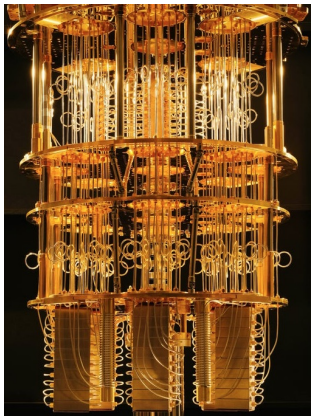
Introduction to post-quantum cryptography

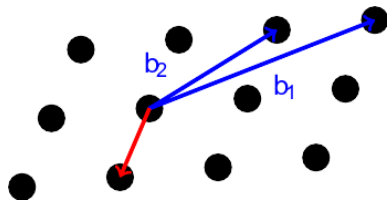
Jean-Sébastien Coron

Overview

- Quantum threat:
  - Quantum computers and their potential to break widely-used cryptosystems: RSA, ECC.

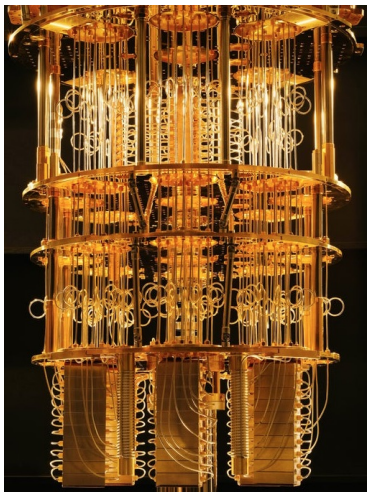


- Post-quantum algorithms:
  - Overview of algorithms believed to be secure against quantum adversaries.
  - Lattice-based, code-based, multivariate polynomial, and others.
- Introduction to lattice-based encryption
  - LWE encryption
  - RLWE encryption



The quantum threat

- Quantum computer
  - Can process a vast number of possible outcomes simultaneously, thanks to superposition of quantum states.
  - Some problems which are hard for classical computers can be solved efficiently by quantum computers.



- Potential threat to classical cryptographic algorithms
  - Shor's algorithm (1994)
  - Breaks RSA and discrete-log based cryptography, including ECC, using a quantum computer.
  - Still far from a concrete threat (number of qbits, error correction, etc.)

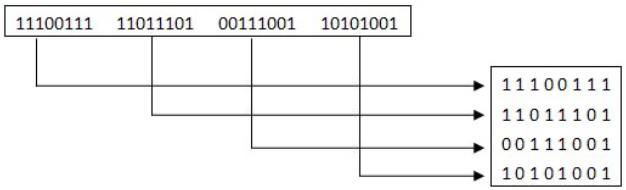
Hard problems in public-key cryptography

- Public-key cryptography is based on hard problems
  - RSA: hardness of factoring $N = pq$
  - ECC: hardness of finding d in $P = d.G$
  - We don't know any classical algorithm that can efficiently solve these problems.
  - but these problems are broken by a quantum computer

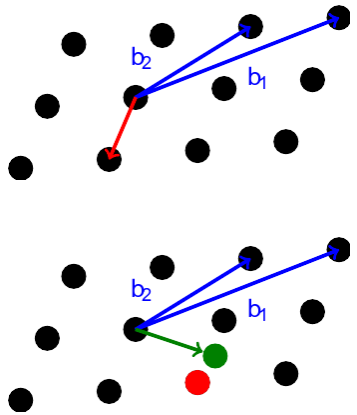
- Post-quantum hardness
  - In the quantum era, a problem should remain hard even when attacked by both classical and quantum computers.
  - Fortunately, we know many such problems !

First ideas in post-quantum cryptography

- Code-based Cryptography (McEliece, 1978)
  - Relies on the hardness of decoding a general linear code
  - McEliece's encryption scheme
  - Large key size

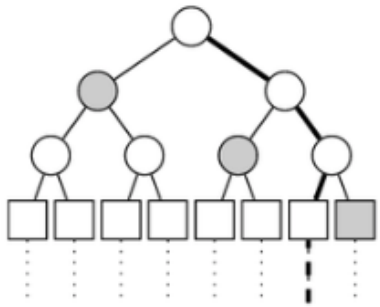


- Lattice-based cryptography
  - Based on the difficulty of certain problems in lattices (SVP and CVP)
  - NTRU (1996), a very fast public-key encryption scheme.



