HAETAE and SMAUG-T: Korean PQC Standards

Hyeongmin Choe

CryptoLab, Inc.

April 25th, 2025

KMS Spring Meeting, KAIST

HEAAN CRYPTO LAB

CRYPTO LAB
주식회사 크립토랩

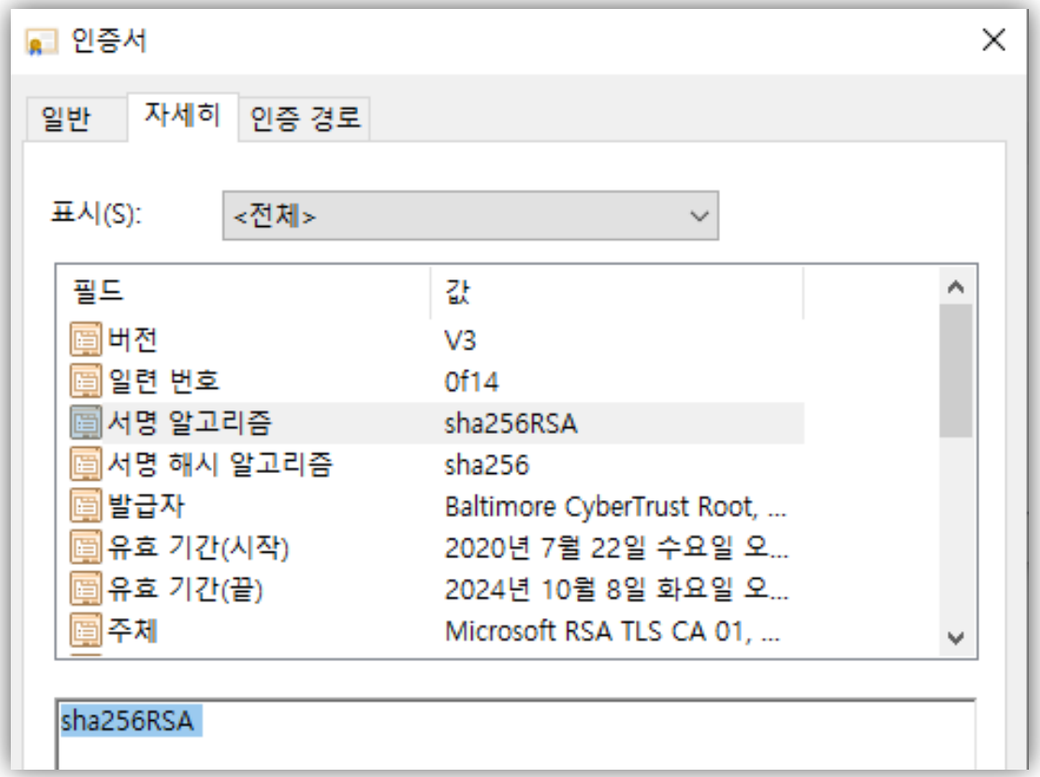
TABLE
OF
CONTENTS

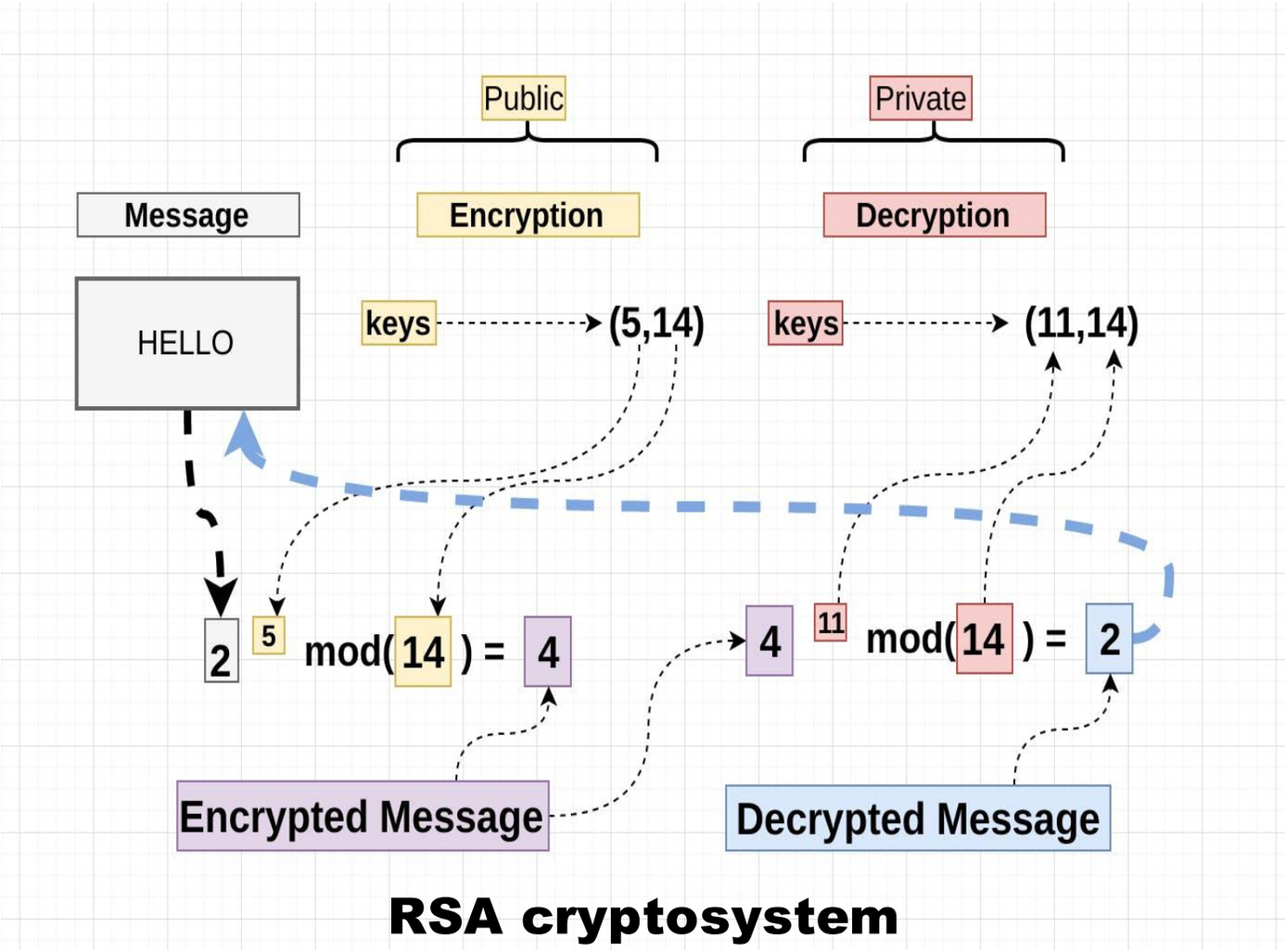
Why Post-Quantum Cryptography?

