EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA

IEGULDĪJUMS TAVĀ NĀKOTNĒ

Theory of quantum computing

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 computing, based on quantum mechanics.
- More powerful than conventional (classical) computing.

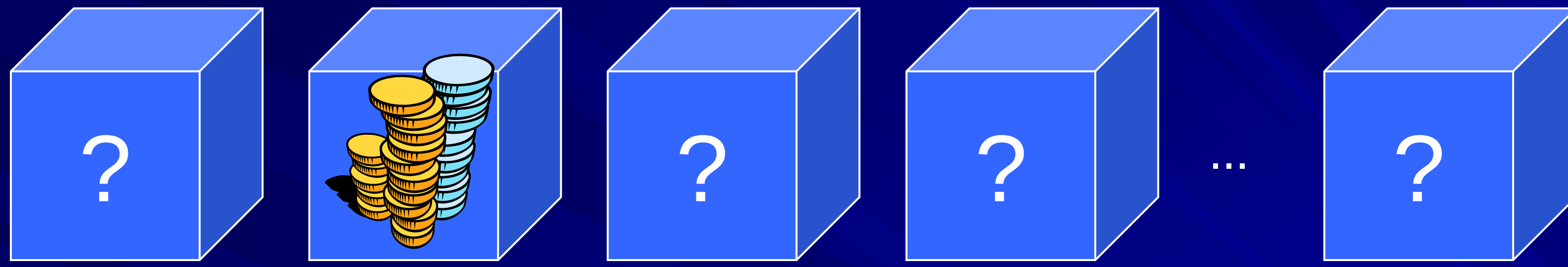
Factoring

- 6231540623 = 93599 * 66577.
- Given 6231540623, find factors?

