International Journal of Innovative Computing, Information and Control
Volume **13**, Number **4**, August **2017**

ICIC International ©2017 ISSN 1349-4198
pp. 1415–1423

A GENERALIZED ALGORITHM FOR JUSTIFYING AND GENERATING BILINEAR MULTIVARIATE QUADRATIC QUASIGROUPS OVER GALOIS FIELDS

Ying Zhang

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

Received November 2016; revised March 2017

Abstract. *As the basic cryptographic structure for MQQ scheme, multivariate quadratic quasigroup (MQQ) has been one of the latest tools in designing cryptographic system. However, it is limited to the operation over $GF(2)$ and lacks the general understanding. In this paper, we propose a necessary and sufficient condition to verify whether a given quasigroup of any order p^{kd} is a bilinear MQQ over $GF(p^k)$, which shows checking whether an arbitrary quasigroup is bilinear MQQ is equivalent to solving a simple matrix equation. Based on this newly established condition, a deterministic algorithm is proposed to judge whether or not a given quasigroup is bilinear MQQ, and to generate bilinear MQQ if it is. Two examples are given to show the validity of our results.*

Keywords: Quasigroup, Multivariate quadratic quasigroup, Vector-valued Boolean functions, Judging method, Generating algorithm

1. Introduction.

Public key cryptography (PKC) plays an important role in secure communication. The most widely used PKCs nowadays are the number theory based cryptosystems such as RSA, DSA, and ECC [1, 2]. However, due to Shor's Algorithm [3], such cryptosystems would become insecure under attacks from a large quantum computer. As a new family of cryptosystems that can resist quantum computer attacks and that are more efficient in terms of computation, post-quantum cryptography (PQC) has been proposed.

Multivariate public key cryptography (MPKC) is the one among a few serious candidates to have risen to prominence as post-quantum options. The security of MPKCs is based on the knowledge that solving a set of multivariate polynomial equations over a finite field, is proven to be an NP-hard problem [4]. A quantum computer has not yet been shown to be efficient in solving this problem. However, this does not guarantee that these cryptosystems are secure. In the last twenty years, MPKC was developed rapidly, many schemes had been proposed and attacked and then amended.

Recently, based on multivariate quadratic quasigroups (MQQ) and Dobbertin transformation, Gligoroski et al. proposed a novel type of MPKC schemes called MQQ scheme [5]. As it only needs the basic operations of XOR and AND between bits during the encryption and decryption processes, its speed of decryption/signature generation is almost as fast as a typical symmetric block cipher [6]. The size of the set of MQQs is rather large, which makes MQQ scheme have a bigger scale of private key and public key than conventional MPKC schemes [5]. Moreover, this scheme offers flexibility in its implementation from parallelization point of view [6]. In a recent work, MQQ scheme has been successfully used in wireless sensor network [7]. Though the original MQQ scheme is considered broken now [8], if a suitable replacement for the Dobbertin transformation is found, MQQ scheme can possibly be made strong enough to resist pure Gröbner attacks for adequate choices of quasigroup size and number of variables [9]. In addition, using left quadratic quasigroups, and excluding some polynomials to make MQQ non-injective, MQQs can be still secure for signing [10]. Experience indicates that the newly proposed signature scheme MQQ-SIG is not vulnerable under the existing successful attacks on MQQ scheme.

