Recommended Paper

Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017

Yasufumi Hashimoto[1,a)] Yasuhiko Ikematsu[2,†1,b)] Tsuyoshi Takagi[2,c)]

Received: December 10, 2018, Accepted: March 5, 2019

Abstract: One of the most efficient post-quantum signature schemes is Rainbow whose hardness 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 1,326 valid signatures.

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

1. Introduction

Shor [15] proposed quantum algorithms to factor large integers and to find discrete logarithms over a finite field of large order in polynomial time. This means that if large-scale quantum computers will be realized in the future, 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 [1]. 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 [11].

Multivariate public key cryptosystems (MPKCs) [5] are considered to be promising candidates for PQC. The early MPKCs are the Matsumoto-Imai scheme [10] and the Moon Letter scheme [16], and many MPKCs have been proposed until now. Among them, some schemes UOV [8] and HFEv$^-$ [12], [13] have survived in two decades, and seem efficient enough. Actually, several MPKCs have been submitted to the NIST PQC standardization. In particular, Rainbow [6], a multi-layered version of the UOV scheme, has been gathered attention because of its efficiency, modest computational cost, high security and simplicity.

The ELSA [14] signature scheme, studied in this paper, is a variant of Rainbow proposed at Asiacrypt 2017 by Shim et al. and is more efficient than Rainbow; that is, its secret key is smaller and its signature generation is faster. Shim et al. actually succeeded in reducing the complexity of signature generation from $O(n^3)$ for Rainbow to $O(n^2)$, where n is the number of variables used in a public key, 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 (see Section 2.3). Furthermore, ELSA has an existential unforgeability against an adaptive chosen-message attack (EUF-CMA), which 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. Note that EUF-CMA security for Rainbow was proven recently [4].

In this paper, we propose a chosen message attack on ELSA, under the condition that we can obtain valid signatures by repeatedly accessing a signing oracle. Recall that ELSA possesses hidden quadratic equations for accelerating the signature generation, that are not used in Rainbow. Once the hidden quadratic equations are recovered, an attacker can obtain an equivalent secret key of ELSA and forge a signature for an arbitrary message by its equivalent secret key. We show that a piece of information in the hidden quadratic equations can be recovered from at most

[1] Department of Mathematical Science, University of the Ryukyus, Nishihara-cho, Okinawa 903–0213, Japan

[2] Department of Mathematical Informatics, the University of Tokyo, Bunkyo, Tokyo 113–8656, Japan

[†1] Presently with Institute of Mathematics for Industry, Kyushu University

[a)] hashimoto@math.u-ryukyu.ac.jp

[b)] ikematsu@imi.kyushu-u.ac.jp

[c)] takagi@mist.i.u-tokyo.ac.jp

This paper has been published in the 13th International Workshop on Security (IWSEC2018) held on September 2018 and recommended to IPSJ Journals by IWSEC2018 program Co-chairs. The preliminary version of this paper was published at the 13th International Workshop on Security (IWSEC 2018) [7].

n^2 valid signatures given by the chosen message attack. Our attack is very efficient. More precisely, its complexity is $O(n^{2\omega})$, where n is the number of variables and $2 \le \omega < 3$ is the linear algebra constant. We implemented our attack on Magma [3], and succeeded in recovering an equivalent secret key with 1,326 valid signatures in 177 seconds for the parameters selected in Ref. [14] as 128-bit security.

Our paper is organized as follows: in Section 2, we briefly summarize the ELSA scheme and its previous security analysis given in Ref. [14]. In Section 3, we discuss our new attack and give a detailed algorithm to obtain an equivalent secret key of ELSA. In Section 4, we perform the complexity analysis of our new attack and present a Magma implementation of our algorithm. We conclude our paper in Section 5.

2. The ELSA Signature Scheme

We briefly explain the basic concept of multivariate signature schemes and summarize the construction of the ELSA scheme and its previous security analysis following [14].

2.1 Multivariate Signature Scheme

Let $n, m \ge 1$ 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 $\mathcal{P}(x_1, \dots, x_n) = {}^t(\mathcal{P}_1(x_1, \dots, x_n), \dots, \mathcal{P}_m(x_1, \dots, x_n))$ given by

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

for $1 \le l \le m$, 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 computes $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{m})$, finds $\mathbf{y}$ with $\mathcal{F}(\mathbf{y}) = \mathbf{z}$, and then computes $\mathbf{w} = \mathcal{S}^{-1}(\mathbf{y})$. A signature for $\mathbf{m}$ is given by $\mathbf{w}$. The verification involves checking whether $\mathcal{P}(\mathbf{w}) = \mathbf{m}$.

2.2 Key Generation of ELSA

We now describe the construction of ELSA [14].

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

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

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

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

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

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

for $1 \le j \le u$. The central map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ of ELSA is given by

$$\mathcal{F}(\mathbf{x}) := {}^t(\mathcal{F}_1(\mathbf{x}), \dots, \mathcal{F}_k(\mathbf{x}), \mathcal{F}_{k+1}(\mathbf{x}), \dots, \mathcal{F}_m(\mathbf{x})).$$

The secret and public keys of ELSA are as follows.

Secret key. Two invertible affine maps $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$, $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$, a linear polynomial $L(\mathbf{x}) = L(\mathbf{x}_L)$, constants $\xi_1, \dots, \xi_r \in \mathbb{F}_q^\times$, and the quadratic map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ constructed above,

Public key. The quadratic map

$$\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^m.$$

2.3 Signature Generation and Verification of ELSA

In this subsection, we describe the signature generation and the verification of ELSA.

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

Signature verification. The signature $\mathbf{w}$ is verified if $\mathcal{P}(\mathbf{w}) = \mathbf{m}$ holds.

In the process of signature generation, $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathcal{F}(\mathbf{y}) = \mathbf{z}$ and $L(\mathbf{y})L_i(\mathbf{y}) = \xi_i$ for $1 \le i \le r$ is found as follows.

