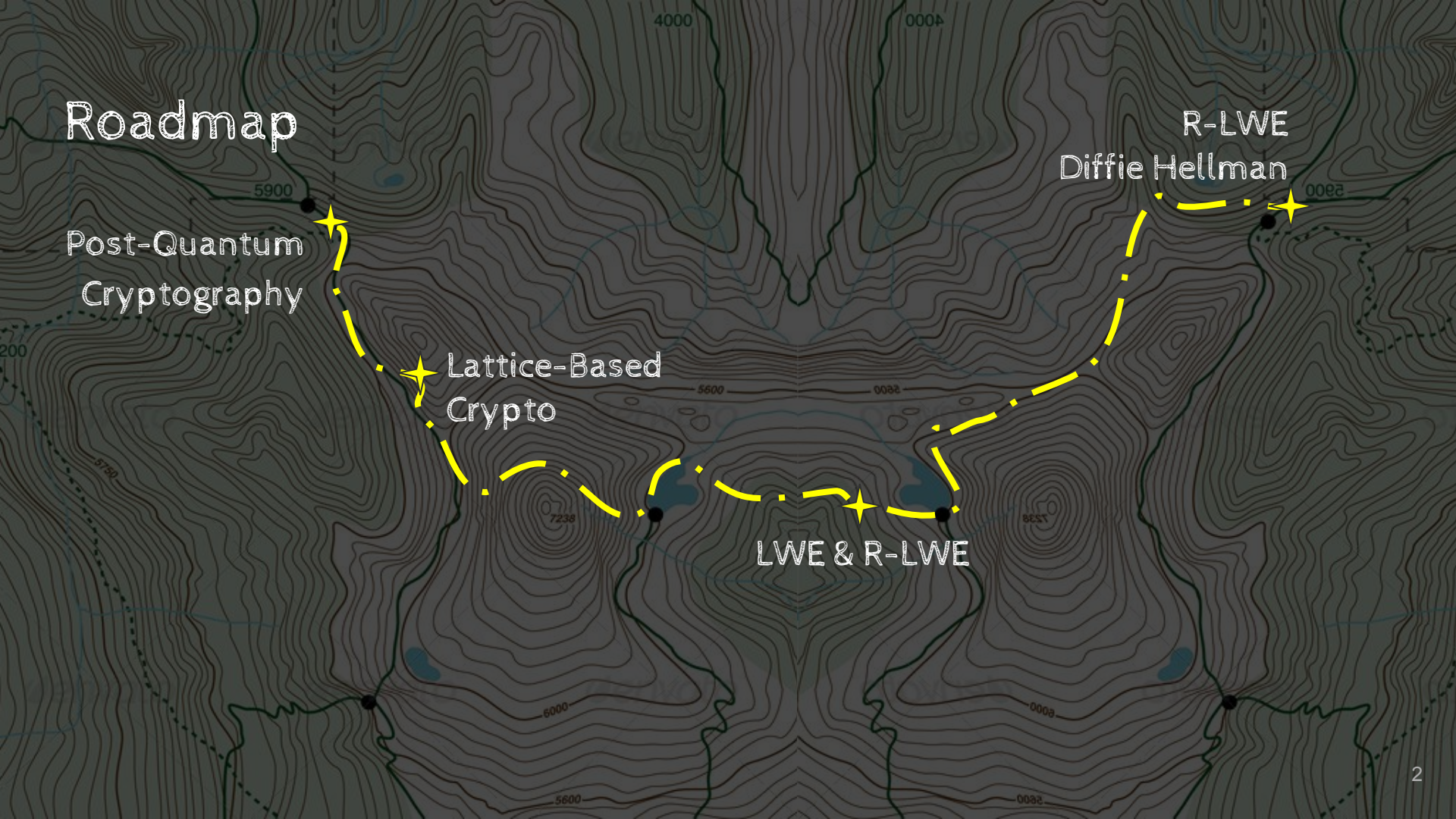
Post-Quantum Crypto Adventure

Introduction to Lattice-Based Cryptography

Presenter:
Pedro M. Sosa

Roadmap


Post-Quantum Cryptography
Lattice-Based Crypto
LWE & R-LWE
R-LWE Diffie Hellman

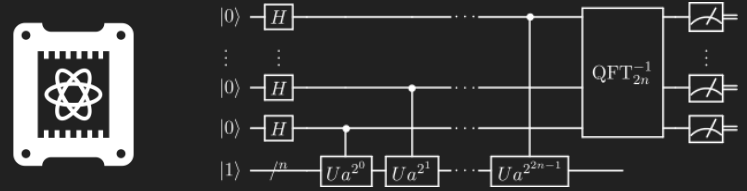
The Upcoming Crypto-Apocalypse

The basis of current cryptographic schemes

Factoring
- Given n; compute p: $n = p \cdot q$

Discrete Logarithm
- Given p, g, y; compute x: $y = g^x \pmod p$

The Problem

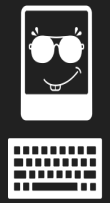


Quantum Computers + Shor's Algorithm

Classic Computers breaking factorization:

$$e^{1.9(logN)^{1/3}(loglogN)^{2/3}}$$

