Probabilistic Computing in Cryptanalysis

Better approximations for the Closest Vector Problem

Why does integer factorisation matter?

Modern digital security relies heavily on the **integer factorisation** problem. Encryption schemes like RSA remain secure because multiplying two large primes is easy, but reversing the process, i.e. finding those primes from their product (a semiprime), is extremely hard for classical computers. While Shor's algorithm could solve this efficiently on a quantum computer, we lack the large-scale, fault-tolerant quantum hardware needed to run it.

Researchers are therefore exploring alternatives. One promising approach is **Schnorr's lattice-based factoring algorithm [1]**, which reframes factoring as a lattice problem called the **Closest Vector Problem (CVP)**.

If the CVP can be found to be solved efficiently, such a breakthrough would pose a fundamental risk not only to legacy cryptographic regimes that depend on prime factorisation, such as RSA, but also modern cryptographic methods for post-quantum cryptographic (PQC), such as the ML-KEM[1] and ML-DSA[2] frameworks standardised by NIST.

Lattices and the CVP

A **lattice** is a multi-dimensional grid of points. The CVP asks: given a target point in space, which lattice point is closest? In factoring, researchers build **prime lattices**, where points near the target vector are strongly correlated with information used to reveal hidden prime factors. As semiprimes grow, these lattices become vast and complex, making the search for the closest point computationally demanding.

[1] https://csrc.nist.gov/pubs/fips/203/final
[2] https://csrc.nist.gov/pubs/fips/204/final

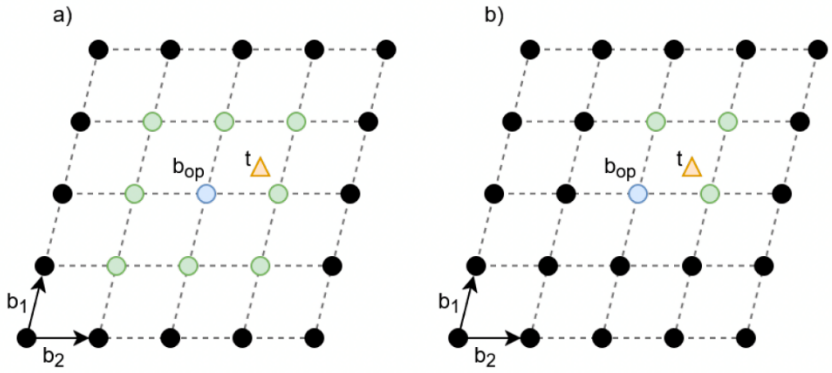


Figure 1: (a) The neighborhood (green) of the CVP approximation (blue) in a 2-dimensional lattice. Each neighbor can be reached by adding or subtracting each basis vector at most once. (b) The reduced neighborhood (green) of the CVP approximation (blue). Each basis vector is assigned a direction (both positive in this example) and each neighbor can be reached by adding or subtracting each basis vector in its assigned direction at most once.

Probabilistic computing to the rescue

Classical computers use bits (0 or 1). Quantum computers use qubits (superpositions of 0 and 1). This research makes use of a third paradigm: the **probabilistic bit, or p-bit**.

A p-bit fluctuates randomly between 0 and 1, but with a controllable bias influenced by its neighbours' values. Networks of p-bits act as natural optimisation systems: as they interact and flip, the network tends toward low-energy states that correspond to optimal solutions for hard problems like CVP. This makes probabilistic computing a powerful **hardware accelerator** for cryptanalysis.

Imagine a lattice as a **dark, hilly landscape** and the target vector as a **beacon in a valley**. A classical computer searches with a flashlight which makes the search slow and local. A probabilistic computer releases thousands of jittering searchers across the hills. These naturally gravitate toward the lowest point near the beacon, revealing the solution far faster than a spot-by-spot search.

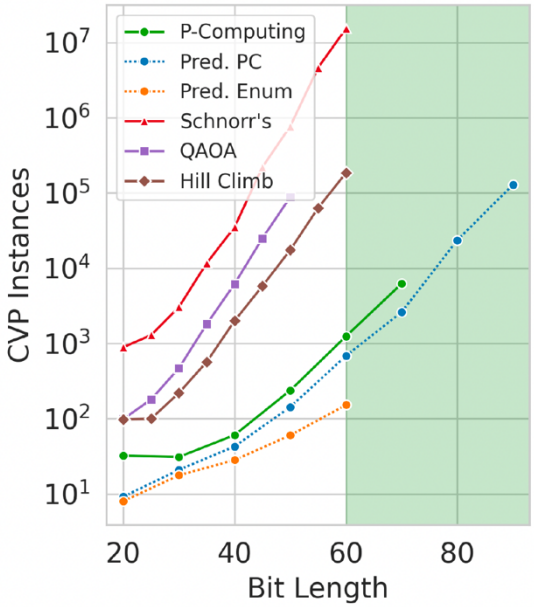
The two-step refinement process

1. Initial guess: Use Babai's Nearest Plane algorithm [2] to find an approximate lattice point near the target.
2. Neighbourhood search: Deploy a p-bit network to explore nearby lattice points, refining the guess to find the closest possible vector.

Our research paper reports significant improvements in CVP refinement. Some of the highlights are:

- The probabilistic approach finds the best point within the search neighbourhood in time that scales polynomially with problem size.

- During the collection phase, the method required **up to 100x fewer lattice instances** compared to previous heuristic approaches to lattice-based factoring.



- Experimentally showed that points closer to the target vector strongly increase the likelihood of finding correct prime relations (**sr-pairs**).
- While refinement is efficient, the overall factoring process still faces exponential growth in lattice count and does not outperform the best-in-class General Number Field Sieve (GNFS) [3] for large-scale factoring.

Significance of results

As organisations transition to an era of PQC, lattice-based cryptographic methods will underpin future data security. This research by Quantum Dice demonstrates that probabilistic computing hardware can accelerate lattice-based optimisation. Although scaling remains a challenge, the 100-fold improvement in lattice instance efficiency marks a meaningful step forward in addressing the CVP, emphasising the relevance of probabilistic computing for cryptographic security.

Interested? Read the full article on ArXiv: https://arxiv.org/abs/2510.19390

Bibliography

[1] C. P. Schnorr, “Fast Factoring Integers by SVP Algorithms, corrected,” *Cryptology ePrint Archive*, 2021. https://eprint.iacr.org/2021/933.
[2] László Babai, “On Lovász’ lattice reduction and the nearest lattice point problem,” *Combinatorica*, vol. 6, no. 1, pp. 1–13, Mar. 1986, doi: https://doi.org/10.1007/bf02579403.
[3] A. Lenstra and H. Lenstra, Eds., *The development of the number field sieve*. Springer Nature, 1993. doi: https://doi.org/10.1007/bfb0091534.