Key exchange protocols over noncommutative rings. The case of End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$)

Joan-Josep Climent[1] * Pedro R. Navarro[2]
Leandro Tortosa[2]

[1] Departament d'Estadística i Investigació Operativa, Universitat d'Alacant

[2] Departament de Ciència de la Computació i Intel·ligència Artificial, Universitat d'Alacant

May 17, 2012

Abstract

In this paper we introduce some key exchange protocols over noncommutative rings. These protocols use some polynomials with coefficients in the center of the ring as part of the private keys. We give some examples over the ring End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$), where p is a prime number. We also give a security analysis of the proposed protocols and conclude that the only possible attack is by brute force.

Keywords: Key exchange protocol, noncommutative ring, center of a ring, polynomial, public key cryptography.

2000 AMS Subject Classification: 16L30, 94A60

1 Introduction

Nowadays, most commonly used public key cryptosystems (PKC) and public key exchange protocols are number theory based. The theoretical strength depends on the structure of abelian groups. Their robustness is based on the difficulty of solving certain problems over finite commutative algebraic structures. One of these problems is the Integer Factorization Problem over the ring $\mathbb{Z}_n$, being n the product of two large prime numbers; the well known cryptosystem RSA [26] is based on this problem. The second classical problem is the Discrete Logarithm Problem (DLP) over a finite field $\mathbb{Z}_p$, being p a large prime; the ElGamal protocol [14] and all its variants are based on this problem.

*The work of this author was partially supported by Spanish grant MTM2011-24858 of the Ministerio de Economía y Competitividad of the Gobierno de España.

Since Diffie and Hellman [12] proposed the first key exchange algorithm, we can find an extensive bibliography on the problem of key exchange protocols in public key cryptography (see, for example, [21, 29, 35] and the references therein). Most of proposed algorithms are related to arithmetic operations on commutative algebraic structures and some efficient attacks based on the commutative property of these structures are well known.

It is believed that the increasing computing power of modern computers has made these techniques less secure (see, for example, [6, 30]). As a consequence of this, there exists an active field of research known as noncommutative algebraic cryptography (see, for example, [4, 11, 20, 23, 27, 28, 33]), aiming to develop and analyze new cryptosystems and key exchange protocols based on noncommutative cryptographic platforms. Currently, the security of cryptosystems on a nonabelian group G is based on any of the following problems:

The Conjugator Search Problem (CSP). Given $(x, y) \in G \times G$, the problem is to find $z \in G$ such that $y = z^{-1}xz$.

The Decomposition Problem (DP). Given $(x, y) \in G \times G$ and $S \subseteq G$, the problem is to find $z_1, z_2 \in S$ such that $y = z_1 x z_2$.

The Symmetric Decomposition Problem (SDP). Given $(x, y) \in G \times G$ and $m, n \in \mathbb{Z}$, the problem is to find $z \in G$ such that $y = z^m x z^n$.

The Generalizing of the Symmetric Decomposition Problem (GSDP). Given $(x, y) \in G \times G$, $S \subseteq G$ and $m, n \in \mathbb{Z}$, the problem is to find $z \in S$ such that $y = z^m x z^n$.

Several authors have used nonabelian groups for public key exchange. Below we mention a few of them without going into details. In [3, 4, 20, 19], the authors suggest to use the braid groups as platform groups for their respective protocols. In [25] the authors propose a PKC scheme whose security is based on the DLP problem for the automorphism defined by the conjugation operation and the difficulty to find the conjugate element on finite nonabelian groups. In [32] the authors suggest the use of a finite representation of a nonabelian group, called Thomson's group, to develop a PKC model, where they raised for the first time the difficulty of solving the SDP problem. Finally, in [36], the authors propose a cryptosystem whose robustness is based on the difficulty of solving the CSP and SDP problems over any noncommutative algebraic structure.

In [17] the authors present a PKC based on rings (the NTRU cryptosystem). We can find some attacks on this cryptosystem in [15, 16]. In [24] the authors introduce the DLP for matrix rings with entries in $\mathbb{F}_q$, while a Diffie-Hellmann key exchange protocol based on matrices can be found in [37]. Menezes and Wu [22] reduced the DLP for matrices to some DLPs over small extensions of $\mathbb{F}_q$. Other implementations of the Diffie-Hellman protocol in matrix rings, for different kind of matrices, are presented in [1, 2, 8, 34, 38]. Satoh and Akari [28] introduce an scheme based on the noncommutative ring of quaternions. Four years later,

Coppersmith [11] performs some attacks over this scheme. More recently, Hurley and Hurley [18] presented a public key cryptosystem using group rings.

