Multivariate Encryption Schemes Based on Polynomial Equations over Real Numbers

Takanori Yasuda[1(✉)], Yacheng Wang[2], and Tsuyoshi Takagi[2]

[1] Okayama University of Science, Okayama, Japan
tyasuda@bme.ous.ac.jp
[2] Department of Mathematical Informatics, University of Tokyo, Tokyo, Japan
{yacheng_wang,takagi}@mist.i.u-tokyo.ac.jp

Abstract. The MQ problem, an NP-complete problem, is related to the security of Multivariate Public Key Cryptography (MPKC). Its variant, the constrained MQ problem, was first considered in constructing secure multivariate encryption schemes using the *pq*-method proposed at ProvSec2018. In this paper, we propose an encryption scheme named PERN, whose key space completely includes that of the *pq*-method. The decryption of PERN uses methods of solving nonlinear equations over the real numbers, which is different from the decryption of the existing encryption schemes in MPKC. The construction of PERN is fairly flexible, which enables us to construct a multivariate encryption scheme, whose public key consists of multivariate polynomials of degree 2, 3 or higher degrees while constraining its public key to a reasonable size.

Keywords: Multivariate Public Key Cryptosystems · Constrained MQ problem · MQ problem · Nonlinear equations · Post-quantum cryptography

1 Introduction

Multivariate Public Key Cryptography (MPKC) [8], which is a candidate for post-quantum cryptography, uses multivariate polynomial systems as its public key, and in most cases, its security is based on the difficulty of solving a set of multivariate polynomials. This problem of solving a set of multivariate polynomials is called the MP problem as follows.

MP problem: For a prime number q and positive integers m, n, let $\mathcal{F}(\mathbf{x})$ be a polynomial system of m polynomials over a finite field $\mathbb{F}_q$ in n variables $\mathbf{x} = (x_1, \ldots, x_n)$. Then, find $\mathbf{x}_0 \in \mathbb{F}_q^n$ such that $\mathcal{F}(\mathbf{x}_0) = \mathbf{0}$.

The constrained MP problem is derived from the MP problem.

Constrained MP problem: For a prime number q and positive integers m, n, L, let $\mathcal{F}(\mathbf{x})$ be a polynomial system of m polynomials over $\mathbb{F}_q$ in n variables $\mathbf{x} = (x_1, \ldots, x_n)$. Then, find $\mathbf{x}_0 = (x_{0,1}, \ldots, x_{0,n}) \in \mathbb{Z}^n$ such that $\mathcal{F}(\mathbf{x}_0) = \mathbf{0}$ and $-\frac{L}{2} < x_{0,i} \leq \frac{L}{2}$ $(i = 1, \ldots, n)$.

J. Ding and J.-P. Tillich (Eds.): PQCrypto 2020, LNCS 12100, pp. 402–421, 2020.
https://doi.org/10.1007/978-3-030-44223-1_22

When only quadratic polynomials are used in the (constrained) MP problem, the problem is called the (constrained) MQ problem. At ProvSec2018, Yasuda [37] introduced the constrained MQ problem for the first time, and proposed a method called the *pq*-method for constructing multivariate encryption schemes whose security is mainly based on the difficulty of solving the constrained MQ problem. The constrained MP problem is also related to the SIS problem. In fact, the SSNE Problem [30] derived from the SIS problem is very similar to the constrained MP problem.

As MPKC encryption schemes, Simple Matrix Scheme [31], EFC [29], and HFERP [16] are known. A detailed cryptanalysis for HFERP is not yet done since it was recently proposed. For Simple Matrix Scheme and EFC, critical attacks have not been reported, but they require using very large parameters, which sacrifices the performance of encryption and decryption. Because of such circumstances, developing new encryption schemes in MPKC becomes an important problem.

One reason that accounts for the difficulty of designing a secure MPKC encryption scheme is the difficulty of constructing trapdoor one-way functions given by injective polynomial maps. However, by adding a restriction on the definition range of a polynomial map, the map can easily become injective. Consequently, it is easy to construct an injective trapdoor one-way function with a constrained polynomial map, and this function can be used to construct MPKC encryption schemes whose security is based on the difficulty of solving the constrained MP problem.

Most of the MPKC encryption schemes uses a bipolar structure. The key generation of a multivariate encryption scheme with the bipolar structure is described as follows.

1. Choose an injective multivariate polynomial map $G(\mathbf{x}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ whose inverse can be computed efficiently.
2. Choose randomly affine isomorphisms S, T on $\mathbb{F}_q^n, \mathbb{F}_q^m$, respectively.
3. Compute $F(\mathbf{x}) = T \circ G(\mathbf{x}) \circ S : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

$F(\mathbf{x})$ is used as a public key, and the secret key consists of $G(\mathbf{x}), T$ and S. $G(\mathbf{x})$ is called the central map of this scheme. Encryption and decryption processes are described as follows.

Encryption: For a plaintext $\mathbf{m} \in \mathbb{F}_q^n$, compute $\mathbf{c} = F(\mathbf{m})$. $\mathbf{c}$ is a ciphertext.
Decryption: For a ciphertext $\mathbf{c} \in \mathbb{F}_q^m$, compute (1) $\mathbf{b}_1 = T^{-1}(\mathbf{c})$, (2) $\mathbf{b}_2 = G^{-1}(\mathbf{b}_1)$, (3) $\mathbf{m}' = S^{-1}(\mathbf{b}_2)$ in this order. $\mathbf{m}'$ coincides with the plaintext $\mathbf{m}$.

The security of the schemes using the bipolar structure is based on the difficulty of solving the (usual) MP problem. If we want to change this security assumption to the constrained MP problem, the map $G(\mathbf{x}) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ should be changed to a constrained polynomial map $G(\mathbf{x}) : \mathcal{I} \to \mathbb{F}_q^m$ where $\mathcal{I}$ is a proper subset of $\mathbb{F}_q^n$ and $\mathbf{m}$ should be chosen from $\mathcal{I}$. Here, $G(\mathbf{x})$ is sufficient to be injective on $\mathcal{I}$. Note that the definition range of $F(\mathbf{x})$ is $S^{-1}(\mathcal{I})$. The *pq*-method also uses the bipolar structure. (However, S is restricted as $\mathcal{I} = S^{-1}(\mathcal{I})$.)

The construction of $G(\mathbf{x})$ in the pq-method is as follows. First, we construct a central map $G_0(\mathbf{x})$ of an (previously proposed) encryption scheme (e.g. the Matsumoto-Imai scheme [22]) over $\mathbb{F}_p$, where p is enough smaller than q. $G_0(\mathbf{x})$ is then lifted into a polynomial map $\Phi(\mathbf{x})$ with integer coefficients. Next, prepare a certain polynomial map $\Psi_R(\mathbf{x})$ with integer coefficients, $G(\mathbf{x})$ is defined by $G(\mathbf{x}) = \Phi(\mathbf{x}) + \Psi_R(\mathbf{x})$. ($\Psi_R(\mathbf{x})$ is a polynomial map appended to enhance security) In the decryption algorithm of the pq-method, the computation of $\mathbf{b}_2 = G^{-1}(\mathbf{b}_1)$ is done as follows: From $\mathbf{b}_1 = G(\mathbf{b}_2) = \Phi(\mathbf{b}_2) + \Psi_R(\mathbf{b}_2)$, the part $\Psi_R(\mathbf{b}_2)$ can be eliminated due to its special design in the pq-method. After that, $\mathbf{b}_2$ can be obtained by inverting $G_0(\mathbf{x})$. We can say that the pq-method is a modifier that changes encryption schemes in MPKC over $\mathbb{F}_p$ to encryption schemes over $\mathbb{F}_q$. However, the pq-method requires a constraint on the domain of $G(\mathbf{x})$. Due to this constraint, $G(\mathbf{x})$ can become injective. By the existence of the constraint, the security of the pq-method is related to the constrained MQ problem.

In this paper, we propose a new multivariate encryption scheme called PERN (Polynomial Equations over the Real Numbers), whose security is mainly based on the difficulty of solving the constrained MP problem. PERN resembles the pq-method, but PERN does not use a central map of a previously proposed encryption scheme for the construction of $G(\mathbf{x})$. As a $\Phi(\mathbf{x})$, we can choose any polynomial map with small integer coefficients. This implies that the key space of PERN completely includes that of the pq-method. In the decryption of PERN, we need to solve a system of $2n$ equations in n variables with integer coefficients. To solve such a system, we use techniques of solving a system of nonlinear equations over the real numbers, and the fact that its solution has integer components. Since these techniques of solving a system of nonlinear equations over the real numbers are applicable to polynomial systems of any degree, $\Phi(\mathbf{x})$ (and $\Psi_R(\mathbf{x})$) can be chosen with any degree in principle. For the first time, techniques for solving the system of nonlinear equations over the real numbers are used for the decryption in MPKC (Table 1).