Quantum Computers breaking factorization:



$(\log N)^2(\log\log N)(\log\log\log N)$

The Push for Post-Quantum

Governments, Companies, Organizations all want to migrate as soon as possible...

Microsoft

NIST

National Institute of Standards and Technology

Post-Quantum Cryptography

5 Main Approaches:

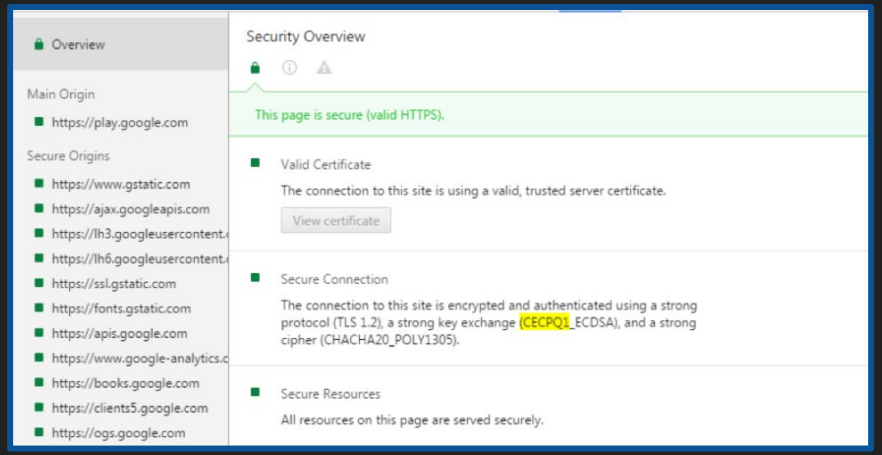
- Lattice-based
- Hash-based
- Code-based
- Multivariate
- Supersingular Elliptic Curve Isogeny

Lattice-based Cryptography

- Lots of history
- Provably secure
- Security based on worst-case prob.
- Efficient (Comp./Comm.)
- Versatile
- Promising standardization candidates

