European Journal of Information Technologies and Computer Science
www.ej-compute.org

TrES: Tropical Encryption Scheme Based on Double Key Exchange

Mariana I. Durcheva

ABSTRACT

Shor's quantum algorithm establishes a polynomial time attack on the discrete logarithm problem in any group. Recent announcements of progress in building quantum computers highlight the need for new concepts to create cryptosystems that are resistant to quantum attacks. In this paper, we present a new message encryption scheme. To enhance the security of the scheme, we suggest double key-exchange protocol (KEP). The first stage of the key exchange uses a matrix power function (MPF) in a tropical semiring. These functions are based on the action of a matrix semiring acting on some matrix set. MPFs can be considered as one-way functions because they are based on some generalized satisfiability problems that are potentially NP-complete. The obtained shared secret key at the first stage of the key exchange serves as an input for the second stage. The security of the second phase relies on the difficulty of the semiring action problem. In our protocol, we suggest using left or right action of the tropical semiring (which can be both min-plus and max-plus) on the group of commutative matrices (circulant matrices, in our case). The fact that the key-exchange protocol works in two phases contributes to its security, since an attacker needs to solve two difficult problems in order to break it. The main advantages of the presented protocol are: the increased efficiency and improved security.

Keywords: Key-exchange protocol, matrix power function, message encryption scheme, tropical semiring.

Published Online: August 29, 2022

ISSN: 2736-5492

DOI :10.24018/ejcompute.2022.2.4.70

M. I. Durcheva
Sami Shamoon College of Engineering, Israel.
Faculty of Applied Mathematics and Informatics, Technical University of Sofia, Bulgaria.
(e-mail: mdurcheva66@gmail.com)

Corresponding Author

I. Introduction

Employing matrix power function (MPF) for cryptographic purposes was first introduced in [1], [2]. The presented protocols belong to so-called non-commutative cryptography, which is of special interest to researchers. The matrix power function is suitable for use in both symmetric and asymmetric cryptography. In 2016, a linear algebra attack on non-commuting cryptography protocols based on a matrix power function was presented in [3]. Since then, a number of MPF-based protocols have been built using a non-commuting algebraic structure as a platform semigroup [4]-[7].

With a somewhat different background, [8], [9] constructed cryptographic protocols using tropical semirings as building blocks. A series of protocols based on different idempotent semirings was proposed by references [10]-[13]. A review of the cryptanalysis of most schemes known from the literature can be seen in [14]. Reference [15] showed attacks on the protocols presented in [8] based on patterns of higher powers of tropical matrices. To attack some of the well-known tropical protocols, [16] used the so-called almost linear periodic property of the matrices. Different cryptanalysis of the tropical protocols based on solving the tropical discrete logarithm problem was suggested in [17] or based on a simple binary search in [18].

For this reason, cryptographic community began to look for other actions on matrices in tropical semirings. In [19], a public key exchange protocol was constructed based on the semidirect product of two cyclic (semi)groups of matrices (which was successfully attacked in [20] - we recommend [21] as a good survey of semidirect product key-exchange schemes).

However, to the best of our knowledge, research in this direction is insufficient and emphasizes the need for new concepts to build cryptosystems that are resistant to quantum attacks. Developing some ideas from [22], we have built a double key-exchange protocol, which is the basis of our message encryption scheme.

This paper is organized as follows. In Section 2, some preliminaries of the theory of matrix power functions, as well as basic concepts of tropical algebra are given. In Section 3, the first key-exchange protocol is presented. In the next Section 4, a toy example is provided to illustrate the action of the protocol. Section 5 describes a scheme for encrypting messages using a double key-exchange protocol, the first phase of which is based on the key-exchange protocol built in Section 4. Section 6 discusses the security analysis of the scheme. Finally, Section 7 draws conclusions.

II. PRELIMINARIES

A. *Matrix power function* (*MPF*)

Let q be a power of prime, F_q be a finite field of order q, $GLn(F_q)$ be a set of $n\times n$ invertible matrices of F_q-entries, and $Mn(F_q)$ is a set of $n\times n$ matrices of F_q-entries. Then a one-side matrix power function (MPF) can be defined in the following way:

Definition 1. Let matrix $Q=(q_{ij})_{n\times n}$ powered by matrix $Y=(y_{ij})_{n\times n}$ from the right be a matrix $P=(p_{ij})_{n\times n}$ (denoted $P=Q^Y$), and matrix Q powered by matrix $X=(x_{ij})_{n\times n}$ from the left be a matrix $S=(s_{ij})_{n\times n}$ (denoted $S={}^XQ$). The entries of the matrix P are computed according to the formula:

$$p_{ij}=\prod_{k=1}^{n} q_{ik}^{\,y_{kj}}$$

the entries of the matrix S are computed according to the formula:

$$s_{ij}=\prod_{k=1}^{n} q_{kj}^{\,x_{ik}}$$

In another way, this can be interpreted as a mapping [5]:

Definition 2. Let the entries of the base matrix Q be chosen from a (semi)group G and the entries of the matrices X and Y be chosen from a ring $\mathbb{Z}_m$, where m is the maximum multiplicative order of the elements of G. *MPF* is a mapping $F_Q(X,Y)$: Mat($\mathbb{Z}_m$)× Mat(G) → Mat(G) (or a mapping $F_Q(X,Y)$: Mat(G) × Mat($\mathbb{Z}_m$)→ Mat(G)), denoted in the following way: $S={}^XQ$ ($P=Q^Y$).

