Quantum Computing & Cryptography

Christian Schaffner

Research Center for Quantum Software

Institute for Logic, Language and Computation (ILLC)
University of Amsterdam

Landing Festival Berlin, 3 April 2019
A little thought experiment...
Quantum Computer

What are you going to do with it?

10-20 quantum bits now
50-100 qubits in the next 5 years!
Quantum Physics

1. Superposition:
   • Of different states

2. Interference:
   • Of states

3. Entanglement:
   • Of two or more physical systems
Quantum Physics

1. **Superposition:**
   - Of different states

2. **Interference:**
   - Of states

3. **Entanglement:**
   - Of two or more physical systems
Superposition

• An object in different states simultaneously:
  o A photon can be at two positions at the same time
  o Schrödinger’s cat: dead and alive

• Experimentally verified:
  o Small systems, such as photons
  o Bigger systems, molecules…
Superposition: An experiment
detector 1

superposition

detector 0
50% detector 0 clicks
50% detector 1 clicks

detector 1

detector 0
Random Number Generator

Swiss company:
id Quantique
Quantum Physics

1. Superposition:
   • Of different states
   • Observation: collapse of the superposition

2. Interference
   • Of an object in superposition

3. Entanglement
   • Of two or more physical systems
no superposition but: beamsplitter reflects 50% and transmits 50%?
Mach-Zehnder interferometer

- Detector 0
- Detector 1
- Mirror
- 50% detector 0 clicks
- 50% detector 1 clicks
- 50%-50% beamsplitter
- Classical reasoning
Mach-Zehnder interferometer

When you perform the experiment

detector 0 clicks ALWAYS !!!
Try it yourself: http://quantumgame.io/

According to quantum mechanics
Quantum Physics

1. Superposition
   • Of different states
   • Observation: collapse of the superposition

2. Interference:
   • Of an object in superposition

3. Entanglement:
   • Of two or more physical systems
Quantum Physics + Computer Science = A Quantum COMPUTER

Feynman 1981  Deutsch 1985

Video: Quantum Computers Animated
Quantum Bit (QuBit)

- Classical bit: 0 or 1
- Quantum bit: superposition of 0 and 1
More Qubits

- 1 qubit superposition of 2 states
- 2 qubits superposition of 4 states
- 3 qubits superposition of 8 states
- 4 qubits superposition of 16 states
- 5 qubits superposition of 32 states
- 6 qubits superposition of 64 states
- 300 qubits superposition of $2^{300}$ states
Quantum Software: Fundamentally Different

- Qubit: superposition of 0 and 1
- 300 qubits: astronomical amount of parallel computation
- How to get the answer out??
  - Measuring destroys computation!!
- Quantum Program
  - Use interference to cancel undesired computations
- Does not always work!

Our focus: how can we optimally use the extra power?
Quantum Programming is like Composing

- **Music**
  - Sound waves interfere
  - Composer creates ‘beautiful’ interference of sound waves

- **Quantum Computer**
  - Qubits in superposition interfere
  - Quantum programmer ensures useful interference of qubit states
What can you do with it?

• Simulation of nature
  - Chemistry, material design, new medicines..

• Efficient communication
  - Quantum internet, entanglement etc.

• Factorizing big numbers [Shor]
  - Breaks frequently used cryptography

• Quantum cryptography [Bennett-Brassard-Ekert]
  - Cryptography using quantum communication

• ???????
Progress In Building Qubits

- Many groups worldwide progress with building qubits
  - Solid state:
    - 50 solid-state qubits IBM
    - 49 Intel
    - 50 Google → 72
    - Fairly stable
  - Trapped ions:
    - 11 qubits Monroe
  - D-Wave:
    - 2048 qubits (not very stable)

https://quantumcomputingreport.com/
What can you do with it?

• Simulation of nature
  - Chemistry, material design, new medicines..

• Efficient communication
  - Quantum internet, entanglement etc.

