arXiv:2505.00664v1 [math.AC] 1 May 2025

Key exchange protocol based on circulant matrix action over congruence-simple semiring

Otero Sanchez, Alvaro*[1]

[1]Department of Mathematics, University of Almería 04120 , Almería, Spain

May 5, 2025

Abstract

We present a new key exchange protocol based on circulant matrices acting on matrices over a congruence-simple semiring. We describe how to compute matrices with the necessary properties for the implementation of the protocol. Additionally, we provide an analysis of its computational cost and its security against known attacks.

1 Introduction

The foundational paper by [1] is considered the beginning of modern cryptography. In its original formulation, a cyclic group $\mathbb{Z}_n$ was used as the algebraic setting for the key exchange protocol. Later, a similar protocol based on elliptic curves was independently proposed by [3] and [5].

These protocols have become the standard in cryptography, and their use is widely spread. However, in [13], Shor presented a quantum algorithm capable of solving the discrete logarithm problem in both algebraic settings. Since the security of these cryptographic protocols relies on the hardness of this problem, a sufficiently large quantum computer would be able to break most of today's key exchange protocols. As a result, the scientific community has initiated the search for new post-quantum cryptographic protocols, that is, protocols secure against quantum attacks.

One such proposal was made in [4], where the authors introduced the use of abelian semigroups. The security of this protocol relies on the following problem:

Problem 1.1. *Let $(G, \cdot)$ be a semigroup, S a set, and let $\varphi : G \times S \to S$ be an action of G on S, i.e., φ satisfies $\varphi(g \cdot h, s) = \varphi(g, \varphi(h, s))$. The Semigroup Action Problem states that, given $x \in S$ and $y \in \varphi(G, x)$, find $g \in G$ such that $\varphi(g, x) = y$.*

*Autor de correspondencia: aos073@ual.es

In their work, the authors define a general framework for a new key exchange protocol using semimodules, which are analogous to modules but where the acting ring is replaced by a semiring, and the underlying structure is a commutative monoid. As an explicit example, they use congruence-simple semirings. In this setting, polynomials over the center of the semiring act on matrices over the semiring via evaluation at two fixed matrices and multiplication. They present an example using a semiring with six elements.

However, in [14], the authors perform a cryptanalysis of this specific example by solving a system of equations derived from the operation tables of the semiring. The viability of the protocol using other semirings remained an open question until [11], where the authors developed a general attack on the protocol for any congruence-simple semiring, assuming only a bound on the degree of the polynomials used in the protocol's definition.

In this paper, we present a new key exchange protocol based on congruence-simple semirings. For this purpose, we consider exponentiation as an action of $\mathbb{N}$ on matrices over the semiring. This key exchange can be seen as a particular instance of the protocol in [4], but with a different action. Additionally, we analyze its resistance to known attacks and evaluate its computational cost.

2 Mathematical setting

First, we will introduce the concept of semigroup

Definition 2.1: A *semigroup* is a set S equipped with an internal binary operation $\cdot : S \times S \to S$ such that the operation is associative; that is, for every $a, b, c \in S$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

We say that S is *commutative* if, in addition, the operation satisfies $a \cdot b = b \cdot a$ for all $a, b \in S$.

Now, we will recall the well know circulant matrix

Definition 2.2: Let R be a ring. A matrix $C \in \mathrm{Mat_n(R)}$ is called circulant if there are $c_0, c_1, \cdots, c_{n-1} \in R$ such that

$$C = \begin{pmatrix} c_0 & c_{n-1} & c_{n-2} & \cdots & c_1 \\ c_1 & c_0 & c_{n-1} & \cdots & c_2 \\ c_2 & c_1 & c_0 & \cdots & c_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{pmatrix}$$

We will denote C as $C = Circ(c_0, \cdots, c_{n-1})$

A famous result regarding the structure of circulant matrix is

Theorem 2.3. *The set $Circ_n(R)$ of ciruclar matrix of $n \times n$ over R form a commutative subring of* $\mathrm{Mat_n(R)}$.

Thanks to this condition, we can define a new action

Theorem 2.4. *Let S be a semigroup and $T \subset S$ a set of conmmutative elements i.e.*

$$ab = ba \forall a, b \in T \tag{1}$$

Then

$$\begin{aligned} Circ_n(\mathbb{N}) \times T^n &\longrightarrow T^n \\ (C, (v_i)_{i=0}^{n-1}) &\longmapsto (\prod v_j^{a_{j-i}})_{i=0}^{n-1} \end{aligned}$$

is an action of the multiplicative semigroup $Circ_n(\mathbb{N})$ over T^n. It will denoted as Cv

Proof. It is clear that if $C \in Circ_n(\mathbb{N}), v \in T^n$ then $Cv \in T^n$, as the elements of Cv are product of elements that commute among each other. We have to prove $A(Bv) = (AB)v$ for all $A, B \in Circ_n(\mathbb{N}), v \in T^n$.

