ICIC Express Letters ICIC International ©2016 ISSN 1881-803X
Volume **10**, Number **12**, December **2016** pp. **2979–2987**

THE JUSTIFYING AND GENERATING ALGORITHM FOR MULTIVARIATE QUADRATIC QUASIGROUPS OF STRICT TYPE

Ying Zhang, Sisi Xiao, Keming Li and Mingyuan Gao

Department of Mathematics
Dalian Maritime University
No. 1, Linghai Road, Dalian 116026, P. R. China
zhgyg77@sina.com

Received May 2016; accepted August 2016

Abstract. *MQQ scheme is a novel type multivariate public key cryptosystem. As the basic step for MQQ scheme, the generation of MQQs is an important and hard task. In order to resist Gröbner bases attack, the authors introduce the notion of "MQQs of strict type" and point the existence and generation of MQQs of strict type $Quad_d^sLin_0^s$ for $d > 3$ still remain an open problem. In this paper, a necessary and sufficient condition that a given quasigroup is an MQQ of strict type $Quad_d^sLin_0^s$ is proposed. By solving a simple matrix equation, the method for justifying whether an arbitrary quasigroup is an MQQ of strict type and generating MQQ if it is, is also obtained. An example provides an MQQ of strict type of order 2^4, which shows the existence of MQQs of strict type $Quad_d^sLin_0^s$ for $d > 3$ and partly answers the above open problem.*

Keywords: Quasigroup, Multivariate quadratic quasigroup, Strict type, Vector-valued Boolean functions

1. **Introduction.**

Solving systems of multivariate quadratic equations is an important problem in cryptology. The problem of solving such systems over finite fields is called the multivariate quadratic (MQ) problem. In the last two decades, several cryptosystems based on the MQ problem had been proposed and attacked and then been amended [1, 2, 3, 4].

Recently, based on multivariate quadratic quasigroups (MQQ) and Dobbertin transformation, Gligoroski et al. proposed a novel type of MQ-based schemes called MQQ scheme [5]. MQQ scheme offers flexibility in its implementation [6] and efficiency in wireless sensor network [7]. As the basic step for MQQ scheme, the generation of MQQs is an important and hard task. Until now, MQQs of various types and the corresponding generation algorithms have been proposed [9, 10, 11, 12, 13].

In a recent research, the authors emphasize linear relations in the above MQQs can be employed to simplify the system of multivariate quadratic equations and eventually solve some underdefined MQ problems [14] and recommend to use MQQs of strict type $Quad_d^sLin_0^s$ or at least MQQs of strict type $Quad_{d-1}^sLin_1^s$ for relatively large d, so as to be resistant to Gröbner bases attack [8]. However, the existence and generation of MQQs of strict type $Quad_d^sLin_0^s$ for $d > 3$ still remain an open problem [9].

In this paper, we shall propose a necessary and sufficient condition that a given quasigroup is an MQQ of strict type $Quad_d^sLin_0^s$. Then we will show checking whether an arbitrary quasigroup is an MQQ of strict type is equivalent to solving a simple matrix equation. The rest of the paper is organized as follows. Section 2 recalls the original MQQ generation scheme [5]. Section 3 gives a necessary and sufficient condition that a given quasigroup is an MQQ of strict type $Quad_d^sLin_0^s$, and the method to justify whether a given quasigroup is an MQQ of strict type and generate the corresponding Boolean functions if it is. An explicit example is presented in Section 4. Finally, we conclude the paper in Section 5.

2. **Original MQQ Generation Scheme.** Unless otherwise defined in this paper, additions and multiplications are operated in the binary field GF(2).

Definition 2.1. (Definition 1 in [9]) *A quasigroup $(Q, *)$ is a set Q with a binary operation $*$ such that for any $a, b \in Q$, there exist unique x, y:*

$$x * a = b; \quad a * y = b. \tag{1}$$

We call that a quasigroup $(Q, *)$ is of order n if the set Q has n elements. Consider a finite quasigroup $(Q, *)$ of order 2^d. One can choose a bijection $Q \to \{0, 1, \cdots, 2^d - 1\}$ and represent $a \in Q$ by a unique d-bit sequence $(x_1, x_2, \cdots, x_d)$. Now the binary operation $*$ on Q can be considered as a vector valued operation $*_{vv} : \{0,1\}^{2d} \to \{0,1\}^d$ defined as

