ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2012, Vol. 41, No. 1

THE MULTIVARIATE QUADRATIC POWER PROBLEM OVER Z_N IS NP-COMPLETE

Eligijus Sakalauskas

Department of Applied Mathematics, Kaunas University of Technology,
Studentu str. 50-324a, Kaunas, LT-51368, Lithuania
e-mail: Eligijus.Sakalauskas@ktu.lt

crossref http://dx.doi.org/10.5755/j01.itc.41.1.821

Abstract. In this paper a new NP-complete problem, named as multivariate quadratic power (MQP) problem, is presented. This problem is formulated as a solution of multivariate quadratic power system of equations over the semigroup (monoid) $\boldsymbol{Z}_n$ and is denoted by MQP($\boldsymbol{Z}_n$), where n is a positive integer. Two sequential polynomial-time reductions from the known NP-complete multivariate quadratic (MQ) problem over the field Z_2, i.e. MQ(Z_2) to MQP($\boldsymbol{Z}_n$), are constructed. It is proved that certain restricted MQP($\boldsymbol{Z}_n$) problem over some subgroup of $\boldsymbol{Z}_n$ is equivalent to MQ(Z_2) problem. This allows us to prove that MQP($\boldsymbol{Z}_n$) is NP-complete also.

The MQP problem is related to matrix power function (MPF) which was used for construction of several cryptographic protocols. We expect that the NP-complete problem announced here could be used to create new candidate one-way functions (OWF) and to construct new cryptographic primitives..

Keywords: NP-complete problem; multivariate quadratic power problem; one-way function; cryptography.

1. Introduction

Despite the first unsuccessful attempt of Merkle and Hellman [9] to construct a public key cryptosystem whose security would be based on solution of an NP-complete problem the significant interest to apply these problems in cryptography remains so far. For example, at Eurocrypt in 1996, Patarin proposed hidden fields equations (HFE) cryptosystem following the idea of the Matsumoto and Imai system. The HFE cryptosystem is designed with the aim to bind the security of cryptosystem with the complexity of solution of system of multivariate quadratic (MQ) equations [10]. This problem is called the MQ problem. Garey and Johnson [7] declared and Patarin and Goubin [12] proved that the MQ problem is NP-complete over any field. In 2004, Wolf and Preneel [17] have summarized main results on HFE cryptosystems achieved up to this time. The investigation in this direction is continuing so far.

We think that cryptographic application of existing NP-complete problems and search of new ones suitable for cryptographic applications is a promising research trend. The confirmation of this attitude can be found in recent results of Shor [16]. Traditional cryptography based on prime factorization and discrete logarithm problem (DLP) is vulnerable to quantum cryptanalytic algorithms. The same is valid also for DLP in elliptic curves. As it is known, these problems are not NP-complete. But at the same time so far there are not known quantum cryptanalytic algorithms solving NP-complete problems in polynomial time.

To the contrary of DLP or integer factorization problems, the sound representatives of NP-complete problems such as MQ problems are defined over small fields. This means that arithmetic operations in these fields are performed avoiding time and space consuming arithmetic operations with large integers and hence can be efficiently implemented in computational restricted environments.

In this paper we introduce a new problem, we named as multivariate quadratic power (MQP) problem, which is represented by the system of MQP equations over multiplicative platform semigroup of integers conventionally denoted by $\boldsymbol{Z}_n=\{0, 1, \ldots, n\text{-}1\}$ where n is a positive integer. We denote the MQP problem over this semigroup by MQP($\boldsymbol{Z}_n$) problem. We construct two sequential polynomial-time reductions from known NP-complete MQ problem over the field $\boldsymbol{Z}_n=\{0,1\}$, denoted by MQ($\boldsymbol{Z}_2$), to the MQP($\boldsymbol{Z}_n$) problem. Hence we prove that MQP($\boldsymbol{Z}_n$) is NP-complete as well.

The MQP($\boldsymbol{Z}_n$) problem is related with so-called matrix power function (MPF) which is reckoned as a candidate one-way function (OWF) and firstly was introduced for the symmetric block cipher construction [14]. The cryptographic primitives based on the MPF represent so-called non-commuting cryptography [10]. Non-commuting cryptography is based on hard problems of non-commuting algebraic structures and is some alternative to classical cryptography based on commuting algebraic structures and number theory. One attractive feature of non-commuting cryptography is that the realization of these algorithms does not require arithmetic operations with big integers which are time and space consuming. Together with key agreement protocol [15], some attempts were commited to create more advanced protocols such as e. signature using MPF. Some preliminary results on creating suitable algebraic structures can be found in [13]. If NP-completeness of the MQP($\boldsymbol{Z_n}$) problem will be proved, then the NP-completeness of MPF will be proved either. Then the protocols based on MPF will be proved to have provably secure property. Recall that informally cryptographic protocol is said to be provably secure if its security relies on the known (recognized) hard problem.

In the second section, the MQ($\boldsymbol{Z}_2$) and MQP($\boldsymbol{Z_n}$) problems are introduced and defined.