* Images from https://www.notebookcheck.net/Scientists-estimate-that-quantum-computers-may-become-powerful-enough-to-crack-the-Bitcoin-encryption-in-a-decade.597437.0.html, https://screenrant.com/quantum-computers-cryptocurrency-threat-are/

Why Post-Quantum Cryptography?

“Classical” Cryptography

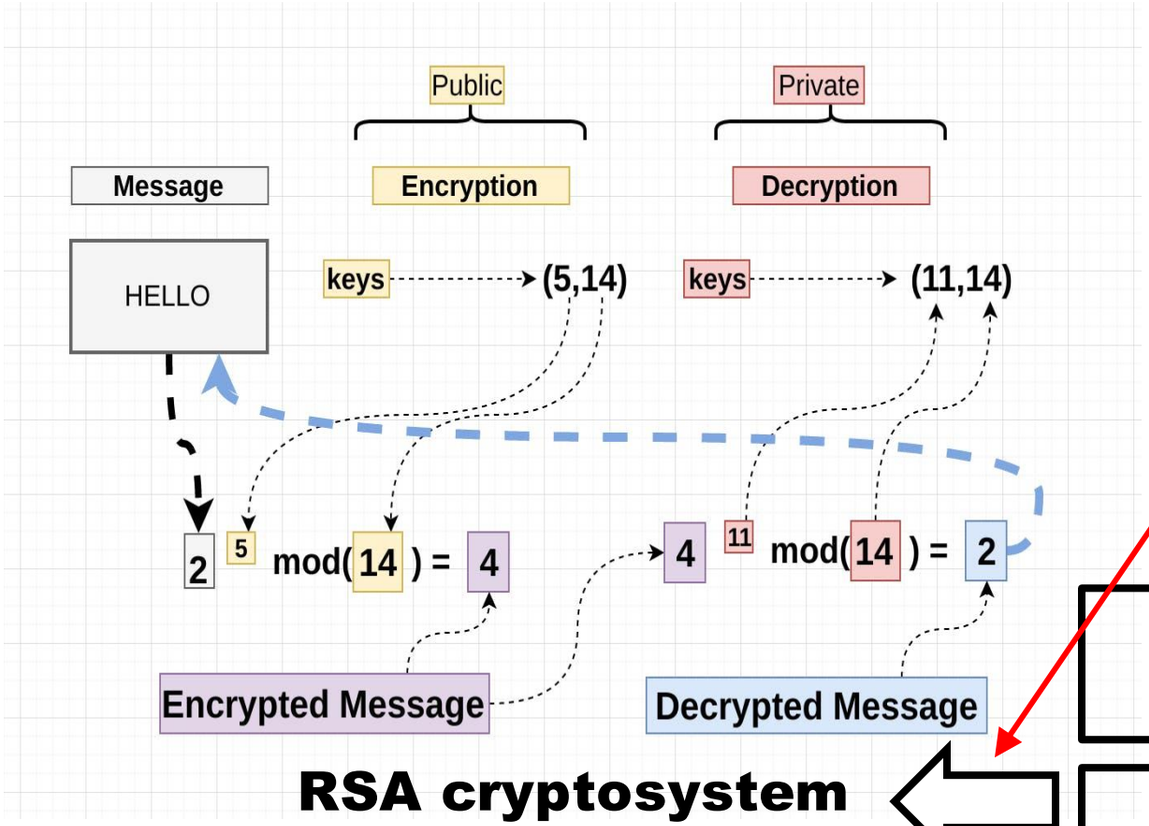




* Image from https://hackernoon.com/how-does-rsa-work-f44918df914b .

Why Post-Quantum Cryptography?

"Classical" Cryptography



Reduction

Integer Factorization problem

RSA problem: ***for given*** $a, e, n \in \mathbb{Z}$, ***find*** $b \in \mathbb{Z}$ ***satisfying*** $a \equiv b^e \bmod n$.

* Image from https://hackernoon.com/how-does-rsa-work-f44918df914b .

Why Post-Quantum Cryptography?

"Classical" Cryptography

Cryptosystem ← **Reduction** ← **Hard problems**

- **RSA Encryption/Signature**
- **Diffie-Hellman Key Exchange**
- **ECDSA/ECDH**

- **Integer Factorization**
- **Discrete Logarithm (DL)**
- **DL in Elliptic Curve over $\mathbb{F}_p$ (ECDL)**

NP!

Shor's algorithm in Quantum Computer

*Image from https://introtoquantum.org/essentials/timelines/.

Why Post-Quantum Cryptography?

