ISSN 2070-0466, p-Adic Numbers, Ultrametric Analysis and Applications, 2024, Vol. 16, No. 1, pp. 23–42. © Pleiades Publishing, Ltd., 2024.

RESEARCH ARTICLES

Public-Key Cryptosystems and Signature Schemes from p-Adic Lattices

Yingpu Deng[1, 2*], Lixia Luo[1, 2], Yanbin Pan[1, 2***], Zhaonan Wang[3, 2****], and Guanju Xiao[4*****]**

[1] *Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, People's Republic of China*

[2] *School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, People's Republic of China*

[3] *Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, People's Republic of China*

[4] *College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, People's Republic of China*

Received June 17, 2023; in final form, November 11, 2023; accepted November 26, 2023

Abstract—In 2018, the longest vector problem and closest vector problem in local fields were introduced, as the p-adic analogues of the shortest vector problem and closest vector problem in lattices of Euclidean spaces. They are considered to be hard and useful in constructing cryptographic primitives, but no applications in cryptography were given. In this paper, we construct the first signature scheme and public-key encryption cryptosystem based on p-adic lattice by proposing a trapdoor function with the norm-orthogonal basis of p-adic lattice. These cryptographic schemes have reasonable key size and the signature scheme is efficient, while the encryption scheme works only for short messages, which shows that p-adic lattice can be a new alternative to construct cryptographic primitives and well worth studying.

DOI: 10.1134/S2070046624010035

Key words: *lattice, local field, SVP, CVP, LVP, signature scheme, public-key cryptosystem.*

1. INTRODUCTION

Since Diffie and Hellman invented public-key cryptography in 1976 [4], quite a few public-key cryptosystems based on computationally hard mathematical problems have been proposed.

Two famous hard problems are integer factorization and discrete logarithm problem, based on which lots of cryptosystems have been constructed. For example, the first practical public-key cryptosystem RSA [21] is based on integer factorization. The ElGamal cryptosystem [7] is based on the discrete logarithm problem in finite fields. The elliptic curve cryptosystem is based on discrete logarithm of elliptic curves over finite fields [10, 17], and hyperelliptic curve cryptosystem is based on discrete logarithm of Jacobian of hyperelliptic curves over finite fields [11]. The two problems have not been proven to be NP-hard yet, and Peter Shor [23] found quantum polynomial time algorithms in 1994 for them, which yields that the classical public-key cryptosystems such as RSA and ElGamal would be broken under future quantum computer.

[*] E-mail: dengyp@amss.ac.cn
[**] E-mail: luolixia@amss.ac.cn
[***] E-mail: panyanbin@amss.ac.cn
[****] E-mail: znwang@amss.ac.cn
[*****] E-mail: gjXiao@amss.ac.cn

However, there are also other computationally hard mathematical problems that can be employed to construct public key cryptosystems. For instance, multivariate cryptography [14] is based on solving system of nonlinear equations over finite fields. The McEliece system [15] is based on decoding a random linear code over finite fields. Lattice-based cryptography [8, 16] is based on the shortest vector problem and closest vector problem in lattices of Euclidean spaces. These computational problems have been shown to be NP-hard, and the corresponding cryptosystems are widely believed to be quantum-resistant, which are the main candidates in the standardization of post quantum cryptography initiated by NIST [26]. Specially, some new hard computational problems have been proposed in the standardization, such as computing isogeny between elliptic curves [6, 13]. But it is still unknown if computing isogeny between elliptic curves is NP-hard or not.

Motivated by lattice-based cryptosystems, one of the most promising post quantum cryptosystems, Deng *et al.* [2, 3] introduced some new computational problems in p-adic lattices of local fields, the longest vector problem and closest vector problem which are the p-adic analogues of the shortest vector problem and closest vector problem in lattices of Euclidean spaces. It was expected in [2, 3] that the new problems can be used to construct public key cryptosystems, which was left as an open problem.

In this paper, we try to solve the problem by constructing a signature scheme and a public-key encryption scheme. The basic idea is very similar to the code-based McEliece system [15] or the lattice-based GGH scheme [8], that is, we adopt a good basis as the private key and transform it into a bad basis as the public key. With the good basis, we can efficiently solve the hard problem in p-adic lattice, while the bad basis looks random that may not help solve the hard problem. We show that a norm-orthogonal basis for a given p-adic lattice can be the good basis. More precisely, we show that if there is a norm-orthogonal basis for a given p-adic lattice, then the longest vector problem and closest vector problem in local fields are easy to solve. Then the norm-orthogonal bases can be used to construct trapdoor information for cryptographic schemes. Finally we propose a signature scheme and a public-key cryptosystem based on p-adic lattices.

We would like to point out that as main candidate of the post quantum cryptography, cryptography based on lattices in Euclidean spaces have obtained extensive study in recent years. However, p-adic lattices do not gain any attention. As the p-adic analogues of the lattices in Euclidean spaces, it is reasonable to expect that the problem could be quantum-resistant. Our results shows that p-adic lattices may be useful in cryptography and it is worth for further study, which provides a new alternative candidate to construct cryptographic primitives. Just as Neal Koblitz said in the Preface of his book [12]: “But in the rapidly growing field of cryptography it is worthwhile to continually explore new one-way constructions coming from different areas of mathematics.”

The paper is organized as follows. We recall basic fact about local fields, the p-adic lattices, the longest vector problem (LVP) and closest vector problem (CVP) in Section 2 and present the fast algorithms to solve LVP and CVP in local fields with the help of a norm-orthogonal basis in Section 3. We then construct a signature scheme in Section 4 and a public-key cryptosystem in Section 5. We give some possible attacks to our schemes in Section 6 and we report our experimental results in Section 7. We present some improvements to the public-key encryption scheme for the purpose of efficiency in Section 8.

2. LOCAL FIELDS AND p-ADIC LATTICES

In this section, we recall some basic facts about local fields, see [2, 3]. For detailed study of local fields, please see [1, 9, 22].

2.1. Basic Facts About Local Fields

Let p be a prime number. For $x \in \mathbb{Q}$ with $x \neq 0$, write $x = p^t \frac{a}{b}$ with $t, a, b \in \mathbb{Z}$ and $p \nmid ab$. Define $|x|_p = p^{-t}$ and $|0|_p = 0$. Then $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}$. Namely, we have: (1) $|x|_p \geq 0$ and $|x|_p = 0$ if and only if x=0; (2) $|xy|_p = |x|_p \cdot |y|_p$; (3) $|x + y|_p \leq \max(|x|_p, |y|_p)$. If $|x|_p \neq |y|_p$, then we must have $|x + y|_p = \max(|x|_p, |y|_p)$.

Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. Denote $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. We have

$$\mathbb{Q}_p = \left\{ \sum_{i=j}^{\infty} a_i p^i : j \in \mathbb{Z}, a_i \in \{0, 1, 2, \ldots, p-1\} \right\},$$

and

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i : a_i \in \{0, 1, 2, \ldots, p-1\} \right\}.$$

$\mathbb{Z}_p$ is compact and $\mathbb{Q}_p$ is locally compact. $\mathbb{Z}_p$ is a discrete valuation ring, it has a unique nonzero principal maximal ideal $p\mathbb{Z}_p$ and p is called a uniformizer of $\mathbb{Q}_p$. The unit group of $\mathbb{Z}_p$ is $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}$. The residue class field $\mathbb{Z}_p/p\mathbb{Z}_p$ is the finite field with p elements.

Let n be a positive integer, and let K be an extension field of $\mathbb{Q}_p$ of degree n. We fix some algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and view K as a subfield of $\overline{\mathbb{Q}}_p$. Such K exists. For example, let $K = \mathbb{Q}_p(\alpha)$ with $\alpha^n = p$. Because $X^n - p$ is an Eisenstein polynomial over $\mathbb{Q}_p$, it is irreducible over $\mathbb{Q}_p$, then K has degree n over $\mathbb{Q}_p$. Further, there are only finitely many extension fields of $\mathbb{Q}_p$ of degree n contained in $\overline{\mathbb{Q}}_p$, see [18]. The p-adic absolute value (or norm) $|\cdot|_p$ on $\mathbb{Q}_p$ can be extended uniquely to K, i.e., for $x \in K$, we have $|x|_p = |N_{K/\mathbb{Q}_p}(x)|_p^{\frac{1}{n}}$, where $N_{K/\mathbb{Q}_p}$ is the norm map from K to $\mathbb{Q}_p$. K is complete with respect to $|\cdot|_p$. See [1] for a proof.

Denote $\mathcal{O}_K = \{x \in K : |x|_p \leq 1\}$. $\mathcal{O}_K$ is also a discrete valuation ring, it has a unique nonzero principal maximal ideal $\pi\mathcal{O}_K$ and π is called a uniformizer of K. $\mathcal{O}_K$ is a free $\mathbb{Z}_p$-module of rank n. $\mathcal{O}_K$ is compact and K is locally compact. The unit group of $\mathcal{O}_K$ is $\mathcal{O}_K^\times = \{x \in K : |x|_p = 1\}$. The residue class field $\mathcal{O}_K/\pi\mathcal{O}_K$ is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p$. Call the positive integer $f = [\mathcal{O}_K/\pi\mathcal{O}_K : \mathbb{Z}_p/p\mathbb{Z}_p]$ the residue field degree of $K/\mathbb{Q}_p$. As ideals in $\mathcal{O}_K$, we have $p\mathcal{O}_K = \pi^e\mathcal{O}_K$. Call the positive integer e the ramification index of $K/\mathbb{Q}_p$. We have $n = [K : \mathbb{Q}_p] = ef$. When $e = 1$, the extension $K/\mathbb{Q}_p$ is unramified, and when $e = n$, $K/\mathbb{Q}_p$ is totally ramified. Each element x of the multiplicative group $K^\times$ of nonzero elements of K can be written uniquely as $x = u\pi^t$ with $u \in \mathcal{O}_K^\times$ and $t \in \mathbb{Z}$. We have $p = u\pi^e$ with $u \in \mathcal{O}_K^\times$, so $|\pi|_p = p^{-\frac{1}{e}}$. The valuation group of K is

$$\{|x|_p : x \in K^\times\} = p^{\frac{\mathbb{Z}}{e}}.$$

2.2. Efficient Computations in Local Fields

In this subsection, we describe how to do efficient computations in local fields.

