Protection against quantum computers through lattice problems

Joel Gärtner
May 22, 2025 — KTH Royal Institute of Technology

Post-Quantum Cryptography (PQC)

- Protection against the threat of quantum computers
- Cryptosystems that serve as drop-in replacements for classical cryptography that is used today
- Security based on the assumed hardness of problems which seem hard to solve even with access to a quantum computer

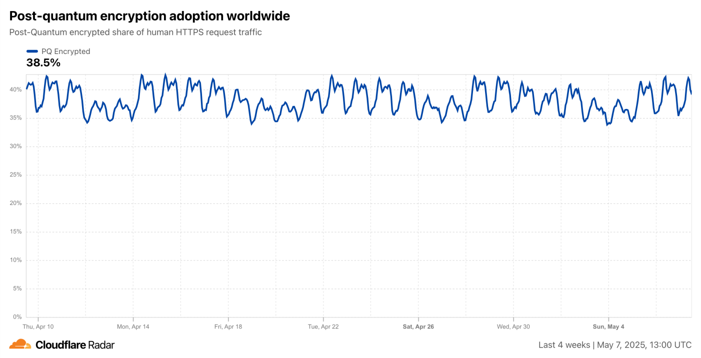
NIST PQC standards

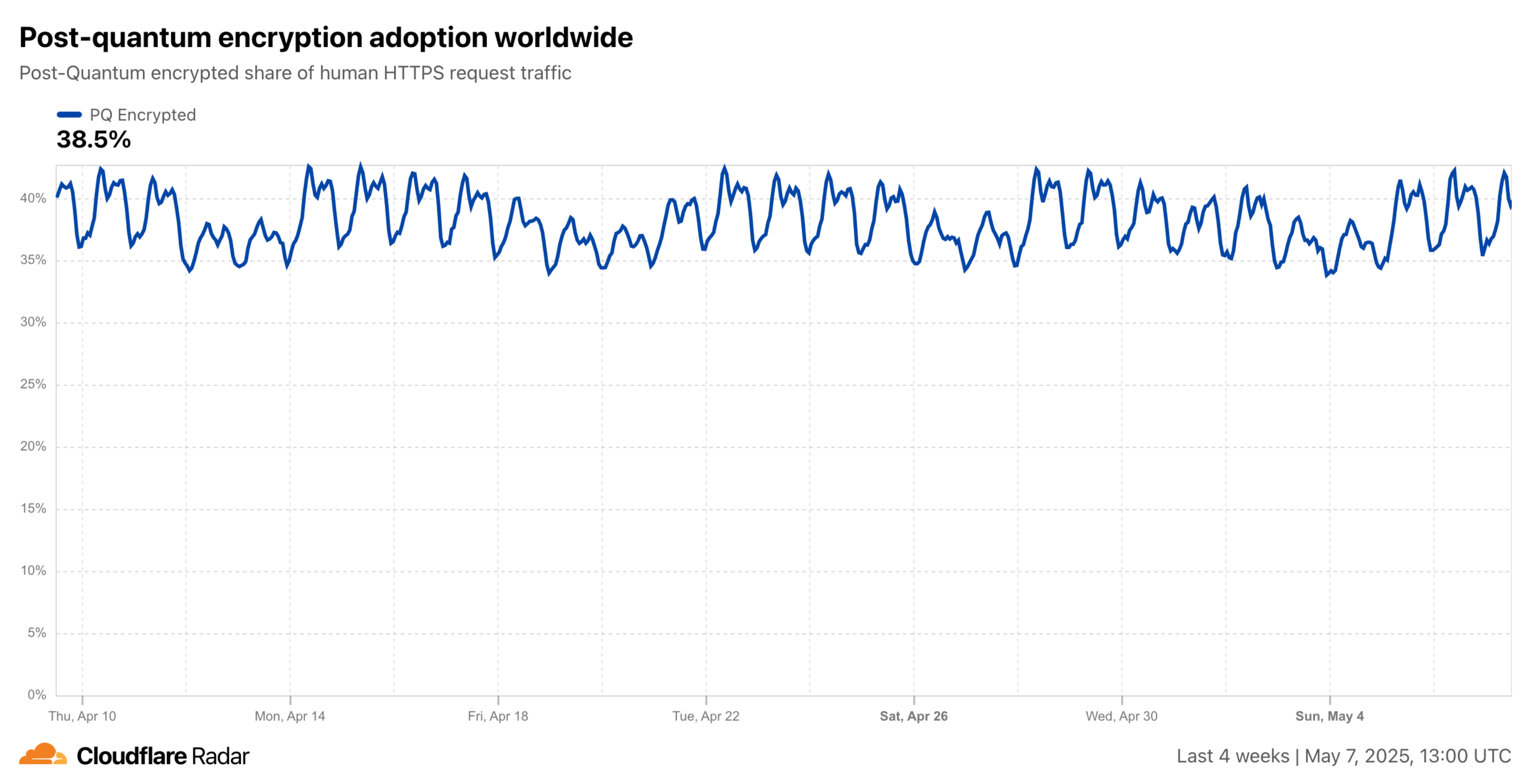
- Standards developed by the NIST first available in 2024
- Result of a multi-year standardization process
- Still ongoing process to standardize additional signature schemes