Example 3. For matrices X, Q and Y of the 2-nd order, we compute the matrices $S={}^XQ$ and $P=Q^Y$ as follows:

$$S={}^{\left(\begin{smallmatrix}x_{11}&x_{12}\\x_{21}&x_{22}\end{smallmatrix}\right)}\begin{pmatrix}q_{11}&q_{12}\\q_{21}&q_{22}\end{pmatrix}=\begin{pmatrix}q_{11}^{\,x_{11}}q_{21}^{\,x_{12}}&q_{12}^{\,x_{11}}q_{22}^{\,x_{12}}\\q_{11}^{\,x_{21}}q_{21}^{\,x_{22}}&q_{12}^{\,x_{21}}q_{22}^{\,x_{22}}\end{pmatrix},$$

$$P=\begin{pmatrix}q_{11}&q_{12}\\q_{21}&q_{22}\end{pmatrix}^{\left(\begin{smallmatrix}y_{11}&y_{12}\\y_{21}&y_{22}\end{smallmatrix}\right)}=\begin{pmatrix}q_{11}^{\,y_{11}}q_{12}^{\,y_{21}}&q_{11}^{\,y_{12}}q_{12}^{\,y_{22}}\\q_{21}^{\,y_{11}}q_{22}^{\,y_{21}}&q_{21}^{\,y_{12}}q_{22}^{\,y_{22}}\end{pmatrix}.$$

Definition 4. The *MPF problem* is to find the matrix X (or Y) when given the base matrix Q and the MPF value matrix S (or P).

B. *Tropical semirings* [23]

A semiring $(R,+,\cdot)$ is called *commutative* if a semigroup $(R,\cdot)$ is commutative. If a commutative semigroup $(R,+)$ is an abelian group, then a semiring is ring. If it is not an abelian group, then the semiring is called a *proper semiring*. An element a of the semiring $(R,+,\cdot)$ is called *additively idempotent* if $a+a=a$. If each element of the semiring is additively idempotent, then R is called an *additively idempotent semiring*. An element a of the semiring $(R,+,\cdot)$ is called *multiplicatively idempotent* if $a\cdot a=a$. If the semiring R is an additively idempotent, then its multiplicatively idempotent elements are called *idempotent elements*, or *idempotents*.

Definition 5. A semiring $R=(R,+,\cdot)$ is called *idempotent* if it is an additively idempotent.

Some examples of idempotent semirings. *Exotic semirings* are idempotent semirings whose elements are from different sets of numbers (it is possible for $-\infty$ and/or $+\infty$ to be included as well) and for which the additive operation is defined by either choosing the minimum or choosing the maximum and the multiplicative operation is the usual addition (+) or multiplication ($\times$).

A semiring $\mathbb{R}_{\max,\min}=\langle\mathbb{R}\cup\{-\infty,+\infty\},\max,\min\rangle$ is an idempotent semiring which is not a semifield. In this semiring $0=-\infty, e=+\infty$. The inverse element with respect to the operation $\min$ does not exist and the maximal element is $+\infty$.

Well studied are the following four idempotent semifields: $\mathbb{R}_{\max,+}=\langle\mathbb{R}\cup\{-\infty\},\max,+\rangle$, $\mathbb{R}_{\min,+}=\langle\mathbb{R}\cup\{+\infty\},\min,+\rangle$, $\mathbb{R}_{\max,\times}=\langle\mathbb{R}_+\cup\{0\},\max,\times\rangle$, $\mathbb{R}_{\min,\times}=\langle\mathbb{R}_+\cup\{+\infty\},\min,\times\rangle$, when $\mathbb{R}$ is the field of the real numbers and $\mathbb{R}_+=\{x\in\mathbb{R}\mid x>0\}$.

Semirings $\mathbb{R}_{\max,+}=\langle\mathbb{R}\cup\{-\infty\},\max,+\rangle$ and $\mathbb{R}_{\min,+}=\langle\mathbb{R}\cup\{+\infty\},\min,+\rangle$ are also called *tropical semirings* in honor of the pioneering work of Imre Simon [24].

