Security Estimation for Post-Quantum Cryptosystems

Michael Gonzalez Harikesh Kailad Alex Lindenbaum
Mentors: Prof. Dana Dachman-Soled Hunter Michael Kippen

January 26, 2023

Post-Quantum Cryptography

- Current cryptographic protocols rely on **hardness assumptions**

Post-Quantum Cryptography

- Current cryptographic protocols rely on **hardness assumptions**
- Large-scale quantum computers will be able to break traditional cryptosystems

Post-Quantum Cryptography

- Current cryptographic protocols rely on **hardness assumptions**
- Large-scale quantum computers will be able to break traditional cryptosystems
- **Post-Quantum**: Can we develop cryptographic systems that are secure against both quantum and classical computers?

Post-Quantum Cryptography

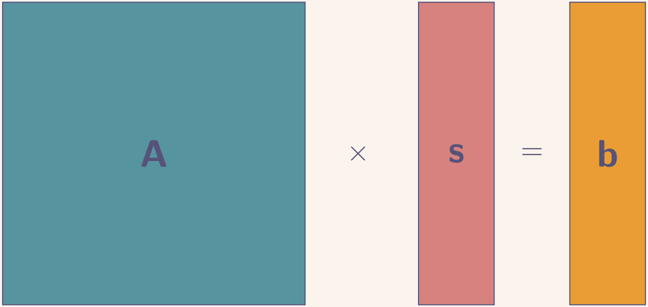
- Current cryptographic protocols rely on **hardness assumptions**
- Large-scale quantum computers will be able to break traditional cryptosystems
- **Post-Quantum**: Can we develop cryptographic systems that are secure against both quantum and classical computers?
- Learning with Errors problem (**LWE**), lattice problems seem hard for classical and quantum computers

Post-Quantum Cryptography

- Current cryptographic protocols rely on **hardness assumptions**
- Large-scale quantum computers will be able to break traditional cryptosystems
- **Post-Quantum**: Can we develop cryptographic systems that are secure against both quantum and classical computers?
- Learning with Errors problem (**LWE**), lattice problems seem hard for classical and quantum computers
- **Motivating question**: Can we crack* LWE? (side channel security estimation)

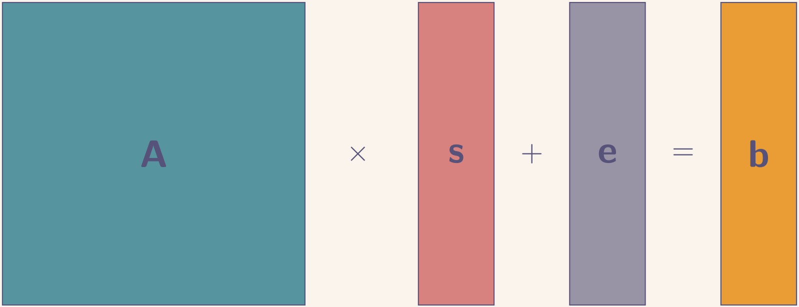
LWE (Almost)

Given $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{b} \in \mathbb{Z}_q^m$, find $\mathbf{s}$ where $\mathbf{As} = \mathbf{b} \mod q$

