# Construction of Multivariate Quadratic Quasigroups (MQQs) in Arbitrary Galois Fields

Simona Samardjiska and Yanling Chen and Danilo Gligoroski
Department of Telematics
Norwegian University of Science and Technology
Trondheim, Norway
Email: {simona.samardjiska, yanling, danilo.gligoroski}@item.ntnu.no

***Abstract*—In this paper we describe two methods for constructing Multivariate Quadratic Quasigroups (MQQ) in Galois fields of any characteristic and order. Our constructions extend the previously known constructions defined for operations over the prime field of characteristic 2. Application of these new constructions can reduce the public key size of the recently introduced family of public key schemes based on MQQs up to 58 times.**

***Index Terms*—Multivariate Quadratic Quasigroups (MQQ); Multivariate Public Key Schemes; Finite Fields;**

## I. Introduction

Multivariate quadratic schemes (MQ schemes) have been an attractive and very active research area for more than 26 years, as a new way of constructing public key cryptosystems. Beside their performance advantages over classical public key schemes based on integer factorization (RSA) and on the discrete logarithm problem in the additive group of points defined by elliptic curves over finite fields (ECC), their popularity increased even more as a post-quantum alternative to the most popular RSA and ECC schemes, since there are no known quantum algorithms that would break MQ schemes.

In the open literature there are in general five schemes that conceptually differ in the construction of the nonlinear quadratic part of the scheme. For the first four classes of multivariate quadratic public key cryptosystems: MIA [1], STS [2], [3], [4], HFE [5] and UOV [6], we suggest the reader to see [7] which is an excellent (but a little bit older survey from 2005) made by Wolf and Preneel.

Recently, in 2008, a fifth multivariate quadratic public key scheme, called MQQ, was proposed [8], [9]. The MQQ scheme is based on the theory of quasigroups and quasigroup string transformations. The crucial part of the scheme is the introduction of a new class of quasigroups called *Multivariate Quadratic Quasigroups* (MQQ). The important characteristic of these quasigroups is that when represented as Boolean functions in their algebraic normal form, their algebraic degree is 2, i.e., they are multivariate quadratic. Compared to other MQ schemes, there is an apparent efficiency advantage of using multivariate quadratic quasigroups for the production of the nonlinear quadratic part of the scheme (the advantage is in the decryption i.e. signing phase), which was demonstrated in practice by the initial software implementations. That fact immediately attracted the attention of cryptographers trying to analyze it. It was first successfully cryptanalyzed independently by Perret [10] using Gröbner basis approach, and Mohamed et al. using MutantXL [11]. Later, an improved cryptanalysis by Faugère et al. in [12] showed exactly why the original MQQ systems were easy to solve in practice.

In order to thwart the previous successful attacks, recently [13] the *minus modifier* was applied in the design of MQQ-SIG, by removing $\frac{1}{2}$ of the public equations of the original MQQ public key algorithm. Although the operational characteristics of MQQ-SIG outperform by two or three orders of magnitude the corresponding schemes based on RSA or ECC, in the current design MQQ-SIG suffers from the common drawback of all MQ schemes defined over $GF(2)$: its public key is very big, from 125 up to 514 Kbytes.

A typical technique to reduce the public key in MQ schemes is to use polynomials over bigger fields $GF(p^k)$. However, depending on the specifics of the design, this transition to a bigger field is not always trivial and straightforward. Concretely, for MQQ-SIG, there are two known techniques for construction of multivariate quadratic quasigroups with operations over $GF(2)$. One is using T-quasigroups [14] as an extension of the concept of T-functions defined by Klimov and Shamir [15]. The other one is a construction of bilinear MQQs [16].

In this paper we extend the work of [14], [16] and generalize the given techniques for the case of arbitrary finite field $GF(p^k)$.

The composition of the paper is as follows: In Section II we provide the basic definitions for quasigroups and multivariate quasigroups and give a brief descriptions of the construction of MQQs defined over $GF(2)$. In Section III we give sufficient conditions for construction of MQQs over $GF(p^k)$, by generalizing the results from [14]. In Section IV we give sufficient conditions for construction of bilinear MQQs with operations over $GF(p^k)$. In Section V we show the gains from the reduction of the public key size using MQQs in bigger fields, and we conclude the paper with the Conclusions.

## II. Preliminaries

### A. Quasigroups

Let $(Q, q)$ be a groupoid and let $a$ be a fixed element of $Q$. The mappings $Q \to Q$, called left and right translations

978-1-4577-2153-3 ©2011 IEEE

(translation mappings), are defined by:

$$L_{q,a}(x) = q(a,x), \quad R_{q,a}(x) = q(x,a),$$

for every $x \in Q$.

*Definition 1:* The groupoid $(Q,q)$ is called a left (right) quasigroup if the mapping $L_{q,a}$ ($R_{q,a}$) is a bijection for every $a \in Q$. If $(Q,q)$ is both left and right quasigroup, than it is simply called a quasigroup.

A finite quasigroup of $n$ elements is said to be a quasigroup of order $n$.

*Definition 2:* Given a quasigroup $(Q,q)$ we can define a new quasigroup operation $q_\backslash$ on $Q$ by

$$q_\backslash(x,y) = z \Leftrightarrow q(x,z) = y,$$

called a parastrophe operation.

