36} & y_{93} = x_8x_{12} \\
y_{27} = x_{27} + x_{21}x_{26} & y_{61} = x_{21} + x_{34}x_{37} & y_{94} = x_9x_{13} \\
y_{28} = x_{28} + x_{22}x_{27} & y_{62} = x_{18} + x_{33}x_{34} & y_{95} = x_{10}x_{11} \\
y_{29} = x_{29} + x_{23}x_{28} & y_{63} = x_{19} + x_{32}x_{35} & y_{96} = x_8x_9 \\
y_{30} = x_{30} + x_{24}x_{29} & y_{64} = x_{16} + x_{15}x_{32} & y_{97} = x_{49}x_5 \\
y_{31} = x_{31} + x_{25}x_{30} & y_{65} = x_{17} + x_{14}x_{33} & y_{98} = x_{48}x_5 \\
y_{32} = x_{32} + x_{26}x_{31} & y_{66} = x_{44}x_{46} & y_{99} = x_{47}x_5 \\
y_{33} = x_{33} + x_{27}x_{32} & y_{67} = x_{45}x_{47} & y_{100} = x_{46}x_5 \\
y_{34} = x_{34} + x_{28}x_{33} & &
\end{array}
$$

Except the following 8 entries, $z_i = y_i$.

$$
\begin{aligned}
z_1 = {} & y_1 + (y_{49} + (y_{46}y_{47} + y_{50}y_{51} + y_{66}y_{67} + y_{84} + y_{84}(y_{44}y_{45} + y_{52}y_{53} + y_{68}y_{69} + \\
& y_{85} + y_{85}(y_{42}y_{43} + y_{54}y_{55} + y_{70}y_{71} + y_{86} + y_{86}(y_{40}y_{41} + y_{56}y_{57} + y_{72}y_{73} + \\
& y_{87} + y_{87}(y_{38}y_{39} + y_{58}y_{59} + y_{74}y_{75} + y_{88} + y_{88}(y_{36}y_{37} + y_{60}y_{61} + y_{76}y_{77} + \\
& y_{89} + y_{89}(y_{34}y_{35} + y_{62}y_{63} + y_{78}y_{79} + y_{90} + y_{90}(y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + \\
& y_{91} + y_{91}y_{92})))))))))(y_{48} + y_{12}y_{13} + y_{82}y_{83} + y_{93}y_{94} + y_{95} + y_{95}y_{96}) \\
= {} & x_1 + x_{48}x_{49}
\end{aligned}
$$

$$
\begin{aligned}
z_2 = {} & y_2 + (y_{44}y_{45} + y_{52}y_{53} + y_{68}y_{69} + y_{85} + y_{85}(y_{42}y_{43} + y_{54}y_{55} + y_{70}y_{71} + y_{86} + \\
& y_{86}(y_{40}y_{41} + y_{56}y_{57} + y_{72}y_{73} + y_{87} + y_{87}(y_{38}y_{39} + y_{58}y_{59} + y_{74}y_{75} + y_{88} + \\
& y_{88}(y_{36}y_{37} + y_{60}y_{61} + y_{76}y_{77} + y_{89} + y_{89}(y_{34}y_{35} + y_{62}y_{63} + y_{78}y_{79} + y_{90} + \\
& y_{90}(y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + y_{91} + y_{91}y_{92}))))))) \\
= {} & x_2 + x_{44}x_{45}
\end{aligned}
$$

$$
\begin{aligned}
z_3 = {} & y_3 + (y_{38}y_{39} + y_{58}y_{59} + y_{74}y_{75} + y_{88} + y_{88}(y_{36}y_{37} + y_{60}y_{61} + y_{76}y_{77} + y_{89} + \\
& y_{89}(y_{34}y_{35} + y_{62}y_{63} + y_{78}y_{79} + y_{90} + y_{90}(y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + y_{91} + \\
& y_{91}y_{92})))) \\
= {} & x_3 + x_1x_2 + x_{38}x_{39}
\end{aligned}
$$