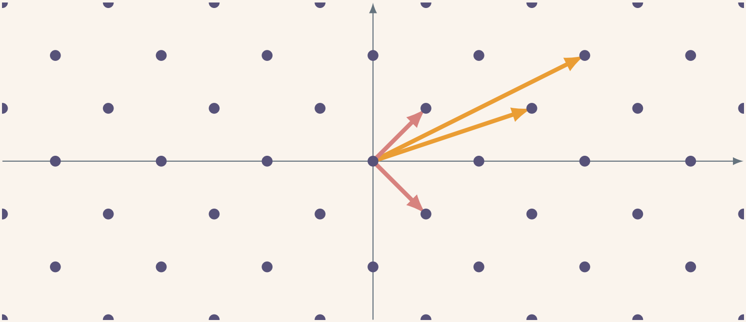


LWE

Now given an *unknown*, small Gaussian error **e**, find **s**



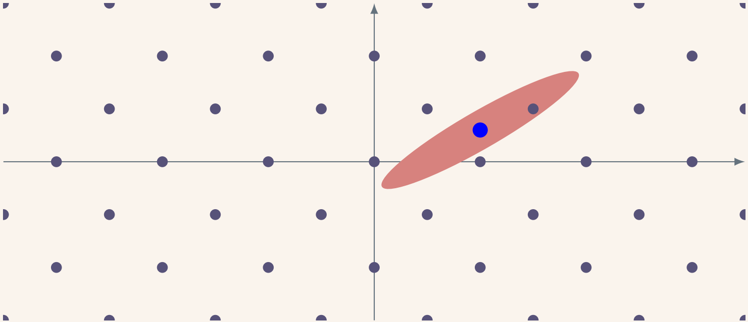
Lattices



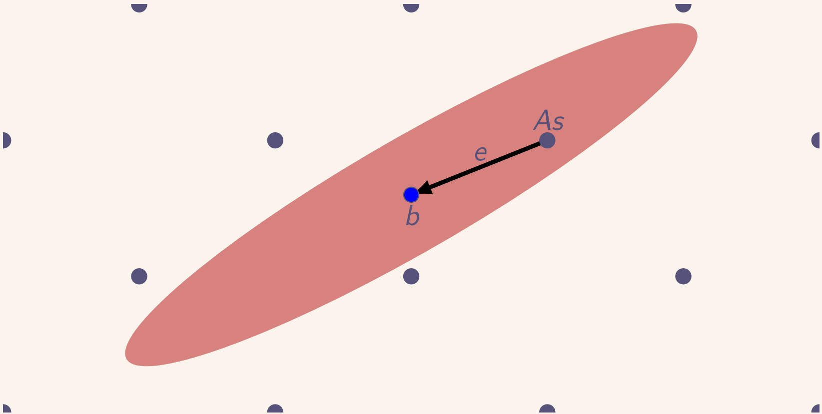
$$\mathcal{L}(B) \stackrel{def}{=} \{Bx \mid x \in \mathbb{Z}^n\}$$

Ellipsoidal Bounded Distance Decoding (EBDD)

Given a lattice Λ, an ellipsoid E with center μ and shape Σ, and the promise that there exists a unique lattice point $x \in \Lambda \cap E$, find x



The EBDD Embedding (LWE $\rightarrow$ EBDD)



LWE: $As + e = b$

Shape: $||As - b||_2^2 \leq m \cdot \sigma^2$ (big simplification)

SVP

- Shortest Vector Problem $\rightarrow$ find the shortest nonzero point in the lattice

SVP

- Shortest Vector Problem $\rightarrow$ find the shortest nonzero point in the lattice
- Very important in Post-Quantum Cryptography

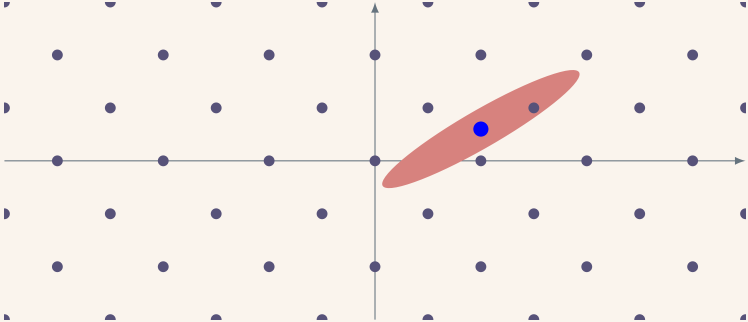
SVP

- Shortest Vector Problem $\rightarrow$ find the shortest nonzero point in the lattice
- Very important in Post-Quantum Cryptography
- BKZ is our exponential-time algorithm for SVP (its a pretty good algorithm)

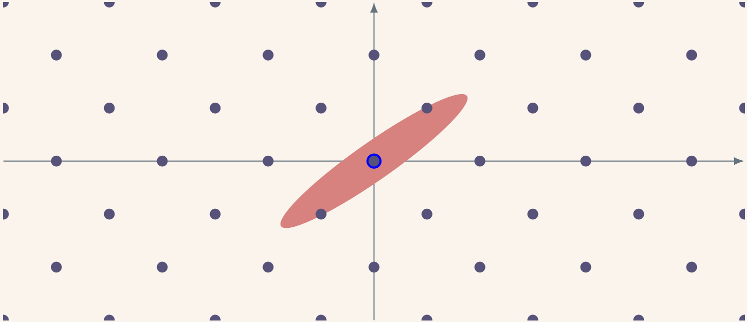
EBDD Reduces to SVP

We have techniques to turn EBDD into the SVP!

