Analysis of four protocols based on tropical circulant matrices

Matvei Kotov

(joint work with Ivan Buchinskiy and Alexander Treier)

Sobolev Institute of Mathematics of SB RAS

Conference "Combinatorial-computational methods of algebra and logic", Omsk, September 30th, 2023

Sidelnikov, Cherepnev, and Yaschenko's key exchange

Sidelnikov, Cherepnev, and Yaschenko proposed the following key exchange method based on non-commutative semigroups. Let G be a non-commutative semigroup, H and R be commutative subsemigroups of G, and $W \in G$.

1. Alice chooses as her secret key two elements $P_A \in H$ and $Q_A \in R$. She computes $K_A = P_A \cdot W \cdot Q_A$ and sends it to Bob.
2. Bob chooses as his secret key two elements $P_B \in H$ and $Q_B \in R$. He computes $K_B = P_B \cdot W \cdot Q_B$ and sends it to Alice.
3. Alice computes the common secret key $K_{AB} = P_A \cdot K_B \cdot Q_A$.
4. Bob computes the common secret key $K_{BA} = P_B \cdot K_A \cdot Q_B$.

They share the same key:
$P_A \cdot (P_B \cdot W \cdot Q_B) \cdot Q_A = P_B \cdot (P_A \cdot W \cdot Q_A) \cdot Q_B$.
[SCY:1993] V. Sidelnikov, M. Cherepnev, and V. Yashchenko, Systems of open distribution of keys on the basis of noncommutative semigroups, Dokl. RAN., 332.5, 1993, 566–567

Linear decomposition attack

[MR:2015] A. Myasnikov, V. Roman'kov, A linear decomposition attack, Groups, Complexity, Cryptology, 2015, 7, 81–94

In this paper, the authors offered a new attack on several known group-based cryptosystems. This attack gives a polynomial time deterministic algorithm that recovers the secret shared key from the public data in all the schemes under consideration. They showed show that in this case the typical computational security assumptions are not very relevant to the security of the schemes, i.e., one can break the schemes without solving the algorithmic problems on which the assumptions are based.

For more information:
[R:2020] V. Roman'kov Algebraic cryptology, Omsk, Omsk State University Press, 2020

Tropical approach

Grigoriev and Shpilrain suggested using tropical algebraic structures.

[GS:2014] D. Grigoriev, V. Shpilrain, Tropical cryptography, Comm. Algebra, 42.6, 2014, 2624–2632
[GS:2019] D. Grigoriev, V. Shpilrain, Tropical cryptography II: extensions by homomorphisms, Comm. Algebra, 47.10, 2019, 4224–4229
[CGS:2023] J. Chen, D. Grigoriev, V. Shpilrain, Tropical cryptography III: digital signatures, arXiv:2309.11256, submitted Sep. 20th, 2023

What are the advantages of the "tropical" protocols?
Improved efficiency because the operations can be performed fast.
Systems of tropical equations are not easy to solve.

Tropical algebras

The extended set of real numbers $\mathbb{R} \cup \{\infty\}$ equipped with two binary operations $\oplus, \otimes$ defined by

$$\begin{aligned} x \oplus y &= \min(x, y), \\ x \otimes y &= x + y. \end{aligned}$$

is called the **min-plus algebra**.

If we consider $\mathbb{R} \cup \{-\infty\}$ and define $\oplus, \otimes$ as

$$\begin{aligned} x \oplus y &= \max(x, y), \\ x \otimes y &= x + y, \end{aligned}$$

we obtain the **max-plus algebra**.

Tropical geometry has a lot of applications in combinatorial optimization, algebraic geometry, auction theory, mechanism design, game theory, scheduling etc.

Tropical algebras

Since the max-plus and min-plus algebras are commutative idempotent semirings, then the following identities hold:

1. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$,
2. $o \oplus a = a \oplus o = a$,
3. $a \oplus b = b \oplus a$,
4. $(a \otimes b) \otimes c = a \otimes (b \otimes c)$,
5. $e \otimes a = a \otimes e = a$,
6. $a \otimes b = b \otimes a$,
7. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$,
8. $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$,
9. $o \otimes a = a \otimes o = o$,
10. $a \oplus a = a$,

where o is $-\infty$ for the max-plus algebra and is ∞ for the min-plus algebra, and e is 0.