The two operations satisfy the identities:

$$q(x, q_\backslash(x,y)) = y, \quad q_\backslash(x, q(x,y)) = y.$$

*Definition 3:* Two quasigroup $(Q,q_1)$ and $(Q,q_2)$ are said to be isotopic, if there exist bijections $\alpha,\beta,\gamma : Q \to Q$ such that

$$(\forall a,b \in Q) \quad \gamma(q_1(a,b)) = q_2(\alpha(a),\beta(b)).$$

We denote the isotopy by $(\alpha,\beta,\gamma)$.

Using the definition, we can effectively construct a new quasigroup isotopic to a known one.

*Proposition 1 ([17]):* Given a binary quasigroup $(Q,q)$, and bijections $\alpha,\beta,\gamma : Q \to Q$, the operation $q'$ defined by

$$q'(x,y) = \gamma^{-1}(q(\alpha(x),\beta(y)))$$

defines a quasigroup $(Q,q')$ isotopic to $(Q,q)$.

### *B. Multivariate Quadratic Quasigroups defined over $GF(2)$*

We will use the representation of finite quasigroups $(Q,q)$ of order $2^d$ by vector valued Boolean functions (v.v.b.f.). That means that the binary operation $q$ on $Q$ can be seen as a v.v.b.f. $q_{vv} : GF(2)^{2d} \to GF(2)^d$ defined by:

$$q(a,b) = c \Longleftrightarrow$$
$$q_{vv}(x_1,x_2,\ldots,x_d,y_1,y_2,\ldots,y_d) = (z_1,z_2,\ldots,z_d),$$

where $x_1 \ldots x_d,\ y_1 \ldots y_d,\ z_1 \ldots z_d$ are the binary representations of $a,b,c$ respectively. Each $z_i$ depends of the bits $x_1,x_2,\ldots,x_d,y_1,y_2,\ldots,y_d$ and is uniquely determined by them. So, each $z_i$ can be seen as a $2d$-ary Boolean function $z_i = q^{(i)}(x_1,\ldots,x_d,y_1,\ldots,y_d)$, where $q^{(i)} : GF(2)^{2d} \to GF(2)$ depends on, and is uniquely determined by, $q$:

$$q(a,b) = c \Longleftrightarrow q_{vv}(x_1,...,x_d,y_1,...,y_d) =$$
$$= (q^{(1)}(x_1,...,x_d,y_1,...,y_d),...,q^{(d)}(x_1,...,x_d,y_1,...,y_d)).$$

Recall that each $k$-ary Boolean function $f(x_1,\ldots,x_k)$ can be represented in a unique way by its algebraic normal form (ANF), i.e., as a sum of products

$$ANF(f) = \alpha_0 \ + \sum_{i=1}^{k} \alpha_i x_i \ + \sum_{1 \le i < j \le k} \alpha_{i,j} x_i x_j \ +$$
$$+ \sum_{1 \le i < j < s \le k} \alpha_{i,j,s} x_i x_j x_s + \ldots,$$

i.e., as a multivariate polynomial over $GF(2)$.

The ANFs of the functions $q^{(i)}$ give us information about the complexity of the quasigroup $(Q,q)$ via the degrees of the Boolean functions $q^{(i)}$. In general, for a randomly generated quasigroup of order $2^d,\ d \ge 4$, the degrees are higher than 2.

*Definition 4:* A quasigroup $(Q,q)$ of order $2^d$ is called a Multivariate Quadratic Quasigroup (MQQ) of type $Quad_{d-k}Lin_k$ if exactly $d-k$ of the polynomials $f_i$ are of degree 2 (i.e., are quadratic) and $k$ of them are of degree 1 (i.e., are linear), where $0 \le k < d$.

Theorem 1 below, gives sufficient conditions for a quasigroup $(Q,*)$ to be a MQQ.

*Theorem 1 ([9]):* Let $\mathbf{A_1} = [f_{ij}]_{d\times d}$ and $\mathbf{A_2} = [g_{ij}]_{d\times d}$ be two $d \times d$ matrices of linear Boolean expressions, and let $\mathbf{b_1} = [u_i]_{d\times 1}$ and $\mathbf{b_2} = [v_i]_{d\times 1}$ be two $d \times 1$ vectors of linear or quadratic Boolean expressions. Let the functions $f_{ij}$ and $u_i$ depend only on the variables $x_1,\ldots,x_d$, and let the functions $g_{ij}$ and $v_i$ depend only on the variables $y_1,\ldots,y_d$. If

$$\mathbf{Det}(\mathbf{A_1}) = \mathbf{Det}(\mathbf{A_2}) = 1 \text{ in } GF(2), \text{ and}$$

$$\mathbf{A_1} \cdot (y_1,\ldots,y_d)^T + \mathbf{b_1} \equiv \mathbf{A_2} \cdot (x_1,\ldots,x_d)^T + \mathbf{b_2}$$

then the vector valued Boolean operation

$$q_{vv}(x_1,\ldots,x_d,y_1,\ldots,y_d) = \mathbf{A_1} \cdot (y_1,\ldots,y_d)^T + \mathbf{b_1}$$

defines a quasigroup $(Q,q)$ of order $2^d$ that is a MQQ.

