Advances in Computational Sciences and Technology (ACST).
ISSN 0973-6107 Volume 10, Number 8 (2017), pp. 2603–2613

http://www.ripublication.com/acst.htm

Key Exchange Protocol Based on Quaternions

Shruti Nathani and B.P. Tripathi

Department of Mathematics,
Govt. N.P.G. College of Science Raipur (C.G.), India.

Abstract

In this paper a key exchange protocol based on quaternions is introduced. We form a quaternion matrix of real numbers which are involved in a quaternion number and then this matrix is used as a part of the private keys. An example is given in support of our proposed scheme. We also give a security analysis of the proposed protocol. The paper is concluded with some advantages and disadvantages of using quaternions in this scheme.

AMS subject classification: 94A60.
Keywords: Quaternions, Key exchange protocol, Polynomial, Public key, Private key.

1. Introduction

Key Exchange, as the name implies, is a process in which principals cooperate in order to establish a session key. In order to establish a confidential channel between two users of a network, classical single-key cryptography requires them to exchange a common secret key over a secure channel. This may work if the network is small and local, but it is infeasible in non-local or large networks.

To simplify the, key exchange problem, modern public key cryptography provides a mechanism in which the keys to be exchanged do not need to be secret.In such a framework, every user possesses a key pair consisting of a(non-secret) public key and a (secret) private key; only public keys are published [9] [8].

Thus a Key exchange protocol or mechanism is a key establishment technique in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of these (ideally) such that no party can predetermined the resulting value.

In 1976, Whitfield Diffie and Martin Hellman proposed the first key exchange protocol in their landmark paper "New directions in cryptography" [11], that enables the users to compute a common key from a secret key and publicly exchanged information. No user is required to hold secret information before entering the protocol and each member makes an independent contribution to the common agreed key.This work invents the revolutionary concept of the public key cryptography and is the most striking development in the history of cryptography.

In 1984, Odoni, Vardharajan and Sanders [10], gave a key exchange scheme based on matrices over a finite field. They use an invertible matrix as a group generator. Then in 1997, Menezes and Wu [3] the algorithm for the cryptanalysis of the protocols based on matrix powers in which the discrete logarithm problem $Y = M^r$, can be broken into simpler discrete logarithms over finite fields. In 2005, E. Stickel [5], gave a new method for exchanging secure keys.Another matrix based key exchange protocol was proposed by Climent et al. [6] in 2006. In 2009, Alvarez et al. [8] [9], proposed a secure key exchange scheme based on block upper traingular matrices.Then Youssef and Kamal [2] proposed a cryptanalysis attack on Alvarez et al. [8] key exchange scheme. In 2011 [7], Climent et al. proposed two key exchange protocols over noncommutative rings. After this paper Youssef and Kamal [1] again gave a cryptanalysis attack on Climent's protocols in 2012 [7].

In this paper we propose a key exchange protocol based on quaternions. We form a quaternion matrix of real numbers which are involved in a quaternion number and use this matrix as private keys in the proposed scheme to establish a secure key exchange protocol which enhance the climent's [7] key exchange protocol.We also give some security analysis of the proposed scheme and also explain the attack proposed by Youssef and Kamal [1] on Climent's [7] protocol is not applied in our proposed key exchange protocol.

2. Preliminaries

The quaternions are denoted by H. The letter H is in honour of Hamilton, their inventor. The quaternion is defined as an expression,

$$a = a_0 + a_1 i + a_2 j + a_3 k.$$

where a_0, a_1, a_2 and a_3 are real numbers and i, j and k are formal symbols satisfying the properties [4]:

$$i^2 = j^2 = k^2 = -1.$$

and

$$ij = k, jk = i, ki = j.$$

The i, j and k are all square roots of -1 but they don't commute, i.e.,

$$ji = -k, kj = -i, ik = -j.$$

2.1. A matrix representation for H [4]

There are various matrix representations for H. This one will make H as a subring of the real matrix ring $M_4(R)$. We will represent 1 by the identity matrix and i, j and k by three other matrices which can satisfy $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, $ki = j$.

For example: let a generic quaternion $a + bi + cj + dk$. Suppose

$$1 \leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$i \leftrightarrow \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$j \leftrightarrow \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},$$

$$k \leftrightarrow \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

We can see here $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, $ki = j$.
So the generic quaternion $a + bi + cj + dk$ corresponds to the matrix

$$\begin{bmatrix} a & -b & -c & -d \\ b & a & -c & d \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}.$$

2.2. The Key Exchange Protocol of Climent et al. [7]

Let us assume that R is a noncommutative ring. If we consider $f(x), g(x) \in Z(R)[x]$ and $k, l \in \mathbb{R}$ although R is not commutative we have that

$$f(m)^k g(m)^l = g(m)^l f(m)^k \text{ for all } M \in \mathbb{R}.$$

This property allows us to establish the following protocol:

PROTOCOL: The element $M, N \in \mathbb{R}$ are public.