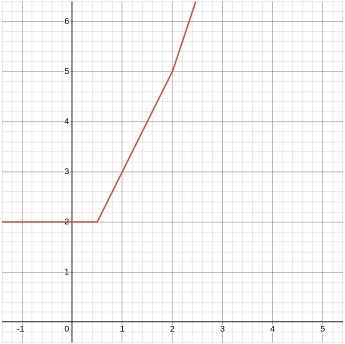
(A semiring is a ring without the requirement that each element must have an additive inverse.)

Tropical polynomials

Consider, for example, the max-plus algebra. We can define a **tropical polynomial**:

$$p(x) = \bigoplus_{k=0}^{d} p_k \otimes x^{\oplus k} = \max_{1 \leq k \leq d} \{p_k + k \cdot x\}.$$

A max-plus polynomial is a convex, piecewise-linear function. For example, $p(x) = -1 \otimes x^{\otimes 3} \oplus 1 \otimes x^{\otimes 2} \oplus x \oplus 2$.



Tropical matrices

The set of all $n \times n$ matrices $\mathrm{Mat}_n(S)$ with entries from a semiring S can be equipped with operations $\oplus$ and $\otimes$ as defined below:

$$(a_{ij}) \oplus (b_{ij}) = (a_{ij} \oplus b_{ij})$$
$$(a_{ij}) \otimes (b_{ij}) = (a_{i1} \otimes b_{1j} \oplus \ldots \oplus a_{in} \otimes b_{nj}).$$

For example, let's consider two matrices over max-times algebra:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & \infty \end{pmatrix}, B = \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix}.$$

Then

$$A \otimes B = \begin{pmatrix} 1 & 2 \\ 0 & \infty \end{pmatrix} \otimes \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix} =$$
$$\begin{pmatrix} 1 \otimes 3 \oplus 2 \otimes 5 & 1 \otimes 4 \oplus 2 \otimes 0 \\ 0 \otimes 3 \oplus \infty \otimes 5 & 0 \otimes 4 \oplus \infty \otimes 0 \end{pmatrix} =$$
$$\begin{pmatrix} 3 \oplus 10 & 4 \oplus 0 \\ 0 \oplus \infty & 0 \oplus 0 \end{pmatrix} = \begin{pmatrix} 10 & 4 \\ \infty & 0 \end{pmatrix}.$$

Tropical matrices

The obtained set of matrices also in an idempotent semiring. In other words, the following identities are true:

1. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$,
2. $O \oplus A = A \oplus O = A$,
3. $A \oplus B = B \oplus A$,
4. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$,
5. $E \otimes A = A \otimes E = A$,
6. $A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$,
7. $(A \oplus B) \otimes C = (A \otimes C) \oplus (B \otimes C)$,
8. $O \otimes A = A \otimes O = O$,
9. $A \oplus A = A$.

Let $A \in \mathrm{Mat}_n(\mathcal{S})$ and $p(x) = \bigoplus_{i=0}^{d} p_i \otimes x^{\otimes i}$, then we denote the matrix $\bigoplus_{i=0}^{d} p_i \otimes A^{\otimes i}$ by $p(A)$.

Grigoriev and Shpilrain's protocol

Let R be a min-plus algebra of $n \times n$ matrices over integers. Let $A, B \in R$ be public matrices satisfying $A \otimes B \neq B \otimes A$.

1. Alice generates random polynomials $p_1(x), p_2(x) \in \mathbb{Z}[x]$ and sends $K_A = p_1(A) \otimes p_2(B)$ to Bob.
2. Bob generates random polynomials $q_1(x), q_2(x) \in \mathbb{Z}[x]$ and sends $K_B = q_1(A) \otimes q_2(B)$ to Alice.
3. Alice computes $K_{AB} = p_1(A) \otimes V \otimes p_2(B)$.
4. Bob computes $K_{BA} = q_1(A) \otimes U \otimes q_2(B)$.

$K = K_{AB} = K_{BA}$.

