Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017

Yasufumi Hashimoto[1], Yasuhiko Ikematsu[2], and Tsuyoshi Takagi[2]

[1] Department of Mathematical Science, University of the Ryukyus
hashimoto@math.u-ryukyu.ac.jp
[2] Department of Mathematical Informatics, University of Tokyo
{ikematsu,takagi}@mist.i.u-tokyo.ac.jp

Abstract. One of the most efficient post-quantum signature schemes is Rainbow whose harness is based on the multivariate quadratic polynomial (MQ) problem. ELSA, a new multivariate signature scheme proposed at Asiacrypt 2017, has a similar construction to Rainbow. Its advantages, compared to Rainbow, are its smaller secret key and faster signature generation. In addition, its existential unforgeability against an adaptive chosen-message attack has been proven under the hardness of the MQ-problem induced by a public key of ELSA with a specific parameter set in the random oracle model. The high efficiency of ELSA is derived from a set of hidden quadratic equations used in the process of signature generation. However, the hidden quadratic equations yield a vulnerability. In fact, a piece of information of these equations can be recovered by using valid signatures and an equivalent secret key can be partially recovered from it. In this paper, we describe how to recover an equivalent secret key of ELSA by a chosen message attack. Our experiments show that we can recover an equivalent secret key for the claimed 128-bit security parameter of ELSA on a standard PC in 177 seconds with 1326 valid signatures.

Keywords: post-quantum cryptography, multivariate public-key cryptography, chosen message attack, Rainbow, ELSA.

1 Introduction

P. Shor [12] proposed quantum algorithms to factor large integers and to solve discrete logarithms in polynomial time. If large-scale quantum computers are built, most currently used public key cryptosystems, such as RSA, DSA and ECC, will be insecure. The aim of Post-Quantum Cryptography (PQC) is to develop cryptosystems that are secure against attacks by future quantum computers [2]. At PQCrypto 2016, the National Institute of Standards and Technology (NIST) started the standardization process of post-quantum cryptography, and there are currently 69 proposals of post-quantum cryptography [9].

Multivariate public key cryptosystems (MPKCs) [4] are considered to be some of the most promising candidates for PQC. A lot of MPKCs have been proposed starting with the Matsumoto-Imai scheme [8]. Among them, the UOV

[6] and HFEv$^-$ [10, 11] signature schemes have in particular remained sound for around two decades, and their signature sizes are relatively small compared with other post-quantum signature schemes. Moreover, there are many submissions of MPKCs to the NIST PQC standardization. Even amongst those, Rainbow [5], a multi-layered version of the UOV scheme, has drawn a lot of attention because of its efficiency, modest computational cost, high security and simplicity.

The ELSA [13] signature scheme, studied in this paper, is a variant of Rainbow; it was proposed at Asiacrypt 2017 by Shim et al. An advantage of ELSA over Rainbow is its higher efficiency; that is, its secret key is smaller and its signature generation is faster. Shim et al. actually succeeded to reduce the complexity of signature generation from $O(n^3)$ for Rainbow to $O(n^2)$, where n is the number of variables, without weakening the security against known attacks. The trick to reducing the complexity is choosing the secret keys sparsely and attaching several hidden quadratic equations in the process of signature generation. Another advantage is that ELSA has existential unforgeability against an adaptive chosen-message attack. This was proven under the hardness of the MQ problem induced by the public key of ELSA with a specific parameter set in the random oracle model.

In this paper, we propose a chosen message attack on ELSA, with which we can obtain valid signatures by repeatedly accessing a signing oracle. Recall that ELSA possesses hidden quadratic equations for accelerating the signature generation; these are not used in Rainbow. Once the hidden quadratic equations are recovered, an attacker can obtain an equivalent secret key of ELSA and forge all signatures of ELSA by using the equivalent secret key. In fact, we show that a piece of information associated with the hidden quadratic equations can be recovered from at most n^2 valid signatures obtained in the chosen message attack. Our attack is very efficient, and we prove that its complexity is $O(n^{2\omega})$, where n is the number of variables and $2 \leq \omega < 3$ is the linear algebra constant. In our experiments using Magma, we succeeded in recovering an equivalent secret key with 1326 valid signatures in 177 seconds for the parameters selected in [13] as 128-bit security.

Our paper is organized as follows: in §2, we briefly summarize the ELSA scheme and its previous security analysis given in [13]. §3 discusses our new attack and give a detailed algorithm to obtain an equivalent secret key of the ELSA scheme. In §4, we preform the complexity analysis of our new attack and present a Magma implementation of our algorithm. We conclude our paper in §5.

2 The ELSA Signature Scheme

Here, we briefly explain the basic concept of multivariate signature schemes and summarize the construction of the ELSA scheme and its previous security analysis following [13].

2.1 Multivariate Signature Scheme

Let $n, m \geq 1$ be integers, q a power of prime, and $\mathbb{F}_q$ a finite field of order q. In a multivariate signature scheme, the public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is a quadratic map, namely $\mathcal{P}(x_1, \ldots, x_n) = {}^t(\mathcal{P}_1(x_1, \ldots, x_n), \ldots, \mathcal{P}_m(x_1, \ldots, x_n))$ given by

$$\mathcal{P}_l(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} \alpha_{ij}^{(l)} x_i x_j + \sum_{1 \leq i \leq n} \beta_i^{(l)} x_i + \gamma^{(l)}$$

for $1 \leq l \leq m$, where $\alpha_{ij}^{(l)}, \beta_i^{(l)}, \gamma^{(l)} \in \mathbb{F}_q$. For such a signature scheme, the public key $\mathcal{P}$ is generated by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ with invertible affine maps $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and a quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ that can be feasibly inverted. Thus the secret key consists of $\mathcal{T}, \mathcal{F}$ and $\mathcal{S}$.

To generate a signature of a message $\mathbf{m} \in \mathbb{F}_q^m$, one recursively computes $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{m}), \mathbf{y} = \mathcal{F}^{-1}(\mathbf{z}), \mathbf{w} = \mathcal{S}^{-1}(\mathbf{y})$. Thus a signature for $\mathbf{m}$ is given by $\mathbf{w}$. Here, $\mathbf{y}$ means an element of the preimage of $\mathbf{z}$ under the central map $\mathcal{F}$. The verification involves checking whether $\mathcal{P}(\mathbf{w}) = \mathbf{m}$.

2.2 Key Generation of ELSA

The ELSA [13] signature scheme is basically constructed in the manner described in §2.1.

