An Existential Unforgeable Signature Scheme Based on Multivariate Quadratic Equations

Kyung-Ah Shim(✉), Cheol-Min Park, and Namhun Koo

Division of Integrated Mathematics, National Institute for Mathematical Sciences, Daejeon, Republic of Korea
{kashim,mpcm,nhkoo}@nims.re.kr

Abstract. A multivariate quadratic public-key cryptography (MQ-PKC) is one of the most promising alternatives for classical PKC after the eventual coming of a quantum computer. We propose a new MQ-signature scheme, ELSA, based on a hidden layer of quadratic equations which is an important role in dramatically reducing the secret key size and computational complexity in signing. We prove existential unforgeability of our scheme against an adaptive chosen-message attack under the hardness of the MQ-problem induced by a public key of ELSA with a specific parameter set in the random oracle model. We analyze the security of ELSA against known attacks and derive a concrete parameter based on the security analysis. Performance of ELSA on a recent Intel processor is the fastest among state-of-the-art signature schemes including classical ones and Post-Quantum ones. It takes 6.3 µs and 13.39 µs for signing and verification, respectively. Compared to Rainbow, the secret size of the new scheme has reduced by a factor of 88% maintaining the same public key size.

Keywords: Isomorphism of polynomials problem · Direct attack · Existential unforgeability · Key recovery attack · Multivariate-quadratic problem

1 Introduction

Online banking, e-commerce, mobile communication, and cloud computing depend fundamentally on the security of the underlying cryptographic algorithms. Public-key cryptography (PKC) is particularly crucial since they provide digital signatures and establish secure communication without requiring in-person meetings. In 1996, Shor [49] proposed a quantum algorithm that solves the integer factorization problem and the discrete logarithm problem in finite fields and on elliptic curves in polynomial time. Thus, the existence of a sufficiently large quantum computer would be a real-world threat to break RSA, Diffie-Hellman key exchange, DSA and ECDSA the most widely used PKC in practice. There are four well-known classes of cryptographic primitives that are believed to remain secure in the presence of a quantum computer:

T. Takagi and T. Peyrin (Eds.): ASIACRYPT 2017, Part I, LNCS 10624, pp. 37–64, 2017.
https://doi.org/10.1007/978-3-319-70694-8_2

code-based cryptography (McEliece encryption [37]), lattice-based cryptography (NTRU [30]), hash-based cryptography (Merkle's hash-tree signatures [38]), and multivariate quadratic (MQ) cryptography (HFEv- [40], UOV [33]). These cryptographic primitives have been resist classical and quantum cryptanalysis which has inspired widespread confidence in their suitability as a post-quantum primitive.

MQ-PKC is based on the hardness of solving large systems of multivariate quadratic equations, called MQ-problem which is known to be NP-complete. To construct MQ-PKC, it needs a way to hide a trapdoor. In MQ-PKC, a public key is a system of multivariate quadratic polynomials and a trapdoor is hidden in secret affine layers using the ASA (affine-substitution-affine) structure. A long-standing challenge is to design PKC based on symmetric cipher components which are similar to those used in mainstream block ciphers such as AES. Solving this appealing but difficult challenge would not only increase the diversity in PKC, but might also help reducing the considerable performance gap between PKC and symmetric cryptography. One of the directions was to design public-key schemes from symmetric components. A typical symmetric cipher is built from layers of affine transformations (A) and S-boxes (S). This has been the mainstream of MQ-PKC. The security of the ASA structure relies on the hardness of the isomorphism-of-polynomials (IP) problem [40].

Several new ideas to build MQ-schemes from symmetric cipher components were recently introduced by Biryukov *et al.* [10] at Asiacrypt 2014. They used the so-called ASASA structure: combining two quadratic mappings S by interleaving random affine layers A. With quadratic S layers, the overall scheme has degree 4, so the polynomial description provided by the public key remains of reasonable size. This is very similar to the 2R scheme by Patarin and Goubin [43], which is broken by several attacks [8,18], including a powerful decomposition attack [25]. At Crypto 2015 and Asiacrypt 2015, Biryukov *et al.*'s two public-key encryption schemes are broken by key recovery attacks [27,39].

Since the first MQ-encryption scheme was proposed by Imai and Matsumoto [36], a number of MQ-schemes in this MQ + IP paradigm have been proposed, i.e., these MQ-schemes are not solely based on the MQ-Problem, but also on some variants of the IP problem. Most of the MQ-schemes have been broken due to the uncertainty of the IP problem. There are only two exceptions from the MQ-IP paradigm: HFEv- variants [42,45] and Unbalanced Oil-and-Vinegar (UOV) variants [16,33] as signature schemes. MQ-schemes require simplicity of operations (matrices and vectors) and small fields avoid multiple-precision arithmetic. So, they require only modest computational resources, which makes them attractive for the use on low cost devices such as smart cards [11,12]. In particular, MQ-signature schemes in the MQ + IP paradigm are superior to other competitors in terms of performance and signature size. Despite these advantages, MQ-schemes in the MQ + IP paradigm has two main problems: (i) it has relatively large key sizes and (ii) all the schemes in the MQ + IP paradigm have been proposed with actual parameters for practical, but they have no security reduction to the hardness of the MQ-problem. The reason for this is that

they require a hidden structure which relies on the hardness of the IP problem. Moreover, cryptanalysis results of many MQ-schemes have shown that the IP-problem relies on the MinRank problem [14,24].

In the last years, a few researchers started designing provably secure MQ-schemes based on the hardness of random instances of the MQ-problem. At PKC 2012, Huang *et al.* [31] proposed a public-key encryption scheme with a security reduction to the hardness of solving a set of quadratic equations whose coefficients of highest degree are chosen according to a discrete Gaussian distributions. The other terms are chosen uniformly at random. Such a problem is a variant of the classical problem of solving a system of non-linear equations (PoSSo, PoSSo problem with degree 2 equations is the MQ-problem), which is known to be hard for random systems. They claimed that their variant is not easier than solving the PoSSo problem for random instances. At PKC 2014, Albrecht *et al.* [2] showed that Huang *et al.*'s new problem is reduced to an easy instance of the Learning With Errors problem. They concluded that one cannot find parameters for a secure and practical scheme: a public-key of at least 1.03 GB is required to achieve 80-bit security against the simplest of their attacks.

Another approach is to construction of an MQ-signature scheme from an identification scheme (IDS) based on the MQ-problem via the Fiat-Shamir transform. The resulting scheme [1] obtained from Sakumoto *et al.*'s IDS based on the MQ-problem [47] via the Fiat-Shamir transform is the first provably secure MQ-signature scheme, which solely relies on the MQ-problem. Recently, Chen *et al.* [13] implemented the resulting signature scheme, MQDSS in [1]. MQDSS solves the problem of large key sizes of MQ-PKC by removing the dependence of the IP-problem, but loses the most significant advantages of MQ-ones, fast performance and short signature size. Like this, the history of the design of public-key schemes show that the stronger security arguments the larger performance gap. Therefore, it still remains an open problem to design a practical MQ-signature scheme with a security reduction to the MQ-problem.

For most practical purposes, one still requires a signature scheme that is sufficiently fast and has a short signature size. There have been several attempts to design MQ-signature schemes with higher performance. Gligoroski *et al.* [28] proposed an MQ-signature scheme, MQQ-SIG, based on multivariate quadratic quasigroups (MQQ). MQQ-SIG is the shortest secret key among MQ-ones and the fastest in signing among known signature schemes, but it requires a huge public key which is about 5.7 times and 12,336 times larger than that of Rainbow and ECDSA, respectively. At PKC 2015, Faugère *et al.* [23] mounted polynomial-time key-recovery attacks on all known constructions based on MQQ. They broke an MQQ-SIG instance of an 80-bit security level in less than 2 days. An enhanced version of the Tame Triangular System scheme (enTTS) [15,52] uses very sparse polynomials which make enTTS very efficient in terms of secret key size and signing time, but its public key size is much bigger than other MQ-ones. In this paper, we provide a solution to the two problems of MQ-schemes in the MQ + IP paradigm by proposing a existential unforgeable MQ-signature scheme with a highly optimized practicability for both performance and signature size.

Our Contributions. We propose a new MQ-signature scheme, ELSA, with faster performance and shorter secret key.

- **A New Signature Scheme.** Our signature scheme is based on a hidden layer of quadratic equations. This method makes it possible to remove the use of the Gaussian elimination by reducing the complexity of signing from $\mathcal{O}(n^3)$ to $\mathcal{O}(n^2)$. It plays an important role in dramatically reducing the secret key size and computational cost in signing.
- **High Speed for Both Signing and Verification.** Our scheme is the fastest public-key signature scheme for both signing and verification among the state-of-the-art signature schemes including classical ones and Post-Quantum ones. We implement our scheme for a secure and optimal parameter at a 128-bit security level. Signing of ELSA is about 3.2 times and hundreds of times faster than that of Rainbow and MQDSS, respectively. Also, signing and verification of ELSA is about 17.2 times and 2.3 times faster than those of BLISS-BI, respectively, and signature size of BLISS-BI is about 8.9 times larger than that of ELSA, where BLISS-BI is currently the most efficient lattice-based signature scheme.
- **Shorter Secret Key Size.** Compared to Rainbow, the secret key size of ELSA has reduced by a factor of 88% maintaining the same public key size. Compared to enTTS, the public key size of ELSA have reduced by a factor of 40%.
- **Existential Unforgeability.** We prove existential unforgeability of ELSA against an adaptive chosen-message attack under the hardness of the MQ-problem induced by a public key of ELSA with a specific parameter set in the random oracle model.

Organization. The rest of the paper is organized as follows. In Sect. 2, we propose a new MQ-signature scheme, ELSA. In Sect. 3, we analyze the security of our scheme against all known attacks. In Sect. 4, we give a security proof of ELSA under the hardness of the MQ-problem in the random oracle model. We evaluate performance of our scheme for a secure and optimal parameter at the 128-bit security level and compare it to the state-of-the-art signature schemes in Sect. 5. We conclude in Sect. 6.

2 A New MQ-Signature Scheme

Here, we propose a new MQ-signature scheme based on a hidden layer of quadratic equations.

Let $\mathbb{F}_q$ be a finite field with elements q. A multivariate quadratic system $\mathcal{P} = (\mathcal{P}^{(1)}, \cdots, \mathcal{P}^{(m)})$ of m equations in n variables is defined by

$$\mathcal{P}^{(k)}(x_1, \cdots, x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} p_i^{(k)} x_i + p_0^{(k)},$$

for $k = 1, \cdots, m$, and $p_{ij}^{(k)}, p_i^{(k)}, p_0^{(k)} \in_R \mathbb{F}_q$. The main idea for the construction of MQ-signature schemes is to choose a system $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ of m quadratic

polynomials in n variables which can be easily inverted. We call $\mathcal{F}$ a central map. After that one chooses two affine or linear invertible maps $S\colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $T\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ to hide the structure of the central map $\mathcal{F}$ in the public key. A public key is the composed quadratic map $\mathcal{P} = S \circ \mathcal{F} \circ T$ which is supposed to be hardly distinguishable from a random system and therefore be difficult to invert. The secret key consists of $(S, \mathcal{F}, T)$ which allows to invert $\mathcal{P}$.

