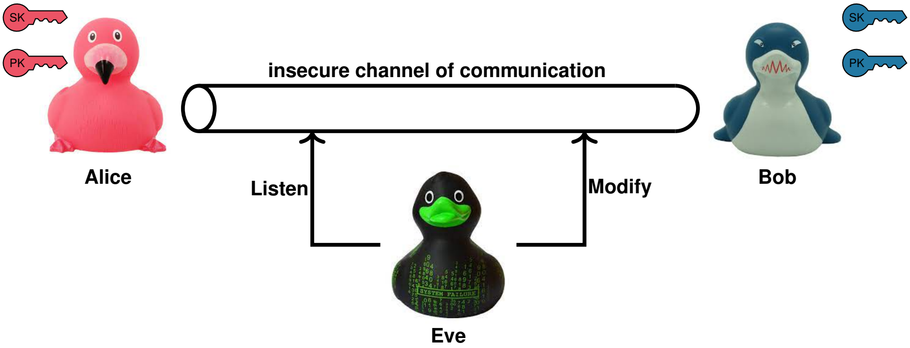
Quantum Algorithms for Lattice-based Cryptography

Yixin Shen

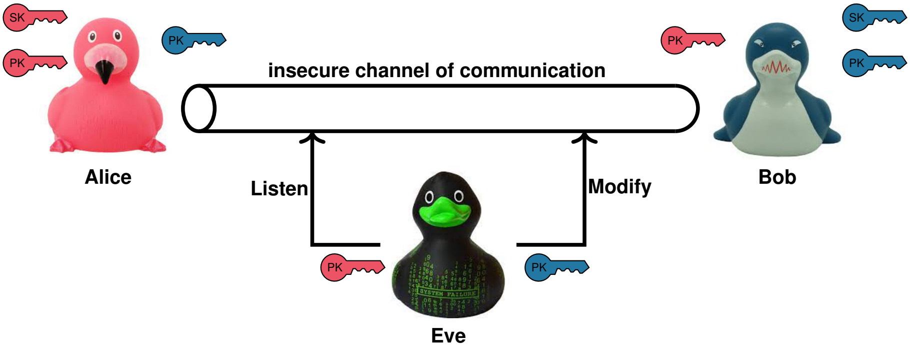
November 4, 2022

Hard Problems in Public Key Cryptography



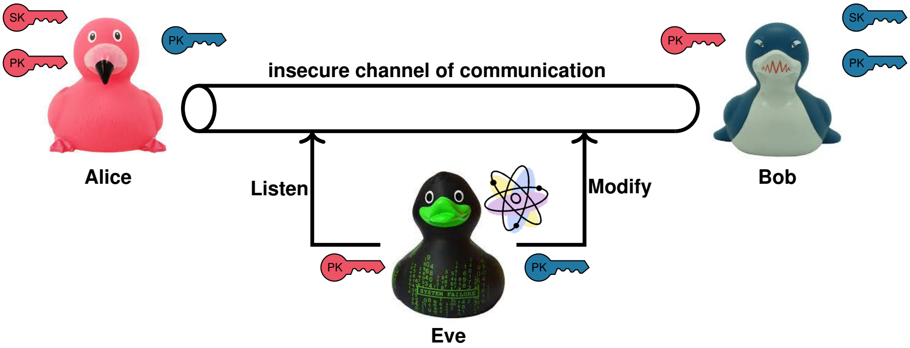
factorisation, discrete logarithm

Hard Problems in Public Key Cryptography



factorisation, discrete logarithm

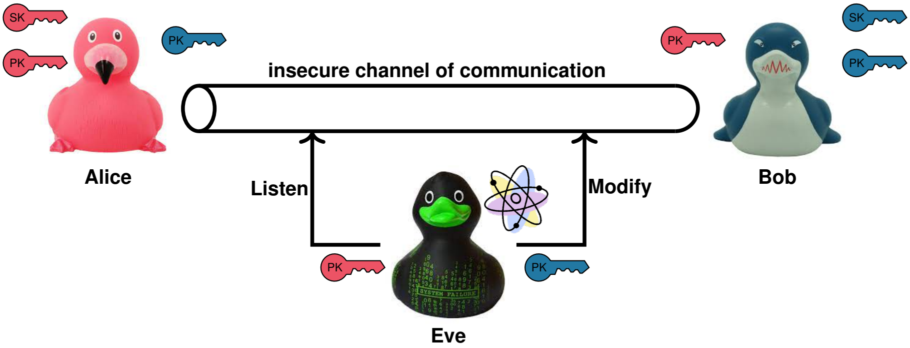
Hard Problems in Public Key Cryptography



~~factorisation, discrete logarithm~~

lattices, codes, ...

Hard Problems in Public Key Cryptography



~~factorisation, discrete logarithm~~

lattices, codes, ...

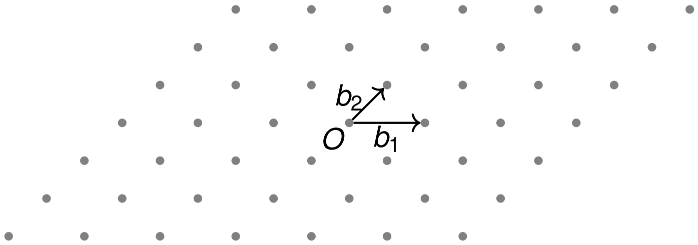
NIST selected algorithms:

- encryption: the only selected candidate is based on lattices
- signatures: 2 out of 3 based on lattices

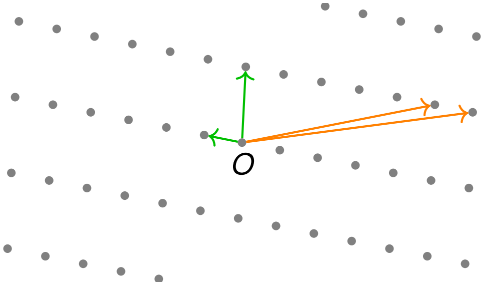
What is a (Euclidean) lattice?

