AIMS Mathematics, 9(8): 20677–20691.
DOI: 10.3934/math.20241005
Received: 07 March 2024
Revised: 28 May 2024
Accepted: 13 June 2024
Published: 26 June 2024

https://www.aimspress.com/journal/Math

Research article

A new semiring and its cryptographic applications

Huawei Huang[1,*], **Xin Jiang**[1], **Changwen Peng**[2] **and Geyang Pan**[1]

[1] School of Mathematical Sciences, Guizhou Normal University, Guiyang 550025, China
[2] School of Mathematics and Information Science, Guiyang University, Guiyang 550005, China

* **Correspondence:** Email: hwhuang7809@163.com.

Abstract: This paper introduced a novel semiring structure involving nonnegative integers, where operations depended on the comparison of the magnitudes of decimal digit sums. Consequently, a corresponding matrix semiring can be established on this commutative semiring. We showed that the 3-satisfiability problem can be polynomial-time reduced to solving systems of quadratic polynomial equations over this semiring. We proposed a key exchange protocol based on this matrix semiring, with its security relying on the two-sided digital circulant matrix action problem over this semiring. This scheme provides a novel cryptographic primitive for post-quantum cryptography.

Keywords: circulant matrix; semiring; key exchange protocols
Mathematics Subject Classification: 15A80, 94A60

1. Introduction

Research on the theory of semiring algebra began in the early twentieth century when Vandiver [1] introduced the concept of semiring in 1934. Semirings encompass all properties of rings except for additive inverses and have extensive applications in combinatorics, functional analysis, topology, automata, computer science theory, and cryptography. Over the past two decades, various algebraic structures have been employed to enhance existing public-key cryptosystems. In 1998, Yamamura [2,3] employed modulo groups to construct cryptosystems; however, in 2001, Steinwandt [4] demonstrated their vulnerability to ciphertext-only attacks. In 2013, Kahrobaei et al. [5] employed the 3×3 matrix over $F_7[S_5]$ to develop a key exchange protocol and cryptosystem, which Eftekhari [6] later successfully cracked. Literature [7–9] proposed cryptosystems based on braid groups, but Hofheinz and Steinwandt [10] demonstrated their insecurity.

Brazilian mathematician Imre Simon [11] introduced the concept of tropical semirings, where addition represents the comparative size of a number, and multiplication corresponds to ordinary addition. Recently, researchers have actively explored the application of tropical semirings in various

cryptographic schemes. Shpilrain and Grigoriev [12, 13] developed a key exchange protocol utilizing tropical matrix semirings.

However, Kotov and Ushakov [14] identified patterns in higher powers of tropical matrices, resulting in an attack on the protocol proposed by Shpilrain and Grigoriev [12]. Rudy and Monico [15] exploited the monotonically decreasing nature of the first part of the sequence $\{(M,H)^m\}$ to propose a fairly effective attack on [13]. Isaac and Kahrobaei [16] utilized the almost linear periodicity of the first part of the sequence $\{(M,H)^m\}$ to propose an attack on [13] and demonstrated that the second protocol cannot be implemented. Muanalifah and Sergeev [17] proposed three types of key exchange protocols using the Jones matrix and Line de la Puente matrix, along with introducing a generalized Kotov-Ushakov attack.

Cryptographic schemes generally rely on the hardness of certain mathematical problems. If such a problem is non-deterministic polynomial-time (NP) complete or NP hard, the corresponding cryptographic scheme is considered to be resistant to quantum attacks. The main types of post-quantum cryptography currently include lattice-based cryptography [18], code-based cryptography [19], and multivariate cryptography [20]. Their security relies on the shortest vector problem of lattice, the closest vector problem of lattice, the problem of decoding random linear codes, and the problem of solving systems of multivariate quadratic equations over finite fields. Lattice-based cryptographic schemes are considered highly secure against quantum attacks. In recent years, this field of research has developed rapidly. For example, Nassr, Anwar, and Bahig [21] proposed a new lattice-based cryptosystem, which offers significant improvements in security and efficiency. The system's security is comparable to that of the number theory research unit (NTRU) and remains robust against attacks by quantum computers.

The 3-satisfiability (3-SAT) problem is a well-known NP-complete problem in the computational complexity theory. It involves determining if there exists an assignment of variables that satisfies a given Boolean formula expressed in conjunctive normal form (CNF) with exactly three literals per clause. Introduced in the early 1970s, the 3-SAT problem is a cornerstone in theoretical computer science, serving as a benchmark for many computational problems and algorithms [22,23].

In the literature [24, 25], several quantum-resistant cryptosystems have been proposed. These cryptosystems utilize the multiple exponential power problem of tropical matrices and the tropical circulant matrix action problem, respectively. Other researchers have proposed cryptosystems based on different types of semirings. For instance, Thiruveni [26] devised an Elgamal-type cryptographic system using regular semirings, while Nivetha [27] extended the Diffie-Hellman key exchange protocol by incorporating exponential semirings within its multiplicative left ideal.

This paper introduces a new semiring called the digital semiring and proposes a key exchange protocol based on the matrix semiring over it. Its security relies on the difficulty of solving quadratic polynomial systems over it. We show that the 3-SAT problem can be polynomial-time reduced to it. The scheme presented in this article introduces a new paradigm for post-quantum cryptography.

