NTNU | Norwegian University of Science and Technology

Privacy-Enhancing Cryptography from Lattices

Tjerand Silde @ PrivCrypt 2025

Introduction

Associate Professor in Cryptology

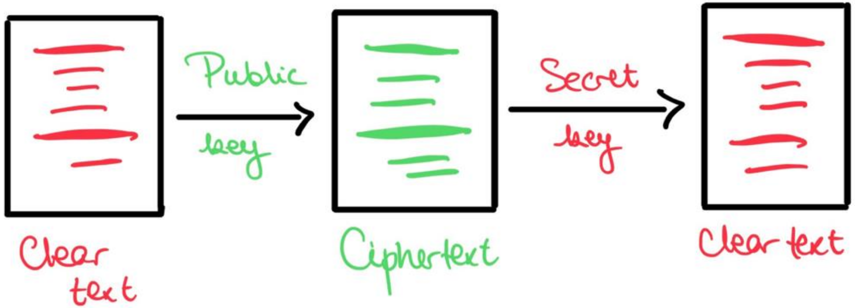
Department of Information Security and Communication Technology at NTNU

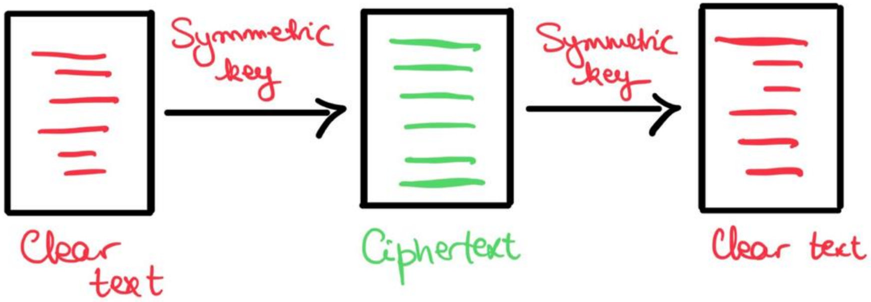
Lead the NTNU Applied Cryptology Lab

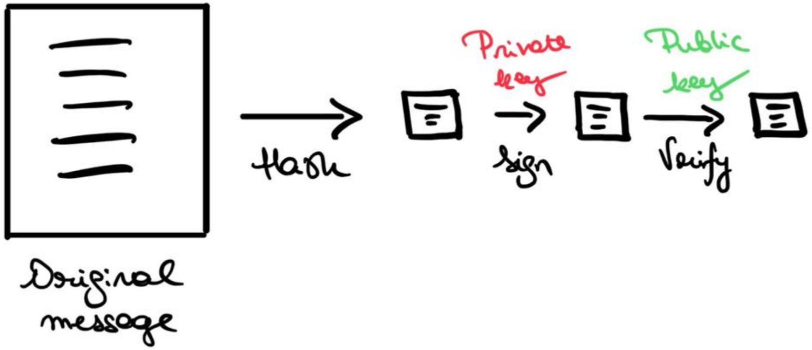
Quantum-safe cryptography and privacy

Part-time position at PONE Biometrics

Cryptography Today





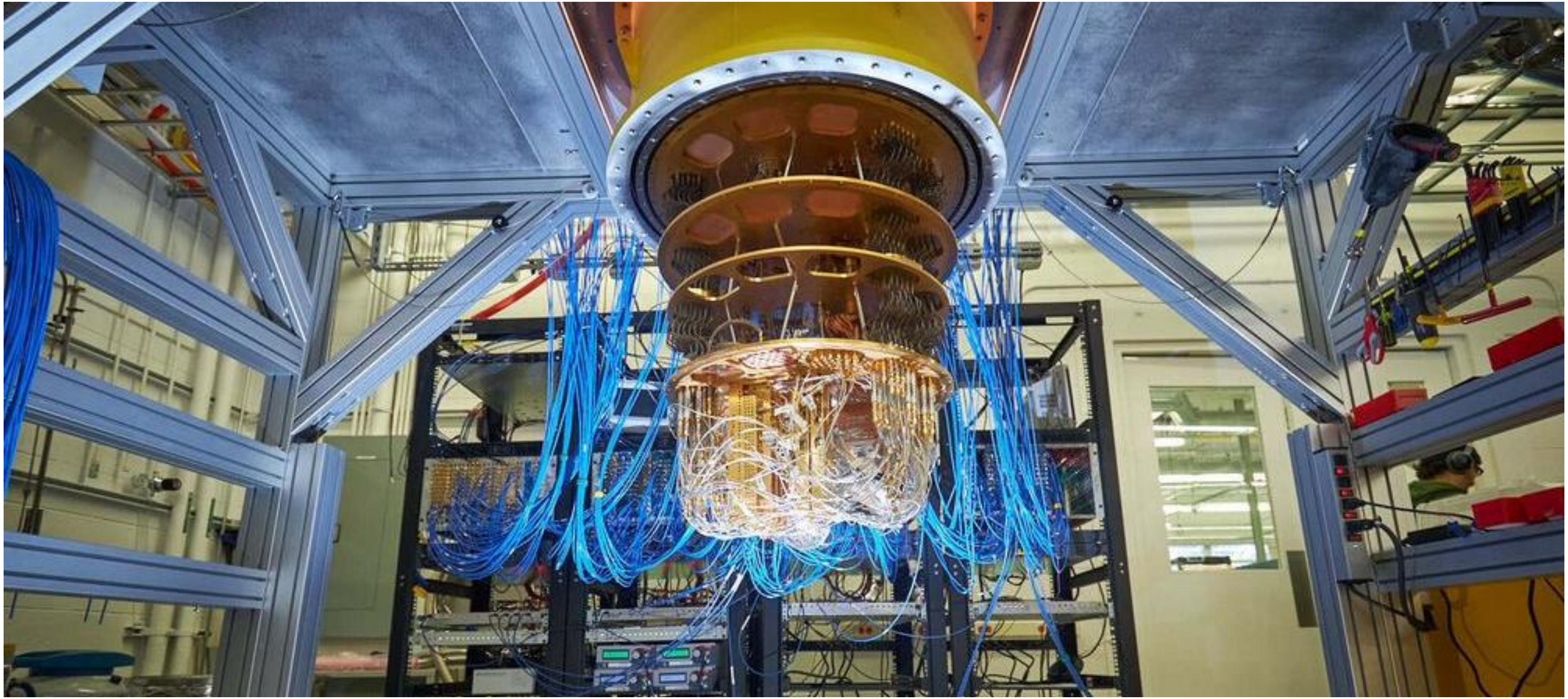


Cryptography Today

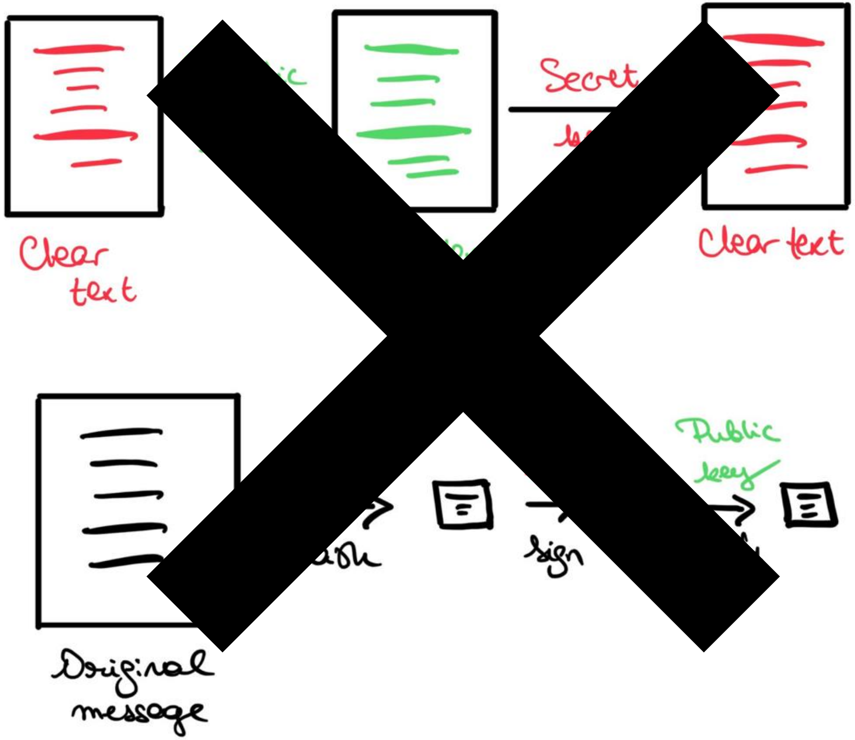