Definition

$\mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \left\{\sum_{i=1}^{n} x_i \boldsymbol{b}_i : x_i \in \mathbb{Z}\right\}$ where $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is a basis of $\mathbb{R}^n$.

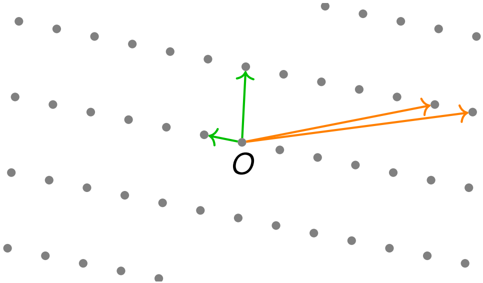


Lattice-based cryptography: fundamental idea



- good basis: private information, makes problem easy
- bad basis: public information, makes problem hard

Lattice-based cryptography: fundamental idea

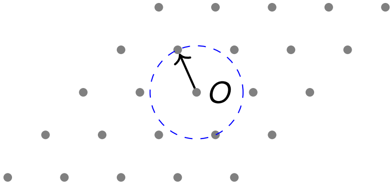


- good basis: private information, makes problem easy
- bad basis: public information, makes problem hard

Basis reduction: transform a bad basis into a good one
Main tool: BKZ algorithm and its variants

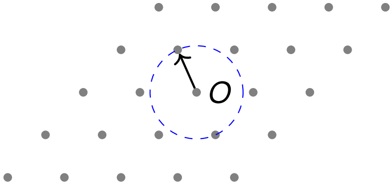
Requires to solve the (approx-)SVP problem in smaller dimensions.