C. *Matrices defined over idempotent semifields* [23]

Let $(K,\oplus,\otimes,\varepsilon,\epsilon)$ be an idempotent semifield with ε and ϵ – the neutral elements for the additive operation $\oplus$ and the multiplicative operation $\otimes$ respectively. Let us consider matrices with entries from K. For some random matrices

$$A=(a_{ij})\in K^{m\times n},\ B=(b_{ij})\in K^{m\times n},\ C=(c_{ij})\in K^{n\times l},$$

the operations addition and multiplication of matrices, as well as the operation multiplication of a matrix and a scalar $x\in K$ are defined in the usual way, according to the formulas:

$$(A\oplus B)_{ij}=a_{ij}\oplus b_{ij},\ (B\otimes C)_{ij}=\bigoplus_{k=1}^{n}b_{ik}\otimes c_{kj},\ (x\otimes A)_{ij}=x\otimes a_{ij}.$$

From the properties of the operations in the semifield K, it follows that so defined operations obtain the following properties (as usual, we shall omit the notation $\otimes$ for the multiplication):

1. $A\oplus(B\oplus C)=(A\oplus B)\oplus C$ (associativity);
2. $A\oplus B=B\oplus A$ (commutativity);
3. $A\oplus O=A$ (existence of zero matrix);
4. $A\oplus A=A$ (idempotence);
5. $x(yA)=(xy)A$ (associativity);
6. $A\epsilon=\epsilon A=A$ (existence of unit);
7. $x(A\oplus B)=xA\oplus xB$ (distributivity);
8. $(x\oplus y)A=xA\oplus yA$ (distributivity),

for all matrices $A,B,C\in K^{m\times n}$ and all elements $x,y\in K$.

According to the so described properties, it follows that the set $K^{m\times n}$, together with operations: matrix addition and

multiplication of a matrix and a scalar, is a semimodule over the idempotent semiring K.

Finally, for arbitrary matrices A, B, C and D (of sufficient size, so that the correspondent matrix multiplications exist), we have the following properties:

1. $A(BC) = (AB)C$ (associativity);
2. $B(C \oplus D) = BC \oplus BD$ (distributivity).

Square matrices over idempotent semifields. Let us consider a square matrix $A \in K^{n\times n}$. As usual, the matrix A is called *diagonal*, if all its nondiagonal entries are zeros. The diagonal matrix A with diagonal entries $a_{11},...,a_{nn}$ is denoted by $A = diag(a_{11},...,a_{nn})$. If $a_{ii} \neq \varepsilon$ for all $i = 1,...,n$, then such matrix is said to be *strongly diagonal*. A strongly diagonal matrix $I = diag(1,...,1)$ is called *unit matrix*. The set $K^{n\times n}$ is closed with respect to the matrix multiplication and for arbitrary matrices $A, B, C \in K^{n\times n}$, the following conditions are satisfied:

1. $A(BC) = (AB)C$ (associativity);
2. $AI = IA = A$ (existence of unit matrix);
3. $A(B \oplus C) = AB \oplus AC$ (distributivity).

With respect to the operations matrix addition and matrix multiplication, the set $K^{n\times n}$ assigns commutative idempotent semiring with one.

The operation matrix exponentiation is introduced in the standard way. For an appropriate matrix $A \neq O$ and an integer $p > 0$ we have

$$A^0 = I,\ A^p = A^{p-1}A = AA^{p-1}, O^p = O.$$

D. Polynomials of matrices

Here we use the definitions and notations from [23].

Polynomials in the semiring $\mathbb{R}_{\min}$**.** Let us denote the $n-$th power of x by

$$x^{\odot^{\cdot} n} = \underbrace{x \odot^{\cdot} x \odot^{\cdot} \ldots \odot^{\cdot} x}_{n} = nx.$$

Definition 6. An expression of the type

$$P(x) = \bigoplus\nolimits_{i=0}^{n} a_i \odot^{\cdot} x^{\odot^{\cdot} i}$$

is called *min polynomial*. The integer $n+1$ determines the *length* of the polynomial.

Polynomials in the semirings $\mathbb{R}_{max}$. Let us denote the $n-$th power of x by $x^{\odot_{\cdot} n} = \underbrace{x \odot_{\cdot} x \odot_{\cdot} \ldots \odot_{\cdot} x}_{n} = nx.$

Definition 7. An expression of the type

$$P(x) = \bigoplus\nolimits_{i=0}^{n} a_i \odot_{\cdot} x^{\odot_{\cdot} i}$$

is called *max polynomial*, where $n+1$ determines the length of the polynomial.

Min and max polynomials are called *tropical polynomials*.

Proposition 8. Let $p(x), t(x)$ be tropical polynomials, and M be a given matrix. Then

$$p(M) \otimes t(M) = t(M) \otimes p(M),$$

where $\otimes$ is a multiplication of the polynomials in the selected semiring.

Proof. Follows from the definitions of operations in tropical semirings.

E. Definition of a Matrix Power Function in Terms of Tropical Algebra

Definition 9. Let the entries of the base matrix Q be chosen from a (semi)group G and the entries of the matrices X and Y be chosen from the tropical semiring $\mathbb{R}_{\min,+} = \langle \mathbb{R} \cup \{+\infty\}, \min, + \rangle$ (or $\mathbb{R}_{\max,+} = \langle \mathbb{R} \cup \{-\infty\}, \max, + \rangle$). Then *MPF* is a mapping

$$F_Q(X) : \mathrm{Mat}(\mathbb{R}_{\min,+}) \times \mathrm{Mat}(G) \to \mathrm{Mat}(G)$$

(denoted in the following way: $S = {}^{X}Q$), or a mapping

$$F_Q(Y) : \mathrm{Mat}(G) \times \mathrm{Mat}(\mathbb{R}_{\min,+}) \to \mathrm{Mat}(G)$$

(denoted: $S = {}^{X}Q$ ($P = Q^{Y}$).