Secure messaging:	Signal, WhatsApp, iMessage,…
Secure connections:	TLS, SSH, IPsec,…
Digital authentication:	FIDO, Digital ID, EU Wallet,…
Payments:	PayPal, VISA / Mastercard, Bitcoin, Apple / Google Pay, Venmo,…

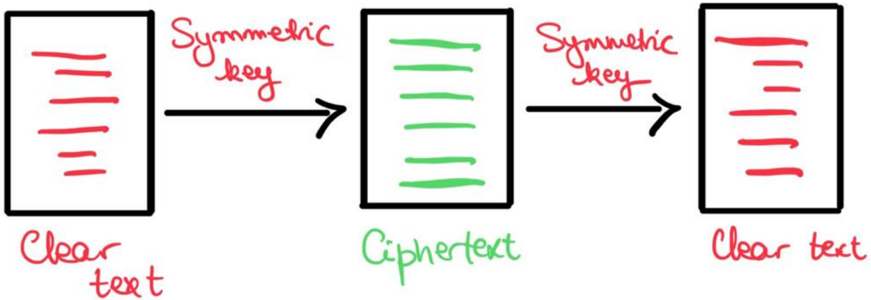
Will these protocols be secure in the future?

Quantum Computers



Cryptography Tomorrow





The Quantum Threat

Quantum computers are not better; they are different

They will generally be worse, but do specific things better

In theory, they can break public key encryption and digital signatures based on factoring and discrete log assumptions