Table 1. Different solvers used in the decryption of MPKCs

Tool	Representative schemes
Power operator	C^* [22], Square [6]
Linear equation solver over $\mathbb{F}_q$	Rainbow [9], ABC [31]
Univariate equation solver over $\mathbb{F}_q$	HFE [26], Gui [27]
Multivariate equation solver over $\mathbb{F}_q$	Multi-HFE [4]
Nonlinear equation solver over $\mathbb{R}$	Proposed scheme

In the proposed scheme, the affine isomorphism S is fixed to be an identity map. Therefore, the set of monomials appearing in $G(\mathbf{x})$ and $F(\mathbf{x})$ can be adjusted freely. This means that the key length can also be adjusted freely.

Hence, we do not need to restrict the degree of polynomials to 2 or 3 due to the key length considerations as in the previous MPKC schemes. As another advantage of the proposed scheme, the complexity of the Gröbner basis attack can be maximized. However, if the number of monomials appearing in $G(\mathbf{x})$ and $F(\mathbf{x})$ is too few, the complexity of the Gröbner basis attack decreases and the attack against the inhomogeneous SIS problem works effectively on the proposed scheme. Moreover, it may increase the number of equivalent keys. Therefore, the proposed scheme should take a large number of monomials.

2 Trapdoor Functions by Multivariate Polynomials with Integer Coefficients

For a positive integer l, we denote the least non-negative remainder of an integer a by $a \bmod l$, and the least absolute remainder of a by $\mathrm{lift}_l(a)$. For $a \in \mathbb{Z}/l\mathbb{Z}$, $a \bmod l$ and $\mathrm{lift}_l(a)$ are defined similarly. I_l is defined by $I_l = (-l/2, l/2] \cap \mathbb{Z}$, then $a \bmod l \in [0, l-1]$ and $\mathrm{lift}_l(a) \in I_l$.

Let $x_1, \ldots, x_n$ be n independent variables and $\mathbf{x} = (x_1, \ldots, x_n)$. Let

$$\Phi(\mathbf{x}) = (\phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x})) \in \mathbb{Z}[\mathbf{x}]^n, \quad \Psi(\mathbf{x}) = (\psi_1(\mathbf{x}), \ldots, \psi_n(\mathbf{x})) \in \mathbb{Z}[\mathbf{x}]^n$$

be two polynomial systems with integer coefficients of which absolute values are small. Let L be an odd positive number, and M_Φ, M_Ψ be positive integers such that

$$M_\Phi \geq \max_{i=1,\ldots,n} \left\{ |\phi_i(\tilde{\mathbf{d}})| \;\middle|\; \tilde{\mathbf{d}} \in I_L^n \right\}, \quad M_\Psi \geq \max_{i=1,\ldots,n} \left\{ |\psi_i(\tilde{\mathbf{d}})| \;\middle|\; \tilde{\mathbf{d}} \in I_L^n \right\}. \tag{1}$$

For example, if $\phi_i^{\mathrm{abs}}(\mathbf{x})$ $(i = 1, \ldots, n)$ are polynomials whose coefficients are given by the absolute value of the corresponding coefficients of $\phi_i(\mathbf{x})$, then

$$M_\Phi = \max_{i=1,\ldots,n} \left\{ \phi_i^{\mathrm{abs}} \left(\frac{L-1}{2} \right) \right\}$$

satisfies (1). This is similar for M_Ψ.

Taking a (large) prime number q, we choose positive integers $r_1, \ldots, r_n$ $(< q)$ such that

$$2M_\Phi < \min_{k=1,\ldots,2M_\Psi} \{ |\mathrm{lift}_q(r_i k)| \} \quad (i = 1, \ldots, n) \tag{2}$$

and define $\Lambda_i = \{ \mathrm{lift}_q(r_i k) \mid k = 0, \pm 1, \pm 2, \ldots, \pm M_\Psi \}$. The existence of such r_i relies on q being sufficiently large. In fact, $q > 4M_\Phi M_\Psi$ is necessary. Moreover, $r_i > 2M_\Phi$ is also needed.

From (2), for $i = 1, \ldots, n$, we have

$$|\mathrm{lift}_q(\lambda - \lambda')| > 2M_\Phi \quad (\forall \lambda, \lambda' \in \Lambda_i \ (\lambda \neq \lambda')). \tag{3}$$

In fact, for $\lambda = r_i k, \lambda' = r_i k' \in \Lambda_i$, from $|k - k'| < 2M_\Psi$,

$$|\mathrm{lift}_q(\lambda - \lambda')| = |\mathrm{lift}_q(r_i(k - k'))| = |\mathrm{lift}_q(r_i |k - k'|)| > 2M_\Phi.$$

We define polynomial systems,

$$\Psi_R(\mathbf{x}) = (r_1\psi_1(\mathbf{x}), \ldots, r_n\psi_n(\mathbf{x})) \in \mathbb{Z}[\mathbf{x}]^n.$$
$$G(\mathbf{x}) = (g_1(\mathbf{x}), \ldots, g_n(\mathbf{x})) = (\Phi(\mathbf{x}) + \Psi_R(\mathbf{x})) \bmod q \in \mathbb{F}_q[\mathbf{x}]^n.$$

Then, $G(\mathbf{x})$ can be regarded as a map $G : \mathbb{Z}^n \to \mathbb{F}_q^n$. Regarding the relation between Φ, Ψ and G, we have the following lemma.

Lemma 1. *For $\widetilde{\mathbf{d}} \in I_L^n$, let $\mathbf{c} = (c_1, \ldots, c_n) = G(\widetilde{\mathbf{d}}) \in \mathbb{F}_q^n$. Then, for $i = 1, \ldots, n$, there is a unique $\lambda_i \in \Lambda_i$ such that $|\mathrm{lift}_q(c_i - \lambda_i)| < M_\Phi$. Moreover, when we write $\tilde{a}_i = \mathrm{lift}_q(c_i - \lambda_i)$, $\tilde{b}_i = \mathrm{lift}_q(\lambda_i/r_i \bmod q)$ $(i = 1, \ldots, n)$,*

$$\Phi(\widetilde{\mathbf{d}}) = (\tilde{a}_1, \ldots, \tilde{a}_n), \quad \Psi(\widetilde{\mathbf{d}}) = (\tilde{b}_1, \ldots, \tilde{b}_n).$$

From this lemma, we know for any $\mathbf{c} = (c_1, \ldots, c_n) \in G(I_L^n)(\subset \mathbb{F}_q^n)$, the following holds:

$\widetilde{\mathbf{d}} \in I_L^n$ is a solution of $G(\mathbf{x}) = \mathbf{c}$.
$\Leftrightarrow \widetilde{\mathbf{d}}$ is a solution of the system of (constrained) nonlinear equations with integer coefficients, $\Phi(\mathbf{x}) = (\tilde{a}_1, \ldots, \tilde{a}_n)$, $\Psi(\mathbf{x}) = (\tilde{b}_1, \ldots, \tilde{b}_n)$ appeared in Lemma 1.

From the above, an algorithm for computing $G^{-1}(\mathbf{c}) \in I_L^n$ is obtained as follows.

1. For all $i = 1, \ldots, n$, find $\tilde{b}_i \in \{0, \pm 1, \pm 2, \ldots, \pm M_\Psi\}$ such that $|\mathrm{lift}_q(c_i - r_i\tilde{b}_i)| < M_\Phi$, and set $\tilde{a}_i = \mathrm{lift}_q(c_i - r_i\tilde{b}_i) \in \mathbb{Z}$.
2. Solve the system of constrained nonlinear equations with integer coefficients,

$$\Phi(\mathbf{x}) = (\tilde{a}_1, \ldots, \tilde{a}_n), \ \Psi(\mathbf{x}) = (\tilde{b}_1, \ldots, \tilde{b}_n),$$

and output a solution $\tilde{\mathbf{d}} \in I_L^n$.

3 Encryption Scheme PERN

3.1 Key Generation, Encryption and Decryption

Let E be a finite subset of $(\mathbb{Z}_{\geq 0})^n$. For $\mathbf{e} = (e_1, \ldots, e_n) \in E$, $\mathbf{x}^{\mathbf{e}}$ denotes the monomial $x_1^{e_1} \cdots x_n^{e_n}$. We define

$$\mathbb{Z}[\mathbf{x}]_E := \mathrm{Span}_{\mathbb{Z}}\{\mathbf{x}^{\mathbf{e}} \mid \mathbf{e} \in E\}(\subset \mathbb{Z}[\mathbf{x}]),$$
$$\mathbb{F}_q[\mathbf{x}]_E := \mathrm{Span}_{\mathbb{F}_q}\{\mathbf{x}^{\mathbf{e}} \mid \mathbf{e} \in E\}(\subset \mathbb{F}_q[\mathbf{x}]).$$

$\Phi(\mathbf{x}), \Psi(\mathbf{x})$ appeared in the previous section are chosen as $\Phi(\mathbf{x}), \Psi(\mathbf{x}) \in (\mathbb{Z}[\mathbf{x}]_E)^n$. Then, we construct $G(\mathbf{x})$ in the same way as shown in the previous section.

