KAUNAS UNIVERSITY OF TECHNOLOGY

ALEKSEJUS MICHALKOVIČ

ASYMETRIC ENCRYPTION SYSTEM BASED ON NON-COMMUTING ALGEBRAIC SYSTEMS CREATION AND INVESTIGATION

Summary of Doctoral Dissertation
Technological Sciences, Informatics Engineering (07T)

2015, Kaunas

The dissertation was prepared at Kaunas University of Technology, Faculty of Mathematics and Natural Sciences, Department of Applied Mathematics in 2010–2014. Scientific research was supported by Lithuanian State Science and Studies Foundation.

Scientific supervisor:
Prof. Dr. Eligijus SAKALAUSKAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).

Dissertation Defense Board of Informatics Engineering Science field:

Chairman: Prof. Dr. Robertas DAMAŠEVIČIUS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).

Members: Prof. Dr. Habil. Antanas ČENYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),

Prof. Dr. Zenonas NAVICKAS (Kaunas University of Technology, Physical Sciences, Mathematics – 01P),

Prof. Dr. Habil. Minvydas Kazys RAGULSKIS (Kaunas University of Technology, Physical Sciences, Informatics – 09P),

Prof. Dr. Julius ŽILINSKAS (Vilnius University, Technological Sciences, Informatics Engineering – 07T).

The official defense of the dissertation will be held at 10 a.m. on 3rd March 2015 at the public meeting of the Board of Informatics Engineering Science field in the Dissertation Defense Hall at the Central Building of Kaunas University of Technology.

Address: K. Donelaičio St. 73, room No. 403, LT-44029, Kaunas, Lithuania
Phone (+370) 37 300042, Fax. (+370) 37 324144, e-mail doktorantura@ktu.lt

The summary of the dissertation was sent out on 3rd February 2015.

The dissertation is available at the library of Kaunas University of Technology (K. Donelaičio St. 20, LT-44239 Kaunas, Lithuania).

KAUNO TECHNOLOGIJOS UNIVERSITETAS

ALEKSEJUS MICHALKOVIČ

ASIMETRINIO ŠIFRAVIMO SISTEMOS, PAREMTOS NEKOMUTATYVIAIS KRIPTOGRAFIJOS METODAIS, SUKŪRIMAS IR SAVYBIŲ TYRIMAS

Daktaro disertacijos santrauka
Technologijos mokslai, informatikos inžinerija (07T)

2015, Kaunas

Disertacija rengta 2010–2014 metais Kauno technologijos universitete, Matematikos ir gamtos mokslų fakultete, Taikomosios matematikos katedroje. Mokslinius tyrimus rėmė Lietuvos valstybinis mokslo ir studijų fondas.

Mokslinis vadovas:
prof. dr. Eligijus SAKALAUSKAS (Kauno technologijos universitetas, tecnnologijos mokslai, informatikos inžinerija – 07T).

Informatikos inžinerijos mokslo krypties disertacijos gynimo taryba:

Pirmininkas: prof. dr. Robertas DAMAŠEVIČIUS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Nariai: prof. habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. dr. Zenonas NAVICKAS (Kauno technologijos universitetas, fiziniai mokslai, matematika – 01P),

prof. habil. dr. Minvydas Kazys RAGULSKIS (Kauno technologijos universitetas, fiziniai mokslai, informatika – 09P),

prof. dr. Julius ŽILINSKAS (Vilniaus universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija ginama viešame informatikos inžinerijos mokslo krypties tarybos posėdyje, kuris įvyks 2015 m. kovo 3 d., 10 val. Kauno technologijos universiteto centrinių rūmų disertacijų gynimo salėje.

Adresas: K. Donelaičio g. 73-403, Kaunas, Lietuva.
Tel. (+370 37) 300042, faksas (+370 37) 324144, el. paštas doktorantura@ktu.lt

Disertacijos santrauka išsiusta 2015 m. vasario 3 d.

Su disertacija galima susipažinti:
Kauno technologijos universiteto bibliotekoje (K. Donelaičio g. 20, LT-44239 Kaunas, Lietuva).

GLOSSARY

Agent – a program, which is used for client services, i.e. provides a secure way to encrypt and decrypt data.

Algebraic cryptanalysis – methods of cryptanalysis, which are aimed at gathering information about user‘s private key from his public key by analyzing algebraic equations used to mathematically link both keys.

Asymmetric encryption protocol – an algorithm, which is used to encrypt plaintext and decrypt ciphertext by using a pair of mathematically linked keys.

Conjugation equation – matrix equation $X^{-1}AX = B$, where matrices A and B are given.

Commutation equation – matrix equation $AX = XB$, where matrices A and B are given.

CSP – conjugation search problem.

Cryptographic primitive – key exchange, encryption or e-signature protocol.

DLA – discrete logarithm attack.

DLP – discrete logarithm problem.

ECC – elliptic curve cypher.

Ideal of semigroup – a subgroup, which is closed under multiplication, for all elements of initial semigroup.

Lookup table – a table which contains all possible values of an algebraic operation.

Matrix power = power matrix.

MP exponent – the value of MPF.

MPAC – matrix power asymmetric cypher.

MPF – matrix power function.

MQ problem – the problem of solving a system of multivariate quadratic equations.

MMQ problem – the problem of solving a matrix equation $XAY = B$, where matrices A and B are known and matrices X and Y are unknown.

NP-complete problem – a problem is in NP class and every other problem in this class can be reduced to this problem in polynomial time.

NP class – a set of decisional problems, which can be verified in polynomial time.

Number ring – a ring that has integers as elements.

One-way function – a function, that can be computed in polynomial time, but is hard to invert, i.e. it is impossible to find an argument of the function in polynomial time if the value is known.

Platform ring – a ring of square matrices which contains possible values of platform matrix Q and MP exponent E.

Polynomial time – the dependence of computational time on system parameters is polynomial.

Power ring – a ring of square matrices, which contains arguments of MPF, i.e. matrices X and Y.

Power matrix – an argument of MPF (matrix X or Y).

RSA – asymmetric encryption protocol, named after its creators (Rivest, Shamir, Adleman).

Symmetric encryption protocol – an algorithm which is used to encrypt plaintext and decrypt ciphertext by using the same secret key.

STR – key exchange protocol, named after its creators (Sakalauskas, Tvarijonas, Raulynaitis).

Statistical cryptanalysis – methods of cryptanalysis, which are aimed at predicting the value of the function using analysis of one-way function based pseudorandom number generator.

NOTATIONS

$\oplus$ – XOR operation (bitwise sum modulo 2).

$|A|$ – the order of set A.

${}^{X}Q$ – matrix Q is powered by matrix power X from the left.

Q^{Y} – matrix Q is powered by matrix power Y from the right.

$\varphi(n)$ – Euler's totient function of n.

$\lambda(n)$ – Carmichael function of n.

$\gcd(a, b)$ – gratest common divider of a and b.

$Id(\boldsymbol{S})$ – an ideal of a semigroup $\boldsymbol{S}$.

L – security level.

m – the order of square matrices.

n – defines the size of multiplicative group $\boldsymbol{Z}_n^*$ or semigroup $\boldsymbol{Z}_n^{\#}$.

p – a prime number which defines a multiplicative semigroup.

r – defines the size of a number ring.

$\boldsymbol{Z}_n$ – a finite ring that has integers from 0 to $n - 1$ as elements. Addition and multiplication in this ring are performed modulo n.

$\boldsymbol{Z}_n^*$ – a multiplicative group that contains integers from 0 to $n - 1$ which are relatively prime with n.

$\boldsymbol{Z}_n^{\#}$ - a multiplicative semigroup which is a union of $\boldsymbol{Z}_n^*$ and $Id(\boldsymbol{Z}_n)$.

1. INTRODUCTION

Our everyday life cannot be imagined without information technology. Electronic mail, social networks, e-banking, e-voting – these are only a small part of services offered to an average user. Often users send out secret information using the Internet. This process needs to be safe, since public knowledge of some secret information could be hazardous not only to user himself, but also to his friend, or sometimes even the government. It is clear that depending on a user and on the importance of information the security of the cipher can differ. It may only be a matter of using a password to protect information against kids, but protecting secret information against government spies is much more complicated. The latter case is the focus of cryptography. Cryptographic security includes such aspects as confidentiality, authenticity, integrity of information, user identification [1]. Such cryptographic primitives as key exchange protocols, data encryption protocols, digital signatures are created for these purposes.

Cryptography also drew much attention during the World War II, when many attempts to break the world famous Enigma cipher were made. This problem was first solved by Alan Turing, who is now considered to be one of the founders of modern cryptography. The Enigma machine is an example of a symmetric cipher, i.e. this machine used the same key for encrypting and decrypting a secret message. For this reason the symmetric encryption protocols can be called as “cryptographic safes”, i.e. anyone who possesses a key can put something in a safe and take something out of the safe. However, if Bob wants to send a message to Carol, he has to agree on a common key with her, which means that Bob now has to store two keys: common key with Alice and common key with Carol. This is an obvious drawback of the symmetric encryption. Note also, that both parties must agree on a common key using secret channels, since otherwise this key would also be available to other users [2].