The Shortest Vector Problem

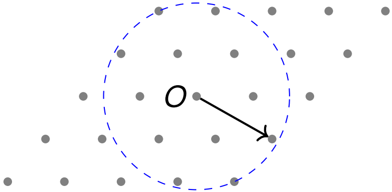


Shortest Vector Problem (SVP):
Given a basis for the lattice $\mathcal{L}$, find a shortest nonzero lattice vector.
$\lambda_1(\mathcal{L})$ = length of such a vector.

The Shortest Vector Problem



Shortest Vector Problem (SVP):
Given a basis for the lattice $\mathcal{L}$, find a shortest nonzero lattice vector.
$\lambda_1(\mathcal{L})$ = length of such a vector.



γ-approx-SVP ($\gamma > 1$):
Given a basis of $\mathcal{L}$, find a nonzero lattice vector of length at most $\gamma \cdot \lambda_1(\mathcal{L})$.
γ is approximation factor.

The Shortest Vector Problem

Depending on the dimension n:

- NP-Hardness (randomized reduction)
- NP $\cap$ co-NP
- Subexponential-time algorithms
- Poly-time algorithms

Approx factor:

- $O(1)$
- $\sqrt{n}$
- $2^{\sqrt{n}}$
- $2^{\frac{n \log \log n}{\log n}}$

The Shortest Vector Problem

Depending on the dimension n:

- NP-Hardness (randomized reduction)
- NP $\cap$ co-NP
- Subexponential-time algorithms
- Poly-time algorithms

Approx factor:

- $O(1)$
- $\sqrt{n}$
- $2^{\sqrt{n}}$
- $2^{\frac{n \log \log n}{\log n}}$

Main approaches for SVP:

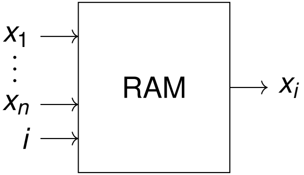
- Enumeration: $2^{O(n\log(n))}$ time and $\mathrm{poly}(n)$ space
- Sieving: $2^{O(n)}$ time and $2^{O(n)}$ space