2.1 Our Construction

To construct a new central map for an MQ-signature scheme, we need to define the following four index sets as

$$L = \{1, \cdots, l\},\ K = \{l+1, \cdots, l+k\},\ R = \{l+k+1, \cdots, l+k+r\},$$

$$U = \{l+k+r+1, \cdots, l+k+r+u\},$$

where $|L| = l, |K| = k, |R| = r$, and $|U| = u$. A central map is a multivariate quadratic system $\mathcal{F} = (\mathcal{F}^{(1)}, \cdots, \mathcal{F}^{(m)})$ of m equations and n variables defined by

$$\begin{cases} \mathcal{F}^{(1)}(\mathbf{x}) = L_1(\mathbf{x_{L+K+R}})R_{11}(\mathbf{x_{L+K}}) + \cdots + L_r(\mathbf{x_{L+K+R}})R_{1r}(\mathbf{x_{L+K}}) + \Phi_1(\mathbf{x_L}), \\ \qquad\vdots \\ \mathcal{F}^{(k)}(\mathbf{x}) = L_1(\mathbf{x_{L+K+R}})R_{k1}(\mathbf{x_{L+K}}) + \cdots + L_r(\mathbf{x_{L+K+R}})R_{kr}(\mathbf{x_{L+K}}) + \Phi_k(\mathbf{x_L}), \end{cases}$$

$$\begin{cases} \mathcal{F}^{(k+1)}(\mathbf{x}) = L_1(\mathbf{x_{L+K+R}})R'_{11}(\mathbf{x}) + \cdots + L_r(\mathbf{x_{L+K+R}})R'_{1r}(\mathbf{x}) + \Psi_1(\mathbf{x_{L+K}}) + L'_1(\mathbf{x_{L+K+R}}), \\ \qquad\vdots \\ \mathcal{F}^{(k+u)}(\mathbf{x}) = L_1(\mathbf{x_{L+K+R}})R'_{u1}(\mathbf{x}) + \cdots + L_r(\mathbf{x_{L+K+R}})R'_{ul}(\mathbf{x}) + \Psi_u(\mathbf{x_{L+K}}) + L'_u(\mathbf{x_{L+K+R}}), \end{cases}$$

where $\mathbf{x_L} = (x_1, \cdots, x_l)$, $\mathbf{x_{L+K}} = (x_1, \cdots, x_{l+k})$, $\mathbf{x_{L+K+R}} = (x_1, \cdots, x_{l+k+r})$, $\mathbf{x} = (x_1, \cdots, x_n)$, $m = k + u$ and $n = l + r + m$. We call $\mathcal{F}^{(i)}$ for $i = 1, \cdots, k$ and $\mathcal{F}^{(i)}$ for $i = k+1, \cdots, k+u$ polynomials in the first layer and the second layer, respectively.

How to Define L_i, R_{ij} and R'_{ij}.

– To define L_i, it needs to construct a hidden layer $\mathcal{L}$ of quadratic equations. L_i is a linear equation in variables $(x_1, \cdots, x_{l+k+r})$ for $i = 1, \cdots, r$. We define a system of r quadratic equations as

$$\mathcal{L}: \begin{cases} L(\mathbf{x_L})L_1(\mathbf{x_{L+K+R}}) = \xi_1, \\ \qquad\vdots \\ L(\mathbf{x_L})L_r(\mathbf{x_{L+K+R}}) = \xi_r, \end{cases}$$

where L is a linear equation in variables $(x_1, \cdots, x_l)$ and $\xi_i \in \mathbb{F}_q^*$. We choose random β_{ij} for $i = 1, \cdots, r$ and $j = 1, \cdots, l+k+r$ such that an $r \times r$

submatrix matrix $\Lambda_r = \begin{pmatrix} \beta_{1l+k+1} \cdots\cdots \beta_{1l+k+r} \\ \cdots \quad \cdots\cdots \quad \cdots \\ \beta_{rl+k+1} \cdots\cdots \beta_{rl+k+r} \end{pmatrix}$ of an $r \times (l+k+r)$ matrix Λ is invertible, where

$$\Lambda = \begin{pmatrix} \beta_{11} \cdots\cdots \beta_{1l+k+r} \\ \beta_{21} \cdots\cdots \beta_{2l+k+r} \\ \cdots \cdots\cdots \quad \cdots \\ \beta_{r1} \cdots\cdots \beta_{rl+k+r} \end{pmatrix}$$

is a coefficient matrix of $(L_1, \cdots, L_r)$.

- Φ_i is a quadratic equation in variables $(x_1, \cdots, x_l)$ for $i = 1, \cdots, k$ defined by $\Phi_i = \sum_{j=1}^{l} \sum_{t=j}^{l} \varphi_{j,t}^{i} x_j x_t$, for $\varphi_{j,t}^{i} \in_R \mathbb{F}_q$.
- R_{ij} is a linear equation in variables $(x_1, \cdots, x_{l+k})$ for $i = 1, \cdots, k$ and $j = 1, \cdots, r$ such that a $k \times k$ submatrix matrix $\Theta_k = \begin{pmatrix} \alpha_{1l+1} \cdots\cdots \alpha_{1l+k} \\ \cdots \quad \cdots\cdots \quad \cdots \\ \alpha_{kl+1} \cdots\cdots \alpha_{kl+k} \end{pmatrix}$ of a $k \times (l+k)$ matrix Θ is invertible, where Θ is a coefficient matrix of $(L(\mathbf{x_L}) \cdot \mathcal{F}^{(1)} - L(\mathbf{x_L}) \cdot \Phi_1(\mathbf{x_L}), \cdots, L(\mathbf{x_L}) \cdot \mathcal{F}^{(k)} - L(\mathbf{x_L}) \cdot \Phi_k(\mathbf{x_L}))$ such that

$$\begin{pmatrix} L(\mathbf{x_L}) \cdot \mathcal{F}^{(1)} - L(\mathbf{x_L}) \cdot \Phi_1(\mathbf{x_L}) \\ L(\mathbf{x_L}) \cdot \mathcal{F}^{(2)} - L(\mathbf{x_L}) \cdot \Phi_2(\mathbf{x_L}) \\ \cdots \\ L(\mathbf{x_L}) \cdot \mathcal{F}^{(k)} - L(\mathbf{x_L}) \cdot \Phi_k(\mathbf{x_L}) \end{pmatrix} = \begin{pmatrix} \xi_1 R_{11}(\mathbf{x}) + \cdots + \xi_r R_{1r}(\mathbf{x_{L+K}}) \\ \xi_1 R_{21}(\mathbf{x}) + \cdots + \xi_r R_{2r}(\mathbf{x_{L+K}}) \\ \cdots \\ \xi_1 R_{k1}(\mathbf{x}) + \cdots + \xi_r R_{kr}(\mathbf{x_{L+K}}) \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{11} \cdots\cdots \alpha_{1l+k} \\ \alpha_{21} \cdots\cdots \alpha_{2l+k} \\ \cdots \cdots\cdots \quad \cdots \\ \alpha_{k1} \cdots\cdots \alpha_{kl+k} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_{l+k} \end{pmatrix}.$$

- Ψ_i is a sparse polynomial in variables $(x_1, \cdots, x_{l+k})$ for $i = k+1, \cdots, k+u$ defined by

$$\Psi_i = \sum_{j=1}^{l+k} \psi_{i,j} x_j x_{(i+j-1)(\mathrm{mod}\ l+k)+1}$$

where $\psi_{i,j} \in_R \mathbb{F}_q$ so that the symmetric matrix of the quadratic part of each Ψ_i has rank $l+k$ and any crossterms in Ψ_i for all $i = k+1, \cdots, k+u$ don't overlap.

- L_i' is a linear equation in variables $(x_1, \cdots, x_{l+k+r})$ for $i = 1, \cdots, u$ defined by $L_i' = \sum_{j=1}^{l+k+r} \nu_j^i x_j$, where $\nu_j^i \in_R \mathbb{F}_q$.
- R_{ij}' is a linear equation in variables $(x_{l+k+r+1}, \cdots, x_n)$ for $i = 1, \cdots, u$ and $j = 1, \cdots, r$. We choose R_{ij}' such that a $u \times u$ submatrix $\Delta_u = \begin{pmatrix} \delta_{1l+k+r+1} \cdots \delta_{1n} \\ \cdots \quad \cdots \cdots \\ \delta_{ul+k+r+1} \cdots \delta_{un} \end{pmatrix}$ of a $u \times n$ matrix $\Delta = \begin{pmatrix} \delta_{11} \cdots \delta_{1n} \\ \cdots \cdots \cdots \\ \delta_{u1} \cdots \delta_{un} \end{pmatrix}$ is invertible, where Δ is a coefficient matrix of $(L(\mathbf{x_L}) \cdot \mathcal{F}^{(k+1)} - L(\mathbf{x_L}) \cdot \Psi_1(\mathbf{x_{L+K}}) - L(\mathbf{x_L}) \cdot$

$L'_1(\mathbf{x_{L+K+R}}), \cdots, L(\mathbf{x_L}) \cdot \mathcal{F}^{(k+u)} - L(\mathbf{x_L}) \cdot \Psi_u(\mathbf{x_{L+K}}) - L(\mathbf{x_L}) \cdot L'_u(\mathbf{x_{L+K+R}}))$ such that

$$\begin{pmatrix} L(\mathbf{x_L}) \cdot \mathcal{F}^{(k+1)} - L(\mathbf{x_L}) \cdot \Psi_1(\mathbf{x_{L+K}}) - L(\mathbf{x_L}) \cdot L'_1(\mathbf{x_{L+K+R}}) \\ L(\mathbf{x_L}) \cdot \mathcal{F}^{(k+2)} - L(\mathbf{x_L}) \cdot \Psi_2(\mathbf{x_{L+K}}) - L(\mathbf{x_L}) \cdot L'_2(\mathbf{x_{L+K+R}}) \\ \cdots \\ L(\mathbf{x_L}) \cdot \mathcal{F}^{(k+u)} - L(\mathbf{x_L}) \cdot \Psi_u(\mathbf{x_{L+K}}) - L(\mathbf{x_L}) \cdot L'_u(\mathbf{x_{L+K+R}}) \end{pmatrix}$$

$$= \begin{pmatrix} \xi_1 R'_{11}(\mathbf{x}) + \cdots + \xi_r R'_{1r}(\mathbf{x}) \\ \xi_1 R'_{21}(\mathbf{x}) + \cdots + \xi_r R'_{2r}(\mathbf{x}) \\ \cdots \\ \xi_1 R'_{u1}(\mathbf{x}) + \cdots + \xi_r R'_{ur}(\mathbf{x}) \end{pmatrix} = \begin{pmatrix} \delta_{11} \cdots \delta_{1n} \\ \cdots \cdots \cdots \\ \delta_{u1} \cdots \delta_{un} \end{pmatrix} \cdot \begin{pmatrix} x_{l+k+r+1} \\ \cdots \\ x_n \end{pmatrix}.$$

– From this construction, we store only $(\mathbf{L}, \mathbf{L}', \Phi, \Psi^S, {\Theta_k}^{-1}, {\Lambda_r}^{-1}, {\Delta_u}^{-1})$ for $\mathcal{F}$ instead of all the coefficients of $\mathcal{F}$, where $\mathbf{L} = \{L, \xi_i\}_{i=1}^{r}$, $\mathbf{L}' = \{L'_i\}_{i=1}^{l+k+r}$, $\Phi = \{\Phi_i\}_{i=1}^{k}$ and $\Psi^S = \{\Psi_i\}_{i=1}^{u}$.

How to Invert the Central Map. Given $\gamma = (\gamma_1, \cdots, \gamma_m)$, to compute $\mathcal{F}^{-1}(\gamma) = \mathbf{s}$, i.e., to find $\mathbf{s}$ such that $\mathcal{F}(\mathbf{x}) = \gamma$, do the followings:

– In the first layer, compute $L(\mathbf{x_L}) \cdot \mathcal{F}^{(i)} = L(\mathbf{x_L}) \cdot \gamma_i$ for $i = 1, \cdots, k$ by getting a linear system of k equations with $l + k$ variables as

$$\begin{cases} \xi_1 R_{11}(\mathbf{x_{L+K}}) + \cdots + \xi_l R_{1r}(\mathbf{x_{L+K}}) = \gamma_1 \cdot L(\mathbf{x_L}) - \Phi_1(\mathbf{x_L}) \cdot L(\mathbf{x_L}), \\ \vdots \\ \xi_1 R_{k1}(\mathbf{x_{L+K}}) + \cdots + \xi_r R_{kr}(\mathbf{x_{L+K}}) = \gamma_k \cdot L(\mathbf{x_L}) - \Phi_k(\mathbf{x_L}) \cdot L(\mathbf{x_L}). \end{cases}$$

- Choose a random Vinegar vector $\mathbf{s_L} = (s_1, \cdots, s_l) \in \mathbb{F}_q^l$. If $L(\mathbf{s}_L) = 0$ then choose another random Vinegar vector. Plug $\mathbf{s_L}$ into the above linear system by getting a new linear system of k equations with k variables.
- Solve the linear system by computing

$$\begin{pmatrix} s_{l+1} \\ s_{l+2} \\ \cdots \\ s_{l+k} \end{pmatrix} = \Theta_k^{-1} \cdot \begin{pmatrix} \gamma_1 \cdot L(\mathbf{s_L}) - \Phi_1(\mathbf{s_L}) \cdot L(\mathbf{s_L}) - c_1 \\ \gamma_2 \cdot L(\mathbf{s_L}) - \Phi_2(\mathbf{s_L}) \cdot L(\mathbf{s_L}) - c_2 \\ \cdots \\ \gamma_k \cdot L(\mathbf{s_L}) - \Phi_k(\mathbf{s_L}) \cdot L(\mathbf{s_L}) - c_k \end{pmatrix},$$

  where c_j is a constant derived from the linear equation $\xi_1 R_{j1}(\mathbf{x_{L+K}}) + \cdots + \xi_l R_{jr}(\mathbf{x_{L+K}})$ for $j = 1, \cdots, k$.