$$a * b = c \Leftrightarrow *_{vv}(x_1, \cdots, x_d, x_{d+1}, \cdots, x_{2d}) = (z_1, \cdots, z_d), \tag{2}$$

where $x_1, \cdots, x_d, x_{d+1}, \cdots, x_{2d}$ and $z_1, \cdots, z_d$ are binary representation of a, b and c, respectively. It is easy to see that each z_s $(1 \le s \le d)$ depends on the $2d$ bits $x_1, \cdots, x_{2d}$. Thus, each z_s can be regarded as a $2d$-ary Boolean function $z_s = f_s(x_1, \cdots, x_{2d})$, where $f_s : \{0,1\}^{2d} \to \{0,1\}$ is determined by $*$. As stated in [5], we have the following lemma.

Lemma 2.1. (Lemma 1 in [5]) *For every quasigroup $(Q, *)$ of order 2^d and for each bijection $Q \to \{0, 1, \cdots, 2^d - 1\}$, there are a uniquely determined vector valued Boolean function $*vv$ and d uniquely determined $2d$-ary Boolean functions $f_1, f_2, \cdots, f_d$ such that for each $a, b, c \in Q$*

$$\begin{aligned} a * b = c \Longleftrightarrow\ & * vv(x_1, \cdots, x_d, x_{d+1}, \cdots, x_{2d}) \\ &= (f_1(x_1, \cdots, x_d, x_{d+1}, \cdots, x_{2d}), \cdots, f_d(x_1, \cdots, x_d, x_{d+1}, \cdots, x_{2d})). \end{aligned} \tag{3}$$

In general, for a randomly generated quasigroup of order 2^d $(d \ge 4)$, the degrees of Boolean functions are usually higher than 2. Such quasigroups are not suitable for the construction of multivariate quadratic public-key cryptosystem.

Definition 2.2. (Definition 3 in [5]) *A quasigroup $(Q, *)$ of order 2^d is called multivariate quadratic quasigroup (MQQ) of type $Quad_{d-k}Lin_k$ if exactly $d - k$ of the polynomials f_s are of degree 2 and k of them are of degree 1, where $0 \le k < d$.*

Due to the fact that the above mentioned MQQs do not reveal its true complexity, Chen refines the definition of MQQs of type $Quad_{d-k}Lin_k$ to a strictly defined type as a security parameter which better characterizes the difficulty of the underneath MQ problem.

Definition 2.3. (Definition 3 in [9]) *A quasigroup $(Q, *)$ of order 2^d is called an MQQ of strict type and denoted as $Quad^s_{d-k}Lin^s_k$ where $0 \le k < d$, if there are at most $d - k$ quadratic polynomials whose linear combinations do not result in a linear form.*

In order to enhance the security performance of MQQ based cryptosystems, the authors recommend to use MQQs of strict type $Quad^s_d Lin^s_0$ or at least MQQs of strict type $Quad^s_{d-1}Lin^s_1$, for relatively large d, so as to be resistant to Gröbner bases attack. However, the existence and generation of MQQs of strict type $Quad^s_d Lin^s_0$ for $d > 3$ still remain an open problem.

3. **Algorithm for Justifying and Generating MQQs of Strict Type.** In this section, we give a necessary and sufficient condition that a given quasigroup is an MQQ of strict type $Quad^s_d Lin^s_0$. First, we will show checking whether an arbitrary quasigroup is an MQQ of strict type $Quad^s_d Lin^s_0$ is equivalent to solving a simple matrix equation. In this paper, additions and multiplications are operated in the binary field GF(2).

Definition 3.1. (see [15]) *Given an $m \times n$ matrix $A = (a_{ij})$, $\overline{vec}(A)$ is a vector defined as*

$$\overline{vec}(A) = (a_{11}, \cdots, a_{1n}, a_{21}, \cdots, a_{2n}, \cdots, a_{m1}, \cdots, a_{mn})^T,$$

where the superscript T denotes the matrix transpose.

Lemma 3.1. (see [15]) *Let A, X, B be matrices conformable for multiplication. Then*

$$\overline{vec}(AXB) = \left(A \otimes B^T\right) \overline{vec}(X),$$

where $\otimes$ denotes tensor product.