The Current State of Lattice Based Crypto

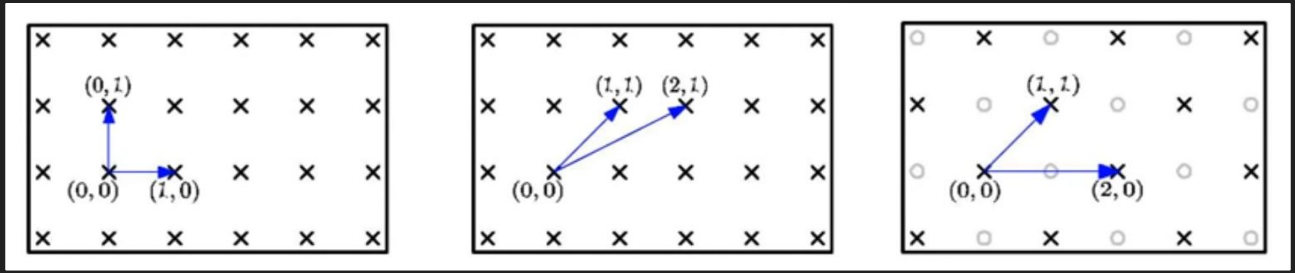
- Key Exchanges:
  - R-LWE, NTRU, New Hope
- Digital Signatures:
  - NTRUSign, TESLA, BLISS
- Authenticated Key Exchanges
  - Del Pino et. al & me :)
- Hash Functions
  - SWIFFT, LASH
- Encryption Schemes
  - Prest's IBE-Scheme, NTRUEncrypt



Google testing Lattice-based PQC KEX

Lattice Based Cryptography

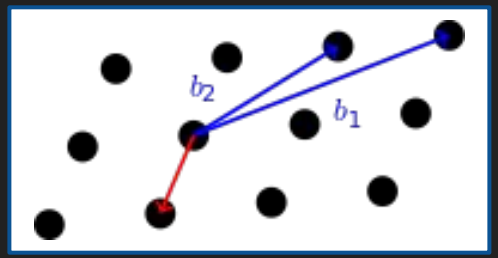
Lattice L(B) = Set of all integer combinations of n linearly independent vectors $B=\{b_1, \dots, b_n\}$ in R^n.



Hard Problems

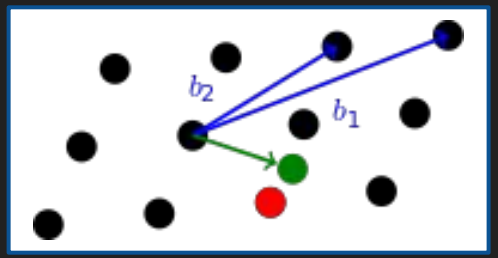
Shortest Vector Problem

Given a basis B, find the shortest vector.



Chosen Vector Problem:

Given a basis B and a vector v, find the vector in L closest to v.



Learning With Errors (LWE)

