This is a previous version of the article published in Advances in Mathematics of Communications. 2016, 10(4): 861-870. doi:10.3934/amc.2016046s

Public Key Protocols over the Ring $E_p^{(m)}$

Joan-Josep Climent[*],
Juan Antonio López-Ramos[†],

June 20, 2016

Abstract

In this paper we use the nonrepresentable ring $E_p^{(m)}$ to introduce public key cryptosystems in noncommutative settings and based on the Semigroup Action Problem and the Decomposition Problem respectively.

1 Introduction

Most public-key cryptosystems are based on certain specific problems of number theory. One of these problems is the *Integer Factorization Problem* (IFP) over the ring $\mathbb{Z}_n$, being n the product of two large prime numbers; the well known cryptosystem RSA [22] is based in 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 Diffie-Hellman key exchange protocol [9] and ElGamal protocol [10] are based on this problem. In general, we can say that their robustness depends on the computational difficulty of solving certain mathematical problems over finite commutative algebraic structures. Some efficient attacks based on the commutative property of these structures are well known: Quadratic Sieve, General Number Field Sieve, Pollard's rho algorithm, Index-Calculus, etc. (see, for example, [19, 28], and the references within these books).

This fact, together with the increase of the computational power of modern computers, has made these techniques become more and more insecure. As a result there exists an active field of research known as noncommutative algebraic cryptography (see, for example, [2, 12, 13, 23, 26]) aiming to develop and analyse new cryptosystems and key

[*] Departament de Matemàtiques, Universitat d'Alacant, email: jcliment@ua.es
[†] Departamento de Matemáticas, Universidad de Almería, email: jlopez@ual.es

exchange protocols based on noncommutative cryptographic platforms. A very good exposition of the problems underlying in this noncommutative approach can be found in [20] and some of them are the following, where G is a nonabelian group:

- *Conjugator Search Problem (CSP):* Given $(x, y) \in G \times G$, the problem is to find $z \in G$ such that $y = z^{-1}xz$.
- *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 $y = z_1 x z_2$.
- *Symmetrical 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 $y = z^m x z^n$.
- *Generalized Symmetrical 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 $y = z^m x z^n$.

Note that for the DP we can assume that G is a semigroup, since in this case we do not need invertible elements.

Several authors have proposed and used certain nonabelian groups for key exchange problems. In [1, 2, 12, 13], the authors suggest to use braid groups as platform groups for their respective protocols. In [21], the authors propose a public key cryptosystem whose security is based on the DLP for the automorphism defined by the conjugation operation and the difficulty to find the conjugate element on finite nonabelian groups. In [24], the authors suggest the use of a finite representation of a nonabelian group, called Thomson's group, to develop a public key cryptosystem, where they raised for the first time the difficulty to find a solution for the SDP. Finally, in [29], the authors propose a cryptosystem whose robustness is based on the difficulty to solve the CSP and SDP over any noncommutative algebraic structure.

In the noncommutative setting, we can find different implementations based on the Diffie-Hellman protocol in matrix rings, for different kind of matrices [4, 27, 30]. A detachable recent work in this setting is [16] where the author shows the usability of a certain class of matrices that arise a noncommutative framework to define the ElGamal cryptosystem and the corresponding Diffie-Hellman protocol as well as its eficiency. Another system based on the discrete logarithm problem in the authomorphisms group is the so-called MOR cryptosystem, recently described for authomorphisms of p-groups whose order is coprime to p in [15, 17].

Moreover, the idea to develop systems of open distribution keys as well as session key exchange protocols, on the basis of noncommutative (semi)groups, is present in [14, 23, 26].

Finally, with the idea to generalize the protocols based on groups and take advantage of the difficulty of to solve the DLP in these groups, Shpilrain and Zapata in [25] give a general framework using actions of groups to define key exchange protocols. In this setting, Maze *et al.* [18] introduce the *Semigroup Action Problem* (SAP) as:

> Let G be a finite semigroup acting on a finite set S. Given $x, y \in S$ with $y = g \cdot x$ for some $g \in G$, find $h \in G$ such that $y = h \cdot x$.