The main idea of this work is the design of some public key exchange protocols over noncommutative rings, in particular over the ring of endomorphisms of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, where p is a prime number. Bergman [5] proved that this ring has p^5 elements, it is semilocal, and it cannot be embebed in matrices over any commutative ring. This last property is what makes this ring very interesting for cryptographic applications, since it is not possible to apply the reduction suggested by Menezes and Wu [22].

The rest of the paper is organized as follows. In Section 2 we recall the arithmetic and some properties of the ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ based on the caracterization by Climent, Navarro, and Tortosa [10]. In Section 3, we give a first key exchange protocol over noncommutative rings and we point out its weakness. This motivates the introduction of two new protocols using polynomials with coefficientes over the center of a noncommutative ring in Section 4. In Section 5, we perform a security analysis of the proposed protocols. Finally, in Section 6 we present the conclusions of the paper. A preliminary version of this paper has appeared in the conference proceedings [9].

2 Preliminaries

Climent, Navarro, and Tortosa [10] established an isomorphism between the ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ and the ring

$$E_p = \left\{ \begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix} \;\middle|\; a,b,c,u,v \in \mathbb{Z}_p \right\},$$

where the addition and multiplication are given by (see [10, Corollary 1])

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & pu_1+v_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ pc_2 & pu_2+v_2 \end{bmatrix}$$
$$= \begin{bmatrix} (a_1+a_2) \bmod p & (b_1+b_2) \bmod p \\ p\left[(c_1+c_2) \bmod p\right] & p\left[\left(u_1+u_2+\left\lfloor \frac{v_1+v_2}{p} \right\rfloor\right) \bmod p\right] + (v_1+v_2) \bmod p \end{bmatrix}$$

and

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & pu_1+v_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ pc_2 & pu_2+v_2 \end{bmatrix}$$
$$= \begin{bmatrix} (a_1a_2) \bmod p & (a_1b_2+b_1v_2) \bmod p \\ p\left[(c_1a_2+v_1c_2) \bmod p\right] & p\left[\left(c_1b_2+u_1v_2+v_1u_2+\left\lfloor \frac{v_1v_2}{p} \right\rfloor\right) \bmod p\right] + (v_1v_2) \bmod p \end{bmatrix}$$

respectively. The additive and multiplicative identities are, respectively

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

As a consequence of that isomorphism, we identify $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ with E_p. We will use this ring for the implementation of our protocols.

The center of this ring will play an important role in the protocols that will be introduced in the next section. It is not difficult to show that the center of E_p is the set

$$\mathcal{Z}(E_p) = \left\{ \begin{bmatrix} x & 0 \\ 0 & py + x \end{bmatrix} \mid x, y \in \mathbb{Z}_p \right\},$$

and that the number of elements of $\mathcal{Z}(E_p)$ is p^2, which coincides with the characteristic of E_p.

On the other hand, E_p is not an integral domain because it has zero divisors; for example, for $a, b, c, u, v \in \mathbb{Z}_p \setminus \{0\}$, we have that

$$\begin{bmatrix} a & 0 \\ pb & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ pc & pu + v \end{bmatrix} \in E_p \setminus \{O\}$$

but

$$\begin{bmatrix} a & 0 \\ pb & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ pc & pu + v \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

So, E_p is not a left nor a right Euclidean ring and, consequently, the ring of polynomials with coefficients in E_p is not Euclidean. Neither $\mathcal{Z}(E_p)$ is an Euclidean ring since it also has divisors of zero. For instance, if $u_1, u_2 \in \mathbb{Z}_p \setminus \{0\}$, then

$$\begin{bmatrix} 0 & 0 \\ 0 & pu_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & pu_2 \end{bmatrix} \in \mathcal{Z}(E_p) \setminus \{O\} \quad \text{but} \quad \begin{bmatrix} 0 & 0 \\ 0 & pu_1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & pu_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

3 A first key exchange protocol over noncommutative rings

Stickel [34] introduces a key exchange protocol using the group $G = \langle C^a S, TD^b \rangle$ generated by the matrices $C^a S$ and TD^b, where C and D are the companion matrices of two irreducible polynomials $p(\mathsf{X})$ and $q(\mathsf{X})$, respectively, of degree n over $\mathbb{F}_2$ (the Galois field with two elements); S and T are two invertible elements in an extension field of $\mathbb{F}_2$ such that SCS^{-1} and TDT^{-1} are diagonal matrices, whose diagonal elements are the roots of $p(\mathsf{X})$ and $q(\mathsf{X})$, respectively, in an extension field of $\mathbb{F}_2$, and a and b are two arbitrary integers. Taking into account the key exchange protocol introduced in [34] we propose the following protocol over a noncommutative ring R.

Protocol 1: The elements M, $N \in R$ are public.

Step 1: Alice and Bob choose their private keys $(r, s), (u, v) \in \mathbb{N}^2$ respectively.

