On the arithmetic of the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$

Joan-Josep Climent Pedro R. Navarro

Leandro Tortosa

Departament de Ciència de la Computació i Intel·ligència Artificial

Universitat d'Alacant

Campus de Sant Vicent del Raspeig

Apartat de correus 99, E–03080 Alacant. Spain

jcliment@ua.es, prnr@alu.ua.es, tortosa@ua.es

November 29, 2010

Abstract

For a prime number p, Bergman (1974) established that $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a semilocal ring with p^5 elements that cannot be embedded in matrices over any commutative ring. We identify the elements of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ with elements in a new set, denoted by E_p, of matrices of size 2×2, whose elements in the first row belong to $\mathbb{Z}_p$ and the elements in the second row belong to $\mathbb{Z}_{p^2}$; also, using the arithmetic in $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$, we introduce the arithmetic in that ring and prove that the ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is isomorphic to the ring E_p. Finally, we present a Diffie-Hellman key interchange protocol using some polynomial functions over E_p defined by polynomial in $\mathbb{Z}[X]$.

1 Introduction

The theoretical foundations for most of the algorithms and protocols used in asymmetric cryptography lie in the intractability in number theory and group theory [6]. On quantum computers, the Discrete Logarithm Problem (DLP) over any group has turned out to be efficiently solved, as we can see in [3, 9].

Cryptographic primitives using more complex algebraic systems rather than traditional finite cyclic groups or finite fields have been proposed in the last decade (see, for example, [1, 4, 7, 8, 10]), and led to a flourishing field of research [12].

In this context, our main objective in this paper is to discuss a characterization of the arithmetic of the ring of endomorphisms $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ in terms of the arithmetic in $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$, for a prime number p.

For a prime number p, Bergman [2] established that the ring of endomorphisms $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a semilocal ring with p^5 elements that cannot be embedded in a ring of matrices over any commutative ring (see Section 2 below). Nevertheless, here we present a characterization of the elements of such ring in terms of some 2×2 matrices, where the elements in the first row belong to $\mathbb{Z}_p$ and the elements in the second row belong to $\mathbb{Z}_{p^2}$, which we refer to as E_p (see Section 3). We also establish the addition and the multiplication of endomorphisms in terms of matrices, taking advantage of the possibilities that matrix arithmetic offers us. In Section 4 we characterize the invertible elements of E_p, in terms of the arithmetic of $\mathbb{Z}_p$ and in Section 5 we count the number of invertible elements of E_p for different values of p. Finally, in Section 6 we introduce a Diffie-Hellman key exchange protocol using some polynomial functions over E_p defined by polynomials in $\mathbb{Z}[X]$.

Recall that $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ is a commutative unitary ring with the addition and multiplication modulo m, that is,

$$x + y = (x + y) \bmod m \quad \text{and} \quad x \cdot y = (xy) \bmod m, \qquad \text{for all } x, y \in \mathbb{Z}_m.$$

Let us assume from now on that p is a prime number and consider the rings $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$. Clearly, we can also assume that $\mathbb{Z}_p \subseteq \mathbb{Z}_{p^2}$, even though $\mathbb{Z}_p$ is not a subring of $\mathbb{Z}_{p^2}$. Then, it follows that notation is utmost important to prevent errors like the following. Suppose that $p = 5$, then

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \quad \text{and} \quad \mathbb{Z}_{5^2} = \{0, 1, 2, 3, \ldots, 23, 24\}.$$

Note that $2, 4 \in \mathbb{Z}_5$ and $2 + 4 = 1 \in \mathbb{Z}_5$; but $2, 4 \in \mathbb{Z}_{5^2}$ equally. However when $2, 4 \in \mathbb{Z}_{5^2}$, $2 + 4 = 6 \in \mathbb{Z}_{5^2}$. Obviously, $1 \neq 6$ in $\mathbb{Z}_{5^2}$. Such error can be easily avoidable if we write, when necessary, $x \bmod p$ and $x \bmod p^2$ to refer the element x when $x \in \mathbb{Z}_p$ and $x \in \mathbb{Z}_{p^2}$, respectively. In this light, the above example could be rewritten as $(2 \bmod 5) + (4 \bmod 5) = 1 \bmod 5$, whereas $(2 \bmod 5^2) + (4 \bmod 5^2) = 6 \bmod 5^2$.

2 The ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$

Consider the additive group $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ of order p^3, where the addition is defined componentwise, and the set $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ of endomorphisms of such additive group. It is well known that $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is a noncommutative unitary ring with the usual addition and composition of endomorphisms, that are defined, for $f, g \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, as

$$(f + g)(x, y) = f(x, y) + g(x, y) \quad \text{and} \quad (f \circ g)(x, y) = f(g(x, y)).$$

The additive and multiplicative identities O and I are defined, obviously, by

$$O(x, y) = (0, 0) \quad \text{and} \quad I(x, y) = (x, y)$$

respectively. The additive identity is also called the null endomorphism.

Te next result not only determines the cardinality of the ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, but also introduces the primary property of such a ring: it cannot be embedded in matrices over any commutative ring.