Lemma 3.2. *Let A, B, C, D be suitably sized matrices. Then*

$$(A + B) \otimes (C + D) = A \otimes C + A \otimes D + B \otimes C + B \otimes D.$$

For convenience of presentation, we introduce some notations as follows. Let a quasigroup $(Q, *)$ of order 2^d be given by the multiplication scheme in Table 1.

Table 1. A quasigroup $(Q, *)$ of order 2^d

$*$	0	1	2	$\cdots$	2^d-1
0	$q_0^{(0)}$	$q_1^{(0)}$	$q_2^{(0)}$	$\cdots$	$q_{2^d-1}^{(0)}$
1	$q_0^{(1)}$	$q_1^{(1)}$	$q_2^{(1)}$	$\cdots$	$q_{2^d-1}^{(1)}$
2	$q_0^{(2)}$	$q_1^{(2)}$	$q_2^{(2)}$	$\cdots$	$q_{2^d-1}^{(2)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^d-1	$q_0^{(2^d-1)}$	$q_1^{(2^d-1)}$	$q_2^{(2^d-1)}$	$\cdots$	$q_{2^d-1}^{(2^d-1)}$

In Table 1, $q_i^{(j)} \in Q$, $(i, j = 0, 1, \cdots, 2^d-1)$. For given i and $\forall j \neq j'$, we have $q_i^{(j)} \neq q_i^{(j')}$; for given j and $\forall i \neq i'$, we have $q_i^{(j)} \neq q_{i'}^{(j)}$. Collect the elements of Table 1 into a vector

$$\left(q_0^{(0)}, q_1^{(0)}, \cdots, q_{2^d-1}^{(0)}, q_0^{(1)}, q_1^{(1)}, \cdots, q_{2^d-1}^{(1)}, \cdots, q_0^{(2^d-1)}, q_1^{(2^d-1)}, \cdots, q_{2^d-1}^{(2^d-1)}\right)^T \tag{4}$$

and convert every element of the vector into a d-bit binary sequence, then we obtain a $2^{2d} \times d$ Boolean matrix $[b_1, \cdots, b_d]$, where every b_s $(s = 1, \cdots, d)$ is 2^{2d} dimensional column vector.

According to Lemma 2.1, whether a given quasigroup is an MQQ of strict type $Quad_d^s Lin_0^s$ mainly lies in whether there is $2d$-ary quadratic Boolean function set $\{f_1, f_2, \cdots, f_d\}$ satisfying Table 1. Note that, any $f_s(x_1, \cdots, x_d, y_1, \cdots, y_d)$ can be written in the form

$$f_s = (x_1, \cdots, x_d, y_1, \cdots, y_d)\mathcal{A}_s \begin{pmatrix} x_1 \\ \vdots \\ x_d \\ y_1 \\ \vdots \\ y_d \end{pmatrix}, \quad (s = 1, 2, \cdots, d), \tag{5}$$

where $\mathcal{A}_s$ is a matrix of order $2d$ over binary field GF(2). By (3) and Table 1, when $(x_1, \cdots, x_d)$ and $(y_1, \cdots, y_d)$ are respectively assigned the ergodic d-bit binary sequence of $\{0, 1, \cdots, 2^d - 1\}$ in turn, i.e., $(x_1, \cdots, x_d, y_1, \cdots, y_d)$ in f_s are assigned all row vectors of the following $2^{2d} \times 2d$ matrix of the form

$$\begin{pmatrix} 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & \cdots & 1 \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 1 & 0 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \cdots & 1 & 0 & \cdots & 0 \\ 1 & \cdots & 1 & 0 & \cdots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & 1 & 1 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{q}_0 \\ \mathbf{q}_1 \\ \mathbf{q}_2 \\ \vdots \\ \mathbf{q}_{2^{2d}-1} \end{pmatrix}, \tag{6}$$

we know that every $\mathbf{q}_k$ $(k = 0, 1, \cdots, 2^{2d} - 1)$ for any b_s $(s = 1, \cdots, d)$ need satisfy

$$\begin{pmatrix} \mathbf{q}_0 \mathcal{A}_s \mathbf{q}_0^T \\ \mathbf{q}_1 \mathcal{A}_s \mathbf{q}_1^T \\ \mathbf{q}_2 \mathcal{A}_s \mathbf{q}_2^T \\ \vdots \\ \mathbf{q}_{2^{2d}-1} \mathcal{A}_s \mathbf{q}_{2^{2d}-1}^T \end{pmatrix} = b_s. \tag{7}$$

