CRYPTANALYSIS OF THE CLR-CRYPTOSYSTEM

GIACOMO MICHELI AND VIOLETTA WEGER

Abstract. In this paper we break a variant of the El-Gamal cryptosystem for a ring action of the matrix space $E_p^{(m)}$ on $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$. Also, we describe a general vulnerability of the protocol using tools from p-adic analysis.

1. Introduction

Due to the threat coming from quantum computing, recently there has been a great interest in building new public key cryptographic schemes based on new primitives (for an overview of the post-quantum world, see [1]). The most popular proposals for post-quantum cryptography are lattice based (see for example [2]), coding based (see for example [3]), or based on multivariate quadratic equations (see for example [4]). Nevertheless, the mathematics and cryptography community is trying to come up with new schemes which will allow more reasonable key sizes and similar security (see for example [5, 6, 7, 8, 9, 10, 11, 13]). These schemes often involve exotic ambient spaces and very original settings which often do not prevent them from classical attacks as most of the structure can be exploited.

In [14] J.J. Climent and J.A. López-Ramos propose a cryptosystem over the ring $E_p^{(m)}$, which is a special ring of matrices involving operations modulo different powers of the same prime (see Definition 1 of this paper). This ring is a generalization of the ring E_p, Climent, Navarro and Tartosa introduced in [15]. The ring $E_p^{(m)}$ admits only few invertible elements [16, Corollary 1], for which it avoids most of the attacks (see [17]). In addition, another nice property of such rings is that they do not admit embeddings into matrix rings over a field (see [18]), which is often the main problem of cryptographic schemes over matrix rings (see for example [19] supported also by the results in [12]).

In this paper we explain that the scheme is breakable also in this case: the attack we propose in fact comes essentially from a surjection from a subring of the $(m \times m)$-matrix ring over the field of p-adic numbers onto the ring $E_p^{(m)}$ (see Section 3). In Section 4 we explain the attack in detail and show that we can extract the secret key by a descent argument through a finite number of congruences which at each step sieves out possible solutions coming from the previous step (Proposition 15). In Subsection 4.1 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

$$\mathrm{Cen}(T) = \{U \in S \mid UR = RU \ \forall \ R \in T\}.$$

Key words and phrases. Finite Fields; Cryptography; p-adic numbers.

The first author is thankful to Swiss National Science Foundation grant number 171248.

When $T = S$, then $\mathrm{Cen}(S)$ is said to be the center of S and will be denoted by $Z(S)$. Let $\mathbb{N}$ denote the natural numbers, i.e. $\mathbb{N} = \{1, 2, \dots\}$ 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 $\mathrm{Mat}_{k\times m}(R)$ the set of k by m matrices with coefficients in R.

2. Cryptography over $E_p^{(m)}$

Climent and López-Ramos presented in [14] a cryptosystem in a non-commutative setting based on the Semigroup Action Problem described in [7]. A similar cryptosystem can be found in [20, Example 4.3.c].

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

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

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

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

A description of $E_p^{(m)}$ is given in [16, Theorem 1]. 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 2. *[14, Theorem 2] The center of $E_p^{(m)}$ is given by the set*

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

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

The CLR-cryptosystem presented in [14] consists of the following protocol.

Protocol 3. *Let $M \in E_p^{(m)}$ and $R \in V$.*

1. *Alice chooses $F \in \mathrm{Cen}(M)$ and computes $T = F \cdot R$.*
2. *Alice publishes (M, R, T) and keeps private F.*
3. *Bob chooses randomly*

$$G = \sum_{i=0}^{k} C_i M^i,$$

where $C_i \in Z\left(E_p^{(m)}\right)$ and $k \in \mathbb{N}$. Let $S \in V$ be the message.

4. *Bob computes*

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

5. *Bob sends (H, D) to Alice.*

6. *Alice can recover the message by computing*

$$D - F \cdot H = S + G \cdot (F \cdot R) - F \cdot (G \cdot R) = S.$$

As observed in [14] the matrices G, F and M should not be chosen in the center of $E_p^{(m)}$, since then it is enough to find $X \in E_p^{(m)}$, s.t. $X \cdot R = T$ to break the cryptosystem.

3. A vulnerability of the protocol based on p-adic analysis

Let us denote by $\mathbb{Z}_p$ the p-adic integers and $\mathbb{Q}_p$ the set of p-adic numbers. In this section we present what we believe being the main mathematical weakness of the scheme, which comes from lifting the cryptographic primitive to a certain ring defined using p-adic numbers.

Definition 4. Let $T_p^{(m)}$ be the following set.

$$T_p^{(m)} = \left\{ [a_{ij}] \in \mathrm{Mat}_{m \times m}(\mathbb{Z}_p) \;\middle|\; a_{ij} \in p^{i-j}\mathbb{Z}_p \text{ if } i > j \right\}.$$

Remark 5. We have a map ϕ, from $T_p^{(m)}$ to $E_p^{(m)}$, which reduces the row i modulo p^i, for all $i \in \{1, \dots, m\}$.

Proposition 6. *We have the following properties of $T_p^{(m)}$ and ϕ.*

i) *$T_p^{(m)}$ defines a ring with the matrix addition and matrix multiplication.*
ii) *The map ϕ is well-defined.*
iii) *The map ϕ is surjective.*
iv) *ϕ is a ring homomorphism.*
v) *The kernel of ϕ is given by*

$$\mathrm{Ker}(\phi) = \left\{ [a_{ij}] \in T_p^{(m)} \;\middle|\; a_{ij} \in p^i\mathbb{Z}_p, \; \forall\, 1 \le i \le m \right\}.$$

vi) $\mathrm{Ker}(\phi)$ *is a two-sided ideal in $T_p^{(m)}$.*

Proof. i)-iii) The properties ii) and iii) follow immediately if $T_p^{(m)}$ is a ring. Hence it is enough to prove the first property. For $T_p^{(m)}$ to be a ring it is enough to check closedness under multiplication, the rest follows as then $T_p^{(m)}$ is clearly a subring of $\mathrm{Mat}_{m\times m}(\mathbb{Z}_p)$. Let $[a_{ij}]$ and $[b_{ij}]$ be in $T_p^{(m)}$, and denote by $[c_{ij}]$ their product. For $i > j$, we have that

$$c_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}.$$

We want to show that $c_{ij} \in p^{i-j}\mathbb{Z}_p$. In fact, for all $k \in \{1, \dots, j-1\}$ we have that $a_{ik} \in p^{i-k}\mathbb{Z}_p \subset p^{i-j}\mathbb{Z}_p$, hence also $a_{ik}b_{kj}$ is in $p^{i-j}\mathbb{Z}_p$. Analogously, for all $k \in \{i+1, \dots, m\}$ we have that $b_{kj} \in p^{k-j}\mathbb{Z}_p \subset p^{i-j}\mathbb{Z}_p$ and hence also $a_{ik}b_{kj}$ is in $p^{i-j}\mathbb{Z}_p$. And for $k \in \{j, \dots, i\}$ we have that $a_{ik}b_{kj} \in p^{i-k}p^{k-j}\mathbb{Z}_p = p^{i-j}\mathbb{Z}_p$.