$$
\begin{aligned}
z_4 = {} & y_4 + (y_{42}y_{43} + y_{54}y_{55} + y_{70}y_{71} + y_{86} + y_{86}(y_{40}y_{41} + y_{56}y_{57} + y_{72}y_{73} + y_{87} + \\
& y_{87}(y_{38}y_{39} + y_{58}y_{59} + y_{74}y_{75} + y_{88} + y_{88}(y_{36}y_{37} + y_{60}y_{61} + y_{76}y_{77} + y_{89} + \\
& y_{89}(y_{34}y_{35} + y_{62}y_{63} + y_{78}y_{79} + y_{90} + y_{90}(y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + y_{91} + \\
& y_{91}y_{92})))))) \\
= {} & x_4 + x_1x_3 + x_{42}x_{43}
\end{aligned}
$$

$$
\begin{aligned}
z_6 = {} & y_6 + (y_{36}y_{37} + y_{60}y_{61} + y_{76}y_{77} + y_{89} + y_{89}(y_{34}y_{35} + y_{62}y_{63} + y_{78}y_{79} + y_{90} + \\
& y_{90}(y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + y_{91} + y_{91}y_{92}))) \\
= {} & x_6 + x_2x_4 + x_{36}x_{37}
\end{aligned}
$$

$$
\begin{aligned}
z_7 = {} & y_7 + (y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + y_{91} + y_{91}y_{92}) \\
= {} & x_7 + x_2x_5 + x_{32}x_{33}
\end{aligned}
$$

$$
\begin{aligned}
z_8 = {} & y_8 + (y_{34}y_{35} + y_{62}y_{63} + y_{78}y_{79} + y_{90} + y_{90}(y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + y_{91} + \\
& y_{91}y_{92})) \\
= {} & x_8 + x_2x_6 + x_{34}x_{35}
\end{aligned}
$$

$$
\begin{aligned}
z_9 = {} & y_9 + (y_{40}y_{41} + y_{56}y_{57} + y_{72}y_{73} + y_{87} + y_{87}(y_{38}y_{39} + y_{58}y_{59} + y_{74}y_{75} + y_{88} + \\
& y_{88}(y_{36}y_{37} + y_{60}y_{61} + y_{76}y_{77} + y_{89} + y_{89}(y_{34}y_{35} + y_{62}y_{63} + y_{78}y_{79} + y_{90} + \\
& y_{90}(y_{32}y_{33} + y_{64}y_{65} + y_{80}y_{81} + y_{91} + y_{91}y_{92}))))) \\
= {} & x_9 + x_2x_7 + x_{40}x_{41}
\end{aligned}
$$

Implementation Example 2

In this example, let n = 100 and m = 60.