In Section 3, it is proved that the MQP($\boldsymbol{Z_n}$) problem is NP-complete using two sequential polynomial-time reductions.

In Section 4, discussions concerning construction of new candidate one-way function (OWF) are presented.

2. Preliminaries

Let $\boldsymbol{Z_n}$={0, 1…, n-1} be a finite ring of integers, where n is a positive integer and where the multiplication and addition are performed modulo n. These operations are associative and commuting and we will take it in mind below by default. Since we are not using the addition operation, we interpret the ring $\boldsymbol{Z_n}$ as a multiplicative monoid with trivial ideal, consisting of zero element.

It is well known that if n is prime, then $\boldsymbol{Z_n}$ is a field. We use the field $\boldsymbol{Z}_2$={0,1} to define the multivariate quadratic (MQ) problem over this field, i.e. MQ($\boldsymbol{Z}_2$). This problem is associated with the system of M equations and N variables and conventionally (e.g. see Patarin and Goubin [12]) is given as

$$\sum_{1\le i<j\le N} a_{ijk}x_ix_j \oplus \sum_{i=1}^{N} l_{jk}x_i = d_k,\ (1 \le k \le M)\quad(2.1)$$

where a_{ijk}, l_{ik} and d_k are binary constants and x_i, x_j are unknown binary variables in $\boldsymbol{Z}_2$. According to convention, $a_{ijk}x_ix_j$ and $l_{ik}x_i$ are bilinear and linear terms of equations, respectively. Notice that if a_{ijk}=0 or l_{ik}=0, then $a_{ijk}x_ix_j$=0 or $l_{ik}x_i$=0. The bilinear and linear monomials are x_ix_j and x_i, respectively. For further considerations, we assume that linear terms and monomials are the special case of bilinear terms and monomials, when one of the variables assigns value 1. Hence we can deal with bilinear terms only. Since a_{ijk} is a constant and x_i, x_j are variables then conventionally the general bilinear term $a_{ijk}x_ix_j$ corresponds to the function defined on the domain set $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2$. But to perform a reduction from the MQ problem to the MQP problem we interpret this bilinear term as a function of three arguments (the argument a_{ijk} is added) defined on the domain set $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$.

For better introduction to the MQP problem, formally we interpret it as a symbolic rewriting of every equation of MQ($\boldsymbol{Z}_2$) system in a multiplicative form. This means that we rewrite every equation of system (2.1) by replacing the addition operation $\oplus$ with multiplication · and multiplication of constants by monomials by powering of constants by monomials. Then by renaming a_{ijk}, l_{ik}, x_i and d_k by c_{ijk}, t_{ik}, y_i and e_k, respectively, we obtain the following MQP system of M equations and N variables

$$\prod_{1\le i<j\le N} c_{ijk}^{y_iy_j} \cdot \prod_{i=1}^{N} t_{ik}^{y_i} = e_k,\ (1 \le k \le M). \qquad (2.2)$$

Let us remind that obtained system (2.2) is only symbolic rewriting of the MQ($\boldsymbol{Z}_2$) system (2.1) without defining the domains of constants and variables and ranges of terms yet. But nevertheless this allows us to point out the following correspondences. In analogy with MQ($\boldsymbol{Z}_2$) system, we name the term $c_{ijk}^{\ y_iy_j}$ as bilinear power term and $t_{ik}^{\ y_i}$ as linear power term being a special case of the former. The bilinear and linear power monomials of the MQP system are expressed as y_iy_j and y_i respectively.

It is well known that $\boldsymbol{Z_n}$ contains trivial ideal (zero element) and zero dividers.

Definition 2.1. If ab=0 and both a and b are in $\boldsymbol{Z_n}$ and not equal to zero, then either a or b is a zero divider in $\boldsymbol{Z_n}$.

For example, if n=pq and both p and q are primes, then the ring $\boldsymbol{Z_n}$ consists of two sets of zero dividers $\boldsymbol{D_p}$={p, 2p…, (q-1)p} and $\boldsymbol{D_q}$={q, 2q…, (p-1)q}. By direct observation we see that if $a\in\boldsymbol{D_p}$ and $b\in\boldsymbol{D_q}$, then a and b satisfy the condition of Definition 2.1 and hence are zero dividers.

If some of c_{ijk}=0 and/or t_{ik}=0, then e_k=0 and we say that the corresponding equation degenerates. The same is valid if some of c_{ijk}=0 and/or t_{ik}=0 are zero dividers.

We exclude MQP problems with degenerated equations from our consideration since the set of values of variables satisfying either the single or the system of degenerated equations can be found effectively. Hence the presence of these equations does not add the extra complexity of the MQP problem.

To avoid the degeneration of MQP equations, zero dividers and zero element should be removed from the set $\boldsymbol{Z_n}$. We reckon this problem being technical since we are considering cases when factorization of n is feasible and the prime factors of n are known. Hence we assume that we are able to construct effectively a non-degenerated MQP system of equations and hence formulate non-degenerate MQP problem in some subset $\boldsymbol{Z_n}'$ of $\boldsymbol{Z_n}$ where zero element and zero dividers are removed.