These problems can be solved using another branch of cryptography – asymmetric encryption, which embraced in 1976. This type of protocols uses two kinds of keys: a secret key and a public key. The secret key is known only to the owner of the key and the public key is mathematically linked to the secret key and is known to any user. One of the main requirements for the public key is that this key should not give away any information about a secret key. Since in this case different keys are used for encryption and decryption, the asymmetric encryption protocols can be called as “cryptographic mailbox”, i.e. anyone can put something in Alice’s mailbox, but only Alice can take something out of it as she is the owner of her secret key. Also since messages are encrypted using public key asymmetric encryption is often called public key encryption. Usually the same asymmetric encryption system is used by many users. These systems allow user to possess only one pair of keys. In this case each public key can be stored in a public database. In this case Alice does not take any part in the protocol until she gets a ciphertext from Bob [2].

In this work we present a new asymmetric cryptography protocol, which is used for secret data encryption. The suggested protocol uses non-commutative algebraic structures, which aggravates the usage of known cryptographic attacks against our protocol.

The four main requirements for our protocol are the correctness of our cipher, the security of the user's public key and the obtained ciphertext and the effective implementation in embedded systems. Based on these requirements in this work we present an original asymmetric encryption protocol. The security of the presented protocol is based on a hard problem, defined in a semigroup of matrices.

Aim and objectives of the research

The aim of this work is to present a new original asymmetric encryption protocol, which security is based on inverting a matrix power function which is postulated a one-way function.

We have the following objectives to achieve our aim:

1. Investigate the algebraic and the statistical properties of the suggested one-way function.
2. Using postulated one-way functions present an asymmetric encryption protocol.
3. Present the investigation methods for our protocol. Evaluate the resistance of our protocol to statistical and algebraic cryptanalysis.
4. Determine the main security parameters of our protocol and their safe values.
5. Evaluate the time consumption of our protocol by comparing it to other commonly used protocols.

Research methods

Methods of algebra, number, probability and complexity theories were used solving the problems of dissertation. Correctness, security and implementation effectiveness of our protocol were investigated using analytical methods and by experiment using software tools created to implement the suggested protocol.

Scientific novelty of the work

1. In this work we present an original asymmetric encryption protocol based on a new one-way function. The suggested function has never before been used for asymmetric encryption. The function is defined in non-commutative algebraic structures. Hence the suggested protocol is one of the non-commutative cryptography class protocols. The protocols of this class are somewhat new and are considered perspective, since they are based on hard non-commutative cryptography problems. The cryptanalysis of these problems is not developed enough to solve them in a reasonable time.

2. The selected algebraic structures allow us to validate the security of our protocol from the statistical analysis point of view.
3. User's secret and public keys are mathematically linked using the one-way function defined in multiplicative semigroup of matrices. The security of the public key is based on solving a new hard problem defined in a finite multiplicative semigroup of matrices. The complexity of this problem is similar to solving a multivariate quadratic system of equations in a finite ring. However, since in our case the equations are non-linear and involve powering to unknown powers, we can assume, that solving of these equations is more complicated than in case of multivariate quadratic system of equations.
4. The proposed protocol can be implemented in embedded systems more effectively than other commonly used asymmetric encryption protocols, since it does not require using processors for operations with large numbers and uses lookup tables to perform algebraic operations.

Dissertation statements presented for defense

1. An original asymmetric encryption protocol is presented. The security of the protocol is based on non-commutative cryptography.
2. Up to now no effective methods of cryptographic analysis for discrediting our protocol are known.
3. The proposed protocol can be effectively implemented in embedded systems.

Approbation of the research results

Four papers on the topic of dissertation have been published. Two of these publications have an „ISI Web of Science" cite index. Two papers are published in conference proceedings. The dissertation topic was presented at Lithuanian Mathematical Society 53rd conference in Klaipeda (Lithuania) two international conferences: BulCrypt 2012 in Sofia (Bulgaria) and Electronics 2013 in Palanga (Lithuania).

2. MATRIX POWER FUNCTION

2.1. The matrix power function definition

Let us denote a ring of square $m \times m$ matrices by $\boldsymbol{M_A}$. The elements of these matrices are selected from a set $\boldsymbol{A}$, which forms an associative ring under addition and multiplication. Matrix addition and multiplication in this ring are defined in a standard way. In this section we are going to define a matrix operation, which we call the *matrix power function* (MPF). This operation formally extends the powering operation to non-commutative semigroup of matrices.

MPF uses one parameter – matrix Q, and one or two arguments – matrices X and Y, depending on a type of MPF (one-sided or two-sided). In general case we can select the elements of matrix Q from any commuting multiplicative semigroup $\boldsymbol{S}$. The

elements of matrices X and Y must, however, be selected from a number ring $\boldsymbol{R}$. We will denote the semigroup of square matrices of order m defined over the semigroup $\boldsymbol{S}$ by $\boldsymbol{M_S}$ and call it the *platform semigroup*. We also denote the ring of square matrices of order m defined over a number ring $\boldsymbol{R}$ by $\boldsymbol{M_R}$ and call it the *power ring*. The result of MPF is in the platform semigroup [3].

We start by defining one-sided MPFs. Let Q and Y be two square matrices of order m. Let matrix $Q = \{q_{ij}\}$ *powered by matrix* $Y = \{y_{ij}\}$ *from the right* be matrix $C = \{c_{ij}\}$, i.e.

$$C = Q^Y. \tag{2.1}$$

where the elements of C are computed by the formula [3], [4]:

$$c_{ij} = \prod_{k=1}^{m} q_{ik}^{\,y_{kj}}. \tag{2.2}$$

We call matrix Q in (2.1) a *platform matrix*, matrix Y *– a power matrix* and matrix C – the *right matrix power* (MP) *exponent*.

In a similar way by *powering matrix Q from the left* by matrix $X = \{x_{ij}\}$ we obtain matrix $D = \{d_{ij}\}$, i.e.

$$D = {}^X Q, \tag{2.3}$$

where the elements of *left MP exponent D* are computed by the formula [3], [4]:

$$d_{ij} = \prod_{k=1}^{m} q_{kj}^{\,x_{ik}} \tag{2.4}$$

Furthermore, we can use the combination of both functions to define a *two- sided MPF* by powering matrix Q from the left and right by matrices X and Y, respectively. Denoting the result matrix by $E = \{e_{ij}\}$ we have the following MPF definition

$$E = {}^X Q^Y. \tag{2.5}$$

The elements of two-sided MP exponent (or MP exponent for short) E are computed by the formula:

$$e_{ij} = \prod_{k=1}^{m} \prod_{l=1}^{m} q_{kl}^{x_{ik} y_{lj}} \tag{2.6}$$

In this work we will often reference to expression (2.5) not only as a notation of the MPF, but also as MPF equation. The problem of solving this equation can be formulated in a following way:

MPF problem. Find matrices X and Y, which satisfy (2.5), if matrices Q and E are given.

We can see from the definition of MPF, that the elements of matrices X and Y are the powers of elements of matrix Q. This is the reason for selecting the elements of matrices X and Y from a number ring. For example, if $\boldsymbol{S} = \boldsymbol{Z}_n^*$, then we can choose $\boldsymbol{R} = \boldsymbol{Z}_{\lambda(n)}$, where $\lambda(n)$ is the Carmichael function of n [5].

Let us now present two lemmas which indicate the important properties of MPF for cryptographic protocols construction. The proofs of these properties can be found in [6].

Lemma 2.1. If $\boldsymbol{R}$ is a commuting numerical semiring and $\boldsymbol{S}$ is a commuting semigroup, then MPF defined by (2.5) is the action of $\boldsymbol{M}_{\boldsymbol{R}} \times \boldsymbol{M}_{\boldsymbol{R}}$ in $\boldsymbol{M}_{\boldsymbol{S}}$ satisfying the following associative law

$$\left({}^{X}Q\right)^{Y} = {}^{X}\left(Q^{Y}\right) = {}^{X}Q^{Y} \tag{2.7}$$

Lemma 2.2. If $\boldsymbol{R}$ is a commuting numerical semiring and $\boldsymbol{S}$ is a commuting semigroup, then MPF defined by (4) is the action of $\boldsymbol{M}_{\boldsymbol{R}} \times \boldsymbol{M}_{\boldsymbol{R}}$ in $\boldsymbol{M}_{\boldsymbol{S}}$ satisfying the following identity

$${}^{X}\left({}^{U}Q^{V}\right)^{Y} = {}^{(XU)}Q^{(VY)} \tag{2.8}$$

Despite the fact that it is not yet been proven if MPF problem is NP-complete K. Luksys pointed out the following advantages of MPF [6]:

1. MPF is resistant to brute force attack. This result can also be achieved using small numbers as elements of the platform matrix if the order of matrices is increased.
2. The value of MPF can be calculated quickly, since addition and multiplication are performed with small numbers. The size of numbers we use is at most 8 bits.

