CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

PQC Forum

後量子密碼論壇

後量子密碼遷移趨勢

TEAM CYBERSECURITY

陳君明

匯智安全科技 / 資通電腦

台大數學系 / EMBA 兼任

Agenda

- 公鑰密碼系統的風險 Risk of PKC
- 後量子密碼標準 PQC Standards
- 後量子密碼遷移 PQC Migrations
- 旁通道攻擊 Side-Channel Attacks

Two Categories of Cryptosystems

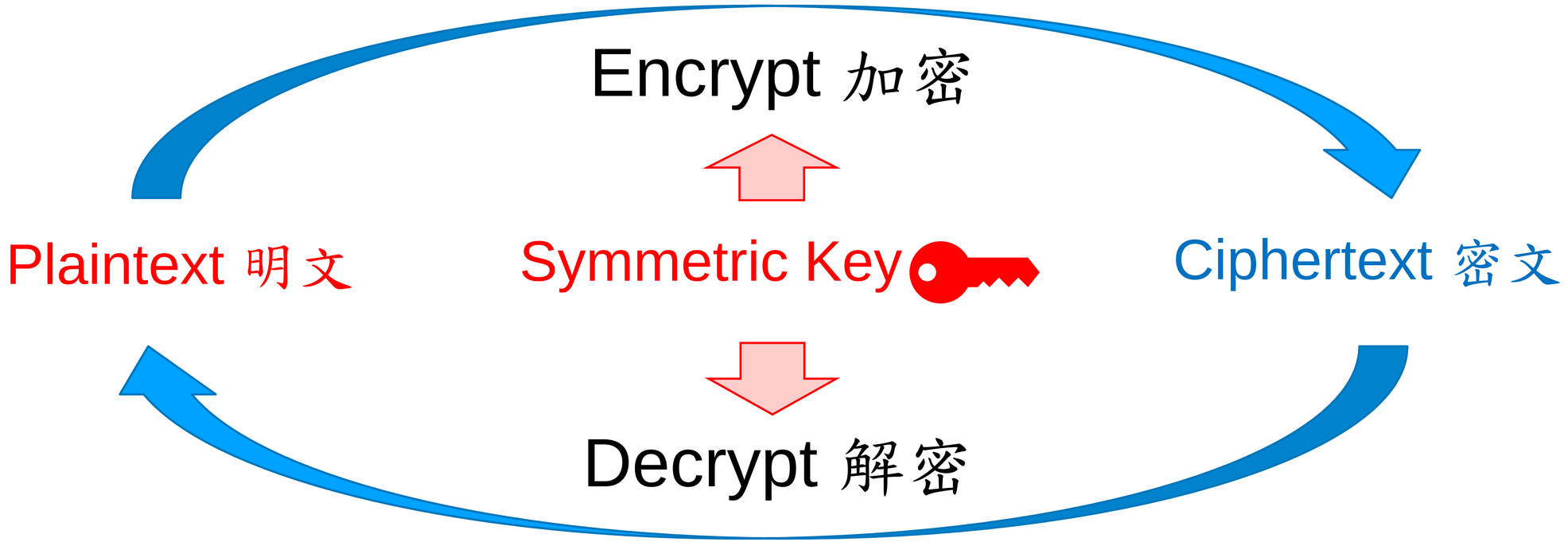
密碼系統兩大類型

- Symmetric
  - 2000+ years
  - DES, AES
  - Slight impact by Grover’s quantum algorithm
  - Security level of half bits in the future
- Asymmetric / PKC (Public-Key Cryptography)
  - Since 1976 (by Diffie & Hellman)
  - RSA, ECC (ECDH, ECDSA)
  - Serious threat by Shor’s quantum algorithm
  - PQC (Post-Quantum Cryptography) is resistant to quantum attacks

Caesar Cipher 凱撒加密

- Gāius Jūlius Caesar (100 BC – 44 BC)
  - A superb general and politician who changed the course of Roman history
- Caesar Cipher
  - Encode 編碼 : A $\leftrightarrow$ 0, B $\leftrightarrow$ 1, …, Y $\leftrightarrow$ 24, Z $\leftrightarrow$ 25
    - Plaintext 明文 : SPY (18 15 24)
    - Ciphertext 密文 : VSB (21 18 1)
  - Encryption 加密： $c = p + 3 \mod 26$
  - Decryption 解密： $p = c - 3 \mod 26$
    - Key 密鑰 : $k = 3$

Symmetric Cryptosystem 對稱密碼系統



AES (Advanced Encryption Standard) / DES (Data Encryption Standard)

NIST Proposes to Standardize a Wider Variant of AES

December 24, 2024

https://csrc.nist.gov/news/2024/nist-proposes-to-standardize-wider-variant-of-aes

The Advanced Encryption Standard (AES) specifies a subset of the Rijndael block cipher family with 128-bit blocks that was submitted to the NIST AES development effort. While this block size remains sufficient for many applications, the increasing demand for processing large volumes of data highlights the potential advantages of a larger block size. This need was pointed out in the public comments received for (Special Publication) SP 800-38A, acknowledged in NIST Internal Report 8459, and further reinforced during two NIST public workshops on block cipher modes of operation.

In August 2024, NIST indicated its interest in vetting another Rijndael variant for approval: Rijndael with 256-bit blocks (i.e., Rijndael-256) with a single key size of 256-bits. NIST plans to develop a draft standard for Rijndael-256 over the next year and requests public comments on this plan by **June 25, 2025**, especially for the following categories:

- **Security analysis**, including any new cryptanalytic results related to the 256-bit block size
- **Performance and efficiency**, particularly in environments with hardware support for AES

Comments may be submitted to ciphermodes@nist.gov with “Comments on Rijndael-256” in the subject line. Comments received in response to this request will be posted on this site after the due date. Submitters’ names and affiliations (when provided) will be included, while contact information will be removed.

NIST IR 8552

Requirements for Cryptographic Accordions

https://csrc.nist.gov/pubs/ir/8552/final

Date Published: April 2025

Author(s)

Yu Long Chen (NIST), Michael Davidson (NIST), Morris Dworkin (NIST), John Kelsey (NIST), Yu Sasaki (NIST), Meltem Sönmez Turan (NIST), Donghoon Chang (Strativia), Nicky Mouha (FWI), Alyssa Thompson (NSA)

Abstract

This report introduces the *cryptographic accordion* as a tweakable, variable-input-length strong pseudorandom permutation (VIL-SPRP) that is constructed from an underlying block cipher. An accordion facilitates the cryptographic processing of messages of various sizes while offering enhanced security compared to the approved block cipher modes of operation that are specified in the NIST SP 800-38 series. This report introduces associated terminology, outlines design requirements for accordions, and describes three categories of applications for them.

Keywords

accordion; authenticated encryption; disk encryption; encode-then-encipher; key wrapping; length-preserving encryption

Lightweight Cryptography

https://csrc.nist.gov/projects/lightweight-cryptography

Overview

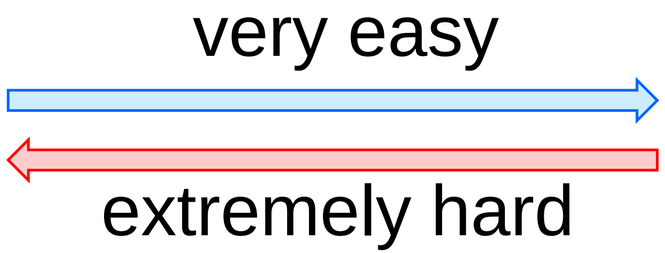
NIST began investigating cryptography for constrained environments in 2013. After two workshops and discussions with stakeholders in industry, government, and academia, NIST initiated a process to solicit, evaluate, and standardize schemes providing authenticated encryption with associated data (AEAD) and optional hashing functionalities for constrained environments where the performance of current NIST cryptographic standards is not acceptable. In 2018, NIST published a call for algorithms to describe the requirements, selection process and the evaluation criteria.

- **Round 1.** In March 2019, NIST received 57 submissions to be considered for standardization. The first round of the NIST lightweight cryptography standardization process began with the announcement of 56 Round 1 in April 2019 and ended in August 2019. NISTIR 8268 explains the evaluation of the first-round candidates and names 32 candidate algorithms advancing to the second round of the evaluation process.
- **Round 2.** The second round of the NIST lightweight cryptography standardization process began when NIST announced the 32 Round 2 in August 2019 and concluded when the finalists were announced in March 2021. NISTIR 8369 explains the evaluation of the second-round candidates and names 10 finalists.
- **Final Round.** The final round of the process began with the announcement of the 10 finalists and ended when NIST announced the selection of the Ascon family in February 2023. NISTIR 8454 describes the evaluation of the finalists and explains the selection of the Ascon family.

The timeline of the standardization process is provided here.

