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

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 \( \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \) is a semilocal ring with \( p^5 \) elements that cannot be embedded in matrices over any commutative ring. We identify the elements of \( \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \) with elements in a new set, denoted by \( E_p \), of matrices of size \( 2 \times 2 \), 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 \( \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \) 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 \( \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \) 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 \( \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \) 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 $2 \times 2$ 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,

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

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, $x \text{ mod } p$ and $x \text{ mod } p^2$ 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 $(2 \text{ mod } 5) + (4 \text{ mod } 5) = 1 \text{ mod } 5$, whereas $(2 \text{ mod } 5^2) + (4 \text{ mod } 5^2) = 6 \text{ mod } 5^2$.

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

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

The next result not only determines the cardinality of the ring $\text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, 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 $\text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ has $p^5$ elements and is semiloal, 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 [2], 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 \( \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \) 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 \( \pi_1 \) and \( \pi_2 \), 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 \( \sigma : \mathbb{Z}_{p^2} \rightarrow \mathbb{Z}_p \) and the natural immersion \( \tau : \mathbb{Z}_p \rightarrow \mathbb{Z}_{p^2} \) that we can define, respectively, as

\[
\sigma(y) = y \mod p \quad \text{and} \quad \tau(x) = px.
\]

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 \( \sigma \) and \( \tau \), respectively, as

\[
\sigma(x, y) = (y \mod p, 0), \quad \text{and} \quad \tau(x, y) = (0, px).
\]

**Theorem 2** The endomorphisms \( \pi_1, \pi_2, \sigma \) and \( \tau \) satisfy the following identities:

\[
\begin{align*}
\pi_1 \circ \pi_1 &= \pi_1, \\
\pi_2 \circ \pi_1 &= O, \\
\pi_1 \circ \pi_2 &= O, \\
\pi_1 \circ \tau &= O, \\
\pi_2 \circ \pi_2 &= O, \\
\pi_2 \circ \tau &= \tau, \\
\sigma \circ \pi_1 &= O, \\
\sigma \circ \pi_2 &= \sigma, \\
\sigma \circ \tau &= O, \\
\tau \circ \sigma &= \sigma, \\
\tau \circ \tau &= \tau, \\
\tau \circ \pi_1 &= O, \\
\tau \circ \pi_2 &= \tau, \\
\pi_1 \circ \sigma &= \sigma, \\
\pi_2 \circ \sigma &= \sigma, \\
\pi_1 \circ \tau &= \tau, \\
\pi_2 \circ \tau &= \tau, \\
\sigma \circ \pi_1 &= \sigma, \\
\sigma \circ \pi_2 &= \sigma, \\
\sigma \circ \tau &= \sigma, \\
\tau \circ \pi_1 &= \tau, \\
\tau \circ \pi_2 &= \tau, \\
\pi_1 \circ \pi_1 &= \pi_1, \\
\pi_2 \circ \pi_2 &= \pi_2, \\
\pi_1 \circ \tau &= \tau, \\
\pi_1 \circ \sigma &= \sigma, \\
\pi_2 \circ \tau &= \tau, \\
\pi_2 \circ \sigma &= \sigma, \\
\sigma \circ \pi_1 &= \sigma, \\
\sigma \circ \pi_2 &= \sigma, \\
\sigma \circ \tau &= \sigma, \\
\tau \circ \pi_1 &= \tau, \\
\tau \circ \pi_2 &= \tau, \\
\pi_1 \circ \pi_1 &= \pi_1, \\
\pi_2 \circ \pi_2 &= \pi_2, \\
\pi_1 \circ \tau &= \tau, \\
\pi_1 \circ \sigma &= \sigma, \\
\pi_2 \circ \tau &= \tau, \\
\pi_2 \circ \sigma &= \sigma, \\
\sigma \circ \pi_1 &= \sigma, \\
\sigma \circ \pi_2 &= \sigma, \\
\sigma \circ \tau &= \sigma, \\
\tau \circ \pi_1 &= \tau, \\
\tau \circ \pi_2 &= \tau, \\
\pi_1 \circ \pi_1 &= \pi_1, \\
\pi_2 \circ \pi_2 &= \pi_2, \\
\pi_1 \circ \tau &= \tau, \\
\pi_1 \circ \sigma &= \sigma, \\
\pi_2 \circ \tau &= \tau, \\
\pi_2 \circ \sigma &= \sigma, \\
\sigma \circ \pi_1 &= \sigma, \\
\sigma \circ \pi_2 &= \sigma, \\
\sigma \circ \tau &= \sigma, \\
\tau \circ \pi_1 &= \tau, \\
\tau \circ \pi_2 &= \tau.
\end{align*}
\]

where \( p\pi_2 \) is the sum of \( \pi_2 \) with itself \( p \) times. Furthermore, the additive order of \( \pi_1, \sigma \) and \( \tau \) is \( p \), while the additive order of \( \pi_2 \) is \( p^2 \).