2. A new semiring and its matrix semiring

Definition 2.1. *[1]* A semiring is a nonempty set S on which the operations of $+$ and $\cdot$ are defined to satisfy the following conditions:

(1) $(S,+)$ is a commutative monoid with identity element 0 ;

(2) $(S, \cdot)$ is a monoid with identity element 1_s;

(3) Multiplication distributes over addition from either side;

(4) $s \cdot 0 = 0 \cdot s = 0$, for all $s \in S$;

(5) $0 \neq 1_s$.

The semiring satisfies all properties of the ring except the additive inverse. If $(S, \cdot)$ is commutative, then S is referred to as a commutative semiring. For example, the set N of natural numbers, including 0, forms a commutative semiring under addition and multiplication.

Let $W = N \cup \{\infty\}$, where N is the set of natural numbers. We define the symbol "( )" as follows:

$$(a) = \begin{cases} b & \text{when } a \in N, \\ \infty & \text{when } a = \infty, \end{cases}$$

where b is the sum of all digits of a. For example, $(123) = 1 + 2 + 3 = 6, (3456) = 3 + 4 + 5 + 6 = 18$.

Definition 2.2. Define two operations $\oplus$ and $\otimes$ over $W = N \cup \{\infty\}$ as follows:

$$a \oplus b = \begin{cases} a & (a) > (b), \\ b & (a) < (b), \\ \max(a, b) & (a) = (b), \end{cases}$$

$$a \otimes b = \begin{cases} a & (a) < (b), \\ b & (a) > (b), \\ \min(a, b) & (a) = (b). \end{cases}$$

Theorem 2.3. $(W, \oplus, \otimes)$ is a semiring.

Proof. (1) First, we prove that W forms a commutative monoid with respect to the operation $\oplus$. Let $a, b, c \in W$.

(A) Since the result of $a \oplus b$ is either a or b, it follows that the operation $\oplus$ satisfies closure property.

(B) The operation $\oplus$ satisfies the associative property. Table 1 shows that the associative law of $\oplus$ when (a), (b), and (c) are pairwise distinct. Table 2 shows that the associative law of $\oplus$ when two of (a), (b), and (c) are equal.

Table 1. The associative property of $\oplus$ ($(a) \neq (b) \neq (c)$).

Possible cases	$a \oplus (b \oplus c)$	$(a \oplus b) \oplus c$
$(a) < (b) < (c)$	$a \oplus c = c$	$b \oplus c = c$
$(a) < (c) < (b)$	$a \oplus b = b$	$b \oplus c = b$
$(b) < (a) < (c)$	$a \oplus c = c$	$a \oplus c = c$
$(b) < (c) < (a)$	$a \oplus c = a$	$a \oplus c = a$
$(c) < (a) < (b)$	$a \oplus b = b$	$b \oplus c = b$
$(c) < (b) < (a)$	$a \oplus b = a$	$a \oplus c = a$

Table 2. The associative property of $\oplus$ ((a), (b), and (c) involve two elements being equal).

Possible cases	$a \oplus (b \oplus c)$	$(a \oplus b) \oplus c$
$(a) = (b) < (c), a \leq b$	$a \oplus c = c$	$b \oplus c = c$
$(a) = (b) < (c), a > b$	$a \oplus c = c$	$a \oplus c = c$
$(a) = (b) > (c), a \leq b$	$a \oplus b = b$	$b \oplus c = b$
$(a) = (b) > (c), a > b$	$a \oplus b = a$	$a \oplus c = a$
$(a) = (c) < (b), a \leq c$	$a \oplus b = b$	$b \oplus c = b$
$(a) = (c) < (b), a > c$	$a \oplus b = b$	$b \oplus c = b$
$(a) = (c) > (b), a \leq c$	$a \oplus c = c$	$a \oplus c = c$
$(a) = (c) > (b), a > c$	$a \oplus c = a$	$a \oplus c = a$
$(b) = (c) < (a), b \leq c$	$a \oplus c = a$	$a \oplus c = a$
$(b) = (c) < (a), b > c$	$a \oplus b = a$	$a \oplus c = a$
$(b) = (c) > (a), b \leq c$	$a \oplus c = c$	$b \oplus c = c$
$(b) = (c) > (a), b > c$	$a \oplus b = b$	$b \oplus c = b$

When $(a) = (b) = (c)$, we have $a \oplus (b \oplus c) = \max(a, b, c) = (a \oplus b) \oplus c$.

(C) $\forall a \in W$, and we have $a \oplus 0 = 0 \oplus a = a$. Thus, 0 is the identity element (zero element) for the operation $\oplus$.

(D) $\forall a, b \in W$, and we have $a \oplus b = b \oplus a$. Therefore, $\oplus$ satisfies the commutative property.

(E) Let $a, b \in W$. If $a \neq 0$, then $a \oplus b \neq 0$. Hence, apart from 0, none of the other elements have additive inverses.

In summary, W forms a commutative monoid with respect to the operation $\oplus$.

(2) Next, we prove that W forms a monoid with respect to the operation $\otimes$.

(A) Since the result of $a \otimes b$ is either a or b, the operation $\otimes$ is closed.

(B) The operation $\otimes$ satisfies the associative property. Table 3 describes the associative law of $\otimes$ when (a), (b), and (c) are pairwise distinct. Table 4 describes the associative law of $\otimes$ when two of (a), (b), and (c) are equal.

Table 3. The associative property of $\otimes$ ($(a) \neq (b) \neq (c)$).