私鑰 / 公鑰

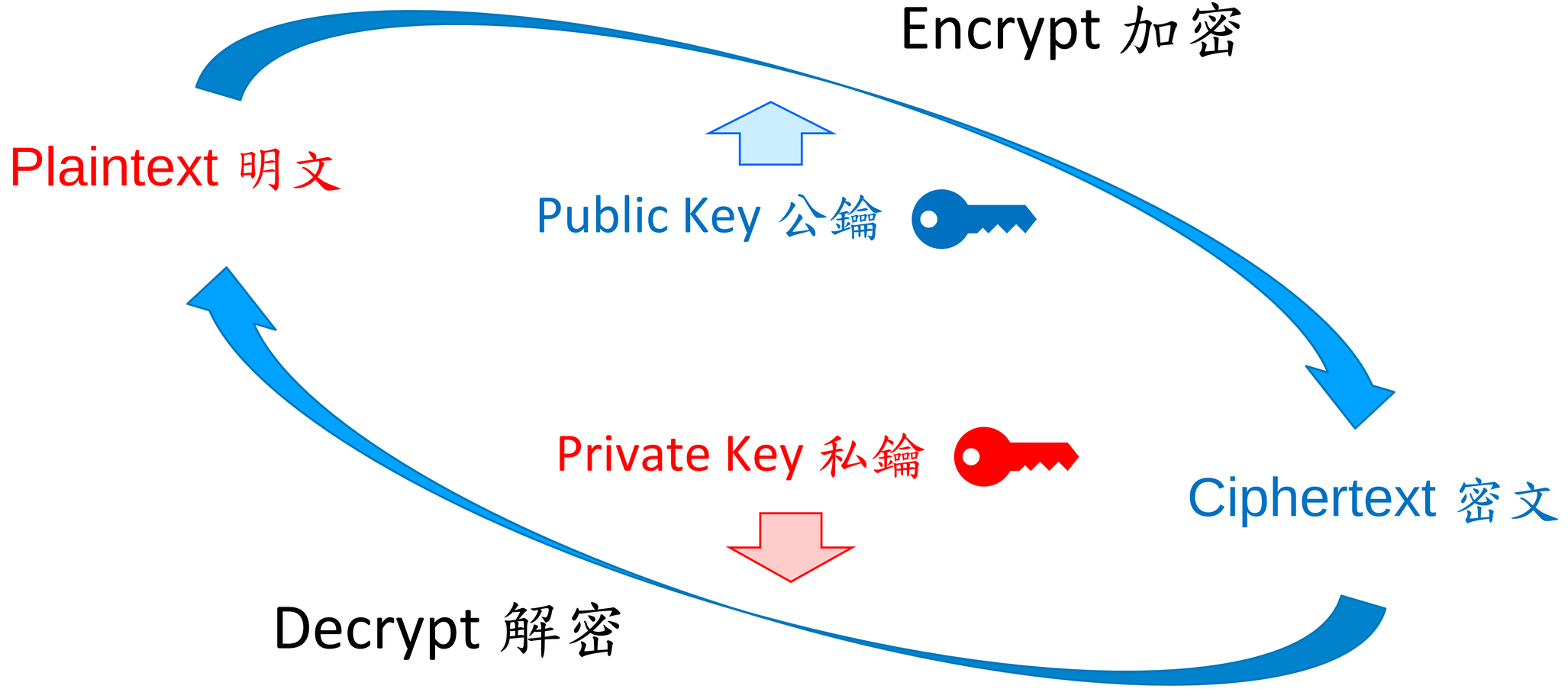
Private Key 私鑰



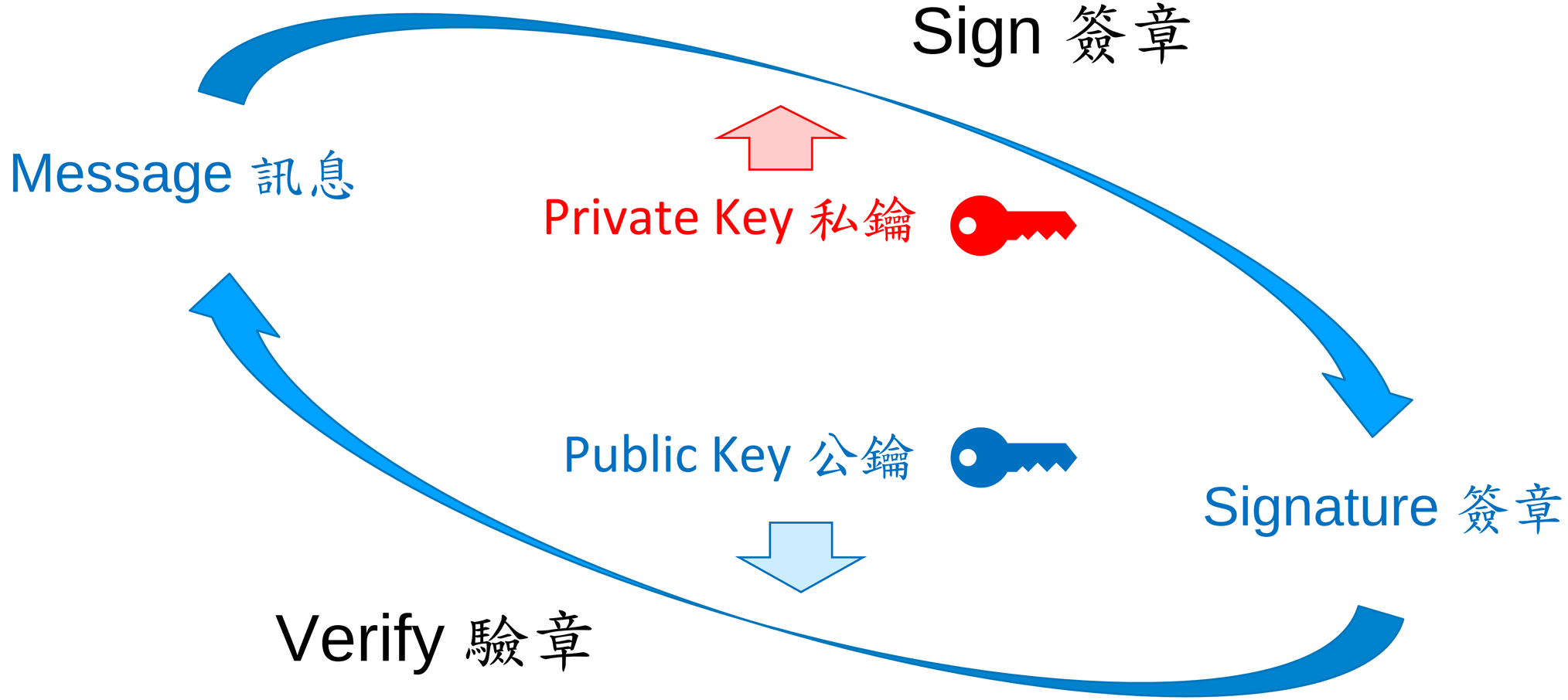
Public Key 公鑰

- The security of all current public-key cryptosystems is based on extremely hard computational problems
  - Integer Factoring：RSA
  - Discrete Logarithm：DHKE (Diffie-Hellman Key Exchange), DSA (Digital Signature Algorithm), ECC (Elliptic Curve Cryptosystems) [ECDH, ECDSA]

PKE (Public-Key Encryption) 公鑰加密



Digital Signature 數位簽章



Shor’s Algorithm

- The algorithm developed by Peter Shor at AT&T’s Bell Labs in 1994, when implemented on a mature, universal, large-scale quantum computer in the future, has the potential to break **all** currently used standard public-key cryptosystems

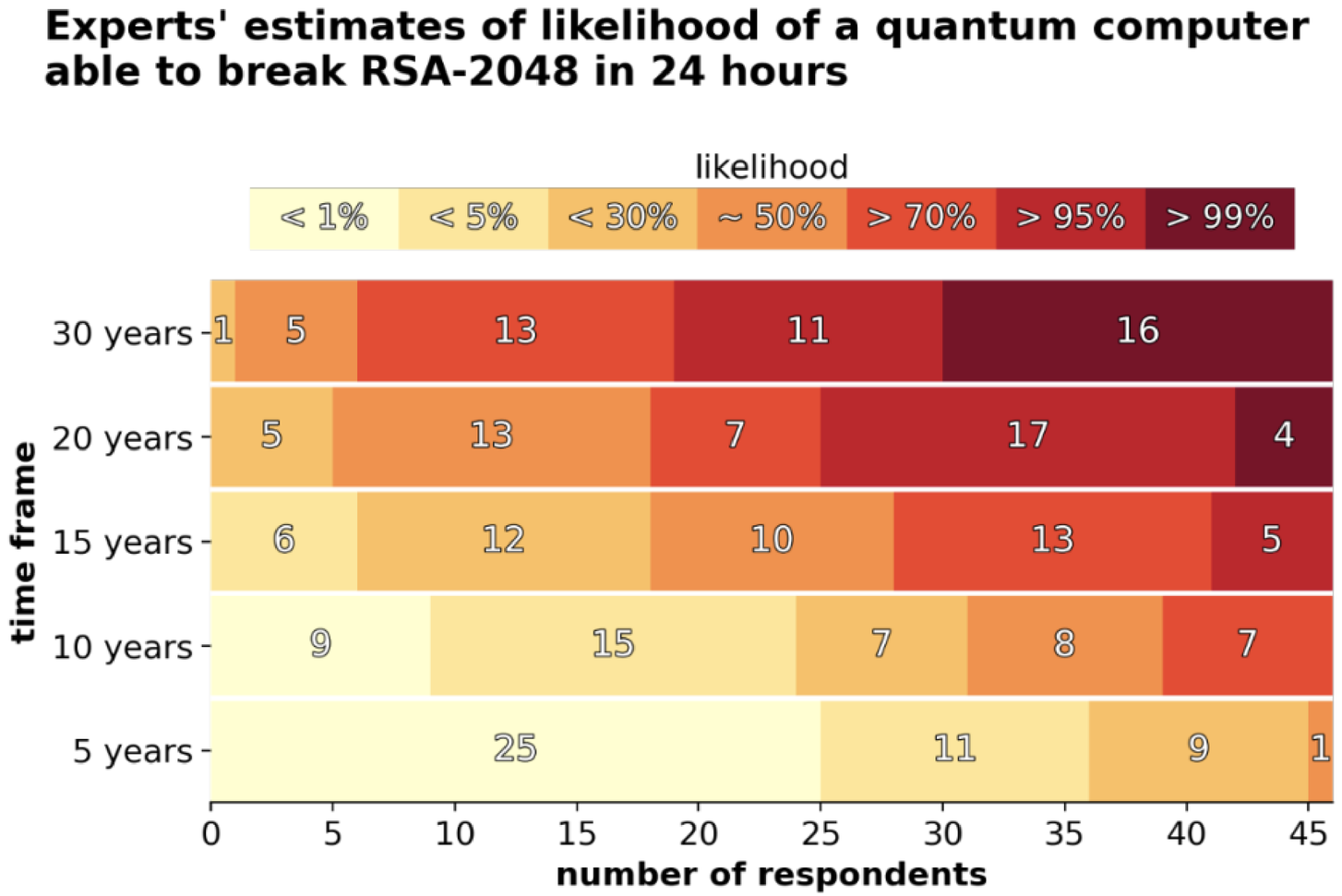
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

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.

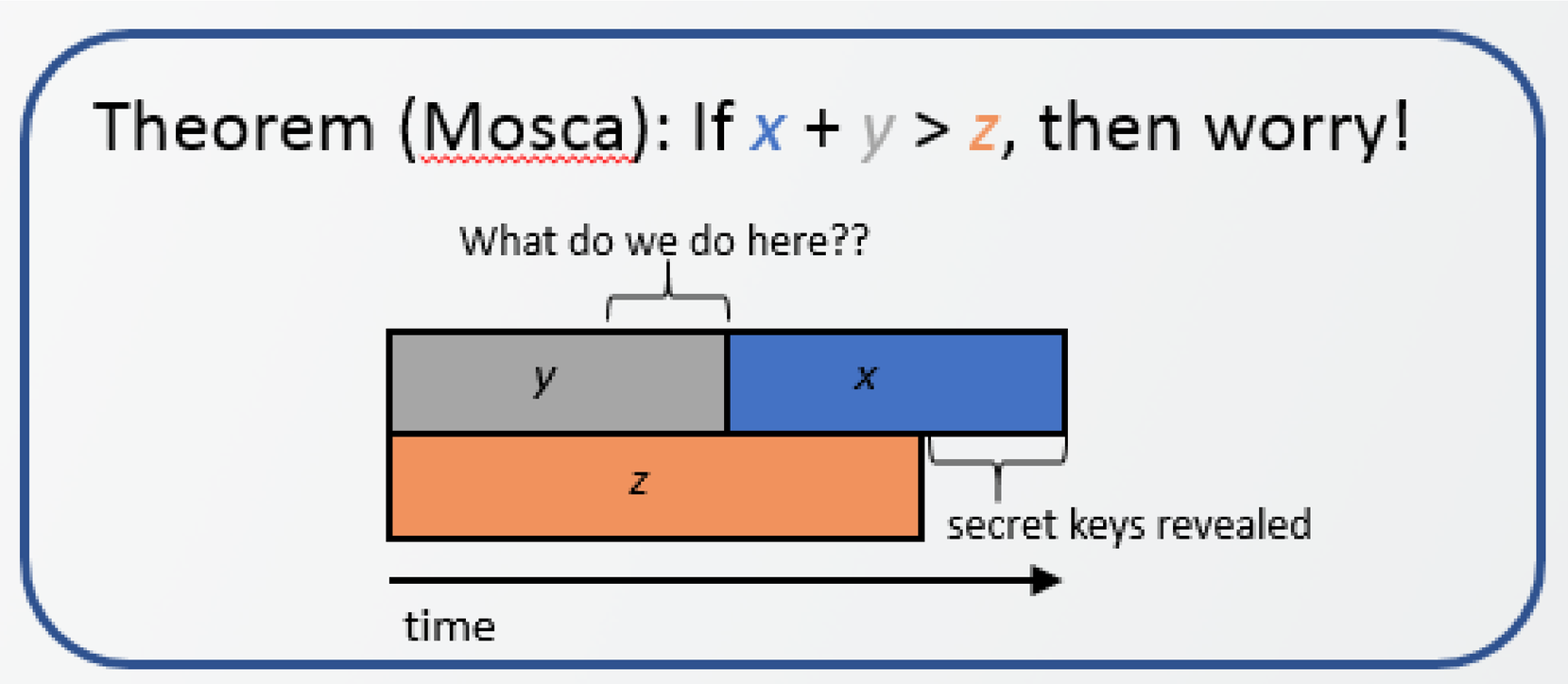
When is RSA-2048 Broken?



ECC is broken a couple of years earlier

2021 Quantum Threat Timeline Report: Global Risk Institute
https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2021-executive-summary-2.pdf/

因應時程



- x – time of maintaining data security
- y – time for PQC standardization and adoption
- z – time for quantum computer to be developed

https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

為何必須立即發展 PQC

- 基於保密期限或產品生命週期 (前頁)
- 全面更換特定類型密碼系統曠日廢時
  - 根據過去經驗可能需長達十年
- 國家級情報單位已開始儲存密文，等待未來量子電腦成熟即可大規模破解
  - “Harvest now, decrypt later” https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later
  - 已經被敵人儲存的密文，毫無挽救機會

Agenda

- 公鑰密碼系統的風險 Risk of PKC
- **後量子密碼標準 PQC Standards**
- 後量子密碼遷移 PQC Migrations
- 旁通道攻擊 Side-Channel Attacks

PQC Standardization

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS$^+$

Latttice-based

Hash-based

Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	Digital Signatures
BIKE	
Classic McEliece	
HQC	
SIKE	(broken)

Code-based

Supersingular Isogeny

NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

March 11, 2025

- NIST has chosen a new algorithm for post-quantum encryption called HQC, which will serve as a backup for ML-KEM, the main algorithm for general encryption.
- HQC is based on different math than ML-KEM, which could be important if a weakness were discovered in ML-KEM.
- NIST plans to issue a draft standard incorporating the HQC algorithm in about a year, with a finalized standard expected in 2027.

https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

Post-Quantum Cryptography: Additional Digital Signature Schemes

Workshops and Timeline

No workshops scheduled at this time.

Timeline

**This is a tentative timeline, provided for information, and subject to change.*

Date	
Sep 6, 2022	Call for Additional Digital Signature Schemes
June 1, 2023	Deadline for submissions
July 17, 2023	Round 1 Additional Signatures announced (40 submissions accepted as "complete and proper")
Oct 24, 2024	Round 2 Additional Signatures announced (14 algorithms)
Jan 17, 2025	Deadline for updated submission packages for Second Round Candidates *See Guidelines for Submitting Tweaks*

PROJECT LINKS

Overview

News & Updates

Publications

ADDITIONAL PAGES

Standardization of Additional Digital Signature Schemes

Call for Proposals

Example Files

Workshops and Timeline

Round 1 Additional Signatures

Round 2 Additional Signatures

Email List (PQC Forum)

PQC Standardization: Main Project

https://csrc.nist.gov/Projects/pqc-dig-sig/standardization/workshops-and-timeline

The following NIST-authored publications are directly related to this project.