Let l, k, u, r be positive integers and set $n = l + k + u + r$ and $m = k + u$. Denote the sets of l, k, u, r and n variables by

$$\begin{aligned}
&\mathbf{x}_L := (x_{L,1}, \ldots, x_{L,l}), \quad \mathbf{x}_K := (x_{K,1}, \ldots, x_{K,k}),\\
&\mathbf{x}_U := (x_{U,1}, \ldots, x_{U,u}), \quad \mathbf{x}_R := (x_{R,1}, \ldots, x_{R,r}),\\
&\mathbf{x} := {}^t(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, \mathbf{x}_R) = {}^t(x_{L,1}, \ldots, x_{R,r}).
\end{aligned}$$

First, we explain the construction of the central map of ELSA consisting of two layers. Let $L_i(\mathbf{x}) = L_i(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R), R_{ij}(\mathbf{x}) = R_{ij}(\mathbf{x}_L, \mathbf{x}_K)$ $(1 \leq i \leq r, 1 \leq j \leq k)$ be linear polynomials and $\Phi_j(\mathbf{x}) = \Phi_j(\mathbf{x}_L)$ $(1 \leq j \leq k)$ quadratic polynomials. The first layer $(\mathcal{F}_1, \ldots, \mathcal{F}_k)$ of the central map of ELSA is

$$\mathcal{F}_j(\mathbf{x}) := \sum_{1 \leq i \leq r} L_i(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R) R_{ij}(\mathbf{x}_L, \mathbf{x}_K) + \Phi_j(\mathbf{x}_L), \quad (1 \leq j \leq k).$$

To construct the second layer, let $R_{i,k+j}(\mathbf{x})$ $(1 \leq i \leq r, 1 \leq j \leq u)$, $L'_j(\mathbf{x}) = L'_j(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R)$ $(1 \leq j \leq u)$ be linear polynomials and $\Phi_{k+j}(\mathbf{x}) = \Phi_{k+j}(\mathbf{x}_L, \mathbf{x}_K)$ $(1 \leq j \leq u)$ quadratic polynomials. The second layer $(\mathcal{F}_{k+1}, \ldots, \mathcal{F}_m)$ is

$$\mathcal{F}_{k+j}(\mathbf{x}) := \sum_{1 \leq i \leq r} L_i(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R) R_{i,k+j}(\mathbf{x}) + \Phi_{k+j}(\mathbf{x}_L, \mathbf{x}_K) + L'_j(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R),$$

for $1 \leq j \leq u$. The central map of ELSA is given by

$$\mathcal{F} := {}^t(\mathcal{F}_1, \ldots, \mathcal{F}_k, \mathcal{F}_{k+1}, \ldots, \mathcal{F}_m) : \mathbb{F}_q^n \to \mathbb{F}_q^n.$$

Next let us explain the secret and public keys of ELSA. Randomly choose two invertible affine maps $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and fix a linear polynomial $L(\mathbf{x}) = L(\mathbf{x}_L)$ and r elements $\xi_1, \ldots, \xi_r \in \mathbb{F}_q^\times$ to generate a signature in ELSA efficiently (see §2.3).

Secret key. The invertible affine maps $\mathcal{T}, \mathcal{S}$, the quadratic map $\mathcal{F}$, the linear polynomial L, and the constants $\xi_1, \ldots, \xi_r \in \mathbb{F}_q^\times$.

Public key. The quadratic map $\mathcal{P} = {}^t(\mathcal{P}_1, \ldots, \mathcal{P}_m) := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

2.3 Signature Generation and Verification of ELSA

Here, we describe signature generation and signature verification of ELSA.

Signature generation. For a message $\mathbf{m} \in \mathbb{F}_q^m$, compute $\mathbf{z} = {}^t(z_1, \ldots, z_m) = \mathcal{T}^{-1}(\mathbf{m})$. Next, find $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathcal{F}(\mathbf{y}) = \mathbf{z}$ and $L(\mathbf{y})L_i(\mathbf{y}) = \xi_i$ $(1 \le i \le r)$. Finally, compute $\mathbf{w} = \mathcal{S}^{-1}(\mathbf{y}) \in \mathbb{F}_q^n$. The signature for $\mathbf{m}$ is $\mathbf{w}$.

Signature verification. Check whether $\mathcal{P}(\mathbf{w}) = \mathbf{m}$ or not.

In the process of the signature generation, $\mathbf{y} \in \mathbb{F}_q^n$ is found as follows.

How to find $\mathbf{y} \in \mathbb{F}_q^n$.

First, randomly choose $\mathbf{y}_L \in \mathbb{F}_q^l$ with $L(\mathbf{y}_L) \neq 0$ and find a solution $\mathbf{y}_K$ to the system of k linear equations in $\mathbf{x}_K$:

$$\sum_{1 \le i \le r} \xi_i R_{ij}(\mathbf{y}_L, \mathbf{x}_K) = L(\mathbf{y}_L)(z_j - \Phi_j(\mathbf{y}_L)), \quad (1 \le j \le k). \tag{1}$$

Next, find a solution $\mathbf{y}_R$ to the system of r linear equations in $\mathbf{x}_R$:

$$L_i(\mathbf{y}_L, \mathbf{y}_K, \mathbf{x}_R) = L(\mathbf{y}_L)^{-1}\xi_i, \quad (1 \le i \le r). \tag{2}$$

Finally, find a solution $\mathbf{y}_U \in \mathbb{F}_q^u$ to the system of u linear equations in $\mathbf{x}_U$:

$$\sum_{1 \le i \le r} \xi_i R_{i,k+j}(\mathbf{y}_L, \mathbf{y}_K, \mathbf{x}_U, \mathbf{y}_R) = L(\mathbf{y}_L)(z_j - \Phi_{k+j}(\mathbf{y}_L, \mathbf{y}_K) - L'_j(\mathbf{y}_L, \mathbf{y}_K, \mathbf{y}_R)) \tag{3}$$

for $1 \le j \le u$. In this way, we find $\mathbf{y} = {}^t(\mathbf{y}_L, \mathbf{y}_K, \mathbf{y}_U, \mathbf{y}_R) \in \mathbb{F}_q^n$ such that $\mathcal{F}(\mathbf{y}) = \mathbf{z}$.

Note that equations (1)-(3) are derived from

$$L(\mathbf{x}_L)\mathcal{F}_j(\mathbf{x}) = L(\mathbf{x}_L)z_j, \quad L(\mathbf{x}_L)L_i(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R) = \xi_i. \tag{4}$$

Thus we see that $\mathbf{y}$ computed above satisfies $\mathcal{F}(\mathbf{y}) = \mathbf{z}$ and $L(\mathbf{y}_L)L_i(\mathbf{y}_L, \mathbf{y}_K, \mathbf{y}_R) = \xi_i$ for $i = 1, \ldots, r$. Since $\mathbf{w} = \mathcal{S}^{-1}(\mathbf{y}) \in \mathbb{F}_q^n$, the signature $\mathbf{w}$ obtained above satisfies

$$L(\mathcal{S}(\mathbf{w})) \cdot L_i(\mathcal{S}(\mathbf{w})) = \xi_i$$

for $i = 1, \ldots, r$. We also have $L(\mathcal{S}(\mathbf{w})) \neq 0$.

Equations (1) for $1 \leq j \leq k$ can be written as

$$\mathbf{x}_K A + \mathbf{c} = L(\mathbf{y}_L)\left[\mathbf{z}_K - \mathbf{b}(\mathbf{y}_L)\right], \tag{5}$$

where A is a $k \times k$ matrix over $\mathbb{F}_q$, $\mathbf{c}$ is an element of $\mathbb{F}_q^k$, $\mathbf{z}_K := (z_1, \ldots, z_k)$ and $\mathbf{b}(\mathbf{y}_L) = (\Phi_1(\mathbf{y}_L), \ldots, \Phi_k(\mathbf{y}_L)) \in \mathbb{F}_q^k$. Since the entries of A do not depend on $\mathbf{y}_K$, the process of finding $\mathbf{y}_K$ of (5) can be implemented as

$$\mathbf{y}_K = L(\mathbf{y}_L)\left[\mathbf{z}_K - \mathbf{b}(\mathbf{y}_L)\right] A_1 - \mathbf{c}A_1,$$

where $A_1 := A^{-1}$. This means that, if we have A_1 as a part of the secret key and l is small enough, $\mathbf{y}_K$ can be computed in $O(k^2) = O(n^2)$ time. We can easily check that equations (2) and (3) are similar. Then, by choosing Φ_{k+j} sparsely as in [13], one can find $\mathbf{y}_R, \mathbf{y}_U$ in $O(n^2)$ time. As a result, the complexity $O(n^2)$ of the signature generation of ELSA is smaller than that the $O(n^3)$ complexity of Rainbow (see [13, §5]).

