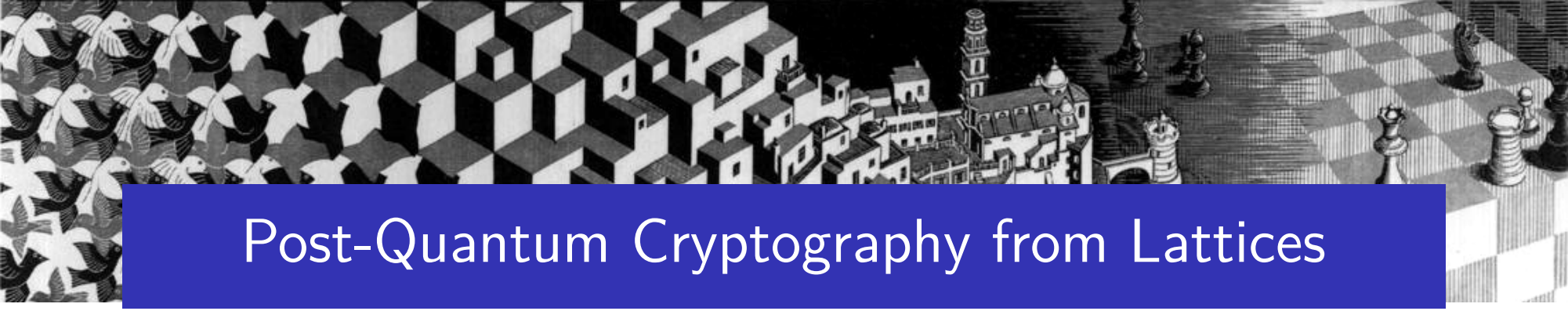


Post-Quantum Cryptography from Lattices

Léo Ducas[1]

CWI, Amsterdam, The Netherlands

CWI Scientific Meeting,
November 2016.

[1]Funded by a PPP Grant, between NXP and CWI.

Cryptography

Cryptography in everyday life and for critical applications

Banking

Individual privacy

Industrial secret

Journalism & Whistleblowing

Diplomacy & Strategy

Modern Cryptography

Provable confidentiality & integrity of communications . . .
under an **assumption**, e.g. *factoring large integers is intractable*

Cryptography

Cryptography in everyday life and for critical applications

Banking

Individual privacy

Industrial secret

Journalism & Whistleblowing

Diplomacy & Strategy

Modern Cryptography

Provable confidentiality & integrity of communications . . .
under an **assumption**, e.g. *factoring large integers is intractable*

Cryptanalysis

Invalidate the assumption	$\Rightarrow$	discard insecure schemes
Quantify intractability	$\Rightarrow$	select key size for standards

The assumptions underlying today's cryptography

Cryptography from factoring

- Secret key: two large prime number p, q
- Public key: the product $N = p \cdot q$

Cryptography from Discrete Logarithm

Cryptography from Elliptic Curves Discrete Logarithm

The assumptions underlying today's cryptography

The Quantum Cryptocalypse

Today's cryptography (Factoring, Discrete Log.) is **broken by Schor's quantum algorithm**

- Serious concerns expressed (NSA)
- Call for Post-Quantum standards (NIST 2017-2020)

Quantum Crypto, Post-Quantum Crypto ?!

	Users	Attacker
Classical Crypto (Today) No Quantum computer exists		

Quantum Crypto, Post-Quantum Crypto ?!

	Users	Attacker
Classical Crypto (Today) No Quantum computer exists		
Post-Quantum Crypto[2] (2030 ?) A few Quantum computers exist		

