Athens Journal of Sciences- Volume 12, Issue 3, September 2025 – Pages 189-204

Tropical Cryptography – The State of the Art and Future Prospects

By Mariana Durcheva[*]

The first paper introducing the use of tropical semirings in public key cryptography was published in 2013. Since then, numerous tropical schemes have been proposed, incorporating various idempotent semirings. The most commonly used idempotent semirings for cryptographic purposes are the min-plus and max-plus semirings, with some schemes also utilizing the max-time and min-time semirings. The main mathematical problems that ensure the security of these schemes include the tropical discrete logarithm problem, the tropical semigroup action problem, the tropical semidirect product problem; the problem of solving two-sided linear systems in tropical semirings; tropical polynomial factorization and finding greatest common divisor problems, and the tropical matrix power function problem. Unfortunately, most of the proposed tropical schemes have been successfully attacked, raising concerns about the future of tropical cryptography. In this work, we review existing tropical schemes, discuss the complexity of the underlying problems, examine current attacks on these schemes, and explore future prospects and directions for cryptography based on tropical semirings.

Keywords: *semirings, tropical semirings, tropical cryptography, tropical problems, crypto attacks*

Introduction

Semirings were introduced by Vandiver (1934), but they remained unnoticed by mathematicians for a long time. According to Vandiver, a semiring is a nonempty set R, equipped with two operations: addition (+) and multiplication ($\cdot$), satisfying the following conditions: $(R, +)$ forms a commutative semigroup, $(R, \cdot)$ forms a semigroup, and multiplication distributes over addition.

Semirings find applications in diverse fields, including automata theory, formal languages, finite state machines, recognizable languages, speech recognition, and image compression. Formal systems used for studying the correctness and effectiveness of computer programs, such as dynamic algebras, Hoare algebras, and Kleene algebras, are closely related to various semirings. Idempotent semirings bridge algebraic formalism and dynamic and temporal logic, enabling the modelling of properties of computer programs and transition systems. Additionally, semirings play a crucial role in large-scale scientific applications, including high-dimensional data and graph analytics for linear algebra computations.

Tropical algebra was first proposed by Cuninghame-Green (1979), while the term *idempotent analysis* was proposed by Maslov (1986). The name *tropical* was coined in honor of Brazilian mathematician Imre Simon, whose work (Simon 1988)

[*]Lecturer, Sami Shamoon College of Engineering, Israel.

https://doi.org/10.30958/ajs.12-3-3 doi=10.30958/ajs.12-3-3

laid important foundations for tropical algebra. In tropical algebra, tropical addition means taking the minimum or maximum of two numbers, while tropical multiplication corresponds to usual addition. The concepts of tropical algebra were further developed through the framework of semirings, leading to the formal definition of the algebraic structure of tropical semirings. This theory introduced a novel approach by replacing the field of real numbers, $\mathbb{R}$, with the semifield $\mathbb{R}_{max}$. One of its key advantages is the ability to transform many problems that are nonlinear over real numbers into linear problems via this new arithmetic. In essence, these problems become linear over the appropriately chosen semiring.

Since 1995, the research field of tropical algebra has experienced remarkable growth, driven by numerous findings and diverse applications in areas such as control theory and optimization, phylogenetics, the modelling of cellular protein production, and railway scheduling. Tropical algebra has become a significant subject of study in algebraic theory. A major research focus in tropical algebra is the investigation of the semigroup of tropical matrices, which includes exploring the structure of multiplicative semigroups, Green's relations, regularity, and abundance. In recent years, the study of the multiplicative semigroup of tropical matrices has gained prominence as a hot research topic. Scholars are increasingly leveraging tropical algebra for cutting-edge research in areas such as noise removal and optimal control. Moreover, researchers are exploring additional methods of tropical algebra to address practical problems, including the variational iteration method and the homotopy perturbation method.

Max-algebra has found significant applications in various fields, including nonlinear partial differential equations and various optimization theories. The min-algebra, which is isomorphic to max-algebra, is utilized in areas such as statistics, computational biology, and net calculus for fading channels. Brunsch et al. (2012) extended the use of idempotent semirings to interval analysis, proposing conditions for the existence of a non-linear projector in the solution set of certain inequalities. Trendafilov & Tzvetkov (2021) introduced the concept of derivations in a product of additively idempotent semirings, highlighting their utility in diverse areas such as switching circuits, automata theory, and decision theory. Krivulin in several papers (Krivulin 2020, Krivulin & Gubanov 2021) proposed different applications of idempotent semirings, including solving location problems with Chebyshev and rectilinear distances in multidimensional space and in the two-dimensional plane. These semirings were also used to address optimal project scheduling problems in project management, with the goal of minimizing deviations in starting times of tasks. Idempotent semirings have additionally been applied in genetic algorithms for solving resource-constrained project scheduling problems (Bulavchuk & Semenova 2023) and for modelling coordination schemes and weighted connectors in component-based systems architectures (Fountoukidou & Pittou 2022).

On the one hand, information security is crucial in today's interconnected world, where data is a key asset. It protects organizations, individuals, and nations from a wide array of risks, ranging from financial loss and reputational damage to personal privacy violations and national security threats. As cyber threats continue to evolve, the importance of maintaining strong and adaptive information security

cannot be overstated, including establishing information security policy (Nagata 2023).