For example if $n=pq$, then we can choose either $\boldsymbol{Z_n}'=\boldsymbol{Z_n}\backslash\{0 \cup \boldsymbol{D_p}\}$ or $\boldsymbol{Z_n}'=\boldsymbol{Z_n}\backslash\{0 \cup \boldsymbol{D_q}\}$, where $\cup$ is a union of sets.

We prove two lemmas concerning the set $\boldsymbol{Z_n}'$ but in the case when $n=pq$. The proof in the general case is performed in a very similar way but requires more manipulations.

Lemma 2.2. The subset $\boldsymbol{Z_n}'$ has no zero dividers.

▼Proof. Let a be a non-trivial zero divider in $\boldsymbol{Z_n}'$. Then there exists $b\neq 0$ in $\boldsymbol{Z_n}'$ such that $ab=0 \mod n$. Then $ab=kn=kpq$ for certain integer k. Since p, q are primes, then a and b should satisfy the following identities $a=k_1p$ ($k_1<q-1$) and $b=k_2q$ ($k_2<p-1$), where $k_1k_2=k$. But then b is divisible by q and is in $\boldsymbol{D_q}$. Hence $b\notin \boldsymbol{Z_n}'$. The obtained contradiction proves the lemma. ▲

Lemma 2.3. The subset $\boldsymbol{Z_n}'$ is a multiplicative monoid.

▼Proof. According to the definition, multiplication operation is associative in $\boldsymbol{Z_n}$. The unity element is 1 both in $\boldsymbol{Z_n}$ and $\boldsymbol{Z_n}'$. We must prove that the subset $\boldsymbol{Z_n}'$ is closed, i.e. if a and b are in $\boldsymbol{Z_n}'$ then ab is also in $\boldsymbol{Z_n}'$. Since q is prime then, $\gcd(a,q)=1$ and $\gcd(b,q)=1$. Using the extended euclidean algorithm we can find integers i_1, i_2, j_1 and j_2 such that

$$i_1a+i_2q=1, j_1b+j_2q=1.$$

By expressing i_1a and j_1b and taking their product we have

$$i_1aj_1b=i_1j_1ab=1-i_2q-j_2q+i_1j_1q^2.$$

The right-hand side of the last equation is not divisible by q and hence i_1j_1ab is also not divisible by q. Then ab is also not divisible by q. This means that ab is also in $\boldsymbol{Z_n}'$. This proves the lemma. ▲

We can define the MQP system of equations over the monoid $\boldsymbol{Z_n}$ or submonoid $\boldsymbol{Z_n}'$ by assigning the values of constants c_{ijk}, t_{ik}, and e_k either in $\boldsymbol{Z_n}$ or in $\boldsymbol{Z_n}'$. Hence we name both $\boldsymbol{Z_n}$ and $\boldsymbol{Z_n}'$ as platform (sub)monoids of the MQP system. Since power monomials are in exponents, then due to Oiler theorem, multiplication of variables must be performed by modulo $\phi(n)$, where $\phi(\ )$ is Oiler's totient function. Hence power monomials are defined over the monoid $\boldsymbol{Z}_{\phi(n)}$.

In our construction, we use the same monomials in both equations (2.1) and (2.2) and hence we denote them by the same symbols x_ix_j. We denote the MQP system of equations over $\boldsymbol{Z_n}$ by MQP($\boldsymbol{Z_n}$) and over $\boldsymbol{Z_n}'$ by MQP($\boldsymbol{Z_n}'$). As it was pointed out above, MQP($\boldsymbol{Z_n}'$) is a non-degenerate system. Further we will consider non-degenerate MQP systems. Analogously to MQ($\boldsymbol{Z}_2$) system, we define bilinear power terms $c_{ijk}^{\,y_iy_j}$ of MQP($\boldsymbol{Z_n}'$) in the set $\boldsymbol{Z_n}'\times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$, where $c_{ijk}\in \boldsymbol{Z_n}'$ and $c_{ijk}^{\,y_iy_j}\in \boldsymbol{Z_n}'$.

Analogously to the MQ($\boldsymbol{Z}_2$) problem, we formulate the decisional and computational versions of the MQP($\boldsymbol{Z_n}'$) problem. Taking in mind that we renamed the variables $\{y_i\}$ in (2.2) by $\{x_i\}$ and that constants $\{c_{ijk}\}$, $\{t_{ik}\}$ and $\{e_k\}$ are defined in $\boldsymbol{Z_n}'$ we can formulate the following definitions.

Definition 2.4. The computational MQP($\boldsymbol{Z_n}'$) problem is to find the unknown variable $\{x_i\}$ values when the constant $\{c_{ijk}\}$, $\{t_{ik}\}$ and $\{e_k\}$ values are given.

Definition 2.5. The decisional MQP($\boldsymbol{Z_n}'$) problem is to give YES answer to the question: are there any input variable $\{x_i\}$ binary values satisfying MQP($\boldsymbol{Z_n}'$) system, when the constant $\{c_{ijk}\}$, $\{t_{ik}\}$ and $\{e_k\}$ values in $\boldsymbol{Z_n}'$ are given.