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

PQC Adoption

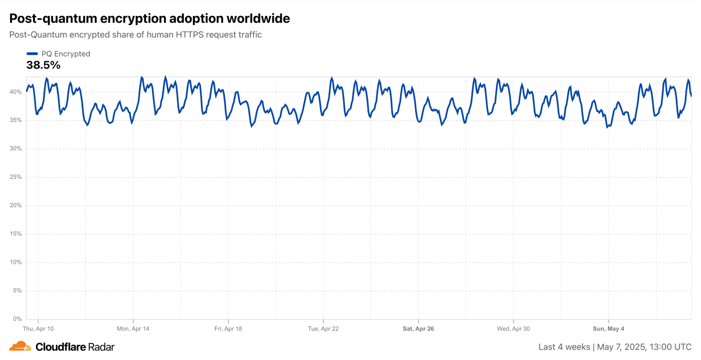
- There is already a significant amount of traffic protected by PQC
- Combining well-tested quantum vulnerable cryptography with newer less mature PQC




Post-quantum encryption adoption worldwide
Post-Quantum encrypted share of human HTTPS request traffic
PQ Encrypted
38.5%
40%
35%
30%
25%
20%
15%
10%
5%
0%
Thu, Apr 10
Mon, Apr 14
Fri, Apr 18
Tue, Apr 22
Sat, Apr 26
Wed, Apr 30
Sun, May 4
Cloudflare Radar
Last 4 weeks | May 7, 2025, 13:00 UTC

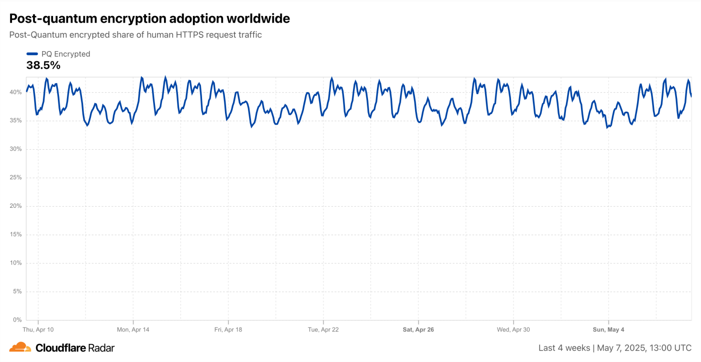
PQC Adoption

- There is already a significant amount of traffic protected by PQC
- Combining well-tested quantum vulnerable cryptography with newer less mature PQC
- Protection for confidentiality implemented, but no large scale support for authenticity