Step 1: Alice chooses her private key $f(x) \in Z(R)[x]$ and $r, s \in \mathbb{N}$. Bob chooses his private key $g(x) \in Z(R)[x]$ and $u, v \in \mathbb{N}$.

Step 2: Alice compute her public key $P_A = f(M)^r N f(M)^s$ and send it to Bob. Analogously, Bob compute his public key $P_B = g(M)^u N g(M)^v$ and send it to Alice.

Step 3: Alice and Bob compute S_A and S_B respectively as $S_A = f(M)^r P_B f(M)^s$ and $S_A = g(M)^u P_A g(M)^v$.

Thus the Shared secret key, $S_A = S_B$ (By using expression 1).

2.3. Attack Proposed by Youssef et al. [1]

The main idea of the attack is based on the following lemma:

Lemma 2.1. Let W_1 and W_2 be the two invertible matrices such that

$$W_1 M = M W_1$$
$$W_2 M = M W_2$$
$$P_B W_2 = W_1 N$$

Then we have

$$S_A = S_B = W_1 P_A {W_2}^{-1}.$$

Proof. Note that $W_i, i = 1, 2$ commutes with M implies that W_i commutes with $f(M)$ ad consequantly W_i commutes with $f(M)^h$ for any $h \in \mathbb{N}$. Also W_i commutes with M implies that ${W_i}^{-1}$ commutes with M.
(This follows by noting that $W_i M = M W_i \Rightarrow W_i M {W_i}^{-1} = M \Rightarrow M {W_i}^{-1} = {W_i}^{-1} M$)
Thus we have

$$\begin{aligned} W_1 P_A {W_2}^{-1} &= W_1 f(M)^r N f(M)^s {W_2}^{-1} \\ &= f(M)^r W_1 N {W_2}^{-1} f(M)^s \\ &= f(M)^r P_B f(M)^s \\ &= S_A. \\ &\Rightarrow W_1 P_A {W_2}^{-1} = S_A. \end{aligned}$$

■

3. Proposed Protocol

Let Alice and Bob agree on the $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$ and $r, s \in \mathbb{N}$. Let

$$N = \begin{bmatrix} n_{11} & n_{12} & n_{13} & n_{14} \\ n_{21} & n_{22} & n_{23} & n_{24} \\ n_{31} & n_{32} & n_{33} & n_{34} \\ n_{41} & n_{42} & n_{43} & n_{44} \end{bmatrix} \in M_4(R)$$

be a 4×4 matrix. These are the public parameters.

Step 1: Alice choose a quaternion number as her private key. Let $q_1 = a_1 + ib_1 + jc_1 + kd_1$ and make a quaternion matrix from q_1, which is M_1. Similarly, Bob chooses an another quaternion number q_2 as his private key, let $q_2 = a_2 + ib_2 + jc_2 + kd_2$ and make a quaternion matrix from q_2, let it be M_2.

Step 2: Then Alice compute $f(M_1)$ from publicly known polynomial $f(x)$ and similarly Bob computes $f(M_2)$ from the polynomial $f(x)$.

Step 3: Now Alice computes her public key $P_A = f(M_1)^r N f(M_1)^s$ and send this value to Bob. Similarly, Bob computes his public key $P_B = f(M_2)^r N f(M_2)^s$ and send this value to Alice.

Step 4: Now Alice and Bob computes $S_A = f(M_1)^r P_B f(M_1)^s$ and $S_B = f(M_2)^r P_A f(M_2)^s$.

Thus $S_A = S_B$ the shared secret key as we can see in the following theorem.

3.1. Correctness of Algorithm

Theorem 3.1. The equation $S_A = S_B$ is correct.

Proof. As we know that $f(x), g(x) \in \mathbb{Z}(R)[X]$ and $k, l \in \mathbb{N}$ we have that $f(M)^k g(M)^l = g(M)^l f(k)^l$ for all $M \in \mathbb{R}$ so,

$$\begin{aligned} S_A &= f(M_1)^r P_B f(M_1)^s \\ &= f(M_1)^r f(M_2)^r N f(M_2)^s f(M_1)^s \\ &= f(M_2)^r f(M_1)^r N f(M_1)^s f(M_2)^s \\ &= f(M_2)^r P_A f(M_2)^s \\ &= S_B. \end{aligned}$$

Thus, $S_A = S_B$. ■

3.2. Example

First, suppose that Alice and Bob agree on a second degree polynomial $f(x) = x^2 + x + 1$ and take $r = 1, s = 2$, also take a 4×4 public matrix

$$N = \begin{bmatrix} 2 & 3 & 8 & 9 \\ 4 & 1 & 2 & 0 \\ 3 & 1 & 4 & 4 \\ 8 & 1 & 10 & 20 \end{bmatrix}$$

These are the public parameters.

