SIGS Special Event in Bern

About and Beyond PKI

9.02.2017

The Quantum Apocalypse

How quantum computers can really influence the cryptographic world

Dr. François Weissbaum
VBS, FUB Kryptologie

Content

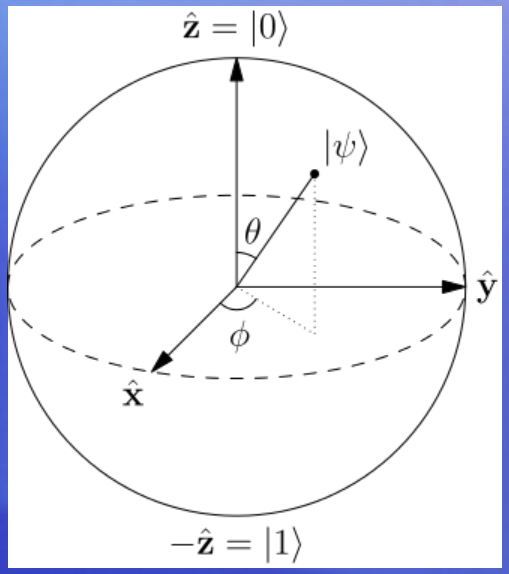
1. What is a Quantum Computer?
2. New Algorithms for Mathematics
3. Influences on Cryptography:
   a) Symmetric Algorithms
   b) Hash Functions
   c) Asymmetric Algorithms
4. Algorithms for PKI
5. Research on Post Quantum Cryptography

What is a Quantum Computer?

Classical computer:
- memory made up of bits
- each bit is either 1 or 0
- fully deterministic

A quantum computer:
- memory made up of qubits
- A single qubit can represent a one, a zero, or **any quantum superposition of those 2 qubit states**
- a pair of qubits can be in any quantum superposition of 4 states
- three qubits in any superposition of 8 states

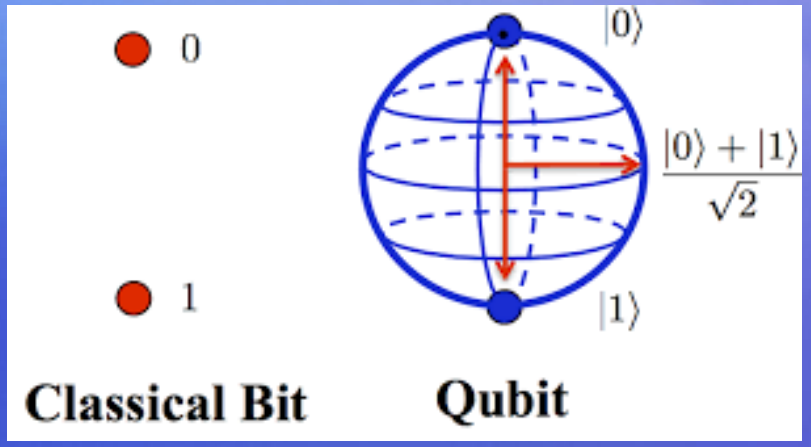
The Bloch Sphere

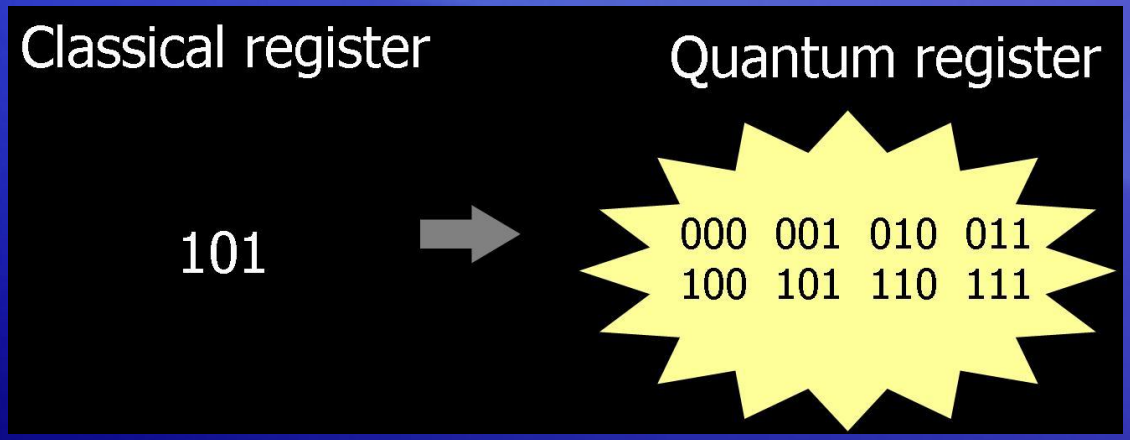


- *image from Wikipedia*

- The Bloch sphere is a representation of a qubit, the fundamental building block of quantum computers

What is a Quantum Computer?