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

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

for $1 \le j \le k$. Next, find a solution $\mathbf{y}_R \in \mathbb{F}_q^r$ of the system of r linear equations of $\mathbf{x}_R$ given by

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

for $1 \le i \le r$. Finally, find a solution $\mathbf{y}_U \in \mathbb{F}_q^u$ of the system of u linear equations of $\mathbf{x}_U$ given by

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

for $1 \le j \le u$. Then $\mathbf{y} := {}^t(\mathbf{y}_R, \mathbf{y}_L, \mathbf{y}_K, \mathbf{y}_U) \in \mathbb{F}_q^n$ is to be found.

Note that the equations (1)–(3) are derived from

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

and then $\mathbf{y} \in \mathbb{F}_q^n$ 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 $1 \le i \le r$.

We now study the efficiency of the signature generation. The system of Eq. (1) is written by

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

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

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

where $A_1 := A^{-1}$ is also independent of $\mathbf{y}_L$. This means that, if we store A_1 as a part of the secret key and choose l small enough, the complexity of finding $\mathbf{y}_K$ is $O(k^2) = O(n^2)$. For the Eqs. (2) and (3), the situations are similar. Then, if one chooses Φ_{k+j} sparsely as given in Ref. [14], the complexities of finding $\mathbf{y}_R$, $\mathbf{y}_U$ are also $O(n^2)$. Thus the total complexity of the signature generation in ELSA is $O(n^2)$, which is smaller than the complexity $O(n^3)$ of the signature generation of Rainbow (see Ref. [14], Section 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 Ref. [14] and state the 128-bit security parameter based on that security analysis.

Direct Attack. The direct attack generates a dummy signature of a given message by solving a system of quadratic equations $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ directly. It is known that, if the polynomial system $\mathcal{P}(\mathbf{x}) - \mathbf{m}$ is semi-regular, the complexity of the hybrid method [2] between the Gröbner basis attack and the exhaustive attack is

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

where d_{reg} is the degree of regularity given as the first non-positive coefficient of $(1-t^2)^m/(1-t)^{n-k}$, and $2 \leq w < 3$ is the linear algebra constant. In Ref. [14], the authors chose Ep. (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 with

$$\varphi(\mathbf{x}) = {}^t\,(L_1(\mathbf{x}), \dots, L_r(\mathbf{x}), \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U)$$

and $\mathcal{F}' := \mathcal{F} \circ \varphi^{-1}$. Note that

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

Due to the discussions in Ref. [14], Section 3.2, we see that the coefficient matrices $F'_1, \dots, F'_m$ of $\mathcal{F}'_1(\mathbf{x}), \dots, \mathcal{F}'_m(\mathbf{x})$, i.e., $\mathcal{F}'_j(\mathbf{x}) = {}^t\mathbf{x}F'_j\mathbf{x}$ + (linear form), are written by

$$F'_j = \begin{cases} \begin{pmatrix} 0_r & * & * & 0 \\ * & *_l & 0 & 0 \\ * & 0 & 0_k & 0 \\ 0 & 0 & 0 & 0_u \end{pmatrix}, & (1 \leq j \leq k), \\[2ex] \begin{pmatrix} *_r & * & * & * \\ * & *_l & * & 0 \\ * & * & *_k & 0 \\ * & 0 & 0 & 0_u \end{pmatrix}, & (k+1 \leq j \leq m). \end{cases} \qquad (7)$$

Then there exist vectors $\mathbf{s} = {}^t(s_1, \dots, s_{n-1}) \in \mathbb{F}_q^{n-1}$ and $\mathbf{t} = {}^t(t_1, \dots, t_m) \in \mathbb{F}_q^m$ such that

$$\sum_{1 \leq i \leq m} t_i \mathcal{P}_i \left(\begin{pmatrix} I_{n-1} & \mathbf{s} \\ 0 & 1 \end{pmatrix} \mathbf{x} \right) = {}^t\mathbf{x} \begin{pmatrix} *_{n-1} & 0 \\ 0 & 0_1 \end{pmatrix} \mathbf{x} + \text{(linear form)}.$$

Such a pair $(\mathbf{s}, \mathbf{t})$ gives partial information of the secret key $(\mathcal{S}, \mathcal{T})$. To recover $(\mathbf{s}, \mathbf{t})$, the attacker has to solve a system of cubic polynomial equations of $\mathbf{s}, \mathbf{t}$. While it is not easy to estimate its complexity in general, the authors of Ref. [14] concluded that ELSA is secure enough against RBS attack under a suitable parameter selection.

Rank Attacks. Let $P_1, \dots, P_m$ be the coefficient matrices of $\mathcal{P}_1(\mathbf{x}), \dots, \mathcal{P}_m(\mathbf{x})$, i.e., P_i is an $n \times n$ (symmetric) matrix with $\mathcal{P}_i(\mathbf{x}) = {}^t\mathbf{x}P_i\mathbf{x}$ + (linear polynomial in $\mathbf{x}$). The rank attack recovers an equivalent secret key partially by finding $\alpha_1, \dots, \alpha_m \in \mathbb{F}_q$ such that the rank of

$$\alpha_1 P_1 + \cdots + \alpha_m P_m$$

is small. By checking the coefficient matrices $F'_1, \dots, F'_m$ of $\mathcal{F}'_1(\mathbf{x}), \dots, \mathcal{F}'_m(\mathbf{x})$ as given in Ep. (7) carefully, the authors of Ref. [14] estimated the complexities of the rank attacks as follows.

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

High-Rank Attack: $O\left(q^u \cdot n^3\right)$.

Kipnis-Shamir's (UOV) Attack. Kipnis and Shamir [9] proposed a polynomial time attack to recover an equivalent secret key of the oil and vinegar signature scheme, and Kipnis et al. [8] 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 Ref. [14] concluded that the complexity of Kipnis-Shamir's attack on ELSA is $O\left(q^{\min\{r-u, k+u, l+r, n-2u-1\}} \cdot \text{(polyn.)}\right)$ by studying the structure of the coefficient matrices $F'_1, \dots, F'_m$ of $\mathcal{F}'_1(\mathbf{x}), \dots, \mathcal{F}'_m(\mathbf{x})$ given in Ep. (7) and the process of this attack carefully.