The new encryption scheme, PERN makes use of $G(\mathbf{x})$ as a trapdoor function. Choose a random affine isomorphism T on $\mathbb{F}_q^n$, then $F(\mathbf{x}) = T \circ G(\mathbf{x})$ is the public key of PERN.

– **Key Generation Algorithm**

Let L, L_G be odd positive integers, n a positive integer, and E a finite subset of $(\mathbb{Z}_{\geq 0})^n$.

1. Randomly choose multivariate polynomial systems $\Phi(\mathbf{x}), \Psi(\mathbf{x}) = (\psi_1(\mathbf{x}), \ldots, \psi_n(\mathbf{x})) \in (\mathbb{Z}[\mathbf{x}]_E)^n$ whose all coefficients belong to I_{L_G}.
2. Compute M_Φ, M_Ψ satisfying (1), and choose an odd prime number q such that $q > 4M_\Phi M_\Psi$.
3. Choose positive integers $(M_\Phi <) r_1, \ldots, r_n (< q)$ such that

$$2M_\Phi < \min_{k=1,\ldots,2M_\Psi} \{|\mathrm{lift}_q(r_i k)|\} \quad (i = 1, \ldots, n).$$

If such $r_1, \ldots, r_n$ can not be found, go back to Step 2 and reselect q.

4. Compute $\Psi_R(\mathbf{x}) = (r_1\psi_1(\mathbf{x}), \ldots, r_n\psi_n(\mathbf{x})) \in (\mathbb{Z}[\mathbf{x}]_E)^n$, and

$$G(\mathbf{x}) = (g_1(\mathbf{x}), \ldots, g_n(\mathbf{x})) = (\Phi(\mathbf{x}) + \Psi_R(\mathbf{x})) \bmod q \in (\mathbb{F}_q[\mathbf{x}]_E)^n.$$

5. Choose an affine isomorphism T on $\mathbb{F}_q^n$.
6. Compute $F(\mathbf{x}) = T \circ G(\mathbf{x}) \in (\mathbb{F}_q[\mathbf{x}]_E)^n$.

The secret key is $\Phi(\mathbf{x}), \Psi(\mathbf{x}), \{r_1, \ldots, r_n\}, T$, and the public key is $F(\mathbf{x})$.

– **Encryption Algorithm**

Let $\mathbf{m} \in I_L^n$ be a plaintext.

1. Compute $\mathbf{c} = F(\mathbf{m}) \in \mathbb{F}_q^n$.

Then, $\mathbf{c}$ is the ciphertext corresponding to $\mathbf{m}$.

– **Decryption Algorithm**

Let $\mathbf{c} \in \mathbb{F}_q^n$ be a ciphertext.

1. Compute $\mathbf{c}' = (c'_1, \ldots, c'_n) = T^{-1}(\mathbf{c})$.
2. For all $i = 1, \ldots, n$, find $\tilde{b}_i \in \{0, \pm 1, \pm 2, \ldots, \pm M_\Psi\}$ satisfying $|\mathrm{lift}_q(c'_i - r_i\tilde{b}_i)| < M_\Phi$ and compute $\tilde{a}_i = \mathrm{lift}_q(c'_i - r_i\tilde{b}_i) \in \mathbb{Z}$.
3. Solve the nonlinear equation system with a box constraint I_L^n,

$$\Phi(\mathbf{x}) = (\tilde{a}_1, \ldots, \tilde{a}_n),\ \Psi(\mathbf{x}) = (\tilde{b}_1, \ldots, \tilde{b}_n).$$

The solution is denoted by $\mathbf{m}' \in I_L^n$.

Then, $\mathbf{m}'$ coincides with the plaintext $\mathbf{m}$.

4 Solving Constrained Nonlinear System with Integer Coefficients

In this section, we consider methods for solving the constrained nonlinear equation system with integer coefficients,

$$\Phi(\mathbf{x}) = (\tilde{a}_1, \ldots, \tilde{a}_n),\ \Psi(\mathbf{x}) = (\tilde{b}_1, \ldots, \tilde{b}_n) \tag{4}$$

appeared in Step 3 of the decryption algorithm. We define $H(\mathbf{x}) : \mathbb{R}^n \to \mathbb{R}^{2n}$ by

$$H(\mathbf{x}) = (h_1(\mathbf{x}), h_2(\mathbf{x}), \ldots, h_{2n}(\mathbf{x})) = (\Phi(\mathbf{x}) - (\tilde{a}_1, \ldots, \tilde{a}_n)) \,\|\, (\Psi(\mathbf{x}) - (\tilde{b}_1, \ldots, \tilde{b}_n)),$$

then the Eq. (4) is equivalent to the equation $H(\mathbf{x}) = \mathbf{0}$.

From the structure of the proposed scheme, we know the plaintext $\mathbf{m}$ is a solution of $H(\mathbf{x}) = \mathbf{0}$.

Let us discuss whether there are other solutions of $H(\mathbf{x}) = \mathbf{0}$ in the definition range $\mathbb{R}^n$ or not. Since the coefficients of $\Phi(\mathbf{x}), \Psi(\mathbf{x})$ are chosen randomly, and by Bézout's theorem, there is a subset S of $\{1, 2, \ldots, 2n\}$ of cardinality n such that the number of the rational points of the variety defined by the ideal $I_S = (h_k(\mathbf{x}) \mid k \in S) \subset \mathbb{R}[\mathbf{x}]$ is less than or equal to $\prod_{k \in S} \deg h_k(\mathbf{x})$ (Bézout's bound). $\mathbf{m}$ is one of such rational points, and the chances of existing other rational points satisfying $h_k(\mathbf{x}) = 0$ for $k \in \{1, 2, \ldots, 2n\} \setminus S$ are really low. In fact, in our actual experiments of 1000 trials with different parameters presented in Table 4, we had always only obtained one rational point. Therefore, we can assume that

$$\text{the system } H(\mathbf{x}) = \mathbf{0} \text{ has only one solution in } \mathbb{R}^n.$$

As explained above, if we obtain a solution of the system $H(\mathbf{x}) = \mathbf{0}$ of unconstrained nonlinear equations with real coefficients, it coincides with the plaintext $\mathbf{m}$. Moreover, from the fact that $\mathbf{m}$ has integer components, if we obtain an approximate solution whose component-wise errors from $\mathbf{m}$ are within less than 0.5, its component-wise rounding to integers becomes the exact solution of the system.

To compute an approximate solution of $H(\mathbf{x}) = \mathbf{0}$, we define

$$\theta(\mathbf{x}) = \frac{1}{2}\|H(\mathbf{x})\|_2^2 = \frac{1}{2}(h_1^2(\mathbf{x}) + h_2^2(\mathbf{x}) + \cdots + h_{2n}^2(\mathbf{x})),$$

and consider the least square problem, i.e. to solve the optimization problem of $\theta(\mathbf{x})$. The line search method is known as a method to solve optimization problems. The line search method uses a point sequence $\mathbf{x}_1, \mathbf{x}_2, \ldots (\in \mathbb{R}^n)$ with a cluster point. $\mathbf{x}_{k+1}$ is given by the previous term $\mathbf{x}_k$ as

$$\mathbf{x}_{k+1} = \mathbf{x}_k + t_k \mathbf{d}_k,$$

where $\mathbf{d}_k (\in \mathbb{R}^n)$ is called a search direction, and $t_k (\in \mathbb{R})$ is called a step size. $\mathbf{d}_k$ is chosen to be a decent direction, i.e. $\mathbf{d}_k$ satisfies

$$(\nabla\theta(\mathbf{x}_k)\,\mathbf{d}_k^{\mathsf{T}}) \;=\; H(\mathbf{x}_k) J_H(\mathbf{x}_k)\,\mathbf{d}_k^{\mathsf{T}} < 0.$$

Here, $J_H(\mathbf{x}_k)$ is the Jacobi matrix $\left(\frac{\partial}{\partial x_j} h_i(\mathbf{x})\right) (\in \mathbb{R}^{2n \times n})$ of $H(\mathbf{x})$. $t_k \in (0, 1)$ is chosen to satisfy the Armijo condition: for an $\alpha \in (0, 1)$,

$$\theta(\mathbf{x}_k + t_k \mathbf{d}_k) - \theta(\mathbf{x}_k) \leq \alpha t_k H(\mathbf{x}_k) J_H(\mathbf{x}_k)\,\mathbf{d}_k^{\mathsf{T}}.$$

Then, the sequence $\{\mathbf{x}_k\}$ is globally convergent to a cluster point $\mathbf{x}^*$, and $\mathbf{x}^*$ becomes a stationary point, i.e. it satisfies

$$\nabla\theta(\mathbf{x}^*) = H(\mathbf{x}^*)J_H(\mathbf{x}^*) = \mathbf{0}. \tag{5}$$

We may assume that the rank of $J_H(\mathbf{x}^*)$ is n, hence the dimension of $\ker J_H(\mathbf{x}^*)$ is n. (5) implies that $H(\mathbf{x}^*) \in \ker J_H(\mathbf{x}^*)$, but does not mean $H(\mathbf{x}^*) = \mathbf{0}$ generally. Accordingly, by reselect a sequence $\{\mathbf{x}_k\}$ over and over again until $H(\mathbf{x}^*) = \mathbf{0}$ is satisfied, we eventually obtain a (approximate) solution of $H(\mathbf{x}) = \mathbf{0}$.