*Example 1 ([9]):* The vector valued Boolean function $q_{vv}(x_1,x_2,x_3,y_1,y_2,y_3) = (q^{(1)},q^{(2)},q^{(3)})$, where

$$\begin{aligned}
q^{(1)} &= x_1 + x_3 + x_1y_1 + x_2y_1 + x_3y_1 + y_2 + x_1y_2 + \\
&\quad + x_2y_2 + x_3y_2 + x_1y_3 + x_2y_3 + x_3y_3, \\
q^{(2)} &= 1 + x_2 + x_3 + y_1 + x_1y_1 + x_2y_1 + x_3y_1 + \\
&\quad + x_1 + y_2 + x_2y_2 + x_3y_2 + x_1y_3 + x_2y_3 + x_3y_3, \\
q^{(3)} &= 1 + x_2 + x_3y_1 + y_2 + x_3y_2 + y_3 + x_1y_3 + \\
&\quad + x_2y_3 + x_3y_3.
\end{aligned}$$

defines the quasigroup $(Q,q)$ of order $2^3 = 8$ given by the multiplication table in Table I.

TABLE I
A MQQ QUASIGROUP $(Q, *)$ OF ORDER 8.

| $*$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 3 | 2 | 6 | 7 | 1 | 0 | 4 | 5 |
| 1 | 5 | 3 | 7 | 1 | 0 | 6 | 2 | 4 |
| 2 | 0 | 6 | 3 | 5 | 4 | 2 | 7 | 1 |
| 3 | 6 | 7 | 2 | 3 | 5 | 4 | 1 | 0 |
| 4 | 7 | 1 | 4 | 2 | 3 | 5 | 0 | 6 |
| 5 | 1 | 0 | 5 | 4 | 2 | 3 | 6 | 7 |
| 6 | 4 | 5 | 1 | 0 | 6 | 7 | 3 | 2 |
| 7 | 2 | 4 | 0 | 6 | 7 | 1 | 5 | 3 |

### C. Construction of MQQs over $GF(2)$ using T-functions

In [14], the authors give necessary and sufficient conditions for a T-function (defined by Klimov and Shamir [15]) to define a MQQ. They call these quasigroups T-Multivariate Quadratic Quasigroups(T-MQQs). Their characterization provides a deterministic construction of MQQs over $GF(2)$.

*Theorem 2 ([14]):* A vector valued Boolean function $q = (q^{(1)}, q^{(2)}, \ldots, q^{(d)}) : GF(2)^{2d} \to GF(2)^d$ such that for every $s = 1, \ldots, d$, the component $q^{(s)}$ is of the form

$$q^{(s)}(x_1, \ldots, x_d, y_1, \ldots, y_d) = x_s + y_s + \sum_{i,j>s} \alpha_{i,j}^{(s)} x_i x_j + \\ + \sum_{i,j>s} \beta_{i,j}^{(s)} y_i y_j + \sum_{i,j>s} \gamma_{i,j}^{(s)} x_i y_j + \delta^{(s)},$$

defines a T-MQQ of order $2^d$.

*Proposition 2 ([14]):* Let $q$ be a T-MQQ of order $2^d$ as defined in Theorem 2. Let $\mathbf{D}, \mathbf{D_1}, \mathbf{D_2}$ be $d \times d$ nonsingular Boolean matrices, and let $\mathbf{c}, \mathbf{c}_1, \mathbf{c}_2$ be Boolean vectors of dimension $d$. Then

$$q_*(x_1, \ldots, x_d, y_1, \ldots, y_d) = \\ \mathbf{D} \cdot q(\mathbf{D_1} \cdot (x_1, \ldots, x_d) + \mathbf{c}_1, \mathbf{D_2} \cdot (y_1, \ldots, y_d) + \mathbf{c}_2) + \mathbf{c}$$

defines a MQQ that is isotopic to $q$.

### D. Bilinear MQQs over $GF(2)$

In [16], the authors provide an equivalent form of Theorem 1, where the sufficient condition is simplified.

We denote

$$\mathbf{A_1^*} = \mathrm{I}_d + \left[ \; (f_1^{ij}, \cdots, f_d^{ij}) \cdot (x_1, \cdots, x_d)^{\mathrm{T}} \; \right]_{d \times d} \quad (1)$$

$$\mathbf{A_2^*} = \mathrm{I}_d + \left[ \; (g_1^{ij}, \cdots, g_d^{ij}) \cdot (y_1, \cdots, y_d)^{\mathrm{T}} \; \right]_{d \times d} \quad (2)$$

where $f_k^{ij}, g_k^{ij}$ can be 0 or 1, in particular, $f_k^{ij} = g_j^{ik}$, for $1 \le i, j, k \le d$. Then according to [16, Theorem 8], we have