Z_{13}^{7x4}

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

$*$

Z_{13}^{4x1}

$=$

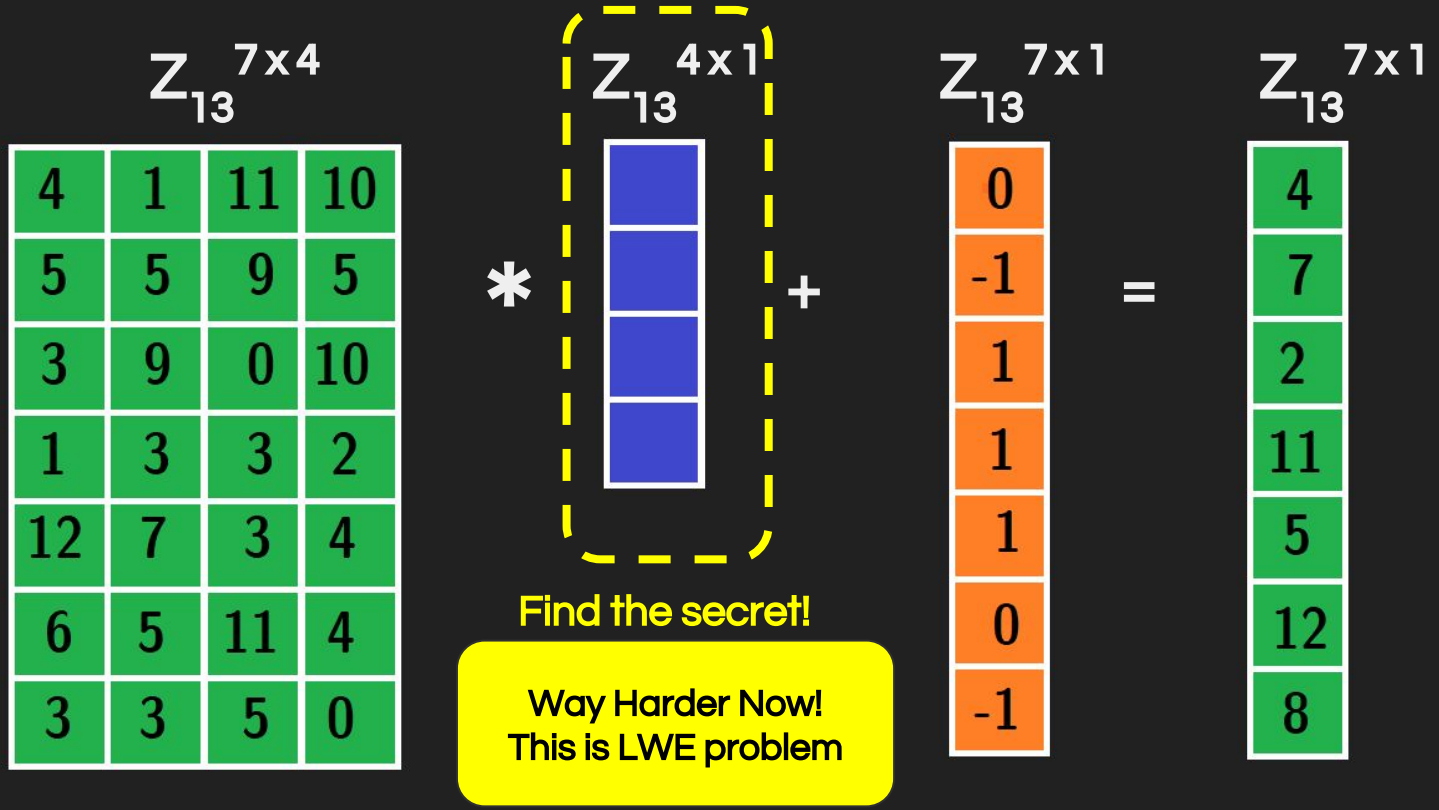
Z_{13}^{7x1}

4
7
2
11
5
12
8

Find the secret!

Solving Method:
Use Gaussian Elimination

Learning With Errors (LWE)