**Proof:** Let \( (x, y) \in \mathbb{Z}_p \times \mathbb{Z}_{p^2} \). According to the definitions of \( \pi_1, \pi_2, \sigma \) and \( \tau \) we have that

\[
(\pi_1 \circ \pi_1)(x, y) = \pi_1(\pi_1(x, y)) = \pi_1(x, 0) = (x, 0) = \pi_1(x, y),
\]

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

\[
(\tau \circ \sigma)(x, y) = \tau(\sigma(x, y)) = \tau(y \mod p, 0) = (0, p(y \mod p)) = (0, py)
\]

\[
= p(0, y) = p\pi_2(x, y) = (p\pi_2)(x, y),
\]

\[
(\sigma \circ \pi_2)(x, y) = \sigma(\pi_2(x, y)) = \sigma(0, y) = (y \mod p, 0) = \sigma(x, y),
\]

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 $\pi_1$, $\sigma$ and $\tau$ 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 $\pi_2$ is $p^2$. □

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

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

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

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

where $\pi_1$, $\sigma$, $\tau$ and $\pi_2$ are the endomorphisms introduced in Section 2.

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

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

Therefore,

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

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 

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

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

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

Theorem 3 establishes that the ring $\text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ 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

\[
\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 + a_2) \mod p & (b_1 + b_2) \mod p \\ pc_1 + c_2) \mod p^2 & (d_1 + d_2) \mod p^2 \end{bmatrix}
\]

and

\[
\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 a_2) \mod p & (a_1 b_2 + b_1 d_2) \mod p \\ pc_1 a_2 + d_1 c_2) \mod p^2 & (pc_1 b_2 + d_1 d_2) \mod p^2 \end{bmatrix}
\]

respectively.

**Proof:** The proof is straightforward. \(\Box\)

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

\[
O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

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 \(f \in \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})\), 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 \(\text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})\) we can establish that the ring introduced in Theorem 4 is isomorphic to the endomorphism ring \(\text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})\).

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

\[
\Phi (a\pi_1 + b\sigma + c\tau + d\pi_2) = \begin{bmatrix} a & b \\ pc & d \end{bmatrix}
\]

is a ring isomorphism.
Proof: That \( \Phi \) is a bijective map follows from Theorem 3. Let \( f, g \in \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \). 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

\[
f + g = (a_1 \pi_1 + b_1 \sigma + c_1 \tau + d_1 \pi_2) + (a_2 \pi_1 + b_2 \sigma + c_2 \tau + d_2 \pi_2)
= ((a_1 + a_2) \mod p) \pi_1 + ((b_1 + b_2) \mod p) \sigma
+ ((c_1 + c_2) \mod p) \tau + ((d_1 + d_2) \mod p^2) \pi_2
\]

and

\[
f \circ g = (a_1 \pi_1 + b_1 \sigma + c_1 \tau + d_1 \pi_2) \circ (a_2 \pi_1 + b_2 \sigma + c_2 \tau + d_2 \pi_2)
=a_1 a_2 (\pi_1 \circ \pi_1) + a_1 b_2 (\pi_1 \circ \sigma) + a_1 c_2 (\pi_1 \circ \tau) + a_1 d_2 (\pi_1 \circ \pi_2)
+ b_1 a_2 (\sigma \circ \pi_1) + b_1 b_2 (\sigma \circ \sigma) + b_1 c_2 (\sigma \circ \tau) + b_1 d_2 (\sigma \circ \pi_2)
+ c_1 a_2 (\tau \circ \pi_1) + c_1 b_2 (\tau \circ \sigma) + c_1 c_2 (\tau \circ \tau) + c_1 d_2 (\tau \circ \pi_2)
+ d_1 a_2 (\pi_2 \circ \pi_1) + d_1 b_2 (\pi_2 \circ \sigma) + d_1 c_2 (\pi_2 \circ \tau) + d_1 d_2 (\pi_2 \circ \pi_2)
=(a_1 a_2 \mod p) \pi_1 + ((a_1 b_2 + b_1 d_2) \mod p) \sigma
+ ((c_1 a_2 + d_1 c_2) \mod p) \tau + ((pc_1 b_2 + d_1 d_2) \mod p^2) \pi_2.
\]