Step 2: Alice computes her public key $P_A = M^r N M^s$ and sends it to Bob.

Similarly, Bob computes his public key $P_B = M^u N M^v$ and sends it to Alice.

Step 3: Alice and Bob compute S_A and S_B, respectively, as

$$S_A = M^r P_B M^s \quad \text{and} \quad S_B = M^u P_A M^v.$$

The shared secret is $S_A = S_B$, as we can see in the following theorem. □

Theorem 1: *With the above notation, it follows that* $S_A = S_B$.

PROOF: The result follows from the fact that $M^k M^l = M^l M^k$, for all $k, l \in \mathbb{N}$. □

Note that if $MN = NM$ then

$$P_A = M^r N M^s = N M^r M^s \quad \text{and} \quad P_B = M^u N M^v = N M^u M^v,$$

therefore

$$NS_A = NM^r M^u N M^v M^s = M^r N M^s M^u N M^v = P_A P_B,$$
$$NS_B = NM^u M^r N M^s M^v = M^u N M^v M^r N M^s = P_B P_A,$$

that is, $NS_A = NS_B$, because $P_A P_B = P_B P_A$. So, the shared secret $S_A = S_B$ may be easily obtained by an unauthorized part, since N, P_A and P_B are public.

Then, we need that $MN \neq NM$; therefore, from now on we will assume that $N \notin \mathcal{Z}(R)$. Thus, the security of this protocol is based on achieving an element M with large order. However, using the ideas of Shpilrain [31] it is easy to cryptanalyze the above protocol because the element M is public. For example, if an attacker is able to find $X, Y \in R$ such that

$$XM = MX, \quad YM = MY \quad \text{and} \quad P_A = XNY$$

then

$$XP_B Y = XM^u N M^v Y = M^u P_A M^v = S_B$$

which is the shared secret.

To avoid this weakness we propose in the next section two new protocols considering the elements $f(M)$ and $g(M)$ obtained from M and two polynomials $f(\mathsf{X}), g(\mathsf{X}) \in \mathcal{Z}(R)[\mathsf{X}]$, instead of considering simply the element M.

4 Key exchange protocols using polynomials over a noncommutative ring

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

$$f(M)^k g(M)^l = g(M)^l f(M)^k, \quad \text{for all } M \in R. \tag{1}$$

This property allows us to establish the following protocol.

Protocol 2: The elements $M \in R$ and $N \in R \setminus \mathcal{Z}(R)$, are public.

Step 1: Alice chooses her private key $f(\mathsf{X}) \in \mathcal{Z}(R)[\mathsf{X}]$ and $r, s \in \mathbb{N}$.

Bob chooses his private key $g(\mathsf{X}) \in \mathcal{Z}(R)[\mathsf{X}]$ and $u, v \in \mathbb{N}$.

Step 2: Alice computes her public key $P_A = f(M)^r N f(M)^s$, and sends it to Bob.

Analogously, Bob computes his public key $P_B = g(M)^u N g(M)^v$, and sends it to Alice.

Step 3: Alice and Bob compute S_A and S_B, respectively, as

$$S_A = f(M)^r P_B f(M)^s \quad \text{and} \quad S_B = g(M)^u P_A g(M)^v. \qquad \square$$

As in Protocol 1, the shared secret is $S_A = S_B$, as we can see in the following theorem.

Theorem 2: *With the above notation, it follows that $S_A = S_B$.*

Proof: The result follows from expression (1). $\square$

In order to simplify the calculations in the following example we take a small value for p, namely $p = 31$, although we must be aware that for practical implementations of the protocols we must consider values for p of the order of 60 decimal digits.

Example 1: In the set up of the protocol we make public the elements

$$M = \begin{bmatrix} 19 & 22 \\ 62 & 893 \end{bmatrix} \in E_{31} \quad \text{and} \quad N = \begin{bmatrix} 22 & 27 \\ 775 & 521 \end{bmatrix} \in R \setminus \mathcal{Z}(E_{31}).$$

Then we go on the protocol steps:

Step 1: Alice chooses her private key $(r, s) = (5, 7)$ and

$$f(\mathsf{X}) = \begin{bmatrix} 15 & 0 \\ 0 & 77 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 777 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 17 & 0 \\ 0 & 482 \end{bmatrix} \mathsf{X}^4 \in \mathcal{Z}(E_{31})[\mathsf{X}].$$

Then, $f(M) = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix}$.

Bob chooses his private key $(u, v) = (9, 8)$ and

$$g(\mathsf{X}) = \begin{bmatrix} 7 & 0 \\ 0 & 472 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 12 & 0 \\ 0 & 508 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & 0 \\ 0 & 869 \end{bmatrix} \mathsf{X}^6 \in \mathcal{Z}(E_{31})[\mathsf{X}].$$

Then $g(M) = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}$.

