Post-Quantum Cryptography based on Lattices

Cecilia Boschini,

IBM Research – Zurich and Universita' della Svizzera Italiana

February 8th , 2018

Quantum-resistant alternatives

Multivariate Equations

Lattice-based algorithms

(LWE, Ring-LWE, NTRU)

Hash-tree based algorithms

Code-based systems

Supersingular isogeny DH (SIDH)

Why lattices?

- Widely studied
(~20 years of literature)

- Versatile
(allow to build complex cryptographic primitives like FHE)

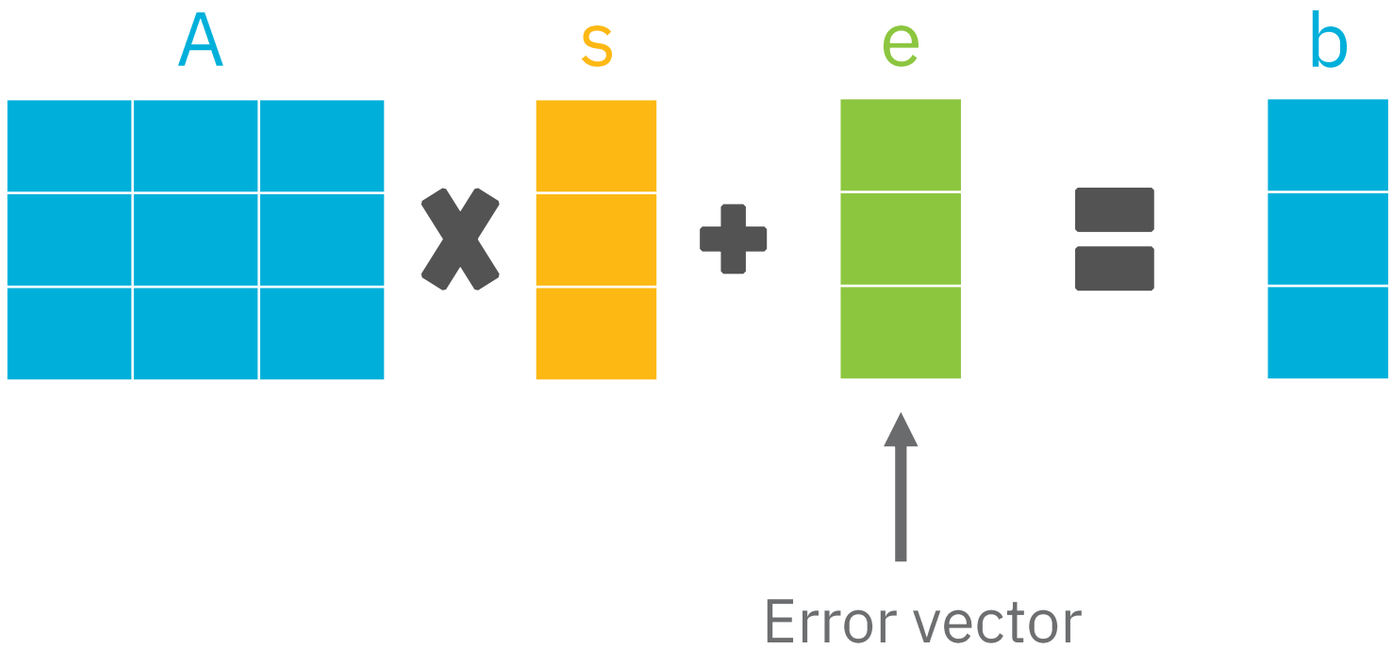
- As fast as RSA or EC schemes
(highly parallelizable)

- Medium sized keys
(shrinking over time)

Learning With Errors (LWE)