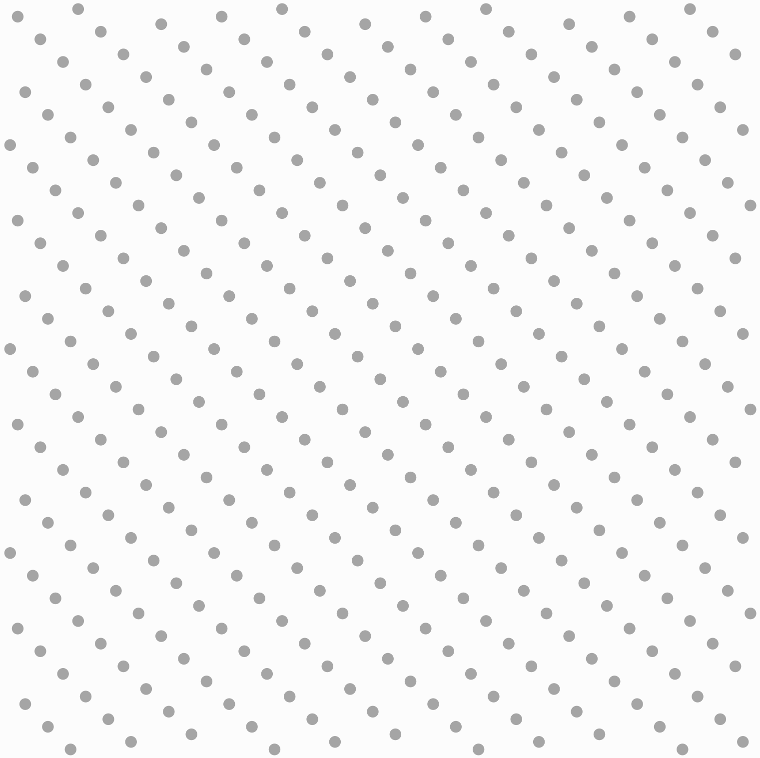
PQC Adoption

- There is already a significant amount of traffic protected by PQC
- Combining well-tested quantum vulnerable cryptography with newer less mature PQC
- Protection for confidentiality implemented, but no large scale support for authenticity
- Lattice-based scheme used for PQC



