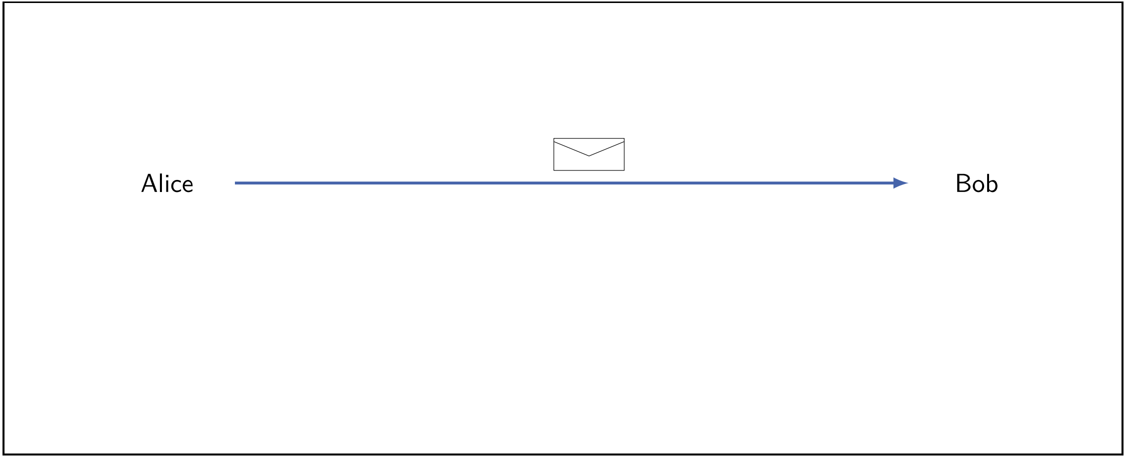
Costing Adversaries on Quantum-secure Cryptography

A Dissertation Talk

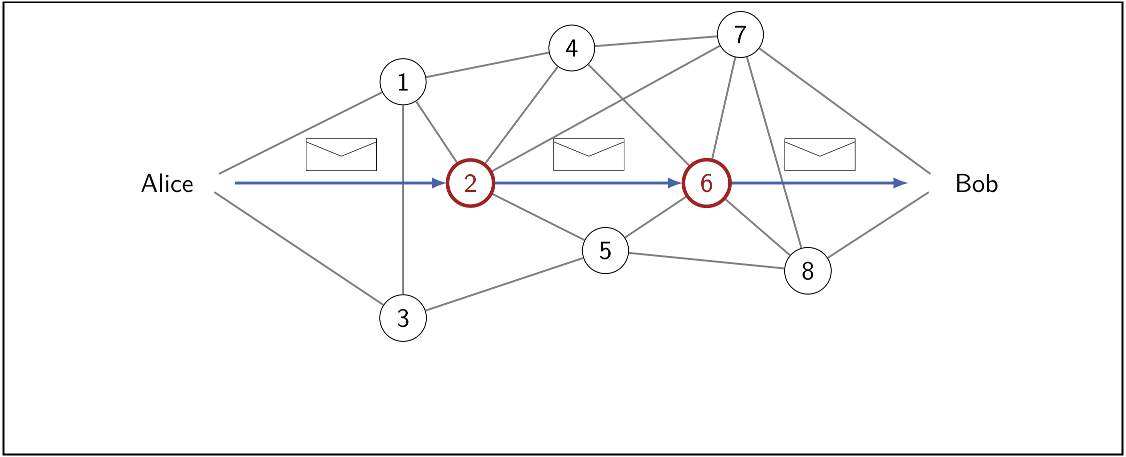
Marcel Tiepelt | January 23rd, 2025

Reviewers Jörn Müller-Quade
Douglas Stebila
Daniel Loebenberger

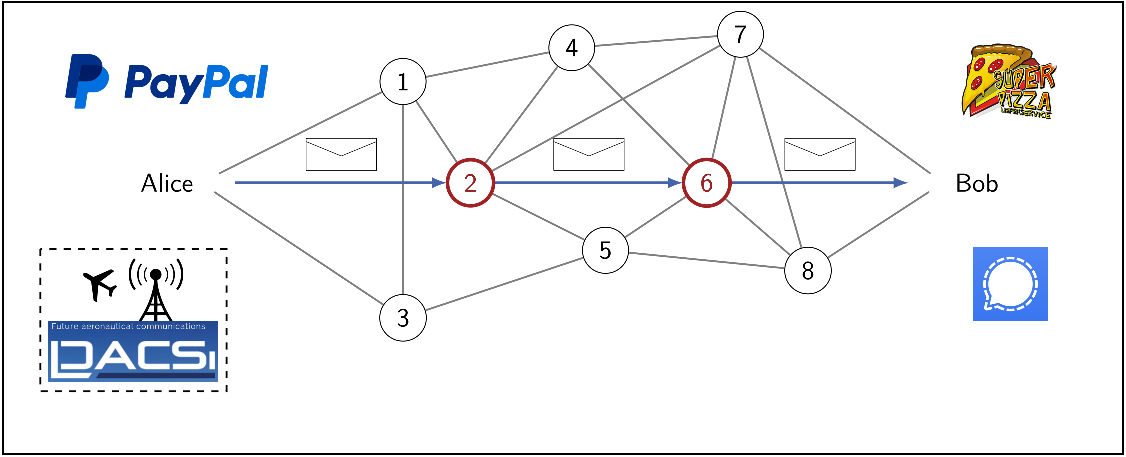
The Internet



The Internet



The Internet



The Internet

Use of encryption

> 90% of internet traffic[1]

> 95% of websites on Google[2]

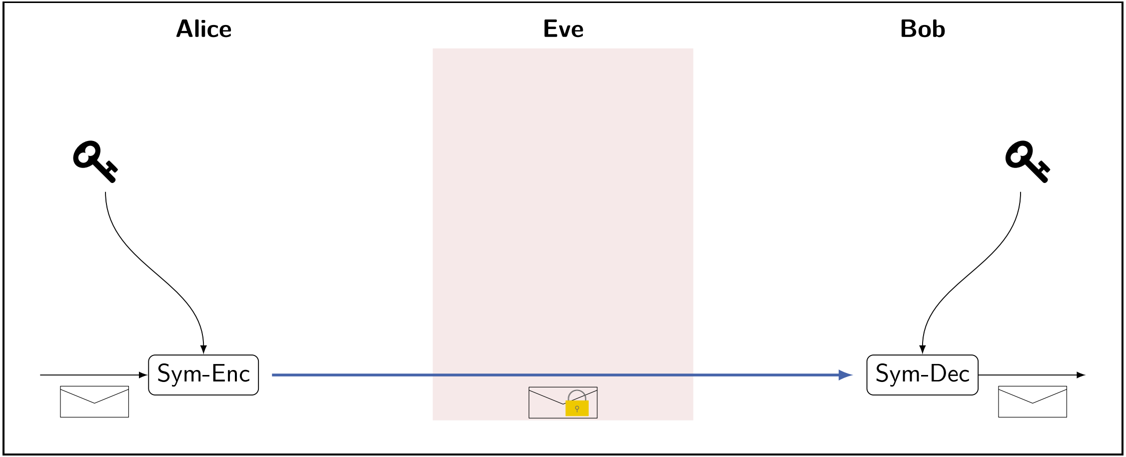
> 99% of browsing time on Google Chrome[3]

