Commun. Math. Res.
doi: 10.4208/cmr.2025-0025

Vol. **41**, No. 4, pp. 297-310
December 2025

An Explicit Construction of Orthogonal Basis in p-adic Fields

Chi Zhang[1,2,*] and Yingpu Deng[1,2]

[1] *State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, P.R. China.*
[2] *School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, P.R. China.*

Received 16 June 2025; Accepted 10 November 2025

Abstract. In 2021, the p-adic signature scheme and public-key encryption cryptosystem were introduced. These schemes have good efficiency but are shown to be not secure. The attack succeeds because the extension fields used in these schemes are totally ramified. In order to avoid this attack, the extension field should have a large residue degree. In this paper, we propose a method of constructing a kind of specific orthogonal basis in p-adic fields with a large residue degree, which would be helpful to modify the p-adic signature scheme and public-key encryption cryptosystem.

AMS subject classifications: Primary 11F85; Secondary 94A60

Key words: Local field, orthogonal basis, p-adic lattice.

1 Introduction

Since Shor [13] proved that the classical public-key cryptosystems such as RSA and ElGamal would be broken by future quantum computer, researchers have been dedicated to finding cryptographic primitives which are quantum-resistant. In 2022, NIST [11] announced four algorithms which passed the third round of post-quantum cryptography standardization solicitation and began the fourth

[*] Corresponding author. *Email addresses:* `zhangchi171@mails.ucas.ac.cn` (C. Zhang), `dengyp@amss.ac.cn` (Y. Deng)

round. They are CRYSTALS-Kyber [2], CRYSTALS-Dilithium [6], Falcon [8] and SPHINCS$^+$ [1]. Three of them are lattice-based and one of them is hash-based. The lack of diversity among post-quantum assumptions is widely recognized as a big, open issue in the field. Therefore, finding new post-quantum assumptions is of vital significance.

The p-adic numbers $\mathbb{Q}_p$ were invented by Hensel in the late 19th century. The concept of a local field is an abstraction of the field $\mathbb{Q}_p$. Local fields provide a natural tool to solve many number-theoretic problems. They are ubiquitous in modern algebraic number theory and arithmetic geometry. Lattices can also be defined in local fields such as p-adic fields, see [15]. Interestingly, p-adic lattices possess some properties which lattices in Euclidean spaces do not have, see [17]. However, applications of p-adic lattices in cryptography were developed only recently.

In 2021, by introducing a trapdoor function with an orthogonal basis of a p-adic lattice, Deng *et al.* [5] constructed the first signature scheme and public-key encryption cryptosystem based on p-adic lattices. As the p-adic analogues of the lattices in Euclidean spaces, it is reasonable to expect hard problems in p-adic lattices to be quantum-resistant, which might provide new alternative candidates to construct post-quantum cryptographic primitives.

The experimental results [5] demonstrated that the new schemes achieve good efficiency. As for security, Zhang [16] found that these schemes are not secure because the extension fields used in these schemes are totally ramified. In order to avoid this attack, he suggested that the extension field should have a large residue degree.

In a totally ramified extension field $K/\mathbb{Q}_p$, a uniformizer π generates an orthogonal basis of K. But in a general extension field $K/\mathbb{Q}_p$, we can not find an orthogonal basis of K as easily as in a totally ramified extension field. Therefore, the crucial point of such a scheme is to construct an orthogonal basis of K.

Given a extension field K over $\mathbb{Q}_p$ of degree n, we can use the Round 2 Algorithm [4] or the Round 4 Algorithm [7] to obtain a basis of the maximal order $\mathcal{O}_K$ and then compute its orthogonal basis. However, these algorithms involve computation of large matrices. They require storage of the order of n^3 in the worst case.

In order to reduce the storage requirement, we consider the problem from another perspective. Instead of trying computing the maximal order, we construct an orthogonal basis directly and then compute the extension field it generates. The storage requirement of this method is of the order of n^2 in the worst case.

This paper is organized as follows. In Section 2, we recall some basic definitions. In Section 3, we give an equivalent condition for orthogonal basis in the