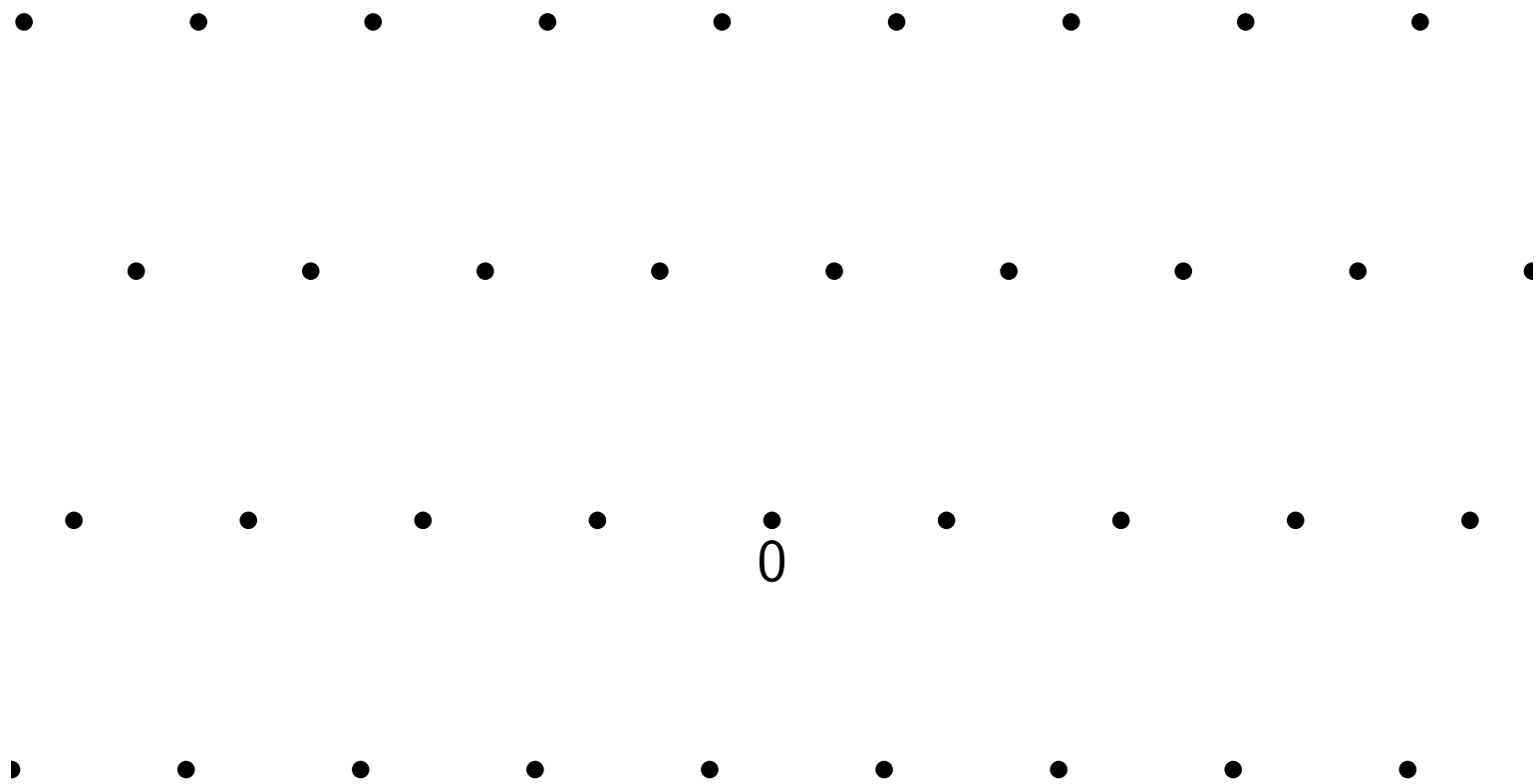
[2] Also called Quantum-Safe Crypto

Quantum Crypto, Post-Quantum Crypto ?!

	Users	Attacker
Classical Crypto (Today) No Quantum computer exists		
Post-Quantum Crypto[2] (2030 ?) A few Quantum computers exist		
Quantum Crypto (2060 ?) All computers and **networks** are Quantum		