Security Parameters. Based on the security analyses above, the following 80, 96, and 128-bit security parameters are estimated.

$$\begin{aligned} &\textbf{ELSA-}80: && (q, r, l, k, u, n, m) = (2^8, 19, 1, 17, 9, 46, 26), \\ &\textbf{ELSA-}96: && (q, r, l, k, u, n, m) = (2^8, 23, 2, 20, 11, 56, 31), \qquad (8) \\ &\textbf{ELSA-}128: && (q, r, l, k, u, n, m) = (2^8, 30, 6, 28, 15, 79, 43). \end{aligned}$$

The 128-bit security parameter ELSA-128 was recommended in Ref. [14], and the others are security parameters we estimated.

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 Eq. (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 Message Attack

A chosen message attack is a standard security notion in signature schemes. Let 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 [14] 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 Eq. (4) in order to accelerate the signature generation. The reduced problem used in ELSA is different from that used in Rainbow, namely, ELSA has a special structure of using Eq. (4), which leaks the information related to the secret key. We propose an attack that recovers the information associated with Eq. (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 Recovering the Hidden Polynomials

In this subsection, we describe how to recover the space

$$\mathcal{L}_{\mathcal{S}} := \mathrm{Span}_{\mathbb{F}_q}\{L_1(\mathcal{S}(\mathbf{x})), \ldots, L_r(\mathcal{S}(\mathbf{x}))\} \subset \mathbb{F}_q[\mathbf{x}] \tag{9}$$

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

Let $W \subset \mathbb{F}_q^n$ be the set of signatures generated by ELSA. Recall Section 2.3 that a signature $\mathbf{w} \in W$ is given by $\mathbf{w} = \mathcal{S}^{-1}(\mathbf{y})$, where $\mathbf{y} \in \mathbb{F}_q^n$ satisfies $L(\mathbf{y}) \neq 0$ and $L(\mathbf{y})L_i(\mathbf{y}) = \xi_i$ for $1 \leq i \leq r$. Then any $\mathbf{w} \in W$ satisfies $L(\mathcal{S}(\mathbf{w})) \neq 0$ and

$$L(\mathcal{S}(\mathbf{w}))L_i(\mathcal{S}(\mathbf{w})) = \xi_i \tag{10}$$

for $1 \leq i \leq r$. Multiplying $L_j(\mathcal{S}(\mathbf{w}))$ to both hand sides of (10), we have

$$\xi_i L_j(\mathcal{S}(\mathbf{w})) - \xi_j L_i(\mathcal{S}(\mathbf{w})) = 0 \tag{11}$$

for $1 \leq i, j \leq r$. Let

$$\mathcal{L}^1_{\mathcal{S}} := \mathrm{Span}_{\mathbb{F}_q}\left\{L_{ij}(\mathbf{x}) := \xi_i L_j(\mathcal{S}(\mathbf{x})) - \xi_j L_i(\mathcal{S}(\mathbf{x}))\right\}_{1\leq i,j\leq r},$$
$$V_1 := \left\{h \in \mathbb{F}_q[\mathbf{x}] \;\middle|\; \deg h \leq 1, h(\mathbf{w}) = 0 \; (\forall \mathbf{w} \in W)\right\}.$$

It is clear that $\mathcal{L}^1_{\mathcal{S}} \subset \mathcal{L}_{\mathcal{S}}$ and $\dim_{\mathbb{F}_q} \mathcal{L}^1_{\mathcal{S}} = r-1$ since any polynomial in $\mathcal{L}^1_{\mathcal{S}}$ is a linear combination of $L_{12}(\mathbf{x}), \ldots, L_{1r}(\mathbf{x})$ and $L_{12}(\mathbf{x}), \ldots, L_{1r}(\mathbf{x})$ are linearly independent. Furthermore, due to Eq. (11), we see that $\mathcal{L}^1_{\mathcal{S}} \subset V_1$, and $\mathcal{L}^1_{\mathcal{S}} = V$ holds if $\dim_{\mathbb{F}_q} V_1 = r-1$. While estimating $\dim_{\mathbb{F}_q} V_1$ theoretically is not easy, we computed it experimentally in 100 times for the parameters (8) and checked that $\dim_{\mathbb{F}_q} V_1 = r-1$ always holds. We can thus consider that $\mathcal{L}^1_{\mathcal{S}} = V_1$. Note that we can recover $\mathcal{L}^1_{\mathcal{S}}$ by using $n+1$ valid signatures since the number of coefficients of a linear form of n variables is $n+1$.

Recall that $\mathcal{L}^1_{\mathcal{S}} \subset \mathcal{L}_{\mathcal{S}}$, $\dim_{\mathbb{F}_q} \mathcal{L}_{\mathcal{S}} = r$ and $\dim_{\mathbb{F}_q} \mathcal{L}^1_{\mathcal{S}} = r-1$. Then one more linear form is required to recover $\mathcal{L}_{\mathcal{S}}$. We can obtain such a linear form by $\mathcal{L}^1_{\mathcal{S}}$ and quadratic forms derived from Eq. (10) in the following way.

Choose a basis $\{\mathcal{L}_1, \ldots, \mathcal{L}_{r-1}\}$ of $\mathcal{L}^1_{\mathcal{S}}$ and recover an invertible affine map $\mathcal{S}_0 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with

$$(\mathcal{L}_i \circ \mathcal{S}_0)(\mathbf{x}) = x_{R,i} \tag{12}$$

for $1 \leq i \leq r-1$. Since $(\mathcal{L}_i \circ \mathcal{S}_0)(\mathcal{S}_0^{-1}(\mathbf{w})) = \mathcal{L}_i(\mathbf{w}) = 0$ holds for $\mathbf{w} \in W$ and $1 \leq i \leq r-1$, the $x_{R,1}, \ldots, x_{R,r-1}$-components of $\mathbf{w}' := \mathcal{S}_0^{-1}(\mathbf{w})$ are zero, i.e. any $\mathbf{w}' \in \mathcal{S}_0^{-1}(W)$ is written by

$$\mathbf{w}' = \left(0, \ldots, 0, w'_{R,r}, \mathbf{w}'_L, \mathbf{w}'_K, \mathbf{w}'_U\right).$$

We can then consider that $\mathcal{S}_0^{-1}(W)$ is a subset of $\mathbb{F}_q^{n-r+1}$.