We give a degree-n extension field K of $\mathbb{Q}_p$ by giving a monic degree-n irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$. Let $\theta \in \overline{\mathbb{Q}}_p$ be a root of $f(x) = 0$, then let $K = \mathbb{Q}_p(\theta)$. If $f(x)$ is an Eisenstein polynomial, then K is totally ramified over $\mathbb{Q}_p$, see [1].

Let $\alpha \in K$, we express α as a polynomial of θ of degree $< n$ with coefficients in $\mathbb{Q}_p$. The map

$$\widehat{\alpha} : K \longrightarrow K$$

is defined as $\widehat{\alpha}(\beta) = \alpha \cdot \beta$, i.e., the map from K to K by multiplying α. This map is $\mathbb{Q}_p$-linear. The norm $N_{K/\mathbb{Q}_p}(\alpha)$ is the determinant of the map $\widehat{\alpha}$. We can take the basis $(1, \theta, \theta^2, \ldots, \theta^{n-1})$ of K over $\mathbb{Q}_p$, then representing the map $\widehat{\alpha}$ by an $n \times n$-matrix over $\mathbb{Q}_p$. The determinant of this matrix is the norm $N_{K/\mathbb{Q}_p}(\alpha)$. So we can efficiently calculate the p-adic absolute value $|\alpha|_p$.

Let $\alpha_1, \ldots, \alpha_n$ be a basis of K over $\mathbb{Q}_p$, and let $\beta \in K$. Using the following method, we can represent β as a $\mathbb{Q}_p$-linear combination of $\alpha_1, \ldots, \alpha_n$. Write

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = B \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{pmatrix}$$

with $B \in GL_n(\mathbb{Q}_p)$. It is clear that

$$\beta = (b_1, b_2, \ldots, b_n) \cdot \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{pmatrix} = (b_1, b_2, \ldots, b_n) \cdot B^{-1} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

2.3. p-Adic Lattices, LVP and CVP

In [2, 3], two new computational problems in p-adic lattices are introduced, they are the Longest Vector Problem and Closest Vector Problem. We first review it briefly.

Let p be a prime number, and let K be an extension field of $\mathbb{Q}_p$ of degree n, where n is a positive integer. Let m be a positive integer with $1 \leq m \leq n$. Let $\alpha_1, \ldots, \alpha_m \in K$ be m many $\mathbb{Q}_p$-linearly independent vectors. A lattice in K is the set

$$\mathcal{L}(\alpha_1, \ldots, \alpha_m) = \left\{ \sum_{i=1}^{m} a_i \alpha_i : a_i \in \mathbb{Z}_p, 1 \leq i \leq m \right\}$$

of all $\mathbb{Z}_p$-linear combinations of $\alpha_1, \ldots, \alpha_m$. The sequence of vectors $\alpha_1, \ldots, \alpha_m$ is called a basis of the lattice $\mathcal{L}(\alpha_1, \ldots, \alpha_m)$. The integers m and n are called the rank and dimension of the lattice, respectively. When $n = m$, we say that the lattice is of full rank.

Since a p-adic lattice of rank m is a free $\mathbb{Z}_p$-module, obviously, two bases of the same lattice is related with a matrix in $GL_m(\mathbb{Z}_p)$, i.e., an $m \times m$ matrix with coefficients in $\mathbb{Z}_p$ and its determinant is in $\mathbb{Z}_p^{\times}$.

2.3.1. Longest vector problem(LVP). For any element $\alpha = \sum_{i=1}^{m} a_i \alpha_i \in \mathcal{L}$, since each $a_i \in \mathbb{Z}_p$, we have

$$|\alpha|_p = \left| \sum_{i=1}^{m} a_i \alpha_i \right|_p \leq \max_{1 \leq i \leq m} (|a_i \alpha_i|_p) \leq \max_{1 \leq i \leq m} (|\alpha_i|_p).$$

This indicates that the length $| \alpha |_p$ of any element of the p-adic lattice $\mathcal{L}$ is bounded above. Since the valuation group of K is discrete, as a subset of K, the set of lengths of elements of the lattice $\mathcal{L}$ is also discrete.

Definition 2.1. *[2, 3] Let $\mathcal{L} = \mathcal{L}(\alpha_1, \ldots, \alpha_m)$ be a lattice in K. We define recursively a sequence of positive real numbers: $\lambda_1, \lambda_2, \lambda_3, \ldots$ as follows.*

$$\lambda_1 = \max_{1 \leq i \leq m} (|\alpha_i|_p)$$

$$\lambda_{j+1} = \max\{|x|_p : x \in \mathcal{L}, |x|_p < \lambda_j\} \textit{ for } j \geq 1.$$

We have $\lambda_1 > \lambda_2 > \lambda_3 > \ldots$ and $\lim_{j \to \infty} \lambda_j = 0$.

Definition 2.2. *[2, 3] Given a lattice $\mathcal{L} = \mathcal{L}(\alpha_1, \ldots, \alpha_m)$ in K, the longest vector problem (LVP) is to find a lattice vector $v \in \mathcal{L}$ such that $|v|_p = \lambda_2$.*

Theorem 2.3. *[2, 3] Given a lattice $\mathcal{L} = \mathcal{L}(\alpha_1, \ldots, \alpha_m)$ in K. Fix an integer $j \geq 2$. There exists an algorithm to find a lattice vector $v_j \in \mathcal{L}$ satisfying $|v_j|_p = \lambda_j$. The algorithm takes $O(p^{m(j-1)})$ many p-adic absolute value computations of elements of K.*

Remark. Since p-adic lattices have essential difference from Euclidean lattices, all about Euclidean lattices including mathematics and algorithms do not hold for p-adic lattices, at least need further study. This is a new research area. One can compare p-adic analysis with classical real and complex analysis.

2.3.2. Closest vector problem(CVP). Given a target vector $t \in K$. Since the function

$$\mathcal{L} \longrightarrow \mathbb{R}$$

$$v \longmapsto |t - v|_p$$

is continuous on the compact set $\mathcal{L}$, it can take the minimum and maximum on $\mathcal{L}$. Set

$$\mu_{\min} = \min_{v \in \mathcal{L}} |t - v|_p \text{ and } \mu_{\max} = \max_{v \in \mathcal{L}} |t - v|_p.$$

If $t \in \mathcal{L}$, it is obvious that we have $\mu_{\min} = 0$ and $\mu_{\max} = \lambda_1$. Here λ_1 is the same as in Definition 2.1. So we below assume $t \notin \mathcal{L}$. Hence $\mu_{\min} > 0$. Since the valuation group of K is discrete, the above distance function will take only finitely many values. So we have the following definition.

Definition 2.4. *[2, 3] Let $\mathcal{L} = \mathcal{L}(\alpha_1, \dots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector. Define s positive real numbers $\mu_1 > \mu_2 > \mu_3 > \cdots > \mu_s$ as follows, where s is a positive integer.*

$$\{\mu_1, \mu_2, \mu_3, \dots, \mu_s\} = \{|t - v|_p : v \in \mathcal{L}\}.$$

So $\mu_{\max} = \mu_1$ and $\mu_{\min} = \mu_s$.

If $|t|_p > \lambda_1$, since $v \in \mathcal{L}, |v|_p \leq \lambda_1$, we have $|t - v|_p = |t|_p$, thus $\mu_{\min} = \mu_{\max} = |t|_p$. So we below assume $|t|_p \leq \lambda_1$.

Definition 2.5. *[2, 3] Let $\mathcal{L} = \mathcal{L}(\alpha_1, \dots, \alpha_m)$ be a lattice in K and let $t \in K - \mathcal{L}$ be a target vector with $|t|_p \leq \lambda_1$. The closest vector problem (CVP) is to find a lattice vector $v \in \mathcal{L}$ such that $|t - v|_p = \mu_{\min}$.*

3. SOLVING LVP AND CVP WITH ORTHOGONAL BASES

3.1. Norm-Orthogonal Bases

Let p be a prime. Let V be a left vector space over $\mathbb{Q}_p$. A norm on V is a function

$$|\cdot| : V \longrightarrow \mathbb{R}$$

such that:

$$(i) \quad |v| \geq 0, \forall v \in V, \text{ and } |v| = 0 \text{ if and only if } v = 0;$$

$$(ii) \quad |xv| = |x|_p \cdot |v|, \forall x \in \mathbb{Q}_p, v \in V;$$

$$(iii) \quad |v + w| \leq \max(|v|, |w|), \forall v, w \in V.$$

If $|\cdot|$ is a norm on V, and if $|v| \neq |w|$ for $v, w \in V$, then we must have $|v + w| = \max(|v|, |w|)$. Weil [25] proved the following proposition:

Proposition 3.1. *[25, p.26] Let V be a left vector space over $\mathbb{Q}_p$ of finite dimension $n > 0$, and let $|\cdot|$ be a norm on V. Then there is a decomposition $V = V_1 + \cdots + V_n$ of V into a direct sum of subspaces V_i of dimension 1, such that*

$$\left|\sum_{i=1}^{n} v_i\right| = \max_{1 \leq i \leq n} |v_i|, \forall v_i \in V_i, i = 1, \dots, n.$$

So we can define the norm-orthogonal basis.