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

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

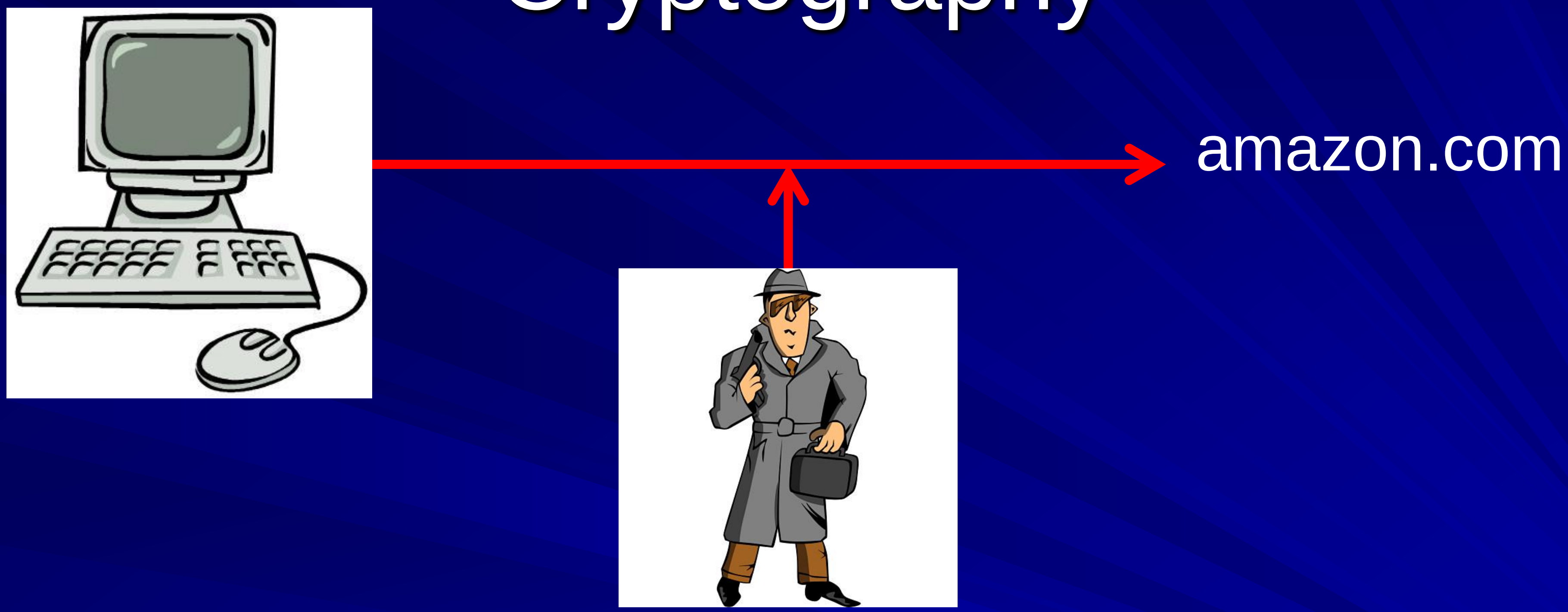
Quantum search



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

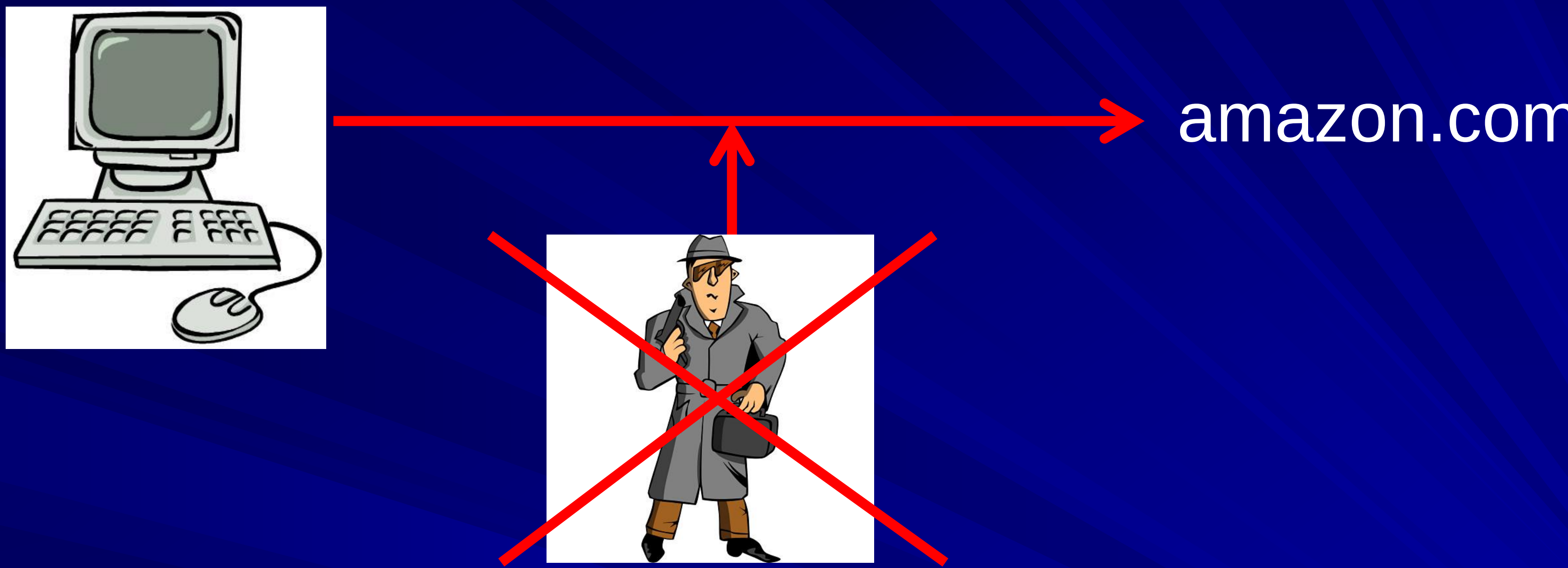
Grover, 1996: can be done in O(√N) quantum steps.

Cryptography



- Two parties who want to communicate secret information.
- Communication channel that may be eavesdropped.

Quantum cryptography



- If quantum state (e.g. polarization of photon) is measured, the measurement changes the state .

  Security guaranteed by quantum mechanics.

Implementing quantum cryptography

- Transmitting quantum information:
  - Faint laser pulse (1 photon per pulse) + polarizer;
- Receiving quantum information:
  - polarizing beam splitter + single photon detector.