2.4 Previous security analysis and parameter selection

In this subsection, we give a short survey of the security analysis of ELSA discussed in [13] and recall the 128-bit security parameter based on that security analysis.

Direct attack. The direct attack generates a dummy signature of a given message by directly solving a system of quadratic equations $\mathcal{P}(\mathbf{x}) = \mathbf{m}$. It is known that, if the polynomial system $\mathcal{P}(\mathbf{x}) - \mathbf{m}$ is semi-regular, the complexity of the hybrid method [1] between the Gröbner basis attack and the exhaustive attack is

$$\ll \min_{k \geq 0} q^k \cdot \left(m \binom{n-k+d_{reg}-1}{d_{reg}} \right)^w, \tag{6}$$

where d_{reg} is the degree of regularity given as the first non-positive coefficient of $(1-t)^m/(1-t)^{m-k}$, and $2 \leq w < 3$ is the linear algebra constant. In [13], the authors chose (6) with $w = 2$ as a lower bound of security against the direct attack.

Rainbow band separation (RBS). Let $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the affine map such that $\varphi(\mathbf{x}) = (\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, L_1(\mathbf{x}), \ldots, L_r(\mathbf{x}))$ and put $\mathcal{F}' := \mathcal{F} \circ \varphi^{-1}$. A similar argument to the one in [13, §3.2] shows that the coefficient matrices $F_1', \ldots, F_m'$ of $\mathcal{F}_1'(\mathbf{x}), \ldots, \mathcal{F}_m'(\mathbf{x})$, i.e. $\mathcal{F}_j'(\mathbf{x}) = {}^t\mathbf{x}F_j'\mathbf{x} + (\text{linear polynomial})$, can be written as follows:

$$F_j' = \begin{pmatrix} *_l & 0 & 0 & * \\ 0 & 0_k & 0 & * \\ 0 & 0 & 0_u & 0 \\ * & * & 0 & 0_r \end{pmatrix} \ (1 \leq j \leq k), \quad \text{and} \quad F_j' = \begin{pmatrix} *_l & * & 0 & * \\ * & *_k & 0 & * \\ 0 & 0 & 0_u & * \\ * & * & * & *_r \end{pmatrix} \ (k+1 \leq j \leq m). \tag{7}$$

Due to these, we see that there exist vectors $\mathbf{t} = {}^t(t_1, \ldots, t_m) \in \mathbb{F}_q^{m-1}$ and $\mathbf{s} = {}^t(s_1, \ldots, s_n) \in \mathbb{F}_q^n$ such that

$$\sum_{1 \le i \le m} s_i \mathcal{P}_i \left(\begin{pmatrix} I_{n-1} & \mathbf{t} \\ 0 & 1 \end{pmatrix} \mathbf{x} \right) = {}^t\mathbf{x} \begin{pmatrix} *_{l+k+u-2} & 0 & * \\ 0 & 0_1 & 0 \\ * & 0 & *_{r+1} \end{pmatrix} \mathbf{x} + (\text{linear polyn.}).$$

Such $(\mathbf{t}, \mathbf{s})$ is part of an equivalent secret key. To recover $(\mathbf{t}, \mathbf{s})$, the attacker has to solve a system of cubic polynomial equations of $\mathbf{t}, \mathbf{s}$. Though it is not easy to estimate its complexity in general, the author of [13] concluded that ELSA is secure enough against RBS attack under a suitable parameter selection.

Rank attacks. Let $P_1, \ldots, P_m$ be the coefficient matrices of $\mathcal{P}_1(\mathbf{x}), \ldots, \mathcal{P}_m(\mathbf{x})$; that is, each P_i is the symmetric matrix of size n such that $\mathcal{P}_i(\mathbf{x}) = {}^t\mathbf{x}P_i\mathbf{x} +$ (linear polynomial in $\mathbf{x}$). The rank attack recovers an equivalent secret key by finding $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_q$ such that the rank of $\alpha_1 P_1 + \cdots + \alpha_m P_m$ is small. By carefully checking the coefficient matrices $F'_1, \ldots, F'_m$ of $\mathcal{F}'_1(\mathbf{x}), \ldots, \mathcal{F}'_m(\mathbf{x})$ given in (7), the authors of [13] estimated the complexities of the rank attacks as follows:

Min-Rank attack: $O(q^{\min\{l+k+1, l+2r-k+1, l+2r+1, 2l+k+1\}} \cdot (\text{polyn.}))$.

High-Rank attack: $O(q^u \cdot \frac{n^3}{6})$.

Kipnis-Shamir's (UOV) attack. Kipnis and Shamir [7] proposed a polynomial time attack to recover an equivalent secret key of the oil and vinegar signature scheme, and Kipnis, Patarin and Goubin [6] generalized it to the unbalanced oil and vinegar signature scheme (UOV). It is known that this attack is also possible when the coefficient matrices are in the form $\begin{pmatrix} 0_o & * \\ * & *_v \end{pmatrix}$ and its complexity is $O(q^{\max\{v-o, 0\}} \cdot (\text{polyn.}))$. The authors of [13] concluded that the complexity of Kipnis-Shamir's attack on ELSA is

$$O(q^{\min\{r-u, k+u, l+r, n-2u-1\}} \cdot (\text{polyn.}))$$

by carefully studying the structure of the coefficient matrices $F'_1, \ldots, F'_m$ of $\mathcal{F}'_1(\mathbf{x}), \ldots, \mathcal{F}'_m(\mathbf{x})$ given in (7) and the process of this attack.

128-bit security parameter recommended by ELSA [13]. On the basis of the above security analysis, the authors of [13] proposed the following 128-bit security parameter

$$\text{ELSA-128}: \quad (q, l, k, u, r, n, m) = (2^8, 6, 28, 15, 30, 79, 43).$$

See [13, Table 4] for a performance comparison with other signature schemes.

3 Our Attack on ELSA

In this section, we describe a chosen message attack on ELSA. Indeed, we show how to recover an equivalent secret key from the information associated with

equations (4) by launching a chosen message attack. We also explain the construction of the equivalent secret key and a method for forging a signature from it.

3.1 Chosen Massage Attack

A chosen message attack is a standard security notion in signature schemes. Let $\mathcal{O}$ be a signing oracle which computes the signature $\mathbf{w} \in \mathbb{F}_q^n$ from a message $\mathbf{m} \in \mathbb{F}_q^m$ using the secret key of ELSA. The chosen message attack tries to generate a valid pair of a message $\mathbf{m}'$ and signature $\mathbf{w}'$ by repeatedly accessing the signing oracle $\mathcal{O}$, where $\mathcal{P}(\mathbf{w}') = \mathbf{m}'$ for the public key $\mathcal{P}$. The authors of ELSA [13] proved that ELSA is existentially unforgeable against the chosen-message attack. However, we show that there is a way to recover an equivalent secret key by launching a chosen message attack. Recall that the signature generation of ELSA uses equations (4) in order to accelerate the signature generation. We also propose an attack that recovers the information associated with equations (4) from the signatures $\mathbf{w}$ given in the chosen message attack.

In a weaker setting, the attacker is not allowed to choose the message $\mathbf{m}$ before asking the signing oracle, which is sometimes called the known message attack. We show that our attack is also feasible in this setting.