FIPS = Federal Information Processing Standards

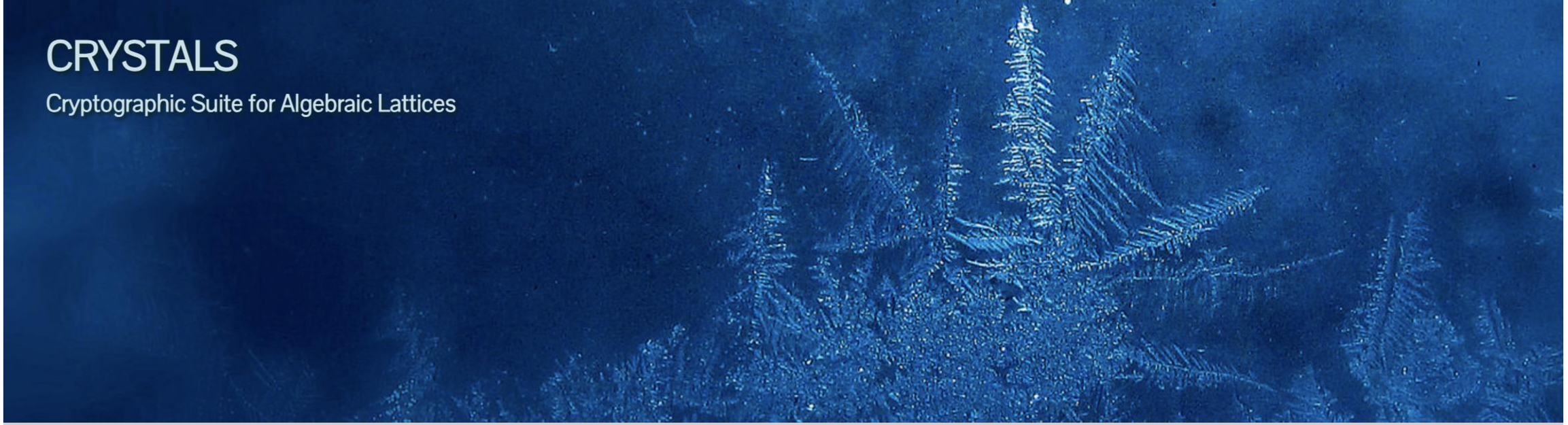
Series & Number	Title	Status	Released
SP 800-227	Recommendations for Key-Encapsulation Mechanisms	Draft	01/07/2025
IR 8547	Transition to Post-Quantum Cryptography Standards	Draft	11/12/2024
IR 8528	Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process	Final	10/24/2024
FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism Standard ML-KEM	Final	08/13/2024
FIPS 204	Module-Lattice-Based Digital Signature Standard ML-DSA	Final	08/13/2024
FIPS 205	Stateless Hash-Based Digital Signature Standard SLH-DSA	Final	08/13/2024
IR 8413	Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process	Final	09/29/2022
IR 8309	Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process	Final	07/22/2020
IR 8240	Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process	Final	01/31/2019
IR 8105	Report on Post-Quantum Cryptography	Final	04/28/2016

CRYSTALS-Kyber

CRYSTALS-Dilithium

SPHINCS+

https://csrc.nist.gov/Projects/post-quantum-cryptography/publications



CRYSTALS | Kyber | Dilithium

The "Cryptographic Suite for Algebraic Lattices" (CRYSTALS) encompasses two cryptographic primitives: Kyber, an IND-CCA2-secure key-encapsulation mechanism (KEM); and Dilithium, a strongly EUF-CMA-secure digital signature algorithm. Both algorithms are based on hard problems over module lattices, are designed to withstand attacks by large quantum computers, and have been submitted to the NIST post-quantum cryptography project.

Module Lattices

https://pq-crystals.org/

CRYSTALS Team

- Roberto Avanzi, ARM Limited (DE)
- Shi Bai, Florida Atlantic University (US)
- Joppe Bos, NXP Semiconductors (BE)
- Jintai Ding, Tsinghua University (CN)
- Léo Ducas, CWI Amsterdam (NL) & Leiden University (NL)
- Eike Kiltz, Ruhr University Bochum (DE)
- Tancrède Lepoint, Amazon Web Services (US)
- Vadim Lyubashevsky, IBM Research Zurich (CH)
- John M. Schanck, Mozilla (US)
- Peter Schwabe, MPI-SP (DE) & Radboud University (NL)
- Gregor Seiler, IBM Research Zurich (CH)
- Damien Stehle, CryptoLab Inc (FR)

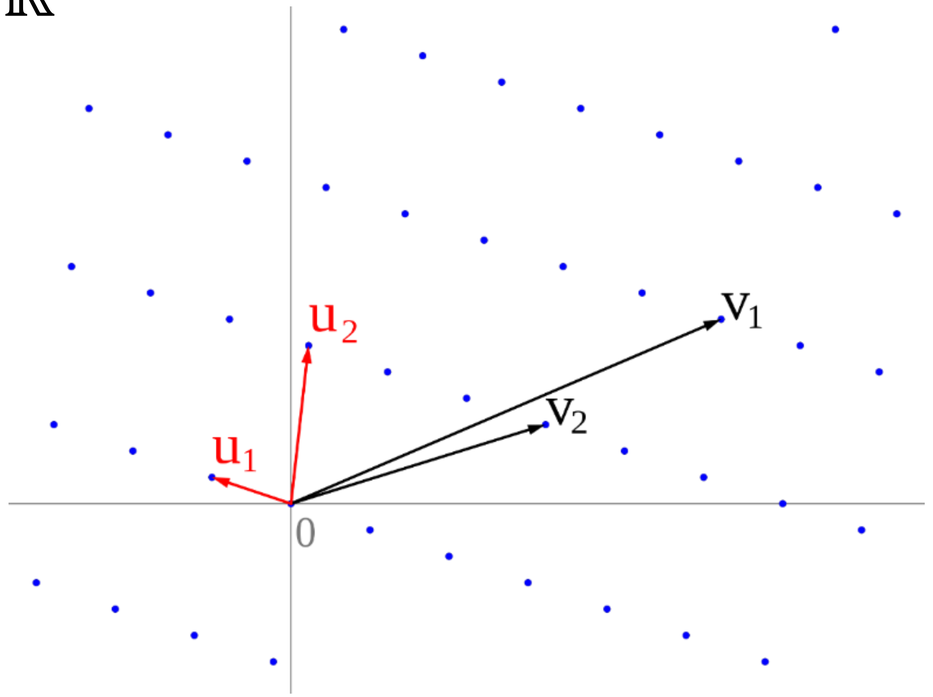
晶格 (Lattice) 上的計算難題

- Given a basis $B = \{b_1, b_2, \ldots, b_n\}$ where $b_i \in \mathbb{R}^n$
- Lattice is a discrete subgroup of $\mathbb{R}^n$:

  $\Lambda(B) = B\mathbb{Z}^n = \{\sum_{i=1}^{n} m_i b_i \mid m_i \in \mathbb{Z}\}$
- Shortest Vector Problem (SVP) :

  Find a shortest $x \in \Lambda(B) \setminus \{0\}$
- Closest Vector Problem (CVP) :

  Find a closest $x \in \Lambda(B)$ to a given $y \in \mathbb{R}^n$



- Lattice basis reduction :

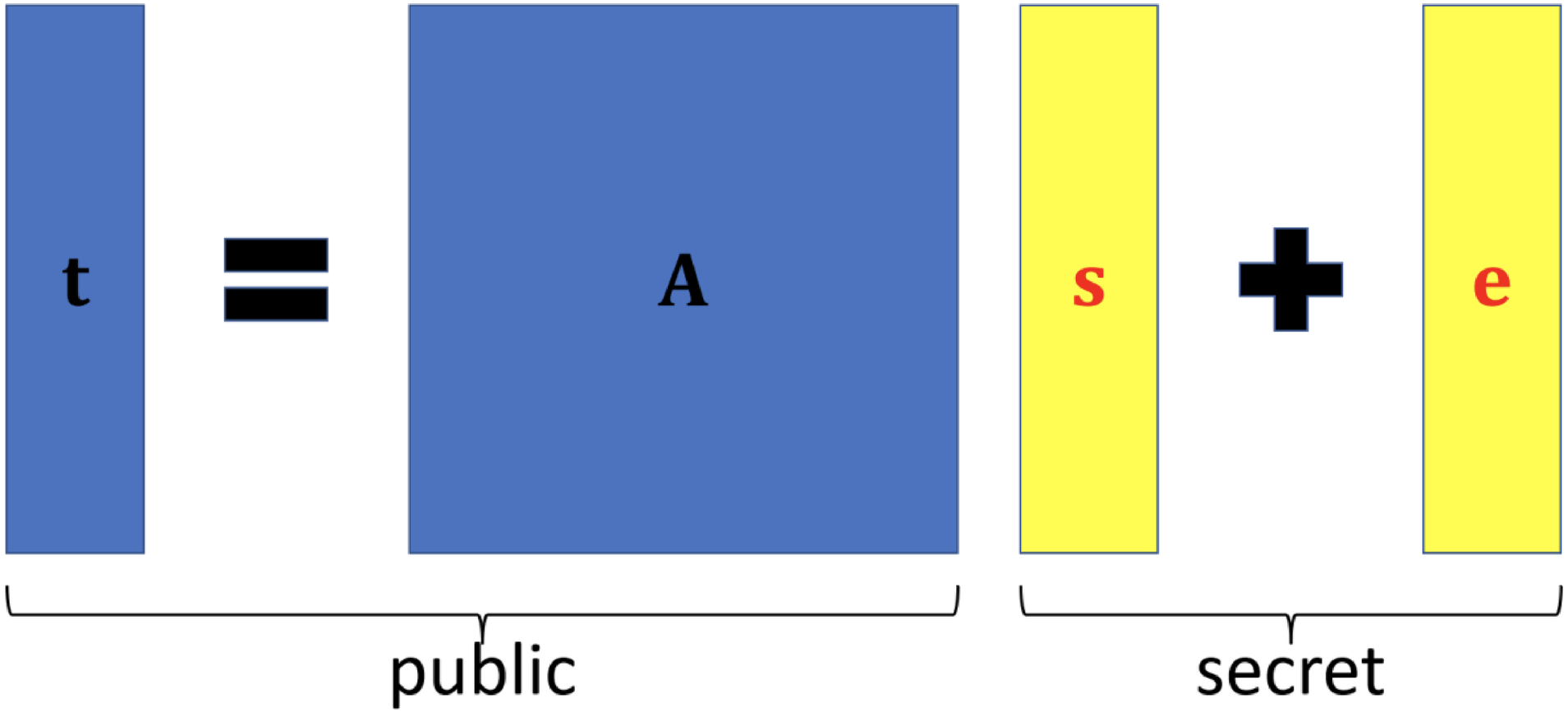
  Given a “bad” basis, find a “good” basis such that SVP or CVP is easier

