AIMS Mathematics, 10(2): 1967–1980.
DOI: 10.3934/math.2025092
Received: 11 October 2024
Revised: 05 December 2024
Accepted: 16 December 2024
Published: 07 February 2025

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

Research article

On the security of the STR key exchange protocol

Aleksejus Mihalkovich*

Department of Applied Mathematics, Kaunas University of Technology, Studentu Str. 50, Kaunas, LT-51368, Lithuania

* **Correspondence:** Email: aleksejus.michalkovic@ktu.lt; Tel: +37060014070.

Abstract: In this paper, we consider the security of the Sakalauskas-Tvarijonas-Raulynaitis (STR) key exchange protocol. We perform an analysis by exploring various cases of the canonical form of the publicly known matrix using elements of linear algebra and number theory. Additionally, we consider the multiplicative order of matrices and show how these two factors affect the security of the considered protocol. We show that regardless of the choice of publicly known matrix, the considered protocol is secure under the discrete logarithm assumption. In other words, if at least one of the secret exponents is found, then the STR protocol can be broken in polynomial time.

Keywords: security analysis; noncommutative cryptography; key exchange protocol; linear algebra; canonical forms
Mathematics Subject Classification: 15A16, 15A18, 15A20, 94A60

1. Introduction

Non-commuting cryptography is currently considered a prospective field of research due to the potentially hard problems defined in noncommutative algebraic structures. In this area of cryptography the first ideas date back to the start of the millennium when the Anshel et al. and Ko et al. key exchange protocols (KEPs) were published [1, 2].

In [2], Ko et al. claimed that the security of their protocol relies on the so-called conjugate search problem, which is defined as follows [3]:

Definition 1. *Let us assume that $\mathbb{S}$ is a noncommutative (semi)group, and the two elements $g, h \in \mathbb{S}$ are fixed. The conjugate search problem is to find an element $x \in \mathbb{S}$ such that*

$$h = xgx^{-1}. \tag{1.1}$$

Let us present the Ko-Lee KEP. Assume that the noncommutative (semi)group $\mathbb{S}$, the subset of

commuting invertible elements $\mathbb{C}$, and the elements

$$g \in \mathbb{S} \setminus \mathbb{C}$$

are all publicly known. Using the conjugation relation (1.1), two entities named Alice and Bob can agree on a shared key by performing the following actions [2]:

(1) Alice chooses an arbitrary element $x \in \mathbb{C}$, and computes the following:

$$a = xgx^{-1}.$$

She keeps x hidden and publishes a online;

(2) Bob picks an arbitrary element $y \in \mathbb{C}$ and calculates the following:

$$b = ygy^{-1}.$$

He keeps y for himself and publishes b;

(3) Alice calculates the shared key

$$k = xbx^{-1}$$

and Bob obtains the same result by calculating

$$k = yay^{-1}.$$

It can be easily checked that the protocol is valid, since x and y come from the subset of commuting elements $\mathbb{C}$; therefore,

$$xy = yx.$$

Interestingly enough, the conjugation relation (1.1) has the following property:

$$x(ygy^{-1})x^{-1} = (xy)g(xy)^{-1}, \tag{1.2}$$

which holds for any $x, y \in \mathbb{S}$. Therefore, Ko-Lee KEP can be viewed as a certain analog of the Diffie-Hellman KEP for noncommutative algebraic structures. In other words, if we use the notation

$$g^x = xgx^{-1},$$

then the Ko-Lee protocol matches the Diffie-Hellman KEP almost word-for-word.

Unfortunately, the Ko-Lee protocol has a flaw revealed in [3], where the authors explained that the conjugate search problem can be replaced with the double coset problem defined below:

Definition 2. *Let us assume that $\mathbb{S}$ is a noncommutative (semi)group, and two elements $g, h \in \mathbb{S}$ are fixed. The double coset problem is to find two elements $x_1, x_2 \in \mathbb{S}$ such that*

$$h = x_1 g x_2. \tag{1.3}$$

Comparing the two problems, we can see that the double coset problem completely ignores the link between the secret elements x and x^{-1} in (1.1). Due to this fact, Alice and Bob can agree on two public subsets of the commuting elements $\mathbb{C}_1$ and $\mathbb{C}_2$ without affecting the validity of the Ko-Lee protocol in

any way. Furthermore, the requirement for x_1 and x_2 to be invertible can be ignored as well. The same is true for y_1 and y_2. Simply put, any links between the secret elements in (1.1) have vanished in (1.3).

In 2007, a Lithuanian group of researchers combined the ideas of the Ko-Lee and Diffie-Hellman KEPs. Their protocol quickly became known as the Sakalauskas-Tvarijonas-Raulynaitis (STR) KEP [4]. This protocol drew the attention of the cryptographic society (see [5–9]). However, based on the properties of matrices, it was pointed out that the STR KEP might not be secure enough to withstand the quantum cryptanalysis [7]. On the other hand, in their papers [5, 9], the authors considered the security of the protocols based on conjugation relation more generally. Here, we wish to focus on one specific protocol and explore its security in more detail. We aim to show that the STR KEP is not quantum-safe, which was stated in [7].