Theorem 1 (Theorem 3 of [2]) *If p is a prime number, then the ring of endomorphisms $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ has p^5 elements and is semilocal, but cannot be embedded in matrices over any commutative ring.*

Remember that a ring is semilocal if its quotient by its Jacobson radical is semisimple artinian (see, for example [5], for more properties about noncommutative rings).

We now introduce a set of endomorphisms of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ which will allow us to characterize the elements of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ as linear combinations of such endomorphisms with coefficients in $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$.

Let us consider the projections

$$\pi_1 : \mathbb{Z}_p \times \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p \quad \text{and} \quad \pi_2 : \mathbb{Z}_p \times \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_{p^2}$$

that can be extended, in a natural way, to endomorphisms of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, which we continue denoting as π_1 and π_2, respectively, as

$$\pi_1(x,y) = (x,0), \quad \text{and} \quad \pi_2(x,y) = (0,y).$$

Let us also consider the quotient map $\sigma : \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ and the natural immersion $\tau : \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2}$ that we can define, respectively, as

$$\sigma(y) = y \bmod p \quad \text{and} \quad \tau(x) = px.$$

These maps can also be extended, in a natural way, to the endomorphisms of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, which we continue denoting as σ and τ, respectively, as

$$\sigma(x,y) = (y \bmod p, 0), \quad \text{and} \quad \tau(x,y) = (0, px).$$

Theorem 2 *The endomorphisms π_1, π_2, σ and τ satisfy the following identities:*

$$\begin{array}{llll}
\pi_1 \circ \pi_1 = \pi_1, & \pi_1 \circ \pi_2 = O, & \pi_1 \circ \tau = O, & \pi_1 \circ \sigma = \sigma, \\
\pi_2 \circ \pi_1 = O, & \pi_2 \circ \pi_2 = \pi_2, & \pi_2 \circ \tau = \tau, & \pi_2 \circ \sigma = O, \\
\tau \circ \pi_1 = \tau, & \tau \circ \pi_2 = O, & \tau \circ \tau = O, & \tau \circ \sigma = p\pi_2, \\
\sigma \circ \pi_1 = O, & \sigma \circ \pi_2 = \sigma, & \sigma \circ \tau = O, & \sigma \circ \sigma = O,
\end{array}$$

where $p\pi_2$ is the sum of π_2 with itself p times. Furthermore, the additive order of π_1, σ and τ is p, while the additive order of π_2 is p^2.

Proof: Let $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_{p^2}$. According to the definitions of π_1, π_2, σ and τ we have that

$$(\pi_1 \circ \pi_1)(x,y) = \pi_1(\pi_1(x,y)) = \pi_1(x,0) = (x,0) = \pi_1(x,y),$$

$$(\pi_2 \circ \tau)(x,y) = \pi_2(\tau(x,y)) = \pi_2(0,px) = (0,px) = \tau(x,y),$$

$$\begin{aligned}(\tau \circ \sigma)(x,y) &= \tau(\sigma(x,y)) = \tau(y \bmod p, 0) = (0, p(y \bmod p)) = (0,py) \\ &= p(0,y) = p\pi_2(x,y) = (p\pi_2)(x,y),\end{aligned}$$

$$(\sigma \circ \pi_2)(x,y) = \sigma(\pi_2(x,y)) = \sigma(0,y) = (y \bmod p, 0) = \sigma(x,y),$$

therefore, $\pi_1 \circ \pi_1 = \pi_1$, $\pi_2 \circ \tau = \tau$, $\tau \circ \sigma = p\pi_2$ and $\sigma \circ \pi_2 = \sigma$.

The remaining of equalities can be proved in a similar way.

Now, let k be a positive integer. Since

$$(k\pi_1)(x,y) = (kx,0), \quad (k\sigma)(x,y) = (ky,0) \quad \text{and} \quad (k\tau)(x,y) = (0,kpx)$$

we have that $k\pi_1 = O$, $k\sigma = O$ and $k\tau = O$ if and only if $p \mid k$. So, the additive order of π_1, σ and τ is p.

Finally, since

$$(k\pi_2)(x, y) = (0, ky)$$

we have that $k\pi_2 = O$ if and only if $p^2 \mid k$ and therefore, the additive order of π_2 is p^2. $\square$

3 A characterization of the ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$

As a consequence of Theorems 1 and 2, we can establish the following characterization of the elements of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Theorem 3 *If p is a prime number, then*

$$\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) = \{a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ and } d \in \mathbb{Z}_{p^2}\}$$

where π_1, σ, τ and π_2 are the endomorphisms introduced in Section 2.

Proof: Let us assume that $a, b, c \in \mathbb{Z}_p$ and $d \in \mathbb{Z}_{p^2}$. Since $\pi_1, \sigma, \tau, \pi_2 \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ it is evident that

$$a\pi_1 + b\sigma + c\tau + d\pi_2 \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}).$$

Therefore,

$$\{a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ and } d \in \mathbb{Z}_{p^2}\} \subseteq \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}).$$

If, for some $a, b, c, a', b', c' \in \mathbb{Z}_p$ and $d, d' \in \mathbb{Z}_{p^2}$ we have that

$$a\pi_1 + b\sigma + c\tau + d\pi_2 = a'\pi_1 + b'\sigma + c'\tau + d'\pi_2$$

then

$$(a\pi_1 + b\sigma + c\tau + d\pi_2)(1, 0) = (a'\pi_1 + b'\sigma + c'\tau + d'\pi_2)(1, 0)$$

that is, $(a, pc) = (a', pc')$ and, consequently, $a = a'$ and $c = c'$.