New Algorithms for Mathematics

Which problems can be solved if a universal quantum computer would be available?

New Algorithms

Shor's algorithm (Peter Shor,1994) is a quantum algorithm for integer factorization. **It runs in polynomial time**

Classical factoring algorithm runs in sub-exponential time

Shor’s algorithm can also be used to compute discrete logarithm in polynomial time

New Algorithms

Grover's algorithm (Lov Grover,1996) is a quantum algorithm that finds with high probability a unique given value in a domain of possible values.

If N is the number of possible values, Grover's algorithm will find the given value in about $O(\sqrt{N})$ evaluations

Grover's algorithm could brute-force a 128-bit symmetric cryptographic key in roughly 2^{64} iterations

Influences on Cryptography

What are the security consequences if a universal quantum computer would be available?

Influences on symmetric algorithms

Only Grover's Algorithm can be applied against symmetric ciphers

One has to double the length of the key to reach the same level of security

Influences on symmetric algorithms

A brute force attack with a classical computer against a 128 bit symmetric cipher

is theoretically equivalently secure to

A brute force attack with a quantum computer against a 256 bit symmetric cipher against

AES-128 -> AES-256

Influences on hash functions

Only Grover's Algorithm can be applied against hash functions

Hash functions with 384 bit ore more are theoretically quantum safe

Influences on hash functions

Controversy on Hash functions with 256 bit (cf. paper of D. Bernstein):

If one has a machine with about 2^{86} Qubits, he can built an attack with a complexity about 2^{86} steps

Such an attack would also be feasible with 2^{86} classical CPU

Do we have really an advantage with a quantum computer vs. classical ?

Influences on hash functions

SHA-384 and SHA-512

SHA3-384 and SHA3-512

are quantum safe

A practicable attack against SHA-256 or SHA3-256 is not possible in a foreseeable future

Influences on asymmetric algorithms

Shor's Algorithm can be applied against factorization and discrete logarithm problems

If a universal quantum computer exists, **all** today standard asymmetric algorithms will not be secure!

Influences on asymmetric algorithms

Algorithms that are not resistant to a universal quantum computer:

- RSA
- Elliptic Curve
- Diffie-Hellmann
- ElGamal
- …

Algorithms for PKI

Which Cryptographic Primitive will be needed to build a standard PKI?

To build a standard PKI, one needs only 2 algorithms

1. Hash Function
2. Digital Signature Algorithm

Classical example:

1. SHA-256
2. RSA-2048 ← Problem!!!

Possible solutions

1. Replace a PKI with a central system (central key infrastructure), that works ***only symmetric***

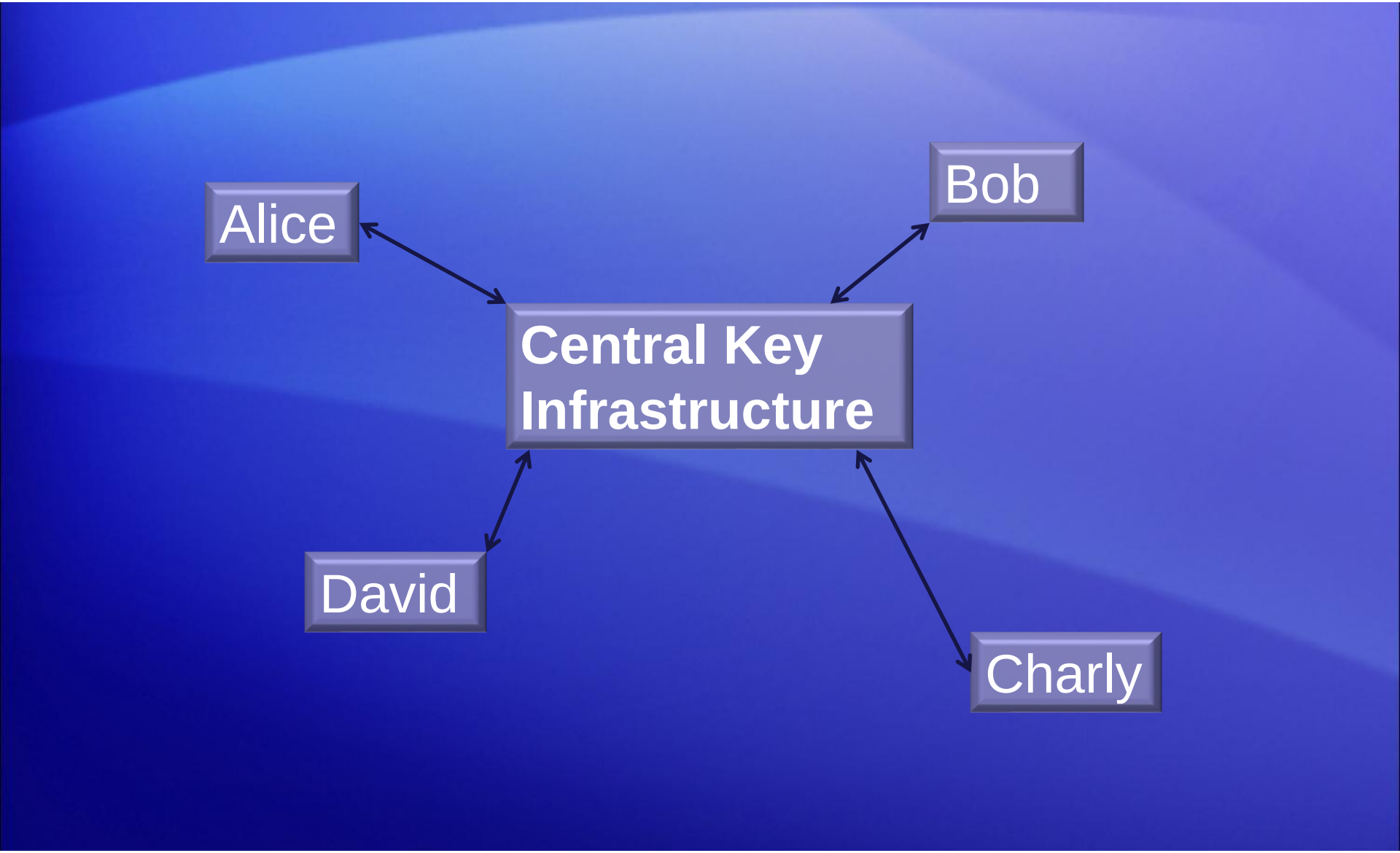
2. Find a new asymmetric algorithm that is ***Quantum Safe***

Central Key Infrastructure

When Alice wants to communicate securely with Bob, she must first contact the central key infrastructure to define a session key

The session key can be then used to encrypt or to authenticate the communication

Centralized and Symmetric Solution



Central Key Infrastructure **problems**

- Number of keys
- Availability
- Protection against hackers
- Access Control for Administrators of the central system
- …

A new asymmetric Algorithm

Researchers (Mathematicians and Cryptographers) are now studying new mathematical directions to find algorithms that are Quantum Safe

A new asymmetric Algorithm: an example

In its Chrome Browser, Google has implemented a post quantum key-exchange algorithm (to replace the Diffie-Hellman protocol)

The **New Hope Algorithm** can build a small number of connections between the browser and Google servers