In this paper, we demonstrate that once at least one of the secret exponents is found, the STR protocol can be broken in polynomial time. Moreover, in some cases, the considered protocol can be broken without restoring the original exponent by computing an alternative key that uses a smaller exponent. Additionally, we demonstrate the case when the true value of the secret exponent is irrelevant.

The rest of this paper is organized as follows: in Section 2, we present the STR protocol and define its main parameters; in Section 3, we formalize the security of the STR protocol in the form of two games; in Section 4, we establish the main tools and perform the attack on the STR KEP; and finally, the conclusions and suggestions for future investigations are presented at the end of this paper.

2. Description of the STR protocol

In this section, we revise the considered protocol. We assume that the STR KEP uses matrices with entries from a field of integers $\mathbb{Z}_p$, where p is a large prime. As usual, the addition and multiplication operations in $\mathbb{Z}_p$ are performed modulo p. We keep this in mind throughout this paper and omit the modulo in all mathematical expressions. Therefore, we limit the analysis of this protocol to one certain class of groups.

The general concept of the STR KEP borrows ideas from the Diffie-Hellman and Ko-Lee protocols and combines them using calculations performed with square matrices of the size m. The group-defining parameter p, a set of commuting square $m \times m$ matrices $\mathbb{G}_m(\mathbb{Z}_p)$, and a matrix

$$\mathbf{Q} \in \mathbb{Z}_p^{m\times m} \setminus \mathbb{G}_m(\mathbb{Z}_p)$$

is published online. Alice and Bob use this public data to agree on a common key K using the following actions [4]:

(1) Alice randomly chooses a matrix $\mathbf{X} \in \mathbb{G}_m(\mathbb{Z}_p)$ and a large integer $r > 1$. She calculates a matrix

$$\mathbf{A} = \mathbf{X}\mathbf{Q}^r\mathbf{X}^{-1},$$

thus obtaining a public key

$$PuK_A = \mathbf{A},$$

which is published online. Her private key

$$PrK_A = (\mathbf{X}, r)$$

is kept hidden.

(2) Bob randomly picks a matrix $\mathbf{Y} \in \mathbb{G}_m(\mathbb{Z}_p)$ and a large integer $s > 1$. He calculates

$$\mathbf{B} = \mathbf{Y}\mathbf{Q}^s\mathbf{Y}^{-1},$$

and thus obtains a public key

$$PuK_B = \mathbf{B},$$

which is published online. He keeps the private key

$$PrK_B = (\mathbf{Y}, s)$$

hidden.

(3) Alice uses Bob's public key $\mathbf{B}$ and her private key $(\mathbf{X}, r)$ to calculate the following:

$$K_A = \mathbf{X}\mathbf{B}^r\mathbf{X}^{-1}.$$

(4) Bob uses Alice's public key $\mathbf{A}$ and his private key $(\mathbf{Y}, s)$ to calculate the following:

$$K_B = \mathbf{Y}\mathbf{A}^s\mathbf{Y}^{-1}.$$

Since $\mathbf{X}$ and $\mathbf{Y}$ commute, we have the following:

$$\begin{aligned}\mathbf{K}_A &= \mathbf{X}\mathbf{B}^r\mathbf{X}^{-1} = \mathbf{X}(\mathbf{Y}\mathbf{Q}^s\mathbf{Y}^{-1})^r\mathbf{X}^{-1}\\ &= \mathbf{X}\mathbf{Y}\mathbf{Q}^{sr}\mathbf{Y}^{-1}\mathbf{X}^{-1} = \mathbf{Y}\mathbf{X}\mathbf{Q}^{rs}\mathbf{X}^{-1}\mathbf{Y}^{-1}\\ &= \mathbf{Y}(\mathbf{X}\mathbf{Q}^r\mathbf{X}^{-1})^s\mathbf{Y}^{-1} = \mathbf{Y}\mathbf{A}^s\mathbf{Y}^{-1} = \mathbf{K}_B.\end{aligned}$$

Furthermore, the integer powers r and s are clearly commuting. Therefore, Alice and Bob have agreed on a shared key:

$$\mathbf{K} = \mathbf{K}_A = \mathbf{K}_B.$$

Note that the private powers r and s are limited above by the multiplicative order of the matrix $\mathbf{Q}$, which we denote by $\mathrm{ord}_p\,\mathbf{Q}$. This important fact implies restrictions on the public matrix $\mathbf{Q}$ to ensure a large enough value of $\mathrm{ord}_p\,\mathbf{Q}$. In fact, we can use the tools of linear algebra along with the group theory to control the value $\mathrm{ord}_p\,\mathbf{Q}$ in $\mathbb{Z}_p$. Here, we use these observations to analyze the security of the STR KEP.

Another important part of the public data is the set of commuting matrices $\mathbb{G}_m(\mathbb{Z}_p)$. For the STR KEP to be secure, this set has to be large and, preferably, its elements (matrices) should be easy to generate. However, there are multiple ways to achieve both of the presented properties. For example, one could either use the set of cyclic invertible matrices or the set of polynomials of some known matrix $\mathbf{M}$. In the latter case, the tools of linear algebra can be used to fit our needs.