iv) For addition this is clear, we only need to prove the multiplication part. For all $[a_{ij}], [b_{ij}] \in T_p^{(m)}$ we want to show that

$$\phi([a_{ij}] \cdot_{T_p^{(m)}} [b_{ij}]) = \phi([a_{ij}]) \cdot_{E_p^{(m)}} \phi([b_{ij}]).$$

For $k \in \{i, \dots, m\}$, since

$$\left(\mathbb{Z}_p/p^k\mathbb{Z}_p\right)/p^i\mathbb{Z}_p \cong \mathbb{Z}_p/p^i\mathbb{Z}_p$$

we have that

$$(a_{ik}b_{kj}) \mod p^i \equiv (a_{ik} \mod p^i)(b_{kj} \mod p^k) \mod p^i.$$

For $k \in \{1, \dots, i-1\}$ we know that $a_{ik} \in p^{i-k}\mathbb{Z}_p$ and then since

$$p^{i-k}\mathbb{Z}_p/p^i\mathbb{Z}_p \cong \mathbb{Z}_p/p^k\mathbb{Z}_p$$

we have that

$$(a_{ik}b_{kj}) \mod p^i \equiv (a_{ik} \mod p^i)(b_{kj} \mod p^k) \mod p^i.$$

v)-vi) These properties follow immediately by the definition of ϕ and the fact that ϕ is a ring homomorphism.

$\square$

Observe that with Proposition 6 we have that

$$E_p^{(m)} \cong T_p^{(m)}/\operatorname{Ker}(\phi).$$

There exists an action of $T_p^{(m)}$ on $\mathbb{Z}_p^m$. Let us denote by ψ the map from $\mathbb{Z}_p^m$ to V, which reduces the row i modulo p^i for all $i \in \{1, \dots, m\}$. We get the following diagram:

$$\begin{array}{ccc} T_p^{(m)} \times \mathbb{Z}_p^m & \xrightarrow{\alpha} & \mathbb{Z}_p^m \\ {\scriptstyle (\phi,\psi)}\big\downarrow & & \big\downarrow{\scriptstyle \psi} \\ E_p^{(m)} \times V & \xrightarrow{\beta} & V \end{array}$$

where α is the action that provides a structure of left $T_p^{(m)}$-module on $\mathbb{Z}_p^m$ and β makes V a left $E_p^{(m)}$-module.

Remark 7. The maps ϕ, ψ commute with the actions, i.e. for any $t \in T_p^{(m)}$ and $u \in \mathbb{Z}_p^m$ we have that $\psi(t(u)) = \phi(t)(\psi(u))$.

We want to show the main weakness of Protocol 3. The actual attack will be provided in Section 4. We take an instance of the problem over $E_p^{(m)}$, i.e. (M, R, T) and lift this instance to $T_p^{(m)}$. Now we want to solve the problem over $\mathbb{Q}_p$, which means to solve the following system of linear equations

$$\begin{aligned} XM &= MX, \\ X \cdot R &= T. \end{aligned} \tag{3.1}$$

If $\mathcal{M}$ is a locally compact group endowed with Haar measure (such as $(\mathrm{Mat}_{m\times m}(\mathbb{Q}_p), +)$), we will say that a certain property is *generic* or *generically* holds over $\mathcal{M}$, if the measure of the set where the property is not satisfied is zero.

Proposition 8. *Generically, the system* (3.1) *has a solution in* $\mathrm{Mat}_{m\times m}(\mathbb{Q}_p)$.

Proof. Note that

$$\{\mathrm{Id}, M, \ldots, M^{m-1}\} \subseteq \mathrm{Cen}(M).$$

Observe that for a fixed degree m, the set of monic non-squarefree polynomials is exactly

$$\{f \in \mathbb{Q}_p[x]_{\leq m} \mid \mathrm{Disc}(f) = 0\}$$

which is Zariski closed. Therefore, the set of squarefree polynomials has Haar measure 1. It follows that almost all (up to a density zero set of matrices) matrices M have all distinct eigenvalues in $\overline{\mathbb{Q}}_p$, which in turn implies that the set of matrices M for which $\{\mathrm{Id}, M, \ldots, M^{m-1}\}$ are $\mathbb{Q}_p$-linearly dependent has measure zero. Therefore, since the M^i are generically linearly independent on $\mathbb{Q}_p$ for $i \in \{0, \ldots, m-1\}$, we get that $\dim(\mathrm{Cen}(M)) \geq m$. Thus we have at most $m^2 - m$ equations arising from the condition $XM = MX$. With the equations from $X \cdot R = T$, we get therefore at most m^2 equations in m^2 unknowns, thus generically this system is solvable over $\mathbb{Q}_p$. $\square$

The following proposition describes a case in which the solution is always guaranteed to exist also in the ring of p-adic integers.

Proposition 9. *Let $A \in \mathrm{Mat}_{n\times n}(\mathbb{Z}_p)$ be invertible over $\mathbb{Q}_p$. Let $b \in \mathbb{Z}_p^n$. Suppose that there exists a solution of $Ax = b$ in $(\mathbb{Z}_p/\det(A)\mathbb{Z}_p)^n$. Then there exists a solution of $Ax = b$ in $\mathbb{Z}_p^n$.*