Structured Lattices

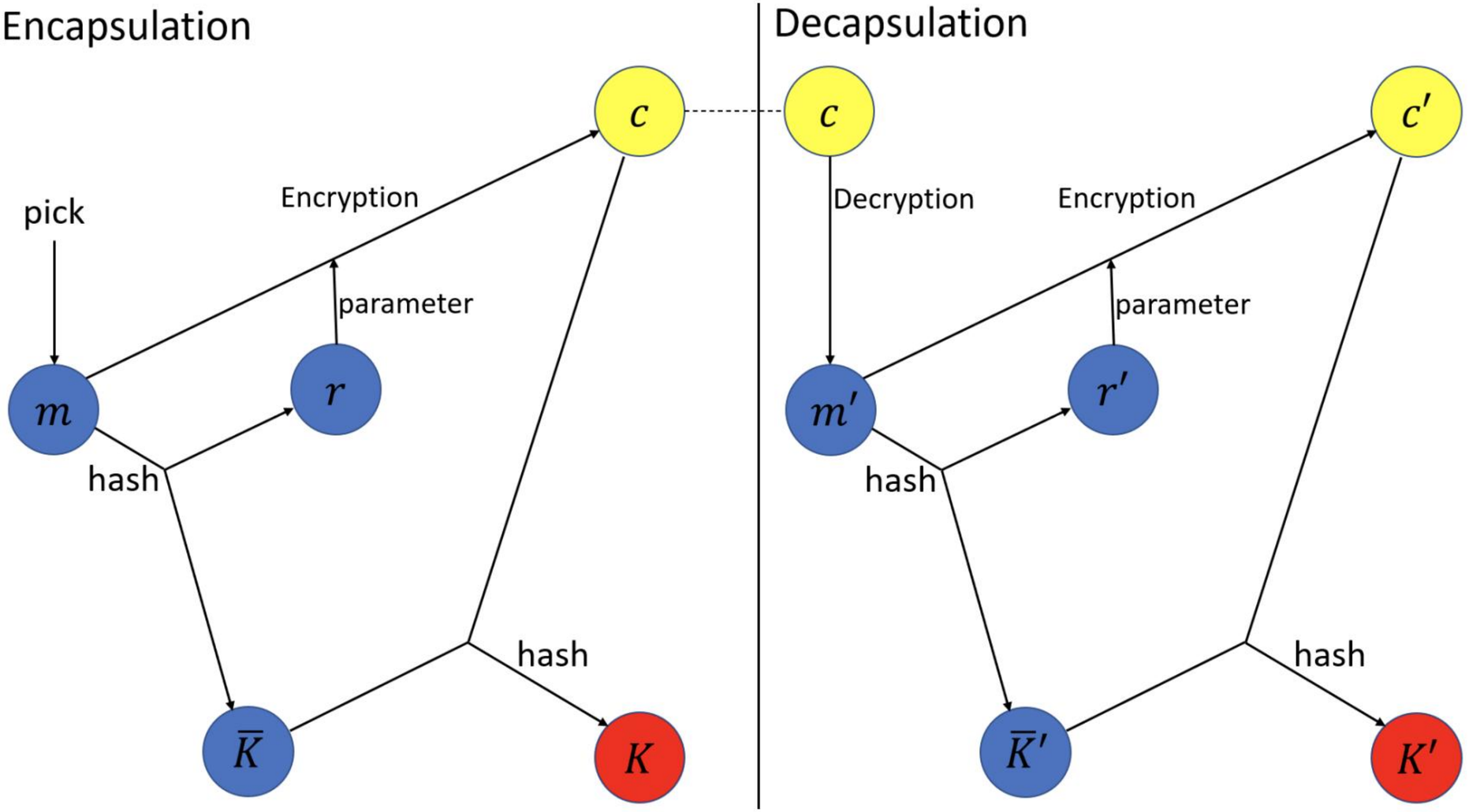
結構化晶格

- FIPS 203 / ML-KEM / CRYSTALS-Kyber
  - $R_q = Z_q[x]/(x^{256}+1)$
  - $q = 3329 = 13 \times 2^8 + 1$
- FIPS 204 / ML-DSA / CRYSTALS-Dilithium
  - $R_q = Z_q[x]/(x^{256}+1)$
  - $q = 8380417 = 2^{23} - 2^{13} + 1$

LWE: Learning With Errors (cf. CVP)



ML-KEM Overview



NTT: Number Theoretic Transform

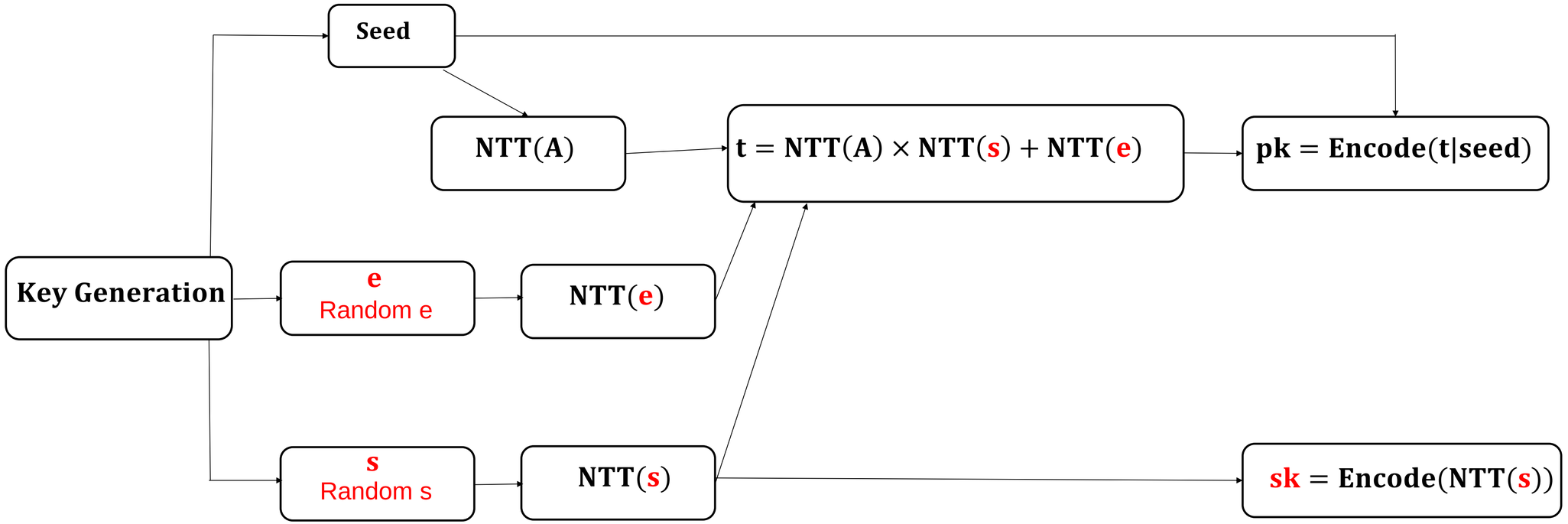
The Number-Theoretic Transform (NTT) can be viewed as a specialized, exact version of the discrete Fourier transform. In the case of ML-KEM, the NTT is used to improve the efficiency of multiplication in the ring R_q. Recall that R_q is the ring $\mathbb{Z}_q[X]/(X^n+1)$ of polynomials of the form $f = f_0 + f_1 X + \cdots + f_{255} X^{255}$ (where $f_j \in \mathbb{Z}_q$ for all j), with the ring operations defined by arithmetic modulo $X^n + 1$.

The ring R_q is isomorphic to another ring T_q, which is a direct sum of 128 quadratic extensions of $\mathbb{Z}_q$. The NTT is a computationally efficient isomorphism between these two rings. When a polynomial $f \in R_q$ is input, the NTT outputs an element $\hat{f} := \text{NTT}(f)$ of the ring T_q, where $\hat{f}$ is called the "NTT representation" of f. The isomorphism property implies that

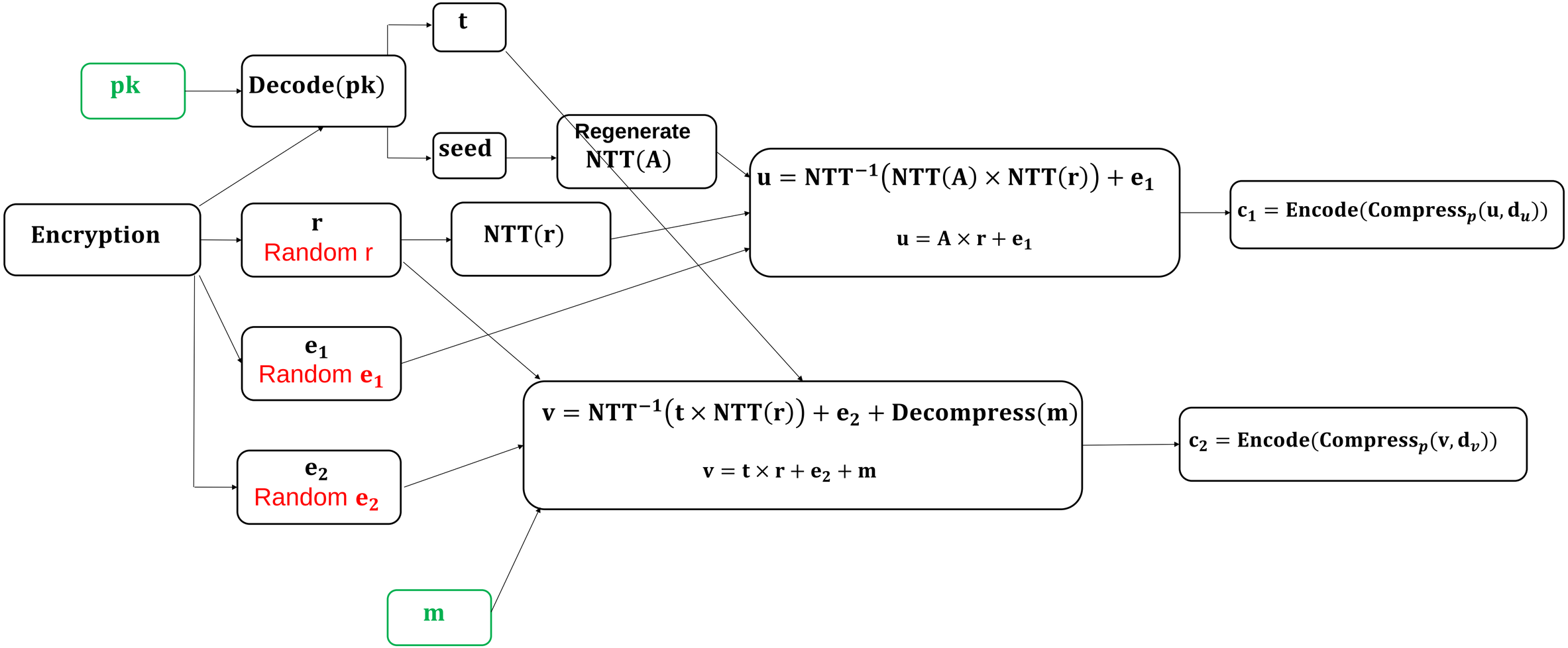
$$f \times_{R_q} g = \text{NTT}^{-1}(\hat{f} \times_{T_q} \hat{g}), \tag{4.9}$$

where $\times_{R_q}$ and $\times_{T_q}$ denote multiplication in R_q and T_q, respectively. Moreover, since T_q is a product of 128 rings that each consist of polynomials of degree at most one, the operation $\times_{T_q}$ is much more efficient than the operation $\times_{R_q}$. For these reasons, the NTT is considered to be an integral part of ML-KEM and not merely an optimization.