3. Security games for STR KEP

We now present formal definitions of the security games for the STR protocol, which are interpreted as interactions between the attacker $\mathcal{A}$ and the challenger C, where the goal of $\mathcal{A}$ is to gain any kind of valuable information to predict the outcome of the actions performed by the challenger. The probability

of $\mathcal{A}$ to win a security game is called *$\mathcal{A}$'s advantage* [10]. For the KEP to be secure against a certain attack, $\mathcal{A}$'s advantage in winning an appropriate security game should be negligible.

The simplest idea of breaking any KEP is to compromise at least one of the private keys, PrA or PrB, in any way possible using mathematical tools. Therefore, the attacker $\mathcal{A}$ may somehow retrieve the actual key used by, say, Alice, or obtain an alternative key, which was not generated by Alice, but produces the same public key. This idea can be formalized by the following experiment:

Security game 1. *Let us assume that the group-defining parameter p, the group of commuting matrices $\mathbb{G}_m(\mathbb{Z}_p)$, and a matrix*

$$\mathbf{Q} \in \mathbb{Z}_p^{m\times m} \setminus \mathbb{G}_m(\mathbb{Z}_p)$$

are fixed.

(1) The challenger C generates the private keys of both Alice and Bob

$$PrK_A = (\mathbf{X}, r)$$

and

$$PrK_B = (\mathbf{Y}, s),$$

where $\mathbf{X}, \mathbf{Y} \in \mathbb{G}_m(\mathbb{Z}_p)$;

(2) C generates public keys

$$\mathbf{A} = \mathbf{X}\mathbf{Q}^r\mathbf{X}^{-1}$$

and

$$\mathbf{B} = \mathbf{Y}\mathbf{Q}^s\mathbf{Y}^{-1},$$

and calculates the shared key

$$\mathbf{K} = (\mathbf{X}\mathbf{Y})\mathbf{Q}^{rs}(\mathbf{X}\mathbf{Y})^{-1};$$

(3) The challenger sends the public keys $(\mathbf{A}, \mathbf{B})$ to $\mathcal{A}$.

Relying on the obtained pair $\mathcal{A}$ outputs a guess for the shared key $\mathbf{K}_{\mathcal{A}}$. He wins the game if

$$\mathbf{K}_{\mathcal{A}} = \mathbf{K}.$$

Here, the goal of attacker $\mathcal{A}$ is to calculate the shared key. Hence, the presented security game is the formal definition of the so-called computational assumption. Essentially, it states that given the public keys of both protocol parties, it is hard to calculate the shared key. Obviously, if $\mathcal{A}$ wins the presented security game, then the protocol is compromised and can no longer be considered safe since $\mathcal{A}$ is able to impersonate one of the parties. Furthermore, $\mathcal{A}$ can decrypt all the messages encrypted with the shared key if it is used for a symmetric encryption.

Another important question in the case of the STR KEP is whether the attacker $\mathcal{A}$ can somehow distinguish between the actual shared key K and a truly random matrix with entries uniformly chosen from $\mathbb{Z}_p$. In other words, given the public keys of both parties and a third matrix $\mathbf{K}_\delta$, can $\mathcal{A}$ decide if $\mathbf{K}_\delta$ is the shared key or not? Now, we present a formal definition of this experiment:

Security game 2. *Let us assume that the group-defining parameter p, the group of commuting matrices $\mathbb{G}_m(\mathbb{Z}_p)$, and a matrix*

$$\mathbf{Q} \in \mathbb{Z}_p^{m\times m} \setminus \mathbb{G}_m(\mathbb{Z}_p)$$

are fixed. For the randomly chosen value of $\delta \in \{0, 1\}$, we define the following experiment:

(1) The challenger C generates the private keys of both Alice and Bob

$$PrK_A = (\mathbf{X}, r)$$

and

$$PrK_B = (\mathbf{Y}, s),$$

where $\mathbf{X}, \mathbf{Y} \in \mathbb{G}_m(\mathbb{Z}_p)$*;*

(2) C generates public keys

$$\mathbf{A} = \mathbf{X}\mathbf{Q}^r\mathbf{X}^{-1}$$

and

$$\mathbf{B} = \mathbf{Y}\mathbf{Q}^s\mathbf{Y}^{-1};$$

(3) If $\delta = 0$*, then C calculates the following shared key:*

$$\mathbf{K}_0 = (\mathbf{X}\mathbf{Y})\mathbf{Q}^{rs}(\mathbf{X}\mathbf{Y})^{-1};$$

(4) If $\delta = 1$*, then C generates a random pair* $(\mathbf{Z}, t)$*, where the matrix* $\mathbf{Z} \in \mathbb{G}_m(\mathbb{Z}_p)$ *and* $t > 1$ *is a large integer. Then, he computes the following:*

$$\mathbf{K}_1 = \mathbf{Z}\mathbf{Q}^t\mathbf{Z}^{-1};$$

(5) The challenger sends the triplet $(\mathbf{A}, \mathbf{B}, \mathbf{K}_\delta)$ *to* $\mathcal{A}$*.*