However, the currently designed MQQ-SIG suffers from the common drawback of all MPKC defined over $GF(2)$: its public key is very big [11]. A typical technique to reduce the public key in MPKC is to use polynomials over bigger fields $GF(p^k)$. For MQQ-SIG, Chen et al. and Samardjiska et al. proposed respectively techniques for constructing two different subclass of MQQs (bilinear MQQs [12] and T-MQQs [13]) as public key. Later, Samardjiska et al. generalize the given techniques for the case of arbitrary finite field $GF(p^k)$, and these new constructions can sharply reduce the public key size of cryptosystems based on MQQs [11]. However, the above works are all to construct straight Boolean polynomials of MQQ according to the characteristic of MQQ. Due to the fact that the existing methods of constructing MQQs are almost all based on the sufficient conditions for quasigroups to be special type MQQs, this will cause some MQQs may be missed. Considering that, Zhang et al. [14, 15] gave the respective necessary and sufficient conditions for quasigroups to be bilinear MQQs and strict type MQQs. At the same time, the corresponding algorithms to justify whether quasigroups of any order 2^d are bilinear MQQs and strict type MQQs over $GF(2)$, are proposed therein. As a result, the algorithms can obtain all the bilinear MQQs and strict type MQQs theoretically. Recently, an algorithm is proposed to justify whether quasigroup of any order p^{kd} is nonbilinear MQQ over $GF(p^k)$ [16]. This result can greatly increase the number of MQQs and reduce the public key size of cryptosystems based on MQQs.

In this paper, we extend the work of [14] and propose a necessary and sufficient condition to verify whether a given quasigroup of any order p^{kd} is a bilinear MQQ over $GF(p^k)$, which shows checking whether an arbitrary quasigroup is bilinear MQQ is equivalent to solving simple matrix equations. Based on the condition, a deterministic algorithm is proposed to judge whether or not a given quasigroup is a bilinear MQQ, and to generate the bilinear MQQ if it is.

The rest of the paper is organized as follows. Section 2 recalls the original MQQ generation scheme [5]. Section 3 gives the necessary and sufficient condition and algorithm for justifying and generating bilinear MQQs. Two explicit examples are presented to show the validity of our algorithm in Section 4. Finally, we conclude the paper in Section 5.

2. Original MQQ Generation Scheme.

In this section, we will review the original MQQ generation scheme.

Definition 2.1. (Definition 1 in [12]) *A quasigroup $(Q, *)$ is a set Q with a binary operation $*$ such that for any $a, b \in Q$, there exist unique x, y:*

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

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

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

In general, for a randomly generated quasigroup of order 2^d $(d \geq 4)$, 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 $0 \leq k < d$.*

If the vector valued Boolean functions defining the MQQ have no terms of the form $x_s x_t$ with $s, t \leq d$ or $s, t > d$ [8], we call such MQQs as bilinear MQQs in order to differ from other MQQs.

3. Algorithm for Justifying and Generating Bilinear MQQs over $GF\left(p^{kd}\right)$.

In this section, we will establish a necessary and sufficient condition for a given quasigroup of order p^{kd} to be a bilinear MQQ over $GF(p^k)$, and then use this condition to propose an algorithm for verifying whether a quasigroup is a bilinear MQQ over $GF(p^k)$ and generating the bilinear MQQ if it is.

For convenience we adopt the following notations. I_n is the identity matrix of order n. $E_{i,j}$ is the 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.

Definition 3.1. (see [17]) *Given an $m \times n$ matrix $A = (a_{ij})$, $\overline{vec}(A)$ is a vector defined as*

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

Lemma 3.1. (see [17]) *Let $A \in R^{m\times u}$, $B \in R^{v\times n}$, $X \in R^{u\times v}$, then*

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

Lemma 3.2. *Let $A = (a_{ij})_{m\times u}$, $B = (b_{lt})_{v\times n}$, $X = (x_{jl})_{u\times v}$, where $a_{ij}, b_{lt}, x_{jl} \in \{0, 1, \ldots, p^k - 1\}$, and p be prime number, then*

$$\overline{vec}\left(AXB \mod p^k\right) = \left(A \otimes B^T \mod p^k\right) \overline{vec}(X) \mod p^k.$$

Let a quasigroup $(Q, *)$ of order p^{kd} be given by the multiplication scheme in Table 1.

