IEGULDĪJUMS TAVĀ NĀKOTNĒ

Classical cryptography that is secure against quantum computers?

Andris Ambainis

University of Latvia

European Social Fund project “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku” Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Quantum computing

- New model of computation based on quantum physics.
- More powerful than conventional computing.

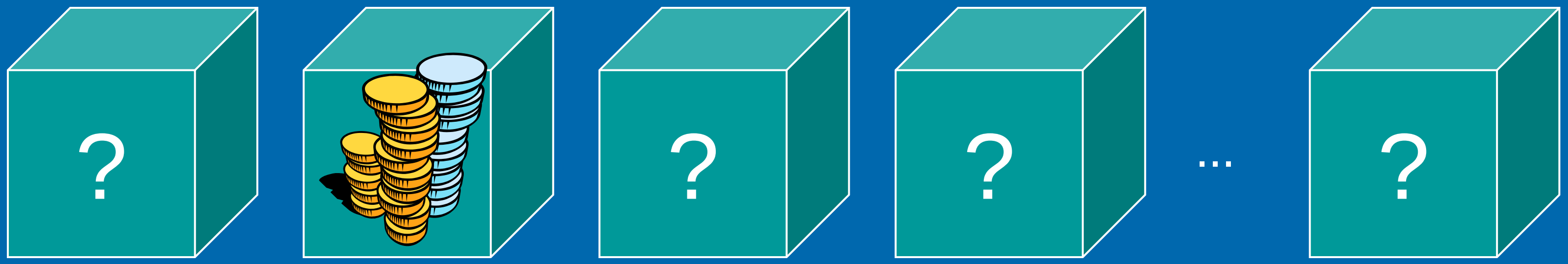
Factoring

- 6231540623 = 93599 * 66577.
- Find 6231540623?

- For large (300 digit) numbers conventional computers are too slow.

Shor, 1994: quantum computers can factor large numbers efficiently.

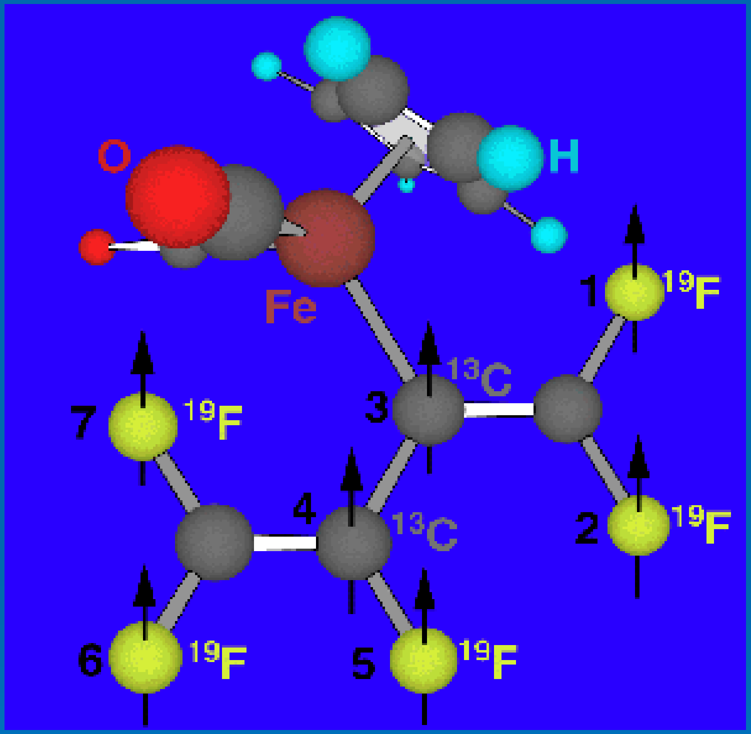
Quantum search



- N objects;
- Find an object with a certain property.

Grover, 1996: can be done in $O(\sqrt{N})$ quantum steps.