Step 2: Alice computes her public key P_A as

$$P_A = f(M)^r N f(M)^s = \begin{bmatrix} 11 & 15 \\ 403 & 355 \end{bmatrix},$$

and sends it to Bob.

Similarly, Bob computes his public key P_B as

$$P_B = g(M)^u N g(M)^v = \begin{bmatrix} 19 & 29 \\ 558 & 562 \end{bmatrix},$$

and sends it to Alice.

Step 3: Alice computes S_A as

$$S_A = f(M)^r P_B f(M)^s = \begin{bmatrix} 25 & 26 \\ 589 & 714 \end{bmatrix}.$$

Bob computes S_B as

$$S_B = g(M)^u P_A g(M)^v = \begin{bmatrix} 25 & 26 \\ 589 & 714 \end{bmatrix}.$$

As we established in Theorem 2, the shared secret is $S_A = S_B$.

Note that an attacker knows the element M since it is public, but the elements $f(\mathsf{X}), g(\mathsf{X}) \in \mathcal{Z}(E_{11})[\mathsf{X}]$ remain unknown. Consequently, the following elements are also unknown

$$f(M)^r = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix}^5 = \begin{bmatrix} 1 & 0 \\ 0 & 94 \end{bmatrix} \quad \text{and} \quad f(M)^s = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix}^7 = \begin{bmatrix} 16 & 12 \\ 558 & 8 \end{bmatrix},$$

as well as

$$g(M)^u = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}^9 = \begin{bmatrix} 29 & 4 \\ 186 & 295 \end{bmatrix} \quad \text{and} \quad g(M)^v = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}^0 = \begin{bmatrix} 20 & 1 \\ 527 & 9 \end{bmatrix}.$$

Let us assume that an attacker intercepts P_A and P_B. Firstly, to obtain the shared secret S, he/she should determine the polynomials $f(\mathsf{X})$ and $g(\mathsf{X})$ and, later, obtain the pairs (r, s) and (u, v) from the expressions

$$f(M)^r N f(M)^s = P_A \quad \text{and} \quad g(M)^u N g(M)^v = P_B.$$

This is equivalent to solve two DP problems because (r, s) and (u, v) are unknown. □

E_p	Degree of the polynomial									
p \ n	2	3	4	5	$\cdots$	12	13	$\cdots$	20	$\cdots$
2	12	16	20	24	$\cdots$	52	56	$\cdots$	84	$\cdots$
3	27	36	45	54	$\cdots$	117	126	$\cdots$	189	$\cdots$
5	75	100	125	150	$\cdots$	325	350	$\cdots$	525	$\cdots$
7	147	196	245	294	$\cdots$	637	686	$\cdots$	1029	$\cdots$
11	363	484	605	726	$\cdots$	1573	1694	$\cdots$	2541	$\cdots$
13	507	676	845	1014	$\cdots$	2197	2366	$\cdots$	3549	$\cdots$
17	867	1156	1445	1731	$\cdots$	3757	4046	$\cdots$	6069	$\cdots$
19	1083	1444	1805	2166	$\cdots$	4693	5054	$\cdots$	7581	$\cdots$
23	1587	2116	2645	3174	$\cdots$	6877	7406	$\cdots$	11109	$\cdots$
29	2523	3364	4205	5046	$\cdots$	10933	11774	$\cdots$	17661	$\cdots$
31	2883	3844	4805	5766	$\cdots$	12493	13454	$\cdots$	20181	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	
97	28227	37636	47045	56454	$\cdots$	122317	131726	$\cdots$	197589	$\cdots$
101	30603	40804	51005	61206	$\cdots$	132613	142814	$\cdots$	214221	$\cdots$
103	31827	42436	53045	63654	$\cdots$	137917	148526	$\cdots$	222789	$\cdots$
107	34347	45796	57245	68694	$\cdots$	148837	160286	$\cdots$	240429	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	

Table 1: Number of polynomials for different degrees n and primes p

We could think on a brute force attack on the set of polynomials with coefficients in the center of the ring. However, an attack of this type is not feasible since the number of polynomials of degree n and coefficients in $\mathcal{Z}(E_p)$, is $(n+1)p^2$. It is enough to take n or p sufficiently large. For example, if we consider $n = 20$ and a prime number p of about 60 decimal digits (these requirements are not too high), the number of polynomials to consider is of the order of 10^{121}. Table 1 shows the values of $(n+1)p^2$ for different values of n and p.

Note that Protocol 2 presents some symmetry in the sense that Alice and Bob uses the same polynomial to multiply element N, both on the right and on the left. To avoid this symmetry we introduce two polynomials for each user in the following protocol.