Table 1. A quasigroup $(Q, *)$ of order p^{kd}

$*$	0	1	2	$\cdots$	$p^{kd}-1$
0	$q_0^{(0)}$	$q_1^{(0)}$	$q_2^{(0)}$	$\cdots$	$q_{p^{kd}-1}^{(0)}$
1	$q_0^{(1)}$	$q_1^{(1)}$	$q_2^{(1)}$	$\cdots$	$q_{p^{kd}-1}^{(1)}$
2	$q_0^{(2)}$	$q_1^{(2)}$	$q_2^{(2)}$	$\cdots$	$q_{p^{kd}-1}^{(2)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$p^{kd}-1$	$q_0^{\left(p^{kd}-1\right)}$	$q_1^{\left(p^{kd}-1\right)}$	$q_2^{\left(p^{kd}-1\right)}$	$\cdots$	$q_{p^{kd}-1}^{\left(p^{kd}-1\right)}$

In Table 1, $q_i^{(j)} \in Q$, $(i, j = 0, 1, \ldots, p^{kd} - 1)$. 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 $q_i^{(j)} \neq q_{i'}^{(j)}$. One can choose two bijections $\kappa : Q \to \{0, 1, \ldots, p-1\}^{dk}$ and $\iota : \{0, 1, \ldots, p-1\}^k \to \{0, 1, \ldots, p^k - 1\}$. Collect the elements of Table 1 into a vector

$$\left(q_0^{(0)}, q_1^{(0)}, \ldots, q_{p^{kd}-1}^{(0)}, q_0^{(1)}, q_1^{(1)}, \ldots, q_{p^{kd}-1}^{(1)}, \ldots, q_0^{\left(p^{kd}-1\right)}, q_1^{\left(p^{kd}-1\right)}, \ldots, q_{p^{kd}-1}^{\left(p^{kd}-1\right)}\right)^T, \qquad (3)$$

and convert every element of the vector into a kd-ary sequence over $GF(p)$ according to the bijection κ. Then, divide every kd-ary sequence into d groups from left to right, where every group is a k-ary sequence, and denote every group by the unique element in $\{0, 1, \ldots, p^k - 1\}$ in terms of the bijection ι. With this method, we get a $p^{2kd} \times d$ matrix $[b_1, \ldots, b_d]$, where every b_s $(s = 1, \ldots, d)$ is a p^{2kd} dimensional column vector over finite field $GF(p^k)$.

By Lemma 2.1, whether or not a given quasigroup is a bilinear MQQ mainly lies in whether there is a $2d$-ary bilinear function set $\{f_1, f_2, \ldots, f_d\}$, which have no terms of the form $x_s x_t$ with $s, t \leq d$ or $s, t > d$, satisfying Table 1. Observe that, for $\forall s$ $(1 \leq s \leq d)$, the bilinear function $f_s(x_1, \ldots, x_d, x_{d+1}, \ldots, x_{2d})$ can be written by

$$f_s = (1, x_1, \ldots, x_d)\mathcal{A}_s \begin{pmatrix} 1 \\ x_{d+1} \\ \vdots \\ x_{2d} \end{pmatrix}, \quad (s = 1, 2, \ldots, d), \tag{4}$$

here $\mathcal{A}_s$ is a matrix of order $d + 1$ over $GF(p^k)$. Let

$$\mathcal{Q}_{kd/k} = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & 0 & 0 & \cdots & 0 & 0 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & 0 & 0 & \cdots & 0 & p^k-1 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & 0 & 0 & \cdots & 0 & p^k-1 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & 0 & 0 & \cdots & p^k-1 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & 0 & 0 & \cdots & p^k-1 & 0 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & 0 & 0 & \cdots & p^k-1 & p^k-1 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & 0 & 0 & \cdots & p^k-1 & p^k-1 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & p^k-1 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & p^k-1 & 0 & \cdots & 0 & 0 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & p^k-1 & 0 & \cdots & 0 & p^k-1 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & p^k-1 & 0 & \cdots & 0 & p^k-1 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & p^k-1 & 0 & \cdots & p^k-1 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & p^k-1 & 0 & \cdots & p^k-1 & 0 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & p^k-1 & 0 & \cdots & p^k-1 & p^k-1 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & p^k-1 & 0 & \cdots & p^k-1 & p^k-1 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & p^k-1 & p^k-1 & \cdots & p^k-1 & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & p^k-1 & p^k-1 & \cdots & p^k-1 & 0 & p^k-1 \\
\ddots & \ddots & \ddots & & \ddots & \ddots & \ddots \\
1 & p^k-1 & p^k-1 & \cdots & p^k-1 & p^k-1 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\
1 & p^k-1 & p^k-1 & \cdots & p^k-1 & p^k-1 & p^k-1
\end{pmatrix}_{p^{kd} \times (d+1)}, \tag{5}$$