Now define the quadratic forms $Q_1(\mathbf{x}), \ldots, Q_r(\mathbf{x})$ by

$$Q_i(\mathbf{x}) := (L \circ \mathcal{S} \circ \mathcal{S}_0)(0, \ldots, 0, x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U)$$
$$\cdot (L_i \circ \mathcal{S} \circ \mathcal{S}_0)(0, \ldots, 0, x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U) - \xi_i,$$

i.e., $Q_i(\mathbf{x})$ is a quadratic form of $n-r+1$ variables $x_{R,r}, x_{L,1}, \ldots, x_{U,u}$, and study the relation between the following two sets.

$$\mathcal{L}^2_{\mathcal{S}} := \mathrm{Span}_{\mathbb{F}_q}\{\, Q_i(\mathbf{x}) \,\}_{1\leq i\leq r},$$
$$V_2 := \Big\{h \in \mathbb{F}_q[x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U] \;\Big|\; \deg h \leq 2, h(\mathbf{w}') = 0 (\forall \mathbf{w}' \in \mathcal{S}_0^{-1}(W))\Big\}.$$

Since

$$Q_i(\mathbf{w}') = (L \circ \mathcal{S} \circ \mathcal{S}_0)(\mathbf{w}') \cdot (L_i \circ \mathcal{S} \circ \mathcal{S}_0)(\mathbf{w}') - \xi_i$$
$$= (L \circ \mathcal{S})(\mathbf{w}) \cdot (L_i \circ \mathcal{S})(\mathbf{w}) - \xi_i = 0 \tag{13}$$

for any $\mathbf{w}' \in \mathcal{S}_0^{-1}(W)$, we have $\mathcal{L}^2_{\mathcal{S}} \subset V_2$. Due to Eq. (11), we see that

$$\xi_1 L_i((\mathcal{S} \circ \mathcal{S}_0)(\mathbf{w}') = \xi_i L_1((\mathcal{S} \circ \mathcal{S}_0)(\mathbf{w}')$$

for $2 \leq i \leq r$ and then the polynomials $Q_2(\mathbf{x}), \ldots, Q_r(\mathbf{x})$ are constant multiples of $Q_1(\mathbf{x})$, namely $\mathcal{L}^2_{\mathcal{S}} = Q_1(\mathbf{x}) \cdot \mathbb{F}_q$. While proving $V_2 = \mathcal{L}^2_{\mathcal{S}} = Q_1(\mathbf{x}) \cdot \mathbb{F}_q$ theoretically is not easy, we computed V_2 experimentally in 100 times for the parameters (8) and checked that $\dim_{\mathbb{F}_q} V_2 = 1$ always holds. We can thus consider that $\mathcal{L}^2_{\mathcal{S}}(= Q_1(\mathbf{x}) \cdot \mathbb{F}_q) = V_2$. Note that we can recover $\mathcal{L}^2_{\mathcal{S}}$ by using $N' := \frac{1}{2}(n-r+2)(n-r+3)$ valid signatures since the number of coefficients of a quadratic form of $n-r+1$ variables is N'.

Once $Q_1(\mathbf{x})$ is recovered, decompose $Q_1(\mathbf{x})$ by

$$Q_1(\mathbf{x}) = D_1(\mathbf{x})D_2(\mathbf{x}) + c$$

with linear forms $D_1(\mathbf{x})$, $D_2(\mathbf{x})$ and a constant $c \in \mathbb{F}_q$. By the definition of $Q_1(\mathbf{x})$, we see that one of $D_1(\mathbf{x}), D_2(\mathbf{x})$ is $L((\mathcal{S} \circ \mathcal{S}_0)(\mathbf{x}))$ and the other is $L_1((\mathcal{S} \circ \mathcal{S}_0)(\mathbf{x}))$. We thus conclude that the space $\mathcal{L}_{\mathcal{S}}$ is one of the following two spaces.

$$\mathrm{Span}_{\mathbb{F}_q}\{\mathcal{L}_1(\mathbf{x}), \ldots, \mathcal{L}_{r-1}(\mathbf{x}), D_1(\mathcal{S}_0^{-1}(\mathbf{x}))\},$$
$$\mathrm{Span}_{\mathbb{F}_q}\{\mathcal{L}_1(\mathbf{x}), \ldots, \mathcal{L}_{r-1}(\mathbf{x}), D_2(\mathcal{S}_0^{-1}(\mathbf{x}))\}.$$

While we cannot distinguish $\mathcal{L}_{\mathcal{S}}$ from the other in the two spaces above at the present time, the number of candidates of $\mathcal{L}_{\mathcal{S}}$ is only two. We can try our attack given in the next subsection for both cases and (at least) one of them will recover a desired equivalent secret key.

3.3 Equivalent Secret Key and Forging a Signature

The aim of our attack is to recover a pair of two maps $(\bar{\mathcal{S}}, \bar{\mathcal{T}})$, which is enough to forge a signature for a given message. In this subsection, we describe such a pair $(\bar{\mathcal{S}}, \bar{\mathcal{T}})$.

Recall Section 2.4 that the invertible affine map $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is defined by

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

$\mathcal{F}' := \mathcal{F} \circ \varphi^{-1}$ and

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

The quadratic forms $\mathcal{F}'_1(\mathbf{x}), \dots, \mathcal{F}'_m(\mathbf{x})$ in $\mathcal{F}'(\mathbf{x})$ are written by the coefficient matrices (7). The equivalent secret key of ELSA is defined as follows.