In this way, any Abelian semigroup G acting on a finite set S provides a Diffie-Hellman key exchange protocol and an ElGamal protocol (cf. [18]).

Our aim in this paper is to provide public key cryptosystems in a noncommutative setting given by the ring $E_p^{(m)}$ based on the SAP and DP. The remainder of this paper is organized as follows. In Section 2 we remind some properties of the nonrepresentable ring $E_p^{(m)}$ that will be used through this paper. In Section 3 we use an action of the ring $E_p^{(m)}$ to introduce a public key cryptosystem based on the SAP. Finally, in Section 4 we use this ring to give a public key cryptosystem based on the DP and we relate security of both introduced cryptosystems.

2 The ring $E_p^{(m)}$

Bergman [3] proved that $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a semilocal ring that cannot be embedded in matrices over any commutative ring. In [6] the authors showed that $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is isomorphic to a ring whose elements can be expressed as square matrices whose rows are given by elements in $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ respectively and with an arithmetic that is similar to matrix addition and multiplication. Then they use this ring to define a key exchange protocol (see also [5, 7]). However this was cryptoanalyzed in [11] using some invertible elements, which motivated the introduction of an extension of such a ring [8] such that almost all elements are noninvertible

This new ring is defined as the set (see [8, Theorem 1])

$$E_p^{(m)} = \left\{ [a_{ij}] \in \mathrm{Mat}_{m\times m}(\mathbb{Z}) \mid a_{ij} \in \mathbb{Z}_{p^i} \text{ if } i \leq j, \text{ and } a_{ij} \in p^{i-j}\mathbb{Z}_{p^j} \text{ if } i > j \right\}$$

with the addition and the multiplication defined, respectively, as follows

$$\begin{aligned} [a_{ij}] + [b_{ij}] &= \left[(a_{ij} + b_{ij}) \bmod p^i \right], \\ [a_{ij}] \cdot [b_{ij}] &= \left[\left(\sum_{k=1}^{m} a_{ik} b_{kj} \right) \bmod p^i \right]. \end{aligned}$$

Here $\mathrm{Mat}_{m\times m}(\mathbb{Z})$ denotes the set of $m \times m$ matrices with entries in $\mathbb{Z}$, and $p^r\mathbb{Z}_{p^s}$ denotes the set $\{p^r u \mid u \in \mathbb{Z}_{p^s}\}$ for positive integers r y s. Moreover, $\left|E_p^{(m)}\right| = p^{(2m^3+3m^2+m)/6}$.

The following results on the ring $E_p^{(m)}$ can be found in [8].

Theorem 1 (Theorem 3 of [8]): *Let $A = [a_{ij}] \in E_p^{(m)}$. Then A is invertible if and only if $a_{ii} \not\equiv_p 0$ for every $i = 1, 2, \ldots, m$.*

As a consequence, the number of invertible elements in $E_p^{(m)}$ is $p^{(2m^3+3m^2-5m)/6}$ (see [8, Corollary 1]). Moreover, the fraction of invertible elements in $E_p^{(m)}$ is $\left(\frac{p-1}{p}\right)^m$. So, an adequate election of p and m may result that the number of invertible elements in $E_p^{(m)}$ is almost zero (see [8, Tables 1 and 2]).

Another needed property is the characterization of the center of the ring $E_p^{(m)}$. The following result provides such a characterization.

Theorem 2 (Page 359 of [8]): *The center of $E_p^{(m)}$ is given by the set*

$$Z(E_p^{(m)}) = \left\{ [a_{ij}] \in E_p^{(m)} \mid a_{ii} = \sum_{j=0}^{i-1} p^j u_j,\ \textit{with } u_j \in \mathbb{Z}_p \textit{ and } a_{ij} = 0 \textit{ if } i \neq j \right\}.$$

As a consequence the number of central elements in $E_p^{(m)}$ is p^m.

3 A public key cryptosystem based on the SAP

Our aim in this section is to use the arithmetic of the ring $E_p^{(m)}$ and an action of this ring to define a public key cryptosystem in a noncommutative setting.