3.2 How to Recover the Information Associated with Equations (4)

As shown in §2.2, in ELSA, we use the hidden quadratic equations $L(\mathbf{x})L_i(\mathbf{x}) = \xi_i$ in (4) to generate a signature. By using the existence of the hidden quadratic equations, we explain to be able to recover the r-dimensional subspace

$$\mathcal{L}_{\mathcal{S}} := \mathrm{Span}_{\mathbb{F}_q} \{L_1(\mathcal{S}(\mathbf{x})), \ldots, L_r(\mathcal{S}(\mathbf{x}))\} \subset \mathbb{F}_q[\mathbf{x}] \tag{8}$$

from N valid signatures, where $N := \max\{n+1, \frac{1}{2}(n-r+2)(n-r+3)\}$.

Let $W \subset \mathbb{F}_q^n$ be the set of signatures generated by the ELSA scheme given in §2.2. From §2.3, for any signature $\mathbf{w} \in W$, we have $L(\mathcal{S}(\mathbf{w})) \cdot L_i(\mathcal{S}(\mathbf{w})) = \xi_i$ and $L(\mathcal{S}(\mathbf{w})) \neq 0$. They imply that for $1 \leq i, j \leq r$,

$$\xi_i L_j(\mathcal{S}(\mathbf{w})) - \xi_j L_i(\mathcal{S}(\mathbf{w})) = 0, \ (\mathbf{w} \in W). \tag{9}$$

Defining $L_{ij}(\mathbf{x}) := \xi_i L_j(\mathcal{S}(\mathbf{x})) - \xi_j L_i(\mathcal{S}(\mathbf{x}))$ and $\mathcal{L}_{\mathcal{S}}^0 := \mathrm{Span}_{\mathbb{F}_q}\{L_{ij}(\mathbf{x})\}_{i,j}$, then it is easy to show that $\mathcal{L}_S^0 \subset \mathcal{L}_{\mathcal{S}}$ and $L_{12}(\mathbf{x}), \ldots, L_{1r}(\mathbf{x})$ form a basis of $\mathcal{L}_{\mathcal{S}}^0$, which implies $\dim_{\mathbb{F}_q} \mathcal{L}_{\mathcal{S}}^0 = r - 1$.

To recover the space $\mathcal{L}_S$, we first explain how to recover the subspace $\mathcal{L}_{\mathcal{S}}^0$. By (9), it is clear that $\mathcal{L}_{\mathcal{S}}^0$ is contained in the space of linear polynomials which vanish at any $\mathbf{w} \in W$. Since a linear polynomial in n-variables $\mathbf{x}$ is determined by $(n+1)$-tuple of a point of $\mathbb{F}_q^n$ and its value, in the following experiment, we confirm that the subspace $\mathcal{L}_{\mathcal{S}}^0$ is equal to the space of linear polynomials in n-variables $\mathbf{x}$ which vanish at $n+1$ valid signatures.

Experiment 1. For $n+1$ valid signatures $\mathbf{w}_1, \ldots, \mathbf{w}_{n+1} \in W$, we experimented whether

$$\mathcal{L}_S^0 = \{f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}] \mid \deg f \leq 1, f(\mathbf{w}_i) = 0,\ 1 \leq i \leq n+1\}\,. \tag{10}$$

We performed the experiment with three parameters: Example-1 and Example-2 defined below, and ELSA-128 in §2.4.

$$\begin{aligned}
&\text{Example-1}: \quad (q, l, k, u, r, n, m) = (2^8, 4, 15, 5, 20, 44, 20),\\
&\text{Example-2}: \quad (q, l, k, u, r, n, m) = (2^8, 5, 20, 10, 25, 60, 30),\\
&\text{ELSA-128}: \quad (q, l, k, u, r, n, m) = (2^8, 6, 28, 15, 30, 79, 43).
\end{aligned}$$

We confirmed that the equality (10) holds in all of 100 experiments for each parameter. The results of Experiment 1 lead to the following lemma:

Lemma 1. *$\mathcal{L}_S^0$ is equal to the space of linear polynomials in n-variables $\mathbf{x}$ which vanish at $n+1$ valid signatures $\mathbf{w}_1, \ldots, \mathbf{w}_{n+1} \in W$. Namely, we can recover $\mathcal{L}_S^0$ from $n+1$ valid signatures.*

Next, we explain how to recover the space $\mathcal{L}_S$ from the subspace $\mathcal{L}_S^0$. In the following, for a polynomial $f(\mathbf{x})$ in variables $\mathbf{x}$, the polynomial $f(\mathbf{x}_L, \mathbf{x}_K)$ means $f(\mathbf{x}_L, \mathbf{x}_K, 0, \ldots, 0)$ and $f(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}) := f(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, 0, \ldots, 0, x_{R,r})$.

Choose a basis $\mathcal{L}_1, \ldots, \mathcal{L}_{r-1}$ of $\mathcal{L}_S^0$. Let $\mathcal{S}_1 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an invertible affine map such that

$$(\mathcal{L}_i \circ \mathcal{S}_1)(\mathbf{x}) = x_{R,i}, \quad (1 \leq i \leq r-1). \tag{11}$$

Set $\mathbf{w}' := \mathcal{S}_1^{-1}(\mathbf{w}) \in \mathbb{F}_q^n$. Since $(\mathcal{L}_i \circ \mathcal{S}_1)(\mathbf{w}') = \mathcal{L}_i(\mathbf{w}) = 0$ by (9), the $x_{R,i}$-component of $\mathbf{w}'$ is zero for $1 \leq i \leq r-1$. Namely, we can write $\mathbf{w}' = (\mathbf{w}'_L, \mathbf{w}'_K, \mathbf{w}'_U, 0, \ldots, 0, w'_{R,r})$. Thus, if we define the quadratic polynomial in $(n-r+1)$-variables $\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}$:

$$Q(\mathbf{x}) := (L \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}) \cdot (L_1 \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}) - \xi_1,$$

then we have

$$\begin{aligned}
Q(\mathbf{w}') =& (L \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{w}'_L, \mathbf{w}'_K, \mathbf{w}'_U, w'_{R,r}) \cdot (L_1 \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{w}'_L, \mathbf{w}'_K, \mathbf{w}'_U, w'_{R,r}) - \xi_1\\
=& (L \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{w}') \cdot (L_1 \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{w}') - \xi_1\\
=& (L \circ \mathcal{S})(\mathbf{w}) \cdot (L_1 \circ \mathcal{S})(\mathbf{w}) - \xi_1\\
=& 0.
\end{aligned}$$

Namely, the quadratic polynomial $Q(\mathbf{x}) = Q(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r})$ in $(n-r+1)$-variables $\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}$ has the property vanishing at $\mathcal{S}_1^{-1}(\mathbf{w})$ for any $\mathbf{w} \in W$. Since a quadratic polynomial in $(n-r+1)$-variables $\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}$ is determined by $N' := \frac{1}{2}(n-r+2)(n-r+3)$-tuple of a point of $\mathbb{F}_q^n$ and its value, in the following experiment, we confirm that, up to a constant factor, $Q(\mathbf{x})$ can be recover from the property vanishing at each $\mathcal{S}_1^{-1}(\mathbf{w}_i)$ for N' valid signatures $\mathbf{w}_1, \ldots, \mathbf{w}_{N'} \in W$.