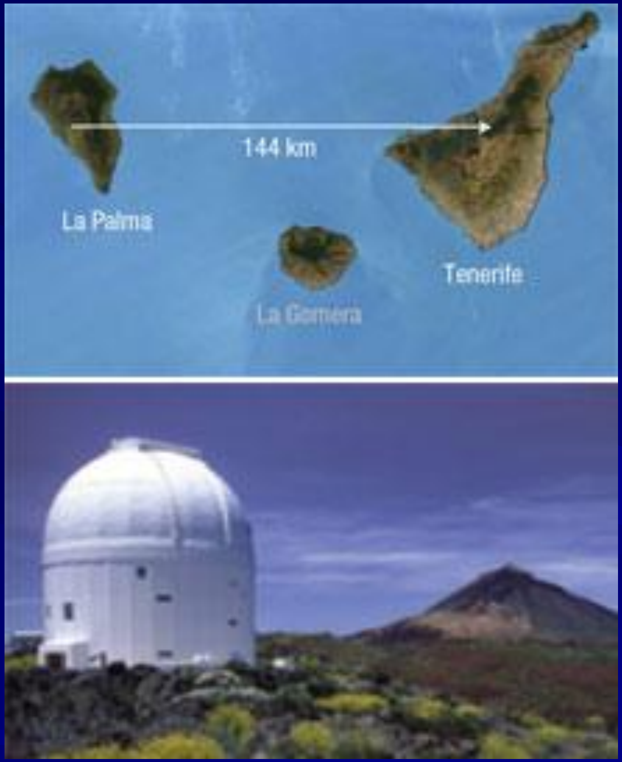
Commercially available systems

MagiQ Technologies

Toshiba

- Quantum communication over optical cable.
- 1Mb/s over 20km distance.
- 10 kb/s over 100km distance.

Next steps



Quantum communication over air

Quantum communication via satellites

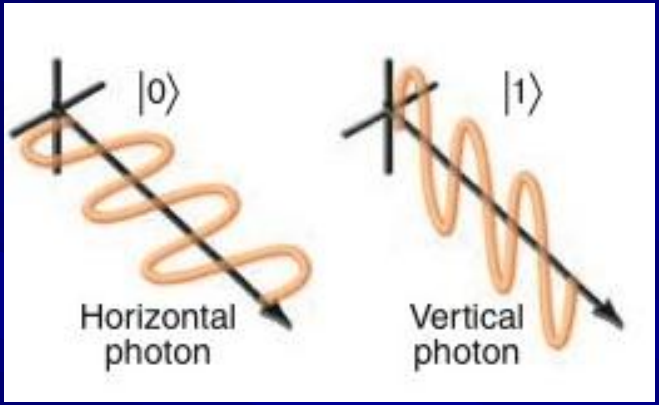
Implementing quantum computing

Divincenzo criteria (1997):

- Well defined quantum bits;
- Reliable state preparation;
- Low decoherence;
- Accurate quantum gate operations;
- Strong quantum measurements.

Implementing QC with photonics

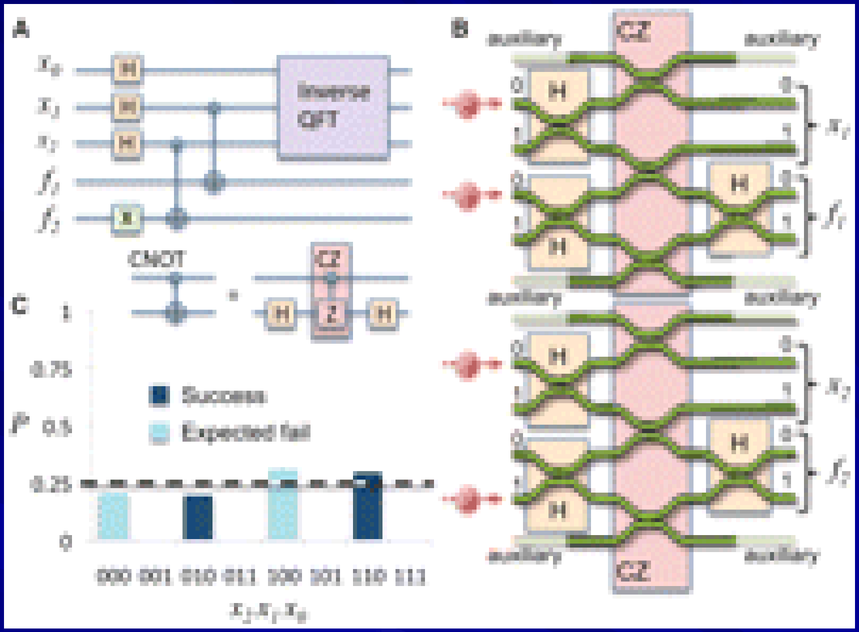
- Photon-polarization:



- Time bin encoding.
- Fock state encoding (presence/absence of a photon).