Thus, based on the multiplication defined on the ring $E_p^{(m)}$ and the structure of its elements we may define an action of the ring $E_p^{(m)}$ over the set $\mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$. As we will show, this action will arise a public key cryptosystem based on the SAP (cf. [18]).

Let us consider the center $Z(E_p^{(m)})$ of the ring $E_p^{(m)}$. For a given $M \in E_p^{(m)}$, let $\mathrm{Cen}(M)$ be the set of elements X in $E_p^{(m)}$ such that $XM = MX$. The algorithm is given by the following

Algorithm 1: *Let $M \in E_p^{(m)}$ be a public value and $S \in \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$ the message that Bob wants to send Alice. Then:*

1. *Alice chooses $R \in \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$, $F \in \mathrm{Cen}(M)$ and computes $T = F \cdot R$.*
2. *Alice makes public the pair (R, T), keeping secret her private key F.*

3. *Bob chooses randomly* $G = \sum_{i=0}^{k} C_i M^i$, *where* $C_i \in Z(E_p^{(m)})$ *and sends Alice the pair* $(H, D) = (G \cdot R, S + G \cdot T)$.

4. *Alice gets the secret by computing* $S = D - F \cdot H$.

Note that the commutativity of F and G gives the correctness of the preceding algorithm and that Alice and Bob could exchange the way they choose the elements appearing through it.

As it is asserted in the general case in [18] we can observe that breaking the preceding algorithm involves solving the SAP, i.e., given the values R and $T = F \cdot R \in \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$, find $A \in E_p^{(m)}$ such that $T = A \cdot R$.

To understand the size of the underlying SAP, let p be a prime, consider $x \in \mathbb{Z}_{p^m}$ coprime to p, and let n be the order of x. Now let $M = [a_{ij}]$ be the element of $E_p^{(m)}$ given by

$$a_{ij} = \begin{cases} x, & \text{for } i = j = m, \\ 0, & \text{otherwise.} \end{cases}$$

For $k = 1, 2, \ldots$, assume that $M^k = [a_{ij}^{(k)}]$; then

$$a_{ij}^{(k)} = \begin{cases} x^k, & \text{for } i = j = m, \\ 0, & \text{otherwise.} \end{cases}$$

Thus it is clear that $M^{n+1} = M$ and $M, M^2, \ldots, M^n$ are pairwise different. Since $M^0 = I$ (by definition), the elements of $G = \sum_{k=0}^{n} C_k M^k$ are in $\mathrm{Cen}(M)$ and have the form

$$G = \mathrm{diag}\left(c_0^{(0)}, c_0^{(0)} + c_1^{(0)} p, \ldots, \sum_{l=0}^{m-2} c_l^{(0)} p^l, \sum_{l=0}^{m-1} c_l^{(0)} p^l + \sum_{k=1}^{n} \left(\sum_{l=0}^{m-1} c_l^{(k)} p^l\right) x^k\right) \tag{1}$$

where, by Theorem 2,

$$C_k = \mathrm{diag}\left(c_0^{(k)}, c_0^{(k)} + c_1^{(k)} p, \ldots, \sum_{l=0}^{m-2} c_l^{(k)} p^l, \sum_{l=0}^{m-1} c_l^{(k)} p^l\right).$$

Thus, accordingly to expression (1), for every possible choice of the element

$$C_0 = \mathrm{diag}\left(c_0^{(0)}, c_0^{(0)} + c_1^{(0)} p, \ldots, \sum_{l=0}^{m-2} c_l^{(0)} p^l, \sum_{l=0}^{m-1} c_l^{(0)} p^l\right)$$

in $Z(E_p^{(m)})$, there are as many elements G as the number of elements of the set

$$\left\{ \sum_{l=0}^{m-1} c_l^{(0)} p^l + \sum_{k=1}^{n} \left(\sum_{l=0}^{m-1} c_l^{(k)} p^l\right) x^k \mid C_1, \ldots, C_n \in Z(E_p^{(m)}) \right\}. \tag{2}$$

We point out that in the preceding expression, $C_1, \ldots, C_n$ are not necessarily distinct and many of them could be the zero element in $E_p^{(m)}$.

