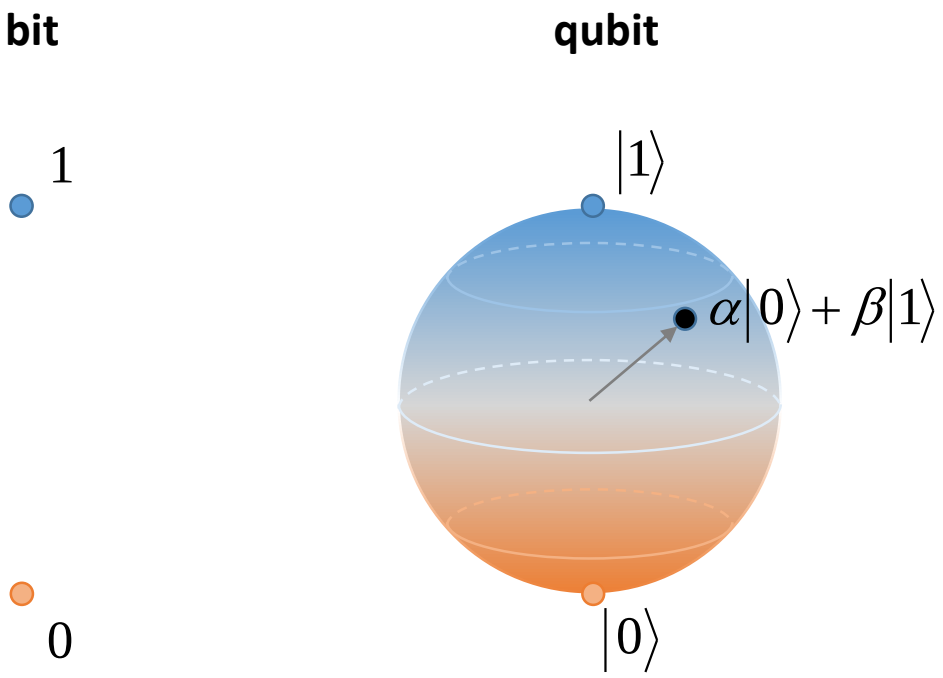
Quantum-Cryptographic Applications

Lattice-based protocols

Csatári Jakab

Quantum Computers

- Units are qubits



- More and more effective quantum computers in the last decade (IBM, Google, USTC: Zuchongzhi)

About Post-Quantum Cryptograpy (PQC)

- 1994 – Shor's algoritm
- Existing protocols CAN be broken (with powerful quantum computers)
- NIST PQC standardization: looking for quantum safe protocols

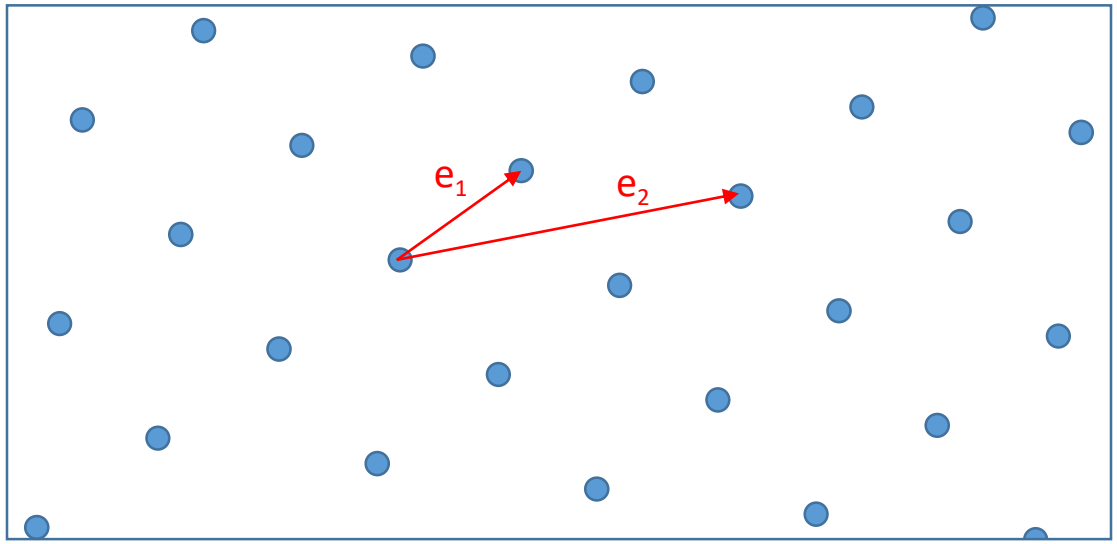
Key-encapsulation mechanisms

- CRYSTALS-KYBER
- NTRU
- SABER
- Classic McEliece

Digital signatures

- CRYSTALS-DILITHIUM
- FALCON
- Rainbow

Lattices



$$L := \left\{ \sum_{i=1}^{n} \lambda_i e_i \middle| \forall \lambda_i \in \mathbb{Z} \right\}$$