– In the hidden layer, plug $\mathbf{s_{L+K}} = (s_1, \ldots, s_{l+k})$ into a quadratic system $\mathcal{L}$ by getting a linear system of r equations with r variables as

$$\begin{cases} L_1(\mathbf{s_{L+K}}, x_{l+k+1}, \cdots, x_{l+k+r}) = L(\mathbf{s}_L)^{-1} \cdot \xi_1, \\ \vdots \\ L_r(\mathbf{s_{L+K}}, x_{l+k+1}, \cdots, x_{l+k+r}) = L(\mathbf{s}_L)^{-1} \cdot \xi_k, \end{cases}$$

where $L(\mathbf{s}_L) \neq 0$. Get a solution $(s_{l+k+1}, \cdots, s_{l+k+r})$ by computing

$$\begin{pmatrix} s_{l+k+1} \\ s_{l+k+2} \\ \cdots \\ s_{l+k+k} \end{pmatrix} = \Lambda_k^{-1} \cdot \begin{pmatrix} L(\mathbf{s}_L)^{-1} \cdot \xi_1 \\ L(\mathbf{s}_L)^{-1} \cdot \xi_2 \\ \cdots \\ L(\mathbf{s}_L)^{-1} \cdot \xi_k \end{pmatrix}.$$

– In the second layer, compute $L(\mathbf{x_L}) \cdot \mathcal{F}^{(i)} = L(\mathbf{x_L}) \cdot \gamma_i$ for $i = k+1, \cdots, k+u$ getting a linear system of u equations with $l+k+r+u$ variables as

$$\begin{cases} \xi_1 R'_{11}(\mathbf{x}) + \cdots + \xi_l R'_{1r}(\mathbf{x}) = \gamma_{k+1} \cdot L(\mathbf{x}_L) - \Psi_1(\mathbf{x}_L) \cdot L(\mathbf{x}_L) - L'_1(\mathbf{x_{L+K+R}}) \cdot L(\mathbf{x}_L), \\ \xi_1 R'_{21}(\mathbf{x}) + \cdots + \xi_l R'_{2r}(\mathbf{x}) = \gamma_{k+2} \cdot L(\mathbf{x}_L) - \Psi_2(\mathbf{x}_L) \cdot L(\mathbf{x}_L) - L'_2(\mathbf{x_{L+K+R}}) \cdot L(\mathbf{x}_L), \\ \qquad\qquad \cdots \\ \xi_1 R'_{u1}(\mathbf{x}) + \cdots + \xi_l R'_{ur}(\mathbf{x}) = \gamma_{k+u} \cdot L(\mathbf{x}_L) - \Psi_u(\mathbf{x}_L) \cdot L(\mathbf{x}_L) - L'_u(\mathbf{x_{L+K+R}}) \cdot L(\mathbf{x}_L), \end{cases}$$

and plug $\mathbf{s_{L+K+R}} = (s_1, \cdots, s_{l+k+r})$ into the linear system getting a linear system of u equations with u variables. Get a solution $(s_{l+k+r+1}, \cdots, s_{l+k+r+u})$ by computing

$$\begin{pmatrix} s_{l+k+r+1} \\ s_{l+k+r+2} \\ \cdots \\ s_{l+k+r+u} \end{pmatrix} = \Delta_u^{-1} \cdot \begin{pmatrix} \gamma_{k+1} \cdot L(\mathbf{s}_L) - \Psi_1(\mathbf{s}_L) \cdot L(\mathbf{s}_L) - c'_1 \\ \gamma_{k+2} \cdot L(\mathbf{s}_L) - \Psi_2(\mathbf{s}_L) \cdot L(\mathbf{s}_L) - c'_2 \\ \cdots \\ \gamma_{k+u} \cdot L(\mathbf{s}_L) - \Psi_u(\mathbf{s}_L) \cdot L(\mathbf{s}_L) - c'_u \end{pmatrix},$$

where c'_i is a constant of the linear equation $\xi_1 R'_{i1}(\mathbf{s_{L+K}}, \mathbf{x}_R) + \cdots + \xi_r R'_{ir}(\mathbf{s_{L+K}}, \mathbf{x}_R)$ for $i = 1, \cdots, u$.

– Finally, we get a solution $(s_1, \cdots, s_n)$ of $\mathcal{F}(\mathbf{x}) = \gamma$ by performing only three matrix multiplications and computation of quadratic terms without using the Gaussian elimination.

Now, we construct a new MQ-signature scheme based on this central map.

■ **ELSA** (**E**fficient **L**ayered **S**igna**t**ure Scheme).

- **KeyGen**(1^λ). For a security parameter λ, generate a public/secret key pair $<PK, SK> = <\mathcal{P}, (\widetilde{S}, \widetilde{T}, \mathcal{F} = (\mathbf{L}, \mathbf{L}', \Phi, \Psi^S, \widetilde{\Theta_r}, \widetilde{\Lambda_k}, \widetilde{\Delta_u}))>$ as
  - Choose randomly two affine maps $\widetilde{S}$ and $\widetilde{T}$. If neither $\widetilde{S}$ nor $\widetilde{T}$ is invertible then choose again, where $\widetilde{X} = X^{-1}$.
  - Choose randomly $\mathbf{L}, \Phi, \Psi^S, \widetilde{\Theta_r}, \widetilde{\Lambda_r}$ and $\widetilde{\Delta_u}$, where $\mathbf{L} = \{L, \xi_i\}_{i=1}^r$, $\mathbf{L}' = \{L'_i\}_{i=1}^u$, $\Phi = \{\Phi_i\}_{i=1}^k$ and $\Psi^S = \{\Psi_i\}_{i=1}^u$ satisfy all the conditions described above. If neither $\widetilde{\Theta_r}$, $\widetilde{\Lambda_k}$ nor $\widetilde{\Delta_u}$ is invertible then choose again. Compute $\mathcal{P}$ from $\mathcal{P} = S \circ \mathcal{F} \circ T$.
- **Sign**$(SK, \mathtt{m})$. Given a message $\mathtt{m}$,
  - Compute $h(\mathtt{m})$ and $\widetilde{S}(h(\mathtt{m})) = \gamma$, where $\gamma = (\gamma_1, \cdots, \gamma_m)$.
  - Compute $\mathbf{s}$ such that $\mathcal{F}^{-1}(\gamma) = \mathbf{s}$, i.e., $\mathcal{F}(\mathbf{s}) = \gamma$ as the above. Then $\mathbf{s} = (s_1, \cdots, s_n)$ is a solution of $F(\mathbf{x}) = \gamma$.
  - Compute $\widetilde{T}(\mathbf{s}) = \sigma$. Then σ is a signature of $\mathtt{m}$.

- **Verify**$(PK, \mathtt{m}, \sigma)$. Given a signature σ on $\mathtt{m}$ and a public key $\mathcal{P}$, check $\mathcal{P}(\sigma) = h(\mathtt{m})$. If it holds, accept σ, otherwise, reject it.

Remark 1. We now explain how the public key and secret key sizes of ELSA are calculated. The public key requires $\frac{m(n+1)(n+2)}{2}$ field elements as their coefficients. The secret maps S and T require $m(m+1)$ and $n(n+1)$ field elements, respectively. It requires $(l+r+l+1)$ field elements for $\mathbf{L}$, $u(l+k+r+1)$ field elements for $\mathbf{L}'$, $\frac{k(l+1)(l+2)}{2}$ field elements for Φ, $u(l+k)$ field elements for Ψ^S, k^2 field elements for $\widetilde{\Theta_k}$, r^2 field elements for $\widetilde{\Lambda_k}$ and u^2 field elements for $\widetilde{\Delta_u}$. Thus, the secret key requires $n(n+1) + m(m+1) + \frac{k(l+1)(l+2)}{2} + u(2l+2k+r+1) + (k^2+r^2+u^2) + (l+r+1)$ field elements.

2. UOV and Rainbow requires the use of Gaussian elimination for solving linear systems in signing. In these schemes, the majority of computational cost for signing count for that of the Gaussian elimination. In ELSA, only three matrix multiplications using ${\Theta_r}^{-1}, {\Lambda_k}^{-1}, {\Delta_u}^{-1}$ are required for solving the resulting linear systems in signing without using the Gaussian elimination. So, it achieves $\mathcal{O}(n^2)$ complexity in signing instead of $\mathcal{O}(n^3)$.

3 Security Analysis of ELSA

The security of all MQ-schemes in the MQ + IP paradigm is not only based on the MQ-Problem, but also on some variant of the Isomorphism of Polynomials (IP) problem. Furthermore, layered MQ-schemes require the hardness of the MinRank problem. These underlying problems are defined as follows:

- **Polynomial System Solving (PoSSo) Problem:** Given a system $\mathcal{P} = (\mathcal{P}^{(1)}, \cdots, \mathcal{P}^{(m)})$ of m nonlinear polynomials defined over $\mathbb{F}_q$ with degree of d in variables $(x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_m) \in \mathbb{F}_q^m$, find $\mathbf{x}' = (x'_1, \cdots, x'_n) \in \mathbb{F}_q^n$ such that $\mathcal{P}(\mathbf{x}') = \mathbf{y}$, i.e., $\mathcal{P}^{(1)}(x'_1, \cdots, x'_n) = y_1, \cdots, \mathcal{P}^{(m)}(x'_1, \cdots, x'_n) = y_m$.
- **EIP (Extended Isomorphism of Polynomials) Problem:** Given a nonlinear multivariate system $\mathcal{P}$ such that $\mathcal{P} = S \circ \mathcal{F} \circ T$ for linear or affine maps S and T, and $\mathcal{F}$ belonging to a special class of nonlinear polynomial system $\mathcal{C}$, find a decomposition of $\mathcal{P}$ such that $\mathcal{P} = S' \circ \mathcal{F}' \circ T'$ for linear or affine maps S' and T', and $\mathcal{F}' \in \mathcal{C}$.
- **MinRank Problem:** Let $m, n, r, k \in \mathbb{N}$ and $r, m < n$. The MinRank(r) problem is, given $(M_1, \cdots, M_l) \in \mathbb{F}_q^{m \times n}$, find a non-zero k-tuple $(\lambda_1, \cdots, \lambda_k) \in \mathbb{F}_q^k$ such that $Rank(\sum_{i=1}^{k} \lambda_i M_i) \leq r$.

The PoSSo problem is proven to be NP-complete [26]. For efficiency, MQ-PKC restrict to quadratic polynomials. The PoSSo problem with all polynomials $(P^{(1)}, \cdots, P^{(m)})$ of degree 2 is called the MQ-Problem for multivariate quadratic. The IP problem was first described by Patarin at Eurocrypt'96 [40], there is not

much known about the difficulty of the IP problem in contrast to the MQ-problem. The problem of finding a low rank linear combination of matrices was originally introduced in [48] as one of the natural questions in linear algebra, and the authors proved its NP-completeness.