$y_1 = x_1$	$z_1 = 7y_1 + y_{21}y_{28}$	$= x_1 + x_{21}x_{28}$
$y_2 = x_2$	$z_2 = y_2 + y_{22}y_{27}$	$= x_2 + x_{22}x_{27}$
$y_3 = x_3 + x_1x_2$	$z_3 = y_3$	$= x_3 + x_1x_2$
$y_4 = x_4 + x_2x_3$	$z_4 = y_4$	$= x_4 + x_2x_3$
$y_5 = x_5 + x_3x_4$	$z_5 = y_5$	$= x_5 + x_3x_4$
$y_6 = x_6 + x_4x_5$	$z_6 = y_6$	$= x_6 + x_4x_5$
$y_7 = x_7 + x_5x_6$	$z_7 = y_7$	$= x_7 + x_5x_6$
$y_8 = x_8 + x_6x_7$	$z_8 = y_8$	$= x_8 + x_6x_7$
$y_9 = x_9 + x_7x_8$	$z_9 = y_9$	$= x_9 + x_7x_8$
$y_{10} = x_{10} + x_8x_9$	$z_{10} = y_{10}$	$= x_{10} + x_8x_9$
$y_{11} = x_{11} + x_9x_{10}$	$z_{11} = y_{11}$	$= x_{11} + x_9x_{10}$
$y_{12} = x_{12} + x_8x_{10}$	$z_{12} = y_{12}$	$= x_{12} + x_8x_{10}$
$y_{13} = x_{13} + x_7x_{10}$	$z_{13} = y_{13}$	$= x_{13} + x_7x_{10}$
$y_{14} = x_{14} + x_6x_{10}$	$z_{14} = y_{14}$	$= x_{14} + x_6x_{10}$
$y_{15} = x_{15} + x_5x_{10}$	$z_{15} = y_{15} + y_{24}y_{47} + y_{25}y_{71}$	$= x_{15} + x_5x_{10} + x_{24}x_{47}$
$y_{16} = x_{16} + x_4x_{10}$	$z_{16} = y_{16} + y_{26}y_{60} + y_{21}y_{74}$	$= x_{16} + x_4x_{10} + x_{26}x_{60}$
$y_{17} = x_{17} + x_3x_{10}$	$z_{17} = y_{17} + y_{25}y_{58} + y_{21}y_{77}$	$= x_{17} + x_3x_{10} + x_{25}x_{58}$
$y_{18} = x_{18} + x_{16}x_{17}$	$z_{18} = y_{18} + y_{27}y_{56} + y_{22}y_{86}$	$= x_{18} + x_{16}x_{17} + x_{27}x_{56}$
$y_{19} = x_{19} + x_{17}x_{18}$	$z_{19} = y_{19} + y_{23}y_{38} + y_{22}y_{61}$	$= x_{19} + x_{17}x_{18} + x_{23}x_{38}$
$y_{20} = x_{20} + x_{18}x_{19}$	$z_{20} = y_{20} + y_{25}y_{40} + y_{21}y_{62}$	$= x_{20} + x_{18}x_{19} + x_{25}x_{40}$
$y_{21} = x_{21}$	$z_{21} = y_{21} + y_{26}y_{98} + y_{22}y_{65}$	$= x_{21} + x_{22}x_{23} + x_{26}x_{49}$
$y_{22} = x_{22}$	$z_{22} = y_{22} + y_{26}y_{42} + y_{23}y_{76}$	$= x_{22} + x_{26}x_{42}$
$y_{23} = x_{23}$	$z_{23} = y_{23} + y_{28}y_{45} + y_{24}y_{72}$	$= x_{23} + x_{28}x_{45}$
$y_{24} = x_{24}$	$z_{24} = y_{24} + y_{25}y_{55} + y_{27}y_{81}$	$= x_{24} + x_{25}x_{55}$
$y_{25} = x_{25}$	$z_{25} = y_{25} + y_{27}y_{48} + y_{26}y_{83}$	$= x_{25} + x_{27}x_{48}$
$y_{26} = x_{26}$	$z_{26} = y_{26} + y_{27}y_{35} + y_{28}y_{63}$	$= x_{26} + x_{27}x_{35}$
$y_{27} = x_{27}$	$z_{27} = y_{27} + y_{51}y_{53} + y_{87}y_{89} + y_{94} + y_{78}y_{91} + y_{94}y_{96}$	$= x_{27} + x_{51}x_{53}$
$y_{28} = x_{28}$	$z_{28} = y_{28} + y_{57}y_{59} + y_{85}y_{88} + y_{100} + y_{80}y_{82} + y_{100}\cdot (y_{94} + y_{51}y_{53} + y_{87}\cdot y_{89} + y_{78}y_{91} + y_{94}y_{96})$	$= x_{28} + x_{57}x_{59}$
$y_{29} = x_{29} + x_{16}x_{18}$	$z_{29} = y_{29}$	$= x_{29} + x_{16}x_{18}$
$y_{30} = x_{30} + x_{17}x_{19}$	$z_{30} = y_{30}$	$= x_{30} + x_{17}x_{19}$
$y_{31} = x_{31} + x_{23}\cdot x_{24}x_{25}x_{26}\cdot x_{27}x_{28}x_{29}\cdot x_{30}$	$z_{31} = y_{31} + y_{32}y_{33} + y_{34}y_{36} + y_{37}y_{39} + y_{61}y_{62} + y_{63}\cdot y_{64} + y_{67}y_{70} + y_{73}y_{76}$	$= x_{31} + x_{32}x_{33} + x_{34}x_{36} + x_{37}x_{39} + x_{24}x_{28}$