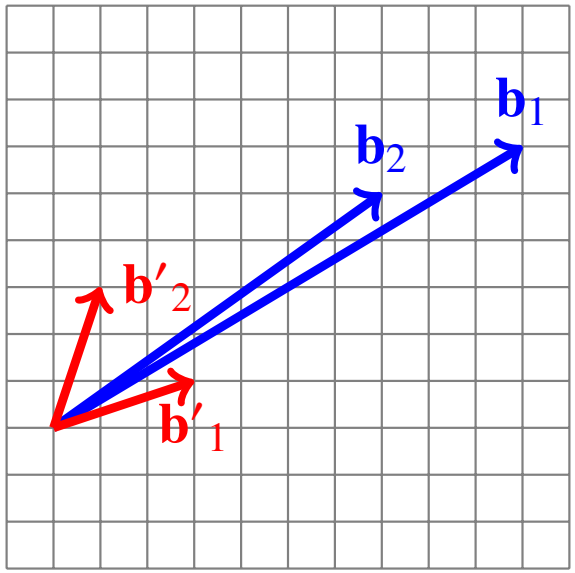
First ideas in post-quantum cryptography (2)

- Multivariate cryptography
  - Matsumoto-Imai C^* scheme (1988), HFE [P96]
  - Security relies on the difficulty of solving systems of multivariate polynomial equations.
  - Short signatures
- Hash-based cryptography (Lamport, 1979)
  - Based on the security of cryptographic hash functions.
  - Mostly used for digital signatures.



Hard lattice problems in cryptography

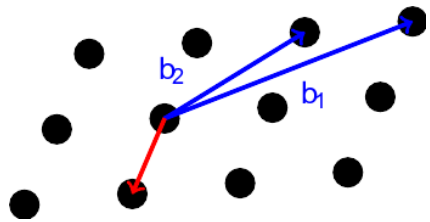
- Lattice
  - Regular grid of points in multidimensional space, defined by a basis of vectors.
- Shortest Vector Problem (SVP)
  - Given a lattice basis, find the shortest non-zero vector.
  - Believed to be hard even for quantum computers.
  - LLL algorithm provides an approximation in polynomial-time.



— Original basis
— Reduced basis

Hard lattice problems in cryptography

- Learning With Errors (LWE) [R05]:
  - Given $\vec{A} \in \mathbb{Z}_q^{\ell \times n}$ such that $\vec{A} \cdot \vec{s} = \vec{e}$ for small $\vec{e}$, recover $\vec{s}$.
- Ring-LWE and Module-LWE:
  - Variant of LWE where the secret and errors come from a polynomial ring.
  - Offers efficiency advantages.
- Significance:
  - Lattice problems serve as a foundation for many post-quantum cryptographic schemes.
  - Believed to be hard against both classical and quantum adversaries.

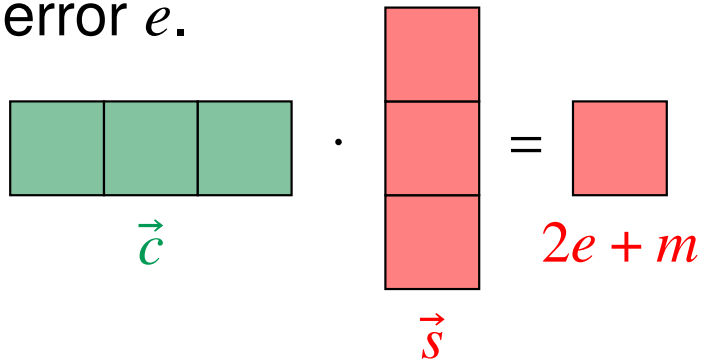


LWE-based encryption [R05]

- Key generation
  - Secret-key: $\vec{s} \in (\mathbb{Z}_q)^n$
- Encryption of $m \in \{0, 1\}$
  - A vector $\vec{c} \in \mathbb{F}_q$ such that

$$\langle \vec{c}, \vec{s} \rangle = 2e + m \pmod{q}$$

  - for a small error e.