Relying on the obtained data $\mathcal{A}$ *outputs a guess* $\delta_{\mathcal{A}}$*. He wins the game if* $\delta_{\mathcal{A}} = \delta$*.*

The presented security game is the formal definition of the decisional assumption for the STR protocol. We refer to it as the *decisional STR assumption*. Notably, this assumption is stronger than the computational one in the following sense: If $\mathcal{A}$ is able to win the Security game 1, then he can obviously win the Security game 2 with an advantage of 1, since he just found the shared key. On the other hand, if $\mathcal{A}$ cannot distinguish between a truly random matrix and the shared key, then he evidently cannot approach Security game 1, since he views the triplet $(\mathbf{A}, \mathbf{B}, \mathbf{K}_\delta)$ as three independent random matrices.

In the next section, we use the notions of the computational and decisional STR assumptions to analyze the security of the STR KEP.

4. Security analysis

4.1. The STR problem

Let us assume that the group-defining parameter p, the generator $\mathbf{M}$ of the group of commuting matrices $\mathbb{G}_m(\mathbb{Z}_p)$, and a matrix

$$\mathbf{Q} \in \mathbb{Z}_p^{m\times m} \setminus \mathbb{G}_m(\mathbb{Z}_p).$$

At the heart of the security of STR KEP lies the following problem:

Definition 3. *The following system of matrix equations:*

$$\begin{cases} \mathbf{X}\mathbf{Q}^r\mathbf{X}^{-1} = \mathbf{A}, \\ \mathbf{X}\mathbf{M} = \mathbf{M}\mathbf{X}, \end{cases} \tag{4.1}$$

where $\mathbf{X} \in \mathbb{G}_m(\mathbb{Z}_p)$ *and the integer* r *are unknown whereas*

$$\mathbf{A} = \mathbf{X}\mathbf{Q}^r\mathbf{X}^{-1}$$

is known, is called an STR problem.

Note that the authors of [5, 6, 9] may refer to this problem by a different name, but the general idea stays the same.

If the attacker $\mathcal{A}$ is able to solve the STR problem, then he can use the obtained pair $(\mathbf{X}, r)$ to compromise the shared key, thus winning both of the security games presented above.

First, let us consider the simplest version of the STR problem (i.e., we assume that the matrix $\mathbf{Q}$ is diagonalizable). In this case, we have the following:

$$\operatorname{ord}_p \mathbf{Q} = \operatorname{lcm}(\operatorname{ord}_p \lambda_1, \operatorname{ord}_p \lambda_2, \ldots, \operatorname{ord}_p \lambda_m),$$

where $\lambda_1, \lambda_2, \ldots, \lambda_m \in \mathbb{Z}_p$ are the eigenvalues of $\mathbf{Q}$, and $\operatorname{ord}_p \lambda_k$ is the multiplicative order of λ_k in $\mathbb{Z}_p$. Therefore, it does not exceed $p - 1$ due to Euler's theorem, and hence the computational STR assumption holds only under the discrete logarithm assumption. Now, we can see that for this choice of matrix $\mathbf{Q}$, STR is as safe as the Diffie-Hellman KEP. This means that it cannot provide protection against quantum cryptanalysis due to the result by P. Shor presented in his paper [11].

On the other hand, we could generate a matrix $\mathbf{Q}$ with all of the eigenvalues equal to the element $1 \in \mathbb{Z}_p$. Note that the latter fact does not mean that $\mathbf{Q}$ is an identity matrix. For example, the following works:

$$\mathbf{Q} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

However, the element 1 is an idempotent (i.e., $1^r = 1$ regardless of the value of r). On the other hand, we can easily check that we clearly have $\operatorname{ord}_p \mathbf{Q} > 1$ in any field $\mathbb{Z}_p$ for the example matrix $\mathbf{Q}$. Similar problems also arise if the eigenvalue of 0 is considered. Moreover, in this case, we may never get back to the original matrix, but rather the cycle may loop at some power r' of $\mathbf{Q}$, i.e., we could have

$$\mathbf{Q}^{r'+\operatorname{ord}_p \mathbf{Q}} = \mathbf{Q}^{r'},$$

but

$$\mathbf{Q}^{r'-1+\operatorname{ord}_p \mathbf{Q}} \neq \mathbf{Q}^{r'-1}.$$

This means that the attacker cannot rely on the eigenvalues alone in his attempts to gain information on the value of $\operatorname{ord}_p \mathbf{Q}$. Additionally, the structure of matrix $\mathbf{Q}$ has to be taken into consideration.

