An introduction to post-quantum cryptography

Andrew Savchenko

NRNU MEPhI, Moscow, Russia

LVEE Winter 2016

Outline

Terminology

What is what:

- Classical cryptography — *usual* cryptography, designed to withstand cryptanalysis using classical computers
- Postquantum cryptography — cryptography *resilient* to quantum computing
- Quantum cryptography has *nothing* to do with post-quantum cryptography.
  - It uses quantum mechanical properties of the matter for crypto applications, e.g.:
    - secure key distribution using entangled particles
    - protection from data copying
  - Requires a very dedicated hardware and connection lines

Terminology

What is what:

- Classical cryptography — *usual* cryptography, designed to withstand cryptanalysis using classical computers
- Postquantum cryptography — cryptography *resilient* to quantum computing
- Quantum cryptography has *nothing* to do with post-quantum cryptography.
  - It uses quantum mechanical properties of the matter for crypto applications, e.g.:
    - secure key distribution using entangled particles
    - protection from data copying
  - Requires a very dedicated hardware and connection lines

Terminology

What is what:

- Classical cryptography — *usual* cryptography, designed to withstand cryptanalysis using classical computers
- Postquantum cryptography — cryptography *resilient* to quantum computing
- Quantum cryptography has *nothing* to do with post-quantum cryptography.
  - It uses quantum mechanical properties of the matter for crypto applications, e.g.:
    - secure key distribution using entangled particles
    - protection from data copying
  - Requires a very dedicated hardware and connection lines

Quantum computing

Base elements:

- qubits (quantum bits)
- quantum logic gates
- quantum algorithm: sequence of quantum gates applied to qubits

Qubits

Each classical bit can be either 0 or 1, but qubits:

- can be 0 and 1 at the same time
- contain wave function of both states (e.g. superposition $|\uparrow\rangle + |\downarrow\rangle$)
- but with *different* probabilities
- usually electron spin is used, but any discernible quantum number is OK
- N qubits $\rightarrow 2^N$ states at the same time vs N classical bits $\rightarrow 1$ state at once

Quantum gates

Quantum logic gate:

- is a rotation (unitary transformation) applied to the wave functions (usually of 1 or 2 qubits)
- They provide full set of logical operations
- All quantum gates are reversible in contrast to classical gates

Quantum computing 2

Caveats:

- *only* N bit can be extracted from 2^N states
- measurement (wave function collapse) is probabilistic:
  - $2 + 2 = 5$ — OK!
  - but $P(2 + 2 = 4) > P(2 + 2 = 5)$

Summary:

- internal data reduction upon measurement
- results must be either:
  - *checked* or
  - *repeated* many times

Quantum computing 2

Caveats:

- *only* N bit can be extracted from 2^N states
- measurement (wave function collapse) is probabilistic:
  - $2 + 2 = 5$ — OK!
  - but $P(2 + 2 = 4) > P(2 + 2 = 5)$

Summary:

- internal data reduction upon measurement
- results must be either:
  - *checked* or
  - *repeated* many times

Shor's algorithm

Solves integer factorisation problem:

$$\text{for known } P \text{ find } N_1, N_2 : \; N_1 \cdot N_2 = P,$$

where N_1, N_2 — primes.

Steps:

- **(C)** factoring problem $\rightarrow$ function f period finding problem
- **(Q)** period finding:
  - Hadamard transformation (equal probability superposition)
  - apply f as quantum transform
  - apply quantum Fourier transform
  - measure the period
- **(C)** obtain prime from the period

For details see [1].

Shor's algorithm

Solves integer factorisation problem:

$$\text{for known } P \text{ find } N_1, N_2 : \; N_1 \cdot N_2 = P,$$

where N_1, N_2 — primes.
Steps:

- **(C)** factoring problem $\rightarrow$ function f period finding problem
- **(Q)** period finding:
  - Hadamard transformation (equal probability superposition)
  - apply f as quantum transform
  - apply quantum Fourier transform
  - measure the period
- **(C)** obtain prime from the period

For details see [1].

Factorisation complexity

Complexity estimation for $N \sim 2^{4096}$:

Algo	Complexity	Operations
GNFS	$O\left(e^{1.9(ln\ N)^{1/3}(ln\ ln\ N)^{2/3}}\right)$	$\sim 10^{46}$
Shor's	$O\left((ln\ N)^2\ (ln\ ln\ N)\ (ln\ ln\ ln\ N)\right)$	$\sim 10^8$

GNFS — General number field sieve, the fastest classical factorisation algorithm.