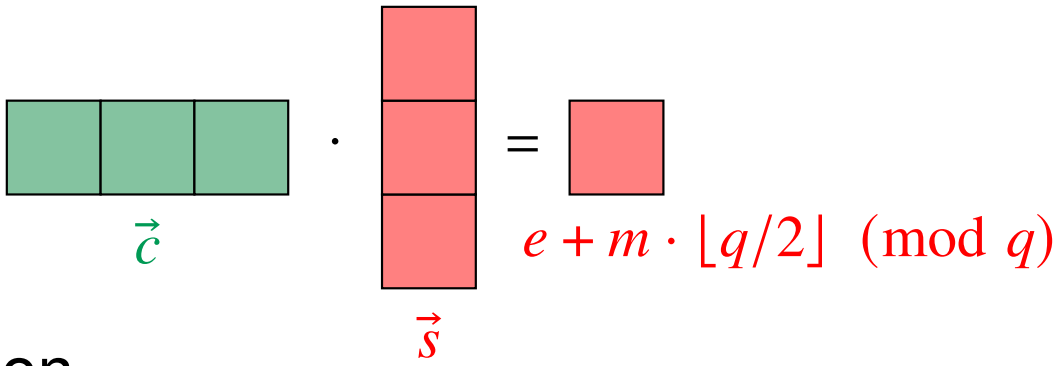


- Decryption
  - Compute $m = (\vec{c} \cdot \vec{s} \bmod q) \bmod 2$
  - Decryption works if $|e| < q/4$

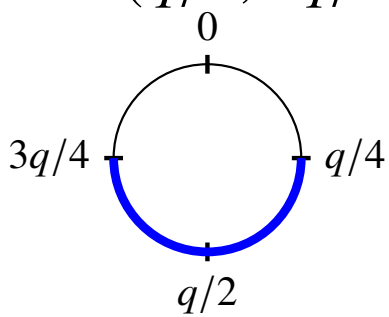
LWE-based encryption: alternative encoding

- The message m can also be encoded in the MSB.
- Encryption of $m \in \{0, 1\}$
  - A vector $\vec{c} \in \mathbb{F}_q$ such that

$$\langle \vec{c}, \vec{s} \rangle = e + m \cdot \lfloor q/2 \rfloor \pmod{q}$$



- Decryption
  - Compute $m = \mathrm{th}(\langle \vec{c}, \vec{s} \rangle \bmod q)$
  - where $\mathrm{th}(x) = 1$ if $x \in (q/4, 3q/4)$, and 0 otherwise.