We already see that the simplest case presented above does not cover the complexity of the STR problem in full, since the eigenvalues of matrix $\mathbf{Q}$ are not the only key factors affecting the multiplicative order. Note that since $\mathbb{Z}_p$ is a field, the canonical form of matrix $\mathbf{Q}$ can be defined. In this case, the structure of the canonical form also influences the value of $\operatorname{ord}_p \mathbf{Q}$ and factors such as the number of Jordan blocks, the eigenvalue of the individual block, and the size of each block all play their part in determining the multiplicative order of $\mathbf{Q}$. Therefore, in this paper, we discuss how these factors affect the complexity of the STR problem.

4.2. Multiplicative order of $\mathbf{Q}$

First, we present several propositions that are related to the multiplicative order of a matrix in a field $\mathbb{Z}_p$. These propositions help us to obtain an upper bound on the matrix exponents r and s.

Proposition 1. *Assume that the matrix* $\mathbf{Q}$ *is similar to the following* $m \times m$ *Jordan block:*

$$\mathbf{J}_m(1) = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \tag{4.2}$$

The multiplicative order of matrix $\mathbf{Q}$ *is a multiple of* p*, i.e.,*

$$\operatorname{ord}_p \mathbf{Q} = kp,$$

where k *is the minimal value that* $kp \geq m$*.*

Proof. The proof of this proposition is based on a well-known fact that by raising the Jordan block $\mathbf{J}_m(1)$ to integer powers, we obtain the binomial coefficients in the upper half of the matrix. More precisely, we have the following:

$$\mathbf{J}_m^r(1) = \begin{pmatrix} 1 & \binom{r}{1} & \binom{r}{2} & \dots & \binom{r}{m-2} & \binom{r}{m-1} \\ 0 & 1 & \binom{r}{1} & \dots & \binom{r}{m-3} & \binom{r}{m-2} \\ 0 & 0 & 1 & \dots & \binom{r}{m-4} & \binom{r}{m-3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & \binom{r}{1} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \tag{4.3}$$

Note that

$$\binom{r}{0} = \binom{r}{r} = 1$$

and by definition

$$\binom{r}{k} = 0,$$

if $k > r$, meaning that there are no ways to choose k items out of r if $k > r$. Additionally, it is known from number theory that for a prime p, all the binomial coefficients $\binom{p}{k}$, aside from $\binom{p}{0}$ and $\binom{p}{p}$, are multiples of p. Therefore, if

$$m = p + 1,$$

then the top right corner entry of $\mathbf{J}_m^r(1)$ is 1 and we need to wait until r reaches $2p$ for the cycle to loop. Similar observations can be made if

$$m > p + 1.$$

□

However, since m is the size of square matrices, we can assume that it is always less than p. Hence, we claim that

$$\operatorname{ord}_p \mathbf{J}_m(1) = p.$$

Furthermore, since the multiplicative order is invariant under the similarity relation, for any matrix $\mathbf{Q}$ similar to $\mathbf{J}_m(1)$, we have the following:

$$\operatorname{ord}_p \mathbf{Q} = p.$$

Proposition 2. *Assume that the matrix $\mathbf{Q}$ is similar to the following $m \times m$ Jordan block:*

$$\mathbf{J}_m(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}, \tag{4.4}$$

where $\lambda \neq 0$. Then, we have the following:

$$\operatorname{ord}_p \mathbf{Q} = \operatorname{lcm}(\operatorname{ord}_p \lambda, \operatorname{ord}_p \mathbf{J}_m(1)).$$

Proof. The proof of this proposition follows directly from the following equality:

$$\mathbf{J}_m^r(\lambda) = \begin{pmatrix} \lambda^r & \binom{r}{1}\lambda^{r-1} & \binom{r}{2}\lambda^{r-2} & \dots & \binom{r}{m-2}\lambda^{r-m+2} & \binom{r}{m-1}\lambda^{r-m+1} \\ 0 & \lambda^r & \binom{r}{1}\lambda^{r-1} & \dots & \binom{r}{m-3}\lambda^{r-m+3} & \binom{r}{m-2}\lambda^{r-m+2} \\ 0 & 0 & \lambda^r & \dots & \binom{r}{m-4}\lambda^{r-m+4} & \binom{r}{m-3}\lambda^{r-m+3} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda^r & \binom{r}{1}\lambda^{r-1} \\ 0 & 0 & 0 & \dots & 0 & \lambda^r \end{pmatrix}. \tag{4.5}$$

Note that $\lambda^k \neq 0$ for any value of k if $\lambda \neq 0$. Therefore, the cycle of powers will loop the first time the two cycles (powers of λ and powers of $\mathbf{J}_m(1)$) will loop at the same point. This point is exactly the $\operatorname{lcm}(\operatorname{ord}_p \lambda, \operatorname{ord}_p \mathbf{J}_m(1))$. □

Corollary 1. *Assume that the matrix $\mathbf{Q}$ is similar to $\mathbf{J}_m(\lambda)$. Then, the maximal value of*

$$\operatorname{ord}_p \mathbf{Q} = (p-1) \cdot \operatorname{ord}_p \mathbf{J}_m(1).$$

This value is achieved, if λ is a generator of $\mathbb{Z}_p^*$.