Possible cases	$a \otimes (b \otimes c)$	$(a \otimes b) \otimes c$
$(a) < (b) < (c)$	$a \otimes b = a$	$a \otimes c = a$
$(a) < (c) < (b)$	$a \otimes c = a$	$a \otimes c = a$
$(b) < (a) < (c)$	$a \otimes b = b$	$b \otimes c = b$
$(b) < (c) < (a)$	$a \otimes b = b$	$b \otimes c = b$
$(c) < (a) < (b)$	$a \otimes c = c$	$a \otimes c = c$
$(c) < (b) < (a)$	$a \otimes c = c$	$b \otimes c = c$

Table 4. The associative property of $\otimes$ ((a), (b), and (c) involve two elements being equal.

Possible cases	$a \otimes (b \otimes c)$	$(a \otimes b) \otimes c$
$(a) = (b) < (c), a \leq b$	$a \otimes b = a$	$a \otimes c = a$
$(a) = (b) < (c), a > b$	$a \otimes b = b$	$b \otimes c = b$
$(a) = (b) > (c), a \leq b$	$a \otimes c = c$	$a \otimes c = c$
$(a) = (b) > (c), a > b$	$a \otimes c = c$	$b \otimes c = c$
$(a) = (c) < (b), a \leq c$	$a \otimes c = a$	$a \otimes c = a$
$(a) = (c) < (b), a > c$	$a \otimes c = c$	$a \otimes c = c$
$(a) = (c) > (b), a \leq c$	$a \otimes b = b$	$b \otimes c = b$
$(a) = (c) > (b), a > c$	$a \otimes b = b$	$b \otimes c = b$
$(b) = (c) < (a), b \leq c$	$a \otimes b = b$	$b \otimes c = b$
$(b) = (c) < (a), b > c$	$a \otimes c = c$	$b \otimes c = c$
$(b) = (c) > (a), b \leq c$	$a \otimes b = a$	$a \otimes c = a$
$(b) = (c) > (a), b > c$	$a \otimes c = a$	$a \otimes c = a$

When $(a) = (b) = (c)$, we have $a \otimes (b \otimes c) = \min(a, b, c) = (a \otimes b) \otimes c$.

(C) $\forall a \in W$, $a \otimes \infty = \infty \otimes a = a$. Therefore, the identity element for $\otimes$ is ∞.

In conclusion, W forms a monoid with respect to the operation $\otimes$.

(3) Next, we prove that the operation $\otimes$ distributes over $\oplus$. Table 5 shows that $\otimes$ satisfies the distributive law over $\oplus$ when (a), (b), and (c) are pairwise distinct. Table 6 shows that $\otimes$ satisfies the distributive law over $\oplus$ when two of (a), (b), and (c) are equal.

When $(a) = (b) = (c)$, we have

$$a \otimes (b \oplus c) = \min(a, \max(b, c)) = \max(\min(a, b), \min(a, c)) = a \otimes b \oplus a \otimes c.$$

Table 5. The distributive property ($(a) \neq (b) \neq (c)$).

Possible cases	$a \otimes (b \oplus c)$	$a \otimes b \oplus a \otimes c$
$(a) < (b) < (c)$	$a \otimes c = a$	$a \oplus a = a$
$(a) < (c) < (b)$	$a \otimes b = a$	$a \oplus a = a$
$(b) < (a) < (c)$	$a \otimes c = a$	$b \oplus a = a$
$(b) < (c) < (a)$	$a \otimes c = c$	$b \oplus c = c$
$(c) < (a) < (b)$	$a \otimes b = a$	$a \oplus c = a$
$(c) < (b) < (a)$	$a \otimes b = b$	$b \oplus c = b$

Table 6. The distributive property (two elements are equal in $(a), (b), (c)$.

Possible cases	$a \otimes (b \oplus c)$	$a \otimes b \oplus a \otimes c$
$(a) = (b) < (c), a \leq b$	$a \otimes c = a$	$a \oplus a = a$
$(a) = (b) < (c), a > b$	$a \otimes c = a$	$b \oplus a = a$
$(a) = (b) > (c), a \leq b$	$a \otimes b = a$	$a \oplus c = a$
$(a) = (b) > (c), a > b$	$a \otimes b = b$	$b \oplus c = b$
$(a) = (c) < (b), a \leq c$	$a \otimes b = a$	$a \oplus a = a$
$(a) = (c) < (b), a > c$	$a \otimes b = a$	$a \oplus c = a$
$(a) = (c) > (b), a \leq c$	$a \otimes c = a$	$b \oplus a = a$
$(a) = (c) > (b), a > c$	$a \otimes c = c$	$b \oplus c = c$
$(b) = (c) < (a), b \leq c$	$a \otimes b = b$	$b \oplus c = b$
$(b) = (c) < (a), b > c$	$a \otimes b = b$	$b \oplus c = b$
$(b) = (c) > (a), b \leq c$	$a \otimes c = a$	$a \oplus a = a$
$(b) = (c) > (a), b > c$	$a \otimes b = a$	$a \oplus a = a$

In conclusion, the distributive property of $\otimes$ over $\oplus$ holds.

Finally, let's prove the last two conditions.

(4) $\forall a \in W$, and we have $a \otimes 0 = 0 \otimes a = 0$.

(5) $0 \neq \infty$.

In conclusion, $(W, \oplus, \otimes)$ forms a semiring and is also a commutative semiring.

For convenience, we refer to it as "digital semiring". It has the following properties:

(1) $(W, \oplus)$ is a commutative monoid with identity element 0 ;

(2) $(W, \otimes)$ is a monoid with identity element ∞;

(3) $a \oplus a = a, a \otimes a = a$, for all $a \in W$.