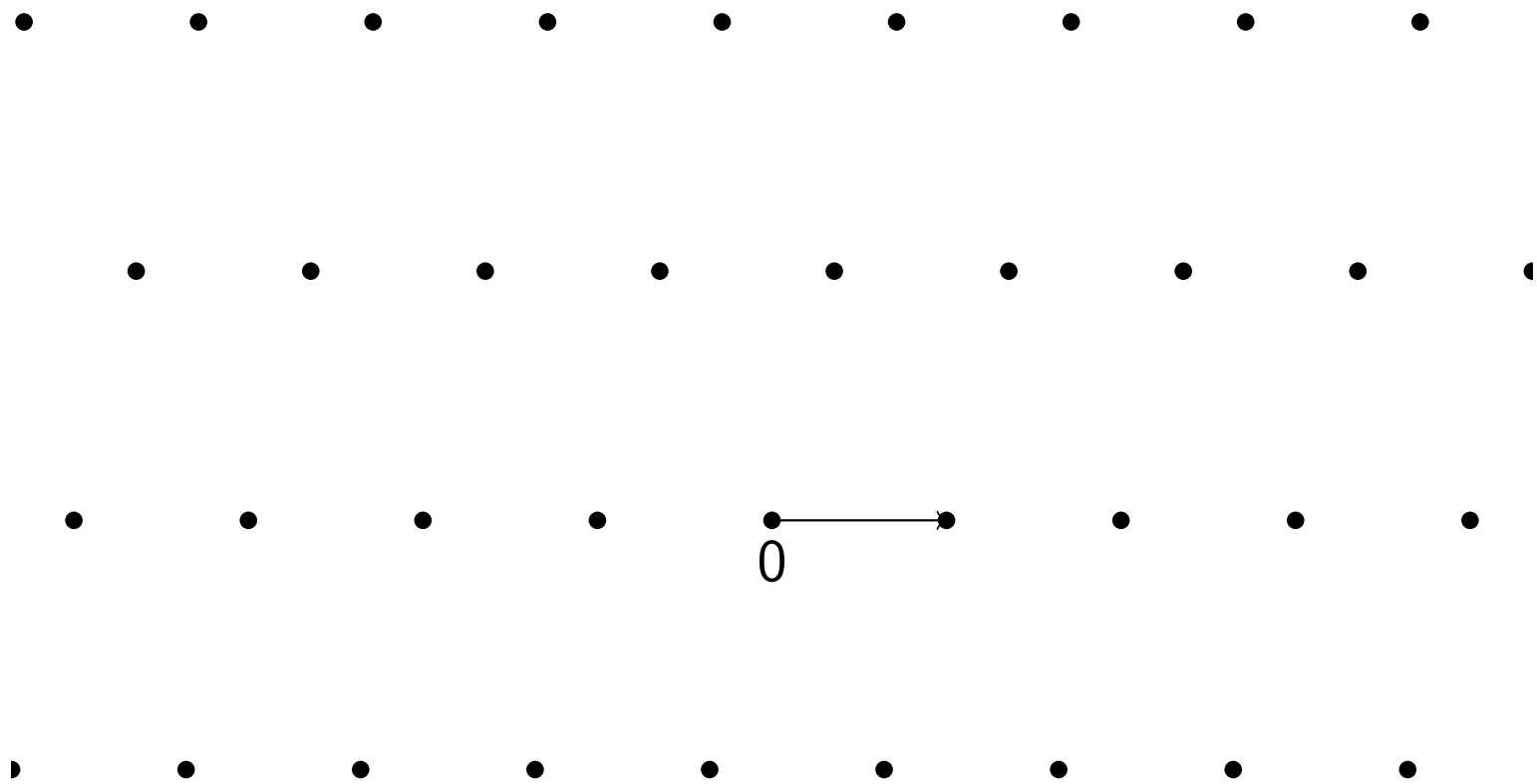
[2] Also called Quantum-Safe Crypto

Lattices: a cryptography for tomorrow



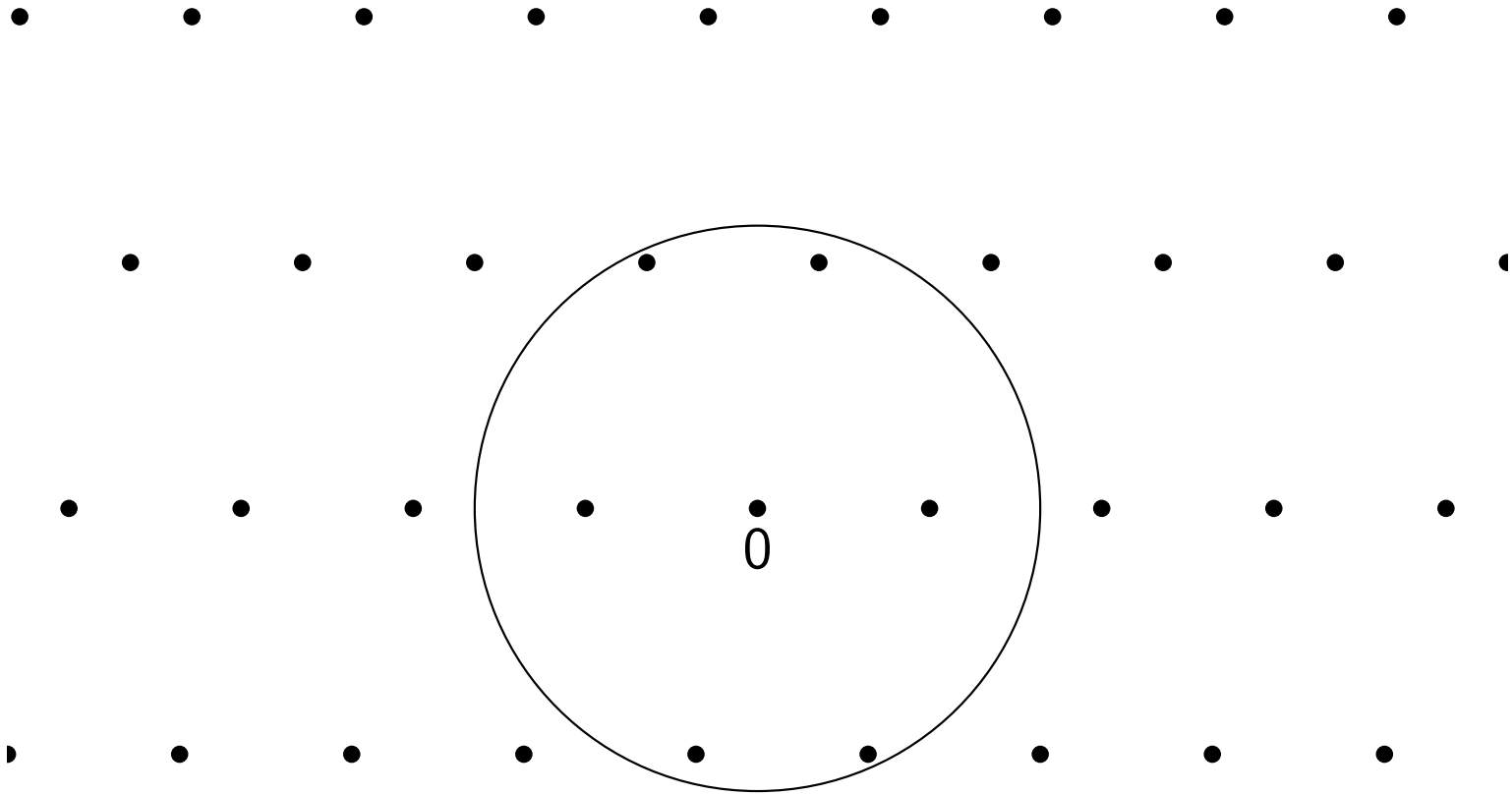
A lattice

Lattices: a cryptography for tomorrow