On the other hand, cryptography is vital to information security, and modern cryptographic methods are used to secure communication, protect stored data, and ensure secure authentication processes.

Before 1976, secret key cryptography was the standard approach to secure communication over open channels. However, Diffie and Hellman (1976) introduced a groundbreaking concept: public key cryptography, which revolutionized the field and opened new direction for research, including methods for interaction between logic gates, blockchain and key generation (Medelin 2022). Numerous applications rely on public-key cryptosystems and protocols, including SSH (Ylonen & Lonvick 2006), OpenPGP (Callas et al. 1998) and SSL/TLS (Dierks and Allen 1999).

Maze et al. (2007) proposed one of the first cryptosystems based on semirings. However, this cryptosystem was successfully attacked by Steinwandt et al. (2011).

Grigoriev and Shpilrain (2013) were the first to demonstrate the use of tropical semirings in public key cryptography. A discussion on the potential of semirings in cryptography can be found in Durcheva (2020). Tropical and supertropical semiring-based protocols have emerged as a powerful solution for modern IoT ecosystems, offering remarkable robustness and efficiency (Durcheva & Danilchenko 2024, Ponmaheshkumar & Perumal 2024, Jackson & Perumal 2024). In these environments, devices often operate with limited resources while requiring both rapid and secure communication. Additionally, such schemes integrate seamlessly into blockchain systems, enhancing the security of trade operations and digital contracts while mitigating common vulnerabilities in distributed networks.

In this paper, we provide a review of tropical schemes, discuss the complexity of the underlying problems, examine existing attacks on these schemes, and explore the future prospects of cryptography based on tropical semirings.

The paper is organized as follows: Section 2 presents relevant preliminaries, Section 3 introduces the state of the art, Section 4 discusses the future of tropical cryptography and Section 5 offers concluding remarks.

Preliminaries

A *semiring*, as defined in Vandiver (1934), consists of a nonempty set R, equipped with two binary operations: addition (+) and multiplication ($\cdot$). These operations satisfy the following requirements:

- $(R, +)$ is a commutative semigroup, i.e. $a + b = b + a$ and $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$;
- $(R, \cdot)$ is a semigroup, i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$;
- the distributive laws hold: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

It is noteworthy to mention that the definition provided by Golan (1999) assumes the presence of a zero and a one in the semiring.

Let $R = (R, +, \cdot)$ be a semiring. If there exists a neutral element 0 in the semigroup $(R, +)$ that satisfies the condition $0 + a = a + 0$ for all $a \in R$, this element is called a *zero*. If there exists a neutral element 1 of the semigroup $(R, \cdot)$, meaning $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$, this element is called a *one*. A semiring R is called *commutative* if the semigroup $(R, \cdot)$ is commutative.

Furthermore, when the commutative semigroup $(R, +)$ is an abelian group, the semiring is referred to as a *ring*; when the multiplicative semigroup $(R, \cdot)$ is a group, then a semigroup is called a *semifield*.

An element a of the semiring $(R, +, \cdot)$ is called *additively idempotent* if $a + a = a$. If every element of the semiring is additively idempotent, then R is referred to as an *additively idempotent semiring*. A semiring is termed *idempotent* if it is an additively idempotent.

We will highlight several important idempotent semirings:

$\mathbb{R}_{max,min} = (\mathbb{R} \cup \{-\infty, +\infty\}, \max, \min)$ is an idempotent semiring, which is not a semifield. In this semiring, $\mathbf{0} = -\infty, \mathbf{1} = +\infty$. The inverse element with respect to the operation *min* does not exist, and the maximal element is $+\infty$.

The following semirings are often utilized as building blocks for different protocols:

$$\mathbb{R}_{max,+} = (\mathbb{R} \cup \{-\infty\}, \max, +); \quad \mathbb{R}_{min,+} = (\mathbb{R} \cup \{+\infty\}, \min, +);$$
$$\mathbb{R}_{max,\times} = (\mathbb{R}_+ \cup \{0\}, \max, \times); \; \mathbb{R}_{min,\times} = (\mathbb{R}_+ \cup \{+\infty\}, \min, \times),$$

when $\mathbb{R}$ is the field of real numbers and $\mathbb{R}_+ = \{x \in \mathbb{R} | x > 0\}$. The semirings $\mathbb{R}_{max,+}$, $\mathbb{R}_{min,+}$, $\mathbb{R}_{max,\times}$, $\mathbb{R}_{min,\times}$ will be referred to as *tropical semirings*.

Over idempotent (tropical) semirings can be considered matrices and polynomials in a usual way. Let $(M, \oplus, \otimes)$ be an idempotent semifield. For some random matrices:

$$A = (a_{ij}) \in M^{n \times n}, \qquad B = (b_{ij}) \in M^{n \times n},$$

the addition and multiplication of matrices, as well as the multiplication of a matrix by a scalar $\alpha \in M$ are defined as follows:

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

$$(\alpha \otimes A)_{ij} = \alpha \otimes a_{ij}.$$

The set $M^{n \times n}$ of $n \times n$ matrices with entries from M equipped with matrix addition, matrix multiplication, and scalar multiplication is an idempotent algebra. In this algebra, there is a null matrix O (where all of entries are 0) and a unit matrix I (where diagonal entries are 1 and all other entries are 0).