But the set given in expression (2) may be expressed as

$$\left\{ \sum_{l=0}^{m-1} c_l^{(0)} p^l + \sum_{l=0}^{m-1} \left(\sum_{k=1}^{n} c_l^{(k)} x^k \right) p^l \mid C_1, \ldots, C_n \in Z(E_p^{(m)}) \right\}$$

which gives all the elements of $\mathbb{Z}_{p^m}$ given that $C_1, \ldots, C_n$ may be chosen in such a way that we get the p-adic decomposition of every element in $\mathbb{Z}_{p^m}$. Therefore, for every element in $Z(E_p^{(m)})$, there are as many elements G as elements in $\mathbb{Z}_{p^m}$, which results that we have $p^m \cdot p^m = p^{2m}$ different possibilities to select the element G.

An analogous result is obtained for $M = [a_{ij}]$ with

$$a_{ij} = \begin{cases} x, & \text{for } i = j = m, \\ y p^{m-1}, & \text{for } i = m \text{ and } j = 1, \\ 0, & \text{otherwise.} \end{cases}$$

and $y \in \mathbb{Z}_p$ is an element of order $p - 1$.

On the other hand, in [18] the authors show that the nearest the semigroup acting on the corresponding set is to be a group, i.e. the bigger the subgroup of units in the semigroup is, the easier is to develop a Polling-Hellman algorithm in the semigroup to compute the corresponding discrete logarithm. In this case, as it was noted previously, the set of noninvertible elements in $E_p^{(m)}$ might be very close to the whole semigroup with an adequate election of p and m.

An additional property of the preceding algorithm is the use of a different G for every encryption. In ElGamal cryptosystem [10] the election of a random parameter in every encryption avoids an attack based on a pair plain text-encrypted text, given the existence of invertible elements. The same idea cannot be developed in this case due to the almost nonexistence of invertible elements. As in ElGamal case, the election of a different G in every encryption avoids repetition attacks.

Now let (R, T) be a public key, with $T = F \cdot R$, where $F \in \mathrm{Cen}(M)$, and let A be a solution of the SAP, i.e., $A \cdot R = T$. Suppose also that G in step 3 of Algorithm 1 is such that $AG = GA$. Then, given the encrypted message

$$(H, D) = (G \cdot R, S + G \cdot T)$$

we have that

$$S + G \cdot T - (AG) \cdot R = S + (GA) \cdot R - (AG) \cdot R = S.$$

Thus it is crucial that the element G in step 3 of Algorithm 1 does not commute with the solution A of the SAP. Therefore to avoid that G commute with any such solution, we must require that G is not in the center of the multiplicative semigroup of $E_p^{(m)}$, which can be easily checked by requiring that there exists at least a nonzero element out of its main diagonal (see Theorem 2).

Then suppose that an attacker tries to find $A \in Z(E_p^{(m)})$ being a solution of the SAP, i.e., $A \cdot R = T$. Thus, again, according to Theorem 2, A must be of the form

$$A = \operatorname{diag}\left(a_0, a_0 + a_1 p, \ldots, \sum_{j=0}^{m-2} a_j p^j, \sum_{j=0}^{m-1} a_j p^j\right), \tag{3}$$

with $a_j \in \mathbb{Z}_p$ for every $j = 0, 1, 2, \ldots, m-1$.

Theorem 3: *Assume that*

$$R = (r_0, r_1, \ldots, r_{m-1}) \quad \textit{and} \quad T = (t_0, t_1, \ldots, t_{m-1})$$

are elements in $\mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$ *such that* $A \cdot R = T$. *If* $r_j \not\equiv_p 0$ *for* $j = 0, 1, 2, \ldots, m-1$ *then*

$$r_0^{-1} t_0 \equiv_p r_1^{-1} t_1 \equiv_p \cdots \equiv_p r_{m-1}^{-1} t_{m-1}.$$

Proof: Since $A \cdot R = T$ it follows that

$$a_0 r_0 \equiv_p t_0, \tag{4}$$

$$(a_0 + p a_1 + \cdots + p^j a_j) r_j \equiv_{p^{j+1}} t_j, \quad \text{for } j = 1, 2, \ldots, m-1. \tag{5}$$

Now, from expression (4) and the fact that $r_0 \not\equiv_p 0$, we obtain that $a_0 \equiv_p r_0^{-1} t_0$.