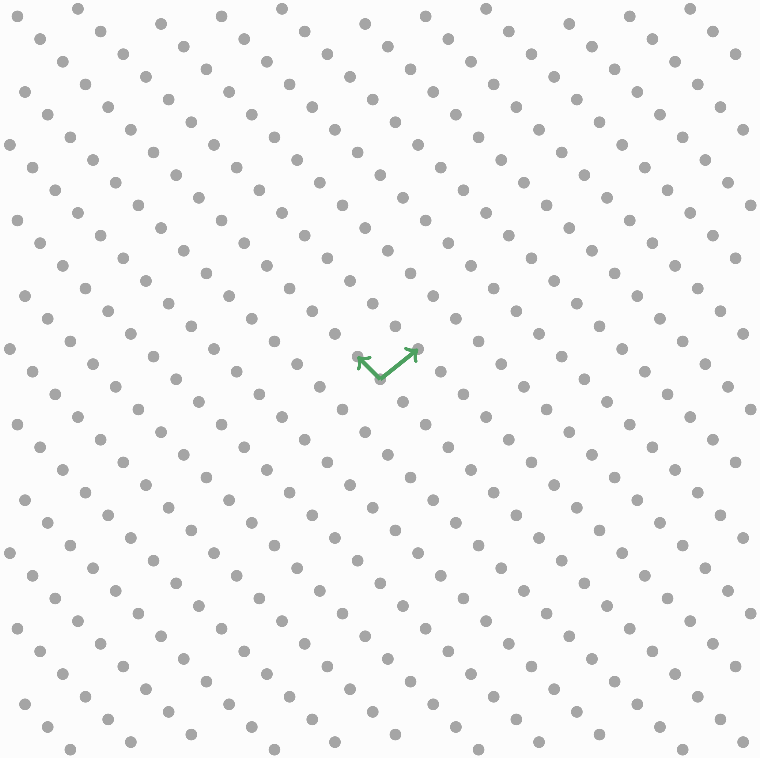
Lattices

- Regular n-dimensional pattern



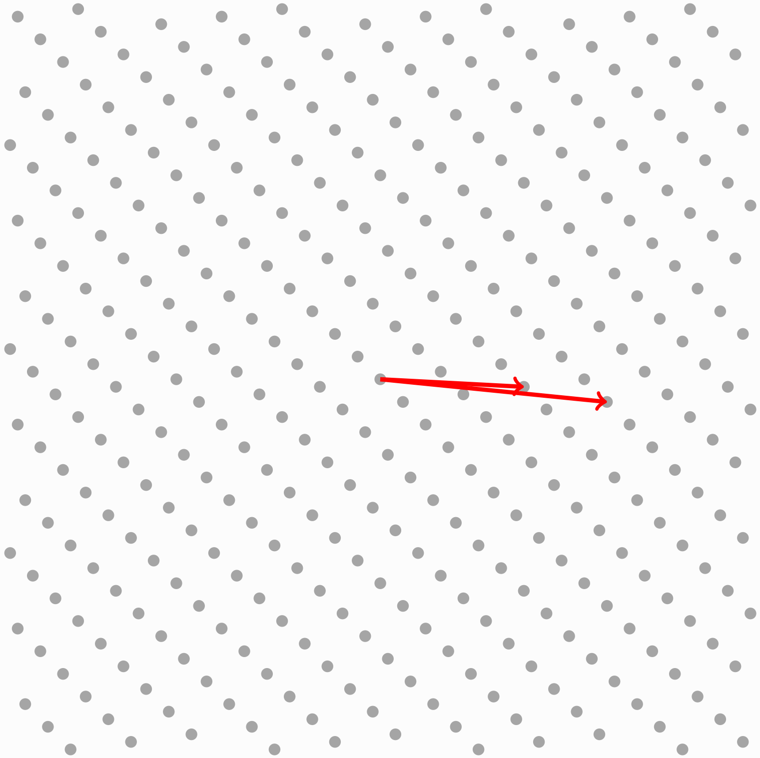
Lattices

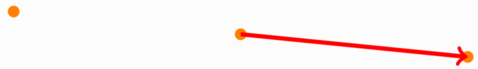
- Regular *n*-dimensional pattern
- Generated by a non-unique basis

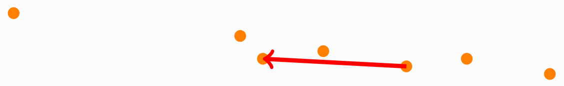


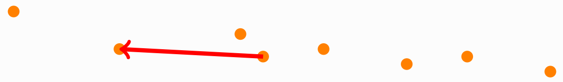
Lattices

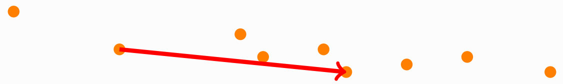
- Regular *n*-dimensional pattern
- Generated by a non-unique basis