Experiment 2. Set $N' := \frac{1}{2}(n-r+2)(n-r+3)$. For N' valid signatures $\mathbf{w}_1, \ldots, \mathbf{w}_{N'} \in W$, we experimented whether

$$\mathbb{F}_q Q(\mathbf{x}) = \{f \in \mathbb{F}_q[\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}] \mid \deg f \leq 2, f(\mathcal{S}_1^{-1}(\mathbf{w}_i)) = 0,\ 1 \leq i \leq N'\}.$$

Here, $\mathbb{F}_q Q(\mathbf{x})$ stands for the vector space generated by $Q(\mathbf{x})$. We performed the experiment on the same three parameters in Experiment 1, and confirmed that the equality holds in all of 100 experiments for each parameter. The Experiment 2 lead us to the following lemma:

Lemma 2. *Up to a constant factor, we can recover $Q(\mathbf{x})$ by computing a quadratic polynomial in $\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}$ such that it vanishes at $\mathcal{S}_1^{-1}(\mathbf{w}_1), \ldots, \mathcal{S}_1^{-1}(\mathbf{w}_{N'})$. Namely, $Q(\mathbf{x})$ (up to a constant factor) can be recovered from N' valid signatures.*

Lemmas 1 and 2 imply the following:

Proposition 1. *Set $N := \max\{n+1, \frac{1}{2}(n-r+2)(n-r+3)\}$. We can recover the following subspaces (a) and (b) of $\mathbb{F}_q[\mathbf{x}]$ from N valid signatures:*

$$(a)\ \mathcal{L}_{\mathcal{S}}, \qquad (b)\ \mathcal{L}_{\mathcal{S}}^0 + \mathbb{F}_q(L \circ \mathcal{S})(\mathbf{x}).$$

Proof. From Lemmas 1 and 2, we can recover $\mathcal{L}_S^0$ and $Q(\mathbf{x})$ (up to a constant factor) from N valid signatures. We can decompose the recovered $Q(\mathbf{x})$ as follows:

$$Q(\mathbf{x}) = D_1(\mathbf{x})D_2(\mathbf{x}) + c,$$

where D_1, D_2 are linear polynomials in $\mathbf{x}$ and $c \in \mathbb{F}_q$. By the definition of $Q(\mathbf{x})$, we know that

$$\{D_1, D_2\} = \{(L \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}), (L_1 \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r})\}.$$

Since $\mathcal{L}_{\mathcal{S}} = \mathcal{L}_{\mathcal{S}}^0 + \mathbb{F}_q(L_1 \circ \mathcal{S})(\mathbf{x})$, we have

$$\left\{\mathcal{L}_{\mathcal{S}}, \mathcal{L}_{\mathcal{S}}^0 + \mathbb{F}_q(L \circ \mathcal{S})(\mathbf{x})\right\} = \left\{\mathcal{L}_{\mathcal{S}}^0 + \mathbb{F}_q(D_1 \circ \mathcal{S}_1^{-1})(\mathbf{x}), \mathcal{L}_S^0 + \mathbb{F}_q(D_2 \circ \mathcal{S}_1^{-1})(\mathbf{x})\right\}.$$

Thus we can recover two subspaces (a) and (b) from N valid signatures. □

From Proposition 1, we have two subspaces, i.e., $\mathcal{L}_{\mathcal{S}}$ and $\mathcal{L}_{\mathcal{S}}^0 + \mathbb{F}_q(L \circ \mathcal{S})(\mathbf{x})$. At this stage, we cannot determine which one is $\mathcal{L}_{\mathcal{S}}$. However, it is not hard to construct an attack on ELSA.

3.3 Equivalent Secret Key of ELSA and Forging a Signature

We construct an equivalent secret key of ELSA by deforming the central map $\mathcal{F}$ as follows. Let $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the invertible affine map such that

$$\varphi(\mathbf{x}) = {}^t\left(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, L_1(\mathbf{x}), \ldots, L_r(\mathbf{x})\right). \tag{12}$$

Put $\mathcal{F}' := \mathcal{F} \circ \varphi^{-1}$. Thus we have

$$\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} = \mathcal{T} \circ \mathcal{F}' \circ (\varphi \circ \mathcal{S}).$$

By a similar argument as [13, §3.2], it is easy to see that $\mathcal{F}'(\mathbf{x}) = {}^t(\mathcal{F}'_1(\mathbf{x}), \ldots, \mathcal{F}'_m(\mathbf{x}))$ can be written as

$$\begin{aligned}
\mathcal{F}'_j(\mathbf{x}) &= \sum_{1 \le i \le r} x_{R,i} R'_{ij}(\mathbf{x}_L, \mathbf{x}_K) + \Phi'_j(\mathbf{x}_L) \\
&= {}^t\mathbf{x} \begin{pmatrix} *_l & 0 & 0 & * \\ 0 & 0_k & 0 & * \\ 0 & 0 & 0_u & 0 \\ * & * & 0 & 0_r \end{pmatrix} \mathbf{x} + (\text{linear polyn.}), \qquad (1 \le j \le k), \qquad (13) \\
\mathcal{F}'_j(\mathbf{x}) &= \sum_{1 \le i \le r} x_{R,i} R'_{ij}(\mathbf{x}) + \Phi'_j(\mathbf{x}_L, \mathbf{x}_K) \\
&= {}^t\mathbf{x} \begin{pmatrix} *_l & * & 0 & * \\ * & *_k & 0 & * \\ 0 & 0 & 0_u & * \\ * & * & * & *_r \end{pmatrix} \mathbf{x} + (\text{linear polyn.}), \qquad (k+1 \le j \le m), \qquad (14)
\end{aligned}$$

for linear polynomials R'_{ij} and quadratic polynomials Φ'_j.

We define an equivalent secret key of ELSA:

Definition 1. *If two invertible affine maps $\bar{\mathcal{T}} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\bar{\mathcal{S}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ satisfy the following conditions, then the pair $(\bar{\mathcal{T}}, \bar{\mathcal{S}})$ is called an equivalent secret key of the ELSA scheme.*

1. $\mathcal{P}' = {}^t(\mathcal{P}'_1, \ldots, \mathcal{P}'_m) := \bar{\mathcal{T}} \circ \mathcal{P} \circ \bar{\mathcal{S}}$.
2. *For* $1 \le j \le k$,
$$\mathcal{P}'_j(\mathbf{x}) = \mathcal{P}'_j(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R) = \sum_{1 \le i \le r} x_{R,i} \cdot (\textit{linear polyn. in } \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R) + (\textit{quadratic polyn. in } \mathbf{x}_L, \mathbf{x}_R).$$
3. *For* $k+1 \le j \le m$,
$$\mathcal{P}'_j(\mathbf{x}) = \sum_{1 \le i \le r} x_{R,i} \cdot (\textit{linear polyn. in } \mathbf{x}) + (\textit{quadratic polyn. in } \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R).$$

From (13) and (14), it is enough to find a pair $(\bar{\mathcal{T}}, \bar{\mathcal{S}})$ such that

$$(\varphi \circ \mathcal{S} \circ \bar{\mathcal{S}})(\mathbf{x}) = \begin{pmatrix} *_l & 0 & 0 & * \\ * & *_k & 0 & * \\ * & * & *_u & * \\ 0 & 0 & 0 & *_r \end{pmatrix} \mathbf{x}, \quad (\bar{\mathcal{T}} \circ \mathcal{T})(\mathbf{y}) = \begin{pmatrix} *_k & 0 \\ * & *_u \end{pmatrix} \mathbf{y},$$

where $\mathbf{y} = {}^t(y_1, \ldots, y_m)$.