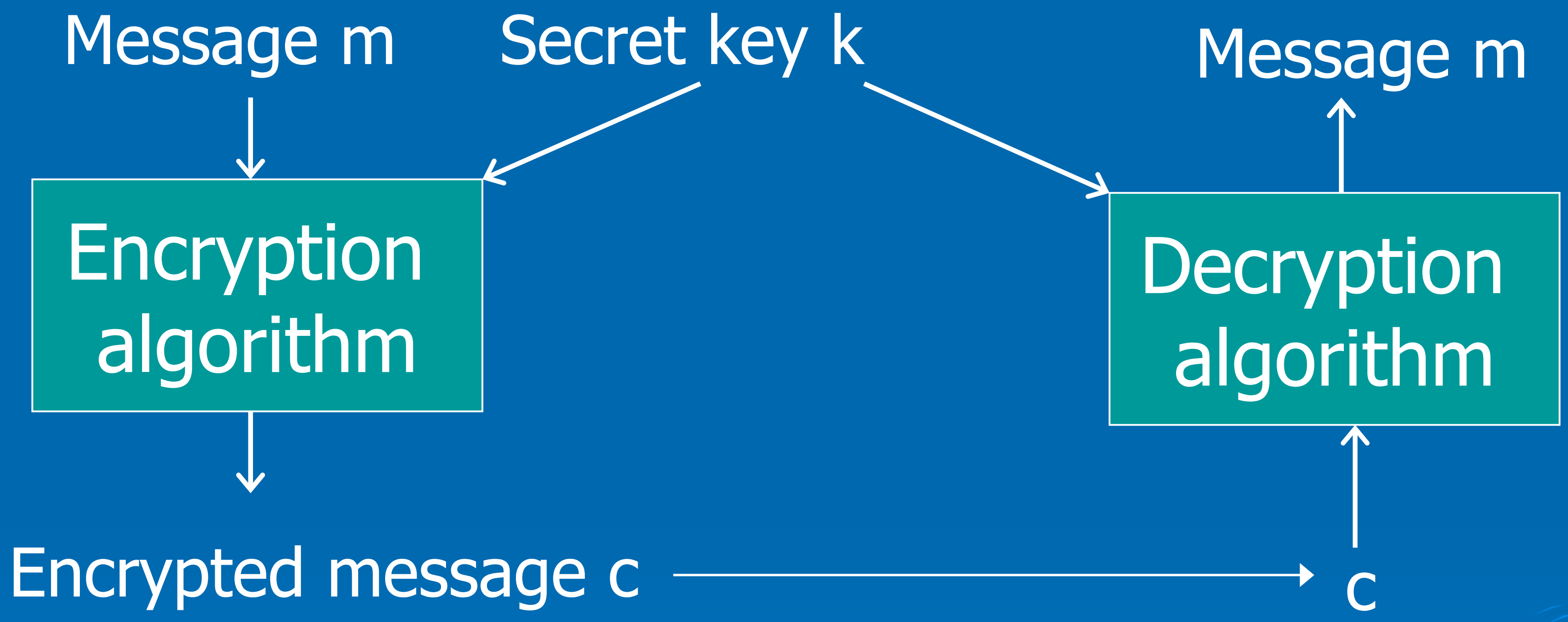
13 bit quantum computer (MIT/Waterloo, 2004)



- Quantum computer = molecule.
- Quantum bits = nuclear spins.
- Manipulate nuclear spins with magnetic field.

Post-quantum cryptography

Cryptography



Symmetric cryptography: same key k for encryption and decryption

4-rotor Enigma, 1942

Codebreaking by exhaustive search

- For each k, test:

Message m → Encryption algorithm → Encrypted message c

↑

Secret key k

Classically: N steps;

Quantum (Grover): O(√N) steps.

Codebreaking by exhaustive search

- 64 bit key $\rightarrow$ $N = 2^{64}$ secret keys.

$N = 2^{64} \approx 18{,}000{,}000{,}000{,}000{,}000{,}000.$
$\sqrt{N} = 2^{32} \approx 4{,}294{,}000{,}000.$

Is this a big advantage for quantum computers?

128 bit key $\rightarrow$ $N = 2^{128}$, $\sqrt{N} = 2^{64}$.

