On the algebraic structure of $E_p^{(m)}$ and applications to cryptography

Karan Khathuria\textsuperscript{1} · Giacomo Micheli\textsuperscript{2} · Violetta Weger\textsuperscript{1}

Received: 3 December 2019 / Accepted: 6 December 2019 / Published online: 13 December 2019

© Springer-Verlag GmbH Germany, part of Springer Nature 2019

Abstract

In this paper we show that the $\mathbb{Z}/p^m\mathbb{Z}$-module structure of the ring $E_p^{(m)}$ is isomorphic to a $\mathbb{Z}/p^m\mathbb{Z}$-submodule of the matrix ring over $\mathbb{Z}/p^m\mathbb{Z}$. Using this intrinsic structure of $E_p^{(m)}$, solving a linear system over $E_p^{(m)}$ becomes computationally equivalent to solving a linear system over $\mathbb{Z}/p^m\mathbb{Z}$. As an application we break the protocol based on the Diffie–Hellman decomposition problem and ElGamal decomposition problem over $E_p^{(m)}$. Our algorithm terminates in a provable running time of $O(m^6)\ Z/p^m\mathbb{Z}$-operations.

Keywords Finite fields · Cryptography · Cayley–Hamilton · Decomposition problem

1 Introduction

Public key cryptosystems are often based on number theoretical problems, such as integer factorization as in RSA [20] or the discrete logarithm problem over finite fields or over elliptic curves. The latter is the base for well known protocols, such as the ElGamal protocol [10] or the Diffie–Hellman key exchange protocol [9]. Increasing computing powers threatens these classical cryptographic schemes and new ambient spaces are demanded, for example involving noncommutative structures (see [1,12,13,21,23]). In nonabelian groups there are two main problems which give rise to cryptographic schemes; the semigroup action problem (SAP) [15], and the decomposition problem

\begin{itemize}
\item Karan Khathuria karan.khathuria@math.uzh.ch
\item Giacomo Micheli gmicheli@usf.edu
\item Violetta Weger violetta.weger@math.uzh.ch
\end{itemize}

\textsuperscript{1} Institute of Mathematics, University of Zurich, Zurich, Switzerland
\textsuperscript{2} Department of Mathematics, University of South Florida, Tampa, USA
(DP). For an overview see [19,22]. These two problems are very similar: in the SAP one is given a finite semigroup $S$ acting on a finite set $A$, for $x, y \in A$, such that there exists an $s \in S$ with $y = s \star x$, one wants to find $t \in S$, such that $y = t \star x$. Whereas in the DP one is given a nonabelian group $G, (x, y) \in G \times G$ and $S \subset G$, one wants to find $z_1, z_2 \in S$, such that $y = z_1 x z_2$.

Based on these two problems J.J. Climent and J.A. López-Ramos proposed three protocols in [5] over a special ring of matrices involving operations modulo different powers of the same prime, called $E_p^{(m)}$. Similar cryptosystems can be found in [14, Example 4.3.c]. This ring is a generalization of the ring $E_p$, Climent, Navarro and Tartosa introduced in [6]. The first cryptographic scheme based on $E_p$ [7], was broken in [11]. This attack can be prevented by admitting only few invertible elements, as it is the case in the ring $E_p^{(m)}$ [8, Corollary 1]. In addition, another nice property of such rings is that they do not admit embeddings into matrix rings over a field (see [3]), which is often the main problem of cryptographic schemes over matrix rings (see for example [17]) and it prevents a reduction to small extensions of finite fields as in [16].

The first protocol proposed in [5] by Climent and López-Ramos based on the semigroup action problem over the ring $E_p^{(m)}$ was broken by Micheli and Weger in [18] using a solution sieve argument. The remaining two protocols proposed in [5] are based on the decomposition problem over $E_p^{(m)}$ and happen to be equivalent. They will be denoted by the Diffie–Hellman Decomposition Problem (DHDP) and the ElGamal Decomposition Problem (EGDP). A cryptanalysis of these two protocols was considered by Zhang in [24], where the Cayley–Hamilton Theorem is used to derive a linear system over $E_p^{(m)}$. However, even though the main idea is correct, the system over $E_p^{(m)}$ is then directly considered over $\mathbb{Z}/p^m \mathbb{Z}$, where the system not necessarily admits a solution, as we will show in an example. The running time of the claimed attack is $O(m^7) \mathbb{Z}/p^m \mathbb{Z}$-operations.