Similarly,

$$(a\pi_1 + b\sigma + c\tau + d\pi_2)(0, 1) = (a'\pi_1 + b'\sigma + c'\tau + d'\pi_2)(0, 1)$$

that is, $(b, d) = (b', d')$ and, consequently, $b = b'$ and $d = d'$.

So, we conclude that

$$\mathrm{Card}\left(\{a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ and } d \in \mathbb{Z}_{p^2}\}\right) = p^5$$

and, since by Theorem 1 the cardinality of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is p^5, necessarily

$$\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) = \{a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ and } d \in \mathbb{Z}_{p^2}\}. \quad \square$$

Theorem 1 establishes that the ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ can not be embedded in a ring of matrices over any commutative ring. Nevertheless, we can obtain a matrix representation of the elements of this ring.

Theorem 4 *The set*

$$E_p = \left\{ \begin{bmatrix} a & b \\ pc & d \end{bmatrix} \mid a, b, c \in \mathbb{Z}_p \text{ and } d \in \mathbb{Z}_{p^2} \right\}$$

is a noncommutative unitary ring with addition and multiplication given by

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 + a_2) \bmod p & (b_1 + b_2) \bmod p \\ p(c_1 + c_2) \bmod p^2 & (d_1 + d_2) \bmod p^2 \end{bmatrix} \tag{1}$$

and

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 a_2) \bmod p & (a_1 b_2 + b_1 d_2) \bmod p \\ p(c_1 a_2 + d_1 c_2) \bmod p^2 & (pc_1 b_2 + d_1 d_2) \bmod p^2 \end{bmatrix} \tag{2}$$

respectively.

Proof: The proof is straightforward. □

Given the fact that $\mathbb{Z}_p \subseteq \mathbb{Z}_{p^2}$, we can consider that $E_p \subseteq \mathrm{Mat}_2(\mathbb{Z}_{p^2})$. However, E_p can never be a subring of $\mathrm{Mat}_2(\mathbb{Z}_{p^2})$ according to the above theorem. So, the elements of E_p may well be considered ordinary 2×2 matrices over $\mathbb{Z}_{p^2}$.

Note that the addition and multiplication of the elements of E_p is analogous to the addition and multiplication of 2×2 matrices with elements in $\mathbb{Z}$, with the particularity that the elements of the first row are reduced modulo p while the elements of the second row are reduced modulo p^2.

From Theorem 4, it follows that

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

are the additive and multiplicative identities of E_p, respectively. Moreover, bearing in mind how the opposites in $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ are computed, it is evident that the opposite of the element $\begin{bmatrix} a & b \\ pc & d \end{bmatrix} \in E_p$ is $\begin{bmatrix} p-a & p-b \\ p(p-c) & p^2-d \end{bmatrix} \in E_p$.

We will establish a characterization of the invertible elements of E_p in the following section.

Note that as a consequence of Theorem 3, if $f \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, then there exists a unique 4-tuple $(a, b, c, d) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ such that

$$f = a\pi_1 + b\sigma + c\tau + d\pi_2.$$

Now, using this characterization of the elements of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ we can establish that the ring introduced in Theorem 4 is isomorphic to the endomorphism ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Theorem 5 *The map* $\Phi : \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \longrightarrow E_p$ *defined by*

$$\Phi\left(a\pi_1 + b\sigma + c\tau + d\pi_2\right) = \begin{bmatrix} a & b \\ pc & d \end{bmatrix} \tag{3}$$

is a ring isomorphism.

Proof: That Φ is a bijective map follows from Theorem 3.

Let $f, g \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. As a consequence of Theorems 2 and 3, if

$$f = a_1\pi_1 + b_1\sigma + c_1\tau + d_1\pi_2 \quad \text{and} \quad g = a_2\pi_1 + b_2\sigma + c_2\tau + d_2\pi_2,$$

then

$$\begin{aligned} f + g =& (a_1\pi_1 + b_1\sigma + c_1\tau + d_1\pi_2) + (a_2\pi_1 + b_2\sigma + c_2\tau + d_2\pi_2) \\ =& \left((a_1 + a_2) \bmod p\right) \pi_1 + \left((b_1 + b_2) \bmod p\right) \sigma \\ & + \left((c_1 + c_2) \bmod p\right) \tau + \left((d_1 + d_2) \bmod p^2\right) \pi_2 \end{aligned} \tag{4}$$