We can forge a signature $\mathbf{w}$ for each message $\mathbf{m} \in \mathbb{F}_q^m$ in the complexity $O(n^3)$ from the equivalent secret key $(\bar{\mathcal{T}}, \bar{\mathcal{S}})$. First compute

$$\bar{\mathbf{m}} = {}^t(\bar{m}_1, \ldots, \bar{m}_m) := \bar{\mathcal{T}}(\mathbf{m}).$$

Then, randomly choose $\mathbf{y}_L \in \mathbb{F}_q^l$ and $\mathbf{y}_R \in \mathbb{F}_q^r$. After that, find a solution $\mathbf{y}_K \in \mathbb{F}_q^k$ of the system of k linear equations in $\mathbf{x}_K$:

$$\bar{m}_j = \mathcal{P}'_j(\mathbf{y}_L, \mathbf{x}_K, \mathbf{y}_R), \quad (1 \le i \le k).$$

Next, find a solution $\mathbf{y}_U \in \mathbb{F}_q^u$ of the system of u linear equations in $\mathbf{x}_U$:

$$\bar{m}_j = \mathcal{P}'_j(\mathbf{y}_L, \mathbf{y}_K, \mathbf{x}_U, \mathbf{x}_R), \quad (k+1 \le j \le m)$$

and compute $\mathbf{w} = \bar{\mathcal{S}}(\mathbf{y}_L, \mathbf{y}_K, \mathbf{y}_U, \mathbf{y}_R)$, which is a signature of the message $\mathbf{m}$.

3.4 How to Recover an Equivalent Secret Key

In §3.2 we showed how to recover the space $\mathcal{L}_{\mathcal{S}}$ in (8) from N valid signatures. Here, we explain how to recover an equivalent secret key of the ELSA scheme from the space $\mathcal{L}_{\mathcal{S}}$.

In this subsection, we choose one subspace from (a) or (b) in Proposition 1, and assume the subspace is equal to $\mathcal{L}_S$ in (8). Then we choose a basis $(\mathcal{L}_1, \ldots, \mathcal{L}_r)$ of the space $\mathcal{L}_{\mathcal{S}}$. We also assume the following, since the argument in this subsection needs only the quadratic part of the polynomials of the central map $\mathcal{F}$ and public key $\mathcal{P}$.

- All linear and quadratic polynomials L_i, R_{ij}, Φ_j in §2.2 are homogeneous,
- the linear polynomials $L'_j(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R)$ $(1 \le j \le u)$ in §2.2 are zero, and
- the secret key $\mathcal{T}, \mathcal{S}$ are linear maps.

Now we explain how to recover an equivalent secret key from the basis $(\mathcal{L}_1, \ldots, \mathcal{L}_r)$ of the space $\mathcal{L}_{\mathcal{S}}$ in (8).

Choose an invertible linear map $\mathcal{S}' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that

$$(\mathcal{L}_i \circ \mathcal{S}')(\mathbf{x}) = x_{R,i}, \quad (1 \le i \le r). \tag{15}$$

Since $\mathcal{L}_i(\mathbf{x})$ is a linear combination of $L_1(\mathcal{S}(\mathbf{x})), \ldots, L_r(\mathcal{S}(\mathbf{x}))$, we have

$$(\varphi \circ \mathcal{S} \circ \mathcal{S}')(\mathbf{x}) = \begin{pmatrix} *_l & * & * & * \\ * & *_k & * & * \\ * & * & *_u & * \\ 0 & 0 & 0 & *_r \end{pmatrix} \mathbf{x}.$$

We now denote the matrix above in the right-hand-side by $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ with matrices A, B, C of the sizes $(l+k+u) \times (l+k+u), (l+k+u) \times r, r \times r$, respectively.

Due to (13) and (14), we can easily check that $\mathcal{P}' = {}^t(\mathcal{P}'_1, \ldots, \mathcal{P}'_m) := \mathcal{P} \circ \mathcal{S}' = \mathcal{T} \circ \mathcal{F}' \circ (\varphi \circ \mathcal{S} \circ \mathcal{S}')$ is given by

$$\mathcal{P}'_j(\mathbf{x}) = {}^t\mathbf{x} \left(\begin{array}{ccc:c} & {}^tA \begin{pmatrix} *_l & * & 0 \\ * & *_k & 0 \\ 0 & 0 & 0_u \end{pmatrix} A & \begin{matrix} * \\ * \\ * \end{matrix} \\ \hdashline * & * & * & *_r \end{array}\right) \mathbf{x}, \quad (1 \le j \le m).$$

Thus, there exists an invertible $(l+k+u) \times (l+k+u)$ matrix S_2 such that

$$\mathcal{P}'_j(\begin{pmatrix} S_2 & 0 \\ 0 & I_r \end{pmatrix} \mathbf{x}) = {}^t\mathbf{x} \begin{pmatrix} *_l & * & 0 & * \\ * & *_k & 0 & * \\ 0 & 0 & 0_u & * \\ * & * & * & *_r \end{pmatrix} \mathbf{x}, \quad (1 \le j \le m) \tag{16}$$

and it holds $AS_2 = \begin{pmatrix} *_l & * & 0 \\ * & *_k & 0 \\ * & * & *_u \end{pmatrix}$. This means that the linear map $\mathcal{S}'' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined by $\mathcal{S}''(\mathbf{x}) = \begin{pmatrix} S_2 & 0 \\ 0 & I_r \end{pmatrix} \mathbf{x}$ satisfies

$$(\varphi \circ \mathcal{S} \circ \mathcal{S}' \circ \mathcal{S}'')(\mathbf{x}) = \begin{pmatrix} AS_2 & B \\ 0 & C \end{pmatrix} \mathbf{x} = \begin{pmatrix} *_l & * & 0 & * \\ * & *_k & 0 & * \\ * & * & *_u & * \\ 0 & 0 & 0 & *_r \end{pmatrix} \mathbf{x}. \tag{17}$$

The following lemma follows immediately from this, (13) and (14).

Lemma 3. *Set $\tilde{\mathcal{S}} := \mathcal{S} \circ \mathcal{S}' \circ \mathcal{S}''$. We obtain*

$$\mathcal{F}_j(\tilde{\mathcal{S}}(\mathbf{x})) = \mathcal{F}'_j(\varphi \circ \tilde{\mathcal{S}}(\mathbf{x})) = \begin{cases} {}^t\mathbf{x} \begin{pmatrix} *_l & * & 0 & * \\ * & *_k & 0 & * \\ 0 & 0 & 0_u & 0 \\ * & * & 0 & *_r \end{pmatrix} \mathbf{x}, & (1 \le j \le k) \\ {}^t\mathbf{x} \begin{pmatrix} *_l & * & 0 & * \\ * & *_k & 0 & * \\ 0 & 0 & 0_u & * \\ * & * & * & *_r \end{pmatrix} \mathbf{x}, & (k+1 \le j \le m). \end{cases}$$

From this lemma, it is clear that if $1 \le j \le k$, then the variables $\mathbf{x}_U$ do not appear in $\mathcal{F}'_j(\varphi \circ \tilde{\mathcal{S}}(\mathbf{x}))$. Also if $k+1 \le j \le m$, then $\mathbf{x}_U$ appear in $\mathcal{F}'_j(\varphi \circ \tilde{\mathcal{S}}(\mathbf{x}))$. From this fact, we have the following corollary:

Corollary 1. *Let $\bar{\mathcal{T}} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be an invertible linear map and define $\mathcal{P}'' = (\mathcal{P}''_1, \ldots, \mathcal{P}''_m) := \bar{\mathcal{T}} \circ \mathcal{P} \circ (\mathcal{S}' \circ \mathcal{S}'') = (\bar{\mathcal{T}} \circ \mathcal{T}) \circ \mathcal{F}' \circ (\varphi \circ \tilde{\mathcal{S}})$. If the variables $\mathbf{x}_U$ do not appear in $\mathcal{P}''_j(\mathbf{x})$ for any $1 \le j \le k$, then each $\mathcal{P}''_j(\mathbf{x})$ is a linear combination of $\mathcal{F}'_1(\varphi \circ \tilde{\mathcal{S}}(\mathbf{x})), \ldots, \mathcal{F}'_k(\varphi \circ \tilde{\mathcal{S}}(\mathbf{x}))$. Thus we have*

$$\bar{\mathcal{T}} \circ \mathcal{T}(\mathbf{y}) = \begin{pmatrix} *_k & 0 \\ * & *_u \end{pmatrix} \mathbf{y}.$$

In (17), we now write $\varphi \circ \tilde{\mathcal{S}}(\mathbf{x}) = (\varphi \circ \mathcal{S} \circ \mathcal{S}' \circ \mathcal{S}'')(\mathbf{x}) = \left(\begin{array}{cc:cc} & & 0 & * \\ & A' & 0 & * \\ \hdashline * & * & *_u & * \\ 0 & 0 & 0 & *_r \end{array}\right) \mathbf{x}$ with the matrix A' of the sizes $(l+k) \times (l+k)$. Since $\mathcal{P}''_j(\mathbf{x})$ $(1 \leq j \leq k)$ is a linear combination of $\mathcal{F}'_1(\varphi \circ \tilde{\mathcal{S}}(\mathbf{x})), \ldots, \mathcal{F}'_k(\varphi \circ \tilde{\mathcal{S}}(\mathbf{x}))$, from (13), we can easily check that

$$\mathcal{P}''_j(\mathbf{x}) = {}^t\mathbf{x} \left(\begin{array}{cc:cc} & & 0 & * \\ & {}^tA' \begin{pmatrix} *_l & 0 \\ 0 & 0_k \end{pmatrix} A' & 0 & * \\ \hdashline & & 0_u & 0 \\ & & 0 & *_r \end{array}\right) \mathbf{x}, \quad (1 \leq j \leq k).$$

Thus, there exists an invertible $(l+k) \times (l+k)$ matrix S_3 such that

$${}^tS_3 {}^tA' \begin{pmatrix} *_l & 0 \\ 0 & 0_k \end{pmatrix} A' S_3 = \begin{pmatrix} *_l & 0 \\ 0 & 0_k \end{pmatrix}$$

and it holds $A'S_3 = \begin{pmatrix} *_l & 0 \\ * & *_k \end{pmatrix}$. If we define the linear map $\mathcal{S}''' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ by $\mathcal{S}'''(\mathbf{x}) = \begin{pmatrix} S_3 & 0 \\ 0 & I_{u+r} \end{pmatrix} \mathbf{x}$ and $\bar{\mathcal{S}} := \mathcal{S}' \circ \mathcal{S}'' \circ \mathcal{S}'''$, then we have

$$(\varphi \circ \mathcal{S} \circ \bar{\mathcal{S}})(\mathbf{x}) = \left(\begin{array}{cc:cc} & & 0 & * \\ & A' & 0 & * \\ \hdashline * & * & *_u & * \\ 0 & 0 & 0 & *_r \end{array}\right) \begin{pmatrix} S_3 & 0 \\ 0 & I_{u+r} \end{pmatrix} \mathbf{x} = \left(\begin{array}{cc:cc} & & 0 & * \\ & A'S_3 & 0 & * \\ \hdashline * & * & *_u & * \\ 0 & 0 & 0 & *_r \end{array}\right) = \begin{pmatrix} *_l & 0 & 0 & * \\ * & *_k & 0 & * \\ * & * & *_u & * \\ 0 & 0 & 0 & *_r \end{pmatrix} \mathbf{x}.$$

From this and Corollary 1, the pair $(\bar{\mathcal{T}}, \bar{\mathcal{S}})$ satisfy Definition 1 in §3.3. Thus we recovered an equivalent secret key from the space $\mathcal{L}_{\mathcal{S}}$ in (8).

In Algorithm 1, we describe the detailed algorithm of our proposed attack in this section. Note that our attack needs $N = \max\{n, \frac{1}{2}(n-r+2)(n-r+3)\}$ valid signatures for ELSA with parameter (q, l, k, u, r, n, m).

4 Complexity Analysis and Experimental Results

This section analyzes the complexity of our attack on ELSA and describes an experiment on it.

4.1 Complexity Analysis for Our Proposed Attack

We will use Algorithm 1 to analyze the complexity of our attack described in §3,

Proposition 2. *The complexity of our proposed attack (Algorithm 1) is $O(n^{2\omega})$, where $2 \leq \omega < 3$ is the linear algebra constant.*

Algorithm 1 The detailed algorithm of our proposed attack in §3

Input: The public key $\mathcal{P}(\mathbf{x}) = {}^t(\mathcal{P}_1(\mathbf{x}), \ldots, \mathcal{P}_m(\mathbf{x})) \in \mathbb{F}_q[\mathbf{x}]^m$ of ELSA with parameter (q, l, k, u, r, n, m) and N valid signatures $\mathbf{w}_1, \ldots, \mathbf{w}_N \in \mathbb{F}_q^n$, where $N := \max\left\{n+1, \frac{1}{2}(n-r+2)(n-r+3)\right\}$.

Output: An equivalent secret key $(\bar{\mathcal{T}}, \bar{\mathcal{S}})$ of Definition 1 in §3.3.

1: Compute a basis $(\mathcal{L}_1(\mathbf{x}), \ldots, \mathcal{L}_{r-1}(\mathbf{x}))$ of the $r-1$ dimensional vector space over $\mathbb{F}_q$:

$$\{f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}] \mid \deg f \leq 1, f(\mathbf{w}_i) = 0,\ i = 1, \ldots, n+1\}.$$

Choose an invertible affine map $\mathcal{S}_1 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that

$$(\mathcal{L}_i \circ \mathcal{S}_1)(\mathbf{x}) = x_{R,i},\ \ (1 \leq i \leq r-1).$$

2: Choose a non-zero polynomial $Q(\mathbf{x})$ of the one-dimensional vector space:

$$\left\{f \in \mathbb{F}_q[\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}] \;\middle|\; \deg f \leq 2, f(\mathcal{S}_1^{-1}(\mathbf{w}_i)) = 0, 1 \leq i \leq N\right\}.$$

Decompose $Q(\mathbf{x})$ as follows:

$$Q(\mathbf{x}) = D_1(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}) D_2(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}) + c,$$

where D_1 and D_2 are linear polynomials in $\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U$, and $x_{R,r}$ and $c \in \mathbb{F}_q$. Set

$$D(\mathbf{x}) := D_1(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}). \tag{18}$$

Choose an invertible affine map $\mathcal{S}' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that

$$(\mathcal{L}_i \circ \mathcal{S}')(\mathbf{x}) = x_{R,i},\ \ (1 \leq i \leq r-1),\quad (D \circ \mathcal{S}_1^{-1} \circ \mathcal{S}')(\mathbf{x}) = x_{R,r}.$$

3: Compute the coefficient matrix $\tilde{P}_j$ of size $l+k+u$ associated with the quadratic polynomial $(\mathcal{P}_j \circ S')(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U)$ for $1 \leq j \leq m$. Find an invertible matrix S_2 of size $l+k+u$ such that ${}^t S_2 \tilde{P}_j S_2 = \begin{pmatrix} *_{l+k} & 0 \\ 0 & 0_u \end{pmatrix}$ for $1 \leq j \leq m$. If there is no such matrix, then return to Step 2 and reset (18)

$$D(\mathbf{x}) := D_2(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U, x_{R,r}).$$

Let $\mathcal{S}'' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the invertible linear map such that $\mathcal{S}''(\mathbf{x}) = \begin{pmatrix} S_2 & 0 \\ 0 & I_r \end{pmatrix} \mathbf{x}$.