In this paper we introduce a new approach for solving the decomposition problem over $E_p^{(m)}$, where we consider a $\mathbb{Z}/p^m \mathbb{Z}$-module isomorphic to $E_p^{(m)}$. The implication is twofold: on one hand, we fix the issue of the inconsistent system (see also beginning of Sect. 3 for additional details and an example where the attack in [24] fails in Sect. 3.2), and on the other hand, we speed up the attack. In particular, this new approach solves the decomposition problem in $O(m^6) \mathbb{Z}/p^m \mathbb{Z}$-operations.

This paper is organized as follows: in Sect. 2 we recall the definitions and properties of the ring $E_p^{(m)}$ and state the DHDP and EGDP protocols over $E_p^{(m)}$. In Sect. 3 we present the practical attack on the DHDP protocol, which in turn will also break the equivalent EGDP protocol. In Sect. 3.2 we show in an example how the attack works.

1.1 Notation

Let $T$ be a subset of a (possibly non-commutative) ring $S$. We will denote the centralizer of $T$ by

$$\text{Cen}(T) = \{ U \in S \mid U R = RU \ \forall \ R \in T \}.$$
When \( T = S \), then \( \text{Cen}(S) \) is said to be the center of \( S \) and will be denoted by \( Z(S) \). Let \( \mathbb{N} \) denote the natural numbers, i.e. \( \mathbb{N} = \{1, 2, \ldots\} \) and \( \mathbb{N}_0 = \mathbb{N} \cup \{0\} \). For any commutative ring \( R \), and any two positive integers \( k, m \in \mathbb{N} \) we will denote by \( \text{Mat}_{k \times m}(R) \) the set of \( k \) by \( m \) matrices with coefficients in \( R \). If \( M \) is an abelian group and \( R \) is a ring acting on \( M \), we denote by \( \text{End}_R(M) \) the set of endomorphisms of \( M \) as an \( R \)-module. Notice that \( \text{End}_R(M) \) has a natural ring structure. Let \( \phi \in \text{End}_R(M) \), we denote by \( R[\phi] \) the smallest subring of \( \text{End}_R(M) \) which contains \( R \) and \( \phi \).

2 The ring \( E_p^{(m)} \) and the decomposition problem

Let us recall the definition of the matrix ring \( E_p^{(m)} \) and its center, which were first introduced in [8, Theorem 1].

**Definition 1** Let \( E_p^{(m)} \) be the following set of matrices.

\[
E_p^{(m)} = \left\{ (a_{ij})_{1 \leq i, j \leq m} \mid a_{ij} \in \mathbb{Z}/p^i\mathbb{Z} \text{ if } i \leq j, \text{ and } a_{ij} \in p^{i-j}\mathbb{Z}/p^i\mathbb{Z} \text{ if } i > j \right\}.
\]

To shorten the notation we will write \( [a_{ij}] = (a_{ij})_{i, j \in \{1, \ldots, m\}} \). This set forms a ring with the addition and multiplication defined, respectively, as follows

\[
[a_{ij}] + [b_{ij}] = \left( a_{ij} + b_{ij} \right) \mod p^i,
\]

\[
[a_{ij}] \cdot [b_{ij}] = \left( \sum_{k=1}^{m} a_{ik} b_{kj} \right) \mod p^i.
\]

Let us denote by \( V \) the set \( \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z} \). The ring \( E_p^{(m)} \) acts on \( V \) by the usual matrix multiplication.

**Theorem 1** [5, Theorem 2] The center \( Z\left( E_p^{(m)} \right) \) of \( E_p^{(m)} \) is given by the set

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

For \( M \in E_p^{(m)} \), let us denote by \( \text{Cen}(M) \) the centralizer of \( M \), i.e. the set of elements \( X \in E_p^{(m)} \), such that \( XM = MX \). Define the set

\[
H(M) = \left\{ \sum_{i=0}^{k} C_i M^i \mid C_i \in Z(E_p^{(m)}), k \in \mathbb{N} \right\}.
\]

Let us recall the Diffie–Hellman decomposition problem, proposed in [22, Example 3].
Definition 2 (DH Decomposition Problem (DHDP)) Let $G$ be a semigroup, $A$, $B \subseteq G$ be two subsemigroups such that $ab = ba$ for every $a \in A$ and $b \in B$ and assume that $x \in G$. Given two elements $a_1 x a_2$ and $b_1 x b_2$, with $a_1, a_2 \in A$ and $b_1, b_2 \in B$, find the element $a_1 b_1 x b_2 a_2$.