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

$$b = \begin{pmatrix} b_0 & b_{n-1} & b_{n-2} & \cdots & b_1 \\ b_1 & b_0 & b_{n-1} & \cdots & b_2 \\ b_2 & b_1 & b_0 & \cdots & b_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & b_{n-2} & b_{n-3} & \cdots & b_0 \end{pmatrix}$$

then

$$AB = \begin{pmatrix} \sum_{i=0}^{n-1} a_i b_{n-i} & \sum_{i=0}^{n-1} a_i b_{n-1-i} & \sum_{i=0}^{n-1} a_i b_{n-2-i} & \cdots & \sum_{i=0}^{n-1} a_i b_{n+1-i} \\ \sum_{i=0}^{n-1} a_i b_{n+1-i} & \sum_{i=0}^{n-1} a_i b_{n-i} & \sum_{i=0}^{n-1} a_i b_{n-1-i} & \cdots & \sum_{i=0}^{n-1} a_i b_{n+2-i} \\ \sum_{i=0}^{n-1} a_i b_{n+2-i} & \sum_{i=0}^{n-1} a_i b_{n+1-i} & \sum_{i=0}^{n-1} a_i b_{n-i} & \cdots & \sum_{i=0}^{n-1} a_i b_{n+3-i} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} a_i b_{n-1-i} & \sum_{i=0}^{n-1} a_i b_{n-2-i} & \sum_{i=0}^{n-1} a_i b_{n-3-i} & \cdots & \sum_{i=0}^{n-1} a_i b_{n-i} \end{pmatrix}$$

where all subindex are taking mod n. De donde, $AB = Cir(c_0, \cdots, c_{n-1})$ con $c_k = \sum_{i=0}^{n-1} a_i b_{k-i}$. Now, we have that

$$\begin{aligned} A(Bv) =& A\left(\prod_{j=0}^{n-1} v_j^{b_{-i+j}}\right)_{i=0}^{n-1} = \left(\prod_{i=0}^{n-1}\left(\prod_{j=0}^{n-1} v_j^{b_{-i+j}}\right)^{a_{i-k}}\right)_{k=0}^{n-1} = \left(\prod_{i=0}^{n-1}\prod_{j=0}^{n-1} v_j^{b_{-i+j}a_{i-k}}\right)_{k=0}^{n-1} \\ &= \left(\prod_{j=0}^{n-1}\prod_{i=0}^{n-1} v_j^{b_{-i+j}a_{i-k}}\right)_{k=0}^{n-1} = \left(\prod_{j=0}^{n-1} v_j^{\sum_{i=0}^{n-1} b_{-i+j}a_{i-k}}\right)_{k=0}^{n-1} = \\ &= \left(\prod_{j=0}^{n-1} v_j^{\sum_{i=0}^{n-1} a_i b_{j-k-i}}\right)_{k=0}^{n-1} = \left(\prod_{j=0}^{n-1} v_j^{c_{k-j}}\right)_{k=0}^{n-1} = (AB)v \end{aligned}$$

□

The previous action is a particular instance of [4], where we consider the $\mathbb{N}-$*module* M generated by T with $\mathbb{N}-$action $n \cdot t = t^n$ for all $n \in \mathbb{N}$, $t \in M$. We will use as T a commutative subset of matrix over semirings.

Definition 2.5: A set R with two internal operations $+$ and $\cdot$ is called a semiring if both operations are associative and verify that $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for every $a, b, c \in R$. We say that S is additively (resp. multiplicatively) commutative in case addition (resp. multiplication) satisfies commutativity. We say that R is commutative in case both operations satisfy commutativity.

The study of semiring for cryptographyc purpouse was starded by [4], which focus on concruence simple semiring for cryptographyc applications

Definition 2.6: A congruence relation on a semiring R is an equivalence relation $\sim$ such that

$$a \sim b \Rightarrow \begin{cases} a + c & \sim & b + c \\ c + a & \sim & c + b \\ a \cdot c & \sim & b \cdot c \\ c \cdot a & \sim & c \cdot b \end{cases}$$

for every $a, b, c \in R$. A semiring R that admits no congruence relations other than the trivial ones, id_R and $R \times R$, is said to be congruence-simple.

