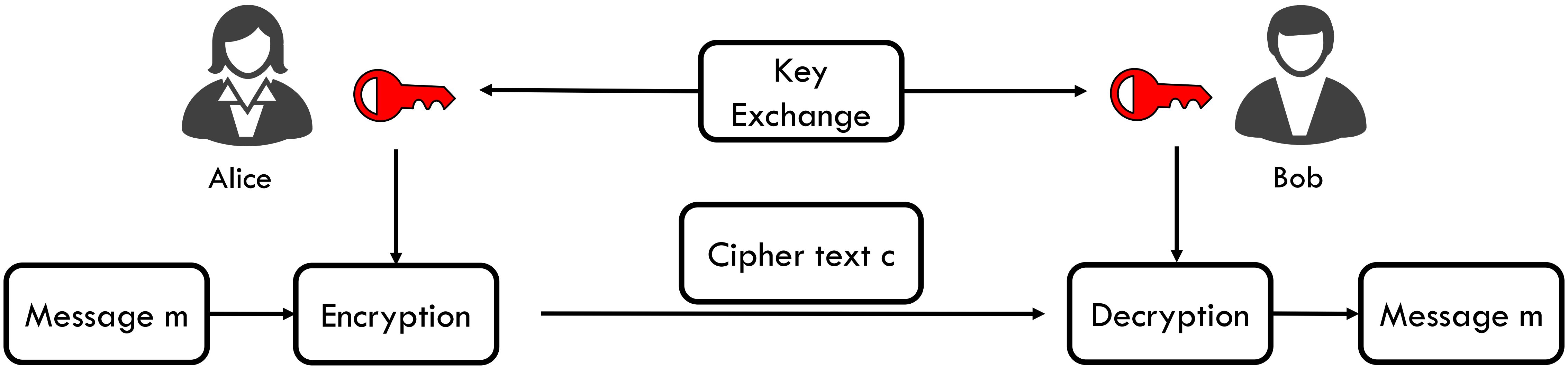
Lattice-Based Cryptography
- an Example for Quantum-Secure Cryptography

C&O URA Seminar
University of Waterloo
27/05/2020

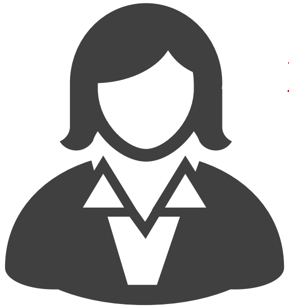
Nina Bindel
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Secret-Key Crypto (Symmetric)



Key exchange

g generator of cyclic group



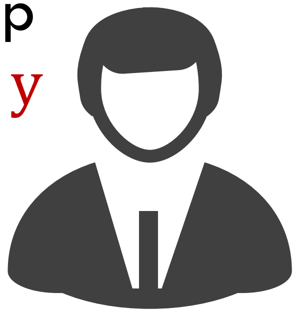
Alice

x

$X = g^x$ →

$Y = g^y$ ←

y



Bob

(key) $= Y^x \quad = g^{xy} = \quad X^y =$ (key)

We can break the scheme if …

we can solve the discrete logarithm problem.

Diffie-Hellmann-Merkle key exchange

1976

RSA Encryption Scheme

Choose primes p, q, Compute $n = p \cdot q$

Find d such that $3 \cdot d \bmod (p-1)(q-1) = 1$ $\Rightarrow \sqrt[3]{c} \bmod n = c^d \bmod n$

secret

public

Message m

Encryption: $m^3 \bmod n = c$

n

Cipher text c

Decryption: $\sqrt[3]{c} \bmod n = c^d \bmod n = m$

d

Message m

RSA by Shamir, Rivest, and Adleman

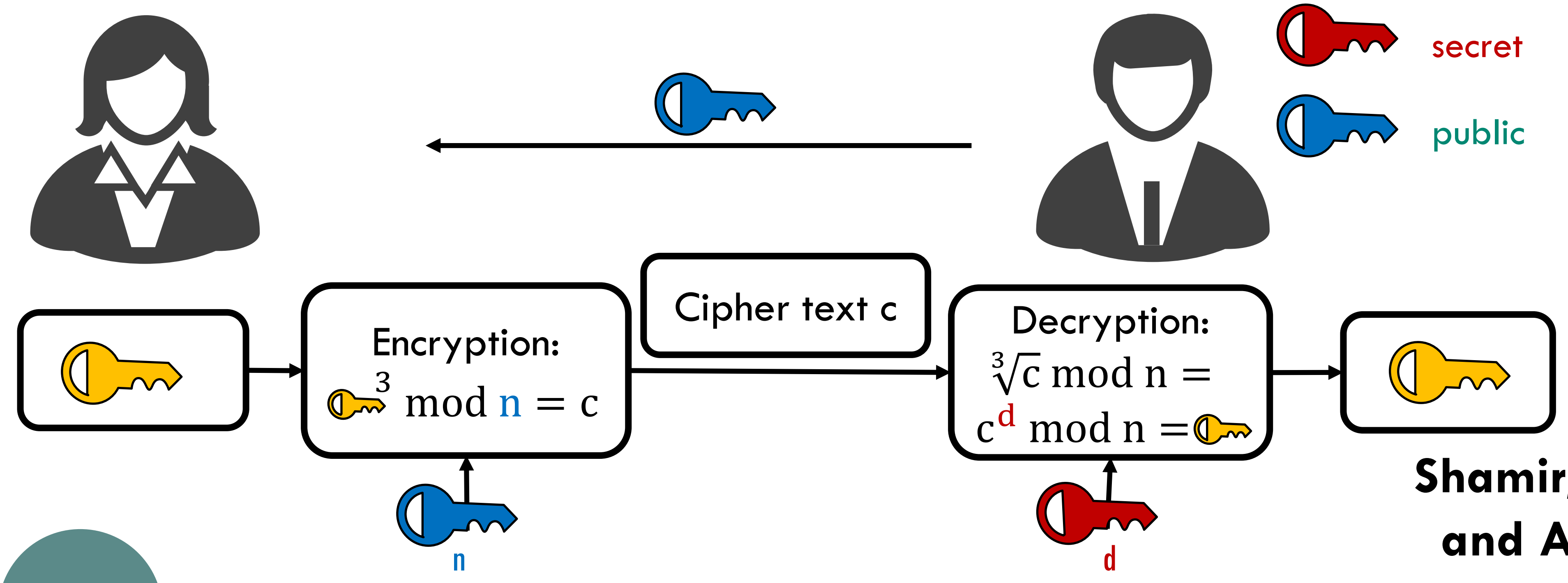
1976

1977

RSA Encryption Scheme

Choose primes p, q, Compute $n = p \cdot q$

Find d such that $3 \cdot d \bmod (p-1)(q-1) = 1$ $\Rightarrow \sqrt[3]{c} \bmod n = c^{d} \bmod n$



RSA by Shamir, Rivest, and Adleman

1976

1977

Visit uwaterloo.ca

Security of RSA

We can break RSA if …

we can factor large integers into their prime factors.

We actually want something else, namely

if an attacker breaks RSA, we can construct an algorithm that factors integers.

As far as we know, only way to attack RSA scheme mathematically is to factor modulus n.

Poll: Is integer factorization a hard problem?

yes, on classical computers (as far as we know)

No, on quantum computer

The Quantum Threat

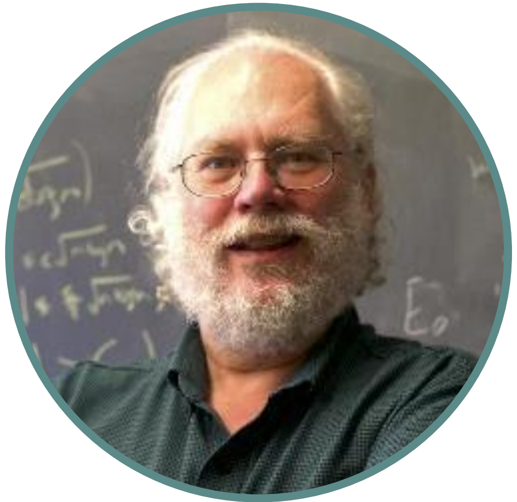
Shor's Quantum Algorithm

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.