In [5], Climent and López-Ramos proposed two protocols based on the decomposition problem over $E_p^{(m)}$, one of the protocols is a Diffie–Hellman key exchange and the other one is an ElGamal protocol, both analogous to the Diffie–Hellman key exchange [9] and the ElGamal cryptosystem [10] respectively.

Protocol 1 (DHDP protocol) Alice and Bob agree on two public elements $M, X \in E_p^{(m)}$ such that $M \not\in \text{Cen}(X)$.

1. Alice chooses $A_1, A_2 \in H(M)$ and sends $G_A = A_1 X A_2$ to Bob.
2. Bob chooses $B_1, B_2 \in \text{Cen}(M)$ such that $B_1 X \neq X B_2$ and sends $G_B = B_1 X B_2$ to Alice.
3. Alice computes $A_1 G_B A_2$.
4. Bob computes $B_1 G_A B_2$.

Since $A_i$ and $B_i$ commute for all $i \in \{1, 2\}$, it is clear that Alice and Bob share a common value.

Protocol 2 (EGDP protocol) Alice and Bob agree on a public element $M \in E_p^{(m)}$. Let $S \in E_p^{(m)}$ be the secret that Bob wants to send Alice.

1. Alice chooses $N \in E_p^{(m)}$ such that $NM \neq MN$ and two elements $A_1, A_2 \in H(M)$ and publishes her public key $(N, A_1 N A_2)$.
2. Bob chooses randomly two elements $B_1, B_2 \in \text{Cen}(M)$ and sends $(F, D) = (B_1 N B_2, S + B_1 A_1 N A_2 B_2)$ to Alice.
3. Alice recovers $S$ by computing $D - A_1 F A_2$.

Since $A_i$ and $B_i$ commute for all $i \in \{1, 2\}$ we have that

$$D - A_1 F A_2 = S + B_1 A_1 N A_2 B_2 - A_1 B_1 N B_2 A_2 = S.$$  

As observed in [5, Theorem 4], breaking the EGDP protocol is equivalent to breaking the DHDP protocol.

3 Solving the decomposition problem in $O(m^6) \mathbb{Z}/p^m \mathbb{Z}$ operations

In this section we provide an algorithm to solve the decomposition problem over $E_p^{(m)}$ and therefore to break the DHDP protocol. It is worth mentioning that in [24] the author claims to have an attack that runs with $O(m^7) \mathbb{Z}/p^m \mathbb{Z}$-operations. Even though the main idea of the attack is correct (i.e. reducing the problem to solving a system of linear equations over $E_p^{(m)}$), it presents an issue when building the actual linear equations. In fact, the equations have different moduli, depending on which row is considered, so the claim that it is enough to solve the system over $\mathbb{Z}/p^m \mathbb{Z}$ is incorrect.
(we provide an explicit example where the attack fails in Sect. 3.2). Moreover, the aforementioned attack would run in $O(m^7)\mathbb{Z}/p^m\mathbb{Z}$-operations, instead our attack runs in $O(m^6)\mathbb{Z}/p^m\mathbb{Z}$-operations, reducing the complexity of the DHDP. As mentioned in Protocols 1 and 2, the two subgroups used are $H(M)$ and Cen($M$) for a publicly known $M \in E_p^{(m)}$.

**Lemma 1** The center of the ring $E_p^{(m)}$ is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$ as rings.

**Proof** It is easy to see that the following map is a ring isomorphism

$$
\psi : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}(E_p^{(m)})
$$

$$
z \mapsto [a_{ij}],
$$

where $a_{ii} = z \mod p^i$ and $a_{ij} = 0$ for $i \neq j$. 