The security of the cryptographic scheme proposed in this paper relies on the problem of solving quadratic polynomial systems over the new semiring. If this problem is NP-hard, then cryptographic schemes based on it will be resistant to quantum attacks. If we can prove that the 3-SAT problem can be polynomial-time reduced to the problem of solving quadratic polynomial systems over the new semiring, then the problem of solving quadratic polynomial systems over the new semiring is NP-hard.

The Boolean satisfiability problem is NP complete. If all expressions are written in the form of a conjunction normal form with 3 variables per clause (3-CNF), then it is still an NP complete problem and called the 3-SAT problem. The theorem below asserts that the problem of solving quadratic polynomial systems over this semiring is usually NP hard.

Theorem 2.4. 3-SAT problem can be polynomial-time reduced to the problem of solving quadratic polynomial systems over this semiring.

Proof: Suppose we have a 3-CNF. We can construct a system of nonlinear equations on a digital semiring. And this system of equations has a solution if and only if there is a solution for the 3-CNF. Let the variable in the 3-CNF be u_i, corresponding to two variables x_i and y_i, where $u_i = x_i$ and $\neg u_i = y_i$.

Suppose a clause in a 3-CNF expression: $u_i \vee \neg u_j \vee u_k$. The corresponding system of polynomial equations can be constructed as follows:

$$\begin{cases} x_i \otimes y_i = 0, \\ x_j \otimes y_j = 0, \\ x_k \otimes y_k = 0, \\ x_i \oplus y_i = 1, \quad (\nabla) \\ x_j \oplus y_j = 1, \\ x_k \oplus y_k = 1, \\ x_i \oplus y_j \oplus x_k = 1. \end{cases}$$

Suppose $u_i \vee \neg u_j \vee u_k$ is TURE, i.e., $u_i = 1$, $u_j = 0$, or $u_k = 1$.

(1) If $u_i = 1$, then $x_i = 1, y_i = 0$, and the system of equations (∇) is satisfied;

(2) if $u_j = 0$, then $x_j = 0, y_j = 1$, and the equation (∇) is satisfied;

(3) if $u_k = 1$, then $x_k = 1, y_k = 0$, and the equation (∇) is satisfied.

So, when $u_i \vee \neg u_j \vee u_k$ is TURE, there is a solution to equation (∇).

Conversely, when there is a solution to equation (∇), i.e., $x_i = 1$, $y_j = 1$, or $x_k = 1$.

(1) If $x_i = 1$, then $u_i = 1$, and $u_i \vee \neg u_j \vee u_k$ is TURE;

(2) if $y_j = 1$, then $\neg u_j = 1$, and $u_i \vee \neg u_j \vee u_k$ is TURE;

(3) if $x_k = 1$, then $u_k = 1$, and $u_i \vee \neg u_j \vee u_k$ is TURE.

Thus, for each clause in the given 3-CNF, we can construct a system of quadratic polynomial equations on a digital semiring. Finally, we obtain the corresponding system of equations over the whole 3-CNF that has a solution if, and only if, the given 3-CNF expression is satisfied. Thus, the 3-CNF satisfiability problem can be effectively reduced to solving a system of quadratic polynomial equations over the digital semiring.

Next, we define the matrix semiring for digital semiring.

Definition 2.5. Let $M_n(W)$ be the set of all $n \times n$ matrices over W. We can define $\oplus$ and $\otimes$ as follows:

$$(A \oplus B)_{ij} = a_{ij} \oplus b_{ij}, (A \otimes B)_{ij} = \bigoplus_{k=1}^{n} \left(a_{ik} \otimes b_{kj}\right), \text{ for all } A, B \in M_n(W).$$

Then, $(M_n(W), \oplus, \otimes)$ is also a semiring with respect to the above operation, which is called a digital matrix semiring.

The identities under $\oplus$ and $\otimes$ on $(M_n(W), \oplus, \otimes)$ are:

$$O = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}, I = \begin{bmatrix} \infty & 0 & \cdots & 0 \\ 0 & \infty & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \infty \end{bmatrix}, \text{ respectively.}$$

Definition 2.6. *[28]* If a matrix A has the following form,

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}$$

then it is called a circulant matrix and it is denoted $A = [a_1, a_2, \cdots, a_n]$. It can be easily verified that if A, B are circulant, then $A \otimes B = B \otimes A$. For example,

$$\begin{pmatrix} 828 & 6086 & 354 \\ 354 & 828 & 6086 \\ 6086 & 354 & 828 \end{pmatrix} \otimes \begin{pmatrix} 939 & 1083 & 5143 \\ 5143 & 939 & 1083 \\ 1083 & 5143 & 939 \end{pmatrix} = \begin{pmatrix} 828 & 6086 & 5143 \\ 5143 & 828 & 6086 \\ 6086 & 5143 & 828 \end{pmatrix},$$

$$\begin{pmatrix} 939 & 1083 & 5143 \\ 5143 & 939 & 1083 \\ 1083 & 5143 & 939 \end{pmatrix} \otimes \begin{pmatrix} 828 & 6086 & 354 \\ 354 & 828 & 6086 \\ 6086 & 354 & 828 \end{pmatrix} = \begin{pmatrix} 828 & 6086 & 5143 \\ 5143 & 828 & 6086 \\ 6086 & 5143 & 828 \end{pmatrix}.$$

3. Key exchange protocol based on digital semiring

3.1. Protocol

Alice and Bob agree to exchange keys over the digital semiring W and randomly select a matrix $M \in M_n(W)$ and a prime p as public keys. To obtain the shared secret, Alice and Bob perform the following steps:

(1) Alice chooses two circulant matrices $A_1, A_2 \in M_n(W)$ as her private keys. She computes her public key $U = A_1 \otimes M \otimes A_2$ and sends it to Bob;

(2) Bob chooses two circulant matrices $B_1, B_2 \in M_n(W)$ as his private keys. He computes his public key $V = B_1 \otimes M \otimes B_2$ and sends it to Alice;

(3) Alice computes: $K_{ab} = A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes M \otimes B_2 \otimes A_2$. Bob computes: $K_{ba} = B_1 \otimes U \otimes B_2 = B_1 \otimes A_1 \otimes M \otimes A_2 \otimes B_2$. By the commutability of the circulant matrix, $K_{ab} = K_{ba}$.