by (2), (4), and Table 1, when $(x_1, \ldots, x_d)$ and $(x_{d+1}, \ldots, x_{2d})^T$ in f_s are respectively assigned d-ary sequences in the order of $\{0, 1, \ldots, p^{kd} - 1\}$ where every element is denoted by d-ary sequence over $GF(p^k)$, we have

$$\mathcal{Q}_{kd/k} \mathcal{A}_s \mathcal{Q}_{kd/k}^T \mod p^k = (\rho_{ji})_{p^{kd} \times p^{kd}}, \tag{6}$$

where ρ_{ji} is the sth element of d-ary sequence obtained by dividing $\kappa\left(q_i^{(j)}\right)$ into d groups and writing every group by an element in $GF\left(p^k\right)$.

Then (6) can be rewritten by

$$\overline{vec}\left(\mathcal{Q}_{kd/k} \mathcal{A}_s \mathcal{Q}_{kd/k}^T \mod p^k\right) = b_s. \tag{7}$$

By Lemma 3.2, (7) can be reshaped into

$$\left(\mathcal{Q}_{kd/k} \otimes \mathcal{Q}_{kd/k} \mod p^k\right) \overline{vec}(\mathcal{A}_s) \mod p^k = b_s. \tag{8}$$

Thus, the given quasigroup in Table 1 is a bilinear MQQ iff there is a set of matrices $\{\mathcal{A}_1, \ldots, \mathcal{A}_d\}$ satisfying the following matrix equation

$$\left(\mathcal{Q}_{kd/k} \otimes \mathcal{Q}_{kd/k} \mod p^k\right) [\overline{vec}(\mathcal{A}_1), \ldots, \overline{vec}(\mathcal{A}_d)] \mod p^k = [b_1, \ldots, b_d], \tag{9}$$

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

$$P = \prod_{i=13}^{1} P_i, \tag{10}$$

where

$$P_1 = \prod_{j=1}^{p^{kd}-1} \prod_{i=1}^{p^{kd}} E_{i+jp^{kd},i}(-1), \tag{11}$$

$$P_2 = \prod_{l=d-1}^{1} \prod_{j=1}^{p^k-1} \prod_{i=1}^{p^{2kd-kl}} E_{i+jp^{2kd-kl},i}(-1), \tag{12}$$

$$P_3 = \prod_{l=1}^{d-1} \prod_{j=1}^{p^k-1} \prod_{i=1}^{p^{kd}} E_{i+jp^{kd+kl},i}(1), \tag{13}$$

$$P_4 = \prod_{u=1}^{d-1} \prod_{l=1}^{p^k-1} \prod_{j=1}^{p^{(d-u)k}-1} \prod_{i=1}^{p^{kd}} E_{lp^{2kd-uk}+jp^{kd}+i,lp^{2kd-uk}+i}(-1), \tag{14}$$

$$P_5 = \prod_{l=1}^{d} \prod_{j=2}^{p^k-1} \prod_{i=1}^{p^{kd}} E_{i+jp^{2kd-kl},i+p^{2kd-kl}}(-j), \tag{15}$$

$$P_6 = \prod_{l=d-1}^{1} \prod_{i=p^{kd}}^{1} \prod_{j=p^{2kd-kl}-p^{kd}-1}^{0} E_{i+p^{2kd-kl}+(l-1)p^{kd}-j,i+p^{2kd-kl}+(l-1)p^{kd}-j-1}, \tag{16}$$

$$P_7 = \prod_{j=0}^{d} \prod_{i=1}^{p^{kd}-1} E_{1+jp^{kd}+i,1+jp^{kd}}(-1), \tag{17}$$

