Theory of Computational Complexity

Lecture 14: Cryptography and Complexity
Quantum Computing and Cryptography

François Le Gall

Nagoya University

Quantum Computing

- ✓ (Relatively) Recent computation paradigm based on the laws of quantum mechanics

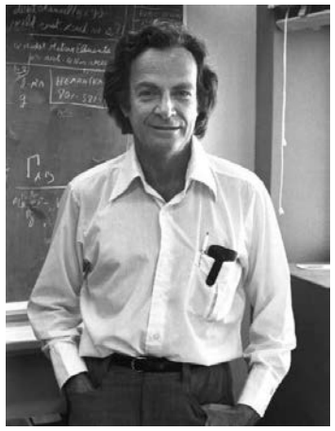
- ✓ Most celebrated achievements:
  - Unconditionally secure quantum cryptography
  - Fast quantum algorithms using quantum parallelism

Shor's algorithm (1994)
integer factoring

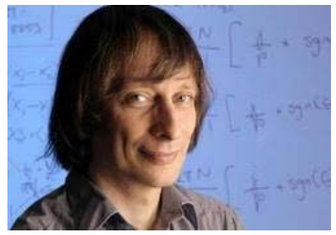
Grover's algorithm (1996)
quantum search

History of Quantum Compting

Proposal of QC



Feynman



Deutsch

first experiments

Wineland Haroche

Nobel Prize in Physics
（2012）

Discovery of fast quantum algorithms

Shor

Grover

First Quantum Boom

Quantum error-correction

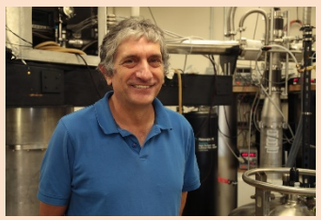
1982 1985 1994 1996 1999

NTT, NEC

Construction of the first quantum computers
(20~100 qubits)

IBM

Google & Martinis



D-Wave

2017 2014 2011 2005

Microsoft,
Rigetti, NTT,...

Second Quantum Boom

Integer Factoring

15 = 3 x 5

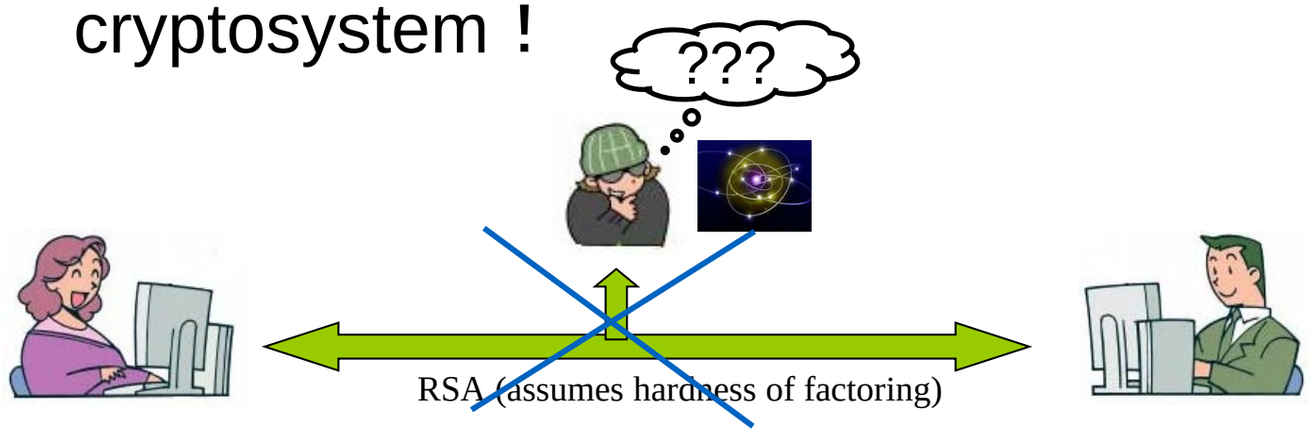
1475739525896764129 27 = 193707721 x 761838257287

✓ requires exponential time with the best known algorithms (this is the basis of the widely used RSA cryptosystem)

✓ there exists a polynomial-time quantum algorithm

Designed in 1994 by Peter Shor

→ If we can construct a quantum computer, we can break RSA cryptosystem !



What to do next?