Equivalent Secret Key. Let $\bar{\mathcal{S}} : \mathbb{F}_q^n \to \mathbb{F}_q^n$, $\bar{\mathcal{T}} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be invertible affine maps and

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

If $\bar{\mathcal{P}}(\mathbf{x}) = \left(\bar{\mathcal{P}}_1(\mathbf{x}), \dots, \bar{\mathcal{P}}_m(\mathbf{x})\right)$ is written in the following form, the pair $(\bar{\mathcal{S}}, \bar{\mathcal{T}})$ is called an *equivalent secret key*.

$$\begin{aligned}
\bar{\mathcal{P}}_j(\mathbf{x}) &= {}^t\mathbf{x} \begin{pmatrix} *_r & * & * & 0 \\ * & *_l & 0 & 0 \\ * & 0 & 0_k & 0 \\ 0 & 0 & 0 & 0_u \end{pmatrix} \mathbf{x} \\
&\quad + (\text{linear form of } \mathbf{x}_R, \mathbf{x}_L, \mathbf{x}_U), \quad (1 \le j \le k), \\
\bar{\mathcal{P}}_j(\mathbf{x}) &= {}^t\mathbf{x} \begin{pmatrix} *_r & * & * & * \\ * & *_l & * & 0 \\ * & * & *_k & 0 \\ * & 0 & 0 & 0_u \end{pmatrix} \mathbf{x} \\
&\quad + (\text{linear form of } \mathbf{x}), \quad (k+1 \le j \le m).
\end{aligned} \tag{14}$$

Due to Eq. (7), we can easily check that $(\bar{\mathcal{S}}, \bar{\mathcal{T}})$ satisfying the following condition is an equivalent secret key.

$$\begin{aligned}
\left(\varphi \circ \mathcal{S} \circ \bar{\mathcal{S}}\right)(\mathbf{x}) &= \begin{pmatrix} *_r & 0 & 0 & 0 \\ * & *_l & 0 & 0 \\ * & * & *_k & 0 \\ * & * & * & *_u \end{pmatrix} \mathbf{x}, \\
\left(\bar{\mathcal{T}} \circ \mathcal{T}\right)(\mathbf{y}) &= \begin{pmatrix} *_k & 0 \\ * & *_u \end{pmatrix} \mathbf{y}.
\end{aligned} \tag{15}$$

Once an equivalent secret key $(\bar{\mathcal{S}}, \bar{\mathcal{T}})$ is recovered, we can forge a signature $\mathbf{w} \in \mathbb{F}_q^n$ for a given message $\mathbf{m} \in \mathbb{F}_q^m$ as follows.

Forging a signature. First, compute $\mathbf{z} = {}^t(z_1, \dots, z_m) := \bar{\mathcal{T}}(\mathbf{m})$ and choose $\mathbf{y}_R \in \mathbb{F}_q^r$, $\mathbf{y}_L \in \mathbb{F}_q^l$ randomly. Next, find a solution $\mathbf{y}_K \in \mathbb{F}_q^k$ of the system of k linear equations of $\mathbf{x}_K$ given by

$$\mathcal{P}'(\mathbf{y}_R, \mathbf{y}_L, \mathbf{x}_K) = z_j, \qquad (1 \le i \le k).$$

After that, find a solution $\mathbf{y}_U \in \mathbb{F}_q^u$ of the system of u linear equations of $\mathbf{x}_U$ given by

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

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

We can easily check that the complexity of forging is $O(n^3)$. While it is larger than the complexity $O(n^2)$ of the signature generation of ELSA, it is enough for attackers.

3.4 Recovering an Equivalent Secret Key

In Section 3.2, we show how to recover the space $\mathcal{L}_{\mathcal{S}}$ defined in Eq. (9) from N valid signatures. In this subsection, we explain how to recover an equivalent secret key in the form Eq. (15) from $\mathcal{L}_{\mathcal{S}}$. For simplicity, we assume that $\mathcal{L}_{\mathcal{S}}$ is correctly chosen, $\mathcal{F}_1(\mathbf{x}), \dots, \mathcal{F}_m(\mathbf{x})$ are homogeneous quadratic forms and $\mathcal{S}, \mathcal{T}$ are linear maps. Note that our attack below can be modified without these assumptions easily.

First, choose a basis $\{\mathcal{L}_1(\mathbf{x}), \dots, \mathcal{L}_r(\mathbf{x})\}$ of the space $\mathcal{L}_{\mathcal{S}}$ and find an invertible linear map $\mathcal{S}_1 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\mathcal{L}_1(\mathcal{S}_1(\mathbf{x})), \dots, \mathcal{L}_r(\mathcal{S}_1(\mathbf{x}))$ are linear forms of $\mathbf{x}_R$. Since $\mathcal{L}_i(\mathbf{x})$ is a linear sum of $L_1(\mathcal{S}(\mathbf{x})), \dots, L_r(\mathcal{S}(\mathbf{x}))$, we have

$$(\varphi \circ \mathcal{S} \circ \mathcal{S}_1)(\mathbf{x}) = \begin{pmatrix} *_r & 0 \\ * & *_{l+k+u} \end{pmatrix} \mathbf{x} =: \begin{pmatrix} A & 0 \\ B & C \end{pmatrix} \mathbf{x},$$

where A, B, C are $r \times r$-, $(l+k+u) \times r$-, $(l+k+u) \times (l+k+u)$-matrices respectively. Due to Eq. (7), we see that

$$\begin{aligned}
\mathcal{P}'(\mathbf{x}) &= {}^t(\mathcal{P}'_1(\mathbf{x}), \dots, \mathcal{P}'_m(\mathbf{x})) \\
&:= (\mathcal{P} \circ \mathcal{S}_1)(\mathbf{x}) = (\mathcal{T} \circ \mathcal{F}' \circ (\varphi \circ \mathcal{S} \circ \mathcal{S}_1))(\mathbf{x})
\end{aligned}$$

is written by

$$\mathcal{P}'_j(\mathbf{x}) = {}^t\mathbf{x} \left(\begin{array}{c|c} *_r & * \\ \hline * & {}^tC \begin{pmatrix} *_l & * & 0 \\ * & *_k & 0 \\ 0 & 0 & 0_u \end{pmatrix} C \end{array}\right) \mathbf{x}$$

for $1 \le j \le m$. Then there exists an invertible $(l+k+u) \times (l+k+u)$ matrix C_1 such that