Definition 3.2 (Norm-orthogonal basis). *Let V be a left vector space over $\mathbb{Q}_p$ of finite dimension $n > 0$, and let $|\cdot|$ be a norm on V. We call $\alpha_1, \ldots, \alpha_n$ a norm-orthogonal basis of V over $\mathbb{Q}_p$ if V can be decomposed into the direct sum of n 1-dimensional subspaces V_i's $(1 \leq i \leq n)$, such that*

$$\left|\sum_{i=1}^{n} v_i\right| = \max_{1\leq i\leq n} |v_i|, \forall v_i \in V_i, i = 1, \ldots, n,$$

where V_i is spanned by α_i. If $\alpha_1, \ldots, \alpha_n$ is a norm-orthogonal basis of the vector space spanned by a lattice $\mathcal{L} = \sum_{i=1}^{n} \mathbb{Z}_p \alpha_i$, then we call $\alpha_1, \ldots, \alpha_n$ a norm-orthogonal basis of the lattice $\mathcal{L}$.

Weil's proof is not constructive, and he did not give a method to find out a norm-orthogonal basis. The following is immediate.

Proposition 3.3. *Let V be a left vector space over $\mathbb{Q}_p$ of finite dimension $n > 0$, and let $|\cdot|$ be a norm on V. Let $\alpha_1, \ldots, \alpha_n$ be a basis of V over $\mathbb{Q}_p$. If*

$$\{|v_i| : v_i \in \mathbb{Q}_p \cdot \alpha_i\} \bigcap \{|v_j| : v_j \in \mathbb{Q}_p \cdot \alpha_j\} = \{0\}, \forall i, j = 1, \ldots, n, i \neq j,$$

then $\alpha_1, \ldots, \alpha_n$ is a norm-orthogonal basis of V over $\mathbb{Q}_p$.

Proposition 3.4. *Let K be an extension field of degree n of $\mathbb{Q}_p$. Let π be a uniformizer of K. Set*

$$V = \sum_{i=0}^{e-1} \mathbb{Q}_p \cdot \pi^i$$

where e is the ramification index of $K/\mathbb{Q}_p$. Then V is an e-dimensional $\mathbb{Q}_p$-vector subspace of K, and $1, \pi, \ldots, \pi^{e-1}$ is a norm-orthogonal basis of V, where the norm of V is given by the p-adic absolute value of the field K.

Proof. We know $1, \pi, \ldots, \pi^{e-1}$ are $\mathbb{Q}_p$-linearly independent, see [1, p.125, Lemma 5.4]. Since $|\pi|_p = p^{-\frac{1}{e}}$,

$$\{|x|_p : x \in \mathbb{Q}_p \cdot \pi^i\} = \{0\} \bigcup p^{\mathbb{Z} - \frac{i}{e}}.$$

Now the result follows from Proposition 3.3. □

3.2. Solving LVP with Orthogonal Bases

We can prove the following theorem.

Theorem 3.5. *Given a lattice $\mathcal{L} = \mathcal{L}(\alpha_1, \ldots, \alpha_m)$ in K. Assume $\alpha_1, \ldots, \alpha_m$ is a norm-orthogonal basis of the lattice $\mathcal{L}$. Fix an integer $j \geq 2$. There exists an algorithm to find a lattice vector $v_j \in \mathcal{L}$ satisfying*

$$|v_j|_p = \lambda_j.$$

The algorithm takes $O(m)$ many p-adic absolute value computations of elements of K.

Proof. Without loss of generality, we can assume

$$\{|\alpha_i|_p : i = 1, \ldots, m\} = \{\nu_1, \ldots, \nu_s\} \text{ with } \nu_1 > \cdots > \nu_s,$$

and

$$|\alpha_i|_p = \nu_i, i = 1, \ldots, s.$$

For any $v \in \mathcal{L}, v \neq 0$, we can write

$$v = \sum_{i=1}^{m} a_i \alpha_i$$

with $a_i \in \mathbb{Z}_p$. Since $\alpha_1, \ldots, \alpha_m$ is a norm-orthogonal basis, we have

$$|v|_p = \max_{1 \le i \le m} \{|a_i|_p \cdot |\alpha_i|_p\}.$$

For nonzero a_i, we have $|a_i|_p = p^{-k}$ with $k \in \mathbb{Z}$ and $k \ge 0$.

Then, obviously,

$$\{\log_p |v|_p : v \in \mathcal{L}, v \ne 0\} = \{\log_p \nu_i - k : i = 1, \ldots, s, k = 0, 1, 2, \cdots\}.$$

Consider the set of valuations

$$S = \{\log_p \nu_i - k : 0 \le k \le j - i, 1 \le i \le \min(s, j)\}.$$

Obviously, in decreasing order, the first number of the set S is $\log_p \nu_1 = \log_p \lambda_1$, and the j-th number is $\log_p \lambda_j$. If $\log_p \lambda_j = \log_p \nu_i - k$, we can take the vector $v_j = p^k \alpha_i$.

The algorithm needs to compute the m many p-adic absolute values of the basis vectors. We ignore the time of comparing.

□

3.3. Solving CVP with Orthogonal Bases

We can prove the following theorem.

Theorem 3.6. *Let $\mathcal{L} = \mathcal{L}(\alpha_1, \ldots, \alpha_m)$ be a lattice in K. Let $t \in K - \mathcal{L}$ be a target vector with $|t|_p \le \lambda_1$. Let $V(\supset \mathcal{L})$ be a k-dimensional $\mathbb{Q}_p$-vector subspace of the field K. Let $\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_k (k \ge m)$ be a norm-orthogonal basis of V. Suppose the target vector $t \in V$. There is an algorithm to find a vector $v_i \in \mathcal{L}$ such that $|t - v_i|_p = \mu_i$, for each $i = 1, 2, \ldots, s$. The algorithm takes $O(n)$ many p-adic absolute value computations of elements of K, where n is the degree of K over $\mathbb{Q}_p$.*

Proof. Write

$$t = \sum_{i=1}^{k} b_i \alpha_i, \quad b_i \in \mathbb{Q}_p, i = 1, \ldots, k.$$

For any lattice vector

$$v = \sum_{i=1}^{m} a_i \alpha_i \in \mathcal{L}, a_i \in \mathbb{Z}_p, i = 1, \ldots, m,$$

we have

$$|t - v|_p = \max\{|b_i - a_i|_p \cdot |\alpha_i|_p (1 \le i \le m), |b_j \alpha_j|_p (m + 1 \le j \le k)\}.$$

If $b_i \notin \mathbb{Z}_p$, then $|b_i - a_i|_p = |b_i|_p > 1$. If $b_i \in \mathbb{Z}_p$, then

$$\{|b_i - a_i|_p : a_i \in \mathbb{Z}_p\} = \{0, p^{-c} (c = 0, 1, 2, \ldots)\}.$$

Without loss of generality, we can assume $b_i \notin \mathbb{Z}_p$ for $1 \le i \le l$ and $b_i \in \mathbb{Z}_p$ for $l + 1 \le i \le m$, where l is an integer with $0 \le l \le m$. Thus,

$$\{|t - v|_p : v \in \mathcal{L}\} = \{\max\{|b_i|_p \cdot |\alpha_i|_p (1 \le i \le l), |b_j \alpha_j|_p (m + 1 \le j \le k),$$

$$p^{-c_u} \cdot |\alpha_u|_p (c_u = 0, 1, 2, 3, \ldots, \infty (l + 1 \le u \le m))\}\},$$

where we set $p^{-\infty} = 0$.

Set

$$N = \max\{|b_i|_p \cdot |\alpha_i|_p (1 \le i \le l), |b_j \alpha_j|_p (m + 1 \le j \le k)\}.$$

Since $t \notin \mathcal{L}$, we have $N > 0$. Obviously, $\mu_s = \mu_{\min} = N$. To obtain the value

$$\max\{N, p^{-c_u} \cdot |\alpha_u|_p (c_u = 0, 1, 2, 3, \ldots, \infty (l+1 \leq u \leq m))\},$$

we can only consider those indices $l+1 \leq u \leq m$ for which $|\alpha_u|_p > N$. Denote d_u the largest non-negative integer with

$$p^{-d_u} \cdot |\alpha_u|_p > N.$$

Consider the set

$$T = \{N, p^{-c_u} \cdot |\alpha_u|_p (c_u = 0, 1, \ldots, d_u \text{ with } |\alpha_u|_p > N(l+1 \leq u \leq m))\}.$$

Listing the number of the set T, in decreasing order, we get the values of the distance function $|t - v|_p, v \in \mathcal{L}$, i.e. the s many positive real numbers $\mu_1 > \mu_2 > \mu_3 > \cdots > \mu_s$ such that

$$\{\mu_1, \mu_2, \mu_3, \ldots, \mu_s\} = \{|t - v|_p : v \in \mathcal{L}\}.$$

And it is easy to find all vectors $v_i \in \mathcal{L}$ such that $|t - v_i|_p = \mu_i, i = 1, 2, \ldots, s$.