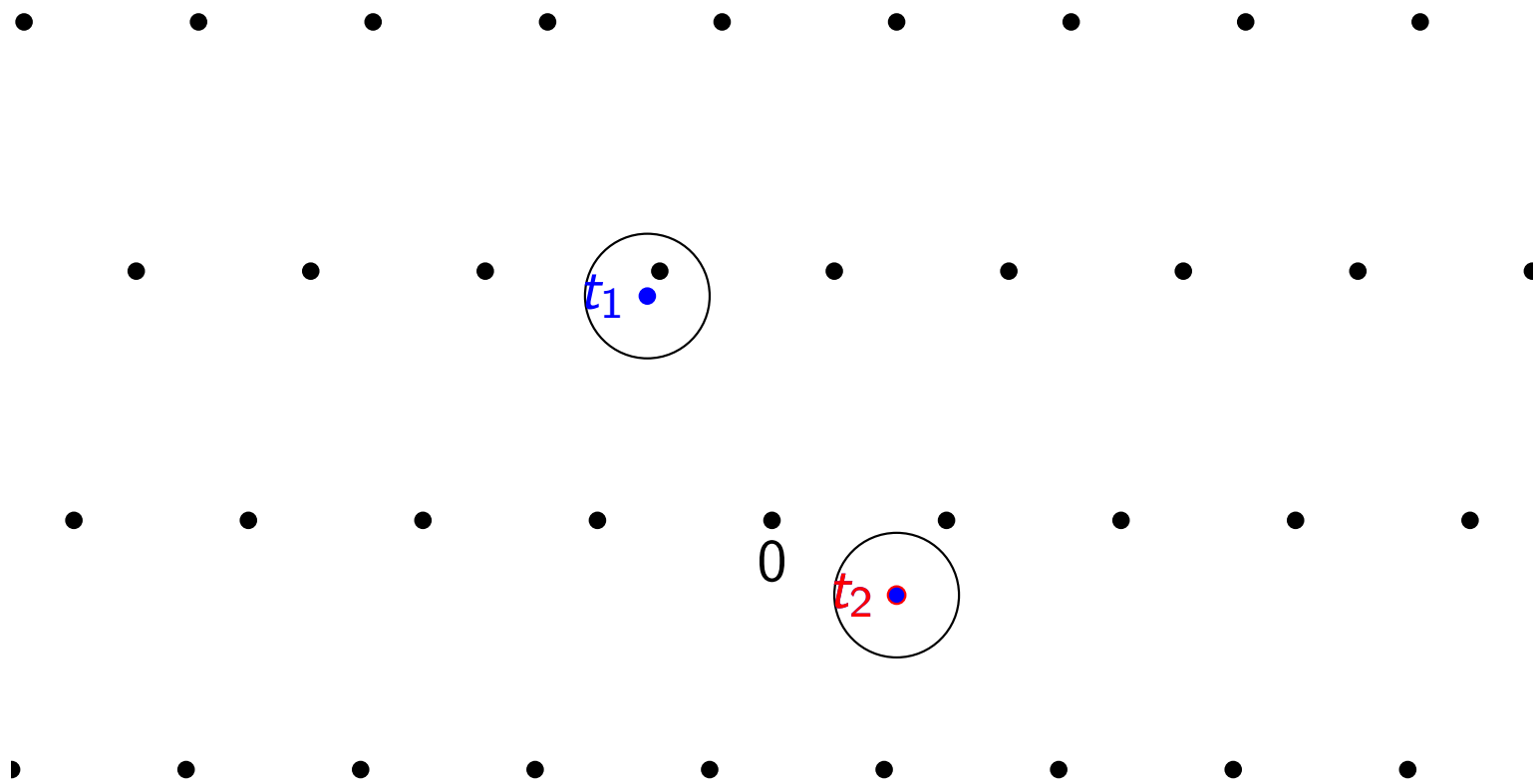
The Shortest Vector Problem (SVP)

Lattices: a cryptography for tomorrow



The Approximate Shortest Vector Problem (Approx-SVP)

Lattices: a cryptography for tomorrow



The Bounded Distance Decoding Problem (BDD)

Lattices: a cryptography for tomorrow

Lattice-based Cryptography

Those problems can be harnessed for cryptography.

Many advantages:

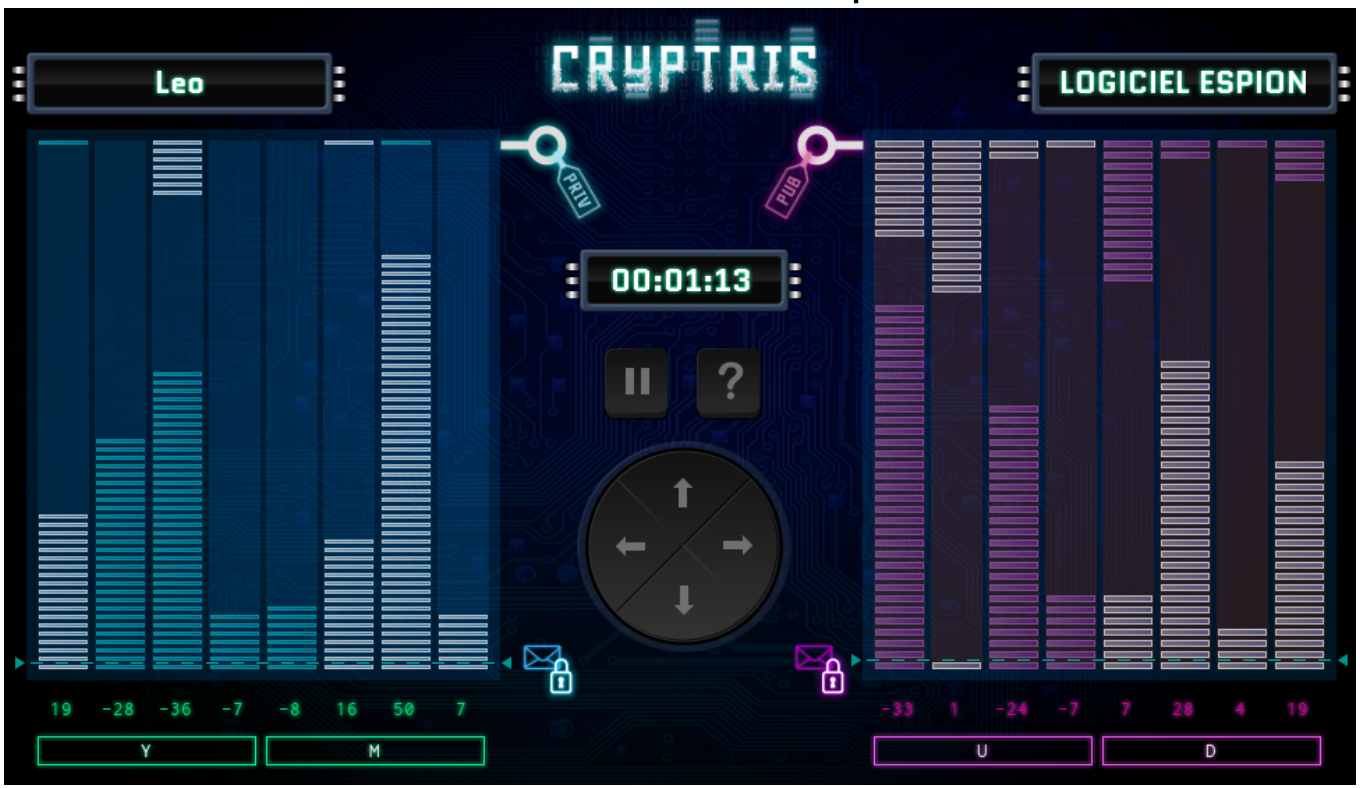
- Hard against quantum computing as far as we know
- Based on worst-case problems, near NP-hard problems
- Unlocks unprecedented features

The Bounded Distance Decoding Problem (BDD)

Lattice-based-crypto is as simple as Tetris

Cryptris: A video game to understand how it works, and why it is secure.

Developed in collaboration with **Inria**



`http://inriamecsci.github.io/cryptris/`

In French only (for now ?)

A New Hope [Alkim, **D.**, Poppelmann, Shwabe, 2016]

Awarded the **the Internet Defense Prize** (Usenix & Facebook)

Many **theoretical** schemes proposed before

no parameters, unrealistic constraints, ...

NewHope: From Theory to **Practice**

- Proposed parameters with very strong **Concrete** security
- Countermeasure to **Backdoors** and **Mass-Surveillance** attack scenario e.g. LogJam attack
- Very Fast, Reasonably Compact, Simple ...
- **Open-Source**
- Integrated in Boring-SSL and Chrome Browser by **Google**.

“Soliloquy, A cautionary tail”, a warning from the GCHQ

[Campbell-Groves-Shepherd 2014]

Algebraic structure greatly improve efficiency

“Soliloquy, A cautionary tail”, a warning from the GCHQ

[Campbell-Groves-Shepherd 2014]

Algebraic structure greatly improve efficiency

but they may open the door the Shor-likes algorithm.

“Soliloquy, A cautionary tail”, a warning from the GCHQ

[Campbell-Groves-Shepherd 2014]

Algebraic structure greatly improve efficiency
but they may open the door the Shor-likes algorithm.

Finding Generators using a quantum computer [Biasse-Song 2015]

Finding Mildly Short Generator [Cramer-**D.**-Peikert-Regev 2015]

Generalization to more ideal lattices [Cramer-**D.**-Wesolowski 2016]

`www.quantamagazine.org/20150908-quantum-safe-encryption/`

"Soliloquy, A cautionary tail", a warning from the GCHQ

[Campbell-Groves-Shepherd 2014]

Algebraic structure greatly improve efficiency
but they may open the door the Shor-likes algorithm.

Finding Generators using a quantum computer [Biasse-Song 2015]

Finding Mildly Short Generator [Cramer-**D.**-Peikert-Regev 2015]

Generalization to more ideal lattices [Cramer-**D.**-Wesolowski 2016]

`www.quantamagazine.org/20150908-quantum-safe-encryption/`

Some obstacle remains

- Midly short is **not enough** for attacks
- (Most) Crypto use lattices with **less structure**

Cryptanalysis only gets better

Much scrutiny is still needed.

Thanks !

Questions ?