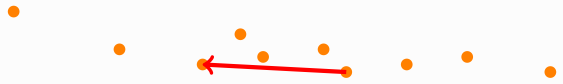


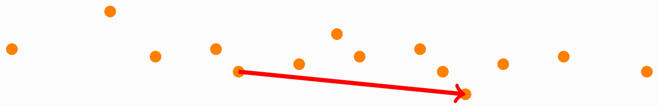


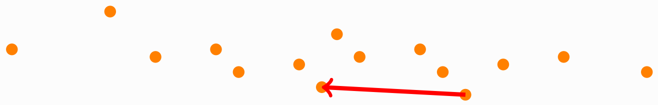


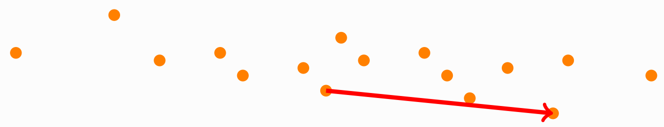


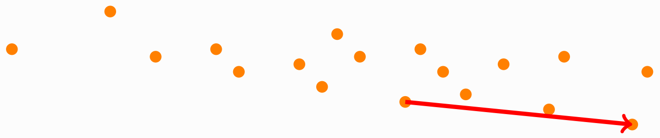


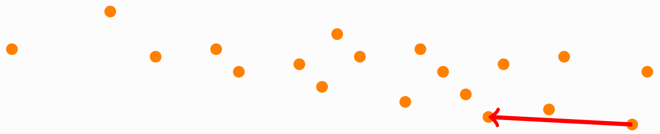


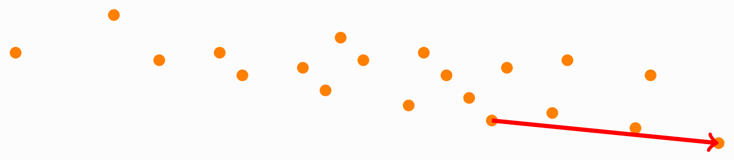


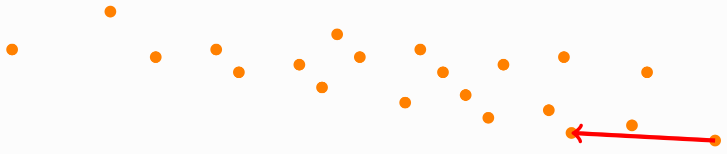


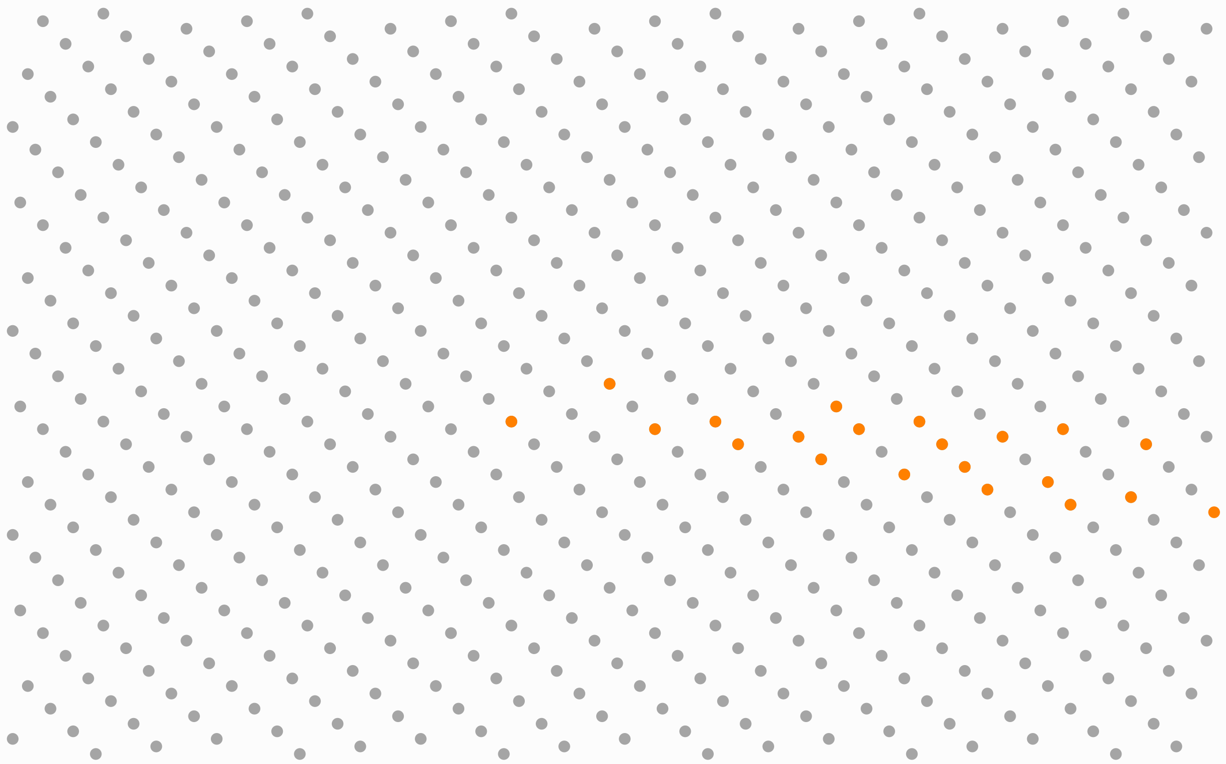