The aim of this paper is to prove that the decisional version of MQP($\boldsymbol{Z_n}'$) problem is NP-complete. Since $\boldsymbol{Z_n}'$ is a submonoid of $\boldsymbol{Z_n}$, then MQP($\boldsymbol{Z_n}'$) problem is a restriction of MQP($\boldsymbol{Z_n}$) and hence MQP($\boldsymbol{Z_n}$) is also NP-complete.

3. The proof of NP-completeness

NP-completeness will be proved by showing that the decisional version of MQP($\boldsymbol{Z_n}$) problem is in NP class and by constructing two sequential polynomial-time reductions from the general NP-complete MQ($\boldsymbol{Z}_2$) problem to the MQP($\boldsymbol{Z_n}'$) problem. These reductions will satisfy the following conditions: 1) given any instance I_{1i} of the MQ($\boldsymbol{Z}_2$) problem, we construct the corresponding instance I_{3k} of the MQP($\boldsymbol{Z_n}'$) problem using intermediate instance I_{2j} of some intermediate problem defined below; 2) the answer of decision problem for any instance I_{1i} is YES if and only if the answer for the corresponding instance I_{3k} (I_{2j}) is YES.

The intermediate problem is the MQP($\boldsymbol{Z}_3^*$) problem, where $\boldsymbol{Z}_3^*=\{1, 2\}$ is a multiplicative group of residues modulo 3. This intermediate problem is not required for the proof of NP-completeness of MQP($\boldsymbol{Z_n}'$) but it is introduced only for methodical interest. We will show that all instances I_1 of MQ($\boldsymbol{Z}_2$) problem have one-to-one correspondence with the instances I_2 of MQP($\boldsymbol{Z}_3^*$). Moreover we will show that they both are equivalent NP-complete problems.

By inspection of the system of equations (2.2) we see that the MQP($\boldsymbol{Z_n}$') problem's satisfiability verification is performed by the same number of multiplication and powering operations as of MQ($\boldsymbol{Z}_2$) problem's (2.1) satisfiability verification using the sum and multiplication operations respectively. Since it is done in polynomial time for the MQ($\boldsymbol{Z}_2$) problem, the same is valid for the MQP($\boldsymbol{Z_n}$') problem. Hence MQP($\boldsymbol{Z_n}$') is in NP class.

We denote the multiplication operations in $\boldsymbol{Z}_3^*$ and $\boldsymbol{Z_n}$' by $\cdot$ and •, respectively. Recall that multiplication operation in $\boldsymbol{Z}_3^*$ is performed by modulo 3 and multiplication operation in $\boldsymbol{Z_n}$' by modulo n. Constants and variables in MQ($\boldsymbol{Z}_2$), MQP($\boldsymbol{Z}_3^*$) and MQP($\boldsymbol{Z_n}$') systems of equations we denote by triplets (a_{ijk}, x_i, x_j), (b_{ijk}, x_i, x_j) and (c_{ijk}, x_i, x_j) respectively. For convenience, we will consider the MQP($\boldsymbol{Z}_3^*$) problem in the form of system (2.2) with constants b_{ijk} written instead of c_{ijk}. As it was mentioned above, to perform reductions we interpret the terms as a functions τ_1, τ_2 and τ_3 providing a mapping from domain set to the range set, and having the following form:

$$\tau_1 : \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \to \boldsymbol{Z}_2,\ \tau_1(a_{ijk}, x_i, x_j)=a_{ijk}x_ix_j, \quad (3.1)$$

$$\tau_2 : \boldsymbol{Z}_3^* \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2\ \ \boldsymbol{Z}_3^*,\ \tau_2(b_{ijk}, x_i, x_j)= b_{ijk}^{x_ix_j}, \quad (3.2)$$

$$\tau_3 : \boldsymbol{Z_n}' \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \to \boldsymbol{Z_n}',\ \tau_3(c_{ijk}, x_i, x_j)= c_{ijk}^{x_ix_j}. \quad (3.3)$$

Notice that according to our construction the power monomial x_ix_j in MQP($\boldsymbol{Z}_3^*$) is computed using multiplication operation in $\boldsymbol{Z}_2$. The same holds true for MQP($\boldsymbol{Z_n}$').

In this section we prove that any instance of MQ($\boldsymbol{Z}_2$) problem is polynomial-time reducible to MQP($\boldsymbol{Z_n}$') problem using two subsequent reductions ρ_1 and ρ_2 from MQ($\boldsymbol{Z}_2$) to MQP($\boldsymbol{Z}_3^*$) and from MQP($\boldsymbol{Z}_3^*$) to MQP($\boldsymbol{Z_n}$') problem, respectively.