3. Since small numbers are used, we can form lookup tables to perform addition and multiplication operations.
4. Each element e_{ij} of matrix E depends on all elements q_{ij} of matrix Q. This property is very important for cryptographic purposes.

However MPF alone cannot be used to construct asymmetric criptographic protocols. For this reason we define extra conjugation constrains. We use these constrains to get important identities, which we will use to construct a protocol.

Before constructing any protocol, based on some function we first have to make sure, that the used function can be considered a one-way function. For this purpose we consider the statistical properties of MPF. We rely on the results presented in [7] and [8].

2.2. Statistical properties of MPF

The statistical vulnerability of MPF will be caused by non-uniform distribution of different elements of MP exponent matrix E. Since in this work we consider finite algebraic structures, we say that a random variable ξ has a uniform distribution in a finite set $\boldsymbol{A}$ if:

$$prob(\xi = a) = \frac{1}{|\mathrm{A}|} \tag{2.9}$$

for all $a \in \boldsymbol{A}$.

The uniform distribution has an important property: uniformly distributed random variable has maximum entropy[1] out of all other dicrete random variables. Large entropy is important in cryptography since in this case an adversary cannot give a priority to any possible choice.

Let us assume that the elements x_{ij} and y_{ij} of power matrices X and Y have a uniform distribution. To prevent statistical attacks we have to select the elements q_{ij} of matrix Q in such a way that the elements of matrix E would be distributed uniformly. Since according to Cauchy theorem the maximal order of the group $\boldsymbol{Z_n}^*$ $\lambda(n)$ divides the order of this group $|\boldsymbol{Z_n}^*|$, elements of order $\lambda(n)$ form a certain cyclic subgroup(s) of $\boldsymbol{Z_n}^*$. We know from a previuos subsection, that in this case the power ring is $\boldsymbol{Z_r}$, where $r = \lambda(n)$. Let us choose a composite number n of the form $n = pq$, where p and q are prime numbers in such a way, that $\boldsymbol{Z_n}^*$ would have at least two cyclic subgroups

[1] Entropy – a characteristic of a random variable, which quantitatively decribes its randomness. Large value of entropy indicates, that it is hard to predict the value of the random variable.

$C_{r.1}$ and $C_{r.2}$. According to Lagrange theorem the maximal possible order of the element of Z_n^* i.e. the value of Carmichael function is less than or equal to $\phi(n)/2$, where (n) is the Euler totient function. Hence the necessary condition for Z_n^* to have a cyclic subgroup C_r of maximal order is

$$\phi(n) = 2\lambda(n). \tag{2.10}$$

Assume that primes are p and q are chosen and two cyclic subgroups $C_{r.1}$ and $C_{r.2}$ of maximal order r exist in Z_n^*. Let $C_{r.1} * C_{r.2}$ be a free product of subgroups $C_{r.1}$ and $C_{r.2}$ defined by the set

$$C_{r.1} * C_{r.2} = \{c = c_1 \cdot c_2 \mid c_1 \in C_{r.1}, c_2 \in C_{r.2}\}, \tag{2.11}$$

where · is a multiplication operation in Z_n^*.

We will use the following known propositions below:

Proposition 2.3. $C_{r.1} * C_{r.2}$ is a group if and only if $C_{r.1}$ and $C_{r.2}$ are abelian groups [1].

We see that it is the case in our construction.

Proposition 2.4. If G_1 and G_2 are two subgroups of some finite group G, then free product $G_1 * G_2$ consists of exactly $|G_1| \, |G_2| / |G_1 \cap G_2|$ different elements [1].

Let $C_{r.1} \cap C_{r.2}$ be some subgroup. Since $\lambda(n)$ is an even number, the maximal possible order of this subgroup is $\lambda(n) / 2$. Referencing the proposition above the following lemma can be formulated.

Lemma 2.5. If $|C_{r.1} \cap C_{r.2}| = \lambda(n)/2$ then $C_{r.1} * C_{r.2} = Z_n^*$.

Proof. Under the conditions defined above we have the following identity

$$\left|C_{r.1} * C_{r.2}\right| = \left|C_{r.1}\right|\left|C_{r.2}\right| / \left|C_{r.1} \cap C_{r.2}\right| = \frac{\lambda^2(n)}{\lambda(n)/2} = 2\lambda(n) = \phi(n)$$

Hence groups $C_{r.1} * C_{r.2}$ and Z_n^* has exactly (n) different elements. Since $C_{r.1}$, $C_{r.2}$ and $C_{r.1} * C_{r.2}$ are subgroups of Z_n^*, this ends the proof of lemma. ■

Let us find the generators of each of cyclic subgroups $C_{r.1}$ and $C_{r.2}$ and denote sets of these elements by Γ_1 ir Γ_2 respectively. The following propositions hold:

Proposition 2.6. For any generator γ in Γ_1 (Γ_2) and $x \in Z_r$ chosen at random, the element γ^x have the same distribution in $C_{r.1}$ ($C_{r.2}$) as x in Z_r [9].

Proposition 2.7. Let $z_0 \in Z_n^*$ be an arbitrary element. Choosing at random an element $z_1 \in Z_n^*$ and setting $z = z_0 \cdot z_1$ gives the same distribution for z as choosing a random element z [9].

Proposition 2.8. If γ_1 and γ_2 are in Γ and if $x, y \in Z_r$ are chosen uniformly at random, then the element z being computed by the expression $z = \gamma_1^x \gamma_2^y$ is uniformly distributed in Z_n^*.

Proof. Let us divide the group Z_n^* in the following sets: $C_{r.1} \cap C_{r.2}$, $C_{r.1} \setminus C_{r.2}$, $C_{r.2} \setminus C_{r.1}$ and $Z_n^* \setminus (C_{r.1} \cap C_{r.2})$. It can be easily shown, that each of the sets has exactly $\lambda(n) / 2$ elements. Consider these equally probable options:

- If γ_1 and γ_2 are in $C_{r.1} \cap C_{r.2}$ respectively, then the element z has a uniform distribution in the set $C_{r.1} \cap C_{r.2}$.
- If γ_1 and γ_2 are in $C_{r.1} \setminus C_{r.2}$ and $C_{r.2} \setminus C_{r.1}$ respectively, then the element z has a uniform distribution in the set $Z_n^* \setminus C_{r.1} \cap C_{r.2}$.
- If γ_1 and γ_2 are in $C_{r.1} \setminus C_{r.2}$ and $C_{r.1} \cap C_{r.2}$ respectively, then the element z has a uniform distribution in the set $C_{r.1} \setminus C_{r.2}$.
- If γ_1 and γ_2 are in $C_{r.1} \cap C_{r.2}$ and $C_{r.2} \setminus C_{r.1}$ respectively, then the element z has a uniform distribution in the set $C_{r.2} \setminus C_{r.1}$.

Since element z has a uniform distribution in each of the sets of Z_n^* it also has a uniform distribution in a whole group. ■

Let us denote $\Gamma = \Gamma_1 \cup \Gamma_2$ and formulate the following corollary:

Corollary 2.9. If $|C_{r.1} \cap C_{r.2}| = \lambda(n) / 2$, if all elements of the platform matrix Q entries $q_{ij} \in \Gamma$ and if elements of matrices X, Y in Z_r are chosen uniformly at random, then the distribution of elements of MP exponent matrix E are uniformly distributed in Z_n^*.

Let us denote the set of solutions of MPF equation (2.5) by $\boldsymbol{Pow}(Q, E) = \{(X, Y): {}^{X}Q^{Y} = E\}$. According to corollary 2.9 the elements of this set have a uniform distribution.

In the previuos subsection we mentioned, that to construct cryptographic protocols based on MPF we have to add extra conjugation constrains. These constrains are defined as follows [9]:

$$\begin{matrix} X^{-1}AX = C \\ Y^{-1}BY = D \end{matrix}, \tag{2.12}$$

where matrices A, B, C, D are known and chosen from the power ring $\boldsymbol{M_R}$, where $\boldsymbol{R} = \boldsymbol{Z_r}$. To break MPF with conjugation constrains an adversary has to find matrices X and Y, satisfying the following system of equations

$$\begin{cases} {}^{X}Q^{Y} = E \\ X^{-1}AX = C \\ Y^{-1}BY = D \end{cases}, \tag{2.13}$$

where other matrices are known [9].

We have already shown that solutions of the first equation of system (2.13) are distributed uniformly. Now we will consider the distribution of solutions of the conjugation equations. We consider an equation

$$X^{-1}AX = C \tag{2.14}$$

We consider this equation in a ring $\boldsymbol{Z_r}$. However it was proven in [9], that if we choose $r = 2s$, where s is a prime number, we can consider equation (2.14) in two fields $\boldsymbol{Z_2}$ and $\boldsymbol{Z_s}$. Our choice for parameter r is based on a fact, that the value of Carmichael function is an even number. By choosing a prime s we minimize the number of possible values of orders of elements of the group $\boldsymbol{Z_n}^*$, which we use to define a platform semigroup and maximize the number of generators of its cyclic subgroups.