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, \( \Phi \) is a ring homomorphism. \( \square \)

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

4 Invertible elements of \( E_p \)

Because in the ring of endomorphisms \( \text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \) 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

\[
f : \mathbb{Z}_p^2 \to \mathbb{Z}_{p^2} \quad \text{given by} \quad f(u, v) = pu + v
\]
is bijective. However, this map is not a homomorphism of the additive group \( \mathbb{Z}_{p^2} \) in the additive group \( \mathbb{Z}_p \), 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 \( a \mod b \) 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
\[
u = \left( u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor \right) \mod p \quad \text{and} \quad v = (v_1 + v_2) \mod p
\]
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
\[
d_1 + d_2 = (pu_1 + v_1) + (pu_2 + v_2)
\]
\[
= p(u_1 + u_2) + (v_1 + v_2)
\]
\[
= p(u_1 + u_2) + p \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor + v
\]
\[
= p \left( u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor \right) + v
\]
Now, since \( pu + v \in \mathbb{Z}_{p^2} \), by the division algorithm in \( \mathbb{Z} \), it is clear that

\[
pu + v = (d_1 + d_2) \mod p^2
\]

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

\[
u = \left( u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor \right) \mod p \quad \text{and} \quad v = (v_1 v_2) \mod p
\]

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

\[
u_1 v_2 + u_2 v_1 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor = p \left( u_1 v_2 + u_2 v_1 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor \right) + u,
\]

and

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

Therefore

\[
d_1 \cdot d_2 = (pu_1 + v_1) \cdot (pu_2 + v_2)
\]

\[
= p^2 u_1 u_2 + pu_1 v_2 + v_1 pu_2 + v_1 v_2
\]

\[
= p^2 u_1 u_2 + p(u_1 v_2 + v_1 u_2) + p \left\lfloor \frac{v_1 v_2}{p} \right\rfloor + v
\]

\[
= p^2 u_1 u_2 + p \left( u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor \right) + v
\]

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

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

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

\[
pu + v = (d_1 \cdot d_2) \mod p^2
\]

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,

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

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

**Proof:** Let us assume that \( d \) is 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

\[
(pu + v) \left\{ p \left[ \left( -u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1} \right) \mod p \right] + v^{-1} \right\}
= p \left\{ uv^{-1} + v \left[ \left( -u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1} \right) \mod p \right] + \left\lfloor \frac{vv^{-1}}{p} \right\rfloor \mod p \right\} \mod p
+ (uv^{-1}) \mod p
= p \left\{ (uv^{-1}) \mod p - (vu(v^{-1})^2) \mod p - \left( v \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1} \right) \mod p + \left\lfloor \frac{vv^{-1}}{p} \right\rfloor \mod p \right\} \mod p + 1
= p \left\{ (uv^{-1}) \mod p - (uv^{-1}) \mod p - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor \mod p + \left\lfloor \frac{vv^{-1}}{p} \right\rfloor \mod p \right\} \mod p + 1
= p \cdot 0 + 1 = 1.
\]

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

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

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

\[
\left\lfloor \frac{vv^{-1}}{p} \right\rfloor \mod p = \left\lfloor \frac{(vv^{-1}) \mod p}{p} \right\rfloor = \left\lfloor \frac{1}{p} \right\rfloor = 0,
\]

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

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

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
\[
\begin{bmatrix}
a_1 & b_1 \\
p c_1 & pu_1 + v_1
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
a_2 & b_2 \\
p c_2 & pu_2 + v_2
\end{bmatrix}
\]
be two elements of \( E_p \). Then
\[
\begin{bmatrix}
a_1 & b_1 \\
p c_1 & pu_1 + v_1
\end{bmatrix} + \begin{bmatrix}
a_2 & b_2 \\
p c_2 & pu_2 + v_2
\end{bmatrix} = \begin{bmatrix}
(a_1 + a_2) \mod p & (b_1 + b_2) \mod p \\
p [(c_1 + c_2) \mod p] & p \left( u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor \mod p \right) + (v_1 + v_2) \mod p
\end{bmatrix}
\]
and
\[
\begin{bmatrix}
a_1 & b_1 \\
p c_1 & pu_1 + v_1
\end{bmatrix} \cdot \begin{bmatrix}
a_2 & b_2 \\
p c_2 & pu_2 + v_2
\end{bmatrix} = \begin{bmatrix}
(a_1 a_2) \mod p & (a_1 b_2 + b_1 v_2) \mod p \\
p [(c_1 a_2 + v_1 c_2) \mod p] & p \left( c_1 b_2 + u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor \mod p \right) + (v_1 v_2) \mod p
\end{bmatrix}
\]

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 \( \mathbb{Z}_{p^2} \).