Protocol 3: The elements $M \in R$, $N \in R \setminus \mathcal{Z}(R)$, are public.

Step 1: Alice chooses her private key $f_1(\mathsf{X}), f_2(\mathsf{X}) \in \mathcal{Z}(R)[\mathsf{X}]$ and $r, s \in \mathbb{N}$.

Bob chooses his private key $g_1(\mathsf{X}), g_2(\mathsf{X}) \in \mathcal{Z}(R)[\mathsf{X}]$ and $u, v \in \mathbb{N}$.

Step 2: Alice computes her public key $P_A = f_1(M)^r N f_2(M)^s$ and sends it to Bob.

Similarly, Bob computes his public key $P_B = g_1(M)^u N g_2(M)^v$, and sends it to Alice.

Step 3: Alice and Bob compute S_A and S_B, respectively, as

$$S_A = f_1(M)^r P_B f_2(M)^s \quad \text{and} \quad S_B = g_1(M)^u P_A g_2(M)^v.$$

Following a similar argument as in Protocol 2, it follows that $S_A = S_B$. □

In the next example, we show how to share a secret using the above protocol.

Example 2: We consider again the elements M and N of E_{31} as in Example 1.

Step 1: Alice chooses her private key $(r, s) = (5, 7)$ and $f_1(\mathsf{X})$, $f_2(\mathsf{X})$ as

$$f_1(\mathsf{X}) = \begin{bmatrix} 15 & 0 \\ 0 & 77 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 777 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 17 & 0 \\ 0 & 482 \end{bmatrix} \mathsf{X}^4 \in \mathcal{Z}(E_{31})[\mathsf{X}],$$

$$f_2(\mathsf{X}) = \begin{bmatrix} 7 & 0 \\ 0 & 472 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 12 & 0 \\ 0 & 508 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & 0 \\ 0 & 869 \end{bmatrix} \mathsf{X}^6 \in \mathcal{Z}(E_{31})[\mathsf{X}].$$

Then, $f_1(M) = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix}$ and $f_2(M) = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}$.

Bob chooses his private key $(u, v) = (9, 8)$ and $g_1(\mathsf{X})$, $g_2(\mathsf{X})$ as

$$g_1(\mathsf{X}) = \begin{bmatrix} 9 & 0 \\ 0 & 71 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 713 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 26 & 0 \\ 0 & 181 \end{bmatrix} \mathsf{X}^4 + \begin{bmatrix} 13 & 0 \\ 0 & 292 \end{bmatrix} \mathsf{X}^5 \in \mathcal{Z}(E_{31})[\mathsf{X}],$$

$$g_2(\mathsf{X}) = \begin{bmatrix} 21 & 0 \\ 0 & 300 \end{bmatrix} + \begin{bmatrix} 4 & 0 \\ 0 & 531 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 30 & 0 \\ 0 & 61 \end{bmatrix} \mathsf{X}^3 + \begin{bmatrix} 14 & 0 \\ 0 & 262 \end{bmatrix} \mathsf{X}^4 \in \mathcal{Z}(E_{31})[\mathsf{X}].$$

Then, $g_1(M) = \begin{bmatrix} 27 & 24 \\ 155 & 817 \end{bmatrix}$ and $g_2(M) = \begin{bmatrix} 20 & 3 \\ 620 & 886 \end{bmatrix}$.

Step 2: Alice computes her public key P_A as

$$P_A = f_1(M)^r N f_2(M)^s = \begin{bmatrix} 2 & 3 \\ 341 & 826 \end{bmatrix},$$

and sends it to Bob.

Similarly, Bob computes his public key P_B as

$$P_B = g_1(M)^u N g_2(M)^v = \begin{bmatrix} 4 & 1 \\ 217 & 522 \end{bmatrix},$$

and sends it to Alice.

Step 3: Alice computes S_A as

$$S_A = f_1(M)^r P_B f_2(M)^s = \begin{bmatrix} 6 & 5 \\ 682 & 957 \end{bmatrix}.$$

Bob computes S_B as

$$S_B = g_1(M)^u P_A g_2(M)^v = \begin{bmatrix} 6 & 5 \\ 682 & 957 \end{bmatrix}.$$

Then, the shared secret is $S_A = S_B$.