and

$$\begin{aligned} f \circ g =& (a_1\pi_1 + b_1\sigma + c_1\tau + d_1\pi_2) \circ (a_2\pi_1 + b_2\sigma + c_2\tau + d_2\pi_2) \\ =& a_1a_2(\pi_1 \circ \pi_1) + a_1b_2(\pi_1 \circ \sigma) + a_1c_2(\pi_1 \circ \tau) + a_1d_2(\pi_1 \circ \pi_2) \\ & + b_1a_2(\sigma \circ \pi_1) + b_1b_2(\sigma \circ \sigma) + b_1c_2(\sigma \circ \tau) + b_1d_2(\sigma \circ \pi_2) \\ & + c_1a_2(\tau \circ \pi_1) + c_1b_2(\tau \circ \sigma) + c_1c_2(\tau \circ \tau) + c_1d_2(\tau \circ \pi_2) \\ & + d_1a_2(\pi_2 \circ \pi_1) + d_1b_2(\pi_2 \circ \sigma) + d_1c_2(\pi_2 \circ \tau) + d_1d_2(\pi_2 \circ \pi_2) \\ =& \left((a_1a_2) \bmod p\right) \pi_1 + \left((a_1b_2 + b_1d_2) \bmod p\right) \sigma \\ & + \left((c_1a_2 + d_1c_2) \bmod p\right) \tau + \left((pc_1b_2 + d_1d_2) \bmod p^2\right) \pi_2. \end{aligned} \tag{5}$$

Now, by expressions (3), (4) and (1) we have that

$$\Phi(f + g) = \Phi(f) + \Phi(g).$$

Analogously, by expressions (3), (5) and (2) we have that

$$\Phi(f \circ g) = \Phi(f) \cdot \Phi(g).$$

So, Φ is a ring homomorphism. $\square$

From now on, we identify the elements of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ with the elements of E_p, and the arithmetic of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ with the arithmetic of E_p.

4 Invertible elements of E_p

Because in the ring of endomorphisms $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ we work with elements in the field $\mathbb{Z}_p$ and the ring $\mathbb{Z}_{p^2}$, the fact that $\mathbb{Z}_p \subseteq \mathbb{Z}_{p^2}$ represents, as we have already mentioned earlier in Section 1, a difficulty with the notation of some elements. For example, if $p = 5$, then $2 \in \mathbb{Z}_5$ and $2 \in \mathbb{Z}_{5^2}$; however, $2^{-1} = 3$, in $\mathbb{Z}_5$, while $2^{-1} = 13$ in $\mathbb{Z}_{5^2}$. Therefore, when we write 2^{-1} we must clearly specify which of the two elements we mean, $3 \in \mathbb{Z}_5$ or $13 \in \mathbb{Z}_{5^2}$. This difficulty could be saved if we took elements only from $\mathbb{Z}_p$ or only from $\mathbb{Z}_{p^2}$; in this way, all the operations will be performed in $\mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$ and not as before where some operations are performed in $\mathbb{Z}_p$ while others in $\mathbb{Z}_{p^2}$.

Note first that if $d \in \mathbb{Z}_{p^2}$, then, according to the division algorithm in $\mathbb{Z}$, there exists a unique pair $(u, v) \in \mathbb{Z}_p^2$ such that $d = pu + v$. So, the map

$$f : \mathbb{Z}_p^2 \longrightarrow \mathbb{Z}_{p^2} \quad \text{given by} \quad f(u, v) = pu + v$$

is bijective. However, this map is not a homomorphism of the additive group $\mathbb{Z}_p^2$ in the additive group $\mathbb{Z}_{p^2}$, as we can see in the following example for $p = 5$ where we have that

$$(2,3) + (4,4) = (2+4, 3+4) = (1,2) \text{ in } \mathbb{Z}_5^2$$

thus

$$f((2,3) + (4,4)) = f(1,2) = 5 \cdot 1 + 2 = 7 \text{ in } \mathbb{Z}_{5^2},$$

while

$$f(2,3) + f(4,4) = (5 \cdot 2 + 3) + (5 \cdot 4 + 4) = 13 + 24 = 12 \text{ in } \mathbb{Z}_{5^2}.$$

However, if we reorganize the previous calculations as

$$(5 \cdot 2 + 3) + (5 \cdot 4 + 4) = 5(2+4) + (3+4) = 5 \cdot 6 + (5 \cdot 1 + 2) = 5(6+1) + 2$$

and reduce modulo 5 the coefficient of 5, we have that

$$(5 \cdot 2 + 3) + (5 \cdot 4 + 4) = 5 \cdot 2 + 2,$$

that is, we obtain the same result as before. However, in this case instead of reducing modulo 5^2, we have first divided the constant term by 5 and then we have carried one unit in the coefficient of 5 to finally reduce it modulo 5. This example suggests that it is possible to reorganize the addition in $\mathbb{Z}_{p^2}$ as we can see in the following result.

As usual, if $a, b \in \mathbb{Z}$, with $b \neq 0$, we denote by $\left\lfloor \frac{a}{b} \right\rfloor$ and $a \bmod b$ the quotient and the remainder of the division of a by b, respectively.

Lemma 1 *Assume that $d_i = pu_i + v_i \in \mathbb{Z}_{p^2}$ with $u_i, v_i \in \mathbb{Z}_p$, for $i = 1, 2$. If*

$$u = \left(u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor \right) \bmod p \qquad \text{and} \qquad v = (v_1 + v_2) \bmod p$$

then $d_1 + d_2 = pu + v \in \mathbb{Z}_{p^2}$ with $u, v \in \mathbb{Z}_p$.

