KU LEUVEN

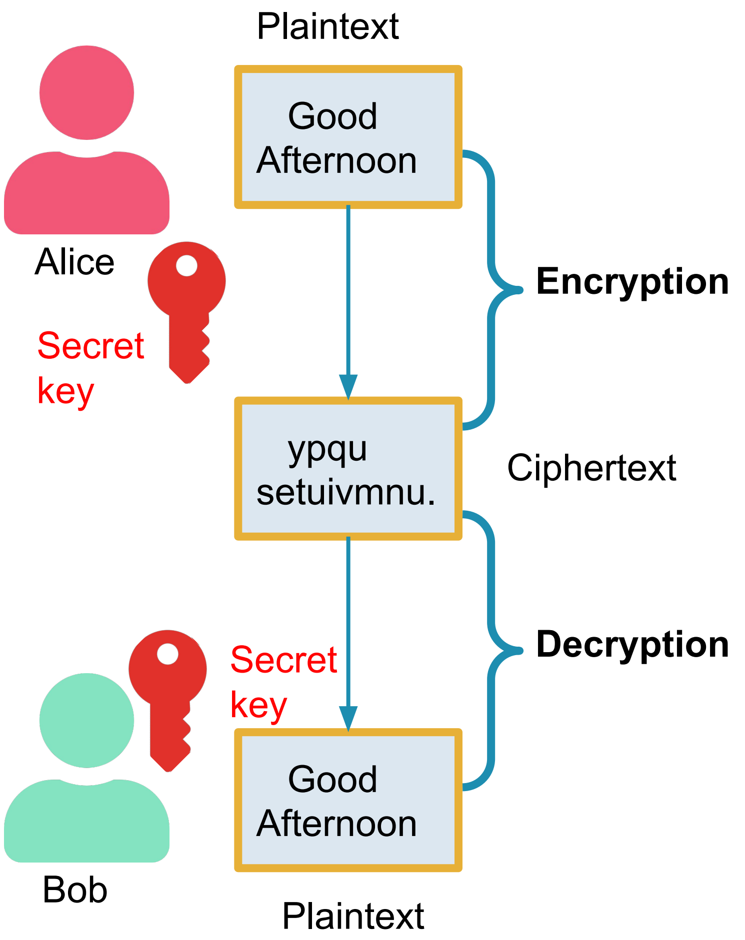
Quantum secure public-key cryptography: history and current developments

Suparna Kundu

Symmetric key cryptography

- Before 1970 people only used Symmetric key Cryptography

- Symmetric key scheme
  - A very strong algorithm
  - Both party shares same secret key



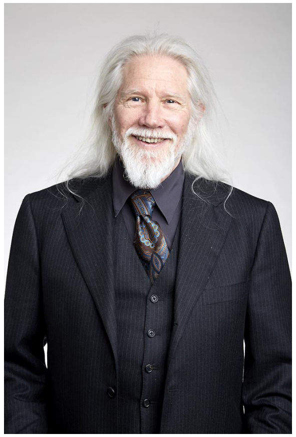
Symmetric-key scheme

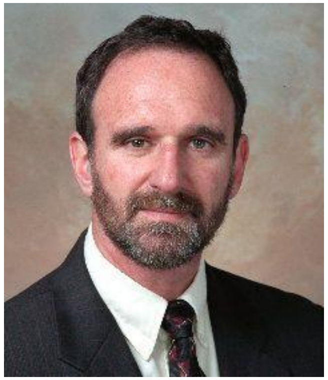
KU LEUVEN

Public key cryptography

1976: Whitfield Diffie and Martin Hellman introduce the concept of Public-key Cryptography

- Deffie-Hellman[1] (DH) protocol





1978: Ron Rivest, Adi Shamir and Leonard Adleman proposed first successful PKC RSA[2]

1985,1987: Elliptic curve cryptography (ECC) introduced by Victor Miller[3] and Neal Koblitz[4]

[1] Diffie, Whitfield; Hellman, Martin E. (November 1976). "New Directions in Cryptography". *IEEE Transactions on Information Theory*. **22** (6): 644–654.
[2] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). *Communications of the ACM*. **21** (2): 120–126.
[3] Miller, V. (1985). "Use of elliptic curves in cryptography". *Advances in Cryptology — CRYPTO '85 Proceedings*. *CRYPTO*. Lecture Notes in Computer Science. **85**. pp. 417–426.
[4] Koblitz, N. (1987). "Elliptic curve cryptosystems". *Mathematics of Computation*. **48** (177): 203–209.

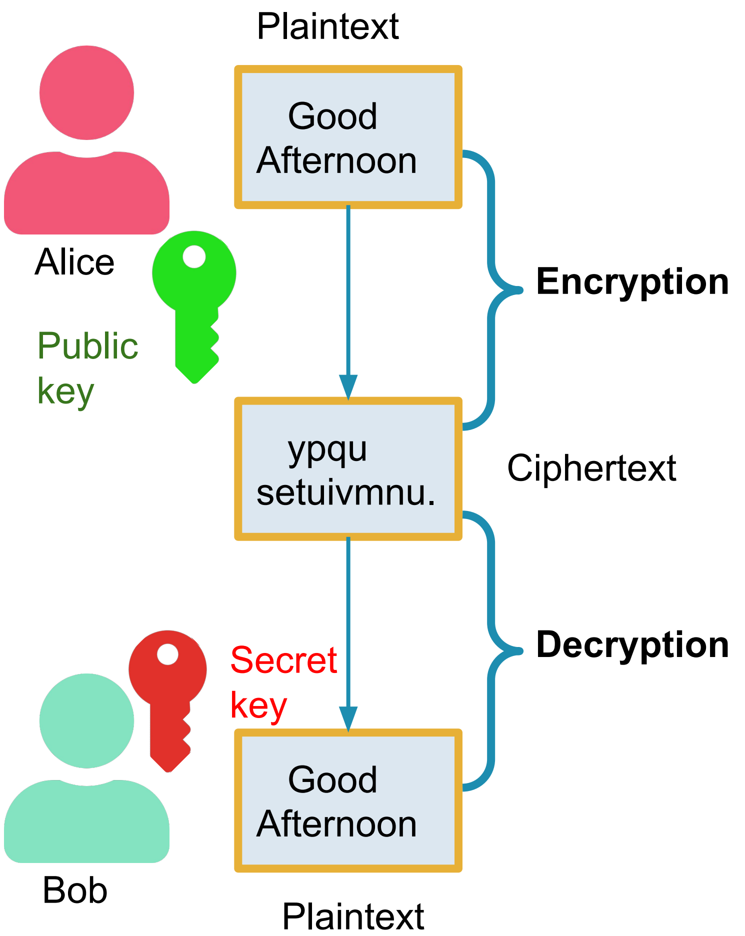
KU LEUVEN

Public key cryptography

Public key crypto system uses:

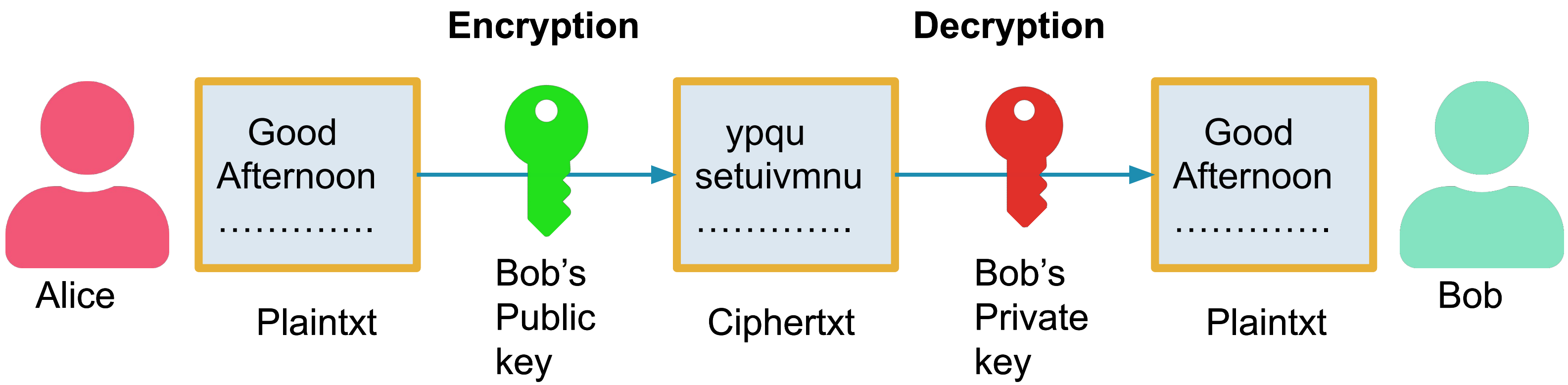
- Two keys
  - Public key → **Encryption**
  - Secret key → **Decryption**

- Cryptographic algorithms are based on mathematical problem (One-way function)
  - RSA: Large integer factorization (Given N=p*q, find p and q)
  - ECC: Elliptic curve discrete logarithm problem (Given xP and P, find x)



Public-key scheme

Public key cryptography



Public-key cryptography

used in

SSL/ TLS

Secure key exchange

Crypto- currencies

Digital signature

G Pay

Digital payment

KU LEUVEN

Quantum Computer and its uses

1980: Paul Benioff[1] proposed quantum mechanical model of the Turing machine

1994: Peter Shor[2] developed a quantum algorithm for factoring integers

- It can break RSA scheme

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting [1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

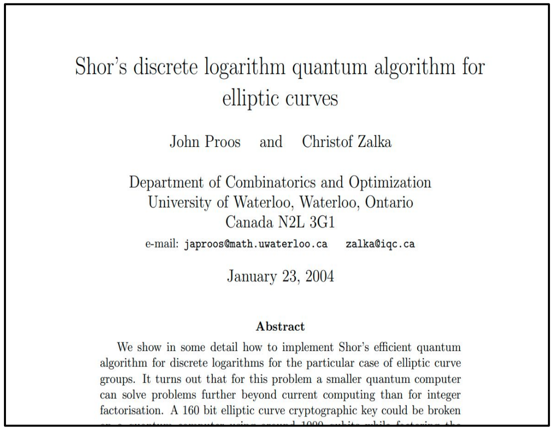
[1] Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". *Journal of Statistical Physics*. **22** (5): 563–591.

[2] Mermin, David (March 28, 2006). "Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm" (PDF). *Cornell University, Physics 481-681 Lecture Notes*. Archived from the original (PDF) on 2012-11-15.

KU LEUVEN

Quantum Computer and its uses

2004: Proos and Zalka[1] presented an algorithm to solve the elliptic curve discrete logarithm problem in polynomial time



Shor's discrete logarithm quantum algorithm for elliptic curves

John Proos and Christof Zalka

Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario
Canada N2L 3G1
e-mail: japroos@math.uwaterloo.ca zalka@iqc.ca

January 23, 2004

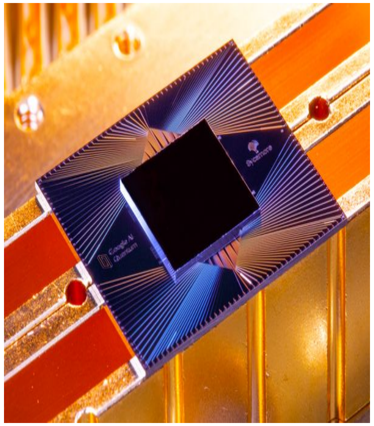
Abstract

We show in some detail how to implement Shor's efficient quantum algorithm for discrete logarithms for the particular case of elliptic curve groups. It turns out that for this problem a smaller quantum computer can solve problems further beyond current computing than for integer factorisation. A 160 bit elliptic curve cryptographic key could be broken

2019: Google AI, with NASA, claimed to achieve 54-qbit quantum supremacy[2]

2020: IBM claimed to achieve 65-qbit quantum supremacy[3]