Let us consider equation (2.14) in a field $\boldsymbol{Z_s}$. Let us assume that matrices A and C are similar to a Jordan matrix J, i.e. these matrices can be expressed in a canonical Jordan form

$$\begin{aligned} A &= K^{-1}JK \\ C &= L^{-1}JL \end{aligned}, \tag{2.15}$$

where K and L are the eigenvector matrices of A and C respectively and

$$J = \begin{pmatrix} \mu & 1 & 0 & \dots & 0 & 0 \\ 0 & \mu & 1 & \dots & 0 & 0 \\ 0 & 0 & \mu & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \mu & 1 \\ 0 & 0 & 0 & \dots & 0 & \mu \end{pmatrix}, \tag{2.16}$$

where μ is an eigenvalue of both matrices.

It was shown in [9], that there are exactly s^m different matrices commuting with J. We denote the set of these matrices by $\boldsymbol{Com}(J)$ and the number of these matrices by $|\boldsymbol{Com}(J)|$. Note that not all matrices of $\boldsymbol{Com}(J)$ have their inverses since zero value cannot be chosen for diagonal elements. If we omit zero diagonal elements, we get exactly $s^{(m-1)}(s-1)$ invertible matrices commuting with J. We denote the set of these matrices by $\boldsymbol{Com}^*(J)$.

Since we obtain all solutions of (2.14) by calculating

$$X = K^{-1}\tilde{X}L \tag{2.17}$$

where matrix $\tilde{X} \in \boldsymbol{Com}^*(J)$, the following proposition holds:

Proposition 2.7. Let A and C be a square matrix of order m defined over a field $\boldsymbol{Z}_s$. If these matrices are similar to Jordan matrix (2.16), then the conjugation equation (2.14) has exactly $s^{(m-1)}(s-1)$ solutions.

Using this proposition we can evaluate the number of solutions of the conjugation equation (2.14), defined in a ring $\boldsymbol{Z}_r$.

Corollary 2.8. If $A_2 = A \bmod 2$ and $A_s = A \bmod s$ are similar to Jordan matrix (2.16) in fields $\boldsymbol{Z}_2$ and $\boldsymbol{Z}_s$ respectively, then conjugation equation (2.14) has exactly $r^{(m-1)}(s-1)$ solutions. Hence $|\boldsymbol{Com}^*(J)| = r^{(m-1)}(s-1)$. We shall denote the set of these solutions by $\boldsymbol{Conj}(A, C)$.

It was proven in [10] that any matrix commuting with Jordan matrix (2.16) can be expressed as a polynomial of J. The degree of polynomial is equal to $(m-1)$, since

there are m linearly independent matrices commuting with J. The proof of the uniform distribution of elements of sets $\boldsymbol{Conj}(A, C)$ and $\boldsymbol{Conj}(B, D)$ relies on this fact [9].

It is clear, that set of solutions of system (2.13) is an intersection of two sets $\boldsymbol{Pow}(Q, E)$ and $\boldsymbol{Conj}(A, C) \times \boldsymbol{Conj}(B, D)$, i.e.

$$\boldsymbol{Sol}\left(Q,E,A,B,C,D\right) = \boldsymbol{Pow}\left(Q,E\right) \cap \left(\boldsymbol{Conj}\left(A,C\right) \times \boldsymbol{Conj}(B,D)\right) \qquad (2.18)$$

Since both these sets contain uniformly distributed elements, the set of solutions of system (2.13) also contains uniformly distributed elements. Hence we have proven the following proposition [9]:

Proposition 2.9. If a base matrix Q is defined over the platform group $\boldsymbol{Z}_n^*$ implying power matrices X and Y to be defined over a power ring $\boldsymbol{Z}_{2^s}$ and if the entries of power matrices are chosen at random with uniform distribution, then MPF equation (2.5) with constraints (2.15), defined over a power ring, yields the matrix E which entries are also uniformly distributed.

Using this proposition we can make a conjecture that MPF can be used to create a pseudorandom number generator and according to proposition 6.2.2 in [7] consider MPF with conjugation constrains to be a one-way function. Hence this function can be used for cryptographic protocols.

3. MATRIX POWER ASYMMETRIC CIPHER

The first version of asymmetric encryption protocol, based on MPF, was suggested in autumn 2011 and published in July 2012. We call the result the matrix power asymmetric cipher (MPAC). The proposed protocol was studied and it was found, that MPAC is vulnerable to a certain algebraic attack. For these reasons the protocol was improved. The results of our research are presented in this section.

3.1. The first version of MPAC protocol

The protocol uses two public parameters: matrix Q selected in the platform semigroup $\boldsymbol{M}_S$ and matrix Z selected in the power ring $\boldsymbol{M}_R$. Alice has her private key – a pair of matrices $\{X, U\} = PrK_{A,,}$ where X is a randomly selected non-singular matrix and matrix U is a polynomial of Z i.e. $U = \boldsymbol{P}_A(Z)$. Alice uses her private key to decrypt Bob's message. Her public key is $PuK_A = \{XZX^{-1} = A, {}^{X}Q^{U} = E\}$. Bob sends a message M to Alice by performing the following actions [4]:

1. Bob randomly chooses a secret non-singular matrix Y in the power ring $\boldsymbol{M}_R$.
2. Bob uses Alice's public key as follows:
   a) He selects a random secret polynomial $\boldsymbol{P}_V(\ )$ and computes a secret matrix $V = \boldsymbol{P}_B(Z)$. Then he takes matrix A and computes $\boldsymbol{P}_B(A) = XVX^{-1}$;

b) He raises matrix ${}^{X}Q^{U}$ to the obtained power matrix $\boldsymbol{P}_B(A)$ on the left and obtains ${}^{XV}Q^{U}$;
c) He raises the result matrix to the power matrix Y on the right and obtains ${}^{XV}Q^{UY} = K$.

The obtained matrix K is used as a key to encrypt the message M and compute the ciphertext C.

3. Bob computes the ciphertext $C = K \oplus M$, where $\oplus$ is a bitwise sum modulo 2 of the entries of matrices K and M.
4. Bob computes matrices $Y^{-1}ZY$ and ${}^{V}Q^{Y}$. We call a pair of these matrices an decryptor and denote it by ε i.e. $\varepsilon = \{Y^{-1}ZY = B, {}^{V}Q^{Y} = F\}$.
5. He sends the dectyptor ε to Alice together with C.

To decrypt Bob's message Alice does the following:

1. Using matrix B Alice computes $\boldsymbol{P}_A(B) = Y^{-1}UY$, since $U = \boldsymbol{P}_A(Z)$.
2. Alice raises matrix F to the power $\boldsymbol{P}_A(B)$ on the right and then raises the result matrix to the power of X on the left and obtains matrix $K = {}^{XV}Q^{UY}$, which is the encryption key.
3. Alice can now decrypt the ciphertext C by using the encryption key K and relation $M = K \oplus C$.

The main advantage of our protocol comparing it to other protocols based on conjugation search problem (CSP) is the fact, that only matrices U and V commute. This fact, however, is not essential, i.e. these matrices do not have to commute to complete the protocol successfully. We will demonstrate this later. Note also that since matrix U is calculated using a polynomial $\boldsymbol{P}_A(Z)$ only coefficients of this polynomial have to be stored. This shortens private key length.

It is also important to point out, that the security of our protocol is not based on the classical discrete logarithm problem (DLP), since we do not use large numbers. For this reason we consider DLP to be solvable in reasonable time and will not use cyclic (semi)groups to define the multiplicative platform semigroup.

Looking at Alice's public key we can see, that the adversary has to solve the CSP in order to find a part of her private key – the matrix X. The theoretical algorithms for solving this problem in matrix rings are known [10]. However in our case as opposed to Ko-Lee protocol [11] the CSP cannot be replaced with decomposition problem [12] since matrix Q is powered by matrix X in (2.5).

Another important fact from cryptographic point of view is that the true value of matrix X cannot be replaced by some other matrix $\tilde{X}$, satisfying (2.14) since in step 3 of our protocol Alice's raises the matrix ${}^{V}Q^{UY}$ to power matrix X from the left. Using

some other matrix $\tilde{X}$ does not guarantee that $\tilde{X}V = XV$, which means that an adversary cannot decrypt the ciphertext C.

The proposed protocol has some similarities to Anshel-Anshel-Goldfeld protocol [13]. Note that since a part of Alice's private key – the matrix U is calculated using a polynomial $\boldsymbol{P}_A(Z)$, we can interpret the set of polynomials as Alice's public subset. Anoteher similarity is the fact that in is not enough for adversary to know the value of U, since Alice calculates the value of $\boldsymbol{P}_A(B)$ in step 1 of decryption. Hence without the coefficients of $\boldsymbol{P}_A(\ )$ adversary still cannot decrypt the ciphertext C.

3.2. Discrete logarithm attack

Note that to break MPAC an adversary has to solve a system of power equations. Since we do not know any algorithms to solve such systems, an adversary has to consider options to replace this problem with another equivalent easier problem, for which theoretical algorithms are known. In this section we will present such an attack, which we call the *discrete logarithm attack* (DLA).