A feature of MQ-PKC in the MQ + IP paradigm is that there exist a large number of different secret keys for a given public key [51]. Informally, suppose that $<\mathcal{P}, (S, \mathcal{F}, T)>$ is a public/secret key pair of an MQ-PKC, we call $(S', \mathcal{F}', T')$ is an equivalent key of $(S, \mathcal{F}, T)$ if $\mathcal{P} = S \circ \mathcal{F} \circ T = S' \circ \mathcal{F}' \circ T'$, where S' and T' are invertible affine maps, and $\mathcal{F}'$ preserves all zero coefficients of $\mathcal{F}$. The concept of equivalent keys plays a major role in the cryptanalysis of MQ-schemes. If an attacker finds any of the equivalent keys then he can forge a signature. Thus, the attacker wants to find an equivalent key with the simplest structure. Known attacks of MQ-schemes be divided into the following two classes:

- **Direct Attack.** Given a public key $\mathcal{P}$ and $\mathbf{y} \in \mathbb{F}_q^m$, find a solution $\mathbf{x} \in \mathbb{F}_q^n$ of $\mathcal{P}(\mathbf{x}) = \mathbf{y}$.
- **Key Recovery Attack (KRA).** Given $\mathcal{P} = S \circ \mathcal{F} \circ T$, find equivalent keys of $(S, \mathcal{F}, T)$:
  - KRAs using equivalent keys and good keys,
  - Rank-based KRAs to find linear combinations associated matrices at some given rank, to find nontrivial invariant subspaces of linear combinations associated matrices and so on: MinRank attack, HighRank attack, Kipnis-Shamir attack.

3.1 Direct Attacks

Direct attacks use equation solvers like XL and Gröbner basis algorithms such as Buchberger, F4 and F5 for solving the MQ-problem. Complexity of the MQ-Problem is determined by that of the HybridF5 (HF5) algorithm [7]. The basic idea is to guess some of the variables to create overdetermined systems before applying Faugère's F5 algorithm [22]. When doing so, one has to run the F5 algorithm several times to find a solution of the original system. When guessing k variables over $\mathbb{F}_q$, this number is given by q^k. The complexity of solving a semi-regular (random) system of m quadratic equations in n variables over $\mathbb{F}_q$ by HF5 can be estimated as

$$C_{HF5}(q, m, n) = min_{k \geq 0}\ q^k \cdot \mathcal{O}\left(\left(m \cdot \binom{n-k+d_{reg}-1}{d_{reg}}\right)^{\omega}\right),$$

where the degree of regularity d_{reg} is the index of the first non-positive coefficient in the $S_{m,n} = \dfrac{(1-z^2)^m}{(1-z)^n}$ and $2 \leq \omega \leq 3$ is the linear algebra constant of solving a linear system. The internal equations used by HF5 are very sparse and thus $\omega = 2$ can be used to obtain a lower bound on the complexity. If we really want to break a scheme, we either calculate the correct α or use $\omega = 2.8$ as an upper bound [50].

Using HF5 algorithm ($\omega = 2$), we summarize the lower bounds of the numbers of equations (m) for solving determined systems defined over $\mathbb{F}_{2^8}$ required to achieve given security levels in Table 1.

Table 1. Lower bounds of the numbers of quadratic equations for determined systems over $\mathbb{F}_{2^8}$ at each security level.

λ	80	96	128	192	256
m	26	31	43	68	93

3.2 Replacement Attacks

Our central map has a special feature for inverting: each central polynomial uses a linear combination of the products of two lines and additional quadratic terms. This feature and hidden quadratic systems make it possible to remove the use of the Gaussian elimination resulting in the reduction of signing cost and secret key size. In particular, L_i for $i = 1, \cdots, r$ are used in all the central polynomials $\mathcal{F}^{(i)}$ for $i = 1, \cdots, k+u$. Thus, one can replace L_i with a new variable via an appropriate changing of variables. More precisely, one can replace $L_i(\mathbf{x_{L+K+R}})$ with y_{l+k+i} for $i = 1, \cdots, r$ and x_j with y_j for $j = 1, \cdots, l+k, l+k+r+1, \cdots, l+k+r+u$. Then one gets a new central map, $\overline{\mathcal{F}} = (\overline{\mathcal{F}}^{(1)}, \cdots, \overline{\mathcal{F}}^{(m)})$ in the new variables $(y_1, \cdots, y_n)$ as

$$\begin{cases} \widehat{\mathcal{F}}^{(1)}(\mathbf{y}) = y_{l+k+1}R_{11}(\mathbf{y_{L+K}}) + \cdots + y_{l+k+r}R_{1r}(\mathbf{y_{L+K}}) + \Phi_1(\mathbf{y_L}), \\ \qquad\vdots \\ \widehat{\mathcal{F}}^{(k)}(\mathbf{y}) = y_{l+k+1}R_{k1}(\mathbf{y_{L+K}}) + \cdots + y_{l+k+r}R_{kr}(\mathbf{y_{L+K}}) + \Phi_k(\mathbf{y_L}), \end{cases}$$

$$\begin{cases} \widehat{\mathcal{F}}^{(k+1)}(\mathbf{y}) = y_{l+k+1}R'_{11}(\mathbf{y}) + \cdots + y_{l+k+r}R'_{1r}(\mathbf{y}) + \Psi_1(\mathbf{y_{L+K}}) + \overline{L_1}(\mathbf{y_{L+K+R}}), \\ \qquad\vdots \\ \widehat{\mathcal{F}}^{(k+u)}(\mathbf{y}) = y_{l+k+1}R'_{u1}(\mathbf{y}) + \cdots + y_{l+k+r}R'_{ur}(\mathbf{y}) + \Psi_u(\mathbf{y_{L+K}}) + \overline{L_u}(\mathbf{y_{L+K+R}}), \end{cases}$$

where $\mathbf{y_L} = (y_1, \cdots, y_l)$, $\mathbf{y_{L+K}} = (y_1, \cdots, y_{l+k})$ and $\mathbf{y_{L+K+R}} = (y_1, \cdots, y_{l+k+r})$. Then the public key can be written as

$$\mathcal{P} = S \circ (\mathcal{F} \circ T_R) \circ (T_R^{-1} \circ T) = S \circ \overline{\mathcal{F}} \circ \overline{T},$$

where $\overline{\mathcal{F}} = \mathcal{F} \circ T_R$, $\overline{T} = T_R^{-1} \circ T$ and T_R is an invertible map defined by

$$T_R(\mathbf{x^T}) = \begin{pmatrix} I_{L+K} & 0 & 0 \\ 0 & L_1 & 0 \\ 0 & L_2 & 0 \\ \cdots & \cdots & \cdots \\ 0 & L_r & 0 \\ 0 & 0 & I_U \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \cdots \\ y_n \end{pmatrix},$$

where I_{L+K} and I_U are an $(l+k) \times (l+k)$-identity matrix and a $u \times u$-identity matrix, respectively. In this case, we can consider the public key $\mathcal{P} = S \circ \overline{\mathcal{F}} \circ \overline{T}$ with the secret key $(S, \overline{\mathcal{F}}, \overline{T})$ since $\overline{\mathcal{F}}$ is still invertible with the same way as in §2.1. We provide security analysis of ELSA against all attacks with respect to these two types of secret keys $(S, \mathcal{F}, T)$ and $(S, \overline{\mathcal{F}}, \overline{T})$ for the public key $\mathcal{P}$.

3.3 Key Recovery Attacks

In 2008, Ding *et al.* [17] presented Rainbow Band Separation (RBS) attacks on Rainbow. Later, Thomae [50] applied the attacks to other MQ-schemes using the concept of good keys which is a generalization of the RBS attacks. In this subsection, we analyze security of ELSA against the key recovery attacks (KRAs) using equivalent keys and good keys.

Let $F^{(i)}$ $(1 \leq i \leq m)$ be symmetric matrices associated to the homogeneous quadratic part of the i-th component of the central map $\mathcal{F}$. The matrices $F^{(i)}$ are depicted in Fig. 1, where white parts denote zero entries and gray parts denote arbitrary entries. The matrices are the same as those of Rainbow [44]. After mounting the replacement attack described in Sect. 3.2, we get symmetric matrices $\overline{F}^{(i)}$ $(1 \leq i \leq m)$ representing the quadratic part of the i-th component of $\overline{\mathcal{F}}^{(i)}$ which is depicted in Fig. 2.

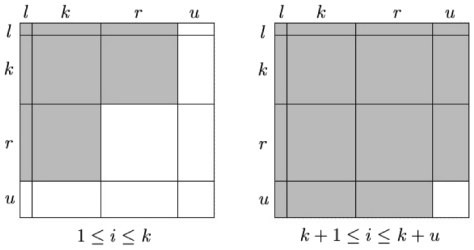

Fig. 1. Symmetric matrices for quadratic parts of $\mathcal{F}$.

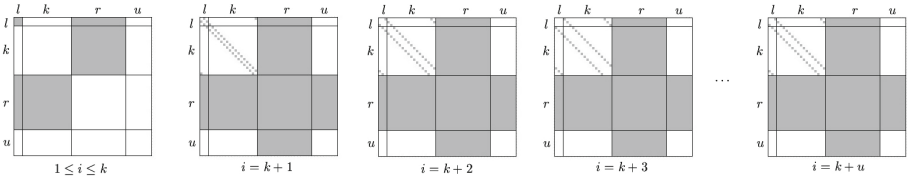

Fig. 2. Symmetric matrices for quadratic parts of $\overline{\mathcal{F}}$.

Analogously, we denote $P^{(i)}$ $(1 \leq i \leq m)$ be symmetric matrices representing the quadratic part of the i-th component of the public key $\mathcal{P}$. Due to the structure

of $\mathcal{F}$, we know that certain coefficients in $\mathcal{F}^{(i)}$ are systematically zero. Since $\mathcal{P} = S \circ \mathcal{F} \circ T$, we obtain $\mathcal{F} = \widetilde{S} \circ \mathcal{P} \circ \widetilde{T}$, where $\widetilde{S} = S^{-1}$ and $\widetilde{T} = T^{-1}$. From this, we get the following equality:

$$\mathcal{F}^{(i)} = \widetilde{T}^{\mathsf{T}} \left(\sum_{j=1}^{m} \widetilde{s}_{ij} P^{(j)} \right) \widetilde{T}, \ \forall 1 \leq i \leq m.$$

The corresponding system of equations is:

$$f_{\beta\gamma}^{(i)} = \sum_{x=1}^{m} \sum_{y=1}^{n} \sum_{z=1}^{n} c_{yz}^{(x)} \widetilde{s}_{ix} \widetilde{t}_{y\beta} \widetilde{t}_{z\gamma} \tag{1}$$

for some coefficient $c_{yz}^{(x)}$, as we have already known that $f_{\beta\gamma}^{(i)} = 0$ for some i, β, γ by the construction of $\mathcal{F}$. Since the number equations obtained by (1) equals the number of zeros in all $\mathcal{F}^{(k)}$, we get $\frac{kr(r+1) + mu(u+1)}{2} + ku(n-u)$ cubic equations. The number of variables in $\widetilde{S}$ and $\widetilde{T}$ is $n^2 + m^2$. The number of equations for $\overline{\mathcal{F}}$ is

$$\frac{k(n-l)(n+l+1) + u(n-r)(n+r+1)}{2} - r[(l+k)k + (n-r)u] - u(l+k).$$

The complexity of solving such systems using HF5 is very large. To improve this complexity, we use the concept of equivalent keys [50,51]. Let $\mathbb{GL}_n(\mathbb{F}_q)$ be a general linear group of degree n over $\mathbb{F}_q$, for an integer n.

Definition 3.1 [Equivalent Key]. Let $S, S' \in \mathbb{GL}_m(\mathbb{F}_q)$ and $T, T' \in \mathbb{GL}_n(\mathbb{F}_q)$ and $\mathcal{F}, \mathcal{F}' \in \mathbb{F}_q[x_1, ..., x_n]^m$. We say that $(\mathcal{F}, S, T)$ is *equivalent* to $(\mathcal{F}', S', T')$ if and only if $S \circ \mathcal{F} \circ T = S' \circ \mathcal{F}' \circ T'$ and $\mathcal{F}|_I = \mathcal{F}'|_I$, that is, $\mathcal{F}$ and $\mathcal{F}'$ share the same structure when restricted to a fixed index set $I = \{I^{(1)}, \cdots I^{(m)}\}$.

If $S \circ \mathcal{F} \circ T = \mathcal{P} = S' \circ \mathcal{F}' \circ T'$, where $\mathcal{F}'$ preserves all systematic zero coefficients of $\mathcal{F}$ then we call S' and T' equivalent keys. Thus, an attacker who has any of equivalent keys can forge signatures on any messages. If we can find simpler equivalent keys, we can reduce the number of variables in S and T. If there are two invertible linear maps $\Sigma \in \mathbb{GL}_m(\mathbb{F}_q)$ and $\Omega \in \mathbb{GL}_n(\mathbb{F}_q)$ such that

$$\mathcal{P} = S \circ \Sigma^{-1} \circ (\Sigma \circ \mathcal{F} \circ \Omega) \circ \Omega^{-1} \circ T,$$

and $\mathcal{F}' (= \Sigma \circ \mathcal{F} \circ \Omega)$ and $\mathcal{F}$ have the same structure then $(\mathcal{F}', S', T')$ is an equivalent key.