Target[3]: 1000-qbit on 2023



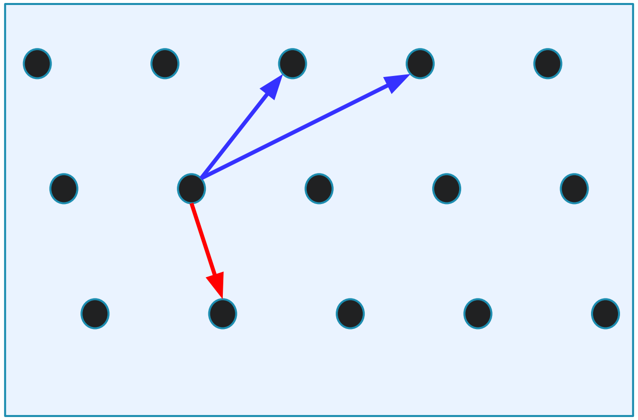
[1] Proos, John & Zalka, Christof. (2003). Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves. Quantum Information & Computation. 3.
[2] https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html
[3] https://research.ibm.com/blog/ibm-quantum-roadmap

Lattice based Cryptography

1996: Miklós Ajtai[1] introduced the first lattice-based cryptographic construction

Hard Problem: Shortest vector problem (SVP)

SVP: Given a lattice L, find the shortest non-zero vector



Basis vectors in blue
Shortest vector in red

[1] Ajtai, Miklós (1996). "Generating Hard Instances of Lattice Problems". *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. pp. 99–108.

KU LEUVEN

Lattice based Cryptography

1998: Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman[1] introduced

- the first lattice-based public-key encryption scheme
- known as NTRU
- This version wasn't provably secure

Nth Degree Truncated Polynomial Ring Units
($R=Z[X]/(X^N-1)$)

[1] Hoffstein, Jeffrey; Pipher, Jill; Silverman, Joseph H. (1998). "NTRU: A ring-based public key cryptosystem". *Algorithmic Number Theory*. Lecture Notes in Computer Science. **1423**. pp. 267–288.

Lattice based Cryptography

2005: Oded Regev[1] introduced

- 1st provably secure lattice-based public-key encryption scheme
- Learning with errors (LWE) problem

$$\underbrace{\begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}}_{\mathbf{A}} \cdot \underbrace{\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}}_{\mathbf{s}} + \underbrace{\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}}_{\mathbf{e}} = \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}}_{\mathbf{b}}$$

Problem: Find **s** in presence of **e**

Search problem:

- Choose $\mathbf{s} \leftarrow Z_q^n$
- Oracle generates

  $\mathbf{a} \leftarrow Z_q^n$ & small $\mathbf{e} \leftarrow \chi$
- Oracle outputs

  $\mathbf{a}, b = \mathbf{a} \cdot \mathbf{s} + \mathbf{e} \; mod \; q$
- repeat with fresh $\mathbf{a}$ and $\mathbf{e}$

[1] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC ’05. pp. 84–93. ACM (2005), http://doi.acm.org/10.1145/ 1060590.1060603

KU LEUVEN

Lattice based Cryptography

LWE decision problem:

LWE distribution	Uniform distribution
Fixed $\mathbf{s} \leftarrow \mathcal{U}(Z_q^n)$	
$\mathbf{a_i} \leftarrow \mathcal{U}(Z_q^n)$ $\mathbf{e_i} \leftarrow \chi$	$\mathbf{a_i} \leftarrow \mathcal{U}(Z_q^n)$ $b_i \leftarrow \mathcal{U}(Z_q^n)$
$\mathbf{a}_1, b_1 = \mathbf{a_1} \cdot \mathbf{s} + \mathbf{e_1} \ mod\ q$	$\mathbf{a}_1, b_1$
• • •	• • •
$\mathbf{a}_n, b_n = \mathbf{a_n} \cdot \mathbf{s} + \mathbf{e_n} \ mod\ q$	$\mathbf{a}_n, b_n$

Problem: Distinguishing the distribution

Lattice based Cryptography

Relation with lattice:

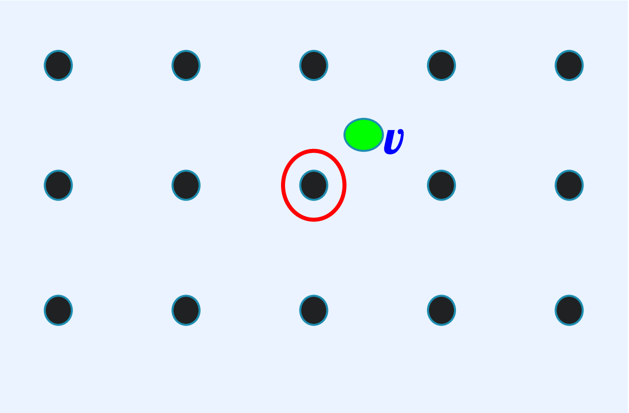
- Given $\mathbf{A} \in Z_q^{n\times n}$ & $\mathbf{b} \in Z_q^n$ with $\mathbf{b} = A \cdot \mathbf{s} + \mathbf{e}$
- small **e** is in [-q/2, q/2]
- The set $\mathcal{L}(A) = \{\mathbf{y} \in Z_q^n : \mathbf{y} = \mathbf{A} \cdot \mathbf{x} \text{, where } \mathbf{x} \in Z_q^n\}$
- $\mathcal{L}(A)$ forms a lattice
  - if y_1, y_2 ϵ $\mathcal{L}(A)$ then $y_1 - y_2$ ϵ $\mathcal{L}(A)$
- If **e** ≠ 0 then **b** $\notin$ $\mathcal{L}(A)$ but close to it

KU LEUVEN

Lattice based Cryptography

Closest vector problem (CVP):

Given lattice $\mathcal{L} \subset V$ and $\boldsymbol{v} \in V$ (may not be in $\mathcal{L}$) then find the closest vector of $\boldsymbol{v}$ in $\mathcal{L}$



Bounded distance decoding (BDD):

Maximum distance of vector $\boldsymbol{v}$ from $\mathcal{L}$ is $\lambda(\mathcal{L})/2$, where $\lambda(\mathcal{L})$ is the shortest non-zero vector in $\mathcal{L}$

