iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: ETPAM-2018 **Issue:** Conference **Month of publication:** March 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Mathematical Cryptography by Tropical Matrix Algebra

Malliga. S[1], M Shobana Priya[2].
[1](II MSC MATHS) Guided by [2]Asst. Professor
Department of Mathematics St. Joseph's College of Arts and Science for Women.

Abstract: ***Cryptography is the branch of mathematics abstract from number theory in algebra. It mainly used to send secret message to communicate. In this paper, we employ tropical algebras as platforms for several cryptographic schemes that would be vulnerable to linear algebra based on "usual" algebras as platforms.***
Keywords: Tropical algebra, encryption, cryptography, public key exchange, applications.

I. INTRODUCTION

In this paper, the schemes themselves are not brand new, similar ideas were used in the classical case i.e. for algebras with the familiar addition and multiplication. We analyze a key-exchange protocol based on tropical matrix algebra. However in classic case these schemes were shown to be vulnerable to various linear algebra attacks. The idea to use an algebra with another addition and multiplication came as an attempt to avoid those attacks, as there are no known algorithms for solving systems of linear equations in tropical sense. However, in the classical case these schemes were shown to be vulnerable to various linear Algebra attacks. Here we make a case for using tropical algebras as platforms by using, among other things, the fact that in the "tropical" case, even solving systems of linear equations is computationally infeasible in general. Yet another advantage is improved efficiency, because in tropical schemes, one does not have to perform any multiplications of numbers since tropical multiplication is the usual addition. We start by giving some necessary information on tropical algebras here.

A. Definitions

1) Ring: A ring is a structure R = (A, $\oplus$,$\odot$, **0**, **1**) where $\oplus$ is the ring's addition operation, $\odot$ is the rings multiplication operation, **0** is the ring's zero element, and **1** is the ring's identity element ($\mathbf{0} \neq \mathbf{1}$).
$\oplus$ and $\odot$ are in commutative operations, a $\oplus$ b = b $\oplus$ a and a $\odot$ b = b $\odot$ a.
$\oplus$ and $\odot$ are in associative operations,
$\oplus$ b) $\oplus$ c = a $\oplus$ (b $\oplus$ c) and (a $\odot$ b) $\odot$ c = a $\odot$ (b $\odot$ c).
Distributivity:
($x \oplus y$) $\odot$ z = ($x \odot z$) $\oplus$ ($y \odot z$).
There are some "counterintuitive" properties as well:
$x \oplus x = x$
$x \odot 0 = x$
$x \oplus 0$ could be either 0 or x.

2) Tropical Matrix Algebra: The set of all n×n matrices $M_n(S)$ with entries from S can be equipped with operations $\oplus$ and $\odot$ as well, as defined below:
$(a_{ij}) \oplus (b_{ij}) = (a_{ij} \oplus b_{ij})$
$(a_{ij}) \odot (b_{ij}) = (a_{i1} \odot b_{1j} \odot : : : \odot a_{in}\ b_{nj})$:
The obtained algebra R = ($M_n(S)$; $\oplus$; $\odot$) is called a tropical matrix algebra. A tropical algebra can be used for matrix operations as well. To perform the $A \oplus B$ operation, the elements m_{ij} of the resulting matrix M are set to be equal to $a_{ij} \oplus b_{ij}$. The $\odot$ operation is similar to the usual matrix multiplication, however, every "+" calculation has to be substituted by a $\oplus$ operation, and every "." calculation by a $\odot$ operation.

3) Cryptography: According to the oxford dictionary is, "A secret manner of writing intelligible only to those possessing the key, also anything written in this way. Generally, the art of writing or solving ciphers". A secret code used in cryptography is called a cipher, the process of using a cipher to turn a plain document into a secret text is called encryption, and the reverse process is called decryption. In modern times, cryptography is considered to be a branch of both mathematics and computer science.

©IJRASET (UGC Approved Journal): All Rights are Reserved

B. Encryption Using Birational Automorphisms Of A Tropical Polynomialalgebra

In this section, we describe a public key encryption scheme that would be susceptible to a linear algebra attack in the "classical" case, but not in tropical case.

C. Protocol

There is a public automorphism $\alpha \in Aut(P)$ given as a tuple of tropical rational functions $(\alpha(x_1), \ldots, \alpha(x_n))$. Alice's private key is α^{-1}. Note that α is also a bijection of the set Z^n, i.e., it is a one-to-one map of the set of all *n*-tuples of integers onto itself. We will use the same notation α for an automorphism of *P* and for the corresponding bijection of Z^n, hoping this will not cause a confusion.

(1) Bob's secret message is a tuple of integers $s = (s_1, \ldots, s_n) \varepsilon Zn$. Bob encrypts his tuple by applying the public automorphism α: $E\ \alpha(s) = \alpha\ s_1, \ldots, s_n)$.

(2) Alice decrypts by applying her private α¡1 to the tuple $E\ \alpha(s)$: $\alpha^{-1}(E\ \alpha(s)) = s = (s_1, \ldots, s_n)$.