University of Bristol, 2009

- Photonic implementation of Shor’s factoring algorithm.
- 3 quantum bits.
- 15=3*5.



A. Politi, J. C. F. Matthews, J. L. O'Brien, Science 325, 1221 (2009)

Quantum computing research at University of Latvia

QCS project

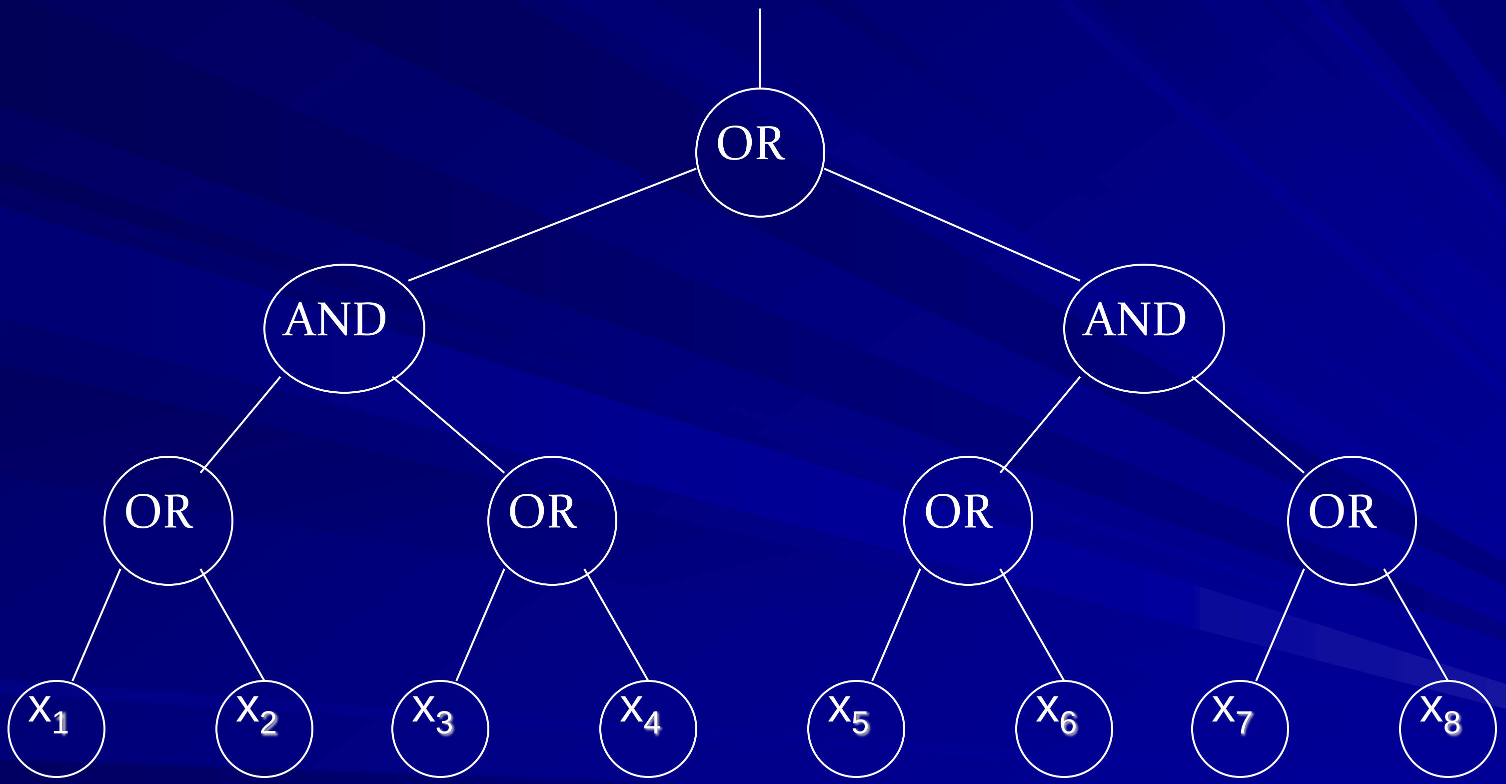
FP7 FET-Open project
“Quantum Computer Science”, 2010-2013

