AI Methods for Post-Quantum Cryptography

Supervisor: Keqin Liu

Members: Bo Wang, Yuan Cheng, Xingyue Fan, Yongrun Huang, Chang Liu, Jialun Luo, Yexi Ren

SurfCode: SURF-2025-0061

Abstract

This poster presents the background and a series of possible evolutionary methods of sieving algorithm (bgj3). We begin with reproducing the original random filtering method, then introduce a deterministic Hybrid-Sieve to replace the randomness with the algebraic structure of the dual lattice. Finally, we explore a powerful shift using Reinforcement Learning (RL), where an intelligent agent learns to produce high quality center sieve vectors.

1. Introduction

The security of post-quantum cryptography hinges on the hardness of the **Shortest Vector Problem (SVP)**. Sieving algorithms are the most powerful tools for solving SVP, but their performance is bottlenecked by a single, critical task: efficiently finding pairs of vectors $(\mathbf{u}, \mathbf{v})$ that combine to form a shorter vector $\mathbf{u} \pm \mathbf{v}$ from a list of billions: $2^{0.2075n+O(n)}$.

Our Contribution: A Principled Evolution

This work charts a clear trajectory, moving from blind randomness towards structured, intelligent search. We demonstrate this evolution through three methodologies:

1. **Baseline: The Random Sieve**
   - **Core Idea:** Filters vectors using random spherical caps.
   - **Represents:** The current "brute-force" state-of-the-art.
2. **Innovation: The Hybrid Sieve**
   - **Core Idea:** Replaces randomness with **structure**. We use vectors from the **dual lattice** ($\mathcal{L}^*$) to create a deterministic Voronoi partition.
   - **Represents:** A more efficient, reproducible, and lattice-aware algorithm.
3. **Paradigm Shift: The RL-based Sieve**
   - **Core Idea:** Elevates the search to an **intelligent** process. A Reinforcement Learning (RL) agent learns an optimal policy to "walk" on the lattice, actively seeking out shorter vectors.
   - **Represents:** The future of SVP solvingan adaptive and targeted exploration.

This progression illustrates a clear path from random searching to structurized and intelligent exploration.

2. Method

Algorithm 1 AllPairSearch bgj3 (Baseline)

Require: A list L of N_0 lattice vectors, repetitions (B_0, B_1, B_2), radii $(\alpha_0, \alpha_1, \alpha_2)$, goal norm l.

Ensure: A list of reducing pairs in L.

```
N ← ∅
for i = 0, ..., B_0 − 1 do
    Pick a random center c_0 ∈ S^{n−1}
    L_i ← {v ∈ L | v passes F_{c_0,α_0}}
    for j = 0, ..., B_1/B_0 − 1 do
        Pick a random center c_1 ∈ S^{n−1}
        L_ij ← {v ∈ L_i | v passes F_{c_1,α_1}}
        for k = 0, ..., B_2/B_1 − 1 do
            Pick a random center c_2 ∈ S^{n−1}
            L_ijk ← {v ∈ L_ij | v passes F_{c_2,α_2}}
            N ← N ∪ {(u, v) ∈ L_ijk^2 | ‖u ± v‖ < l}
        end for
    end for
end for
return N
```

3. Key Results

1. First itemtext
2. Second itemtext
3. Last itemtext

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1. First itemtext
2. Second itemtext

4. Examples

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

$$\int \vec{F} \cdot d\vec{q} = -U \tag{1}$$

5. Future Work

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

1. First itemtext
2. Second itemtext

6. Plots

References

[1] Zhao, Z., Ding, J., Yang, B.-Y. (2025). Sieving with Streaming Memory Access. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(2), 362-384. Available from: https://doi.org/10.46586/tches.v2025.i2.362-384

[2] Chinberg, T., Kalbach, A. LLLAlgorithmforLatticeBasisReduction. Available from: arXiv:2410.22196v2 [math.NT] 20 Nov 2024.