(4) Alice and Bob compute the shared key:

$$K = \left(\sum_{i=1}^{n} a_{1i}, \sum_{i=1}^{n} a_{2i}, \cdots, \sum_{i=1}^{n} a_{ni} \right) \bmod p, \quad a_{ij} \in K_{ab}, 1 \le i, j \le n.$$

An example with small parameter.

Alice and Bob choose $p = 199$ and the public matrix M,

$$M = \begin{pmatrix} 75908 & 263379 & 841480 & 305528 & 181377 \\ 194915 & 62915 & 549784 & 877525 & 578192 \\ 467300 & 907097 & 86372 & 271936 & 176267 \\ 245134 & 578159 & 386596 & 937699 & 196995 \\ 62727 & 321244 & 820495 & 823705 & 615166 \end{pmatrix}.$$

(1) Alice chooses two circulant matrices $A_1, A_2 \in M_5(W)$ and computes U;

$$A_1 = [211034, 686963, 978737, 940353, 370520],$$
$$A_2 = [983661, 534026, 194077, 276808, 138247],$$
$$U = \begin{pmatrix} 276808 & 907097 & 983661 & 983661 & 578192 \\ 276808 & 983661 & 983661 & 983661 & 983661 \\ 276808 & 983661 & 983661 & 983661 & 983661 \\ 75908 & 263379 & 820495 & 75908 & 263379 \\ 276808 & 276808 & 983661 & 983661 & 578192 \end{pmatrix}.$$

(2) Bob chooses two circulant matrices $B_1, B_2 \in M_5(W)$ and computes V;

$$B_1 = [680091, 792838, 334272, 935627, 522570],$$
$$B_2 = [787257, 284933, 18528, 186041, 365280],$$
$$V = \begin{pmatrix} 284933 & 935627 & 787257 & 877525 & 935627 \\ 176267 & 907097 & 284933 & 820495 & 176267 \\ 284933 & 578159 & 787257 & 787257 & 787257 \\ 284933 & 194915 & 935627 & 935627 & 578192 \\ 176267 & 907097 & 284933 & 271936 & 176267 \end{pmatrix}.$$

(3) Alice and Bob's shared matrix is

$$K_{ab} = \begin{pmatrix} 276808 & 983661 & 983661 & 983661 & 983661 \\ 276808 & 983661 & 983661 & 983661 & 983661 \\ 276808 & 907097 & 935627 & 935627 & 578192 \\ 276808 & 935627 & 983661 & 983661 & 935627 \\ 276808 & 935627 & 983661 & 983661 & 935627 \end{pmatrix}.$$

(4) Alice and Bob's shared key is

$$K = (4211452, 4211452, 3633351, 4115384, 4115384) \bmod 199 = (15, 15, 9, 64, 64).$$

Table 7 shows the size of the private and public key matrices under different parameters, as well as the time of key generation, where the elements of the matrix are randomly selected in $\left[0, 10^6\right]$ and $p = 199$.

Table 7. Performance comparison under different parameters.

n	Size of private key B	Size of public key (B)	Key generation s
20	49.83	996.57	0.2066
25	62.29	1557.14	0.4029
30	74.74	2,242.28	0.6872
35	87.20	3051.20	1.1041
40	99.66	3,986.28	1.6526
45	112.11	5,045.14	2.3468

Our tests were run on Intel Core: Intel(R) Core (TM) i5-1155G7@2.50GHz

4. Security analysis

In this section, we evaluate the security of the proposed key exchange protocol.

Definition 4.1. Let $A_1, A_2 \in M_n(W)$ be circulant matrices and $M \in M_n(W)$ be an arbitrary matrix. Suppose that $A_1 \otimes M \otimes A_2 = U$. The two-side digital circulant matrix action problem (MAP) is to find two circulant matrices $A_1, A_2 \in M_n(W)$ such that $A_1 \otimes M \otimes A_2 = U$, given the matrices M, U.

Definition 4.2. Let $A_1, A_2, B_1, B_2 \in M_n(W)$ be circulant matrices and $M \in M_n(W)$ be an arbitrary matrix. Suppose that $A_1 \otimes M \otimes A_2 = U$ and $B_1 \otimes M \otimes B_2 = V$. The computational two-side digital circulant

matrix action problem (CMAP) is to find a matrix $K_{ab} \in M_n(W)$ such that $A_1 \otimes B_1 \otimes M \otimes B_2 \otimes A_2 = K_{ab}$, given the matrices M, U, and V.

Proposition 4.3. An algorithm that solves MAP can be used to solve CMAP.

Proof. Suppose there is an algorithm $\mathcal{A}$ of solving MAP. Then, for M, U, V in definition 4.2, $\mathcal{A}(M, U) = (A_1, A_2)$ such that $A_1 M A_2 = U$.