Proof: From the definition of u and v we have that

$$u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor = p \left\lfloor \frac{u_1 + u_2 + \left\lfloor \frac{v_1+v_2}{p} \right\rfloor}{p} \right\rfloor + u$$

and

$$v_1 + v_2 = p \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor + v.$$

Therefore

$$\begin{aligned} d_1 + d_2 &= (pu_1 + v_1) + (pu_2 + v_2) \\ &= p(u_1 + u_2) + (v_1 + v_2) \\ &= p(u_1 + u_2) + p \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor + v \\ &= p \left(u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor \right) + v \end{aligned}$$

$$= p \left(p \left\lfloor \frac{u_1 + u_2 + \lfloor \frac{v_1+v_2}{p} \rfloor}{p} \right\rfloor + u \right) + v$$
$$= p^2 \left\lfloor \frac{u_1 + u_2 + \lfloor \frac{v_1+v_2}{p} \rfloor}{p} \right\rfloor + pu + v.$$

Now, since $pu + v \in \mathbb{Z}_{p^2}$, by the division algorithm in $\mathbb{Z}$, it is clear that

$$pu + v = (d_1 + d_2) \bmod p^2$$

that is, we have that $d_1 + d_2 = pu + v$ in $\mathbb{Z}_{p^2}$. $\square$

Following a similar argument we establish the following result.

Lemma 2 *Assume that $d_i = pu_i + v_i \in \mathbb{Z}_{p^2}$ with $u_i, v_i \in \mathbb{Z}_p$, for $i = 1, 2$. If*

$$u = \left(u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor \right) \bmod p \quad \textit{and} \quad v = (v_1 v_2) \bmod p$$

then $d_1 d_2 = pu + v \in \mathbb{Z}_{p^2}$ with $u, v \in \mathbb{Z}_p$.

Proof: From the definition of u and v we have that

$$u_1 v_2 + u_2 v_1 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor = p \left\lfloor \frac{u_1 v_2 + u_2 v_1 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor}{p} \right\rfloor + u,$$

and

$$v_1 v_2 = p \left\lfloor \frac{v_1 v_2}{p} \right\rfloor + v.$$

Therefore

$$\begin{aligned}
d_1 \cdot d_2 &= (pu_1 + v_1) \cdot (pu_2 + v_2) \\
&= p^2 u_1 u_2 + pu_1 v_2 + v_1 p u_2 + v_1 v_2 \\
&= p^2 u_1 u_2 + p(u_1 v_2 + v_1 u_2) + p \left\lfloor \frac{v_1 v_2}{p} \right\rfloor + v \\
&= p^2 u_1 u_2 + p \left(u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor \right) + v \\
&= p^2 u_1 u_2 + p \left(p \left\lfloor \frac{u_1 v_2 + v_1 u_2 + \lfloor \frac{v_1 v_2}{p} \rfloor}{p} \right\rfloor + u \right) + v \\
&= p^2 \left(u_1 u_2 + \left\lfloor \frac{u_1 v_2 + v_1 u_2 + \lfloor \frac{v_1 v_2}{p} \rfloor}{p} \right\rfloor \right) + pu + v.
\end{aligned}$$

Now, since $pu + v \in \mathbb{Z}_{p^2}$, by the division algorithm in $\mathbb{Z}$, it is clear that

$$pu + v = (d_1 \cdot d_2) \bmod p^2$$

that is, we have that $d_1 \cdot d_2 = pu + v$ in $\mathbb{Z}_{p^2}$. $\square$

So, as a consequence of the two previous results, it is easy to compute addition and multiplication of the elements in $\mathbb{Z}_{p^2}$ using only arithmetic in $\mathbb{Z}$ and $\mathbb{Z}_p$. Before turning to the characterization of invertible elements of E_p, we characterize invertible elements in $\mathbb{Z}_{p^2}$.

The following result establishes a necessary and sufficient condition for an element $d = pu + v \in \mathbb{Z}_{p^2}$ with $u, v \in \mathbb{Z}_p$ to be invertible and, therefore, provides the way to compute $d^{-1} \in \mathbb{Z}_{p^2}$ using only arithmetic in $\mathbb{Z}$ and $\mathbb{Z}_p$.

Lemma 3 *Assume that $d = pu + v \in \mathbb{Z}_{p^2}$ with $u, v \in \mathbb{Z}_p$. Then d is invertible in $\mathbb{Z}_{p^2}$ if and only if $v \neq 0$ and, in this case,*

$$d^{-1} = p\left[\left(-u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p\right] + v^{-1},$$

where $v^{-1} \in \mathbb{Z}_p$ is the inverse of v.

Proof: Let us assume that d es invertible; then $\gcd(d, p^2) = 1$. However, if $v = 0$ then

$$1 = \gcd(d, p^2) = \gcd(pu, p^2) = p,$$

which is a contradiction, so $v \neq 0$.