A direct generalization of Theorem 5 in [6] shows that if one considers $\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$ as a $\mathbb{Z}$-module, then $E_p^{(m)}$ is isomorphic to $\text{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z})$. Using this fact and the Cayley–Hamilton Theorem, we can prove that the subring generated by a matrix in $E_p^{(m)}$ is a finite dimensional $\mathbb{Z}$-module. To see this in detail, let us now recall the general statement of the Cayley–Hamilton Theorem.

**Theorem 2** [2, Proposition 2.4] Let $R$ be a ring, let $M$ be a finitely generated $R$-module, let $\phi : M \to M$ be a module morphism and let $I \subset R$ be an ideal of $R$, such that $\phi(M) \subseteq IM$. Let $n \in \mathbb{N}$ be the number of elements needed to generate $M$. Then there exist $a_{n-1}, \ldots, a_0 \in I$, such that

$$
\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0 = 0.
$$

We now prove the corollary we are interested in.

**Corollary 1** For every $A \in E_p^{(m)}$, there exists $a_0, \ldots, a_{m-1} \in \mathbb{Z}$, such that

$$
A^m = a_0 + a_1A + \cdots + a_{m-1}A^{m-1}.
$$

**Proof** In Theorem 2, set $I = R = \mathbb{Z}$ and $M = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$, hence $n = m$ and $\phi$ is a matrix in $E_p^{(m)}$. It follows now immediately that $\mathbb{Z}[\phi]$ has dimension less than or equal to $m$ (as a $\mathbb{Z}$-module).

**Remark 1** Notice that in the statement and the proof of Corollary 1, $\mathbb{Z}$ could as well be replaced by $\mathbb{Z}/p^m\mathbb{Z}$ since any element in $p^m\mathbb{Z}$ acts as the zero morphism over $M$.

**Lemma 2** Let $M \in E_p^{(m)}$. Then the map $\psi : (\mathbb{Z}/p^m\mathbb{Z})[x] \to H(M)$ given by $\psi(f(x)) = f(M)$ is a surjective $\mathbb{Z}/p^m\mathbb{Z}$-algebra homomorphism.

**Proof** First, using Lemma 1 one can identify the center of $E_p^{(m)}$ with $\mathbb{Z}/p^m\mathbb{Z}$, from which follows that the map is well defined. To see that $\psi$ is a surjective homomorphism, it is enough to consider $E_p^{(m)}$ as $\text{End}_{\mathbb{Z}/p^m\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z})$ and to notice that
\[ H(M) \cong \mathbb{Z}/p^m\mathbb{Z}[M] \]: in fact, using Lemma 1, there exist \( u_0, \ldots, u_k \in \mathbb{Z}/p^m\mathbb{Z} \) such that each \( C_i \) of a matrix in \( H(M) \) can be written as the diagonal matrix with entries \( (u_i \mod p, u_i \mod p^2, \ldots, u_i \mod p^m) \).

**Proposition 1** Let \( M, X \in E_p^{(m)} \) and \( G_A = A_1 X A_2 \) for some \( A_1, A_2 \in H(M) \). Then there exists \( \lambda_{11}, \lambda_{12}, \ldots, \lambda_{mm} \in \mathbb{Z}/p^m\mathbb{Z} \) such that

\[ G_A = \sum_{i,j=0}^{m-1} \lambda_{ij} M^i X M^j. \]

**Proof** Combining Lemma 2 and Corollary 1, we can write \( A_1 = \sum_{i=0}^{m-1} u_i M^i \) and \( A_2 = \sum_{i=0}^{m-1} v_i M^i \) for some \( u_0, \ldots, u_{m-1}, v_0, \ldots, v_{m-1} \in \mathbb{Z}/p^m\mathbb{Z} \). Then

\[ G_A = A_1 X A_2 = \left( \sum_{i=0}^{m-1} u_i M^i \right) X \left( \sum_{j=0}^{m-1} v_j M^j \right) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} u_i v_j M^i X M^j = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \lambda_{ij} M^i X M^j, \]

for \( \lambda_{ij} = u_i v_j \). \( \square \)

### 3.1 The pseudo-\( E_p^{(m)} \) approach

In this subsection we solve the linear system given in Proposition 1 by defining the following \( \mathbb{Z}/p^m\mathbb{Z} \)-modules:

**Definition 3** Let \( F_p^{(m)} \subseteq \text{Mat}_{m \times m}(\mathbb{Z}/p^m\mathbb{Z}) \) be the following set of matrices.

\[ F_p^{(m)} = \left\{ (a_{ij})_{i,j \in \{1,\ldots,m\}} \mid a_{ij} \in p^\ell \mathbb{Z}/p^m\mathbb{Z} \text{ where } \ell = \max(m-i, m-j) \right\}. \]

It is easy to check that \( F_p^{(m)} \) is a \( \mathbb{Z}/p^m\mathbb{Z} \)-submodule of \( \text{Mat}_{m \times m}(\mathbb{Z}/p^m\mathbb{Z}) \). Moreover the following proposition shows that \( F_p^{(m)} \) is isomorphic to \( E_p^{(m)} \) as \( \mathbb{Z}/p^m\mathbb{Z} \)-modules, where the scalar multiplication in \( E_p^{(m)} \) is as follows: for \( r \in \mathbb{Z}/p^m\mathbb{Z} \) and \( [a_{i,j}] \in E_p^{(m)} \) we have that

\[ r[a_{i,j}] = [ra_{i,j}] = \left( ra_{i,j} \mod p^i \right)_{i,j \in \{1,\ldots,m\}}. \]
On the algebraic structure of $E_p^{(m)}$ and applications to...

Proposition 2 $E_p^{(m)}$ is isomorphic to $F_p^{(m)}$ as $\mathbb{Z}/p^m\mathbb{Z}$-modules.

Proof One can easily check that the following map is an isomorphism between $E_p^{(m)}$ and $F_p^{(m)}$

$$\delta : \quad E_p^{(m)} \rightarrow F_p^{(m)}$$

$$(a_{ij})_{i,j \in \{1, \ldots, m\}} \mapsto (a_{ij} p^{m-i})_{i,j \in \{1, \ldots, m\}}.$$ 

Corollary 2 Let $M_1, M_2, \ldots, M_k, G \in E_p^{(m)}$. Then $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in (\mathbb{Z}/p^m\mathbb{Z})^k$ is a solution for $\sum_{i=1}^{k} \lambda_i M_i = G$ if and only if $\sum_{i=1}^{k} \lambda_i \delta(M_i) = \delta(G)$.

Proof The proof follows directly by applying the isomorphism $\delta$ to both sides of the equation $\sum_{i=1}^{k} \lambda_i M_i = G$. 

Now we are ready for the main result.

Theorem 3 DHDP protocol over $E_p^{(m)}$ can be broken in polynomial time.

Proof Let $M, X \in E_p^{(m)}$ such that $MX \neq XM$, and let $A_1, A_2 \in H(M)$ and $B_1, B_2 \in \text{Cen}(M)$. Given $M, X, G_A = A_1 X A_2$ and $G_B = B_1 X B_2$, we have to find $A_1 G_B A_2$.

Using Proposition 1, we know that there exist $\lambda_{11}, \ldots, \lambda_{mm} \in \mathbb{Z}/p^m\mathbb{Z}$ such that $G_A = \sum_{i,j=0}^{m-1} \lambda_{ij} M^i X M^j$. We use Corollary 2 to solve this system of linear equations for $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{mm}$. Then the exchanged secret is given by

$$\sum_{i,j=0}^{m-1} \lambda_{ij} M^i G_B M^j = \sum_{i,j=0}^{m-1} \lambda_{ij} M^i B_1 X B_2 M^j$$

$$= \sum_{i,j=0}^{m-1} \lambda_{ij} B_1 M^i X M^j B_2$$

$$= B_1 \left( \sum_{i,j=0}^{m-1} \lambda_{ij} M^i X M^j \right) B_2$$

$$= A_1 G_B A_2 = B_1 G_A B_2.$$ 

Algorithm 1 provides a formal way to solve the DHDP protocol over $E_p^{(m)}$. 