Step 1: Alice choose her private quaternion number $q_1 = 1 + 2i + 3j + 4k$. To form a matrix from q_1, she suppose that

$$1 \leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$i \leftrightarrow \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$j \leftrightarrow \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},$$

$$k \leftrightarrow \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Which satisfy, $i^2 = j^2 = k^2 = -1$ and $ij = k, jk = i, ki = j$. So the matrix corresponds to the quaternion number $q_1 = 1 + 2i + 3j + 4k$ is

$$M_1 = \begin{bmatrix} 1 & -2 & -3 & -4 \\ 2 & 1 & -4 & 3 \\ 3 & 4 & 1 & -2 \\ 4 & -3 & 2 & 1 \end{bmatrix}.$$

Similarly, Bob choose his private key that is another quaternion number $q_2 = 2 + 4i + 5j + k$. To form a matrix from q_2, he suppose that

$$1 \leftrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$i \leftrightarrow \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$j \leftrightarrow \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix},$$

$$k \leftrightarrow \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

Which satisfy, $i^2 = j^2 = k^2 = -1$ and $ij = k, jk = i, ki = j$. So the matrix corresponds to the quaternion number $q_2 = 2 + 4i + 5j + k$ is

$$M_2 = \begin{bmatrix} 2 & 4 & 5 & 1 \\ -4 & 2 & -1 & 5 \\ -5 & 1 & 2 & -4 \\ -1 & -5 & 4 & 2 \end{bmatrix}.$$

Step 2: Then Alice compute $f(M_1)$ from

$$f(x) = x^2 + x + 1,$$

$$f(M_1) = \begin{bmatrix} 1 & -2 & -3 & -4 \\ 2 & 1 & -4 & 3 \\ 3 & 4 & 1 & -2 \\ 4 & -3 & 2 & 1 \end{bmatrix}^2 + \begin{bmatrix} 1 & -2 & -3 & -4 \\ 2 & 1 & -4 & 3 \\ 3 & 4 & 1 & -2 \\ 4 & -3 & 2 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$f(M_1) = \begin{bmatrix} -26 & -6 & -9 & -12 \\ 6 & -26 & -12 & 9 \\ 9 & 12 & -26 & -6 \\ 12 & -9 & 6 & -26 \end{bmatrix}.$$

Similarly, Bob computes $f(M_2)$ from $f(x) = x^2 + x + 1$,

$$f(M_2) = \begin{bmatrix} 2 & 4 & 5 & 1 \\ -4 & 2 & -1 & 5 \\ -5 & 1 & 2 & -4 \\ -1 & -5 & 4 & 2 \end{bmatrix}^2 + \begin{bmatrix} 2 & 4 & 5 & 1 \\ -4 & 2 & -1 & 5 \\ -5 & 1 & 2 & -4 \\ -1 & -5 & 4 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$$f(M_2) = \begin{bmatrix} -35 & 20 & 25 & 5 \\ -20 & -35 & -5 & 25 \\ -25 & 5 & -35 & -20 \\ -5 & -25 & 20 & -35 \end{bmatrix}.$$

Step3: Then Alice computes her public value, $P_A = [f(M_1)]^r N [f(M_1)]^s$.

$$P_A = \begin{bmatrix} -26 & -6 & -9 & -12 \\ 6 & -26 & -12 & 9 \\ 9 & 12 & -26 & -6 \\ 12 & -9 & 6 & -26 \end{bmatrix}^1 \begin{bmatrix} 2 & 3 & 8 & 9 \\ 4 & 1 & 2 & 0 \\ 3 & 1 & 4 & 4 \\ 8 & 1 & 10 & 20 \end{bmatrix} \begin{bmatrix} -26 & -6 & -9 & -12 \\ 6 & -26 & -12 & 9 \\ 9 & 12 & -26 & -6 \\ 12 & -9 & 6 & -26 \end{bmatrix}^2.$$

$$P_A = \begin{bmatrix} 444383 & -109719 & -155572 & -403998 \\ -153656 & 41299 & -75334 & 59250 \\ 93972 & -40307 & -7316 & -121277 \\ 230042 & -143111 & -34682 & -339640 \end{bmatrix}$$

