Evil Qubits
The Threat of Quantum Cryptanalysis Explained

Tomas Rosa
Raiffeisen BANK International Cryptology and Biometrics Competence Centre
Postulate #1: Qubit state belongs to Hilbert space of dimension 2

\[ |\psi\rangle = \omega_0 |0\rangle + \omega_1 |1\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right), \quad \omega_i \in \mathbb{C} \]

\[ |\omega_0|^2 + |\omega_1|^2 = 1 \]
Postulate #2: Qubit evolution is given by a unitary transformation

\[ i\hbar \frac{\partial |\psi\rangle}{\partial t} = H |\psi\rangle \]

\[ |\psi_t\rangle = U_t |\psi_0\rangle, \quad U_t = e^{-iHt/\hbar} \]

\[ e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \ldots \]
Postulate #3: Projective probabilistic measurement

- When measured, quantum state collapses into one of particular eigenstates comprising the basis vectors of the corresponding Hilbert space.

- For a qubit, these are labeled $|0\rangle$ and $|1\rangle$. So called computational basis.

- Superposition cannot be seen directly. It governs the probability of the measurement outcome; coefficients $\omega_i$ called *probability amplitudes*.

$$P[\text{result} = |i\rangle] = \left| \omega_i \right|^2 = \omega_i \cdot \omega_i^*$$
Postulate #4: Qubit register state belongs to $H_2 \otimes H_2 \otimes \ldots \otimes H_2$

- Exponential growth of dimension: n-qubit register belongs to Hilbert space of dimension $2^n$ and can be in a superposition of all of its $2^n$ eigenstates.

- together with linear operators acting on this register, this is the source of so-called quantum parallelism

- however, the superposition still cannot be seen directly, it still just governs the probability of the measurement outcome

- eigenstates (computational basis) $|00\ldots0\rangle$, $|00\ldots1\rangle$, $\ldots$, $|11\ldots1\rangle$

- sometimes, the tensor product is noted explicitly $|00\ldots0\rangle = |0\rangle|0\rangle\ldots|0\rangle$, etc.
Separable Register State Example (Note the Pure Tensor Product…)

\[ |\psi\rangle = \frac{1}{\sqrt{8}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \]
Entanglement (Note the Unavoidable Sum of Tensor Products...)

\[ |\psi\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \]
Computational Aspects

- Actually, we have already reformulated the quantum mechanics postulates slightly to tailor them to qubits and qubit registers.

- We can continue further to derive computational paradigms. For instance:
  - quantum parallelism (already noted above)
  - interference (constructive / destructive, enabled by the complex amplitudes)
  - entangled states (seen as an extra power for algorithms)
Computational Interference

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}
\]

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & -1 \end{pmatrix}
\]
This was just a computational version of Mach-Zehnder experiment.
Time to Say: “Hello World!”
Deutsch-Jozsa: Quantum Computation “Hello World”

- Let us have \( f: \{0, 1\}^N \rightarrow \{0, 1\} \) that is promised to be either constant or balanced (nothing else). Balanced means the function vector has exactly \( 2^{N-1} \) ones (and zeros).

  - we have to decide what kind of function we have

  - to give a deterministic answer classically, we need at least \( 2^{N-1} + 1 \) invocations of \( f \)

  - on a quantum computer, it suffices to do just one invocation of \( f \)

  - exponential speed up thanks to the quantum parallelism and interference
Simple Case for $N = 1$

<table>
<thead>
<tr>
<th>$x, f(x)$</th>
<th>Constant function</th>
<th>Balanced function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>
DJ Quantum Computation Scheme (with balanced $f$ example)
Device: ibmqx4

Quantum State: Computation Basis

Quantum Circuit

OPENQASM 2.0
1 include "qelib1.inc";
2 qreg q[5];
3 creg c[5];
4 x q[0];
5 h q[0];
6 h q[1];
Quantum State: Computation Basis

Quantum Circuit

```plaintext
include "qelib1.inc";
qreg q[5];
creg c[5];
x q[0];
h q[0];
h q[1];
```

Open in Composer
Qiskit

Earth Air Fire Water
RSA (since 1977)

\[ x = y^e \mod N \]

easy way

hard way

\[ x, y < N \]
RSA - Going Back and Forth

\[ x^d \mod N = y \]

hard easy way

\[ x, y < N \]
How to get the private exponent “d”?

\[ N = pq \]

\[ d = e^{-1} \mod \text{lcm}(p-1,q-1) \]

easy way if we can factorise \( N \)
Period Finding and Factorisation (Shor’s Algorithm)