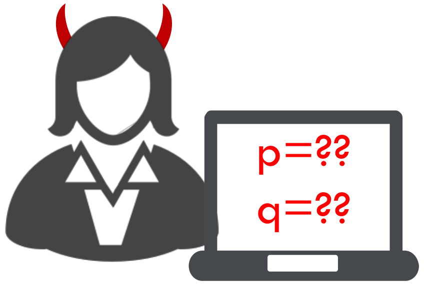
1976

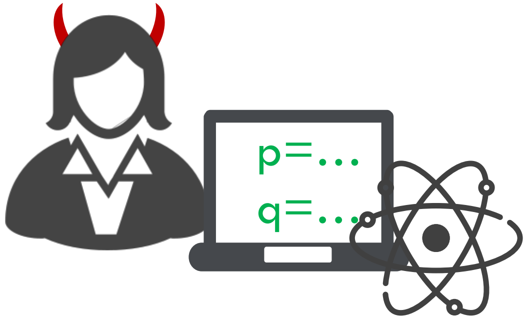
1977

1997

RSA module n = pq of uwaterloo.ca

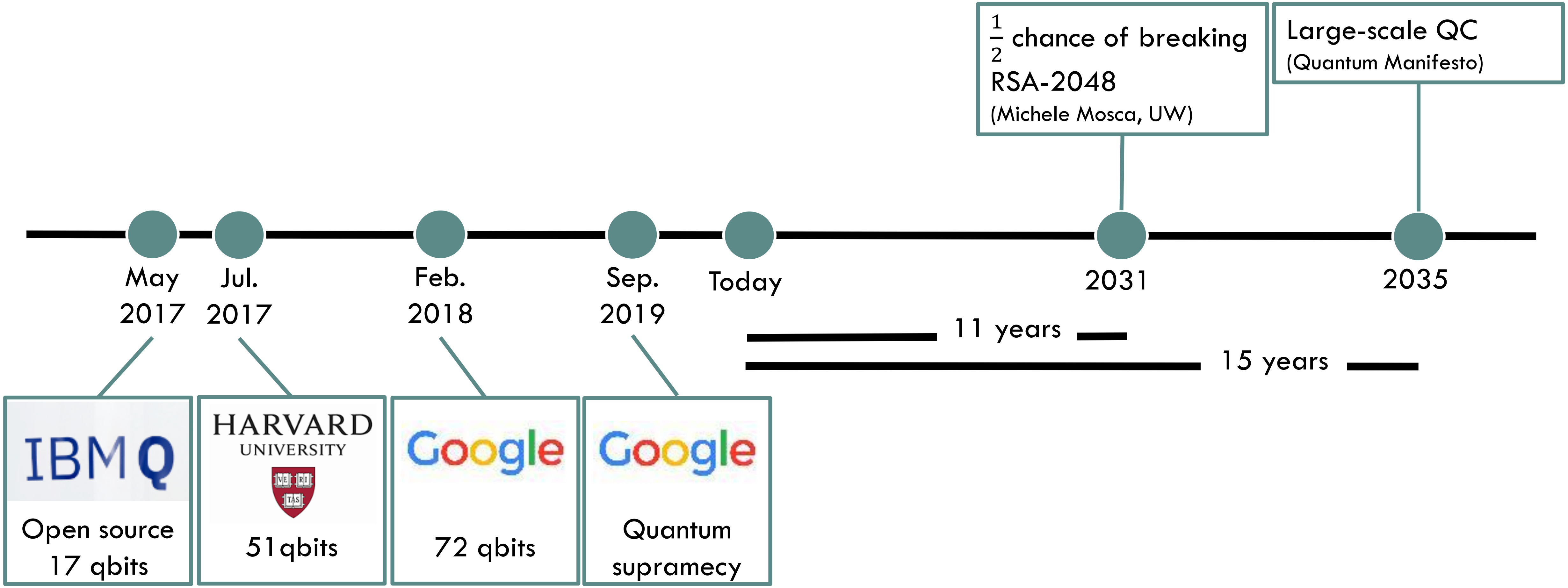
n = 27360491602425362828680840196812567822251222564884830144447558268409134978642455969952846499126889652292166253642172893760654225329572782645157892635535141029491949562413167674335240085393438845057088656724564737664150021918497392498273927495195585325077812529900360260990915310960744901794290914580055666815284992894648321319516386959677596799929027929752894690176118563779993397770180774643391675861048885719222754751891615073957946010135296075470961045287321748001022366106147271788615455706576546577870700629797960856858045126586160833217863031055823490552386814232179570998341873251262081257275400886614852802269





… in polynomial time

Quantum computing: State-of-the-art and estimations

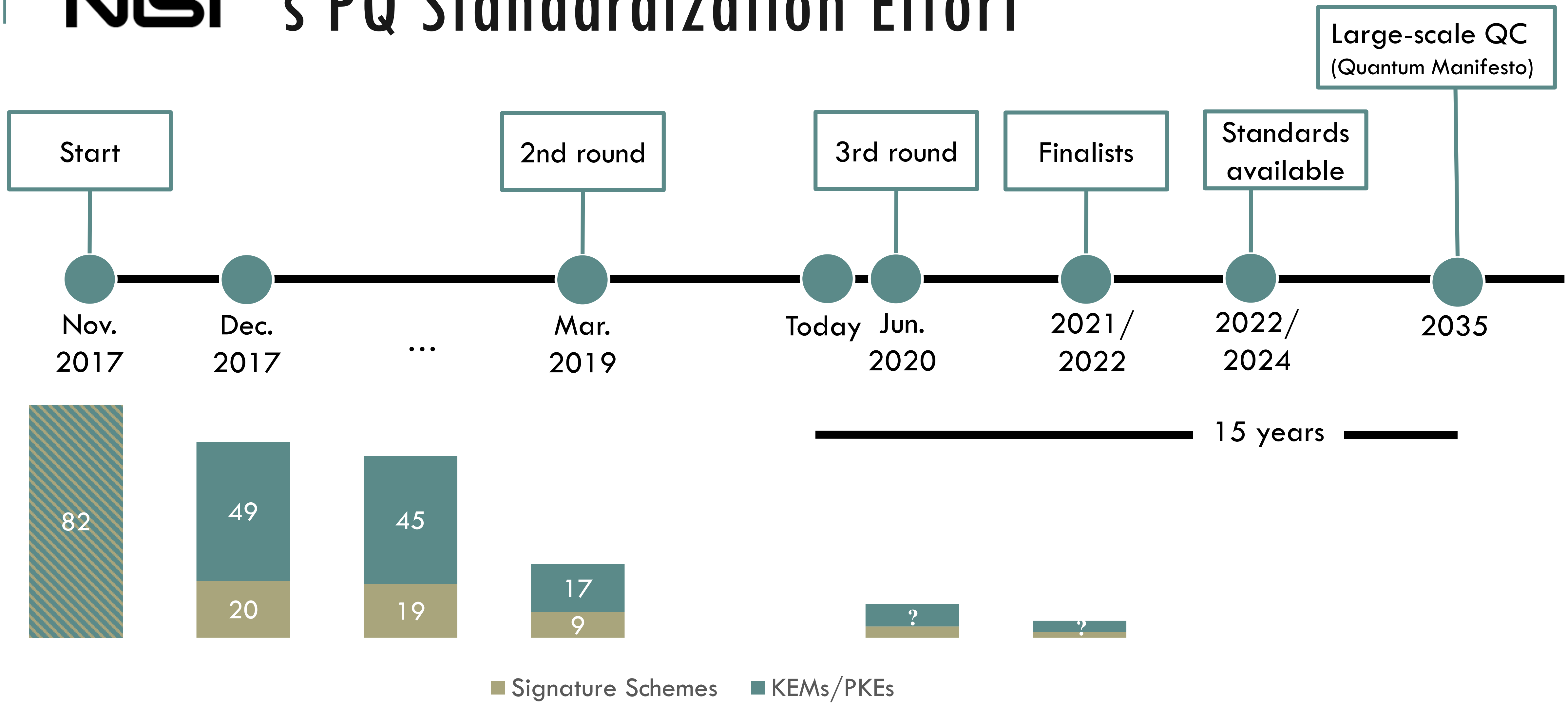


Better safe than sorry:
NIST`s PQ Standardization Effort

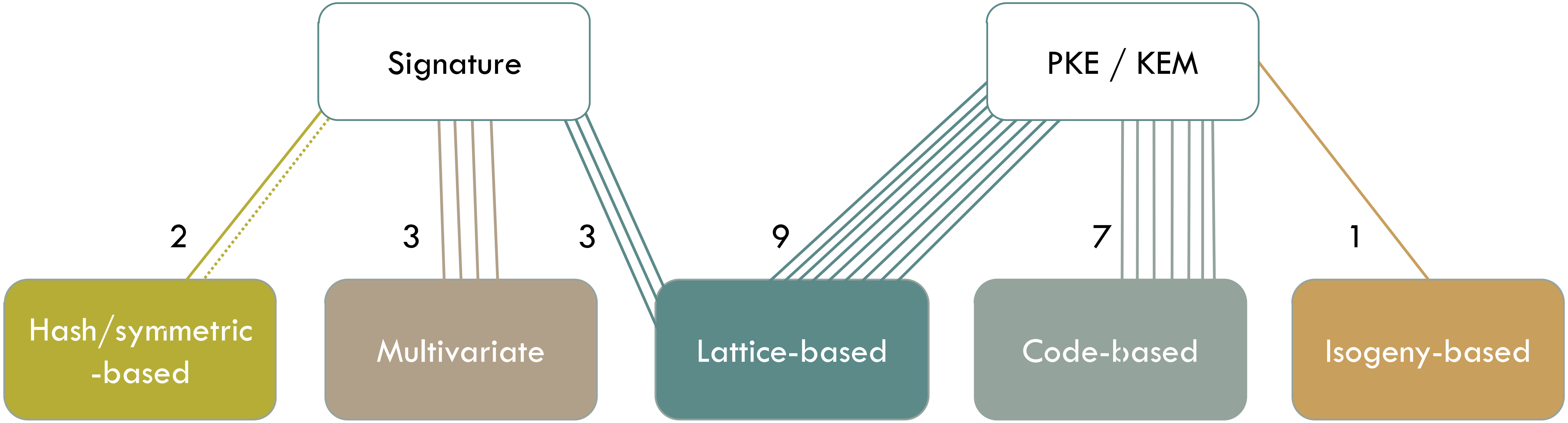
GOAL:
standardize cryptographic algorithms that are secure against quantum adversaries
= post-quantum or quantum-secure algorithms