$$P_8 = \prod_{u=0}^{d} \prod_{l=d-1}^{1} \prod_{j=1}^{p^k-1} \prod_{i=1}^{p^{(d-l)k}} E_{i+up^{kd}+jp^{(d-l)k},i+up^{kd}}(-1), \tag{18}$$

$$P_9 = \prod_{l=0}^{d} \prod_{j=1}^{d-1} \prod_{i=1}^{p^k-1} E_{1+ip^{jk}+lp^{kd},1+lp^{kd}}(1), \tag{19}$$

$$P_{10} = \prod_{u=0}^{d} \prod_{l=1}^{d-1} \prod_{j=1}^{p^k-1} \prod_{i=2}^{p^{(d-l)k}} E_{jp^{(d-l)k}+up^{kd}+i, jp^{(d-l)k}+up^{kd}+1}(-1), \tag{20}$$

$$P_{11} = \prod_{l=0}^{d} \prod_{j=1}^{d} \prod_{i=2}^{p^k-1} E_{1+ip^{(d-j)k}+lp^{kd}, 1+p^{(d-j)k}+lp^{kd}}(-i), \tag{21}$$

$$P_{12} = \prod_{l=0}^{d} \prod_{j=d-1}^{1} \prod_{i=p^{(d-j)k}-2}^{0} E_{j+p^{(d-j)k}+lp^{kd}-i, j+p^{(d-j)k}+lp^{kd}-i-1}, \tag{22}$$

$$P_{13} = \prod_{l=d}^{1} \prod_{j=d+1}^{1} \prod_{i=lp^{kd}-l(d+1)-1}^{0} E_{j+lp^{kd}-i, j+lp^{kd}-i-1}. \tag{23}$$

Then

$$P\left(\mathcal{Q}_{kd/k} \otimes \mathcal{Q}_{kd/k} \mod p^k\right) = \begin{pmatrix} \mathbf{I}_{(d+1)^2} \\ \mathbf{0}_{p^{2kd}-(d+1)^2,(d+1)^2} \end{pmatrix}. \tag{24}$$

Furthermore, let

$$P[b_1, \ldots, b_d] \mod p^k = \begin{pmatrix} \bar{b}_1, \ldots, \bar{b}_d \\ \tilde{b}_1, \ldots, \tilde{b}_d \end{pmatrix}. \tag{25}$$

If $\left(\tilde{b}_1, \ldots, \tilde{b}_d\right) = \mathbf{0}_{p^{2kd}-(d+1)^2,d}$, then the matrix Equation (9) has unique solution $\left(\bar{b}_1, \ldots, \bar{b}_d\right)$. Thus, $\{f_1, f_2, \ldots, f_d\}$ can be obtained by (4).

By now we have proved the following necessary and sufficient condition that a given quasigroup in $GF\left(p^{kd}\right)$ is a bilinear MQQ in $GF\left(p^k\right)$.

Theorem 3.1. *For a given quasigroup $(Q, *)$ of order p^{kd}, change every element of $(Q, *)$ into a kd-ary sequence over $GF(p)$ in terms of the bijection κ, divide every kd-ary sequence into d groups from left to right, and denote every k-ary sequence by the unique element in $\left\{0, 1, \ldots, p^k - 1\right\}$ in terms of the bijection ι. Then $(Q, *)$ is a bilinear MQQ in $GF(p^k)$ of type $Quad_{d-l}Lin_l$ if and only if the matrix Equation (9) has solution. Furthermore, f_s ($s = 1, 2, \ldots, d$) obtained by (4) are just d polynomials of the bilinear MQQ, and their degrees are not more than 2.*

Remark 3.1. *Compared with the existing bilinear MQQ-generating methods which are based on sufficient conditions for MQQs over $GF\left(p^k\right)$* [11]*, the method of Theorem 3.1 is based on a necessary and sufficient condition for a given quasigroup of order p^{kd} to be a bilinear MQQ over $GF\left(p^k\right)$. As a result, all the bilinear MQQs can be obtained theoretically by our work.*

4. **Two Examples.**

In this section, we use quasigroups of orders 2^4 and 3^2 to show how our methods work. We first justify that the given quasigroups are bilinear MQQs over $GF(2^2)$ and $GF(3)$ respectively, and then generate the corresponding polynomials.