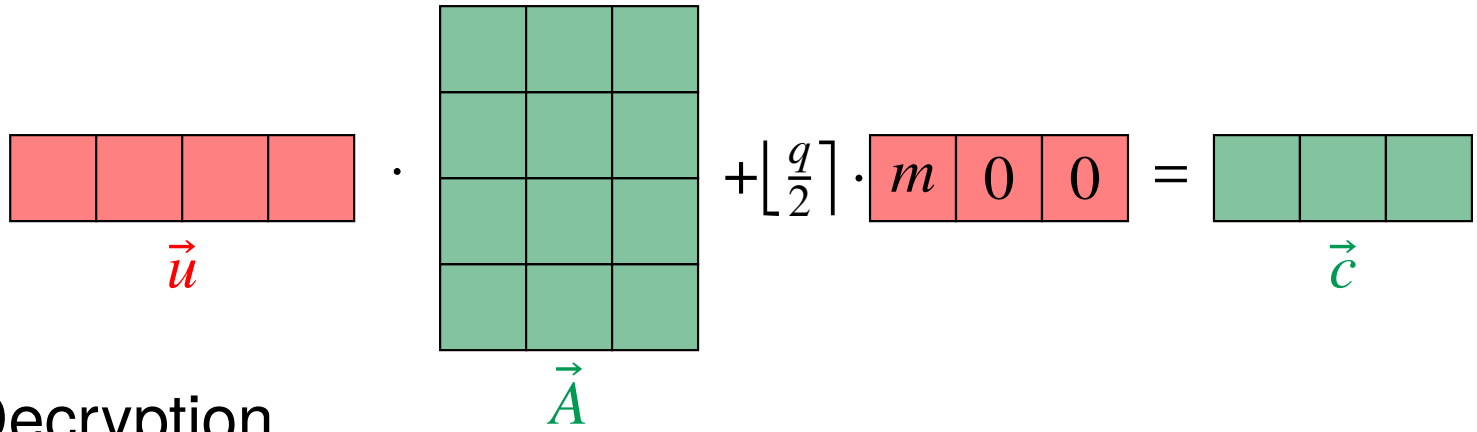


LWE-based public-key encryption

- Key generation
  - Secret-key: $\vec{s} \in (\mathbb{Z}_q)^n$, with $s_1 = 1$.
  - Public-key: $\vec{A}$ such that $\vec{A} \cdot \vec{s} = \vec{e}$ for small $\vec{e}$
    - Every row of $\vec{A}$ is an LWE encryption of 0.
- Encryption of $m \in \{0, 1\}$

$$\vec{c} = \vec{u} \cdot \vec{A} + (m \cdot \lfloor q/2 \rceil, 0, \ldots, 0)$$

  - for a small $\vec{u}$



- Decryption
  - Compute $m = \mathrm{th}(\langle \vec{c}, \vec{s} \rangle \bmod q)$

RLWE-based schemes

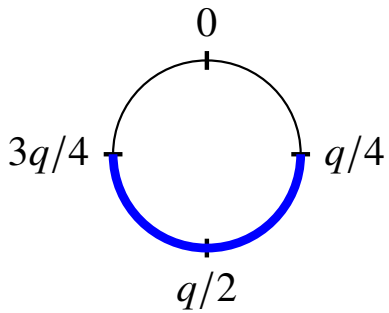
- RLWE-based scheme
  - We replace $\mathbb{Z}_q$ by the polynomial ring $R_q = \mathbb{Z}_q[x]/< x^\ell + 1 >$, where ℓ is a power of 2.
  - Addition and multiplication of polynomials are performed modulo $x^\ell + 1$ and prime q.
  - We can take $m \in R_2 = \mathbb{Z}_2[x]/< x^\ell + 1 >$ instead of $\{0, 1\}$: more bandwidth.
- Ring Learning with Error (RLWE) assumption [LPR13]
  - $t = a \cdot s + e$ for small s, $e \leftarrow R$
  - Given t, a, it is difficult to recover s.

RLWE-based public-key encryption

- Key generation
  - $t = a \cdot s + e$ for random $a \leftarrow R_q$ and small $s, e \leftarrow R$.
- Public-key encryption of $m \in R_2$
  - $c = (a \cdot r + e_1,\ t \cdot r + e_2 + \lfloor q/2 \rceil m)$, for small e_1, e_2 and r.
- Decryption of $c = (u, v)$
  - Compute $m = \mathsf{th}(v - s \cdot u)$

$$\begin{aligned} v - s \cdot u &= t \cdot r + e_2 + \lfloor q/2 \rceil m - s \cdot (a \cdot r + e_1) \\ &= (t - a \cdot s) \cdot r + e_2 + \lfloor q/2 \rceil m - s \cdot e_1 \\ &= \lfloor q/2 \rceil m + \underbrace{e \cdot r + e_2 - s \cdot e_1}_{\text{small}} \end{aligned}$$

  - $m \in R_2 = \mathbb{Z}_2[x]/<x^\ell + 1>$: more bandwidth.



Conclusion

- Quantum threat
  - Quantum computers can undermine existing cryptographic infrastructure.
  - this prompts a shift to post-quantum algorithms
- Post-quantum algorithms
  - Lattice-based, code-based, and multivariate polynomial have emerged as viable alternatives.

References

R05 Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC 2005: 84-93.

LPR13 Vadim Lyubashevsky, Chris Peikert, Oded Regev: On Ideal Lattices and Learning with Errors over Rings. J. ACM 60(6): 43:1-43:35 (2013).