Assume, that matrix Q is defined over some cyclic group $\boldsymbol{G}$ i.e. $\boldsymbol{S} = \boldsymbol{G}$. Let the generator of $\boldsymbol{G}$ be given (we denote it by g). We define a discrete logarithm with the base of g of matrix Q, which we denote by $\mathrm{ld}_g Q$, as follows [14]:

$$\mathrm{ld}_g Q = \{\mathrm{ld}_g q_{ij}\}. \tag{3.1}$$

A discrete logarithm function (3.1) can be applied to (2.5) to obtain:

$$\mathrm{ld}_g Q^Y = \left(\mathrm{ld}_g Q\right) \cdot Y = \mathrm{ld}_g C. \tag{3.2}$$

If the inverse matrix $(\mathrm{ld}_g Q)^{-1}$ exists, then, by multiplying both sides of (3.2) by it we get:

$$Y = \left(\mathrm{ld}_g Q\right)^{-1} \cdot \mathrm{ld}_g C. \tag{3.3}$$

In the same way we can apply the discrete logarithm function to MPF (2.5) to get

$$\mathrm{ld}_g \left({}^X Q^Y\right) = X \cdot \left(\mathrm{ld}_g Q\right) \cdot Y = XTY = \mathrm{ld}_g E, \tag{3.4}$$

where $T = \mathrm{ld}_g Q$.

We can see from (3.4) that by using the discrete logarithm function (3.1) we were able to transform the initial system of power equation to multivariate quadratic (MQ) system of equations. Since we can clearly see similarities between both problems, we can evaluate the security of MPAC by considering the security requirements of the MQ system of equations. Hence we can formulate the following problem [14]:

Matrix multivariate quadratic equations **(MMQ)** ***problem***: Find matrices X and Y, satisfying (3.4), if matrices T ir $\mathrm{ld}_g E$ are given.

An adversary can break the proposed protocol if he is able to solve either MPF problem or an equivalent MMQ problem. Due to similarities of these problems we can see, that the complexity of both problems is similar. Since MMQ problem is similar to an NP-complete problem, we think that both problems (MPF and MMQ) are hard to solve. However we think, that if the described transformation is not possible, the initial system of power equations is harder to solve. It has been shown in [14], that this transformation is possible in the following cases:

- A cyclic (semi)group is used to define the multiplicative platform semigroup.
- In case of non-cyclic group more than one conjugation constrain has to be used.

For these reasons we constructed the following semigroup in [14]:

$$\boldsymbol{Z}_{\boldsymbol{n}}^{\#} = \boldsymbol{Z}_{\boldsymbol{n}}^{*} \cup Id_q\left(\boldsymbol{Z}_{\boldsymbol{n}}\right) \tag{3.5}$$

In expression (3.5) $Id_q(\boldsymbol{Z_n}) = \{j = i \cdot q;\ i = 1, \ldots, p-1\}$ is an ideal of semigroup $\boldsymbol{Z_n}$. Furthermore, we used two non-commuting matrices Z_1 and Z_2 to define two conjugation constrains:

$$\begin{aligned} XZ_1X^{-1} &= A_1 \\ XZ_2X^{-1} &= A_2 \end{aligned} \tag{3.6}$$

In this case matrix U is formed using some function $f_U(Z_1, Z_2)$. The transformation of MPF problem to MMQ problem is then impossible if none of the matrices ${}^{Z_1}Q$, ${}^{Z_2}Q$, Q^{Z_1} ir Q^{Z_2} can be logarithmized. This condition can be ensured if exactly one element of the platform matrix Q is selected from the set of the generators of $Id_q(\boldsymbol{Z_n})$ and all other elements are selected from the set of generators of $\boldsymbol{Z}_{\boldsymbol{n}}^{*}$.

We see that to avoid the DLA we have to use multiple conjugation constrains. Furthermore, the choice of platform semigroup is important as well. In the next

subsection we are going to define a new semigroup more suitable for our purposes and suggest a modified version of our protocol.

3.3. The improved version of MPAC protocol

Consider group $\boldsymbol{Z_n}^*$. The maximal order of elements of this group is $\lambda(n)$ which is obviously a composite number. It is also clear that the maximum entropy of each term q_{ij}^{α} can be achieved if and only if q_{ij} is a generator in $\boldsymbol{Z_n}^*$. This is also true for some cyclic group $\boldsymbol{G}$. However, our suggestion of using the generators of $\boldsymbol{G}$ as elements of the base matrix Q is not only based on the maximal entropy of terms, but also on the statistical security of MPF, which we discussed in subsection 2.2.

Let the parameter n of ring $\boldsymbol{Z_n}^*$ be a composite integer and let $\lambda(n)$ be of the form $\lambda(n) = pq$ where p is prime and $\gcd(p, q) = 1$. According to the Sylow theorem the the Sylow subgroup of the prime order p exists in $\boldsymbol{Z_n}^*$ [15]. We denote this subgroup as $\boldsymbol{\Gamma_{p,n}}$. Since, according to the Lagrange theorem, the order of the element $\gamma \in \boldsymbol{\Gamma_{p,n}}$ has to divide p, the only orders possible in group $\boldsymbol{\Gamma_p}$ are 1 and p. Hence every non-identity element γ is the generator of $\boldsymbol{\Gamma_p}$. We can use this group to ensure the maximum entropy of the entries of the result matrix E. However, it was shown in [14] that using a cyclic group as the platform makes MPF vulnerable to the DLA. Hence we have to construct a structure similar to $\boldsymbol{Z_n}^{\#}$.

Let j be an idempotent of ring $\boldsymbol{Z_n}$. Since the order of the element is a multiplicative function, we can multiply each element of group $\boldsymbol{\Gamma_{p,n}}$ by j to obtain a new cyclic group $\boldsymbol{J_{p,n}} = j\,\boldsymbol{\Gamma_{p,n}}$. The identity of this group is j and we assume, that the order of every non-identity element is p. We construct a semigroup $\boldsymbol{\Gamma_{p,n}}^{\#}$ as a union of $\boldsymbol{\Gamma_{p,n}}$ and $\boldsymbol{J_{p,n}}$ i.e.

$$\boldsymbol{\Gamma}^{\#}_{\boldsymbol{p,n}} = \boldsymbol{\Gamma}_{\boldsymbol{p,n}} \cup \boldsymbol{J}_{\boldsymbol{p,n}} \tag{3.7}$$

We use this semigroup to avoid direct application of a discrete logarithm function to MPF, since $\boldsymbol{J_{p,n}}$ is the ideal of $\boldsymbol{\Gamma_{p,n}}^{\#}$. Note that no additional constraints for parameter n and the entries of Q are needed as compared to $\boldsymbol{Z_n}^{\#}$.

The main advantage of $\boldsymbol{\Gamma_{p,n}}^{\#}$ is the prime order of non-idempotent elements. Since the order of $\boldsymbol{\Gamma_{p,n}}^{\#}$ determines the modulo of the power ring $\boldsymbol{M_R}$, we obtain a power ring defined over the field $\boldsymbol{R} = \boldsymbol{Z_p}$. Hence, the conjugation constrains (3.6) are defined over a field $\boldsymbol{Z_p}$.

The modified version of MPAC protocol uses three public parameters: matrix Q selected over $\boldsymbol{\Gamma_{p,n}}^{\#}$ and two non-commuting matrices Z_1 and Z_2 selected over field $\boldsymbol{Z_p}$. Matrix Q is chosen to be resistant to the discrete logarithm attack as described above. Alice has her private key – a pair of matrices $\{X, U\} = PrK_A$, where X is a randomly selected non-singular matrix and $U = \boldsymbol{f}_U(Z_1, Z_2)$. Alice uses her private key to decrypt

Bob's message. Her public key is a triplet of matrices, i.e. $PuK_A = \{A_1, A_2, E\}$, where A_1, A_2 are defined by (3.6) and E is defined by (2.5). Bob sends a message M to Alice by performing the following actions:

1. Bob randomly chooses a secret non-singular matrix Y over field $\boldsymbol{Z_p}$.
2. He selects a random secret function $\boldsymbol{f}_V(\ )$ and computes a secret matrix $V = \boldsymbol{f}_V(Z_1, Z_2)$. Then he takes matrices A_1, A_2 and computes $\boldsymbol{f}_V(A_1, A_2) = XVX^{-1}$;
3. He raises matrix ${}^{X}Q^{U}$ to the obtained power matrix XVX^{-1} on the left and obtains ${}^{XV}Q^{U}$;
4. He raises the result matrix to the power of matrix Y on the right and obtains ${}^{XV}Q^{UY} = K$. Matrix K is used as a key to encrypt message M and compute ciphertext C;
5. Bob computes ciphertext $C = K \oplus M$;
6. Bob computes matrices $B_1 = Y^{-1}Z_1Y$, $B_2 = Y^{-1}Z_2Y$ and $F = {}^{V}Q^{Y}$ which we denote by ε i.e. $\varepsilon = \{B_1, B_2, {}^{V}Q^{Y}\}$.
7. He sends the dectyptor ε to Alice together with C.