Tropical polynomials are defined in the conventional manner as follows:

$$P(x) = \bigoplus_{i=0}^{n} a_i \otimes x^{\otimes i},$$

where $x^{\otimes i} = \underbrace{x \otimes x \otimes \ldots \otimes x}_{i \text{ times}}$ and $a_i \in M$ for $i = 0, 1, \cdots, n$.

It follows from the properties of operations in tropical semirings that:

$$P(x) \otimes Q(x) = Q(x) \otimes P(x).$$

For further information on semirings, including matrices and polynomials over semirings, we recommend the monograph by Golan (1999).

The State of the Art

Key Problems Ensuring the Security of Tropical Protocols and Corresponding Attacks

In this section, we discuss the main hard problems that underpin the security of tropical protocols, the schemes that utilize these problems, and the attacks against these schemes. We note that all coefficients of tropical polynomials, as well as the entries of tropical matrices are from some tropical semiring *T*, which can be specified if needed for a protocol.

- **The Tropical Discrete Logarithm Problem (TDLP)**

We begin by recalling the classical Discrete Logarithm Problem (DLP). Given a cyclic group G with a generator g and an element h in G, the DLP involves finding an integer x such that: $g^x = h$.

Let A, B, C be suitable tropical matrices, and m be a positive integer. The TDLP is defined as follows: Given the matrices A, B, C, find m from the equation:

$$C = A \otimes B^{\otimes m} \text{ (or } C = B^{\otimes m} \otimes A). \quad (1)$$

Protocols, such as the one proposed by Muanalifah et al. (2023), rely on this problem for their security. The discrete logarithm problem in a tropical semiring can be completely solved in certain cases (specifically, on a group and a module). In other cases, a 100% success rate can be achieved through alternative methods (Muanalifah & Sergeev 2022).

Most often, this problem needs to be solved in its two-sided form. Given matrices *A, B, C* and *D*, the goal is to find the positive integers *m* and *n* from the equation:

$$C = A^{\otimes m} \otimes D \otimes B^{\otimes n}. \quad (2)$$

- **The Tropical Semigroup Action Problem (TSAP)**

We first recall the *Semigroup Action Problem* (SAP) as defined in (Maze et al. 2007).

An *action* of a finite set S on a semigroup $(G, \cdot)$ is a map $\varphi: G \times S \to S$ such that:

$$\varphi(g \cdot h, s) = \varphi\big(g, \varphi(h, s)\big). \tag{3}$$

The *Semigroup Action Problem* is then formulated as follows: Given a semigroup G acting on a finite set S through the (left) action φ, and elements $s \in S, t \in \varphi(g, s)$, find an element $g \in G$ such that $\varphi(g, s) = t$.

Tropical Semigroup Action (τ). A semigroup G is said to act on a tropical semiring T:

$$\tau: G \times T \to T$$

if the following conditions hold:

(1) For any element a of the tropical semiring T and an element g of the semigroup G, there exists an element a^g that belongs to the tropical semiring T.
(2) For any elements a, b of the tropical semiring T and element g, h of the semigroup G, the following properties are satisfied:

$$(a \otimes b)^g = a^g \otimes b^g, \qquad a^{gh} = (a^g)^h .$$

Tropical Semigroup Action Problem. Given a semigroup G acting on a tropical semiring T through the action (τ) and elements $a \in T, b \in \tau(g, a)$, the problem is to find an element g of the semigroup G such that $\tau(g, a) = b$.

It is claimed in Goel et al. (2020) that the Semigroup Action Problem can be considered a generalization of the Discrete Logarithm Problem. Huang et al. (2024b) argue that most cryptosystems based on the SAP, DLP, and matrix-action problem on a group and on a module cannot resist quantum cryptanalysis. However, cryptographic systems based on the SAP on a semi-module are likely more resilient against quantum attacks.

Additionally, a protocol based on the bi-semigroup action problem (BSAP) is proposed by Trendafilov & Durcheva (2010).

- **The Tropical Semidirect Product Problem (TSPP)**

We first recall the *Semidirect Product Problem* (SPP) in arbitrary semigroups (Shpilrain 2018): Given a semigroup G and elements $(g, h, h^{-m}(hg)^m, h^{-n}(hg)^n)$ in G, the goal is to find $h^{-(m+n)}(hg)^{m+n}$, where $m, n \in \mathbb{N}$.

Tropical Semidirect Product. For a semigroup G and a tropical semiring $\mathbb{R}_{max}$ ($\mathbb{R}_{min}$), the semidirect product is defined by the following condition:

$$(a, g)(b, h) = (a^h \otimes b, g \otimes h) \tag{4}$$

for any elements a, b in the tropical semiring and elements g, h in the semigroup G.

We formulate the *Tropical Semidirect Product Problem* (TSPP) in the matrix semiring, since it has been used in this setting (Grigoriev & Shpilrain 2019): Given the tropical matrix semiring $(M_n(\mathbb{Z}),\oplus,\otimes)$, two matrices, M and H, chosen from $M_n(\mathbb{Z})$, and knowing the first components A, B of the expressions $(M,H)^m = (A,H^m)$, and $(M,H)^n = (B,H^n)$, the problem is to determine $(M,H)^{m+n}$.

