Cryptography in a Post-Quantum World: Exploring New Polynomials for the SVP in Ideal Lattices

Katharine Ahrens
Advised by Dr. Ernest Stitzinger and Dr. Scott Batson
Department of Mathematics, North Carolina State University

Background

An n-dimensional lattice $\mathcal{L}$ is the set of all integer linear combinations of n linearly independent (non-unique) basis vectors. The **shortest vector problem (SVP)** requires finding a vector of minimal Euclidean norm in $\mathcal{L}$. The SVP is widely conjectured to a be quantum hard problem. While in theory $\mathcal{L}$ is an arbitrary lattice, in practice $\mathcal{L}$ is taken to be a special class of lattice called an **ideal lattice**, which improves cryptosystem efficiency in time and space. It is conjectured, although not proven, that the SVP is as hard in ideal lattices as in the general case.

A common approach to the SVP is use of a lattice reduction algorithm such as the Lenstra-Lesntra-Lovasz (LLL), which works by converting a "bad" (non-orthogonal) basis to a "good" (orthogonal) basis. These algorithms solve an approximate version of the SVP in polynomial time in the dimension of the lattice.

Motivation

Lattice-based cryptosystems are a leading candidate for post-quantum cryptographic schemes. The polynomials used to construct the ideal lattice are nearly always the **cyclotomic polynomials** $\phi_n(x)$. However, recent concerns [?] have been raised about the inherent security of the cyclotomic construction.

Here, we perform some initial SVP experiments for a new class of polynomials $x^n - p$, for integer n and prime p, and compare the effectiveness of LLL on ideal lattices generated with $\phi_n(x)$ and $x^n - p$ on two classes of lattice bases.

Cyclotomics: Random Basis

The authors of [?] propose a standard way of generating ideal lattices, which prior to 2013 did not exist. They use the **root Hermite factor** as a measure of algorithm performance. As a baseline for our other experiments, we reimplemented their generation algorithm in Sage and solved the SVP with LLL.

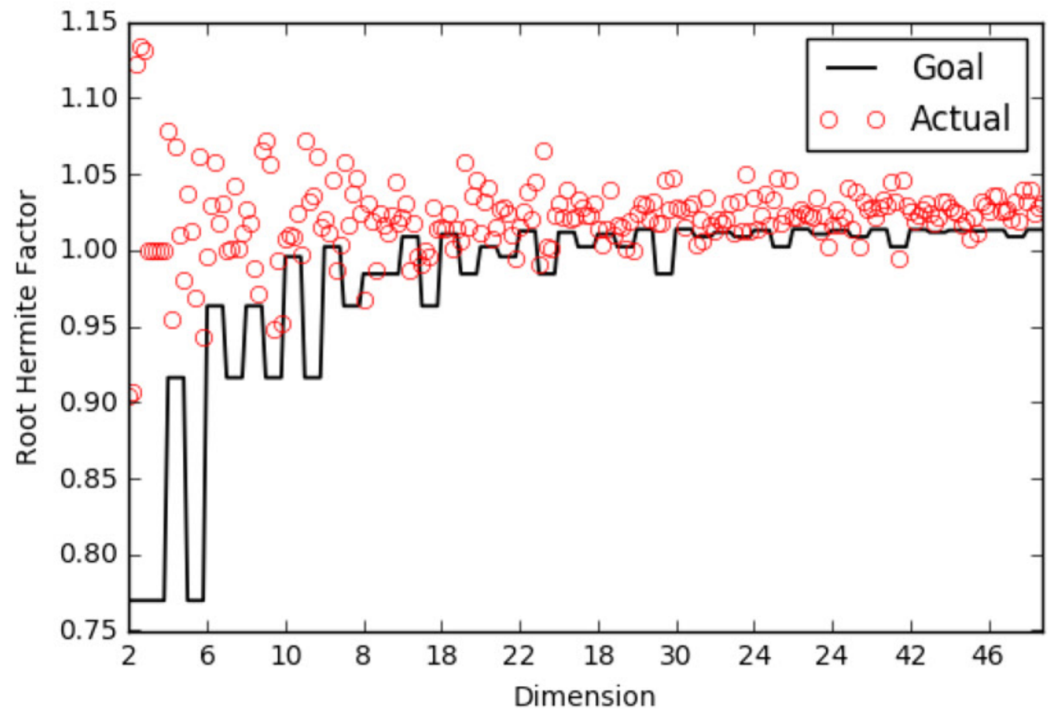


Figure 1: SVP trials for 5 random generators in each dimension $\phi(i)$ for $i < 50$.