Proof. Clearly $Ax = b$ has a solution in $\mathbb{Q}_p^n$ since A is invertible over $\mathbb{Q}_p$. Let A^+ be the adjoint matrix of A. Clearly $A^+ \in \mathrm{Mat}_{n\times n}(\mathbb{Z}_p)$. Let $u \in (\mathbb{Z}_p/\det(A)\mathbb{Z}_p)^n$ be a solution of $Ax = b$, such that

$$Au \equiv b \mod \det(A)\mathbb{Z}_p.$$

Multiplying by A^+ we get

$$\det(A)u = A^+b \mod \det(A)\mathbb{Z}_p.$$

So it follows that

$$0 \equiv A^+b \mod \det(A)\mathbb{Z}_p.$$

Hence we have that

$$\det(A) \mid (A^+b),$$

which means $\det(A)$ divides each component of A^+b. Let us now go back to $Ax = b$ over $\mathbb{Q}_p$. There exists a solution, say v in $\mathbb{Q}_p^n$, such that $Av = b$. Then $\det(A)v = A^+b$ over $\mathbb{Q}_p$. But then since $\det(A) \mid (A^+b)$, A^+b can be written as

$$(A^+b) = \det(A)w$$

for some $w \in \mathbb{Z}_p^n$. This forces that

$$\det(A)v = \det(A)w$$

and hence $v = w \in \mathbb{Z}_p^n$. $\square$

Remark 10. Let A be the matrix representation of the system (3.1), as we already observed in the proof of Proposition 8 we have that A is in $\mathrm{Mat}_{m^2\times m^2}(\mathbb{Z}_p)$. If the valuation

$$\nu_p(\det(A)) \leq 1,$$

then the system (3.1) has a solution over $\mathbb{Z}_p$: in fact, either $\det(A)$ is a unit over $\mathbb{Z}_p$ and hence invertible there, or p divides only once $\det(A)$ and we have that

$$\mathbb{Z}_p/\det(A)\mathbb{Z}_p \cong \mathbb{F}_p.$$

And since there exists a solution (the private key F) of the system over $E_p^{(m)}$, there also exists a solution over $\mathbb{F}_p$, as we have the projection map of $E_p^{(m)}$ in $\mathrm{Mat}_{m\times m}(\mathbb{Z}/p\mathbb{Z})$. And thus we have that the conditions of Proposition 9 are satisfied.

In the next section we produce an attack which works for any instance of the problem over $E_p^{(m)}$.

4. The practical attack

We will first give an efficient algorithm to solve a system of congruences modulo p^i. Let $\mathcal{R}$ be a local unitary commutative ring with principal maximal ideal $\mathfrak{m} = (p) \subseteq \mathcal{R}$. Notice that $\mathcal{R}$ does not have to be a domain. Let k be the order of nilpotence of $\mathcal{R}$, i.e.

$$k = \min\{n \in \mathbb{N} \cup \{\infty\} \mid \mathfrak{m}^n = 0\}.$$

Observe that if $k = \infty$, then $\mathcal{R}$ is a domain. We will assume in the following that $k \neq \infty$.

Definition 11. Let ν be the pseudo-valuation function defined as

$$\begin{array}{rcl} \nu : \mathcal{R} & \to & \{0, \dots, k\} \\ u & \mapsto & \nu(u) = \max\{n \in \{0, \dots, k\} \mid u \in \mathfrak{m}^n\}, \end{array}$$

where $\mathfrak{m}^0 = \mathcal{R}$.

Proposition 12. *We have the following properties of ν.*

i) *$\forall x \in \mathcal{R}$, if $\nu(x) = 0$, then x is invertible in $\mathcal{R}$.*
ii) *$\forall x, y \in \mathcal{R}$, we have that $\nu(xy) = min\{k, \nu(x) + \nu(y)\}$.*
iii) *Let k be the order of nilpotence of $\mathcal{R}$ and $c \in \mathcal{R}$. Write $c = c'p^{\nu(c)}$ for some invertible $c' \in \mathcal{R}$. Let $a \leq \nu(c)$. The set of solutions of*

$$p^a x = c$$

is given by

$$p^{\nu(c)-a}c' + p^{k-a}\mathcal{R}.$$

Proof. i) Let $x \in \mathcal{R}$ be s.t. $\nu(x) = 0$, then $x \notin \mathfrak{m}$. If we look at (x), which is the ideal generated by x, then since $(x) \not\subseteq \mathfrak{m}$, we have that $(x) = \mathcal{R}$. Hence x is invertible in $\mathcal{R}$.

ii) Let $\nu(x) = s$ and $\nu(y) = t$. If $s + t < k$, then clearly $xy \in \mathfrak{m}^s\mathfrak{m}^t = \mathfrak{m}^{s+t}$. It is enough to show that $xy \notin \mathfrak{m}^{s+t+1}$. By definition we can write

$$\begin{array}{rcl} x & = & x'p^s, \\ y & = & y'p^t, \end{array}$$

where $\nu(x') = \nu(y') = 0$. By i) we have that x', y' and therefore also $x'y'$ are invertible in $\mathcal{R}$. Now we can write

$$xy = x'y'p^{s+t} \notin \mathfrak{m}^{s+t+1}.$$

Hence $\nu(xy) = s + t = \min\{k, s + t\}$.
If $s + t \geq k$, then $xy \in \mathfrak{m}^k = 0$, hence $\nu(xy) = k = \min\{k, s + t\}$.

iii) First observe that solving $p^a x = c$ is equivalent to solving

$$p^a(x - p^{\nu(c)-a}c') = 0.$$

Clearly

$$x \in p^{\nu(c)-a}c' + p^{k-a}\mathcal{R}$$

solves $p^a x = c$. We want to prove that these are *all* the solutions. Let $\bar{x}$ be any solution of $p^a x = c$, hence

$$p^a(\bar{x} - p^{\nu(c)-a}c') = 0.$$

We have that

$$\nu(p^a(\bar{x} - p^{\nu(c)-a}c')) = k.$$

By ii) we have that

$$\begin{aligned} k &= \nu(p^a(\bar{x} - p^{\nu(c)-a}c')) \\ &= \min\{k, a + \nu(\bar{x} - p^{\nu(c)-a}c')\}. \end{aligned}$$

Thus

$$\nu(\bar{x} - p^{\nu(c)-a}c') \geq k - a.$$

And then since

$$\bar{x} - p^{\nu(c)-a}c' \in p^{k-a}\mathcal{R}$$

we have the claim.

□

Solving linear systems over chain rings such as $\mathcal{R}$ is a well known problem. In what follows we produce an algorithm to solve a system over $\mathcal{R}$, obtaining the solutions in a special format, which will be suitable for our cryptanalytic purposes. For related work see for example [21, 22, 23].

A classic result is the Smith normal form for square matrices with entries over a principal ideal domain. We now give an algorithm to compute the analogous of such normal form for rectangular matrices over $\mathcal{R}$. In turn, this will allow us to solve systems of linear equations over $\mathcal{R}$.