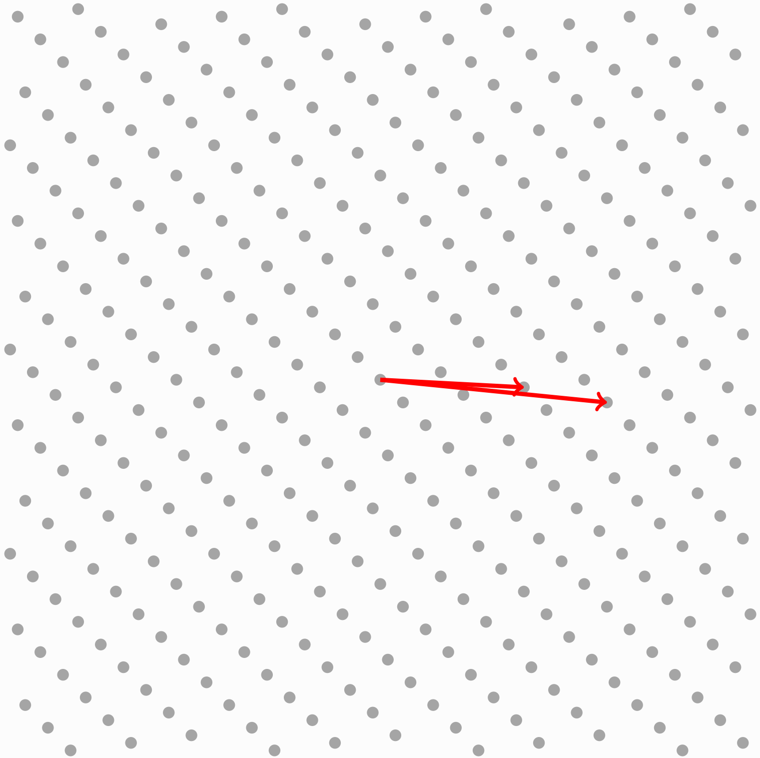






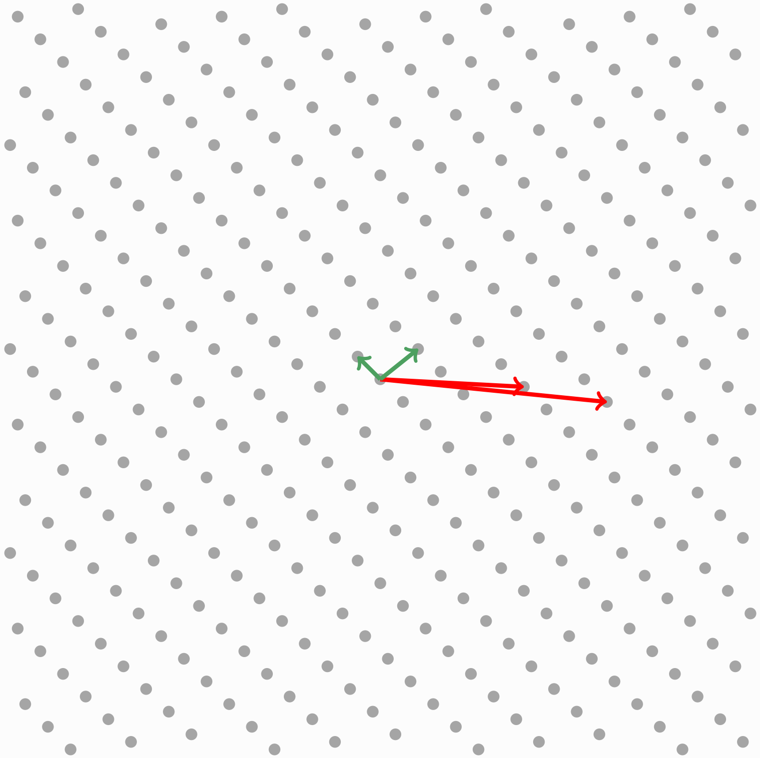
Lattices

- Regular *n*-dimensional pattern
- Generated by a non-unique basis



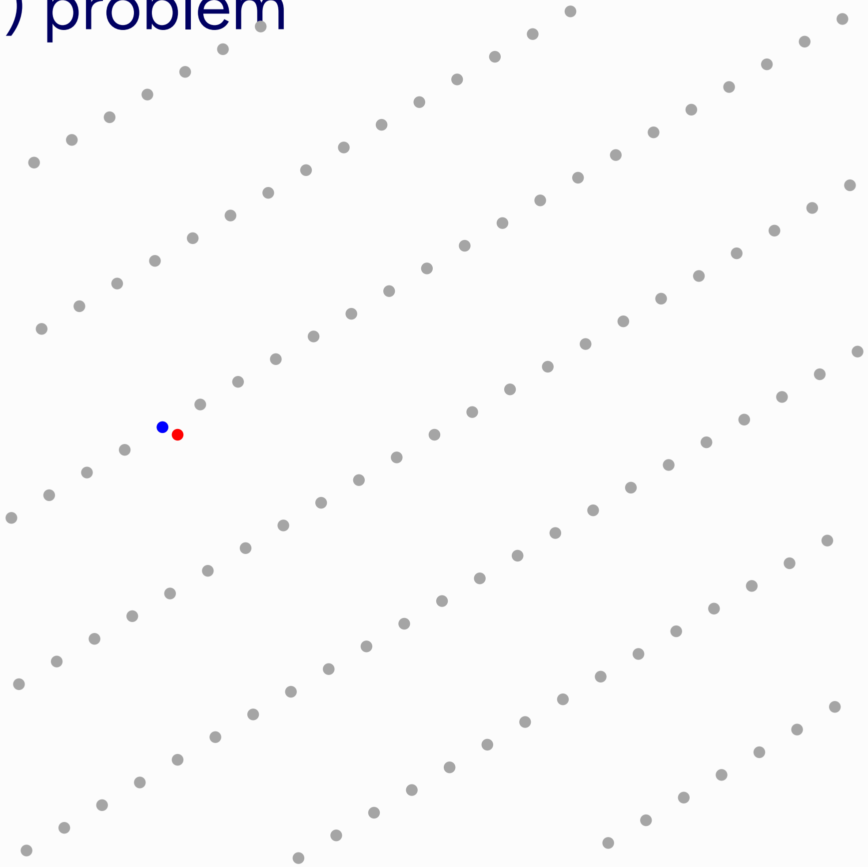
Lattices

- Regular *n*-dimensional pattern
- Generated by a non-unique basis
- A good basis makes solving lattice problems easier than with a bad basis