[1] Lee et al., TLS 1.3 in Practice:How TLS 1.3 Contributes to the Internet
[2,3] `https://serpwatch.io/blog/ssl-stats/`

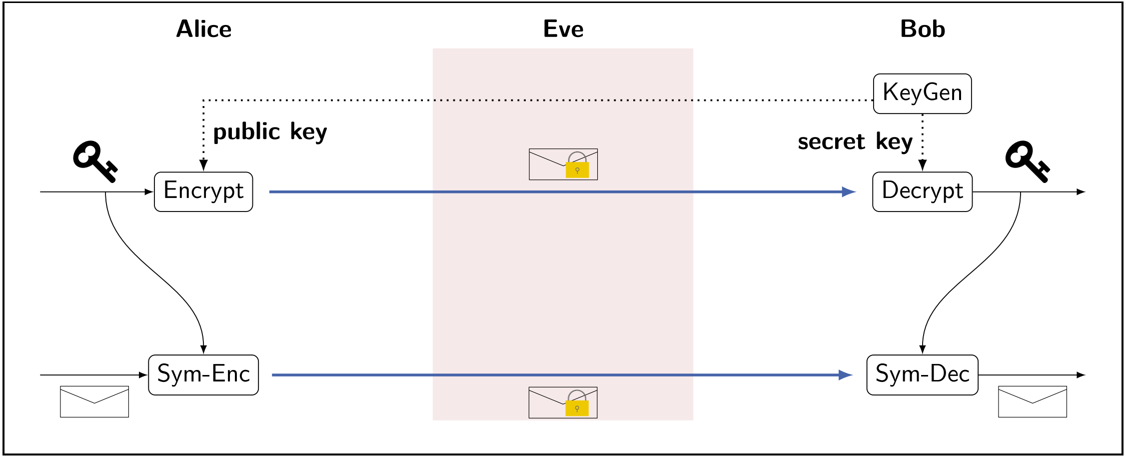
The Internet — simplified

Alice **Eve** **Bob**

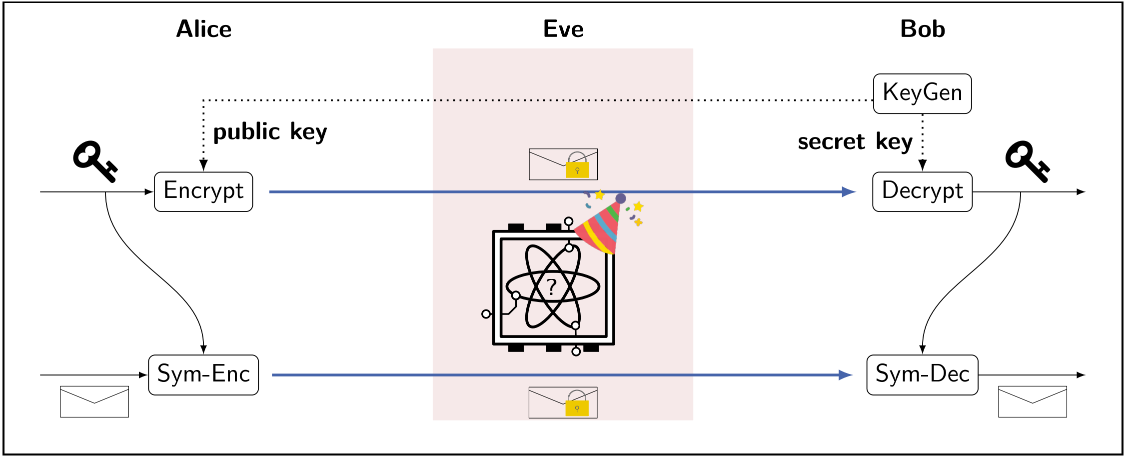
The Internet — simplified



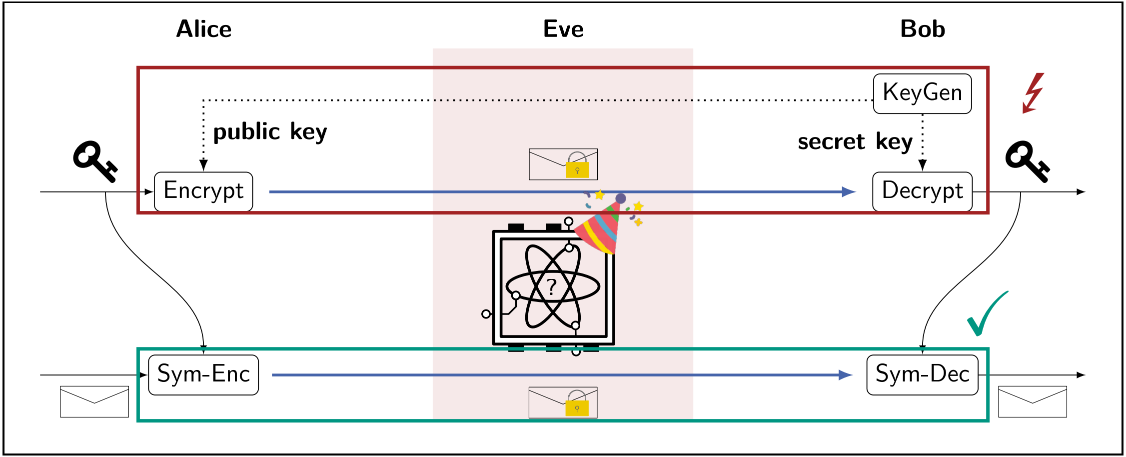
The Internet — simplified



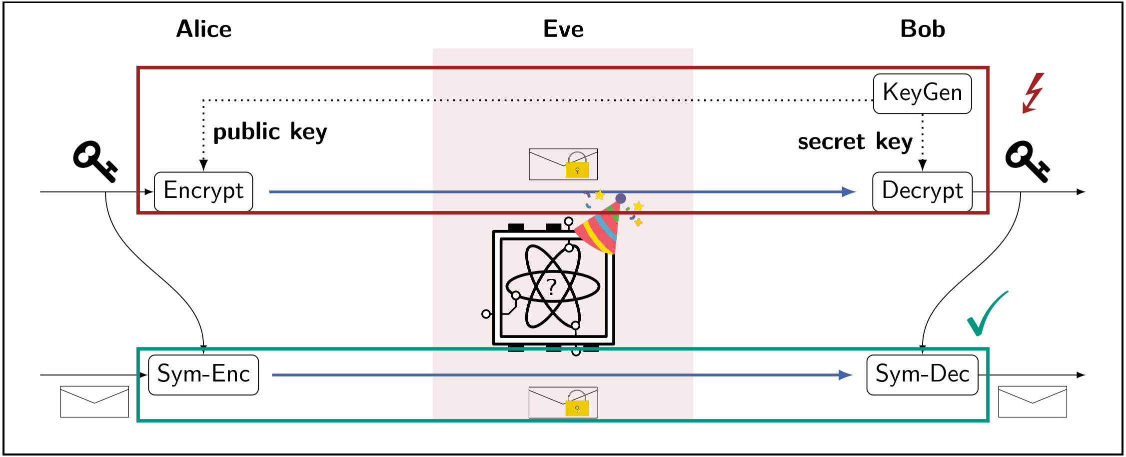
The Internet — simplified



The Internet — simplified



The Internet — simplified



How does quantum computing affect the security of public-key cryptography?