The following result, first appears in [6], establishes a classification of congruence simple semiring

Theorem 2.7. *[6, Theorem 4.1] Let R be a finite, additively commutative, congruence-simple semiring. Then one of the following holds:*

1. $|R| \leq 2$.
2. $R \cong \mathrm{Mat_n}(\mathbb{F_q})$*, for some finite field* $\mathbb{F}_q$ *and some* $n \geq 1$.
3. *R is a zero multiplication ring of prime order.*
4. *R is additively idempotent, i.e.,* $x + x = x$ *for every* $x \in R$.
5. *R contains an absorbing element* ∞*, i.e.* $x \cdot \infty = \infty \cdot x = \infty$ *for every* $x \in R$ *and* $R + R = \{\infty\}$.

To obtain a commutative set, we will use the following result from [6]

Definition 2.8: Let R be a semiring with center

$$C_R = \{r \in R \mid rs = sr \text{ for all } s \in R\},$$

and let $A \in \mathrm{Mat}_{n\times n}(R)$ be a matrix. Define $C_R[A]$ to be the set of polynomials in A with coefficients in C_R.

Lemma 2.9: Let R, C_R, and A be as above. The set $C_R[A]$ is a commutative subsemiring of the matrix semiring $\mathrm{Mat}_{n\times n}(R)$.

As a result, we will use the multiplicative semigroup of matrix over a semiring, and as a commutative subset we will use elements of $C_R[A]$, with $A \in Mat_n(R)$ with $n \in \mathbb{N}$. In addition, in [6] it is also proven that

Lemma 2.10: Let R be an additively commutative semiring with 1 and 0, and let $\sim$ be a congruence relation on $\mathrm{Mat}_n(R)$. Then there exists a congruence relation $\sim_0$ on R such that

$$A \sim B \in \mathrm{Mat}_n(R) \quad \Leftrightarrow \quad a_{ij} \sim_0 b_{ij}, \quad \forall 0 \leq i, j \leq n.$$

So we can ensure that the new semiring will be also simple. Under this circunstances, we can introduce the following key exchange protocol

Protocol 2.11. *Alice and Bob agree on a simple semiring R, a matrix $M \in \mathrm{Mat_n(R)}$ with large order, and $v = (M_i)_{i=0}^{n-1} \in C_R[M]^n$ and make them public.*

1. *Alice chose $A \in Circ_n(\mathbb{N})$ and makes public $pk_1 = Av$*
2. *Bob chose $B \in Circ_n(\mathbb{N})$ and makes public $pk_2 = Bv$*
3. *Alice computes Apk_2 and Bob computes Bpk_1*

The common key is

$$Apk_2 = A(Bv) = (AB)v = (BA)v = B(Av) = Bpk_1$$

For computational purposes, Alice and Bob can take matrix A, B with $a_i, b_i \leq m$ been $m \in \mathbb{N}$ an upper bound computationally assumable by both parties.

The security of the protocol relies on the following problem

Problem 2.12. *Let R a simple semiring and $M \in \mathrm{Mat_n(R)}$. Given $v, Av, Bv \in C_R[M]^n$ with $A, B \in Circ_n(\mathbb{N})$, compute ABv.*

An easier problem that implies solve the previous one is

Problem 2.13. *Let R a simple semiring and $M \in \mathrm{Mat_n(R)}$. Given $v, Av \in C_R[M]^n$ with $A \in Circ_n(\mathbb{N})$, find $C \in Circ_n(\mathbb{N})$ such that $Av = Cv$.*

To avoid a brute force attack, we need to ensure that the set $C[A]$ is large enought. For this, we need the following definition

Definition 2.14: Let $a = \{a_k\}_{k \in \mathbb{N}}$ be a sequence in a finite set such that

$$a_n = a_m \Rightarrow a_{n+1} = a_{m+1}.$$

The *order* $\mathrm{ord}(a)$ of a is the least positive integer m for which there exists $k < m$ with $a_k = a_m$. The *preperiod* $\mathrm{pr}(a)$ of a is the largest non-negative integer m such that for all $k > m$ we have $a_k \neq a_m$. The *period* $\mathrm{per}(a)$ of a is the least positive integer m for which there exists an integer N such that

$$a_{m+k} = a_k \quad \text{for all } k > N.$$

If g is an element of a semigroup, then we set

$$\mathrm{ord}(g) = \mathrm{ord}(\{g^n\}_{n \in \mathbb{N}}), \quad \mathrm{per}(g) = \mathrm{per}(\{g^n\}_{n \in \mathbb{N}}), \quad \mathrm{pr}(g) = \mathrm{pr}(\{g^n\}_{n \in \mathbb{N}}).$$