- Public-key encryption scheme & key encapsulation mechanisms
- Digital signature schemes

Better safe than sorry:
NIST`s PQ Standardization Effort

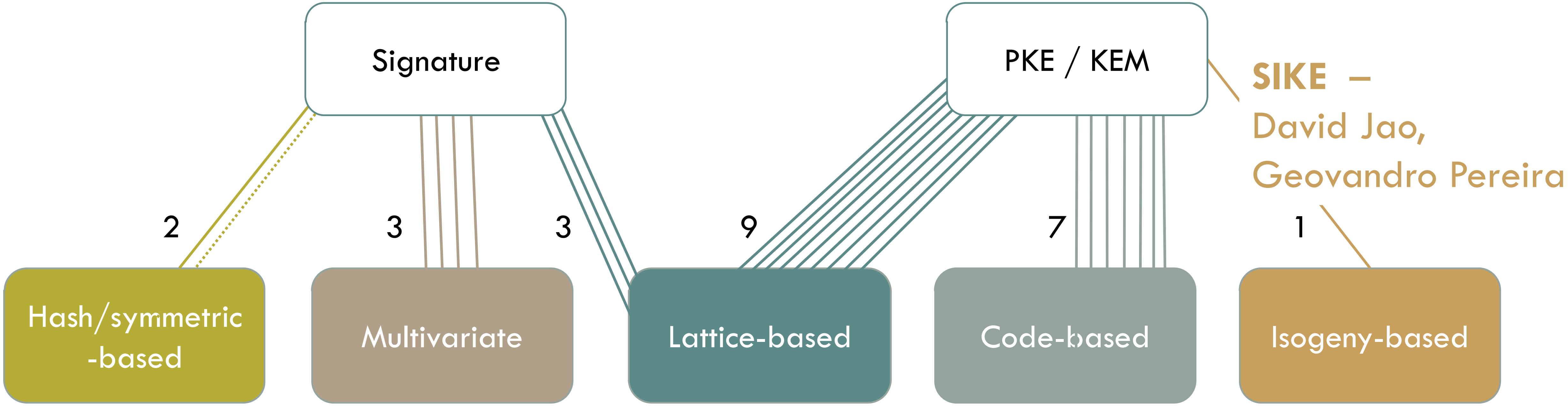


NIST candidates – 2nd round



With courtesy of Denis Butin and Johannes Buchmann

NIST candidates – 2nd round affilitated to UNIVERSITY OF WATERLOO



Ted Eaton, Nina Bindel – **qTESLA**

CRYSTALS-Kyber – John Schanck
Frodo – Douglas Stebila
NewHope – Douglas Stebila
NTRU – John Schanck

With courtesy of Denis Butin and Johannes Buchmann

Introduction to Lattices

Definition lattice

Definition

$L \subseteq \mathbb{R}^n$ is called a lattice if L is a

- discrete and
- additive subgroup of $\mathbb{R}^n$.

$\Updownarrow$

Definition

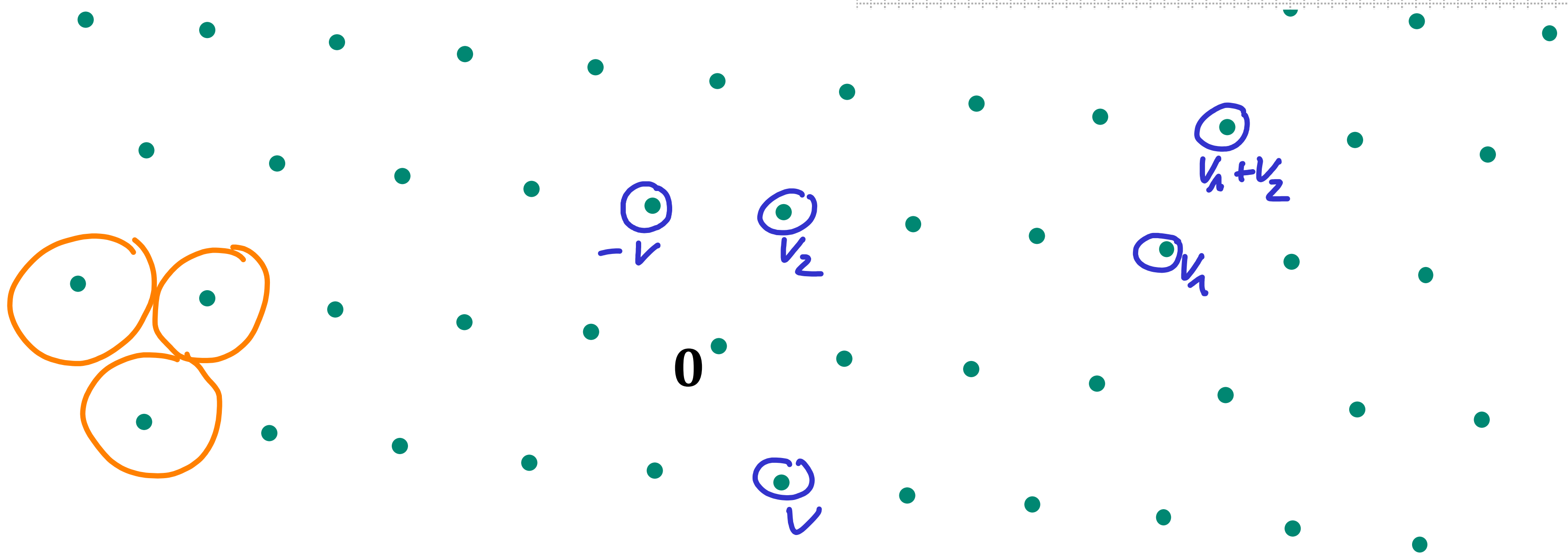
$L \subseteq \mathbb{R}^n$ is called a lattice if $\exists\, b_1, \dots, b_m$ linearly independent such that
$L = \{ \sum_{i=1}^{m} x_i \cdot b_i,\ x_i \in \mathbb{Z}, 1 \leq i \leq m \}$.

We then call $B = (b_1, \dots, b_m)$ a basis of $L = L(B)$.