Grover's algorithm

A quantum brute-force (BF) algorithm.

Black box setup:

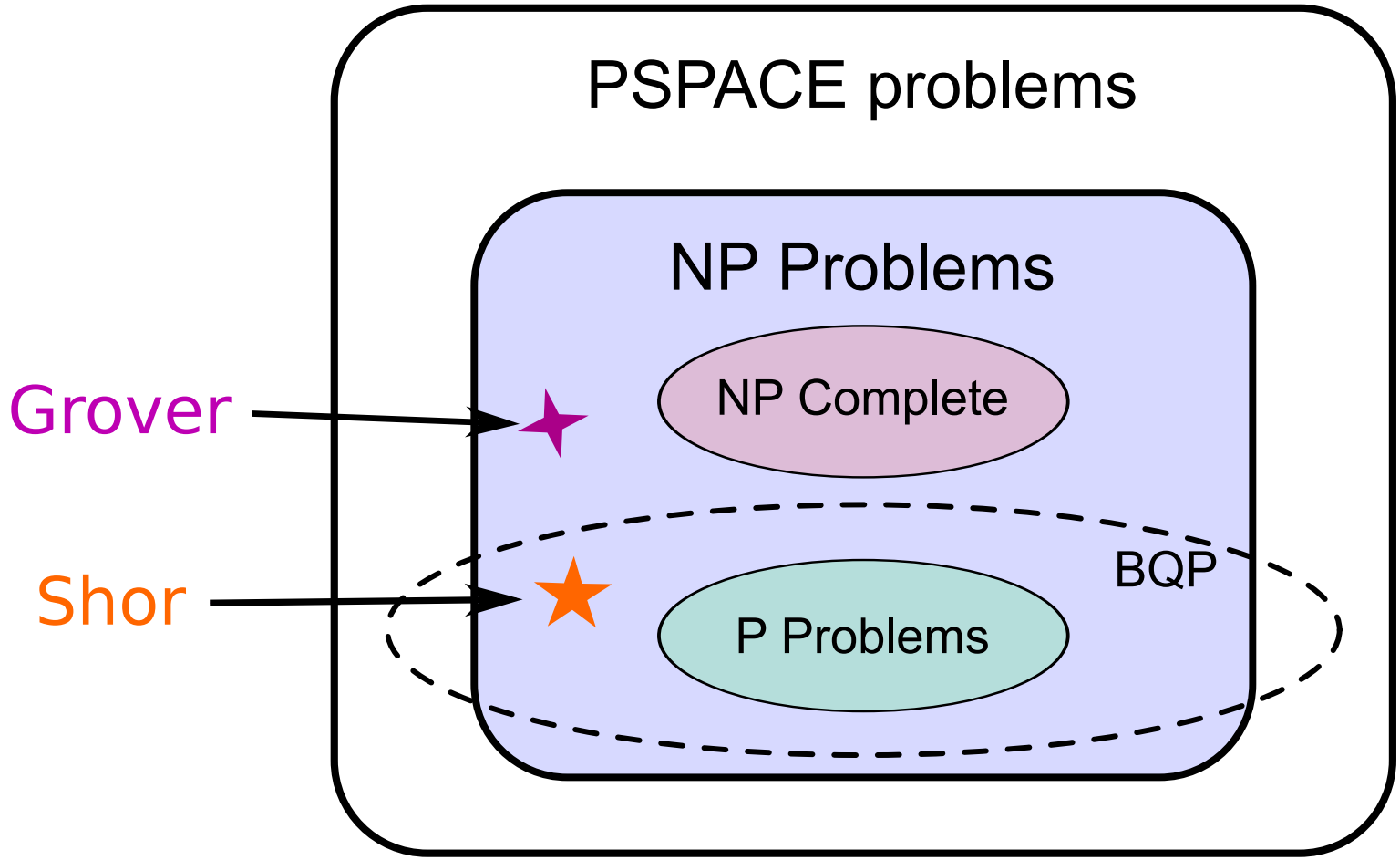
- 1 known output
- N unknown inputs

Complexity estimation for $N \sim 2^{256}$:

Algo	Complexity	Operations
BF	$O(N)$	$\sim 10^{77}$
Grover's	$O\left(\sqrt{N}\right)$	$\sim 10^{38}$

For details see [2].