• Factorizing big numbers [Shor]
  - Breaks frequently used cryptography

• Quantum cryptography [Bennett-Brassard-Ekert]
  - Cryptography using quantum communication

• ????????
“Cyber Security provides security, safety and privacy solutions that are **vital for our economy** including but not limited to critical infrastructures, smart cities, cloud computing, online services and e-government.”
Quantum Algorithm for Factorization

- Peter Shor 1994: efficient quantum algorithm for factoring integer numbers
- $15 = 3 \times 5$
- $27 = 3 \times 3 \times 3$
- $31 = 1 \times 31$
- $57 = 3 \times 19$
- $91 = 7 \times 13$
- $173 = 1 \times 173$
- RSA-100 = 152260502792253360535618378132637429718068114961380688657908494580122963258952897654000350692006139

Peter Shor 1994: efficient quantum algorithm for factoring integer numbers

$15 = 3 \times 5$

$27 = 3 \times 3 \times 3$

$31 = 1 \times 31$

$57 = 3 \times 19$

$91 = 7 \times 13$

$173 = 1 \times 173$

RSA-100 = 152260502792253360535618378132637429718068114961380688657908494580122963258952897654000350692006139
Quantum Computer Breaks Public-Key Crypto

• Peter Shor 1994: efficient quantum algorithm for factoring integer numbers

• For a 600-digit number (RSA-2048)
  • Classical: age of universe (exponential time)
  • Quantum: few minutes (polynomial time)

• Consequence: Large enough quantum computers break all currently used public-key cryptosystems!!!
## Current Cryptography Under Quantum Attack

<table>
<thead>
<tr>
<th>Security level systems</th>
<th>Conventional attacks</th>
<th>Quantum attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric-key encryption (AES-256)</td>
<td>256 bits of security</td>
<td>128 bits</td>
</tr>
<tr>
<td>Hash functions (SHA3-256)</td>
<td>128 bits</td>
<td>85 bits</td>
</tr>
<tr>
<td>Public-key crypto (key exchange, digital signatures, encryption) (RSA-2048, ECC-256)</td>
<td>112 bits</td>
<td>~ 0 bits</td>
</tr>
</tbody>
</table>

Products, services, businesses relying on security either stop functioning or do not provide expected levels of security!
When Do We Need To Worry?

Depends on:
• How long do you need to keep your secrets secure? \( (x \text{ years}) \)
• How much time will it take to re-tool the existing infrastructure? \( (y \text{ years}) \)
• How long will it take for a large-scale quantum computer to be built? \( (z \text{ years}) \)
• Theorem (Mosca): If \( x + y > z \), then worry.

\[ \begin{align*}
\text{time} & \\
2019 & \quad \text{secrets revealed} \quad 2029 ?
\end{align*} \]

• If \( x > z \) or \( y > z \), you are in big trouble!

slide by Michele Mosca
Conventional Quantum-Safe Cryptography

• **Wanted**: new assumptions to replace factoring and discrete logarithms in order to build conventional public-key cryptography

[Image: CSRC In Search of: Post-Quantum Crypto Algorithms]

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

• NIST “competition”: 82 submissions (23 signature, 59 encryption schemes)
• Aug 2019: Second-round workshop in California
• Expected: 3-5 years of crypto-analysis
• New standards, world-wide adoption
The Future is Quantum: Governments

- QuTech in Delft, NL: €135 million
- €18.8 Mio for 10 years: Quantum Software Consortium
- Germany: €650 million for quantum technologies
- UK: £235 million five-year in quantum computing
- Sweden: €100 million for 10 years for WACQT
- EU Flagship: €1 billion and a duration of 10 years
- US: $1.2 billion National Quantum Initiative Act
- China: $1 billion initial funding for National Laboratory for Quantum Information Sciences
- Canada, Australia, Singapore, …

https://sciencebusiness.net/news/eu-runs-catch-governments-pledge-more-cash-quantum-computing
The Future is Quantum: Business

- Quantum networks
- Quantum cloud

Y. Dulek, C. Schaffner, and F. Speelman, arXiv:1603.09717
Quantum homomorphic encryption for polynomial-sized circuits
Summary

<table>
<thead>
<tr>
<th>Security systems</th>
<th>Standard attacks</th>
<th>Quantum attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric</td>
<td>256 bits of security</td>
<td>128 bits</td>
</tr>
<tr>
<td>Hash</td>
<td>128 bits</td>
<td>85 bits</td>
</tr>
<tr>
<td>Public-key</td>
<td>112 bits</td>
<td>~ 0 bits</td>
</tr>
</tbody>
</table>

security systems

2019

secrets revealed

2029 ?

Research Center for Quantum Software
“About your cat Mister Schrödinger…
I’ve got good and bad news.”