Interlude: quantum memory models

classical access

quantum access

classical data



standard

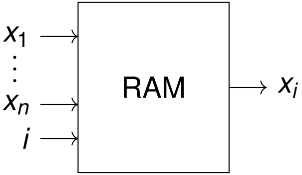
quantum data

Assumption: $O(1)$ time cost

Interlude: quantum memory models

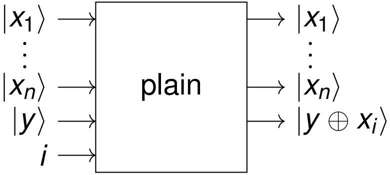
classical access | quantum access

classical data



standard

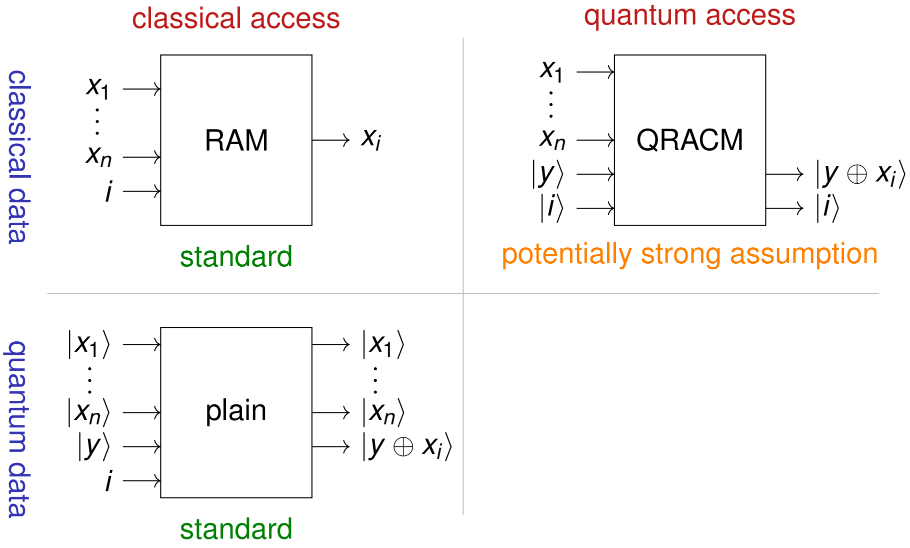
quantum data



standard

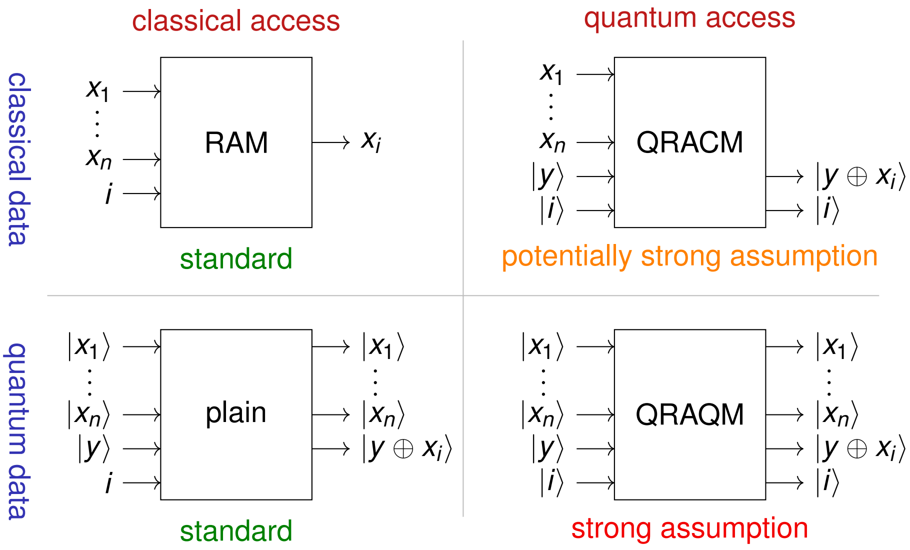
Assumption: $O(1)$ time cost

Interlude: quantum memory models



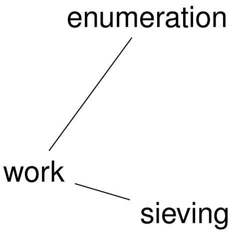
Assumption: $O(1)$ time cost

Interlude: quantum memory models



Assumption: $O(1)$ time cost

Overview of my work



Overview of my work

- work
  - enumeration
    - quantum circuit [ANS18]
    - VQE [APSW22*]
  - sieving

Overview of my work

- work
  - enumeration
    - quantum circuit [ANS18]
    - VQE [APSW22*]
  - sieving
    - provable [ACKS21]
    - heuristic [BCSS22*]

Overview of my work

- work
  - enumeration
    - quantum circuit [ANS18]
    - VQE [APSW22*]
  - sieving
    - provable [ACKS21]
      - quantum circuit
      - QRACM
    - heuristic [BCSS22*]
      - QRAQM

Overview of my work

- work
  - enumeration
    - quantum circuit [ANS18]
    - VQE [APSW22*]
  - sieving
    - provable [ACKS21]
      - quantum circuit
      - QRACM
    - heuristic [BCSS22*]
      - QRAQM
  - LWE

Overview of my work

- work
  - enumeration
    - quantum circuit [ANS18]
    - VQE [APSW22*]
  - sieving
    - provable [ACKS21]
      - quantum circuit
      - QRACM
    - heuristic [BCSS22*]
      - QRAQM
  - LWE
    - QRACM [AS22*]
    - classical [CST22*]

Overview of my work

- work
  - enumeration
    - quantum circuit [ANS18]
    - VQE [APSW22*]
  - sieving
    - provable [ACKS21]
      - quantum circuit
      - QRACM
    - heuristic [BCSS22*]
      - QRAQM
      - future work: quantum circuit?
  - LWE
    - QRACM [AS22*]
    - classical [CST22*]