Learning With Errors (LWE) problem

- Primary problem used for lattice-based cryptography
- Corresponds to finding a lattice point close to a target point
- Strong theoretical arguments for its asymptotic hardness
- Plenty of analysis of concrete hardness of problem
- My work analyzed gap between concrete and theoretical hardness



Key-Encapsulation Mechanisms (KEM)

- Method to establish a shared key between Alice and Bob
- Bob's public key pk is available for everyone
- Alice makes use of pk to encapsulate a random secret key K into a ciphertext c
- Given c, Bob can use his private key to recover K
- The eavesdropper Eve is unable to recover K when given c and pk

PQC KEM Algorithms

- CRYSTALS-Kyber and HQC two algorithms chosen to be standardized by NIST
- The standard ML-KEM (FIPS 203) based on CRYSTALS-Kyber is already available
- HQC was recently chosen as an additional algorithm to standardize

ML-KEM

- Built on module version of LWE problem
- Currently used as hybrid solution with classical ECDH

	ML-KEM	ECDH
Public Key	1184	32
Ciphertext	1080	32

Table: Public key and ciphertext sizes in bytes.

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

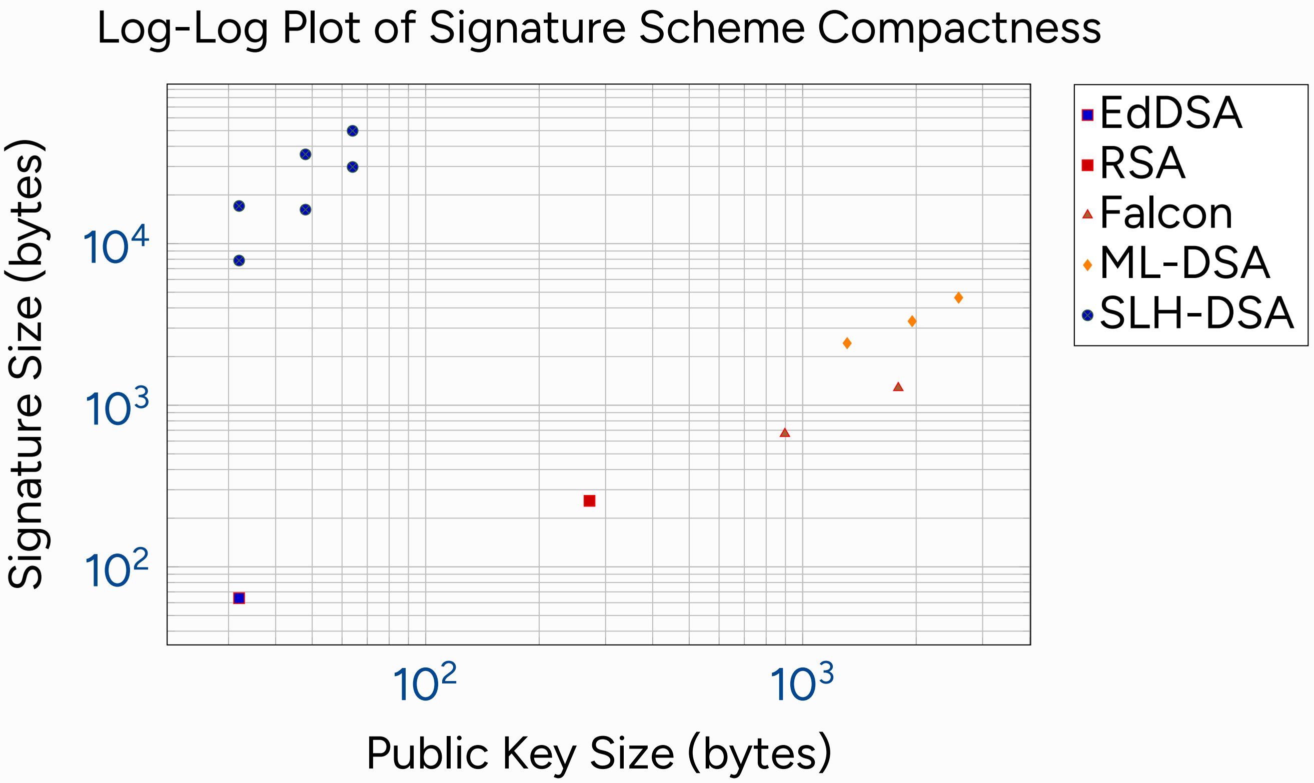
Published August 13, 2024

Digital Signature Algorithms

- Method for Alice to securely sign a message M
- Alice's public key pk is available to everyone
- Signature Sig for message M produced by Alice
- Anyone with access to pk and Sig is able to verify that Alice signed M