Running time. The running time of Algorithm 1 is given by solving $m^2$ linear equations in $m^2$ unknowns over $\mathbb{Z}/p^m\mathbb{Z}$, which costs $O((m^2)^3) \mathbb{Z}/p^m\mathbb{Z}$-operations, or $O(m^8 \log(p)^2)$ bit operations. In [8], Climent et. al. proposed to use the DHDP protocol and EGDP protocol for the parameters $p = 2$ and $m = 128$. In our implementation, Algorithm 1 took 23.1 days to break these parameters. The results were obtained by a MAGMA [4] implementation using a personal computer with processor Intel Core 6C i7-8700K at 3.7 GHz and 64 GB RAM (see www.math.uzh.ch/aa/uploads/media/attack_CLR.txt).
Algorithm 1 Break protocol based on DHDP over $E_p^{(m)}$ using pseudo-$E_p^{(m)}$

Input: $M, X, G_A, G_B \in E_p^{(m)}$
Output: the exchanged secret $A_1G_BA_2 \in E_p^{(m)}$

1: Construct the matrix of linear equations arising from $A_1XA_2 = G_A$ using Proposition 1, given by

$$G_A = m^{-1}\sum_{i,j=0}^{m-1} \lambda_{ij}M^iXM^j,$$

where $\lambda_{ij}$’s are unknown.

2: Apply the $\mathbb{Z}/p^m\mathbb{Z}$-module isomorphism $\delta$ mentioned in Lemma 2 to the above equation

$$\delta(G_A) = m^{-1}\sum_{i,j=0}^{m-1} \lambda_{ij}\delta(M^iXM^j).$$

3: Solve the system of $m^2$ linear equations in $m^2$ unknowns over $\mathbb{Z}/p^m\mathbb{Z}$, generated by equating entries of above matrix equality. By Proposition 1 and Corollary 2, such a solution exists.

4: Return $\sum_{i,j=0}^{m-1} \lambda_{ij}M^iG_BM^j$.

3.2 A $2 \times 2$ example

In the following we provide an example, which serves two purposes, first it shows the Algorithm 1 in practice and second it provides an example where the claimed attack in [24] does not work.

Let $m = 2$, $p = 5$ and let $M = \begin{bmatrix} 4 & 3 \\ 15 & 20 \end{bmatrix}$ and $X = \begin{bmatrix} 0 & 4 \\ 15 & 4 \end{bmatrix}$ be public elements.

Alice chooses

$$A_1 = \begin{bmatrix} 1 & 3 \\ 15 & 17 \end{bmatrix} \quad A_2 = \begin{bmatrix} 0 & 3 \\ 15 & 11 \end{bmatrix}$$

and publishes $G_A = \begin{bmatrix} 0 & 1 \\ 20 & 23 \end{bmatrix}$. Bob chooses

$$B_1 = \begin{bmatrix} 3 & 3 \\ 15 & 9 \end{bmatrix} \quad B_2 = \begin{bmatrix} 3 & 0 \\ 0 & 18 \end{bmatrix}$$

and publishes $G_B = \begin{bmatrix} 0 & 2 \\ 5 & 3 \end{bmatrix}$. The shared secret is then

$$A_1G_BA_2 = B_1G_AB_2 = \begin{bmatrix} 0 & 1 \\ 15 & 21 \end{bmatrix}.$$

The attacker sees only $M, X, G_A, G_B$ and wants to find $A_1G_BA_2 \in E_5^{(2)}$. 

\textcopyright Springer
In Step 1 of Algorithm 1, the attacker constructs

\[ G_A = \sum_{i,j=0}^{m-1} \lambda_{ij} M^i X M^j \]

\[ = \lambda_{00} \begin{bmatrix} 0 & 4 \\ 15 & 4 \end{bmatrix} + \lambda_{01} \begin{bmatrix} 10 & 5 \\ 20 & 0 \end{bmatrix} + \lambda_{10} \begin{bmatrix} 20 & 3 \\ 0 & 15 \end{bmatrix} + \lambda_{11} \begin{bmatrix} 0 & 20 \\ 0 & 0 \end{bmatrix}. \]  

(1)

In the second step the attacker applies \( \delta \) getting

\[ \delta(G_A) = \begin{bmatrix} 0 & 5 \\ 20 & 23 \end{bmatrix} = \lambda_{00} \begin{bmatrix} 0 & 20 \\ 15 & 4 \end{bmatrix} + \lambda_{01} \begin{bmatrix} 0 & 0 \\ 20 & 0 \end{bmatrix} + \lambda_{10} \begin{bmatrix} 0 & 15 \\ 0 & 0 \end{bmatrix} + \lambda_{11} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \]