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
\[
M^{-1} = \begin{bmatrix}
\frac{a^{-1}}{p} \left( -u^{-1} - (v^{-1})^2 \right) & \frac{(-a^{-1} b v^{-1})}{p} \\
\left( c a^{-1} b (v^{-1})^2 - u (v^{-1})^2 - \left\lfloor \frac{u^{-1} v^{-1}}{p} \right\rfloor \mod p \right) & \left( v^{-1} \right) \mod p
\end{bmatrix}
\]

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, we have that \( 1 = (ax) \mod p \) and \( 1 = (vs) \mod p \), 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
\[
x = (aa^{-1}) \mod p = 1,
\]

\[ y = [a(-a^{-1}b v^{-1}) + b v^{-1}] \mod p = (-b v^{-1} + b v^{-1}) \mod p = 0, \]
\[ z = [c a^{-1} + v(-v^{-1}c a^{-1})] \mod p = (c a^{-1} - c a^{-1}) \mod p = 0, \]
\[ t = p \left \{ \left \lceil c(-a^{-1}b v^{-1}) + u v^{-1} + v \left ( c a^{-1}b (v^{-1})^2 - u (v^{-1})^2 - \left \lceil \frac{vu^{-1}}{p} \right \rceil v^{-1} \right \right \rceil + \left \lceil \frac{vu^{-1}}{p} \right \rceil \right \} \mod p \right \} + (v v^{-1}) \mod p \]
\[ = p \left \{ \left \lceil -c a^{-1}b v^{-1} + u v^{-1} + c a^{-1} b v^{-1} - u v^{-1} - \left \lceil \frac{vu^{-1}}{p} \right \rceil + \left \lceil \frac{vu^{-1}}{p} \right \rceil \right \rceil \mod p \right \} + 1 \]
\[ = p \cdot 0 + 1 = 1. \]

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 \( \left[ \begin{array}{cc} a & b \\ pc & pu + v \end{array} \right] \) 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 \( \left[ \begin{array}{cc} 0 & b \\ pc & pu + v \end{array} \right] \) is \( p^4. \) Also, the number of elements of the form \( \left[ \begin{array}{cc} a & b \\ pc & pu \end{array} \right] \) is \( p^3. \) Subtracting the \( p^3 \) elements of the form \( \left[ \begin{array}{cc} 0 & b \\ pc & pu \end{array} \right] \), 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

\[ p^5 - 2p^4 + p^3 = p^3(p-1)^2. \]