$y_{32} = x_{32} + x_{23} \cdot x_{24}x_{25}x_{26}$	$z_{32} = y_{32} + y_{41}y_{43} + y_{65}y_{68} + y_{71}y_{74}$	$= x_{32} + x_{23}x_{25} + x_{41}x_{43}$
$y_{33} = x_{33} + x_{27} \cdot x_{28}x_{29}x_{30}$	$z_{33} = y_{33} + y_{44}y_{46} + y_{66}y_{69} + y_{72}y_{75}$	$= x_{33} + x_{27}x_{29} + x_{44}x_{46}$
$y_{34} = x_{34} + x_{23} \cdot x_{25}x_{33}$	$z_{34} = y_{34} + y_{49}y_{50} + y_{77}y_{99} + y_{79}y_{97} + y_{81}y_{95}$	$= x_{34} + x_{47}x_{48} + x_{49}x_{50}$
$y_{35} = x_{35} + x_{28}x_{32}$	$z_{35} = y_{35}$	$= x_{35} + x_{28}x_{32}$
$y_{36} = x_{36} + x_{24}x_{26}$	$z_{36} = y_{36}$	$= x_{36} + x_{24}x_{26}$
$y_{37} = x_{37} + x_{27} \cdot x_{29}x_{32}$	$z_{37} = y_{37} + y_{52}y_{54} + y_{83}y_{93} + y_{84}y_{92} + y_{86}y_{90}$	$= x_{37} + x_{50}x_{51} + x_{52}x_{54}$
$y_{38} = x_{38} + x_{22}x_{33}$	$z_{38} = y_{38}$	$= x_{38} + x_{22}x_{33}$
$y_{39} = x_{39} + x_{28}x_{30}$	$z_{39} = y_{39}$	$= x_{39} + x_{28}x_{30}$
$y_{40} = x_{40} + x_{21}x_{36}$	$z_{40} = y_{40}$	$= x_{40} + x_{21}x_{36}$
$y_{41} = x_{41} + x_{23}x_{24}$	$z_{41} = y_{41}$	$= x_{41} + x_{23}x_{24}$
$y_{42} = x_{42} + x_{23}x_{37}$	$z_{42} = y_{42}$	$= x_{42} + x_{23}x_{37}$
$y_{43} = x_{43} + x_{25}x_{26}$	$z_{43} = y_{43}$	$= x_{43} + x_{25}x_{26}$
$y_{44} = x_{44} + x_{27}x_{28}$	$z_{44} = y_{44}$	$= x_{44} + x_{27}x_{28}$
$y_{45} = x_{45} + x_{24}x_{44}$	$z_{45} = y_{45}$	$= x_{45} + x_{24}x_{44}$
$y_{46} = x_{46} + x_{29}x_{30}$	$z_{46} = y_{46}$	$= x_{46} + x_{29}x_{30}$
$y_{47} = x_{47} + x_{25}x_{41}$	$z_{47} = y_{47}$	$= x_{47} + x_{25}x_{41}$
$y_{48} = x_{48} + x_{26}x_{32}$	$z_{48} = y_{48}$	$= x_{48} + x_{26}x_{32}$
$y_{49} = x_{49} + x_{25}x_{47}$	$z_{49} = y_{49}$	$= x_{49} + x_{25}x_{47}$
$y_{50} = x_{50} + x_{33}x_{48}$	$z_{50} = y_{50}$	$= x_{50} + x_{33}x_{48}$
$y_{51} = x_{51} + x_{35}x_{38}$	$z_{51} = y_{51}$	$= x_{51} + x_{35}x_{38}$
$y_{52} = x_{52} + x_{27}x_{50}$	$z_{52} = y_{52}$	$= x_{52} + x_{27}x_{50}$
$y_{53} = x_{53} + x_{40}x_{42}$	$z_{53} = y_{53}$	$= x_{53} + x_{40}x_{42}$
$y_{54} = x_{54} + x_{32}x_{51}$	$z_{54} = y_{54}$	$= x_{54} + x_{32}x_{51}$
$y_{55} = x_{55} + x_{27}x_{48}$	$z_{55} = y_{55}$	$= x_{55} + x_{27}x_{48}$
$y_{56} = x_{56} + x_{22}x_{51}$	$z_{56} = y_{56}$	$= x_{56} + x_{22}x_{51}$
$y_{57} = x_{57} + x_{46}x_{51}$	$z_{57} = y_{57}$	$= x_{57} + x_{46}x_{51}$
$y_{58} = x_{58} + x_{21}x_{33}$	$z_{58} = y_{58}$	$= x_{58} + x_{21}x_{33}$
$y_{59} = x_{59} + x_{47}x_{53}$	$z_{59} = y_{59}$	$= x_{59} + x_{47}x_{53}$
$y_{60} = x_{60} + x_{21}x_{43}$	$z_{60} = y_{60}$	$= x_{60} + x_{21}x_{43}$
$y_{61} = x_{23}x_{33}$	$z_{61} = y_{61}$	$= x_{23}x_{33}$
$y_{62} = x_{25}x_{36}$	$z_{62} = y_{62}$	$= x_{25}x_{36}$
$y_{63} = x_{27}x_{32}$	$z_{63} = y_{63}$	$= x_{27}x_{32}$
$y_{64} = x_{29}x_{39}$	$z_{64} = y_{64}$	$= x_{29}x_{39}$
$y_{65} = x_{23} + x_{26}x_{41}$	$z_{65} = y_{65}$	$= x_{23} + x_{26}x_{41}$
$y_{66} = x_{27} + x_{30}x_{44}$	$z_{66} = y_{66}$	$= x_{27} + x_{30}x_{44}$
$y_{67} = x_{28} + x_{26}x_{34}$	$z_{67} = y_{67}$	$= x_{28} + x_{26}x_{34}$
$y_{68} = x_{25} + x_{24}x_{43}$	$z_{68} = y_{68}$	$= x_{25} + x_{24}x_{43}$