send this value to Bob.
Similarly, Bob computes his public value

$$P_B = [f(M_2)]^r N [f(M_2)]^s$$

$$P_B = \begin{bmatrix} -35 & 20 & 25 & 5 \\ -20 & -35 & -5 & 25 \\ -25 & 5 & -35 & -20 \\ -5 & -25 & 20 & -35 \end{bmatrix}^1 \begin{bmatrix} 2 & 3 & 8 & 9 \\ 4 & 1 & 2 & 0 \\ 3 & 1 & 4 & 4 \\ 8 & 1 & 10 & 20 \end{bmatrix} \begin{bmatrix} -35 & 20 & 25 & 5 \\ -20 & -35 & -5 & 25 \\ -25 & 5 & -35 & -20 \\ -5 & -25 & 20 & -35 \end{bmatrix}^2.$$

$$P_B = \begin{bmatrix} -252875 & -354375 & -92750 & -93625 \\ 875 & 504875 & -455000 & 182000 \\ -1421875 & -762125 & 1450750 & -553875 \\ -997500 & -585375 & 1426250 & -408625 \end{bmatrix}.$$

Step 4: Now Alice and Bob computes their shared secret key. Alice computes

$$S_A = f(M_1)^r P_B f(M_1)^s.$$

$$S_A = \begin{bmatrix} -26 & -6 & -9 & -12 \\ 6 & -26 & -12 & 9 \\ 9 & 12 & -26 & -6 \\ 12 & -9 & 6 & -26 \end{bmatrix}^1 \begin{bmatrix} -252875 & -354375 & -92750 & -93625 \\ 875 & 504875 & -455000 & 182000 \\ -1421875 & -762125 & 1450750 & -553875 \\ -997500 & -585375 & 1426250 & -408625 \end{bmatrix}$$

$$\begin{bmatrix} -26 & -6 & -9 & -12 \\ 6 & -26 & -12 & 9 \\ 9 & 12 & -26 & -6 \\ 12 & -9 & 6 & -26 \end{bmatrix}^2.$$

$$S_A = \begin{bmatrix} 11449587625 & 38980029375 & 13296424750 & 7013286875 \\ 4580219000 & -7948257625 & -529313750 & 10533800375 \\ 21962929625 & 64885877875 & 7895088250 & 4277597625 \\ 14435255625 & 23220348375 & -4079750500 & 2055746000 \end{bmatrix}.$$

similarly, Bob computes

$$S_B = f(M_2)^r P_A f(M_2)^s.$$

$$S_B = \begin{bmatrix} -35 & 20 & 25 & 5 \\ -20 & -35 & -5 & 25 \\ -25 & 5 & -35 & -20 \\ -5 & -25 & 20 & -35 \end{bmatrix}^1 \begin{bmatrix} 444383 & -109719 & -155572 & -403998 \\ -153656 & 41299 & -75334 & 59250 \\ 93972 & -40307 & -7316 & -121277 \\ 230042 & -143111 & -34682 & -339640 \end{bmatrix}$$

$$\begin{bmatrix} -35 & 20 & 25 & 5 \\ -20 & -35 & -5 & 25 \\ -25 & 5 & -35 & -20 \\ -5 & -25 & 20 & -35 \end{bmatrix}^2.$$

$$S_B = \begin{bmatrix} 11449587625 & 38980029375 & 13296424750 & 7013286875 \\ 4580219000 & -7948257625 & -529313750 & 10533800375 \\ 21962929625 & 64885877875 & 7895088250 & 4277597625 \\ 14435255625 & 23220348375 & -4079750500 & 2055746000 \end{bmatrix}.$$

Thus, we have $S_A = S_B$.

4. Security Analysis

We have shown in section 3, in the proposed protocol the attacker needs to solve the following system of equation

$$P_A = [f(M_1)]^r N[f(M_1)]^s,\ P_B = [f(M_2)]^r N[f(M_2)]^s.$$

This is equivalent to solve DP problems. Thus the security of the proposed protocol is based on the difficulty posed to solve the DP problem, for which no polynomial time probabilistic algorithm capable of solving this problem is known.

Here we also shown that the proposed protocol meets the following desirable attributes.