*Theorem 3:* For $\mathbf{A_1^*}, \mathbf{A_2^*}$ as defined in (1) and (2), if

$$\det(\mathbf{A_1^*}) = \det(\mathbf{A_2^*}) = 1, \quad (3)$$

then for any nonsingular binary matrices $\mathrm{B}_1, \mathrm{B}_2$ and a binary vector c, the vector valued Boolean operation $q_{vv}(x_1, \cdots x_d, y_1, \cdots, y_d)$ which is equal to

$$\mathbf{A_0} \cdot \mathrm{B}_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} + \mathrm{B}_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \mathrm{B}_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} + \mathrm{c}, \quad (4)$$

defines a MQQ of order $2^d$. Here

$$\mathbf{A_0} = \left[ \; (f_1^{ij}, \cdots, f_d^{ij}) \cdot \mathrm{B}_1 \cdot (x_1, \cdots, x_d)^{\mathrm{T}} \; \right]_{d \times d}.$$

Note that (4) has a bilinear nature, where the first term represents the bilinear form, the next two terms are the linear part, and the last one is a constant. Hence, in general, these quasigroups can be seen as bilinear quasigroups, and also (4) can be seen as a standard form of quasigroups constructed using Theorem 1.

Even more, using the above theorem, in order to generate MQQs, one only needs to find appropriate $\mathbf{A_1^*}$ (thus $\mathbf{A_2^*}$) such that the condition (3) is satisfied. This significantly simplifies the method deployed in [9], where one needs to search for appropriate $\mathbf{A_1}, \mathbf{A_2}, \mathbf{b_1}, \mathbf{b_2}$ which fulfill Theorem 1.

## III. CONSTRUCTION OF MQQS OVER $GF(p^k)$ USING GENERALIZED T-FUNCTIONS

The construction of MQQs from Theorem 2 as vectors of quadratic polynomials over $GF(2)$ can be generalized for the case of any finite field $GF(p^k)$, where $p$ is prime and $k \ge 1$.

*Theorem 4:* Let $p_1^{(s)}, p_2^{(s)}$, $s = 1, \ldots, d$, be quadratic permutations over $GF(p^k)$. The function

$$q = (q^{(1)}, q^{(2)}, \ldots, q^{(d)}) : GF(p^k)^{2d} \to GF(p^k)^d$$

such that for every $s = 1, \ldots, d$, the component $q^{(s)}$ is of the form

$$q^{(s)}(x_1, \ldots, x_d, y_1, \ldots, y_d) = p_1^{(s)}(x_s) + p_2^{(s)}(y_s) + \\ + \sum_{i,j>s} \alpha_{i,j}^{(s)} x_i x_j + \sum_{i,j>s} \beta_{i,j}^{(s)} y_i y_j + \sum_{i,j>s} \gamma_{i,j}^{(s)} x_i y_j + \\ + \sum_{i>s} \delta_i^{(s)} x_i + \sum_{i>s} \epsilon_i^{(s)} y_i + \eta^{(s)}, \quad (5)$$

defines a MQQ $(GF(p^k)^d, q)$ of order $p^{kd}$.

*Proof:* We will use induction in $d$, i.e. prove that $q = (q^{(1)}, q^{(2)}, \ldots, q^{(d)}) : GF(p^k)^{2d} \to GF(p^k)^d$ defines a quasigroup for every $d \in \mathbb{N}$.

Let $d = 1$. Then $q(x_1, y_1) = (q^{(1)}(x_1, y_1))$, where $q^{(1)}(x_1, y_1) = p_1^{(1)}(x_1) + p_2^{(1)}(y_1) + \eta^{(1)}$.

We need to show that the left and right translations of $q$ are bijections. Let $\mathbf{a} = (a_1) \in GF(p^k)$. Then

$$L_{q,\mathbf{a}}(y_1) = q(a_1, y_1) = (q^{(1)}(a_1, y_1)) = \\ = (p_1^{(1)}(a_1) + p_2^{(1)}(y_1) + \eta^{(1)}) = (p_2^{(1)}(y_1) + \mu^{(1)})$$

Since $p_2^{(1)}(y_1)$ is a permutation, so is $p_2^{(1)}(y_1)+\mu^{(1)}$. Hence $L_{q,\mathbf{a}}$ is a bijection. Similarly $R_{q,\mathbf{a}}$ is a bijection. It follows that $q(x_1,y_1)$ is a quasigroup of order $p^k$.

Now, let

$$q(x_1,x_2,\ldots,x_{d-1},y_1,y_2,\ldots,y_{d-1}) = \\ = (q^{(1)}(x_1,\ldots,x_{d-1},y_1,\ldots,y_{d-1}),\ldots \\ \ldots,q^{(d-1)}(x_1,\ldots,x_{d-1},y_1,\ldots,y_{d-1}))$$

define a quasigroup of order $p^{k(d-1)}$.

For $d$ we have the function $q=(q^{(1)},q^{(2)},\ldots,q^{(d)})$, where each component $q^{(s)}$ has the form (5), and thus depends only on the variables $x_s,\ldots,x_d,y_s,\ldots,y_d$, i.e.,

$$q(x_1,\ldots,x_d,y_1,\ldots,y_d)=(q^{(1)}(x_1,\ldots,x_d,y_1,\ldots,y_d), \\ q^{(2)}(x_2,\ldots,x_d,y_2,\ldots,y_d),\ldots,q^{(d)}(x_d,y_d)).$$

By the induction hypothesis,

$$q'(x_2,\ldots,x_d,y_2,\ldots,y_d) = \\ = (q^{(2)}(x_2,\ldots,x_d,y_2,\ldots,y_d),\ldots,q^{(d)}(x_d,y_d)).$$

is a quasigroup of order $p^{k(d-1)}$. Again, we have to prove that the left and right translations of $q$ are bijections.