Complexity classes



P — easy to solve and verify
NP — hard to solve, but easy to verify
BQP — easy to solve on quantum computer and verify

Impact on crypto algos

Symmetric crypto:

- Key sizes are halved

Common asymmetric crypto:

- Elliptic curves are very *dead*
- RSA and alike are *dead*

Quantum resistant asymmetric crypto:

- Hash-based [3]
- Lattice-based [3]
- Code-based [3]
- Multivariative quadratic equations [3]
- Supersingular elliptic curve isogeny [4]
- ...

Impact on crypto algos

Symmetric crypto:

- Key sizes are halved

Common asymmetric crypto:

- Elliptic curves are very *dead*
- RSA and alike are *dead*

Quantum resistant asymmetric crypto:

- Hash-based [3]
- Lattice-based [3]
- Code-based [3]
- Multivariative quadratic equations [3]
- Supersingular elliptic curve isogeny [4]
- ...

Impact on crypto algos

Symmetric crypto:

- Key sizes are halved

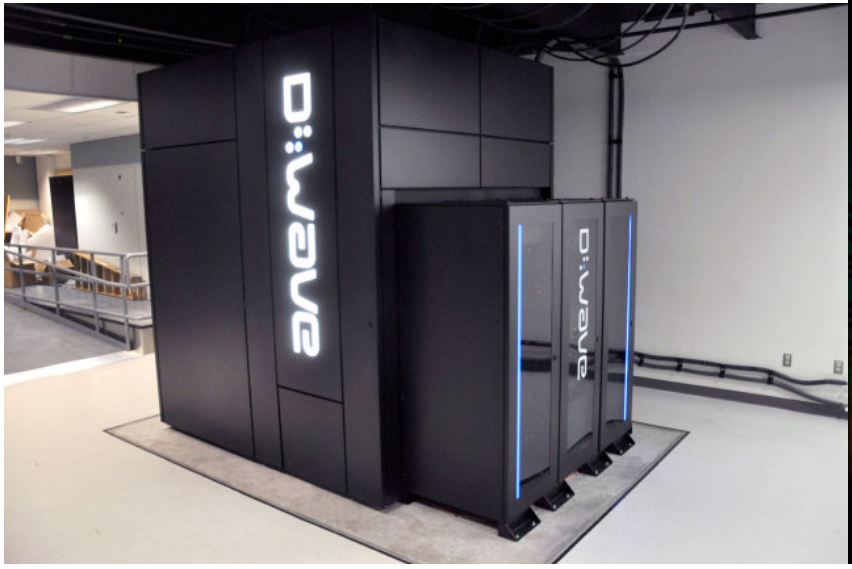
Common asymmetric crypto:

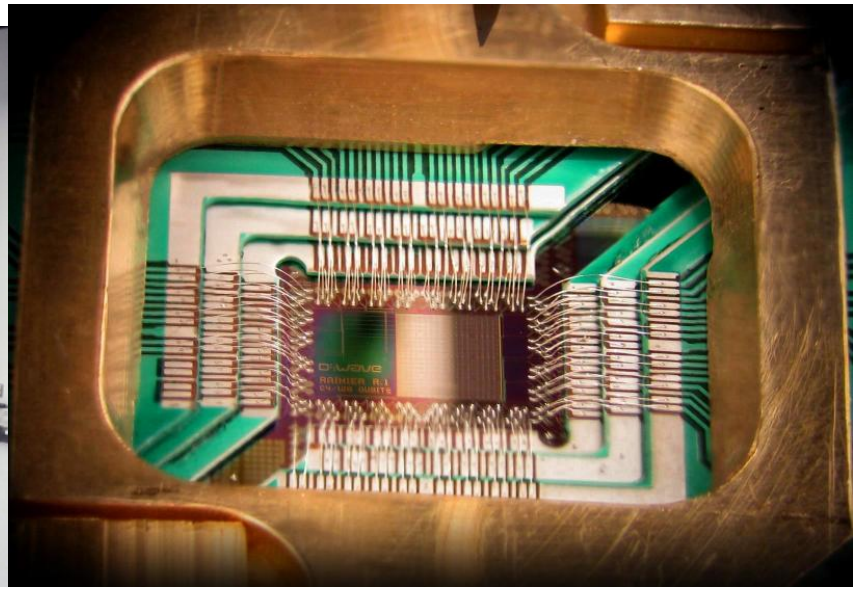
- Elliptic curves are very *dead*
- RSA and alike are *dead*

Quantum resistant asymmetric crypto:

- Hash-based [3]
- Lattice-based [3]
- Code-based [3]
- Multivariative quadratic equations [3]
- Supersingular elliptic curve isogeny [4]
- ...