Reciprocally, assume now that $v \neq 0$. Since $\mathbb{Z}_p$ is a field, there exists $v^{-1} \in \mathbb{Z}_p$. Now, by Lemma 2, we have that

$$\begin{aligned}
&(pu + v)\left\{p\left[\left(-u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p\right] + v^{-1}\right\} \\
&\quad = p\left\{uv^{-1} + v\left[\left(-u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p\right] + \left\lfloor \frac{vv^{-1}}{p} \right\rfloor\right\} \bmod p \\
&\qquad + (vv^{-1}) \bmod p \\
&\quad = p\left\{(uv^{-1}) \bmod p - (vu(v^{-1})^2) \bmod p - \left(v\left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p + \left\lfloor \frac{vv^{-1}}{p} \right\rfloor \bmod p\right\} \bmod p + 1 \\
&\quad = p\left((uv^{-1}) \bmod p - (uv^{-1}) \bmod p - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor \bmod p + \left\lfloor \frac{vv^{-1}}{p} \right\rfloor \bmod p\right) \bmod p + 1 \\
&\quad = p \cdot 0 + 1 = 1.
\end{aligned}$$

Therefore, $pu + v$ is invertible in $\mathbb{Z}_{p^2}$ and

$$(pu + v)^{-1} = p\left[\left(-u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor\right) \bmod p\right] + v^{-1}. \qquad \square$$

Note that the above expression can be confusing and misleading because we can assume that

$$\left\lfloor \frac{vv^{-1}}{p} \right\rfloor \bmod p = \left\lfloor \frac{(vv^{-1}) \bmod p}{p} \right\rfloor = \left\lfloor \frac{1}{p} \right\rfloor = 0,$$

which is false, as we can see by considering $p = 5$ and $v = 2$; then $v^{-1} = 3$ and

$$\left\lfloor \frac{vv^{-1}}{p} \right\rfloor \bmod p = \left\lfloor \frac{2 \cdot 3}{5} \right\rfloor \bmod 5 = \left\lfloor \frac{6}{5} \right\rfloor = 1.$$

We obtain the following characterization of addition and multiplication in E_p, in terms of the arithmetic of $\mathbb{Z}$ and $\mathbb{Z}_p$.

Corollary 1 *Let*

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & pu_1+v_1 \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} a_2 & b_2 \\ pc_2 & pu_2+v_2 \end{bmatrix}$$

be two elements of E_p. Then

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

and

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

Proof: The proof involves the direct application of the expressions (1) and (2) for the addition and multiplication, respectively, and the use of Lemmas 1 and 2 for the addition and multiplication of elements in $\mathbb{Z}_{p^2}$. $\square$

We can now to establish a characterization of the invertible elements of E_p.

Theorem 6 *Assume that $M = \begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix} \in E_p$ with $a, b, c, u, v \in \mathbb{Z}_p$. M is invertible if and only if $a \neq 0$ and $v \neq 0$, and in this case*

$$M^{-1} = \begin{bmatrix} a^{-1} & (-a^{-1}bv^{-1}) \bmod p \\ p\left[(-v^{-1}ca^{-1}) \bmod p\right] & p\left[\left(ca^{-1}b(v^{-1})^2 - u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p\right] + v^{-1} \end{bmatrix}. \quad (6)$$

Proof: Assume that M is invertible. Then there exists $\begin{bmatrix} x & y \\ pz & pr+s \end{bmatrix} \in E_p$, with $x, y, z, r, s \in \mathbb{Z}_p$, such that

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix} \begin{bmatrix} x & y \\ pz & pr+s \end{bmatrix}.$$

Now, from Corollary 1,

$$1 = (ax) \bmod p \quad \text{and} \quad 1 = (vs) \bmod p,$$

and therefore, $a \neq 0$ and $v \neq 0$.

Reciprocally, assume now that $a \neq 0$ and $v \neq 0$, then, there exist $a^{-1}, v^{-1} \in \mathbb{Z}_p$. Assume that $N \in E_p$ is the element defined by the righthand side of expression (6). Then, from Corollary 1, we have that $MN = \begin{bmatrix} x & y \\ pz & t \end{bmatrix}$, where

$x = (aa^{-1}) \bmod p = 1,$

$$y = \left[a(-a^{-1}bv^{-1}) + bv^{-1}\right] \bmod p = \left(-bv^{-1} + bv^{-1}\right) \bmod p = 0,$$

$$z = \left[ca^{-1} + v(-v^{-1}ca^{-1})\right] \bmod p = \left(ca^{-1} - ca^{-1}\right) \bmod p = 0,$$

$$\begin{aligned} t &= p\left\{\left[c(-a^{-1}bv^{-1}) + uv^{-1} + v\left(ca^{-1}b(v^{-1})^2 - u(v^{-1})^2 - \left\lfloor\frac{vv^{-1}}{p}\right\rfloor v^{-1}\right) + \left\lfloor\frac{vv^{-1}}{p}\right\rfloor\right] \bmod p\right\} \\ &\quad + (vv^{-1}) \bmod p \\ &= p\left[\left(-ca^{-1}bv^{-1} + uv^{-1} + ca^{-1}bv^{-1} - uv^{-1} - \left\lfloor\frac{vv^{-1}}{p}\right\rfloor + \left\lfloor\frac{vv^{-1}}{p}\right\rfloor\right) \bmod p\right] + 1 \\ &= p \cdot 0 + 1 = 1. \end{aligned}$$

And consequently $MN = I$.