□

Similar to Theorem 2.3, if there is no any norm-orthogonal basis, exponential time algorithms are given in [2, 3].

4. A SIGNATURE SCHEME

We present our signature scheme as follows.

Key Generation: We first choose a totally ramified K of degree n over $\mathbb{Q}_p$, i.e., choose an Eisenstein polynomial $f(x) = x^n + f_1 x^{n-1} + \ldots + f_{n-1}x + f_n \in \mathbb{Z}_p[x]$ satisfying $|f_n|_p = p^{-1}$ and $|f_i|_p < 1$ for $1 \leq i \leq n-1$. Let θ be a root of $f(x) = 0$. Choose another $\zeta \in \mathcal{O}_K = \mathbb{Z}_p[\theta]$ such that $\mathbb{Z}_p[\zeta] = \mathbb{Z}_p[\theta]$. It is easy to generate such a ζ, see Section 7.2. Then $K = \mathbb{Q}_p(\zeta)$. Let $F(x) \in \mathbb{Z}_p[x]$ be the minimum polynomial of ζ over $\mathbb{Q}_p$ which is also monic and of degree n. Choose n non-negative integers $j_i \in \mathbb{Z}$ such that the $j_i \pmod{n} (1 \leq i \leq n)$ are distinct. Set $\alpha_i = \theta^{j_i} (1 \leq i \leq n)$. By Proposition 3.3, we see that $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}_p$, thus $\alpha_1, \ldots, \alpha_n$ is a norm-orthogonal basis. All elements of $\mathcal{O}_K$ should be expressed as polynomials in ζ of degree $< n$ with coefficients in $\mathbb{Z}_p$ and ζ is just a formal symbol.

Choose a matrix $A \in \mathrm{GL}_m(\mathbb{Z}_p)$, where m is a positive integer with $m \leq n$. Put

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

such that the m vectors $\beta_1, \ldots, \beta_m$ have the same length or have almost same lengths. In our experiments, it is easy to generate such a matrix A, see Section 7.2. Notice that in practice coefficients of the polynomials f and F, as well as the p-adic integers β_i, α_j are rational numbers represented by irreducible fractions whose denominators are co-prime to p, see Section 7.1.

Set

$$\mathcal{L} = \mathbb{Z}_p \cdot \beta_1 + \ldots + \mathbb{Z}_p \cdot \beta_m = \mathbb{Z}_p \cdot \alpha_1 + \ldots + \mathbb{Z}_p \cdot \alpha_m.$$

We need a hash function

$$H : \{0,1\}^* \longrightarrow W := \{x : x \in K - \mathcal{L}, |x|_p = \lambda_1\},$$

where λ_1 is the maximum value of the lengths of all vectors in $\mathcal{L}$. In our experiments, it is easy to generate an element of the set W, see Section 7.3.

This hash function can be implemented as follows. For the message $M \in \{0,1\}^*$, compute $seed = SHA - 3(M)$, then use this seed to generate an element in W. That is, we use this seed as the coefficient sequence of a polynomial in ζ to yielding an element in the field K. Our experiment shows that this element is in the set W with probability 1, see Section 7.3.

Public key is set to be: $(F(x), H, (\beta_1, \ldots, \beta_m))$.

Private key is set to be: $(f(x), (\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n))$.

Signing algorithm: For any message $M \in \{0,1\}^*$, choose a random number r of fixed length, say, $r \in \{0,1\}^{256}$. Compute

$$t = H(M \parallel r).$$

Using the norm-orthogonal basis $(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n)$ and the secret polynomial $f(x)$, Bob computes a lattice vector $v \in \mathcal{L}$ which is the closest one to t. If the minimum value of the distance from t to $\mathcal{L}$ is strictly less than λ_1, then output the signature (r, v). If the minimum value of the distance from t to $\mathcal{L}$ is equal to λ_1, then choose a new $r \in \{0,1\}^{256}$ until the minimum value of the distance from t to $\mathcal{L}$ is strictly less than λ_1.

Verification algorithm: The signature is valid if and only if $t = H(M \parallel r), v \in \mathcal{L}$ and $|t - v|_p < \lambda_1$.

The correctness is obvious. For the efficiency, what needs to illustrate is how many random r's can yield a valid signature. We have not proven it in theory by now, but in our experiments, we always generated a valid signature with just one r, see Section 7.3. Hence, our signature scheme is very efficient.

Remark. Notice that, if (r, v) is a true signature, then we must have $|v|_p = \lambda_1$. This is because $t \in W$, so $|t|_p = \lambda_1$; if $|v|_p < \lambda_1$, then we would have $|t - v|_p = \lambda_1$, a contradiction. Keeping the notation in the proof of Theorem 3.6, if there is an index u with $l + 1 \leq u \leq m$ such that $|b_u \alpha_u|_p > N$, then it holds that the minimum distance from t to $\mathcal{L}$ is strictly less than $|t|_p$.

Parameter selection. To attain the 128-bit security level, one should select $n \geq m$ and $p^m \approx 2^{128}$. This follows from the CVP algorithm given in [2, 3].

5. A PUBLIC-KEY CRYPTOSYSTEM

We first present an original public-key cryptosystem as follows.

Key Generation For the sake of clarity, we repeat the necessary notation. We first choose a totally ramified K of degree $n > 1$ over $\mathbb{Q}_p$, i.e., choose an Eisenstein polynomial $f(x) = x^n + f_1 x^{n-1} + \ldots + f_{n-1}x + f_n \in \mathbb{Z}_p[x]$ satisfying $|f_n|_p = p^{-1}$ and $|f_i|_p < 1$ for $1 \leq i \leq n-1$. Let θ be a root of $f(x) = 0$. Choose another $\zeta \in \mathcal{O}_K = \mathbb{Z}_p[\theta]$ such that $\mathbb{Z}_p[\zeta] = \mathbb{Z}_p[\theta]$. It is easy to generate such a ζ, see Section 7.2. Then $K = \mathbb{Q}_p(\zeta)$. Let $F(x) \in \mathbb{Z}_p[x]$ be the minimum polynomial of ζ over $\mathbb{Q}_p$ which is also monic and of degree n. Choose n non-negative integers $j_i \in \mathbb{Z}$ such that the $j_i \pmod{n} (1 \leq i \leq n)$ are distinct. Set $\alpha_i = \theta^{j_i} (1 \leq i \leq n)$. By Proposition 3.3, we see that $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Q}_p$, thus $\alpha_1, \ldots, \alpha_n$ is a norm-orthogonal basis.

Choose a positive integer $m \leq n$. Choose a real number $\delta \geq 0$. All elements of $\mathcal{O}_K$ should be expressed as polynomials in ζ of degree $< n$ with coefficients in $\mathbb{Z}_p$.

Choose a matrix $A \in \mathrm{GL}_m(\mathbb{Z}_p)$. Put

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

such that the m vectors $\beta_1, \ldots, \beta_m$ have the same length or have almost same lengths. In our experiments, it is easy to generate such a matrix A, see Section 7.2. Notice that in practice coefficients of the polynomials f and F, as well as the p-adic integers β_i, α_j are rational numbers represented by irreducible fractions whose denominators are co-prime to p, see Section 7.1. Set

$$\mathcal{L} = \mathbb{Z}_p \cdot \beta_1 + \ldots + \mathbb{Z}_p \cdot \beta_m = \mathbb{Z}_p \cdot \alpha_1 + \ldots + \mathbb{Z}_p \cdot \alpha_m.$$

Public key is set to be: $(F(x), \delta, (\beta_1, \ldots, \beta_m))$.

Private key is set to be: $(f(x), A, (\alpha_1, \ldots, \alpha_n))$.

Encryption: For any plaintext $(a_1, \ldots, a_m) \in \{0, 1, \ldots, p-1\}^m$, Alice first chooses randomly $r \in K$ with $|r|_p < p^{-\delta}$, computes the ciphertext

$$C = a_1\beta_1 + \cdots + a_m\beta_m + r \in K$$

and sends C to Bob.

Decryption: When Bob receives the ciphertext C, using Theorem 3.6 with the norm-orthogonal basis $(\alpha_1, \ldots, \alpha_n)$, he computes a lattice vector $v \in \mathcal{L}$ which is the closest one to C. Write

$$v = b_1\alpha_1 + \ldots + b_m\alpha_m, \quad b_i \in \mathbb{Z}_p,$$

then the plaintext is

$$(b_1, \ldots, b_m) \cdot A^{-1} \pmod{p}.$$

For the correctness, we can prove that:

Theorem 5.1. *The decryption is correct if it holds that $j_i \leq \delta n$ for $1 \leq i \leq m$.*

Proof. Since there is a lattice vector $a_1\beta_1 + \cdots + a_m\beta_m$ such that $|C - (a_1\beta_1 + \cdots + a_m\beta_m)|_p < p^{-\delta}$, we have $|C - v|_p < p^{-\delta}$. Write $C = v + r'$ with $|r'|_p < p^{-\delta}$. We have

$$C = (a_1, \ldots, a_m) \cdot A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} + r = (b_1, \ldots, b_m) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} + r'.$$

Set

$$(c_1, \ldots, c_m) = (a_1, \ldots, a_m) \cdot A, \quad c_i \in \mathbb{Z}_p.$$

We have

$$\left| \sum_{i=1}^{m} (c_i - b_i) \cdot \alpha_i \right|_p = |r' - r|_p \leq \max\{|r|_p, |r'|_p\} < p^{-\delta}.$$

Since $\alpha_1, \ldots, \alpha_m$ is a norm-orthogonal basis, we have

$$\left| \sum_{i=1}^{m} (c_i - b_i) \cdot \alpha_i \right|_p = \max_{1 \leq i \leq m} (|c_i - b_i|_p \cdot |\alpha_i|_p) < p^{-\delta}.$$

Since

$$|\alpha_i|_p = |\theta^{j_i}|_p = p^{-\frac{j_i}{n}},$$

if there is some index $1 \leq i \leq m$ with $c_i - b_i \in \mathbb{Z}_p^{\times}$, then we have

$$p^{-\frac{j_i}{n}} < p^{-\delta}$$

i.e., $\delta < \frac{j_i}{n}$. So $c_i \equiv b_i \pmod{p}$ for each $1 \leq i \leq m$ if we have $j_i \leq \delta n$ for $1 \leq i \leq m$.