A scheme whose security relies on this problem is presented by Grigoriev & Shpilrain (2019). This scheme has been attacked in several works, including Jackson & Perumal (2023), Rudy & Monico (2021), Isaac & Kahrobaei (2021), and Muanalifah & Sergeev (2022).

- **The problem of solving a two-sided linear system in tropical semiring**

Let A, B, C, D, X, Y, K be suitable tropical matrices (matrices over tropical semiring). Solving a two-sided tropical linear system involves finding the unknown matrices X and Y from the given matrices A, B, C in the following system:

$$\begin{cases} A \otimes X = X \otimes A, \\ Y \otimes B = B \otimes Y, \\ X \otimes Y = C. \end{cases} \tag{5}$$

Solving this system is equivalent to solving the two-sided tropical equation**:** given the matrices $K, C, D,$ find the unknown matrices *X* and *Y* from the equation:

$$X \otimes D \otimes Y = K, \tag{6}$$

with the condition that

$$X \otimes Y = C.$$

Several protocols, including Grigoriev & Shpilrain (2013), Huang et al. (2022), Amutha & Perumal (2023), Durcheva (2013), Durcheva & Trendafilov (2012), Durcheva (2014a), Durcheva (2014b), Durcheva & Rachev (2015), Durcheva & Ivanova (2018), Ahmed et al. (2022), rely on this problem or on similar problems for their security.

The problem represented by equation (6) turns out to be polynomially equivalent to the problem of determining the winner in *mean payoff games* (Grigoriev 2013). This problem is known to belong to the intersection of NP and coNP complexity classes.

One of the most important attacks (Isaac & Kahrobaei 2021) on the protocols whose security is based on the difficulty of solving of system (5) (or eq. (6)) in tropical semirings ($\mathbb{R}_{min,+}$ and $\mathbb{R}_{max,+}$) exploits the property known as *almost linear periodicity* of tropical matrices.

A sequence of matrices $A^n, n \in \mathbb{N}$ over tropical semirings ($\mathbb{R}_{min,+}$ and $\mathbb{R}_{max,+}$) is called *almost linear periodic* if there exists a period *p,* a linear factor a, and a defect d such that for all $n > d$, the following holds:

$$A_{ij}^{n+p} = a + A_{ij}^{n}.$$

For the semirings $\mathbb{R}_{min,\times}$ and $\mathbb{R}_{max,\times}$, the sequence of matrices exhibits almost linear periodicity if:

$$A_{ij}^{n+p} = a \cdot A_{ij}^{n} .$$

Based on this property, the corresponding two-sided system, similar to system (5) in these semirings, was successfully attacked in Buchinskiy et al. (2023b). Further improvements to these types of attacks have also been proposed in the review paper (Ahmed et al. 2023).

Another attack on system (5), proposed by Kotov and Ushakov (2018), employes the idea of representing the unknown matrices X and Y in the following form:

$$\oplus_{i=0}^{u} x_i \otimes A^{\otimes i}, \ \oplus_{j=0}^{u} y_j \otimes B^{\otimes i},$$

where the coefficients $x_i, y_j \in \mathbb{Z}$ are unknown and u is the upper bound for degrees of polynomials in the protocol.

The idea presented by Kotov and Ushakov is generalized in Alhussaini et al. (2023), where finding the smallest cover is suggested instead of enumerating all possible covers. Such kind of attacks have been applied to several protocols based on modified circulants, like those suggested in Ponmaheshkumar & Perumal (2023), Huang et al. (2022) and Amutha & Perumal (2023).

To avoid linear periodicity, in Ahmed et al. (2022) a modified protocol based on pairs is proposed. Several attacks to this protocol are proposed in Alhussaini et al. (2024), where the ultimate periodicity of those columns and rows of tropical matrix powers whose indices correspond to the critical nodes is exploited.

Another approach for avoiding linear periodicity involves the use of a commutative subset of duo circulant matrices, as stated in Amutha & Perumal (2024).

- **Factorization of tropical polynomials. Finding the GCD of two tropical polynomials.**

The problem of the *factorization of a tropical polynomial* is as follows:

Let $r(x), p(x), q(x)$ be one-variable tropical polynomials: $r(x), p(x), q(x)$. For a given polynomial $r(x)$, find $p(x)$ and $q(x)$ from the equation: $r(x) = p(x) \otimes q(x)$.

The problem of *finding a Great Common Divisor* (*GCD*) *of tropical polynomials* is as follows: Given the tropical polynomials $\text{Pol}_1 = (p_1(x) \otimes q_1(x))$ and $\text{Pol}_2 = \big(p_2(x) \otimes q_2(x)\big)$, find a common divisor of Pol_1 and Pol_2.

The problem of factoring polynomials over a tropical semiring, under several conditions, is NP-complete (Th 7, Kim & Roush 2005). Additionally, the GCD of polynomials over a tropical semiring is not in general unique.

A cryptographic scheme based on this problem was introduced by Chen et al. (2023). This protocol was subsequently attacked in Panny (2023) and Brown & Monico (2023). To overcome these attacks, Géraud-Stewart et al. (2023) suggested

the use of the Fiat-Shamir Transform (FST) claiming that this approach could also be applied to other cryptosystems.