By Lemma 3.1, (7) can be reshaped into

$$\begin{pmatrix} \mathbf{q}_0 \otimes \mathbf{q}_0 \\ \mathbf{q}_1 \otimes \mathbf{q}_1 \\ \mathbf{q}_2 \otimes \mathbf{q}_2 \\ \vdots \\ \mathbf{q}_{2^{2d}-1} \otimes \mathbf{q}_{2^{2d}-1} \end{pmatrix} \overline{vec}(\mathcal{A}_s) = b_s. \tag{8}$$

Thus, the given quasigroup in Table 1 is an MQQ of strict type $Quad_d^s Lin_0^s$ iff there is a set of matrices $\{\mathcal{A}_1, \cdots, \mathcal{A}_d\}$ satisfying the following matrix equation

$$\begin{pmatrix} \mathbf{q}_0 \otimes \mathbf{q}_0 \\ \mathbf{q}_1 \otimes \mathbf{q}_1 \\ \mathbf{q}_2 \otimes \mathbf{q}_2 \\ \vdots \\ \mathbf{q}_{2^{2d}-1} \otimes \mathbf{q}_{2^{2d}-1} \end{pmatrix} [\overline{vec}(\mathcal{A}_1) \cdots, \overline{vec}(\mathcal{A}_d)] = [b_1, \cdots, b_d], \tag{9}$$

where $[\overline{vec}(\mathcal{A}_1) \cdots, \overline{vec}(\mathcal{A}_d)]$ is regarded as an unknown matrix $[x_1, \cdots, x_d]$.

For convenience we adopt the following notations. I_n is the identity matrix of order n. $E_{i,j}$ is shorthand for the elementary matrix of switching all matrix elements on row i with their counterparts on row j of I_n. $E_{i,j}(1)$ is the elementary matrix of adding all matrix elements on row j (column i) to their counterparts on row i (column j) of I_n. In addition, write

$$\mathcal{Q}_d = \begin{pmatrix} \mathbf{0} \otimes \mathbf{0} \\ \mathbf{q}_1 \otimes \mathbf{q}_1 \\ \mathbf{q}_2 \otimes \mathbf{q}_2 \\ \vdots \\ \mathbf{q}_{2^{2d}-1} \otimes \mathbf{q}_{2^{2d}-1} \end{pmatrix},$$

and $[\mathcal{Q}_d, b_1, \cdots, b_d]$ is the augmented matrix associated with matrix Equation (9).

Whether (9) has solution depends on whether the rank of $\mathcal{Q}_d$ is equal to the rank of $[\mathcal{Q}_d, b_1, \cdots, b_d]$. Firstly, we compute the rank of $\mathcal{Q}_d$. Write

$$\begin{pmatrix} \mathbf{0} \\ \mathbf{q}_1 \\ \mathbf{q}_2 \\ \mathbf{q}_3 \\ \vdots \\ \mathbf{q}_{2^{2d}-1} \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{p}_1 \\ \mathbf{p}_2 \\ \mathbf{p}_2 + \mathbf{p}_1 \\ \vdots \\ \mathbf{p}_{2d} + \mathbf{p}_{2d-1} + \cdots + \mathbf{p}_2 + \mathbf{p}_1 \end{pmatrix}, \tag{10}$$

and then $\mathcal{Q}_d$ can be denoted by

$$\begin{pmatrix} \mathbf{0} \otimes \mathbf{0} \\ \mathbf{p}_1 \otimes \mathbf{p}_1 \\ \mathbf{p}_2 \otimes \mathbf{p}_2 \\ (\mathbf{p}_2 + \mathbf{p}_1) \otimes (\mathbf{p}_2 + \mathbf{p}_1) \\ \vdots \\ (\mathbf{p}_{2d} + \mathbf{p}_{2d-1} + \cdots + \mathbf{p}_2 + \mathbf{p}_1) \otimes (\mathbf{p}_{2d} + \mathbf{p}_{2d-1} + \cdots + \mathbf{p}_2 + \mathbf{p}_1) \end{pmatrix}. \tag{11}$$