Assume now that $j = 1, 2, \ldots, m-1$. From expression (5) we have that

$$(a_0 + p a_1 + \cdots + p^j a_j) r_j - t_j = p^{j+1} h, \quad \text{for some } h \in \mathbb{Z},$$

so, $p \mid (t_j - a_0 r_j)$. Therefore, $a_0 r_j \equiv_p t_j$ and using the fact that $r_j \not\equiv_p 0$, we obtain that $a_0 \equiv_p r_j^{-1} t_j$. □

As an immediate consequence we get the following result.

Corollary 1: *Let* $F \in E_p^{(m)}$ *as in Algorithm 1 defining a public key* (R, T), *of some user, with* $T = F \cdot R$, *being* $R = (r_0, r_1, \ldots, r_{m-1})$ *and* $T = (t_0, t_1, \ldots, t_{m-1})$ *with* $r_j, t_j \in \mathbb{Z}_{p^{j+1}}$, *for* $j = 0, 1, 2, \ldots, m-1$. *If* $p \nmid r_j$ *for every* $j = 0, 1, 2, \ldots, m-1$ *and there exits* k *such that* $r_k^{-1} t_k \not\equiv_p r_0^{-1} t_0$, *then an attacker cannot compute* $A \in Z(E_p^{(m)})$ *such that* $T = A \cdot R$.

4 A public key cryptosystem based on the DP

Our aim in this section is to give a trap-door function based on the DP in $E_p^{(m)}$ following ElGamal's ideas in the case of the DLP. ElGamal [10] introduced his cryptosystem based on the Diffie-Hellman key exchange protocol [9]. Thus we provide a key exchange in the ring $E_p^{(m)}$ following the CAKE concept introduced in [25, Definition 3].

To do so, given $M \in E_p^{(m)}$, we will consider the set

$$H(M) = \left\{ \sum_{i=0}^{k} C_i M^i \mid C_i \in Z(E_p^{(m)}), k \in \mathbb{Z}^+ \right\} \tag{6}$$

where $Z(E_p^{(m)})$ is the center of the semiring $E_p^{(m)}$ (see Theorem 2) and $\mathbb{Z}^+$ denotes the set of positive integers.

Protocol 1 (DHDP protocol): *Alice and Bob agree on two public elements $X, M \in E_p^{(m)}$ such that $M \notin \mathrm{Cen}(X)$.*

1. *Alice chooses two different elements $A_1, A_2 \in H(M)$ and transmits $G_A = A_1XA_2$ to Bob.*

2. *Bob chooses $B_1, B_2 \in \mathrm{Cen}(M)$ such that $B_1X \neq XB_2$ and transmits $G_B = B_1XB_2$ to Alice.*

3. *Alice computes $A_1G_BA_2$.*

4. *Bob computes $B_1G_AB_2$.*

Now it is clear that both Alice and Bob share a common value and that they could exchange their roles in the way they choose their corresponding private information. The latter is a particular case of [25, Example 3], where the authors illustrate a protocol based on the DP in a general semigroup.

Trying to break the preceding protocol, in its general setting as it is shown in [25, Example 3] gives rise to the following problem directly related to the DP.

Definition 1: Let G be a semigroup, $A, B \subseteq G$ two subsemigroups such that $ab = ba$ for every $a \in A$ and $b \in B$ and assume that $x \in G$. The **DH Decomposition Problem (DHDP)** consists in given two elements a_1xa_2 and b_1xb_2, with $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that provide a DHDP key exchange as above, find the element $a_1b_1xb_2a_2$.

It is immediate that being able to solve the DP implies that we will be able to solve the DHDP.