To decrypt Bob's message Alice does the following:

1. Using matrices B_1, B_2 Alice computes $\boldsymbol{f}_U(B_1, B_2) = Y^{-1}UY$, since $U = \boldsymbol{f}_U(Z_1, Z_2)$.
2. Alice raises matrix ${}^{V}Q^{Y}$ to the power of $Y^{-1}UY$ on the right and then raises the result matrix to the power of X on the left and hence obtains matrix ${}^{XV}Q^{UY}$ which is the encryption key K.
3. Alice can now decrypt ciphertext C by using encryption key K and relation $M = K \oplus C$.

The security of MPAC protocol relies on the MPF and the following two principles:

1. By a certain definition of matrix Q the transmitted data, i.e. public keys of both parties, cannot be used for discrete logarithm application to reduce MPF equation to the MMQ problem in order to facilitate the cryptanalysis of the proposed protocol.
2. Using a specially defined matrix $U = f(Z_1, Z_2)$ the DLA fails as is shown in [13]. The same is true for matrix V.

4. SECURITY PARAMETERS AND IMPLEMENTATION OF MPAC PROTOCOL

4.1. Security parameters and their secure values

It may seem from subsection 3.1 that the main parameters of MPAC are the integer n, which defines the non-cyclic multiplicative group $\boldsymbol{Z_n}^*$, and the order of square matrices m. However since we are seeking to minimize the order of the

multiplicative group and maximize the order of its generators we suggest to select a value of n of the form $n = 3p$, where $p = 2s + 1$ is a prime number, such that s is also prime [14], [16]. In this case $\lambda(n) = p - 1$, and hence the power ring is defined over a number ring $\boldsymbol{Z}_r$, where $r = 2s$. We can see that parameter p is more important than the parameter n. Hence the main parameters of MPAC are p and m.

Another important parameter of any protocol is the security level L. However the choice of the value of this parameter is based on such factors as hardware options, the importance and the relevance of the data etc. One of the main factors for the choice of L is amount of mathematical operations performed when the protocol is attacked. Since DLA only facilitates cryptanalysis of MPAC, the main attack against our protocol is brute force. Based on this fact we interpret the security level L as the number of elements of the set of polynomials of degree $(m - 1)$ defined over a ring $\boldsymbol{Z}_r$.

Consider Alice's private key $PrK_A = \{X, U\}$. Matrix X can be chosen freely and the only restriction for this matrix is the existence of its inverse. Matrix U commutes with publically known matrix Z and is calculated using a polynomial of this matrix. Hence to determine the safe values of the main parameters for a fixed value of security level we are relying on the following facts [16]:

- The number of matrices commuting with a public matrix Z, defined over a power ring, should be at least 2^L. Every commuting matrix should be obtained using polynomials of matrix Z.
- The number of matrices conjugating with a public matrix A, defined over a power ring should be at least 2^L.

If these requirements are satisfied, total scan of matrices X and U is infeasible. Note that to our knowledge there are no significantly faster algorithms for solving MPF problem (2.5) of MMQ problem (2.5) than total scan. Based on these two presented facts and our previous research we obtained a following result for parameter m [15]:

$$m \geq \left\lceil \frac{(L+1)\ln 2 + \ln(p-1) - \ln(p-3)}{\ln(p-1)} \right\rceil \qquad (4.1)$$

Since introduced protocol has two main security parameters, which have to satisfy the inequality (4.1), one of them must be chosen for other reasons. Therefore we advice that parameter p must be chosen taking the compromise between the available memory and required computation time.

To compare the efficiency of our algorithm with other known algorithms we introduce a term of computational cost defined by the number of elementary operations executed in the custom microprocessor. Since our algorithm uses less elementary operations in the case of $p = 47$ as compared to the case of $p = 11$, we

compare its computation cost to a classical El-Gamal-2048 bits asymmetric encryption scheme [17] and elliptic curve ECC-521 asymmetric encryption scheme [18] on 32 bit microprocessor.

The objective results of obtained comparison are presented in Table 4.1 [16].

Table 4.1 Comparison of computational costs of asymmetric encryption schemes

Algorithm	Computational cost (elem. op.)
El-Gamal-2048	23.5×10^6
ECC-521	6.9×10^6
Our algorithm, $p = 11$	8.0×10^5
Our algorithm, $p = 47$	1.04×10^5

The explanation of the obtained results can be based on the fact that the realization of both El-Gamal-2048 and ECC-521 relies on the usage of arithmetic operations with large integers. Despite the fact that integers in ECC-521 are 4 times shorter than in El-Gamal-2048, the cost of each operation of ECC-521 is longer since these operations themselves are more complicated.

4.2. Implementation of MPAC protocol

We are planning to implement our protocol in an international project "Internet of Things". This project focuses on the study of physical devices called IoT things. Since IoT is a complex network which uses various communication protocols, the main objectives of the project are the following:

- The study of communication protocols and adaptation of these protocols to smart environments;
- Creation and study of the methods for cryptanalysis of cryptographic security of these protocols;
- Contracting and studying the prototypes for the integration of smart environment things stack.

To implement our protocol we created software tools to simulate a server agent, who generates public data for MPAC protocol, and two client agents, which communicate with each other using the improved version of MPAC protocol. We used the semigroup $\boldsymbol{Z_n^{\#}}$ to define a platform semigroup.

Using the created software we tested our protocol on a computer with the following system properties:

- Processor: Intel Core 2 Duo T6400 2.00 GHz;
- Memory (RAM): 4.00 GB;
- 32-bit Windows operating system.

In this subsection we will present the results of the elapsed time tests, i.e. we monitored the time it takes to perform public data generation, key generation, encryption of the plaintext and decryption of the ciphertext. We performed these tests for different values of p and L. We considered two values of the security level: $L = 80$ and $L = 112$. The latter value was considered based on NIST standards [19], where it was noted that all security systems should use 112 bit security level. The plaintext we used is a 42 bit file ExampleB.txt which contains a message „The quick brown fox jumps over a lazy dog". Since the estimated time t is a random variable, we rely on the law of large numbers to minimize the randomness of t, i.e. we calculate an estimator

$$\hat{t} = \frac{1}{N}\sum_{i=1}^{N} t_i \tag{4.2}$$

which loses its randomness in N tends to infinity [20]. We have chosen $N = 20$, i.e. we run each step of our protocol 20 times. The results of this test are displayed below (we measured the elapsed time in microseconds):

Table 4.2 The elapsed time (ms) analysis of MPAC for security level $L = 80$.

p	n	m	Public data	Key generation	Encryption			Decryption	
					K	XOR	ε	K	XOR
7	21	32	21,489	211,869	290,110	0,002	16,948	159,042	0,002
11	33	25	93,570	81,353	122,597	0,002	9,355	76,936	0,003
23	69	19	49,994	31,340	52,238	0,003	5,312	28,292	0,003
47	141	15	105,069	14,045	22,458	0,003	2,781	12,536	0,003
59	177	14	182,839	9,442	18,295	0,003	2,526	9,554	0,003
83	249	13	304,661	8,448	14,916	0,003	2,121	7,797	0,003

Table 4.3 The elapsed time (ms) analysis of MPAC for security level $L = 112$.

p	n	m	Public data	Key generation	Encryption			Decryption	
					K	XOR	ε	K	XOR
7	21	44	221,691	525,810	964,289	0,002	44,686	493,475	0,002
11	33	35	116,578	227,305	385,037	0,002	22,351	208,643	0,002
23	69	26	76,774	89,695	129,817	0,002	9,834	87,158	0,003
47	141	21	148,640	42,005	76,946	0,003	7,370	42,510	0,003
59	177	20	172,314	39,762	57,037	0,003	5,360	35,881	0,003
83	249	18	303,137	23,154	47,922	0,003	5,505	24,398	0,003

We can see from the tables that public data generation can be time consuming regardless of the value of parameter p. This comes from the fact, that for large values of p the generation of lookup tables is long. This process can take more than 99% of total time. Long generation of public data for small values of p comes from the facts, that it is harder to generate nonsingular matrices and longer calculation of polynomials. We can see from the obtained results, that larger values of the parameter p are superior to smaller ones.

We compared our protocol to RSA asymmetric encryption protocol [21]. The elapsed times for each step of the RSA protocol were obtained using the internet software [22]. We studied RSA protocol with widely used 1024 and 2048 bit keys and with 3072 and 4096 bit keys. In each case the maximum length text was used. Each step was run 20 times. The results are displayed below:

Table 4.4 The elapsed time (ms) analysis of RSA.

Step	RSA-1024	RSA-2048	RSA-3072	RSA-4096
Key generation	465,250	3615,750	25506,600	54424,550
Encryption	2,550	4,950	8,800	10,400
Decryption	18,600	103,650	316,350	497,350

Since MPAC performance is the fastest if $p = 83$, to compare two asymmetric ciphers we have to select a value of matrix order m to encrypt a comparable message. For this reason we have selected the following values of m:

- For RSA-1024 we selected $m = 12$. Key size – 1152 bits.
- For RSA-2048 – $m = 16$. Key size – 2048 bits.
- For RSA-3072 – $m = 20$. Key size – 3200 bits.
- For RSA-4096 – $m = 23$. Key size – 4232 bits.