Now, to give some bounds, we need the landau function.

$$g(n) = \max\{\text{ord}(\sigma) \mid \sigma \in S_n\} = \max\{\text{lcm}\{a_1, a_2, \ldots, a_m\} \mid a_i > 0, a_1 + \cdots + a_m = n\}.$$

Which, in [9] it is proven that

$$n\ln(n) \leq \ln(g(n)) \leq \sqrt{n}\ln(n)\left(1 + \frac{\ln\ln(n)}{2\ln(n)}\right)$$

finally, in [4] it is established that

Theorem 2.15. *Let $n \in \mathbb{N}$ and R be a semiring with 0 and 1, and center C. Then there is an $n \times n$ matrix M with entries in R such that the order of M is larger than $g(n)$. In particular, the size of $C[M]$ is larger than $g(n)$ as well.*

In order to obtain suitable matrix, we will use the following result

Lemma 2.16: Let $P, A \in Mat_{n\times n}(R)$ with P inversible. Then $ord(A) = ord(PAP^{-1})$.

Proof. We have that $PAP^{-1} \cdot PAP^{-1} = PA^2P^{-1}$. Hence, $(PAP^{-1})^n = PA^nP^{-1}$. Moreover,

$$(PAP^{-1})^n = (PAP^{-1})^k \iff PA^nP^{-1} = PA^kP^{-1} \iff A^n = A^k.$$

In the last equivalence, we multiplied both sides by P and by P^{-1}. □

To proceed, we need to understand the invertible matrices over our semiring R. To that end, we first introduce the notions of the sum and the direct sum of semigroups.

Definition 2.17: Let $(R, +)$ be a finite semigroup, and let $A, B \leq R$ sub semigroups. The sum of semigroups A, B is defined as

$$A + B := \{a + b : a \in A, b \in B\}$$

Definition 2.18: Let $(R, +)$ be a semigroup, and let $A, B \leq R$ be two subsemigroups such that $A \cap B = \emptyset$ and for all $c \in A + B$, there exist unique elements $a \in A$ and $b \in B$ such that $a + b = c$. Then the sum $A + B$ is said to be a direct sum, and it is denoted by $A \oplus B$.

Due to direct sum, we can define the concept of irreducible and reducible semigroup

Definition 2.19: Let $(R, +)$ be a finite semigroup. We say that R is reducible if there exist proper subsemigroups $A, B \lneq R$ such that $R = A \oplus B$. Otherwise, we say that R is irreducible.

Now we will present a sufficient condition for irreducibility of a semigroup wiht neutral element. For this, we will use the following easy proof fact

Lemma 2.20: Let $(R, +)$ a finite reducible semigroup with cardinal n, with $R = A \oplus B$. Entonces $1 < |A|, |B| < n$.

The following theorem is a new result with a suficient condition of irreducibility of a finite semigroup

Theorem 2.21. *Let $(R, +)$ be a finite semigroup. If there exists an element $x \in R$ such that*

$$z + y = x \Longrightarrow z = x \text{ ó } .y = x$$

$$x + y = y + x = x \; \forall y \in R$$

Then R is irreducible.

Proof. The proof proceeds by contradiction. Suppose there exist subsemigroups A, B such that $A \oplus B = R$, and let x be the element mentioned earlier. Then, since $R = A \oplus B$, there exist $(a, b) \in A \times B$ such that $a + b = x$. By the first property, this implies that either $a = x$ or $b = x$. Without loss of generality, assume that $x \in A$.

By the previous lemma, we have $|B| \geq 2$, so there exist distinct elements $d, b \in B$ with $d \neq b$. However, this implies $x + d = x + b = x$, which contradicts the uniqueness of the representation. Hence, the assumption must be false. □

Example 2.1: In [4] it is presented a semiring with 20 elements for its cryptographyc applications.