Several methods for selecting a search direction have been proposed, and the difference of those methods results in different properties of convergence and efficiency of solving. In this paper, the following 4 line search methods are considered.

1. Steepest decent method
2. Levenberg-Marquardt method
3. Quasi-Newton method
4. Newton method (for optimization problems)

In the steepest decent method, the search direction is chosen by $\mathbf{d}_k = -\nabla\theta(\mathbf{x}_k)$, and in the Levenberg-Marquardt Method,

$$\mathbf{d}_k = -\nabla\theta(\mathbf{x}_k)(J_H(\mathbf{x}_k)^{\mathsf{T}}J_H(\mathbf{x}_k) + w_k I_n)^{-1}.$$

Here, $w_1, w_2, \ldots$ are a sequence of non-negative real numbers converging to 0, and have the effect of making $J_H(\mathbf{x}_k)^{\mathsf{T}}J_H(\mathbf{x}_k) + w_k I_n$ a positive definite symmetric matrix. Now, because $J_H(\mathbf{x}_k)$ is a $(2n, n)$-matrix, we can assume that $J_H(\mathbf{x}_k)^{\mathsf{T}}J_H(\mathbf{x}_k)$ is always a positive definite symmetric matrix, therefore we can take $w_k = 0$. In the quasi-Newton method, a sequence $\{B_k\}$ of matrices are used,

$$\mathbf{d}_k = -\nabla\theta(\mathbf{x}_k)B_k.$$

B_{k+1} is defined by the BFGS update,

$$B_{k+1} = B_k - \frac{\mathbf{s}_k^{\mathsf{T}}\mathbf{y}_k B_k + (\mathbf{y}_k B_k)^{\mathsf{T}}\mathbf{s}_k}{(\mathbf{s}_k, \mathbf{y}_k)} + \left(1 + \frac{(\mathbf{y}_k, B_k\mathbf{y}_k)}{(\mathbf{s}_k, \mathbf{y}_k)}\right)\frac{\mathbf{s}_k^{\mathsf{T}}\mathbf{s}_k}{(\mathbf{s}_k, \mathbf{y}_k)}.$$

Here, $\mathbf{s}_k = \mathbf{x}_{k+1} - \mathbf{x}_k$, $\mathbf{y}_k = \nabla\theta(\mathbf{x}_{k+1}) - \nabla\theta(\mathbf{x}_k)$, and $(\,\cdot\,,\,\cdot\,)$ denotes the usual inner form. B_1 is defined by $(J_H(\mathbf{x}_1)^{\mathsf{T}}J_H(\mathbf{x}_1))^{-1}$. In the Newton method (for optimization problems), we take $\mathbf{d}_k = -\nabla\theta(\mathbf{x}_k)(\nabla^2\theta(\mathbf{x}_k))^{-1}$ where $\nabla^2\theta(\mathbf{x})$ is the Hessian matrix of $\theta(\mathbf{x})$.

For the steepest decent method, the Levenberg-Marquardt method and quasi-Newton method, it is known that $\mathbf{d}_k$ is a decent direction. For the Newton method, generally, $\mathbf{d}_k$ is not a decent direction, but we have checked that it is a decent direction in our experiment. Table 2 compares the performance of 4 line search methods. $H(\mathbf{x})$ consists of quadratic polynomials and all solutions are contained in $[-5, 5] \cap \mathbb{Z} = I_{11}$. We experimented 1,000 times for

$n = 30, 40, 50$ with each method. In the table, "time" represents the average time (unit: milli seconds) of solving, "♯ seq" represents the average number of sequences up to reaching the solution $\mathbf{m}$, and "♯ terms" represents the average number of the terms up to reaching a stationary point $\mathbf{x}^*$ for a sequence. Table 2 shows remarkable feature of each method, and overall, the most efficient solving algorithm is the Levenberg-Marquardt method, so that we adopted the Levenberg-Marquardt method in the decryption of the proposed scheme. The algorithm of the Levenberg-Marquardt method is as follows. $\|\cdot\|_\infty$ represents the maximum of the absolute values of the components of a vector, and (2-6) judges whether a sequence gets close enough to a stationary point or not. $\mathrm{round}(\mathbf{x}_0)$ represents the component-wise rounding $\mathbf{x}_0$ to integers.

Table 2. Comparison of algorithms for solving $H(\mathbf{x}) = \mathbf{0}$

Method	$n = 30$			$n = 40$			$n = 50$		
	Time (ms)	♯ seq	♯ terms	Time (ms)	♯ seq	♯ terms	Time (ms)	♯ seq	♯ terms
SD	170.07	**1.75**	80.70	426.95	**1.72**	84.92	1202.48	**1.79**	91.51
L-M	**4.12**	2.03	14.15	**10.87**	2.16	15.83	**25.36**	2.12	17.58
Q-N	23.01	2.09	48.70	75.25	1.99	60.27	232.19	2.13	68.10
Newton	553.28	126.76	**6.41**	2005.96	198.57	**6.93**	6068.22	248.05	**7.39**

Levenberg-Marquardt Method

[Input] $H(\mathbf{x})$, an odd number $L \in \mathbb{Z}_{>0}$, $\alpha, \beta, \gamma \in (0, 1)$.
[Output] A (constrained) solution of $H(\mathbf{x}) = \mathbf{0}$ with integer components.

1. Choose $\mathbf{x}_0 \in [-(L-1)/2, (L-1)/2]^n$ in the range of real numbers randomly.
2. Repeat (2-1)–(2-6):
   - 2-1. Compute $\mathbf{e} = -H(\mathbf{x}_0)J_H(\mathbf{x}_0)$.
   - 2-2. Compute $S = J_H(\mathbf{x}_0)^\mathsf{T} J_H(\mathbf{x}_0)$.
   - 2-3. Solve the linear equation $\mathbf{x}\, S = \mathbf{e}$, its solution is denoted by $\mathbf{d}_0$.
   - 2-4. Compute the minimal non-negative integer l satisfying the following condition, and set $t_0 = \beta^l$:

$$\theta(\mathbf{x}_0 + \beta^l \mathbf{d}_0) - \theta(\mathbf{x}_0) \leq -\alpha\beta^l \mathbf{e}\, \mathbf{d}_0^\mathsf{T}.$$

   - 2-5. $\mathbf{x}_0 \leftarrow \mathbf{x}_0 + t_0\mathbf{d}_0$.
   - 2-6. If $\|t_0\mathbf{d}_0\|_\infty < \gamma$ then finish the loop, and move to 3.
3. $\tilde{\mathbf{x}}_0 \leftarrow \mathrm{round}(\mathbf{x}_0)$.
4. If $H(\tilde{\mathbf{x}}_0) = \mathbf{0}$ then output $\tilde{\mathbf{x}}_0$, otherwise go back to 1.

The algorithms of the steepest decent method, quasi-Newton method and Newton method are described in the appendix.

Remark 1. The 4 methods explained as above have the only difference of taking the search direction $\mathbf{d}_k$, and other parts is common. In these methods, for any $\mathbf{x}_k$, $H(\mathbf{x}_k + \mathbf{d})$ is approximated by quadratic polynomials

$$m_{\mathbf{x}_k}(\mathbf{d}) = H(\mathbf{x}_0) + \mathbf{d}\,\nabla H(\mathbf{x}_k) + \frac{1}{2}\mathbf{d}\, A_k \mathbf{d}^\mathsf{T} \quad (A_k \in \mathbb{R}^{n\times n}),$$

$\mathbf{d}_k$ is chosen by the solution $\mathbf{d}$ of the (unconstrained) optimization problem of $m_{\mathbf{x}_k}(\mathbf{d})$. For the steepest decent method, $A_k = I_n$ is taken, for the Levenberg-Marquardt method, $A_k = J_H(\mathbf{x}_0)^{\mathsf{T}} J_H(\mathbf{x}_0)$, for the quasi-Newton method, $A_k = B_k^{-1}$, for Newton method, $A_k = \nabla^2\theta(\mathbf{x}_k)$ are taken, respectively.

5 Security Analysis of the Proposed Scheme

The security of the proposed scheme is mainly based on the difficulty of solving the constrained MP problem.

> **Constrained MP problem:** For positive integers m, n, L, let $\mathcal{F}(\mathbf{x})$ be a polynomial system which consists of m polynomials over $\mathbb{F}_q$ in variables $\mathbf{x} = (x_1, \ldots, x_n)$. Then, find $\mathbf{x}_0 \in I_L^n$ such that $\mathcal{F}(\mathbf{x}_0) = \mathbf{0}$.