$x^n - p$: Random Basis

We adapted the algorithm of [?] for $x^n - p$. We show only the results for $p = 19$ below, since the SVP quality seemed independent t of the choice of p; a 90-digit prime yielded a very similar plot to $p = 19$.

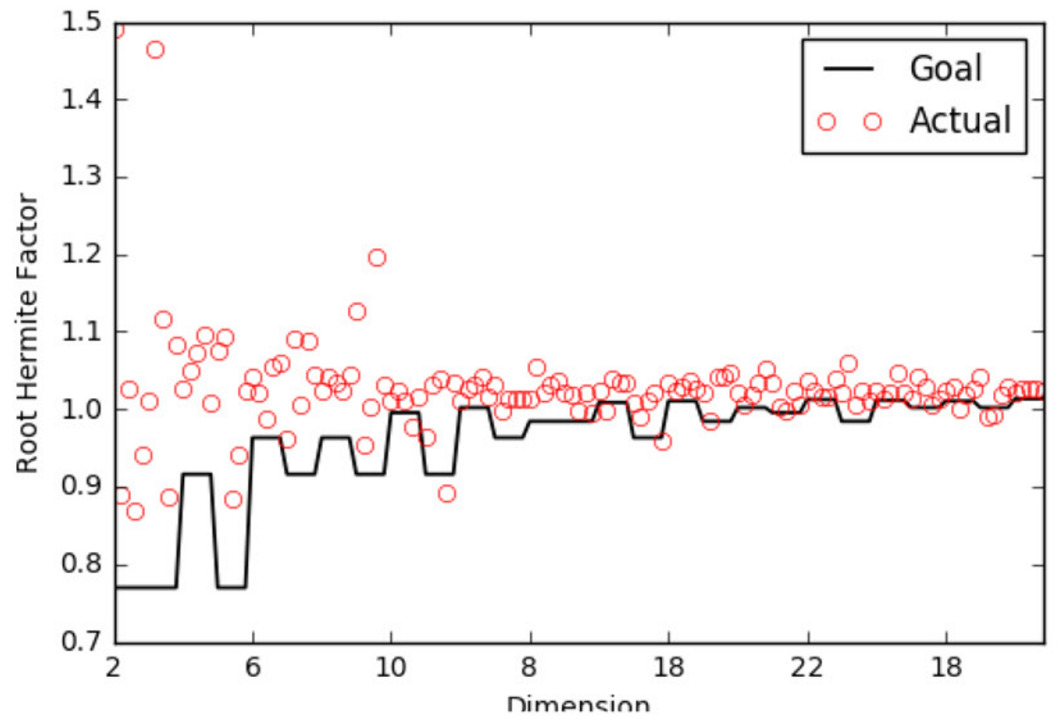


Figure 2: SVP trials for 5 random generators in each dimension $\phi(i)$ for $i < 30$. where $p = 19$.

Cyclotomics: Rotation Basis

A **rotation basis** is a highly structured basis constructed from a random generator. As shown in [?], most of the time the LLL simply returns the original generator. We sought to examine the quality of this shortest vector.

