The quantum threat to cryptography

Michele Mosca
8 May 2016

Vienna, Austria
Cryptography in the context of quantum computers

E. Lucero, D. Mariantoni, and M. Mariantoni

© Harald Ritsch

Y. Colombe/NIST
How secure will our current crypto algorithms be?

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key Length</th>
<th>Security level (Conventional Computer)</th>
<th>Security level (Quantum Computer)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>1024 bits</td>
<td>80 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>2048 bits</td>
<td>112 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>ECC-256</td>
<td>256 bits</td>
<td>128 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>ECC-384</td>
<td>384 bits</td>
<td>192 bits</td>
<td>~0 bits</td>
</tr>
<tr>
<td>AES-128</td>
<td>128 bits</td>
<td>128 bits</td>
<td>~64 bits</td>
</tr>
<tr>
<td>AES-256</td>
<td>256 bits</td>
<td>256 bits</td>
<td>~128 bits</td>
</tr>
</tbody>
</table>
How much of a problem is quantum computing, really?
How soon do we need to worry?

Depends on*:

- How long do you need your cryptographic keys to be secure? – *security shelf-life* (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years) – *migration time*
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (z years) – *collapse time*
- “Theorem”: If x + y > z, then worry.

Business bottom line

- **Fact:** If $x+y > z$, then you will not be able to provide the required $x$ years of security.

- **Fact:** If $y > z$ then cyber-systems will collapse in $z$ years with no quick fix.

- **Prediction:** In the next 6-24 months, organizations will be differentiated by whether or not they have a well-articulated quantum risk management plan.
NSA [August 2015]: NSA’s Information Assurance Directorate “will initiate a transition to quantum resistant algorithms in the not too distant future.”

NSA [January 2016]: CNSA Suite and Quantum Computing FAQ

NIST [April 2016]: NISTIR 8105 Report on Post-Quantum Cryptography “outlines NIST’s initial plan to move forward in this space”.
http://dx.doi.org/10.6028/NIST.IR.8105

ETSI white paper [2014]:
Building a large quantum computer

Superconducting Circuits for Quantum Information: An Outlook

M. H. Devoret\textsuperscript{1,2} and R. J. Schoelkopf\textsuperscript{1*}

Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.
Towards a fault-tolerant design

IARPA [July 2015]: “BAA Summary – Build a logical qubit from a number of imperfect physical qubits by combining high-fidelity multi-qubit operations with extensible integration.”

Several leading groups internationally have reported receiving awards.
What I don’t worry about

• Implementations of quantum factoring to date (except where they demonstrate meaningful benchmarks towards fault-tolerance)

• “Quantum computing” approaches that do not have an articulated plan for fault-tolerantly implementing quantum algorithms such as Shor’s and Grover’s.
Quantum compilers

The efficiency of each step in the translation from high level algorithm to physical device impacts the efficiency of quantum attacks.

Diagram:
- Quantum algorithm
  - Logical circuits
    - Fault tolerant protocol
      - Fault tolerant gate set
        - Clifford + T
      - Quantum control
    - Physical layer gate set
  - Physical system
Quantum cost estimation

The efficiency of each step in the translation from high level algorithm to physical device impacts the efficiency of quantum attacks.
What is ‘z’?

Mosca:
[NIST April 2015, ISACA September 2015]:
“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”

Microsoft Research [October 2015]: Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer within a decade. ...Use of a quantum computer enables much larger and more accurate simulations than with any known classical algorithm, and will allow many open questions in quantum materials to be resolved once a small quantum computer with around one hundred logical qubits becomes available.
Managing the quantum risk

- At a high level, we need to assess $x$, $y$ and $z$ for the range of information assets and business functions.

\[ \text{Security Shelf life} + \text{Migration Time} > \text{Collapse Time} \rightarrow \text{Urgent action required to minimize losses} \]

\[ \text{Security Shelf life} + \text{Migration Time} < \text{Collapse Time} \rightarrow \text{Acting now will avoid losses} \]
Assessing and managing ‘y’

- This is the part of the equation we have some control over.

- We have known about this threat since 1994.
- Progress on building large-scale quantum computers has been public and relatively gradual.
- So there is no fundamental reason for panic or rush.
- To avoid a future panic or rush, we need a concerted effort now.
Quantum-safe cryptographic tool-chest

quantum-resistant conventional cryptography
Deployable without quantum technologies
Believed/hoped to be secure against quantum computer attacks of the future

quantum cryptography
Requires some quantum technologies (less than a large-scale quantum computer)
Typically no computational assumptions and thus known to be secure against quantum attacks

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem
Is Quantum Key Establishment (QKD) “out-of-band”? i.e. comparable to trusted courier?

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Uses untrusted communication channel?</th>
<th>Uses any standard telecommunications channels?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-quantum</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Trusted Courier</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>QKD</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>
Are we ready to deploy post-quantum crypto?