The elements of the matrix P are computed according to the formula:

$$p_{ij} = \bigotimes_{k=1}^{n} q_{ik}^{\otimes y_{kj}} = \sum_{k=1}^{n} q_{ik} \cdot y_{kj} \qquad (1)$$

and the elements of the matrix S are computed according to the formula:

$$s_{ij} = \bigotimes_{k=1}^{n} q_{kj}^{\otimes x_{ik}} = \sum_{k=1}^{n} q_{kj} \cdot x_{ik}\ . \qquad (2)$$

Example 10. For tropical matrices X, Q and Y of the 2-nd order, we compute the matrices $S = {}^{X}Q$ and $P = Q^{Y}$ in the following way:

$$S = {}^{\otimes\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}}\begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix} =$$

$$\begin{pmatrix} q_{11}^{\otimes x_{11}} \otimes q_{21}^{\otimes x_{12}} & q_{12}^{\otimes x_{11}} \otimes q_{22}^{\otimes x_{12}} \\ q_{11}^{\otimes x_{21}} \otimes q_{21}^{\otimes x_{22}} & q_{12}^{\otimes x_{21}} \otimes q_{22}^{\otimes x_{22}} \end{pmatrix} =$$

$$\begin{pmatrix} q_{11}x_{11} + q_{21}x_{12} & q_{12}x_{11} + q_{22}x_{12} \\ q_{11}x_{21} + q_{21}x_{22} & q_{12}x_{21} + q_{22}x_{22} \end{pmatrix},$$

$$P = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}^{\otimes\begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}} =$$

$$\begin{pmatrix} q_{11}^{\otimes y_{11}} \otimes q_{12}^{\otimes y_{21}} & q_{11}^{\otimes y_{12}} \otimes q_{12}^{\otimes y_{22}} \\ q_{21}^{\otimes y_{11}} \otimes q_{22}^{\otimes y_{21}} & q_{21}^{\otimes y_{12}} \otimes q_{22}^{\otimes y_{22}} \end{pmatrix} =$$

$$\begin{pmatrix} q_{11}y_{11} + q_{12}y_{21} & q_{11}y_{12} + q_{12}y_{22} \\ q_{21}y_{11} + q_{22}y_{21} & q_{21}y_{12} + q_{22}y_{22} \end{pmatrix}.$$

Proposition 11. The MPF is one-side (left-side or right-side) associative, i.e., the following identities hold:

$${}^{Z}\left({}^{X}Q\right) = {}^{ZX}Q = {}^{XZ}Q\ ,\ \left(Q^{Y}\right)^{T} = Q^{YT} = Q^{TY}\ .$$

Proof. Follows from the definition of MPF.

F. Employing circulant matrices

In our protocol, we need commutative matrices, so we suggest using a set of circulant matrices [25], [26].

Lemma 12. Let Q, S and P be circulant matrices. Then the matrices $P = Q^{Y}$ and $S = {}^{X}Q$ are also circulant.

Proof. Follows from the definition of circulant matrices and (1), (2).

Lemma 13. Let Q, A and B be circulant matrices. Then

$${}^{B}Q \otimes {}^{A}Q = {}^{A}Q \otimes {}^{B}Q,\ Q^{B} \otimes Q^{A} = Q^{A} \otimes Q^{B}.$$

Proof. Follows from Lemma 12 and the definition of circulant matrices.

Theorem 14. Let Q_1, Q_2, A_1, A_2, B_1, B_2 be circulant matrices. Then

$${}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2, \quad (3)$$

$$Q_1{}^{B_1} \otimes Q_2{}^{B_2} \otimes Q_1{}^{A_1} \otimes Q_2{}^{A_2} = Q_1{}^{A_1} \otimes Q_2{}^{A_2} \otimes Q_1{}^{B_1} \otimes Q_2{}^{B_2}. \quad (4)$$

Proof. Matrices ${}^{A_1}Q_1$, ${}^{A_2}Q_2$, ${}^{B_1}Q_1$, ${}^{B_2}Q_2$, $Q_1{}^{A_1}, Q_2{}^{A_2}, Q_1{}^{B_1}, Q_2{}^{B_2}$ are circulant. Then (3) and (4) follow from Lemma 13.

III. Key Exchange Protocol using MPF

The implementation of the protocol requires the definition of both a matrix semiring over a commutative semiring ***Ms*** and a set of matrices M over a semigroup G. We suggest ***Ms*** to be the set of circulant matrices over the tropical semiring $\mathbb{R}_{\min,+} = \langle \mathbb{R}, \min, + \rangle$ (or $\mathbb{R}_{\max,+} = \langle \mathbb{R}, \max, + \rangle$) and G be the semigroup of matrices with entries from $\mathbb{R}$. The protocol works both in the case of a left action and in the case of a right action.

