Journal of Natural Sciences and Mathematics Research
J. Nat. Scien. & Math. Res. Vol. 9 No. 2 (2023) 151-157
ISSN: 2460-4453 (Online); 2614-6487 (Printed)
Available online at http://journal.walisongo.ac.id/index.php/jnsmr

The tropical version of El Gamal Encryption

Any Muanalifah[1*], Ayus Riana I.[2], Rosalia Artes Jr.[3], Nurwan[4]
[1,2]Department of Mathematics, UIN Walisongo, Indonesia.
[3]Mathematics and Science Department, Mindanao State University, Philippines.
[4]Department of Mathematics, Universitas Negeri Gorontalo, Indonesia.

[*]Corresponding author(s). E-mail(s): any.muanalifah@walisongo.ac.id;
Contributing authors: ariana@walisongo.ac.id; rosalioartes@mustawi-tawi.edu.pd; nurwan@ung.ac.id .

ABSTRACT
In this paper, we consider the new version of tropical cryptography protocol, i.e the tropical version of El Gamal encryption. We follow the ideas and modify the clasical El Gamal encryption using tropical matrices and matrix power in tropical algebra. Then we also provide a toy example for the reader's understanding.
Keywords: Tropical algebra; tropical matrix; tropical cryptography; El Gamal Encryption.

Introduction

El Gamal encryption was inveted in 1985 by Taher Gamal (Elgamal, 1985) . The idea of this algorithm based on the most popular public key exchange protocol,i.e., the Diffie-Hellman protocol. Furthermore, he made the Diffie-Hellman system better and came up with two algorithms that could be used for encryption and authentication. Since El Gamal Encryption using the idea of Diffie-Hellamn protocol then the security based on the complexity to solve the Discrete Logarithm Problem (DLP). As we know there is no efficient algorithm can be solved the DLP unless quantum computer can be used.

The effectiveness and safety of any cryptography system are determined by the algorithm and the platform employed. Some researcher are trying to find the best platform to construct the new protocol. There is a new study cryptography in tropical algebra. Tropical algebra studies linear algebra over semiring. Tropical algebra is a semiring $\mathbb{R} \cup \{-\infty\}$ endowed with two binary operations i.e maximisation $(\oplus)$ and addition $(\otimes)$. The algebraic structure is denoted by $\mathbb{R}_{\max} = (\mathbb{R} \cup \{-\infty\}, \oplus, \otimes)$. Suppose we have $a, b \in \mathbb{R}_{\max}$, then we define $a \oplus b := \max(a, b)$ and $a \otimes b := a + b$. For further reading in tropical algebra, we can find in, e.g, (Butkovič, 2010), (Baccelli et al., 1992), (Burkard & Butkovic, 2003), (Bart & Boom, 2008) and (Cohen et al., 1999) .

Since tropical multiplication is equivalent to addition, computing in a tropical setting is unquestionably faster than its classical analogue. Many previous attempts have been made to provide a practical and safe key exchange mechanism based on tropical matrix algebra. The researchers who introduced the new concept of tropical cryptography are Dima Grigoriev and Vladimir Sphilrain (Grigoriev & Shpilrain, 2014). They modify the Stickel's protocol using polynomial over tropical matrix algebra. Then some studies in tropical cryptography are followed such that (Grigoriev & Ponomarenko, 2005), (Grigoriev & Shpilrain, 2018), (Grigoriev & Shpilrain, 2019),(Muanalifah & Sergeev, 2020), (Ahmed et al., 2023a),(Ahmed et al., 2023b), (Durcheva et al., 2014). For analysis security the tropical cryptography, there are also some studies such that (Kotov & Ushakov, 2018),(Muanalifah & Sergeev, 2022),(Isaac & Kahrobaei, 2021),(Rudy & Monico, 2020), (Huang et al., 2022).

Therefore, in this paper we introduce a new tropical version of El Gamal encryption. Using the similar ideas to the classical one we replace the integers number by matrix over tropical algebra. Since the invertible matrices in tropical algebra only diagonal matrix and permutation matrix then we use tropical diagonal matrices for decryption step. We also give a toy example for the reader's understanding.