E_{31}	Degree of the polynomials									
m \ n	4	6	8	10	12	14	16	18	20	$\cdots$
3	18470420	25858588	33246756	40634924	48023092	55411260	62799428	70187596	77575764	$\cdots$
5	27705630	38787882	49870134	60952386	72034638	83116890	94199142	105281394	116363646	$\cdots$
7	36940840	51717176	66493512	81269848	96046184	110822520	125598856	140375192	155151528	$\cdots$
9	46176050	64646470	83116890	101587310	120057730	138528150	156998570	175468990	193939410	$\cdots$
11	55411260	77575764	99740268	121904772	144069276	166233780	188398284	210562788	232727292	$\cdots$
13	64646470	90505058	116363646	142222234	168080822	193939410	219797998	245656586	271515174	$\cdots$
15	73881680	103434352	132987024	162539696	192092368	221645040	251197712	280750384	310303056	$\cdots$
17	83116890	116363646	149610402	182857158	216103914	249350670	282597426	315844182	349090938	$\cdots$
19	92352100	129292940	166233780	203174620	240115460	277056300	313997140	350937980	387878820	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Table 2: Number of polynomials for different values of the degrees for $p = 31$

Note that an attacker knows M since it is public, but $f_1(\mathsf{X}), f_2(\mathsf{X}), g_1(\mathsf{X}), g_2(\mathsf{X}) \in \mathcal{Z}(E_{31})[\mathsf{X}]$ remain unknown. Consequently,

$$f_1(M)^r = \begin{bmatrix} 1 & 0 \\ 0 & 94 \end{bmatrix} \quad \text{and} \quad f_2(M)^s = \begin{bmatrix} 17 & 15 \\ 217 & 162 \end{bmatrix},$$

are unknown, as well as

$$g_1(M)^u = \begin{bmatrix} 23 & 0 \\ 0 & 178 \end{bmatrix} \quad \text{and} \quad g_2(M)^v = \begin{bmatrix} 19 & 18 \\ 837 & 751 \end{bmatrix}.$$

Following a similar argument as for Protocol 2, an attacker who wants to discover the shared secret must obtain, firstly, the polynomials $f_1(\mathsf{X})$, $f_2(\mathsf{X})$, $g_1(\mathsf{X})$, and $g_2(\mathsf{X})$ and later to find (r, s) and (u, v) from the expressions

$$f_1(M)^r N f_2(M)^s = P_A \quad \text{and} \quad g_1(M)^u N g_2(M)^v = P_B.$$

This is equivalent to solve two DP problems. □

In this protocol a user needs two polynomials with degrees m and n, respectively; therefore the number of possible polynomials becomes $(m+1)(n+1)p^4$. Note that for a prime number p of about 60 decimal digits (as in the previous case) and for $m = 9$ and $n = 10$ the number of polynomials that an attacker must consider is of the order of 10^{242}. Table 2 shows the values of $(m+1)(n+1)p^4$ for different values of m, n and p.

5 Security analysis of the proposed protocols

In this section we discuss some possible attacks on the protocols introduced in Section 4, briefly explaining the reasons why those attacks will ever be successful. Let us note first that classic attacks on finite fields, like Index-Calculus, Square Root, Quadratic Sieve or Number

Field Sieve are not feasible in these protocols because the underlying structure is a finite noncommutative ring. Furthermore, given that for any prime number p, the ring E_p is not Euclidean, then $\mathcal{Z}(E_p)$ is not Euclidian either, any attack based on the use of the Euclidean division can never be applicable here. See, for example, the attack proposed by Dubois and Kammerer [13] for the protocols designed by Boucher *et al.* [7].

As we have already mentioned in Section 4, the security of the protocols are based on the difficulty posed to solve the DP problem, for which no polynomial-time probabilistic algorithm capable of solving this problem in a noncommutative ring is known. In our case, for each protocol, an attacker needs to solve the DP problem by solving the following system of equations

$$X_A X_B = X_B X_A, \tag{2}$$
$$Y_A Y_B = Y_B Y_A, \tag{3}$$
$$X_A N Y_A = P_A, \tag{4}$$
$$X_B N Y_B = P_B, \tag{5}$$

being P_A and P_B the public keys of Alice and Bob, respectively. The elements $M \in R$, $N \in R \setminus \mathcal{Z}(R)$ are also known by an attacker.

The first aim of an adversary to break Protocol 2 is to find the elements X_A, X_B, Y_A and Y_B. To perform this task, the attacker will try to find two polynomials $h_1(\mathsf{X}), h_2(\mathsf{X}) \in \mathcal{Z}(R)[\mathsf{X}]$ and natural numbers $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}$ such that

$$h_1(M)^{\alpha_1} = X_A, \quad h_1(M)^{\alpha_2} = Y_A \qquad \text{and} \qquad h_2(M)^{\beta_1} = X_B, \quad h_2(M)^{\beta_2} = Y_B.$$

Then, conditions (2) and (3) are guaranteed. Note that the number of polynomials with coefficients in the center of R determines a set of possible combinations of choice. At this point the attacker should also check conditions (4) and (5). This leads to a brute force attack, which is not feasible if the set of polynomials with coefficients in the center is large enough.