There are many recent developments in quantum computing

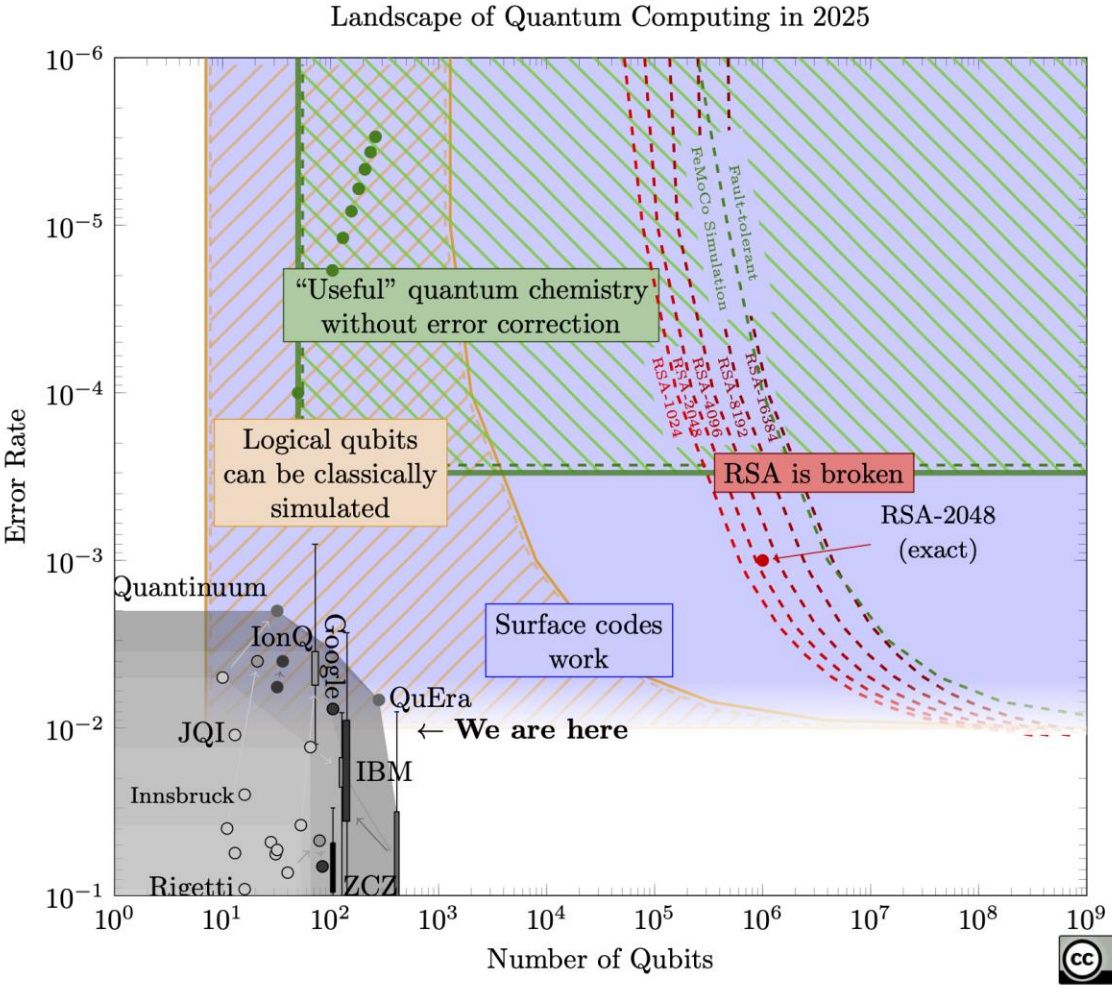
How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.



sam-jaques.appspot.com/quantum_landscape_2025

Quantum-Safe Cryptography

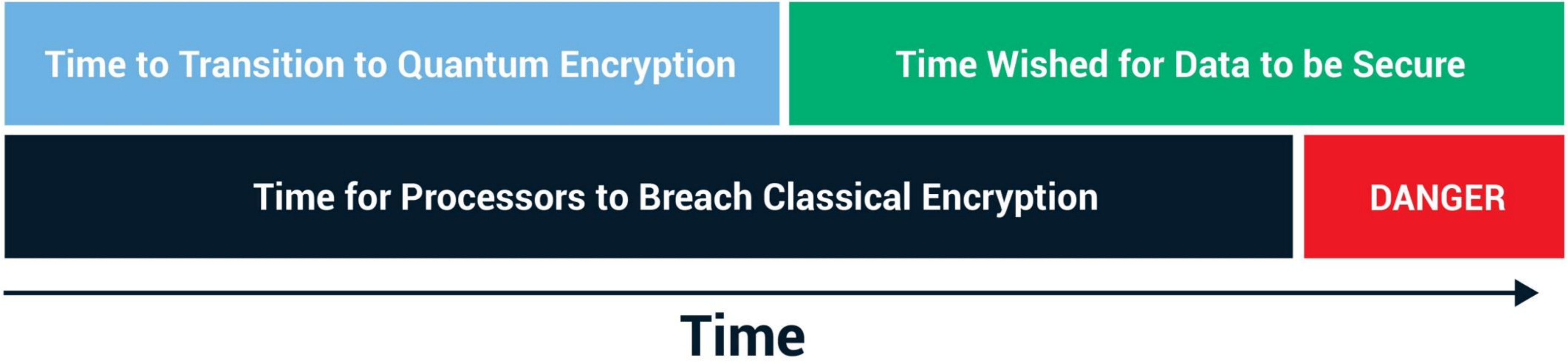
Cryptography that runs on classical computers, but
is secure against attacks from quantum computers

Cryptographers have been working on this since ~2000

We have recently standardized several algorithms

There are tradeoffs in choosing which algorithms to use

Urgency: Mosca's Inequality



Don't wait - upgrade your encryption now!