D. Possible Attacks

There are the following two attacks that adversary may attempt.

Trying to compute α^{-1} from the public automorphism α. The problem with this attack is that the degree of α^{-1} may be exponentially greater than the degree of α, which makes any commonly used attack (e.g. a linear algebra attack) infeasible.

Trying to recover Bob's secret message *s* from α (*s*). This translates into a system of tropical polynomial equations; solving such a system is an NP-hard problem.

E. Key Exchange Using Matrices Over A Tropical Algebra

We are now going to offer a key exchange protocol building on an idea of Stickel who used it for matrices over "usual" algebras, which made his scheme vulnerable to linear algebra attacks. Since we believe that Stickel's idea itself has a good potential, we suggest here to use matrices over a tropical algebra as the platformfor his scheme, in order to prevent linear algebra attacks.We start by recalling the original Stickel's protocol. Let *G* be a public non-commutative semigroup, $a,b \varepsilon G$ public elements such that $ab \neq ba$. The key exchangeprotocol goes as follows.

F. Protocol 1

1) Alice picks two random natural numbers *n,m* and sends $u = a^n b^m$ to Bob.

2) Bob picks two random natural numbers *r, s* and sends $v = a^r b^s$ to Alice

3) Alice computes $KA = a^n v b^m = a^{n+r} b^{m+s}$.

4) Bob computes $KB = a^r v b^s = a^{n+r} b^{m+s}$.

Thus, Alice and Bob end up with the same group element $K = KA = KB$ which can serve as the shared secret key.

G. Protocol 2

Let *R* be a public non-commutative ring (or a semi ring),

$a, b \varepsilon R$ public elements such that $ab \neq ba$.

Alice picks two random polynomials $p_1(x)$, $p_2(x)$ (say, with positive integer co- efficients) and sends $p_1(a) \cdot p_2(b)$ to Bob.

Bob picks two random polynomials $q_1(x)$, $q_2(x)$ and sends $q_1(a) \cdot q_2(b)$ to Alice.

Alice computes $KA = p_1(a) \cdot (q_1(a) \cdot q_2(b)) \cdot p_2(b)$.

Bob computes $KB = q_1(a) \cdot (p_1(a) \cdot p_2(b)) \cdot q_2(b)$.

Thus, since $p_1(a) \cdot q_1(a) = q_1(a) \cdot p_1(a)$ and $p_2(b) \cdot q_2(b) = q_2(b) \cdot p_2(b)$, Alice and Bobend up with the same element $K = KA = KB$ which can serve as the shared secret key.

H. Theorem

Let *p* be a prime and let *a* be a number not divisible by *p*. Then if $r \equiv s \bmod (p-1)$ we have $ar \equiv as \bmod p$. In brief, when we work mod *p*, exponents can be taken mod $(p-1)$. We've seen this used in calculations. For example to find $2^{402} \bmod 11$, we start with Fermat's theorem: $2^{10} \equiv 1 \bmod 11$. Raise to the 40th power to get $2^{400} \equiv 1 \bmod 11$. Now multiply by $2^2 = 4$ to get $2^{402} \equiv 4 \bmod 11$. In the language of the above theorem, $p = 11$, and so $p - 1 = 10$. We can thus take the exponent 402 mod 10 to get $2^{402} \equiv 22 \bmod 11$. Thus $402 \equiv 2 \bmod 10$; so $2^{402} \equiv 22 \bmod 11$.

The following is a useful corollary of Fermat's little theorem, which is used today in cryptography.

©IJRASET (UGC Approved Journal): All Rights are Reserved

I. Computational Assumption.

For a passive eavesdropper to break the protocol means to be able to compute the value of K based on the values of A,B,U, V . For that it clearly suffices to find a pair of matrices

X, Y satisfying the following conditions:

$X \odot A = A \odot X,$

$Y \odot B = B \odot Y,$

$X \odot Y = U,$

or to solve a similar system for Bob's public key. Indeed, if X, Y satisfy the conditions above, then the product $X \odot V \odot Y$ is equal to K. In the case of matrix algebra over (Z,+,._) one would reduce the system above to a system of linear equations . The same approach does not seem to work with tropical algebra.

J. Applications

1) Historically, cryptography was used to assure only secrecy. Wax seals, signatures and other physical mechanisms were typically used to assure integrity of the media and authenticity

2) Cryptography is at the heart of a vast range of daily activities such as electronic Commerce, bankcard payments and electronic building access to name a few.

3) Cryptography can play an important role in securing online services

4) The most obvious use of cryptography and the one that all of us use frequently I encrypting communications between us and another system.

II. CONCLUSION

The protocol described is not secure when used with the proposed parameter values. It is not clear how to modify key generation to provide a sufficient level of security. We encourage an interested reader to use our code and perform his/her computational experiments over the tropical algebra.

REFERENCES

[1] M. Bezem, R. Nieuwenhuis, E. Rodrguez-Carbonell, Hard problems in maxalgebra, control theory, hypergraphs and othe areas, Information Processing Letters 110(4) (2010), 133-138.