Let $\mathbf{a}=(a_1,\ldots,a_d)\in GF(p^k)^d$.

$$L_{q,\mathbf{a}}(y_1,\ldots,y_d)=(q^{(1)}(a_1,\ldots,a_d,y_1,\ldots,y_d), \\ q^{(2)}(a_2,\ldots,a_d,y_2,\ldots,y_d),\ldots,q^{(d)}(a_d,y_d)).$$

By the induction hypothesis,

$$L_{q',\mathbf{a}'}(y_2,\ldots,y_d) = \\ = (q^{(2)}(a_2,\ldots,a_d,y_2,\ldots,y_d),\ldots,q^{(d)}(a_d,y_d)),$$

where $\mathbf{a}'=(a_2,\ldots,a_d)$, is a bijection. For simplicity, let's write

$$L_{q,\mathbf{a}}(y_1,\ldots,y_d) = \\ = (q^{(1)}(a_1,\ldots,a_d,y_1,\ldots,y_d),L_{q',\mathbf{a}'}(y_2,\ldots,y_d)).$$

Suppose $L_{q,\mathbf{a}}$ is not a bijection. This means that there exist $(b_1,\ldots,b_d)\neq(c_1,\ldots,c_d)$ such that

$$L_{q,\mathbf{a}}(b_1,\ldots,b_d)=L_{q,\mathbf{a}}(c_1,\ldots,c_d). \tag{6}$$

If $(b_2,\ldots,b_d)\neq(c_2,\ldots,c_d)$, then since

$$L_{q',\mathbf{a}'}(b_2,\ldots,b_d)=L_{q',\mathbf{a}'}(c_2,\ldots,c_d),$$

we get a contradiction to the inductive hypothesis. Hence $(b_2,\ldots,b_d)=(c_2,\ldots,c_d)$. Now,

$$q^{(1)}(a_1,\ldots,a_d,b_1,\ldots,b_d)=p_1^{(1)}(a_1)+p_2^{(1)}(b_1)+ \\ +\sum_{i,j>1}\alpha_{i,j}^{(1)}a_ib_j+\sum_{i,j>1}\beta_{i,j}^{(1)}b_ib_j+\sum_{i,j>1}\gamma_{i,j}^{(1)}a_ib_j+ \\ +\sum_{i>1}\delta_i^{(1)}a_i+\sum_{i>1}\epsilon_i^{(1)}b_i+\eta^{(1)}=p_1^{(1)}(a_1)+p_2^{(1)}(c_1)+ \\ +\sum_{i,j>1}\alpha_{i,j}^{(1)}a_ic_j+\sum_{i,j>1}\beta_{i,j}^{(1)}c_ic_j+\sum_{i,j>1}\gamma_{i,j}^{(1)}a_ic_j+ \\ +\sum_{i>1}\delta_i^{(1)}a_i+\sum_{i>1}\epsilon_i^{(1)}c_i+\eta^{(1)}+p_2^{(1)}(b_1)-p_2^{(1)}(c_1)= \\ =q^{(1)}(a_1,\ldots,a_d,c_1,\ldots,c_d)+p_2^{(1)}(b_1)-p_2^{(1)}(c_1),$$

i.e., $p_2^{(1)}(b_1)=p_2^{(1)}(c_1)$. As $p_2^{(1)}$ is a bijection, this can not be true for any $b_1\neq c_1$, a contradiction to (6).

Hence, $L_{q,\mathbf{a}}$ is a bijection. Similarly, $R_{q,\mathbf{a}}$ is a bijection.

So, $q$ is a quasigroup. ■

Note that the proof of Theorem 4 applies to Theorem 2 as well, and is different from the one given in [14], where the specific structure of $GF(2)$ is exploited.

Next, let's determine the shape of the permutations $p_1^{(s)},p_2^{(s)}$, $s=1,\ldots,d$. As we need them to be at most quadratic over $GF(p^k)$, the following theorem by Mollin and Small [18], gives a complete characterization.

*Theorem 5 ([18]):* Let $f(x)$ be a polynomial over $GF(p^k)$, with degree at most 2. $f(x)$ is permutation polynomial if and only if one of the next two conditions is satisfied.

- $f(x)=ax+b$, where $a,b\in GF(p^k), a\neq 0$,
- $f(x)=ax^2+b$, where $a,b\in GF(p^k), a\neq 0$, and $p=2$.

Using Theorems 4 and 5, and a linear isotopy defined over $GF(p^k)$, one can construct a general MQQ of order $p^{kd}$, suitable for cryptographic purposes.

*Example 2:* We give an example of a MQQ of order $2^{2\times 3}$ defined using quadratic polynomials over the field $GF(2^2)$.

First using Theorem 4, we obtain the quasigroup $q=(q^{(1)},q^{(2)},q^{(3)})$ as

$$q(x_1,x_2,x_3,y_1,y_2,y_3) = \\ = \begin{bmatrix} 3x_1^2+x_2^2+2x_2x_3+3x_2y_2+x_2y_3++x_3^2+3x_3y_2+ \\ +x_3+3y_1^2+y_2^2+3y_2y_3+y_2+2y_3^2+3 \\ \\ x_2+3x_3^2+2x_3y_3+y_2^2+2y_3^2+y_3 \\ \\ 2x_3^2+y_3+3 \end{bmatrix}$$

which has a "triangular" structure.