Tropical Algebra

In this section, we define tropical algebra and tropical matrices in their most fundamental form.

2.1 Basic Definition

Let us introduce the definition of semiring

Definition 2.1. Given a non empty set S with two binary operations $+$ and $\times$ then we call $(S, +, \times)$ semiring if for all $a, b, c \in S$ which satisfy the following conditions:

1. $(S, +)$ is an abelian monoid, that means:
   (i) Associativity
   $(a + b) + c = a + (b + c)$
   (ii) Identity element
   There exists $0 \in S$ such that $0 + a = a + 0 = a$
   (iii) Commutativity
   $a + b = b + a$
2. $(S, \times)$ is a monoid, that means:
   (i) Associativity
   $(a + b) + c = a + (b + c)$
   (ii) Identity element
   There exists $1 \in S$ such that $1 \times a = a \times 1 = a$
3. $(S, +, \times)$ is distributive
   (i) $a \times (b + c) = (a \times b) + (a \times c)$
   (ii) $(b + c) \times a = (b \times a) + (c \times a)$
4. Absorbing property of 0: $0 \times 1 = 1 \times 0 = 0$

Then some studies in tropical algebra are followed such that (Gaubert & Plus, 1997), and (Akian et al., 2013). Tropical algebra is one of example of semiring:

Example 2.1. Let the set $\mathbb{R} \cup \{-\infty\}$ with two binary operations $\oplus$ and $\otimes$ be defined as tropical semiring $(\mathbb{R}_{\max} = (\mathbb{R} \cup \{-\infty\}, \oplus, \otimes))$. For all $a, b \in \mathbb{R}_{\max}$ then we have

$$a \oplus b = \max(a, b),\ a \otimes b = a \times b$$

The element identity respect to maximization and also addition are $-\infty$ and 0, respectively.

2.2 Tropical Matrices

In the section, we will introduce some terms in tropical matrices.

Definition 2.2. Let us define the tropical matrix identity $I \in \mathbb{R}_{\max}^{n \times n}$ where the diagonal entries equals to 0 and non diagonal entries equals to $-\infty$.

Definition 2.3. If the diagonal entries of tropical square matrix equal to any numbers in $\mathbb{R}_{\max}$ and non diagonal entries equal to $-\infty$ then we called this kind of matrix as tropical diagonal matrix denoted by D.

We can also extend the arithmetic operation of $\oplus$ and $\otimes$ to vectors and matrices as in the following definition:

Definition 2.4. (Matrix addition and multiplication)

Let k be a scalar in $\mathbb{R}_{\max}$ and matrix $A = (a_{ij}) \in \mathbb{R}^{m\times n}$, (i.e tropical matrix with dimension $m \times n$), then we define

$$(k \otimes A)_{ij} = k \otimes (a_{ij}), \forall i = 1, \dots, m \text{ and } j = 1, \dots, n.$$

If we have two tropical matrices $A = (a_{ij})$ and $B = (b_{ij})$ with the same dimension $m \times n$, then we define

$$(A \oplus B)_{ij} = \max(a_{ij}, b_{ij}), \forall\, i = 1, \dots, m \text{ and } j = 1, \dots, n.$$

If we have two matrices $A = (a_{ij}) \in \mathbb{R}_{\max}^{m\times p}$ and $B = (b_{ij}) \in \mathbb{R}_{\max}^{p\times n}$ then we define

$$(A \otimes B)_{ij} = \bigoplus_{k=1}^{p} a_{ik} \otimes b_{kj}, \forall\, i = 1, \dots, m \text{ and } j = 1, \dots, n.$$

Next, we will discuss the definition of tropical matrix powers.

Definition 2.5 (Tropical Matrix powers)

Let A be a tropical square matrix. Then we define the nth tropical matrix of A

$$A^{\otimes n} = \underbrace{A \otimes A \otimes \dots \otimes A}_{n}$$

We have $A^{\otimes 0} = I$.