- Computational domain:
  vectors in Z_q : they have coefficients bounded by q

- Public random matrix and vector
- Secret vector with small components

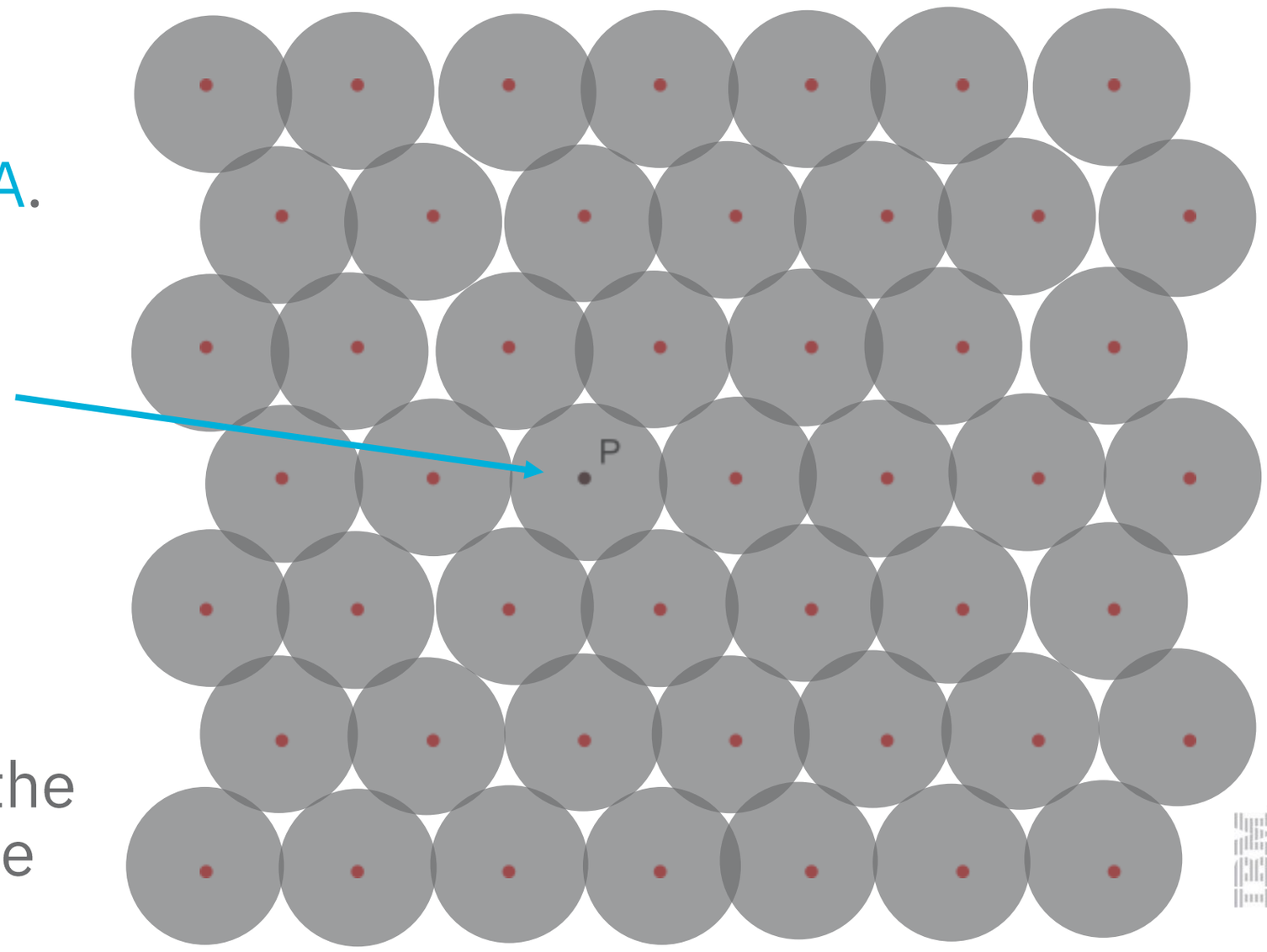


Hardness of LWE

Intuition:

A lattice is a grid of point identified by a matrix, e.g., A.

As is a point P in the lattice identified by A.



Adding e means perturbing the lattice so that now P could be anywhere in the space.

Hardness of LWE

Factoring

Fix a length l (i.e., the number of ciphers).
Given a number N find a *prime* p that divides N.

The security of the schemes based on factoring relies on N.
How to choose N? Let’s try with random N.

99’848’813 = 9887 * 10099

Hardness of LWE

Factoring

Fix a length l (i.e., the number of ciphers).
Given a number N find a *prime* p that divides N.

The security of the schemes based on factoring relies on N.
How to choose N? Let’s try with random N.

99’848’810 Not hard: 2 divides N!

Hardness of LWE

Factoring

Fix a length l (i.e., the number of ciphers).
Given a number N find a *prime* p that divides N.

The security of the schemes based on factoring relies on N.
How to choose N? Let’s try with random N.