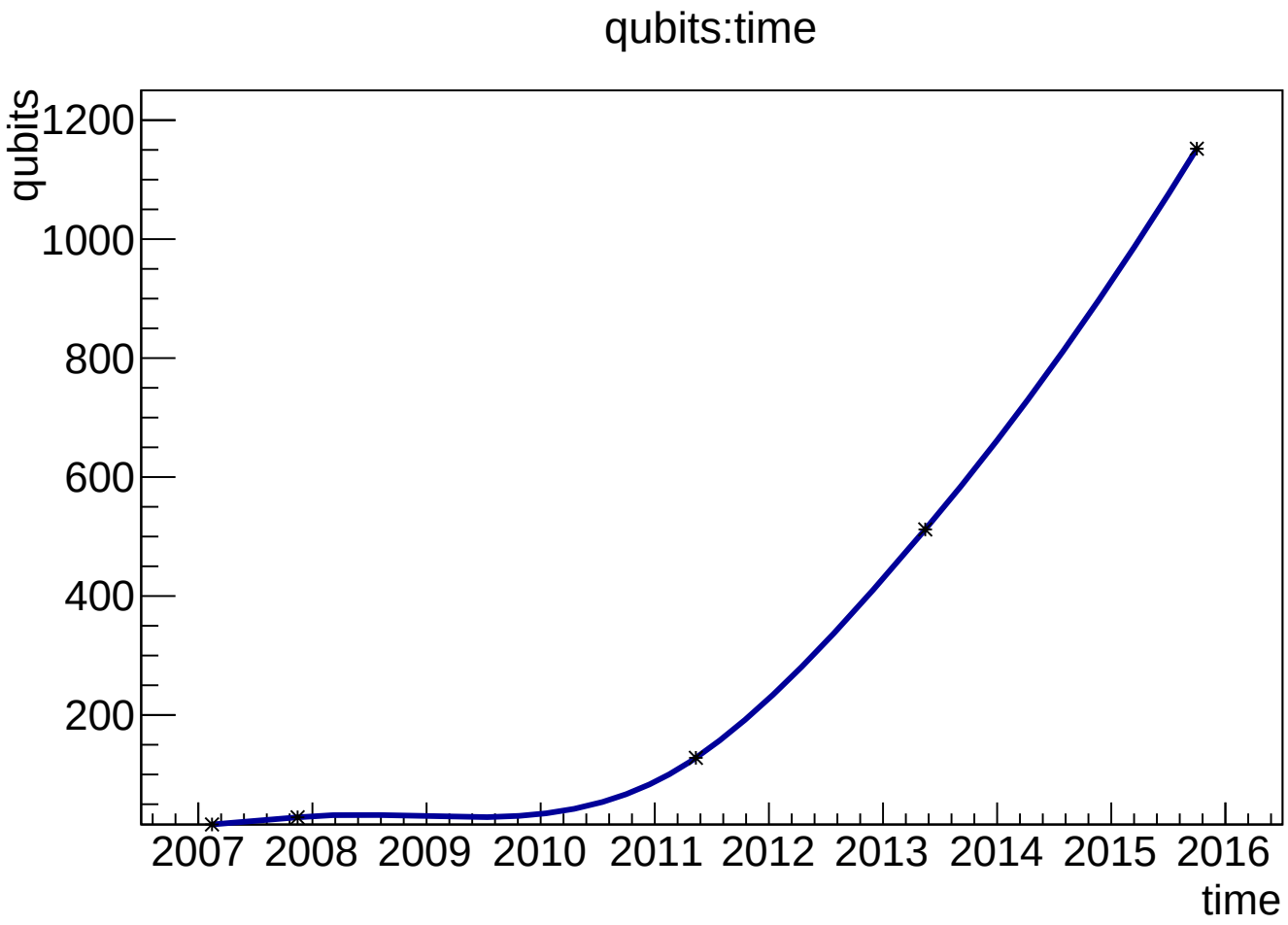
D-Wave Systems





- Computing in adiabatic quantum approximation [5].
- Declared to be suitable only for discrete optimisation [5, 6].
- Operates just at 0.015K :)

D-Wave Systems Timeline



Present: $1000 + \div 1152$ qubits from 2048-qubit chip.

Timeline

Year 2012.

- CIA $30m investment in D-Wave [7]

Year 2014.

- $56153 = 233 * 241$ factored on *4* qubits [8] at 300 K!
- mr. Snowden revealed that NSA spent $80m on a quantum computer development [9, 10]

Year 2015.