- **Tropical Matrix Power Function problem**

The concept of a *Matrix Power Function* (*MPF*) (Sakalauskas et al. 2017) is defined as follows: Given a matrix $Q = (q_{ij})_{n\times n}$, raising it to the power of a matrix $Y = (y_{ij})_{n\times n}$ from the right produces a resulting matrix $P = (p_{ij})_{n\times n}$ (denoted $P = Q^Y$), where $p_{ij} = \prod_{k=1}^{n} {q_{ik}}^{y_{kj}}$. Similarly, raising Q to the power of a matrix $X = (x_{ij})_{n\times n}$, from the left gives a matrix $S = (s_{ij})_{n\times n}$ (denoted $S = {}^{X}Q$), where $s_{ij} = \prod_{k=1}^{n} {q_{kj}}^{x_{ik}}$.

We first recall the *Matrix Power Function Problem* (*MPFP*) problem as defined by Sakalauskas et al. (2017): Let A, B, C, D, X, Y, Q be suitable matrices, and matrices A, B, C, D, Q be given. The MPF problem (MPF) involves finding unknown matrices *X* and *Y* from the system:

$$\begin{cases} {}^{X}Q^{Y} = E, \\ X^{-1}AX = C, \\ Y^{-1}BY = D. \end{cases} \tag{7}$$

Sakalauskas & Mihalkovich (2018) proved that the MPF problem, under certain constrains, is NP-Complete.

In tropical algebra, this problem is known as the *Tropical Matrix Power Function* (TMPF) problem and it can be defined as follows: Given a tropical matrix *K*, and tropical circulant matrices Q_1 and Q_2, find the unknown tropical matrices X and Y from the equation:

$${}^{X}Q_1 \otimes {}^{Y}Q_2 \otimes M = K \text{ (or } {Q_1}^{X} \otimes {Q_2}^{Y} \otimes M = K). \tag{8}$$

The security of the first stage of the protocol presented by Durcheva (2022) relies on the difficulty of solving the Tropical Matrix Power Function Problem. Some attacks to this protocol are suggested in Jiang et al. (2023) and Buchinskiy et al. (2023a).

Additional analysis of protocols based on the *MPF* problem, including the *TMPF* problem is provided in Mihalkovich et al. (2024). The discussion presented in this Section is summarized in Table 1.

Table 1. *Schemes and the Attacks on them*

Scheme	Semiring	Hard problem	Attack	Method used in the attack
Grigoriev & Shpilrain (2013)	Min-plus	Solving two-sided linear system in a tropical semiring	Kotov& Ushakov (2018) Alhussaini et al. (2023)	1) Generating a set containing all the minimal covers. 2) Applying a heuristic algorithm. Improving the attacks of (KU,2018) by suggesting the identification of the smallest cover instead of enumerating all possible covers.
Durcheva (2013 Durcheva & Trendafilov (2012)	Max-plus	Solving two-sided linear system in a tropical semiring	Ahmed et al. (2023)	Utilizing the linear periodicity property of powers of tropical matrices.
Durcheva (2014a) Durcheva (2014b) Durcheva & Rachev (2015) Durcheva & Ivanova (2018)	Dual semirings: max-plus/ min-plus; max-time/ min-time	Solving a two-sided linear system comprising dual idempotent semirings	Ahmed et al. (2023) Buchinskiy et al. (2023a)	Utilizing the linear periodicity property of powers of tropical matrices in semirings (max+, min+). For max-time/min-time matrices, the relationship between corresponding elements of successive powers is not linear. Utilizing the behavior of sequences of powers of matrices over max-times and min-times algebras.
Grigoriev & Shpilrain (2019)	Min-plus with adjoint multipli-cation	The Tropical Semidirect Product problem	Rudy & Monico (2021) Isaac & Kahrobaei (2021) Muanalifah & Sergeev (2022) Jackson & Perumal (2023)	Utilizing the linearity in the order of the sequence of the employing matrices. Exploiting the “almost linear periodic property” exhibited by the sequence of matrices in use. Solving the TDLP in certain cases and reducing it to the optimal paths problem in others. Utilizing the fact that the difference between the secret key and the product of the shared matrices is independent of the users' choice of public parameters.

Huang et al. (2022) Amutha& Perumal (2023)	Min-plus	Solving the two-sided tropical circular matrix action problem	Buchinskiy et al. (2023b) Alhussaini et al. (2023)	Using some heuristic tricks to reduce checking a small portion of the covers. Using the isomorphism between max-times and max-plus semirings, while improving the attacks of (KU, 2018).
Ponmahesh-kumar & Perumal (2023)	Max-time	Solving a max-product non-linear system	Alhussaini et al. (2023)	Heuristic implementation of the (KU, 2018) attack utilizing a cover.
Ahmed et al. (2022)	Max-plus	Solving tropical two-sided non-linear equation with 6 unknown variables	Alhussaini et al. (2024)	Exploiting the ultimate periodicity of the columns and rows of matrix powers whose indices correspond to the critical nodes.
Durcheva (2022) 2- phase key exchange protocol	Min-plus; Max-plus	Solving MPF problem in tropical semiring	Jiang et al. (2023) attacked 1st phase Buchinskiy et al. (2023a) attacked 2nd phase	Solving the linear equations on the tropical semiring. Computing the defect and period of a public matrix M.
Chen et al. (2023)	Min-plus	Factoring one-variable tropical polynomial	Panny (2023) Brown & Monico (2023)	1) Searching for small modifications to the coefficients of the resultant matrices. 2) Instead of full factorization, finding only small-degree divisors. Swapping certain symbols involved in computing the signature; factoring the hash; factoring the public key; re-hashing an honest signature.