So, we have

$$A_1 \otimes V \otimes A_2 = A_1 \otimes B_1 \otimes M \otimes B_2 \otimes A_2 = K_{ab}.$$

Proposition 4.4. Solving CMAP is equivalent to finding the matrix K_{ab} from the public information of the protocol.

Proof. Suppose there is an algorithm $\mathcal{A}$ of solving CMAP. Let the public information in the protocol be public matrix M, Alice's public key U, and Bob's public key V. Then,

$$\mathcal{A}(M, U, V) = A_1 \otimes B_1 \otimes M \otimes B_2 \otimes A_2 = K_{ab}.$$

Conversely, suppose there is an algorithm $\mathcal{B}$ which can compute the matrix K_{ab} when the input is the public information in the protocol. Let the instance of CMAP be (M, U, V). Then we can take M as the public matrix, U as Alice's public key, and V as Bob's public key. So, $\mathcal{B}(M, U, V) = K_{ab}$. According to Definition 4.2, this solves the problem of CMAP.

Proposition 4.5. MAP can be reduced to the problem of solving quadratic polynomial systems over the digital semiring.

Proof. Suppose there is an algorithm $\mathcal{A}$ which can solve the systems of quadratic polynomial equations over this semiring. That is,

$$\mathcal{A}((f_1, b_1), (f_2, b_2) \cdots, (f_m, b_m)) = (a_1, \cdots, a_n),$$

where $f_i = f_i(x_1, \cdots, x_n)$ is a quadratic polynomial over this semiring and $a_i \in W$ such that

$$\begin{cases} f_1(a_1, a_2, \cdots, a_n) = b_1, \\ f_2(a_1, a_2, \cdots, a_n) = b_2, \\ \cdots \\ f_m(a_1, a_2, \cdots, a_n) = b_m. \end{cases}$$

Suppose that we are given $U, M \in M_n(W)$, where $U = A_1 M A_2$ for some $A_1, A_2 \in M_n(W)$. Then we can find A_1, A_2 by the algorithm $\mathcal{A}$. Let

$$A_1 = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_n & x_1 & x_2 & \cdots & x_{n-1} \\ x_{n-1} & x_n & x_1 & \cdots & x_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_2 & x_3 & x_4 & \cdots & x_1 \end{pmatrix},$$

and

$$A_2 = \begin{pmatrix} y_1 & y_2 & y_3 & \cdots & y_n \\ y_n & y_1 & y_2 & \cdots & y_{n-1} \\ y_{n-1} & y_n & y_1 & \cdots & y_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_2 & y_3 & y_4 & \cdots & y_1 \end{pmatrix}.$$

By $U = A_1MA_2$, we can obtain a system of quadratic polynomial equations with $2n$ unknowns $x_1, \cdots, x_n, y_1, \cdots, y_n$ and n^2 equations as follows,

$$\begin{cases} g_1(x_1, \cdots, x_n, y_1, \cdots, y_n) = d_1, \\ g_2(x_1, \cdots, x_n, y_1, \cdots, y_n) = d_2, \\ \cdots \\ g_{n^2}(x_1, \cdots, x_n, y_1, \cdots, y_n) = d_{n^2}. \end{cases}$$

Now, we can compute its solution by the algorithm $\mathcal{A}$ since $g_1, \cdots, g_{n^2}$ are the quadratic polynomial equations over the semiring.

Proposition 4.6. The computational complexity of solving the CMAP by enumeration is $O\left(\left(n^2+1\right)t^{n^2}\right)$, where n is the order of the matrix and t is the number of distinct elements in U, V, M.

Proof. K_{ab} is completely dependent on the matrices U, V, and M, that is, K_{ab} is a certain combination of different elements in U, V, and M. If we solve CMAP through an exhaustive attack, we need to enumerate all possible scenarios, which requires $O(t^{n^2})$ operations, where t is the number of different elements in U, V, and M, and n is the order of the matrix. After each operation, we need to determine whether the possible value is equal to K_{ab}, each determination requires $O\left(n^2\right)$ operations, and verifying all possible values requires $O\left(n^2t^{t^{n^2}}\right)$ operations. Therefore, in the worst case, where all combinations need to be verified, $O\left(\left(n^2+1\right)t^{n^2}\right)$ operations are required. Therefore, the computational complexity of solving CMAP through exhaustive search is $O\left(\left(n^2+1\right)t^{n^2}\right)$.

In summary, it is infeasible for an attacker to obtain the shared secret key using exhaustive search methods. The attacker's only option is to acquire the shared matrix K_{ab} by solving the MAP or CMAP. However, the currently known methods for solving MAP involve addressing quadratic polynomial systems over the digital semiring. Theorem 2.4 demonstrates that solving such systems of equations is typically NP-hard.

In the appendix, we explain why the key exchange protocol based on the digital semiring is resistant to Kotov-Ushakov(KU) attacks.

5. Conclusions

This paper introduces a novel semiring structure called the digital semiring and proposes a new key exchange protocol based on it. The shared matrix K_{ab} in this protocol is entirely dependent on the matrices U, V, and M, but this does not compromise the security of the protocol. Solving K_{ab} through U, V, and M is equivalent to solving the CMAP. Proposition 4.6 states that the computational complexity of CMAP is $O((n^2+1)t^{n^2})$. Current methods for solving CMAP involve addressing quadratic polynomial systems over the digital semiring. Theorem 2.4 demonstrates that solving such systems is an NP-hard problem. Additionally, the traditional KU attack cannot be applied within the digital semiring.

This work highlights the application value of the digital semiring in cryptography. This semiring possesses many intriguing properties that are yet to be discovered, presenting ample opportunities for future research. We recommend further exploration of the structure and properties of the digital semiring to uncover its full potential in cryptography and related fields.