Now, let

$$\mathbf{D_1}=\begin{bmatrix}0&0&1\\2&2&1\\1&2&3\end{bmatrix},\ \mathbf{D_2}=\begin{bmatrix}0&3&2\\2&1&2\\2&1&0\end{bmatrix},\ \mathbf{D}=\begin{bmatrix}0&1&3\\1&2&1\\0&1&0\end{bmatrix},$$

be $3\times 3$ nonsingular matrices over $GF(2^2)$, and $c_1=(3,2,2)$, $c_2=(0,1,0)$ and $c=(3,1,3)$ be vectors over $GF(2^2)$. Then the quasigroup

$$q_*(x_1,x_2,x_3,y_1,y_2,y_3) = \\ \mathbf{D}\cdot q(\mathbf{D_1}\cdot(x_1,x_2,x_3)+\mathbf{c}_1,\mathbf{D_2}\cdot(y_1,y_2,y_3)+\mathbf{c}_2)+\mathbf{c}= \\ = \begin{bmatrix} 2x_1^2+3x_1y_1+2x_1y_2+2x_1+x_2^2+x_2y_1+3x_2y_2+ \\ +2x_2+3x_3^2+2x_3y_1+x_3y_2+x_3+2y_1^2+2y_1+ \\ +3y_2^2+y_2+3y_3^2+3 \\ \\ 2x_1^2+2x_1x_2+x_1y_1+3x_1y_2+3x_1y_3+2x_1+3x_2^2+ \\ +x_2x_3+x_2y_1+3x_2y_2+x_2+3x_3y_1+2x_3y_2+2x_3y_3+ \\ +x_3+3y_1^2+2y_1y_3+3y_1+y_2y_3+2y_2+2y_3 \\ \\ 3x_1^2+3x_1y_1+2x_1y_2+2x_1+2x_2^2+x_2y_1+3x_2y_2+ \\ +2x_2+x_3^2+2x_3y_1+x_3y_2+x_3+2y_1^2+3y_1+ \\ +3y_2^2+2y_2+3y_3^2+2 \end{bmatrix}$$

is a MQQ of order $2^{2\times 3}$ isotopic to $q$.

## IV. Construction of bilinear MQQs over $GF(p^k)$

In this section, we extend the construction of MQQs from Theorem 3 as vectors of quadratic polynomials over $GF(2)$ to the case of any finite field $GF(p^k)$, where $p$ is prime and $k \geq 1$. Note that in this section addition, multiplication and calculation of determinants are operated over $GF(p^k)$.

We consider

$$\mathbf{A_1'} = \mathrm{I}_d + \left[ \begin{array}{c} (f_1^{ij}, \cdots, f_d^{ij}) \cdot (x_1, \cdots, x_d)^{\mathrm{T}} \end{array} \right]_{d \times d} \quad (7)$$

$$\mathbf{A_2'} = \mathrm{I}_d + \left[ \begin{array}{c} (g_1^{ij}, \cdots, g_d^{ij}) \cdot (y_1, \cdots, y_d)^{\mathrm{T}} \end{array} \right]_{d \times d} \quad (8)$$

where $f_k^{ij}, g_k^{ij} \in GF(p^k)$, in particular, $f_k^{ij} = g_j^{ik}$, for $1 \leq i, j, k \leq d$. Then we have the following theorem:

*Theorem 6:* For $\mathbf{A_1'}, \mathbf{A_2'}$ as defined in (7) and (8), if

$$\det(\mathbf{A_1'}) \neq 0 \quad \text{and} \quad \det(\mathbf{A_2'}) \neq 0, \quad (9)$$

for any realizations of $(x_1, \cdots, x_d)$ and $(y_1, \cdots, y_d)$, where $x_i, y_i \in GF(p^k)$ and $1 \leq i \leq d$, then for any non-singular matrices $\mathrm{B}_1, \mathrm{B}_2$ over $GF(p^k)$ and any vector c with elements $c_i$ over $GF(p^k)$, the vector valued operation $q_{vv}(x_1, \cdots x_d, y_1, \cdots, y_d)$ which is equal to

$$\mathbf{A_0} \cdot \mathrm{B}_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} + \mathrm{B}_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \mathrm{B}_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} + \begin{pmatrix} c_1 \\ \vdots \\ c_d \end{pmatrix}, \quad (10)$$

defines a MQQ of order $p^{kd}$. Here

$$\mathbf{A_0} = \left[ \begin{array}{c} (f_1^{ij}, \cdots, f_d^{ij}) \cdot \mathrm{B}_1 \cdot (x_1, \cdots, x_d)^{\mathrm{T}} \end{array} \right]_{d \times d}. \quad (11)$$

*Proof:* First we notice that (10) can also be written as

$$\mathbf{A_0'} \cdot \mathrm{B}_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \mathrm{B}_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \mathrm{B}_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} + \begin{pmatrix} c_1 \\ \vdots \\ c_d \end{pmatrix}, \quad (12)$$

where

$$\mathbf{A_0'} = \left[ \begin{array}{c} (g_1^{ij}, \cdots, g_d^{ij}) \cdot \mathrm{B}_2 \cdot (y_1, \cdots, y_d)^{\mathrm{T}} \end{array} \right]_{d \times d}.$$

The equality between (10) and (12) holds because of the special structure of $\mathbf{A_1'}, \mathbf{A_2'}$ as defined in (7) and (8).