For the original central map $\mathcal{F}$, its equivalent keys are the same as those of Rainbow since the matrices $(F^{(1)}, \cdots, F^{(m)})$ are the same as those of Rainbow [50]. Thus, the equivalent keys for $\mathcal{F}$ are of the form given in Fig. 3, in this case, $\mathcal{F}'^{(i)}$ also have same form as $\mathcal{F}'^{(i)}$ given in Fig. 1.

Next, we find equivalent keys for the central map $\overline{\mathcal{F}}$. To preserve the structure in second layer, we can find Ω and Σ of the form given in Fig. 4, so we

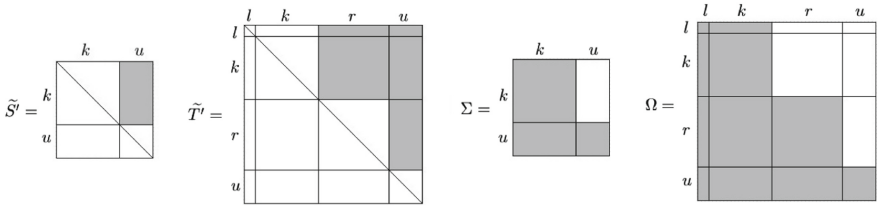

Fig. 3. Equivalent keys of ELSA w.r.t. $\mathcal{F}$.

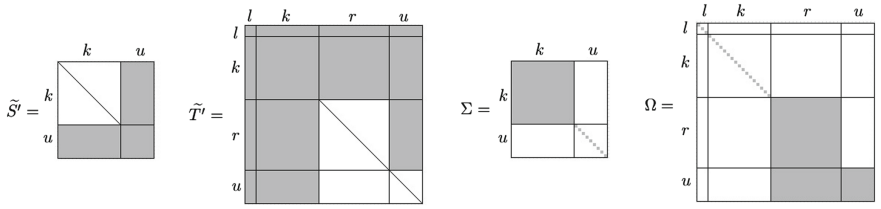

Fig. 4. Equivalent keys of ELSA w.r.t. $\overline{\mathcal{F}}$.

get equivalent keys of the form given in Fig. 4. However, we can find simpler equivalent keys than ones given in Fig. 4 to improve the complexity significantly by changing the preservation set, i.e., the set of indices for the quadratic terms with zero coefficients. For it, we consider the generalized version of $\overline{\mathcal{F}}$ denoted by $\widehat{\mathcal{F}}$ which is depicted in Fig. 5. So, we need to find equivalent keys $(\widehat{\mathcal{F}}', S', T')$ such that $\widehat{\mathcal{F}'}^{(i)}$ preserves the generalized version $\widehat{\mathcal{F}}^{(i)}$.

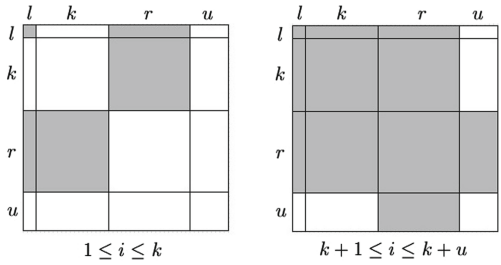

Fig. 5. $\widehat{\mathcal{F}}$: Generalized version of $\overline{\mathcal{F}}$.

Lemma 3.1. For the generalized central map $\widehat{\mathcal{F}}$ given in Fig. 5, we can find equivalent keys S' and T' of the form given in Fig. 6 with high probability, where gray parts denote arbitrary entries and white parts denote zero entries and there are ones at the diagonal.

Proof. As in [50], we can find Σ and Ω given in Fig. 6. With high probability, there exist equivalent keys (S', T') of the form given in Fig. 6. □

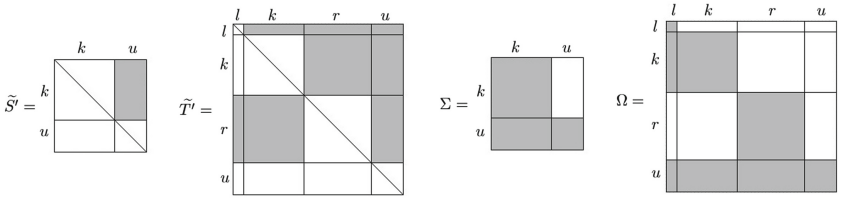

Fig. 6. Equivalent keys of ELSA w.r.t. $\widehat{\mathcal{F}}$.

After applying the transformations Σ and Ω in Lemma 3.1., we also get the central map $\widehat{\mathcal{F}'} = \Sigma \circ \widehat{\mathcal{F}} \circ \Omega$ as in Fig. 5. From the equivalent key given in Fig. 6, we get a system of $\dfrac{k(n-l)(n+l+1)}{2} - kr(l+k)$ cubic equations and $\dfrac{u^2(2l+2k+u+1)}{2}$ quadratic equations with $n(n-u)+k(u-k-r)-l^2-r^2$ variables. However, the complexity of solving such a system is still large: for ELSA with $(\mathbb{F}_q, l, k, r, u) = (\mathbb{F}_{2^8}, 6, 28, 30, 15)$, lower bound on the complexity of solving the system by HF5 is 2^{1696}. To further decrease this complexity, we use the notion of good keys which is a generalization of equivalent keys. Good keys don't preserve all the zero coefficients of $\mathcal{F}$, but just some of them. Hence, we can choose Σ and Ω more widely and further reduce the number of variables.

Definition 3.2 [Good Key]. Let $S, S'' \in \mathbb{GL}_n(\mathbb{F}_q)$ and $T, T'' \in \mathbb{GL}_m(\mathbb{F}_q)$ and $\mathcal{F}, \mathcal{F}'' \in \mathbb{F}_q[x_1, ..., x_n]^m$, and $J = \{J^{(1)}, \cdots, J^{(m)}\} \subset I = \{I^{(1)}, \cdots, I^{(m)}\}$ for all k with at least one $J^{(k)} \neq \phi$. We say that $(\mathcal{F}'', S'', T'')$ is a *good key* for $(\mathcal{F}, S, T)$ if and only if $S \circ \mathcal{F} \circ T = S'' \circ \mathcal{F}'' \circ T''$ and $\mathcal{F}|_J = \mathcal{F}''|_J$.

To find good keys, let $(\mathcal{F}', S', T')$ be an equivalent key for ELSA. If

$$\mathcal{P} = S' \circ \mathcal{F}' \circ T' = (S' \circ \Sigma'^{-1}) \circ (\Sigma' \circ \mathcal{F}' \circ \Omega') \circ (\Omega'^{-1} \circ T')$$

for some two linear maps $\Sigma' \in \mathbb{GL}_m(\mathbb{F}_q)$ and $\Omega' \in \mathbb{GL}_n(\mathbb{F}_q)$, and $\mathcal{F}'' = \Sigma' \circ \mathcal{F}' \circ \Omega'$ satisfies the condition in above definition, then

$$(\mathcal{F}'',\ S'',\ T'') = (\Sigma' \circ \mathcal{F}' \circ \Omega',\ S' \circ \Sigma'^{-1},\ \Omega'^{-1} \circ T'),$$

S'' and T'' are good keys. The following proposition shows the existence of good keys for ELSA.

Lemma 3.2. Let $(S', \widehat{\mathcal{F}'}, T')$ be an equivalent key for ELSA given in Fig. 6. Then there are good keys $(S'', \widehat{\mathcal{F}''}, T'')$ of the form given in Fig. 7. Only the last column of $\widetilde{T''}$ contains arbitrary values in the first $l+k+r$ rows, which are equal to the corresponding values in $\widetilde{T'}$. Respectively, only u values of the k-th row of $\widetilde{S''}$ contain arbitrary values, which are equal to the corresponding values in $\widetilde{S'}$.

Proof. Using linear algebra, we can obtain unique Σ' and Ω' given in Fig. 7. It shows the existence of a good key (S'', T'') of the form given in Fig. 7. □

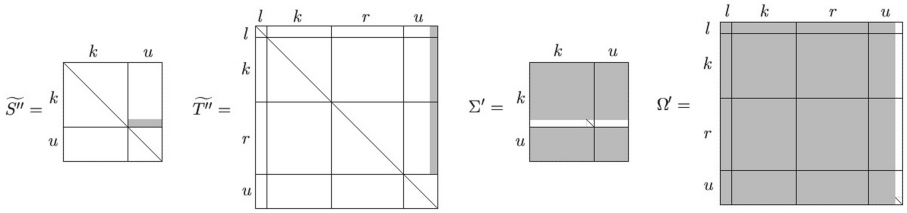

Fig. 7. Good keys of ELSA.

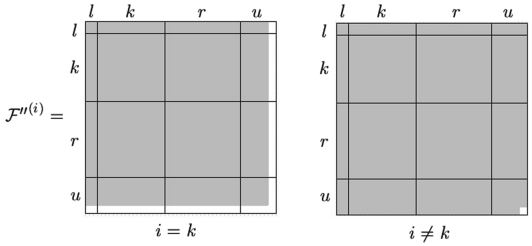

Fig. 8. Central map $\widehat{\mathcal{F}}''$ after applying Σ' and Ω' in Lemma 3.2.

Finally, after applying the transformations Σ' and Ω', we get the central map $\widehat{\mathcal{F}}'' = \Sigma' \circ \widehat{\mathcal{F}}' \circ \Omega'$ as given in Fig. 8. Finally, we obtain the following Theorem.

Theorem 3.1. The main complexity of the key recovery attack using good keys on ELSA is determined by solving $n - 1$ bihomogeneous equations and m quadratic equations with n variables.

After obtaining one column of T' and one row of S', all the other parts of T' and S' are revealed by linear equations as in [50]. Consequently, we recover the equivalent keys T' and S'.

We find different equivalent keys for three types of central maps $\mathcal{F}$, $\overline{\mathcal{F}}$ and $\widehat{\mathcal{F}}$, where $\mathcal{F}$, $\overline{\mathcal{F}}$ and $\widehat{\mathcal{F}}$ are the original central map, the resulting central map after the replacement attack and the general version of $\overline{\mathcal{F}}$, respectively. The KRAs using equivalent keys for $\widehat{\mathcal{F}}$ are more effective than those for $\mathcal{F}$ and $\overline{\mathcal{F}}$. However, $\mathcal{F}$, $\overline{\mathcal{F}}$ and $\widehat{\mathcal{F}}$ have the same forms of good keys resulting in the same complexities given in Theorem 3.1. Table 2 shows improvements of lower bound ($\alpha = 2$) and upper bound ($\alpha = 2.8$) on the complexities of solving such a system by HF5 achieved by the KRAs using equivalent keys and good keys for ELSA with $(\mathbb{F}_q, l, k, r, u) = (\mathbb{F}_{2^8}, 6, 28, 30, 15)$.