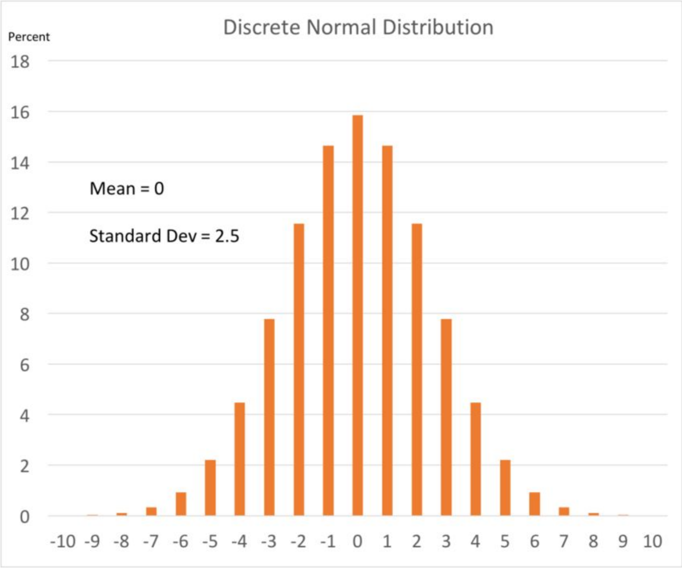
By solving BDD where $|\mathbf{e}| \leq \lambda(\mathcal{L})/2$ we can find $\mathbf{s}$ of $\mathbf{b} = A \cdot \mathbf{s} + \mathbf{e}$

KU LEUVEN

Lattice based Cryptography

Few properties of LWE problem:

- The error distribution χ usually discrete Gaussian distribution $(0, \sigma)$ over Z
- Oded Regev[1] and Chris Peikert[2] proved that LWE problem is as hard as worst case lattice problems
  - For this $\sqrt{2\pi}\sigma > \sqrt{n}$
- Search LWE problem and Decision LWE problem is equivalent



Taken from: https://www.researchgate.net/profile/Sebastian-Schneeweiss

[1] O. Regev. New lattice-based cryptographic constructions. Journal of the ACM, 51(6):899–942, 2004. Preliminary version in STOC'05.
[2] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In Proc. 41st ACM Symp. on Theory of Computing (STOC), pages 333–342. 2009.

KU LEUVEN

Lattice based Cryptography

LWE based Encryption: Key generation

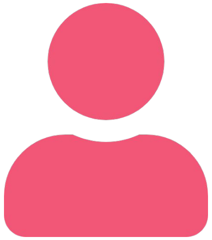
$$A \in Z_q^{n \times n}$$

$$s \leftarrow Z_q^n \quad e \leftarrow [-q/2, q/2]$$

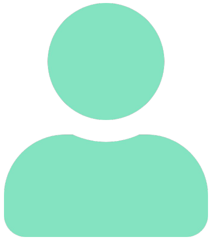
$$\mathbf{b} = A \cdot s + e$$

$A, \mathbf{b}$ ←

Alice



Bob



A s + e = b

Lattice based Cryptography

LWE based Encryption: Encryption

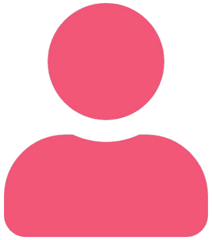
$$A \in Z_q^{n \times n}$$

$$\mathbf{s} \leftarrow Z_q^n \quad e \leftarrow [-q/2, q/2]$$

$$\mathbf{b} = A \cdot s + e$$

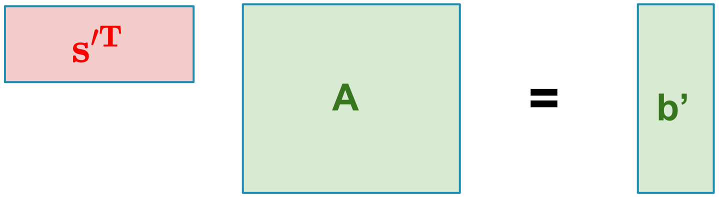
$A, \mathbf{b}$

Alice

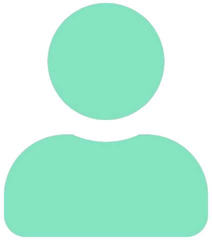


$$\mathbf{s}' \leftarrow Z_q^n$$

$$\mathbf{b}' = s'^T \cdot A$$



Bob



Lattice based Cryptography

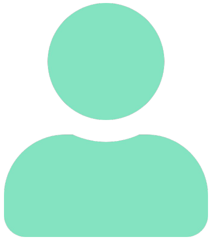
LWE based Encryption: Encryption

$$A \in Z_q^{n\times n}$$

$$\mathbf{s} \leftarrow Z_q^n \quad e \leftarrow [-q/2, q/2]$$

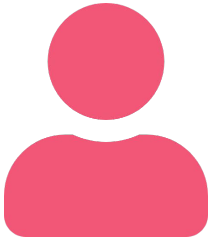
$$\mathbf{b} = A \cdot s + e$$

Bob



$A, \mathbf{b}$

Alice



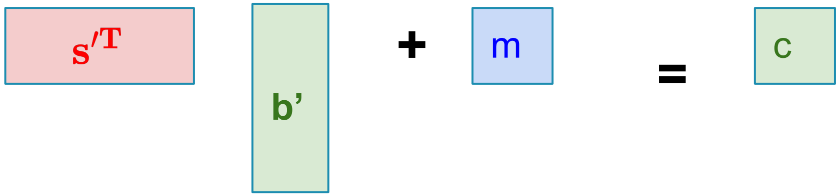
$$\mathbf{s}' \leftarrow Z_q^n$$

$$\mathbf{b}' = s'^T \cdot A$$

$$m \in \{0, 1\}$$

$$c = s'^T \cdot \mathbf{b} + m \cdot \lfloor q/2 \rfloor$$

$\mathbf{b}', c$



KU LEUVEN

Lattice based Cryptography

LWE based Encryption: Decryption

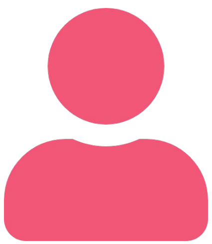
$A \in Z_q^{n \times n}$

$\mathbf{s} \leftarrow Z_q^n \quad e \leftarrow [-q/2, q/2]$

$\mathbf{b} = A \cdot s + e$

$A, \mathbf{b}$

Alice



$\mathbf{s}' \leftarrow Z_q^n$

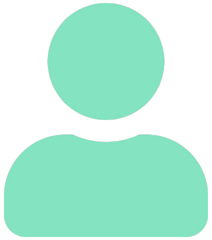
$\mathbf{b}' = s'^T \cdot A$

$m \in \{0, 1\}$

$c = s'^T \cdot \mathbf{b} + m \cdot \lfloor q/2 \rfloor$

$\mathbf{b}', c$

Bob



$r = c - \mathbf{s}^T \cdot \mathbf{b}'$

c - s^T b' = r

$$m' = \begin{cases} 0 & -\lfloor q/4 \rfloor \leq r < \lfloor q/4 \rfloor \\ 1 & else \end{cases}$$