We can also study the behaviour of tropical matrix powers (Elsner & Driessche, 1999), (Elsner & Driessche, 2001), ,(Sergeev & Schneider, 2012), (Akian et al., 2013), (Nishida, 2023), and apply it for analyse the security of our cryptosystem.

Tropical Version of El Gamal Encryption

We first recall the classical version of El Gamal encryption as follows:

Algorithm 3.1 (El gamal Encryption).

Alice and Bob agree on public parameter: finite group $\mathbb{Z}_{p,}$ prime number p and generator $g \in \mathbb{Z}_p$

Key Generation

In this part, Alice will generate her public key and sends it to Bob.

1. Alice chooses random integer number x and computes $u = g^x \bmod p$
2. Alice sends the public key u to Bob

Encryption Bob is here with a message m and he wants to send the message to Alice. In order to protect his message then Bob encrypt the message as follows.

- Bob randomly chooses integer number y.
- Bob computes his public key $v = g^x$.
- Bob then computes his secret key using u and get $K_B = (u)^y \bmod p$.
- Using his secret key K_B then he decrypt the message into chiper text $c = m \otimes S$.
- Bob then sends c and v to Alice

Decryption

In order to reveal the message m, Alice does the following step:

- Compute $K_A = v^x$
- Compute $m = c \otimes K_A^{-1}$

Following the idea of classical El Gamal encryption then we modify the algorithm (3.1) using matrix over tropical algebra.

Let us define the set $\mathbb{Z} \cup \{-\infty\}$ subset of $\mathbb{R} \cup \{-\infty\}$ then we can also define the subsemiring $\mathbb{Z}_{\max}$ of $\mathbb{R}_{\max}$ in this paper we use $\mathbb{Z}_{\max}$ instead of $\mathbb{R}_{\max}$

We next introduce the tropical version of El Gamal Encryption.

Algorithm 3.2 (Tropical El Gamal Encryption)

Alice and Bob agree on public parameters: prime number p and matrix $G \in M_n(\mathbb{Z}_{\max})$ (i.e matrix $n \times n$ with entries in $\mathbb{Z}_{\max}$).

Key Generation

- Alice chooses a random integer x
- Alice computes $U = G^{\otimes x} \bmod p$ and sends it to Bob

Encryption

Bob has message m

- Bob randomly chooses integer number y
- Bob computes $K_B = U^{\otimes y} \bmod p$
- He computes $V = G^{\otimes y}$
- Bob change matrix K_B to matrix diagonal form and then encrypt the message $c = m \otimes K_B$
- Then Bob sends c and V to alice

Decryption

Alice then decrypts the messge in the folloing steps:

- Alice computes her private $K_A = V^x$ and then change it to diagonal matrix.
- Alice decrypts the message $m = m \otimes K_A^{-1}$

Since the invertible matrices in tropical algebra only tropical diagonal matrices and permutation matrices then we transform the secret key of Alice K_A and the secret key of Bob K_B to diagonal matrices (replace non diagonal entries with $-\infty$).

A Toy Example

We give toy example as follows: Let Alice and Bob agree on public parameter $p = 73$ and public matrix $G = \begin{pmatrix} 67 & 71 \\ 23 & 56 \end{pmatrix} \in M_2(\mathbb{Z}_{max})$.

Key Generation

In this part, Alice generates the public key and private key in the following steps:

1. Alice picks at random integer number $x = 57$
2. Alice computes her public key $U = G^x = \begin{pmatrix} 67 & 71 \\ 23 & 56 \end{pmatrix}^{57} = \begin{pmatrix} 819 & 3823 \\ 3775 & 3779 \end{pmatrix} \bmod 73 = \begin{pmatrix} 23 & 27 \\ 52 & 56 \end{pmatrix}$.
3. Alice sends U to Bob

Encryption

In this part, Bob has a message $M = Eve$ want to kill you. Before he sends the message to Alice then Bob divide the message into some blocks of matrices as follows:

$$m_1 = \begin{pmatrix} E & v \\ e & space \end{pmatrix}, m_2 = \begin{pmatrix} w & a \\ n & t \end{pmatrix}, m_3 = \begin{pmatrix} t & o \\ space & k \end{pmatrix}, m_4 = \begin{pmatrix} i & l \\ l & u \end{pmatrix}, m_5 = \begin{pmatrix} y & o \\ u & space \end{pmatrix}$$