From this we get the system of \( m^2 \) linear equations in \( m^2 \) unknowns \( \lambda_{ij} \), but since we applied \( \delta \) these are now equations over \( \mathbb{Z}/pm\mathbb{Z} \):

\[
\begin{align*}
0\lambda_{00} + 0\lambda_{01} + 0\lambda_{10} + 0\lambda_{11} &= 0, \\
20\lambda_{00} + 0\lambda_{01} + 15\lambda_{10} + 0\lambda_{11} &= 5, \\
15\lambda_{00} + 20\lambda_{01} + 0\lambda_{10} + 0\lambda_{11} &= 20, \\
4\lambda_{00} + 0\lambda_{01} + 15\lambda_{10} + 0\lambda_{11} &= 23.
\end{align*}
\]

One particular solution of this system over \( \mathbb{Z}/p^m\mathbb{Z} \) is given by

\((\lambda_{00}, \lambda_{01}, \lambda_{10}, \lambda_{11}) = (2, 22, 1, 0)\).

The attacker now computes

\[
\sum_{i,j=0}^{m-1} \lambda_{ij} M^i G_B M^j = 2G_B + 22G_B M + 1MG_B + 0MG_B M
\]

\[= \begin{bmatrix} 0 & 1 \\ 15 & 21 \end{bmatrix} = A_1 G_B A_2.\]

Compared to our attack, the approach presented in [24] does not make use of Lemmas 1, 2 and Corollary 2. Instead the elements of \( Z(E_p^{(m)}) \) are seen as diagonal matrices having entries \( (a_0, a_0 + pa_1, \ldots, a_0 + pa_1 + \cdots + p^{m-1}a_{m-1}) \) where \( 0 \leq a_0, a_1, \ldots, a_{m-1} \leq p - 1 \). Using this representation and Cayley–Hamilton theorem results in a linear system over \( E_p^{(m)} \) of \( m^2 \) equations in \( m^3 \) unknowns, as mentioned in Theorem 2 of [24]. One should observe that this system does not necessarily admit a solution over \( \mathbb{Z}/p^m\mathbb{Z} \), which is the approach used in [24]. The above mentioned example provides an instance where this approach fails.

Using the approach in [24], the analogue of Eq. (1) is

\[ G_A = \sum_{i,j=0}^{m-1} W_{ij} M^i X M^j. \]
where \( W_{ij} = \begin{bmatrix} a_{ij}^0 & 0 \\ 0 & a_{ij}^0 + 5a_{ij}^1 \end{bmatrix} \in Z(E_p^{(m)}) \). This results in the following system of linear equations:

\[
\begin{align*}
0a_{00}^0 + 0a_{10}^0 + 0a_{01}^0 + 0a_{11}^0 + 0a_{00}^{10} + 0a_{10}^{10} + 0a_{01}^{10} + 0a_{11}^{10} + 0a_{11}^{11} &= 0 \mod 5, \\
4a_{00}^0 + 0a_{10}^0 + 0a_{01}^0 + 0a_{11}^0 + 15a_{00}^{10} + 0a_{10}^{10} + 0a_{01}^{10} + 0a_{11}^{10} + 0a_{11}^{11} &= 5 \mod 5, \\
15a_{00}^0 + 0a_{10}^0 + 0a_{01}^0 + 0a_{11}^0 + 0a_{00}^{10} + 0a_{10}^{10} + 0a_{01}^{10} + 0a_{11}^{10} + 0a_{11}^{11} &= 20 \mod 25, \\
4a_{00}^0 + 20a_{01}^0 + 0a_{10}^0 + 0a_{11}^0 + 15a_{00}^{10} + 5a_{10}^{10} + 0a_{01}^{10} + 0a_{11}^{10} + 0a_{11}^{11} &= 23 \mod 25.
\end{align*}
\]

In Section 4 of [24], the author claims that it is enough to consider this system over \( \mathbb{Z}/25\mathbb{Z} \). However in this example the claim does not hold and shows that the approach used in [24] to solve a linear system over \( E_p^{(m)} \) is incorrect.