Future prospects

It is well-known that finding cryptographic primitives to serve as building blocks for cryptosystems that can resist quantum computer attacks is highly challenging. The problem of developing a secure key-exchange scheme over an insecure (public) channel remains unsolved. Taking into account the vulnerabilities of key-exchange protocols based on tropical algebra, we pose the question: Could tropical (or, more broadly, idempotent) cryptography provide a solution to this issue?

Looking ahead, we contemplate the future of cryptography based on idempotent algebra and envision several potential directions.

Exploring Different Hard Problems/Different Cryptographic Primitives within Tropical Semirings

Examples of such protocols include:

- The protocols proposed by Huang et al. (2024a) and Huang & Li (2022), which are based on the problem of finding the multiple exponentiations of tropical matrices (METM).

The authors of these protocols assert that the *METM* problem can be transformed into a constructive membership problem of a semigroup in polynomial time, which is a hard problem resisting quantum computer attack, as demonstrated in (Childs & Ivanyos 2014). In a recent paper (Huang et al. 2024b), it is stated that it has not yet been proven that the *METM* problem can be reduced to the Hidden Subgroup Problem, which is vulnerable to the quantum cryptanalysis.

- The protocol suggested by Durcheva & Danilchenko (2024), which utilized tropical block matrices as building blocks.

The security of this protocol relies on the matrix decomposition problem based on block matrices. Although a recent attack on this protocol in certain cases has been discussed in (Otero Sánchez et al. 2024), we believe that employing tropical block matrices as a cryptographic primitive offers a promising approach.

Building Alternative Types of Protocols, which Combines Various Techniques

Examples of such protocols include:

- An encryption protocol based on max-plus (MP) wavelet transforms.

MP-Wavelets are computationally simple and efficient, as noted by the authors of the protocol presented in (Subiono et al. 2022). The advantage of using them for building an encryption scheme is that the number of possible decryption keys is very large, even if the plaintext is short.

- Protocols based on T-norms.

The authors of several Stickel's like protocols based on max-min (max-T) semirings (Alhussaini & Sergeev 2024) argue that the advantage of max-min protocols over tropical ones is that the max-min protocols demonstrate greater resilience against the two-sided discrete logarithm attacks. Existing attacks such as the Kotov-Ushakov method (Kotov & Ushakov 2018) have been shown to be not very successful.

Utilizing Enriched Idempotent Semirings, such as Complete Idempotent Semirings (Quantales)

The connection between quantales and tropical mathematics is discussed by Fujii (2019). While no cryptosystems have been built yet based on this algebraic structure, we believe it represents a promising direction for future development.

Conclusions

We have been conducting research on semirings since 2010, with a specific focus on idempotent semirings and cryptography based on them since 2013. Over this period, dozens of tropical protocols have been developed. However, a significant portion of these proposed protocols has been exposed to various types of attacks, revealing vulnerabilities in key exchange protocols based on tropical algebra. Additionally, the advent of quantum computing has posed significant threats to classical public-key cryptosystems, raising the legitimate question of whether tropical cryptography has a viable future. Post-quantum cryptography relies on NP-hard problems that are considered harder than those used in classical cryptography and are specifically designed to resist quantum attacks. According to NIST's Post-Quantum Cryptography Project (https://www.nist.gov/pqcrypto), the main categories of post-quantum cryptography currently include *Hash-Based Cryptography*; *Lattice-Based Cryptography; Code-Based Cryptography*; *Multivariate- Based Cryptography,* and *Isogeny-Based Cryptography*. Although tropical-based cryptography has not yet been included in this list, certain problems in different semirings can be considered computationally hard, as no known quantum algorithm has been proven to solve them efficiently. For example, the security of certain cryptosystems, such as the one proposed by Huang et al. (2024c), which utilizes the digital semiring, is based on the 3-satisfiability problem. This problem can be polynomially reduced to solving systems of quadratic polynomial equations over the semiring, a task that is recognized as NP-hard.

In this paper, we provided a review of the current state of tropical cryptography and shared our insights on its future directions. We envision several approaches for its development, including exploring different hard problems or different cryptographic primitives within tropical semirings; developing alternative types of protocols that combine various techniques; and utilizing enriched idempotent semirings, such as complete idempotent semirings (quantales).

References

Ahmed K, Pal S, Mohan R (2022) Key exchange protocol based upon a modified tropical structure. *Communications in Algebra* 51(1): 214–223.

Ahmed K, Pal S, Mohan R (2023) A review of the tropical approach in cryptography. *Cryptologia* 47(1): 63–87.

Alhussaini S, Sergeev S (2024) *On implementation of Stickel's key exchange protocol over max-min and max-T semirings*. Preprint. Available at: https://eprint.iacr.org/2024/519.pdf.

Alhussaini S, Collett C, Sergeev S (2023) *Generalized Kotov-Ushakov Attack on Tropical Stickel Protocol Based on Modified Circulants*. Preprint. Available at: https://ia.cr/2023/1904.

Alhussaini S, Collett C, Sergeev S (2024) *On the tropical two-sided discrete logarithm and a key exchange protocol based on the tropical algebra of pairs*. IACR Cryptol. ePrint Arch., 10.