Then Bob needs to encrypt the message in the following steps:

1. Bob translates the message into ASCII code as follows:
$$m_1 = \begin{pmatrix} 69 & 118 \\ 101 & 32 \end{pmatrix}, m_2 = \begin{pmatrix} 119 & 97 \\ 110 & 16 \end{pmatrix}, m_3 = \begin{pmatrix} 116 & 111 \\ 32 & 107 \end{pmatrix},$$
$$m_4 = \begin{pmatrix} 105 & 108 \\ 108 & 32 \end{pmatrix}, m_5 = \begin{pmatrix} 121 & 111 \\ 117 & 32 \end{pmatrix}$$
2. Bob picks integer $y = 43$
3. He computes $K_B = U^{\otimes y} = \left(G^{\otimes x}\right)^{\otimes y} = \begin{pmatrix} 2375 & 2379 \\ 2404 & 2408 \end{pmatrix} mod\ 73 \begin{pmatrix} 39 & 43 \\ 68 & 72 \end{pmatrix}$
4. Bob also computes his public key $V = G^{\otimes x} = \begin{pmatrix} 2881 & 2885 \\ 2837 & 2841 \end{pmatrix} mod\ 73 = \begin{pmatrix} 0 & 4 \\ 42 & 3 \end{pmatrix}$
5. Bob changes matrix K_B into diagonal matrix and we have $K_B = \begin{pmatrix} 39 & -\infty \\ -\infty & 72 \end{pmatrix}$.
6. Bob computes $c_i = m_i \otimes S$ for $i = 1, \dots, 5$ and we have the following cipher text:
$$c_1 = \begin{pmatrix} 108 & 190 \\ 140 & 104 \end{pmatrix}, c_2 = \begin{pmatrix} 158 & 169 \\ 149 & 88 \end{pmatrix}, c_3 = \begin{pmatrix} 155 & 183 \\ 71 & 179 \end{pmatrix}, m_4 = \begin{pmatrix} 144 & 180 \\ 147 & 104 \end{pmatrix},$$
$$c_5 = \begin{pmatrix} 160 & 183 \\ 156 & 104 \end{pmatrix}$$
7. Bob sends c_i and V to Alice.

Decryption

After Alice receives the chiper text c_i and public key V. Then she decrypt the chiper text to reveal the message.

1. Alice then computes $K_A = V^{\otimes x} = \left(G^{\otimes y}\right)^{\otimes x}$, and Alice transform S into diagonal matrix $S = \begin{pmatrix} 39 & -\infty \\ -\infty & 72 \end{pmatrix}$.
2. Alice decrypt the chiper text $d = c_1 \otimes K_A^{-1}$ and then reveal the message from Bob: Eve want to kill you.

Conclusions

In this paper, a new version of ElGamal encryption based on tropical matrices are presented. This new version using tropical matrix powers and diagonal matrices. We also give a toy example. We give a suggestion for parameters to avoid brute attack. For further research, we will consider to analyse the security using tropical discrete logarithm problem (Muanalifah & Sergeev, 2022).

References

Ahmed, K., Pal, S., & Mohan, R. (2023a). A review of the tropical approach in cryptography. *Cryptologia*, *47*(1), 63–87. https://doi.org/10.1080/01611194.2021.1994486

Ahmed, K., Pal, S., & Mohan, R. (2023b). Key exchange protocol based upon a modified tropical structure. *Communications in Algebra*, *51*(1), 214–223. https://doi.org/10.1080/00927872.2022.2095566

Akian, M., Bapat, R., & Gaubert, S. (2013). Max-Plus Algebra, In L. Hogben, editor, Handbook of linear algebra, chapter 25. *Chapman and Hall/CRC, Boca Raton, FL, 2 Edition*.

Baccelli, F., Cohen, G., Olsder, G. J., & Quadrat, J.-P. (1992). *Synchronization and Linearity: An Algebra for Discrete Event Systems*. Wiley.