Since almost always $m < p$, we can simplify the expression in Corollary 1 to the following:

$$\operatorname{ord}_p \mathbf{Q} = p(p-1).$$

This fact has to be taken into consideration when the Security game 1 is played. By considering the eigenvalue λ alone, the attacker can only obtain its power r modulo $(p-1)$. We denote this power by r_p.

Now, let us denote the direct sum of the two matrices $\mathbf{A}$ and $\mathbf{B}$ by $\oplus$. In other words, we have the following:

$$\mathbf{A} \oplus \mathbf{B} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}.$$

Proposition 3. *Assume that the matrix* $\mathbf{Q}$ *is similar to a Jordan matrix*

$$\mathbf{J} = \mathbf{J}_{m_1}(\lambda_1) \oplus \mathbf{J}_{m_2}(\lambda_2) \oplus \ldots \oplus \mathbf{J}_{m_k}(\lambda_k),$$

where

$$\sum_{i=1}^{k} m_i = m$$

and $\lambda_1, \lambda_2, \ldots, \lambda_k$ *are eigenvalues of* $\mathbf{Q}$ *(not necessarily distinct). Then, we have the following:*

$$\operatorname{ord}_p \mathbf{Q} = \operatorname{lcm}(\operatorname{ord}_p \mathbf{J}_{m_1}(\lambda_1), \operatorname{ord}_p \mathbf{J}_{m_2}(\lambda_2), \ldots, \operatorname{ord}_p \mathbf{J}_{m_k}(\lambda_k)).$$

Therefore, we can see that the maximal multiplicative order of matrix $\mathbf{Q}$ with eigenvalues from the initial field $\mathbb{Z}_p$ is determined as follows:

$$\operatorname{ord}_p \mathbf{Q} = p(p-1).$$

This can only be changed if the eigenvalues of $\mathbf{Q}$ are contained in some extension of $\mathbb{Z}_p$. However, we do not consider this case here, since the basic ideas remain the same, only in slightly more complicated algebraic structures.

Lastly, due to (4.5), note that $\mathbf{J}_m(0)$ is a nilpotent matrix with its m-th power equal to a zero matrix. However, since m is usually reasonably small, the first m powers can easily be considered separately.

As of now, it seems that for the setup considered here, the attacker $\mathcal{A}$ has to calculate the secret exponents r and s modulo $\operatorname{ord}_p \mathbf{Q}$. Unfortunately, in the next section, we show that it is enough to restore one of the secret exponents modulo $(p-1)$. Moreover, the STR protocol becomes insecure once we find the secret exponent.

4.3. Attack on STR KEP

First, let us consider the case when $\mathbf{Q}$ is similar to $\mathbf{J}_m(1)$. Without a loss of generality, we assume that

$$\mathbf{Q} = \mathbf{J}_m(1)$$

and denote it $\mathbf{J}$ for short. Furthermore, since the similarity relation lies at the heart of the STR protocol, which preserves not only the eigenvalues, but the Jordan blocks as well, we assume that the public key matrix $\mathbf{A}$ can be expressed as follows:

$$\mathbf{A} = \mathbf{S}^{-1}\mathbf{J}\mathbf{S}.$$

Note that regardless of the power r in the relation

$$\mathbf{A} = \mathbf{X}^{-1}\mathbf{J}^r\mathbf{X},$$

the general expression for $\mathbf{J}^r$ is given by (4.3), and, since 1 is an idempotent, $\mathbf{J}^r$ is similar to $\mathbf{J}$ regardless of the value of r. Therefore, we express

$$\mathbf{J}^r = \mathbf{T}^{-1}\mathbf{J}\mathbf{T}$$

for some matrix $\mathbf{T}$.

Now, we consider the first matrix equation of the STR problem (4.1). We have the following:

$$\begin{aligned}\mathbf{X}^{-1}\mathbf{J}^r\mathbf{X} &= \mathbf{S}^{-1}\mathbf{J}\mathbf{S},\\ \mathbf{S}\mathbf{X}^{-1}\mathbf{J}^r\mathbf{X}\mathbf{S}^{-1} &= \mathbf{J},\\ \mathbf{S}\mathbf{X}^{-1}T^{-1}\mathbf{J}T\mathbf{X}\mathbf{S}^{-1} &= \mathbf{J}.\end{aligned}$$

We can now denote

$$\mathbf{T}\mathbf{X}\mathbf{S}^{-1} = \mathbf{U}.$$

Then, we obtain the following:

$$\mathbf{U}^{-1}\mathbf{J}\mathbf{U} = \mathbf{J}.$$

Despite the fact that we have lost the relation of $\mathbf{U}$ to the generator matrix $\mathbf{M}$ in the original STR problem (4.1), the latter equation can be easily solved using linear algebra, since it can be transformed to the following homogeneous matrix equation:

$$\mathbf{J}\mathbf{U} - \mathbf{U}\mathbf{J} = \mathbf{0}.$$

Hence, despite the upper bound for r being p, the value of r contributes nothing to the complexity of the STR problem. Furthermore, since matrix $\mathbf{X}$ may be restored from $\mathbf{U}$, the computational and hence decisional assumptions do not hold for this choice of $\mathbf{Q}$.