KU LEUVEN

Lattice based Cryptography

2012: Jintai Ding[1] first proposed

- the idea of key exchange by using LWE problem and
- Variant of LWE Ring-LWE problem
- Uses the ring $R_q^n = Z_q[x]/f(x)$
- $f(x)$ is n degree polynomial

Ring-LWE problem:
Matrix-vector multiplication replaced by polynomial multiplication

$$(\longleftarrow a \in R_q^n \longrightarrow) \cdot \begin{pmatrix} \uparrow \\ s \in R_q^n \\ \downarrow \end{pmatrix} + \begin{pmatrix} \uparrow \\ e \in R_q^n \\ \downarrow \end{pmatrix}$$

$$(\longleftarrow a \in R_q^n \longrightarrow)$$

ax^3+bx^2+cx+d

a	b	c	d
b	c	d	-a
c	d	-a	-b
d	-a	-b	-c

= **A**

[1] Ding, Jintai; Xie, Xiang; Lin, Xiaodong (2012). *A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem*

Lattice based Cryptography

Cryptosystems based on LWE

- Inefficient due to matrix-vector multiplication
- But have strong security

Cryptosystems based on Ring-LWE

- Fast polynomial multiplication
- Some researchers are skeptical about hardness of hard lattice problems in ideal lattices

Lattice based Cryptography

2016: Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe jointly proposed

- practical key-exchange mechanism (KEM) NewHope[1]
- Security depends on hardness of the Ring-LWE problem
- Followed Ding's idea with modification
- Selected for Google's post-quantum experiment

[1] Erdem Alkim, Philipp Jakubeit, Peter Schwabe: NewHope on ARM Cortex-M. SPACE 2016: 332-349

Lattice based Cryptography

NewHope[1]:

- Used ring $R_q^n = Z_q[x]/f(x)$ with q prime and f(x)= $(1+x^n)$, n power-of-2
- One of the most costly operations is polynomial multiplication
- Number theoretic transformation (NTT) method is used for this
- res=a*b as
- The complexity is O(n log n)
- They achieved a very good efficiency due to their design choices

$$\mathbf{b} = A \cdot s + e$$
$$\mathbf{b}' = s'^T \cdot A$$
$$c = s'^T \cdot \mathbf{b} + m \cdot \lfloor q/2 \rfloor$$

res= NTT^{-1}(NTT(a)*NTT(b))

[1] Erdem Alkim, Philipp Jakubeit, Peter Schwabe: NewHope on ARM Cortex-M. SPACE 2016: 332-349

NIST's contribution in post-quantum cryptography

2016: NIST National Institute of Standards and Technology U.S. Department of Commerce initiated a post-quantum PKC standardization process

Categories:

- KEM / Encryption
- Digital signature

NIST Released NISTIR 8105, Report on Post-Quantum Cryptography

"........The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. In recent years, there has been a substantial amount of research on quantum computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere……."

[1] https://csrc.nist.gov/News/2016/NIST-Released-NISTIR-8105,-Report-on-Post-Quantum

NIST's contribution in post-quantum cryptography

2017: First round:

	Digital Signature	KEM/Encryption	Total
Lattice-based	5	21	29
Code-based	3	16	19
Multi-variate	7	2	9
Hash-based	3	0	3
Others	2	6	8

Kyber[1] (2017)

Kyber[1] team introduced another new variant of LWE problem

- Module-LWE problem:
  - Trade off between ring and standard LWE
  - Fast operations
  - Strong security

$$\begin{pmatrix} a_{1,1} \in \mathrm{R'}_q & \cdots & a_{1,k} \in \mathrm{R'}_q \\ \vdots & \ddots & \vdots \\ a_{k,1} \in \mathrm{R'}_q & \cdots & a_{k,k} \in \mathrm{R'}_q \end{pmatrix} \cdot \begin{pmatrix} s_1 \in \mathrm{R'}_q \\ \vdots \\ s_k \in \mathrm{R'}_q \end{pmatrix} + \begin{pmatrix} e_1 \in \mathrm{R'}_q \\ \vdots \\ e_k \in \mathrm{R'}_q \end{pmatrix}$$

- Modulus q of underlying ring $\mathrm{R}'_q = Z_q[X]/(X^n+1)$ is prime and n = 256
- Polynomial multiplication
  - One of most costly operation
  - Used NTT

[1] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé: CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. EuroS&P 2018: 353-367

Saber[1] (2018)

Learning with rounding (LWR) problem:

Given samples $(\mathbf{a}, b = \lfloor \mathbf{a} \cdot \mathbf{s} \rceil_p)$ for $\mathbf{a}, \mathbf{s} \in Z_q^n$, and rounding modulus p, find secret **s**

Errors are generated *inherently* → less randomness

At least as hard as LWE (Banerjee et al.[2], Rosen et al.[3])

Similar to LWE, for LWR can define

- Ring-LWR
- Module-LWR

[1]Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren: Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM. AFRICACRYPT 2018: 282-305
[2] Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: EUROCRYPT 2012. pp. 719–737 (2012), https://doi.org/10.1007/978-3-642- 29011-4_42
[3] Alperin-Sheriff, J., Apon, D.: Dimension-preserving reductions from LWE to LWR. Cryptology ePrint Archive, Report 2016/589 (2016)

Saber[1] (2018)