- Promising approaches include hash-based signatures, lattice-based, code-based, multi-variate equation based, elliptic curve isogenies, …

- In various stages of readiness. Some are quite mature. Still require further work on robust implementation and integration into applications.

- **But quantum algorithmic analysis has been quite limited.** Much more work is needed to achieve high levels of confidence. One mitigation strategy is to use post-quantum in a “hybrid” fashion with ECC.
Finding shortest lattice vectors faster using quantum search

Thijs Laarhoven\textsuperscript{1} · Michele Mosca\textsuperscript{2,3,4} · Joop van de Pol\textsuperscript{5}

Received: 15 October 2014 / Revised: 12 March 2015 / Accepted: 16 March 2015 / Published online: 14 April 2015 © The Author(s) 2015. This article is published with open access at Springerlink.com

Abstract By applying a quantum search algorithm to various heuristic and provable sieve algorithms from the literature, we obtain improved asymptotic quantum results for solving the shortest vector problem on lattices. With quantum computers we can provably find a shortest vector in time $2^{1.799n+o(n)}$, improving upon the classical time complexities of $2^{2.465n+o(n)}$ of Pujol and Stehlé and the $2^{2n+o(n)}$ of Micciancio and Voulgaris, while heuristically we expect to find a shortest vector in time $2^{0.268n+o(n)}$, improving upon the classical time complexity of $2^{0.298n+o(n)}$ of Laarhoven and De Weger. These quantum complexities will be an important guide for the selection of parameters for post-quantum cryptosystems based on the hardness of the shortest vector problem.

e.g. quantum searching can be applied to speed up parts of complex classical algorithms, e.g. finding short vectors in a lattice.
NEW ALGORITHMS AND ALGORITHMIC PARADIGMS
http://math.nist.gov/quantum/zoo/ (maintained by S. Jordan)
How easy is it to evolve from one cryptographic algorithm to a quantum-secure one?

Are the standards and practices ready?
Standards activities:

**ETSI ISG on Quantum Key Distribution (since 2008)**

**Scope:**

To develop GSs (ETSI Group Specifications) describing quantum cryptography for ICT networks. Quantum Key Distribution is the essential credential in order to use quantum cryptography on a broad basis. It is the main task of the QKD ISG to specify a system for Quantum Key Distribution and its environment.

The activities of the QKD ISG will be performed in close co-operation with relevant standards activities within and outside ETSI. External relationships will be established where and when ever needed, Formal relationships will be established using the normal ETSI processes via the ETSI Secretariat.
Standards activities:

Quantum Safe Cryptography and Security
An introduction, benefits, enablers and challenges

June 2015
ISBN No. 979-10-92620-03-0
Standards activities:

ETSI 2nd Quantum-Safe Crypto Workshop in partnership with the IQC
6 - 7 October, 2014, Ottawa, Canada

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography, hosted by SK Telecom
5-7 October, 2015, Seoul, Korea

4th ETSI/IQC Workshop on Quantum-Safe Cryptography
19-21 September, 2016, Toronto, Canada
Standards activities:

ETSI ISG on Quantum Safe Cryptography (since 2015)

• Focus is on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, benchmarking and practical architectural considerations
• Currently hold 5 regular meetings each year at ETSI headquarters in Sophia Antipolis, France
• The work may feed into other standards groups.
Cryptography leaders guide the future to new information security standards

Cryptography experts and decision makers met in France last week to set out a plan for a global quantum-safe cryptographic tools for the 21st century.

What is cryptography?
Cryptography is about keeping data and communications secure. People around the world depend on cryptography to keep their data and communication secure and reliable. Information

What are we working on?
Quantum technologies are revolutionizing our world, simultaneously posing new challenges and providing new tools for the future of information security. Quantum-safe

Prepare the workforce:
cryptoworks21.com
What do we do today?
Suggestions

• Get quantum-safe options on roadmaps
  • Routinely ask about vulnerability of systems to quantum attacks
  • Include quantum-safe options as desired features
  • Keep switching costs low
• Make quantum risk management a part of cybersecurity roadmaps
• (If appropriate) request the standards for the quantum-safe tools needed
• Request the information/studies needed to make wise decisions going forward.
• Encourage (quantum and classical) cryptanalysis of post-quantum schemes, and benchmarking of post-quantum tools.
• Applaud and reward organizations that take this seriously.
Thank you!

• Comments, questions and feedback are very welcome.

Michele Mosca
University Research Chair, Faculty of Mathematics
Co-Founder, Institute for Quantum Computing www.iqc.ca/~mmosca
Director, CryptoWorks21 www.cryptoworks21.com
University of Waterloo
mmosca@uwaterloo.ca
Co-founder and CEO, evolutionQ Inc.
michele.mosca@evolutionq.com

• Upcoming workshop of interest:
  4th ETSI/IQC Workshop on Quantum-Safe Cryptography
  19-21 September 2016
  Toronto, Canada