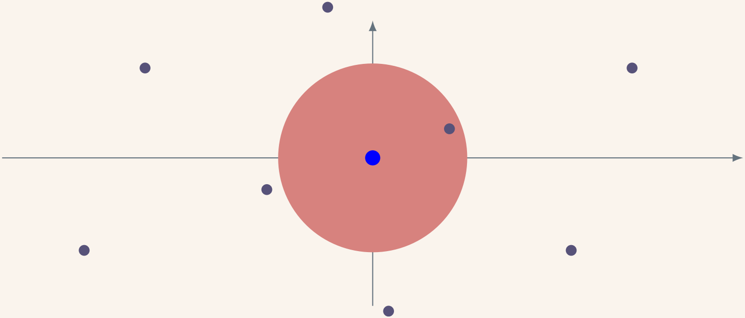
EBDD Reduces to SVP



EBDD Reduces to SVP

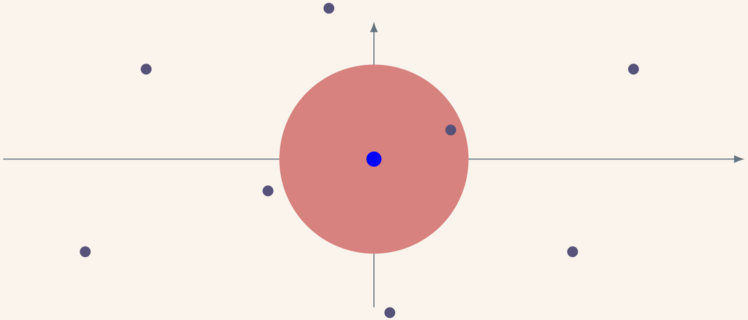


EBDD Reduces to SVP



BKZ!

EBDD Reduces to SVP



BKZ!

smaller EBDD ellipsoids $\Longrightarrow$ **easier** SVP instances

Why LWE $\rightarrow$ EBDD $\rightarrow$ SVP?

- LWE $\rightarrow$ SVP already exists, so why LWE $\rightarrow$ EBDD $\rightarrow$ SVP?

Why LWE $\to$ EBDD $\to$ SVP?

- LWE $\to$ SVP already exists, so why LWE $\to$ EBDD $\to$ SVP?
- EBDD gives a visual representation of the LWE instance (contrast with shortest vector problem)

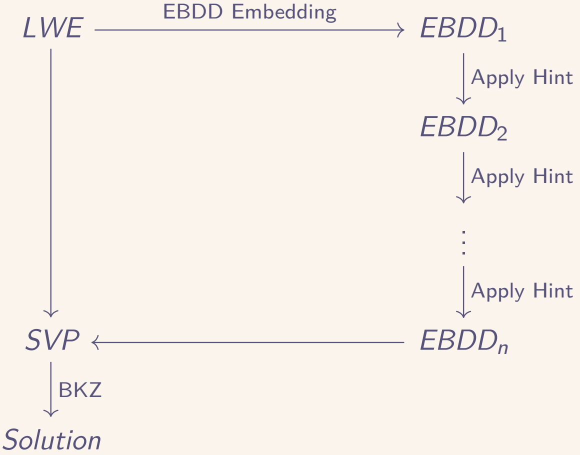
Why LWE $\rightarrow$ EBDD $\rightarrow$ SVP?

- LWE $\rightarrow$ SVP already exists, so why LWE $\rightarrow$ EBDD $\rightarrow$ SVP?
- EBDD gives a visual representation of the LWE instance (contrast with shortest vector problem)
- Offers different perspectives

Why LWE $\rightarrow$ EBDD $\rightarrow$ SVP?

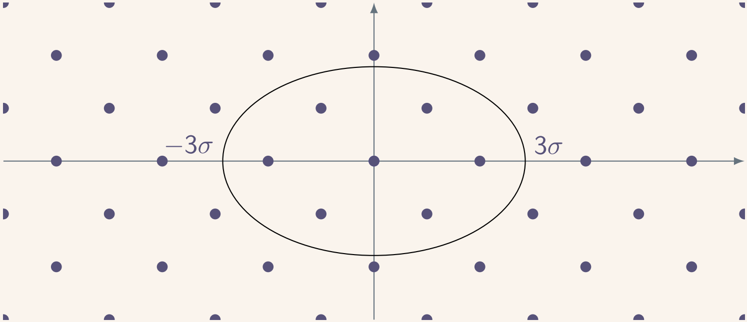
- LWE $\rightarrow$ SVP already exists, so why LWE $\rightarrow$ EBDD $\rightarrow$ SVP?
- EBDD gives a visual representation of the LWE instance (contrast with shortest vector problem)
- Offers different perspectives
- Apply hints, side-channel information to decrease ellipsoid volume

