# Quantum Cryptanalysis on Lattices and Codes

Ph.D. defense

Johanna Loyer

# Public-key cryptography

## Cryptographic problem

$$\textbf{Secret key} \quad \underset{\xleftarrow[\text{hard}]{\qquad\qquad}}{\xrightarrow{\text{easy}}} \quad \textbf{Public key}$$

## Factorization problem

$$\text{Large primes } p, q \quad \underset{\xleftarrow[\text{hard}]{\qquad\qquad}}{\xrightarrow{\text{easy}}} \quad p \cdot q$$

# Public-key cryptography

## Cryptographic problem

$$\textbf{Secret key} \; \underset{\text{hard}}{\overset{\text{easy}}{\rightleftarrows}} \; \textbf{Public key}$$


## Factorization problem

$$\text{Large primes } p, q \; \underset{\cancel{\text{hard}}}{\overset{\text{easy}}{\rightleftarrows}} \; p \cdot q$$

easy
for quantum computers

[Sho94] Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring.

# Leads for quantum-safe cryptography

Lattices

Codes

Multivariate polynomials

Isogenies

# My contributions

**Lattice-based cryptography:**

- [CL21] Chailloux-**Loyer**. Lattice sieving via quantum random walks. (ASIACRYPT21)
- [CL23] Chailloux-**Loyer**. Classical and Quantum 3 and 4-Sieves to Solve SVP with Low Memory. (PQCrypto23)

**Code-based cryptography:**

- [Loy23] **Loyer**. Quantum security analysis of Wave. (Submitted)
- [Wave] Banegas-Carrier-Chailloux-Couvreur-Debris-Gaborit-Karpman-**Loyer**-
-Niederhagen-Sendrier-Smith-Tillich.
(NIST submission to the post-quantum cryptography standardization)

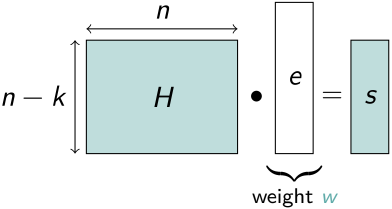
1 Wave quantum security

# Outline

1. Wave quantum security

# Syndrome Decoding problem

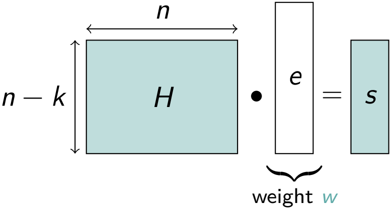
- **Public**: matrix $H$ and vector $s$ with elements in $\{0, 1\}$, weight $w \in [\![0, n]\!]$
- **Secret**: $e \in \{0, 1\}^n$ such that:



## Syndrome Decoding problem

**Public**: matrix $H$ and vector $s$ with elements in $\{0,1\}$, weight $w \in [\![0,n]\!]$

**Secret**: $e \in \{0,1\}^n$ such that:




- WAVE digital signature:
  - $H$ **structured** matrix $(U, U+V)$
  - **Ternary** : $\{0,1,2\}$ instead of $\{0,1\}$
  - **Large** weight $w$

# Attacks on Wave

**Key attack**: Distinguish the secret key from the uniform random

- Find $\mathbf{e} = (\mathbf{u}, \mathbf{u})$ solution to the Syndrome Decoding problem.

# Attacks on Wave

**Key attack**: Distinguish the secret key from the uniform random

- Find $\mathbf{e} = (\mathbf{u}, \mathbf{u})$ solution to the Syndrome Decoding problem.

**Forgery attack**: Produce a fake signed document that passes the authenticity test

- Find couple $\mathbf{s}$ and $\mathbf{e} = (\mathbf{u}, \mathbf{u})$ solution to the Syndrome Decoding problem.

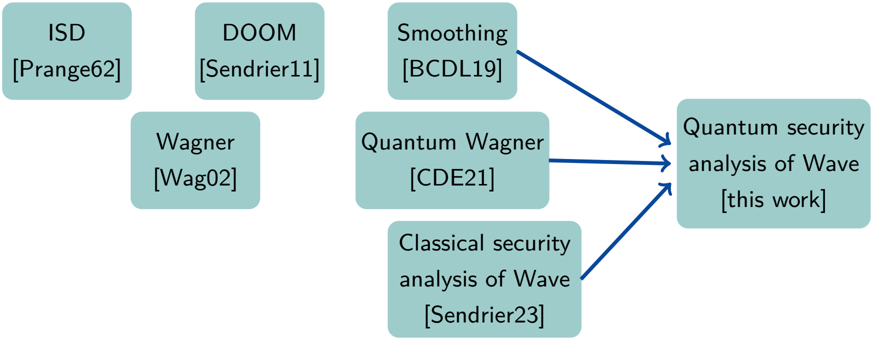
# Attacks on Wave

**Key attack**: Distinguish the secret key from the uniform random

- Find $\mathbf{e} = (\mathbf{u}, \mathbf{u})$ solution to the Syndrome Decoding problem.

**Forgery attack**: Produce a fake signed document that passes the authenticity test

- Find couple $\mathbf{s}$ and $\mathbf{e} = (\mathbf{u}, \mathbf{u})$ solution to the Syndrome Decoding problem.



# Wave security

$x$ bits of security: known attacks run in time $\geq 2^x$.

| | Classical | | Quantum | |
|---|---|---|---|---|
| NIST settings | Key attack | Forgery attack | Key attack | Forgery attack |
| (I) | 138 | 129 | **80** | **78** |
| (III) | 206 | 194 | **120** | **117** |
| (V) | 274 | 258 | **160** | **156** |

# Takeaway

## Conclusion

- First quantum key attack against Wave
- Improvement of the quantum forgery attack
- NIST submission

# Ongoing and future works

- Code sieving via quantum walks
  Collision finding and two filtering layers for code sieving [DEEK23]
- Optimal quantum algorithm for multiple collisions
  Extend [BCSS23] to all parameter ranges.
- $2^k$-sieve with combined filtering techniques
  Trade-off from best memory to best time.

# Thank you for your attention!