Definition Lattice

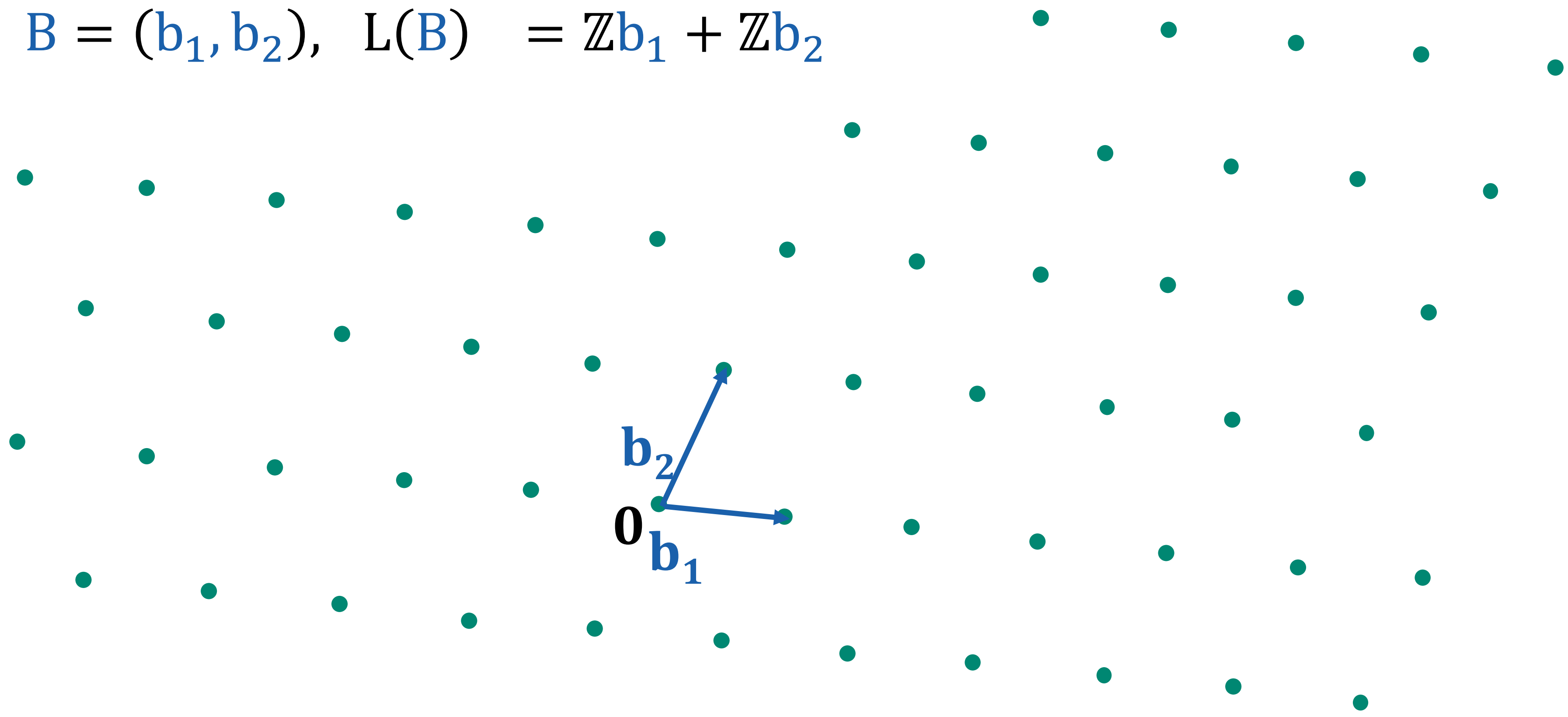
Lattice L

- Additive subgroup of $\mathbb{R}^2$:
  - $0 \in \mathrm{L}$ ✓
  - $\mathrm{v}_1, \mathrm{v}_2 \in \mathrm{L} \rightarrow \mathrm{v}_1 + \mathrm{v}_2 \in \mathrm{L}$ ✓
  - $\mathrm{v} \in \mathrm{L}\ \exists\ -\mathrm{v} \in \mathrm{L}$ such that $\mathrm{v} + (-\mathrm{v}) = 0$ ✓
- Discrete ✓



Basis of L

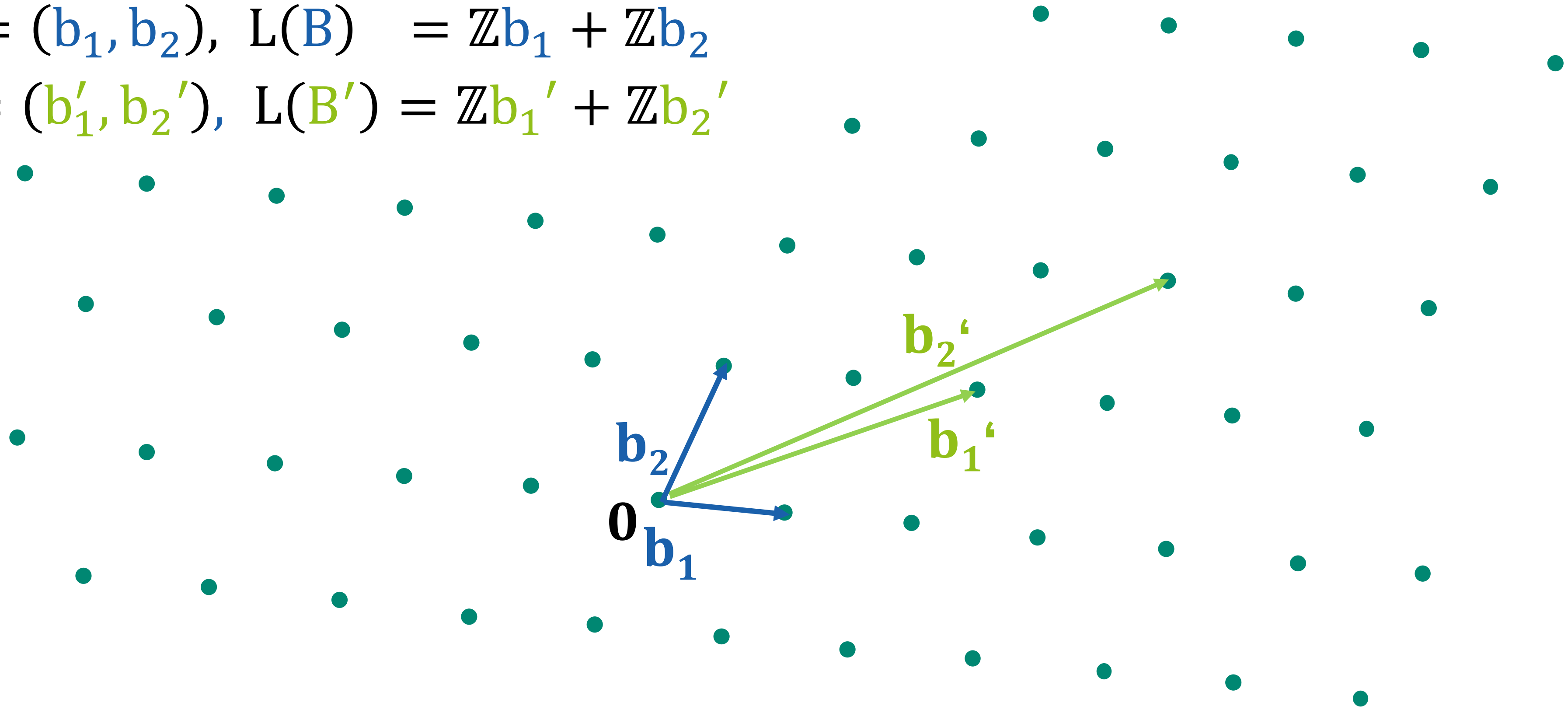
$B = (b_1, b_2)$, $L(B) = \mathbb{Z}b_1 + \mathbb{Z}b_2$