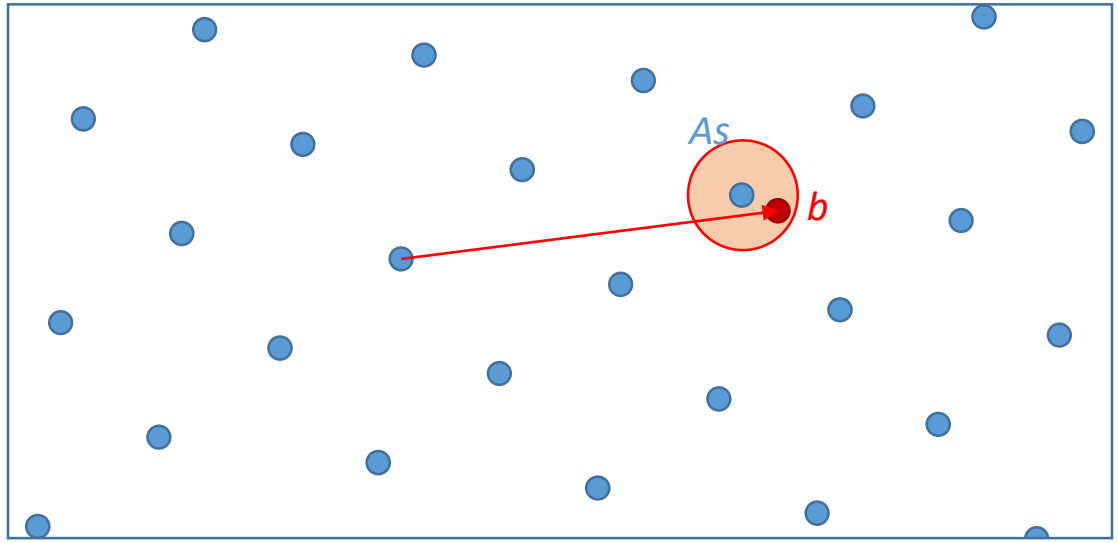
- Integer coefficients in linear combination of basis
- There are multiple hard problems related to lattices
- Ajtai: worst-case hardness of cryptographic scheme based on SVP

Learning With Errors problem (LWE)

- Given R_q ring, $s \in R_q^n$, χ distribution
- Sample: $a \in R_q^n$, $e \xleftarrow{\chi} R_q$, we compute: $(a,b) := (a, \langle a, s \rangle + e)$
- Goal: determine s from arbitrary samples

$$A = \begin{pmatrix} | & | & | & & | \\ a_1 & a_2 & a_3 & \cdots & a_m \\ | & | & | & & | \end{pmatrix} \qquad b = As + e$$

Learning With Errors problem (LWE)



$$A = \begin{pmatrix} | & | & | & & | \\ a_1 & a_2 & a_3 & \cdots & a_m \\ | & | & | & & | \end{pmatrix} \qquad b = As + e$$

- As determines the lattice:

  $L = \{v \mid v = As \pmod q\}$

In cryptographic schemes

private key: (s, e)
public key: $(A, As + e)$

KEM comparison

KYBER

- $R_q = \mathbb{Z}_q[X]/(X^n + 1)$
- uses NTT domain to multiply As
- Based on MLWE
- Faster than Frodo
  Similar to SABER

SABER

- $R_q = \mathbb{Z}_q[X]/(X^n + 1)$
- uses rounding: $[As + e]_{q \to p} = [As]_{q \to p}$
- Based on MLWR
- Faster than Frodo
  Similar to KYBER

FrodoKEM

- $R_q = \mathbb{Z}_q$
- multiplies matrices $AS + E$
- Based on LWE
- Slower than KYBER
  Slower than SABER

Note: they all are slower than those, we use today (RSA, ECC)

LWE in Digital Signatures

- LWE is also used in the PQC signature protocol – DILITHIUM
- Also uses NTT and is based on MLWE

- Performance: KeyGen is much faster than in FALCON or Rainbow
  Sign is similar for all three
  Verify is slightly slower than in FALCON or Rainbow

- Size: Much better than in Rainbow, slightly worse than in FALCON

Thank you for your attention!