Lemma 13. *Let $B \in \mathrm{Mat}_{\ell\times h}(\mathcal{R})$ with $\ell \leq h$. Then for some $\bar{\ell} \leq \ell$ there exist $S \in GL_\ell(\mathcal{R})$ and $T \in GL_h(\mathcal{R})$, s.t.*

$$B' = SBT = \begin{bmatrix} b_{r_1c_1} & & 0 & \\ & \ddots & & 0 \\ 0 & & b_{r_{\bar{\ell}}c_{\bar{\ell}}} & \\ & 0 & & 0 \end{bmatrix}, \tag{4.1}$$

with the property

$$\nu(b_{r_ic_i}) \leq \nu(b_{r_jc_j}) \ \forall\ 1 \leq i \leq j \leq \bar{\ell}.$$

Moreover this form can be computed in polynomial time.

Proof. Applying Algorithm 1 brings B in the desired form. The idea of the algorithm is to bring the element with the minimal pseudo-valuation to the pivot position and then use this entry to delete all other entries in this row and column. Then we iterate this procedure for the next pivot position.

Observe that step 9 of Algorithm 1 can be performed thanks to the choice made in step 7. Algorithm 1 clearly ends in polynomial time as it only involves pivot

Algorithm 1 Reduced form over $\mathcal{R}$

Input: $B \in \mathrm{Mat}_{\ell \times h}(\mathcal{R})$ with $\ell \leq h$
Output: $(S, T, B', \mathrm{rk}(B))$, where B' is of the form (4.1)

$k \leftarrow 1$
$B_1 \leftarrow B$
$C_1 \leftarrow B$
$S \leftarrow \mathrm{Id}$
$T \leftarrow \mathrm{Id}$
while $k \leq \ell$ and C_k is not the zero matrix **do**
  In the submatrix C_k, find a pair of indices $(r_k, e_k) \in \{k, \dots, \ell\} \times \{k, \dots, h\}$, s.t. $\nu(b_{r_k e_k})$ is minimal, i.e.
$$\nu(b_{r_k e_k}) \leq \nu(b_{ij}) \; \forall \; (i,j) \in \{k, \dots, \ell\} \times \{k, \dots, h\}.$$
  Move $b_{r_k e_k}$ to the position (k,k) (of B_k). Obtaining a row and a column permutation E_k and E'_k, s.t.
$$E_k B_k E'_k = \begin{bmatrix} b_{r_1 e_1} & & 0 & \\ & \ddots & & 0 \\ 0 & & b_{r_k e_k} & \star \\ & 0 & \star & \bigstar \end{bmatrix}.$$
  Delete all entries of the k-th row and k-th column, (but the entry in (k,k)), using elementary invertible row and column operations, getting two matrices F_k, F'_k, s.t.
$$F_k E_k B_k E'_k F'_k = \begin{bmatrix} b_{r_1 e_1} & & 0 & \\ & \ddots & & 0 \\ 0 & & b_{r_k e_k} & \mathbf{0} \\ & 0 & \mathbf{0} & U \end{bmatrix}.$$
  $C_{k+1} \leftarrow U$
  $S \leftarrow F_k E_k S$
  $T \leftarrow T E'_k F'_k$
  $B_{k+1} \leftarrow SBT = F_k E_k B_k E'_k F'_k$
  $k \leftarrow k+1$
return $(S, T, B_k, k-1)$

searching ($\mathcal{O}(\ell \cdot h)$ operations) and matrix multiplications. This algorithm then runs in $\mathcal{O}(h^4)$ $\mathcal{R}$-operations. □

Lemma 14. *Let $B \in \mathrm{Mat}_{\ell \times h}(\mathcal{R})$ with $\ell \leq h$, and $c \in \mathcal{R}^\ell$. The set of solutions of*

$$By = c \tag{4.2}$$

is either empty or of the form

$$\{\bar{y} + P\lambda \mid \lambda \in \mathcal{R}^h\},$$

where P is a $h \times h$ matrix. Also, P and $\bar{y}$ can be found in polynomial time.

Proof. The idea is to apply Algorithm 1 to B, i.e. we get $(S, T, B', \bar{\ell})$, where $B' = SBT$ is of the form (4.1) with

$$\nu(b_{r_i e_i}) \leq \nu(b_{r_j e_j}) \; \forall \; 1 \leq i \leq j \leq \bar{\ell}.$$

We want to reduce B' even more. Define $\nu_i = \nu(b_{r_i e_i})$. We can write for all $i \in \{1, \ldots, \bar{\ell}\}$

$$b_{r_i e_i} = p^{\nu_i} b'_{r_i e_i},$$

where $b'_{r_i e_i}$ is invertible in $\mathcal{R}$. Define D to be the $\ell \times \ell$ diagonal matrix with entries

$$d_{ii} = \begin{cases} b'^{-1}_{r_i e_i} & \text{if } 1 \leq i \leq \bar{\ell}, \\ 1 & \text{if } \bar{\ell} + 1 \leq i \leq \ell. \end{cases}$$

We compute $DB' = \bar{B}$ which is now of the form

$$\bar{B} = \begin{bmatrix} p^{v_1} & & 0 & \\ & \ddots & & 0 \\ 0 & & p^{v_{\bar{\ell}}} & \\ & 0 & & 0 \end{bmatrix}.$$

For $S' = DS$, we have $S'BT = \bar{B}$. Hence the system (4.2), i.e. $By = c$ is equivalent to

$$S'BTT^{-1}y = S'c.$$

For $z = T^{-1}y = (z_1, \ldots, z_h)$ and $\bar{c} = S'c$ the system (4.2) is equivalent to

$$\bar{B}z = \bar{c}.$$

Let k be the order of nilpotence of $\mathcal{R}$. If for some $i \in \{1, \ldots, \bar{\ell}\}$ we have that

$$\nu_i > \nu(\bar{c}_i),$$

then the solution set to (4.2) is empty: in fact, if there exists a solution z_i for all $i \in \{1, \ldots, \bar{\ell}\}$, then we can write

$$p^{\nu_i} z_i = \bar{c}_i = p^{\nu(\bar{c}_i)} \bar{c}'_i,$$

and by Proposition 12 ii) we have that

$$\begin{aligned} \nu(\bar{c}_i) &= \nu(p^{\nu_i} z_i) = \min\{k, \nu(p^{\nu_i}) + \nu(z_i)\} \\ &= \min\{k, \nu_i + \nu(z_i)\} \geq \nu_i. \end{aligned}$$