Today's talk

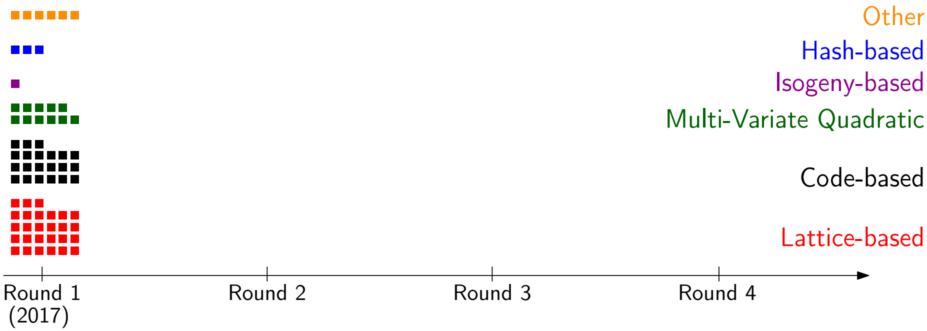
The Internet

I. Advancements in quantum-secure cryptography

II. When is a cryptographic protocol quantum-secure?

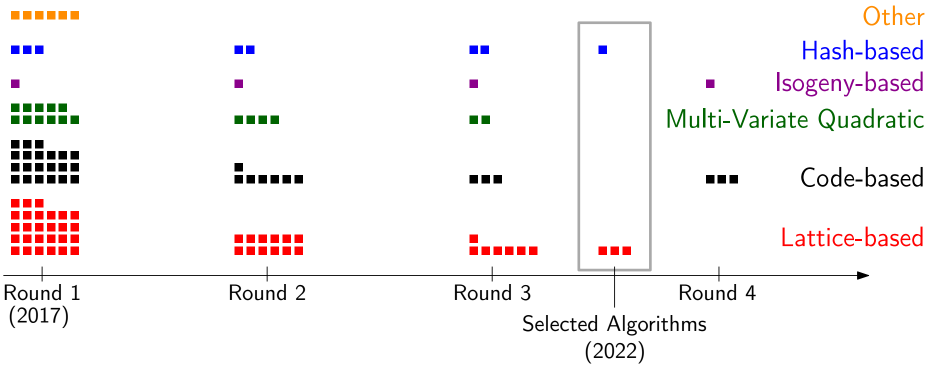
III. The impact of quantum lattice enumeration

NIST post-quantum standardization



Uncertainty in security

NIST post-quantum standardization



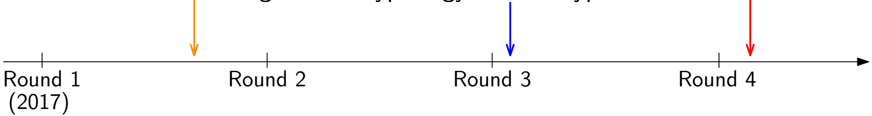
Uncertainty in security $\xrightarrow{\text{public evaluation}}$ *Confidence* in security

Contributions in the thesis: Part I

Exploiting Decryption Failures in Mersenne Number Cryptosystems
PKC at AsiaCCS 2020

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

Forging SPHINCS$^+$-Haraka Signatures on a Fault-Tolerant Quantum Computer
Progress in Cryptology – Latincrypt 2021



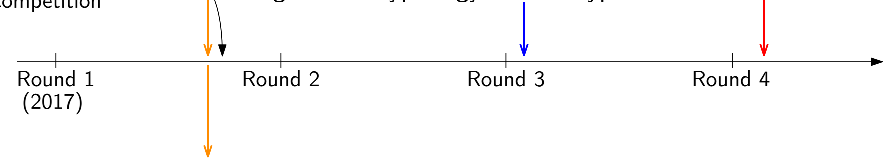
Contributions in the thesis: Part I

Exploiting Decryption Failures in Mersenne Number Cryptosystems
PKC at AsiaCCS 2020

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

Forging SPHINCS$^+$-Haraka Signatures on a Fault-Tolerant Quantum Computer
Progress in Cryptology – Latincrypt 2021

Mersenne-number cryptosystems dropped out of competition



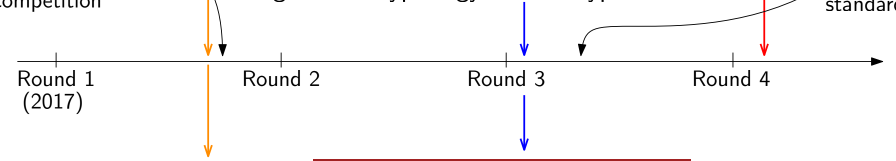
Full security break from decryption failures.

Contributions in the thesis: Part I

Exploiting Decryption Failures in Mersenne Number Cryptosystems
PKC at AsiaCCS 2020

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

Forging SPHINCS$^+$-Haraka Signatures on a Fault-Tolerant Quantum Computer
Progress in Cryptology – Latincrypt 2021



Full security break from decryption failures.

Identify best point of attack and estimate concrete resources.

Contributions in the thesis: Part I

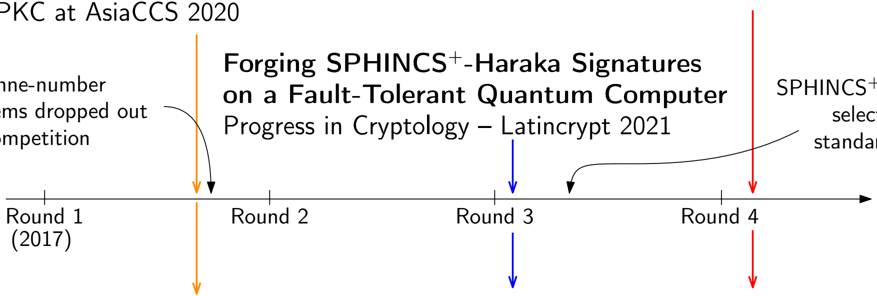
Exploiting Decryption Failures in Mersenne Number Cryptosystems
PKC at AsiaCCS 2020

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

Forging SPHINCS^{+}-Haraka Signatures on a Fault-Tolerant Quantum Computer
Progress in Cryptology – Latincrypt 2021

Mersenne-number cryptosystems dropped out of competition

SPHINCS^{+}-Haraka not selected for standardization



Full security break from decryption failures.

Identify best point of attack and estimate concrete resources.