4.1. **Example 1.**

A quasigroup $(Q, *)$ of order 2^4 and its corresponding representations based on $GF(2^2)$ are given in Table 2.

By Theorem 3.1, the problem of finding 2-ary quadratic functions set $\{f_1, f_2\}$ satisfying (2) transforms into the problem of finding 3×3 matrices set $\{\mathcal{A}_1, \mathcal{A}_2\}$. Furthermore, whether $\{\mathcal{A}_1, \mathcal{A}_2\}$ exists or not relies on whether the matrix equation

$$(\mathcal{Q}_{4/2} \otimes \mathcal{Q}_{4/2} \mod 4)[\overline{vec}(\mathcal{A}_1), \overline{vec}(\mathcal{A}_2)] \mod 4 = [b_1, b_2],$$

has solutions. By new algorithm for generating MQQs, we have that

$$[\overline{vec}(\mathcal{A}_1), \overline{vec}(\mathcal{A}_2)] = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 2 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 2 \end{pmatrix}$$

TABLE 2. A quasigroup $(Q, *)$ of order 2^4 and its representations based on $GF(2^2)$

*	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	11	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

*	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
00	00	01	02	03	10	11	12	13	20	21	22	23	30	31	32	33
01	01	00	03	02	11	10	13	12	21	20	23	22	31	30	33	32
02	02	03	00	01	12	13	10	11	22	23	20	21	32	33	30	31
03	03	02	01	00	13	12	11	10	23	22	21	20	33	32	31	30
10	10	11	12	13	00	1	02	03	30	31	32	33	20	21	22	23
11	11	10	13	12	01	0	03	02	31	30	33	32	21	20	23	22
12	12	13	10	11	02	03	00	01	32	33	30	31	22	23	20	21
13	13	12	11	10	03	02	01	00	33	32	31	30	23	22	21	20
20	20	21	22	23	30	31	32	33	00	01	02	03	10	11	12	13
21	21	20	23	22	31	30	33	32	01	00	03	02	11	10	13	12
22	22	23	20	21	32	33	30	31	02	03	00	01	12	13	10	11
23	23	22	21	20	33	32	31	30	03	02	01	00	13	12	11	10
30	30	31	32	33	20	21	22	23	10	11	12	13	00	01	02	03
31	31	30	33	32	21	20	23	22	11	10	13	12	01	00	03	02
32	32	33	30	31	22	23	20	21	12	13	10	11	02	03	00	01
33	33	32	31	30	23	22	21	20	13	12	11	10	03	02	01	00

So, the corresponding bilinear Boolean functions are achieved as follows:

$$f_1=(1,x_1,x_2)\mathcal{A}_1\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=(1,x_1,x_2)\begin{pmatrix}0&1&0\\1&2&0\\0&0&0\end{pmatrix}\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=x_1+x_3+2x_1x_3,$$

$$f_2=(1,x_1,x_2)\mathcal{A}_2\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=(1,x_1,x_2)\begin{pmatrix}0&0&1\\0&0&0\\1&0&2\end{pmatrix}\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=x_2+x_4+2x_2x_4.$$

This is a bilinear MQQ.

4.2. **Example 2.** A quasigroup $(Q,*)$ of order 3^2 and its corresponding representations based on $GF(3)$ are given in Table 3.