□

For the efficiency, what needs to illustrate is how efficient to generate a random $r \in K$ with $|r|_p < p^{-\delta}$. As δ becomes bigger, it is harder to generate such r. In Section 7, we present some experimental results. How to choose the parameters n, m, δ and p, see Section 7.5.

Remark. Our scheme is similar in its algorithmic nature to GGH scheme [8] based on lattices in Euclidean spaces and McEliece scheme [15], but the domains in which these operations take place are vastly different. The main difference between our scheme and GGH scheme [8] is the choice of "error r", in our scheme, r is an element of the field K, not just a vector as in the Euclidean case. This makes some efficient attacks in the Euclidean case do not work at all for our scheme, see sections 6.4. and 6.5.

6. HEURISTIC SECURITY ANALYSIS

Our scheme is similar to GGH scheme [8] and McEliece scheme [15], and these two schemes have no security proof up to now. Our scheme is based on p-adic lattices which are depend strictly on p-adic analysis, and much knowledge of p-adic analysis is unknown. The p-adic analysis has many difference from the classical analysis and many notions and theories in p-adic analysis need to be redefined and developed. So it may be impossible to give any formal security proof for our cryptosystems in the current situation. Instead, we give some possible attacks to our schemes in this section.

6.1. Recovering a Uniformizer

Given a local field K, even a special local field, e.g., a totally ramified one, if we could find out a uniformizer of K, then the above public-key cryptosystem and signature scheme would be broken completely. This is because expressing elements of the public basis as polynomials in the uniformizer, we can easily solve LVP and CVP by the algorithms given in sections 3.2 and 3.3.

However, as mentioned in [2, 3], uniformizers are just the second longest vectors in the p-adic lattice $\mathcal{O}_K$, so recovering a uniformizer is a special LVP-instance in $\mathcal{O}_K$. Since there is no second algorithm to compute it except the one mentioned in [2, 3], which is exponential in the dimension of the lattice, it seems that it is hard to recover a uniformizer of a given local field.

6.2. Finding a Norm-Orthogonal Basis

Now, given a general basis of a vector space V over $\mathbb{Q}_p$ and a norm on V, there is no any known algorithm to find out a norm-orthogonal basis of V. Similarly, given a general basis of a p-adic lattice, there is no any known algorithm to find out a norm-orthogonal basis of the lattice if it has. Notice that, not all p-adic lattices necessarily have norm-orthogonal bases. It seems that a norm-orthogonal basis of a p-adic lattice is hard to compute, and it is difficult to recover the private key from the public key in our cryptographic schemes.

6.3. Solving CVP-Instances

Obviously, if we could efficiently solve the CVP-instances, then the above public-key cryptosystem and signature scheme would be broken completely. If the CVP is hard under a random basis of a lattice, then there is no apparent way to forge a true signature without solving the CVP-instances.

One may argue that it may be not necessary to solve the CVP problem to break the encryption cryptosystem, since what we need to recover the plaintext is not $(d_1,\ldots,d_m) = (b_1,\ldots,b_m)\cdot A^{-1}$, but just $(d_1,\ldots,d_m) \mod p$. Notice that the ciphertext C is closest to $(d_1,\ldots,d_m)\cdot\begin{pmatrix}\beta_1\\ \vdots\\ \beta_m\end{pmatrix}$ by the decryption process. Given an m-dimensional p-adic lattice basis B and a target t, we define $\mathrm{CVP}_p(B,t)$ as the problem to recover $(d_1,\ldots,d_m) \mod p$, where $(d_1,\ldots,d_m)$ are the coefficients of some lattice vector closest to t under the basis B. It is easy to show that given an oracle to solve $\mathrm{CVP}_p(B,t)$, we can find a very good approximation of the vector in $\mathcal{L}(B)$ closest to t, which means that even to find the coefficients modulo p is very difficult. Roughly speaking, we can run the oracle to solve $\mathrm{CVP}_p(B,t)$ and get a returned solution $(\bar{d}_1,\ldots,\bar{d}_m)$. Then we know there exists $(d_1,\ldots,d_m)\in\mathbb{Z}_p^m$ such that $(d_1,\ldots,d_m)\cdot B$ is a lattice vector closest to t, and $(d_1,\ldots,d_m) \mod p = (\bar{d}_1,\ldots,\bar{d}_m)$. We can continue to run the oracle to solve $\mathrm{CVP}_p(pB, t-(\bar{d}_1,\ldots,\bar{d}_m)B)$ and get a returned solution $(\tilde{d}_1,\ldots,\tilde{d}_m)$. Then we know there exists $(d_1,\ldots,d_m)\in\mathbb{Z}_p^m$ associated with a closest vector, such that $(d_1,\ldots,d_m) \mod p^2 = (\bar{d}_1+p\tilde{d}_1,\ldots,\bar{d}_m+p\tilde{d}_1)$. Repeating the process several times, we can recover $(d_1,\ldots,d_m) \mod p^k$ for k polynomial in m, which is enough to yield a lattice vector that is very close to the target. Hence, to find the coefficients modulo p is still very difficult.

6.4. Modulo p Attack

We look at a so-called Modulo p attack for the above public-key cryptosystem. It is similar to Nguyen's attack [19] for the GGH cryptosystem.

For the ciphertext

$$C = a_1\beta_1 + \cdots + a_m\beta_m + r$$

with $|r|_p < p^{-\delta}$. Denote the ring of integers of K by $\mathcal{O}_K$, i.e., those elements x of K with $|x|_p \leq 1$. We know $\mathcal{O}_K = \mathbb{Z}_p[\zeta]$. We express $C, \beta_1, \ldots, \beta_m, r$ as polynomials of ζ with coefficients in $\mathbb{Z}_p$, then equating the coefficients of $1, \zeta, \ldots, \zeta^{n-1}$ of the two sides of the above equation, we obtain a system of n linear equations with coefficients in $\mathbb{Z}_p$. Write

$$r = \sum_{i=0}^{n-1} r_i \cdot \zeta^i, \quad r_i \in \mathbb{Z}_p.$$

If ζ would be a uniformizer of K, then since $|\zeta^i|_p = p^{-\frac{i}{n}}$, we have

$$|r|_p = \max_{0\leq i\leq n-1}(|r_i|_p \cdot p^{-\frac{i}{n}}).$$

Since $|r|_p < p^{-\delta}$, we have

$$|r_i|_p < p^{\frac{i-\delta n}{n}}.$$

If $i \leq \delta n$, then $p \mid r_i$. Since the $r_i's$ are unknown, reducing the above system of linear equations modulo p, we get a system of R linear equations over the finite field $\mathbb{F}_p$, and the unknowns are just the plaintext $(a_1, \ldots, a_m)$, where R is the number of indices $0 \leq i \leq n-1$ with $i \leq \delta n$. Assume the linear equations are linearly independent over $\mathbb{F}_p$, we can determine R unknowns as functions of other unknowns. We have proved the following.

Proposition 6.1. *If ζ would be a uniformizer of K, then the above Modulo p attack can at most reduce the search space of plaintexts from p^m to p^{m-R}, where R is the number of indices $0 \leq i \leq n-1$ with $i \leq \delta n$.*

However, in general, ζ is not a uniformizer of K, so $1, \zeta, \ldots, \zeta^{n-1}$ is not an orthogonal basis, so the above Modulo p attack fails. Further, we can let ζ be a unit of $\mathcal{O}_K$. Usually, the positive real number δ is < 1. Otherwise, if $\delta \geq 1$, it is easily seen that, when writing r as a polynomial of ζ, the coefficients are all divisible by p and the above Modulo p attack will apply.

6.5. Transcript Attacks to Our Signature

Given some pairs (*message*, *signature*), the authors in [5, 20] described successful transcript attacks to GGH signature and NTRU signature. The basic observation in [5, 20] is that a list of known pairs (*message*, *signature*) gives rise to the following learning problem, which they call the hidden parallelepiped problem (HPP): given many random points uniformly distributed over an unknown n-dimensional parallelepiped, recover the parallelepiped or an approximation thereof. They transform the HPP into a multivariate optimization problem based on the fourth moment of one-dimensional projections and this problem can be solved by a gradient descent.

However, these signatures are based on lattices in Euclidean spaces. The above attack depends strictly on knowledge of classical analysis (real analysis and probability theory). Our p-adic lattices are completely different from lattices in Euclidean spaces and they depend strictly on the p-adic analysis (and p-adic probability theory). The p-adic analysis has many differences from the classical analysis and many notions and theories in p-adic analysis need to be redefined and developed. So the transcript attacks in [5, 20] are not suitable to p-adic lattices, at least the whole theory needs to be redeveloped.