Lattice-based schemes: Lower bound cost of “best” attack

Contributions in the thesis: Part II

Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements
ESORICS 2023

Post-Quantum Ready Key Agreement for Aviation
Communications in Cryptology 2024

Contributions in the thesis: Part II

Quantum-Annoying: Intermediate security for Password Authenticated Key Exchange

↑

Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements
ESORICS 2023

Post-Quantum Ready Key Agreement for Aviation
Communications in Cryptology 2024

Contributions in the thesis: Part II

Quantum-Annoying: Intermediate security for Password Authenticated Key Exchange

Quantum-secure data-link for civil aviation from NIST post-quantum schemes.

Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements
ESORICS 2023

Post-Quantum Ready Key Agreement for Aviation
Communications in Cryptology 2024

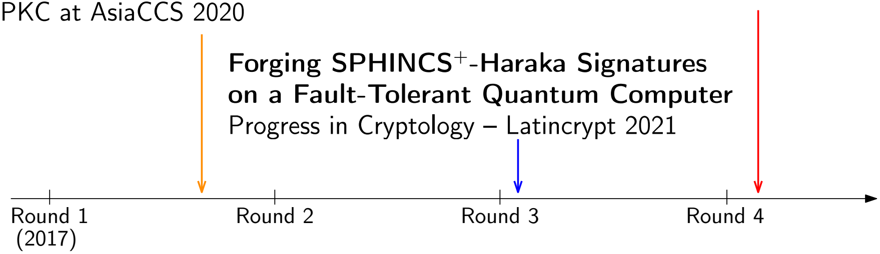
Protocol under standardization by ICAO

Contributions highlighted in this talk

Exploiting Decryption Failures in Mersenne Number Cryptosystems
PKC at AsiaCCS 2020

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

Forging SPHINCS$^+$-Haraka Signatures on a Fault-Tolerant Quantum Computer
Progress in Cryptology – Latincrypt 2021

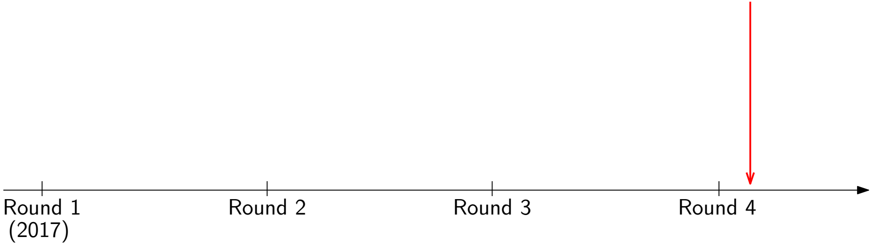


Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements
ESORICS 2023

Post-Quantum Ready Key Agreement for Aviation
Communications in Cryptology 2024

Contributions highlighted in this talk

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

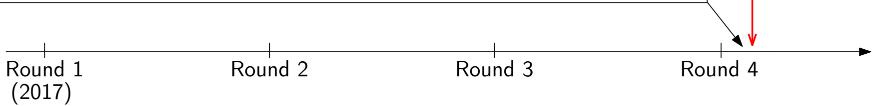


Contributions highlighted in this talk

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

August 2024, Federal Information Processing Standards:

- FIPS 203: Kyber
- FIPS 204: Dilithium

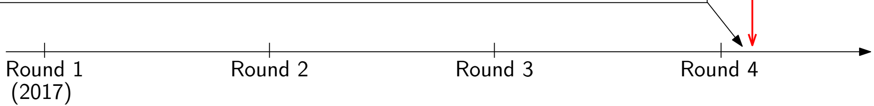


Contributions highlighted in this talk

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

August 2024, Federal Information Processing Standards:

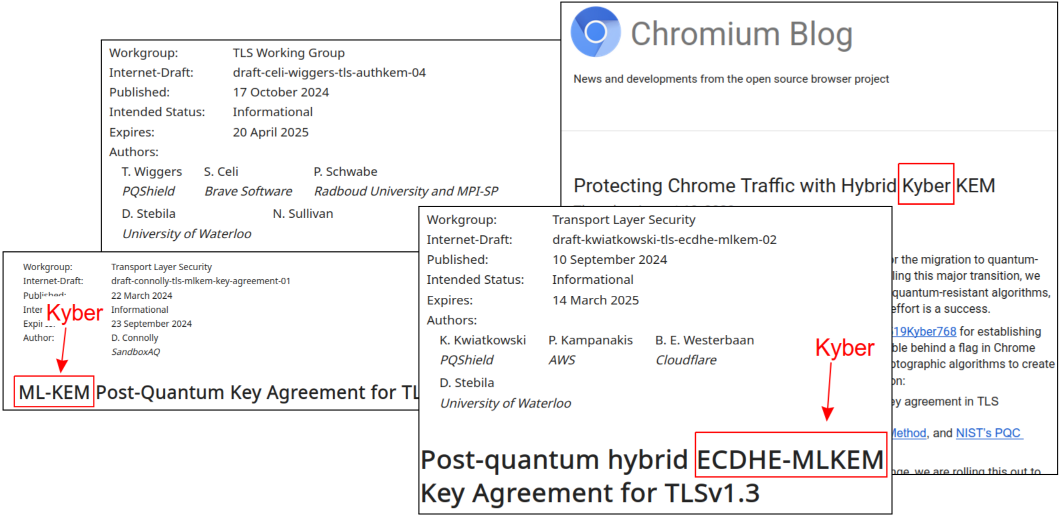
- FIPS 203: Kyber
- FIPS 204: Dilithium



- Goal: Lower bound cost of “best” attack on lattice-based cryptography
- Analysis-Tool[a], Kyber as case study example

[a] available on Github

RFC = technical documentation and development of the internet



Today's talk

The Internet

I. Advancements in quantum-secure cryptography

II. When is a cryptographic protocol quantum-secure?

III. The impact of quantum lattice enumeration

When is a cryptosystem quantum-secure?

1) A cryptosystem is secure, if a certain computational problem is *difficult*.

When is a cryptosystem quantum-secure?

Kyber ↓ Shortest Vector Problem (SVP) ↓

1) A cryptosystem is secure, if a certain computational problem is *difficult*.

When is a cryptosystem quantum-secure?

Kyber → cryptosystem; Shortest Vector Problem (SVP) → computational problem

1) A cryptosystem is secure, if a certain computational problem is *difficult*.

2) Computational problem is believed to be *difficult*, if the best algorithm requires an infeasible amount of resources to solve it.

When is a cryptosystem quantum-secure?

Kyber

Shortest Vector Problem (SVP)

1) A cryptosystem is secure, if a certain computational problem is *difficult*.

2) Computational problem is believed to be *difficult*, if the best algorithm requires an infeasible amount of resources to solve it.

Justification

What is the best algorithm to solve SVP?

What is the best algorithm to solve SVP?

We don't know for sure.

What is the best algorithm to solve SVP?

We don't know for sure.

Lattice-reduction performs significantly better than other known algorithms.

What is the best algorithm to solve SVP?

We don't know for sure.

Lattice-reduction performs significantly better than other known algorithms.