$$\mathcal{P}'_j\left(\begin{pmatrix} I_r & 0 \\ 0 & C_1 \end{pmatrix} \mathbf{x}\right) = {}^t\mathbf{x} \left(\begin{array}{c|ccc} *_r & * & * & * \\ \hline * & *_l & * & 0 \\ * & * & *_k & 0 \\ * & 0 & 0 & 0_u \end{array}\right) \mathbf{x}$$

for $1 \le j \le m$. Such a matrix C_1 can be recovered easily and it holds $CC_1 = \begin{pmatrix} *_l & * & 0 \\ * & *_k & 0 \\ 0 & 0 & 0_u \end{pmatrix}$. This means that the linear map $\mathcal{S}_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined by $\mathcal{S}_2(\mathbf{x}) = \begin{pmatrix} I_r & 0 \\ 0 & C_1 \end{pmatrix} \mathbf{x}$ satisfies

$$\tilde{\mathcal{S}}(\mathbf{x}) := (\varphi \circ \mathcal{S} \circ \mathcal{S}_1 \circ \mathcal{S}_2)(\mathbf{x}) = \begin{pmatrix} *_r & 0 & 0 & 0 \\ * & *_l & * & 0 \\ * & * & *_k & 0 \\ * & * & * & *_u \end{pmatrix} \mathbf{x}. \tag{16}$$

Due to Eqs. (7) and (16), we have

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

Since $\mathcal{P}' \circ \mathcal{S}_2 = \mathcal{T} \circ \mathcal{F}' \circ \tilde{\mathcal{S}}$, there exists an invertible linear map $\mathcal{T}_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$ such that

$$\begin{aligned}\mathcal{P}''(\mathbf{x}) &= (\mathcal{P}_1''(\mathbf{x}), \ldots, \mathcal{P}_m''(\mathbf{x}))\\ &:= (\mathcal{T}_1 \circ \mathcal{P}' \circ \mathcal{S}_2)(\mathbf{x}) = \left((\mathcal{T}_1 \circ \mathcal{T}) \circ \mathcal{F}' \circ \tilde{\mathcal{S}}\right)(\mathbf{x})\end{aligned}$$

is given by

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

It is easy to see that such $\mathcal{T}_1$ satisfies

$$(\mathcal{T}_1 \circ \mathcal{T})(\mathbf{y}) = \begin{pmatrix} *_k & 0\\ * & *_u\end{pmatrix}\mathbf{y}. \tag{17}$$

Let C_2 be the $(l+k)\times(l+k)$ matrix with $\tilde{\mathcal{S}}(\mathbf{x}) = \begin{pmatrix} *_r & 0 & 0\\ * & C_2 & 0\\ * & * & *_u\end{pmatrix}\mathbf{x}$. Due to Eqs. (7), (16) and (17), we see that $\mathcal{P}_1''(\mathbf{x}), \ldots, \mathcal{P}_k''(\mathbf{x})$ are written by

$$\mathcal{P}_j''(\mathbf{x}) = {}^t\mathbf{x}\left(\begin{array}{c:c:c} *_r & * & 0\\ \hdashline * & {}^tC_2\begin{pmatrix} *_l & 0\\ 0 & 0_k\end{pmatrix}C_2 & 0\\ \hdashline 0 & 0 & 0_u\end{array}\right)\mathbf{x}$$

for $1 \le j \le k$. Then there exists an invertible $(l+k)\times(l+k)$ matrix C_3 with

$$\mathcal{P}_j''\left(\begin{pmatrix} I_r & 0 & 0\\ 0 & C_3 & 0\\ 0 & 0 & I_u\end{pmatrix}\mathbf{x}\right) = {}^t\mathbf{x}\begin{pmatrix} *_r & * & * & 0\\ * & *_l & 0 & 0\\ * & 0 & 0_k & 0\\ 0 & 0 & 0 & 0_u\end{pmatrix}\mathbf{x}$$

for $1 \le j \le k$ and it holds $C_2C_3 = \begin{pmatrix} *_l & 0\\ * & *_k\end{pmatrix}$. Note that such a matrix C_3 can be recovered easily. The linear map $\mathcal{S}_3 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined by $\mathcal{S}_3(\mathbf{x}) = \begin{pmatrix} I_r & 0 & 0\\ 0 & C_3 & 0\\ 0 & 0 & I_u\end{pmatrix}\mathbf{x}$ then satisfies

$$\begin{aligned}\left(\tilde{\mathcal{S}} \circ \mathcal{S}_3\right)(\mathbf{x}) &= (\varphi \circ \mathcal{S} \circ \mathcal{S}_1 \circ \mathcal{S}_2 \circ \mathcal{S}_3)(\mathbf{x})\\ &= \begin{pmatrix} *_r & 0 & 0 & 0\\ * & *_l & 0 & 0\\ * & * & *_k & 0\\ * & * & * & *_u\end{pmatrix}\mathbf{x}.\end{aligned} \tag{18}$$

We thus conclude that $(\bar{\mathcal{S}}, \bar{\mathcal{T}}) = (\mathcal{S}_1 \circ \mathcal{S}_2 \circ \mathcal{S}_3, \mathcal{T}_1)$ is an equivalent secret key recovered from the space $\mathcal{L}_S$.