Timeline

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1^{st} round candidates

2018 The 1^{st} NIST PQC standardization Conference

2019 Announced 26 2^{nd} round candidates. The 2^{nd} NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021 The 3^{rd} NIST PQC Standardization Conference

2022 Announced the 3^{rd} round selection and the 4^{th} round candidates, the 4^{th} NIST PQC conference

2023 Released draft standards for public comments

2024 5^{th} NIST PQC standardization conference (April 10-12)

2024 Publication of FIPS 203, 204, 205

2025 Released draft **FIPS 206** for public comments and 4^{th} round selection

2022 Called for additional signatures

2023 Received 50 signature submissions and 40 of them were selected as the first- round candidates

2024 Announced 14 candidates as the second-round additional signatures for PQC process

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Basic Lattice Cryptography

The concepts behind Kyber (ML-KEM) and Dilithium (ML-DSA)

Vadim Lyubashevsky

IBM Research Europe, Zurich

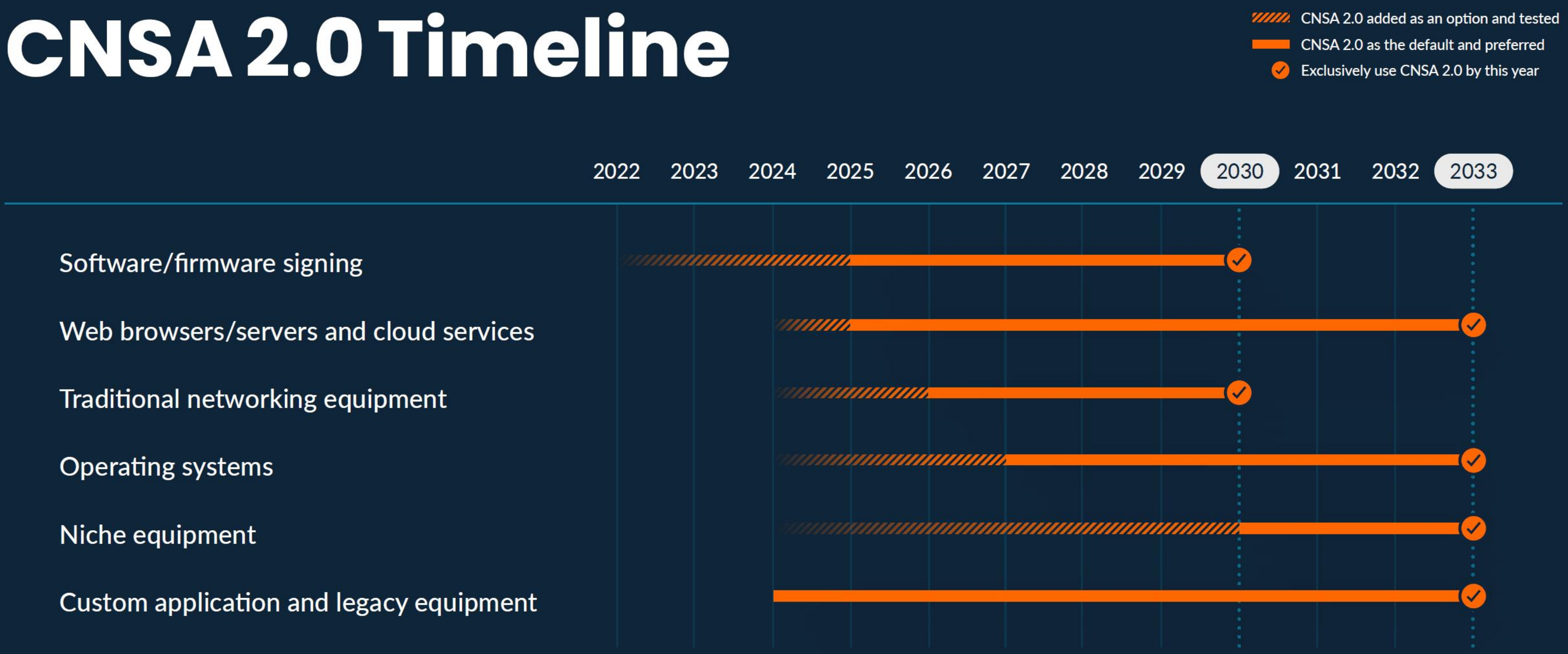
vad@zurich.ibm.com

NTNU | Norwegian University of Science and Technology

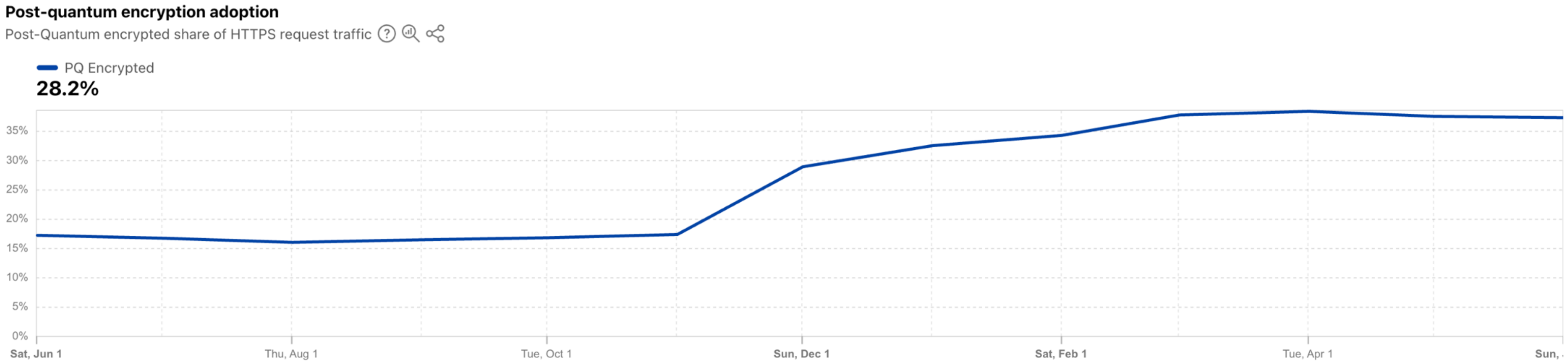
NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