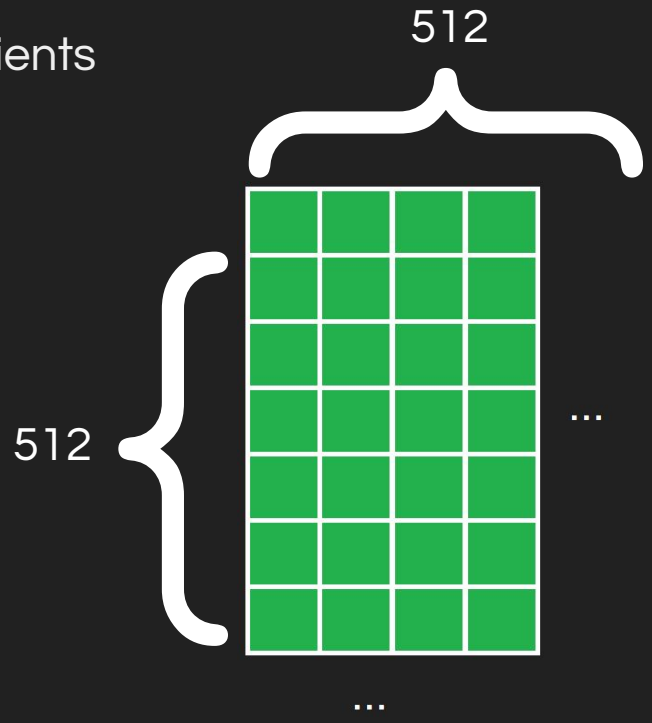


The problem with LWE

In reality we need large matrixes with large coefficients

Eg. $Z_{12289}^{512 \times 512}$ = 512*512*14 bits = **458 KiB !!!**

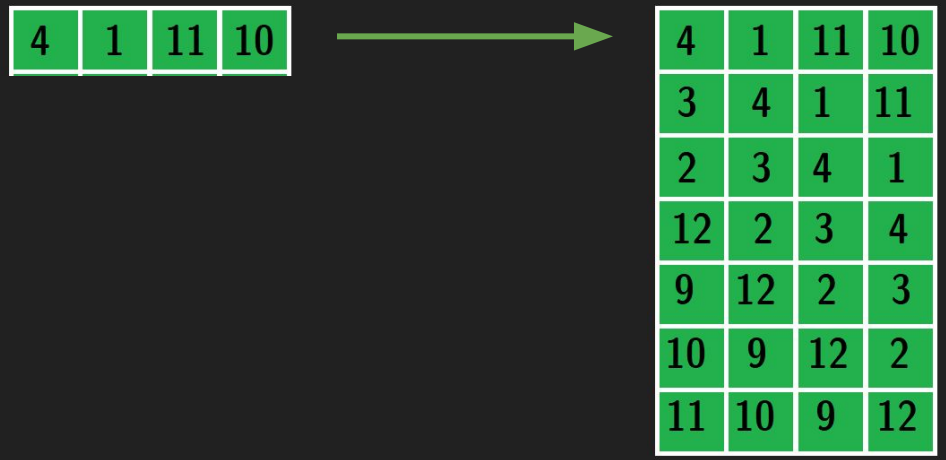
Too Big...



Ring Learning with Errors

We need Order!

- Each row is the Cyclic shift of the row above
- Special wrapping rule: x wraps to -x mod 13



Ring Learning with Errors

$Z_{13}[x] / < x^4 + 1 >$

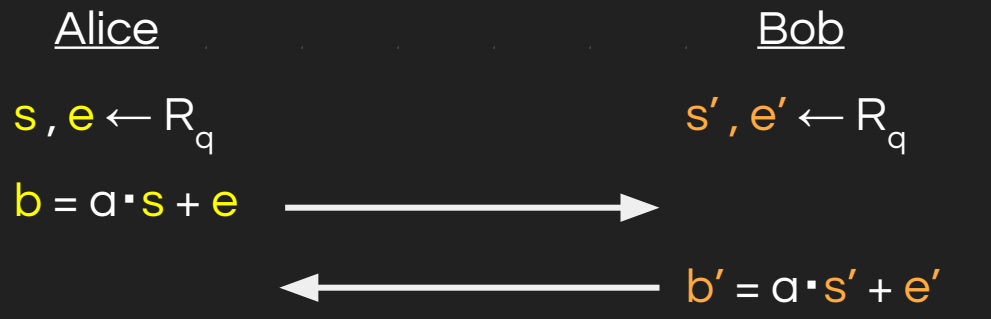
	$4 + 1x + 11x^2 + 10x^3$	random
x	$1 + 0x - 1x^2 + 2x^3$	small secret
+	$0 - 1x + 1x^2 + 1x^3$	small noise
=	$10+5x +10x^2 + 7x^3$	looks random

Decision Ring-LWE problem: Given **green** can you distinguish **yellow** from random?

Hardness: Can be reduced to SIVP.