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

Algorithm 1 The Proposed attack on ELSA

```
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 $(q, r, l, k, u, n, m)$ 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 $(\bar{\mathcal{S}}, \bar{\mathcal{T}})$ defined in §3.3.
1: Compute a basis $\{\mathcal{L}_1(\mathbf{x}), \ldots, \mathcal{L}_{r-1}(\mathbf{x})\}$ of the following $r-1$ dimensional
   vector space over $\mathbb{F}_q$.
       $\left\{h(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}] \;\middle|\; \deg h \le 1, h(\mathbf{w}_i) = 0,\ (1 \le i \le n+1)\right\}.$
   Find an invertible affine map $\mathcal{S}_0 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that
       $(\mathcal{L}_i \circ \mathcal{S}_0)(\mathbf{x}) = x_{R,i}$
   for $1 \le i \le r-1$.
2: Compute a non-zero polynomial $Q(\mathbf{x})$ of the following one-dimensional
   vector space.
       $\left\{h \in \mathbb{F}_q[x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U] \;\middle|\; \deg h \le 2, h(\mathcal{S}_0^{-1}(\mathbf{w}_i)) = 0, (1 \le i \le N)\right\}.$
   Decompose $Q(\mathbf{x})$ by
       $Q(\mathbf{x}) = D_1(x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U) \cdot D_2(x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U) + c$
   with linear forms $D_1(x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U), D_2(x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U)$ and a constant
   $c \in \mathbb{F}_q$.
3: Let
       $D(\mathbf{x}) := D_1(x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U).$            (19)
   Find an invertible affine map $\mathcal{S}_1 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that
       $(D \circ \mathcal{S}_0^{-1} \circ \mathcal{S}_1)(\mathbf{x}) = x_{R,r},$
       $(\mathcal{L}_i \circ \mathcal{S}_1)(\mathbf{x}) = x_{R,i}$
   for $1 \le i \le r-1$.
4: Let $\tilde{P}_j'$ be the coefficient matrix of size $l+k+u$ associated with the
   quadratic polynomial $(\mathcal{P}_j \circ \mathcal{S}_1)(0, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U)$ for $1 \le j \le m$. Find an
   invertible $(l+k+u) \times (l+k+u)$ matrix $C_1$ such that
       ${}^tC_1\tilde{P}_j'C_1 = \begin{pmatrix} *_{l+k} & 0\\ 0 & 0_u\end{pmatrix}$
   for $1 \le j \le m$. If there is no such matrix, return to Step 3 and reset (19)
   by
       $D(\mathbf{x}) := D_2(x_{R,r}, \mathbf{x}_L, \mathbf{x}_K, \mathbf{x}_U).$
   Let $\mathcal{S}_2 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the invertible linear map with
       $\mathcal{S}_2(\mathbf{x}) = \begin{pmatrix} I_r & 0\\ 0 & C_1\end{pmatrix}\mathbf{x}.$
5: Find an invertible linear map $\mathcal{T}_1 : \mathbb{F}_q^m \to \mathbb{F}_q^m$ such that the variables $\mathbf{x}_U$
   do not appear in $\mathcal{P}_j''(\mathbf{x})$ for $1 \le j \le k$, where
       $\mathcal{P}''(\mathbf{x}) = (\mathcal{P}_1''(\mathbf{x}), \ldots, \mathcal{P}_m''(\mathbf{x})) := (\mathcal{T}_1 \circ \mathcal{P} \circ (\mathcal{S}_1 \circ \mathcal{S}_2))(\mathbf{x}),$
   namely $\mathcal{P}_1''(\mathbf{x}), \ldots, \mathcal{P}_k''(\mathbf{x})$ are quadratic forms of $\mathbf{x}_R, \mathbf{x}_L, \mathbf{x}_K$.
6: Let $P_j''$ be the coefficient matrix of size $l+k$ associated with
   $\mathcal{P}_j''(0, \mathbf{x}_L, \mathbf{x}_K, 0)$ for $1 \le j \le k$. Find an invertible $(l+k) \times (l+k)$ ma-
   trix $C_3$ such that
       ${}^tC_3P_j''C_3 = \begin{pmatrix} *_l & 0\\ 0 & 0_k\end{pmatrix}$
   for $1 \le j \le k$. Let $\mathcal{S}_3 : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the invertible linear map such that
       $\mathcal{S}_3(\mathbf{x}) = \begin{pmatrix} I_r & 0 & 0\\ 0 & C_3 & 0\\ 0 & 0 & I_u\end{pmatrix}\mathbf{x}.$
   The equivalent secret key is
       $(\bar{\mathcal{S}}, \bar{\mathcal{T}}) = (\mathcal{S}_1 \circ \mathcal{S}_2 \circ \mathcal{S}_3, \mathcal{T}_1).$
```

Table 1 Experiments of our attack on ELSA.

Parameters	(q, r, l, k, u, n, m)	N	Running Time
ELSA-80	$(2^8, 19, 1, 17, 9, 46, 26)$	435	9.42 sec.
ELSA-96	$(2^8, 23, 2, 20, 11, 56, 31)$	630	25.00 sec.
ELSA-128	$(2^8, 30, 6, 28, 15, 79, 43)$	1326	176.68 sec.

4. Complexity and Experiments of Our Attack

In this section, we estimate the complexity of our attack proposed in Section 3 and describe the experimental results.

4.1 Complexity

In the first step of Algorithm 1, we solve a system of $n+1$ linear equations of $n+1$ variables to find the space

$$\left\{h \in \mathbb{F}_q[\mathbf{x}] \;\middle|\; \deg h \le 1, h(\mathbf{w}_i) = 0,\ (1 \le i \le n+1)\right\}.$$

Then the complexity of Step 1 is $O(n^\omega)$. Similarly, we can estimate the complexity of Step 2 by $O(N^\omega) = O(n^{2\omega})$. In Step 3, we can find C_1 such that ${}^tC_1P'_1C_1 = \begin{pmatrix} *_{k+l} & 0 \\ 0 & 0_u \end{pmatrix}$ with the complexity $O((l+k+u)^\omega)$ and verify that C_1 satisfies ${}^tC_1P'_jC_1 = \begin{pmatrix} *_{k+l} & 0 \\ 0 & 0_u \end{pmatrix}$ also for $2 \le j \le m$. Then the complexity of Step 3 is at most $O(n^{\omega+1})$. Similarly, we can estimate the complexities of Step 4 and 5 by $O(n^{\omega+1})$. We thus conclude that the total complexity of our attack is $O(n^{2\omega})$.

This means that our attack is efficient enough to break ELSA. As shown in the next subsection, we implemented our attack on Magma and succeeded in recovering an equivalent secret key efficiently. To preserve 128-bit security for ELSA under the security $O(n^{2\omega})$, one must choose n sufficiently larger than 2^{20}. It is no longer practical.

4.2 Experiments

We implemented our attack on Magma V2.21-6 [3] with a 1.6 GHz Intel® Core™ i5 processor and using an 8 GB of memory for the three parameters (8). **Table 1**, we describe the averages of the running times of 100 experiments to recover equivalent secret keys by Algorithm 1. Note that $N := \max\{n+1, \frac{1}{2}(n-r+2)(n-r+3)\}$ is the number of valid signatures required in our attack. These experimental results show that our attack works well and is quite efficient to recover an equivalent secret key of ELSA.