Attack:
[KU: 2018] M. Kotov, A. Ushakov, Analysis of a key exchange protocol based on tropical matrix algebra, J. Math. Cryptol., 12.3, 2018, 137–141

Two classes of commuting matrices

[MS:2020] A. Muanalifah, S. Sergeev, Modifying the tropical version of Stickel's key exchange protocol, Appl. Math., 65.6, 2020, 727–753

Let $A = (a_{ij})$ be an $n \times n$ tropical matrix which satisfies the following property:

$$a_{ij} \otimes a_{jk} \leq a_{ik} \otimes a_{jj} \, \forall i, j, k \in [n].$$

Then A is called a *Jones matrix*.

Let $A = (a_{ij})$ be a Jones matrix and $\alpha \in \mathbb{R}$. Matrix $A = (a_{ij}^{(\alpha)})$ defined by

$$a_{ij}^{(\alpha)} = a_{ij} \otimes (a_{ii} \oplus a_{jj})^{\otimes(\alpha-1)} \, \forall i, j \in [n].$$

is called a *deformation* of A.

Matrix B is called a *quasi-polynomial* of A if

$$B = \bigoplus_{\alpha \in R} a_\alpha \otimes A^{(\alpha)}$$

for some finite subset R of rational numbers in $[0, 1]$ and $a_\alpha \in \mathbb{R}_{\max}$ for $\alpha \in R$.

Two classes of commuting matrices

[MS:2020] A. Muanalifah, S. Sergeev, Modifying the tropical version of Stickel's key exchange protocol, Appl. Math., 65.6, 2020, 727–753

For arbitrary real number $r \leq 0$ and real number $k \geq 0$, we denote by $[2r, r]_n^k$ the set of matrices $A \in \mathbb{R}_{\max}^{n \times n}$ such that $a_{ii} = k$, for all $i \in [n]$ and $a_{ij} \in [2r, r]$ for $i, j \in [n]$ and $i \neq j$. Matrices of this form is called *Linde-De la Puente matrices*.

Let $A \in [2r, r]_n^{k_1}$, $B \in [2s, s]_n^{k_2}$ for any $r, s \leq 0$ and $a_{ii} = k_1 \geq 0$, $b_{ii} = k_2 \geq 0$ then $A \otimes B = B \otimes A = k_2 \otimes A \oplus k_1 \otimes B$.

Circulant matrices

A *circulant* matrix is a matrix of the form

$$\begin{pmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{pmatrix}.$$

It is easy to show that all the circulant matrices of order n form a commutative algebra, since the sum and the product of two circulant matrices are circulant, and $A \otimes B = B \otimes A$.

Circulant matrices

Let t be an integer. A matrix of the form

$$\begin{pmatrix} a_0 & a_{n-1} \otimes t & a_{n-2} \otimes t & \cdots & a_1 \otimes t \\ a_1 & a_0 & a_{n-1} \otimes t & \cdots & a_2 \otimes t \\ a_2 & a_1 & a_0 & \cdots & a_3 \otimes t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{pmatrix}$$

is called an *upper-t-circulant* matrix of order n.
Lower-t-circulant matrices are defined in a similar way.
It is possible to show that all the upper-t-circulant (lower-t-circulant) matrices of order n form a commutative semiring.

Circulant matrices

Let p and t be integers. A matrix of the form

$$\begin{pmatrix} a_0 \otimes t & a_{n-1} \otimes t & \cdots & a_2 \otimes t & a_1 \\ a_1 \otimes t & a_0 \otimes t & \cdots & a_3 & a_2 \otimes t \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2} \otimes t & a_{n-3} & \cdots & a_0 \otimes t & a_{n-1} \otimes t \\ a_{n-1} & a_{n-2} \otimes t & \cdots & a_1 \otimes t & a_0 \otimes t \end{pmatrix}$$

is called an *anti-t-p-circulant* matrix if $a_k - a_{k+1} = p$ for each k.

Huang, Li, and Deng's protocol

Huang, Li, and Deng offered the following key exchange protocol based on tropical upper-t-circulant matrices.