Analogously, for Protocol 3 the attacker should find the elements X_A, X_B, Y_A and Y_B. Therefore, it is neccesary to find two pairs of polynomials $h_1(\mathsf{X}), k_1(\mathsf{X}), h_2(\mathsf{X}), k_2(\mathsf{X}) \in \mathcal{Z}(R)[\mathsf{X}]$ and natural numbers $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}$ such that

$$h_1(M)^{\alpha_1} = X_A \quad k_1(M)^{\alpha_2} = Y_A \qquad \text{and} \qquad h_2(M)^{\beta_1} = X_B \quad k_2(M)^{\beta_2} = Y_B.$$

Conditions (2) and (3) are again guaranteed, but the number of polynomials has increased, representing an extra difficulty in case the cardinality of the set of polynomials is large.

Summing up, a brute force attack to the protocols leads us to an attempt to solve a DP problem. To perform this, the only possibility of solving a DP problem is by carrying on a brute force attack on the set of polynomials with coefficients in the center of the ring, which

turns out to be unfeasible if the cardinal of the set of these polynomials is large. In the case of the ring E_p it is enough to consider a prime number p with 60 digits and polynomials with coefficients in the center of E_p with degree 10, as we mentioned for each protocol in Section 4.

6 Conclusion

In this paper we have shown how noncommutative rings can be used in order to provide protocols that allow a key exchange in a secure manner. More precisely, we give two protocols based on the characterization of the ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, for a prime number p, given by [10] and denoted in this paper by E_p. These protocols enhance Stickel's protocol for key exchange and use polynomials with coefficients in the center of the ring that are part of each user's private key. Thus, an attacker who wants to recover the shared secret must obtain the polynomial $f(\mathsf{X})$ and then solve the equation

$$f(M)^k N f(M)^l = P \tag{6}$$

for (k, l), or obtain the polynomials $f_1(\mathsf{X})$ and $f_2(\mathsf{X})$ and then solve the equation

$$f_1(M)^k N f_2(M)^l = P \tag{7}$$

for (k, l). Solving equations (6) and (7) are equivalent to solve a DP problem.

Furthermore, as we already mentioned in the preliminaries, the ring E_p is not Euclidean, nor is $\mathcal{Z}(E_p)$. So the ring of polynomials with coefficients in $\mathcal{Z}(E_p)$ is not Euclidean. Therefore attacks based on the existence of an Euclidean division in a noncommutative ring, are not viable in this case.

Acknowledgements

The authors are very grateful to the anonymous reviewers for their comments and suggestions which have led to significant improvements.

References

[1] R. Álvarez, L. Tortosa, J. Vicent and A. Zamora. A non-abelian group based on block upper triangular matrices with cryptographic applications. In M. Bras-Amorós and T. Høholdt (editors), *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, volume 5527 of *Lecture Notes in Computer Science*, pages 117–126. Springer-Verlag, Berlin, 2009.

[2] R. Álvarez, L. Tortosa, J.-F. Vicent and A. Zamora. Analysis and design of a secure key exchange scheme. *Information Sciences*, **179**: 2014–2021 (2009).

[3] I. Anshel, M. Anshel, B. Fisher and D. Goldfeld. New key agreement protocols in braid group cryptography. In D. Naccache (editor), *Topics in Cryptology – CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 13–27. Springer-Verlag, Berlin, 2001.

[4] I. Anshel, M. Anshel and D. Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, **6**: 1–5 (1999).

[5] G. M. Bergman. Some examples in PI ring theory. *Israel Journal of Mathematics*, **18**: 257–277 (1974).

[6] D. Boneh and R. J. Lipton. Quantum cryptanalysis of hidden linear functions. In D. Coppersmith (editor), *Advances in Cryptology – CRYPT0 '95*, volume 963 of *Lecture Notes in Computer Science*, pages 424–437. Springer-Verlag, Berlin, 1995.

[7] D. Boucher, P. Gaborit, W. Geiselmann, O. Ruatta and F. Ulmer. Key exchange and encryption schemes based on non-commutative skew polynomials. In N. Sendrier (editor), *Post-Quantum Cryptography*, volume 6061 of *Lecture Notes in Computer Science*, pages 126–141. Springer-Verlag, Berlin, 2010.

[8] J.-J. Climent, F. Ferrández, J.-F. Vicent and A. Zamora. A nonlinear elliptic curve cryptosystem based on matrices. *Applied Mathematics and Computation*, **174**: 150–164 (2006).

[9] J.-J. Climent, P. R. Navarro and L. Tortosa. Key exchange protocols over non-commutative rings. The case $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. In J. Vigo Aguiar (editor), *Proceedings of the 11th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2011)*, pages 357–364. 2011.

[10] J.-J. Climent, P. R. Navarro and L. Tortosa. On the arithmetic of the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *Applicable Algebra in Engineering, Communication and Computing*, **22(2)**: 91–108 (2011).