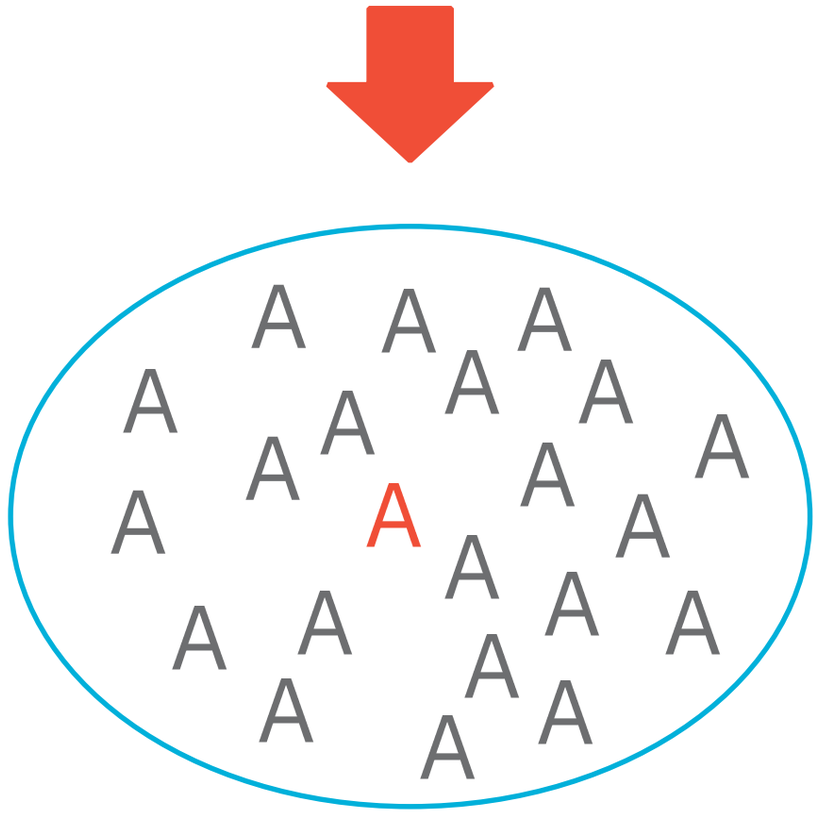
N should be chosen carefully!

Hardness of LWE

Worst-case to average-case reduction

If I can solve an instance of LWE chosen at random, then I can solve the worst possible LWE instance.

Lattices of dimension n.

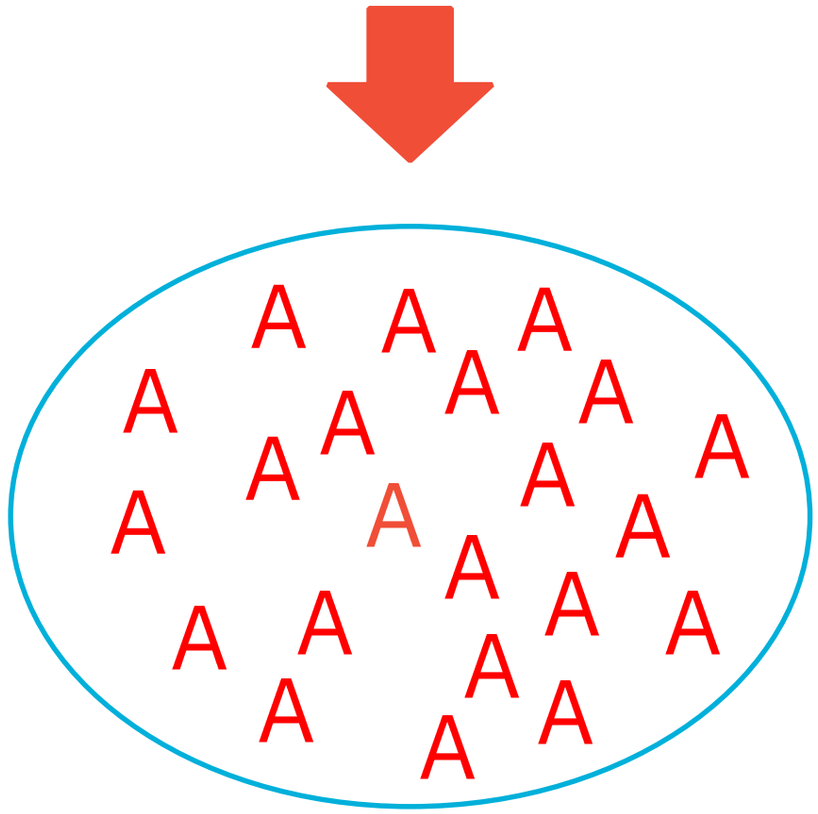


Hardness of LWE

Worst-case to average-case reduction

If I can solve an instance of LWE chosen at random, then I can solve the worst possible LWE instance.

Lattices of dimension n.



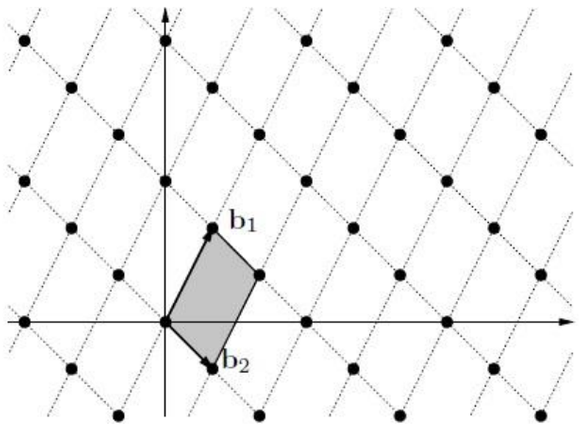
Hardness of LWE

Worst-case to average-case reduction

If I can solve an instance of LWE chosen at random, then I can solve the worst possible LWE instance.