The parameters of the domain are: tropical semiring $\mathbb{R}_{\min,+} = \langle \mathbb{R}, \min, + \rangle$ (or $\mathbb{R}_{\max,+} = \langle \mathbb{R}, \max, + \rangle$), two circulant matrices Q_1 and Q_2 from ***Ms***, and a randomly chosen matrix M whose entries are from $\mathbb{R}$.

1) Alice selects as her secret key two circulant matrices A_1 and A_2. She calculates her public key
$$K_A = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M.$$
2) Alice sends her public key K_A to Bob.
3) Bob selects as his secret key two circulant matrices B_1 and B_2. He calculates his public key
$$K_B = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M.$$
4) Bob sends his public key K_B to Alice.
5) Alice computes the common secret key:
$$K_{AB} = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes K_B = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M.$$
6) Bob computes the common secret key:
$$K_{BA} = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes K_A = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M.$$

Proposition 15. Alice's key K_{AB} and Bob's key K_{BA} are equal.

Proof. Theorem 14 implies that for circulant matrices Q_1, Q_2, A_1, A_2, B_1, B_2 holds:

$${}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes {}^{A_1}Q_1 \otimes {}^{A_2}Q_2.$$

Then

$$K = K_{AB} = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M =$$
$${}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M = K_{BA}.$$

The security of the protocol relies on the difficulty of the following

Tropical Matrix Power Function Problem 16. Given a matrix K_A, two circulant matrices Q_1, Q_2, and a matrix find two circulant matrices A_1, A_2 such that

$$K_A = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M$$

(or solve a similar problem for Bob's public key K_B).

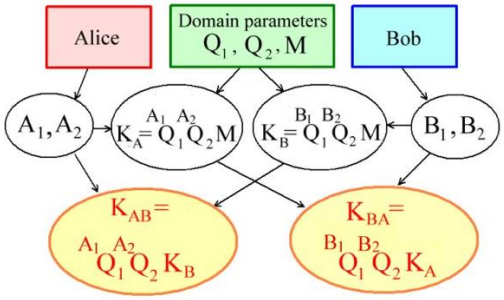

Fig. 1. Key-exchange protocol based on tropical MPF.

The difficulty of this problem is based on the difficulty of the MPF problem which "can be a candidate one-way function, since the effective (polynomial-time) inversion algorithm for it is not yet known" [2] and the matrix decomposition problem [27]. Fig. 1 shows the concept of the key-exchange process.

IV. A Toy Example

The parameters of the domain are: tropical semiring $\mathbb{Z}_{\min,+} = \langle \mathbb{N}, \min, + \rangle$, two circulant matrices Q_1 and Q_2 from ***Ms***, and a randomly selected matrix M which elements are from $\mathbb{N}$.

$$Q_1 = \begin{pmatrix} 7 & 13 & 22 \\ 22 & 7 & 13 \\ 13 & 22 & 7 \end{pmatrix}, Q_2 = \begin{pmatrix} 5 & 16 & 25 \\ 25 & 5 & 16 \\ 16 & 25 & 5 \end{pmatrix}, M = \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix}$$

1) Alice selects as her secret key two circulant matrices:
$$A_1 = \begin{pmatrix} 6 & 30 & 20 \\ 20 & 6 & 30 \\ 30 & 20 & 6 \end{pmatrix}, A_2 = \begin{pmatrix} 10 & 12 & 27 \\ 27 & 10 & 12 \\ 12 & 27 & 10 \end{pmatrix}.$$

She calculates $K_A = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M$:

$${}^{A_1}Q_1 = \begin{pmatrix} 6 & 30 & 20 \\ 20 & 6 & 30 \\ 30 & 20 & 6 \end{pmatrix}^{\otimes} \begin{pmatrix} 7 & 13 & 22 \\ 22 & 7 & 13 \\ 13 & 22 & 7 \end{pmatrix} =$$
$$= \begin{pmatrix} 962 & 728 & 662 \\ 662 & 962 & 728 \\ 728 & 662 & 962 \end{pmatrix},$$

$${}^{A_2}Q_2 = \begin{pmatrix} 10 & 12 & 27 \\ 27 & 10 & 12 \\ 12 & 27 & 10 \end{pmatrix}^{\otimes} \begin{pmatrix} 5 & 16 & 25 \\ 25 & 5 & 16 \\ 16 & 25 & 5 \end{pmatrix} =$$
$$= \begin{pmatrix} 782 & 895 & 577 \\ 577 & 782 & 895 \\ 895 & 577 & 782 \end{pmatrix},$$

$$^{A_1}Q_1 \otimes {}^{A_2}Q_2 = \begin{pmatrix} 962 & 728 & 662 \\ 662 & 962 & 728 \\ 728 & 662 & 962 \end{pmatrix} \otimes \begin{pmatrix} 782 & 895 & 577 \\ 577 & 782 & 895 \\ 895 & 577 & 782 \end{pmatrix}$$

$$= \begin{pmatrix} 1305 & 1239 & 1444 \\ 1444 & 1305 & 1239 \\ 1239 & 1444 & 1305 \end{pmatrix},$$

$$K_A = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes M =$$

$$\begin{pmatrix} 1305 & 1239 & 1444 \\ 1444 & 1305 & 1239 \\ 1239 & 1444 & 1305 \end{pmatrix} \otimes \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix}$$

$$= \begin{pmatrix} 1267 & 1253 & 1252 \\ 1242 & 1246 & 1258 \\ 1247 & 1241 & 1254 \end{pmatrix}.$$

2) Alice sends her public key K_A to Bob.