CNSA 2.0 Timeline



Google Chrome + Cloudflare servers



LATTICES

Lattice Assumptions

Three main lattice assumptions: SIS, LWE, and NTRU

Have shown to be very expressive and quantum-secure

Hard to set parameters for correctness and security

Short Integer Solution

Definition 4 (MSIS [**LS15**]). *Let k, ℓ be positive integers and $0 < \eta \ll q$. Then, given $\mathbf{A} \leftarrow R_q^{k\times\ell}$, the Module-SIS problem asks an adversary $\mathcal{A}$ to find $\mathbf{z} \in R_q^{\ell}$ such that $\mathbf{Az} = \mathbf{0}$ and $0 < \|\mathbf{z}\|_2 \leq \eta$. $\mathcal{A}$ is said to have advantage ϵ_{MSIS} in solving $\mathsf{MSIS}_{k,\ell,\eta}$ if*

$$\Pr\left[0 < \|\mathbf{z}\|_2 \leq \eta \wedge \mathbf{Az} = \mathbf{0} \mid \mathbf{A} \leftarrow R_q^{k\times\ell}; \mathbf{z} \leftarrow \mathcal{A}(\mathbf{A})\right] \geq \epsilon_{\mathsf{MSIS}}.$$

Learning With Errors

Definition 5 (MLWE [**LS15**]). *Let k, ℓ be positive integers, and χ be a probability distribution over R_q. The Module-LWE problem then asks an adversary $\mathcal{A}$ to distinguish between the following two cases:*

1. $(\mathbf{A}, \mathbf{A}\mathbf{s})$ *for public* $\mathbf{A} \leftarrow R_q^{k\times(\ell+k)}$ *and secret* $\mathbf{s} \leftarrow \chi^{\ell+k}$,
2. $(\mathbf{A}, \mathbf{b}) \leftarrow R_q^{k\times(\ell+k)} \times R_q^k$ *where both are sampled uniformly.*

Then $\mathcal{A}$ is said to have advantage ϵ_{MLWE} in solving $\mathsf{MLWE}_{k,\ell,\chi}$ if

$$\Big| \Pr\left[b = 1 \mid \mathbf{A} \leftarrow R_q^{k\times(\ell+k)}; \mathbf{s} \leftarrow \chi^{\ell+k}; b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{A}\mathbf{s})\right] - \Pr\left[b = 1 \mid \mathbf{A} \leftarrow R_q^{k\times(\ell+k)}; \mathbf{b} \leftarrow R_q^k; b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{b})\right] \Big| \geq \epsilon_{\mathsf{MLWE}}.$$

NTRU

Definition 3 (MNTRU [CPS+20]). *Let n, m be positive integers, $\sigma_{\mathsf{NTRU}} \in \mathbb{R}$, and $D_{\sigma_{\mathsf{NTRU}}}$ a bounded distribution over R_q. The Module-NTRU problem then asks an adversary $\mathcal{A}$ to distinguish between the following two cases:*

0. $\mathbf{F}^{-1}\mathbf{G} \in R_q^{n\times m}$ *for secret* $(\mathbf{F}, \mathbf{G}) \leftarrow D_{\sigma_{\mathsf{NTRU}}}^{n\times n} \times D_{\sigma_{\mathsf{NTRU}}}^{n\times m}$,
1. $\mathbf{H} \in R_q^{n\times m}$ *for uniformly sampled* $\mathbf{H} \xleftarrow{\$} R_q^{n\times m}$.

Then $\mathcal{A}$ is said to have advantage ϵ in solving $\mathsf{MNTRU}_{n,m,\sigma_{\mathsf{NTRU}}}$ *if*

$$\Big| \Pr\left[b = 1 \mid (\mathbf{F}, \mathbf{G}) \leftarrow D_{\sigma_{\mathsf{NTRU}}}^{n\times n} \times D_{\sigma_{\mathsf{NTRU}}}^{n\times m} \; ; \; b \leftarrow \mathcal{A}(\mathbf{F}^{-1}\mathbf{G})\right] - \Pr\left[b = 1 \mid \mathbf{H} \xleftarrow{\$} R_q^{n\times m} \; ; \; b \leftarrow \mathcal{A}(\mathbf{H})\right] \Big| \geq \epsilon.$$

Lattice Estimator

Security Estimates for Lattice Problems

launch binder docs passing

This Sage module provides functions for estimating the concrete security of Learning with Errors instances.

The main purpose of this estimator is to give designers an easy way to choose parameters resisting known attacks and to enable cryptanalysts to compare their results and ideas with other techniques known in the literature.

Quick Start

We currently provide evaluators for the security of the LWE, NTRU, and SIS problems. Our estimator integrates simulators for the best known attacks against these problems, and provides bit-security estimates relying on heuristics to predict the cost and shape of lattice reduction algorithms. The default models are configured in conf.py.