TABLE 3. A quasigroup $(Q,*)$ of order 3^2 and its representations based on $GF(3)$

$*$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

$*$	00	01	02	10	11	12	20	21	22
00	00	01	02	10	11	12	20	21	22
01	01	02	00	11	12	10	21	22	20
02	02	00	01	12	10	11	22	20	21
10	10	11	12	20	21	22	00	01	02
11	11	12	10	21	22	20	01	02	00
12	12	10	11	22	20	21	02	00	01
20	20	21	22	00	01	02	10	11	12
21	21	22	20	01	02	00	11	12	10
22	22	20	21	02	00	01	12	10	11

By Theorem 3.1, the problem of finding 2-ary quadratic functions set $\{f_1,f_2\}$ satisfying (2) transforms into the problem of finding 3×3 matrices set $\{\mathcal{A}_1,\mathcal{A}_2\}$. Further, whether $\{\mathcal{A}_1,\mathcal{A}_2\}$ exists or not relies on whether the matrix equation

$$(\mathcal{Q}_{2,1}\otimes\mathcal{Q}_{2,1}\mod 3)\left[\overline{vec}\left(\mathcal{A}_1\right),\overline{vec}\left(\mathcal{A}_2\right)\right]\mod 3=[b_1,b_2],$$

has solution. This is a bilinear MQQ. By new algorithm for generating MQQs, we get that

$$[\overline{vec}(\mathcal{A}_1),\overline{vec}(\mathcal{A}_2)]=\begin{pmatrix}0&0\\1&0\\0&1\\1&0\\0&0\\0&0\\0&1\\0&0\\0&0\end{pmatrix}$$

So, the corresponding bilinear Boolean functions are achieved as follows:

$$f_1=(1,x_1,x_2)\mathcal{A}_1\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=(1,x_1,x_2)\begin{pmatrix}0&1&0\\1&0&0\\0&0&0\end{pmatrix}\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=x_1+x_3,$$

$$f_2=(1,x_1,x_2)\mathcal{A}_2\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=(1,x_1,x_2)\begin{pmatrix}0&0&1\\0&0&0\\1&0&0\end{pmatrix}\begin{pmatrix}1\\x_3\\x_4\end{pmatrix}=x_2+x_4.$$

5. **Conclusions.** This paper reports a method for justifying and generating bilinear MQQs over Galois Field. We establish a necessary and sufficient condition to verify whether the given quasigroup of any order p^{kd} is bilinear MQQ over $GF(p^k)$, and propose an algorithm to judge whether the given quasigroup is bilinear MQQ and obtain the corresponding functions if it is. As a result, all the bilinear MQQs can be obtained theoretically by our work. To find a highly efficient method for constructing bilinear MQQs over $GF(p^k)$ is our future research 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. 3132017050 and 3132017054.

REFERENCES

[1] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol.21, 1978.

[2] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, vol.48, pp.203-209, 1987.

[3] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, *The 35th Annual Symposium on Foundation of Computer Science*, 1994.

[4] M. R. Garey and D. S. Johnson, *Computers and Intractability – A Guide to the Theory of NP-Completeness*, W. H. Freeman and Company, 1979.

[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 Lecture Notes in Computer Science*, vol.6480, pp.64-78, 2010.

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

[9] M. S. Mohamed, J. T. Ding, J. Buchmann and F. Werner, Algebraic attack on the MQQ public key cryptosystem, *Cryptology and Network Security, LNCS*, vol.5888, pp.392-401, 2009.

[10] D. Gligoroski, R. S. Ødegård, R. E. Jensen, L. Perret, J.-C. Faugère, S. J. Knapskog and S. Markovski, MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme, *INTRUST 2011, LNCS*, 2011.

[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] 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.

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

[14] Y. Zhang and H. Zhang, An algorithm for judging and generating bilinear multivariate quadratic quasigroups, *Applied Mathematics Information Sciences*, vol.7, no.5, pp.2071-2076, 2013.

[15] Y. Zhang, S. Xiao, K. Li and M. Gao, The justifying and generating algorithm for multivariate quadratic quasigroups of strict type, *ICIC Express Letters*, vol.10, no.12, pp.2979-2987, 2016.

[16] Y. Zhang and H. Zhang, An algorithm for judging and generating multivariate quadratic quasigroups over Galois fields, *SpringerPlus*, vol.5, no.1845, pp.1-16, 2016.

[17] 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.