4: Compute an invertible linear map $\bar{\mathcal{T}} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ such that the variables $\mathbf{x}_U$ do not appear in $\mathcal{P}''_j(\mathbf{x})$ for any $1 \leq j \leq k$, where $\mathcal{P}'' = (\mathcal{P}''_1, \ldots, \mathcal{P}''_m) := \bar{\mathcal{T}} \circ \mathcal{P} \circ (\mathcal{S}' \circ \mathcal{S}'')$. Namely, $\mathcal{P}''_j(\mathbf{x}) = \mathcal{P}''_j(\mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_R)$ for $1 \leq j \leq k$.

5: Compute the coefficient matrix $\tilde{P}''_j$ of size $l+k$ associated with $\mathcal{P}''_j(\mathbf{x}_L, \mathbf{x}_K)$ for $1 \leq j \leq k$. Find an invertible matrix S_3 of size $l+k$ such that for $1 \leq j \leq m$, ${}^t S_3 \tilde{P}''_j S_3 = \begin{pmatrix} *_l & 0 \\ 0 & 0_k \end{pmatrix}$. Let $\mathcal{S}''' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the invertible linear map such that $\mathcal{S}'''(\mathbf{x}) = \begin{pmatrix} S_3 & 0 \\ 0 & I_{u+r} \end{pmatrix} \mathbf{x}$. Finally compute $\bar{\mathcal{S}} := \mathcal{S}' \circ \mathcal{S}'' \circ \mathcal{S}'''$.

Proof. In Step 1, we solve a linear system of size $n+1$ to compute

$$\{f(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}] \mid \deg f \leq 1, f(\mathbf{w}_i) = 0,\ i = 1, \ldots, n+1\}.$$

This complexity is $O(n^\omega)$. Similarly, in Step 2, we solve a linear system of size N. Thus the complexity is $O(N^\omega) = O(n^{2\omega})$. In Step 3, we must compute the intersection of the kernel of $\tilde{P}_i$ $(1 \leq i \leq m)$ of size $l+k+u$. This complexity is $O((l+k+u)^{\omega+1}) = O(n^{\omega+1})$. In Step 4, we solve a linear system of size m $(< n)$. In Step 5, we compute the intersection of the kernel of $\tilde{P}'_i$ $(1 \leq i \leq m)$ of size $l+k$. This complexity is $O((l+k)^{\omega+1}) = O(n^{\omega+1})$. Therefore, the complexity of our attack is $O(n^{2\omega})$. □

4.2 Experimental Results of Our Proposed Attack

The experimental results of Algorithm 1 in §3 are presented in Table 1. All the experiments were performed using Magma V2.21-6 [3] running on a 1.6 GHz Intel® Core™ i5 processor with 8GB of memory.

We experimented with three different parameters: Example-1, Example-2, and ELSA-128. ELSA-128 is the 128-bit security parameter in §2.4. For each parameter, we measured the time taken to generate an equivalent secret key with our algorithm and to forge a signature using the equivalent secret key. Table 1 presents the average times of 100 experiments for each parameter. Here, $N := \max\{n+1, \frac{1}{2}(n-r+2)(n-r+3)\}$ is the number of valid signatures needed to recover an equivalent secret key of ELSA with parameter (q, l, k, u, r, n, m).

Table 1. Experimental results (second) of our attack against ELSA with parameter (q, l, k, u, r, n, m) and $N = \max\{n+1, \frac{1}{2}(n-r+2)(n-r+3)\}$ is the number of valid signatures.

Parameters	(q, l, k, u, r, n, m)	N	Algorithm 1	forging a signature
Example-1	$(2^8, 4, 15, 5, 20, 44, 20)$	351	7.928	0.021
Example-2	$(2^8, 5, 20, 10, 25, 60, 30)$	703	40.19	0.069
ELSA-128	$(2^8, 6, 28, 15, 30, 79, 43)$	1326	176.68	0.101

For example, the number of valid signatures in ELSA-128 needed for our attack to succeed is 1326. It is possible to generate an equivalent secret key in about 176.68 seconds and forge a signature in about 0.101 seconds.

5 Conclusion

We studied the security of the post-quantum signature scheme ELSA, which is an efficient variant of Rainbow. In order to accelerate signature generation, ELSA uses special hidden quadratic equations. We proved such hidden quadratic equations can be recovered by using valid signatures, and obtained an equivalent secret key of ELSA from the hidden quadratic equations. According to our

experiments conducted using Magma on a standard personal computer, it takes about 177 seconds to recover an equivalent secret key from 1326 valid signatures for the claimed 128-bit security parameter of ELSA.

Finally, we stress that the original Rainbow has no hidden quadratic equations discussed in this paper, and thus it is infeasible to apply our attack to Rainbow.

Acknowledgements. This work was supported by JST CREST no.JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181.

References

1. L. Bettale, J.C. Faugère, L. Perret, Solving polynomial systems over finite fields: Improved analysis of the hybrid approach, ISSAC 2012 (2012), pp.67–74.
2. D.J. Bernstein, J. Buchmann, E. Dahmen (Eds.): Post-Quantum Cryptography. Springer, 2009.
3. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (1997), pp. 235–265.
4. J. Ding, J. E. Gower, D. S. Schmidt: Multivariate Public Key Cryptosystems, Springer, 2006.
5. J. Ding, D. Schmidt, Rainbow, a new multivariate polynomial signature scheme, ACNS'05, LNCS 3531 (2005), pp.164–175.
6. A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt'99, LNCS 1592 (1999), pp.206–222.
7. A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, Crypto'98, LNCS 1462 (1998), pp.257–267.
8. T. Matsumoto, H. Imai, Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. EUROCRYPT 1988. LNCS 330 (1988), pp. 419–453.
9. NIST, Post-Quantum Cryptography Standardization `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/`
10. J. Patarin, N. Courtois, L. Goubin: QUARTZ, 128-bit long digital signatures. CTRSA 2001, LNCS 2020 (2001), pp. 282–297.
11. A. Petzoldt, M.S. Chen, B.Y. Yang, C. Tao, J. Ding: Design principles for HFEv-based signature schemes. Asiacrypt 2015 Part I, LNCS 9452 (2015), pp. 311–334.
12. P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), pp.1484–1509.
13. K.-A. Shim, C.-M. Park, N. Koo, An existential unforgeable signature scheme based on multivariate quadratic equations. Asiacrypt 2017, LNCS 10624 (2017), pp. 37-64.
14. B.-Y. Yang, J.-M. Chen, Building secure tame-like multivariate public-key cryptosystems: the new TTS, ACISP'05, LNCS 3574 (2005), pp.518–531.