By Lemma 3.2, (11) can be written by

$$\begin{pmatrix} \mathbf{0} \otimes \mathbf{0} \\ \mathbf{p}_1 \otimes \mathbf{p}_1 \\ \mathbf{p}_2 \otimes \mathbf{p}_2 \\ \mathbf{p}_2 \otimes \mathbf{p}_2 + \mathbf{p}_2 \otimes \mathbf{p}_1 + \mathbf{p}_1 \otimes \mathbf{p}_2 + \mathbf{p}_1 \otimes \mathbf{p}_1 \\ \vdots \\ \mathbf{p}_{2d} \otimes \mathbf{p}_{2d} + \cdots + \mathbf{p}_{2d} \otimes \mathbf{p}_1 + \mathbf{p}_1 \otimes \mathbf{p}_{2d} + \mathbf{p}_1 \otimes \mathbf{p}_1 \end{pmatrix}. \tag{12}$$

After a succession of elementary row operations, namely left multiplicating by the matrix below:

$$\begin{aligned} P_1 = & \left(\prod_{t=2d-1}^{2} \prod_{0 \le i_1 < \cdots < i_t < t} \left[\prod_{s=t}^{2} \prod_{1 \le j_1 < \cdots < j_s \le t} \prod_{l=1}^{s} E_{1+2^t+\sum\limits_{l=1}^{s} 2^{i_{j_l}}, 1+2^t+2^{i_{j_l}}}(1) \right] \right) \\ & \times \left(\prod_{j=2d-1}^{1} \prod_{i=2}^{2^j} E_{i+2^j, 1+2^j}(1) \right) \times \left(\prod_{j=1}^{2d-1} \prod_{i=1}^{2^j} E_{i+2^j, i}(1) \right), \end{aligned} \tag{13}$$

(12) can be reduced to the form $P_1 \cdot \mathcal{Q}_d$ only having the following nonzero rows which are linearly independent:

$$\begin{aligned} \mathbf{p}_i \otimes \mathbf{p}_i, \quad & (i = 1, \cdots, 2d); \\ \mathbf{p}_i \otimes \mathbf{p}_j + \mathbf{p}_j \otimes \mathbf{p}_i, \quad & (1 \le j < i \le 2d). \end{aligned} \tag{14}$$

It is obvious that the number of such rows is $2d^2 + d$, so the rank of $\mathcal{Q}_d$ is $2d^2 + d$. Furthermore, by multiplying $P_1 \cdot \mathcal{Q}_d$ on the left with the matrix

$$\begin{aligned} P_2 = & \, E_{2d^2+d, 2d^2+d+1} \\ & \times \left(\prod_{l=0}^{2d-3} \left[\prod_{j=0}^{l} \prod_{i=2^{l+1}+2^j-2}^{0} E_{2^{l+1}+2^j-i+(l-j)+\sum\limits_{v=0}^{2d-l-3}(2d-v), 2^{l+1}+2^j-i+(l+1-j)+\sum\limits_{v=0}^{2d-l-3}(2d-v)} \right] \right. \\ & \left. \times \left[\prod_{i=2^{l+1}-1}^{0} E_{2^{l+1}-i+\sum\limits_{v=0}^{2d-l-3}(2d-v), 1+2^{l+1}-i+\sum\limits_{v=0}^{2d-l-3}(2d-v)} \right] \right) \end{aligned}$$

$$\times\left(\prod_{j=0}^{2d-2}\prod_{i=2^{2d-1}+2^j-2}^{0}E_{(2d-2-j)+2^{2d-1}+2^j-i,(2d-1-j)+2^{2d-1}+2^j-i}\right)\tag{15}$$
$$\times\left(\prod_{i=2^{2d-1}-1}^{0}E_{2^{2d-1}-i,1+2^{2d-1}-i}\right).$$

$P_1\cdot\mathcal{Q}_d$ can be changed into the matrix $\begin{pmatrix}\bar{\mathcal{Q}}_d\\ \mathbf{0}_{\left(2^{2d}-2d^2-d\right)\times d}\end{pmatrix}$, where $\bar{\mathcal{Q}}_d$ is row full rank.

Write

$$P_2\cdot P_1\cdot[\mathcal{Q}_d,b_1,\cdots,b_d]=\begin{pmatrix}\bar{\mathcal{Q}}_d & \bar{b}_1 & \cdots & \bar{b}_d\\ \mathbf{0} & \tilde{b}_1 & \cdots & \tilde{b}_d\end{pmatrix},$$

(9) has solution if and only if $\left[\tilde{b}_1,\cdots,\tilde{b}_d\right]=\mathbf{0}_{\left(2^{2d}-2d^2-d\right)\times d}$.