7. EXPERIMENTAL RESULTS

To verify the efficiency of our cryptosystems, we did some experiments on a personal laptop with Windows 10 operation system, i5-10210U CPU and 8-GB memory. We report some experimental results in this section.

7.1. General Strategies

Denote $\mathbb{Z}_{(p)} := \{x \in \mathbb{Q} \mid |x|_p \leq 1\}$, i.e., the localization of $\mathbb{Z}$ at p. We can choose an Eisenstein polynomial $f(x) = x^n + f_1x^{n-1} + \ldots + f_{n-1}x + f_n \in \mathbb{Z}_{(p)}[x]$ satisfying $|f_n|_p = p^{-1}$ and $|f_i|_p < 1$ for $1 \leq i \leq n-1$. Choose $\zeta \in \mathbb{Z}_{(p)}[\theta]$ such that $\theta \in \mathbb{Z}_{(p)}[\zeta]$. Then $F(x) \in \mathbb{Z}_{(p)}[x]$. Choose the matrix $A \in \mathrm{GL}_m(\mathbb{Z}_{(p)})$. Let

$$\begin{pmatrix} 1 \\ \zeta \\ \vdots \\ \zeta^{n-1} \end{pmatrix} = B \begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{pmatrix}$$

such that the matrix B is in $\mathrm{GL}_m(\mathbb{Z}_{(p)})$, then we have $\theta \in \mathbb{Z}_{(p)}[\zeta]$. Then all computations can be done via polynomials in ζ of degree $< n$ with coefficients in $\mathbb{Z}_{(p)}$ and ζ is just a formal symbol. Note that $\mathbb{Z} \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$ and $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, so $\mathbb{Z}_{(p)}$ is large enough to work with.

For a positive integer D, denote

$$C(D) = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, |a| \leq D, 0 < b \leq D, p \nmid b\right\} \subset \mathbb{Z}_{(p)}.$$

In our experiments, when randomly choosing elements of K, we choose a polynomial of ζ with coefficients in $C(D)$ for some $D > 0$.

7.2. Generating the Keys

It is easy to generate the keys needed in our signature scheme and public-key cryptosystem. We provide a relatively small example as follows.

For $n = 200$ and $p = 2$, we construct polynomials $f(x) = x^{200} + \sum_{i=1}^{199} f_i 2x^i + 2$ with $f_i \in \{0, 1\}$. The calculations are all in GP/PARI Version 2.13.0. For instance,

$$\begin{aligned} f(x) = {} & x^{200} + 2x^{197} + 2x^{195} + 2x^{190} + 2x^{189} + 2x^{185} + 2x^{180} + 2x^{179} + 2x^{175} \\ & + 2x^{174} + 2x^{171} + 2x^{167} + 2x^{163} + 2x^{161} + 2x^{158} + 2x^{157} + 2x^{153} + 2x^{152} \\ & + 2x^{150} + 2x^{149} + 2x^{145} + 2x^{144} + 2x^{143} + 2x^{141} + 2x^{138} + 2x^{137} + 2x^{135} \\ & + 2x^{132} + 2x^{131} + 2x^{126} + 2x^{122} + 2x^{120} + 2x^{116} + 2x^{115} + 2x^{114} + 2x^{113} \\ & + 2x^{111} + 2x^{109} + 2x^{108} + 2x^{106} + 2x^{105} + 2x^{104} + 2x^{98} + 2x^{95} + 2x^{93} \\ & + 2x^{90} + 2x^{88} + 2x^{87} + 2x^{85} + 2x^{83} + 2x^{82} + 2x^{81} + 2x^{79} + 2x^{73} + 2x^{72} \\ & + 2x^{66} + 2x^{63} + 2x^{62} + 2x^{61} + 2x^{59} + 2x^{58} + 2x^{57} + 2x^{55} + 2x^{53} \\ & + 2x^{52} + 2x^{51} + 2x^{49} + 2x^{48} + 2x^{44} + 2x^{42} + 2x^{38} + 2x^{36} + 2x^{35} + 2x^{34} \\ & + 2x^{32} + 2x^{30} + 2x^{28} + 2x^{27} + 2x^{24} + 2x^{23} + 2x^{13} + 2x^{12} + 2x^{11} + 2x^{10} \\ & + 2x^{9} + 2x^{8} + 2x^{7} + 2x^{6} + 2x^{5} + 2x^{3} + 2x + 2. \end{aligned}$$

Let $\zeta = 1 + \sum_{i=1}^{199} B_{2,i+1}\theta^i$ with $B_{2,i+1} \in \{0, 1\}$. We use the function “random()" to construct ζ in GP/PARI. Moreover, we get the matrix B and compute whether $B \in \mathrm{GL}_{200}(\mathbb{Z}_{(p)})$ or not. In this example, we construct 20 ζ’s and there are 9 ζ’s satisfying $\mathbb{Z}_{(2)}[\zeta] = \mathbb{Z}_{(2)}[\theta]$.

In our experimental results, for a fixed $f(x)$, the probability of $\mathbb{Z}_{(p)}[\zeta] = \mathbb{Z}_{(p)}[\theta]$ is about $1 - 1/p$. Note that we do not need to prove the probability. Our experimental results show that it is easy to construct B such that $\mathbb{Z}_{(p)}[\zeta] = \mathbb{Z}_{(p)}[\theta]$.

For $m = 100$, we construct a lattice $\mathcal{L} = \oplus_{i \in S} \mathbb{Z}_2 \theta^i$ with rank 100, where $S =$

$$\{0, 1, 6, 8, 9, 11, 14, 15, 17, 19, 20, 21, 22, 23, 25, 27, 28, 29, 30, 31, 32, 42, 43, 45, 47, 48,$$

$$49, 50, 51, 53, 54, 55, 61, 67, 70, 72, 75, 80, 82, 83, 84, 87, 89, 91, 96, 97, 98, 101, 104, 106$$

$$107, 108, 109, 110, 111, 112, 113, 114, 117, 118, 119, 120, 124, 126, 127, 130, 131, 132,$$

$$137, 138, 139, 140, 147, 149, 150, 152, 154, 156, 158, 159, 161, 162, 163, 164, 165, 167,$$

$170, 173, 177, 178, 180, 181, 183, 185, 187, 190, 191, 192, 194, 198\}$.

Let

$$\begin{aligned}\zeta =& 1 + \theta + \theta^{6} + \theta^{11} + \theta^{14} + \theta^{15} + \theta^{21} + \theta^{22} + \theta^{27} + \theta^{28} + \theta^{30} + \theta^{43} + \theta^{48} + \theta^{50} \\ &+ \theta^{51} + \theta^{55} + \theta^{61} + \theta^{70} + \theta^{83} + \theta^{84} + \theta^{91} + \theta^{97} + \theta^{101} + \theta^{104} + \theta^{109} + \theta^{112} \\ &+ \theta^{117} + \theta^{119} + \theta^{120} + \theta^{124} + \theta^{126} + \theta^{127} + \theta^{130} + \theta^{131} + \theta^{138} + \theta^{139} + \theta^{150} \\ &+ \theta^{154} + \theta^{161} + \theta^{167} + \theta^{170} + \theta^{177} + \theta^{180} + \theta^{187} + \theta^{190} + \theta^{191} + \theta^{194} + \theta^{198}.\end{aligned}$$

We have that $\mathbb{Z}_{(2)}[\zeta] = \mathbb{Z}_{(2)}[\theta]$. Moreover, let $\beta_i = \zeta^{i-1}$, we can construct a matrix $A \in \mathrm{GL}_{100}(\mathbb{Z}_{(2)})$ and get a basis $\beta_1, \ldots, \beta_{100}$ of $\mathcal{L}$ and all $\beta_1, \ldots, \beta_{100}$ have length 1.

7.3. Generating a Valid Signature is Easy

Using the example in the previous section, for any element in W (see Section 4), we find that we can always generate a valid signature with just one r. That is, for any generated $t \in W$ in our experiments, i.e., $t \in K - \mathcal{L}$ and $|t|_2 = \lambda_1 = 1$, we can always find a lattice vector $v \in \mathcal{L}$ such that $|t - v|_2 < 1$. So it is very easy to generate a valid signature for a legal user.

7.4. Generating Error Vectors in the Public-Key Cryptosystem

In our experiments, we choose $r = \sum_{i=0}^{199} r_i \zeta^i$, where the r_i can be chosen randomly. For instance, we assume $r_i \in \{0, 1, 2, 3\}$. We choose randomly 1000 such r's, the length distribution is as follows.

$\log_2 \lvert r\rvert_2$	0	$-\frac{1}{200}$	$-\frac{2}{200}$	$-\frac{3}{200}$	$-\frac{4}{200}$	$-\frac{5}{200}$	$-\frac{6}{200}$	$-\frac{7}{200}$	$-\frac{8}{200}$	$-\frac{9}{200}$	$-\frac{10}{200}$
# of r's	531	232	114	54	32	15	12	3	2	4	1

Thus, when we choose a suitable positive number δ, which depends on n, it is relatively easy to generate an error vector r needed in our public-key cryptosystem when δ is small. Notice that by modulo p attack, if δ is small, the schemes appear more secure. However, by Theorem 5.1, if δ is small, the size of plaintext should be also small to ensure the correct decryption. Our experiments show that the scheme can at least work well for short messages.