It is an **unauthenticated key-exchange**

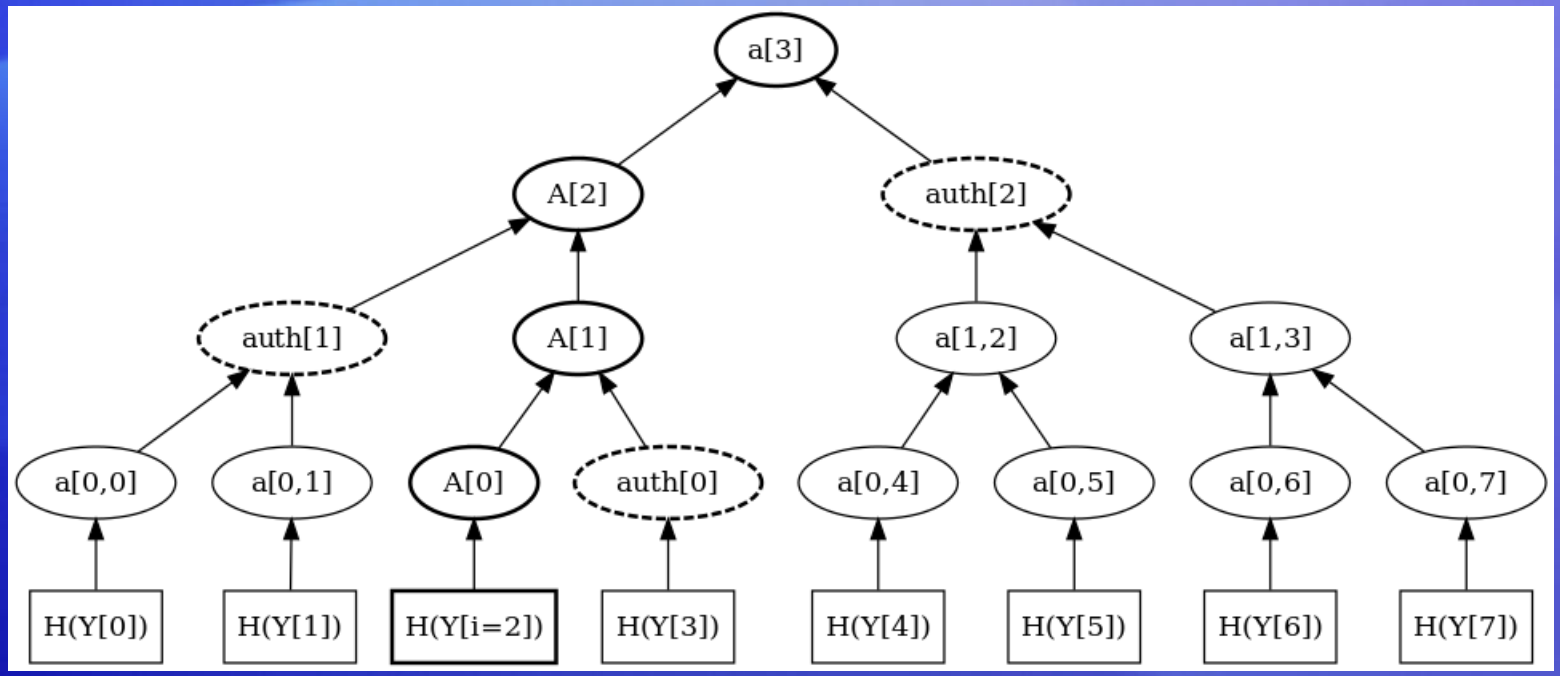
Research on Post-quantum Cryptography

Are there asymmetric algorithms that are quantum safe?

There are 4 Main Directions

1. Hash-based Cryptography
2. Code-based Cryptography
3. Lattice-based Cryptography
4. Multivariate Quadratic Equations (MQ) Cryptography