$y_{69} = x_{29} + x_{28}x_{46}$	$z_{69} = y_{69}$	$= x_{29} + x_{28}x_{46}$
$y_{70} = x_{24} + x_{30}x_{37}$	$z_{70} = y_{70}$	$= x_{24} + x_{30}x_{37}$
$y_{71} = x_{24}x_{41}$	$z_{71} = y_{71}$	$= x_{24}x_{41}$
$y_{72} = x_{28}x_{44}$	$z_{72} = y_{72}$	$= x_{28}x_{44}$
$y_{73} = x_{30}x_{34}$	$z_{73} = y_{73}$	$= x_{30}x_{34}$
$y_{74} = x_{26}x_{43}$	$z_{74} = y_{74}$	$= x_{26}x_{43}$
$y_{75} = x_{30}x_{46}$	$z_{75} = y_{75}$	$= x_{30}x_{46}$
$y_{76} = x_{26}x_{37}$	$z_{76} = y_{76}$	$= x_{26}x_{37}$
$y_{77} = x_{25}x_{33}$	$z_{77} = y_{77}$	$= x_{25}x_{33}$
$y_{78} = x_{38}x_{51}$	$z_{78} = y_{78}$	$= x_{38}x_{51}$
$y_{79} = x_{47} + x_{33}x_{49}$	$z_{79} = y_{79}$	$= x_{47} + x_{33}x_{49}$
$y_{80} = x_{51}x_{57}$	$z_{80} = y_{80}$	$= x_{51}x_{57}$
$y_{81} = x_{25}x_{48}$	$z_{81} = y_{81}$	$= x_{25}x_{48}$
$y_{82} = x_{53}x_{59}$	$z_{82} = y_{82}$	$= x_{53}x_{59}$
$y_{83} = x_{27}x_{32}$	$z_{83} = y_{83}$	$= x_{27}x_{32}$
$y_{84} = x_{50} + x_{32}x_{52}$	$z_{84} = y_{84}$	$= x_{50} + x_{32}x_{52}$
$y_{85} = x_{47} + x_{51}x_{59}$	$z_{85} = y_{85}$	$= x_{47} + x_{51}x_{59}$
$y_{86} = x_{27}x_{51}$	$z_{86} = y_{86}$	$= x_{27}x_{51}$
$y_{87} = x_{35} + x_{42}x_{51}$	$z_{87} = y_{87}$	$= x_{35} + x_{42}x_{51}$
$y_{88} = x_{46} + x_{53}x_{57}$	$z_{88} = y_{88}$	$= x_{46} + x_{53}x_{57}$
$y_{89} = x_{40} + x_{38}x_{50}$	$z_{89} = y_{89}$	$= x_{40} + x_{38}x_{53}$
$y_{90} = x_{32}x_{54}$	$z_{90} = y_{90}$	$= x_{32}x_{50}$
$y_{91} = x_{42}x_{53}$	$z_{91} = y_{91}$	$= x_{42}x_{53}$
$y_{92} = x_{51} + x_{27}x_{54}$	$z_{92} = y_{92}$	$= x_{51} + x_{27}x_{54}$
$y_{93} = x_{29} + x_{52}x_{54}$	$z_{93} = y_{93}$	$= x_{29} + x_{52}x_{54}$
$y_{94} = x_{35}x_{40}$	$z_{94} = y_{94}$	$= x_{35}x_{40}$
$y_{95} = x_{33}x_{47}$	$z_{95} = y_{95}$	$= x_{33}x_{47}$
$y_{96} = x_{38}x_{42}$	$z_{96} = y_{96}$	$= x_{38}x_{42}$
$y_{97} = x_{48} + x_{25}x_{50}$	$z_{97} = y_{97}$	$= x_{48} + x_{25}x_{50}$
$y_{98} = x_{49} + x_{22}x_{41}$	$z_{98} = y_{98}$	$= x_{49} + x_{22}x_{41}$
$y_{99} = x_{23} + x_{49}x_{50}$	$z_{99} = y_{99}$	$= x_{23} + x_{49}x_{50}$
$y_{100} = x_{46}x_{47}$	$z_{100} = y_{100}$	$= x_{46}x_{47}$