We express the polynomial-time reduction ρ_1 in the following way

$$\rho_1 : \text{MQ}(\boldsymbol{Z}_2) \Rightarrow \text{MQP}(\boldsymbol{Z}_3^*). \quad (3.4)$$

This reduction will be defined if we transform the terms of MQ($\boldsymbol{Z}_2$) system to the terms of MQP($\boldsymbol{Z}_3^*$) system and transform $\oplus$ (sum) operation of terms in MQ($\boldsymbol{Z}_2$) to $\cdot$ (multiplication) operation of terms in MQP($\boldsymbol{Z}_3^*$). Then we transform every instance I_{1i} of MQ($\boldsymbol{Z}_2$) to the corresponding instance I_{2j} of MQP($\boldsymbol{Z}_3^*$). Recall that we are considering the only bilinear terms since the linear terms are the partial case of the formers. We must construct the following mappings: ∂_1 for term domains and φ_1 for term ranges, respectively

$$\partial_1: \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \to \boldsymbol{Z}_3^* \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2. \quad (3.5)$$

$$\varphi_1 : \boldsymbol{Z}_2 \to \boldsymbol{Z}_3^*. \quad (3.6)$$

We define the following mapping rule for φ_1

$$\varphi_1(0)=1,\ \varphi_1(1)=2. \quad (3.7)$$

For example, let we have the bilinear term $a_{ijk}x_ix_j=x_ix_j=1$, when $a_{ijk}=1$. Then $\varphi_1(a_{ijk}x_ix_j)=2^{x_ix_j}$. Let we have two terms $a_1=a_{ijk}\,x_ix_j$, $a_2=a_{rsk}\,x_rs_j$ in MQ($\boldsymbol{Z}_2$) and corresponding two terms $b_1=\varphi_1(a_1)= b_{ijk}^{x_ix_j}$, $b_2=\varphi_1(a_2)= b_{rsk}^{x_rx_s}$ in MQP($\boldsymbol{Z}_3^*$). Having defined binary sum operation $\oplus$ of terms in $\boldsymbol{Z}_2$ and binary multiplication operation $\cdot$ of power terms in $\boldsymbol{Z}_3^*$ we characterize the reduction ρ_1 in Table 1.

Table 1. The reduction ρ_1 characterization

a_1	a_2	$a=a_1\oplus a_2$	$b_1=\varphi_1(a_1)$	$b_2=\varphi_1(a_2)$	$b=b_1\cdot b_2$
0	0	0	1	1	1
0	1	1	1	2	2
1	0	1	2	1	2
1	1	0	2	2	1

Lemma 3.1. The function φ_1 is an isomorphism from the additive group in $\boldsymbol{Z}_2$ to the multiplicative group $\boldsymbol{Z}_3^*$.

▼Proof. From direct observation of Table 1, we can deduce that for any a_1, a_2 in $\boldsymbol{Z}_2$ and for $a=a_1\oplus a_2$, there exists an unique $b=b_1\cdot b_2$ in $\boldsymbol{Z}_3^*$ such that $\varphi_1(a_1\oplus a_2)=\varphi_1(a)=b=b_1\cdot b_2= \varphi_1(a_1)\cdot\varphi_1(a_2)$. ▲

All bilinear, linear terms and right-hand side constants of (2.1) can be transformed to corresponding bilinear, linear power terms and right-hand side constants of (2.2) using isomorphism φ_1. Then every instance I_{1i} of the MQ($\boldsymbol{Z}_2$) problem represented by the system (2.1) can be by one-to-one transformation reduced to certain instance I_{2i} of the MQP($\boldsymbol{Z}_3^*$) problem represented by the system (2.2) and vice versa.

Lemma 3.2. The answer of the decisional MQ($\boldsymbol{Z}_2$) problem for every instance I_{1i} is YES if and only if the answer of the decisional MQP($\boldsymbol{Z}_3^*$) problem for corresponding instance I_{2j} is YES.

▼Proof. Let we have an instance I_{1i} defined by some collection of constants $\{a_{ijk}\}$, $\{l_{ik}\}$,$\{d_k\}$. Let there is a binary vector (x_1^s, …, x_N^s) satisfying MQ($\boldsymbol{Z}_2$) system. Hence this vector provides the answer YES for decisional MQ($\boldsymbol{Z}_2$) problem. For example, let us take a k-th equation in (2.1). If d_k=0, then there must exist an even number of terms $a_{ijk}\,x_ix_j=x_i^sx_j^s$ such that $x_i^sx_j^s$=1. We can transform this equation to the corresponding equation of the MQP($\boldsymbol{Z}_3^*$) system using the isomorphism φ_1, since it is operation preserving mapping. Hence we obtain the corresponding k-th equation with bilinear power terms $\varphi_1(a_{ijk}x_i^sx_j^s)= b_{ijk}^{x_i^s x_j^s}$. Then according to Table 1, for all $a_{ijk}x_i^sx_j^s=x_i^sx_j^s=1$ bilinear power term $b_{ijk}^{x_i^s x_j^s}$ = $2\in\boldsymbol{Z}_3^*=\{1,2\}$. Since the number of such multiplicative terms (which are equal to 2) is even, then their total product is equal to 1, i.e. e_k=1=d_k+1, where d_k and e_k are the right-hand sides of (2.1) and (2.2) respectively. This consideration can be generalized to any equation of (2.1) and to any value $d_k \in \boldsymbol{Z}_2=\{0,1\}$. Hence using the fact that φ_1 is isomorphism (i.e. operation preserving mapping) we can transform any instance of I_{1i} with answer YES to the corresponding instance of I_{2j} with the same answer YES. Notice also that the number of instances of I_1 and I_2 is the same.