Using the selected values of m we encrypt the same message as using RSA protocol corresponding to the value of m. The obtained results are displayed below:

Table 4.5 The dependence of the elapsed time (ms) of MPAC protocol on the matrix order m.

Step	MPAC, $m = 12$	MPAC, $m = 16$	MPAC, $m = 20$	MPAC, $m = 23$
Key generation	8,634	18,663	34,438	52,392
Encryption	12,911	35,597	77,614	114,814
Decryption	5,885	15,832	38,401	64,206

We can see from the obtained results, that MPAC encryption is slower, but the decryption is much faster than in case of RSA. The reason for this is the calculation of the decryptor in encryption step. In decryption step only the decryption key has to be calculated. Comparison of the total time to encrypt and decrypt the message is presented in figure 4.1. We can see from the presented chart, that the total time of encryption and decryption is smaller in case of MPAC. This difference is more significant for larger keys.

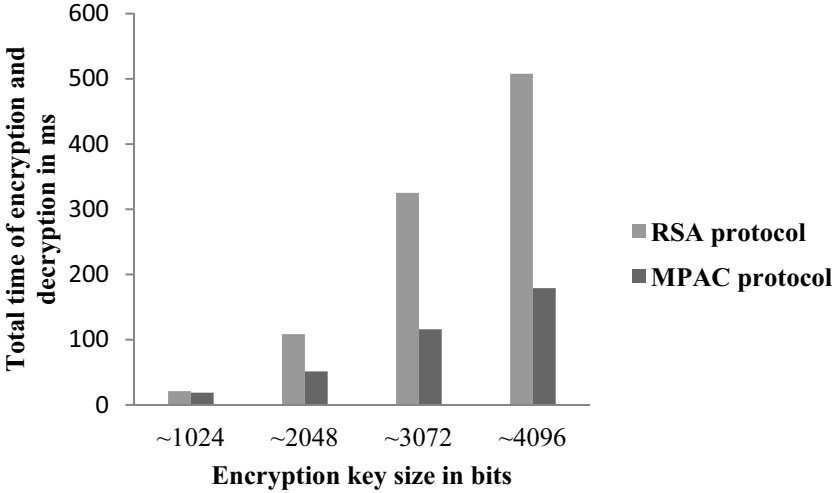

Fig. 4.1. The comparison of total time to encrypt and decrypt a message

To determine the best values of parameter p we consider the resistance of MPAC protocol to DLA. Using experiments we were able to find, that MP exponent matrix E is resistant to DLA if either matrix X or matrix U has zero elements. More precisely, if we denote a place of the element of an ideal by (i_0, j_0), where i_0, j_0 are row and column indexes respectively, then matrix E is resistant to DLA if at least one of the elements of an i_0-th column of matrix X or an j_0-th row of matrix U is equal to zero. It is clear, that the resistance of matrix E depends on the parameter of the number ring r and the order of matrix m. Calculating the probability of an opposite event we obtain a following formula to evaluate the probability of the resistance of matrix E to DLA:

$$prob(r,m) = 1 - \left(\frac{r-1}{r}\right)^{2m} \tag{4.3}$$

Since the parameter of a number ring $r = p - 1$ and the matrix order m depends on p and L, we present the dependence of the defined probability on these parameters. We measure the probability in percents.

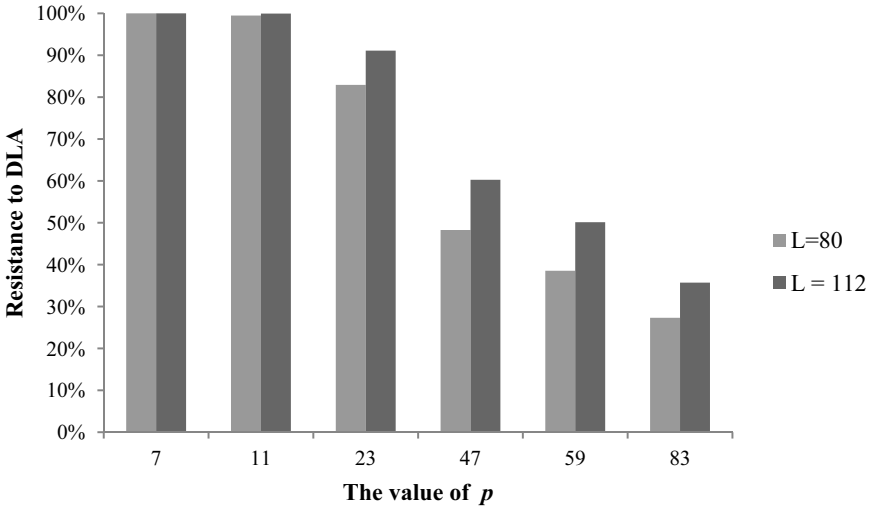

Fig. 4.2. The dependence of the probability of the resistance of matrix E to DLA on p and L

We can see that for small values of parameter p matrix E is almost always resistant to DLA, since in this case matrices are large and the number ring is small. Hence from this point of view small values of parameter p are superior to the larger ones.

We can see from the results of this subsection that for small values of parameter p encryption and decryption steps take longer running time, but the public matrix E is more resistant to DLA. For larger values of p encryption and decryption steps take less running time, but server actions require longer running time. Also the memory requirements for smaller values of p are lower.

5. CONCLUSIONS

1. Algebraic properties of MPF were investigated and a new algebraic platform structure based on Sylow theorem was suggested. It was proven that MPF with conjugation constrains is secure from the statistical cryptanalysis point of view.
2. While analyzing MPF with conjugation constrains based on the suggested algebraic structure we found, that the cryptographic security of this function relies on complexity of the system of power equations, which is similar to MQ system of equations. Since it is proven that the latter problem is NP-complete, we make a conjecture, that systems of power equations, used in our work, satisfy the cryptographic complexity requirements and MPF is resistant to algebraic attacks.

3. We constructed an original asymmetric encryption protocol using MPF with conjugation constrains. The security of this protocol relies on the complexity of MPF problem. Based on the results of our research we make a conclusion, that the suggested protocol is resistant to statistical and algebraic attacks.
4. While analyzing the resistance of our protocol to algebraic attacks we suggested using the discrete logarithm function in matrix semigroup. Using this function we presented an attack on the first version of MPAC, which facilitates the analysis of the MPF problem by reducing it to MMQ problem. We made improvements of our protocol to avoid the usage of discrete logarithm function for cryptanalysis.
5. Using experiments we found, that MP exponent matrix E is resistant to DLA if either matrix X or matrix U has zero elements. We evaluated the probability to resist DLA attack using this property.
6. The main security parameters of MPAC protocol are p, m and L. Parameter p defines the order of multiplicative semigroup, m defines the order of square matrices and L is the security level. The dependence of m on other main security parameters has been determined. This parameter is directly proportional to the security level and inversely proportional to parameter p.
7. Since the main attack against MPAC is the total scan of power matrices, we suggested interpreting the security level L as the order of the set of polynomials of $(m - 1)$ degree defined over $\boldsymbol{Z}_r$.
8. We compared the implementation of our protocol on 32-bit microprocessor to the implementation of El-Gamal-2048 and ECC-521 on the same platform from the elementary operations point of view. The computational cost of the first version of MPAC are in average 235 times less than in case of El-Gamal-2048 protocol and 69 times less than in case of ECC-521 protocol.
9. The performed experimental study of MPAC protocol shows that the total time to encrypt and decrypt a message is less than in case of RSA. This difference is more significant for longer keys. This fact allows us to flexibly adapt the encryption key length and the amount of encrypted information to user's needs.

BIBLIOGRAPHY

[1] Katz, J., & Lindell, Y. (2008). *Introduction to modern cryptography.* Chapman & Hall/CRC.

[2] Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons.

[3] Mihalkovich, A., Sakalauskas, E. (2012) Asymmetric cipher based on MPF and its security parameters evaluation. In: Proc. of the Lithuanian Mathematical Society, Ser. A., *Lietuvos Matematikos Rinkinys*, Vol. 53, pp. 72-77.

[4] Luksys, K. & Sakalauskas, E. (2012) *Matrix power cipher. Information technology and control.* Kaunas: Technologija.

[5] Carmichael, R. D. (1912) On Composite Numbers P Which Satisfy the Fermat Congruence. *The American Mathematical Monthly 19*(2), pp. 363–385.

[6] Lukšys, K. (2013). *Matrix power cipher and its analysis. PhD thesis.* Kaunas: KTU.

[7] Hastad, J., Impagliazzo, R., Levin, L., & Luby, M. (1999). A pseudorandom generator from any one-way function. *Siam Journal on Computation, 28*(4), pp. 1364–1396.