5. Conclusion

We studied the security of ELSA [14], an efficient variant of Rainbow. ELSA uses special hidden quadratic equations to accelerate signature generation. However, such hidden quadratic equations weaken the security. In fact, we proved that such hidden quadratic equations can be recovered from sufficiently many valid signatures, and an equivalent secret key of ELSA can be obtained from the hidden quadratic equations. Our attack implemented on Magma with a standard personal computer succeeded in recovering an equivalent secret key in about 177 seconds with 1,326 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. Our attack is thus unusable on Rainbow.

Acknowledgments This work was supported by JST CREST (Grant Number JPMJCR14D6). The first author was also supported by JSPS Grant-in-Aid for Scientific Research (C) no. 17K05181. The authors would like to thank the anonymous reviewers for their comments.

References

[1] Bernstein, D.J., Buchmann, J. and Dahmen, E. (Eds.): *Post-Quantum Cryptography*, Springer (2009).

[2] Bettale, L., Faugère, J.C. and Perret, L.: Solving polynomial systems over finite fields: Improved analysis of the hybrid approach, *Proc. 37th International Symposium on Symbolic and Algebraic Computation* (*ISSAC 2012*), pp.67–74 (2012).

[3] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system. I. The user language, *J. Symbolic Comput*, Vol.24, pp.235–265 (1997).

[4] Ding, J., Chen, M.C., Petzoldt, A., et al.: Rainbow, NIST, Post-Quantum Cryptography Standardization, Round 1 Submissions (2017).

[5] Ding, J., Gower, J.E. and Schmidt, D.S.: *Multivariate Public Key Cryptosystems*, Springer (2006).

[6] Ding, J. and Schmidt, D.: Rainbow, a new multivariate polynomial signature scheme, *Proc. Applied Cryptography and Network Security 2005* (*ACNS 2005*), LNCS 3531, pp.164–175 (2005).

[7] Hashimoto, Y., Ikematsu, Y., and Takagi, T.: Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017, *Proc. 13th International Workshop on Security* (*IWSEC 2018*), LNCS 11049, pp.3–18 (2018).

[8] Kipnis, A., Patarin, J. and Goubin, L.: Unbalanced oil and vinegar signature schemes, *Proc. Eurocrypt 1999*, LNCS 1592, pp.206–222 (1999).

[9] Kipnis, A. and Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme, *Proc. Crypto 1998*, LNCS 1462, pp.257–267 (1998).

[10] Matsumoto, T. and Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, *Proc. EUROCRYPT 1988*, LNCS 330, pp.419–453 (1988).

[11] NIST, Post-Quantum Cryptography Standardization, available from ⟨https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/⟩.

[12] Patarin, J., Courtois, N. and Goubin, L.: QUARTZ, 128-bit long digital signatures, Proc. CTRSA 2001, LNCS 2020, pp. 282–297 (2001).

[13] Petzoldt, A., Chen, M.S., Yang, B.Y., et al.: Design principles for HFEv- based signature schemes, *Proc. Asiacrypt 2015 Part I*, LNCS 9452, pp.311–334 (2015).

[14] Shim, K.A., Park, C.M. and Koo, N.: An existential unforgeable signature scheme based on multivariate quadratic equations, *Proc. Asiacrypt 2017*, LNCS 10624, pp.37–64 (2017).

[15] Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.*, Vol.26, No.5, pp.1484–1509 (1997).

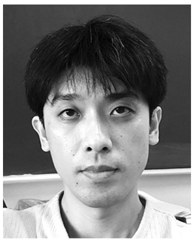
[16] Tsujii, S., Itoh, T., Fujioka, A., et al.: A public-key cryptosystem based on the difficulty of solving a system of non-linear equations, *Systems and Computers in Japan*, Vol.19, No.2, pp.10–18 (1988).

Editor's Recommendation

In this paper, they proposed an efficient chosen message attack method for the existential forgeability of ELSA, that is a signature scheme based on the solving Multivariate Quadratic problem (MQ) of multivariate quadratic polynomials appeared a conference of Asiacrypt2017.

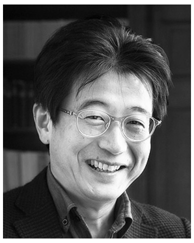
Not only an efficient attack method for the structure of central quadratic map on ELSA, but also they reported results of an implementation and an experimentation. Consequently we selected as IWSEC2018 best paper, so we would like to recommend this paper to IPSJ journals.

(The 13th International Workshop on Security (IWSEC2018)
Program Co-Chairs Atsuo Inomata)



Yasufumi Hashimoto received his Ph.D. in Mathematics in 2006 from Kyushu University. He is currently an associate professor in Department of Mathematical Sciences, University of the Ryukyus. His research interests include Representation Theory, Number Theory and Cryptology.

Yasuhiko Ikematsu received his Ph.D. in mathematics in 2016 from Kyushu University. He was a research fellow in Institute of Mathematics for Industry, Kyushu University from 2016 to 2018 and in Department of Mathematical Informatics, University of Tokyo from April to December in 2018. He is currently an assistant professor in Institute of Mathematics for Industry, Kyushu University. His research interests include number theory and multivariate cryptography.



Tsuyoshi Takagi received his B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively. He had engaged in the research on network security at NTT Laboratories from 1995 to 2001. He received his Ph.D. from Technical University of Darmstadt in 2001. He was an Assistant Professor in the Department of Computer Science at Technical University of Darmstadt until 2005. He is currently a Professor in Department of Mathematical Informatics, University of Tokyo. His current research interests are information security and cryptography. He has received DOCOMO Mobile Science Award in 2013, IEICE Achievement Award in 2013, and JSPS Prize in 2014. He is a Program Chair of the 7th International Conference on Post-Quantum Cryptography PQCrypto 2016, a Program Co-Chair of Asiacrypt 2016 and 2017 and PQCrypto 2017.