Technologies Quantiques et Sécurité
Enjeux Sociétaux

Dr. Grégoire Ribordy
ID Quantique SA

Janvier 2018
ID Quantique – Company Profile

Founded in 2001
Geneva, Switzerland
Boston, USA (sales office)
Hangzhou, PRC (JV)
Bristol, UK (set up)

By 4 quantum physicists from the University of Geneva
55 employees in CH, including 30 engineers/scientists

Develops technologies and products based on quantum physics within 2 business units:
Quantum-Safe Security
Quantum Sensing

Performs R&D, production, professional services, integration, support

Clients: Governments / Banks / Gaming Industry / Universities / IT Security
Cybersecurity

- Cybertechnologies are becoming increasingly pervasive.

- Cybersecurity is a growing and fundamental part of safety and security of individuals, organizations and society.
... is a foundational pillar of cybersecurity

- Cryptography allows us to achieve information security while using untrusted communication systems.

- Example: Do you use e-banking? Why do you trust the system?
What can be done with cryptography?

Confidentiality  Integrity

Information Security

Authentication  Non-Repudiation
"We announce preliminary plans for transitioning to quantum resistant algorithms."  Aug. 2015
Overview

- Quantum Technologies and Quantum Computing
- Impact on Cryptography
- When worry?
- Quantum-Safe Cryptography
- Conclusion
IBM Announces Advances to IBM Quantum Systems & Ecosystem

- Client systems with 20 qubits ready for use; next-generation IBM Q system in development with first working 80 qubit processor
- IBM expands its open-source quantum software package Qiskit; offers the world’s most advanced ecosystem for quantum computing
We announce preliminary plans for transitioning to quantum resistant algorithms.
Overview

- Quantum Technologies and Quantum Computing
- Impact on Cryptography
- When worry?
- Quantum-Safe Cryptography
- Conclusion
What can be done with cryptography?

Confidentiality

Integrity

Authentication

Non-Repudiation

Information Security
Confidentiality + other similar primitives for other goals (digital signatures, etc.)
Cryptographic Protocol

Alice

Message

Secret Key

Symmetric Cryptography

+  

Scrambled Message

10101010101100
10101011010100
00110110101010
10101010110010

Eve

Message

Secret Key

Asymmetric Cryptography

Bob

Secret Key

Public Key

Private Key

2'357 x 4'201 = ?

A x B = 9'901'757
Computational Security

Computer Science

10101010101100
10101011010100
00110110101010
10101010110010

= 452'65'896'84'41'00'9

Hard!

= 553'105'223' x 817'504'253

Easy!
Cryptography in a World with Quantum Computers

Computer Science

10101010101100
10101011010100
00110110101010
10101010110010

Physics

Easy!

Hard! Easy!

\[
\frac{452,165,896,841}{1009} = \underline{535,105,223} \times 817,504,253
\]
Quantum Algorithms & Impact on Today’s Cryptography

**Shor’s Algorithm**
- Peter Shor, 1994
- Quantum algorithm for integer factorization
  \[ \mathcal{O}((\log N)^3) \text{ vs. } \mathcal{O}(e^{1.9 (\log N)^{1/3} \ (\log \log N)^{2/3}}) \]

**Grover’s Algorithm**
- Lov Grover, 1996
- Quantum algorithm to perform search in an unsorted database
  \[ \mathcal{O}(n^{1/2}) \text{ vs. } \mathcal{O}(n) \]
- Key halfed for symmetric cryptography
  - AES-128 $\rightarrow$ 64 bits security
  - AES-256 $\rightarrow$ 128 bits security

Can break RSA, Elliptic Curve & Diffie Hellman
Cryptographic Primitives

Symmetric crypto primitives: ok (if key long enough)

Asymmetric crypto primitives: at risk
Overview

- Quantum Technologies and Quantum Computing
- Impact on Cryptography
- When worry?
- Quantum-Safe Cryptography
- Conclusion
One day in the future!

**TLS Protocol Insecure**
- E-banking stops working
- E-commerce stops working

**Digital Signature can be forged**
- Upgrades become insecure and hackers can implant malicious code
- Crypto-currencies loose value

**Message Authentication can be forged**
- Power grids vulnerable
- Autonomous cars can be hacked

**Network Encryption Insecure**
- Patient data become vulnerable
- Interbank clearing stops working
Deployment: public-key/hybrid

- PCs/mobile phones/tables (>3B): automatic updates
- EMV: RSA smart cards (>1B)
  - upgrading to ECC: 2015-2030
- Electronic ID cards and E-passports (~100M)
- TLS/SSL web servers (~10M)
- DNSSEC
- Skype (~500M)
- Bitcoin (~1M)
- The Internet of Things in 2020 (~20-50B)

Bart Preneel, Qcrypt 2014
When Do We Need to Worry?

- How long do you need encryption to be secure?
  
  *German law on healthcare data protection:* «Beyond lifetime of patient»

- How much time will it take to re-tool the existing infrastructure with a quantum-safe solution?
  