The key exchange protocol proposed in this study offers a new primitive for post-quantum cryptography. This not only enriches the theoretical framework of cryptography but also provides new

methods for constructing secure encryption systems. Future work could include the following directions:

(1) In-depth analysis of the algebraic properties of the digital semiring: Investigate its behavior under different operations to identify possible optimizations and enhancements.

(2) Expanding the application scope of the digital semiring: Explore its potential use in other cryptographic problems, such as signature algorithms and zero-knowledge proofs.

(3) Improving efficiency and security of the protocol: Enhance the performance and resistance to attacks by refining algorithms and incorporating new mathematical tools.

(4) Experimental validation and practical implementation: Test the protocol's performance and security in real-world applications to facilitate its practical adoption.

In conclusion, the digital semiring offers new perspectives and tools for cryptographic research, and we anticipate that future studies will further explore its potential, contributing new insights and advancements to the field of cryptography.

Author contributions

Huawei Huang: Methodology, supervision, writing-review & editing; Xin Jiang: writing-original draft, software, validation; Changwen Peng: Writing-review & editing, investigation; Geyang Pan: Software, validation. All authors have read and approved the final version of the manuscript for publication.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work is supported by the Science and Technology Foundation of Guizhou Province (QIANKEHEJICHU-ZK [2021] Ordinary313), the National Key Research and Development Program of China (No.2022YFB2701401), the National Natural Science Foundation of China (No. 62272124, 61462016, U1836205).

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. H. S. Vandiver, Note on a simple type of algebra in which the cancellation 1 aw of addition does not hold, *Bull. Amer. Math. Soc.*, **40** (1934), 914–920. https://doi.org/10.1090/S0002-9904-1934-06003-8

2. A. Yamamura, A functional cryptosystem using a group action, In: *Information Security and Privacy*, Berlin: Springer, 1999. https://doi.org/10.1007/3-540-48970-3_26

3. A. Yamamura, Public-key cryptosystems using the modular group, In: *Public Key Cryptography*, Berlin: Springer, 1998. https://doi.org/10.1007/BFb0054026

4. R. Steinwandt, Loopholes in two public key cryptosystems using the modular group, In: *Public Key Cryptography*, Berlin: Springer, 2001. https://doi.org/10.1007/3-540-44586-2_14

5. D. Kahrobaei, C. Koupparis, V. Shpilrain, Public key exchange using matrices over group rings, *Groups Complex. Crypt.*, **5** (2013), 97–115. https://doi.org/10.1515/gcc-2013-0007

6. M. Eftekhari, *Cryptanalysis of some protocols using matrices over group rings*, In: Progress in Cryptology-AFRICACRYPT 2017, Cham: Springer, 2017. https://doi.org/10.1007/978-3-319-57339-7_13

7. I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography, *Math. Res. Lett.*, **6** (1999), 287–291, https://doi.org/10.4310/MRL.1999.v6.n3.a3

8. K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang, C. Park, *New public-key cryptosystem using Braid groups*, In: *Advances in Cryptology-CRYPTO 2000*, Berlin: Springer, 2000. https://doi.org/10.1007/3-540-44598-6_10

9. I. Anshel, M. Anshel, B. Fisher, D. Goldfeld, New key agreement protocols in Braid group cryptography, In: *Topics in Cryptology-CT-RSA 2001*, Berlin: Springer, 2001. https://doi.org/10.1007/3-540-45353-9_2

10. D. Hofheinz, R. Steinwandt, A practical attack on some braid group based cryptographic primitives, In: *Public Key Cryptography-PKC 2003*, Berlin: Springer, 2003. https://doi.org/10.1007/3-540-36288-6_14

11. D. Sypeyer, B. Sturmfels, Tropical mathematics, *Math. Mag.*, **82** (2009), 163–173, https://doi.org/10.1080/0025570X.2009.11953615

12. D. Grigoriev, V. Shpilrain, Tropical cryptography, *Commun. Algebra*, **42** (2014), 2624–2632. https://doi.org/10.1080/00927872.2013.766827

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

14. M. Kotov, A. Ushakov, Analysis of a key exchange protocol based on tropical matrix algebra, *J. Math. Cryptol.*, **12** (2018), 137–141. https://doi.org/10.1515/jmc-2016-0064

15. D. Rudy, C. Monico, Remarks on a tropical key exchange system, *J. Math. Cryptol.*, **15** (2021), 280–283. https://doi.org/10.1515/jmc-2019-0061

16. S. Isaac, D. Kahrobaei, A closer look at the tropical cryptography, *Int. J. Comput. Math. Co.*, **6** (2021), 137–142. https://doi.org/10.1080/23799927.2020.1862303

17. A. Muanalifah, S. Sergeev, Modifying the tropical version of Stickel's key exchange protocol, *Appl. Math.*, **65** (2022), 727–753. https://doi.org/10.21136/AM.2020.0325-19

18. O. Regev, On lattices, learning with errors, random linear codes, and cryptography, *J. ACM*, **56** (2009), 1–40. https://doi.org/10.1145/1568318.1568324

19. R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, *Deep Space Netw. Progr. Rep.*, **44** (1978), 114–116.

20. J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms, In: *Advances in Cryptology-EUROCRYPT'96*, Berlin: Springer, 1996. https://doi.org/10.1007/3-540-68339-9_4

21. D. I. Nassr, M. Anwar, H. M. Bahig, New public key cryptosystem (First version), Cryptology ePrint Archive, 2021.

22. D. S. Johnson, M. R. Garey, *Computers and intractability: A guide to the theory of NP-completeness*, WH Freeman, 1979.