Next, suppose (9) has solution, then the solution matrix can be obtained.

Note that, $\mathcal{Q}_d[x_1,\cdots,x_d]=[b_1,\cdots,b_d]$ is equivalent to the matrix equation

$$\bar{\mathcal{Q}}_d[x_1,\cdots,x_d]=\left[\bar{b}_1,\cdots,\bar{b}_d\right].\tag{16}$$

Since the rank of $\bar{\mathcal{Q}}_d$ is $2d^2+d$, there exists invertible matrix Q of order $4d^2$ such that

$$\bar{\mathcal{Q}}_dQ=\left[I_{2d^2+d},\mathbf{0}_{(2d^2+d)\times(2d^2-d)}\right],\tag{17}$$

where

$$Q=\left(\prod_{j=2}^{2d}\prod_{i=j}^{2d}E_{(j-2)\cdot 2d+i,j-1+(i-1)\cdot 2d}(1)\right)$$
$$\times\left(\prod_{l=2}^{2d}\prod_{i=l}^{2d}\prod_{j=0}^{\frac{1}{2}l(l-1)-1}E_{(l-1)\cdot 2d+i-j-1,(l-1)\cdot 2d+i-j}\right).\tag{18}$$

Obviously, (16) is equivalent to the matrix equation

$$\bar{\mathcal{Q}}_dQQ^{-1}[x_1,\cdots,x_d]=\left[\bar{b}_1,\cdots,\bar{b}_d\right].\tag{19}$$

Letting $Q^{-1}[x_1,\cdots,x_d]=[y_1,\cdots,y_d]$, (19) can be rewritten by

$$\left[I_{2d^2+d},\mathbf{0}_{(2d^2+d)\times(2d^2-d)}\right][y_1,\cdots,y_d]=\left[\bar{b}_1,\cdots,\bar{b}_d\right].\tag{20}$$

According to the theory of linear system, the solution matrices of (20) can be represented by

$$[y_1,\cdots,y_d]=\begin{pmatrix}\bar{b}_1 & \bar{b}_2 & \cdots & \bar{b}_d\\ k_{11} & k_{12} & \cdots & k_{1d}\\ k_{21} & k_{22} & \cdots & k_{2d}\\ \vdots & \vdots & \vdots & \vdots\\ k_{2d^2-d,1} & k_{2d^2-d,2} & \cdots & k_{2d^2-d,d}\end{pmatrix},\tag{21}$$

where k_{uv} value is randomly from $\{0,1\}$, $(u=1,\cdots,2d^2-d;v=1,\cdots,d)$. Furthermore, (16) has the following solution matrices

$$[\overline{vec}(\mathcal{A}_1)\cdots,\overline{vec}(\mathcal{A}_d)]=Q\cdot\begin{pmatrix}\bar{b}_1 & \bar{b}_2 & \cdots & \bar{b}_d\\ k_{11} & k_{12} & \cdots & k_{1d}\\ k_{21} & k_{22} & \cdots & k_{2d}\\ \vdots & \vdots & \vdots & \vdots\\ k_{2d^2-d,1} & k_{2d^2-d,2} & \cdots & k_{2d^2-d,d}\end{pmatrix}.\tag{22}$$

For an arbitrary solution matrix, $\{\mathcal{A}_1,\cdots,\mathcal{A}_d\}$ can be got immediately. Further, by (5) we can obtain d quadratic functions of the MQQ of strict type. According to Definition

2.3, we need show the linear combinations of the d quadratic functions do not result in a linear form. The vector valued Boolean functions $f_1, \cdots, f_d$ in (5) have no terms of the linear form, so their linear combinations do not result in a linear form.

Until now, we gave the necessary and sufficient condition that a given quasigroup is an MQQ of strict type $Quad_d^s Lin_0^s$.