Let I_{2j} be satisfied. Then applying unique inverse isomorphism φ_1^{-1} we find that I_{1i} is also satisfied. ▲

Referencing to the above presented results, we proved the following theorem.

Theorem 3.3. The MQP(Z_3^*) problem is NP-complete.

We also proved that the MQ($\boldsymbol{Z}_2$) problem is equivalent to the MQP($\boldsymbol{Z}_3^*$) problem: the sets of instances with answer YES in MQ($\boldsymbol{Z}_2$) and MQP($\boldsymbol{Z}_3^*$) have the same cardinality.

We define the second polynomial-time reduction ρ_2 in the following way

$$\rho_2 : \mathrm{MQP}(\boldsymbol{Z}_3^*) \Rightarrow \mathrm{MQP}(\boldsymbol{Z}_n'). \quad (3.8)$$

Analogously to previous reduction, we define transformation of terms of the MQ($\boldsymbol{Z}_3^*$) system to the terms of the MQP($\boldsymbol{Z}_n$') system and transformation of · (multiplication) operation in the MQ($\boldsymbol{Z}_3^*$) system to • (multiplication) operation in the MQP($\boldsymbol{Z}_n$') system. We construct two functions ∂_2 and φ_2 for transformation of the term domains and ranges

$$\partial_2 : \boldsymbol{Z}_3^* \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \rightarrow \boldsymbol{Z}_n' \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2, \quad (3.9)$$

$$\varphi_2 : \boldsymbol{Z}_3^* \rightarrow \boldsymbol{Z}_n'. \quad (3.10)$$

We see that unlike ∂_1 and φ_1, functions ∂_2 and φ_2 perform mappings “in” $\boldsymbol{Z}_n$' but not “onto” $\boldsymbol{Z}_n$', if n>4. We define a subset S_n={1, n-1} in $\boldsymbol{Z}_n$', being a range set for ∂_2 and φ_2 instead of $\boldsymbol{Z}_n$' in order to construct one-to-one functions ∂_2 and φ_2.

Lemma 3.4: The subset $\boldsymbol{S}_n$ with defined binary operation • is a subgroup of $\boldsymbol{Z}_n$'.

▼Proof. It is evident that 1 is neutral element both in $\boldsymbol{Z}_n$' and $\boldsymbol{S}_n$. We prove that the set $\boldsymbol{S}_n$ is closed under multiplication operation • in $\boldsymbol{Z}_n$' and n-1 has its inverse in $\boldsymbol{S}_n$. Hence it is sufficient to show that $(n\text{-}1)^2$=1. Using the definition of multiplication operation • in $\boldsymbol{Z}_n$' we have: $(n-1)^2=(n-1)\bullet(n-1)=(n-1)(n-1) \bmod n = n^2-2n+1 \bmod n = 1$. ▲

We define the functions ∂_2 and φ_2 we define as one-to-one mappings substituting $\boldsymbol{Z}_n$' by subset $\boldsymbol{S}_n$ in (3.9) and (3.10). We define the following mapping rule for φ_2

$$\varphi_2: \boldsymbol{Z}_3^* \rightarrow \boldsymbol{S}_n \,;\ \varphi_2(1)=1,\ \varphi_2(2)=n\text{-}1. \quad (3.11)$$

In this way we can define the MQP problem over subgroup $\boldsymbol{S}_n$, i.e. MQP(Sn), by choosing appropriate coefficients in (2.2).

Analogously to the reduction ρ1, it is evident that the reduction ρ2 from the MQP(Z3*) to the MQP(Sn) is performed in polynomial time. Then having defined multiplication operations · and •, we characterize the reduction ρ_2 in Table 2.

Table 2. The reduction ρ_2 characterization

b_1	b_2	$b=b_1 \cdot b_2$	$c_1=\varphi_2(b_1)$	$c_2=\varphi_2(b_2)$	$c=c_1 \cdot c_2$
1	1	1	1	1	1
1	2	2	1	n-1	n-1
2	1	2	n-1	1	n-1
2	2	1	n-1	n-1	1

Lemma 3.5. The function φ_2 defined in (3.11) is isomorphic.

▼Proof. The proof is analogous to that of Lemma 3.1 and follows from Table 2.▲

The composition of functions φ_1 and φ_2 corresponding to reductions ρ_1 and ρ_2 is presented in Table 3.

Table 3. The composition of functions φ_1 and φ_2

Domain $\boldsymbol{Z}_2$	Range $\varphi_1(Z_2)=\boldsymbol{Z}_3^*$	Range $\varphi_2(\boldsymbol{Z}_3^*)=\varphi_2(\varphi_1(Z_2))=\boldsymbol{S}_n$
0	1	1
1	2	n-1

Since φ_2 is a one-to-one function, then analogously to previous reduction every instance I_{2i} of the decisional MQP($\boldsymbol{Z}_3^*$) problem can be transformed by one-to-one mapping to certain instance I_{3i} of the decisional MQP($\boldsymbol{S}_n$) problem and vice versa.