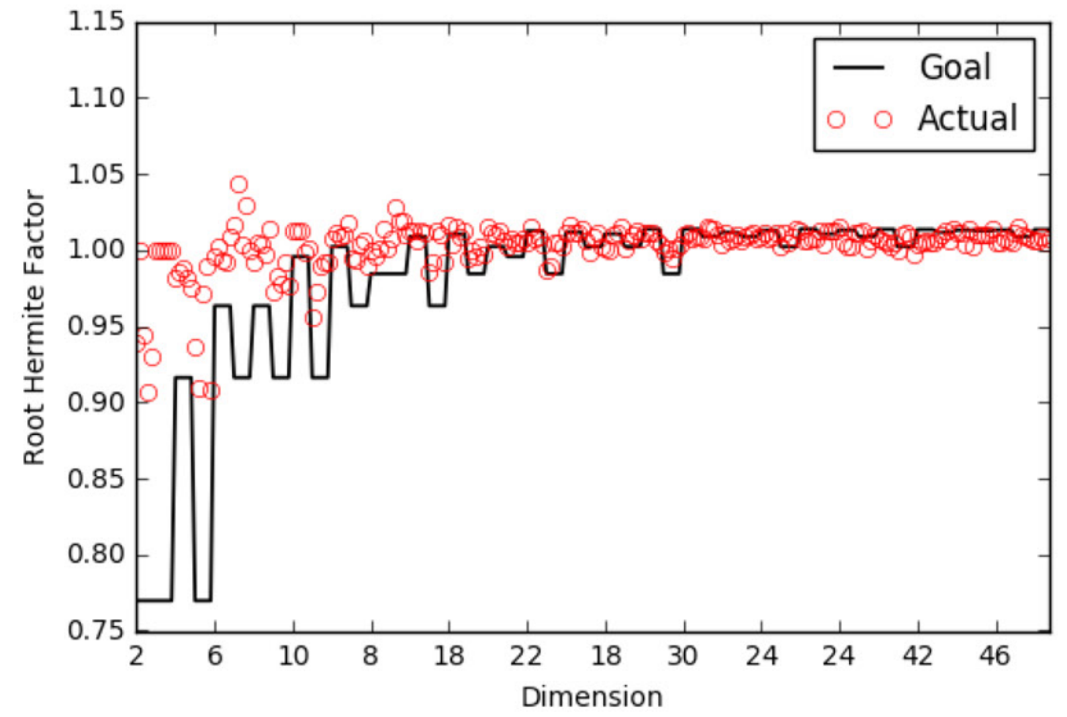


Figure 3: SVP trials for 5 random generators in each dimension $\phi(i)$ for $i < 50$.

$x^n - p$: Rotation Basis

Constructing the rotation basis matrix for our class of polynomials involves knowing for which n, p pairs $x^n - p$ has an integral power basis. We completely categorized these n, p pairs for $n < 40, p < 500$ using Sage and repeated the SVP experiments.