- The hard problem is Module-LWR
- Underlying ring is $R_q = Z_q[X]/(X^n + 1)$, n=256
- Note that there is two modulus
    - ring modulus q and rounding modulus p
    - both are power-of-2
- Polynomial multiplication
    - As q is not prime
    - Can't use NTT
    - But use hibrid multiplication
        - a combination of Toom-Cook, karatsuba and schoolbook
    - Approximately as efficient as NTT

KU LEUVEN

Round 3 finalists of NIST's competition

2020: Third round:

	Digital Signature	KEM/Encryption	Total
Lattice-based	2	3	5
Others	1	1	2

	KEM/Encryption	Schemes
Lattice-based	3	Kyber, NTRU, Saber

KU LEUVEN

Brief overview of our work

Motivation:

- After NIST’s PQC standardization process many new results published
  - cryptanalysis[5], mathematical results[3],
  - implementation design[1,2] and new techniques[4]
- Improving existing schemes incorporating these results
- Creating new schemes focused on
  - Improved efficiency
  - Without degrading security

[1]Jose Maria Bermudo Mera, Furkan Turan, Angshuman Karmakar, Sujoy Sinha Roy, Ingrid Verbauwhede: Compact domain-specific co-processor for accelerating module lattice-based key encapsulation mechanism. IACR Cryptology ePrint Archive 2020: 321 (2020), https://eprint.iacr.org/2020/321
[2]Angshuman Karmakar, Jose Maria Bermudo Mera, Sujoy Sinha Roy, Ingrid Verbauwhede: Saber on ARM CCA-secure module lattice-based key encapsulation on ARM. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 243-266 (2018), https://doi.org/10.13154/tches.v2018.i3.243-266
[3]Le H.Q., Mishra P.K., Duong D.H., Yasuda M. (2018) Solving LWR via BDD Strategy: Modulus Switching Approach. In: Camenisch J., Papadimitratos P. (eds) Cryptology and Network Security. CANS 2018. Lecture Notes in Computer Science, vol 11124. Springer, Cham, https://doi.org/10.1007/978-3-030-00434-7_18
[4]https://estimate-all-the-lwe-ntru-schemes.github.io/docs/
[5]Martin R. Albrecht and Benjamin R. Curtis and Amit Deo and Alex Davidson and Rachel Player and Eamonn W. Postlethwaite and Fernando Virdia and Thomas Wundere : Estimate all the {LWE, NTRU} schemes! , Cryptology ePrint Archive, Report 2018/331 (2018), https://eprint.iacr.org/2018/331/

Brief overview of our work

Scabbard[1]:

- A suite of efficient LWR based KEM
- Both modulus q and p here power-of-2
- Contains 3 different schemes
  - Florete
  - Sable
  - Espada

[1]Jose Maria Bermudo Mera, Angshuman Karmakar, Suparna Kundu, Ingrid Verbauwhede: Scabbard: a suite of efficient learning with rounding key-encapsulation mechanisms. IACR Cryptol. ePrint Arch. 2021: 954 (2021)

KU LEUVEN

Brief overview of our work

Florete[1]:

- Underlying ring is $\mathrm{R}_q^n = Z_q[X]/(X^{768} - x^{384} + 1)$
- Hardness depends on Ring-LWR
  - Secure assuming Ring-LWE is hard
  - No error sampling is needed
- Polynomial multiplication:
  - hybrid multiplication
  - But more efficient than Saber
  - due to the hard problem choice
- Another costly operation: Pseudo random number sampling
  - Need less due to smaller parameter size than Saber
- One of the fastest KEM

[1] Jose Maria Bermudo Mera, Angshuman Karmakar, Suparna Kundu, Ingrid Verbauwhede: Scabbard: a suite of efficient learning with rounding key-encapsulation mechanisms. IACR Cryptol. ePrint Arch. 2021: 954 (2021)

Brief overview of our work

Sable, alternate Saber[1]:

- Underlying ring $R_q = Z_q[X]/(X^n + 1)$, n=256
- Hardness depends on Module-LWR
- Better Performance and less memory needed than Saber
    - 2 ring moduli with few other parameters are smaller than Saber
    - Less pseudo random number generation
- It was possible due to fine-grain security analysis and few recent works

[1]Jose Maria Bermudo Mera, Angshuman Karmakar, Suparna Kundu, Ingrid Verbauwhede: Scabbard: a suite of efficient learning with rounding key-encapsulation mechanisms. IACR Cryptol. ePrint Arch. 2021: 954 (2021)

Brief overview of our work

Espada[1]:

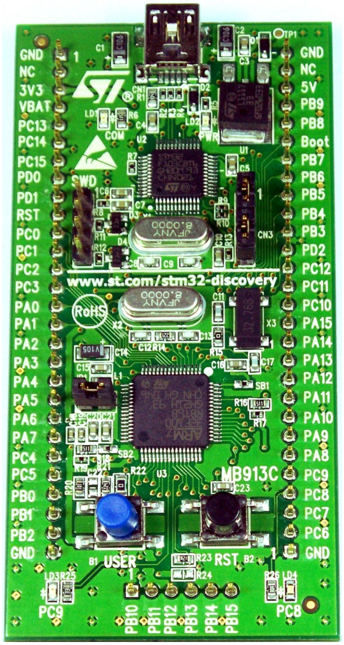
- Small base ring $R_q = Z_q[X]/(X^n + 1)$, n=64
  - Helps to reduce memory footprint
  - Suitable for low memory devices
- Hardness depends on Module-LWR
- One of the lowest stack memory used KEM
- Downside:
  - Need a lot pseudo random number generation
  - Which affect the performance
- Solution: Faster pseudo random number generator helps

[1]Jose Maria Bermudo Mera, Angshuman Karmakar, Suparna Kundu, Ingrid Verbauwhede: Scabbard: a suite of efficient learning with rounding key-encapsulation mechanisms. IACR Cryptol. ePrint Arch. 2021: 954 (2021)

Brief overview of our work

Cortex-M4:

- Huge applications of Internet of Things (IoT)
- ARM Cortex-M4 is a small resource constrained device
- It is used in many IoT devices
- Preferred choices to demonstrate the usefulness of the schemes for IoT applications
- [KRSS][1] invests effort to construct a framework for PQC KEM



[1] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen.PQM4: Post-quantum crypto library for the ARM Cortex-M4.