Background: Recap



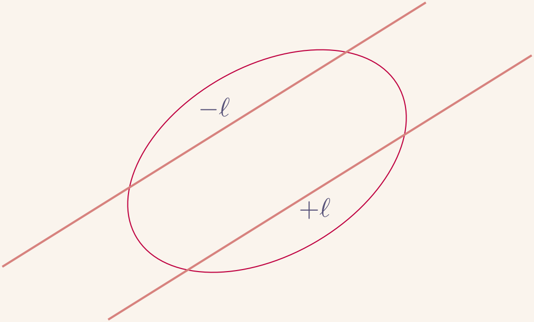
Ellipsoid Based on Distributional Knowledge

$\mathbf{s}, \mathbf{e}$ are Gaussian-distributed, so 95% confidence intervals can define a new ellipsoid



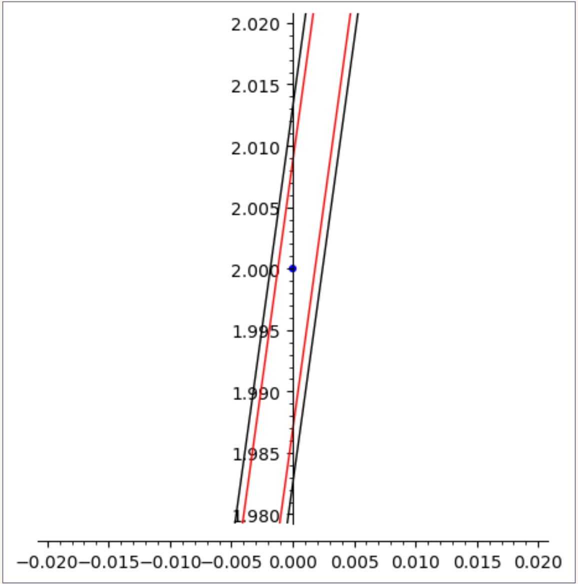
Alpha Cuts

- The error term **e** is small: in particular, each e_i is between $-\ell$ and $+\ell$.
- This gives *m* parallel lines intersecting our ellipsoid, with the secret in between



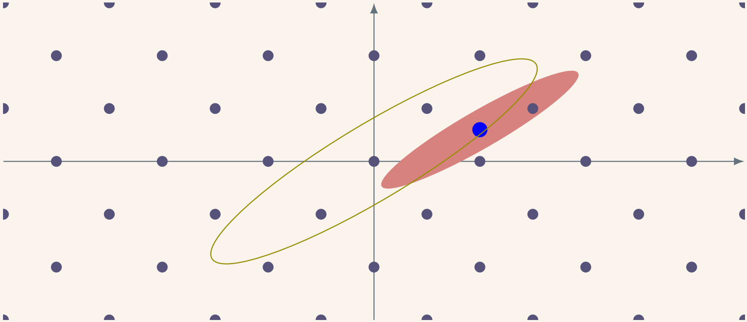
Alpha Cuts

- The error term **e** is small: in particular, each e_i is between $-\ell$ and $+\ell$.
- This gives *m* parallel lines intersecting our ellipsoid, with the secret in between
- **Lowner-John ellipsoid**



Sage plot. Distribution ellipse is outside figure, black is new ellipse

Ellipsoid Intersections



- Does the distribution ellipse (after alpha cuts) ∩ EBDD ellipse give a smaller ellipsoid?

What we did: Recap

1. Developed the alpha cuts method

What we did: Recap

1. Developed the alpha cuts method
2. Attemped to get provable bounds for change in volume from alpha cuts

What we did: Recap

1. Developed the alpha cuts method
2. Attemped to get provable bounds for change in volume from alpha cuts
3. Building of the LWE Sage toolkit, programmed the distributional ellipse and alpha cuts

What we did: Recap

1. Developed the alpha cuts method
2. Attemped to get provable bounds for change in volume from alpha cuts
3. Building of the LWE Sage toolkit, programmed the distributional ellipse and alpha cuts
4. Tested performance of alpha cuts at $n = m = 1, 10, 20, 50, 70$; comparable to EBDD.

What we did: Recap

1. Developed the alpha cuts method
2. Attemped to get provable bounds for change in volume from alpha cuts
3. Building of the LWE Sage toolkit, programmed the distributional ellipse and alpha cuts
4. Tested performance of alpha cuts at $n = m = 1, 10, 20, 50, 70$; comparable to EBDD.
5. Ellipsoidal intersection

Acknowledgements

I'd like to thank Prof. Dachman-Soled (University of Maryland) and Hunter Kippen (University of Maryland) for their mentorship through this project, and Ms. Angelique Bosse for all her guidance and support.

Questions?