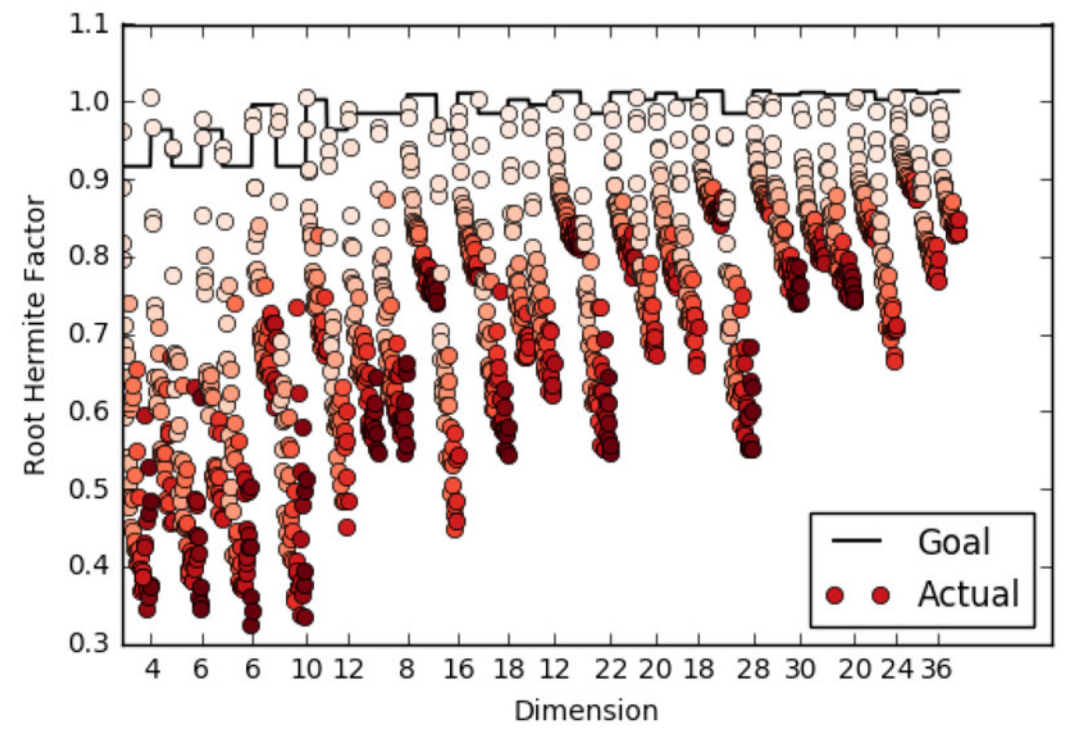


Figure 4: SVP trials for 1 random generator for dimension $\phi(n), n < 40$ and each $p < 500$ which gives an integral power bases. Darker red corresponds to a larger prime.

Conclusions

Our work gives some indiction of the challenges and considerations which must be taken into account when adapting ideal lattice constructions over cyclotomics to other polynomial rings. For random bases, it appears that $x^n - p$ behaves much like the cyclotomic case. The value of p does not appear to matter, as we obtained nearly identical results for a 2-digit and a 90-digit prime.

In the rotation basis case, the SVP results for $x^n - p$ have a vastly different pattern than the cyclotomic case and the value of p matters very much, with much smaller root Hermite factors for larger p.

Future Work

We plan to consider the following:

- Examining whether the results hold over other reduction algorithms such as BKZ.
- Investigating the security of using $x^n - p$ in a cryptosystem such as Soliloquy [**?**].
- Using the structure of the rotation basis matrix (for either polynomial class) as the private key of some cryptosystem.

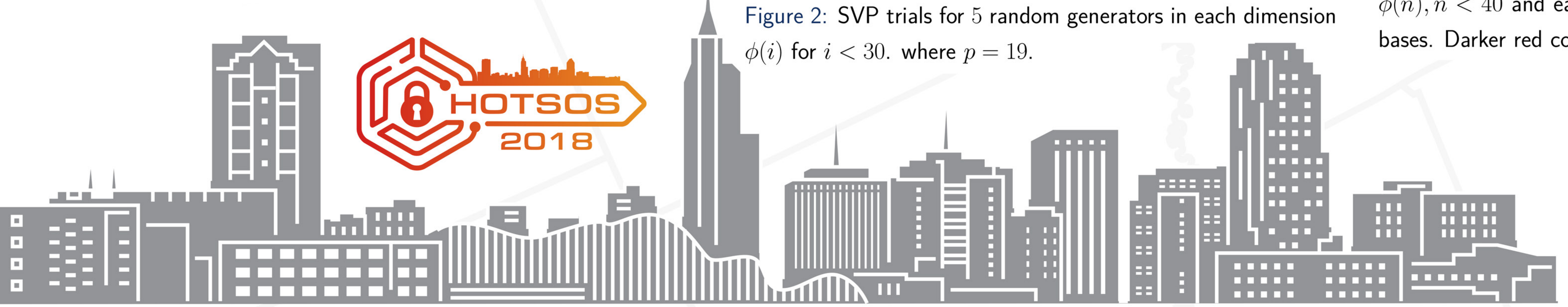
Selected References

[1] Peter Campbell, Michael Groves and Dan Shepherd. *Soliloquy: A Cautionary Tale.*

[2] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal. *NTRU Prime: reducing attack surface at low cost.*

[3] Thomas Plantard and Michael Schneider. "Creating a Challenge for Ideal Lattices".

[4] Scott C. Batson. "On the Relationship Between Two Embeddings of Ideals into Geometric Space and the Shortest Vector Problem in Principal Ideal Lattices." PhD Thesis.



5TH ANNUAL HOT TOPICS in the SCIENCE OF SECURITY
APRIL 10-11, 2018 | RALEIGH, NORTH CAROLINA