Lemma 3.6. The answer of the decisional MQP($\boldsymbol{Z}_3^*$) problem for every instance I_{2i} is YES if and only if the answer of the decisional MQP($\boldsymbol{S}_n$) problem for corresponding instance I_{3j} is YES.

▼Proof. The proof is analogous to the proof of Lemma 3.2, taking into account that φ_2 is an isomorphism. ▲

Hence we proved the following theorem.

Theorem 3.7. The MQP($\boldsymbol{S}_n$) problem is NP-complete.

Since all variables $\{x_i\}$ take values from $\boldsymbol{Z}_2$={0,1} of the corresponding problems MQ($\boldsymbol{Z}_2$), MQP($\boldsymbol{Z}_3^*$) and the following inclusions Sn⊂ Zn'⊂Zn are taking place, we can make the following corollary.

Corollary 3.8. The MQP($\boldsymbol{Z}_n$') and MQP($\boldsymbol{Z}_n$) problems are NP-complete.

4. Discussions

The system of MQP equations (2.2) can be considered as some MQP function F with parameters $\{c_{ijk}\}$, $\{t_{ik}\}$ and arguments $\{y_i\}$. The value of function F is a vector (e_1, …, e_M). The direct value of F (i.e. of MQP) computation corresponds to the vector (e_1, …, e_M) value computation, when the values of constants $\{c_{ijk}\}$, $\{t_{ik}\}$ and arguments $\{y_i\}$ are given. The solution of (2.2) with respect to $\{y_i\}$, when $\{c_{ijk}\}$, $\{t_{ik}\}$ and $\{e_k\}$ are given, is the inversion of the function F. In Section 3 we showed that direct value computation of F is performed effectively (in polynomial time), but its inverse value computation corresponds to the NP-complete problem. Putting aside the cardinal question either polynomial time problem is not equivalent to non-deterministic polynomial time problem (i.e. P≠NP) or not and according to convention we can assume that MQP(Z_n) is a candidate one-way function.

Since MQP($\boldsymbol{Z_n}$) and MQ($\boldsymbol{Z}_2$) problems have many similarities the analysis of actual complexity of MQP($\boldsymbol{Z_n}$) problem we perform by referencing to the complexity of MQ($\boldsymbol{Z}_2$) problem which is more or less investigated so far. Grobner basis algorithm [2] and its modifications are classic methods to solve MQ problems over the fields, e.g. XL or XSL methods are effective if MQ system of equations is sparse and overdefined [3, 4]. The other recently appeared approach to solve MQ problems is a SAT-solvers technique using polynomial time reductions from a MQ problem to the SAT problem. In particular, in [1] it was shown that if the system of equations is sparse or over-defined, then the SAT-solvers technique works faster than brute-force exhaustive search. If the system is both sparse and over-defined, then this system can be solved quite effectively. In the case if the system is neither sparse nor over-defined, the efficiency of SAT-solvers significantly decreases. In general, if we are considering general MQ($\boldsymbol{Z}_2$) problem, we obtain long XOR terms which add a big number of disjunctors. This phenomena causes a difficulties for SAT-solvers [5].

Let $n=p$ be a prime number. Then $\boldsymbol{Z}_p^*=\{1, 2, \ldots, p\text{-}1\}$ is a multiplicative group. Let us consider a computational version of the MQP($\boldsymbol{Z}_p^*$) problem. Then for every MQP equation over $\boldsymbol{Z}_p^*$ we can take a discrete logarithm with respect to the base of any generator in $\boldsymbol{Z}_p^*$. As a consequence, due to Fermat theorem we obtain a system of multivariate quadratic (MQ) equations defined over the ring $\mathcal{Z}_{p\text{-}1}$. Since the MQ problem over the field is NP-complete and is hard for certain class of instances, we can expect that MQ problem over the ring is no less hard due to the fact that not all elements in the ring have they inverses, i.e. division operation can't be performed with some elements of the ring. This simply means that computations in the ring are more complex than in the field. For example, it is widely recognized that the solution of linear system of equations over the ring is more complex than over the field.

Faugere and Joux used Grobner basis algorithms for algebraic cryptanalysis of hidden field equations (HFE) cryptosystems [6]. According to this analysis they concluded that solution of MQ($\boldsymbol{Z}_2$) systems like (2.1) with the number of equations and variables more that 80 using Grobner basis algorithms is hopeless.

In our case, we have a monoid $\boldsymbol{Z_n}'$ ($\boldsymbol{Z_n}$) instead of the field $\boldsymbol{Z}_2$. Since $\boldsymbol{Z_n}'$ has no generators, there is no polynomial-time transformation from MQP($\boldsymbol{Z_n}'$) system to some MQ system (the discrete logarithm operation cannot be applied). This means that known algorithms for solution of MQ problems cannot be applied as well.

So far we do not know any algorithms being able to deal with MQP systems of equations and we have no imagination yet on how to try to solve them. We think it could be a matter of further investigations.