  *Upgrade of ATM’s from DES to 3DES between 2000 and 2010: up to 10 years*

- How long will it take for a large scale quantum computer to be built (or for any other relevant advance)
  
  «Probability = 1/7 by 2026 and 1/2 by 2031» Prof. Michele Mosca, University of Waterloo

\[
x + y > z \quad \text{Not possible to provide the required } x \text{ years of security}
\]

\[
x + 5 \text{ years} > 10 \text{ years}
\]

\[
y > z \quad \text{System will collapse in } z \text{ years with no easy fix}
\]
Why Is this Important? A Classical Risk Analysis

Risk = Probability of threat currently low but increasing \times Impact of threat Extremely high if no action taken

- Conduct Quantum-Risk Assessment
- Engineer Crypto Agility
- Enter in the Post-Quantum Era
Overview

▶ Quantum Technologies and Quantum Computing
▶ Impact on Cryptography
▶ When worry?
▶ Quantum-Safe Cryptography
▶ Conclusion
The Solution: Quantum-Safe Cryptographic Infrastructure

- “Post-quantum” algorithms (aka quantum-resistant algorithms)
  \[ e = r \times h + m \pmod{q} \]

- Classical codes deployable without quantum technologies.
  - Eg. Lattice, matrix-based algorithms

- Believed to be secure against Shor’s algorithm but no guarantee that there will not be other quantum attacks.

- Recommended for quantum-safe digital signatures & end point encryption.

Quantum Key Distribution

- Hardware solution.
- Typically no computational assumptions and thus known to be secure against future quantum attacks.
- Recommended for encryption of high-value information with requirement for long-term confidentiality.
  - Eg. Data center interconnect, government data
Quantum Cryptography = Quantum Key Distribution (QKD)

Fragile!

Alice

Symmetric Cryptography

Secret Key

+++

Scrambled Message

10101010101100
101010110100100
00110110101010
10101010110010

Bob

Secret Key

++

ID Quantique PROPRIETARY
Quantum-Enabled Network Encryption: Today

- **Transparent Layer 2 Encryption**
  - AES-256 up to 100Gbps
  - Multiprotocol (Ethernet, Fibre Channel)

- **Provably secure key distribution**
  - Distilled key distribution rate: 1000 bps over 25km/6dB
  - Range: 100km

![Diagram showing a quantum key server and quantum channel configurations](Diagram.png)
In 2007 Geneva government installed QKD
- Confidentiality & integrity of data during federal & cantonal elections
- Deployed by banks and governments since then to protect data-center interconnect
- But inherent distance limitation in optical-fibre based QKD
QKD in Data Centers for Financial Companies

- QKD-secured data center link large financial institution in the Netherlands.
- Installed in 2010.
  - High-speed encryption
  - 4 x Ethernet 1G links
  - 2 x FC-4 links
Some connectivity between close locations may require expensive fiber installations to minimize distances.

No connections between remote locations.

Data sharing using complicated routing and encryption schemes.

QKD Trusted Node Networks
Large Scale Quantum Networks

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes
- 31 fiber links
- Metropolitan networks
  - Existing: Hefei, Jinan
  - New: Beijing, Shanghai
- Total Investment: 560 M RMB, Half by NDRC, Half by Local government
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

WP3: UK Quantum Network

- Establish large-scale Quantum Network test-bed in UK

Implemented in stages
- Metro networks in Cambridge and Bristol
- Long-haul network connecting Cambridge-London-Bristol (NDFIS) with possibility to extend
- Access networks providing multi-user connectivity

- A focus for application development, industrial standardisation and user engagement
- Potential test-bed for the other QT Hubs and associated projects
Global Quantum Cryptography
Overview

- Quantum Technologies and Quantum Computing
- Impact on Cryptography
- When worry?
- Quantum-Safe Cryptography
- Conclusion
Recommendations for Industry and Governments

- Get quantum-safe options on vendor roadmaps
- Routinely ask about vulnerability of systems to quantum attacks
- Include quantum-safe options as desired features
- Engage in pilot deployments to prepare for quantum-safe transition
- Prioritize by conducting quantum risk assessment
- Keep switching costs low
- (If appropriate) request the necessary standards for the quantum-safe tools needed
- Request the information/studies needed to make wise decisions going forward
- Applaud and reward organizations that take this seriously
Protect the Assets in Line with the Risk

Use QRA for encryption here

Digitally sign with QRA

Use QKD for link encryption and QRA for authentication here
Conclusion

- Quantum Computing poses a systemic threat to our current approach to information security

- It is now essential to carry out a «Quantum Risk Assessment»
  & start planning a transition to Quantum-Safe approaches

- A full Quantum-Safe cryptographic architecture will involve a combination of QKD and «Math-based» approaches

- Security is a choice!
Thank you for your attention

- Grégoire Ribordy
gregoire.ribordy@idquantique.com

- ID Quantique SA
  Geneva, Switzerland
  www.idquantique.com