In this section, fixing a ciphertext $\mathbf{c} \in \mathbb{F}_q^n$, we consider a polynomial system $\mathcal{F}(\mathbf{x}) = F(\mathbf{x}) - \mathbf{c}$ for a public key $F(\mathbf{x})$ constructed by the proposed scheme. With this $\mathcal{F}(\mathbf{x})$, by solving the constrained MP problem, the plaintext corresponding to $\mathbf{c}$ is obtained.

5.1 Constrained MP Problem

For $\mathcal{F}(\mathbf{x}) = (\hat{f}_1(\mathbf{x}), \ldots, \hat{f}_n(\mathbf{x}))$, each component $\hat{f}_i(\mathbf{x})$ has $s = \sharp E$ monomials. (If E does not include the constant term, $s = \sharp E + 1$.) Determining an order of these monomials, a vector $\mathbf{a}_i \in \mathbb{Z}^s$ is defined as the vector of coefficients lifted to integers from the coefficients of $\hat{f}_i(\mathbf{x})$. The q-ary lattice generated by $\mathbf{a}_1, \ldots, \mathbf{a}_n$ is denoted by $\mathcal{A}$. We assume that by solving the Shortest Independent Vector Problem (SIVP) for $\mathcal{A}$, n linearly independent short vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^s$ in $\mathcal{A}$ are obtained. The polynomial over $\mathbb{Z}$ corresponding to the vector $\mathbf{b}_i$ is denoted by $\hat{h}_i(\mathbf{x})$, and let $\mathcal{H}(\mathbf{x}) = (\hat{h}_1(\mathbf{x}), \ldots, \hat{h}_n(\mathbf{x}))$. Then, the problem solving the equation $\mathcal{F}(\mathbf{x}) = \mathbf{0}$ is reduced to the problem solving the equation $\mathcal{H}(\mathbf{x}) \equiv \mathbf{0} \bmod q$. Here, let us assume that for a solution $\mathbf{x}_0$ of the constrained MP problem,

$$|\hat{h}_i(\mathbf{x}_0)| < \frac{q-1}{2} \quad (i = 1, \ldots, n) \tag{6}$$

is satisfied. Beware that $\mathbf{x}_0$ is not only a solution of $\mathcal{H}(\mathbf{x}) \equiv \mathbf{0} \bmod q$, but also a solution of the equation over $\mathbb{Z}$, $\mathcal{H}(\mathbf{x}) = 0$. Therefore, $\mathbf{x}_0$ can be obtained by solving the equation over $\mathbb{Z}$. Solving the equation $\mathcal{H}(\mathbf{x}) = 0$ is efficiently carried out by combining techniques to solve approximately nonlinear equations over the real numbers with the fact that $\mathbf{x}_0$ has integer components. The approximate solution of $\mathcal{H}(\mathbf{x}) = 0$ can be obtained by, for example, the solving method of the (constrained) optimization problem (least square problem) of the function $\|\mathcal{H}(\mathbf{x})\|_2^2$ where $\|\cdot\|_2$ is the usual Euclid norm [5,25].

First, let us consider the possibility that $\mathcal{H}(\mathbf{x})$ satisfies (6) for a general constrained MP problem. Since $\mathrm{vol}(\mathcal{A}) = q^{s-n}$, by the Gaussian heuristic [24], it is expected that

$$\|\mathbf{b}_i\|_2 \approx \sqrt{\frac{s}{2\pi e}} q^{1-\frac{n}{s}} \quad (i = 1, \ldots, n).$$

Here, e is Napier's constant. Simply, assuming that $\sqrt{\frac{s}{2\pi e}}$ components of $\mathbf{b}_i$ are close to q, the probability satisfying (6) is negligible if s is sufficiently large.

Next, consider the case of the constrained MP problem obtained by the proposed scheme. $\Phi(\mathbf{x}), \Psi(\mathbf{x})$ have small coefficients, but, the distribution of $r_1, \ldots, r_n$ is close to the uniformly distribution on $[2M_\Phi, q - 2M_\Phi - 1]$. Therefore, taking account of the definition of $G(\mathbf{x})$, any coefficient of components of $G(\mathbf{x})$ behaves as chosen randomly in $[M_\Phi, q - M_\Phi - 1]$. Since M_Φ is small enough compared to q, similarly for general constrained MP problem, the probability satisfying (6) must be negligible. The above argument implies that the part $\Psi_R(\mathbf{x})$ is indispensable in the definition of $G(\mathbf{x})$.

5.2 Attack Against Inhomogeneous SIS Problem

For $\mathbf{e} \in E$, $v_\mathbf{e}$ denotes the row vector enumerating the coefficients with respect to $\mathbf{x}^\mathbf{e}$ of components of $F(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_n(\mathbf{x}))$. Taking an order on E, a matrix $A \in \mathbb{F}_q^{n \times \sharp E}$ is defined by the matrix enumerating the column vector $v_\mathbf{e}$ ($\mathbf{e} \in E$). Then, for a solution $\mathbf{x}_0 \in I_L^n$ of the constrained MP problem, $\mathbf{w}_0 = (\mathbf{x}_0^\mathbf{e})_{\mathbf{e} \in E} \in \mathbb{Z}^{\sharp E}$ is a solution of the linear equation,

$$A\mathbf{w} = \mathbf{c}, \tag{7}$$

and $\mathbf{w}_0$ has a considerably smaller Euclid norm among solutions of the linear equation. This means that $\mathbf{w}_0$ is a solution of the inhomogeneous SIS problem obtained from (7). Therefore, we can consider the attack as follows: First, we gather solutions of the inhomogeneous SIS problem obtained from (7). Next, we search $\mathbf{w}_0$ in the set of the solutions. The inhomogeneous SIS problem is changed to the SVP for a lattice $\mathcal{B}$ of dimension $\sharp E + 1$ (or $\sharp E$), where the co-volume of $\mathcal{B}$, $\mathrm{vol}(\mathcal{B}) = q^n$.

Theorem 1 ([15]). *For an m-dimensional lattice $\mathcal{L}$, we define*

$$N_\mathcal{L}(r) = \sharp\{v \in \mathcal{L} \mid \|v\|_2 \leq r\}.$$

If $m \geq 5$, then we have

$$N_\mathcal{L}(r) = \frac{V_m}{\mathrm{vol}(\mathcal{L})} r^m + \mathcal{O}(r^{m-2}).$$

Here, V_m is the volume of the unit sphere of $\mathbb{R}^m$.

From this theorem, the number of elements of $\mathcal{B}$ whose Euclid norm is almost same as r is close to

$$\frac{d}{dr}\left(\frac{V_m}{\mathrm{vol}(\mathcal{L})} r^m\right) \cdot 1 = \frac{m\, V_m}{\mathrm{vol}(\mathcal{L})} r^{m-1}.$$

Going back to our setting, the number of elements of $\mathcal{B}$ whose Euclid norm is almost same as $\|\mathbf{w}_0\|_2$ is about

$$\frac{b\,V_b\,\|\mathbf{w}_0\|_2^{b-1}}{q^n} = \frac{\pi^{\frac{b}{2}}\,b\,\|\mathbf{w}_0\|_2^{b-1}}{\Gamma(\frac{b}{2}+1)\,q^n} \approx \left(\frac{2\pi e}{b}\right)^{\frac{b}{2}} \frac{b\,\|\mathbf{w}_0\|_2^{b-1}}{\sqrt{b\pi}\,q^n} \quad (b = \dim\mathcal{B} = \sharp E + 1 \text{ or } \sharp E).$$

Since the solution of the constrained MP problem is unique, the complexity of the attack is the same as this value. Moreover, if a large scale quantum computer is available, the complexity is the 1/2-th power of this value by the Grover's algorithm.

5.3 Key Recovery Attack

Once the linear transformation part of the affine transformation T is known, $G(\mathbf{x})$ is also known from the public key, and $r_1, \ldots, r_n$, $\Phi(\mathbf{x}), \Psi(\mathbf{x})$ can be computed easily from $G(\mathbf{x})$, thus, the secret information which is necessary for decryption is obtained entirely. Therefore, let us consider an attack discovering the linear transformation part T_1 of T.

An adversary who knows r_j for some j can compute the j-th row vector of T_1^{-1} by the following procedure.