ML-KEM Key Generation



ML-KEM Encryption



ML-KEM Decryption

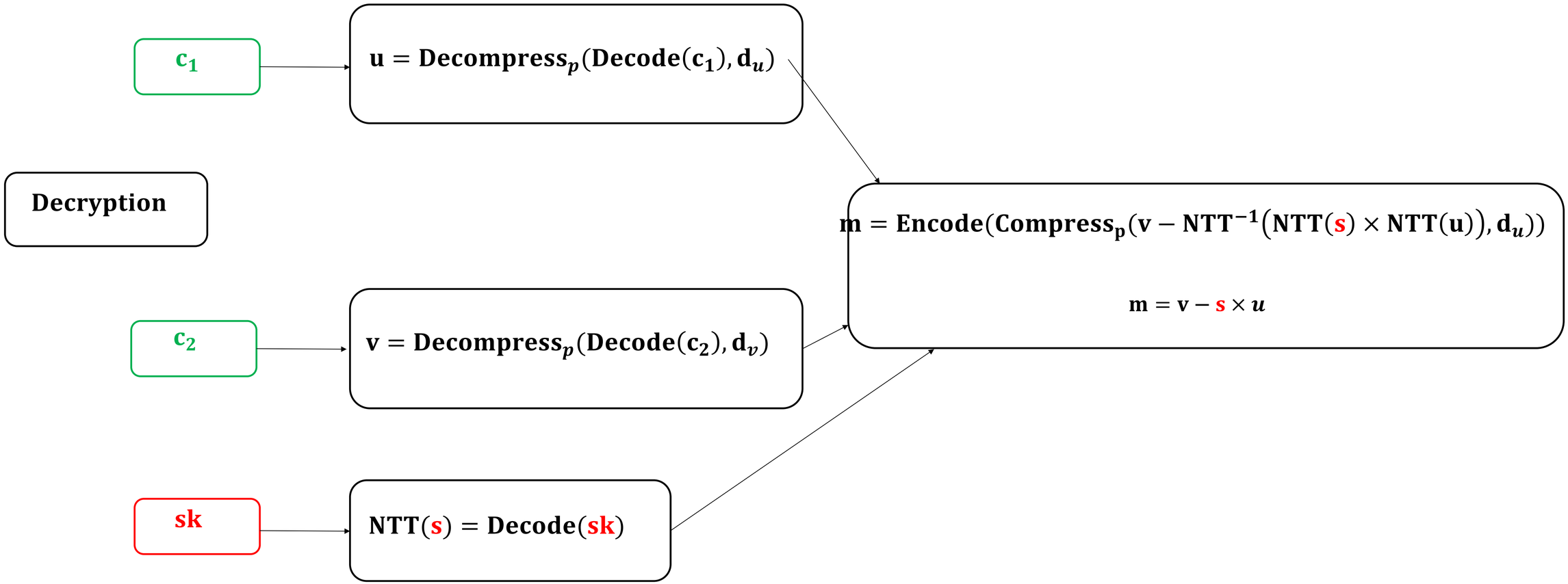


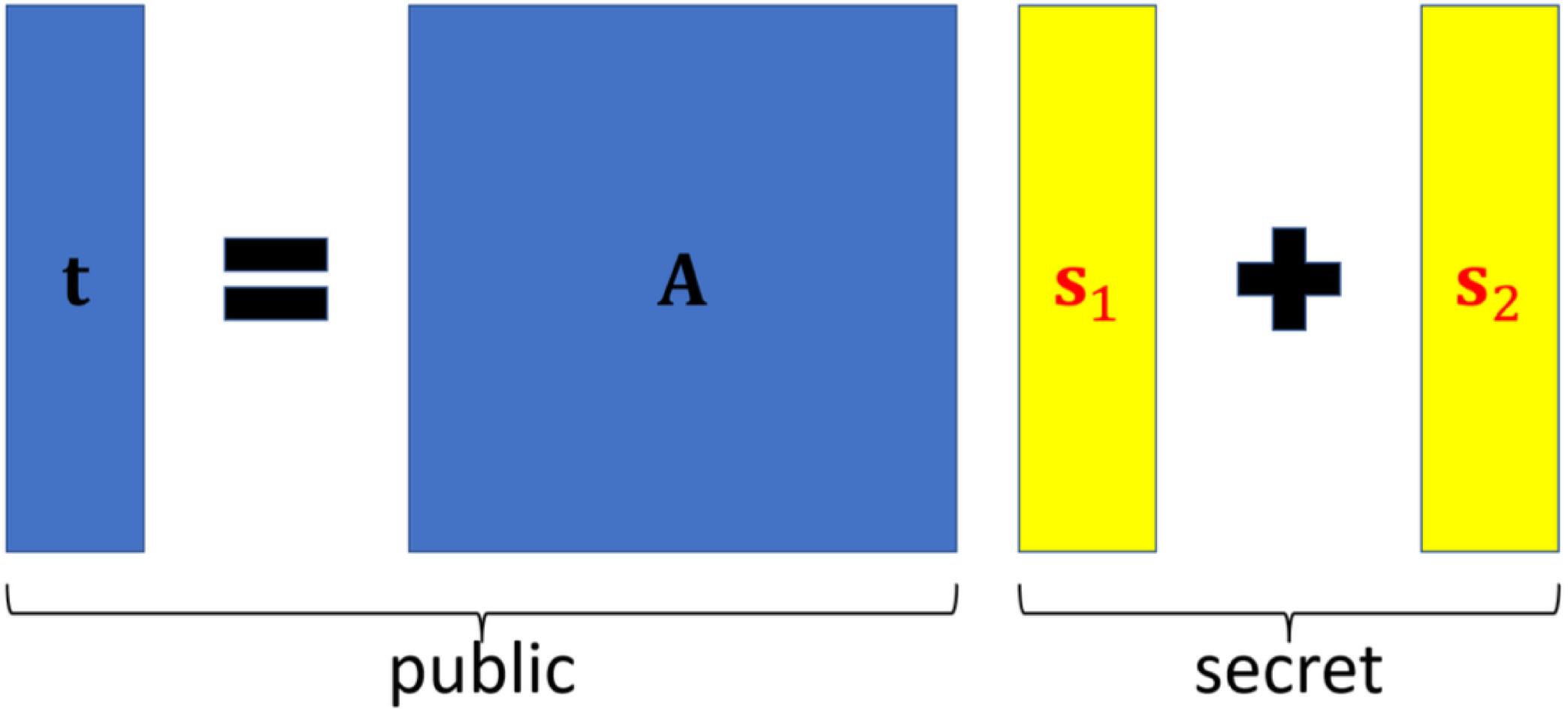
Table 1. Decapsulation failure rates for ML-KEM

Parameter set	Decapsulation failure rate
ML-KEM-512	$2^{-138.8}$
ML-KEM-768	$2^{-164.8}$
ML-KEM-1024	$2^{-174.8}$

Table 3. Sizes (in bytes) of keys and ciphertexts of ML-KEM

	encapsulation key	decapsulation key	ciphertext	shared secret key
ML-KEM-512	800	1632	768	32
ML-KEM-768	1184	2400	1088	32
ML-KEM-1024	1568	3168	1568	32

Private and Public Key of MS-DSA



Simplified ML-DSA Overview

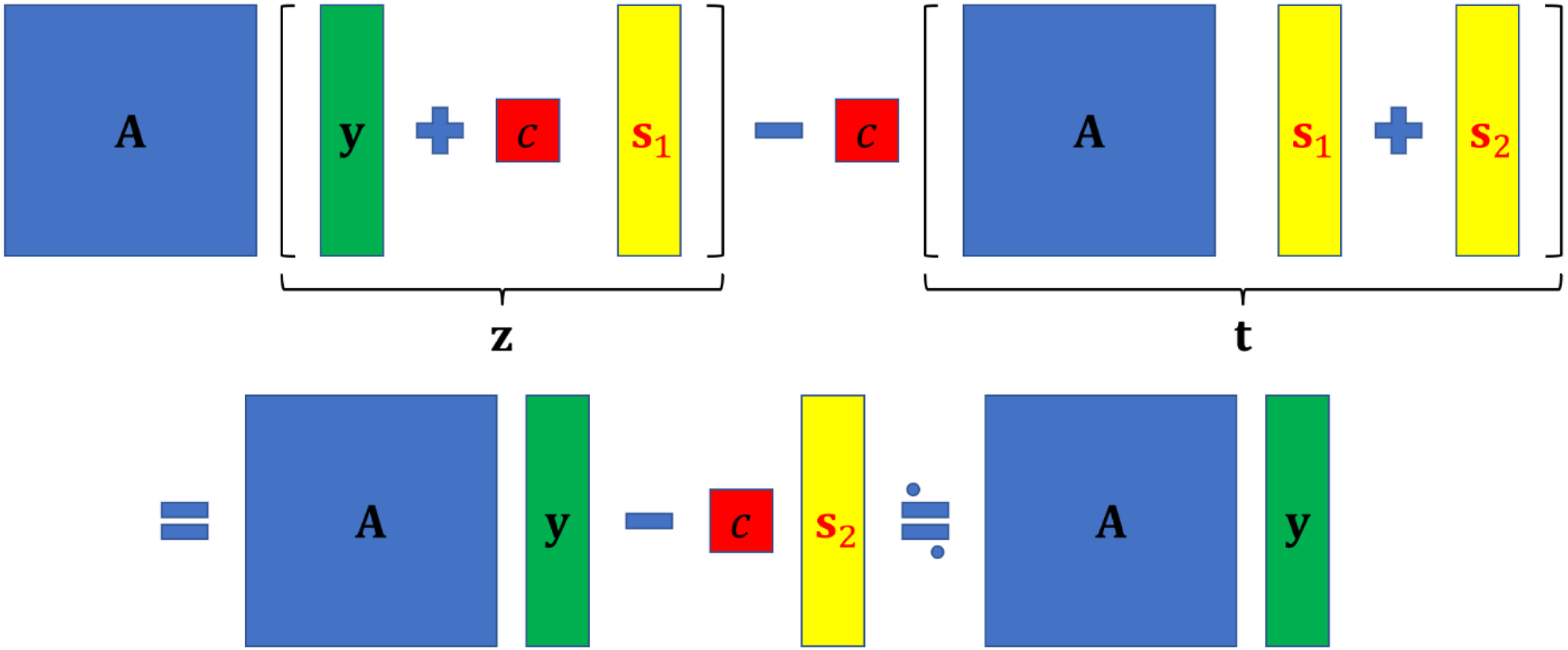


Table 2. Sizes (in bytes) of keys and signatures of ML-DSA

	Private Key	Public Key	Signature Size
ML-DSA-44	2560	1312	2420
ML-DSA-65	4032	1952	3309
ML-DSA-87	4896	2592	4627

Candidate	Claimed Security	Public key	Private key	Signature
Dilithium	Level 2	1312	2528	2420
	Level 3	1952	4000	3293
	Level 5	2592	4864	4595
FALCON-512	Level 1	897	7553	666
FALCON-1024	Level 5	1793	13953	1280
SPHINCS$^+$-128s	Level 1	32	64	7856
SPHINCS$^+$-128f	Level 1	32	64	17088
SPHINCS$^+$-192s	Level 3	48	96	16224
SPHINCS$^+$-192f	Level 3	48	96	35664
SPHINCS$^+$-256s	Level 5	64	128	29792
SPHINCS$^+$-256f	Level 5	64	128	49856

Candidate	Claimed Security	Key generation	Signing	verification
Dilithium	Level 2	124031	259172	118412
	Level 3	256403	428587	179424
	Level 5	298050	538986	279936
FALCON-512	Level 1	19872000	386678	82339
FALCON-1024	Level 5	63135000	789564	168498
SPHINCS$^+$-128s	Level 1	84964790	644740090	861478
SPHINCS$^+$-128f	Level 1	1334220	33651546	2150290
SPHINCS$^+$-192s	Level 3	125310788	1246378060	1444030
SPHINCS$^+$-192f	Level 3	1928970	55320742	3492210
SPHINCS$^+$-256s	Level 5	80943202	1025721040	1986974
SPHINCS$^+$-256f	Level 5	5067546	109104452	3559052

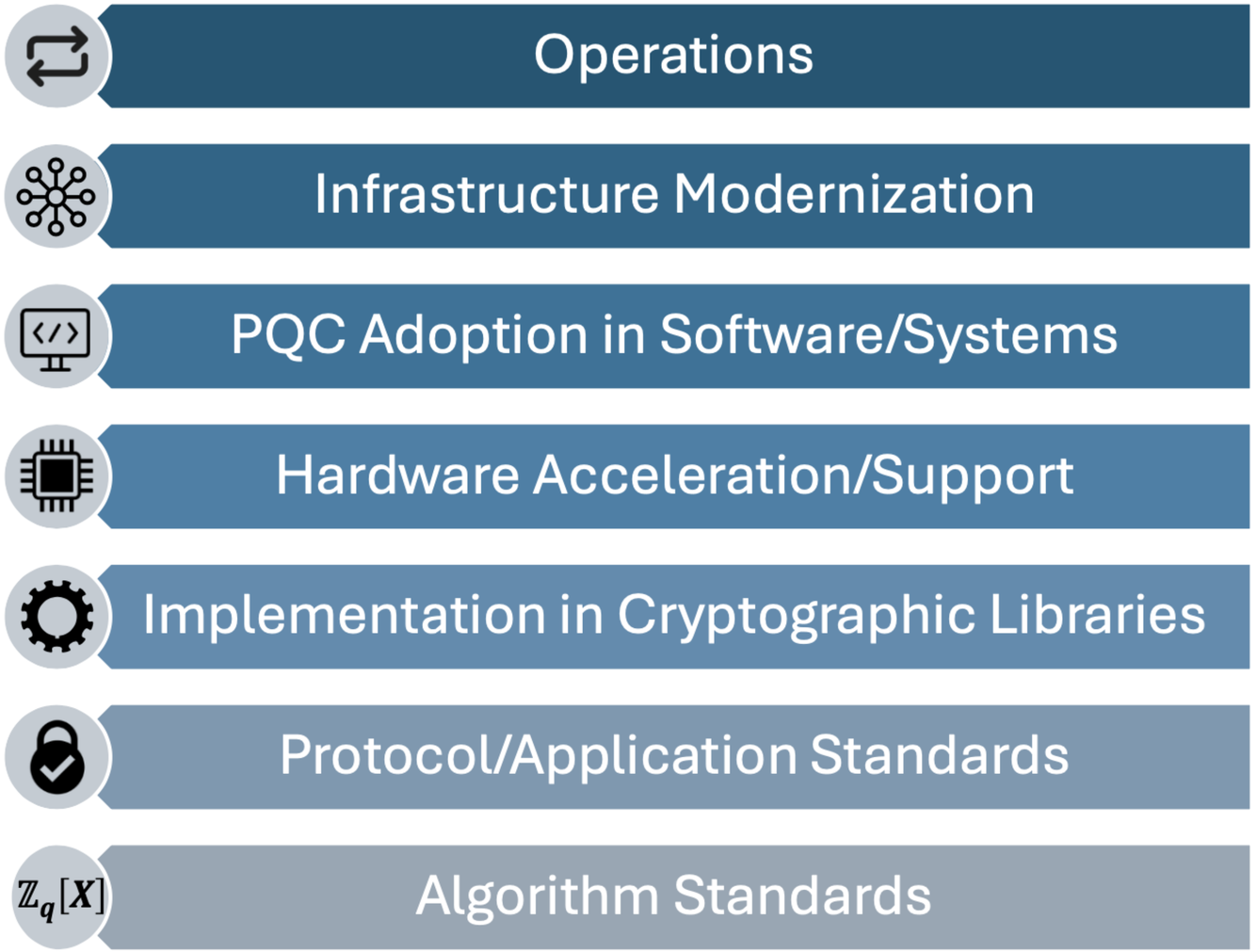
Table 4: Runtime benchmarks (in cycles) for the signature candidates.