On the other hand, in [6] (see also [5, 7]) the authors introduce a key exchange protocol over the noncommutative ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ that fits with the previous protocol. In [11] the authors solve the DHDP problem using some invertible elements in $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ resulting a cryptanalysis of that proposal.

From the key exchange based on the DP, and analogously to the ElGamal cryptosystem, we can derive a public key cryptosystem whose cryptanalysis is computationally equivalent to the DHDP. We will give it in a general setting for semigroups, but let us introduce first the following notation. Let $t \in \mathbb{Z}^+$ and consider a one-to-one map $\beta : G \longrightarrow \mathbb{Z}_2^t$; so, for $x \in G$, $\beta(x)$ is the binary representation of t digits of x. Moreover, we denote by $\oplus$ the bitwise xor operation in $\mathbb{Z}_2^t$.

Protocol 2 (ElGamal DP protocol (EGDP protocol)): *Let G be a semigroup and assume that $A, B \subseteq G$ are two subsemigroups such that $ab = ba$ for every $a \in A$ and $b \in B$. Let m be the message that Bob desires to send Alice.*

1. *Alice chooses $x \in G$ such that $xa \neq ax$, for every $a \in A$, and chooses $a_1, a_2 \in A$.*
2. *Alice makes public the pair (x, a_1xa_2).*
3. *Bob chooses $b_1, b_2 \in B$ randomly and such that $xb_i \neq b_ix$ for $i = 1, 2$ and sends Alice the pair $(f, d) = (b_1xb_2, \beta^{-1}(\beta(m) \oplus \beta(b_1a_1xa_2b_2))$.*
4. *Alice recovers m by computing $m = \beta^{-1}(\beta(d) \oplus \beta(a_1fa_2))$.*

Part 4 of the above protocol is correct because

$$\begin{aligned}\beta(d) \oplus \beta(a_1fa_2) &= \beta(d) \oplus \beta(a_1b_1xb_2a_2)\\ &= \beta(\beta^{-1}(\beta(m) \oplus \beta(b_1a_1xa_2b_2))) \oplus \beta(a_1b_1xb_2a_2)\\ &= \beta(m) \oplus \beta(b_1a_1xa_2b_2) \oplus \beta(a_1b_1xb_2a_2)\\ &= \beta(m)\end{aligned}$$

since $\beta(b_1a_1xa_2b_2) = \beta(a_1b_1xb_2a_2)$ as $b_ia_i = a_ib_i$ for $i = 1, 2$. Consequently,

$$\beta^{-1}(\beta(d) \oplus \beta(a_1fa_2)) = \beta^{-1}(\beta(m)) = m.$$

We point out that if we are considering a ring R instead of a semigroup G, then we can substitute the map $\beta : G \longrightarrow \mathbb{Z}_2^t$ by the identity map in R and the xor operation $\oplus$ by the addition in R. Here we need the existence of a zero element in order to get $m = d - a_1fa_2$.

Example 1: 1. If the semigroup G is commutative, then we have that EGDP corresponds to the ElGamal public key cryptosystem defined by the action of G over itself (cf. [18]). In this case, as we pointed out in Section 1, the security of the cryptosystem is based on the difficulty of what the authors in [18] called the SAP.

2. Let us consider the ring $E_p^{(m)}$. Then Alice and Bob can agree in a public element $M \in E_p^{(m)}$. Now let $S \in E_p^{(m)}$ be the secret that Bob wants to send Alice. Then S may be sent in a confidential manner in the following way:

   (a) Alice chooses $N \in E_p^{(m)}$ such that $NM \neq MN$ and two elements $A_1, A_2 \in H(M)$ (see equation (6)), and publishes her public key (N, A_1NA_2).

   (b) Bob chooses randomly two other elements $B_1, B_2 \in \mathrm{Cen}(M)$ (or simply $B_1, B_2 \in H(M)$ as Alice) and sends her the pair given by $(F, D) = (B_1NB_2, S + B_1A_1NA_2B_2)$.