Two bases of L

$B = (b_1, b_2),\ \ L(B) = \mathbb{Z}b_1 + \mathbb{Z}b_2$

$B' = (b_1', b_2'),\ \ L(B') = \mathbb{Z}b_1' + \mathbb{Z}b_2'$

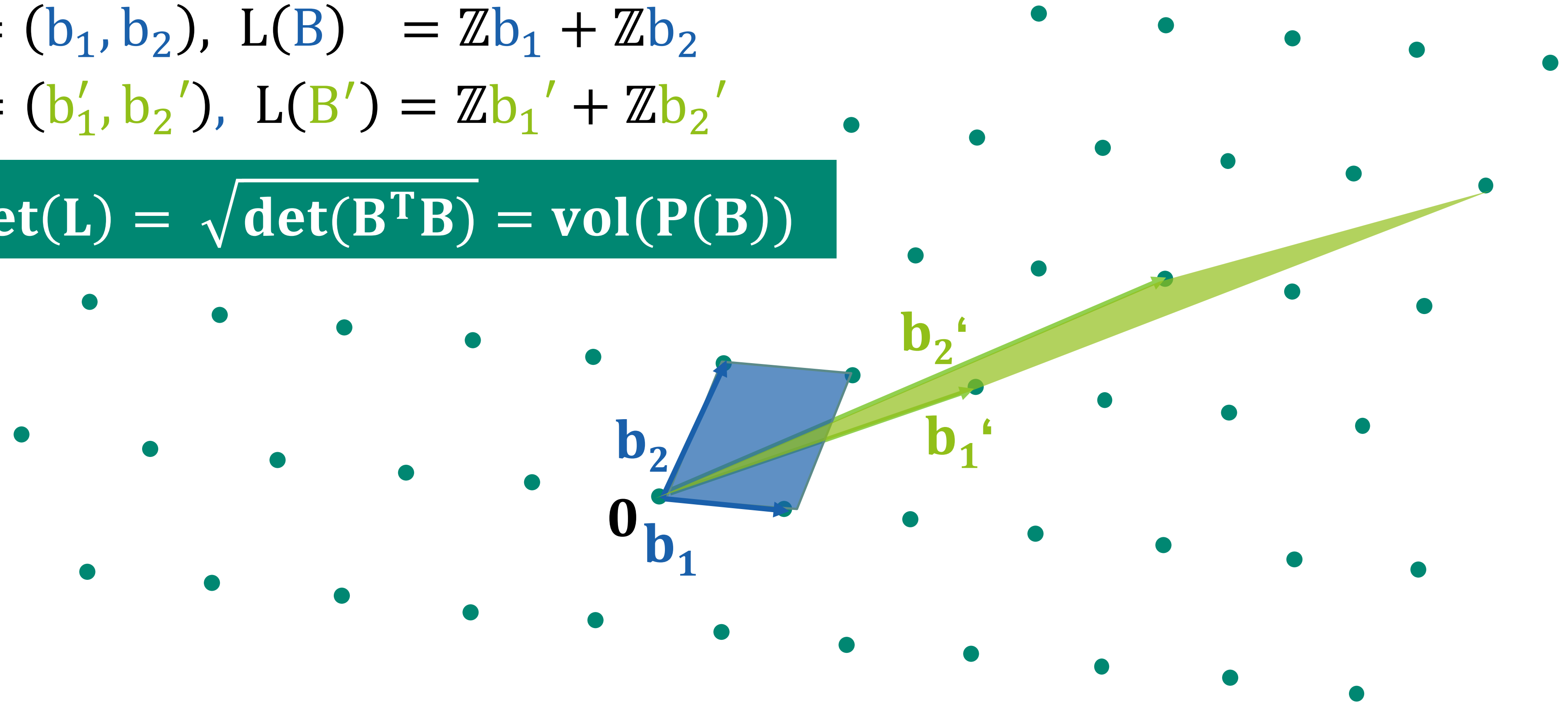


Determinant of L

$B = (b_1, b_2),\ L(B) = \mathbb{Z}b_1 + \mathbb{Z}b_2$

$B' = (b_1', b_2'),\ L(B') = \mathbb{Z}b_1' + \mathbb{Z}b_2'$

$$\det(L) = \sqrt{\det(B^T B)} = \mathrm{vol}(P(B))$$



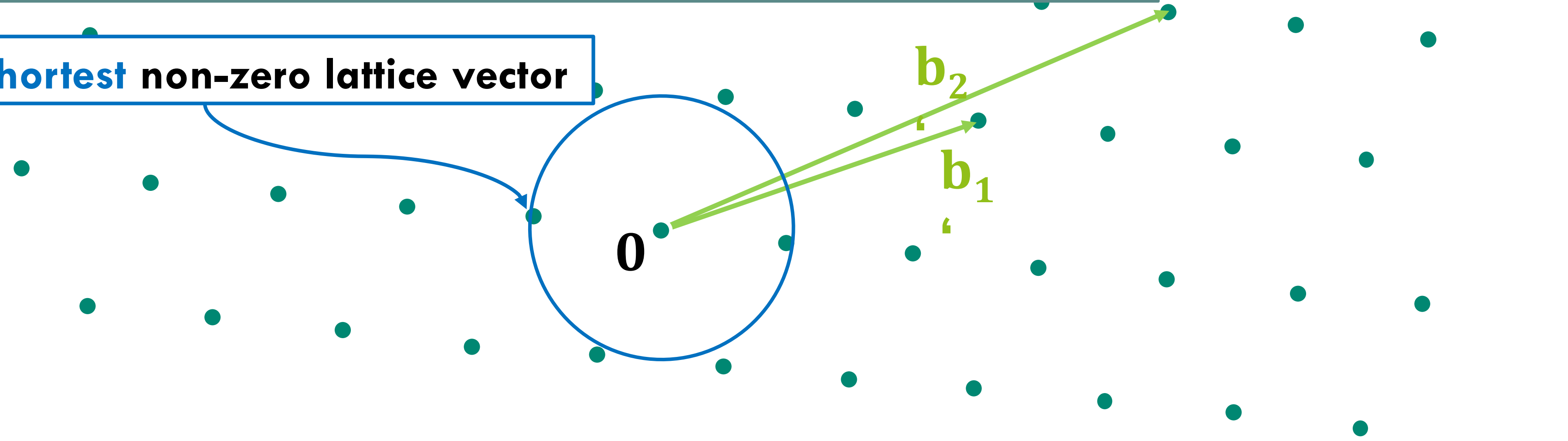
Shortest Vector Problem (SVP)

Problem (Shortest Vector Problem (SVP))

Given: B

Find: $v \in L(B), \neq 0 : \|v\| = \min\{\|v\| \mid v \in L\} =: \lambda_1(L)$

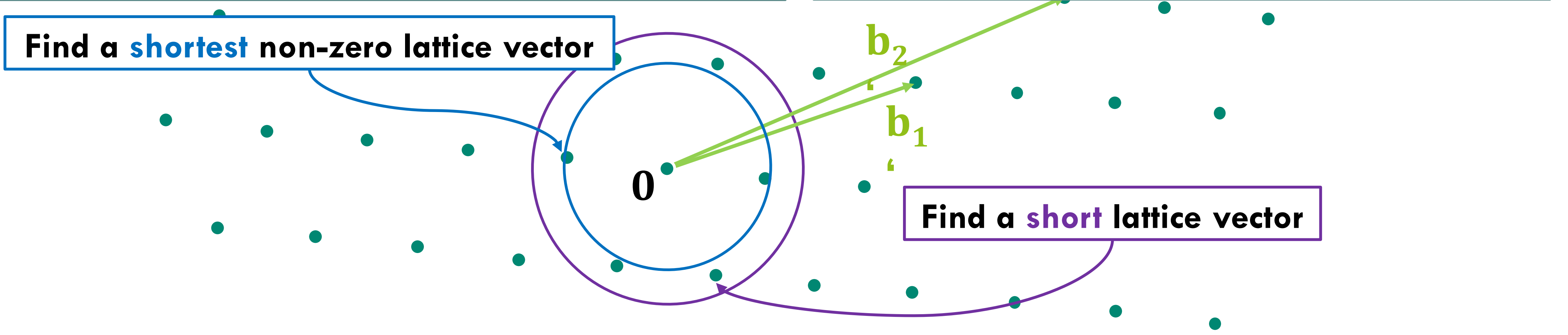
Find a shortest non-zero lattice vector



Shortest Vector Problem (SVP)

Problem (Shortest Vector Problem (SVP))
Given: B
Find: $\mathrm{v} \in \mathrm{L}(\mathrm{B}), \neq 0 : \|v\| = \lambda_1(\mathrm{L})$

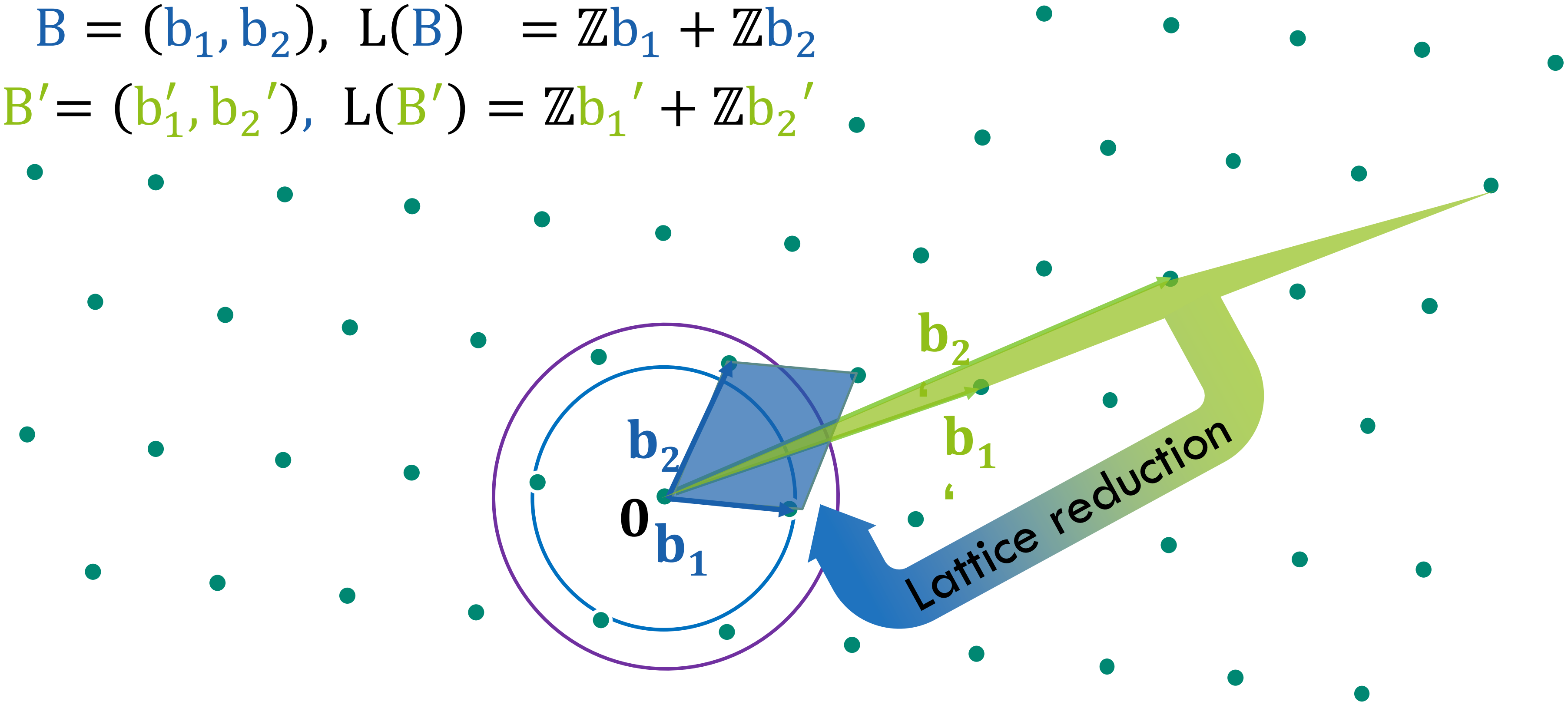
Problem (α-SVP)
Given: $\alpha \geq 1, \mathrm{B}$
Find: $\mathrm{v} \in \mathrm{L}(\mathrm{B}), \neq 0 : \|v\| \leq \alpha\lambda_1(\mathrm{L})$