We still don't know how to construct a large scale quantum computer, so RSA is safe now and at last for the next 20 years

Let's replace RSA cryptosystem with another cryptosystem secure even against quantum computers

Currently used public-key cryptosystems:

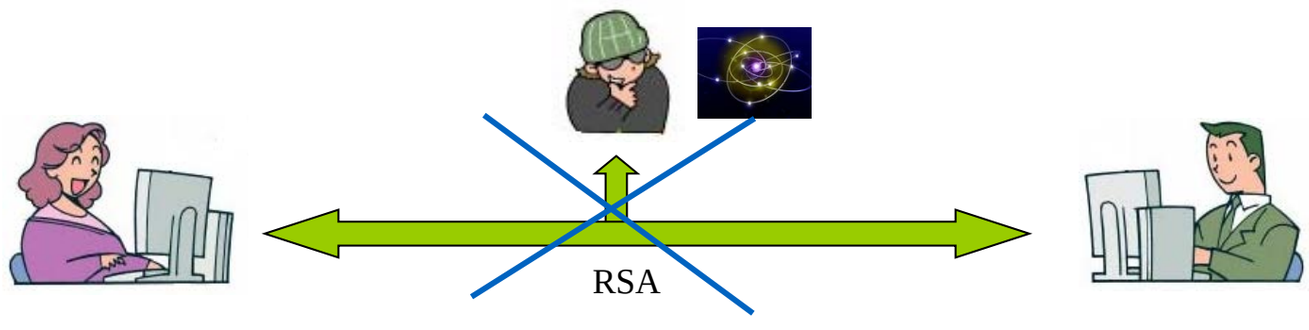
(candidates for trapdoor one-way functions)

~~RSA cryptosystem~~ — broken by quantum computers

~~ElGamal cryptosystem~~ — broken by quantum computers

~~Elliptic curves cryptosystems~~ — broken by quantum computers

? Lattice based cryptosystems — partially broken by quantum computers



Security in a Post-Quantum World

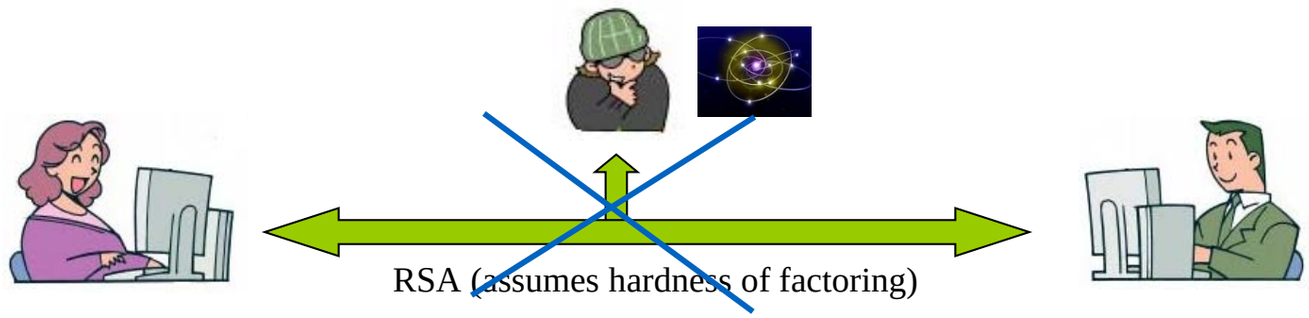
Let's replace RSA cryptosystem with another cryptosystem secure even against quantum computers

- ✓ Designing new cryptosystems secure against quantum computer is one of the most active topics in cryptography

"Post Quantum Cryptography"

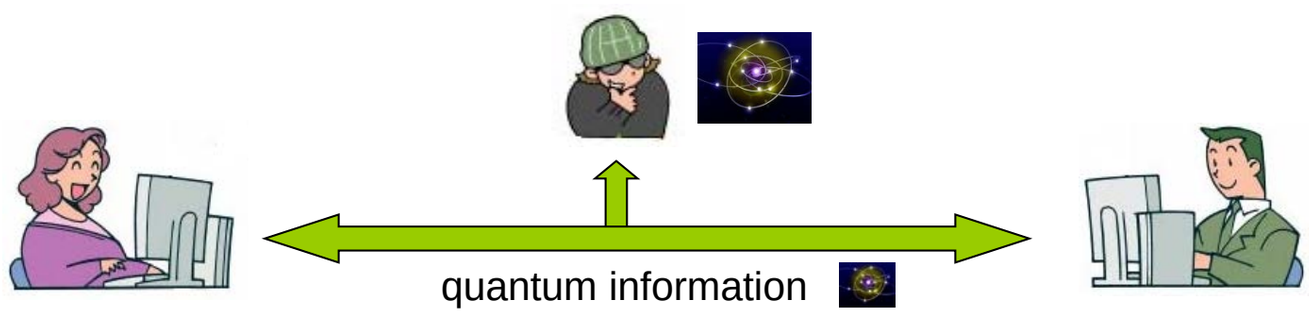
- ✓ Security agencies now explicitly list security against quantum computer as a requirement for next generation cryptographic standards
  - Europe: PQCrypto project from 2014
  - USA: NSA/NIST new calls for proposal in 2015
- ✓ Why now?
  - since its takes many years to design a good cryptosystem
  - protect current communications against future decryption

Quantum Cryptography



First solution：post quantum cryptography

Another solution：quantum cryptography
(perfectly secure from the uncertainty principle of quantum mechanics)



quantum information cannot be observed without perturbing its contents

any eavesdropping is detected

In practice: quantum cryptography used for secure key distribution (private-key classical cryptosystems like AES are then used)

Quantum Cryptography: on sale!