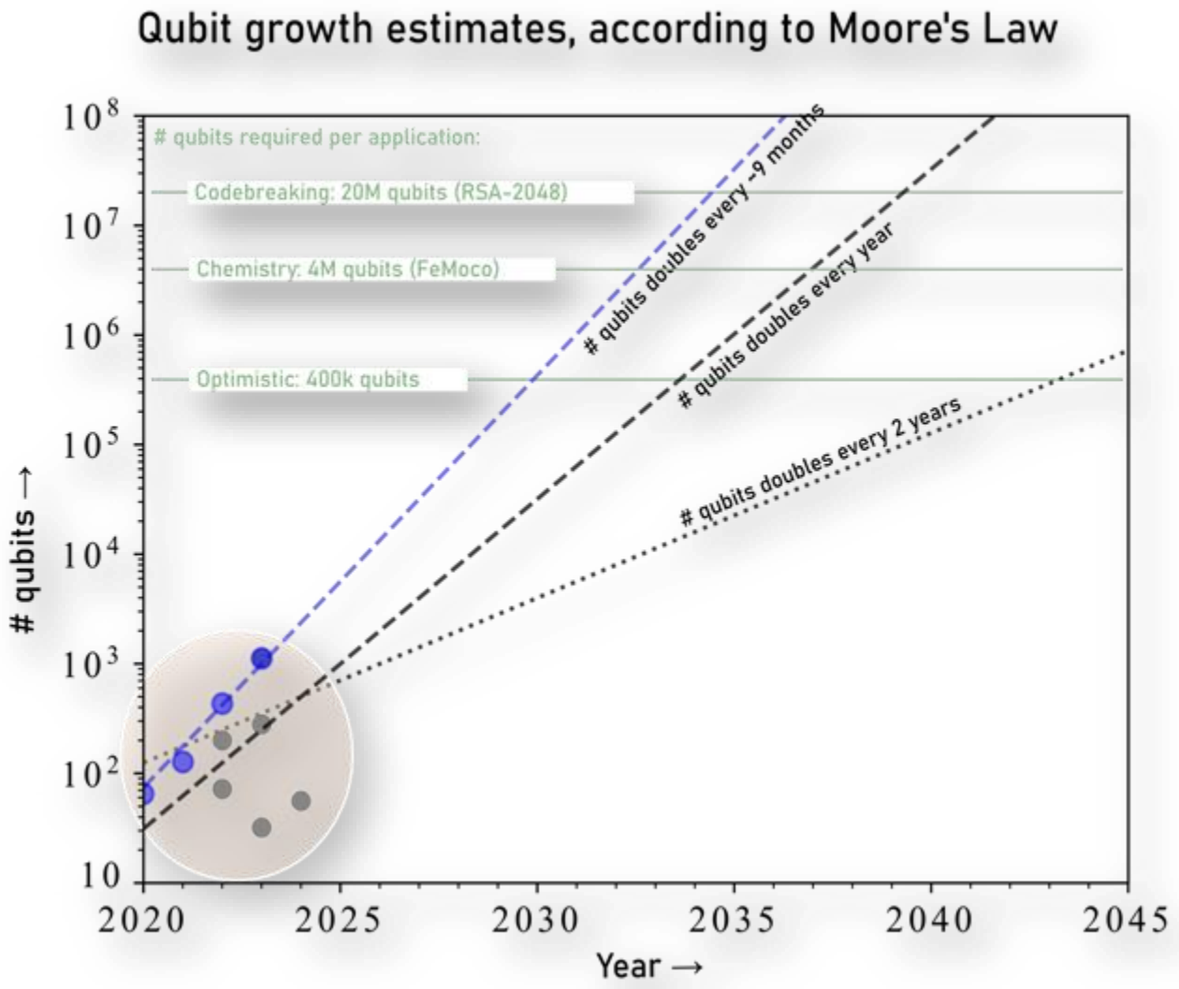
"Classical" Cryptography

Crypto

- RSA Encrypt

- Diffie-Hellma

- ECDSA/ECDI



ems

NP!

)L)

ver $\mathbb{F}_p$ (ECDL)

RSA2048: billions of years vs. several seconds in 4,000-logical-cubit quantum computer.

(expected, when quantum computers are commercialized… but when?)

*Image from https://introtoquantum.org/essentials/timelines/.

Why Post-Quantum Cryptography?

Post-Quantum Cryptography

Post-Quantum Cryptography

Reduction

Hard problems (even) against Quantum Algorithms

- **Lattice-based cryptography**

- **Code-based cryptography**

⋮

- **Shortest/Closest Vector Problem (SVP/CVP)**
  - ≈ **Learning With Errors (LWE)**
  - ≈ **Learning With Rounding (LWR)**
  - ≈ **Short Integer Solution (SIS)**

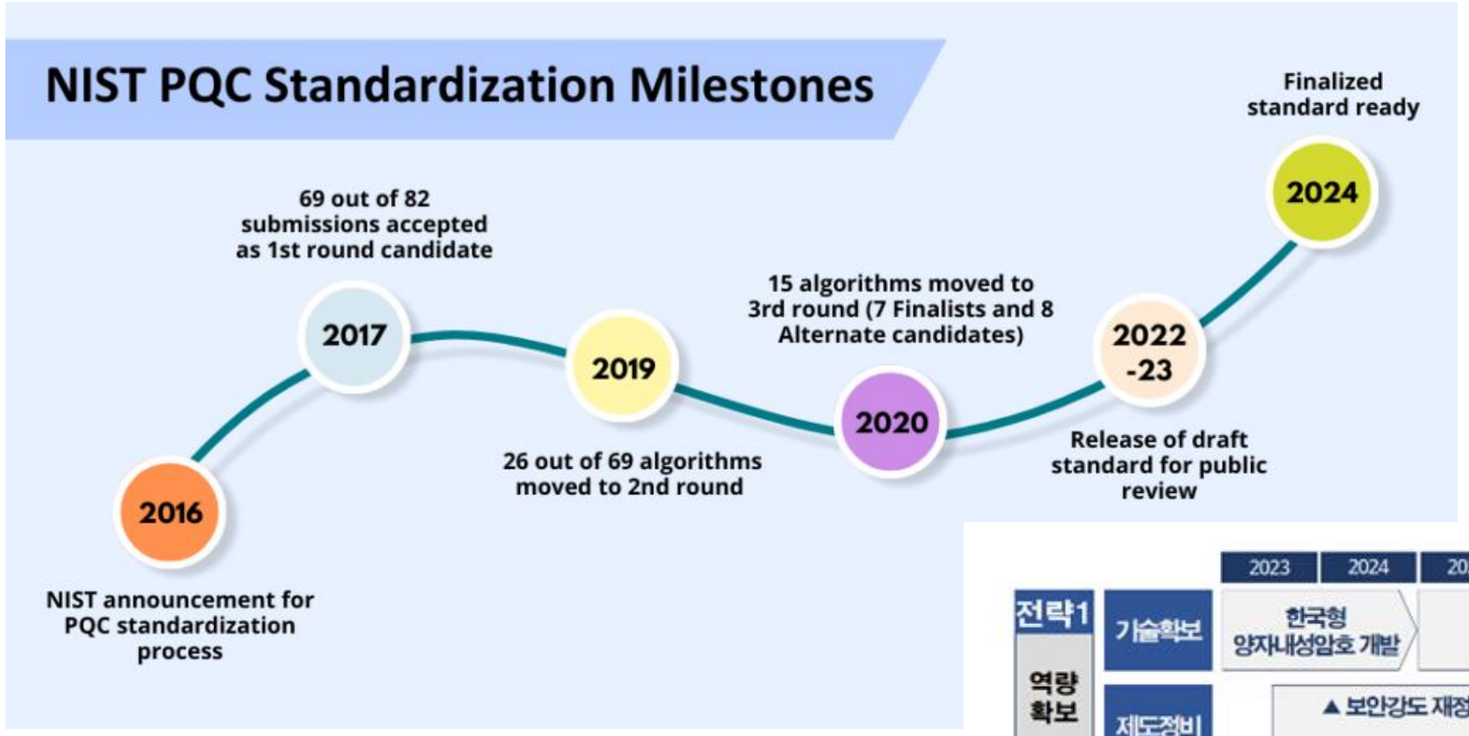
- **Syndrome Decoding Problem (SDP)**

⋮

NP-hard!*

Why Post-Quantum Cryptography?