$+$	0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	1
0	0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	1
a	a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	1
b	b	b	b	c	e	e	f	g	h	i	k	k	l	m	n	o	p	q	r	1
c	c	c	c	c	f	f	f	h	h	i	l	l	l	1	n	p	p	q	r	1
d	d	d	e	f	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	1
e	e	e	e	f	e	e	f	g	h	i	k	k	l	m	n	o	p	q	r	1
f	f	f	f	f	f	f	f	h	h	i	l	l	l	1	n	p	p	q	r	1
g	g	g	g	h	g	g	h	g	h	i	m	m	1	m	n	o	p	q	r	1
h	h	h	h	h	h	h	h	h	h	i	1	1	1	1	n	p	p	q	r	1
i	i	i	i	i	i	i	i	i	i	i	n	n	n	n	n	q	q	q	r	n
j	j	j	k	l	j	k	l	m	1	n	j	k	l	m	n	o	p	q	r	1
k	k	k	k	l	k	k	l	m	1	n	k	k	l	m	n	o	p	q	r	1
l	l	l	l	l	l	l	l	1	1	n	l	l	l	1	n	p	p	q	r	1
m	m	m	m	1	m	m	1	m	1	n	m	m	1	m	n	o	p	q	r	1
n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	q	q	q	r	n
o	o	o	o	p	o	o	p	o	p	q	o	o	p	o	q	o	p	q	r	p
p	p	p	p	p	p	p	p	p	p	q	p	p	p	p	q	p	p	q	r	p
q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	q	r	q
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
1	1	1	1	1	1	1	1	1	1	n	1	1	1	1	n	p	p	q	r	1

$\cdot$	0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	0	0	0	0	0	0	0	0	0	0	a	a	a	a	a	b	b	b	c	a
b	0	0	0	0	a	a	a	b	b	c	a	a	a	b	c	b	b	c	c	b
c	0	a	b	c	a	b	c	b	c	c	a	b	c	b	c	b	c	c	c	c
d	0	0	0	0	0	0	0	0	0	0	d	d	d	d	d	g	g	g	i	d
e	0	0	0	0	a	a	a	b	b	c	d	d	d	e	f	g	g	h	i	e
f	0	a	b	c	a	b	c	b	c	c	d	e	f	e	f	g	h	h	i	f
g	0	0	0	0	d	d	d	g	g	i	d	d	d	g	i	g	g	i	i	g
h	0	a	b	c	d	e	f	g	h	i	d	e	f	g	i	g	h	i	i	h
i	0	d	g	i	d	g	i	g	i	i	d	g	i	g	i	g	i	i	i	i
j	0	0	0	0	0	0	0	0	0	0	j	j	j	j	j	o	o	o	r	j
k	0	0	0	0	a	a	a	b	b	c	j	j	j	k	l	o	o	p	r	k
l	0	a	b	c	a	b	c	b	c	c	j	k	l	k	l	o	p	p	r	l
m	0	0	0	0	d	d	d	g	g	i	j	j	j	m	n	o	o	q	r	m
n	0	d	g	i	d	g	i	g	i	i	j	m	n	m	n	o	q	q	r	n
o	0	0	0	0	j	j	j	o	o	r	j	j	j	o	r	o	o	r	r	o
p	0	a	b	c	j	k	l	o	p	r	j	k	l	o	r	o	p	r	r	p
q	0	d	g	i	j	m	n	o	q	r	j	m	n	o	r	o	q	r	r	q
r	0	j	o	r	j	o	r	o	r	r	j	o	r	o	r	o	r	r	r	r
1	0	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	1

This semiring is irreducible as r satisfy the conditions of the previous lemma

Definition 2.22: Let R be a semiring, and let $A \in \mathrm{Mat}_{n\times n}(R)$. We say that A is a generalized permutation matrix if each row and each column contains exactly one nonzero entry, and this entry is invertible.

In the article [10], an interesting relationship is established between the additive semigroup structure of a semiring and the invertibility of matrices with entries in that semiring.

Theorem 2.23. *Let $(R, +, \cdot)$ be a finite semiring such that $(R, +)$ is irreducible, and let $A \in \mathrm{Mat}_{n\times n}(R)$. Then A is invertible if and only if A is a generalized permutation matrix.*

Now, we will see how to obtain the matrices we need. First, we take a congruence-free semiring R and a natural number n. We choose elements $a_i \in \mathbb{N}$, for $i = 1, \ldots, k$, such that LCM = $\mathrm{lcm}(a_1, \ldots, a_k)$ is sufficiently large, with the constraint that $\sum_{i=1}^{n} a_i \leq n$. Then, we construct the matrix associated with this partition as in Theorem 2.15. This matrix will be of the form:

$$\left(\begin{array}{c|c|c|c|c} T_{a_1} & 0 & \cdots & 0 & 0 \\ \hline 0 & T_{a_2} & \cdots & 0 & 0 \\ \hline \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline 0 & 0 & \cdots & T_{a_r} & 0 \\ \hline 0 & 0 & \cdots & 0 & Id_s \end{array}\right)$$