Verified experimentally (currently up to 120km)

optical fiber (20kn)

On sale by some companies (Id Quantique,…)

Drawback: the sender and the receiver need to use quantum devices

Security in a Post Quantum World

We would like a classical cryptosystem (i.e., a cryptosystem sending classical information)

Let's replace RSA cryptosystem with another cryptosystem secure even against quantum computers

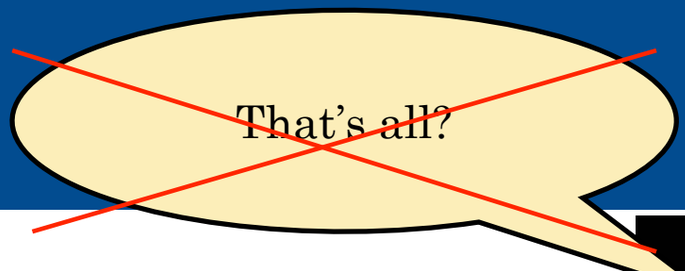
- ✓ Designing new cryptosystems secure against quantum computer is one of the most active

First we need to understand the power of quantum computation

"Post Quantum Cryptography"

- ✓ Security agencies now explicitly list security against quantum computer as a requirement for next generation cryptographic standards
  - Europe: PQCrypto project from 2014
  - USA: NSA/NIST new calls for proposal in 2015
- ✓ Why now?
  - since its takes decades to design a good cryptosystem
  - all communications can be decrypted in the future

Quantum Algorithms



Algorithmically, what can we do with a quantum computer?

quantum algorithm for integer factoring [Shor 1994]
quantum algorithm for search [Grover 1996]

Shor's algorithm (1994)
integer factoring
(would break RSA)

Grover's algorithm (1996)
quantum search

- qu… …ation [Brassard+
- qu… …Fahri+ 2000]
- qu… …[Ambainis 20…
- qu… …m + 2002]
- qu… …n [Hallgren 2…
- qu… …[Childs 2004]
- qu… …uperberg 200…
- qu… …[Hallgren 200…
- qu… …niez+ 2005]
- qu… …iants [Aharon…
- qu… …ll 2006]
- quantum algorithms for hidden nonlinear structures [Childs+ 2007]
- quantum algorithms for evaluating NAND formulas [Fahri+ 2007]
- quantum algorithms for group isomorphism [Le Gall 2010]
- quantum algorithms for matrix multiplication [Le Gall 2011]
- quantum algorithms using span programs [Belovs 2011]
- quantum algorithms for matrix inversion [Ta-Shma 2013]
- quantum algorithms for pattern matching [Montanaro 2014]
- ….

Quantum Algorithm Zoo

http://math.nist.gov/quantum/zoo/

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@nist.gov. Your help is appreciated and will be acknowledged.

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\widetilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n/3+o(1)})$ [252]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring "semiprimes", which are widely used in croptography is given in [271]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, *cf.* [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

Algorithm: Discrete-log
Speedup: Superpolynomial
Description: We are given three *n*-bit numbers *a*, *b*, and *N*, with the promise that $b = a^s \mod N$ for some *s*. The task is to find *s*. As shown by Shor [82], this can be achieved on a quantum computer in poly(*n*) time. The fastest known classical algorithm requires time superpolynomial in *n*. By similar techniques to those in [82], quantum computers can solve the discrete logarithm problem on elliptic curves, thereby breaking elliptic curve cryptography [109]. The superpolynomial quantum speedup has also been extended to the discrete logarithm problem on semigroups [203, 204]. See also Abelian Hidden Subgroup.

Algorithm: Pell's Equation
Speedup: Superpolynomial
Description: Given a positive nonsquare integer *d*, Pell's equation is $x^2 - dy^2 = 1$. For any such *d* there are infinitely many pairs of integers (*x*,*y*) solving this equation. Let (x_1, y_1) be the pair that minimizes $x + y\sqrt{d}$. If *d* is an *n*-bit integer (*i.e.* $0 \leq d < 2^n$), (x_1, y_1) may in general require

278 entries (December 8th, 2019)