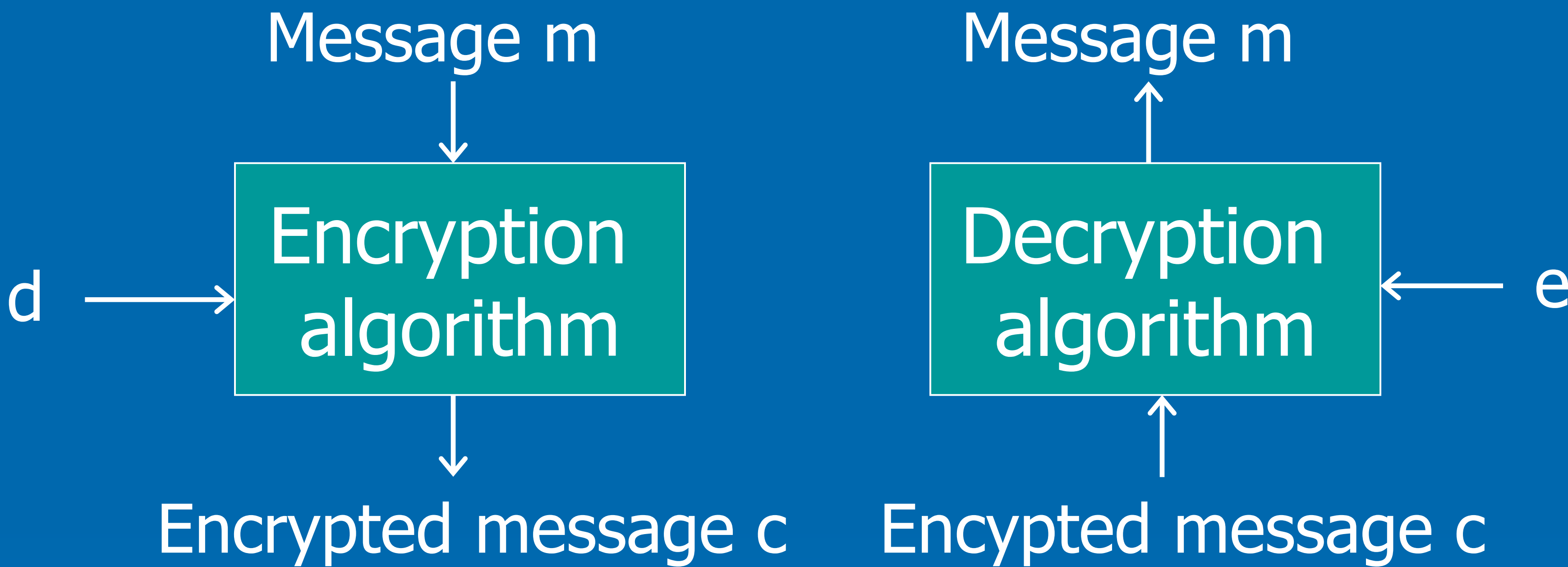
Cryptography

4252 1890 6767 1345

amazon.com

Where do we get a secret key?

Public-key cryptography (RSA, 1977)



One key for encryption – d, one for decryption – e.

Computing e from d – difficult.

Public key cryptography

e

Encrypt(4252 ..., e)

amazon.com

4252 1890 6767 1345

Eavesdropper does not have decryption key d

RSA

- Rivest, Shamir, Adleman, 1977;
- Computing decryption key d from encryption key e is roughly equivalent to factoring a large number.
- Factoring large (300-digit) number N = pq into p and q is very difficult.

Factoring becomes easy if we have a quantum computer.

Lattice-based cryptography

Lattices

- Set of vectors $v_1, \ldots, v_m$ in n dimensions;
- Lattice L = { $a_1v_1+\ldots+a_mv_m$:
  $a_1, \ldots, a_m$ - integers}.
- Shortest vector problem (SVP): given $v_1, \ldots, v_m$, find the shortest vector in L.

Breaking a lattice-based cryptosystem ≈ SVP

Versions of SVP

- SVP: find the shortest vector v_{min} in L;
- γ-SVP: find a vector v: $||v|| \leq \gamma\ ||v_{min}||$;
- γ-Unique-SVP: find v_{min} if we are promised that $||v|| \geq \gamma\ ||v_{min}||$, unless $v = c \bullet v_{min}$.