3) Bob selects as his secret key two circulant matrices:

$$B_1 = \begin{pmatrix} 2 & 10 & 21 \\ 21 & 2 & 10 \\ 10 & 21 & 2 \end{pmatrix}, B_2 = \begin{pmatrix} 15 & 24 & 17 \\ 17 & 10 & 24 \\ 24 & 17 & 10 \end{pmatrix}.$$

He calculates $K_B = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M$:

$$^{B_1}Q_1 = {}^{\otimes \begin{pmatrix} 2 & 10 & 21 \\ 21 & 2 & 10 \\ 10 & 21 & 2 \end{pmatrix}} \begin{pmatrix} 7 & 13 & 22 \\ 22 & 7 & 13 \\ 13 & 22 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 507 & 558 & 321 \\ 321 & 507 & 558 \\ 558 & 321 & 507 \end{pmatrix},$$

$$^{B_2}Q_2 = {}^{\otimes \begin{pmatrix} 15 & 24 & 17 \\ 17 & 10 & 24 \\ 24 & 17 & 10 \end{pmatrix}} \begin{pmatrix} 5 & 16 & 25 \\ 25 & 5 & 16 \\ 16 & 25 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 947 & 785 & 844 \\ 844 & 947 & 785 \\ 785 & 844 & 947 \end{pmatrix},$$

$$^{B_1}Q_1 \otimes {}^{B_2}Q_2 = \begin{pmatrix} 507 & 558 & 321 \\ 321 & 507 & 558 \\ 558 & 321 & 507 \end{pmatrix} \otimes \begin{pmatrix} 947 & 785 & 844 \\ 844 & 947 & 785 \\ 785 & 844 & 947 \end{pmatrix}$$

$$= \begin{pmatrix} 1106 & 1165 & 1268 \\ 1268 & 1106 & 1165 \\ 1165 & 1268 & 1106 \end{pmatrix},$$

$$K_B = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes M =$$

$$\begin{pmatrix} 1106 & 1165 & 1268 \\ 1268 & 1106 & 1165 \\ 1165 & 1268 & 1106 \end{pmatrix} \otimes \begin{pmatrix} 8 & 2 & 15 \\ 28 & 14 & 13 \\ 3 & 7 & 19 \end{pmatrix}$$

$$= \begin{pmatrix} 1114 & 1108 & 1121 \\ 1134 & 1120 & 1119 \\ 1109 & 1113 & 1125 \end{pmatrix}.$$

4) Bob sends his public key K_B to Alice.

5) Alice computes the common key

$$K_{AB} = {}^{A_1}Q_1 \otimes {}^{A_2}Q_2 \otimes K_B =$$

$$\begin{pmatrix} 1305 & 1239 & 1444 \\ 1444 & 1305 & 1239 \\ 1239 & 1444 & 1305 \end{pmatrix} \otimes \begin{pmatrix} 1114 & 1108 & 1121 \\ 1134 & 1120 & 1119 \\ 1109 & 1113 & 1125 \end{pmatrix}$$

$$= \begin{pmatrix} 2373 & 2359 & 2358 \\ 2348 & 2352 & 2364 \\ 2353 & 2347 & 2360 \end{pmatrix}.$$

6) Bob computes the common key

$$K_{BA} = {}^{B_1}Q_1 \otimes {}^{B_2}Q_2 \otimes K_A =$$

$$\begin{pmatrix} 1106 & 1165 & 1268 \\ 1268 & 1106 & 1165 \\ 1165 & 1268 & 1106 \end{pmatrix} \otimes \begin{pmatrix} 1267 & 1253 & 1252 \\ 1242 & 1246 & 1258 \\ 1247 & 1241 & 1254 \end{pmatrix}$$

$$= \begin{pmatrix} 2373 & 2359 & 2358 \\ 2348 & 2352 & 2364 \\ 2353 & 2347 & 2360 \end{pmatrix}.$$

At the end of the protocol they share the same key *K*.

V. Message Encryption Scheme Based on MPF

A comparison between symmetric and asymmetric encryption protocols [28], [29] has shown that symmetric algorithms (like AES) are better than asymmetric algorithms (like RSA), mainly due to the better execution time. One of the goals of asymmetric cryptography researchers is to find new primitives in order to improve the execution time of the protocols. MPF-based protocol presented in [2] and [7] is in some respects more efficient than RSA asymmetric encryption [30]. This motivates us to build a protocol using MPF, but in tropical algebra, where the operations are faster than in usual algebra. The encryption scheme proposed here is based on a double KEP, the first phase of which is the presented in Section 3 protocol.