Let R be the min-plus semiring, $n, s, t \in \mathbb{Z}_{>0}$, and $Y \in Mat_n(R) \setminus (UC_n(R, s) \cup UC_n(R, t))$. These numbers, semiring, and matrix are public.

1. Alice chooses two matrices $P_1 \in UC_n(R, s)$ and $Q_1 \in UC_n(R, t)$. She computes her public key $K_A = P_1 \otimes Y \otimes Q_1$ and sends it to Bob.
2. Bob chooses two matrices $P_2 \in UC_n(R, s)$ and $Q_2 \in UC_n(R, t)$. He computes his public key $K_B = P_2 \otimes Y \otimes Q_2$ and sends it to Alice.
3. Alice computes her secret key $K_{AB} = P_1 \otimes K_B \otimes Q_1$.
4. Bob computes his secret key $K_{BA} = P_2 \otimes K_A \otimes Q_2$.

Alice and Bob end up with the same key $K_{AB} = K_{BA} = K$, which can serve as the secret key.

[HLD:2022] H. Huang, C. Li, and L. Deng, Public-Key Cryptography Based on Tropical Circular Matrices, Appl. Sci., 12.15, 2022, 7401

Amutha and Perumal's protocol 1

Amutha and Perumal suggested a similar protocol based on lower-t-circulant matrices.
Let R be the min-plus semiring, $n \in \mathbb{Z}_{>0}$, $s, t \in \mathbb{Z}$, and $Y \in M_n(R)$.

1. Alice chooses two matrices $P_1 \in LC_n(R, s)$ and $Q_1 \in LC_n(R, t)$. She computes her public key $K_A = P_1 \otimes Y \otimes Q_1$ and sends it to Bob.
2. Bob chooses two matrices $P_2 \in LC_n(R, s)$ and $Q_2 \in LC_n(R, t)$. He computes his public key $K_B = P_2 \otimes Y \otimes Q_2$ and sends it to Alice.
3. Alice computes her secret key $K_{AB} = P_1 \otimes K_B \otimes Q_1$.
4. Bob computes his secret key $K_{BA} = P_2 \otimes K_A \otimes Q_2$.

Then, Alice and Bob share the same key $K_{AB} = K_{BA} = K$.
[AP:2023] B. Amutha, R. Perumal, Public key exchange protocols based on tropical lower circulant and anti-circulant matrices, AIMS Math., 8.7, 2023, 17307–17334

Amutha and Perumal's protocol 2

Also, B. Amutha and R. Perumal suggested another protocol based on anti-p-t-circulant matrices.

Let R be the min-plus semiring, $n \in \mathbb{Z}_{>0}$, $s, t, p \in \mathbb{Z}$, and $Y \in M_n(R)$.

1. Alice chooses two matrices $P_1 \in AC_n(R, p, s)$ and $Q_1 \in AC_n(R, p, t)$. She computes her public key $K_A = P_1 \otimes Y \otimes Q_1$ and sends it to Bob.
2. Bob chooses two matrices $P_2 \in AC_n(R, p, s)$ and $Q_2 \in AC_n(R, p, t)$. He computes his public key $K_B = P_2 \otimes Y \otimes Q_2$ and sends it to Alice.
3. Alice computes her secret key $K_{AB} = P_1 \otimes K_B \otimes Q_1$.
4. Bob computes his secret key $K_{BA} = P_2 \otimes K_A \otimes Q_2$.

It is possible to show that Alice and Bob share the same key $K_{AB} = K_{BA} = K$.

[AP:2023] B. Amutha, R. Perumal, Public key exchange protocols based on tropical lower circulant and anti-circulant matrices, AIMS Math., 8.7, 2023, 17307–17334

Durcheva's protocol

Durcheva offered a protocol that employs circulant matrices.

[D:2022] M. I. Durcheva, TrES: Tropical Encryption Scheme Based on Double Key Exchange, Eur. J. Inf. Tech. Comp. Sci., 2.4, 2022, 11–17.