KU LEUVEN

Brief overview of our work

Results: Performance (X1000 clock cycles)

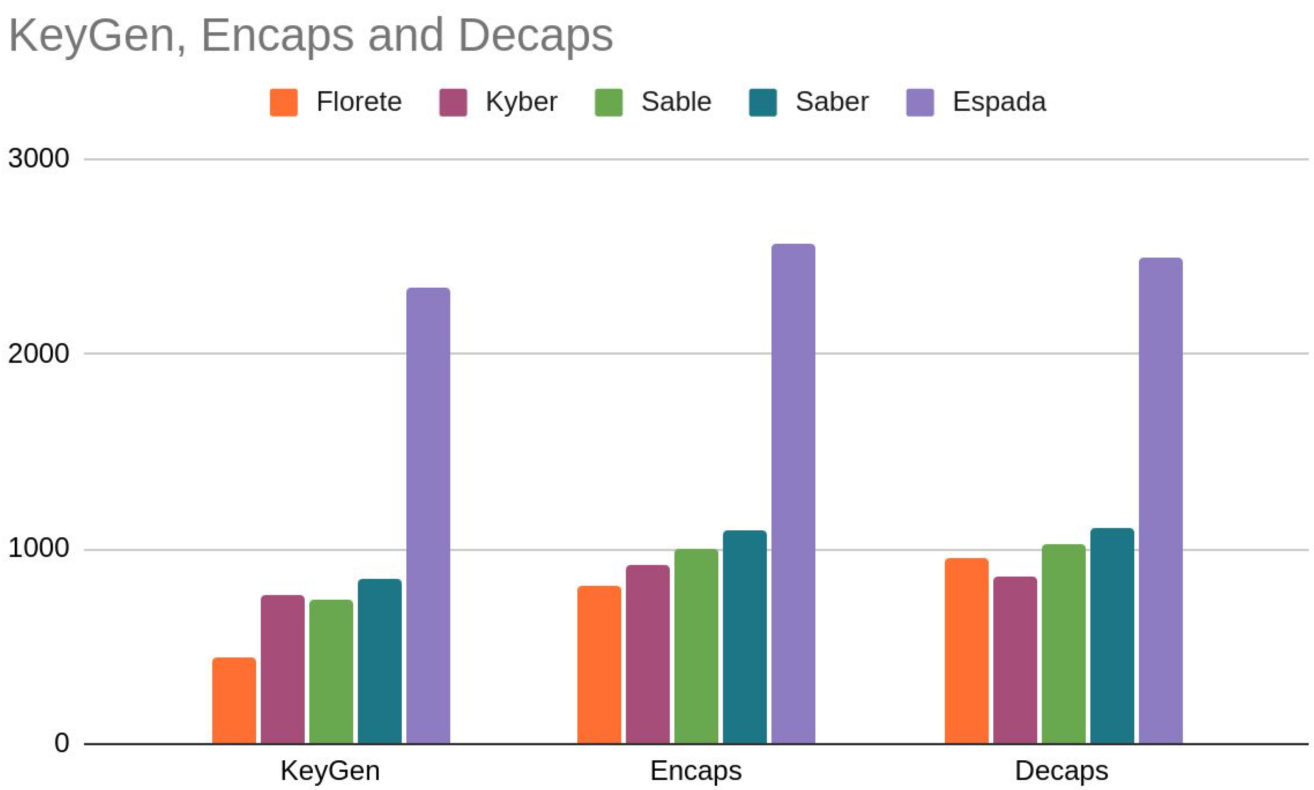
- Cortex-M4: STM32F4DISCOVERY board running at 24 MHz
- By using the framework provided by [KRSS][1]

Scheme	KeyGen	Encaps	Decaps
Florete	439 (48%)	814 (25%)	953 (14%)
Sable	745 (11%)	1004 (8%)	1028 (7%)
Espada	2343 (-63%)	2568 (-57%)	2497 (-55%)
Saber	846	1098	1112
Kyber	763	923	862

[1] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen.PQM4: Post-quantum crypto library for the ARM Cortex-M4.

Brief overview of our work

Results: Performance (X1000 clock cycles)



KU LEUVEN

Brief overview of our work

Results: Memory in bytes

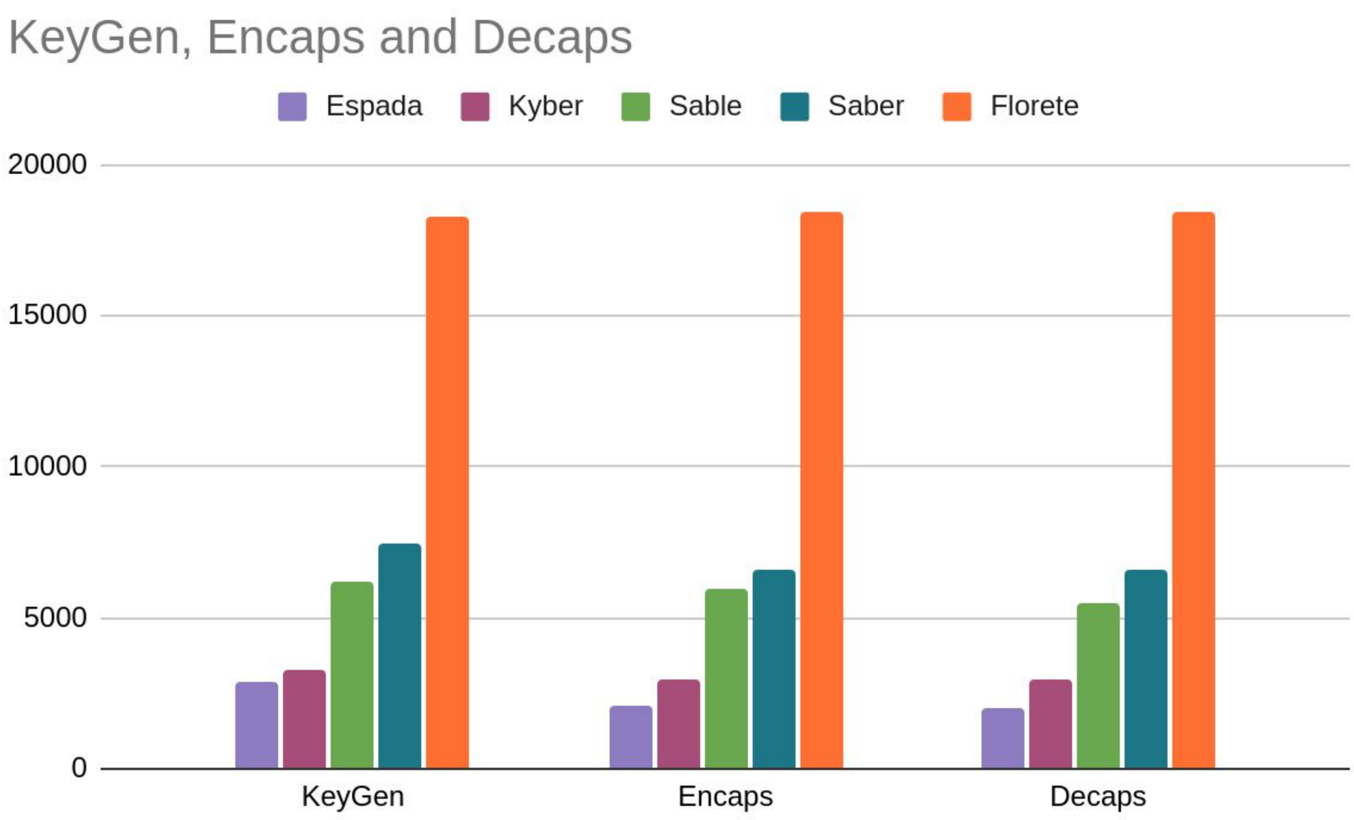
- Cortex-M4: STM32F4DISCOVERY board running at 24 MHz
- By using the framework provided by [KRSS][1]