Amutha B, Perumal R (2023) Public key exchange protocols based on tropical lower circulant and anti-circulant matrices. *AIMS Mathematics* 8(7): 17307–17334.

Amutha B, Perumal R (2024) Two party key exchange protocol based on duo circulant matrices for the IoT environment. *International Journal of Information Technology* 10(Jun): 3585–3596.

Brown DR, Monico C (2023) *More forging (and patching) of tropical signatures.* IACR Cryptol. ePrint Arch., 1837.

Brunsch T, Hardouin L, Maia CA, Raisch J (2012) Duality and interval analysis over idempotent semirings. *Linear Algebra and its Applications* 437: 2436–2454.

Buchinskiy I, Kotov M, Treier A (2023a) An attack on a key exchange protocol based on max-times and min-times algebras. *Indian Journal of Pure and Applied Mathematics* 56(Jul): 180–190.

Buchinskiy I, Kotov M, Treier A (2023b) *Analysis of four protocols based on tropical circulant matrices.* IACR Cryptol. ePrint Arch., 1707.

Bulavchuk A, Semenova D (2023) Application of idempotent algebra methods in genetic algorithm for solving the scheduling problem. *Prikladnaya Diskretnaya Matematika.* Available at: https://doi.org/10.17223/20710410/58/11.

Callas J, Donnerhacke L, Finney H, Thayer R (1998) *OpenPGP message format*. Internet RFC 2440.

Chen J, Grigoriev D, Shpilrain V (2023) *Tropical cryptography III: digital signatures*. IACR Cryptol. ePrint Arch., 1475.

Childs AM, Ivanyos G (2014) Quantum computation of discrete logarithms in semigroups. *Journal of Mathematical Cryptology* 8(4): 405–416.

Cuninghame-Green R (1979) *Mini–max algebra, v. 166 of Lecture Notes in Economica and Mathematical Systems*. Berlin: Springer-Verlag.

Dierks T, Allen C (1999) *RFC 2246: The TLS Protocol Version 1.0. IETF RFC 2246*. Available at: http://www.ietf.org/rfc/rfc2246.txt.

Diffie W, Hellman ME (1976) New directions in cryptography. *IEEE Transactions on Information Theory* IT-22(6): 644–654.

Durcheva M (2013) Public key cryptography with max-plus matrices and polynomials, In *AIP Conference Proceedings* 1570, 491.

Durcheva M (2014a) Public Key Cryptosystem Based on Two-Sided Action of Different Exotic Semirings. *Journal of Mathematics and System Science* 4(Jan).

Durcheva M (2014b) An application of different dioids in public key cryptography. In *AIP Conference Proceedings* 1631, 336.

Durcheva M (2020) *Semirings as Building Blocks in Cryptography*. Cambridge, UK: Cambridge Scholars Publishing.

Durcheva M (2022) TrES: Tropical Encryption Scheme Based on Double Key Exchange. *European Journal of Information Technologies and Computer Science* 2(4).

Durcheva M, Trendafilov I (2012) Public key cryptosystem based on max-semirings. In *AIP Conference Proceedings* 1497, 357.

Durcheva M, Rachev M (2015) A public key encryption scheme based on idempotent semirings. In *AIP Conference Proceedings* 1690, 060008.

Durcheva M, Ivanova M (2018) Key Agreement Protocol for Distributed Secure Multicast For eAssessment. *International Journal on Information Technologies & Security* 10(1).

Durcheva M, Danilchenko K (2024) Secure Key Exchange in Tropical Cryptography: Leveraging Efficiency with Advanced Block Matrix Protocols. *Mathematics* 12: 1429.

Fountoukidou C, Pittou M (2022) A formal algebraic approach for the quantitative modeling of connectors in architectures. In D Poulakis, G Rahonis (eds.), *Algebraic Informatics*. LNCS, vol. 13706. Springer.

Fujii S (2019) Enriched categories and tropical mathematics. In *arXiv: Category Theory*.

Géraud-Stewart R, Naccache D, Yifrach-Stav O (2023) *Fiat-Shamir Goes Tropical*. Preprint. Available at: https://ia.cr/2023/1954.

Goel N, Gupta I, Dass BK (2020) Survey on SAP and its application in public-key. *Journal of Mathematical Cryptology* 14(1): 144–152.

Golan J (1999) *Semirings and Their Applications*. Dordrecht: Kluwer.

Grigoriev D (2013) Complexity in Tropical Algebra. In *Proceedings of the International Workshop on Computer Algebra in Scientific Computing*, 148–154. Berlin, Germany.

Grigoriev D, Shpilrain V (2013) Tropical cryptography. *Communications in Algebra* 42: 2624–2632.

Grigoriev D, Shpilrain V (2019) Tropical cryptography II: Extensions by homomorphisms, *Communications in Algebra* 47(10): 1–6.

Huang H, Li C (2022) Tropical Cryptography Based on Multiple Exponentiation Problem of Matrices. *Security and Communication Networks* 1024161.

Huang H, Li C, Deng L (2022) Public-Key Cryptography Based on Tropical Circular Matrices. *Applied Science* 12(15): 7401.

Huang H, Kong W, Xu T (2024a) Asymmetric Cryptography Based on the Tropical Jones Matrix. *Symmetry* 16(4): 456.