Ring-LWE Diffie Hellman Key Exchange

$$a \leftarrow R_q = Z_q[x] / < x^n+1 >$$



round(s·b′) = round(b·s′)

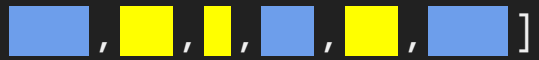
(s·a·s′) + s·e′ ~ (s·a·s′) + s′·e

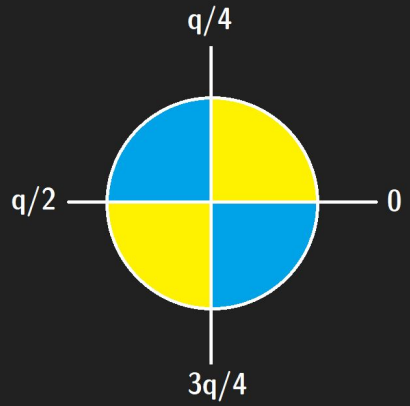
Rounding

Bob sends extra information

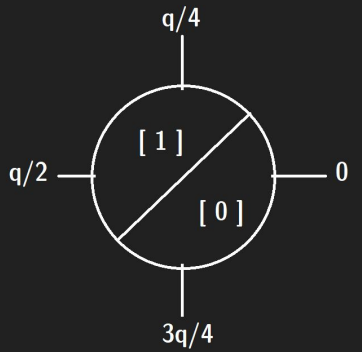
Assume: $R_{128} / < x^6 + 1 >$

Bob Key : [100 , 94 , 1 , 44 , 31 , 126]

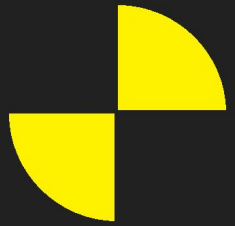
u : []

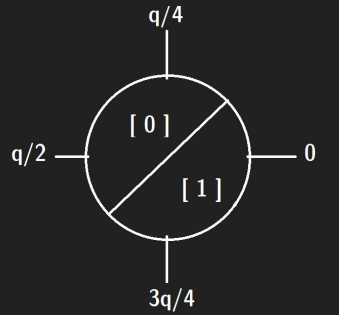


IF



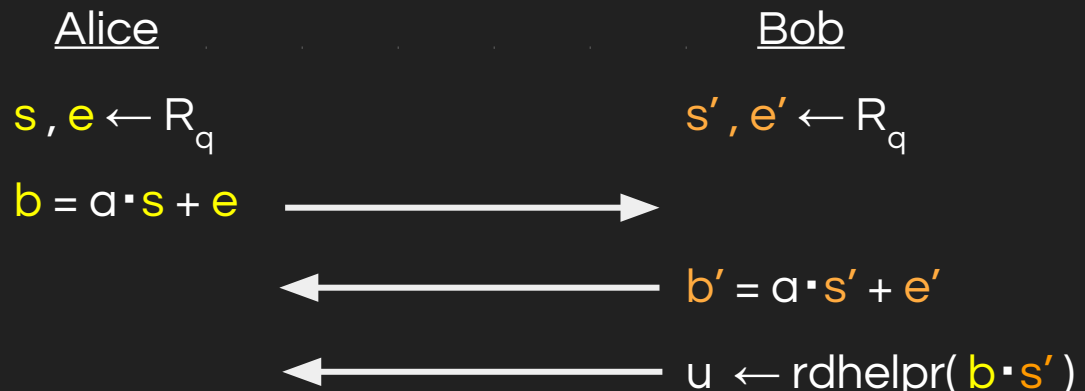
IF





Ring-LWE Diffie Hellman Key Exchange

$$a \leftarrow R_q = Z_q[x] / < x^n + 1 >$$



Conclusion

- **We need PQC**, yet this field is still young and expanding. **Tons of research to do!**
- Lattice-based Cryptography is among it's **most promising approaches**
- R-LWE Python reference code available at: **github.com/pmsosa/rlwe-kex**

Some Other Fantastic Talks

- Winter School on Cryptography: Introduction to Lattices - Oded Regev
  - https://www.youtube.com/watch?v=4ulHOV8iLls

- Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem - Douglas Stebila
  - https://www.youtube.com/watch?v=BCmSzzQ2ges

- Lattice-Based Cryptography - Chris Peikert
  - https://www.youtube.com/watch?v=DmemT_OPn2Q