Let the sender Bob be willing to send a message *S* to the receiver Alice. Alice and Bob need to agree on: a tropical semiring $\mathbb{Z}_{\min,+} = \langle \mathbb{N}, \min, + \rangle$ (or $\mathbb{Z}_{\max,+} = \langle \mathbb{N}, \max, + \rangle$), an action (left or right), two circulant matrices Q_1 and Q_2 from

$\boldsymbol{M_S}$, and a randomly chosen matrix M whose entries are from $\mathbb{N}$. Additionally, each user needs to choose two tropical polynomials. According to the structure of the proposed scheme, S is a matrix (of the same order as the previously selected matrices Q_1, Q_2 and M) with entries coded in binary form.

First key-exchange phase. Alice and Bob obtain the same secret key K using the key-exchange protocol (KEP) described in Section 3.

Second key-exchange phase. At this phase, the obtained shared secret key K serves as an input.

1) Bob chooses two tropical polynomials $d(x), e(x)$.
2) He computes his public matrix
$$B = d(M) \otimes K \otimes e(M)$$
and sends it to Alice.
3) Alice chooses two tropical polynomials $p(x), t(x)$.
4) She computes her public matrix
$$A = p(M) \otimes K \otimes t(M)$$
and sends it to Bob.

Encryption phase.

5) Bob computes his secret key:
$$F = d(M) \otimes A \otimes e(M) =$$
$$d(M) \otimes p(M) \otimes K \otimes t(M) \otimes e(M).$$
6) Bob computes the ciphertext $C = F \oplus S$, where $\oplus$ is bitwise sum modulo 2 of all entries of the matrices F and S, and sends it to Alice.

Decryption phase.

7) Alice computes her secret key:
$$p(M) \otimes B \otimes t(M) =$$
$$p(M) \otimes d(M) \otimes K \otimes e(M) \otimes t(M).$$
According to Proposition 8, Alice obtained the same secret key F as Bob:
$$p(M) \otimes B \otimes t(M) =$$
$$p(M) \otimes d(M) \otimes K \otimes e(M) \otimes t(M) =$$
$$d(M) \otimes p(M) \otimes K \otimes t(M) \otimes e(M) = F.$$
8) Alice can now decrypt the ciphertext C using the decryption key F and the relation:
$$S = F \oplus C = F \otimes F \oplus S.$$

VI. Security Analysis

To enhance the security of the presented message encryption scheme, we suggested double KEP. So, in order to break this protocol, an attacker needs first to solve the following problem:

- **The Tropical Matrix Power Function Problem 16** to obtain the secret key K.

Even if the attacker was able to break the first KEP and get K, in the second stage, he needs to solve:

- **The Semiring Action Problem**. Given two matrices $M \in \mathbb{M}^{n\times n}(\bar{D})$, $K \in \mathbb{M}^{n\times n}(S)$, and a matrix of the type
$$T \in S_1[M] \otimes K \otimes S_1[M], \quad (5)$$
find two matrices $U_1 \in S_1[M]$ and $U_2 \in S_1[M]$, such that
$$T = U_1 \otimes K \otimes U_2.$$

In this case, matrix T can be matrix A, which is Alice's public key, or (which is the same) Bob's matrix B and $S_1[M]$ is the matrix semiring generated by the matrix M. This means that in order to break the protocol, the following two-sided matrix equation must be solved:
$$T = U_1 \otimes K \otimes U_2,$$
where U_1 and U_2 are unknown matrices, and T, K are known matrices.

A general solution to the equation of this type is not known [23].

An attacker has two options for breaking this double KEP:

A. In the first one, he must first solve the **Tropical Matrix Power Function Problem 16,** and then, knowing K, to solve **The Semiring Action Problem;**
B. In the second one, the attacker does not know the matrix K. So, he needs to find a solution to (5), knowing only matrices T and M.

Since such problems as those posed in B are not solved in the literature known to us, we believe that in both cases, the attacker needs to solve hard problems, which guarantees the security of the proposed scheme.

VII. Conclusion

In this paper, we introduced a new message encryption scheme based on the double key-exchange protocol. For the first phase of the KEP, we constructed a key-exchange protocol using a matrix power function as the action of a tropical semiring on the set of matrices. The obtained common secret key serves as an input for the second phase of the KEP.

For our protocols we suggest using both left and right action, as well as isomorphic tropical semirings $\mathbb{Z}_{\min,+} = \langle \mathbb{N}, \min, + \rangle$ and $\mathbb{Z}_{\max,+} = \langle \mathbb{N}, \max, + \rangle$.

We note that in the KEP of the first phase, no power of a matrix is used, so all standard attacks based on solving the tropical discrete logarithm problem are not applicable here. Due to the fact that tropical matrices are non-invertible, the KEP of second phase is not vulnerable to linear algebra attacks.

As it is well known, one of the advantages of tropical algebra over classical algebra is increased efficiency, since tropical addition is actually finding a minimum or maximum, and multiplication is usual addition.

Therefore, we believe that the increased efficiency along with improved security makes our protocol very suitable for a cryptographic implementation.