[8] Yao, A.: Theory and Applications of Trapdoor functions, Proceedings of the 23rd FOCS, IEEE, pp. 80-91 (1982)

[9] Sakalauskas, E., Mihalkovich, A. (2012) Candidate One-Way Function Based on Matrix Power Function with Conjugation Constraints, In: *Bulgarian cryptography days 2012*. Conference proceedings, pp. 29-37

[10] Gantmacher, F. (1966). *The theory of matrices.* Nauka, Moskow. (In Russian)

[11] Ko, K. H., Lee, S. J., Cheon, J. H., Han, J. W., Kang, J. S., & Park, C. (2000, January). New public-key cryptosystem using braid groups. In *Advances in Cryptology—CRYPTO 2000* (pp. 166-183). Springer Berlin Heidelberg.

[12] Shpilrain, V., & Ushakov, A. (2006). The conjugacy search problem in public key cryptography: unnecessary and insufficient. *Applicable Algebra in Engineering, Communication and Computing*, *17*(3-4), pp 285-289.

[13] Anshel, I., Anshel, M., & Goldfeld, D. (1999). An algebraic method for public-key cryptography. *Mathematical Research Letters*, *6*, pp. 287-292.

[14] Sakalauskas, E., Mihalkovich, A. (2014). New Asymmetric Cipher of Non-commuting Cryptography Class Based on Matrix Power Function. *Informatica*. 25(2) pp. 283-298.

[15] Kammüller, F., & Paulson, L. C. (1999). A Formal Proof of Sylow's Theorem. *Journal of Automated Reasoning*, *23*(3), pp 235-264.

[16] Mihalkovich, A., Sakalauskas, E., & Venckauskas, A. (2013). New Asymmetric Cipher Based On Matrix Power Function and Its

Implementation in Microprocessors Efficiency Investigation. *Electronics & Electrical Engineering*, *19*(10), pp. 119-122.
[17] ElGamal, T. (1985). A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory, 31*(4), pp. 469–472.
[18] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), pp. 203-209.
[19] NIST. (2013). *Digital Signature Standard (DSS). FIPS 186-4.* National Institute of Standards and Technology.
[20] Aksomaitis, A. (2000). Tikimybių teorija ir statistika. *Kaunas: Technologija*.
[21] Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), pp. 120-126.
[22] Crypt-online (2014). RSA asymmetric cipher system. Available at: http://www.crypt-online.narod.ru/crypts/rsa/

LIST OF SCIENTIFIC PUBLICATIONS ON THE THEME OF THE DISSERTATION

Articles in journals, with impact factor, from the list of Institute of Scientific Information database „ISI Web of Science“

1. Michalkovič, Aleksejus; Sakalauskas, Eligijus; Venčkauskas, Algimantas. New Asymmetric Cipher Based On Matrix Power Function and Its Implementation in Microprocessors Efficiency Investigation. // Elektronika ir elektrotechnika. ISSN 1392-1215. 2013, No. 19(10), p. 119–122 [Science Citation Index Expanded (Web of Science); INSPEC; Computers & Applied Sciences Complete; Central & Eastern European Academic Source].
2. Sakalauskas, Eligijus; Michalkovič, Aleksejus. New Asymmetric Cipher of Non-commuting Cryptography Class Based on Matrix Power Function.// Informatica 25(2) pp. 283-298 / Vilniaus universitetas. Vilnius : Matematikos ir Informatikos institutas. ISSN 0868-4952. [Science Citation Index Expanded (Web of Science); INSPEC].

Articles in conference proceedings

1. Mihalkovich, Aleksejus, Sakalauskas, Eligijus. Asymmetric cipher based on MPF and its security parameters evaluation// Proc. of the Lithuanian Mathematical Society, Ser. A.. Klaipėda : ISSN 0132-2818. 2012, Vol. 53, pp. 72-77.
2. Sakalauskas, Eligijus; Michalkovič, Aleksejus. Candidate One-Way Function Based on Matrix Power Function with Conjugation Constraints// Bulgarian cryptography days 2012. Conference proceedings. Sofia : ISBN 978-954-2946-22-9. 2012, pp. 29–35.

INFORMATION ABOUT THE AUTHOR OF DISSERTATION

Aleksejus Mihalkovich was born on the 21st of January in 1985, Kaunas, Lithuania. During 2004-2008 years he studied at Kaunas University of Technology and achieved the bachelor's degree of applied mathematics. During 2008–2010 years he studied at KTU and achieved the master's degree of applied mathematics. During 2010–2014 years – the doctoral studies at KTU. Currently he is working in the Department of Applied Mathematics in KTU as an assistant. You can contact him via e. mail Aleksejus.Michalkovic@ktu.lt.

Author's areas of interest: cryptography, number theory, algebra.

REZIUMĖ

Šiame darbe pristatomas originalus asimetrinio šifravimo protokolas, kurio saugumas yra paremtas matricinio laipsnio funkcija (MLF). Ši funkcija suriša vartotojo slaptąjį ir viešąjį raktus ir iki šiol nebuvo naudojama asimetriniam šifravimui.

Disertaciją sudaro 10 skyrių. Pirmajame įvadiniame skyriuje apibrėžiami pagrindiniai darbo tikslai ir uždaviniai bei pateikiamas temos aktualumas. Antrajame skyriuje yra patektas matematinis aparatas, kuris yra naudojamas sudarant mūsų protokolą ir atliekant sukurto protokolo tyrimą. Trečiame skyriuje yra pateikta literatūros apžvalga. Šiame skyriuje pateikti komutatyvios ir nekomutatyvios asimetrinės kriptografijos protokolai, su kuriais yra lyginamas mūsų protokolas. Nurodyti protokolų privalumai ir trūkumai.

Ketvirtame skyriuje yra pristatoma MLF ir nagrinėjamos šios funkcijos algebrinės savybės. Taip pat skyriuje nagrinėjamos MLF su jungtinumo apribojimais statistinės savybės siekiant įrodyti, kad ši funkcija gali būti naudojama kriptografiniams protokolams.

Penkto skyriaus pagrindinis tikslas yra pristatyti mūsų protokolą ir ištirti jį naudojant vienkryptės funkcijos algebrines savybes. Protokolo veikimas yra demonstruojamas naudojant pavyzdį. Naudojant skaičių teorijos elementus yra parodoma, kad pirmoji siūlomo protokolo versija nėra atspari diskretinio logaritmo atakai. Dėl šios priežasties šiame skyriuje yra siūloma nauja multiplikatyvi pusgrupė, kuri yra formuojama naudojant Sylovo teoriją. Taip pat siūloma padidinti jugtinumo apribojimų skaičių, kas leidžia išvengti diskretinio logaritmo atakos.

Šeštame skyriuje yra nagrinėjami pagrindiniai siūlomo protokolo parametrai ir pateikiama saugių viešųjų duomenų generavimo metodika. Taip pat šiame skyriuje siūlomas protokolas yra palyginamas su El-Gamal-2048 ir ECC-521 protokolais elementariųjų operacijų prasme. Tyrimo rezultatai parodė, kad naudojant pirmąją protokolo versiją skaičiavimų sanaudos yra vidutiniškai 235 kartų mažesnės lyginant su El-Gamal-2048 protokolu ir 69 kartus mažesnės lyginant su ECC-521 protokolu.

Septintame skyriuje yra pateikiami pagrindiniai algoritmai, kurie buvo naudojami kuriant programinę priemonę siūlomam protokolui realizuoti. Naudojant sukurtą programinę priemonę siūlomas protokolas yra palyginamas su RSA asimetrinio šifravimo protokolu greitaveikos prasme. Nustatyta, kad, nors naudojant RSA protokolas pranešimas užšifruojamas greičiau, bendras užšifravimo ir iššifravimo laikas yra mažesnis, kai yra naudojamas mūsų protokolas. Taip pat šiame skyriuje mūsų protokolas lyginamas su Diffie-Hellman'o ir elipsinių kreivių raktų apsikeitimo protokolais greitaveikos prasme. Rezultatai parodė, kad lyginant DH-1024 protokolą su panašaus šifravimo rakto ilgio MLAŠ protokolu gauname pagreitėjimą iki 12,7 kartų užšifravimo ir 24,4 kartų iššifravimo atveju, o lyginant ECDH-571 protokolą su panašaus šifravimo rakto ilgio MLAŠ protokolu pagreitėjimas siekia 120 kartų užšifravimo ir 228 kartus iššifravimo atveju.

Paskutiniuose skyriuose yra pateikiamos bendros šios disertacijos išvados, cituotos literatūros sąrašas ir paskelbtų disertacijos tema publikacijų sąrašas.

Disertacijos tema yra paskelbti du straipsniai, kurie turi mokslinės duomenų bazės „ISI Web of Science" citavimo indeksą. Dar du straipsniai yra konferencijų pranešimų medžiagoje. Disertacijos tema buvo pristatyta Lietuvos Matematikos Draugijos 53-ioje konferencijoje Klaipėdoje bei tarptautinėse konferencijoje „BulCrypt 2012" Sofijoje ir „Electronics 2013" Palangoje.

UDK 004.056.55(043.3)

SL344. 2015-01-08. 2,25 leidyb. apsk. l. Tiražas 70 egz. Užsakymas 9.

Išleido leidykla „Technologija", Studentų g. 54, 51424 Kaunas

Spausdino leidyklos „Technologija" spaustuvė, Studentų g. 54, 51424 Kaunas