- Leading cost is **enumeration** or sieving[1]

[1] Chailloux et al. 2021 Lattice Sieving via Quantum Random Walks

What is the best algorithm to solve SVP?

We don't know for sure.

Lattice-reduction performs significantly better than other known algorithms.

- Leading cost is **enumeration** or sieving[1]
- Limitation: For quantum enumeration only asymptotic upper bound[2,3] known

[1] Chailloux et al. 2021 Lattice Sieving via Quantum Random Walks
[2] Bai et al. 2023 Concrete Analysis of Quantum Lattice Enumeration
[3] Aono et al. 2018 Quantum Lattice Enumeration and Tweaking Discrete Pruning

What is the best algorithm to solve SVP?

We don't know for sure.

Lattice-reduction performs significantly better than other known algorithms.

- Leading cost is **enumeration** or sieving[1]
- Limitation: For quantum enumeration only asymptotic upper bound[2,3] known

! Concrete cost of quantum enumeration not clear

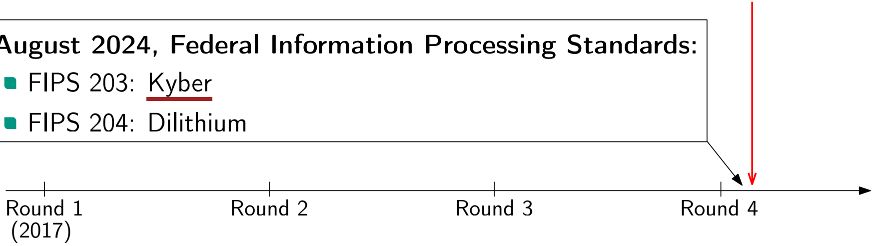
[1] Chailloux et al. 2021 Lattice Sieving via Quantum Random Walks
[2] Bai et al. 2023 Concrete Analysis of Quantum Lattice Enumeration
[3] Aono et al. 2018 Quantum Lattice Enumeration and Tweaking Discrete Pruning

Why analyzing lattice enumeration matters

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

August 2024, Federal Information Processing Standards:

- FIPS 203: Kyber
- FIPS 204: Dilithium

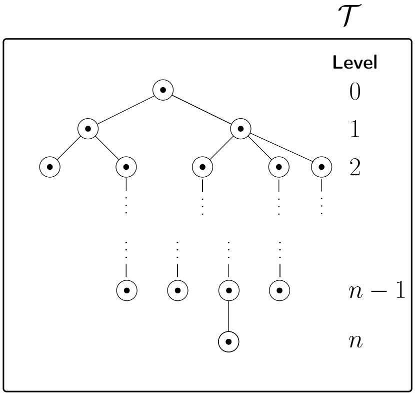


Concrete **security** of cryptographic standards remains **unknown**.

Lattice enumeration algorithm

Classical **enumeration** with extreme pruning[1]

- Search space is *n*-dimensional lattice

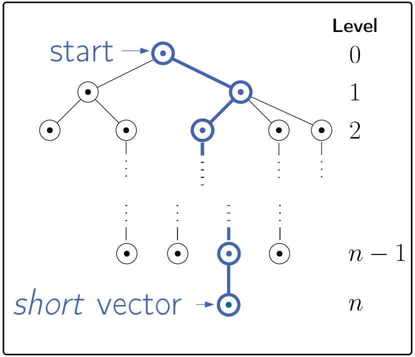


Lattice enumeration algorithm

Classical **enumeration** with extreme pruning[1]

- Search space is n-dimensional lattice
- **DFS** over enumeration tree

Depth First Search on $\mathcal{T}$



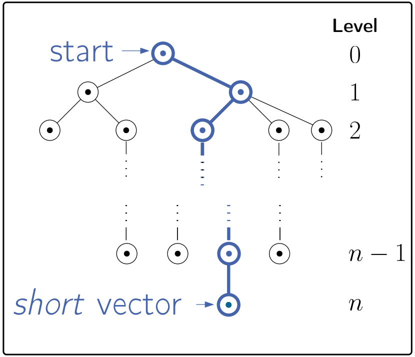
[1] Gama et al. 2010 Lattice Enumeration Using Extreme Pruning

Lattice enumeration algorithm

Classical **enumeration** with extreme pruning[1]

- Search space is *n*-dimensional lattice
- **DFS** over enumeration tree
- Complexity: $O(\#\mathcal{T})$

Depth First Search on $\mathcal{T}$



[1] Gama et al. 2010 Lattice Enumeration Using Extreme Pruning

Lattice enumeration algorithm

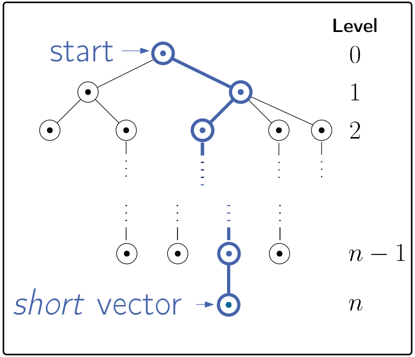
Classical **enumeration** with extreme pruning[1]

- Search space is n-dimensional lattice
- **DFS** over enumeration tree
- Complexity: $O(\#\mathcal{T})$

DFS as repetition of quantum walks[2]

$$\#\text{QW} \times \underbrace{O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \times \overbrace{\mathcal{W}}^{\text{quantum operator}}}_{\text{quantum walk}}$$

Depth First Search on $\mathcal{T}$



[1] Gama et al. 2010 Lattice Enumeration Using Extreme Pruning
[2] Montanaro 2018, Quantum-Walk Speedup of Backtracking Algorithms

When is a cryptosystem quantum-secure?

Kyber

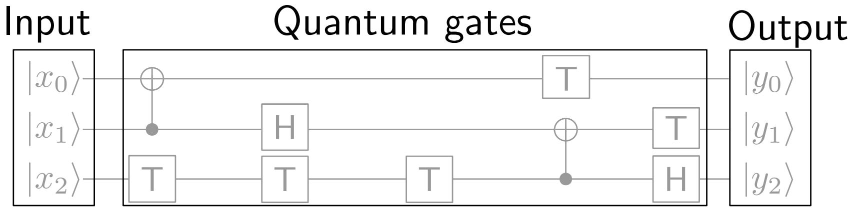
Shortest Vector Problem (SVP)

quantum
enumeration ✓

1) A cryptosystem is secure, if a certain computational problem is *difficult*.

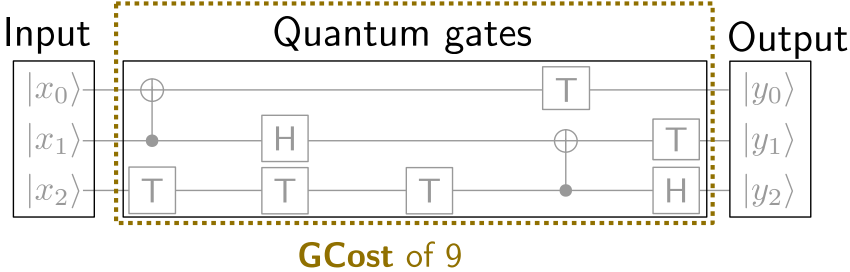
2) Computational problem is believed to be *difficult*, if the best algorithm requires an infeasible amount of resources to solve it.