- CRYSTALS-Dilithium / ML-DSA / FIPS 204 is recommended as the primary signature algorithm for general use
- FALCON / FN-DSA / future FIPS 206 would be a better choice for applications if it is not necessary to implement on constrained devices
- SPHINCS$^+$ / SLH-DSA / FIPS 205 is selected to be an alternative option as lattice-based schemes are threatened.

Agenda

- 公鑰密碼系統的風險 Risk of PKC
- 後量子密碼標準 PQC Standards
- **後量子密碼遷移 PQC Migrations**
- 旁通道攻擊 Side-Channel Attacks

Path of PQC Migration



https://pqcrypto2025.iis.sinica.edu.tw/slides/Invited1.pdf

CNSA: Commercial National Security Algorithm

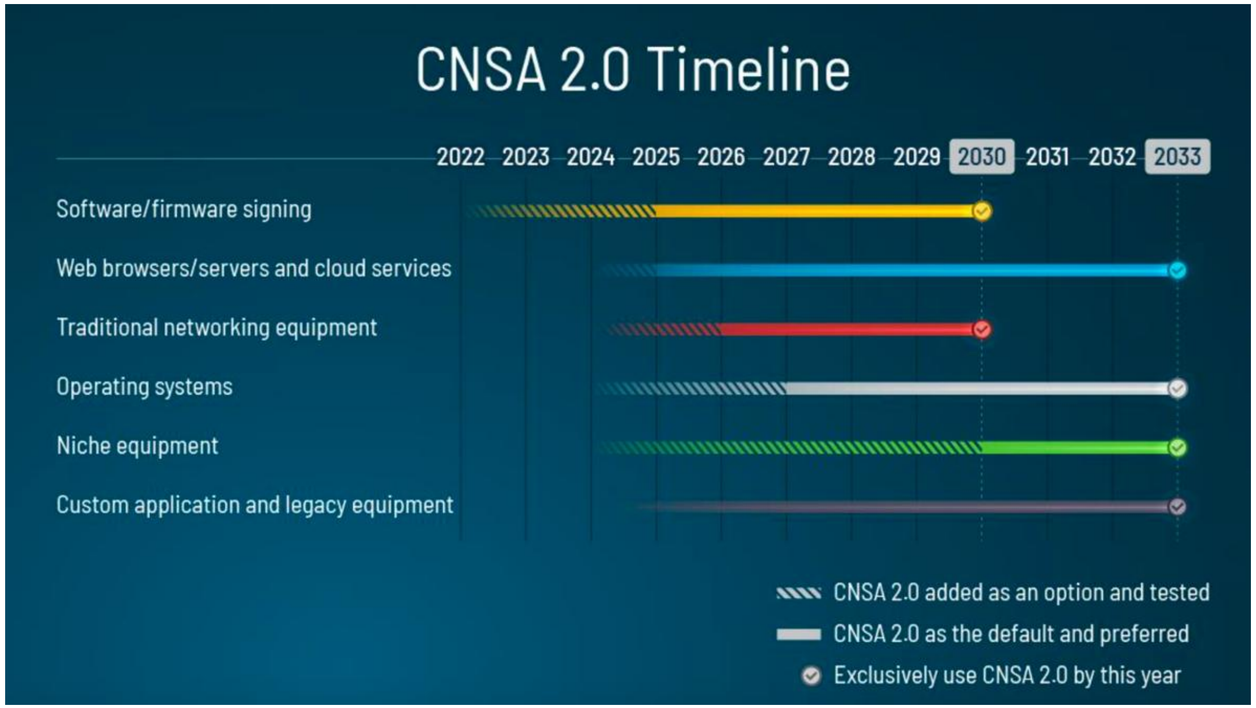
Table: Commercial National Security Algorithm Suite 2.0

Algorithm	Function	Specification	Parameters
General Purpose Algorithms			
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.
ML-DSA (previously CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	ML-DSA-87 for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Algorithms Allowed in Specific Applications			
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.
Secure Hash Algorithm 3 (SHA3)	Algorithm used for computing a condensed representation of information as part of hardware integrity	FIPS PUB 202	SHA3-384 or SHA3-512 allowed for internal hardware functionality only (e.g., boot-up integrity checks)

U/OO/194427-22 | PP-24-4014 | December 2024 Ver. 2.1

https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF

CNSA 2.0 Timeframe



- **Software- and firmware-signing:** begin transitioning immediately, support and prefer CNSA 2.0 by 2025 where available, *exclusively* use CNSA 2.0 by 2030.
- **Web browsers/servers and cloud services**: support and prefer CNSA 2.0 by 2025, *exclusively*[8] use CNSA 2.0 by 2033.
- **Traditional networking equipment (e.g., virtual private networks, routers):** support and prefer CNSA 2.0 by 2026, *exclusively* use CNSA 2.0 by 2030.
- **Operating systems**: support and prefer CNSA 2.0 by 2027, *exclusively* use CNSA 2.0 by 2033.
- **Niche equipment (e.g., constrained devices, large public-key infrastructure systems)**: support and prefer CNSA 2.0 by 2030, *exclusively* use CNSA 2.0 by 2033.
- **Custom applications and legacy equipment**: update or replace by 2033.

U/OO/194427-22 | PP-22-1338 | SEP 2022 Ver. 1.0

U/OO/194427-22 | PP-24-1178 | April 2024 Ver. 2.0

Timeframe

Q: What timeframe information can NSA provide for adoption of CNSA 2.0?

A: NSA intends that all NSS will be quantum-resistant by 2035, in accordance with the goal espoused in NSM-10. NSA's recent update to CNSSP 15 has set several dates to aid in this transition in the commercial space, with the hope of completing much of the transition sooner.

Any NSS currently validated against a NIAP or CSfC profile continues to be approved for the life of that validation, and no requirement to transition will be enforced prior to December 31, 2025. However, any NSS not CNSA 1.0 compliant has six months from the publication date of the updated CNSSP 15 to come into compliance with CNSA 2.0, or 90 days to request a waiver.

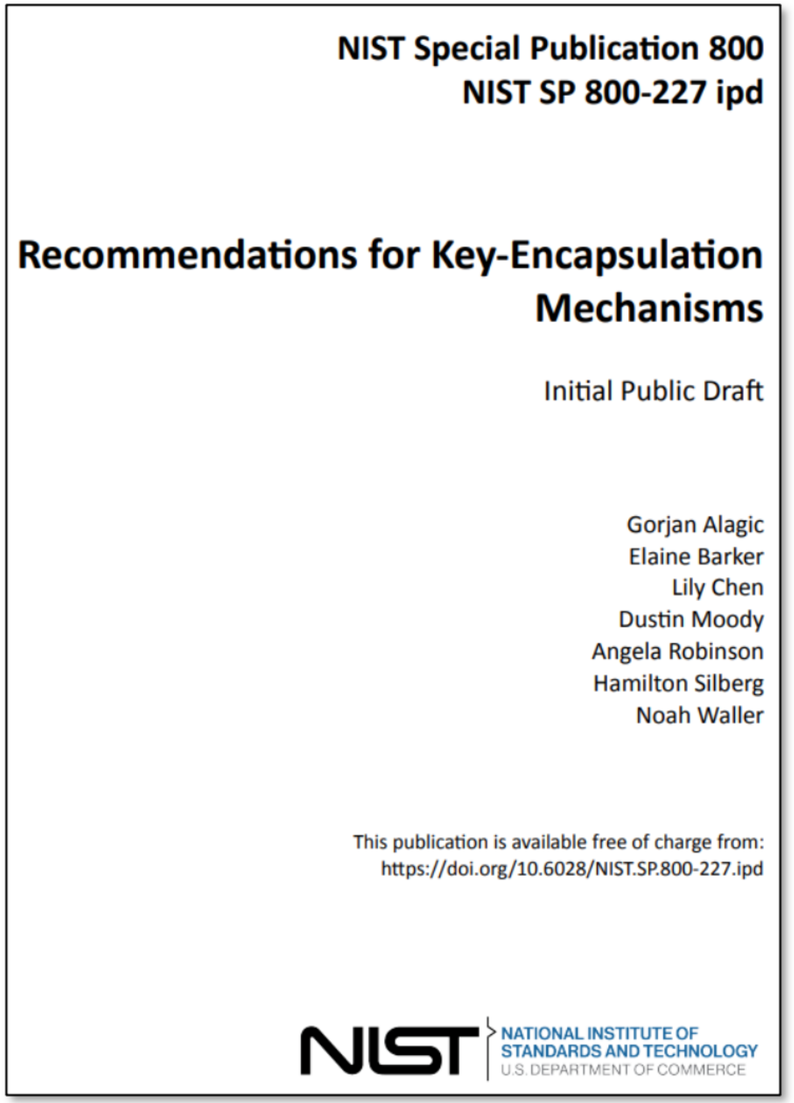
CNSSP 15 states that by January 1, 2027, all new acquisitions for NSS will be required to be CNSA 2.0 compliant unless otherwise noted.

By December 31, 2030, all equipment and services that cannot support CNSA 2.0 must be phased out unless otherwise noted, and by December 31, 2031, CNSA 2.0 algorithms are mandated for use unless otherwise noted.

CNSSP = Committee on National Security Systems Policy

Draft NIST SP 800-227, Recommendations for KEMs

- ***Released:*** January 7, 2025
  - Comment period ended: March 7th, 2025
- Draft describes the basic definitions, properties, and applications of KEMs
- Provides recommendations for implementing and using KEMs in a secure manner
- Contains some guidance on hybrid key establishment
- ***NIST Workshop on Guidance for KEMs***
  - Held on February 25-26th
  - Intended to facilitate discussions on draft guidance for KEMs
  - Slides available at: https://csrc.nist.gov/Events/2025/workshop-on-guidance-for-kems



NIST Special Publication 800
NIST SP 800-227 ipd

Recommendations for Key-Encapsulation Mechanisms

Initial Public Draft

Gorjan Alagic
Elaine Barker
Lily Chen
Dustin Moody
Angela Robinson
Hamilton Silberg
Noah Waller

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-227.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

https://pqcrypto2025.iis.sinica.edu.tw/slides/Invited1.pdf

NIST IR 8547 (Initial Public Draft)

Transition to Post-Quantum Cryptography Standards

Date Published: November 12, 2024
Comments Due: January 10, 2025 (public comment period is CLOSED)
Email Questions to: pqc-transition@nist.gov

Planning Note (01/21/2025):

The public comments received are now available.

Author(s)

Dustin Moody (NIST), Ray Perlner (NIST), Andrew Regenscheid (NIST), Angela Robinson (NIST), David Cooper (NIST)

Announcement

This report describes NIST's expected approach to transitioning from quantum-vulnerable cryptographic algorithms to post-quantum digital signature algorithms and key-establishment schemes. It identifies existing quantum-vulnerable cryptographic standards and the current quantum-resistant standards that will be used in the migration. This report should inform the efforts and timelines of federal agencies, industry, and standards organizations for migrating information technology products, services, and infrastructure to PQC. Comments received on this draft will be used to revise this transition plan and feed into other algorithm- and application-specific guidance for the transition to PQC.

DOCUMENTATION

Publication:
https://doi.org/10.6028/NIST.IR.8547.ipd
Download URL

Supplemental Material:
Public comments received (pdf)

Document History:
11/12/24: IR 8547 (Draft)

TOPICS

Security and Privacy
post-quantum cryptography

https://csrc.nist.gov/pubs/ir/8547/ipd

- **Acceptable** means that the algorithm and key length/ strength in a FIPS or SP are **approved** for use in accordance with any associated guidance.
- **Deprecated** means that the algorithm and key length/strength may be used, but there is some security risk. The data owner must examine this risk potential and decide whether to continue to use a **deprecated** algorithm or key length.
- **Disallowed** means that the algorithm, key length/strength, parameter set, or scheme is no longer allowed for the stated purpose.
- **Legacy use** means that the algorithm, scheme, or parameter set may only be used to process already protected information (e.g., to decrypt ciphertext data or to verify a digital signature).