References

[1] Sakalauskas E, Listopadskis N, Tvarijonas P. Key agreement protocol (KAP) based on matrix power function. *Advanced Studies in Software and Knowledge Engineering, Information Science and Computing.* 2008: 92–96.
[2] Sakalauskas E, Mihalkovich A. New Asymmetric Cipher of Non-Commuting Cryptography Class Based on Matrix Power Function. *INFORMATICA*. 2014; 25(2): 283–298.
[3] Liu J, Zhang H, Jia J. A linear algebra attack on the non-commuting cryptography class based on matrix power function. *International Conference on Information Security and Cryptology*, Springer: Cham, Switzerland, 2016: 343–354.

[4] Sakalauskas E, Mihalkovich A. MPF Problem over Modified Medial Semigroup Is NP-complete. *Symmetry* 2018; 10: 571.
[5] Mihalkovich A, Sakalauskas E, Luksys K. Key Exchange Protocol Defined over a Non-Commuting Group Based on an NP- complete Decisional Problem. *Symmetry* 2020; 12(9): 1389,
[6] Sakalauskas E. Enhanced matrix power function for cryptographic primitive construction, *Symmetry*. 2018; 10(2): 43.
[7] Sakalauskas E, Mihalkovich A. New Asymmetric Cipher of Non-Commuting Cryptography Class Based on Matrix Power Function. *INFORMATICA*. 2017; 28(3): 517–524.
[8] Grigoriev D, Shpilrain V. Tropical cryptography. *Communications in Algebra*. 2014; 42: 2624–2632.
[9] Grigoriev D, Shpilrain V. Tropical cryptography II: extensions by homomorphisms. *Communications in Algebra*. 2019; 47(10): 4224–4229,
[10] Durcheva M, Trendafilov I. Public Key Cryptosystem Based on Max – Semirings. *AMEE, 38th International Conference, AIP Conference Proceeding*. 2012; 1497(1): 357- 364.
[11] Durcheva M. Public Key Cryptography with max-plus matrices and polynomials. *AMEE 39th International Conference, AIP Conference Proceeding*. 2013, 1570(1): 491–498.
[12] Durcheva M. An application of different dioids in public key cryptography. *AMEE 40th International Conference, AIP Conference Proceeding*. 2014; 1631(1): 336–345.
[13] Durcheva M, Rachev M. A public key encryption scheme based on idempotent semirings. *AMEE 41th International Conference, AIP Conference Proceeding*. 2015; 1690(1): 060008.
[14] Ahmed K, Pal S, Mohan R. A review of the tropical approach in cryptography. *Cryptologia*. 2022.
[15] Kotov M, Ushakov A. Analysis of a Key Exchange Protocol based on Tropical Matrix Algebra. *Journal of Mathematical Cryptology*. 2018; 12(3): 137–141.
[16] Isaac S, Kahrobaei D. A closer look at the tropical cryptography. *International Journal of Computer Mathematics: Computer Systems Theory*. 2021; 6(2): 137-142.
[17] Muanalifah A, Sergeev S. On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *Communications in Algebra*. 2020.
[18] Rudy D, Monico C. Remarks on a Tropical Key Exchange System. *Journal of Mathematical Cryptology*. 2020; 15(1): 280–283.
[19] Rahman N, Shpilrain V. MAKE: A matrix action key exchange. *Journal of Mathematical Cryptology*. 2022; 16(1): 64-72.
[20] Brown DRL, Koblitz N, LeGrow JT. Cryptanalysis of "MAKE", *Journal of Mathematical Cryptology*. 2022; 16: 98–102.
[21] Battarbee C, Kahrobaei D, Shahandashti S. Semidirect Product Key Exchange: the State of Play, Arxiv. [Preprint] 2022. Available from: https://arxiv.org/pdf/2202.05178.pdf.
[22] Ayoub M. Key Exchange Protocol Based on MPF and Circulant Matrix over Tropical Algebras. M. S. Thesis. Capital University of Science and Technology, Islamabad, 2021.
[23] Durcheva M. Semirings as building blocks in cryptography. *Monograph, Cambridge Scholars Publishing*. 2020.
[24] Pin J-E. Tropical Semirings. 1998: 50-69.
[25] Davis PJ. Circulant Matrices. 1994.
[26] Fuhrmann PA. A Polynomial Approach to Linear Algebra. *Universitext, Springer*. 1996.
[27] Bassino F, Kapovich I, Lohrey M, Miasnikov A, Nicaud C, Nikolaev A, et al. 6 Problems in group theory motivated by cryptography, *Complexity and Randomness in Group Theory*: *GAGTA BOOK 1*. 2020: 317-348.
[28] Singh G, Supriya. A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*. 2013; 67(19).
[29] Marqas RB, Almufti SM, Ihsan RR. Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. *Journal of Xi'an University of Architecture & Technology*. 2020; III(1006-7930).
[30] Mihalkovich A, Levinskas M. Investigation of Matrix Power Asymmetric Cipher Resistant to Linear Algebra Attack. *Springer Nature Switzerland AG* 2019. 2019: 197–208.