Attack:

[JHP:2023] X. Jiang, H. Huang, G. Pan, Cryptanalysis of Tropical Encryption Scheme Based on Double Key Exchange, J. Cyber Secur. Mobil., 12.02, 2023, 205–220

Attack

To break the method, for an eavesdropper it suffices to find a solution to the equation

$$X \otimes W \otimes Y = K_A,$$

if $X \in H$ can be presented as a finite sum $X = \bigoplus_i x_i \otimes B_i$, and $Y \in R$ can be presented as a finite sum $Y = \bigoplus_j y_j \otimes C_j$. Indeed,

$$\left(\bigoplus_{i=1}^{D_1} x_i \otimes B_i\right) \otimes W \otimes \left(\bigoplus_{j=1}^{D_1} y_j \otimes C_j\right) = K_A$$

.

Denoting $T^{ij} = B_i \otimes W \otimes C_j - K_A$, we obtain

$$\bigoplus_{i,j} (x_i \otimes y_j) \otimes T^{ij} = E,$$

where E is the matrix of the corresponding size with all entries equal to 0.

Attack

Therefore we have the following system of equations:

$$\min_{ij}(x_i + x_j + T_{kl}^{ij}) = 0 \text{ for each } k, l \in [1, n]. \qquad (1)$$

Solving this system is the main goal of the attack. Compute $m_{ij} = \min_{k,l} T_{kl}^{ij}$ and $P_{ij} = \operatorname{argmin}_{k,l} T_{kl}^{ij}$.
It is possible to show that, to find a solution to (1), we need to find a cover $C \subseteq \{P_{ij}\}_{i,j}$ of the set $[1, n] \times [1, n]$ and values $x_i, y_i, i, j \in [0, D]$, satisfying

$$\begin{cases} x_i + y_j = -m_{ij} & \text{if } P_{ij} \in C, \\ x_i + y_j \geq -m_{ij} & \text{otherwise.} \end{cases} \qquad (2)$$

Hence, in order to solve this system, we can enumerate the minimal covers, and then choose that cover that defines the consistent system of equations and inequalities (2).
It is known that finding a minimal set cover problem is one of Karp's 21 problems shown to be NP-complete in 1972.
Nevertheless, using some ideas and heuristics, it is enough to check a small portion of the covers.

Attack

Any upper-t-circulant matrix can be presented as

$$a_0 \otimes I \oplus a_1 \otimes P \oplus \cdots \oplus a_{n-1} \otimes P^{\otimes n-1}, \tag{3}$$

where

$$P = \begin{pmatrix} o & o & o & \cdots & o & t \\ e & o & o & \cdots & o & o \\ o & e & o & \cdots & o & o \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ o & o & o & \cdots & e & o \end{pmatrix}.$$

Also, we can present as a finite linear combination of matrices any lower-t-circulant matrix and any anti-t-p-circlulant matrix.

Experimental results

Protocol	$n = 5$	$n = 10$	$n = 25$	$n = 50$
Amutha and Perumal's prot. 1	0.38	0.38	0.69	7.16
Amutha and Perumal's prot. 2	0.36	0.34	0.40	0.69
Durcheva's prot., 2nd phase	0.37	0.53	2.37	20.75
Grigoriev and Shpilrain prot.	0.32	0.41	1.71	13.87
Huang, Li, and Deng's prot.	0.29	0.30	0.63	6.63

Table: Experimental results of the attack (time in seconds). The success rate is 100% for all the experiments.

The number of tests for each size of matrices is 100. For Durcheva's and for Grigoriev and Shpilrain's prot. elements of randomly generated matr. are in $[0, 10^5]$. For the other protocols elements of circulant matrices and parameters are in $[-10^5, 10^5]$. The deg. of the poly. are in $[5, 15]$, and the coefficients are in $[-10^5, 10^5]$. The bound used in the attack on Durcheva's is 20.

System: Python 3.10, Windows 10, Intel Core i7-12700H 2.70 GHz, 16.0 GB RAM.

Conclusion

[BKT:2023] I. Buchinskiy, M. Kotov, A. Treier, Analysis of four protocols based on tropical circulant matrices, in preparation

This paper showed that the protocol described in [D:2022], [AP2023], and [HLD:2022] are insecure. We showed that the attack from [KU:2018] with some changes can be applied here successfully. The success rate of our attack is 100%. Our analysis can further be used to analyze other protocols based on tropical matrix algebras.