Key Recovery Attacks using Linear Part of the Central Map. It is also known that some coefficients of linear terms in the central map are zero. This does not significantly affect the KRAs since the number of quadratic terms with zero coefficients is much larger than that of linear terms with zero coefficients. When we reduce the number of variables in good key recovery, we use Ω' where

Table 2. Lower-bounds/upper-bounds on the complexities of the KRAs using equivalent keys and good keys for ELSA under different forms of central maps, $\mathcal{F}$, $\overline{\mathcal{F}}$ and $\widehat{\mathcal{F}}$ with $(F_{2^8}, 6, 28, 30, 15)$

ELSA	# of Equ.	# of Vari.	d_{reg}	Comp. (low./upp.)
KRA ($\mathcal{F}$)	45,060(Cubic)	8,090	1017	$2^{9215}/2^{12901}$
KRA ($\overline{\mathcal{F}}$)	77,197(Cubic)	8,090	727	$2^{7263}/2^{10169}$
KRA ($\widehat{\mathcal{F}}$)	68,782(Cubic)	8,090	779	$2^{7632}/2^{10686}$
KRA Equi. ($\mathcal{F}$)	28,980(Cubic) + 16,080(Quad.)	2,400	53	$2^{760}/2^{1064}$
KRA Equi. ($\overline{\mathcal{F}}$)	77,197(Cubic)	5,731	425	$2^{4481}/2^{6274}$
KRA Equi. ($\widehat{\mathcal{F}}$)	59,332(Cubic) + 9,450(Quad.)	3,588	135	$2^{1696}/2^{2375}$
KRA Good	121(Quad.)	79	16	$2^{131}/2^{183}$

each coordinate function has at least $n-1$ linear terms (See Lemma 3.2). Even if $\mathcal{F}'^{(k)}$ has only one linear term for each k, $\mathcal{F}'^{(k)} \circ \Omega'$ has at least $n-1$ linear terms. Nevertheless, if there is no linear term in $\mathcal{F}$, we can get nm linear terms with zero coefficients of $\mathcal{F}' \circ \Omega'$ and n variables in the constant part of $\widetilde{T''}$ by choosing Ω and Ω' carefully satisfying Lemmas 3.1 and 3.2. Then we can set $\Sigma' = \left(\widetilde{S'}\right)^{-1} = S'$ so that the variables in $\widetilde{S''}$ are removed. Finally, we get a system of $m(n+1)$ quadratic equations with $2n-u$ variables. In this case, for ELSA with $(F_{2^8}, 6, 28, 30, 15)$, the complexity of solving this system by HF5 is 2^{71}.

3.4 Rank-Based Attacks

• **MinRank attack.** In MinRank attacks, one tries to find linear combinations $M = \sum_{i=1}^{m} \mu_i P^{(i)}$ of the matrices $P^{(i)}$, where M has a minimal rank. Underlying idea of an algorithm to solve this MinRank problem [48] is to search for a vector lying in the kernel of the desired linear combination M. Complexity of the MinRank attack is determined by that of finding the linear combination. Since the forms of symmetric matrices of ELSA w.r.t. $\mathcal{F}$ are the same as those of Rainbow, we can get that its complexity against the attack is q^{l+k+1} from [9,44]. Next, by using similar technique, we investigate the complexity of ELSA w.r.t. $\widehat{\mathcal{F}}$ against the attack in Proposition 3.1.

Proposition 3.1. The complexity of ELSA w.r.t. $\widehat{\mathcal{F}}$ against the MinRank attack is $min\{q^{l+2r-k+1}, q^{l+2r+1}, q^{2l+k+1}\}$.

Proof. In MinRank attacks, we must find a vector $v \in \mathbb{F}_q^n$ such that $v \in \ker P$, where P is a matrix with the minimal rank in $\mathrm{Span}\{P^{(i)}\}$. The probability for finding such a vector is the same as that of finding $v' \in \mathbb{F}_q^n$ such that $v' \in \ker Q$, where Q is a matrix with the minimal rank in $\mathrm{Span}\{\widehat{F}^{(i)}\}$ and $\widehat{F}^{(i)}$ is the matrix of the quadratic part of $\widehat{\mathcal{F}}$. More precisely, $\widehat{F}^{(i)}$ has of the form $\begin{pmatrix} * & 0 & * \\ 0 & 0 & * \\ * & * & 0 \end{pmatrix}$ in

the first layer as given in Fig. 2. Then $\widehat{F}^{(i)} \cdot (0,*,0)^T = (0,0,*)^T$. Let $w_i = \widehat{F}^{(i)} \cdot (0,*,0)^T = (0,0,*)^T$. Then the probability that w_i is linearly dependent is

$$1 - \prod_{i=0}^{k-1}(1 - \frac{q^i}{q^r}) > 1/q^{r-k+1}.$$

Note that $\sum_{i=1}^{k} \lambda_i \widehat{F}^{(i)}$ has a minimal rank. Hence, the probability of $v' \in \ker(\sum_{i=1}^{k} \lambda_i \widehat{F}^{(i)})$ for a random vector v' and non-trivial λ_i is $1/q^{l+r} \cdot 1/q^{r-k+1} = 1/q^{l+2r-k+1}$, where the provability that the vector v' has of the form $(0,*,0)$ is $1/q^{l+r}$. Similarly, the probabilities for $\widehat{F}^{(i)} \cdot (*,0,0)$ and $\widehat{F}^{(i)} \cdot (0,0,*)$ are $1/q^{l+2r+1}$ and $1/q^{2l+k+1}$, respectively. □

Finally, the complexity of ELSA against the MinRank attack is $min\{q^{l+k+1}, q^{l+2r-k+1}, q^{l+2r+1}, q^{2l+k+1}\}$.

- **HighRank Attack.** In HighRank attacks, one tries to identify the variables appearing the lowest number of times in the central polynomials. The variables $x_{l+k+r+1}, \cdots, x_n$ appear only in the quadratic terms of the central polynomials $(\mathcal{F}^{(k+1)}, \cdots, \mathcal{F}^{(k+u)})$ of the second layer of ELSA. Thus, it is similar to that of Rainbow. As in [44], we get its complexity against the HighRank attacks is $q^u \cdot \frac{n^3}{6}$.
- **Kipnis-Shamir Attack (UOV Attack).** Kipnis-Shamir attack [34] was originally used to break the balanced Oil and Vinegar signature scheme [41]. We consider the generalization to the unbalanced case. We have already known that the complexity of ELSA w.r.t. $\mathcal{F}$ against the Kipnis-Shamir attack is $q^{n-2u-1} \cdot u^4$ as in [44] since the forms of symmetric matrices of ELSA w.r.t. $\mathcal{F}$ are the same as those of Rainbow.

Now, we give security analysis of ELSA with the central map $\widehat{\mathcal{F}}$ against the Kipnis-Shamir attacks. We first define the following four index sets as

$$D_1 = \{i | 1 \le i \le l\},\ D_2 = \{i | l+1 \le i \le l+k\},$$
$$D_3 = \{i | l+k+1 \le i \le l+k+r\},\ D_4 = \{i | l+k+r+1 \le i \le n\}.$$

We define five meaningful subspaces of $\mathbb{F}_q^n$ for the attacks on ELSA as

$$V_{1000} = \{(x_1, \cdots, x_n) | x_i = 0, i \notin D_1\}, V_{0100} = \{(x_1, \cdots, x_n) | x_i = 0, i \notin D_2\},$$
$$V_{0010} = \{(x_1, \cdots, x_n) | x_i = 0, i \notin D_3\}, V_{0001} = \{(x_1, \cdots, x_n) | x_i = 0, i \notin D_4\},$$
$$V_{1110} = \{(x_1, \cdots, x_n) | x_i = 0, i \in D_4\}.$$

The goal of the attacks is to find the preimage of the above subspaces under an equivalent key T'. We use the following property: any linear combinations of the matrices $\widehat{F}^{(1)}, \cdots, \widehat{F}^{(m)}$ is of the form $\begin{pmatrix} * & * & * & 0 \\ * & * & * & 0 \\ * & * & * & * \\ 0 & 0 & * & 0 \end{pmatrix} \cdots (*)$ from Fig. 2. The following Theorems show why invariant subspaces exist with a certain probability.

Lemma 3.3. Let $\phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a linear transformation of the form $(*)$. Then we get that $\phi(V_{0001})$, $\phi(V_{1000})$, and $\phi(V_{0100})$ are subspaces of V_{0010}, V_{1110} and V_{1110}, respectively.

Note that the image of other subspaces except the three subspaces in Lemma 3.3 under the map ϕ is the full space $\mathbb{F}_q^n$.

Let $H = \sum_{i=1}^{m} \lambda_i \widehat{F}^{(i)}$ be a linear combination of the matrices $\widehat{F}^{(i)}$. Note that H has the form of $(*)$. Then we get the following Theorem as in [34].

Theorem 3.2. Assume that, for some k $(1 \leq k \leq m)$, the matrix $\widehat{F}^{(k)}$ is invertible. Then, the map $(\widehat{F}^{(k)})^{-1} \cdot H$ has nontrivial invariant subspace $\phi(V_{0001})$, $\phi(V_{1000})$ and $\phi(V_{0100})$ with probability not less than q^{-r+u}, q^{-k-r} and q^{-l-r}, respectively.

Proof. They are obtained from the following fact: $[(\widehat{F}^{(k)})^{-1} \cdot \widehat{F}^{(i)}](V_{0001}) \subset (\widehat{F}^{(k)})^{-1}(V_{0010})$ and $V_{0001} \subset (\widehat{F}^{(k)})^{-1}(V_{0010})$, let $\Phi = (\widehat{F}^{(k)})^{-1} \cdot \widehat{F}^{(i)}$, then as in [33], we have

$$Pr[\Phi(V_{0001}) \subset V_{0010}] \geq q^{-r+u},$$

where $u = dim(V_{0001})$ and $r = dim(V_{0010})$. Thus, we get a nontrivial invariant subspace V_{0001} with probability not less than q^{-r+u}. □

Theorem 3.3. Let $W = \sum_{i=1}^{m} \lambda_i P^{(i)}$ be a linear combination of the matrices $P^{(i)}$ and let $P^{(k)}$ (for some k, $1 \leq k \leq m$) be invertible. Then the map $(P^{(k)})^{-1} \cdot W$ has nontrivial invariant subspaces V_{0010}, V_{1110} and V_{1110} which are subspaces of $T^{-1}(V_{0010})$, $T^{-1}(V_{1000})$ and $T^{-1}(V_{0100})$ with probability not less than q^{-r+u}, q^{-k-r} and q^{-l-r}, respectively.

Proof. They are obtained from the Theorem 3.2 and the following:

$$(P^{(k)})^{-1} \cdot W = (P^{(k)})^{-1} \cdot \sum_{i=1}^{m} \lambda_i P^{(i)} = (T^T \cdot F^{(k)} \cdot T)^{-1} \cdot \sum_{i=1}^{m} \lambda_i \cdot (T^T \cdot \widehat{F}^{(i)} \cdot T)$$
$$= T^{-1} \cdot (\sum_{i=1}^{m} \lambda_i (\widehat{F}^{(k)})^{-1} \cdot \widehat{F}^{(i)}) \cdot T.$$

$$(P^{(k)})^{-1} \cdot W(T^{-1}(V_{0001})) = (T^{-1} \cdot (\sum_{i=1}^{m} \lambda_i (\widehat{F}^{(k)})^{-1} \cdot \widehat{F}^{(i)}) \cdot T)(T^{-1}(V_{0001}))$$
$$= T^{-1} \cdot (\sum_{i=1}^{m} \lambda_i (F^{(k)})^{-1} \cdot F^{(i)})(V_{0001}) \subset T^{-1}(V_{0010}).$$

Thus, we get a nontrivial invariant subspace V_{0001} with probability not less than q^{-r+u}. □

Consequently, the complexity of ELSA against the Kipnis-Shamir attack is $min\{q^{r-u}, q^{k+r}, q^{l+r},\ q^{n-2u-1} \cdot u^4\}$.

Based on these security analysis, we can select secure parameter sets $(\mathbb{F}_q, l, k, r, u)$ that achieve given security levels.

4 Existential Unforgeability of ELSA

Here, we prove existential unforgeability of ELSA against an adaptive chosen-message attack under the hardness of the MQ-problem induced by a public key of ELSA.

4.1 Formal Security Model and Complexity Assumption

In this section, we describe formal security models of signature schemes. The most general security notion of signature schemes is existential unforgeability against an adaptive chosen-message attack. Its formal security model is defined as follows:

Existential Unforgeability against Adaptive Chosen-Message Attacks (EUF-acma). An adversary $\mathcal{A}$'s advantage $Adv_{\mathcal{PKS},\mathcal{A}}$ is defined as its probability of success in the following game between a challenger $\mathcal{C}$ and $\mathcal{A}$:

- **Setup.** The challenger runs `Setup` algorithm and its resulting system parameters are given to $\mathcal{A}$.
- **Sign Queries.** $\mathcal{A}$ issues the following queries: adaptively, $\mathcal{A}$ requests a signature on a message $\mathtt{m}_i$, $\mathcal{C}$ returns a signature σ_i.
- **Output.** Eventually, $\mathcal{A}$ outputs σ^* on a message $\mathtt{m}^*$ and wins the game if
  (i) $\mathtt{Verify}(\mathtt{m}^*, \sigma^*) = 1$,
  (ii) $\mathtt{m}^*$ has never requested to the `Sign` oracle.