1. Choose an integer t such that $n < t \leq \sharp E$, and choose a (ordered) subset M of E with cardinality t.
2. For $F(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_n(\mathbf{x}))$ and $i = 1, \ldots, n$, compute a vector $\mathbf{a}_i \in \mathbb{Z}^t$ of coefficients lifted to integers from coefficients of $f_i(\mathbf{x})$ with respect to M. The q-ary lattice of $\mathbb{Z}^t$ generated by $\mathbf{a}_1, \ldots, \mathbf{a}_n$ is denoted by $\mathcal{A}$.
3. Choose $\mathbf{b} = (b_1, \ldots, b_s) \in I_{L_G}^t$ randomly.
4. Compute the vector $\mathbf{a}$ in $\mathcal{A}$ closest to $r_j\mathbf{b}$. If $\|r_j\mathbf{b} - \mathbf{a}\|_\infty < L/2$ is satisfied, output the coefficient vector $(c_1, \ldots, c_n)$ of the linear combination $\mathbf{a} = c_1\mathbf{a}_1 + \cdots + c_n\mathbf{a}_n$, and terminate. Otherwise, go back to Step 3.

Since $\mathbf{b}$ satisfying the inequality in Step 4 exists uniquely, even if the cost for searching the closest vector is estimated as 1, the complexity of the above algorithm becomes $\mathcal{O}(L_G^t)$, which in particular, is larger than $\mathcal{O}(L_G^n)$.

Moreover, the above attack can exchange the roll of $\Phi(\mathbf{x})$ and $\Psi(\mathbf{x})$. Namely, if the above algorithm is changed by $r_i \to 1/r_i$, it works as an attack. The complexity of this attack is also $\mathcal{O}(L_G^t)(> \mathcal{O}(L_G^n))$. If the Grover's algorithm is available, the complexity is $\mathcal{O}(L_G^{\frac{t}{2}})(> \mathcal{O}(L_G^{\frac{n}{2}}))$.

5.4 Exhaustive Search

For a ciphertext $\mathbf{c}$, the complexity of finding the solution of $F(\mathbf{x}) = \mathbf{c}$ by the exhaustive search is $\mathcal{O}(L^n)$. In the case of using the Grover's algorithm, the complexity is $\mathcal{O}(L^{\frac{n}{2}})$.

5.5 Algebraic Attack

The algebraic attack uses algebraic equation solver like XL [36] and Gröbner basis technique [12,13] for solving the usual MP problem. The complexity of the algebraic attack is estimated by the complexity of the hybrid approach [1] of computing a Gröbner basis and exhaustive search. In the process of exhaustive search in [1], all elements in a finite field are substituted for several variables, but, in the proposed scheme, the finite field must be changed into I_L. A solution $\mathbf{x}_0$ of $\mathcal{F} = (\hat{f}_1(\mathbf{x}), \ldots, \hat{f}_n(\mathbf{x})) = \mathbf{0}$ in I_L^n is also a zero point of

$$\hat{g}_j(\mathbf{x}) = \prod_{-\frac{L-1}{2} \le a \le \frac{L-1}{2}} (x_j - a) \qquad (j = 1, 2, \ldots, n). \tag{8}$$

Therefore, the ideal we should consider is

$$I = \langle \hat{f}_1(\mathbf{x}), \ldots, \hat{f}_n(\mathbf{x}), \hat{g}_1(\mathbf{x}), \ldots, \hat{g}_n(\mathbf{x}) \rangle.$$

For $k = 0, 1, \ldots, n$, we randomly choose $(v_{n-k+1}, v_{n-k+2}, \ldots, v_n) \in {I_p}^k$. We denote the polynomial system in $n-k$ variables obtained by substituting $(x_{n-k+1}, \ldots, x_n) = (v_{n-k+1}, \ldots, v_n)$ for $\mathcal{F}(\mathbf{x})$ by $\mathcal{F}_k(\mathbf{x}^{(k)})$. Here, $\mathbf{x}^{(k)} = (x_1, \ldots, x_{n-k})$. Note that $\mathcal{F}_0(\mathbf{x}^{(0)})$ is the same as $\mathcal{F}(\mathbf{x})$.

For $\mathcal{F}_k(\mathbf{x}^{(k)}) = (\hat{f}_1(\mathbf{x}^{(k)}), \ldots, \hat{f}_n(\mathbf{x}^{(k)}))$, the homogeneous part of $\hat{f}_i(\mathbf{x}^{(k)})$ of the maximal degree $(i = 1, \ldots, n)$ is denoted by $\hat{f}_i^h(\mathbf{x}^{(k)})$, and the homogeneous ideal $J^{(k)}$ of $\mathbb{F}_q[\mathbf{x}^{(k)}]$ is defined by

$$J^{(k)} = \langle \hat{f}_1^h(\mathbf{x}^{(k)}), \ldots, \hat{f}_n^h(\mathbf{x}^{(k)}) \rangle.$$

For $d \ge 0$, let $\mathbb{F}_q[\mathbf{x}^{(k)}]_d$ denote the subspace of $\mathbb{F}_q[\mathbf{x}^{(k)}]$ consisting of homogeneous polynomials of degree d, and $J_d^{(k)} = J^{(k)} \cap \mathbb{F}_q[\mathbf{x}^{(k)}]_d$. The Hilbert series of the quotient ring $\mathbb{F}_q[\mathbf{x}^{(k)}]/J^{(k)}$ is defined by

$$\mathrm{HS}_{\mathbb{F}_q[\mathbf{x}^{(k)}]/J^{(k)}}(t) = \sum_{d=0}^{\infty} \dim_{\mathbb{F}_q}(\mathbb{F}_q[\mathbf{x}^{(k)}]_d / J_d^{(k)})\, t^d \in \mathbb{Z}[[t]].$$

If the Krull-dimension of $J^{(k)}$ is zero, $\mathrm{HS}_{\mathbb{F}_q[\mathbf{x}^{(k)}]/J^{(k)}}(t)$ becomes a polynomial. Then, the degree of regularity, $d_{\mathrm{reg}}(k)$ is defined by $d_{\mathrm{reg}}(k) = \deg(\mathrm{HS}_{\mathbb{F}_q[\mathbf{x}^{(k)}]/J^{(k)}}(t)) + 1$. For any $S(t) \in \mathbb{Z}[[t]]$, the power series obtained by truncating $S(t)$ at its first non positive coefficient is denoted by $[S(t)]_+ \in \mathbb{Z}_{>0}[[t]]$. If

$$\mathrm{HS}_{\mathbb{F}_q[\mathbf{x}^{(k)}]/J^{(k)}}(t) = \left[\frac{(1-t^L)^{n-k} \prod_{i=1}^{n} (1-t^{d_i})}{(1-t)^{n-k}} \right]_+ \tag{9}$$

is satisfied, it is said that $\mathcal{F}_k(\mathbf{x}^{(k)})$ is semi-regular. Here, d_i is the total degree of $\hat{f}_i(\mathbf{x})$.

Remark 2. Taking the result in [35] into consideration, for most of random systems, the right hand side of (9) may seem to be equal to

$$\left[\frac{(1-t^L)^{n-k}\cdot\prod_{i=1}^{n}(1-t^{d_i})}{(1-t)^{n-k}\cdot(1-t^{d_iL})^n}\right]_+,$$

but, actually, the part $(1-t^{d_iL})^n$ is not needed. This is because, different from the case of the usual MP problem considered in [35], in the constrained MP problem, $f_i(\mathbf{x})^L - f_i(\mathbf{x}) = 0$ $(i = 1, 2, \ldots, n)$ (or this analogue) does not hold.

The complexity of the Gröbner basis computation for $J^{(k)}$ is described by

$$\mathcal{O}\left(\binom{n-k+d_{\mathrm{reg}}(k)-1}{d_{\mathrm{reg}}(k)}^{\omega}\right). \tag{10}$$

Here, $2 \leq \omega \leq 3$ is the linear algebra constant of solving a linear system. From (10), the complexity of the hybrid attack is described as follows [1]:

$$\min_{0\leq k\leq n}\mathcal{O}\left(L^k\binom{n-k+d_{\mathrm{reg}}(k)-1}{d_{\mathrm{reg}}(k)}^{\omega}\right). \tag{11}$$

If the Grover's algorithm is used for searching elements for substitution, the complexity is changed to

$$\min_{0\leq k\leq n}\mathcal{O}\left(L^{\frac{k}{2}}\binom{n-k+d_{\mathrm{reg}}(k)-1}{d_{\mathrm{reg}}(k)}^{\omega}\right). \tag{12}$$

From randomness of the coefficients of $\Phi(\mathbf{x}), \Psi(\mathbf{x})$, and taking Fröberg conjecture [14] into consideration, it is expected that $J^{(k)}$ is semi-regular. In fact, for $n = 3, 4, \ldots, 15$, we confirmed that $J^{(k)}$ is semi-regular experimentally. Our experiment used Magma. Based on the experiment result, we assume that any $\mathcal{F}_k(\mathbf{x}^{(k)})$ is semi-regular (in particular, for estimation of security parameters).