Next, we proceed to modify the elements above the block diagonal, obtaining a matrix of the form:

$$M = \left(\begin{array}{c|c|c|c|c|c} T_{a_1} & A_{1,2} & A_{1,3} & \cdots & A_{1,r} & A_{1,r+1} \\ \hline 0 & T_{a_2} & A_{2,2} & \cdots & A_{2,r} & A_{2,r+1} \\ \hline 0 & 0 & T_{a_3} & \cdots & A_{2,r} & A_{2,r+1} \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline 0 & 0 & 0 & \cdots & T_{a_r} & A_{r,r+1} \\ \hline 0 & 0 & 0 & \cdots & 0 & Id_s \end{array}\right)$$

Where the matrices $A_{i,j} \in Mat_{a_i \times a_j}(R)$ are rectangular matrices with entries in the semiring R. Since the diagonal and the zero blocks below it remain unchanged, the powers of this matrix will be of the form:

$$M^s = \left(\begin{array}{c|c|c|c|c|c} T^s_{a_1} & B_{1,2} & B_{1,3} & \cdots & B_{1,r} & B_{1,r+1} \\ \hline 0 & T^s_{a_2} & B_{2,2} & \cdots & B_{2,r} & B_{2,r+1} \\ \hline 0 & 0 & T^s_{a_3} & \cdots & B_{2,r} & B_{2,r+1} \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \hline 0 & 0 & 0 & \cdots & T^s_{a_r} & B_{r,r+1} \\ \hline 0 & 0 & 0 & \cdots & 0 & Id_s \end{array}\right)$$

with $B_{i,j} \in \mathrm{Mat}_{a_i \times a_j}(R)$.

By previous result, the unique inversible matrix are generalized permutation matrix. So we can change rows and collumns of a matrix to make more difficult to calculate its powers. As this changes are in biyection with S_n, there are $n!$ possible movements. For n large enough, an attack of brute force to invert this process is not computationaly feasible.

Example 2.2: We will take the semiring of 20 elements introduced in [4], and let $n = 6$. We take the partition $[2, 3]$. Then, $\mathrm{lcm}(2, 3) = 6$, and we obtain the block matrix:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

In this matrix, we modify the elements above the diagonal randomly, obtaining

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & r & b & l \\ 0 & 0 & 0 & 1 & 0 & e \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Now, we conjugate this matrix by a generalized permutation matrix. Upon performing the calculations, we obtain

Output

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \mathrm{e} \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & \mathrm{r} & 0 & \mathrm{b} & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Generalized permutation matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example 2.3: Now, we will show an example with at least 280 distinct powers and of size 20×20. To do this, it is enough to notice that the set $[8, 5, 7]$ satisfies that its sum is 20 and they are pairwise coprime, so their least common multiple is $8 \cdot 5 \cdot 7 = 280$. The matrix resulting from this partition would be:

$$\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

In this matrix, we modify the elements above the diagonal randomly, obtaining

$$\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & f & k & r & 0 & c & g & f & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & o & 0 & p & 0 & h & 0 & g & 0 & 0 & 0 & 0 & e \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & m & 0 & g & b & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & l & l & j & b & 0 & 0 & 0 & p & 0 & 0 & q & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & k & 0 & o & 0 & 0 & i & 0 & 0 & 0 & n & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & j & 0 & 0 & k & b & 0 & 0 & p & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & d & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & q & g & 0 & p & d & d \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & o & b & 1 & 0 & r & 0 & l \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & c & 0 & o & m & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & o & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Now, we conjugate this matrix by a generalized permutation matrix. Upon performing the calculations, we obtain

Output

$$\begin{pmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & d & a & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
n & 0 & k & 0 & 0 & i & 1 & 0 & 0 & 0 & 0 & 0 & 0 & o & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
p & 1 & 0 & 0 & 0 & k & 0 & 0 & 0 & 0 & 0 & 0 & b & j & 0 & 0 & 0 & 0 & 0 & 0 \\
f & 0 & 0 & 0 & 0 & r & 0 & 0 & 0 & 1 & f & k & 0 & 0 & 0 & 0 & 0 & g & 0 & c \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & b & 0 & 1 & m & 0 & g & 0 \\
0 & 0 & 0 & e & 0 & g & 0 & 0 & 1 & 0 & h & 0 & 0 & 0 & 0 & 0 & o & 0 & p & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & o & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
m & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & c & 0 & 0 & 0 & 0 & o & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
q & 0 & l & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p & b & 0 & 0 & l & 0 & j & 0 \\
d & 0 & 1 & d & 0 & q & 0 & 0 & 0 & 0 & 0 & 0 & g & 0 & 0 & 0 & 0 & p & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & l & 0 & b & 0 & 0 & 0 & 0 & 0 & o & 1 & 1 & 0 & 0 & 0 & r & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}$$