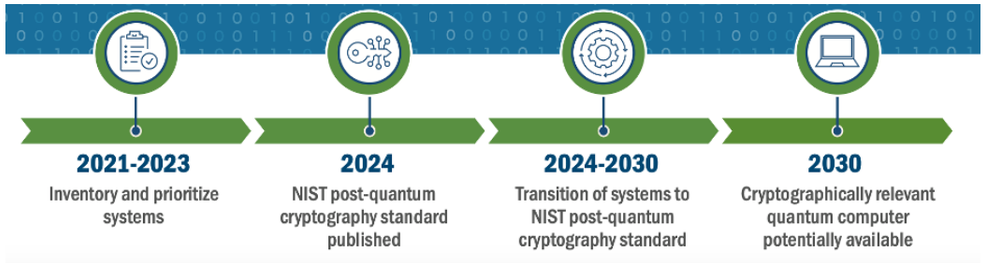
Global Movement



ETSI White Paper No. 8

Quantum Safe Cryptography and Security

An introduction, benefits, enablers and challenges



* Images from https://media.bitsol.tech/wp-content/uploads/2023/08/Blog-img-1-1024x5121.png and https://cdn.news2day.co.kr/data2/content/image/2023/07/13/.cache/512/20230713500265.png

KpqC Competition

- 2021년, 국립보안기술연구소에서 한국형 양자내성암호 확보를 목표로 공모
  - 공개 키 암호(PKE)와 키 캡슐화(KEM) 분야: 7개 알고리즘
  - 전자서명(Digital Signature) 분야: 9개 알고리즘

- 2025년, 최종 4개 알고리즘 선정

KpqC 2025 Selected	PKE/KEM	Signatures	Overall
Lattice-based	SMAUG-T NTRU+	HAETAE	3
Symmetric-based		AIMer	1

SMAUG-T

HEAAN CRYPTO LAB

Defense Counterintelligence Command

SMAUG-T

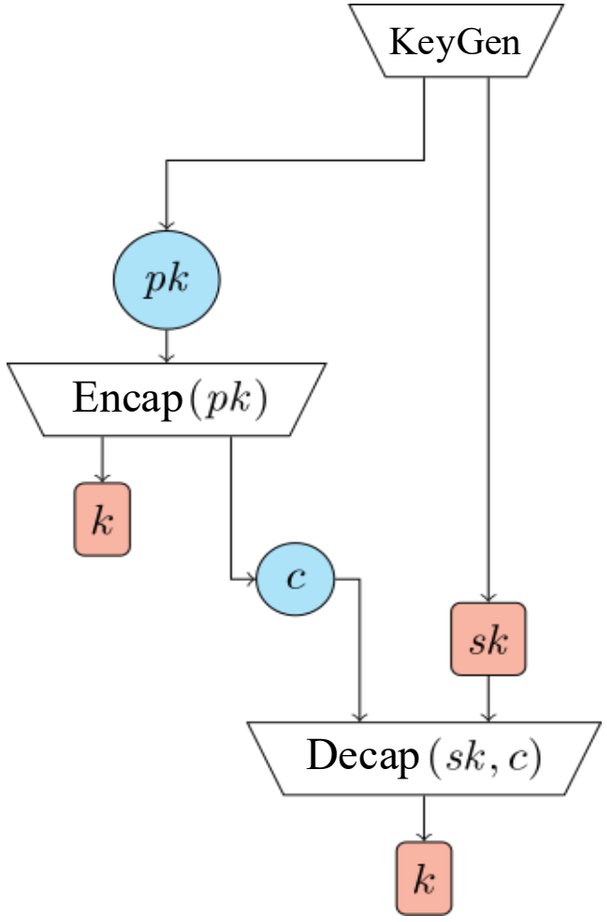
서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

HEAAN CRYPTO LAB

국군방첩사령부
Defense Counterintelligence Command

Joint work between **Seoul National University (서울대학교)**, **CryptoLab Inc. ((주)크립토랩)**,
and **Defense Counterintelligence Command (국군방첩사령부).**

- Key Encapsulation Mechanism (KEM):



0. $(sk, pk) \leftarrow$ KeyGen

pk

(knows sk)

Alice

(knows pk)