Acknowledgements We would like to thank Alessandro Neri for fruitful discussions and Juan-Antonio López-Ramos and Joan-Josep Climent for bringing [24] to our knowledge. The authors would also like to thank the anonymous reviewers for their helpful comments. The second author is thankful to the Swiss National Science Foundation under Grant Number 171249. This work has also been supported partly by the Swiss National Science Foundation under Grant Number 169510.

References

1. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Math. Res. Lett. 6, 287–292 (1999)
2. Atiyah, M., MacDonald, I.G.: Introduction to Commutative Algebra. Addison-Wesley Series in Mathematics. Avalon Publishing, New York (1994)
3. Bergman, G.M.: Some examples in PI ring theory. Israel J. Math. 18(3), 257–277 (1974)
4. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. 24(3–4), 235–265 (1997). (Computational algebra and number theory (London, 1993))
5. Climent, J., Ramos, J.A.L.: Public key protocols over the Ring \( E_p^{(m)} \). Adv. Math. Commun. 10(4), 861–870 (2016)
6. Climent, J.-J., Navarro, P.R., Tortosa, L.: On the arithmetic of the endomorphisms ring end \( (\mathbb{Z}_p \times \mathbb{Z}_p^2) \). Appl. Algebra Eng. Commun. Comput. 22(2), 91–108 (2011)
7. Climent, J.-J., Navarro, P.R., Tortosa, L.: Key exchange protocols on noncommutative rings. The case of End \( (\mathbb{Z}_p \times \mathbb{Z}_p^2) \). Int. J. Comput. Math. 89(13–14), 1753–1763 (2012)
8. Climent, J.-J., Navarro, P.R., Tortosa, L.: An extension of the noncommutative Bergman’s ring with a large number of noninvertible elements. Appl. Algebra Eng. Commun. Comput. 25(5), 347–361 (2014)
9. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory 22(6), 644–654 (1976)
10. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory 31(4), 469–472 (1985)
11. Kamal, A.A., Youssef, A.M.: Cryptanalysis of a key exchange protocol based on the endomorphisms ring \( (\mathbb{Z}_p \times \mathbb{Z}_p^2) \). Appl. Algebra Eng. Commun. Comput. 23(3), 143–149 (2012)
12. Ko, K.H., Lee, J.W., Thomas, T.: Towards generating secure keys for braid cryptography. Des. Codes Cryptogr. 45(3), 317–333 (2007)
13. Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J., Park, C.: New public-key cryptosystem using braid groups. In: Annual International Cryptology Conference, pp. 166–183. Springer (2000)
14. López-Ramos, J.A., Rosenthal, J., Schipani, D., Schnyder, R.: Group key management based on semigroup actions. J. Algebra Appl. 16(8), 1750148 (2017)
15. Maze, G., Monico, C., Rosenthal, J.: Public key cryptography based on semigroup actions. Adv. Math. Commun. 1(4), 489–507 (2007)
16. Menezes, A.J., Wu, Y.-H.: The discrete logarithm problem in $GL(n, q)$. Ars Comb. 47, 23–32 (1997)
17. Micheli, G.: Cryptanalysis of a non-commutative key exchange protocol. Adv. Math. Commun. 9(2), 247–253 (2015)
18. Micheli, G., Weger, V.: Cryptanalysis of the CLR-cryptosystem. Des. Codes Cryptogr. 87(5), 1069–1086 (2018)
19. Myasnikov, A., Shpilrain, V., Ushakov, A.: Group-Based Cryptography. Springer, Berlin (2008)
20. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21(2), 120–126 (1978)
21. Sakalauskas, E., Burba, T.: Basic semigroup primitive for cryptographic session key exchange protocol (SKEP). Inf. Technol. Control 3, 28 (2003)
22. Shpilrain, V., Zapata, G.: Combinatorial group theory and public key cryptography. Appl. Algebra Eng. Commun. Comput. 17, 11 (2004)
23. Sidelnikov, V.M. Cherepnev, M.A., Yashchenko, V.V.: Systems of open distribution of keys on the basis of noncommutative semigroups. In: Russian Academy of Sciences-Doklady Mathematics, Vol. 48, pp. 384–386. Providence: American Mathematical Society c1993- (1994)
24. Zhang, Y.: Cryptanalysis of a key exchange protocol based on the ring $E^{(m)}_p$. Appl. Algebra Eng. Commun. Comput. 29(2), 103–112 (2018)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.