Hence we can assume that

$$\nu_i \leq \nu(\bar{c}_i) \; \forall \; i \in \{1, \ldots, \bar{\ell}\}.$$

We want to solve for all $i \in \{1, \ldots, \bar{\ell}\}$

$$p^{\nu_i} z_i = p^{\nu(\bar{c}_i)} \bar{c}'_i. \tag{4.3}$$

Proposition 12 iii) ensures that

$$z_i \in p^{\nu(\bar{c}_i) - \nu_i} \bar{c}'_i + p^{k - \nu_i} \mathcal{R}.$$

So we found z_i's for $i \in \{1, \ldots, \bar{\ell}\}$ which solve (4.3). The z_i's for $i \in \{\bar{\ell} + 1, \ldots, h\}$ are free variables. Thus the solution to $\bar{B}z = \bar{c}$ is of the form

$$\bar{z} + G\lambda,$$

where

$$\bar{z}_i = \begin{cases} p^{\nu(\bar{c}_i)-\nu_i}\bar{c}'_i & \text{if } 1 \leq i \leq \bar{\ell}, \\ 0 & \text{if } \bar{\ell}+1 \leq i \leq h, \end{cases}$$

and G is a $h \times h$ matrix, which is defined as follows

$$G = \begin{bmatrix} H & \mathbf{0}_{\bar{\ell}\times(h-\bar{\ell})} \\ \mathbf{0}_{(h-\bar{\ell})\times\bar{\ell}} & \mathbf{Id}_{(h-\bar{\ell})\times(h-\bar{\ell})} \end{bmatrix},$$

where H is a $\bar{\ell} \times \bar{\ell}$ diagonal matrix, with

$$h_{ii} = p^{k-\nu_i} \ \forall\ i \in \{1, \dots, \bar{\ell}\}.$$

H is introduced to make sure we obtain all the solutions and the identity matrix is introduced for the free variables. Let $\lambda = (\lambda_1, \dots, \lambda_h)$ be a vector of variables. Define $\bar{y} = T\bar{z}$ and $P = TG \in \mathrm{Mat}_{h\times h}(\mathcal{R})$, then we get that the set of solution of the system (4.2) is

$$\{\bar{y} + P\lambda \mid \lambda \in \mathcal{R}^h\}.$$

Observe that this solves the system by construction. Algorithm 2 shows how to obtain the set of solutions of the system (4.2) following the procedure described in this proof.

Notice that the running time of Algorithm 2 coincides with the running time of Algorithm 1, as applying Algorithm 1 makes up the biggest part of the procedure. Hence with a running time of $\mathcal{O}(h^4)$ $\mathcal{R}$-operations we get the claim.

□

Proposition 15. *Protocol 3 can be broken in polynomial time.*

Proof. We are looking for $X \in E_p^{(m)}$, such that

$$\begin{aligned} XM &= MX, \\ X \cdot R &= T. \end{aligned} \tag{4.4}$$

Observe that any solution to this system breaks the scheme, since if $X_0 \in E_p^{(m)}$ solves the system (4.4) it is enough to compute

$$D - X_0 \cdot H = S + G \cdot (X_0 \cdot R) - X_0 \cdot (G \cdot R) = S.$$

For each $i \in \{1, \dots, m\}$ there is a system of linear congruences modulo p^i arising from the system (4.4) and the fact that X lives in $E_p^{(m)}$. Set the entries of X as unknown variables $x_{s,t}$'s. Partition the congruences according to their moduli obtaining the equations

$$A^{(i)}x \equiv b_i \mod p^i, \tag{i}$$

for all $i \in \{1, \dots, m\}$, for some $A^{(i)}$ in $\mathrm{Mat}_{(2m-i+1)\times m^2}(\mathbb{Z})$ and $b_i \in \mathbb{Z}^{2m-i+1}$. Let us briefly explain how we get desired dimensions first for $A^{(1)}$ and b_1. We have to count how many equations $\mod p$ we have: this will give both the number of components of b_1 and the number of rows of $A^{(1)}$ (the number of columns of $A^{(1)}$ is clearly m^2 since there are m^2 unknowns in X): one equation is given by the first entry of $X \cdot R$ equal to the first entry of T, other m equations are given by the first row of XM equal to the first row of MX, finally since X has to be in $E_p^{(m)}$, $x_{s+1,s}$ must be congruent to zero modulo p for all $s \in \{1, \dots m-1\}$, which leads to further $m-1$ equations, for a total of $2m$ equations in at most m^2 variables.

Algorithm 2 Solve system of linear equations over $\mathcal{R}$

Input: $B \in \mathrm{Mat}_{\ell \times h}(\mathcal{R}), c \in \mathcal{R}^{\ell}$ with $\ell \leq h$
Output: $(\bar{y}, P)$, s.t.

$$\{\bar{y} + P\lambda \mid \lambda \in \mathcal{R}^{h}\}$$

is the set of solutions of $By = c$ (or the empty set, if there is no solution).

Apply Algorithm 1 to B, getting $(S, T, B, \bar{\ell})$, with B of the form (4.1), i.e.

$$B = \begin{bmatrix} b_{r_1 e_1} & & 0 & \\ & \ddots & & 0 \\ 0 & & b_{r_{\bar{\ell}} e_{\bar{\ell}}} & \\ & 0 & & 0 \end{bmatrix}$$

Write $b_{r_i e_i} = b'_{r_i e_i} p^{\nu(b_{r_i e_i})}$ for all $i \in \{1, \ldots, \bar{\ell}\}$
Define $D = (d_{ij})_{1 \leq i,j \leq \ell}$, with

$$d_{ij} = \begin{cases} b'^{-1}_{r_i e_i} & \text{if } 1 \leq i \leq \bar{\ell}, \\ 1 & \text{if } \bar{\ell} + 1 \leq i \leq \ell, \\ 0 & \text{if } i \neq j. \end{cases}$$

$S \leftarrow DS$
$c \leftarrow Sc$
if $\exists i \in \{1, \ldots, \bar{\ell}\}$ with $\nu(c_i) < \nu(b_{r_i e_i})$ or $\exists i \in \{\bar{\ell} + 1, \ldots, \ell\}$ with $c_i \neq 0$ **then**
    return $\emptyset$
else
    Write $c_i = c'_i p^{\nu(c_i)}$ for all $i \in \{1, \ldots, \ell\}$
    Define $\bar{z}$ as

$$\bar{z}_i = \begin{cases} p^{\nu(c_i) - \nu(b_{r_i e_i})} c'_i & \text{if } 1 \leq i \leq \bar{\ell}, \\ 0 & \text{if } \bar{\ell} + 1 \leq i \leq h. \end{cases}$$

    Define H as the $\bar{\ell} \times \bar{\ell}$ diagonal matrix with

$$h_{ii} = p^{k - \nu(b_{r_i e_i})} \ \forall i \in \{1, \ldots, \bar{\ell}\}.$$

    Define G as

$$G = \begin{bmatrix} H & \mathbf{0}_{\bar{\ell} \times (h - \bar{\ell})} \\ \mathbf{0}_{(h - \bar{\ell}) \times \bar{\ell}} & \mathbf{Id}_{(h - \bar{\ell}) \times (h - \bar{\ell})} \end{bmatrix},$$

    $\bar{y} \leftarrow T\bar{z}$
    $P \leftarrow TG$
    return $(\bar{y}, P)$ as the set of solutions is given by

$$\{\bar{y} + P\lambda \mid \lambda \in \mathcal{R}^{h}\}.$$

For $A^{(i)}$ and b_i the situation is similar: the i-th row of MX equal to the i-th row of XM gives rise to m equations modulo p^i and the equality between the i-th component of XR and the i-th component of T gives rise to one additional equation, furthermore there are $m - i$ additional equations coming from the condition $x_{s+i,s} \equiv 0 \mod p^i$ for $s \in \{1, \ldots m - i\}$. It is worth noticing that b_i has only one entry different from zero, which is the entry corresponding to the the i-th component of T (appearing in the equation $XR = T$).