   (c) Alice recovers S by computing $D - A_1FA_2$ due to the fact that A_i and B_i commute for $i = 1, 2$. ■

The following result shows the relation between the cryptanalysis of the EGDP and DHDP protocols.

Theorem 4: *Breaking the EGDP protocol is equivalent to solve the DHDP.*

Proof: Assume that Eve can solve the DHDP and she wants to get m from

$$(b_1xb_2, \beta^{-1}(\beta(m) \oplus \beta(b_1a_1xa_2b_2))).$$

Since Eve is able to solve the DHDP, then she gets $b_1a_1xa_2b_2$ from b_1xb_2 and the Alice's public key a_1xa_2. Thus she can recover

$$m = \beta^{-1}(\beta(m) \oplus \beta(b_1a_1xa_2b_2) \oplus \beta(b_1a_1xa_2b_2)).$$

Now assume that Eve can solve the EGDP. Then she can obtain any message m from the information $x, a_1xa_2, b_1xb_2, \beta^{-1}(\beta(m) \oplus \beta(b_1a_1xa_2b_2))$. If Eve wishes to get $b_1a_1xa_2b_2$ from x, a_1xa_2, b_1xb_2, then she encrypts m using b_1xb_2 as random element in step 3 of Protocol 2, to get $d = \beta^{-1}(\beta(m) \oplus \beta(b_1a_1xa_2b_2))$ and thus, she gets the solution to the DHDP. □

Let us show how an analogous reasoning to the one used in the cryptanalysis introduced in [11] may apply to break the EGDP protocol. Let us assume that Bob sends Alice the pair

$$(f, d) = (b_1xb_2, \beta^{-1}(\beta(m) \oplus \beta(b_1a_1xa_2b_2)))$$

as in the EGDP algorithm and that Eve is able to find w_1, w_2 commuting with every element in A and such that $fw_2 = w_1 x$. Suppose also that w_2 is invertible in the semigroup G. Then

$$w_1 a_1 x a_2 w_2^{-1} = a_1 w_1 x w_2^{-1} a_2 = a_1 f a_2$$

and thus $\beta^{-1}(\beta(d) \oplus \beta(w_1 a_1 x a_2 w_2^{-1})) = m$.

Therefore, the further the subgroup of units in G is from being G, the more difficult will be to apply this reasoning to break the EGDP protocol. This applies to the case of $E_p^{(m)}$ since as we mentioned previously, a suitable choice of p and m provides a ring such that almost all its elements are not units.

We will finish this paper by giving some conditions on the public key used for the EGDP protocol in the case of the ring $E_p^{(m)}$ in order to avoid an attack by reducing it to find a solution to a certain SAP.

Let us assume that Alice's public key is given by the pair $(X, A_1 X A_2)$ and let Eve be an attacker. If Eve is able to find $M \in Z(E_p^{(m)})$ such that it is a solution of the SAP $MX = A_1 X A_2$, then Eve may choose $H \in Z(E_p^{(m)})$ and invertible, say

$$H = \operatorname{diag}\left(h_0, h_0 + h_1 p, \ldots, \sum_{l=0}^{m-2} h_l p^l, \sum_{l=0}^{m-1} h_l p^l\right),$$

with $h_0 \not\equiv_p 0$ (cf. [8]). Thus Eve writes $MH^{-1}H$ and gets that

$$A_1 X A_2 = MX = MH^{-1} X H,$$

solving the DP and therefore she solves the DHDP.

As previously noted, the next result gives conditions on the public key of the EGDP protocol that avoid breaking it by reducing the DP to a SAP as above explained. Its proof is a direct application of Corollary 1.

Corollary 2: *In the precedent situation, let (X, P), with $P = A_1 X A_2$, be the public key of some user of the EGDP protocol over the ring $E_p^{(m)}$. If there exists $k = 1, 2, \ldots, m$ such that $X_{i,k} \not\equiv_p 0$ for every $i = 1, 2, \ldots, m$ and there exists j such that $X_{j,k}^{-1} P_{j,k} \not\equiv_p X_{1,k}^{-1} P_{1,k}$, then an attacker cannot break the EGDP by reducing it to solve a SAP over the ring $E_p^{(m)}$.*

Acknowledgments

The authors would like to thank the reviewers their valuable comments as well as some references that helped to enhance the paper.