Solving the SVP

$B = (b_1, b_2),\ L(B) = \mathbb{Z}b_1 + \mathbb{Z}b_2$

$B' = (b_1', b_2'),\ L(B') = \mathbb{Z}b_1' + \mathbb{Z}b_2'$



Lattice reduction – LLL Algorithm

Arjen Lenstra,
Hendrik Lenstra,
László Lovász

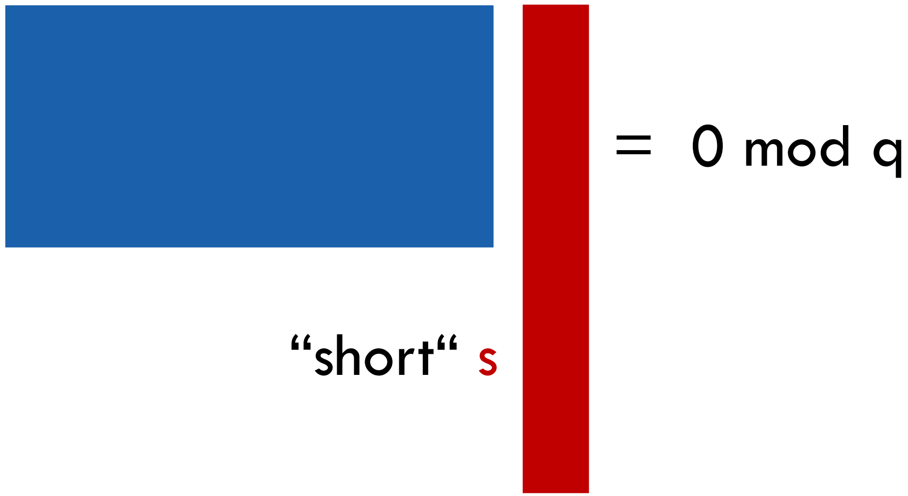
+ Polynomial runtime (in dimension)
- Basis quality (shortness/orthogonality) is poor

- Currently fastest lattice reduction used to break lattice problems:
  Block Korkine Zolotarev (BKZ) algorithm
- BKZ uses LLL as subroutine

1976 — 1977 — 1982 — 1997

Lattice-Based Cryptography

Short Integer Solution Problem



Problem (Short Integer Solution Problem (SIS))

Given : $A \leftarrow_{\$} \mathbb{Z}_q^{n\times m}, \beta$

Find: s with $||s|| \leq \beta$ such that $As = 0 \bmod q$

Ajtai

Example instance SIS

$q = 16$

$\beta = 3$

$$\underbrace{\begin{bmatrix} 2 & 10 & 0 & 12 \\ 7 & 1 & 11 & 7 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} -2 \\ 0 \\ 1 \\ 1 \end{bmatrix}}_{s} = 0 \mod q$$

hardness comes from the "smallness" of s

$$\|s\| = \sqrt{4+1+1} = \sqrt{6} \leq 3$$

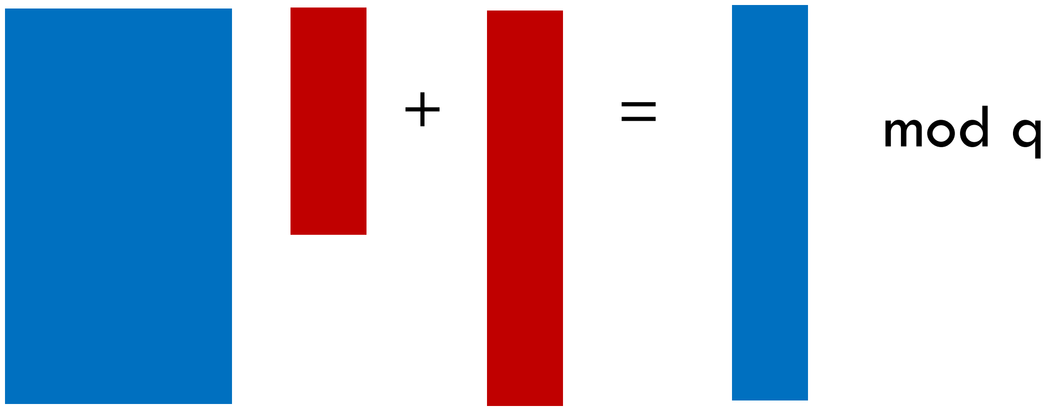
Learning With Errors Problem

Problem (Learning with Errors (LWE))

Given: (A,b) with $A \leftarrow_\$ \mathbb{Z}_q^{m\times n}$, $s \leftarrow_\sigma \mathbb{Z}^n$, $e \leftarrow_\sigma \mathbb{Z}^n$, $b = As + e \bmod q$

Find: s

discrete Gaussian distribution



LWE problem by Regev

1976 · 1977 · 1982 · 1996 · 1997 · 2005

Example instance LWE

$$\begin{bmatrix} 2 & 7 \\ 10 & 1 \\ 0 & 11 \\ 12 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 12 \\ 6 \\ 13 \\ 15 \end{bmatrix} \mod 16$$

$A \quad s \quad e \quad b$

adding "error"/"noise" makes LWE a hard problem

$As = b \mod q$ would be an easy problem, solved by Gaussian elimination

Learning With Errors Problem

Problem (Learning with Errors (LWE))

Given: (A,b) with A $\leftarrow_{\$} \mathbb{Z}_q^{m\times n}$, s $\leftarrow_{\sigma} \mathbb{Z}^n$, e $\leftarrow_{\sigma} \mathbb{Z}^n$, b $=$ As $+$ e mod q

Find: s

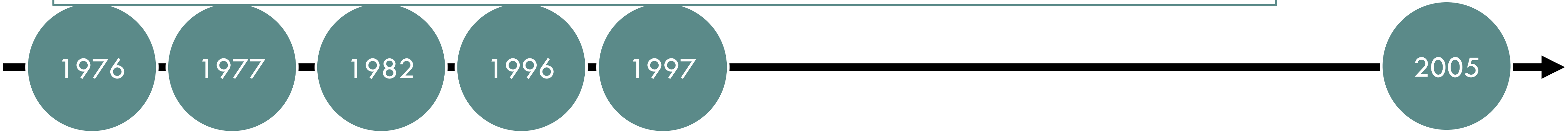
Problem (Decisional LWE Problem)

Let s $\leftarrow_{\sigma} \mathbb{Z}_q^n$ and $\mathrm{D}_{s}^{LWE} \rightarrow$ (A, As $+$ e mod q)

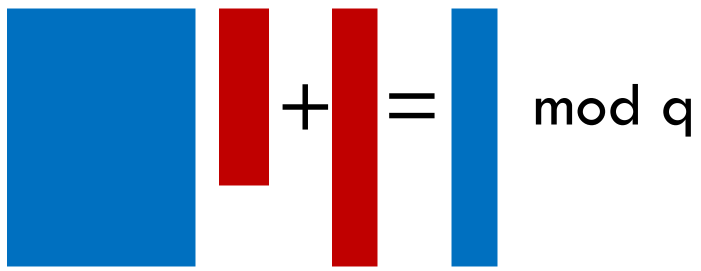
Given: (A,b)