We consider the equation

$$q_{vv}(a_1, \cdots, a_d, y_1, \cdots, y_d) = (q_1, \cdots, q_d)^{\mathrm{T}},$$

where $a_i, q_i \in GF(p^k)$ are known, while $y_i$, $1 \leq i \leq d$ are unknown. Let $(b_1, \cdots, b_d) = \mathrm{B}_1 \cdot (a_1, \cdots, a_d)^{\mathrm{T}}$. According to (10) we have

$$\mathbf{A}_{\mathrm{b}} \cdot \mathrm{B}_2 \cdot (y_1, \cdots, y_d)^{\mathrm{T}} = (z_1, \cdots, z_d)^{\mathrm{T}} \quad (13)$$

where $z_i = q_i - b_i - c_i$ over $GF(p^k)$ for $1 \leq i \leq d$, and $\mathbf{A}_{\mathrm{b}}$ is the valuation of $\mathbf{A_1'}$ at $(x_1, \cdots, x_d) = (b_1, \cdots, b_d)$. Due to (9), the linear system (13) has a unique solution $(y_1, \cdots, y_d)^{\mathrm{T}} = (\mathrm{B}_2)^{-1} \cdot (\mathbf{A}_{\mathrm{b}})^{-1} \cdot (z_1, \cdots, z_d)^{\mathrm{T}}$. In a similar manner a unique solution of the equation

$$q_{vv}(x_1, \cdots, x_d, a_1, \cdots, a_d) = (q_1, \cdots, q_d)^{\mathrm{T}}$$

can be found by applying (12), which is equal to (10). Therefore (10) defines a quasigroup. In addition, it is quadratic and has $p^{kd}$ elements, thus it is a MQQ of order $p^{kd}$. ■

*Example 3:* We give an example of a bilinear MQQ of order $2^{2\times 3}$ defined over the field $GF(2^2)$. Let

$$\mathbf{B_1} = \begin{bmatrix} 0 & 0 & 3 \\ 2 & 0 & 3 \\ 2 & 1 & 0 \end{bmatrix}, \ \mathbf{B_2} = \begin{bmatrix} 0 & 1 & 0 \\ 2 & 0 & 1 \\ 3 & 3 & 1 \end{bmatrix},$$

be $3\times 3$ nonsingular matrices over $GF(2^2)$, and $c = (2, 0, 0)^{\mathrm{T}}$ be a vector over $GF(2^2)$. Then

$$\mathbf{A_0} = \begin{bmatrix} 2x_1 + 3x_2 + 2x_3 & 2x_2 + 3x_3 & x_1 + 2x_2 + x_3 \\ 3x_1 + 2x_2 + 2x_3 & 0 & 2x_1 + x_2 + x_3 \\ 3x_1 + x_2 + 3x_3 & 3x_2 + x_3 & 2x_1 + 3x_2 + 2x_3 \end{bmatrix},$$

and the obtained quasigroup $q = (q^{(1)}, q^{(2)}, q^{(3)})$ is

$$q(x_1, x_2, x_3, y_1, y_2, y_3) =$$

$$= \begin{bmatrix} 3x_1y_1 + x_1y_2 + x_1y_3 + 2x_2y_1 + 2x_2y_2 + 2x_3y_1 + \\ +x_3y_2 + 2x_3y_3 + 3x_3 + y_2 + 2 \\ \\ x_1y_1 + 2x_1y_2 + 2x_1y_3 + 2x_1 + 3x_2y_1 + x_2y_2 + x_2y_3 + \\ +3x_3y_1 + x_3y_2 + x_3y_3 + 3x_3 + 2y_1 + y_3 \\ \\ x_1y_1 + 2x_1y_2 + 2x_1y_3 + 2x_1 + 3x_2y_1 + 3x_2y_2 + x_2 + \\ +3x_3y_1 + 2x_3y_2 + 3x_3y_3 + 3y_1 + 3y_2 + y_3 \end{bmatrix}$$

which is a MQQ of order $2^{2\times 3}$.

## V. Benefits of using MQQs defined over $GF(p^k)$

Although in the previous sections we gave constructions of MQQs over any field $GF(p^k)$, in this section we will focus our interest on the fields $GF(2^k)$ where $k$=1, 2, 4 and 8. That is due to the fact that in software and hardware implementations, these are the most common values used.