[2] P. Butkovic, Max-linear systems: theory and algorithms, Springer-Verlag London, 2010.

[3] M. Garey, J. Johnson, Computers and Intractability, A Guide to NP-Completeness, W. H. Freeman, 1979

[4] L. Goubin, N. Courtois, Cryptanalysis of the TTM cryptosystem, in: ASIACRYPT 2000, Lecture

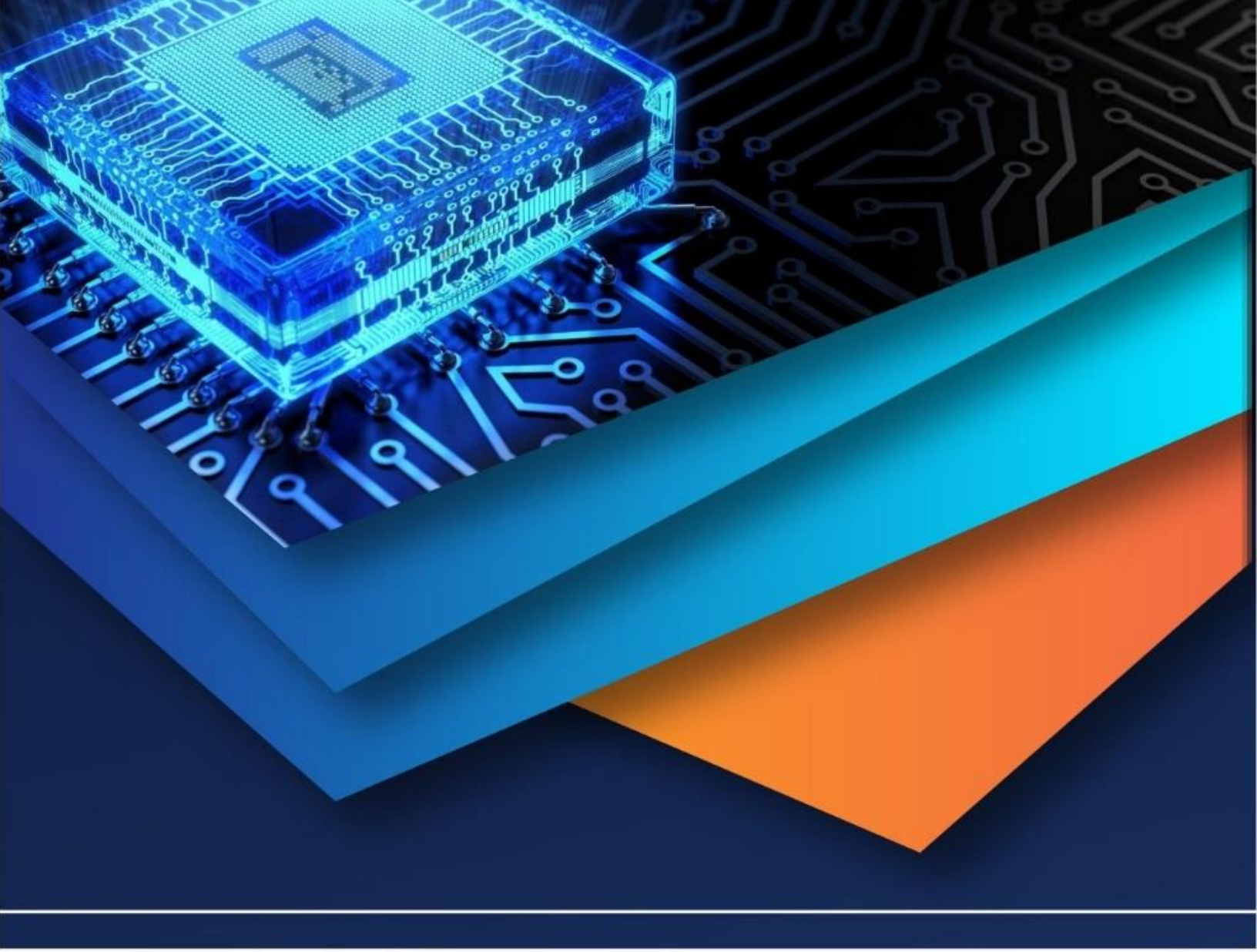
[5] M. Kotov and A. Ushakov. Implementation of attacks on a key excange protocol basedon tropical matrix algebra. Available at https://github.com/mkotov/tropical.

[6] A. G. Miasnikov, V. Shpilrain, and A. Ushakov. Non-Commutative Cryptography andComplexity of Group-Theoretic Problems. Mathematical Surveys and Monographs.AMS, 2011.

[7] C. Mullan. Cryptanalysing variants of Stickel's key agreement scheme. preprint, 2010.

[8] V. Shpilrain. Cryptanalysis of Stickel's key exchange scheme. In Computer Science in Russia { CSR 2008, volume 5010 of Lecture Notes Comp. Sc., pages 283{288. Springer, 2008.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)