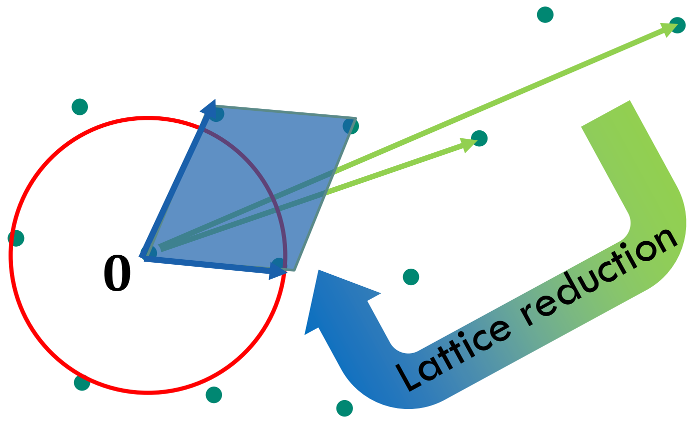
Decide: (A,b) $\leftarrow \mathrm{D}_{s}^{LWE}$ or (A,b) $\leftarrow_{\$} \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^n$

LWE problem by Regev



Solving LWE by solving SVP





Given $\mathbf{A}\mathbf{s} + \mathbf{e} = \mathbf{b} \bmod q$ → **1** Construct

$$\mathrm{L} = \left\{ \mathrm{v} \in \mathbb{Z}^m \mid \exists\, \mathrm{x} \in \mathbb{Z}^n : \begin{pmatrix} \mathrm{A} & \mathrm{b} \\ 0 & 1 \end{pmatrix} \cdot \mathrm{x} = \mathrm{v} \bmod q \right\}$$

$\mathrm{e} \in \mathrm{L}$:

$$\begin{pmatrix} \mathrm{A} & \mathrm{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\mathrm{s} \\ 1 \end{pmatrix} = \begin{pmatrix} -\mathrm{As} + \mathrm{b} \\ 0 \cdot \mathrm{s} + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} \mathrm{e} \\ 1 \end{pmatrix} =: \mathrm{v}$$

↓

2 Solve SVP in L to find $\begin{pmatrix} \mathrm{e} \\ 1 \end{pmatrix}$ → **3** Compute s from

$$\mathrm{b} - \mathrm{e} = \mathrm{As} \bmod q$$

LWE-Based Encryption Scheme

Key generation

secret key

$$A \cdot S + E = B \mod q$$

public key

Encryption

A B m

public key message

$$A \cdot S + E = B \mod q$$

$$A \cdot S' + E' = C \mod q$$

$$\underbrace{B \cdot S' + E''}_{\approx V} + \lfloor q/4 \rceil m = C' \mod q$$

Why is it not secure to use E' for both, C and C'?

Decryption

Example

A (5) B (7) m (1)

$A \cdot S + E = B \mod q$ (5 · 1 + 2 = 7)

$A \cdot S' + E' = C \mod q$ (5 · −1 + 1 = −4)

$B \cdot S' + E'' + \lfloor q/4 \rceil m = C' \mod q$ (7 · −1 + 2 + 1 = −1)

$B \cdot S' + E'' \approx V$

$B \cdot S' = ASS' + ES' \approx ASS'$

$C \cdot S = AS'S + E'S \approx AS'$

S (1) C (−4) C' (−1)

secret key cipher text

$\lfloor (C' - C \cdot S) 4/q \rceil = m$ (−1, −4, 1)

$m = 1 = \lfloor 3/4 \rceil$

Security of LWE-based encryption schemes

Theorem

If the decisional LWE is hard then the encryption scheme is IND-CPA secure.

Proof idea:

If there exists an adversary A that can break the IND-CPA security of the encryption scheme, then we can construct an algorithm B that solves the decisional LWE problem.

INDistinguishability under Chosen-Plaintext Attacks (IND-CPA)

Security experiment

S E A B $\leftarrow$ KeyGen

m_0 m_1 $\leftarrow$ A B

b $\leftarrow_{\$} \{0,1\}$

C C‘ $\leftarrow$ Encrypt(A B , m_b)

b' $\leftarrow$ A B C C‘

return $[[b = b']]$

IND-CPA by Goldwasser and Micali

1976 — 1977 — 1982 — 1996 — 1997 — 2005 — 1984

INDistinguishability under Chosen-Plaintext Attacks (IND-CPA)

Proof idea:

If A B  can decide

$$C' \stackrel{?}{=} B \cdot S' + E'' + \lfloor q/4 \rceil\, m_0$$

or

$$C' \stackrel{?}{=} B \cdot S' + E'' + \lfloor q/4 \rceil\, m_1$$

then  distinguishing the LWE-distribution from the uniform distribution.

Example 2

5 · 1 + 2 = 7 mod 16

5 7 1

5 · ~~-1~~ -2 + 1 = ~~-4~~ 7 mod 16

7 · ~~-1~~ -2 + 2 + 4 1 = ~~-1~~ 8 mod 16

1 ~~-4~~ 7 ~~-1~~ 8 ⌊(~~-1~~ 8 - ~~-4~~ 7 · 1)1/4⌉= 1

$\lfloor 1/4 \rceil = 0 \neq 1$

! Decryption error / decryption failure

Correctness definition

Definition (Correctness of a PKE)

An encryption scheme P is **correct** if

$$\Pr[\mathrm{Decrypt}(\mathrm{Encrypt}(\mathrm{m}, \mathrm{pk}), \mathrm{sk}) = \mathrm{m}] = 1$$

(randomness is taken over keys and random coins).

Definition (δ -Correctness of a PKE)

An encryption scheme P is **δ-correct** if

$\Pr[\mathrm{Decrypt}(\mathrm{Encrypt}(\mathrm{m}, \mathrm{pk}), \mathrm{sk}) = \mathrm{m}] \geq 1 - \delta.$

Example statement:
Frodo NIST submission, Section 2.2.7

The next lemma states bounds on the size of errors that can be handled by the decoding algorithm.

Lemma 2.18. *Let* $q = 2^D$, $B \leq D$. *Then* $\mathrm{dc}(\mathrm{ec}(k) + e) = k$ *for any* $k, e \in \mathbb{Z}$ *such that* $0 \leq k < 2^B$ *and* $-q/2^{B+1} \leq e < q/2^{B+1}$.

$$\lfloor (C' - C \cdot S) 4/q \rceil = m$$

$$= B \cdot S' + E'' + \lfloor q/4 \rceil m - (A \cdot S' + E') S$$

$$= (A \cdot S + E) S' + E'' + \lfloor q/4 \rceil m - (A \cdot S' + E') S$$

$$= E S' + E'' + E' S + \lfloor q/4 \rceil m$$

Discussion:

Do you think the (in-)correctness of an encryption scheme impacts the security? Or is it merely an inconvience one has to overcome, e.g., when implementing the scheme?

Impact of decryption errors

Every decryption error tells us…

E S‘ + E“ + E‘ S $\geq q/2^{B+1}$

or

E S‘ + E“ + E‘ S $< -q/2^{B+1}$

Many decryption errors reveal information about the secret key S.