[11] D. Coppersmith. Weakness in quaternion signatures. *Journal of Cryptology*, **14(2)**: 77–85 (2001).

[12] W. D. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, **22(6)**: 644–654 (1976).

[13] V. Dubois and J.-G. Kammerer. Cryptanalysis of cryptosystems based on non-commutative skew polynomials. In D. Catalano, N. Fazio, R. Gennaro and

A. Nicolosi (editors), *Public Key Cryptography – PKC 2011*, volume 6571 of *Lecture Notes in Computer Science*, pages 459–472. Springer-Verlag, Berlin, 2011.

[14] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **31(4)**: 469–472 (1985).

[15] C. Gentry. Key recovery and message attacks on NTRU-composite. In B. Pfitzmann (editor), *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 182–194. Springer-Verlag, Berlin, 2001.

[16] C. Gentry and M. Szydlo. Cryptanalysis of the revised NTRU signature scheme. In L. Knudsen (editor), *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320. Springer-Verlag, Berlin, 2002.

[17] J. Hoffstein, J. Pipher and J. H. Silverman. NTRU: a ring-based public key cryptosystem. In J. P. Buhler (editor), *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer-Verlag, Berlin, 1998.

[18] B. Hurley and T. Hurley. Group ring cryptography. *International Journal of Pure and Applied Mathematics*, **60(1)**: 67–86 (2011).

[19] K. H. Ko, J. W. Lee and T. Thomas. Towards generating secure keys for braid cryptography. *Designs, Codes and Cryptography*, **45(3)**: 317–333 (2007).

[20] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J.-s. Kang and C. Park. New public-key cryptosystem using braid groups. In M. Bellare (editor), *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 166–183. Springer-Verlag, Berlin, 2000.

[21] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1996.

[22] A. J. Menezes and Y.-H. Wu. The discrete logarithm problem in $GL(n, q)$. *Ars Combinatoria*, **47**: 23–32 (1997).

[23] A. G. Myasnikov, V. Shpilrain and A. Ushakov. *Group-based cryptography*. Birkhäuser Verlag, Basel, Switzerland, 2008.

[24] R. W. K. Odoni, V. Varadharajan and P. W. Sanders. Public key distribution in matrix rings. *Electronics Letters*, **20**: 386–387 (1984).

[25] S.-H. Paeng, K.-C. Ha, J. H. Kim, S. Chee and C. Park. New public key cryptosystem using finite non abelian groups. In J. Kilian (editor), *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 470–485. Springer-Verlag, Berlin, 2001.

[26] R. L. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21(2)**: 120–126 (1978).

[27] E. Sakalauskas and T. Burba. Basic semigroup primitive for cryptographic session key exchange protocol (SKEP). *Information Technology and Control*, **28(3)**: 76–80 (2003).

[28] T. Satoh and K. Araki. On construction of signature scheme over a certain noncommutative ring. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E80-A(1)**: 40–45 (1997).

[29] B. Schneier. *Applied Cryptography.* John Wiley & Sons, New York, NY, second edition, 1996.

[30] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, **26(5)**: 1484–1509 (1997).

[31] V. Shpilrain. Cryptanalysis of Stickel's key exchange scheme. In E. A. Hirsch, A. A. Razborov, A. Semenov and A. Slissenko (editors), *Computer Science – Theory and Applications*, volume 5010 of *Lecture Notes in Computer Science*, pages 283–288. Springer-Verlag, Berlin, 2008.

[32] V. Shpilrain and A. Ushakov. A new key exchange protocol based on the decomposition problem. *Contemporary Mathematics*, **418**: 161–167 (2006).

[33] V. M. Sidelnikov, M. A. Cherepnev and V. V. Yashchenko. Systems of open distribution of keys on the basis of noncommutative semigroups. *Russian Academy of Sciences. Doklady Mathematics*, **48(2)**: 384–386 (1994).

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

[35] D. R. Stinson. *Cryptography. Theory and Practice.* CRC Press, Boca Raton, FL, 1995.

[36] T. Thomas and A. K. Lal. A zero-knowledge undeniable signature scheme in non-abelian group setting. *International Journal of Network Security*, **6(3)**: 265–269 (2008).

[37] V. Varadharajan and R. W. K. Odoni. Security of public key distribution in matrix rings. *Electronics Letters*, **22**: 46–47 (1986).

[38] H. Yoo, S. Hong, S. Lee, J. Lim, O. Yi and M. Sung. A proposal of a new public key cryptosystem using matrices over a ring. In E. Dawson, A. Clark and C. Boyd (editors), *Information Security and Privacy*, volume 1841 of *Lecture Notes in Computer Science*, pages 41–48. Springer-Verlag, Berlin, 2000.