Resources: The quantum circuit model



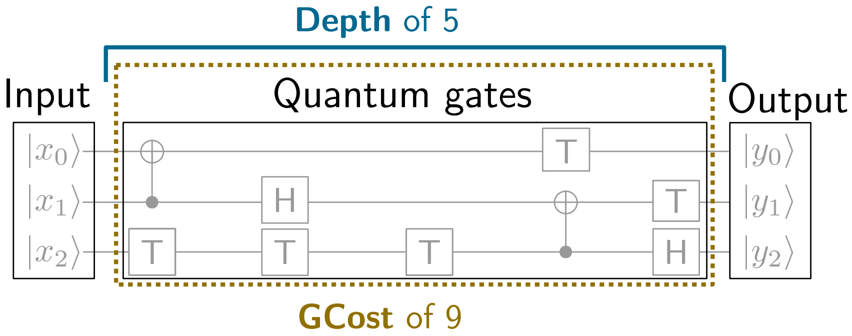
Resources: The quantum circuit model

- **GCost**: Number of universal quantum gates ▷ *lower bound on computation*



Resources: The quantum circuit model

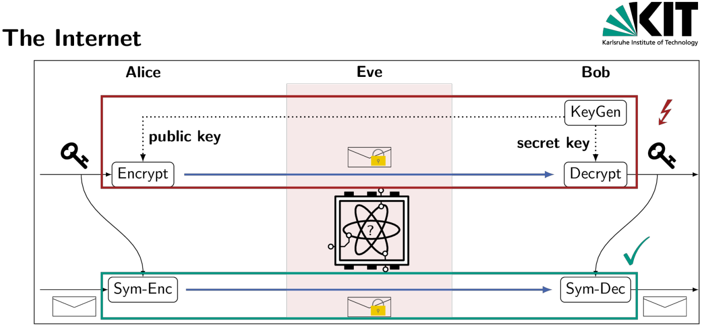
- **GCost**: Number of universal quantum gates ▷ *lower bound on computation*
- **Depth**: Circuit depth ▷ *lower bound on time*



Infeasible amount

Infeasible amount

a) Advanced Encryption Standard (AES) believed to be *quantum-secure*[1]



[1] Jaques et al. 2020 Implementing Grover Oracles for Quantum Key Search on AES and LowMC

Infeasible amount

Karlsruhe Institute of Technology

a) Advanced Encryption Standard (AES) believed to be *quantum-secure*[1]

Kyber *quantum-secure*[2],
if **GCost**("attacking Kyber") $\geq$ **GCost**("attacking AES")

AES-128	Kyber-512
AES-192	Kyber-768
AES-256	Kyber-1024

[1] Jaques et al. 2020 Implementing Grover Oracles for Quantum Key Search on AES and LowMC
[2,3] National Institute for Standards and Technology 2017, Post-Quantum Cryptography Call for Proposals

Infeasible amount

a) Advanced Encryption Standard (AES) believed to be *quantum-secure*[1]

Kyber *quantum-secure*[2],
if **GCost**("attacking Kyber") $\geq$ **GCost**("attacking AES")

AES-128	Kyber-512
AES-192	Kyber-768
AES-256	Kyber-1024

b) NIST's hypothetical $\textsc{MaxDepth} \in \{2^{40}, 2^{64}, 2^{96}\}$ for **Depth**

"number of gates [...] quantum computing [...] expected to serially perform [...]"[3]

[1] Jaques et al. 2020 Implementing Grover Oracles for Quantum Key Search on AES and LowMC
[2,3] National Institute for Standards and Technology 2017, Post-Quantum Cryptography Call for Proposals

When is a cryptosystem quantum-secure?

Kyber ↓   Shortest Vector Problem (SVP) ↓   quantum enumeration ✓

1) A cryptosystem is secure, if a certain computational problem is *difficult*.

2) Computational problem is believed to be *difficult*, if the best algorithm requires an infeasible amount of resources to solve it.

$$\textbf{GCost}(\text{“quantum enumeration”}) \geq \textbf{GCost}(\text{“attacking AES”})$$
$$\textbf{Depth}(\text{“quantum enumeration”}) \leq \textsc{MaxDepth}$$ ✓

Today's talk

The Internet

I. Advancements in quantum-secure cryptography

II. When is a cryptographic protocol quantum-secure?

III. The impact of quantum lattice enumeration

Contribution: Lower bound on quantum enumeration

Enumeration as quantum walk: $\#\mathrm{QW} \times \underbrace{O\left(\sqrt{\#\mathcal{T} \cdot n}\right) \times \mathcal{W}}_{\text{quantum walk}}$

Contribution: Lower bound on quantum enumeration

Enumeration as quantum walk: $\#\mathrm{QW} \times \underbrace{O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \times \mathcal{W}}_{\text{quantum walk}}$

- **GCost**$(\textsc{QEnum}) \quad = \#\mathrm{QW} \cdot O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \cdot$ **GCost**$(\mathcal{W})$

Contribution: Lower bound on quantum enumeration

Enumeration as quantum walk: $\#\mathrm{QW} \times \underbrace{O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \times \mathcal{W}}_{\text{quantum walk}}$

- $\textbf{GCost}(\mathrm{QE}\textsc{num}) = \#\mathrm{QW} \cdot O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \cdot \textbf{GCost}(\mathcal{W})$
- $\textbf{Depth}(\mathrm{QE}\textsc{num}) = O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \cdot \textbf{Depth}(\mathcal{W})$

Contribution: Lower bound on quantum enumeration

Enumeration as quantum walk: $\#\mathrm{QW} \times \underbrace{O\left(\sqrt{\#\mathcal{T} \cdot n}\right) \times \mathcal{W}}_{\text{quantum walk}}$

- **GCost**$(\textsc{QEnum}) = \boxed{\#\mathrm{QW}} \cdot \boxed{O\left(\sqrt{\#\mathcal{T} \cdot n}\right)} \cdot \boxed{\mathbf{GCost}(\mathcal{W})}$
- **Depth**$(\textsc{QEnum}) = \boxed{O\left(\sqrt{\#\mathcal{T} \cdot n}\right)} \cdot \boxed{\mathbf{Depth}(\mathcal{W})}$

Asymptotic lower bounds ✓
Heuristics, experiments
Constant/ polynomial factors
...