We will not list all the solutions, since some of these congruence systems might contain too many solutions, and this would need too much memory. We also have the issue that some of the solutions of a system modulo p^i might not be pushed to a solution modulo p^j for $j < i$ for the system

$$A^{(j)}x \equiv b_j \mod p^j.$$

Since the proof will be rather technical, we briefly explain the idea of the intermediate step in this paragraph. We proceed with a descending induction as follows: for $i \in \{1, \dots m\}$ in the i-th step we assume we have a set Sol_{m-i+1} which solves the system of congruences

$$A^{(j)}x \equiv b_j \mod p^j \; \forall \; j \in \{m, \dots, m-i+1\}.$$

On this set we impose the condition

$$A^{(m-i)}x \equiv b_{m-i} \mod p^{m-i}$$

getting a non-empty set Sol_{m-i}, solving the congruences

$$A^{(j)}x \equiv b_j \mod p^j \; \forall \; j \in \{m, \dots, m-i\}.$$

The set of solutions will be at each step non-empty since we will show that, given the private key F, then $F \mod p^{m-i} \in \mathrm{Sol}_{m-i} \mod p^{m-i}$. In what follows we do this in detail.

We start with the system (m), i.e.

$$(m) \qquad A^{(m)}x \equiv b_m \mod p^m.$$

The solution set of (m) is not empty, since the private key F is a solution. Lemma 14 applied over the ring $\mathbb{Z}/p^m\mathbb{Z}$, ensures the existence of a vector $\bar{x}_m \in (\mathbb{Z}/p^m\mathbb{Z})^{m^2}$, and a matrix $S_m \in \mathrm{Mat}_{m^2 \times m^2}(\mathbb{Z}/p^m\mathbb{Z})$ such that the solution set of (m) is

$$\{\bar{x}_m + S_m y_m \mid y_m \in (\mathbb{Z}/p^m\mathbb{Z})^{m^2}\}.$$

For our purposes we have to consider a lift of the set above over $\mathbb{Z}$ and sieving from there, finally extracting a solution of (4.4). This is necessary because otherwise we would be losing information about the candidate keys while pushing from higher degree congruences to lower degree ones. Thus, consider now

$$\mathrm{Sol}_m = \{\bar{x}_m + S_m y_m \mid y_m \in \mathbb{Z}^{m^2}\},$$

with the small abuse that S_m is a fixed representative of S_m in $\mathrm{Mat}_{m^2 \times m^2}(\mathbb{Z})$. Take now any representative of F over $\mathbb{Z}^{m^2}$. The set Sol_m verifies two properties: $F \mod p^m \in \mathrm{Sol}_m \mod p^m$, and every element of Sol_m solves (m).

For $i \in \{1, \dots, m-1\}$ we now inductively build Sol_{m-i} satisfying: $F \mod p^{m-i} \in \mathrm{Sol}_{m-i} \mod p^{m-i}$ and every element of Sol_{m-i} solves $(m), \dots, (m-i)$.

Suppose we are given

$$\mathrm{Sol}_{m-i+1} = \{\bar{x}_{m-i+1} + S_{m-i+1} y_{m-i+1} \mid y_{m-i+1} \in \mathbb{Z}^{m^2}\},$$

for some $\bar{x}_{m-i+1} \in \mathbb{Z}^{m^2}$ and $S_{m-i+1} \in \mathrm{Mat}_{m^2 \times m^2}(\mathbb{Z})$.

Thanks to the inductive hypothesis, Sol_{m-i+1} satisfies the following properties

- $F \mod p^{m-i+1} \in \mathrm{Sol}_{m-i+1} \mod p^{m-i+1}$,

- every element of Sol_{m-i+1} solves (m) , ..., $(m-i+1)$.

In the system of equation $(m-i)$, i.e.

$$(m-i) \qquad A^{(m-i)}x \equiv b_{m-i} \mod p^{m-i},$$

we replace x with $\bar{x}_{m-i+1} + S_{m-i+1}y_{m-i+1}$. We get

$$((m-i)^*) \qquad A^{(m-i)}(\bar{x}_{m-i+1} + S_{m-i+1}y_{m-i+1}) \equiv b_{m-i} \mod p^{m-i}.$$

The system $((m-i)^*)$ has a solution: since $F \mod p^{m-i+1} \in \mathrm{Sol}_{m-i+1} \mod p^{m-i+1}$ there exists $\tilde{y}_{m-i+1} \in \mathbb{Z}^{m^2}$, s.t.

$$F \equiv \bar{x}_{m-i+1} + S_{m-i+1}\tilde{y}_{m-i+1} \mod p^{m-i+1}.$$

And since $F \mod p^{m-i}$ solves the system $(m-i)$ we have that $\tilde{y}_{m-i+1}$ solves the system $((m-i)^*)$.

Lemma 14 applied over the ring $\mathbb{Z}/p^{m-i}\mathbb{Z}$ to $B = A^{(m-i)}S_{m-i+1}$ and $c = b_{m-i} - A^{(m-i)}\bar{x}_{m-i+1}$ ensures that a set of representatives over $\mathbb{Z}^{m^2}$ for the set of solutions of $((m-i)^*)$ is

$$\{\bar{y}_{m-i+1} + T_{m-i}y_{m-i} \mid y_{m-i} \in \mathbb{Z}^{m^2}\},$$

for some $\bar{y}_{m-i+1} \in \mathbb{Z}^{m^2}$ and $T_{m-i} \in \mathrm{Mat}_{m^2\times m^2}(\mathbb{Z})$.