Challenges with Lattices

Masking is complicated since secrets have short norms

- Must use rejection sampling or noise drowning

There exist efficient trapdoors for lattices

- Must prove that an instance is generated honestly

Homomorphic operations and challenges impact norms

- Must use specialized techniques to deal with this

Signatures from ZKPs: ML-DSA

<u>Gen</u>

$\mathbf{A} \leftarrow R_q^{k \times \ell}$
$(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$
$\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$
$\textbf{return } (pk = (\mathbf{A}, \mathbf{t}), sk = (\mathbf{A}, \mathbf{t}, \mathbf{s}_1, \mathbf{s}_2))$

<u>Sign(sk, M)</u>

$\mathbf{z} := \perp$
$\textbf{while } \mathbf{z} = \perp \text{ do}$
$\quad \mathbf{y} \leftarrow S_{\gamma_1 - 1}^\ell$
$\quad \mathbf{w}_1 := \mathsf{HighBits}(\mathbf{A}\mathbf{y}, 2\gamma_2)$
$\quad c \in B_\tau := \mathsf{H}(M \parallel \mathbf{w}_1)$
$\quad \mathbf{z} := \mathbf{y} + c\mathbf{s}_1$
$\quad \textbf{if } \|\mathbf{z}\|_\infty \geq \gamma_1 - \beta \text{ or } \|\mathsf{LowBits}(\mathbf{A}\mathbf{y} - c\mathbf{s}_2, 2\gamma_2)\|_\infty \geq \gamma_2 - \beta, \text{ then } \mathbf{z} := \perp$
$\textbf{return } \sigma = (\mathbf{z}, c)$

<u>Verify$(pk, M, \sigma = (\mathbf{z}, c))$</u>

$\mathbf{w}_1' := \mathsf{HighBits}(\mathbf{A}\mathbf{z} - c\mathbf{t}, 2\gamma_2)$
$\textbf{if return } [\![\|\mathbf{z}\|_\infty < \gamma_1 - \beta]\!] \textbf{ and } [\![c = \mathsf{H}(M \parallel \mathbf{w}_1')]\!]$

Hint Module Learning With Errors

Definition 2 (H-MLWE [**KLSS23**]). *Let k, ℓ, Q be positive integers, χ_1 and χ_2 be probability distributions over R_q, and $\mathcal{C}$ be a subset of R_q. The Hint-MLWE problem* $\mathsf{H\text{-}MLWE}_{k,\ell,\chi_1,\chi_2,Q}$ *then asks an adversary $\mathcal{A}$ to distinguish between the following two cases:*

1. $(\mathbf{A}, \mathbf{As}, (c_i, \mathbf{z}_i)_{i\in[Q]})$ *for* $\mathbf{A} \leftarrow R_q^{k\times(\ell+k)}$,
2. $(\mathbf{A}, \mathbf{b}, (c_i, \mathbf{z}_i)_{i\in[Q]})$ *for* $\mathbf{A} \leftarrow R_q^{k\times(\ell+k)}$, $\mathbf{b} \leftarrow R_q^k$,

where $\mathbf{s} \leftarrow \chi_1^{\ell+k}$, $c_i \leftarrow \mathcal{C}$ *for* $i \in [Q]$, *and* $\mathbf{z}_i := c_i \cdot \mathbf{s} + \mathbf{y}_i$ *where* $\mathbf{y}_i \leftarrow \chi_2^{\ell+k}$ *for* $i \in [Q]$. *We denote by* $\epsilon_{\mathsf{H\text{-}MLWE}}$ *the advantage of* $\mathcal{A}$ *in solving* $\mathsf{H\text{-}MLWE}_{k,\ell,\chi_1,\chi_2,Q}$.

$\mathcal{A}$ *has advantage* $\epsilon_{\mathsf{H\text{-}MLWE}}$ *in solving* $\mathsf{H\text{-}MLWE}_{k,\ell,\chi_1,\chi_2,Q}$ *if*

$$\left| \Pr\left[b = 1 \;\middle|\; \begin{array}{c} \mathbf{A} \leftarrow R_q^{k\times(\ell+k)}; \mathbf{s} \leftarrow \chi_1^{\ell+k}; c_i \leftarrow \mathcal{C}; \\ \mathbf{y}_i \leftarrow \chi_2^{\ell+k}; z_i := c_i\mathbf{s} + \mathbf{y}_i \text{ for } i \in [Q]; \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{As}, (c_i, \mathbf{z}_i)_{i\in[Q]}) \end{array} \right] - \Pr\left[b = 1 \;\middle|\; \begin{array}{c} \mathbf{A} \leftarrow R_q^{k\times(\ell+k)}; \mathbf{b} \leftarrow R_q^k; \\ \mathbf{s} \leftarrow \chi_1^{\ell+k}; c_i \leftarrow \mathcal{C}; \mathbf{y}_i \leftarrow \chi_2^{\ell+k} \\ z_i := c_i\mathbf{s} + \mathbf{y}_i \text{ for } i \in [Q]; \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{b}) \end{array} \right] \right| \geq \epsilon_{\mathsf{MLWE}}.$$