PQC algorithms for digital signatures

- RSA and EdDSA quantum vulnerable signature schemes used today
- ML-DSA and SLH-DSA already standardized by NIST
- Falcon an additional signature scheme that is in the process of being standardized


Log-Log Plot of Signature Scheme Compactness
Signature Size (bytes)
10^4
10^3
10^2
10^2
10^3
Public Key Size (bytes)
EdDSA
RSA
Falcon
ML-DSA
SLH-DSA

ML-DSA

- Built on module version of LWE problem
- Primary signature algorithm standardized by NIST

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024

SLH-DSA

- Much larger signatures than for currently used digital signature schemes
- Small public keys and conservative security assumption

FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security **Subcategory: Cryptography**

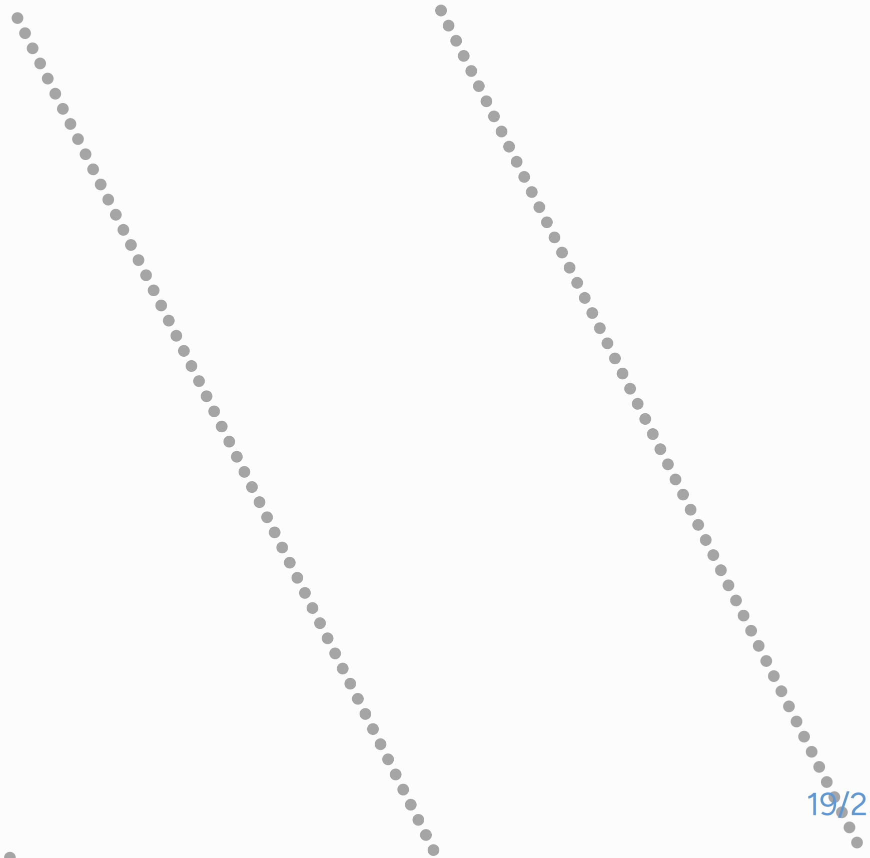
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205

Published: August 13, 2024

NTRU problem

- Alternative problem used for lattice-based cryptography
- Corresponds to finding a dense sublattice



FALCON

- Digital signature scheme based upon the NTRU problem
- More compact than the other lattice-based signature scheme ML-DSA
- Much more complex to implement in a secure manner
- Unsuitable for some applications

Security	$\sim$ 128 bits	$\sim$ 192 bits	$\sim$ 256 bits
Falcon	(897, 666)	-	(1793, 1280)
ML-DSA	(1312, 2420)	(1952, 3309)	(2592, 4627)

Table: (Public key size, Signature size) in bytes.

NTWE problem

- Combination of NTRU and LWE problems introduced in my thesis
- NTWE-based schemes with benefits over LWE and NTRU-based schemes

More compact signature scheme

- New method to produce signatures developed
- Same basic idea as for ML-DSA but with compactness similar to Falcon

Scheme	Security Level	VK Size	Signature Size	Total
Falcon-512	120	897	666	1563
Our scheme	120	928	775	1703
ML-DSA-44	123	1312	2420	3732
Falcon-1024	273	1793	1280	3073
Our Scheme	257	1568	1694	3262
ML-DSA-87	252	2592	4595	7187

KTH
VETENSKAP
OCH KONST