Generalized permutation matrix

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{pmatrix}$$

3 Key exchange protocol and its security

First, we will see the computational cost of the key exchange Coste del set up

Theorem 3.1. *La matriz $M \in Mat_m(R)$, tomamos como cota para los polynomios $h \in \mathbb{N}$, y n elementos de la base. El coste del set up para el protocolo es a lo sumo $O(nH)$ operaciones matriciales, o $O(nhm^3)$ operaciones en R*

Proof. Para cada elemento de la base, tenemos que calcular a lo sumo h potencias, y dado que cada una se puede realizar con una multiplicacion de matrices de orden m, tenemos un coste de $O(2log_2(h)m^3)$, tras eso, debemos realizar la suma, teniendo a lo sumo H matrices que sumar, obteniendo $O(2log_2(h)m^3 + 2log_2(h)) = O(2log_2(h)m^3)$ operaciones en R. Puesto a que hay n elementos en la base, el coste total es de $O(n2log_2(h)m^3)$ □

Coste del algoritmo post set up

Theorem 3.2. *Si $A \in Circ_n([0,k]$, entonces el coste de calcular $A(M_i)_{i=1}^n$ es $O(n(2log_2k+n)m^3)$ operaciones en R*

Proof. Cada producto o potencia tiene coste m^3. Tenemos que calcular potencias hasta k, lo cual tiene un coste de $O(2log_2k)$ potencias, dando lugar a $O(2log_2km^3$ en R, tras lo cual hay que multiplicar todas las matrices, por lo que añadimos $O(nm^3)$ operaciones en R. Hay que repetir esto n veces, obteniendo $O(n(2log_2k + n)m^3)$ operaciones en R □

Now, we will see the security of the previous protocol against known attacks.

3.1 Brute force and random attack

An attacker could try a brute-force or random attack against the protocol. If m is an upper bound to the coefficient of the circulant matrix, an attacker must try m^n different matrix in a brute force attack. To avoid this, it is necessary that m is large enough so m^n is unfeasseble.

However, this is not sufficient, as if the set $Pkey = \{C \in Circ_n(\mathbb{N}); Cv = Av\}$ is too large, the brute force or random attack could find one instance with ease. Computational experiments shows that for matrix of form 2.3 that a random attack is not effective against it. In addition, we present a result that ensure us that under certain conditions, our private key is unique.

Theorem 3.3. *If $n = 1$, and $A = a_1 \leq pord(M_1) - 1$, then the solution of $Xv = Av$ is only $X = A$*

Theorem 3.4. *Let $n \in \mathbb{N}$. Let $v = \{M^{b_i}\}_{i=1}^n$ such that $B = Cir[b_1, \cdots, b_n]$ with $det(B) \neq 0$, and A such that $\sum_i a_i b_{i+k} \leq pord(M) - 1 \forall k = 0 \cdots, n-1$, then the solution of $Xv = Av$ is only $X = A$*

3.2 Pohlig-Hellman type attacks

First, we recall the following well-known result:

Theorem 3.5. *Let $n \in \mathbb{N}$, then $U(Mat_n(\mathbb{N}))$ are the permutation matrices.*

As a corollary, we have:

Theorem 3.6. *Let $n \in \mathbb{N}$, then $U(Circ_n(\mathbb{N}))$ are the permutation matrices.*

As indicated in [12], Shanks' baby-step-giant-step method attacks as well as a Pollard-rho type attack require the existence of a large number of inverses to be efficient methods. Given the reduced number of invertible elements in our semigroup, these attacks would not be efficient.

For the Pohlig-Hellman reduction in [12], the fact that the semigroup is finite is exploited, and an element $m \in S$ is chosen in such a way that solving the problem on mS becomes easier, thus obtaining the original solution. In our case, the semigroup $\mathrm{Circ}_n(\mathbb{N})$ is infinite, and the applicability on computers arises by bounding the coefficients by a positive natural number m. Therefore, if an attacker takes $C \in \mathrm{Circ}_n([0, h])$ and tries to perform the reduction, they will face solving the problem on $\mathrm{Circ}_n([0, th])$, where they effectively have not reduced the number of possible candidates to find the solution. Hence, we do not see how this could provide an advantage for the attacker.