- NSA announce development of Suite B algorithms resistible to quantum computing [11]

Free software solutions

Codecrypt [12] — GnuPG-like encryption tool

- Signatures: hash-tree based (Merkle-tree signature)
- Asymmetric encryption: code based McEliece cryptosystem [13])
- Symmetric encryption: up to 4096-bit keys

Keys generation:

```
ccr --gen-key sig --name ”John Doe” # signature key
ccr --gen-key enc --name ”John Doe” # encryption key

# the same with manual key choise
ccr -g FMTSEQ256H20C-CUBE512-CUBE256  -N username
ccr -g MCEQCMDPC256FO-SHA512-CHACHA20 -N username
```

Free software solutions

Codecrypt [12] — GnuPG-like encryption tool

- Signatures: hash-tree based (Merkle-tree signature)
- Asymmetric encryption: code based McEliece cryptosystem [13])
- Symmetric encryption: up to 4096-bit keys

Keys generation:

```
ccr --gen-key sig --name ”John Doe” # signature key
ccr --gen-key enc --name ”John Doe” # encryption key

# the same with manual key choise
ccr -g FMTSEQ256H20C-CUBE512-CUBE256  -N username
ccr -g MCEQCMDPC256FO-SHA512-CHACHA20 -N username
```

Free software solutions

Sign and encrypt:

```
ccr -se -r Frank < letter.txt > letter.ccr
```

Decrypt and verify:

```
ccr -dv -o reply.txt < reply.ccr
```

Upstream is very dynamic and responsive.

Quantum Computing Language: QCL [14]

- quantum assembler and routines
- emulator of a quantum computer

Free software solutions

Sign and encrypt:

```
ccr -se -r Frank < letter.txt > letter.ccr
```

Decrypt and verify:

```
ccr -dv -o reply.txt < reply.ccr
```

Upstream is very dynamic and responsive.

Quantum Computing Language: QCL [14]

- quantum assembler and routines
- emulator of a quantum computer

Summary

- Symmetric cryptography is still secure,
  but *double* key size
- Drop RSA and elliptic curves in the long run
- Use codecrypt and other systems, but with caution.
- Combine multiple crypto systems

Outlook:

- Popular projects (*SSL, GnuPG) should include post-quantum algos one day
- Raise post-quantum awareness

Thank you for your attention!

LVEE Winter
Linux Vacation / Eastern Europe

Summary

- Symmetric cryptography is still secure,
  but *double* key size
- Drop RSA and elliptic curves in the long run
- Use codecrypt and other systems, but with caution.
- Combine multiple crypto systems

Outlook:

- Popular projects (*SSL, GnuPG) should include post-quantum algos one day
- Raise post-quantum awareness

Thank you for your attention!

LVEE Winter
Linux Vacation / Eastern Europe

Bibliography I


Shor's algorithm. —
URL: https://en.wikipedia.org/wiki/Shor's_algorithm.


Grover's algorithm. —
URL: https://en.wikipedia.org/wiki/Grover's_algorithm.


Bernstein Daniel J., Buchmann Johannes, Dahmen Erik. Post-quantum cryptography. —
Berlin : Springer, 2009. —
ISBN: 978-3-540-88701-0. —
URL: https://pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf.


Supersingular isogeny Diffie–Hellman key exchange. —
URL: https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange.


D-Wave Systems. —
URL: http://www.dwavesys.com/.


D-Wave Systems. —
URL: https://en.wikipedia.org/wiki/D-Wave_Systems.

Bibliography II


CIA and Amazon Founder Greedily Eye D-Wave's Quantum Computer. —

URL: http://www.dailytech.com/CIA+and+Amazon+Founder+Greedily+Eye+DWaves+Quantum+Computer/article27866.htm.


Dattani Nikesh S., Bryans Nathaniel. Quantum factorization of 56153 with only 4 qubits. —
2014. —
URL: http://arxiv.org/abs/1411.6758.


Snowden docs: NSA building encryption-cracking quantum computer. —

URL: http://www.theregister.co.uk/2014/01/03/snowden_docs_show_nsa_building_encryptioncracking_quantum_system/.


NSA seeks to build quantum computer that could crack most types of encryption. —
URL: https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-c2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html.


NSA Suite B Cryptography. —
URL: https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml.

Bibliography III


Codecrypt (post-quantum crypto suite). —
URL: http://e-x-a.org/codecrypt/.


McEliece cryptosystem. —
URL: https://en.wikipedia.org/wiki/McEliece_cryptosystem.


QCL (quantum computing language and quantum computer emulator). —
URL: http://tph.tuwien.ac.at/~oemer/qcl.html.