Scheme	KeyGen	Encaps	Decaps
Florete	18252 (2x)	18420 (3x)	18420 (3x)
Sable	6184 (.8x)	5992 (.9x)	5496 (.8x)
Espada	2896 (.4x) (61%)	2120 (.3x) (67%)	2000 (.3x) (69%)
Saber	7488	6560	6568
Kyber	3276	2964	2988

[1] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen.PQM4: Post-quantum crypto library for the ARM Cortex-M4.

Brief overview of our work

Results: Memory in bytes



KU LEUVEN

Future works

- Most of lattice-based schemes are using variants of LWE
  - Well studied problems of mathematics
  - Thanks to NIST's competition, few more variants has published
    - e.g: Middle-product LWE
  - With suitable parameters and hard problem and newly published results
  - More efficient schemes may be constructed
- Polynomial multiplication is a costly operation
  - Little improvement can make a scheme efficient
- Side channel attack resistant implementation
  - Exploit weakness of implementation
  - Masking, hiding technique helps
  - Costs performance degradation
  - New technique needed

ANY QUESTIONS ?

Thank You!

Results: C and AVX implementation

Platform: Intel Core i7 with hyper-threading, Turbo-Boost and multi-core support disabled

Compiled with: gcc -o3

Scheme	C (X1000 clock cycles)			AVX (X1000 clock cycles)		
	KeyGen	Encaps	Decaps	KeyGen	Encaps	Decaps
Florete	86 (45%)	147 (26%)	193 (10%)	58 (45%)	87 (26%)	97 (13%)
Sable	152 (4%)	186 (7%)	207 (3%)	80 (25%)	95 (19%)	89 (20%)
Espada	334(-52%)	354 (-43%)	350 (-38%)	258 (-58%)	273 (-56%)	267 (-58%)
Saber	159	201	215	107	118	112
Kyber	252	324	365	537	594	557

Results: Cortex-M4 implementation

Cortex-M4: STM32F4DISCOVERY board running at 24 MHz

By using the framework provided by [KRSS][1]

Scheme	Performance (X1000 clock cycles)			Memory (X1000 clock cycles)		
	KeyGen	Encaps	Decaps	KeyGen	Encaps	Decaps
Florete	439 (48%)	814 (25%)	953 (14%)	18252 (2x)	18420 (3x)	18420 (3x)
Sable	745 (11%)	1004 (8%)	1028 (7%)	6184 (.8x)	5992 (.9x)	5496 (.8x)
Espada	2343 (-63%)	2568 (-57%)	2497 (-55%)	2896 (.4x) (61%)	2120 (.3x) (67%)	2000 (.3x) (69%)
Saber	846	1098	1112	7488	6560	6568
Kyber	763	923	862	3276	2964	2988

[1] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen.PQM4: Post-quantum crypto library for the ARM Cortex-M4.

KU LEUVEN

Accepted in TCHES 2021 issue 4

Jose Maria Bermudo Mera, Angshuman Karmakar, Suparna Kundu, Ingrid Verbauwhede
"Scabbard: a suite of efficient learning with rounding key-encapsulation mechanisms"

Module-Learning with errors (LWE)

$$\mathbf{A} \cdot \mathbf{s} + \mathbf{e} = \mathbf{b}$$

$$R_q = \mathbb{Z}_q[x]/f(x)$$

polynomial of degree n

$$\begin{pmatrix} a_{1,1}(x) & \cdots & a_{l,1}(x) \\ \vdots & \ddots & \vdots \\ a_{l,1}(x) & \cdots & a_{l,l}(x) \end{pmatrix} \cdot \begin{pmatrix} s_1(x) \\ \vdots \\ s_l(x) \end{pmatrix} + \begin{pmatrix} e_1(x) \\ \vdots \\ e_l(x) \end{pmatrix} = \begin{pmatrix} b_1(x) \\ \vdots \\ b_l(x) \end{pmatrix}$$

$a_{i,j}(x) \longleftarrow \mathcal{U}(R_q)$ $\quad$ $s_i(x), \; e_i(x) \longleftarrow \chi(R_q)$ with s.d. σ

Hard Problem (Decision): Given $(\mathbf{A}, \mathbf{b})$

$\mathbf{b}$: sampled uniformly / $\mathbf{b}$: LWE sample

LWR problem: $\mathbf{b} = \lfloor \mathbf{A} \cdot \mathbf{s} \rceil_p$ and $\mathbf{e}$ is rounding error (deterministic)