1. University of Latvia - coordinator;
2. University of Bristol (UK);
3. Cambridge University (UK);
4. University of Paris Diderot (France);
5. Centrum Wiskunde & Informatica (Netherlands);
6. Tel Aviv University (Israel);
7. Universite Libre de Bruxelles (Belgium);
8. Institut de Ciences Fotoniques (Spain);

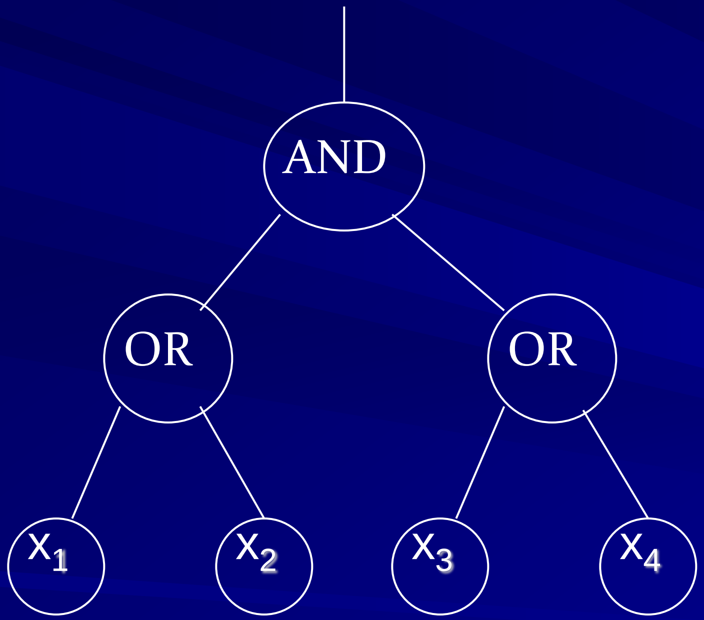
Research directions

1. Algorithms for quantum computers.
2. Impossibility results for quantum algorithms.
3. Quantum cryptography, quantum non-locality.
4. Mathematical questions about quantum states.

Formula evaluation



Evaluating AND-OR trees



- Variables x_i accessed by queries to a black box:
  - Input i;
  - Black box outputs x_i.
- Quantum case:

$$\sum_i a_i |i\rangle \rightarrow \sum_i a_i (-1)^{x_i} |i\rangle$$

- Evaluate T with the smallest number of queries.

Our results

- [A, Childs, Reichardt, Spalek, Zhang, 2007]: $O(N^{1/2+o(1)})$ time quantum algorithm for evaluating any logic formula of size N.
- [Reichardt, 2010]: $O(\sqrt{N})$ quantum algorithm.

The problem

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\
&\ldots \\
a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &= b_n
\end{aligned}
$$

- Given a_{ij} and b_i, find x_i.
- Best classical algorithm: $O(N^{2.37\ldots})$.

Harrow, Hassidim, Lloyd, 2008

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2$$
$$\ldots$$
$$a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n$$

- Running time for producing $\sum_{i=1}^{n} x_i |i\rangle$: O(log^c N), but with dependence on two other parameters.

Exponential speedup, if the other parameters are good.

Dependence on other parameters

Condition number of A.

$$k = \frac{\mu_{\max}}{\mu_{\min}}$$

μ_{max} and μ_{min} – biggest and smallest eigenvalues of A

- [HHL, 2008]: $O(k^2 \log^c N)$.

[A, 2010]: $O(k^{1+o(1)} \log^c N)$.

When can we achieve big quantum speedups?

Examples

0	1	0	$\cdots$	0
x_1	x_2	x_3		x_N

- Period-finding:
  - Promise: exists p: $x_{i+p}=x_p$.
  - O(1) queries quantumly*;
  - $\Theta(N^{1/4})$ queries classically.

* with some assumptions on x_i.

Polynomial vs. exponential speedups

- Search: is there $i : x_i = 1$?
- Period-finding: find p: $x_i = x_{i+p}$.

Symmetric

Non-symmetric

[Aaronson, A, 2011]

- Let $f(x_1, ..., x_N)$ – symmetric w.r.t. permuting $x_1, ..., x_N$ and permuting possible values for $x_1, ..., x_N$.
- If f – computable by quantum algorithm with Q queries, then f – computable with $O(Q^9)$ queries.