Theorem 3.1. *For a given quasigroup* $(Q, *)$ *of order* 2^d *and binary bijection* $Q \rightarrow \{0, 1, \cdots, 2^d - 1\}$. *Suppose* P_1, P_2 *and* Q *are defined by (13), (15) and (18) respectively. Let*

$$P_2 P_1 [b_1, \cdots, b_d] = \begin{pmatrix} \bar{b}_1 & \cdots & \bar{b}_d \\ \tilde{b}_1 & \cdots & \tilde{b}_d \end{pmatrix}. \tag{23}$$

$(Q, *)$ *is an MQQ of strict type* $Quad_d^s Lin_0^s$ *if and only if* $\left[\tilde{b}_1, \cdots, \tilde{b}_d\right] = \mathbf{0}_{\left(2^{2d} - 2d^2 - d\right) \times d}$ *holds. Further, for any* $k_{uv} = 0$ *or* 1, $(u = 1, \cdots, 2d^2 - d; v = 1, \cdots, d)$, $f_1, \cdots, f_d$ *are obtained by (5) and (22).*

4. **An Example.** In [9], Chen et al. point that the existence and generation of MQQs of strict type $Quad_d^s Lin_0^s$ for $d > 3$ still remain an open problem. In this section, we will give an MQQ of strict type of order 2^4. This example not only partly answers the above problem, but also shows how our method works and verifies the validity of our results. A quasigroup $(Q, *)$ of order 2^4 based on GF(2) is given in Table 2.

Table 2. A quasigroup $(Q, *)$ of order 2^4 based on GF(2)

$*$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	1	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Suppose $P_2 P_1 [b_1, b_2, b_3, b_4] = \begin{pmatrix} \bar{b}_1 & \bar{b}_2 & \bar{b}_3 & \bar{b}_4 \\ \tilde{b}_1 & \tilde{b}_2 & \tilde{b}_3 & \tilde{b}_4 \end{pmatrix}$. Since $\left(\tilde{b}_1, \tilde{b}_2, \tilde{b}_3, \tilde{b}_4\right) = \mathbf{0}_{220,4}$, for a random matrix

$$(k_{uv})_{28 \times 4} = \begin{pmatrix} 0&1&0&1&1&1&0&0&0&1&0&1&1&1&0&0&0&1&0&1&0&0&0&0&1&1&1&0 \\ 1&1&0&1&0&0&0&0&0&0&0&0&1&1&0&0&0&1&0&0&1&0&0&0&0&0&1&1 \\ 1&0&0&0&1&0&0&0&1&1&1&0&1&0&1&0&1&0&0&1&1&0&1&1&0&0&0&0 \\ 1&1&1&1&1&0&1&1&0&1&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&1&0&0 \end{pmatrix}^T, \tag{24}$$

the corresponding functions are achieved as follows:

$$\begin{aligned}
f_1 =&(x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4)\begin{pmatrix}1&0&1&1&0&0&0&0\\0&0&0&1&0&1&0&0\\1&0&0&1&0&1&1&0\\1&1&1&0&1&1&0&1\\0&0&0&1&1&0&1&1\\0&1&1&1&0&0&0&1\\0&0&1&0&1&0&0&0\\0&0&0&1&1&1&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\y_1\\y_2\\y_3\\y_4\end{pmatrix}=x_1^2+y_1^2,\\
f_2 =&(x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4)\begin{pmatrix}0&1&1&1&0&0&0&0\\1&1&0&0&0&0&0&0\\1&0&0&0&0&1&1&0\\1&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&0\\0&0&1&1&0&1&1&1\\0&0&1&0&0&1&0&1\\0&0&0&0&0&1&1&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\y_1\\y_2\\y_3\\y_4\end{pmatrix}=x_2^2+y_2^2,\\
f_3 =&(x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4)\begin{pmatrix}0&1&0&0&0&1&0&0\\1&0&0&1&0&0&1&1\\0&0&1&0&1&1&0&1\\0&1&0&0&1&0&0&0\\0&0&1&1&0&1&1&0\\1&0&1&0&1&0&1&0\\0&1&0&0&1&1&1&0\\0&1&1&0&0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\y_1\\y_2\\y_3\\y_4\end{pmatrix}=x_3^2+y_3^2,\\
f_4 =&(x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4)\begin{pmatrix}0&1&1&1&1&1&0&0\\1&0&1&1&1&1&0&0\\1&1&0&0&0&1&0&0\\1&1&0&1&1&1&1&0\\1&1&0&1&0&0&0&1\\1&1&1&1&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\\y_1\\y_2\\y_3\\y_4\end{pmatrix}=x_4^2+y_4^2.
\end{aligned} \tag{25}$$

It is obvious that any linear combination of f_1, f_2, f_3, f_4 will not be linear terms. So $(Q,*)$ is an MQQ of strict type $Quad_d^sLin_0^s$.