7.5. Parameters Selection

The main parameters in our public-key cryptosystem are n, m, δ and p. We first look at the distribution of error vectors. An error vector $r \in K$ is a polynomial in ζ of degree $< n$. We can think that r is a random polynomial in the uniformizer θ of degree $< n$:

$$r = r_0 + r_1\theta + r_2\theta^2 + \ldots + r_{n-1}\theta^{n-1}$$

with $r_i \in \mathbb{Z}_p$ for $0 \leq i \leq n-1$. Since

$$|r|_p = \max_{0\leq i\leq n-1}\{|r_i|_p \cdot |\theta|_p^i\} = \max_{0\leq i\leq n-1}\{|r_i|_p \cdot p^{-\frac{i}{n}}\},$$

we see that, $|r|_p = 1$ if $r_0 \in \mathbb{Z}_p^\times$. So the probability of $|r|_p = 1$ is $\frac{p-1}{p}$. If $r_0 \in p\mathbb{Z}_p$ and $r_1 \in \mathbb{Z}_p^\times$, then we have $|r|_p = p^{-\frac{1}{n}}$. So the probability of $|r|_p = p^{-\frac{1}{n}}$ is $\frac{1}{p} \cdot \frac{p-1}{p}$. Similarly, the probability of $|r|_p = p^{-\frac{i}{n}}$ is

$$\left(\frac{1}{p}\right)^i \cdot \frac{p-1}{p} \text{ for } 0 \leq i \leq n-1,$$

and the probability of $|r|_p \leq p^{-1}$ is $\frac{1}{p^n}$.

For $p = 2$, we see from above, the probability of $|r|_2 = 2^{-\frac{i}{n}}$ is $\frac{1}{2^{i+1}}$ for $0 \leq i \leq n-1$, and the probability of $|r|_2 \leq 2^{-1}$ is $\frac{1}{2^n}$. This explains very well the experimental results in section 7.4.

When choosing an error vector r in K, if the allowable error probability is at most $1/10$, i.e., to choose one suitable r, we need to produce at most 10 r's, then we suggest the parameters selected as follows. p should be at most 7. Of course, if we can allow smaller error probability, we will have more free choice of parameters.

For $p = 2$, $\delta = 0, 1/n, 2/n$, the error probability is $1/2, 1/4, 1/8$, respectively. Using the technique in section 8.1, we can always assume $m = n$. We can encrypt messages of 1, 2, 3 bits, respectively. To obtain a cryptographic security level at least 2^{80}, n should be at least 80.

For $p = 3$, $\delta = 0, 1/n$, the error probability is $1/3, 1/9$, respectively. $m = n \geq 50$.

For $p = 5$, $\delta = 0$, the error probability is $1/5$. $m = n \geq 34$.

For $p = 7$, $\delta = 0$, the error probability is $1/7$. $m = n \geq 28$.

7.6. A Toy Example

In order to illustrate the encryption and decryption of our public-key cryptosystem, we provide a simple example in this subsection.

For $n = 20$ and $p = 2$, we choose an Eisenstein polynomial $f(x) = x^{20} + 2x^{13} + 2x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^3 + 2x + 2$. Let θ be a root of $f(x)$. Let $\zeta = 1 + \theta + \theta^3$, and we can prove that $\mathbb{Z}_2[\zeta] = \mathbb{Z}_2[\theta]$. The minimal polynomial of ζ is

$$\begin{aligned}F(x) =& x^{20} - 20x^{19} + 190x^{18} - 1120x^{17} + 4555x^{16} - 13470x^{15} + 29670x^{14} \\ &- 48500x^{13} + 54972x^{12} - 26650x^{11} - 57366x^{10} + 202684x^9 - 378052x^8 \\ &+ 504970x^7 - 502444x^6 + 370306x^5 - 200173x^4 + 79034x^3 - 21942x^2 \\ &+ 3548x - 167.\end{aligned}$$

Choose $m = 4$, $\delta = \frac{1}{5}$, $\alpha_1 = 1$, $\alpha_2 = \theta$, $\alpha_3 = \theta^3$, $\alpha_4 = \theta^4$ and $\alpha_5 = \theta^2$ and $\alpha_i = \theta^{i-1}$ for $6 \leq i \leq 20$. We also choose a matrix

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

such that

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix}.$$

Set

$$\mathcal{L} = \mathbb{Z}_2 \cdot \beta_1 + \ldots + \mathbb{Z}_2 \cdot \beta_4 = \mathbb{Z}_2 \cdot \alpha_1 + \ldots + \mathbb{Z}_2 \cdot \alpha_4.$$

By simple computation, $\beta_1 = 1$ and $\beta_2 = \zeta$.

Denote $c = 755873885678037304696930874820307$, and we use $\{1, \zeta, \ldots, \zeta^{19}\}$ to represent β_3 and β_4 as follows.

$$\begin{aligned}
\beta_3 = &- 27108923760453500594114368147861/c \cdot \zeta^{19} \\
&+ 521865611374523349857486121811703/c \cdot \zeta^{18} \\
&- 4760849839441657400327526846175084/c \cdot \zeta^{17} \\
&+ 26816406582145252327839682159453914/c \cdot \zeta^{16} \\
&- 103574920689378774115698374019031382/c \cdot \zeta^{15} \\
&+ 288537866250541205172041717367828630/c \cdot \zeta^{14} \\
&- 591666988994440980962096953798261066/c \cdot \zeta^{13} \\
&+ 880486236199407313977260487157615142/c \cdot \zeta^{12} \\
&- 847065367242050264224160859445656349/c \cdot \zeta^{11} \\
&+ 108784039738974345225480374806101259/c \cdot \zeta^{10} \\
&+ 1622622535668312013674731473089538162/c \cdot \zeta^{9} \\
&- 4291035648498285373550387869383382644/c \cdot \zeta^{8} \\
&+ 7094982023780788047526123629913039130/c \cdot \zeta^{7} \\
&- 8499558345651875542941790231225642428/c \cdot \zeta^{6} \\
&+ 7430432812182187849978710739691760199/c \cdot \zeta^{5} \\
&- 4649814507849649080544670183272509081/c \cdot \zeta^{4} \\
&+ 2064853893471783755461823390280876643/c \cdot \zeta^{3} \\
&- 649379287606029887924510269811865169/c \cdot \zeta^{2} \\
&+ 123558509986637049018722991077975950/c \cdot \zeta \\
&- 5663239729863841192248147669379477/c,
\end{aligned}$$

$$\begin{aligned}\beta_4 = &-14485353108585552555664586328940/c \cdot \zeta^{19}\\ &+ 28214236055428082467685777002514 8/c \cdot \zeta^{18}\\ &- 26043356620444016295641448385812 34/c \cdot \zeta^{17}\\ &+ 148540850399194745019031595881219 40/c \cdot \zeta^{16}\\ &- 58145345752844012352543292792092682/c \cdot \zeta^{15}\\ &+ 164358157674744212292212426862311214/c \cdot \zeta^{14}\\ &- 342605897386084548079649731170297612/c \cdot \zeta^{13}\\ &+ 520399035260841934352319686515883387/c \cdot \zeta^{12}\\ &- 519018682404601896574333009249126758/c \cdot \zeta^{11}\\ &+ 108673223779901487310589235888361376/c \cdot \zeta^{10}\\ &+ 890836547840047572823549831049505128/c \cdot \zeta^{9}\\ &- 246453973398019631668234166772791006 9/c \cdot \zeta^{8}\\ &+ 416679988098285167655759163944545575 0/c \cdot \zeta^{7}\\ &- 509646147461937933882176480855699844 0/c \cdot \zeta^{6}\\ &+ 456121948490165303524711665697506378 2/c \cdot \zeta^{5}\\ &- 293076036459407139698849422188766181 2/c \cdot \zeta^{4}\\ &+ 133630341074283639564648568185546307 8/c \cdot \zeta^{3}\\ &- 43102997516162509373185924026602832 8/c \cdot \zeta^{2}\\ &+ 85030353159786174819149798559520150/c \cdot \zeta\\ &- 3439240388429674931731785244955445/c.\end{aligned}$$

Public key is set to be: $(F(x), \delta = \frac{1}{5}, (\beta_1, \beta_2, \beta_3, \beta_4))$.

Private key is set to be: $(f(x), A, (\alpha_1, \alpha_2, \ldots, \alpha_{20}))$.

Encryption: For the plaintext $(1,1,0,1) \in \{0,1\}^4$, Alice first chooses $r = \zeta^{19} + \zeta^{18} + 3\zeta^{16} + 2\zeta^{15} + 3\zeta^{14} + \zeta^{13} + 3\zeta^{12} + 2\zeta^{10} + 3\zeta^{9} + 2\zeta^{7} + 2\zeta^{6} + 3\zeta^{4} + 3\zeta^{3} + 1 \in K - \mathcal{L}$ with $2^{-1} < |r|_2 = 2^{-\frac{1}{4}} < 2^{-\delta}$, computes the ciphertext

$$C = \beta_1 + \beta_2 + \beta_4 + r \in K$$

as a polynomial in ζ and sends C to Bob.