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%.
<table>
<thead>
<tr>
<th>$p$</th>
<th>Elements in $E_p$</th>
<th>Number of invertible elements</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>32</td>
<td>8</td>
<td>25.0000</td>
</tr>
<tr>
<td>3</td>
<td>243</td>
<td>108</td>
<td>44.4444</td>
</tr>
<tr>
<td>5</td>
<td>3 125</td>
<td>2 000</td>
<td>64.0000</td>
</tr>
<tr>
<td>7</td>
<td>16 807</td>
<td>12 348</td>
<td>73.4694</td>
</tr>
<tr>
<td>11</td>
<td>161 051</td>
<td>133 100</td>
<td>82.6446</td>
</tr>
<tr>
<td>13</td>
<td>371 293</td>
<td>316 368</td>
<td>85.2071</td>
</tr>
<tr>
<td>17</td>
<td>1 419 857</td>
<td>1 257 728</td>
<td>88.5813</td>
</tr>
<tr>
<td>19</td>
<td>2 476 099</td>
<td>2 222 316</td>
<td>89.7507</td>
</tr>
<tr>
<td>23</td>
<td>6 436 343</td>
<td>5 888 828</td>
<td>91.4934</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>8 587 340 257</td>
<td>8 411 194 368</td>
<td>97.9488</td>
</tr>
<tr>
<td>101</td>
<td>10 510 100 501</td>
<td>10 303 010 000</td>
<td>98.0296</td>
</tr>
<tr>
<td>103</td>
<td>11 592 740 743</td>
<td>11 368 731 708</td>
<td>98.0677</td>
</tr>
<tr>
<td>107</td>
<td>14 025 517 307</td>
<td>13 764 583 148</td>
<td>98.1396</td>
</tr>
<tr>
<td>109</td>
<td>15 386 239 549</td>
<td>15 105 218 256</td>
<td>98.1736</td>
</tr>
<tr>
<td>113</td>
<td>18 424 351 793</td>
<td>18 099 699 968</td>
<td>98.2379</td>
</tr>
<tr>
<td>127</td>
<td>33 038 369 407</td>
<td>32 520 128 508</td>
<td>98.4314</td>
</tr>
<tr>
<td>131</td>
<td>38 579 489 651</td>
<td>37 992 737 900</td>
<td>98.4791</td>
</tr>
<tr>
<td>137</td>
<td>48 261 724 457</td>
<td>47 559 745 088</td>
<td>98.5455</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>211</td>
<td>418 227 202 051</td>
<td>414 272 357 100</td>
<td>99.0544</td>
</tr>
<tr>
<td>223</td>
<td>551 473 077 343</td>
<td>546 538 220 028</td>
<td>99.1051</td>
</tr>
<tr>
<td>227</td>
<td>602 738 989 907</td>
<td>597 440 211 308</td>
<td>99.1209</td>
</tr>
<tr>
<td>229</td>
<td>629 763 392 149</td>
<td>624 275 284 176</td>
<td>99.1285</td>
</tr>
<tr>
<td>233</td>
<td>686 719 856 393</td>
<td>680 837 914 688</td>
<td>99.1435</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1009</td>
<td>1 045 817 322 864 049</td>
<td>1 043 745 372 262 656</td>
<td>99.8019</td>
</tr>
<tr>
<td>1013</td>
<td>1 066 712 113 176 293</td>
<td>1 064 607 107 052 368</td>
<td>99.8027</td>
</tr>
<tr>
<td>1019</td>
<td>1 098 679 244 081 099</td>
<td>1 096 523 915 038 316</td>
<td>99.8038</td>
</tr>
<tr>
<td>1021</td>
<td>1 109 503 586 489 101</td>
<td>1 107 331 284 444 000</td>
<td>99.8042</td>
</tr>
<tr>
<td>1031</td>
<td>1 164 912 556 234 151</td>
<td>1 162 653 879 971 900</td>
<td>99.8061</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10007</td>
<td>100 350 490 343 120 066 807</td>
<td>100 330 435 286 394 092 348</td>
<td>99.9800</td>
</tr>
<tr>
<td>10501</td>
<td>127 688 943 139 852 552 501</td>
<td>127 664 624 910 485 250 000</td>
<td>99.9810</td>
</tr>
<tr>
<td>20011</td>
<td>3 208 809 685 325 464 261 051</td>
<td>3 208 488 388 757 658 533 100</td>
<td>99.9900</td>
</tr>
<tr>
<td>40009</td>
<td>102 524 251 851 665 312 259 049</td>
<td>102 519 127 306 153 088 686 656</td>
<td>99.9950</td>
</tr>
<tr>
<td>60013</td>
<td>778 442 765 119 100 568 670 293</td>
<td>778 416 822 863 939 144 476 368</td>
<td>99.9967</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 $\text{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ in terms of the elements of $E_p$; that is, in terms of addition and multiplication of $2 \times 2$ 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, $P_A = f(M)^rNf(M)^s$ and sends it to Bob. Analogously, Bob computes his public key $P_B = g(M)^rNg(M)^s$ and sends it to Alice.

Step 3: Alice and Bob compute $S_A = f(M)^rP_Bf(M)^s$ and $S_B = g(M)^rP_Ag(M)^s$ 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. $\square$

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 know that
\[ \text{Card}(E_{11}) = 11^5 = 161051. \]

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

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
\[
P_A = f(M)^3Ng(M)^5 = \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^3 \begin{bmatrix} 10 & 3 \\ 77 & 37 \end{bmatrix} \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^5 = \begin{bmatrix} 10 & 5 \\ 110 & 119 \end{bmatrix}
\]
and sends it to Bob.

Bob computes his public key $P_B$ as
\[
P_B = g(M)^3Pg(M)^5 = \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^3 \begin{bmatrix} 10 & 3 \\ 77 & 37 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^5 = \begin{bmatrix} 10 & 10 \\ 11 & 16 \end{bmatrix}.
\]

and sends it to Alice.

Step 3: Alice computes $S_A$ as
\[
S_A = f(M)^3P_Bf(M)^5 = \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^3 \begin{bmatrix} 10 & 10 \\ 11 & 16 \end{bmatrix} \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix}^5 = \begin{bmatrix} 10 & 7 \\ 22 & 113 \end{bmatrix}.
\]

Bob computes $S_B$ as
\[
S_B = g(M)^3P_Ag(M)^5 = \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^3 \begin{bmatrix} 10 & 5 \\ 110 & 119 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}^5 = \begin{bmatrix} 10 & 7 \\ 22 & 113 \end{bmatrix}.
\]

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