5. **Conclusions.**

In order to resist Gröbner bases attack, the authors introduce the notion of "MQQs of strict type" and point that the existence and generation of MQQs of strict type $Quad_d^sLin_0^s$ for $d>3$ still remain an open problem.

In this paper, we first establish a necessary and sufficient condition to justify whether a given quasigroup is MQQ of strict type. Then, based on this condition, we propose a method to judge whether a given quasigroup is an MQQ of strict type and obtain the corresponding Boolean functions if it is. The last example provides an MQQ of strict type of order 2^4, which shows the existence of MQQs of strict type $Quad_d^sLin_0^s$ for $d>3$ and partly answers the above open problem. Though our method may not be highly efficient for generating of MQQs of strict type, all the MQQs of strict type can be obtained theoretically with our method. To find a highly efficient method for constructing MQQs of strict type is our future study direction.

Acknowledgment. This work was supported by the National Natural Science Foundation of China under Grant Nos. 61402071 and 61671099, Liaoning Province Natural Science Foundation under Grant Nos. 2015020006 and 2015020011, and the Fundamental Research Funds for the Central Universities Nos. 3132015230 and 3132016111.

REFERENCES

[1] H. Imai and T. Matsumoto, Algebraic methods for constructing asymmetric cryptosystems, *The 3rd International Conference on Algebraic Algorithms and Error Correcting Codes, LNCS*, vol.29, pp.108-119, 1985.

[2] A. Shamir, Efficient signature schemes based on birational permutations, *Advances in Cryptology, LNCS*, vol.773, pp.1-12, 1993.

[3] J. Patarin, Hidden field equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms, *Advances in Cryptology, LNCS*, vol.1070, pp.33-48, 1996.

[4] A. Kipnis, J. Patarin and L. Goubin, Unbalanced oil and vinegar signature schemes, *Advances in Cryptology, LNCS*, vol.1592, pp.206-222, 1999.

[5] D. Gligoroski, S. Markovski and S. J. Knapskog, A public key block cipher based on multivariate quadratic quasigroups, *Cryptology ePrint Archive*, Report 320, 2008.

[6] M. E. Hadedy, D. Gligoroski and S. J. Knapskog, High performance implementation of a public key block cipher – MQQ, for FPGA platforms, *International Conference on Reconfigurable Computing and FPGAs*, pp.427-432, 2008.

[7] R. J. M. Maia, P. S. L. M. Barreto and B. T. de Oliveira, Implementation of multivariate quadratic quasigroup for wireless sensor network, *Trans. Computational Science XI, LNCS*, vol.6480, pp.64-78, 2010.

[8] J. C. Faugĕre, R. S. Ødegård, L. Perret and D. Gligoroski, Analysis of the MQQ public key cryptosystem, *Cryptology and Network Security, LNCS*, vol.6467, pp.169-183, 2010.

[9] Y. L. Chen, S. J. Knapskog and D. Gligoroski, Multivariate quadratic quasigroups (MQQs): Construction, bounds and complexity, *The 6th International Conference on Information Security and Cryptology*, Science Press of China, 2010.

[10] S. Samardjiska, S. Markovski and D. Gligoroski, Multivariate quasigroups defined by t-functions, *Symbolic Computation and Cryptography*, pp.117-127, 2010.

[11] S. Samardjiska, Y. Chen and D. Gligoroski, Construction of multivariate quadratic quasigroups (MQQs) in arbitrary Galois fields, *The 7th International Conference on Information Assurance and Security*, pp.314-319, 2011.

[12] A. Christov, *Quasigroup Based Cryptography*, Ph.D. Thesis, Department of Algebra, Charles University in Prague, 2009.

[13] R. Ahlawat, K. Gupta and S. K. Pal, Fast generation of multivariate quadratic quasigroups for cryptographic applications, *Proc. of Mathematics in Defence*, 2009.

[14] N. Courtois, L. Goubin, W. Meier and J. D. Tacier, Solving underdefined systems of multivariate quadratic equations, *Proc. of Public Key Cryptography, LNCS*, vol.2274, pp.211-227, 2002.

[15] G. H. Golub and C. F. V. Loan, *Matrix Computations*, 3rd Edition, Johns Hopkins Studies in the Mathematical Sciences, Johns Hopkins University Press, Baltimore, Md, USA, 1996.