5. About the Decomposition of $\phi_3 \circ \phi_2$

We want to point out an obvious fact that the decomposition of $\phi_3 \circ \phi_2$ is not unique. In the following example, we show that the composition of ϕ_2 and ϕ_3 has another decomposition (up to permutations) ϕ_2' and ϕ_3', which are both of degree 2. Note that the original ϕ_3 has a Q_4 component. Hence, we shall keep in mind that a Q_n component with big n sometimes still gives a weak key since the composition of ϕ_2 and ϕ_3 may have another decomposition. There are some tricks to create

Q_n components such that the situation happened in the following example can be avoided. We hope to return to this matter elsewhere. However, decompositions of polynomial maps into tame transformations for higher dimension are still completely unknown.

$$
\begin{array}{lll}
y_1 = x_1 & z_1 = y_1 + Q_4\langle x_8x_9\rangle & = x_1 + x_8x_9 \\
y_2 = x_2 + x_1^2 & z_2 = y_2 & = x_2 + x_1^2 \\
y_3 = x_3 + x_1x_2 & z_3 = y_3 & = x_3 + x_1x_2 \\
y_4 = x_4 + x_2x_3 & z_4 = y_4 & = x_4 + x_2x_3 \\
y_5 = x_5 + x_4^2 & z_5 = y_5 & = x_5 + x_4^2 \\
y_6 = x_6 + x_4x_5 & z_6 = y_6 & = x_6 + x_4x_5 \\
y_7 = x_7 + x_5x_6 & z_7 = y_7 & = x_7 + x_5x_6 \\
y_8 = x_8 + x_1x_4 & z_8 = y_8 & = x_8 + x_1x_4 \\
y_9 = x_9 + x_4x_7 & z_9 = y_9 & = x_9 + x_4x_7 \\
y_{10} = x_1 + x_3x_5 & z_{10} = y_{10} & = x_1 + x_3x_5 \\
y_{11} = x_4 + x_2x_6 & z_{11} = y_{11} & = x_4 + x_2x_6 \\
y_{12} = x_1x_5 & z_{12} = y_{12} & = x_1x_5 \\
y_{13} = x_2x_4 & z_{13} = y_{13} & = x_2x_4 \\
y_{14} = x_2x_5 & z_{14} = y_{14} & = x_2x_5 \\
y_{15} = x_3x_6 & z_{15} = y_{15} & = x_3x_6 \\
y_{16} = x_3x_4 & z_{16} = y_{16} & = x_3x_4 \\
y_{17} = x_6x_7 & z_{17} = y_{17} & = x_6x_7 \\
y_{18} = x_2 + x_4x_6 & z_{18} = y_{18} & = x_2 + x_4x_6 \\
y_{19} = x_5 + x_3x_7 & z_{19} = y_{19} & = x_5 + x_3x_7
\end{array}
$$