Signatures from HMLE: Raccoon

Alg. 1: $\mathsf{KeyGen}(1^\kappa)$

$\mathbf{A} \leftarrow \mathcal{R}_q^{k\times\ell}$ ▷ Uniform matrix
$(\mathbf{s}, \mathbf{e}) \leftarrow \mathcal{D}_{\mathbf{t}}^{\ell} \times \mathcal{D}_{\mathbf{t}}^{k}$ ▷ Small secret and noise
$\mathbf{t} := \lfloor \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \rceil_{\nu_{\mathbf{t}}}$ ▷ Part of public key in $\mathcal{R}_{q_{\mathbf{t}}}^{k}$
return $\mathsf{vk} := (\mathbf{A}, \mathbf{t})$, $\mathsf{sk} := \mathbf{s}$

Alg. 2: $\mathsf{Sign}(\mathsf{vk}, \mathsf{sk}, \mathsf{msg})$

$(\mathbf{r}, \mathbf{e}') \leftarrow \mathcal{D}_{\mathbf{w}}^{\ell} \times \mathcal{D}_{\mathbf{w}}^{k}$ ▷ Small randomness and noise
$\mathbf{w} := \lfloor \mathbf{A} \cdot \mathbf{r} + \mathbf{e}' \rceil_{\nu_{\mathbf{w}}}$ ▷ (Rounded) commitment in $\mathcal{R}_{q_{\mathbf{w}}}^{k}$
$c := \mathsf{H}_c(\mathsf{vk}, \mathsf{msg}, \mathbf{w})$ ▷ Challenge
$\mathbf{z} := c \cdot \mathbf{s} + \mathbf{r}$ ▷ Response in $\mathcal{R}_q^{\ell}$
$\mathbf{y} := \lfloor \mathbf{A} \cdot \mathbf{z} - 2^{\nu_{\mathbf{t}}} \cdot c \cdot \mathbf{t} \rceil_{\nu_{\mathbf{w}}}$ ▷ Intermediate value in $\mathcal{R}_{q_{\mathbf{w}}}^{k}$
$\mathbf{h} := \mathbf{w} - \mathbf{y}$ ▷ Hint in $\mathcal{R}_{q_{\mathbf{w}}}^{k}$
return $\sigma := (c, \mathbf{z}, \mathbf{h})$

Alg. 3: $\mathsf{Verify}(\mathsf{vk}, \mathsf{msg}, \sigma)$

$(c, \mathbf{z}, \mathbf{h}) := \mathsf{parse}(\sigma)$
$c' := \mathsf{H}_c(\mathsf{vk}, \mathsf{msg}, \lfloor \mathbf{A} \cdot \mathbf{z} - 2^{\nu_{\mathbf{t}}} \cdot c \cdot \mathbf{t} \rceil_{\nu_{\mathbf{w}}} + \mathbf{h})$
if $\{c = c'\}$ **and** $\{\|(\mathbf{z}, 2^{\nu_{\mathbf{w}}} \cdot \mathbf{h})\|_2 \leq B_2\}$ **then**
  return 1
return 0

PEC FROM LATTICES

Categories of Quantum-Safe Crypto

No changes necessary:	AES, SHA-2/3, HMAC, …
Almost drop-in replacements:	PKE, KEM, DSA
More advanced primitives:	**Privacy-Enhancing Crypto** (and some other categories)
Only from lattices:	FHE and Obfuscation

Zero-Knowledge Proofs

Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General*

Vadim Lyubashevsky[1], Ngoc Khanh Nguyen[1,2], and Maxime Plançon[1,2]

[1] IBM Research Europe, Zurich
[2] ETH Zurich, Zurich

Exact proof of As+e and short s and e in ~14 KB

Group and Ring Signatures

BLOOM: Bimodal Lattice One-Out-of-Many Proofs and Applications

Vadim Lyubashevsky[1] and Ngoc Khanh Nguyen[2]

[1] IBM Research Europe, Zurich
[2] EPFL, Lausanne

Signatures or size ~15-20 KB for 2^20 users

Private Transactions

MatRiCT^{+}: More Efficient Post-Quantum Private Blockchain Payments

Muhammed F. Esgin
Monash University and *CSIRO's Data61*
Australia
muhammed.esgin@monash.edu

Ron Steinfeld
Monash University
Australia
ron.steinfeld@monash.edu

Raymond K. Zhao
Monash University
Australia
raymond.zhao@monash.edu

Private transactions using ZKP at ~40 KB

Blind Signatures

Lattice-Based Blind Signatures: Short, Efficient, and Round-Optimal

Ward Beullens
IBM Research Europe - Zurich
Switzerland

Vadim Lyubashevsky
IBM Research Europe - Zurich
Switzerland

Ngoc Khanh Nguyen
EPFL
Switzerland

Gregor Seiler
IBM Research Europe - Zurich
Switzerland

Signatures of ~22 KB and communication of ~60 KB

Must prove the evaluation of a RO in ZKP

Blind Signatures

Non-interactive Blind Signatures: Post-quantum and Stronger Security*

Foteini Baldimtsi
George Mason University†

Jiaqi Cheng
UW–Madison§

Rishab Goyal
UW–Madison‡

Aayush Yadav
George Mason University¶

Signatures of ~68 KB and communication of ~1 KB

Electronic Voting

Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions*

Diego F. Aranha
dfaranha@cs.au.dk
Aarhus University
Aarhus, Denmark

Carsten Baum
cabau@dtu.dk
DTU Compute
Copenhagen, Denmark

Kristian Gjøsteen
kristian.gjosteen@ntnu.no
Norwegian University of Science and Technology
Trondheim, Norway