Remark 3. In the case of that $\mathcal{F}_k(\mathbf{x}^{(k)})$ is semi-regular, the degree of regularity can be computed by using (9). Moreover, in this case, it is expected that the first fall degree $d_{\mathrm{FF}}(k)$ [10] coincides with the degree of regularity. In general, the complexity of the Gröbner basis computation for $J^{(k)}$ is also expressed by

$$\mathcal{O}\left(\binom{n-k+d_{\mathrm{FF}}(k)-1}{d_{\mathrm{FF}}(k)}^{\omega}\right). \tag{13}$$

If $d_{\mathrm{reg}}(k) = d_{\mathrm{FF}}(k)$, the complexity (13) is equal to the complexity (10). Therefore, in the estimation of security parameters, we use the complexity (11), (12) with $\omega = 2$.

Remark 4. In the security analysis of the *pq*-method in [37], the algebraic attack does not consider the polynomial (8) as one of generators of an ideal, but, this polynomial should be considered.

6 Security Parameters and Implementation

As a set of monomials E used to design the proposed scheme, we take $E = E_{\leq 2} = \{\mathbf{e} \in (\mathbb{Z}_{\geq 0})^n \mid \deg \mathbf{e} \leq 2\}$. Here, $\deg(e_1, \ldots, e_n) = \sum_{i=1}^{n} e_i$, i.e. $E_{\leq 2}$ corresponds to the whole monomials of degree less than or equal to 2. Table 3 shows the security parameters of (n, L, L_G) estimated based on the security analysis in Sect. 5. Secure parameters are estimated considering attacks on classical computers and quantum computers.

Table 3. Security parameter (n, L, L_G)

Security level	Classical attack only	Quantum attack
128 bits	$(65, 7, 5)$	$(80, 15, 11)$
192 bits	$(100, 7, 5)$	$(122, 15, 9)$
256 bits	$(135, 7, 5)$	$(166, 15, 9)$

Tables 4 and 5 show performance result of PERN with an implementation using Intel Core i7-6700, 3.4 GHz. Our implementation used C++ programming language with g++ compiler. $|q|_2$ represents the average of the bit length of q. Key gen., enc. and dec. represent the average time of key generation, encryption and decryption (unit: milli seconds). And SK and PK represent the secret key length and public key length (unit: kilobytes). $\|\mathbf{w}_0\|_2$ represents the minimal integer of $\|\mathbf{w}_0\|_2$ appeared in the analysis in Sect. 5.2 to maintain the corresponding security level. Moreover, in Table 5, $\|\mathbf{w}_0\|_2$ is estimated considering the Grover's algorithm.

Table 4. Performance of PERN with parameters for classical attacks)

(n, L, L_G)	Level	$\|q\|_2$	Key gen. (ms)	Enc. (ms)	Dec. (ms)	SK (kB)	PK (kB)	$\|\mathbf{w}_0\|_2$
(65, 7, 5)	128	31.58	44.62	0.24	56.03	125	575	23
(100, 7, 5)	192	34.01	225.01	1.01	285.01	429	2,189	29
(135, 7, 5)	256	35.71	843.73	3.51	914.06	1,026	5,659	35

6.1 Implementation for Higher Degrees

For non-negative integers a, b, we define $E_{a,b} = \{a\,\mathbf{e}_i + b\,\mathbf{e}_j \in (\mathbb{Z}_{\geq 0})^n \mid 1 \leq i, j \leq n\}$ where $\mathbf{e}_i$ is the i-th fundamental vector. We implemented the PERN with $E' = E_{2,1} \sqcup E_{\leq 2}$ and $E'' = E_{3,1} \sqcup E_{\leq 2}$ as E. The case of E' uses cubic polynomials, and the case of E'' uses quartic polynomials. For the fixed parameter (n, L, L_G), it is expected that the PERN with E' or E'' is more secure than the PERN with $E_{\leq 2}$, but whether this is true or not is a future study issue, a performance comparison of PERN for $E = 2, E', E''$ under $(n, L, LG) = (65, 7, 5)$ is shown in Table 6.

Table 5. Performance of PERN (with parameters for quantum attacks)

(n, L, L_G)	Level	$\|q\|_2$	Key gen. (ms)	Enc. (ms)	Dec. (ms)	SK (kB)	PK (kB)	$\|\mathbf{w}_0\|_2$
(80, 15, 11)	128	39.99	477.53	0.71	185.18	298	1,328	30
(122, 15, 9)	192	41.79	1499.66	1.87	828.81	1,009	4,884	35
(166, 15, 9)	256	43.55	4369.40	6.47	2526.77	2,481	12,807	43

Table 6. Comparison of PERN for $E_{\leq 2}$, E', E'' ($(n, L, L_G) = (65, 7, 5)$)

E	Level	$\|q\|_2$	Key gen. (ms)	Enc. (ms)	Dec. (ms)	SK(kB)	PK(kB)
$E_{\leq 2}$	128	31.58	44.62	0.24	56.03	125	575
E'	-	37.27	237.29	0.54	302.83	128	665
E''	-	41.33	404.61	0.76	529.17	130	737

7 Conclusion

We proposed an encryption scheme called PERN whose security was mainly based on the constrained MP problem. The proposed scheme is flexible to use multivariate polynomials of any degree in its public key. And this public key polynomial system is semi-regular, which indicates the proposed scheme is strong against the algebraic attack.

For inverting the central polynomial map during the decryption process of the proposed scheme, methods for solving nonlinear equations over the real numbers are used, which is used for the first time in MPKC. In this paper, the line search method is used as a solving method for nonlinear equations. However, for solving unconstrained nonlinear equations, there are several solving techniques such as the trust region method [7,11,19–21,34,38]. Moreover, the solving method for constrained nonlinear equations can be related to the decryption of the proposed scheme, and in particular, for the case of the box constraint as I_L^n, there are many research results [2,3,17,18,23,28,32,33]. We, therefore, would like to work on efficient algorithms for solving nonlinear equations from now on to improve the decryption efficiency of the proposed scheme.

Acknowledgement. This work was supported by JSPS Grant-in-Aid for Scientific Research(C) with KAKENHI Grant Number JP17K00197, JSPS Grand-in-Aid for JSPS Fellows with KAKENHI Grant Number JP18J20866 and JST CREST Grant Number JPMJCR14D6.

A Solving Algorithms of Nonlinear Equations Except For the Levenberg-Marquardt Method

Steepest Decent Method

[Input] $H(\mathbf{x})$, an odd number $L \in \mathbb{Z}_{>0}$, $\alpha, \beta, \gamma \in (0,1)$.
[Output] A (constrained) solution of $H(\mathbf{x}) = \mathbf{0}$ with integer components.

1. Choose $\mathbf{x}_0 \in [-(L-1)/2, (L-1)/2]^n$ in the range of real numbers randomly.
2. Repeat (2-1)–(2-4):
   - 2-1. Compute $\mathbf{d}_0 = -H(\mathbf{x}_0) J_H(\mathbf{x}_0)$.
   - 2-2. Compute the minimal non-negative integer l satisfying the following condition, and set $t_0 = \beta^l$.

$$\theta(\mathbf{x}_0 + \beta^l \mathbf{d}_0) - \theta(\mathbf{x}_0) \leq -\alpha \beta^l \|\mathbf{d}_0\|_2^2.$$

   - 2-3. $\mathbf{x}_0 \leftarrow \mathbf{x}_0 + t_0 \mathbf{d}_0$.
   - 2-4. If $\|t_0 \mathbf{d}_0\|_\infty < \gamma$ then finish the loop, and move to 3.
3. $\tilde{\mathbf{x}}_0 \leftarrow \mathrm{round}(\mathbf{x}_0)$.
4. If $H(\tilde{\mathbf{x}}_0) = \mathbf{0}$ then output $\tilde{\mathbf{x}}_0$, otherwise go back to 1.

Quasi-Newton Method

[Input] $H(\mathbf{x})$, an odd number $L \in \mathbb{Z}_{>0}$, $\alpha, \beta, \gamma \in (0,1)$.
[Output] A (constrained) solution of $H(\mathbf{x}) = \mathbf{0}$ with integer components.