Observe that $\tilde{y}_{m-i+1}$ is contained in the set of solution of $((m-i)^*)$, hence there exists a $\tilde{y}_{m-i} \in \mathbb{Z}^{m^2}$, s.t.

$$\tilde{y}_{m-i+1} \equiv \bar{y}_{m-i+1} + T_{m-i}\tilde{y}_{m-i} \mod p^{m-i}.$$

And hence

$$F \equiv \bar{x}_{m-i+1} + S_{m-i+1}(\bar{y}_{m-i+1} + T_{m-i}\tilde{y}_{m-i}) \mod p^{m-i}.$$

Let us define

$$\begin{aligned} \bar{x}_{m-i} &= \bar{x}_{m-i+1} + S_{m-i+1}\bar{y}_{m-i+1}, \\ S_{m-i} &= S_{m-i+1}T_{m-i}. \end{aligned}$$

Then we want to show that

$$\mathrm{Sol}_{m-i} = \{\bar{x}_{m-i} + S_{m-i}y_{m-i} \mid y_{m-i} \in \mathbb{Z}^{m^2}\}$$

satisfies the requested properties. In fact, every element of Sol_{m-i} solves $(m), \dots,$ $(m-i+1)$, since $\mathrm{Sol}_{m-i} \subseteq \mathrm{Sol}_{m-i+1}$ and every element of Sol_{m-i} solves $(m-i)$ by construction. Also $F \mod p^{m-i}$ can be written as observed before as

$$\begin{aligned} F &\equiv \bar{x}_{m-i+1} + S_{m-i+1}(\bar{y}_{m-i+1} + T_{m-i}\tilde{y}_{m-i}) \mod p^{m-i} \\ &\equiv \bar{x}_{m-i} + S_{m-i}\tilde{y}_{m-i} \mod p^{m-i} \end{aligned}$$

for some $\tilde{y}_{m-i} \in \mathbb{Z}^{m^2}$, hence $F \mod p^{m-i} \in \mathrm{Sol}_{m-i} \mod p^{m-i}$.

Algorithm 3 provides a formal way to break Protocol 3.

Let us analyse the running time. Observe that in the i-th step we apply Algorithm 2 to an $m^2 \times m^2$ matrix. By the running time of Algorithm 2 we have $\mathcal{O}((m^2)^4)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations in the i-th step. Since we repeat this step m times, we get that to run Algorithm 3 we need $\mathcal{O}(m^9)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations. □

Algorithm 3 Break cryptosystem over $E_p^{(m)}$

Input: $M \in E_p^{(m)}, R \in V, T \in V$
Output: $X \in E_p^{(m)}$ which breaks the Protocol 3

Find the equations arising from the conditions

$$\begin{aligned} X &\in E_p^{(m)}, \\ XM &= MX, \\ X \cdot R &= T. \end{aligned}$$

Partition the congruences according to their moduli obtaining the equations

$$A^{(i)}x \equiv b_i \bmod p^i, \tag{i}$$

for all $i \in \{1, \ldots, m\}$.
$S \leftarrow \mathrm{Id}_{m^2}$
$\bar{x} \leftarrow \mathbf{0}$
$i \leftarrow 0$
while $i \leq m-1$ **do**
    In the equation $(m-i)$ replace x with $\bar{x} + Sy$
    Apply Algorithm 2 to solve this system, i.e. $\mathcal{R} = \mathbb{Z}/p^{m-i}\mathbb{Z}$, $B = A^{(m-i)}S$ and $c = b_{m-i} - A^{(m-i)}\bar{x}$, getting $(\bar{y}, T)$
    $S \leftarrow ST$
    $\bar{x} \leftarrow \bar{x} + S\bar{y}$
    $i \leftarrow i + 1$
Return $\bar{x}$

4.1. **A** 2×2 **example.** Let $m = 2, p = 3$. The attacker sees

$$M = \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}, \ R = \begin{pmatrix} 1 \\ 5 \end{pmatrix}, \ T = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

and wants to find $X \in E_3^{(2)}$, such that

$$\begin{aligned} MX &= XM, \\ X \cdot R &= T. \end{aligned}$$

Therefore the attacker gets the following equations in $E_3^{(2)}$

$$\begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix},$$

$$\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{pmatrix} 1 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

and in addition one wants that $3 \mid x_{21}$, so that the solution will be in $E_3^{(2)}$. One can partition the congruences according to their moduli getting

$$\begin{aligned} x_{21} &\equiv 0 \mod 3 \\ x_{11} + x_{21} - x_{11} - 3x_{12} &\equiv 0 \mod 3 \\ x_{12} + x_{22} - x_{11} - 4x_{12} &\equiv 0 \mod 3 \\ x_{11} + 5x_{12} &\equiv 1 \mod 3 \end{aligned}$$

and

$$\begin{aligned} 3x_{11} + 4x_{21} - x_{21} - 3x_{22} &\equiv 0 \mod 9 \\ 3x_{12} + 4x_{22} - x_{21} - 4x_{22} &\equiv 0 \mod 9 \\ x_{21} + 5x_{22} &\equiv 1 \mod 9. \end{aligned}$$

Setting

$$A^{(1)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 \end{bmatrix}, \qquad b_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

$$A^{(2)} = \begin{bmatrix} 3 & 0 & 3 & -3 \\ 0 & 3 & -1 & 0 \\ 0 & 0 & 1 & 5 \end{bmatrix}, \qquad b_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

and

$$x = \begin{pmatrix} x_{11} \\ x_{12} \\ x_{21} \\ x_{22} \end{pmatrix},$$

we get that the final system is

$$\begin{aligned} A^{(1)}x &\equiv b_1 \mod 3, \\ A^{(2)}x &\equiv b_2 \mod 9. \end{aligned}$$

As first step we want to solve with Algorithm 2 the system $A^{(2)}x \equiv b_2 \mod 9$. First we bring $A^{(2)}$ in the reduced form of (4.1). Using Algorithm 1 we get

$$B' = SA^{(2)}T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{bmatrix},$$

where

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & -3 \end{bmatrix}, \quad T = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & -5 & 0 & 3 \\ 0 & 1 & 0 & -6 \end{bmatrix}.$$

Using Algorithm 2 we obtain also the diagonal matrix D

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Let $S' = DS$, then we have

$$\bar{B} = DB' = S'A^{(2)}T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{bmatrix}.$$

We define $z = T^{-1}x$ and $\bar{c} = S'b_2$, i.e.