The number $\tau(k, n)$ of all possible quadratic terms of a multivariate quadratic polynomial $p(x_1, \ldots, x_n)$ differs depending on the underlying field we are working in, i.e., whether we are working in the prime field $GF(2)$ or in another finite field $GF(2^k)$, $k > 1$ and is given by the expression:

$$\tau(k, n) = \begin{cases} 1 + \frac{n(n+1)}{2}, & \text{if } k = 1, \\ 1 + \frac{n(n+3)}{2}, & \text{if } k > 1 \end{cases}$$

Consequently, the size of the public key in multivariate quadratic schemes depends on the number $n$ of variables and on the number of polynomials in the public key. If instead of the original construction of MQQ-SIG in $GF(2)$ as it is in [13], one would use our designed MQQs over $GF(2^k)$, the formula for calculating the size of the public key (in bytes) would be given by the following expression:

$$\text{MQQ-SIGPublicKeySize}(k, n) = \lceil \frac{n}{16} \rceil \times \tau(k, \lceil \frac{n}{k} \rceil)$$

For the most typical values of $n$: 160, 192, 224 and 256 the size of the public key for different values of $k$ is given in Table II. There we see that the reduction of the size of the public key can be up to 58 times.

TABLE II
PUBLIC KEY SIZE OF MQQ-SIG DEFINED BY MQQS IN DIFFERENT $GF(2^k)$. THE COLUMN $GF(2)$ IS FROM THE ORIGINAL DESIGN [13], AND THE OTHER VALUES ARE RESULTS OF THIS PAPER.

| | Size in Kbytes | | | |
|---|---|---|---|---|
| $n$ | $GF(2)$ | $GF(2^2)$ | $GF(2^4)$ | $GF(2^8)$ |
| 160 | 125.79 | 32.43 | 8.41 | 2.26 |
| 192 | 217.14 | 55.70 | 14.36 | 3.81 |
| 224 | 344.55 | 88.06 | 22.60 | 5.95 |
| 256 | 514.02 | 131.02 | 33.52 | 8.77 |

## VI. CONCLUSIONS

We have given two new constructions of Multivariate Quadratic Quasigroups (MQQs) in any finite field $GF(p^k)$. The proposed methods are a natural extension of the methods that were previously developed for MQQs defined over $GF(2)$. The benefit of using our newly designed MQQs over $GF(2^k)$ where $k$=1, 2, 4 or 8, is the reduction of the size of the public key up to 58 times.

As a followup of this work we want to mention that one crucial part about using MQQs is the use of their parastrophes in the decryption or the signing process. This part will be included in the extended version of this paper.

## REFERENCES


[1] H. Imai and T. Matsumoto, "Algebraic methods for constructing asymmetric cryptosystems," in *Proceedings of the 3rd International Conference on Algebraic Algorithms and Error-Correcting Codes*, ser. AAECC-3. London, UK: Springer-Verlag, 1986, pp. 108–119.

[2] A. Shamir, "Efficient signature schemes based on birational permutations." in *CRYPTO*, ser. Lecture Notes in Computer Science, D. R. Stinson, Ed., vol. 773. Springer, 1993, pp. 1–12.

[3] T. Moh, "A public key system with signature and master key functions," Communications in Algebra, pp. 2207–2222, 1999.

[4] L. Goubin and N. Courtois, "Cryptanalysis of the TTM cryptosystem," ser. ASIACRYPT '00. London, UK: Springer-Verlag, 2000, pp. 44–57.

[5] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," ser. EUROCRYPT'96. Berlin, Heidelberg: Springer-Verlag, 1996, pp. 33–48.

[6] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes." in *EUROCRYPT*, 1999, pp. 206–222.

[7] C. Wolf and B. Preneel, "Taxonomy of public key schemes based on the problem of multivariate quadratic equations," Cryptology ePrint Archive, Report 2005/077, 2005.

[8] D. Gligoroski, S. Markovski, and S. J. Knapskog, "Public key block cipher based on multivariate quadratic quasigroups," In Cryptology ePrint Archive, Report 2008/320.

[9] ——, "Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups," in *MATH'08: Proceedings of the American Conference on Applied Mathematics*. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2008, pp. 44–49.

[10] L. Perret, "Personal e-mail communication with Danilo Gligoroski," 2008.

[11] M. S. Mohamed, J. Ding, J. Buchmann, and F. Werner, "Algebraic attack on the MQQ public key cryptosystem," in *CANS '09: Proceedings of the 8th International Conference on Cryptology and Network Security*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 392–401.

[12] J.-C. Faugère, R. S. Ødegård, L. Perret, and D. Gligoroski, "Analysis of the MQQ public key cryptosystem," in *CANS*, ser. Lecture Notes in Computer Science, S.-H. Heng, R. N. Wright, and B.-M. Goi, Eds., vol. 6467. Springer, 2010, pp. 169–183.

[13] 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," Proceedings of INTRUST 2011, in print for LNCS Springer, 2011.

[14] S. Samardjiska, S. Markovski, and D. Gligoroski, "Multivariate quasigroups defined by t-functions," in *Proceedings of SCC2010 - The 2nd International Conference on Symbolic Computation and Cryptography*, 2010.

[15] A. Klimov and A. Shamir, "A new class of invertible mappings." in *CHES*, ser. Lecture Notes in Computer Science, B. S. K. Jr., etin Kaya Ko, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 470–483.

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

[17] A. Albert, "Quasigroups. I." *Trans. Am. Math. Soc.*, vol. 54, pp. 507–519, 1943.

[18] R. Mollin and C. Small, "On permutation polynomials over finite fields." *International Journal of Mathematics and Mathematical Sciences*, vol. 10, pp. 535–544, 1987.