Known Key Security: If Alice and Bob execute the regular protocol run, they clearly share their unique session key K because

$$\begin{aligned} S_A &= f(M_1)^r P_B f(M_1)^s \\ &= f(M_1)^r f(M_2)^r N f(M_2)^s f(M_1)^s \\ &= f(M_2)^r f(M_1)^r N f(M_1)^s f(M_2)^s \\ &= f(M_2)^r P_A f(M_2)^s = S_B. \end{aligned}$$

Perfect Forward Secrecy: In our proposed protocol the parameters r and s are publicly known. If we consider r and s as the long term private keys of our principals (Alice and Bob). That is Alice choose privately r_1 and s_1 and Bob chooses privately r_2 and s_2 then the protocol should be run as

$$P_A = [f(M_1)]^{r_1} N[f(M_1)]^{s_1},\ P_B = [f(M_2)]^{r_2} N[f(M_2)]^{s_2}$$

. Then the protocol should be run as

$$\begin{aligned} S_A &= [f(M_1)]^{r_1} P_B[f(M_1)]^{s_1} = [f(M_1)]^{r_1}[f(M_2)]^{r_2} N[f(M_2)]^{s_2}[f(M_1)]^{s_1} \\ &= [f(M_2)]^{r_2}[f(M_1)]^{r_1} N[f(M_1)]^{s_1}[f(M_2)]^{s_2} = [f(M_2)]^{r_2} P_A[f(M_2)]^{s_2} = S_B. \end{aligned}$$

Now if the attacker knows the long term private keys (r_1, s_1), (r_2, s_2) of Alice and Bob respectively, although the secrecy of session key S_A and S_B should not be affected. This meets the perfect forward secrecy in our proposed protocol.

Unknown Key Share Attack: An unknown key share attack is valid if the adversary does not know the private key corresponding to the certified public key. Our proposed protocol is secure against this attack because in our proposed protocol from the given certified public parameters the adversary does not recover the private keys.

As we explain in section 2.3, Youssff et al. [1] proposed an attack which is based on two invertible matrices W_1 and W_2. Here both the matrices W_1 and W_2 are commute with M, which satisfies:

$$W_1 M = M W_1$$

$$W_2 M = M W_2$$

$$P_B W_2 = W_1 N$$

This type of attack is possible only when M and N both matrices are publicly known. In our proposed protocol the matrix M is formed by Alice and Bob by their secretly choosen quaternion number. That means there is no possibility to find W_1 and W_2 that satisfies the above equations. Thus this type of attacks are also not applicable in our proposed work.

5. Conclusion

In this paper we use a quaternion number to form a quaternion matrix as the part of private keys of the proposed protocol that allow a key exchange in a secure manner. The advantage of taking quaternion is that Alice and Bob choose quaternion number as their private key and form quaternion matrices from those quaternion numbers. This step makes the protocol more secure from the security point of view. The only disadvantage of our scheme is that because of taking quaternions the order of matrices are limited to 4×4.

References

[1] A.A. Kamal, A. M. Youssef, (2012), "Cryptanalysis of a key exchage protocol based on the endomorphisms ring END($\mathbb{Z}_P \times {\mathbb{Z}_p}^2$)", Springer-Verlag.

[2] A.A. Kamal, A. M. Youssef, (2013), "Cryptanalysis of Alvarez et al. key exchange scheme", information Sciences 223, 317–321.

[3] A. J. Menezes, (1997), "The discrete logarithm problem in $GL(n, q)$". Ars combiatoria, 47:23–32.

[4] David Joyce, (2008), "Introduction to mordern Algebra." Clark Uiversity, version 0.06.

[5] E. Stickel, (2005), "A new method for exchanging secret keys". In Proceeding of the Third International Conference on Information Technology and Application (ICITA'05) pages 426–430. Sidney, Australia.

[6] J. Climent, E. Gorla and J. Rosenthal, (2007), "Cryptanalysis of the CFVZ cryptosystem Advances in mathematics of computations." pp. 1–11.

[7] J.J. Climent, P.R. Navarro and L. Tortosa, (2012), "Key exchange protocols over non-commutative rings, The case of END($\mathbb{Z}_P \times \mathbb{Z}_p{}^2$)", AMS.

[8] R. Alvarez, L. Tortosa, J.F. Vicent and A. Zamora, (2009), "Analysis and design of a secure key exchange scheme". Information scieces, 179:20146–2021.

[9] R. Alvarez, F. Martinez, J.F. Vicent and A. Zamora, (2007), "A New public Key Cryptosystem based on Matrices", 6th WSEAS International Conferece on information Security and privacy, Tenerife, Spain December 14–16.

[10] R.W.K. Odoni and V. Vardharajan and P.W. Sanders, (1984), "Public key distribution in matrix rings." Electronic letters, 20:386–387.

[11] W. Diffie, M. Hellman, (1976), "New Directions In Cryptography", IEEE Transactions on information theory 22, 644–654.