Quantum Computing and Data Security

Marie-Christine Röhsner
Quantum Information Science and Quantum Computation Group, Faculty of Physics, University of Vienna

IPEN workshop
09.06.2017
Overview

<table>
<thead>
<tr>
<th>Quantum Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>A threat to classical cryptography</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quantum Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security guaranteed by the laws of physics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Blind Quantum Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perfect data privacy in cloud computing</td>
</tr>
</tbody>
</table>
Quantum Computers

- Computers based on the laws of quantum physics

**Bit**

**Qubit**

\[ |0\rangle \]

\[ |-\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]

\[ |1\rangle \]

Easy readout

N qubits – \(2^N\) basis states

Need measurement to readout \(\rightarrow\) collapse the state
Quantum Computers

<table>
<thead>
<tr>
<th>Disadvantages</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Instable</td>
<td>• New resources</td>
</tr>
<tr>
<td>▫ Errors</td>
<td>▫ Parallelism</td>
</tr>
<tr>
<td>▫ Loss of quantum properties</td>
<td>▫ Interference</td>
</tr>
<tr>
<td>• Hard to build</td>
<td>▫ Entanglement</td>
</tr>
<tr>
<td>▫ Isolation</td>
<td>• Fast solutions for</td>
</tr>
<tr>
<td>▫ Up-scaling</td>
<td>▫ Quantum Simulation</td>
</tr>
<tr>
<td>▫ Memories</td>
<td>▫ Search (Grover)</td>
</tr>
<tr>
<td></td>
<td>▫ Factorization (Shor)</td>
</tr>
</tbody>
</table>
Shor’s Algorithm

- Algorithm for integer factorization \((N=p\times q)\)
- RSA encryption is based on assumption that factoring is hard
- Quantum computer can solve it in polynomial time (BQP)
- Relies on superposition and quantum Fourier transform
- Therefore a large, universal quantum computer would break RSA
Quantum Computers - state of the art

• Different implementations
  ▫ Photons (~10 qubits)
  ▫ Ions (~14 qubits)
  ▫ Superconductors (IBM: 17 qubits)

• Specialized machines (e.g. D-Wave >2000 “qubits”)
Solution

Post quantum cryptography

- Classical Cryptography
- Not breakable by any known quantum algorithm
- Security not proven

Quantum cryptography

- Based on quantum systems
- Security theoretically guaranteed by the laws of physics
- First systems are commercially available
Quantum Cryptography

- Quantum Key Distribution (QKD)
- Distribution of a random one-time-pad
- Alice and Bob can find out if someone is listening
Quantum Cloud Computation

- Nearly classical clients can evaluate quantum algorithms
- Without leaking input, output or algorithm
When will this become a problem?

Time until full scale quantum computers

2017

Time needed to implement changes in security system

Time data needs to be secure

When will this become a problem?

2017

Time needed to implement changes in security system

Time data needs to be secure
Thank you!