Bob

1. key k and ciphertext c
$(k, c) \leftarrow \text{Encap}(pk)$

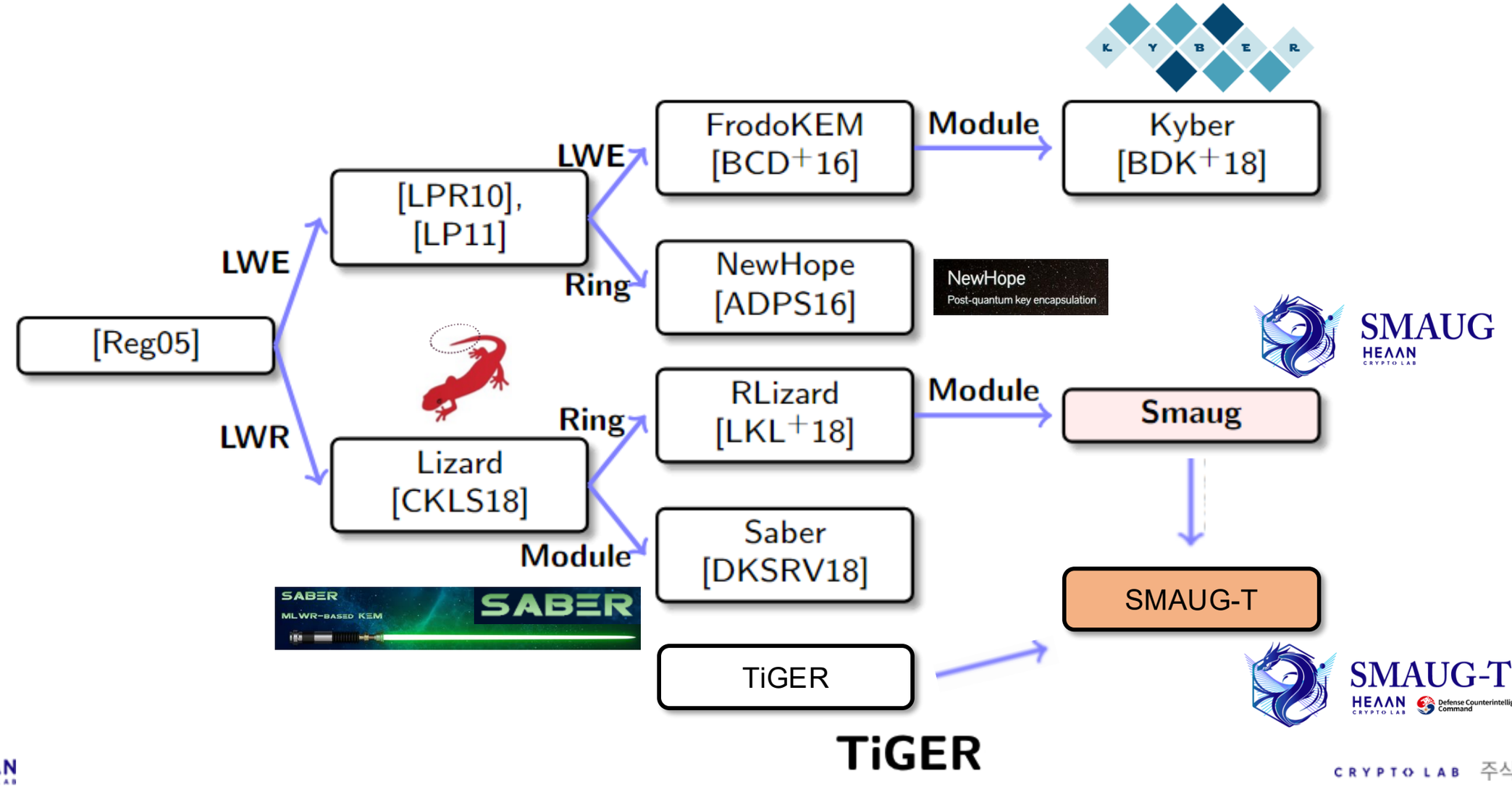
c

2. Shared key
$k \leftarrow \text{Decap}(sk, c)$

➔ Both have the same key k

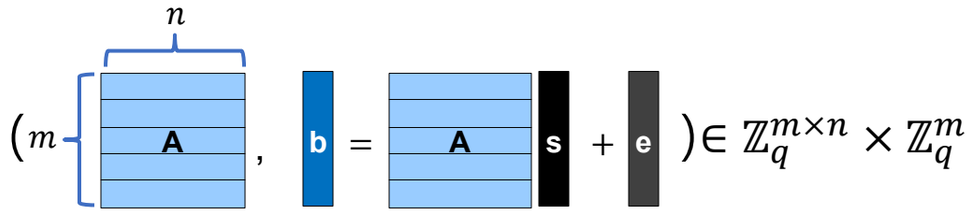
* Image from https://en.wikipedia.org/wiki/Key_encapsulation_mechanism

THE History


[Reg05]
LWE
LWR
[LPR10], [LP11]
Lizard [CKLS18]
LWE
Ring
Ring
Module
FrodoKEM [BCD+16]
NewHope [ADPS16]
RLizard [LKL+18]
Saber [DKSRV18]
TiGER
Module
Module
Kyber [BDK+18]
Smaug
SMAUG-T
NewHope
Post-quantum key encapsulation
SABER
MLWR-BASED KEM
SABER
KYBER
SMAUG
HEAAN
CRYPTO LAB
SMAUG-T
HEAAN
CRYPTO LAB
Defense Counterintelligence Command
TiGER

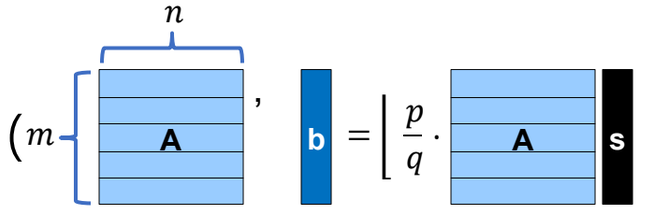
LWE, LWR and their Module Variants

- **Learning With Errors (LWE)**
  - Gaussian noise is added:



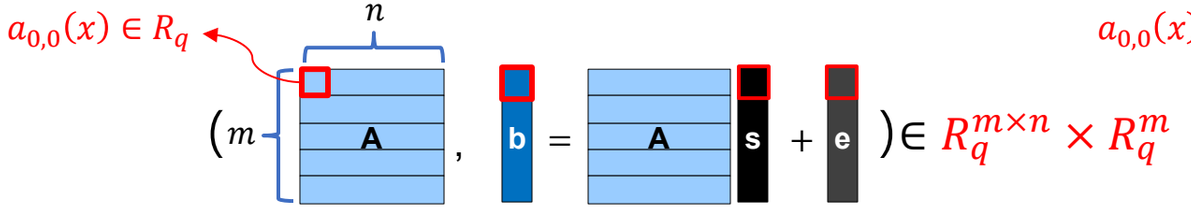
$$\in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$$

- **Learning With Rounding (LWR)**
  - Noise comes from rounding:



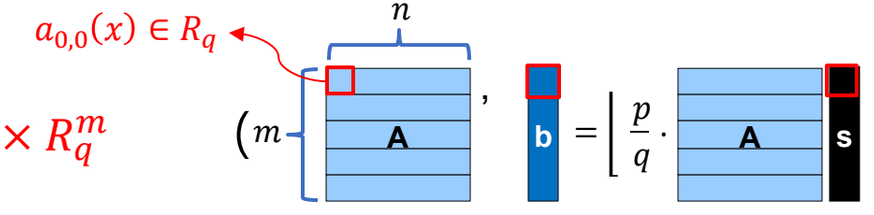
$$\in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_p^m$$

- **Module LWE (MLWE)**
  - Gaussian noise is added:



$$\in R_q^{m \times n} \times R_q^m$$

- **Module LWR (MLWR)**
  - Noise comes from rounding:



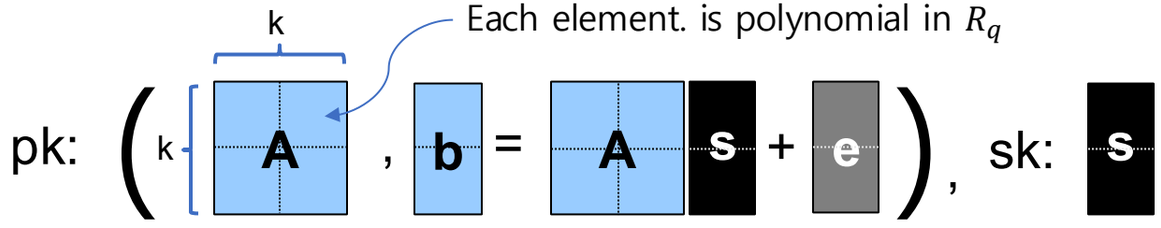
$$\in R_q^{m \times n} \times R_p^m$$

n: power of two integer
$R = \mathbb{Z}[x]/(x^n + 1)$

$$n = 256$$
$$R = \mathbb{Z}[x]/(x^n + 1)$$

- **SMAUG-T.PKE**
  - MLWE-based Public Key

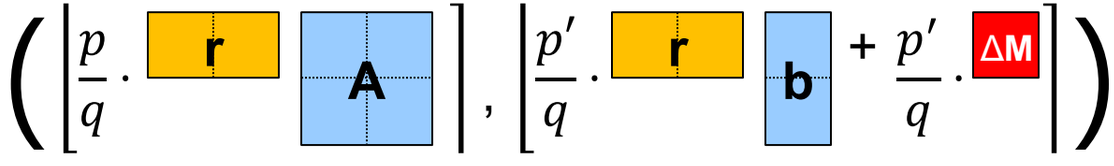
* secret (s): sparse ternary (HWT)
* noise (e): discrete Gaussian (dG)



$$\boldsymbol{A} \in R_q^{k \times k},\ \boldsymbol{b} \in R_q^k \text{ for } k = 2, 3, 4$$

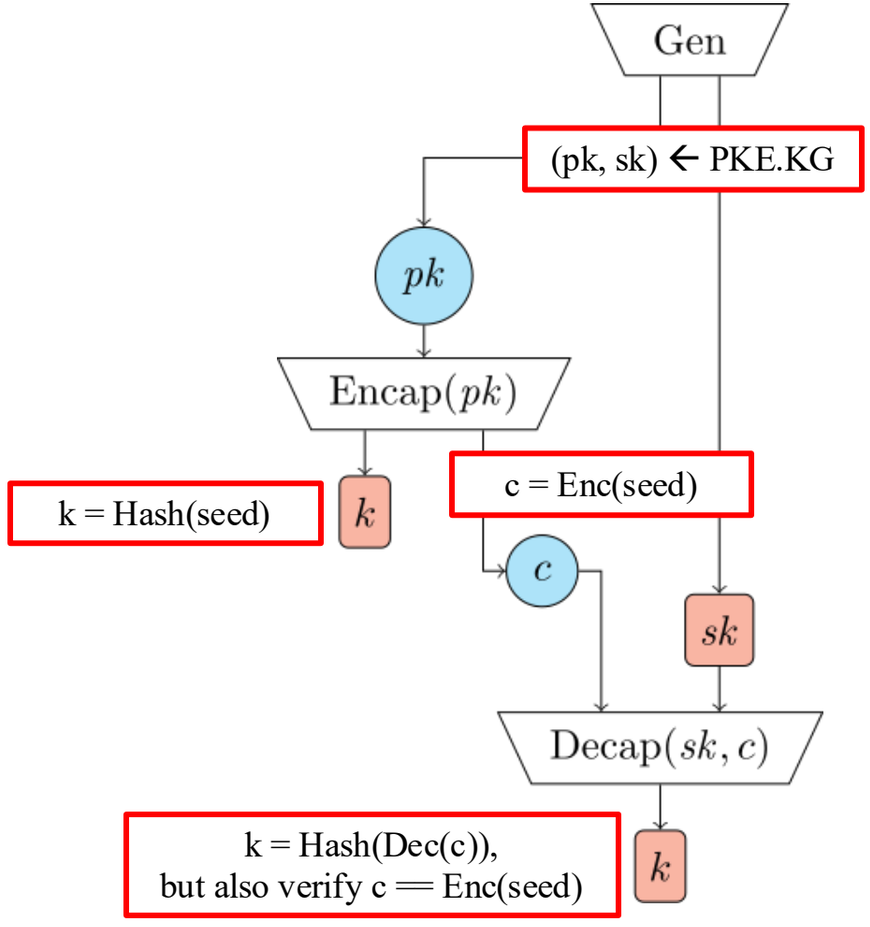
  - MLWR-based Encryption

* random (r): sparse CBD (spCBD)
* noise: rounding error



$$\boldsymbol{r} \in R_q^k$$

- **Fujisaki-Okamoto Transform (FO):**
  - **SMAUG-T.PKE → SMAUG-T.KEM**



SMAUG-T

HEAAN CRYPTO LAB

Defense Counterintelligence Command

HAETAE

HEAAN

CRYPTO LAB

HAETAE

서 울 대 학 교

SEOUL NATIONAL UNIVERSITY

HEAAN

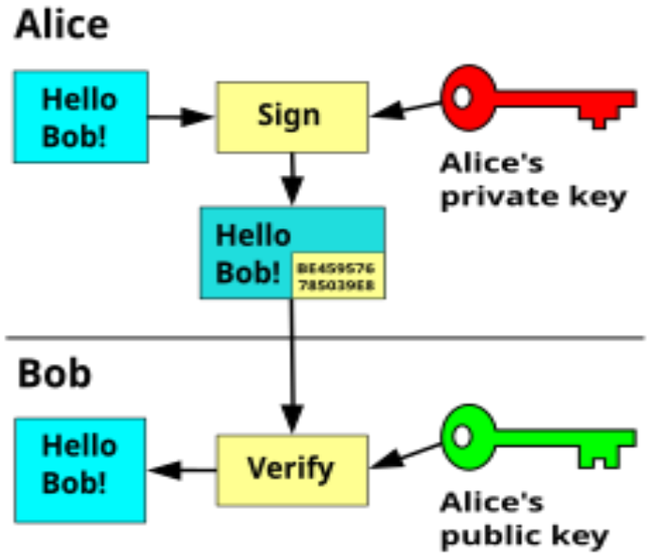
CRYPTO LAB

ENS DE LYON

RUB

Joint work between **Seoul National University (서울대학교)**, **CryptoLab, Inc. ((주)크립토랩)**,
École Normale Supérieure de Lyon (ENS de Lyon), **Ruhr-Universität Bochum (RUB)**,
and **Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI).**

- **Digital signatures**



$(\mathrm{sk}, \mathrm{vk}) \leftarrow$ KeyGen and broadcast vk

(knows sk)

(knows vk)

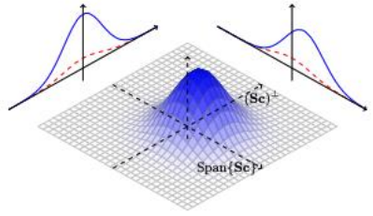
signature $\sigma \leftarrow \mathrm{Sign}(\mathrm{sk}, m)$