Following a similar argument we have that $NM = I$, and therefore, M is invertible and $M^{-1} = N$.

5 Number of invertible elements in E_p

Once we have characterized the invertible elements of E_p we wonder how many elements are invertible for each value of p. The next result will provide an answer to this question.

Theorem 7 *The number of invertible elements of E_p is $p^3(p-1)^2$.*

Proof: To determine the number of invertible elements $\begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix}$ in E_p, we count the noninvertible elements, that is, from Theorem 6 those elements for which $a = 0$ or $v = 0$.

Clearly, the number of elements of the form $\begin{bmatrix} 0 & b \\ pc & pu+v \end{bmatrix}$ is p^4. Also, the number of elements of the form $\begin{bmatrix} a & b \\ pc & pu \end{bmatrix}$ is p^4. Subtracting the p^3 elements of the form $\begin{bmatrix} 0 & b \\ pc & pu \end{bmatrix}$, we have that the total number of noninvertible elements in E_p is $2p^4 - p^3$.

So, we conclude that the number of invertible elements in E_p is

$$p^5 - 2p^4 + p^3 = p^3(p-1)^2. \qquad \square$$

Since

$$\frac{p^3(p-1)^2}{p^5} = \left(\frac{p-1}{p}\right)^2 \approx 1,$$

we can say that for large values of p, almost all the elements of E_p are invertible. Table 1 shows the percentage of invertible elements of E_p for certain values of p. Note that for $p = 211$ the number of invertible elements represents over 99% of all the elements of E_{211}. However, for values of p with five digits, we reach 99.99%.

Note that even for small values of p the number of invertible elements in the ring E_p is very high. So even by taking values of p with three digits, the probability that an element of E_p is invertible is more than 98%.

p	Elements in E_p	Number of invertible elements	%
2	32	8	25.0000
3	243	108	44.4444
5	3 125	2 000	64.0000
7	16 807	12 348	73.4694
11	161 051	133 100	82.6446
13	371 293	316 368	85.2071
17	1 419 857	1 257 728	88.5813
19	2 476 099	2 222 316	89.7507
23	6 436 343	5 888 828	91.4934
$\vdots$	$\vdots$	$\vdots$	$\vdots$
97	8 587 340 257	8 411 194 368	97.9488
101	10 510 100 501	10 303 010 000	98.0296
103	11 592 740 743	11 368 731 708	98.0677
107	14 025 517 307	13 764 583 148	98.1396
109	15 386 239 549	15 105 218 256	98.1736
113	18 424 351 793	18 099 699 968	98.2379
127	33 038 369 407	32 520 128 508	98.4314
131	38 579 489 651	37 992 737 900	98.4791
137	48 261 724 457	47 559 745 088	98.5455
$\vdots$	$\vdots$	$\vdots$	$\vdots$
211	418 227 202 051	414 272 357 100	99.0544
223	551 473 077 343	546 538 220 028	99.1051
227	602 738 989 907	597 440 211 308	99.1209
229	629 763 392 149	624 275 284 176	99.1285
233	686 719 856 393	680 837 914 688	99.1435
$\vdots$	$\vdots$	$\vdots$	$\vdots$
1009	1 045 817 322 864 049	1 043 745 372 262 656	99.8019
1013	1 066 712 113 176 293	1 064 607 107 052 368	99.8027
1019	1 098 679 244 081 099	1 096 523 915 038 316	99.8038
1021	1 109 503 586 489 101	1 107 331 284 344 400	99.8042
1031	1 164 912 556 234 151	1 162 653 879 971 900	99.8061
$\vdots$	$\vdots$	$\vdots$	$\vdots$
10007	100 350 490 343 120 066 807	100 330 435 286 394 092 348	99.9800
10501	127 688 943 139 852 552 501	127 664 624 910 485 250 000	99.9810
20011	3 208 809 685 325 464 261 051	3 208 488 388 757 658 533 100	99.9900
40009	102 524 251 851 665 312 259 049	102 519 127 306 153 088 686 656	99.9950
60013	778 442 765 119 100 568 670 293	778 416 822 863 939 144 476 368	99.9967
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 1: Percentage of invertible elements of E_p for some values of p

The set of invertible elements of a ring is widely known to be a multiplicative group. Therefore, if we denote by U_p that set, then the above theorem (together with Theorem 4) establishes that U_p is a nonabelian group of order $p^3(p-1)^2$.

6 Cryptographic applications

Theorem 4 allows us to establish the addition and the composition of the elements of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ in terms of the elements of E_p; that is, in terms of addition and multiplication of 2×2 matrices $\begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix}$, where $a, b, c, u, v \in \mathbb{Z}_p$, introduced in Theorem 3 and Corollary 1.