Without a loss of generality, let us assume that

$$\mathbf{Q} = \mathbf{J}_m(\lambda),$$

where $\lambda \neq 1$. In this case, we can express $\mathbf{A}$ as follows:

$$\mathbf{A} = \mathbf{S}^{-1}\mathbf{J}_m(\mu)\mathbf{S},$$

where $\mathbf{J}_m(\mu)$ is a Jordan block, and $\mathbf{S}$ is the change-of-basis matrix. However, due to the STR problem (4.1), the eigenvalues λ and μ are mathematically linked via a congruence

$$\lambda^r \equiv \mu \bmod p. \tag{4.6}$$

Note that since $\mathbb{Z}_p$ is a field, the change-of-basis matrix $\mathbf{S}$ can be computed using methods of linear algebra and number theory.

We can now see that, despite the upper bound for r being $p(p-1)$, the attacker $\mathcal{A}$ is only interested in finding the following value:

$$r_p = r \bmod (p-1).$$

This comes from the fact that matrices $\mathbf{Q}^r$ and $\mathbf{Q}^{r_p}$ have the same eigenvalues; hence, these matrices are linked via the similarity relation:

$$\mathbf{Q}^r = \mathbf{T}^{-1}\mathbf{Q}^{r_p}\mathbf{T}.$$

Then, by performing transformations as in the previous case, we end up with the following equation:

$$\mathbf{Q}^{r_p} \cdot \mathbf{U} - \mathbf{U} \cdot \mathbf{J}_m(\mu) = \mathbf{0},$$

where

$$\mathbf{U} = \mathbf{TXS}^{-1}$$

is an unknown matrix. However, this equation is linear and can be easily solved. Therefore, the computational STR assumption only holds under the discrete logarithm assumption. Moreover, the decisional STR assumption does not hold, since the attacker can obtain a non-negligible advantage in winning the Security game 2 by inspecting the canonical form of the $\mathbf{K}_\delta$. Simply put, if the discrete logarithm problem is solved, then the STR problem is solved as well.

Finally, let us consider the general representation of

$$\mathbf{Q} = j_{m_1}(\lambda_1) \oplus \mathbf{J}_{m_2}(\lambda_2) \oplus \ldots \oplus \mathbf{J}_{m_k}(\lambda_k),$$

where $\lambda_1, \lambda_2, \ldots, \lambda_k$ are elements of $\mathbb{Z}_p$. Then, we can express $\mathbf{A}$ as follows:

$$\mathbf{A} = \mathbf{S}^{-1}\mathbf{JS},$$

where

$$\mathbf{J} = \mathbf{J}_{m_1}(\mu_1) \oplus \mathbf{J}_{m_2}(\mu_2) \oplus \ldots \oplus \mathbf{J}_{m_k}(\mu_k)$$

for some eigenvalues $\mu_1, \mu_2, \ldots, \mu_k$. An attacker can use any pair (λ_i, μ_i) to solve Eq (4.6), where $\lambda_i \neq 1$. Then he reconstructs all the actions presented for previous cases. For example, the choice of a suitable pair (λ_i, μ_i) can be based on the size of the Jordan blocks. Therefore, the hardest canonical form to consider is the one where all the Jordan blocks have equal sizes, since it is harder for the attacker to find μ_j matching λ_i. However, the size of matrices m is assumed to be reasonably small; hence, the attacker can simply explore all possible pairs to find matches.

We can sum up all of the presented cases in the following proposition:

Proposition 4. *Let us consider the STR problem* (4.1)*. We have the following:*

- *If all the eigenvalues of the matrix* $\mathbf{Q}$ *are in* $\mathbb{Z}_p$*, then the STR KEP is secure under the discrete logarithm assumption;*
- *If all the eigenvalues of the matrix* $\mathbf{Q}$ *are in* $\mathbb{Z}_p$*, then the secret exponent has to be restored modulo* $(p-1)$ *in* $\mathbb{Z}_p$*;*
- *If all the eigenvalues of* $\mathbf{Q}$ *are in* $\mathbb{GF}(p^m)$*, then the STR KEP is secure under the discrete logarithm assumption in* $\mathbb{GF}(p^m)$*;*
- *If the secret exponent is revealed, then the STR KEP can be broken in polynomial time.*

Therefore, the general algorithm for the attack on the STR KEP consists of the following steps:

(1) Find the canonical form of the public key matrix $\mathbf{A}$.

(2) Choose a pair of eigenvalues (λ_i, μ_i) of the matrices $\mathbf{Q}$ and $\mathbf{A}$, respectively. Then, construct Eq (4.6) and solve it. This step may be repeated multiple times to increase the chance of the successful attack.

(3) Use the secret exponent to obtain the system of linear equations to find the private matrix $\mathbf{U}$.