3.3 O-L attack

In [11], the authors cryptoanalysis the original key exchange protocol presented in [4]. To do so, given $A, B, M, p(A)Mq(B) \in \mathrm{Mat_n(R)}$ with $p(x), q(x) \in C_R[X]$ they compute a three non commuting variable polynomial $F[X, Y, Z] \in C_R[X, Y, Z]$ such that $F[A, M, B] = p(A)Mq(B)$ and that, for all $h(x), l(x) \in C_R[X]$ $F[A, h(A)Ml(B), B] = h(A)p(A)Mq(B)l(B)$.

In our case, an attacker may use this algorithm to find a $p_i(x) \in C_r[x]$ such that $p_i(M) = M_i$. However, this does not provide information on the shared key, neither of the private keys. If the attacker uses this algorithm to find $P_i^A[x_0, \cdots, x_{n-1}] \in C_R[x_0, \cdots, x_{n-1}]$ polynomial in n non commuting variables such that $(P_i^A(v))_{i=0}^{n-1} = Av$, this does not assert that $(P_i^A(Bv))_{i=0}^{n-1} = ABv$ as in the original case, identity that is false in general.

3.4 Quantum attack

In [13], a quantum algorithm for computing discrete logarithms over abelian groups is introduced. Furthermore, in [15], the authors present a generalization of this algorithm that can compute discrete logarithms over semigroups.

In our case, if the commutator set is chosen as powers of a matrix M, the aforementioned algorithm would yield a system of linear Diophantine equations, which could be solved to recover the private key.

To prevent such an attack, the commutator set should instead consist of polynomials in M, avoiding the use of monoids. Under these circumstances, the authors are not aware of any method to adapt the existing algorithm to compromise the security of the protocol. Moreover, knowledge of the order or pre-order of M does not appear to impact the protocol's security.

4 Conclusion

In this work, we have successfully developed a new key exchange protocol based on the action of circulant matrices on matrices over a congruence-simple semiring. Throughout the study, we effectively addressed the explicit construction of matrices with the required algebraic properties to ensure the correct and secure functioning of the protocol. This involved a careful exploration of the underlying mathematical structures, ensuring that the elements used satisfied the necessary conditions to maintain the system's security.

Furthermore, we conducted a detailed analysis of the computational cost associated with each stage of the protocol, allowing us to assess its practical feasibility compared to existing approaches. Known attack were also examined, and it was shown that the protocol exhibits strong resistance to these attacks.

References

[1] W. Diffie, M. E. Hellman. New directions in cryptography, *IEEE Trans. Inf. Theory* **22** (1976) 644-654.

[2] R. El Bashir, J. Hurt, A. Jančařík, T. Kepka. Simple commutative semirings. *J. Algebra* **236** (2001) 277-306.

[3] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.* 48 (1987) 203-209.

[4] G. Maze, C. Monico, J. Rosenthal, Public key cryptography based on semigroup actions, *Adv. Math. Commun.,* **1** (2007) 489-507.

[5] V.S. Miller. (1986). Use of Elliptic Curves in Cryptography n: Williams, H.C. (eds) Advances in Cryptology - CRYPTO ' 85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg, 417-426.

[6] C. Monico, On finite congruence-simple semirings, *J. Algebra* **271** (2004) 846-854.

[7] R. Steinwandt, A. Suárez. Cryptanalysis of a 2-party key establishment based on a semigroup action problem, *Adv. Math. Commun.* **5** (2011) 87-92.

[8] J. Zumbrägel, Classification of finite congruence-simple semirings with zero, *J. Algebra Appll.* **7** (2008) 363-377.

[9] J.-P. Massias, Majoration explicite de l'ordre maximum d'un élément du groupe symétrique, *Ann. Fac. Sci. Toulouse Math. (5)* **6** (1985), 269–281.

[10] A. Kendziorra, S.E. Schmidt, and J. Zumbrägel, Invertible Matrices over Finite Additively Idempotent Semirings, *Semigroup Forum* **86** (2013) 525–536, https://doi.org/10.1007/s00233-012-9427-x.

[11] A. Otero Sánchez, J. A. López Ramos. Cryptanalysis of a key exchange protocol based on a congruence-simple semiring action, *J. Algebra Appl.*

[12] O. W. Gnilke and J. Zumbrägel, "Cryptographic group and semigroup actions," in: *Journal of Algebra and Its Applications*, vol. 23, no. 07, 2024.

[13] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," in: *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[14] R. Steinwandt and A. Suárez, "Cryptanalysis of a 2-party key establishment based on a semigroup action problem," in: *Advances in Mathematics of Communications*, vol. 5, pp. 87–92, 2011.

[15] A. M. Childs and G. Ivanyos, "Quantum computation of discrete logarithms in semigroups," *J. Math. Cryptol.* **8** (2014), no. 4, 405–416.