Burkard, R. E., & Butkovic, P. (2003). Max algebra and the linear assignment problem. *Mathematical Programming*, *98*(1–3), 415–429. https://doi.org/10.1007/s10107-003-0411-9

Butkovič, P. (2010). *Max-linear Systems: Theory and Algorithms*. Springer London. https://doi.org/10.1007/978-1-84996-299-5

Cohen, G., Gaubert, S., & Quadrat, J.-P. (1999). Max-plus algebra and system theory: Where we are and where to go now. *Annual Reviews in Control*, *23*, 207–219. https://doi.org/10.1016/S1367-5788(99)90091-3

Bart, D. S., & Boom, T. van den. (2008). *Max-plus algebra and max-plus linear discrete event systems: An introduction "Proceedings of the 9th International Workshop on Discrete Event Systems (WODES'08)."*

Durcheva, M. I., Trendafilov, I. D., & Rachev, M. (2014). *Public key cryptosystem based on endomorphism semirings of a finite chain*. 330–335. https://doi.org/10.1063/1.4902494

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, *31*(4), 469–472. https://doi.org/10.1109/TIT.1985.1057074

Elsner, L., & Driessche, P. van den. (1999). On the power method in max algebra. *Linear Algebra and Its Applications*, *302–303*, 17–32. https://doi.org/10.1016/S0024-3795(98)10171-4

Elsner, L., & Driessche, P. van den. (2001). Modifying the power method in max algebra. *Linear Algebra and Its Applications*, *332–334*, 3–13. https://doi.org/10.1016/S0024-3795(00)00062-8

Gaubert, S., & Plus, M. (1997). *Methods and applications of (max,+) linear algebra* (pp. 261–282). https://doi.org/10.1007/BFb0023465

Grigoriev, D., & Ponomarenko, I. (2005). *Constructions in public-key cryptography over matrix groups*.

Grigoriev, D., & Shpilrain, V. (2014). Tropical Cryptography. *Communications in Algebra*, *42*(6), 2624–2632. https://doi.org/10.1080/00927872.2013.766827

Grigoriev, D., & Shpilrain, V. (2018). *Tropical cryptography II: extensions by homomorphisms*. https://doi.org/https://doi.org/10.48550

Grigoriev, D., & Shpilrain, V. (2019). Tropical cryptography II: Extensions by homomorphisms. *Communications in Algebra*, *47*(10), 4224–4229. https://doi.org/10.1080/00927872.2019.1581213

Huang, H., Li, C., & Deng, L. (2022). Public-Key Cryptography Based on Tropical Circular Matrices. *Applied Sciences*, *12*(15), 7401. https://doi.org/10.3390/app12157401

Isaac, S., & Kahrobaei, D. (2021). A closer look at the tropical cryptography. *International Journal of Computer Mathematics: Computer Systems Theory*, *6*(2), 137–142. https://doi.org/10.1080/23799927.2020.1862303

Kotov, M., & Ushakov, A. (2018). Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, *12*(3), 137–141. https://doi.org/10.1515/jmc-2016-0064

Muanalifah, A., & Sergeev, S. (2020). Modifying the tropical version of Stickel's key exchange protocol. *Applications of Mathematics*, *65*(6), 727–753. https://doi.org/10.21136/AM.2020.0325-19

Muanalifah, A., & Sergeev, S. (2022). On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product. *Communications in Algebra*, *50*(2), 861–879. https://doi.org/10.1080/00927872.2021.1975125

Nishida, Y. (2023). *Algorithm for the CSR expansion of max-plus matrices using the characteristic polynomial*. https://doi.org/https://doi.org/10.48550/arXiv.2311.03844

Rudy, D., & Monico, C. (2020). Remarks on a Tropical Key Exchange System. *Journal of Mathematical Cryptology*, *15*(1), 280–283. https://doi.org/10.1515/jmc-2019-0061

Sergeev, S., & Schneider, H. (2012). CSR expansions of matrix powers in max algebra. *Transactions of the American Mathematical Society*, *364*(11), 5969–5994. https://doi.org/10.1090/S0002-9947-2012-05605-4