Let $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Z}[X]$; for a fixed element $M \in E_p$, we can consider the element

$$f(M) = a_0I + a_1M + a_2M^2 + \cdots + a_nM^n \in E_p,$$

where I is the multiplicative identity of E_p. Now, we can use the properties of E_p and the commutative multiplicative semigroup

$$\mathbb{Z}[M] = \{f(M) \mid f(X) \in \mathbb{Z}[X]\}$$

to introduce a key exchange protocol (see, for example, [11]).

The key exchange protocol that we propose can be summarized as follows:

Start: Elements $r, s \in \mathbb{N}$ and $M, N \in E_p$ are public.

Step 1: Alice and Bob choose their private keys $f(X), g(X) \in \mathbb{Z}[X]$, respectively.

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

$$P_B = g(M)^r N g(M)^s$$

and sends it to Alice.

Step 3: Alice and Bob compute

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

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

Theorem 8 *With the above notation, it follows that $S_A = S_B$.*

Proof: The result follows because the multiplication in $\mathbb{Z}[M]$ is commutative. □

Note that if in the above protocol we take M and N such that $MN = NM$, then

$$S_A = f(M)^r f(M)^s P_B = P_A g(M)^r g(M)^s$$

and therefore, $S_A N = P_A P_B$. So, if N is invertible (which occurs in more than 99% of cases, if p has more than three digits, as we see in Table 1), then $S_A = P_A P_B N^{-1}$, that is, the shared secret is the product of three elements of E_p that are public. This is the only weakness that we know of this protocol.

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

Example 1 *Assume that $p = 11$, from Theorem 1 and 5, we now that*

$$\mathrm{Card}\,(E_{11}) = 11^5 = 161\,051.$$

The starting point of the protocol consists on the sharing of $r, s \in \mathbb{N}$ and $M, N \in E_{11}$ by Alice and Bob. For this example, let us assume that $r = 3$, $s = 5$ and

$$M = \begin{bmatrix} 5 & 8 \\ 44 & 102 \end{bmatrix}, \qquad N = \begin{bmatrix} 10 & 3 \\ 77 & 37 \end{bmatrix}. \tag{7}$$

Now, we run the steps of the protocol.

Step 1: *Alice chooses*

$$f(X) = 3 + 3X + 9X^2 + 5X^3 \in \mathbb{Z}[X]$$

and Bob chooses

$$g(X) = 9 + 6X + 5X^2 \in \mathbb{Z}[X].$$

So,

$$f(M) = 3\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 3\begin{bmatrix} 5 & 8 \\ 44 & 102 \end{bmatrix} + 9\begin{bmatrix} 5 & 8 \\ 44 & 102 \end{bmatrix}^2 + 5\begin{bmatrix} 5 & 8 \\ 44 & 102 \end{bmatrix}^3 = \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix},$$

$$g(M) = 9\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 6\begin{bmatrix} 5 & 8 \\ 44 & 102 \end{bmatrix} + 5\begin{bmatrix} 5 & 8 \\ 44 & 102 \end{bmatrix}^2 = \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}.$$

Step 2: *Alice computes her public key P_A as*

$$P_A = f(M)^3 N f(M)^5 = \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^3 \begin{bmatrix} 10 & 3 \\ 77 & 37 \end{bmatrix} \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^5 = \begin{bmatrix} 10 & 5 \\ 110 & 119 \end{bmatrix}$$

and sends it to Bob.

Bob computes his public key P_B as

$$P_B = g(M)^3 N g(M)^5 = \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^3 \begin{bmatrix} 10 & 3 \\ 77 & 37 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^5 = \begin{bmatrix} 10 & 10 \\ 11 & 16 \end{bmatrix}.$$

and sends it to Alice.

Step 3: *Alice computes S_A as*

$$S_A = f(M)^3 P_B f(M)^5 = \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^3 \begin{bmatrix} 10 & 10 \\ 11 & 16 \end{bmatrix} \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^5 = \begin{bmatrix} 10 & 7 \\ 22 & 113 \end{bmatrix}.$$

Bob computes S_B as

$$S_B = g(M)^3 P_A g(M)^5 = \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^3 \begin{bmatrix} 10 & 5 \\ 110 & 119 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^5 = \begin{bmatrix} 10 & 7 \\ 22 & 113 \end{bmatrix}.$$

As we established in Theorem 8, the shared secret is

$$S_A = \begin{bmatrix} 10 & 7 \\ 22 & 113 \end{bmatrix} = S_B.$$

Acknowledgements

The authors would like to thank the referees for their valuable comments and suggestions.

References

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

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

[3] 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.

[4] 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.

[5] T.-Y. Lam. *A First Curs in Noncommutative Rings*. Number 131 in Graduate Texts in Mathematics. Springer, New York, NY, 2001.

[6] S. S. Magliveras, D. R. Stinson and T. van Trung. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *Journal of Cryptology*, **15**: 285–297 (2002).

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

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

[9] 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).

[10] 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).

[11] 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.

[12] B. Tsaban. Combinatorial Group Theory and Cryptography Bulletin (CGC Bulletin). `http://u.cs.biu.ac.il/~tsaban/CGC/cgc.html`.