23. S. A. Cook, The complexity of theorem-proving procedures, In: *Logic, Automata, and Computational Complexity: The Works of Stephen A. Cook*, 1971, 151–158.

24. H. Huang, C. Li, Tropical cryptography based on multiple exponentiation problem of matrices, *Secur. Commun. Netw.*, **2022** (2022), 1024161. https://doi.org/10.1155/2022/1024161

25. H. Huang, C. Li, L. Deng, Public-key cryptography based on tropical circular matrices, *Appl. Sci.*, **12** (2022), 7401. https://doi.org/10.3390/app12157401

26. V. Thiruveni, Elgamal encryption using regular semiring, 2018.

27. S. Nivetha, M. Chandramouleeswaran, Action of a semiring to encrypt asymmetric key elgamal, *J. New Front. Math. Stat.*, **2** (2021), 1–10.

28. G. Robert, Toeplitz and circulant matrices: A review, *Found. Trends Commun.*, **2** (2006), 155–239. https://doi.org/10.1561/0100000006

Appendix: Resist KU attack

The tropical semiring $(a \oplus_1 b = \min(a, b), a \otimes_1 b = a + b)$ has higher computational efficiency, which has attracted many cryptologists' research in recent years. However, there are also many attacks. In particular, the KU attack has a significant impact on two-side tropical matrix action. Next, we will describe the KU attack and explain how our scheme can resist this attack.

KU attack [14]:

Assuming matrices A, B, and U $(= p_1(A) \otimes_1 p_2(B))$ are known, find X and Y such that $U = X \otimes_1 Y$.

(1) suppose $X = \overset{D}{\underset{i=0}{\oplus}} x_i \otimes_1 A^i, Y = \overset{D}{\underset{j=0}{\oplus}} y_j \otimes_1 B^j$;

(2)

$$U = X \otimes_1 Y = \overset{D}{\underset{i=0,j=0}{\oplus_1}} \left(x_i \otimes_1 y_j\right) \otimes_1 A^i \otimes_1 B^j = \overset{D}{\underset{i=0,j=0}{\oplus_1}} \left(x_i \otimes_1 y_j\right) \otimes_1 V^{ij}$$

where $V^{ij} = A^i \otimes_1 B^j$;

(3) From the properties of tropical semiring operations, we can obtain:

$$\min_{i,j} \left(x_i + y_j + T_{kl}^{ij}\right) = 0, T_{kl}^{ij} = V_{kl}^{ij} - U_k,$$

where $T^{ij} = A^i \otimes_1 B^j - U$;

(4) Compute $m_{ij} = \min_{i,j} \left(T_{rs}^{ij}\right), P_{ij} = \left\{(r, s) \mid T_{rs}^{ij} = m_{ij}\right\}$;

(5) Among all minimal covers of Cartesian product $[1,2,\cdots,n]\times[1,2,\cdots,n]$ by P_{ij}, that is, all minimal subsets $\tau\subseteq[0,1,\cdots,D]\times[0,1,\cdots,D]$ such that

$$\underset{(i,j)\in\tau}{\cup}P_{ij}=[1,2,\cdots,n]\times[1,2,\cdots,n]$$

find a cover for which the system $\begin{cases} x_i+y_j=-m_{ij},(i,j)\in\tau \\ x_i+y_j\geq -m_{ij},(i,j)\notin\tau \end{cases}$ is solvable.

We can find that from step (2) to step (3):

$$U=\overset{D}{\underset{i=0,j=0}{\oplus_1}}x_i\otimes_1 y_j\otimes_1 V^{ij}\rightleftarrows 0=\overset{D}{\underset{i=0,j=0}{\oplus_1}}\left(x_i\otimes_1 y_j\right)\otimes_1 V^{ij}-U\rightleftarrows\min_{i,j}\left(x_i+y_j+T_{kl}^{ij}\right)=0,T_{kl}^{ij}=V_{kl}^{ij}-U_{kl}\cdot(\diamond)$$

Now, regarding the new semiring in this article, we analyze whether similar methods are feasible. Since any circulant matrix can be linearly represented by a basic circulant matrix, that is,

$$A=a_0\otimes I\oplus a_1\otimes P\oplus a_2\otimes P^2\oplus\cdots\oplus a_{n-1}\otimes P^{n-1},$$

where

$$P=\begin{bmatrix} 0 & 0 & \cdots & 0 & \infty \\ \infty & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \infty & 0 \end{bmatrix},$$

0 is the additive identity element, and ∞ is the multiplicative identity element.

In our protocol,

(a) let $A_1=\bigoplus_{i=0}^{n-1}a_i\otimes P^i, A_2=\bigoplus_{j=0}^{n-1}b_j\otimes P^j$, such that $U=A_1\otimes M\otimes A_2$;

(b) $U=A_1\otimes M\otimes A_2=\bigoplus_{i=0,j=0}^{n-1}(a_i\otimes b_j)\otimes P^i\otimes M\otimes P^j=\bigoplus_{i=0,j=0}^{n-1}(a_i\otimes b_j)\otimes V^{ij}$ where $V^{ij}=P^i\otimes M\otimes P^j$.

However, due to the difference of operation between digital semiring and tropical semirings, the implication relationship similar to $(\diamond)$ cannot be established on the digital semiring. Therefore, our protocol can resist the KU attack.

AIMS Press

© 2024 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)