$$\bar{c} = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}.$$

Hence we get the system $\bar{B}z \equiv \bar{c} \mod 9$. Define $\bar{z} = \begin{pmatrix} 1 \\ 2 \\ -1 \\ 0 \end{pmatrix}$ and

$$G = \begin{bmatrix} 9 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

then the set of solution of $\bar{B}z \equiv \bar{c} \mod 9$ is given by

$$\left\{ \bar{z} + Gy_2 \;\middle|\; y_2 \in \mathbb{Z}^4 \right\}.$$

Define $S_2 = TG$ and $\bar{x}_2 = T\bar{z} = \begin{pmatrix} -1 \\ 0 \\ 0 \\ 2 \end{pmatrix}$. Then we get the solution set of $A^{(2)}x \equiv b_2 \mod 9$ is

$$\mathrm{Sol}_2 = \left\{ \bar{x}_2 + S_2 y_2 \;\middle|\; y_2 \in \mathbb{Z}^4 \right\}.$$

As second step we want to sieve the solutions. Hence we set in the system $A^{(1)}x \equiv b_1 \mod 3$ the solution of $A^{(2)}x \equiv b_2 \mod 9$ and get

$$A^{(1)}S_2y_2 \equiv b_1 - A^{(1)}\bar{x}_2 \mod 3$$

and hence

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} y_2 \equiv \begin{pmatrix} 0 \\ 0 \\ 0 \\ 2 \end{pmatrix} \mod 3,$$

We can see that $\bar{y}_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ is a solution to this and hence if we define

$$\bar{x}_1 = \bar{x}_2 + S_2\bar{y}_2 = \begin{pmatrix} -1 \\ 1 \\ 3 \\ -4 \end{pmatrix}$$

we get that

$$X = \begin{bmatrix} -1 & 1 \\ 3 & -4 \end{bmatrix}.$$

One can check directly that X breaks the protocol.

Acknowledgment

The first author is thankful to the Swiss National Science Foundation under grant number 171248. The second author has been supported by the Swiss National Science Foundation under grant number 169510. We would also like to thank Karan Khathuria for his valuable inputs for the implementation of the attack. The authors are very grateful to the three anonymous referees whose suggestions greatly improved both the mathematics and the readability of the paper.

References

[1] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post-Quantum Cryptography.* Springer Science & Business Media, 2009.

[2] Daniele Micciancio and Oded Regev. Lattice-based Cryptography. In *Post-Quantum Cryptography*, pages 147–191. Springer, 2009.

[3] Robert J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114–116, January 1978.

[4] Jintai Ding and Bo-Yin Yang. Multivariate Public Key Cryptography. In *Post-Quantum Cryptography*, pages 193–241. Springer, 2009.

[5] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Group-based Cryptography.* Springer Science & Business Media, 2008.

[6] Benjamin Fine, Maggie Habeeb, Delaram Kahrobaei, and Gerhard Rosenberger. Aspects of Nonabelian Group Based Cryptography: A Survey and Open Problems. *JP Journal of Algebra, Number Theory and Applications*, 21(1):1–40, 2011.

[7] Gérard Maze, Chris Monico, and Joachim Rosenthal. Public Key Cryptography based on Semigroup Actions. *Advances in Mathematics of Communications*, 1(4):489–507, 2007.

[8] David Jao and Luca De Feo. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[9] David Naccache and Jacques Stern. A new Public-Key Cryptosystem. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 27–36. Springer, 1997.

[10] Benoît Chevallier-Mames, David Naccache, and Jacques Stern. Linear Bandwidth Naccache-Stern Encryption. In *International Conference on Security and Cryptography for Networks*, pages 327–339. Springer, 2008.

[11] Giacomo Micheli and Michele Schiavina. A General Construction for Monoid-Based Knapsack Protocols. *Advances in Mathematics of Communications*, 8(3):343–358, 2014.

[12] Giacomo Micheli, Joachim Rosenthal and Paolo Vettori. Linear spanning sets for matrix spaces. *Linear Algebra and its Applications*, 483:309–322, 2015.

[13] Giacomo Micheli, Joachim Rosenthal, and Reto Schnyder. An Information Rate Improvement for a Polynomial Variant of the Naccache-Stern Knapsack

Cryptosystem. In *Physical and Data-Link Security Techniques for Future Communication Systems*, pages 173–180. Springer International Publishing, 2016.

[14] Joan-Josep Climent and Juan Antonio López Ramos. Public Key Protocols over the Ring $E_p^{(m)}$. *Advances in Mathematics of Communications*, 10(4):861–870, 2016.

[15] Joan-Josep Climent, Pedro R. Navarro, and Leandro Tortosa. On the Arithmetic of the Endomorphisms ring End $(\mathbb{Z}_p \times \mathbb{Z}_p^2)$. *Applicable Algebra in Engineering, Communication and Computing*, 22(2):91–108, 2011.

[16] Joan-Josep Climent, Pedro R. Navarro, and Leandro Tortosa. An Extension of the Noncommutative Bergmans Ring with a large Number of Noninvertible Elements. *Applicable Algebra in Engineering, Communication and Computing*, 25(5):347–361, 2014.

[17] Abdel Alim Kamal and Amr M. Youssef. Cryptanalysis of a Key Exchange Protocol based on the Endomorphisms ring End $(\mathbb{Z}_p \times \mathbb{Z}_p^2)$. *Applicable Algebra in Engineering, Communication and Computing*, 23(3):143–149, 2012.

[18] George M. Bergman. Some Examples in PI Ring Theory. *Israel Journal of Mathematics*, 18(3):257–277, 1974.

[19] Giacomo Micheli. Cryptanalysis of a non-commutative Key Exchange Protocol. *Advances in Mathematics of Communications*, 9(2):247–253, 2015.

[20] Juan Antonio López-Ramos, Joachim Rosenthal, Davide Schipani, and Reto Schnyder. Group Key Management based on Semigroup Actions. *Journal of Algebra and Its Applications*, 16(8), 2017.

[21] Chen Feng, Roberto W. Nóbrega, Frank R. Kschischang, and Danilo Silva. Communication Over Finite-Chain-Ring Matrix Channels. *IEEE Transactions on Information Theory*, 60(10):5899–5917, 2014.

[22] Roberto W Nóbrega, Chen Feng, Danilo Silva, and Bartolomeu F Uchôa-Filho. On multiplicative matrix channels over finite chain rings. In *Network Coding (NetCod), 2013 International Symposium on*, pages 1–6. IEEE, 2013.

[23] Bernard R. McDonald. Enumeration of classes of row equivalent matrices over a principal ideal domain modulo p^n. *Duke Mathematical Journal*, 37(1):163–169, 1970.

Mathematical Institute, University of Oxford, Woodstock Rd,, Oxford OX2 6GG, United Kingdom

E-mail address: giacomo.micheli@maths.ox.ac.uk

Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland,

E-mail address: violetta.weger@math.uzh.ch