Hash Based Signature



Merkle tree with path A and authentication path for i = 2

Image from
https://en.wikipedia.org/wiki/Merkle_signature_scheme

Binary Hash Chain

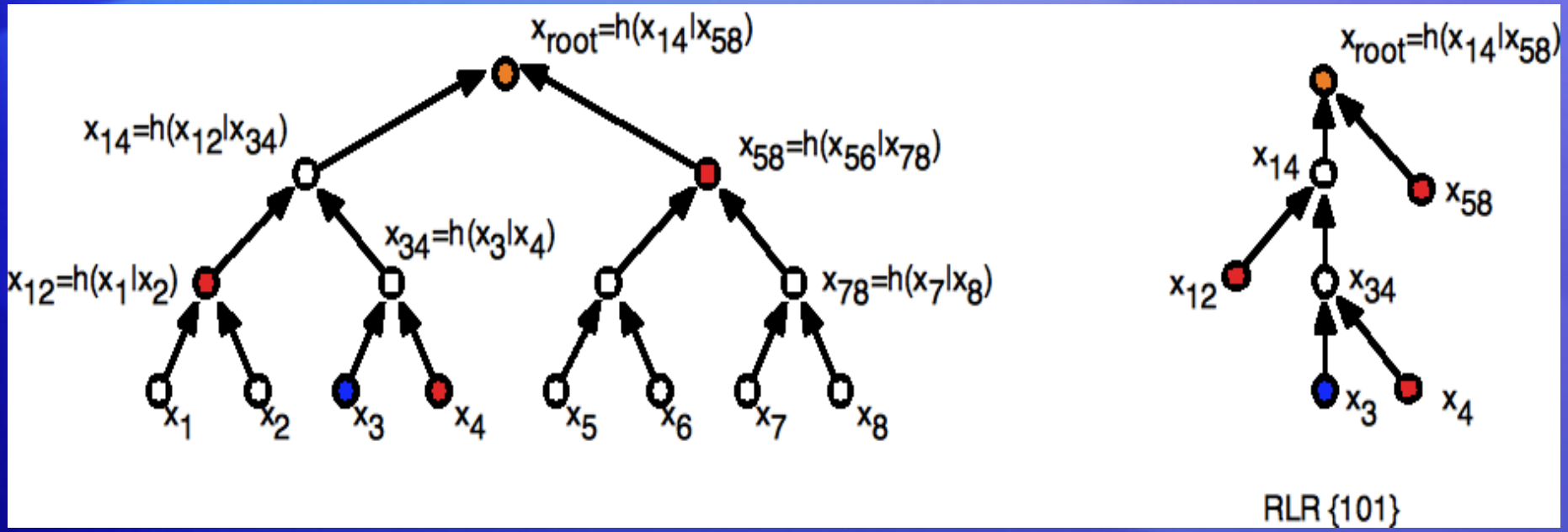


Image from
https://en.wikipedia.org/wiki/Hash_chain

Hash-Based Cryptography

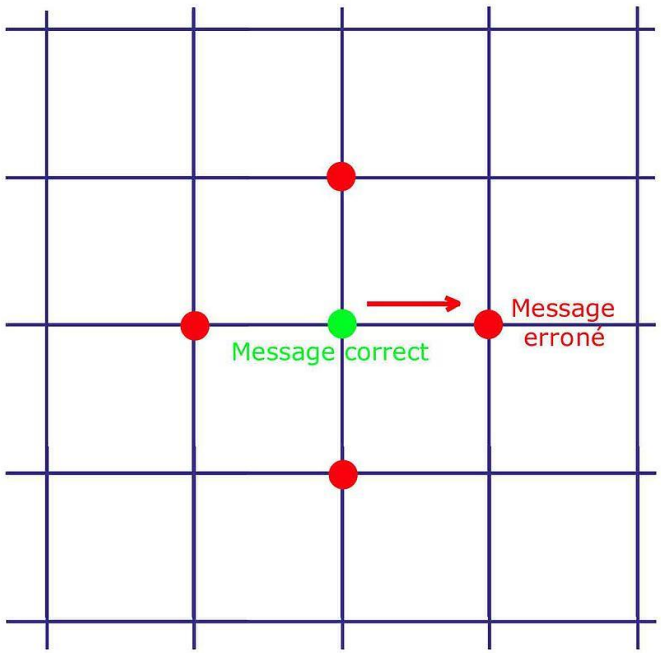
Pro:

- Well-known Primitives that are secure (SHA-512 or SHA-3)

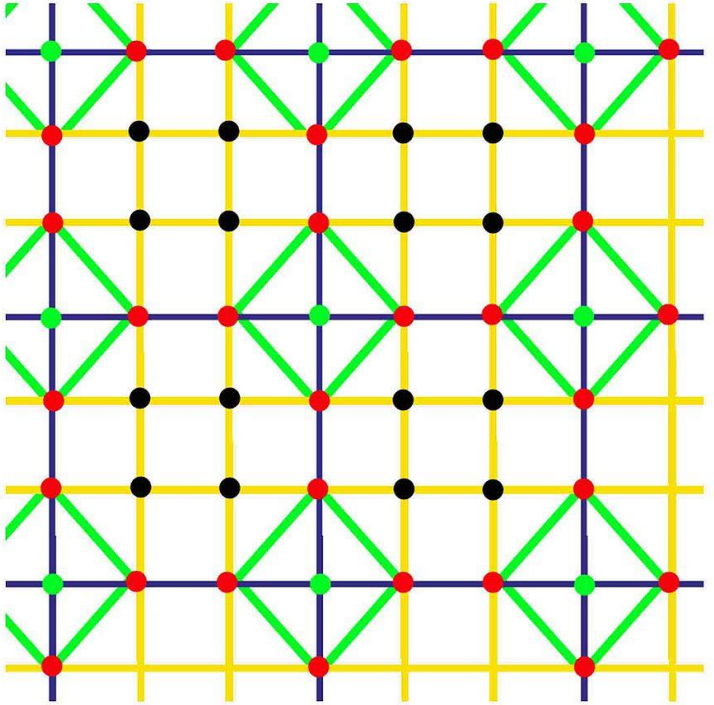
Contra:

- Need a huge number of public keys (for each message, you need a new public key…)

Code-Based Cryptography



Code sans redondance



Code correcteur

Image from
https://fr.wikipedia.org/wiki/Code_correcteur

Code-Based Cryptography

- Code Based Cryptosystems use an error correcting code
- The ciphertext is a codeword of the given code to which some errors have been added
- Only the owner of the private key can remove the errors

Code-Based Cryptography

McEliece cryptosystem. The algorithm is based on the hardness of decoding a general linear code, which is known to be NP-hard

Code-Based Cryptography

Pro:

- Starting with an NP-Hard Problem

Contra:

- For resiliency against quantum computers, the size of public key is about 8 MB

Lattice-Based Cryptography

It’s based on lattices:

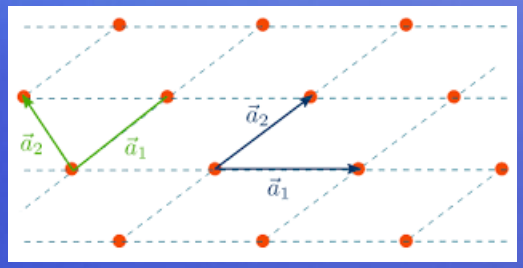
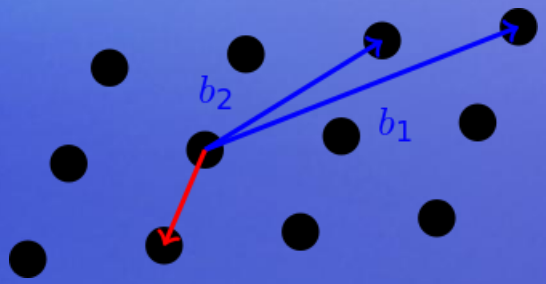


Image from
http://www.physics-in-a-nutshell.com/article/4

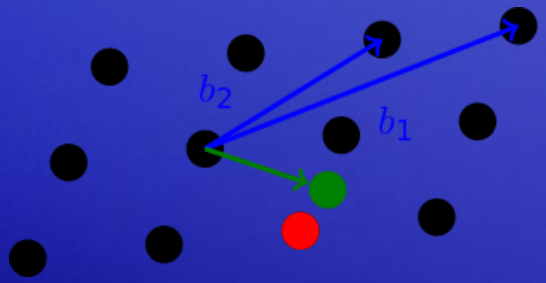
“Learning with Errors”: variant of lattice-based cryptography; security proofs demonstrate that breaking the cryptography is equivalent to solving known hard problems on lattices.

Lattice-Based Cryptography

Shortest Vector Problem (SVP):



Closest Vector Problem (CVP)



Images from
https://en.wikipedia.org/wiki/Lattice_problem

Multivariate Quadratic Equations (MQ) Cryptography

Based on multivariate polynomials over a finite field F

Polynomials of degree two are used generally (quadratics polynomials)

Solving systems of multivariate polynomial equations is proven to be NP-hard or NP-complete.

Multivariate Quadratic Equations (MQ) Cryptography

Techniques are now strong and stable

Provides the shortest signature among post-quantum algorithms

Time for Quantum Computing?

The most optimistic physicists say that the quantum computer will be built in 10 to 15 years

Today, there is **no threat** for:

- Authentication processes
- “Standard” Signature
- Encryption of information that is not long-term sensible

There is **a threat** for:

- Encryption of information that is long-term sensible
- Signature that must be valid in more than 10 years

Post-Quantum Crypto Project

The National Institute of Standards and Technology (NIST) is now accepting submissions for quantum-resistant public-key cryptographic algorithms.

The deadline for submission is **November 30, 2017.**