References

[1] Iris Anshel, Michael Anshel, Benji Fisher, and Dorian Goldfeld. New key agreement protocols in braid group cryptography. In David Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 13–27. Springer-Verlag, Berlin, 2001.

[2] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 6:1–5, 1999.

[3] George M. Bergman. Some examples in PI ring theory. *Israel Journal of Mathematics*, 18:257–277, 1974.

[4] Joan-Josep Climent, Francisco Ferrández, José-Francisco Vicent, and Antonio Zamora. A nonlinear elliptic curve cryptosystem based on matrices. *Applied Mathematics and Computation*, 174:150–164, 2006.

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

[6] Joan-Josep Climent, Pedro R. Navarro, and Leandro 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.

[7] Joan-Josep Climent, Pedro R. Navarro, and Leandro Tortosa. Key exchange protocols over noncommutative rings. The case of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *International Journal of Computer Mathematics*, 89(13–14):1753–1763, 2012.

[8] Joan-Josep Climent, Pedro R. Navarro, and Leandro Tortosa. An extension of the noncommutative Bergman's ring with a large number of noninvertible elements. *Applicable Algebra in Engineering, Communication and Computing*, 25(5):347–361, 2014.

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

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

[11] Abdel Alim Kamal and Amr M. Youssef. Cryptanalysis of a key exchange protocol based on the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *Applicable Algebra in Engineering, Communication and Computing*, 23(3–4):143–149, 2012.

[12] Ki Hyoung Ko, Jang Won Lee, and Tony Thomas. Towards generating secure keys for braid cryptography. *Designs, Codes and Cryptography*, 45(3):317–333, 2007.

[13] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In Mihir Bellare, editor, *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 166–183. Springer-Verlag, Berlin, 2000.

[14] Ayan Mahalanobis. The Diffie-Hellman key exchange and non-abelian nilpotent groups. *Israel Journal of Mathematics*, 165:161–187, 2008.

[15] Ayan Mahalanobis. A simple generalization of the ElGamal cryptosystem to non-abelian groups. *Communications in Algebra*, 36(10):3878–3889, 2008.

[16] Ayan Mahalanobis. Are matrices useful in public-key cryptography? *International Mathematical Forum*, 8(39):1939–1953, 2013.

[17] Ayan Mahalanobis. The MOR cryptosystem and finite p-groups. In Delaram Kahrobaei and Vladimir Shpilrain, editors, *Algorithmic Problems of Group Theory, Their Complexity, and Applications to Cryptography*, volume 633 of *Contemporary Mathematics*, pages 81–95. American Mathematical Society, Providence, RI, 2015.

[18] Gérard Maze, Chris Monico, and Joachim Rosenthal. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, 1(4):489–507, 2007.

[19] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, FL, 1996.

[20] Alexei G. Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Group-based cryptography.* Birkhäuser Verlag, Basel, Switzerland, 2008.

[21] Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik Park. New public key cryptosystem using finite non abelian groups. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 470–485. Springer-Verlag, Berlin, 2001.

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

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

[24] Vladimir Shpilrain and Alexander Ushakov. A new key exchange protocol based on the decomposition problem. *Contemporary Mathematics*, 418:161–167, 2006.

[25] Vladimir Shpilrain and Gabriel Zapata. Combinatorial group theory and public key cryptography. *Applicable Algebra in Engineering, Communication and Computing*, 17(3–4):291–302, 2006.

[26] 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.

[27] Eberhard 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.

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

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

[30] Heajoung Yoo, Seokhie Hong, Sangjin Lee, Jongin Lim, Okyeon Yi, and Maenghee Sung. A proposal of a new public key cryptosystem using matrices over a ring. In Ed Dawson, Andrew Clark, and Colin Boyd, editors, *Information Security and Privacy*, volume 1841 of *Lecture Notes in Computer Science*, pages 41–48. Springer-Verlag, Berlin, 2000.