Tjerand Silde[†]
tjerand.silde@ntnu.no
Norwegian University of Science and Technology
Trondheim, Norway

Ciphertexts of 80 KB, shuffle 290 KB, decryption 157 KB

Electronic Voting

More Efficient Lattice-Based Electronic Voting from NTRU

Patrick Hough[a,1], Caroline Sandsbråten[2] and Tjerand Silde[2]

[1] University of Oxford, Mathematical Institute, Oxford, United Kingdom
[2] Norwegian University of Science and Technology, Department of Information Security and Communication Technology, Trondheim, Norway

Ciphertexts of 15 KB, shuffle 115 KB, decryption 85 KB

Electronic Voting

Efficient Verifiable Mixnets from Lattices, Revisited

Jonathan Bootle[1], Vadim Lyubashevsky[1], and Antonio Merino-Gallardo[1,2*]

[1] IBM Research Europe, Zurich, Switzerland
{jbt,vad}@zurich.ibm.com
[2] Hasso-Plattner-Institute, University of Potsdam, Potsdam, Germany
antonio@m-g.es

Ciphertexts of ~6.5 KB, shuffle + decryption of 110 KB

Private Set Intersection

LEAP: A Fast, Lattice-based OPRF With Application to Private Set Intersection*

Lena Heimberger[1] [0009-0001-9404-7699], Daniel Kales[2] [0000-0001-9541-9792], Riccardo Lolato[3**] [0009-0000-2356-339X], Omid Mir[4], Sebastian Ramacher[4] [0000-0003-1957-3725], and Christian Rechberger[1,2] [0000-0003-1280-6020]

Communication of ~23 KB per item

6 rounds and semi-honest

(zk-)SNARKs

LaBRADOR: Compact Proofs for R1CS from Module-SIS*

Ward Beullens and Gregor Seiler

IBM Research Europe

Proofs of ~60-100 KB for essentially any (lattice) statement

Linear time verification and high-memory cost

Anonymous Credentials

A Framework for Practical Anonymous Credentials from Lattices

Jonathan Bootle
jbt@zurich.ibm.com
IBM Research Europe - Zurich, Switzerland

Vadim Lyubashevsky
vad@zurich.ibm.com
IBM Research Europe - Zurich, Switzerland

Ngoc Khanh Nguyen
khanh.nguyen@epfl.ch
EPFL, Switzerland

Alessandro Sorniotti
aso@zurich.ibm.com
IBM Research Europe - Zurich, Switzerland

Credentials of ~30-130 KB for 16 attributes

Ad-hoc lattice assumptions

Open-Source Implementations

The LaZer Library: Lattice-Based Zero Knowledge and Succinct Proofs for Quantum-Safe Privacy

Vadim Lyubashevsky
IBM Research Europe
Zurich, Switzerland
vad@zurich.ibm.com

Gregor Seiler
IBM Research Europe
Zurich, Switzerland
gseiler@posteo.net

Patrick Steuer
IBM Research Europe
Zurich, Switzerland
ick@zurich.ibm.com

Important step towards practical lattice implementations

Still new and has bugs and restrictions

OPEN PROBLEMS

GENERIC VS SPECIALIZED METHODS

Generic vs Specialized Methods

Most approaches are based on what we do from DLOG

Generic transforms or frameworks are great, but limited

Often needs more specialized methods to gain efficiency

SPECIALIZED LATTICE ASSUMPTIONS

Two-Round Threshold Signature from Algebraic One-More Learning with Errors

Thomas Espitau[1], Shuichi Katsumata[1,2], Kaoru Takemure* [1,2]

[1]PQShield

{thomas.espitau, shuichi.katsumata, kaoru.takemure}@pqshield.com

[2]AIST

NTNU | Norwegian University of Science and Technology

The Algebraic One-More MISIS Problem and Applications to Threshold Signatures

Chenzhi Zhu and Stefano Tessaro

Paul G. Allen School of Computer Science & Engineering
University of Washington, Seattle, US
{zhucz20,tessaro}@cs.washington.edu

malb.io

SIS with Hints Zoo

An attempt to keep track of all those new SIS-like assumptions that hand out additional hints. Some of these venture into LWE land, but for now I want to keep it more or less SIS focused.

- **Designers**: Please consider whether you can re-use one of those many newfangled assumptions before introducing yet another one.
- **Cryptanalysts**: Analyse them!

malb.io/sis-with-hints.html

Hollow LWE: A New Spin

Unbounded Updatable Encryption from LWE and PCE

Martin R. Albrecht[1⋆], Benjamin Benčina[2⋆⋆], and Russell W. F. Lai[3⋆⋆⋆]

[1] King's College London and SandboxAQ
martin.albrecht@{kcl.ac.uk,sandboxaq.com}
[2] Royal Holloway, University of London
benjamin.bencina.2022@live.rhul.ac.uk
[3] Aalto University
russell.lai@aalto.fi

OPEN-SOURCE IMPLEMENTATIONS

Open-Source Implementations

The ML-KEM and ML-DSA code bases are really great

We have several FHE libraries for lattice cryptography

LaZeR is the only library for lattice-based zero-knowledge

Most papers, if there is an implementation at all, are usually ad-hoc adaptations of number theory libraries

NTNU | Norwegian University of Science and Technology

Thanks! Questions?

tjerand.silde@ntnu.no
https://tjerandsilde.no