Contribution: Lower bound on quantum enumeration

Enumeration as quantum walk: $\#\mathrm{QW} \times \underbrace{O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \times \mathcal{W}}_{\text{quantum walk}}$

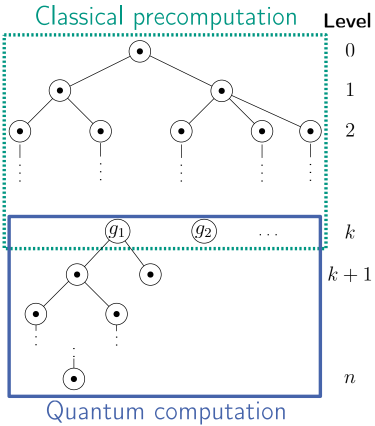
- **GCost**$(\textsc{QEnum}) = \#\mathrm{QW} \cdot O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \cdot$ **GCost**$(\mathcal{W})$
- **Depth**$(\textsc{QEnum}) = O\left(\sqrt{\#\mathcal{T}} \cdot n\right) \cdot$ **Depth**$(\mathcal{W})$

Asymptotic lower bounds
Heuristics, experiments
Constant/ polynomial factors
...
✓

- Restriction: **Depth** $\leq \textsc{MaxDepth} \in \{2^{40}, 2^{64}, 2^{96}\}$: Adapt algorithm. ✓

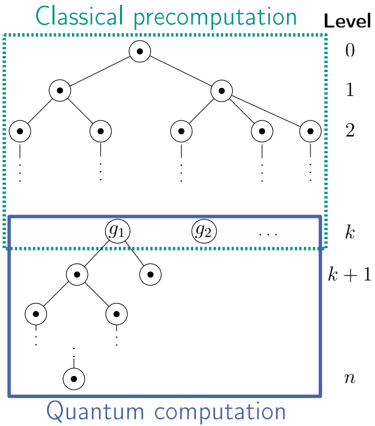
A new quantum-classical algorithm (simplified)

- Classical precomputation: up to level k



A new quantum-classical algorithm (simplified)

- Classical precomputation: up to level k
- QENUM for every node g_i on level k

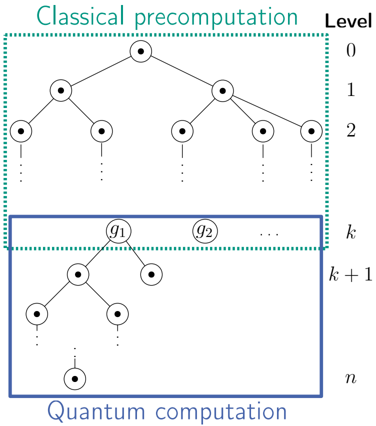


A new quantum-classical algorithm (simplified)

- Classical precomputation: up to level k
- $\textsc{QEnum}$ for every node g_i on level k
- Choose level k such that

$$\textbf{Depth}(\textsc{QEnum}) \leq \textsc{MaxDepth}$$

… and also reducing overall **GCost**.



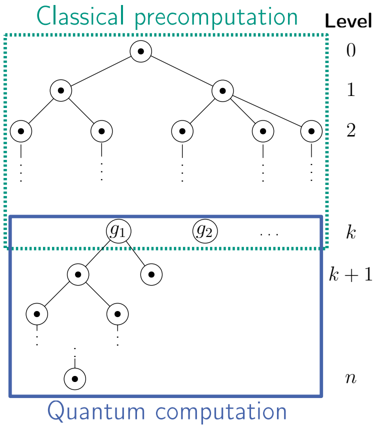
A new quantum-classical algorithm (simplified)

- Classical precomputation: up to level k
- $\textsc{QEnum}$ for every node g_i on level k
- Choose level k such that

$$\textbf{Depth}(\textsc{QEnum}) \leq \textsc{MaxDepth}$$

… and also reducing overall **GCost**.

$$\textbf{Total Cost} = \text{Classical precomputation} + \sum_{\text{for each } g_i \text{ on level k}} \textbf{GCost}(\textsc{QEnum})$$



Simplified results

$$\log(\text{Lower bound}(\textbf{Total Cost})) \overset{?}{\geq} \log(\textbf{GCost}(\text{"attacking AES"}))$$

Simplified results

$$\log(\text{Lower bound}(\textbf{Total Cost})) \stackrel{?}{\geq} \log(\textbf{GCost}(\text{“attacking AES”}))$$

MaxDepth	Kyber-512	AES-128	Kyber-768	AES-192	Kyber-1024	AES-256
2^{40}						
2^{64}						
2^{96}						

Simplified results

$$\log(\text{Lower bound}(\textbf{Total Cost})) \overset{?}{\geq} \log(\textbf{GCost}(\text{“attacking AES”}))$$

MaxDepth	Kyber-512 AES-128	Kyber-768 AES-192	Kyber-1024 AES-256
2^{40}	$94 < 117$		
2^{64}	$75 < 93$		
2^{96}	$75 < 83$		

quantum enumeration

cheaper than **GCost**(“attacking AES”)

This does not mean that Kyber-512 is insecure!

Simplified results

$$\log(\text{Lower bound}(\textbf{Total Cost})) \overset{?}{\geq} \log(\textbf{GCost}(\text{“attacking AES”}))$$

MaxDepth	Kyber-512 AES-128	Kyber-768 AES-192	Kyber-1024 AES-256
2^{40}	$94 < 117$	$197 > 181$	$312 > 245$
2^{64}	$75 < 93$	$173 > 157$	$288 > 221$
2^{96}	$75 < 83$	$143 > 125$	$232 > 189$

quantum enumeration

Kyber-512: cheaper than **GCost**(“attacking AES”)

Kyber-768 and Kyber-1024: more expensive than **GCost**(“attacking AES”)

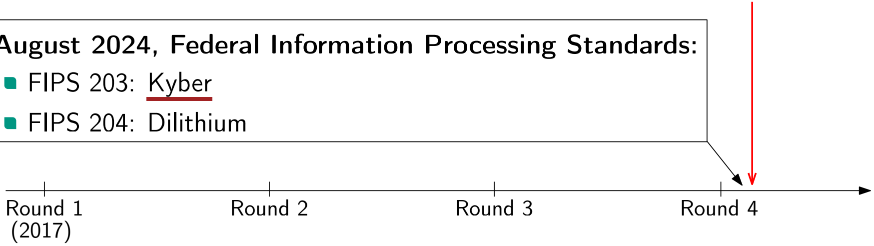
This does not mean that Kyber-512 is insecure!

Impact on post-quantum standards

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

August 2024, Federal Information Processing Standards:

- FIPS 203: Kyber
- FIPS 204: Dilithium

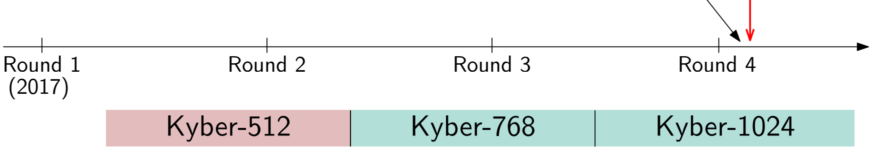


Impact on post-quantum standards

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

August 2024, Federal Information Processing Standards:

- FIPS 203: Kyber
- FIPS 204: Dilithium

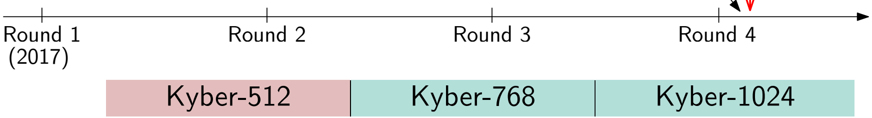


Impact on post-quantum standards

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

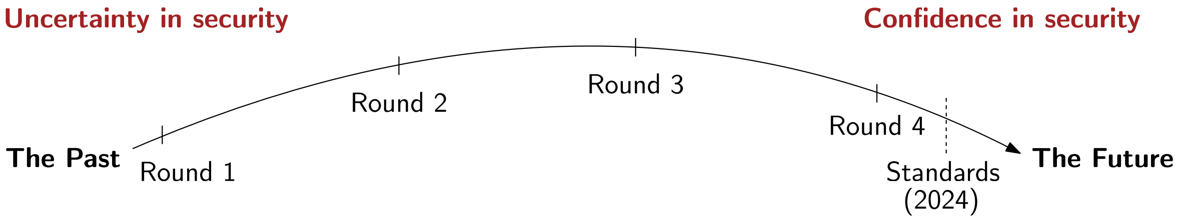
August 2024, Federal Information Processing Standards:

- FIPS 203: Kyber
- FIPS 204: Dilithium

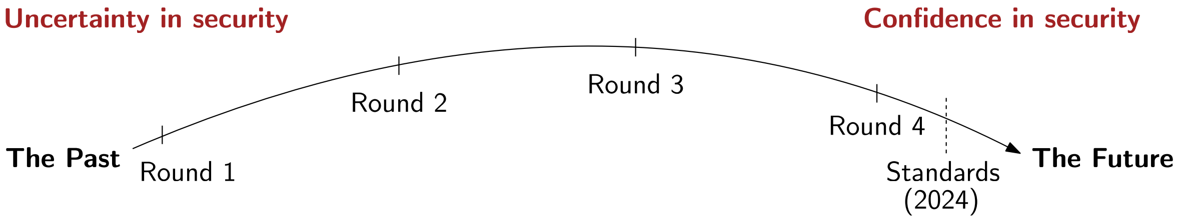


Lattice-based cryptography is **secure** for large parameters.
("The Internet" and civil aviation are saved)

A bridge to the future

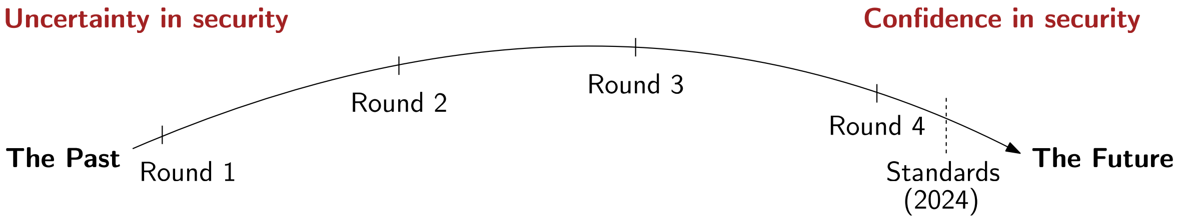


A bridge to the future



Research advances understanding and provides confidence in quantum-secure cryptography.

A bridge to the future



Research advances understanding and provides confidence in quantum-secure cryptography.

Uncertainty remains a challenge for new technologies, applications and protocols.

On to many more bridges

Exploiting Decryption Failures in Mersenne Number Cryptosystems
PKC at AsiaCCS 2020

Lattice Enumeration in Limited Depth
Advances in Cryptology – CRYPTO 2024

Forging SPHINCS$^+$-Haraka Signatures on a Fault-Tolerant Quantum Computer
Progress in Cryptology – Latincrypt 2021

Round 1 (2017) | Round 2 | Round 3 | Round 4

Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements
ESORICS 2023

Post-Quantum Ready Key Agreement for Aviation
Communications in Cryptology 2024

My research advances cryptography to protect our digital future.

Bibliography I

[1] Yoshinori Aono, Phong Q. Nguyen, and Yixin Shen. "Quantum Lattice Enumeration and Tweaking Discrete Pruning". In: 2018. DOI: 10.1007/978-3-030-03326-2_14.

[2] Shi Bai et al. "Concrete Analysis of Quantum Lattice Enumeration". English. In: *Advances in Cryptology – ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*. Germany, 2023. ISBN: 9789819987269. DOI: 10.1007/978-981-99-8727-6_5.

[3] Robin M. Berger and **Marcel Tiepelt**. "On Forging SPHINCS$^+$-Haraka Signatures on a Fault-Tolerant Quantum Computer". In: *Progress in Cryptology - LATINCRYPT 2021*. Vol. 12912. 2021. DOI: 10.1007/978-3-030-88238-9_3.

[4] Nina Bindel, Xavier Bonnetain, **Marcel Tiepelt**, and Fernando Virdia. "Quantum Lattice Enumeration in Limited Depth". In: *Advances in Cryptology – CRYPTO 2024*. Cham, 2024. ISBN: 978-3-031-68391-6. DOI: 10.1007/978-3-031-68391-6_3.

Bibliography II

[5] André Chailloux and Johanna Loyer. "Lattice Sieving via Quantum Random Walks". In: *Advances in Cryptology – ASIACRYPT 2021*. Cham, 2021. ISBN: 978-3-030-92068-5. DOI: 10.1007/978-3-030-92068-5_3.

[6] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. "Lattice Enumeration Using Extreme Pruning". In: 2010. DOI: 10.1007/978-3-642-13190-5_13.

[7] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. "Implementing Grover Oracles for Quantum Key Search on AES and LowMC". In: 2020. DOI: 10.1007/978-3-030-45724-2_10.

[8] Hyunwoo Lee, Doowon Kim, and Yonghwi Kwon. "TLS 1.3 in Practice:How TLS 1.3 Contributes to the Internet". In: *Proceedings of the Web Conference 2021*. Ljubljana, Slovenia, 2021. ISBN: 9781450383127. DOI: 10.1145/3442381.3450057.

Bibliography III

[9] Ashley Montanaro. "Quantum-Walk Speedup of Backtracking Algorithms". In: *Theory Comput.* 14.1 (2018). DOI: 10.4086/toc.2018.v014a015.

[10] National Institute for Standards and Technology. *Post-Quantum Cryptography Call for Proposals*. 2017.

[11] Peter Schwabe et al. *CRYSTALS-KYBER*. Tech. rep. National Institute of Standards and Technology, 2022.

[12] **Marcel Tiepelt** and Jan-Pieter D'Anvers. "Exploiting Decryption Failures in Mersenne Number Cryptosystems". In: *Public-Key Cryptography Workshop, APKC at AsiaCCS 2020.* 2020. DOI: 10.1145/3384940.3388957.

Bibliography IV

[13] **Marcel Tiepelt**, Edward Eaton, and Douglas Stebila. "Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements". In: *ESORICS 2023*. Vol. 14344. 2023. DOI: 10.1007/978-3-031-50594-2_9.

[14] **Marcel Tiepelt**, Christian Martin, and Nils Mäurer. "Post-Quantum Ready Key Agreement for Aviation". In: 1.1 (Apr. 9, 2024). ISSN: 3006-5496. DOI: 10.62056/aebn2isfg.