Huang H, Peng C, Deng L (2024b) Reduction of the semigroup-action problem on a module to the hidden-subgroup problem. *Quantum Information Processing* 23(Aug): 300.

Huang H, Jiang X, Peng C, Pan G (2024c) A new semiring and its cryptographic applications. *AIMS Mathematics* 9(8): 20677–20691.

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

Jackson J, Perumal R (2023) Another Cryptanalysis of a Tropical Key Exchange Protocol. *IAENG International Journal of Computer Science* 50(4).

Jackson J, Perumal R (2024) A Public Key Exchange Protocol Using Tropical Determinant for IoT Environment. Lecture Notes in Networks and Systems. In *Proc. of the 3rd International Conference on Adv. Comp. and Appl.*, 81–93. Kolkata, India, 23–24 February 2024. Singapore: Springer.

Jiang X, Huang H, Pan G (2023) Cryptanalysis of Tropical Encryption Scheme Based on Double Key Exchange. *Journal of Cyber Security and Mobility* 12(2): 205–220.

Kim KH, Roush FW (2005) Factorization of polynomials in one variable over the tropical semiring. In *arXiv: Combinatorics*.

Kotov M, Ushakov A (2018) Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology* 12(3): 137–141.

Krivulin N (2020) Algebraic solution of minimax single facility constrained location problems with Chebyshev and rectilinear distances. *Journal of Logical and Algebraic Methods in Programming* 115(Oct): 100578.

Krivulin N, Gubanov S (2021) Algebraic solution of a problem of optimal project scheduling in project management. *Vestnik St. Petersburg University: Mathematics* 8: 73–87.

Maslov V (1986) *New superposition principle for optimization problems.* Sem. sur les Equations avec Dérivées Partielles 1985/6. Centre Mathématique de l'Ecole Polytechnique Palaiseau, esp. 24.

Maze G, Monico C, Rosenthal J (2007) Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications* 1(4): 489–507.

Medelin JM (2022) Generation, Regeneration and Validation of Binary Secret Keys through Blockchain in IoT Devices. *Athens Journal of Sciences* 9(1): 25–46.

Mihalkovich A, Zitkevicius J, Sakalauskas E (2024) The security analysis of the key exchange protocol based on the matrix power function defined over a family of non-commuting groups. *AIMS Mathematics* 9(10): 26961–26982.

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.

Muanalifah A, Riana A, Artes JrR, Nurwan (2023) The tropical version of El Gamal Encryption. *Journal of Natural Sciences and Mathematics Research* 9(2): 151–157.

Nagata K (2023) Automatic Generating System of Information Security Policy. *Athens Journal of Technology and Engineering* 10(4): 227–236.

NIST Post-Quantum Cryptography Project. Available at: https://www.nist.gov/pqcrypto [Accessed 2 September 2024].

Otero Sánchez Á, Camazón Portela D, López-Ramos JA (2024) On the Solutions of Linear Systems over Additively Idempotent Semirings. *Mathematics* 12: 2904.

Panny L (2023) *Forging tropical signatures*. IACR Cryptol. ePrint Arch., 1748.

Ponmaheshkumar A, Perumal R (2023) Toeplitz matrices based key exchange protocol for the internet of things. *International Journal of Information Technology* 65(11).

Ponmaheshkumar A, Perumal R (2024) Enhancing vehicle IoT security through matrix power functions in supertropical semiring. *Math. Eng. Sci. Aerosp. (MESA)* 15: 213.

Rudy D, Monico C (2021) Remarks on a Tropical Key Exchange System. *Journal of Mathematical Cryptology* 15: 280–283.

Sakalauskas E, Mihalkovich A (2018) MPF Problem over Modified Medial Semigroup Is NP-Complete. *Symmetry* 10: 571.

Sakalauskas E, Mihalkovich A, Venckauskas A (2017) Improved Asymmetric Cipher Based on Matrix Power Function with Provable Security. *Symmetry* 9(1): 9.

Shpilrain V (2018) Problems in group theory motivated by cryptography. In *arXiv: 1802.07300*.

Simon I (1988) Recognizable sets with multiplicities in the tropical semiring. Mathematical Foundations of Computer Science. In *Proceedings of the 13th Symposium*, 107–120. Carlsbad, Czechoslovakia, 29 Aug–2 Sep 1988. Germany: Springer.

Steinwandt R, Suarez Corona A (2011) Cryptanalysis of a 2-party key establishment based on a semigroup action problem. *Advances in Mathematics of Communications* 5(1): 87–92.

Subiono JC, Dieky A, Davvaz B (2022) A cryptographic algorithm using wavelet transforms over max-plus algebra. *Journal of King Saud University – Computer and Information Sciences* 34: 627–635.

Trendafilov I, Durcheva M (2010) Discrete logarithm in finite fields. Some algorithms for computing new public key cryptosystem. In *AIP Conference Proceedings* 1293.

Trendafilov I, Tzvetkov R (2021) Derivations in a product of additively idempotent semirings. In *AIP Conference Proceedings* 2333, 110003.

Vandiver HS (1934) Note on a simple type of algebra in which cancellation law of addition does not hold. *Bulletin of American Mathematical Society* 40(12): 914–920.

Ylonen T, Lonvick C (2006) *The Secure Shell (SSH) Protocol Architecture*. Technical Report 4251. RFCEditor.