SVP is NP-hard;
Hardness of γ-SVP and γ-Unique-SVP depends on γ.

γ-Unique-SVP

- Task: find v_{min} if we are promised that $||v|| \geq \gamma \, ||v_{min}||$, unless $v = c \bullet v_{min}$.
- Lenstra-Lenstra-Lovasz, 1982: efficiently solvable if $\gamma = 2^n$.
- Thought to be difficult for classical algorithms if $\gamma = n^c$.
- Regev, 2002: idea for quantum algorithm.

Quantum state

- States of a classical system: 1, 2, ..., n.
- Quantum system: basis states $|1\rangle$, $|2\rangle$, ..., $|n\rangle$.
- General state: $a_1|1\rangle + a_2|2\rangle + \ldots + a_n|n\rangle$

$$|a_1|^2 + |a_2|^2 + \ldots + |a_n|^2 = 1$$

- For example: $\frac{4}{5}|1\rangle + \frac{3}{5}|2\rangle$

Measurements

$$|\Psi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \dots + \alpha_M |M\rangle$$

Measurement

	1	2	…	M
prob.	$\lvert\alpha_1\rvert^2$	$\lvert\alpha_2\rvert^2$		$\lvert\alpha_M\rvert^2$

We can apply transformations on $|\Psi\rangle$ without measuring it.

Partial measurements

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Measure the 1st bit

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle \qquad \alpha_{10}|10\rangle + \alpha_{01}|11\rangle$$

Quantum algorithm for SVP?

- Set of vectors $v_1, \ldots, v_m$ in n dimensions;
- Lattice L = { $a_1v_1+\ldots+a_mv_m$:

  $a_1, \ldots, a_m$ - integers}.
- Task: find v_{min} if we are promised that $\|v\| \geq \gamma \|v_{min}\|$, unless $v = c \bullet v_{min}$.

Step 1: prepare

$$\sum_{a_1,\ldots,a_n \in \{-M,\ldots,M\}} \left| a_1x_1 + a_2x_2 + \ldots + a_mx_m \right\rangle$$

Quantum algorithm for SVP?

Step 2: measure the most significant bits of

$$\sum_{a_1,\ldots,a_n\in\{-M,\ldots,M\}} \left| a_1x_1 + a_2x_2 + \ldots + a_mx_m \right\rangle$$

Result:

$$\left|x\right\rangle + \left|x+v_{\min}\right\rangle$$

$$\left|x\right\rangle + \left|x+v_{\min}\right\rangle + \left|x+2v_{\min}\right\rangle$$

Missing step

- How do we get v_{min} from

$$\left| x \right\rangle + \left| x + v_{\min} \right\rangle ?$$

Measuring the state gives x or $x+v_{min}$, but not v_{min}.

Period-finding

- Basis states |1⟩, |2⟩, ..., |N⟩.
- State

$$|x\rangle + |x+r\rangle + |x+2r\rangle + \ldots + |x+kr\rangle$$

$$\Big\Downarrow \text{ Quantum Fourier Transform}$$

One of numbers $\frac{N}{r}, \frac{2N}{r}, \ldots$

Open problems

- Can we extract v_{min} from

$$|x\rangle + |x + v_{\min}\rangle ?$$

- Applying QFT + measuring provides enough information;
- Computing v_{min} from this information is difficult.
- Other versions of SVP?

McEliece cryptosystem

McEliece cryptosystem

- Based on coding theory;
- Public key:

$$G = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

Matrix of an error-correcting code + some scrambling

- Private key: how G was generated.

McEliece cryptosystem

$$v = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \longrightarrow Gv = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Decoding Gv $\rightarrow$ v can be performed if we know the structure of G.

Key size

- Key = k*n matrix

$$G = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

- Typical parameters: k = 3556, n = 4084.
- Encryption key = 1.5 Mbytes.

Attack by quantum search.
Can be defeated by increasing key size 4 times.