1. Choose $\mathbf{x}_0 \in [-(L-1)/2, (L-1)/2]^n$ in the range of real numbers randomly.
2. Compute $\mathbf{e}_1 = -H(\mathbf{x}_0) J_H(\mathbf{x}_0)$.
3. Compute $B = (J_H(\mathbf{x}_0)^\mathsf{T} J_H(\mathbf{x}_0))^{-1}$.
4. Repeat (4-1)–(4-8):
   - 4-1. Compute $\mathbf{d}_0 = \mathbf{e}_1 B$.
   - 4-2. Compute the minimal non-negative integer l satisfying the following condition, and set $t_0 = \beta^l$.

$$\theta(\mathbf{x}_0 + \beta^l \mathbf{d}_0) - \theta(\mathbf{x}_0) \leq -\alpha \beta^l \mathbf{e}_1 \mathbf{d}_0^\mathsf{T}.$$

   - 4-3. $\mathbf{s}_0 = t_0 \mathbf{d}_0$, $\mathbf{x}_0 \leftarrow \mathbf{x}_0 + \mathbf{s}_0$.
   - 4-4. If $\|\mathbf{s}_0\|_\infty < \gamma$ then finish the loop, and move to 5.
   - 4-5. $\mathbf{e}_2 \leftarrow \mathbf{e}_1$.
   - 4-6. Compute $\mathbf{e}_1 = -H(\mathbf{x}_0) J_H(\mathbf{x}_0)$.
   - 4-7. $\mathbf{y}_0 = \mathbf{e}_1 - \mathbf{e}_2$.
   - 4-8. $B \leftarrow B - \frac{\mathbf{s}_0^\mathsf{T} \cdot \mathbf{y}_0 B + (\mathbf{y}_0 B)^\mathsf{T} \cdot \mathbf{s}_0}{(\mathbf{s}_0, \mathbf{y}_0)} + \left(1 + \frac{(\mathbf{y}_0, B\mathbf{y}_0)}{(\mathbf{s}_0, \mathbf{y}_0)}\right) \frac{\mathbf{s}_0^\mathsf{T} \cdot \mathbf{s}_0}{(\mathbf{s}_0, \mathbf{y}_0)}$.
5. $\tilde{\mathbf{x}}_0 \leftarrow \mathrm{round}(\mathbf{x}_0)$.
6. If $H(\tilde{\mathbf{x}}_0) = \mathbf{0}$ then output $\tilde{\mathbf{x}}_0$, otherwise go back to 1.

Newton Method

[Input] $H(\mathbf{x})$, an odd number $L \in \mathbb{Z}_{>0}$, $\alpha, \beta, \gamma \in (0,1)$.
[Output] A (constrained) solution of $H(\mathbf{x}) = \mathbf{0}$ with integer components.

1. Choose $\mathbf{x}_0 \in [-(L-1)/2, (L-1)/2]^n$ in the range of real numbers randomly.
2. Repeat (2-1)–(2-6):
   - 2-1. Compute $\mathbf{e} = -H(\mathbf{x}_0)J_H(\mathbf{x}_0)$.
   - 2-2. Compute the Hessian matrix $S = \nabla^2\theta(\mathbf{x}_0)$.
   - 2-3. Solve the linear equation $\mathbf{x}\,S = \mathbf{e}$ in the range of real numbers, its solution is denoted by $\mathbf{d}_0$.
   - 2-4. Compute the minimal non-negative integer l satisfying the following condition, and set $t_0 = \beta^l$.

$$\theta(\mathbf{x}_0 + \beta^l \mathbf{d}_0) - \theta(\mathbf{x}_0) \leq -\alpha\beta^l \mathbf{e}\,\mathbf{d}_0^{\mathsf{T}}.$$

   - 2-5. $\mathbf{x}_0 \leftarrow \mathbf{x}_0 + t_0\mathbf{d}_0$.
   - 2-6. If $\|t_0\mathbf{d}_0\|_\infty < \gamma$ then finish the loop, and move to 3.
3. $\tilde{\mathbf{x}}_0 \leftarrow \mathrm{round}(\mathbf{x}_0)$.
4. If $H(\tilde{\mathbf{x}}_0) = \mathbf{0}$ then output $\tilde{\mathbf{x}}_0$, otherwise go back to 1.

References

1. Bettale, L., Faugère, J.-C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. J. Math. Cryptol. **3**(3), 177–197 (2009)
2. Bellavia, S., Macconi, M., Morini, B.: An affine scaling trust-region approach to bound-constrained nonlinear systems. Appl. Numer. Math. **44**, 257–280 (2003)
3. Bellavia, S., Morini, B.: An interior global method for nonlinear systems with simple bounds. Optim. Methods Softw. **20**, 1–22 (2005)
4. Bettale, L., Faugère, J.-C., Perret, L.: Cryptanalysis of multivariate and odd-characteristic HFE variants. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 441–458. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_27
5. Bertsekas, D.P.: Nonlinear Programming, 3rd edn. Athena Scientific, Nashua (2016)
6. Clough, C., Baena, J., Ding, J., Yang, B.-Y., Chen, M.: Square, a new multivariate encryption scheme. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 252–264. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00862-7_17
7. Dennis, J.E., Schnabel, R.B.: Numerical Methods for Unconstrained Optimization and Nonlinear Equations. Prentice-Hall, Englewood Cliffs (1983)
8. Ding, J., Gower, J.E., Schmidt, D.S.: Multivariate Public Key Cryptosystems, Advances in Information Security, vol. 25. Springer, Heidelberg (2006). https://doi.org/10.1007/978-0-387-36946-4
9. 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
10. Dubois, V., Gama, N.: The degree of regularity of HFE systems. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 557–576. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_32
11. Fan, J.Y., Pan, Y.X.: On the quadratic convergence of the Levenberg-Marquardt method without nonsingularity assumption. Computing **74**, 23–39 (2005)
12. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra **139**, 61–88 (1999)

13. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of ISSAC 2002, pp. 75–83. ACM Press (2002)
14. Fröberg, R.: An inequality for Hilbert series of graded algebras. Mathematica Scandinavia **56**, 117–144 (1985)
15. Götze, F.: Lattice point problems and value of quadratic forms. Invent. math. **157**, 195–226 (2004)
16. Ikematsu, Y., Perlner, R., Smith-Tone, D., Takagi, T., Vates, J.: HFERP - a new multivariate encryption scheme. In: Lange, T., Steinwandt, R. (eds.) PQCrypto 2018. LNCS, vol. 10786, pp. 396–416. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-79063-3_19
17. Kanzow, C.: An active-set type newton method for constrained nonlinear systems. In: Complementarity: Applications, Algorithms and Extensions, pp. 179–200. Kluwer Academic (2001)
18. Kanzow, C., Yamashita, N., Fukushima, M.: Levenberg-Marquardt methods with strong local convergence properties for solving nonlinear equations with convex constraints. J. Comput. Appl. Math. **172**(2), 375–397 (2004)
19. Kelly, C.T.: Iterative Methods for Linear and Nonlinear Equations. SIAM, Philadelphia (1995)
20. Levenberg, K.: A method for the solution of certain nonlinear problems in least square. Quart. Appl. Math. **2**, 164–166 (1944)
21. Marquardt, D.W.: An algorithm for least-square estimation on nonlinear problems. SIAM J. Appl. Math. **11**, 431–441 (1963)
22. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Barstow, D., et al. (eds.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-45961-8_39
23. Monteiro, R.D.C., Pang, J.S.: A potential reduction Newton method for constrained equations. SIAM J. Optim. **9**, 729–754 (1999)
24. Nguyen, P.Q.: Hermite's constant and lattice algorithms. In: Nguyen, P., Vallée, B. (eds.) The LLL Algorithm: Survey and Applications, pp. 19–69. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02295-1_2
25. Nocedal, J., Wright, S.J.: Numerical Optimization, 2nd edn. Springer, Heidelberg (2006). https://doi.org/10.1007/978-0-387-40065-5
26. 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
27. 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
28. Qi, L., Tong, X.J., Li, D.H.: An active-set projected trust region algorithm for box constrained nonsmooth equations. J. Optim. Theor. Appl. **120**, 601–649 (2004)
29. Szepieniec, A., Ding, J., Preneel, B.: Extension field cancellation: a new central trapdoor for multivariate quadratic systems. In: Takagi, T. (ed.) PQCrypto 2016. LNCS, vol. 9606, pp. 182–196. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29360-8_12
30. Szepieniec, A., Preneel, B.: Short solutions to nonlinear systems of equations. Cryptology ePrint archive: report 2017/1175. https://eprint.iacr.org/2017/1175

31. Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp. 231–242. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38616-9_16
32. Ulbrich, M.: Nonmonotone trust-region methods for vound-constrained semismooth equations with applications to nonlinear mixed complementarity problems. SIAM J. Optim. **11**, 889–917 (2001)
33. Wang, T., Monteiro, R.D.C., Pang, J.S.: An interior point potential reduction method for constrained equations. Math. Program. **74**, 159–195 (1996)
34. Yamashita, N., Fukushima, M.: On the rate of convergence of the LM method. In: Alefeld, G., Chen, X. (eds.) Computing Supplementa, vol. 15, pp. 237–249. Springer, Heidelberg (2001). https://doi.org/10.1007/978-3-7091-6217-0_18
35. Yang, B.-Y., Chen, J.-M.: Theoretical analysis of XL over small fields. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 277–288. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-27800-9_24
36. Yang, B.-Y., Chen, J.-M.: All in the XL family: theory and practice. In: Park, C., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 67–86. Springer, Heidelberg (2005). https://doi.org/10.1007/11496618_7
37. Yasuda, T.: Multivariate encryption schemes based on the constrained MQ problem. In: Baek, J., Susilo, W., Kim, J. (eds.) ProvSec 2018. LNCS, vol. 11192, pp. 129–146. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01446-9_8
38. Yuan, Y.X.: Recent advances in numerical methods for nonlinear equations and nonlinear least squares. Numer. Algebra Control Optim. **1**, 15–34 (2011)