(4) Since the matrices $\mathbf{T}$ and $\mathbf{S}^{-1}$ are known, the adversary computes

$$\mathbf{X} = \mathbf{T}^{-1}\mathbf{U}\mathbf{S}.$$

The first step in this attack is the key step. Therefore, one of the possible solutions to escape this attack is for Alice and Bob to agree on an algebraic structure $\mathbb{S}$, where the canonical form of matrix $\mathbf{Q}$ is hard to find (or undefined if it is possible). Then, the mapping used in the STR KEP can be modified so that the entries of the matrix $\mathbf{Q}$ are chosen from $\mathbb{S}$, whereas the entries of $\mathbf{X}$ and $\mathbf{Y}$ are picked from $\mathbb{Z}_{\mathrm{ord}\,\mathbb{S}}$. Furthermore, the following identity must hold:

$$\mathbf{X}\mathbf{Q}^{r}\mathbf{X}^{-1} = (\mathbf{X}\mathbf{Q}\mathbf{X}^{-1})^{r}, \tag{4.7}$$

i.e., the scalar values of the matrices $\mathbf{X}$ and $\mathbf{Y}$ have to somehow interact with the entries of $\mathbf{Q}$ to ensure the correctness of the protocol. Here, the main obstacle is the fact that exponentiation of the matrix $\mathbf{Q}$ requires both addition and multiplication operations in $\mathbb{S}$. However, the existence of both these operations could potentially lead to the existence of the canonical form of the matrix $\mathbf{Q}$. Moreover, it is not clear whether the interaction between the two structures $\mathbb{S}$ and $\mathbb{Z}_{\mathrm{ord}\,\mathbb{S}}$ satisfies the identity (4.7) is possible.

5. Conclusions

In this paper, we considered the security of the STR KEP. Though the maximal value of the secret exponents r and s are limited above by the multiplicative order of the matrix $\mathbf{Q}$, we have shown that it is enough to restore one of the secret exponents modulo $(p-1)$. Furthermore, if the secret exponent is found, then the STR protocol is no different from the Ko-Lee KEP since the middle matrix is known in the first equation of (4.1). However, note that we limited our investigation to the fields of integers $\mathbb{Z}_p$. Additionally, we left out the case of eigenvalues being in $\mathbb{GF}(p^m)$, since the basic ideas presented here remain the same. The only thing that changes is the group size.

We showed that the computational STR assumption only holds under the discrete logarithm assumption for any matrix $\mathbf{Q}$. This fact means that we have to increase the public parameter p to an impractical bit size for the STR KEP to be secure. For example, we may consider a 2048-bit long prime p. However, such a large value defeats the original purpose of the STR KEP to achieve security without using operations with huge numbers. Furthermore, the decisional STR assumption does not hold, since it is enough to find the canonical form of $\mathbf{K}_{\delta}$. This fact means that an attacker can see certain relations between the publicly-known matrix $\mathbf{Q}$ and the user's public key.

All in all, we can see that for the algebraic structures considered here, the STR KEP is not quantum-safe. Therefore, future investigations may involve searching for other algebraic structures (commuting or not) where the canonical form of the matrix is either undefined or hard to find. However, as of now, it is not clear if such structures exist.

Use of Generative-AI tools declaration

The author declares he has not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The author declares no conflict of interest.

References

1. 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
2. K. Ko, S. Lee, J. Cheon, J. W. Han, J. S. Kang, C. Park, New public-key cryptosystem using braid groups, In: M. Bellare, *Advances in cryptology-CRYPTO 2000*, Springer, 2000, 166–183. https://doi.org/10.1007/3-540-44598-6_10
3. V. Shpilrain, A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, *Appl. Algebra Eng. Commun. Comput.*, **17** (2006), 285–289, http://doi.org/10.1007/s00200-006-0009-6
4. E. Sakalauskas, P. Tvarijonas, A. Raulynaitis, Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level, *Informatica*, **18** (2007), 115–124. http://doi.org/10.15388/Informatica.2007.167
5. M. Eftekhari, A Diffie-Hellman key exchange using matrices over non-commutative rings, *Groups Complexity Cryptology*, **4** (2012), 167–176. http://doi.org/10.1515/gcc-2012-0001
6. M. Sracic, Quantum circuits for matrix multiplication, *Comput. Sci. Phys. Math.*, 2011.
7. A. Myasnikov, A. Ushakov, Quantum algorithm for discrete logarithm problem for matrices over finite group rings, *Groups Complexity Cryptology*, **6** (2014), 31–36. http://doi.org/10.1515/gcc-2014-0003
8. A. Myasnikov, A. Ushakov, Cryptanalysis of matrix conjugation schemes, *J. Math. Cryptology*, **8** (2014), 95–114. http://doi.org/10.1515/jmc-2012-0033
9. A. Pandey, I. Gupta, D. K. Singh, On the security of DLCSP over $GL_n(\mathbb{F}_q[S_r])$, *Appl. Algebra Eng. Commun. Comput.*, **34** (2023), 619–628. http://doi.org/10.1007/s00200-021-00523-6
10. D. Boneh, V. Shoup, A graduate course in applied cryptography, *Draft 0.5*, 2023.
11. P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Rev.*, **41** (1999), 303–332. http://doi.org/10.1137/S0097539795293172

AIMS Press