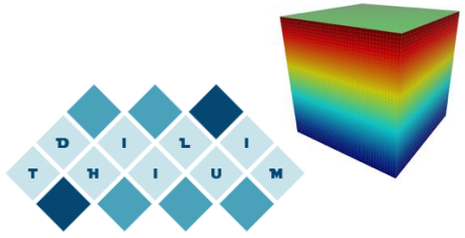
(m, σ)

Verify(vk, m, σ) = accept (or reject)

* Image from https://en.wikipedia.org/wiki/Digital_signature

THE History





[Lyu09]

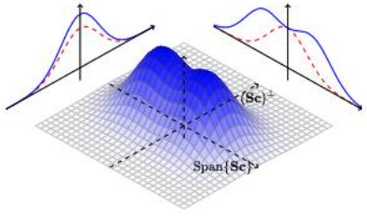
[Lyu12]

[GLP12]

[BG14]

Dilithium
[DKL+18]

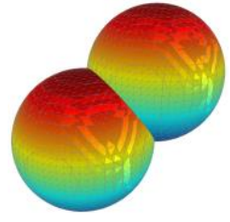
BLISS(-B)
[DDLL13,
Duc14]



[DFPS22]

HAETAE

HAETAE
HEAAN
CRYPTO LAB



Short Integer Solution (SIS) and its Module Variant

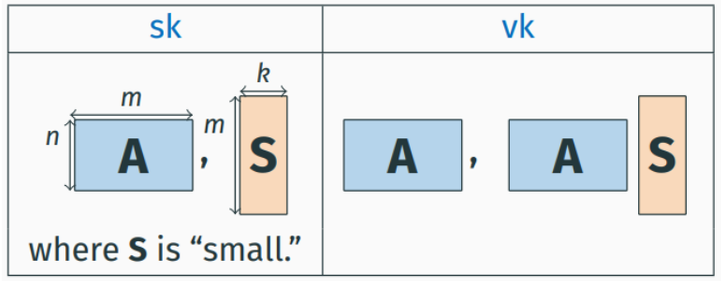
- **Short Integer Solution (SIS)**
  - Can we find a short solution $\boldsymbol{x} \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{n}} \setminus \{\boldsymbol{0}\}$ of $\boldsymbol{Ax} \equiv \boldsymbol{0}\ \boldsymbol{mod}\ \boldsymbol{q}$ for given $\boldsymbol{A} \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{m}\times\boldsymbol{n}}$?

- **Module Variant (MSIS)**
  - Can we find a short solution $\boldsymbol{x} \in R_{\boldsymbol{q}}^{\boldsymbol{n}} \setminus \{\boldsymbol{0}\}$ of $\boldsymbol{Ax} \equiv \boldsymbol{0}$ in R_q for given $\boldsymbol{A} \in R_{\boldsymbol{q}}^{\boldsymbol{m}\times\boldsymbol{n}}$?

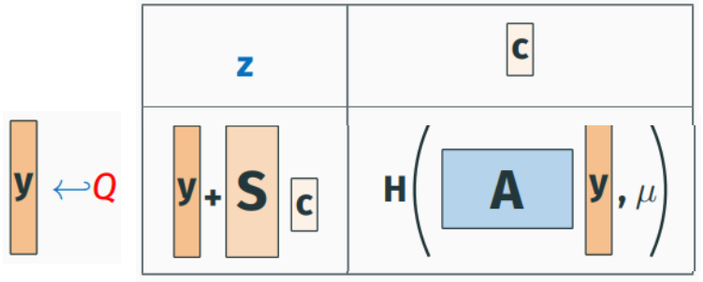
* Image from https://en.wikipedia.org/wiki/Digital_signature

"Fiat-Shamir with Abort" Paradigm

- KeyGen

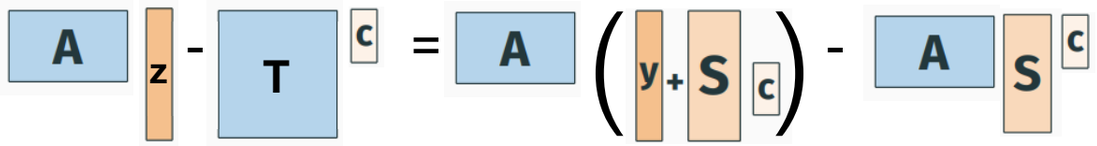


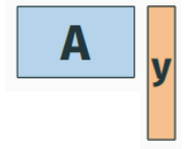
- Sign



But with rejection sampling, since

- Verify
  - Is z short?
  - Is c = H(Az-Tc)?

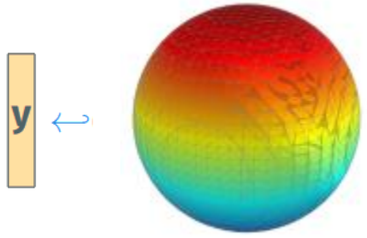




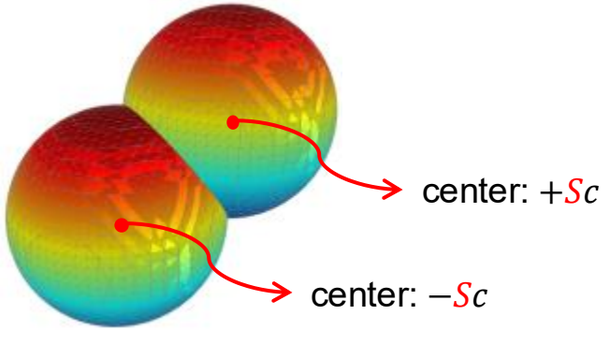
Figures borrowed from **Julien Devevey**'s slide: https://iacr.org/submit/files/slides/2022/asiacrypt/asiacrypt2022/286/slides.pdf.