Since MQP($\boldsymbol{Z_n}$) problem is NP-complete, the further step should be to create a candidate one-way function (OWF) based on this problem being suitable for cryptographic applications. After that, the provable security property will be proved for existing protocols and the new ones could be created on this base.

The effective realization of these computations is based on the fact that we use platform monoid $\boldsymbol{Z_n}$ of low cardinality n. The cardinality n can be chosen as a product of two small primes pq, say $n\in\{6, 10, 15, 21, \ldots\}$. Then power and multiplication operations could be performed using lookup tables. The lookup table for multiplication operation consists of 20x20=400 entries and for power operation of 20x12=240 entries when n=21. If we consider the MQP system (2.2) with 80 equations and variables, then the number of look-up power operations, multiplications and sum operations does not exceed 6500, 6500 and 3280, respectively. Hence according to the OWF definition the direct value computation can be performed quite effectively and considerably more effective than in the case of classical cryptographic methods based on arithmetic with large integers in high order cyclic groups or high characteristic rings and elliptic curve groups.

Acknowledgements

The author acknowledges the reviewers for very valuable comments and suggestions for paper improvement.

Many thanks especially to one of them who showed a great patient correcting language, grammar and style. Moreover, the valuable advices were presented improving statements enunciation and consistency. The proof of Lemma 3.2 became more transparent and clear as it is presented in the existing form due to the proposal of this and other reviewers.

References

[1] **G. B. Bard, N. T. Courtois, C. Jefferson.** Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers, Cryptology ePrint Archive, Report 2007/024. Available at http://eprint.iacr.org/2007/024.pdf.

[2] **B. Buchberger.** *Gröbner-bases: an algorithmic method in polynomial ideal theory.* In *Recent Trends in*

Multidimensional Systems Theory, Reidel Publishing Company, 1985, pp. 184-232.

[3] **N. T. Courtois, A. Klimov, J. Patarin, A. Shamir.** *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Eurocrypt 2000, LNCS 1807, 2000, pp. 392-407.

[4] **N. T. Courtois, J. Pieprzyk.** *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, Asiacrypt 2002, LNCS 2501, 2002, pp. 267-287.

[5] **N. Creignou, H. Daude.** *Satisfiability threshold for random xor-cnf formulas*. Discrete Applied Mathematics, 96-97, 1999, pp. 41-53.

[6] **J.-C. Faugere, A. Joux.** *Algebraic Cryptanalysis of Hidden Field Equations (HFE) Cryptosystems Using Grobner Bases*, Crypto 2003, LNCS 2729, 2003, pp. 44-60, 2003.

[7] **M. Garey, D. Johnson.** *Computers and Intractability: a Guide to Theory of NP-Completeness*, H. Freeman, New York, 1979.

[8] **K. Luksys, P. Nefas.** *Matrix Power S-Box Analysis*. In: Advanced Studies in Software and Knowledge Engineering. No. 4, Information Science & Computing, No 4, Suppl. to: Informations Technologies and Knowledge, Sofia: ITHEA. ISSN 1313-0455, vol. 2, 2008, pp. 97–102 (2008).

[9] **R. Merkle, M. Hellman.** *Hiding information and signatures in trapdoor knapsacks*, IEEE Transactions on Information Theory, 24, 1978, pp. 525-530. Available at http://ieeexplore.ieee.org/search/freesrchabstract.jsp?tp=&arnumber=1055927.

[10] **A. Myasnikov, V. Shpilrain, A. Ushakov.** *Group-based Cryptography*, Birkhäuser Verlag, 2008.

[11] **J. Patarin**. *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new Families of Asymmetric Algorithms.* Eurocrypt 1996, 1996, pp. 33-48. Available at http://www.minrank.org/hfe.pdf.

[12] **J. Patarin, L. Goubin.** *Trapdoor One-Way Permutations and Multivariate Polynomials.* Proceedings of the First International Conference on Information and Communication Security, LNCS 1334, 1997, pp. 356-368.

[13] **E. Sakalauskas.** One Digital Signature Scheme in Semimodule over Semiring. Informatica, 16, 2007, pp. 383-394.

[14] **E. Sakalauskas, K. Lukšys.** *Matrix Power S-Box Construction.* Cryptology ePrint Archive: Report 2007/214. Available at http://eprint.iacr.org/2007/214.

[15] **E. Sakalauskas, N. Listopadskis, P. Tvarijonas.** *Key Agreement Protocol (KAP) Based on Matrix Power Function*. In: Advanced Studies in Software and Knowledge Engineering. No. 4, Information Science & Computing, No 4, Suppl. to: Informations Technologies and Knowledge, Sofia: ITHEA. ISSN 1313-0455, vol. 2, 2008, pp. 92-96.

[16] **P. V. Shor.** *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM J. Computing, 26, 1997, pp. 1484-1509. Available at: http://arXiv.org/abs/quant-ph/9508027.

[17] **C. Wolf, B. Preneel.** *Equivalent Keys in HFE, C*, and variations*. Cryptology ePrint Archive, Report 2004/360. Available at: http://eprint.iacr.org.

Received October 2011.