Decryption: When Bob receives the ciphertext C, using the orthogonal basis $(\alpha_1, \ldots, \alpha_{20})$, he computes

$$\begin{aligned}C = &\,694593336\theta^{19} + 3645400020\theta^{18} + 7672558669\theta^{17} + 12564257705\theta^{16}\\ &+ 17775907726\theta^{15} + 22344434481\theta^{14} + 24831163382\theta^{13} + 24727330889\theta^{12}\\ &+ 24329033350\theta^{11} + 23536540088\theta^{10} + 22276159912\theta^{9} + 20538044444\theta^{8}\\ &+ 18408250085\theta^{7} + 16117496655\theta^{6} + 14081433327\theta^{5} + 12919864471\theta^{4}\\ &+ 12066189903\theta^{3} + 9363862258\theta^{2} + 6772589923\theta + 239627447.\end{aligned}$$

By Theorem 3.6, he computes a lattice vector $v = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$ which is the closest one to C. The plaintext is

$$(1,1,1,1) \cdot A^{-1} \equiv (1,1,0,1) \pmod 2.$$

8. IMPROVEMENTS TO THE PUBLIC-KEY SCHEME

In this section, we present some improvements to increase the efficiency of the public-key encryption scheme.

8.1. Expanding the Plaintext

Note that we require $j_i \leq \delta n$ for $1 \leq i \leq m$ for which the decryption is correct, see Theorem 5.1. Usually, the number of indices $j_i (1 \leq i \leq n)$ such that $j_i \leq \delta n$ is small, so we can only encrypt short messages.

For simplicity, let us suppose the first $l (< m)$ indices $j_i (1 \leq i \leq l)$ satisfying $j_i \leq \delta n$. Checking carefully the proof of Theorem 5.1, if we let the transform matrix A between the public basis and private basis have the property that those last $m - l$ elements of the first l columns of A^{-1} are divisible by p (i.e., let $A^{-1} = (b_{ij})$ where the (i, j)-element of A^{-1} is b_{ij}, then we require $b_{ij} \equiv 0 \pmod{p}$ for $l + 1 \leq i \leq m$ and $1 \leq j \leq l$), then the decryption algorithm can correctly recover the first l components of the plaintext. Of course, this will decrease partially the randomness of the transform matrix A (i.e., we prespecify $l(m - l)$ elements of A^{-1}). However, the advantage is that we can expand the plaintext via a random padding as follows.

We revise the original cryptosystem a bit. In the key generation, after generating j_i's and δ, denote by I the set of indices j_i with $j_i \leq \delta n$. Alice additionally chooses a set $Z \subseteq I$ and sends the size $l = \#Z$ to Bob. Then Alice can permute the set of α_i's such that $\{\alpha_1, \cdots, \alpha_l\} = \{\theta^{j_i} | j_i \in Z\}$ and generate public key as before.

In the encryption algorithm, the plaintext becomes $(a_1, \ldots, a_l) \in \{0, 1, \ldots, p - 1\}^l$. For any plaintext $(a_1, \ldots, a_l)$, Bob firstly extends it into

$$(a_1, \ldots, a_m) \in \{0, 1, \ldots, p - 1\}^m$$

with random $a_{l+1}, \ldots, a_m$, then encrypts it as before. In the decryption algorithm, Alice just accepts the first l components of the recovered vector.

8.2. The Coefficient Explosion Problem

For the open basis $(\beta_1, \ldots, \beta_m)$, since we finally perform a modulo p operation in the decryption procedure, it is obvious that we can publish $(\beta_1, \ldots, \beta_m) \pmod{p}$ only. This can solve the problem of coefficient explosion in the open basis $(\beta_1, \ldots, \beta_m)$. For example, in the section 7.6, we can publish the open basis as follows.

$$(\beta_1, \beta_2, \beta_3, \beta_4) \pmod{2} = (1, \zeta, \zeta^{19} + \zeta^{18} + \zeta^{11} + \zeta^{10} + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + 1, \zeta^{12} + \zeta^8 + 1).$$

Another problem is the coefficient explosion of the open field polynomial $F(x)$ of K. For the private field polynomial $f(x)$, we can choose small numbers as coefficients of $f(x)$. But, in general, $F(x)$ will have large coefficients. The example in the section 7.6 yields this phenomenon.

For an element $r \in K$, we use the method in section 2.2 to compute $|r|_p$. I.e.,

$$|r|_p = |N_{K/\mathbb{Q}_p}(r)|_p^{1/n},$$

and $N_{K/\mathbb{Q}_p}(r)$ is the determinant of the $n \times n$-matrix M of the multiplication-by-r linear map. That is, multiply every element in the set $\{1, \zeta, \ldots, \zeta^{n-1}\}$ by r, write the results as $\mathbb{Z}_p$-linear combinations of $1, \zeta, \ldots, \zeta^{n-1}$. For a random r, the probability of $|r|_p \leq p^{-1}$ is $1/p^n$, see section 7.5. So it is impossible to get a r with $|r|_p \leq p^{-1}$. Hence, computing the determinant of the $n \times n$-matrix $M = (c_{ij})$, for any element in M, we can drop the part divisible by p^n. That is, we can only compute the determinant of the $n \times n$-matrix $\overline{M} = (c_{ij} \pmod{p^n})$ without affect the final answer. Therefore, we can only publish $F(x)$ $\pmod{p^n}$.

Furthermore, for example, if we choose $p = 2, \delta = 2/n$, we can drop the parts divisible by 2^3. We can only publish $F(x) \pmod{2^3}$.

Therefore, using this technique, we solve perfectly the coefficient explosion problem in the public key and norm computation.

9. CONCLUSION

LVP and CVP in local fields may have further applications in cryptography and other areas. In this paper, we just mention one possibility. The signature scheme and the public-key cryptosystem constructed in this paper are just an illustration. LVP and CVP in local fields are new computationally difficult mathematical problems, it is worth for further study and there is much work to do.

For example, is there a p-adic analogue of the Gram-Schmidt orthogonalization process in Euclidean spaces? Notice that the Gram-Schmidt orthogonalization is only for an l_2-norm, not for any norm. We suspect that there is a p-adic orthogonalization process for the norm defined in this paper. Is there a p-adic analogue of the LLL algorithm for lattices in Euclidean spaces? Is there a p-adic analogue of the Minkowski's theorems for lattices in Euclidean spaces [24]? More importantly, we do not know whether the LVP and CVP are NP-hard, if so, how to do complexity reduction. We believe that there are many other problems to study.

FUNDING

This work was supported by National Natural Science Foundation of China (No. 12271517) and National Key Research and Development Project of China (No. 2018YFA0704705).

CONFLICT OF INTEREST

The authors of this work declare that they have no conflicts of interest.

REFERENCES

1. J. W. S. Cassels, *Local Fields* (Cambridge University Press, Cambridge, 1986).
2. Y. Deng, L. Luo and G. Xiao, 'On some computational problems in local fields," Cryptology ePrint Archive, Report 2018/1229, http: //eprint.iacr.org/2018/1229 (2018).
3. Y. Deng, L. Luo, Y. Pan and G. Xiao, "On some computational problems in local fields," J. Syst. Sci. Comp. **35**, 1191–1200 (2022).
4. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theo. **22**, 644–654 (1976).
5. L. Ducas and P. Nguyen, "Learning a zonotope and more: cryptanalysis of NTRUSign countermeasures," In: X. Wang and K. Sako (Eds.), ASIACRYPT 2012, LNCS **7658**, 433–450 (2012).
6. K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison and C. Petit, "Supersingular isogeny graphs and endomorphism rings: reductions and solutions," In: J.B. Nielsen and V. Rijmen (Eds.), EUROCRYPT 2018, LNCS **10822**, 329–368 (2018).
7. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theo. **31**, 469–472 (1985).
8. O. Goldreich, S. Goldwasser and S. Halevi, "Public-key cryptosystems from lattice reduction problems," In: B. S. Kaliski Jr. (Ed.), Adv. Crypt.- CRYPTO'97, LNCS **1294**, 112–131 (1997).
9. N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, Second edition (Springer, New York, 1984).
10. N. Koblitz, "Elliptic curve cryptosystems," Math. Comput. **48**, 203–209 (1987).
11. N. Koblitz, "Hyperelliptic cryptosystems," J. Cryptology **1**, 139–150 (1989).
12. N. Koblitz, *Algebraic Aspects of Cryptography* (Springer, Berlin, 1998).
13. D. Kohel, *Endomorphism Rings of Elliptic Curves over Finite Fields*, Ph.D. thesis (University of California, Berkeley, 1996).
14. T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," In: C. G. Guenther (Ed.), Adv. Crypt. - EUROCRYPT'88, LNCS **330**, 419–453 (1988).
15. R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Prog. Rep. **42-44**, 114–116 (Jet Propulsion Laboratory, 1978).
16. D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems, A Cryptographic Perspective* (Kluwer, Boston, 2002).
17. V. S. Miller, "Use of elliptic curves in cryptography," In: H.C. Williams (Ed.), Adv. Crypt. - CRYPTO'85, LNCS **218**, 417–426 (1986).
18. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Third edition (Springer, New York, 2004).

19. P. Nguyen, "Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto'97," In: M. Wiener (Ed.), Adv. Crypt. - CRYPTO'99, LNCS **1666**, 288–304 (1999).
20. P. Nguyen and O. Regev, "Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures," In: S. Vaudenay (Ed.), EUROCRYPT 2006, LNCS **4004**, 271–288 (2006).
21. R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Comm. ACM, **21**, 120–126 (1978).
22. J.-P. Serre, *Local Fields* (Springer, New York, 1979).
23. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE Comp. Soc. Press, pp. 124–134 (Los Alamitos, CA, 1994).
24. C. L. Siegel, *Lectures on the Geometry of Numbers* (Springer, Berlin, 1989).
25. A. Weil, *Basic Number Theory*, Third edition (Springer, New York, 1974).
26. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

Publisher's Note. Pleiades Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.