HAETAE

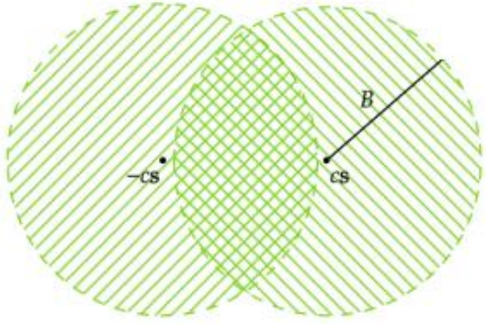
- HAETAE
  - Randomness y

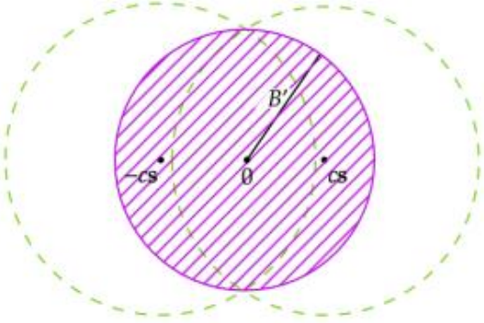


  - $z = y + (-1)^b \cdot Sc$



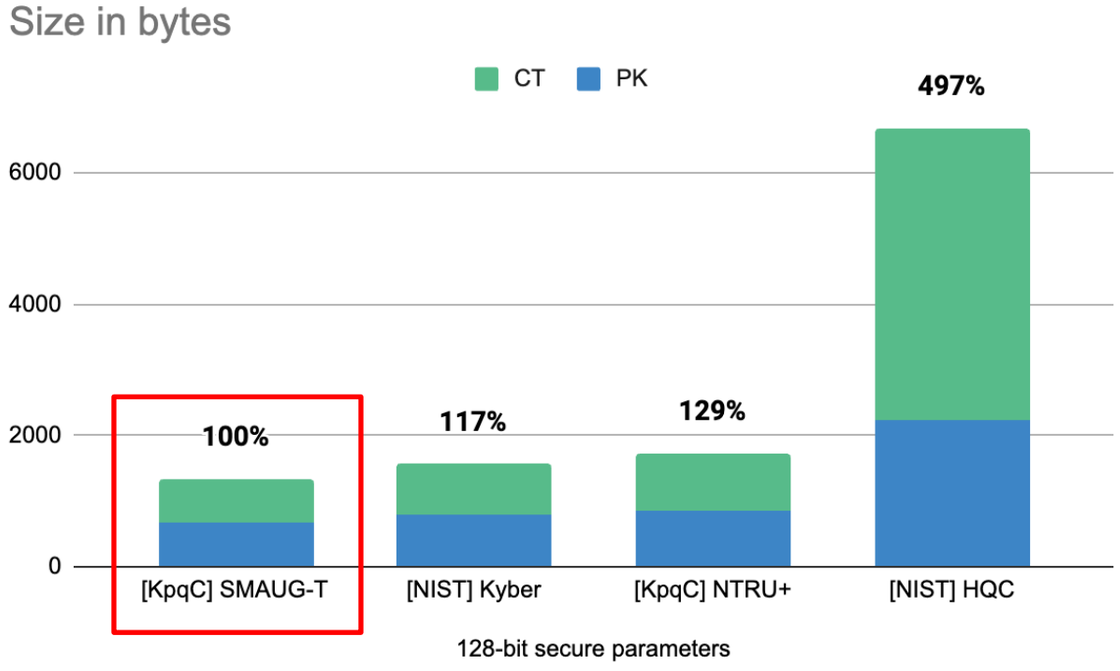
- Rejection sampling on z
  - From: hyperball centered at $\pm Sc$
  - To: smaller hyperball centered at 0



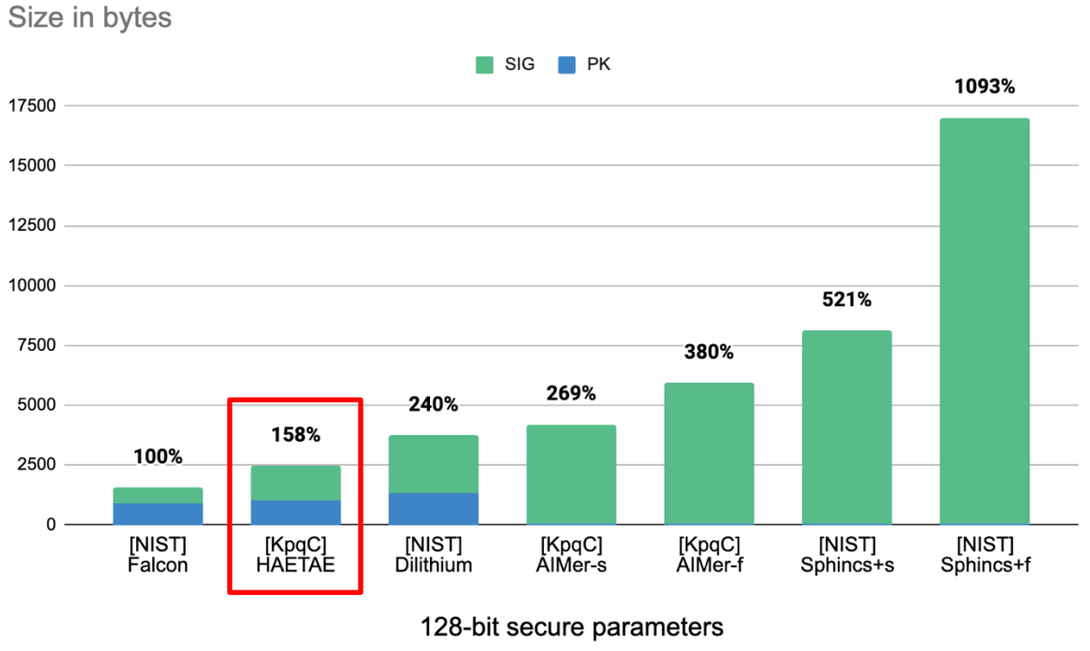


SMAUG-T and HAETAE

KEM



Digital Signatures



- Concretely-proven security
- Small sizes with good performance

NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography PQC

KOREAN POST-QUANTUM CRYPTOGRAPHY
KpqC
양자내성암호연구단

From Competition to Standard

* Images from https://pqshield.com/wp-content/uploads/2024/08/PQS_News_NIST-Announcement-1.png, https://standard.go.kr/streamdocs/view/sd;streamdocsId=72340810148664438

- **Migration to PQC**
  - When? ASAP, Harvest Now, Decrypt Later (HNDL) attacks!

x: time that products and data must remain secure
y: time it takes to migrate to post-quantum cryptography
z: time it takes until cryptographically-relevant quantum computers will be available

  - **See HEaaN PQC Alliance Program at https://heaanpqc.com !!!**

*Image from https://www.bosch.com/stories/quantum-computing-threat-how-to-prepare-for-a-smooth-transition-to-post-quantum-cryptography/

Future Plan

- **Korean Standards**
  - Ongoing efforts for governmental/industrial usages!

- **Hybrid** with..
  - Classical algorithms?
  - NIST-selected US standards?

- Some **Improvements**..

Thank You

HEAAN CRYPTO LAB

CRYPTO LAB
주식회사 크립토랩