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Table 4: Quantum-vulnerable key-establishment schemes

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Table 1: Post-Quantum Security Categories

Security Category	Attack Type	Example
1	Key search on a block cipher with a 128-bit key	AES-128
2	Collision search on a 256-bit hash function	SHA-256
3	Key search on a block cipher with a 192-bit key	AES-192
4	Collision search on a 384-bit hash function	SHA3-384
5	Key search on a block cipher with a 256-bit key	AES-256

Table 6: Block ciphers

Block Cipher	Parameter Sets	Security Strength	Security Category
AES [FIPS197]	AES-128	128 bits	1
	AES-192	192 bits	3
	AES-256	256 bits	5

Table 3. Post-quantum digital signature algorithms

Digital Signature Algorithm Family	Parameter Sets	Security Strength	Security Category
ML-DSA [FIPS204]	ML-DSA-44	128 bits	2
	ML-DSA-65	192 bits	3
	ML-DSA-87	256 bits	5
SLH-DSA [FIPS205]	SLH-DSA-SHA2-128[s/f] SLH-DSA-SHAKE-128[s/f]	128 bits	1
	SLH-DSA-SHA2-192[s/f] SLH-DSA-SHAKE-192[s/f]	192 bits	3
	SLH-DSA-SHA2-256[s/f] SLH-DSA-SHAKE-256[s/f]	256 bits	5
LMS, HSS [SP800208]	With SHA-256/192 With SHAKE256/192	192 bits	3
	With SHA-256 With SHAKE256	256 bits	5
XMSS, XMSS^{MT} [SP800208]	With SHA-256/192 With SHAKE256/192	192 bits	3
	With SHA-256 With SHAKE256	256 bits	5

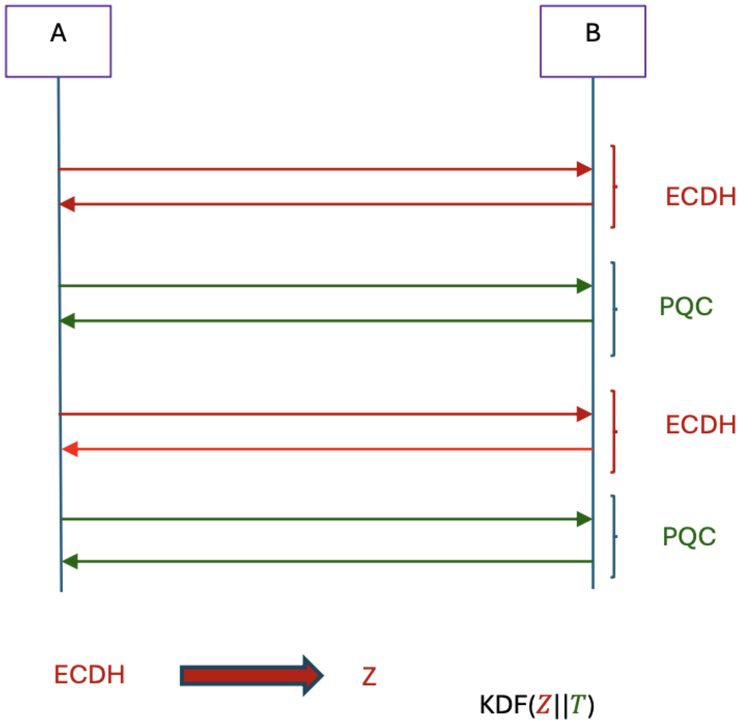
Table 5: Post-quantum key-establishment schemes

Key Establishment Scheme	Parameter Sets	Security Strength	Security Category
ML-KEM [FIPS203]	ML-KEM-512	128 bits	1
	ML-DSA-768	192 bits	3
	ML-DSA-1024	256 bits	5

- System migration timelines will depend on use case or application
- Priorities:
  - Systems with long-term confidentiality needs– *e.g., VPN, TLS*
  - Broad, long-lived cryptographic infrastructures– *e.g., PKI, PIV, code signing*
- NIST will develop/update application-specific guidance throughout the transition, e.g.,
  - **FIPS 201**– *Personal Identity Verification (PIV) of Federal Employees and Contractors*
  - **NIST SP 800-52**– *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
  - **NIST SP 800-77**– *Guide to IPSec VPNs*
  - **NIST SP 800-57 Part 3** – *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*

Hybrid Schemes

- **Hybrid**: using classical and PQC algorithms together
  - A hybrid mode combines a classical algorithm with a PQC algorithm
  - Reduces risks from uncertainty if either is broken
  - More complexity / slower performance
  - Can get FIPS 140 validation
  - More guidance in SP 800-227 – order of schemes not important
- Several approaches to hybrid KEMs and certificates
  - Composite approaches
  - Non-composite hybrid approaches
- Use of hybrid will depend on community and application-specific needs
  - NIST does not intend to recommend for/against hybrid schemes
  - Implementers should consider complexity and migration issues
- Architectures /applications may support multiple algorithms



Recommendations & FIPS 140 Testing

- NIST provided guidance for transition in the past (SP 800-131A) and will provide PQC transition guidance

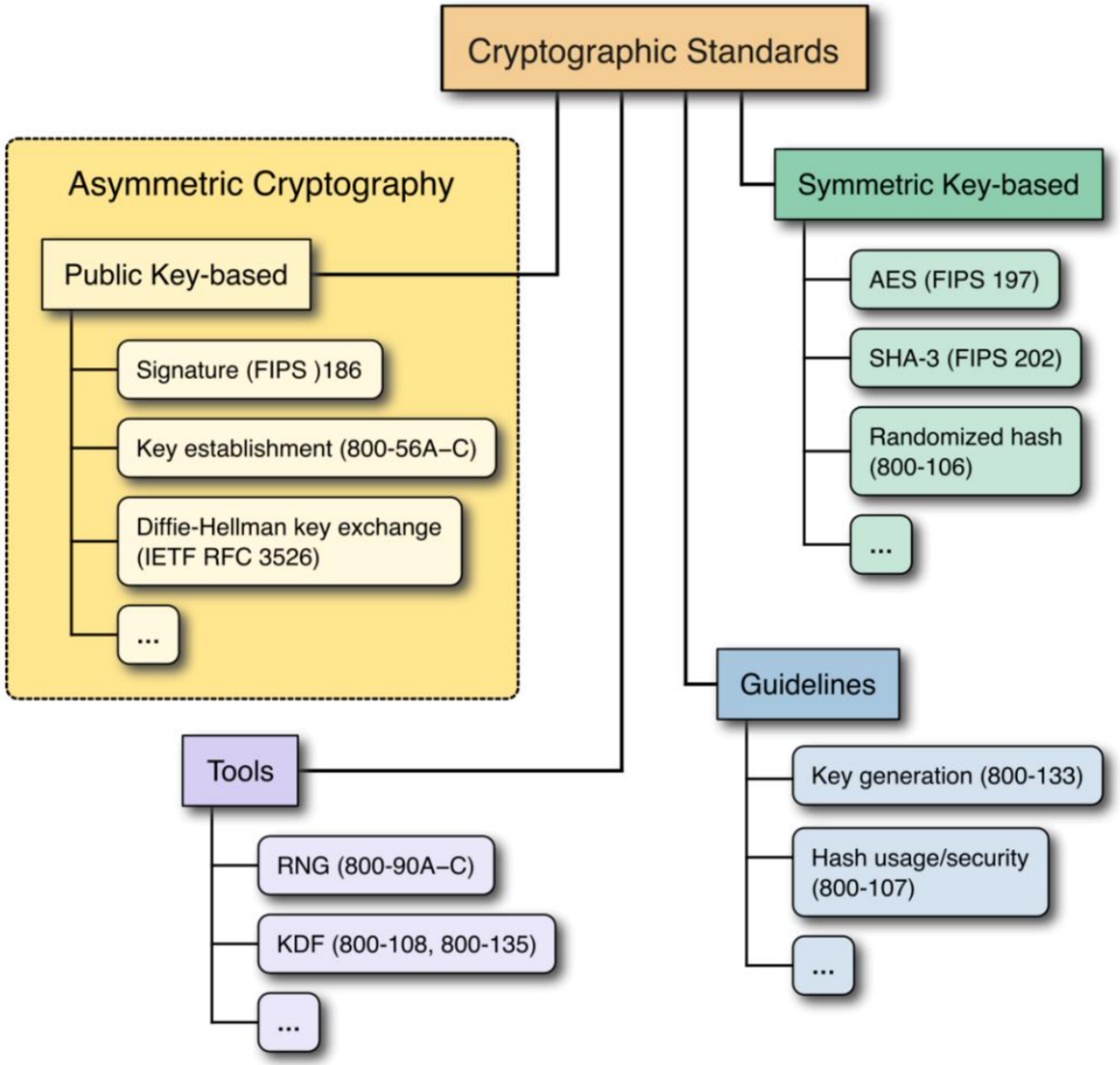
- **Cryptographic Algorithm Validation Program**
  - Automated Cryptographic Validation Testing System (ACVTS) https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/how-to-access-acvts
  - Testing for algorithm standards to enable production/official testing

    https://github.com/usnistgov/ACVP-Server

    Test vectors are available:

    https://github.com/usnistgov/ACVP-Server/tree/master/gen-val/

- NIST CAVP is already testing new PQC algorithms for FIPS 140 validation



National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

https://www.nccoe.nist.gov/sites/default/files/2022-06/Migration-to-PQC-05-16.pdf

Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography

- SP 1800-38A
- Collaborating organizations:

Consortium Members	
Amazon Web Services, Inc. (AWS)	JPMorgan Chase Bank, N.A.
Cisco Systems, Inc.	Microsoft
Crypto4A Technologies, Inc.	National Security Agency (NSA)
CryptoNext Security	PQShield
Dell Technologies	Samsung SDS Co., Ltd.
DigiCert	SandboxAQ
Entrust	Thales DIS CPL USA, Inc.
IBM	Thales Trusted Cyber Technologies
Information Security Corporation	VMware, Inc.
InfoSec Global	wolfSSL
ISARA Corporation	

https://www.nccoe.nist.gov/sites/default/files/2023-04/pqc-migration-nist-sp-1800-38a-preliminary-draft.pdf

Draft NIST SP 1800-38B

Quantum Readiness: Cryptographic Discovery

- Functional test plan that exercises the cryptographic discovery tools to determine baseline capabilities
- Describes a use case to provide context and scope
- Identifies threats addressed in this demonstration
- Provides a multifaceted approach to start the discovery process
- Describes the high-level architecture that integrates contributed discovery tools in our lab

Draft NIST SP 1800-38C

Quantum Readiness: Testing Draft Standards for Interoperability and Performance

- Identification of compatibility issues between quantum-ready algorithms
- Explore interoperability issues in a controlled, non-production environment
- Reduction of time spent by individual organizations performing similar interoperability testing for their own PQC migration efforts

- ***Crypto agility*** describes the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures without interrupting the flow of a running system to achieve resiliency

- NIST Cybersecurity White Paper Considerations for Achieving Cryptographic Agility: Strategies and Practices is to survey the current practice and inspire sector specific approaches
  - Bring crypto agility awareness for different players
  - Accommodate communications between cryptographers, developers, and practitioners
  - Explore operational mechanisms in each implementation environment to achieve crypto agility
  - Encourage developing sector/standards specific guidelines

- NIST will hold a virtual crypto agility workshop April 17-18, 2025
  https://csrc.nist.gov/Events/2025/crypto-agility-workshop
  Submission deadline ended: March 31, 2025

Agenda

- 公鑰密碼系統的風險 Risk of PKC
- 後量子密碼標準 PQC Standards
- 後量子密碼遷移 PQC Migrations
- **旁通道攻擊 Side-Channel Attacks**

Side Channel Attack (SCA)

旁通道攻擊

ECDSA Key Extraction 隔空抓鑰

- ECDSA Key Extraction from Mobile Devices: Fully extract secret signing keys from OpenSSL and CoreBitcoin running on iOS devices

https://www.tau.ac.il/~tromer/mobilesc

EUCLEAK

Side-Channel Attack on the YubiKey 5 Series

(Revealing and Breaking Infineon ECDSA Implementation on the Way)

Thomas Roche

NinjaLab, Montpellier, France
thomas@ninjalab.io

September 3^{rd}, 2024

https://ninjalab.io/wp-content/uploads/2024/09/20240903_eucleak.pdf

yubico

Subscribe Store

Security Advisory YSA-2024-03 Infineon ECDSA Private Key Recovery

Published Date: 2024-09-03
Tracking IDs: YSA-2024-03
CVE: In Process
CVSS Severity: 4.9

Summary

A vulnerability was discovered in Infineon's cryptographic library, which is utilized in YubiKey 5 Series, and Security Key Series with firmware prior to 5.7.0 and YubiHSM 2 with firmware prior to 2.4.0. The severity of the issue in Yubico devices is moderate.

An attacker could exploit this issue as part of a sophisticated and targeted attack to recover affected private keys. The attacker would need physical possession of the YubiKey, Security Key, or YubiHSM, knowledge of the accounts they want to target, and specialized equipment to perform the necessary attack. Depending on the use case, the attacker may also require additional knowledge including username, PIN, account password, or authentication key. See Affected Use Cases and Mitigations for more details.