Definition 4.1. A forger $\mathcal{A}(t, g_H, q_S, \epsilon)$-breaks a signature scheme if $\mathcal{A}$ runs in time at most t, $\mathcal{A}$ makes at most q_H queries to the hash oracle, q_S queries to the signing oracle and $Adv_{\mathcal{PKS},\mathcal{A}}$ is at least ϵ. A signature scheme is (t, q_E, q_S, ϵ)-EUF-acma if no forger (t, q_H, q_S, ϵ)-breaks it in the above game.

Next, we need to define the following sets as:

- $\mathcal{MQ}_{ELSA}(\mathbb{F}_q, m, n)$: a set of all quadratic equations defined over $\mathbb{F}_q$ with m equations and n variables induced by all public keys of ELSA$(\mathbb{F}_q, l, k, r, u)$, where $m = k + u$ and $n = l + r + m$.
- $\mathcal{MQ}_R(\mathbb{F}_q, m, n)$: a set of all random quadratic equations defined over $\mathbb{F}_q$ of m equations and n variables.

Definition 4.2. We say that the MQ-problem in $\mathcal{MQ}_X(\mathbb{F}_q, m, n)$ is (t, ϵ)-hard if no t-time algorithm has advantage at least ϵ in solving the MQ-problem in $\mathcal{MQ}_X(\mathbb{F}_q, m, n)$.

To prove existential unforgeability of ELSA against an adaptive chosen-message attack, we want to find a reduction to the hardness of MQ-problem in $\mathcal{MQ}_{ELSA}(\mathbb{F}_q, m, n)$. The hardness of the MQ-problem for a system of m quadratic equations with n variables mainly depends on the selection of $\mathbb{F}_q$, m and n. However, the security of ELSA against the attacks presented in §3 depends on the selection of the specific parameter set $(\mathbb{F}_q, l, k, r, u)$ such that

$m = k + u$ and $n = l + r + m$. If the parameter set $(\mathbb{F}_q, l, k, r, u)$ is chosen be secure against the MinRank attack, HighRank attack and Kipnis-Shamir attack, then it remains only two attacks to consider: the direct attack and KRAs with good keys. In Theorem 3.1, we have shown that the security of KRAs with good keys for ELSA is still reduced to the intractability of the MQ-problem, i.e., the complexity of the KRAs using good keys on ELSA is determined by solving $n-1$ bihomogeneous equations and m quadratic equations with n variables.

4.2 Existential Unforgeability

Now, we prove existential unforgeability of ELSA against an adaptive chosen-message attack under the hardness of the MQ-problem induced by a public key of ELSA in the random oracle model.

Theorem 4.1. If the MQ-problem in $\mathcal{MQ}_{ELSA}(\mathbb{F}_q, m, n)$ is (t', ε')-hard, ELSA $(\mathbb{F}_q, l, k, r, u)$ is $(t, q_H, q_S, \varepsilon)$-EUF-acma, for any t and ε satisfying

$$\varepsilon \geq \mathtt{e} \cdot (q_S + 1) \cdot \varepsilon', \ t' \geq t + q_H \cdot c_V + q_S \cdot c_S,$$

where $\mathtt{e}$ is the base of the natural logarithm, and c_S and c_V are time for a signature generation and a signature verification, respectively, where $m = k+u$, and $n = l+r+m$ if the parameter set $(\mathbb{F}_q, l, k, r, u)$ is chosen to be secure against the MinRank attack, HighRank attack, Kipnis-Shamir attack and KRAs using good keys.

Proof. An instance $(\mathcal{P}, \eta)$ of the MQ-problem in $\mathcal{MQ}_{ELSA}(\mathbb{F}_q, m, n)$ is given, where $\mathcal{P}$ is a quadratic system of m equations and n variables. Suppose that $\mathcal{A}$ is a forger who breaks ELSA$(\mathbb{F}_q, l, k, r, u)$ with the target public key $\mathcal{P}$. We will construct an algorithm $\mathcal{B}$ which outputs a solution $\mathbf{x} \in \mathbb{F}_q^n$ such that $\mathcal{P}(\mathbf{x}) = \eta$ by using $\mathcal{A}$. Algorithm $\mathcal{B}$ performs the following simulation by interacting with $\mathcal{A}$.

Setup. Algorithm $\mathcal{B}$ sets $PK = \mathcal{P}$, which is a public key of ELSA$(\mathbb{F}_q, l, k, r, u)$.

At any time, $\mathcal{A}$ can query a random oracle H and `Sign` oracle. To answer these queries, $\mathcal{B}$ does the following:

H-Queries. For H-queries, $\mathcal{B}$ maintains a list of tuples $(\mathtt{m}_i, c_i, \tau_i)$ as explained below. We call this list H-`list`. When $\mathcal{A}$ queries H at $\mathtt{m}_i \in \{0,1\}^*$,

1. If the query already appears on H-`list` in a tuple $(\mathtt{m}_i, c_i, \tau_i, \mathcal{P}(\tau_i))$ then $\mathcal{B}$ returns $H(\mathtt{m}_i) = \mathcal{P}(\tau_i)$.
2. Otherwise, $\mathcal{B}$ picks a random coin $c_i \in \{0,1\}$ with $Pr[c_i = 0] = \frac{1}{q_S+1}$.
   - If $c_i = 1$ then $\mathcal{B}$ chooses a random $\tau_i \in \mathbb{F}_q^n$, adds a tuple $(\mathtt{m}_i, c_i, \tau_i, \mathcal{P}(\tau_i))$ to H-`list` and returns $H(\mathtt{m}_i) = \mathcal{P}(\tau_i)$.
   - If $c_i = 0$ then $\mathcal{B}$ adds $(\mathtt{m}_i, c_i, *, \eta)$ to H-`list` from the instance and returns $H(\mathtt{m}_i) = \eta$.

Sign Queries. When $\mathcal{A}$ makes a `Sign`-query on $\mathtt{m}_i$, $\mathcal{B}$ finds the corresponding tuple $(\mathtt{m}_i, c_i, \tau_i, \mathcal{P}(\tau_i))$ from H-`list`.

– If $c_i = 1$ then $\mathcal{B}$ responds with τ_i.
– If $c_i = 0$ then $\mathcal{B}$ reports failure and terminates.

All responses to `Sign` queries not aborted are valid. If $\mathcal{B}$ doesn't abort as a result of $\mathcal{A}$'s `Sign` query then $\mathcal{A}$'s view in the simulation is identical to its view in the real attack.

Output. Finally, $\mathcal{A}$ produces a signature τ^* on a message $\mathtt{m}^*$. If it is not valid then $\mathcal{B}$ reports failure and terminates. Otherwise, a query on m^* already appears on H-`list` in a tuple $(\mathtt{m}^*, c^*, \tau^*, \mathcal{P}(\tau^*))$: if $c_* = 1$ then reports failure and terminates. Otherwise, $c^* = 0$, i.e., $(c^*, \mathtt{m}^*, *, \eta)$, then $\mathcal{P}(\tau^*) = \eta$. Finally, $\mathcal{B}$ outputs τ^* is a solution of $\mathcal{P}$.

To show that $\mathcal{B}$ solves the given instance with probability at least ε', we analyze three events needed for $\mathcal{B}$ to succeed:

– E_1: $\mathcal{B}$ doesn't abort as a result of $\mathcal{A}$'s `Sign` query.
– E_2: $\mathcal{A}$ generates a valid and nontrivial signature forgery τ_i on $\mathtt{m}_i$.
– E_3: Event E_2 occurs, $c_i = 0$ for the tuple containing $\mathtt{m}_i$ in H-`list`.

Algorithm $\mathcal{B}$ succeeds if all of these events happen. The probability $Pr[E_1 \wedge E_3]$ is decomposed as

$$Pr[E_1 \wedge E_3] = Pr[E_1] \cdot Pr[E_2 \wedge E_1] \cdot Pr[E_3 | E_1 \wedge E_2] \ \cdots \ (**).$$

The probability that $\mathcal{B}$ doesn't abort as a result of $\mathcal{A}$'s `Sign` query is at least $(1 - \frac{1}{q_S+1})^{q_S}$ since $\mathcal{A}$ makes at most q_S queries to the `Sign` oracle. Thus, $Pr[E_1] \geq (1 - \frac{1}{q_S+1})^{q_S}$. If $\mathcal{B}$ doesn't abort as a result of $\mathcal{A}$'s `Sign` query then $\mathcal{A}$'s view is identical to its view in the real attack. Hence, $Pr[E_1 \wedge E_2] \geq \varepsilon$. Given that events E_1, E_2 and E_3 happened, $\mathcal{B}$ will abort if $\mathcal{A}$ generates a forgery with $c_i = 1$. Thus, all the remaining c_i are independent of $\mathcal{A}$'s view. Since $\mathcal{A}$ could not have issued a signature query for the output we know that c is independent of $\mathcal{A}$'s current view and therefore $Pr[c = 0 | E_1 \wedge E_2] = \frac{1}{q_S+1}$. Then we get $Pr[E_3 | E_1 \wedge E_2] \geq \frac{1}{q_S+1}$. From $(**)$, $\mathcal{B}$ produces the correct answer with probability at least

$$(1 - \frac{1}{q_S+1})^{q_S} \cdot \varepsilon \cdot \frac{1}{q_S+1} \ \geq \ \frac{1}{\mathtt{e}} \cdot \frac{\varepsilon}{(q_S+1)} \ \geq \ \varepsilon'.$$

Algorithm $\mathcal{B}$'s running time is the same as $\mathcal{A}$'s running time plus the time that takes to respond to q_H H-queries, and q_S `Sign`-queries. The H- and `Sign`-queries require a signature verification and a signature generation, respectively. We assume that a signature generation and a signature verification take time c_S and c_V, respectively. Thus, the total running time is at most $t' \geq t + q_H \cdot c_V + q_S \cdot c_S$. □

5 Selection of Parameter and Implementation

Here, we evaluate practical feasibility of ELSA targeting a recent Intel processor. We choose a secure and optimal parameter for ELSA and provide comparisons between ours, classical ones and Post-Quantum ones in terms of performance, key sizes and signature sizes.

5.1 Selection of Secure and Optimal Parameter

We want to select secure parameter set $(\mathbb{F}_q, l, k, r, u)$ for ELSA with the optimal secret key size at a 128-bit security level where $m = k + u$ and $n = l + r + m$. Based on our security analysis in Sect. 3, we choose $(\mathbb{F}_{2^8}, 6, 28, 30, 15)$ at the 128-bit security level. We summarize complexities of our parameter against the known attacks in Table 3. For computing of complexities against direct attacks and KRAs using good keys, we use HF5 with $\omega = 2$.

Table 3. Complexities of ELSA$(\mathbb{F}_{2^8}, 6, 28, 30, 15)$ against all the attacks.

$(\mathbb{F}_q, l, k, r, u)$	Direct	KRA (Good)	Kipnis-Shamir attack	MinRank	HighRank
$(\mathbb{F}_{2^8}, 6, 28, 30, 15)$	2^{131}	2^{131}	2^{136}	2^{280}	2^{143}

Table 4. Performance, key sizes and signature sizes of ours, classical-ones and post-quantum ones.