where $Q_4\langle x_8x_9\rangle = (y_{14} + y_3y_6 + y_{10}y_{11} + y_{12}y_{13} + y_{14}y_{15})(y_{15} + y_4y_7 + y_{14}y_{15} + y_{16}y_{17} + y_{18}y_{19})$

$$
\begin{array}{lll}
y_1 = x_8 & z_1 = y_1 + Q_2\langle x_1x_4\rangle & = x_8 + x_1x_4 \\
y_2 = x_9 & z_2 = y_1 + Q_2\langle x_4x_7\rangle & = x_9 + x_4x_7 \\
y_3 = x_1 + x_8x_9 & z_3 = y_3 & = x_1 + x_8x_9 \\
y_4 = x_2 + x_1^2 & z_4 = y_4 & = x_2 + x_1^2 \\
y_5 = x_3 + x_1x_2 & z_5 = y_5 & = x_3 + x_1x_2 \\
y_6 = x_4 + x_2x_3 & z_6 = y_6 & = x_4 + x_2x_3 \\
y_7 = x_5 + x_4^2 & z_7 = y_7 & = x_5 + x_4^2 \\
y_8 = x_6 + x_4x_5 & z_8 = y_8 & = x_6 + x_4x_5 \\
y_9 = x_7 + x_5x_6 & z_9 = y_9 & = x_7 + x_5x_6 \\
y_{10} = x_1 + x_3x_5 & z_{10} = y_{10} & = x_1 + x_3x_5 \\
y_{11} = x_4 + x_2x_6 & z_{11} = y_{11} & = x_4 + x_2x_6 \\
y_{12} = x_1x_5 & z_{12} = y_{12} & = x_1x_5 \\
y_{13} = x_2x_4 & z_{13} = y_{13} & = x_2x_4
\end{array}
$$

$$
\begin{array}{lll}
y_{14} = x_2x_5 & z_{14} = y_{14} & = x_2x_5 \\
y_{15} = x_3x_6 & z_{15} = y_{15} & = x_3x_6 \\
y_{16} = x_3x_4 & z_{16} = y_{16} & = x_3x_4 \\
y_{17} = x_6x_7 & z_{17} = y_{17} & = x_6x_7 \\
y_{18} = x_2 + x_4x_6 & z_{18} = y_{18} & = x_2 + x_4x_6 \\
y_{19} = x_5 + x_3x_7 & z_{19} = y_{19} & = x_5 + x_3x_7
\end{array}
$$

where $Q_2\langle x_1x_4\rangle = (y_{14} + y_3y_6 + y_{10}y_{11} + y_{12}y_{13} + y_{14}y_{15})$ and $Q_2\langle x_4x_7\rangle = (y_{15} + y_4y_7 + y_{14}y_{15} + y_{16}y_{17} + y_{18}y_{19})$

Acknowledgement

We would like to express our deep gratitude to Professor Moh for kindly explaining his work to us. We need to thank Professor J. Chen for showing us an example of automorphisms which have two decompositions up to permutations. We are also grateful to Professor C. Chou for useful discussions on this subject.

References

1. J. Chen, Square-free Component Q_8 in TTM Cryptosystem, *preprint*.
2. C. Chou, D. Guan and J. Chen, A Systematic Construction of a Q_{2^k}-module in TTM, *preprint*.
3. C. Chou and D. Guan, Square-free Q_4, Q_6 and Q_8 modules in TTM, *preprint*.
4. L. Goubin and N. T. Courtois, Cryptanalysis of the TTM Cryptosystem, Accepted by *Asiacrypt 2000*, Dec. 2000.
5. T. Moh, A Public System With Signature And Master Key Functions, *Communications in Algebra*, **27(5)** (1999), 2207-2222.
6. T. Moh, On the Goubin-Courtois Attack on TTM, *Cryptology ePrint Archive* (2001/072).
7. T. Moh, On The Method of XL and Its Inefficiency Against TTM, *Cryptology ePrint Archive* (2001/047).

Lih-Chung Wang and Fei-Hwang Chang
Department of Applied Mathematics
National Donghwa University
Shoufeng, Hualien 974
Taiwan, R.O.C.
E-mail: lcwang@mail.ndhu.edu.tw