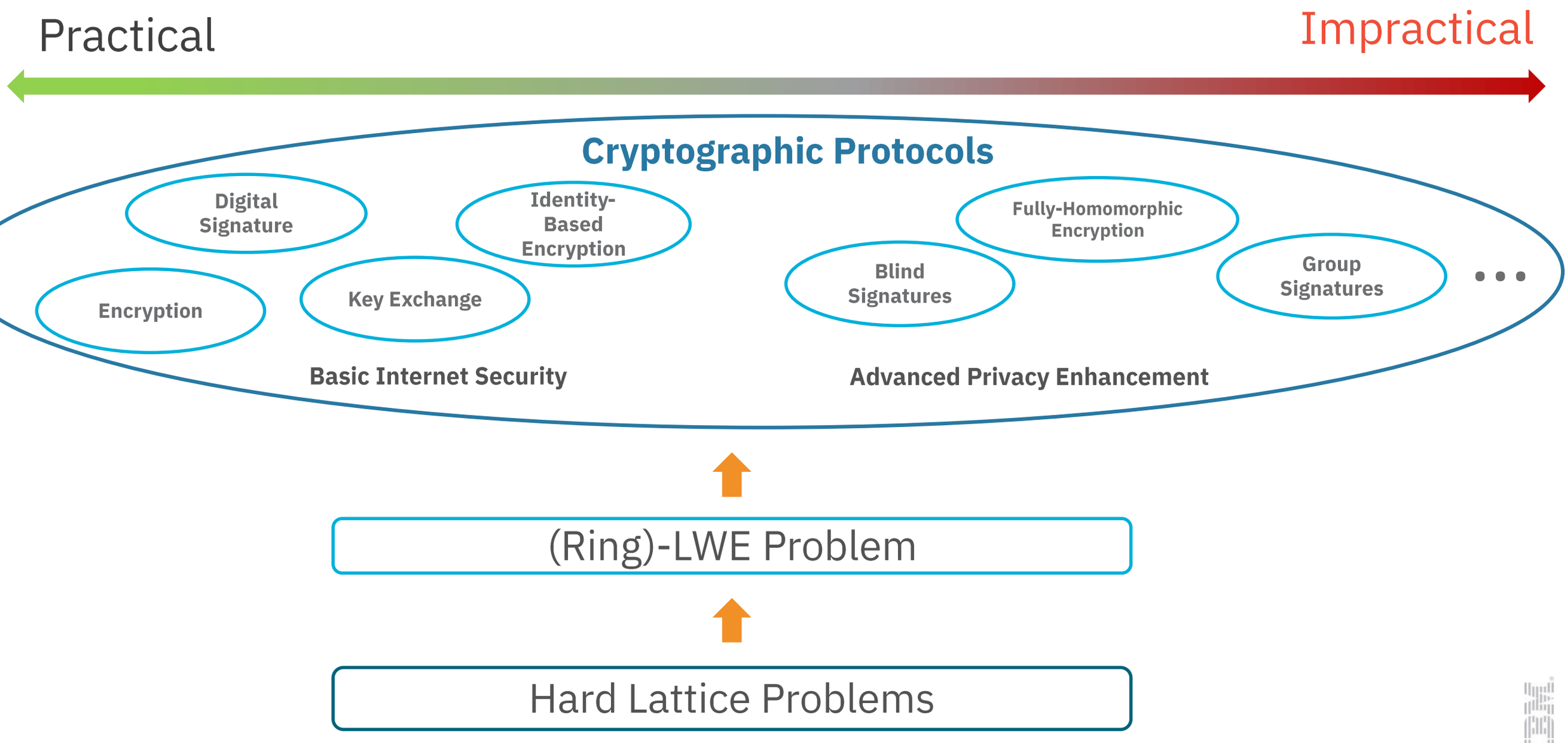
Result:

Choose a random matrix A.



LWE is hard to solve!

State of the art



Challenges

No efficient quantum resistant solutions for advanced cryptographic schemes are known.

In classic crypto advanced schemes are constructed by composing crypto primitives.

Known quantum resistant realizations of crypto primitives

- do not compose efficiently and
- lack features needed for using them as building block.

Summary:

✦ Well-studied problems

✦ Basic crypto primitives are already practical:

- Google tested a lattice-based signature (NewHope)

- NIST standardization process ongoing.

✦ Advanced protocols are the new focus of research.

THANK YOU!