The moderate vulnerability primarily impacts FIDO use cases because the FIDO standard relies on the affected functionality by default. YubiKey PIV and OpenPGP applications and YubiHSM 2 usage may also be impacted depending on configuration and algorithm choices by the end user.

As part of ongoing improvements in Yubico products and to reduce exposure to our supply chain, the dependency on Infineon's cryptographic library has been removed in favor of Yubico's own cryptographic library.

https://www.yubico.com/support/security-advisories/ysa-2024-03/

Apple Chips Are Vulnerable to Side-Channel Attacks That Could Expose Credit Card Information

Published January 29, 2025 |  Written by Megan Crouse

Macs, iPhones, and iPads made during and after 2021 may be at risk. However, no attackers have taken advantage. Apple is aware of the security vulnerabilities.

https://www.techrepublic.com/article/apple-m-chips-side-channel-vulnerabilities/

Side-Channel Attack on Kyber

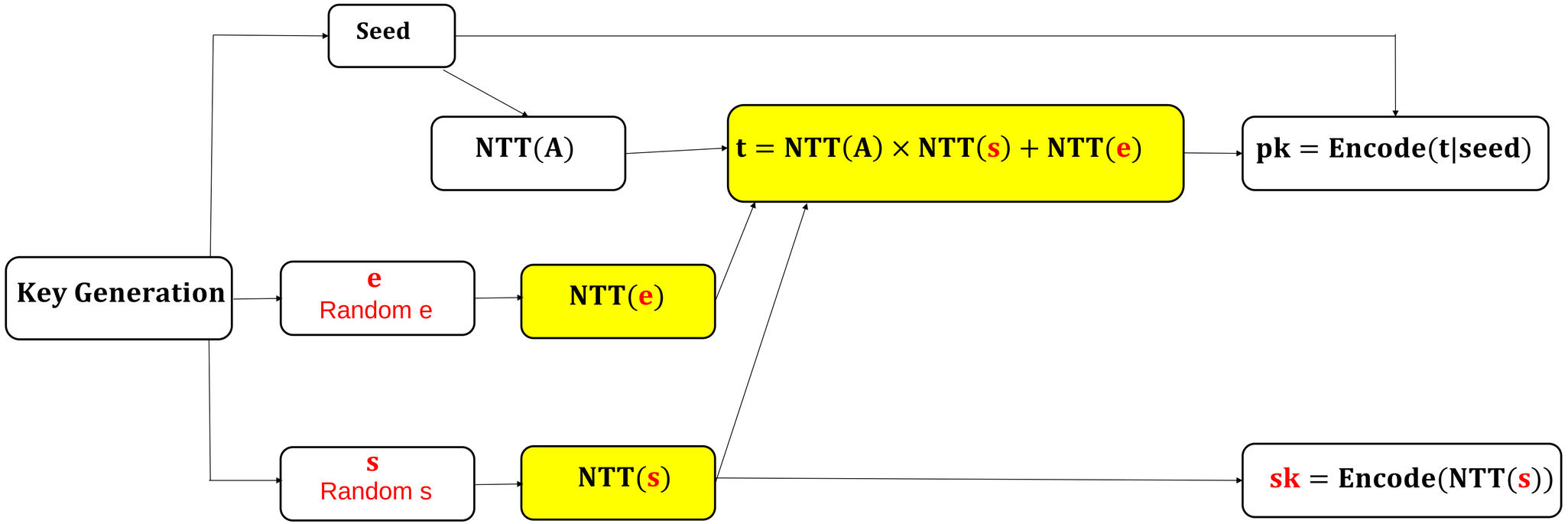
Power Analysis Attack

Cache Attack

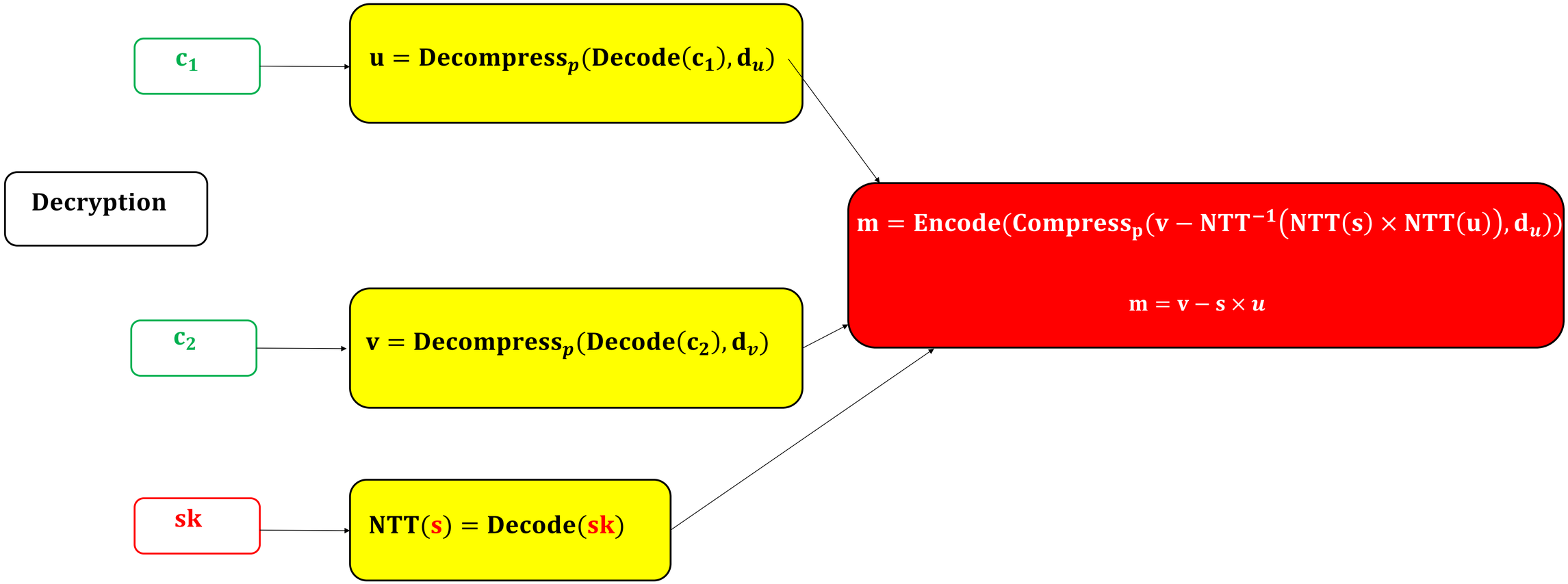
Timing Attack

Electromagnetic Analysis Attacks

Side-Channel Attack on Kyber



Side-Channel Attack on Kyber



Many SCAs on Kyber Implementations

Magnifying Side-Channel Leakage of Lattice-Based Cryptosystems with Chosen Ciphertexts: The Case Study of Kyber

Zhuang Xu, Owen Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng

Abstract—Lattice-based cryptography, as an active branch of post-quantum cryptography (PQC), has drawn side-channel analysis researchers in recent years. Despite the various side-channel targets examined in prev revealing the secret-dependent information efficiently is less studied. In this paper, we propose adaptive EM s carefully constructed ciphertexts on Kyber, which is a finalist of NIST PQC standardization project. We demo chosen ciphertexts allow an adversary to modulate the leakage of a target device and enable full key extracti traces through simple power analysis. Compared to prior research, our techniques require fewer traces and a templates. We practically evaluate our methods using both a reference implementation and the ARM-specific library. For the reference implementation, we target the leakage of the output of the inverse NTT computation with only four traces. For the pqm4 implementation, we develop a message-recovery attack that leads to extra with between eight and 960 traces, depending on the compiler optimization level. We discuss the relevance o lattice-based schemes and explore potential countermeasures.

Index Terms—Lattice-based cryptography, Kyber, side-channel analysis, chosen-ciphertext attack.

A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber

Yanning Ji
KTH Royal Institute of Technology
Stockholm, Sweden
yanning@kth.se

Ruize Wang
KTH Royal Institute of Technology
Stockholm, Sweden
ruize@kth.se

Kalle Ngo
KTH Royal Institute of Technology
Stockholm, Sweden
kngo@kth.se

Elena Dubrova
KTH Royal Institute of Technology
Stockholm, Sweden
dubrova@kth.se

Linus Backlund
KTH Royal Institute of Technology
Stockholm, Sweden
lbackl@kth.se

***Abstract*—CRYSTALS-Kyber has been recently selected by the NIST as a new public-key encryption and key-establishment algorithm to be standardized. This makes it important to assess how well CRYSTALS-Kyber implementations withstand side-channel attacks. Software implementations of CRYSTALS-Kyber have been already analyzed and the discovered vulnerabilities were patched in the subsequently released versions. In this paper, we present a profiling side-channel attack on a hardware implementation of CRYSTALS-Kyber with the security parameter $k = 3$, Kyber768. Since hardware implementations carry out** knowledge, no successful attack on a hardware implementation of CRYSTALS-Kyber has been reported until now. Hardware implementations are typically significantly more difficult to break than software variants because they carry out the computation in parallel. There are opinions that the parallelism, in a combination with a smaller minimum feature size of application-specific integrated circuits (ASICs) of field-programmable gate array (FPGAs) process technologies may

Many SCAs on Kyber Implementations

Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber

Mike Hamburg[1], Julius Hermelink[2], Robert Primas[3], Simona Samardjiska[4], Thomas Schamberger[5], Silvan Streit[6], Emanuele Strieder[7] Christine van Vredendaal[8]

[1] Rambus Labs, USA mhamburg@rambus.com
[2] Universität der Bundeswehr München, Germany julius.hermelink@uni
[3] Graz University of Technology, Austria robert.primas@iaik.tugraz
[4] Radboud University, The Netherlands simonas@cs.ru.nl
[5] Technical University of Munich (TUM), Germany t.schamberger@tu
[6] Fraunhofer Institute AISEC, Germany silvan.streit@aisec.fraunhof
[7] Fraunhofer Institute AISEC, Germany emanuele.strieder@aisec.fraunh
[8] NXP Semiconductors christine.cloostermans@nxp.com

Abstract.
Single-trace attacks are a considerable threat to implementations of classic pu schemes, and their implications on newer lattice-based schemes are still understood. Two recent works have presented successful single-trace attacks t the Number Theoretic Transform (NTT), which is at the heart of many latti schemes. However, these attacks either require a quite powerful side-channel a or are restricted to specific scenarios such as the encryption of ephemeral se is still an open question if such attacks can be performed by simpler adversari targeting more common public-key scenarios.

In this paper, we answer this question positively. First, we present a for crafting ring/module-LWE ciphertexts that result in sparse polynomial input of inverse NTT computations, independent of the used private key.

Pushing the Limits of Generic Side-Channel Attacks on LWE-based KEMs - Parallel PC Oracle Attacks on Kyber KEM and Beyond

Gokulnath Rajendran[2], Prasanna Ravi[1,2], Jan-Pieter D'Anvers[3], Shivam Bhasin[1] and Anupam Chattopadhyay[1,2]

[1] Temasek Laboratories, Nanyang Technological University, Singapore
[2] School of Computer Science and Engineering, Nanyang Technological University, Singapore
[3] imec-COSIC KU Leuven, Kasteelpark Arenberg 10 - bus 2452, 3001 Leuven, Belgium
gokulnat002@e.ntu.edu.sg prasanna.ravi@ntu.edu.sg
janpieter.danvers@esat.kuleuven.be sbhasin@ntu.edu.sg anupam@ntu.edu.sg

Abstract. In this work, we propose generic and novel adaptations to the binary Plaintext-Checking (PC) oracle based side-channel attacks for Kyber KEM. Binary PC oracle-based side-channel attacks are fairly generic and easy to mount on a given target, as the attacker requires very minimal information about the target device. However, these attacks have an inherent disadvantage of requiring a few thousand traces to perform full key recovery, as they only recover a single bit of information per trace. We propose novel *parallel PC oracle* based side-channel attacks, which are capable of recovering an arbitrary P number of bits of information about the secret key in a single trace. We experimentally validated our attacks on

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Et tu, Brute? Side-Channel Assisted Chosen Ciphertext Attacks Using Valid Ciphertexts on HQC KEM

Thales B. Paiva
Prasanna Ravi
Dirmanto Jap
Shivam Bhasin
***Sayan Das** **
Anupam Chattopadhyay

FIPS 140-3 Security Level of Certification

- The requirement includes the previous level
  - From level 2, authentication is required
  - From level 3, side channel countermeasure is required

Certification Security Level	Requirement
1	All components must be production-grade
2	Physical tamper-evidence, role-based authentication
3	Identity-based authentication, physical or logical separation, side channel countermeasure
4	Multi-factor authentication, invasive environmental protection

謝謝

TEAM CYBERSECURITY