“One failure is not an option…“

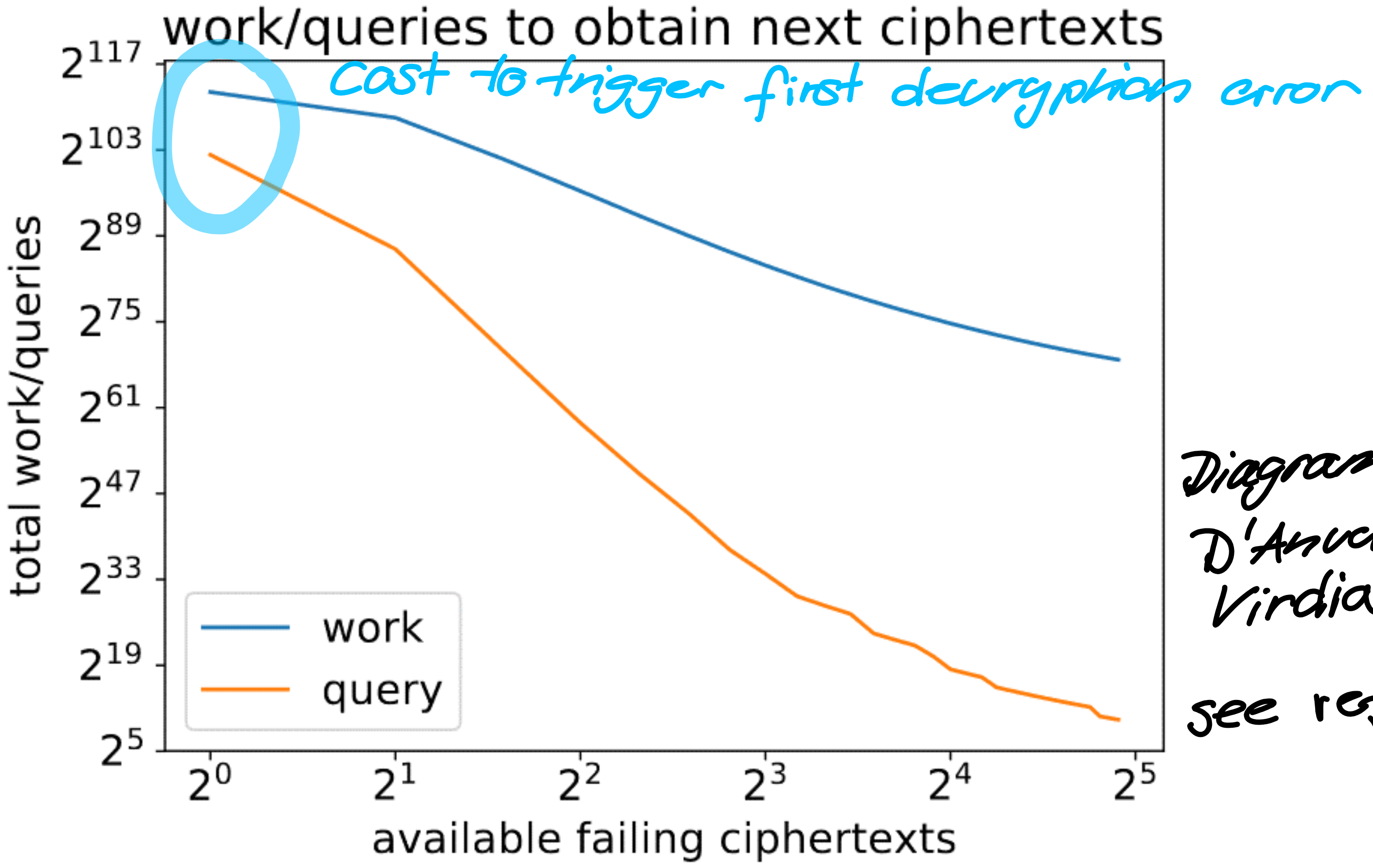


Diagram by D'Anvers, Rossi and Virdia

see references

Impact of decryption errors

Every decryption error tells us…

$$E\,S' + E'' + E'\,S \geq q/2^{B+1}$$

or

$$E\,S' + E'' + E'\,S < -q/2^{B+1}$$

Every successful decryption tells us…

$$-q/2^{B+1} \leq E\,S' + E'' + E'\,S < q/2^{B+1}$$

Even garther information from successful decryption.

Research at UW & Wrap-up

Post-quantum crypto at UWaterloo (and in KW)

Research areas

- Design of cryptosystems
- Cryptanalysis on classical and quantum computers
- Efficient implementations
- Adapting network protocols to post-quantum algorithms

PQ categories

- Lattice-based
- Isogeny-based

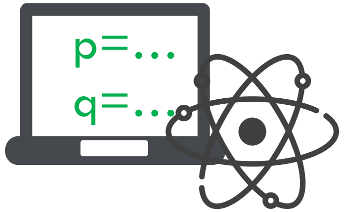
Research projects

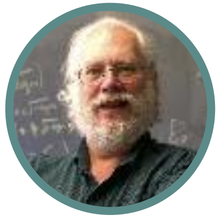
- OQS: Open Quantum Safe open source software project
- CryptoWorks21 graduate training program

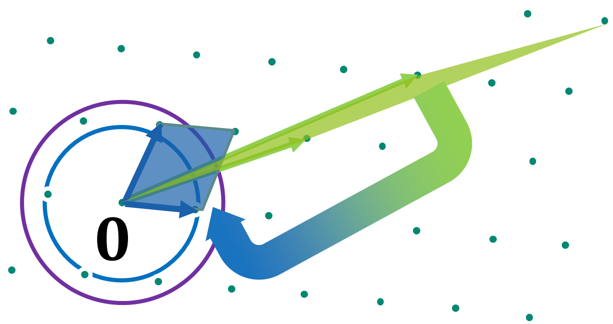
PQ companies in KW

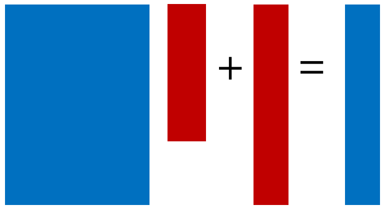
- evolutionQ
- ISARA

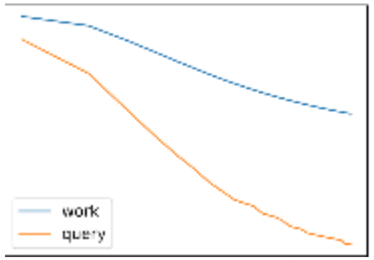
Conclusion

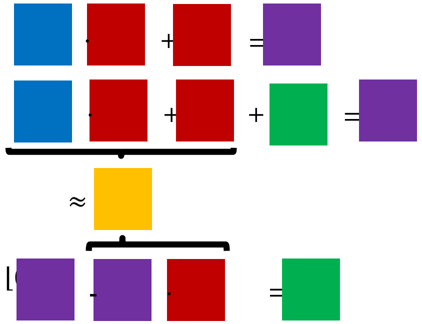












Classical crypto

Shor's alg. QC, NIST

Defining & solving lattice problems

SIS LWE

LWE-based encryption

Nina Bindel
nlbindel@uwaterloo.ca

THANKS

References 1/3

Classical crypto

1. W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6):644–654, 1976.
2. R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signature and public-key cryptosystems. Communications of the Association for Computing Machinery, 21(2):120–126, 1978.

Shor‘s algorithm, Quantum computer, Post-quantum crypto

1. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26:1484–1509, 1997.
2. M. Mosca. Cybersecurity in an era with quantum computers: Will we be ready? Cryptology ePrint Archive, Report 2015/1075, 2015.
3. QUROPE Quantum Information Processing and Communication in Europe, „The Quantum Manifesto- A New Era of Technology“, unter http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf, Mai 2016
4. https://en.wikipedia.org/wiki/Quantum_computing
5. D. J. Bernstein, J. Buchmann, and E. Dahmen, editors. Post-quantum cryptography. Mathematics and Statistics Springer-11649; ZDB-2-SMA. Springer, 2009.

References 2/3

NIST

1. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/projects/postquantum-cryptography, 2017
2. E. Alkim, R. Avanzi, J. Bos, L. D. Ducas, A. de la Piedra, T. Pöppelmann, P. Schwabe, and D. Stebila. NewHope. NIST Post-Quantum Standardization [164], 2017. https://newhopecrypto.org/.
3. E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, D. Stebila, K. Easterbrook, and B. LaMacchia. FrodoKEM–Learning With Errors Key Encapsulation. NIST Post-Quantum Standardization [164], 2017. https://frodokem.org/.
4. J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehlé. CRYSTALS–Kyber: a CCA-secure module-latticebased KEM. NIST Post-Quantum Standardization [164], 2017. https://pqcrystals.org/kyber/index.shtml.
5. Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Krämer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, and Gustavo Zanon. The lattice-based digital signature scheme qTESLA – Submission to the NIST's post-quantum cryptography standardization process, 2017. https://www.qtesla.org.

References 3/3

Lattices, LWE&SIS, LWE-based encryption scheme and decryption failures

1. Y. Chen and P. Q. Nguyen. BKZ 2.0: Better lattice security estimates. In ASIACRYPT 2011, volume 7073 of LNCS, pages 1–20. Springer, Heidelberg, 2011.
2. R. Lindner and C. Peikert. Better key sizes (and attacks) for LWE-based encryption. In CT-RSA 2011, volume 6558 of LNCS, pages 319–339. Springer, Heidelberg, 2011.
3. C. Peikert. A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4):283–424, 2016.
4. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In 37th ACM STOC, pages 84–93. ACM Press, 2005.
5. J.P. D'Anvers, M. Rossi, F. Virdia: (One) failure is not an option: Bootstrapping the search for failures in lattice-based encryption schemes. Cryptology ePrint Archive, Report 2019/1399 (2019), https://eprint.iacr.org/2019/1399
6. N. Bindel, J.M. Schanck, Decryption failure is more likely after success, Cryptology ePrint Archive, Report 2019/1392, https://eprint.iacr.org/2019/1392
7. M. Mosca and D. Stebila. Open quantum safe – software for prototyping quantum-resistant cryptography, 2018. https://openquantumsafe.org/
8. https://cryptoworks21.uwaterloo.ca/

IND-CPA

1. S. Goldwasser, S. Micali: *Probabilistic encryption*. In: *Journal of Computer and System Sciences*. Band 28, Nr. 2, 1984, S. 270–299