Scheme λ	Sig. size (bytes)	PK (bytes)	SK (bytes)	Sign (bytes)	Verify (bytes)	CPU
Classical ones						
RSA-3072^e 128	361	384	3072	8,802,242	87,360	Intel Core i5-6600 3.3 GHz
ECDSA-256^e 128	64	64	96	163,994	310,048	Intel Core i5-6600 3.3 GHz
ed25519^e [4] 128	64	32	64	48,976	165,322	Intel Core i5-6600 3.3 GHz
Lattice-based						
TESLA-416^t [3] 128	1,280	1,331,200	1,011,744	697,940	250,264	Intel Core i7-4770K(Haswell)
TESLA-768^t [3] $>$ 128	2,336	4,227,072	3,293,216	2,232,906	863,790	Intel Core i7-4770K(Haswell)
BLISS-BI [19,20] 128	700	875	250	358,400	102,000	Intel Core i7 3.4 GHz
ntrumls 439x^e [29] 128	988	1,112	1,305	485,580	223,488	Intel Core i5-6600 3.3 GHz
Hash-based						
SPHINCS 256^s [5] 256	41,000	1,056	1,088	51,636,372	1,451,004	Intel Xeon E3-1275 3.5 GHz
Code-based						
CFS [35] 80	75	20,968,300	4,194,300	4,200,000,000	–	Intel Xeon W3670 3.2 GHz
MQ-based						
MQDSS-31-64 [13] $>$ 128	40,952	72	64	8,510,616	5,752,616	Intel Core i7-4770K 3.5 GHz
enTTS $(\mathbb{F}_{2^8}, 15, 60, 88)$ [15,52] 128	88	234,960	13,051	–	–	–
Rainbow^o $(\mathbb{F}_{2^8}, 36, 21, 22)$ [6] 128	79	139,320	105,006	64,658	44,397	Intel Core i5-6600 3.3 GHz
ELSA $(\mathbb{F}_{2^8}, 6, 28, 30, 15)$ 128	**79**	**139,320**	**12,427**	**20,880**	**44,190**	Intel Core i5-6600 3.3 GHz

Sig. Size, PK and SK represent signature size, public key and secret key, respectively.
ed25519 is EdDSA signatures using Curve25519.
$>$128 means that the scheme achieves 2^λ security level, where $\lambda > 128$.
^{t} The scheme has a tight security reduction to the underlying problem.
^{s} The scheme is provably secure in the standard model.
^{e} The result is given by the eBACS project [6].
^{o} We implement Rainbow based on the code in [6] at the 128-bit security level on Intel Core i5-6600 3.3 GHz.

5.2 Result and Comparison

We implement ELSA($\mathbb{F}_{2^8}, 6, 28, 30, 15$) on an Intel Core i5-6600 3.3 GHz whose result is an average of 1,000 measurements for each function using the C++ programming language with g++ compiler. We follow the standard practice of disabling Turbo Boost and hyperthreading. For comparison, we also implement Rainbow($\mathbb{F}_{2^8}, 36, 21, 22$) on the same platform based on open source codes given by the eBACS project [6] since there is no record for Rainbow at the 128-bit security level. Table 4 gives benchmarking results of ELSA and compares the benchmarks to state-of-the-art results from the literatures or given by the eBACS project [6].

Our scheme is the fastest signature scheme in both signing and verification among classical ones and Post-Quantum ones. Compared to Rainbow, the secret key size of ELSA is reduced by a factor of 88% maintaining the same public key size. Compared to enTTS, the public key size of ELSA have reduced by a factor of 40%. Signing of ELSA is about 3.2 times faster than that of Rainbow. Signing and verification of ELSA is hundreds of times faster than those of MQDSS, respectively. Signing and verification of ELSA is about 17.2 times and 2.3 times faster than those of BLISS-BI, respectively. It takes 6 µs and 13.3 µs for signing and verification, respectively.

6 Conclusion

We have proposed a new MQ-signature scheme, ELSA, based on a hidden layer of quadratic equations. Our scheme is the fastest signature scheme in both signing and verification among classical ones as well as Post-Quantum ones. Compared to Rainbow, the secret key size in ELSA is reduced by a factor of 88% maintaining the same public key size. Signing of ELSA is about 3.2 times than that of Rainbow on Intel Core i5-6600. It takes 6.3 µs and 13.39 µs for signing and verification, respectively. There is still room for improvements in terms of performance. We believe that our scheme is a leading candidate for low-cost constrained devices. We have also shown that ELSA($\mathbb{F}_q, l, k, r, u$) is existential unforgeable against an adaptive chosen-message attack under the hardness of the MQ-problem in $\mathcal{MQ}_{ELSA}(\mathbb{F}_q, m, n)$ in the random oracle model. However, this reduction doesn't mean the reduction to the MQ-problem in $\mathcal{MQ}_R(\mathbb{F}_q, m, n)$ although it haven't been proved that the public key of the MQ-schemes could be distinguished from random one. It still remains an open problem to construct a high-speed MQ-signature schemes with a security reduction to the hardness of the MQ-problem in $\mathcal{MQ}_R(\mathbb{F}_q, m, n)$.

References

1. El Yousfi Alaoui, S.M., Dagdelen, Ö., Véron, P., Galindo, D., Cayrel, P.-L.: Extended security arguments for signature schemes. In: Mitrokotsa, A., Vaudenay, S. (eds.) AFRICACRYPT 2012. LNCS, vol. 7374, pp. 19–34. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31410-0_2

2. Albrecht, M.R., Faugére, J.-C., Fitzpatrick, R., Perret, L., Todo, Y., Xagawa, K.: Practical cryptanalysis of a public-key encryption scheme based on new multivariate quadratic assumptions. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 446–464. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_26
3. Alkim, E., Bindel, N., Buchmann, J., Dagdelen, O., Schwabe, P.: TESLA: tightly-secure efficient signatures from standard lattices, Cryptology ePrint Archive: Report 2015/755 (2015)
4. Bernstein, D.J.: Curve25519: new diffie-hellman speed records. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 207–228. Springer, Heidelberg (2006). https://doi.org/10.1007/11745853_14
5. Bernstein, D.J., et al.: SPHINCS: practical stateless hash-based signatures. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 368–397. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_15
6. Bernstein, D.J., Lange, T.: eBACS: ECRYPT benchmarking of cryptographic systems. http://bench.cr.yp.to. Accessed 30 Sept 2016
7. Bettale, L., Faugére, J.-C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. J. Math. Cryptol. **3**, 177–197 (2009)
8. Biham, E.: Cryptanalysis of patarin's 2-round public key system with S boxes (2R). In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 408–416. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_28
9. Billet, O., Gilbert, H.: Cryptanalysis of rainbow. In: Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 336–347. Springer, Heidelberg (2006). https://doi.org/10.1007/11832072_23
10. Biryukov, A., Bouillaguet, C., Khovratovich, D.: Cryptographic schemes based on the ASASA structure: black-box, white-box, and public-key (extended abstract). In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 63–84. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_4
11. Bogdanov, A., Eisenbarth, T., Rupp, A., Wolf, C.: Time-area optimized public-key engines: $\mathcal{MQ}$-cryptosystems as replacement for elliptic curves? In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 45–61. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85053-3_4
12. Chen, A.I.-T., et al.: SSE implementation of multivariate PKCs on modern x86 CPUs. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 33–48. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04138-9_3
13. Chen, M.-S., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: From 5-pass $\mathcal{MQ}$-based identification to $\mathcal{MQ}$-based signatures. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 135–165. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_5
14. Courtois, N.T.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 402–421. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_24
15. Czypek, P., Heyse, S., Thomae, E.: Efficient implementations of MQPKS on constrained devices. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 374–389. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33027-8_22
16. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005). https://doi.org/10.1007/11496137_12

17. Ding, J., Yang, B.-Y., Chen, C.-H.O., Chen, M.-S., Cheng, C.-M.: New differential-algebraic attacks and reparametrization of rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 242–257. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68914-0_15
18. Ding-Feng, Y., Kwok-Yan, L., Zong-Duo, D.: Cryptanalysis of "2R" schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 315–325. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_20
19. Ducas, L.: Accelerating bliss: the geometry of ternary polynomials, Cryptology ePrint Archive: Report 2014/874 (2014)
20. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal Gaussians. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8042, pp. 40–56. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_3
21. Düll, M., Haase, B., Hinterwälder, G., Hutter, M., Paar, C., Sánchez, A.H., Schwabe, P.: High-speed curve25519 on 8-bit, 16-bit and 32-bit microcontrollers. Des. Codes Crypt. **77**(2–3), 493–514 (2015)
22. Faugére, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: ISSAC 2002, pp. 75–83 (2002)
23. Faugère, J.-C., Gligoroski, D., Perret, L., Samardjiska, S., Thomae, E.: A polynomial-time key-recovery attack on MQQ cryptosystems. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 150–174. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_7
24. Faugère, J.-C., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 280–296. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_16
25. Faugére, J.-C., Perret, L.: High order derivatives and decomposition of multivariate polynomials. In: ACM International Symposium on Symbolic and Algebraic Computation, pp. 207–214 (2009)
26. Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, New York (1979)
27. Gilbert, H., Plût, J., Treger, J.: Key-recovery attack on the ASASA cryptosystem with expanding S-boxes. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 475–490. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_23
28. Gligoroski, D., Ødegård, R.S., Jensen, R.E., Perret, L., Faugère, J.-C., Knapskog, S.J., Markovski, S.: MQQ-SIG. In: Chen, L., Yung, M., Zhu, L. (eds.) INTRUST 2011. LNCS, vol. 7222, pp. 184–203. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32298-3_13
29. Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H., Whyte, W.: Transcript secure signatures based on modular lattices. In: Mosca, M. (ed.) PQCrypto 2014. LNCS, vol. 8772, pp. 142–159. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11659-4_9
30. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054868
31. Huang, Y.-J., Liu, F.-H., Yang, B.-Y.: Public-key cryptography from new multivariate quadratic assumptions. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 190–205. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_12

32. Hülsing, A., Rijneveld, J., Song, F.: Mitigating multi-target attacks in hash-based signatures. In: Cheng, C.-M., Chung, K.-M., Persiano, G., Yang, B.-Y. (eds.) PKC 2016. LNCS, vol. 9614, pp. 387–416. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49384-7_15
33. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_15
34. Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 257–266. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0055733
35. Landais, G., Sendrier, N.: Implementing CFS. In: Galbraith, S., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 474–488. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34931-7_27
36. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Barstow, D., Brauer, W., Brinch Hansen, P., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmüller, G., Stoer, J., Wirth, N., Günther, C.G. (eds.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-45961-8_39
37. McEliece, R.: A public-key cryptosystem based on algebraic coding theory, DSN progress report 42–44. Jet Propulsion Laboratories, Pasadena (1978)
38. Merkle, R.C.: A digital signature based on a conventional encryption function. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 369–378. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-48184-2_32
39. Minaud, B., Derbez, P., Fouque, P.-A., Karpman, P.: Key-recovery attacks on ASASA. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 3–27. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48800-3_1
40. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_4
41. Patarin, J.: The oil and vinegar signature scheme. In: Dagstuhl Workshop on Cryptography, September 1997
42. Patarin, J., Courtois, N., Goubin, L.: QUARTZ, 128-bit long digital signatures. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 282–297. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45353-9_21
43. Patarin, J., Goubin, L.: Asymmetric cryptography with S-boxes is it easier than expected to design efficient asymmetric cryptosystems? In: Han, Y., Okamoto, T., Qing, S. (eds.) ICICS 1997. LNCS, vol. 1334, pp. 369–380. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0028492
44. Petzoldt, A.: Selecting and reducing key sizes for multivariate cryptography, Ph.D. thesis (2013)
45. Petzoldt, A., Chen, M.-S., Yang, B.-Y., Tao, C., Ding, J.: Design principles for HFEv- based multivariate signature schemes. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 311–334. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_14
46. Pöppelmann, T., Oder, T., Güneysu, T.: High-performance ideal lattice-based cryptography on 8-bit ATxmega microcontrollers. In: Lauter, K., Rodríguez-Henríquez, F. (eds.) LATINCRYPT 2015. LNCS, vol. 9230, pp. 346–365. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22174-8_19

47. Sakumoto, K., Shirai, T., Hiwatari, H.: Public-key identification schemes based on multivariate quadratic polynomials. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 706–723. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_40
48. Shallit, J.O., Frandsen, G.S., Buss, J.F.: The computational complexity of some problems of linear algebra, BRICS series report, Aarhus, Denmark, RS-96-33. http://www.brics.dk/RS/96/33
49. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
50. Thomae, E.: About the security of multivariate quadratic public key schemes, Dissertation Thesis by Dipl. math. E. Thomae, RUB (2013)
51. Wolf, C., Preneel, B.: Large superfluous keys in $\mathcal{M}$ultivariate $\mathcal{Q}$uadratic asymmetric systems. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 275–287. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30580-4_19
52. Yang, B.-Y., Chen, J.-M.: Building secure tame-like multivariate public-key cryptosystems: the new TTS. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 518–531. Springer, Heidelberg (2005). https://doi.org/10.1007/11506157_43

http://www.springer.com/978-3-319-70693-1

Advances in Cryptology – ASIACRYPT 2017
23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I
Takagi, T.; Peyrin, Th. (Eds.)
2017, XXVI, 813 p. 121 illus., Softcover
ISBN: 978-3-319-70693-1