Let \( f(k) = a^k \mod N \)
and let us find \( r: f(k + r) = f(k) \)

\[ \Rightarrow a^{k+r} \mod N = a^k \mod N \]
\[ \Rightarrow a^r \mod N = 1, \text{so } N \text{ divides } a^r - 1 \]
\[ \Rightarrow \text{for even } r, N \text{ divides } (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) \]
\[ \Rightarrow \text{for } N \mid (a^{\frac{r}{2}} \pm 1), \text{ gcd}(a^{\frac{r}{2}} \pm 1, N) \text{ are factors of } N \]
Quantum Parallelism...

\[ |\psi\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle |a^k \mod N\rangle \]
Quantum Parallelism… (Example)

\[ \left| \psi \right\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \left| k \right\rangle \left| a^k \mod N \right\rangle \]

\[ M = 16, \, N = 15, \, a = 7 \]

\[ \left| \psi \right\rangle = \frac{1}{4} \left( \left| 0 \right\rangle \left| 1 \right\rangle + \left| 1 \right\rangle \left| 7 \right\rangle + \left| 2 \right\rangle \left| 4 \right\rangle + \left| 3 \right\rangle \left| 13 \right\rangle + \left| 4 \right\rangle \left| 1 \right\rangle + \left| 5 \right\rangle \left| 7 \right\rangle + \ldots + \left| 15 \right\rangle \left| 13 \right\rangle \right) \]
Feeling of the Period

\[ |\psi\rangle = \frac{1}{4} (|0\rangle + |4\rangle + |8\rangle + |12\rangle)|1\rangle \]
\[ + \frac{1}{4} (|1\rangle + |5\rangle + |9\rangle + |13\rangle)|7\rangle \]
\[ + \frac{1}{4} (|2\rangle + |6\rangle + |10\rangle + |14\rangle)|4\rangle \]
\[ + \frac{1}{4} (|3\rangle + |7\rangle + |11\rangle + |15\rangle)|13\rangle \]
Quantum Fourier Transform (QFT) of Eigenstate

\[ |ur + k\rangle |a^k\rangle \rightarrow \frac{1}{\sqrt{m}} \sum_{v=0}^{m-1} e^{\frac{2\pi i(ur+k)v}{m}} |v\rangle |a^k\rangle \]

\[
= \frac{1}{\sqrt{m}} \left( \sum_{v=0}^{m-1} e^{\frac{2\pi i kv}{m}} \cdot e^{\frac{2\pi i uv}{r}} \right) |v\rangle |a^k\rangle
\]

fixed phase swallow interference control
Superposing QFT

\[ \sum_{(u)} \left| ur + k \right\rangle \left| a^k \right\rangle \rightarrow \frac{1}{\sqrt{m}} \sum_{(u)} \sum_{v=0}^{m-1} e^{\frac{2\pi i (ur+k)v}{m}} \left| v \right\rangle \left| a^k \right\rangle \]

\[ = \frac{1}{\sqrt{m}} \left[ \sum_{v=0}^{m-1} e^{\frac{2\pi i kv}{m}} \left( \sum_{(u)} e^{\frac{2\pi i uv}{r}} \left| v \right\rangle \right) \right] \]

fixed phase swallow interference control
Exploiting the Parallelism via QFT Interference
It is not only about the Shor’s algorithm

- **Grover’s search method**
  - quadratic speed-up, usable for both asymmetric and symmetric algorithms

- **Simon’s period finding**
  - exponencial speed-up, usable for both asymmetric and symmetric algorithms

- **Hidden subgroup problem**
  - exponencial speed-up
  - generalises Simon’s, Shor’s, and a lot of other algorithms

— [http://quantumalgorithmzoo.org](http://quantumalgorithmzoo.org)
How’s your quantum computer prototype coming along?

Great!

The project exists in a simultaneous state of being both totally successful and not even started.

Can I observe it?

That’s a tricky question.
Main Challenges for Quantum Computers Today

- We have a **Noisy Intermediate-Scale Quantum** (NISQ) technology
  - coherence time
  - scalability

[Electronic Numerical Integrator and Computer - ENIAC]
IBM Q quantum computing systems

Refrigerator to cool qubits to 10 - 15 mK with a mixture of $^3$He and $^4$He

Chip with superconducting qubits and resonators

PCB with the qubit chip at 15 mK Protected from the environment by multiple shields

[Sutor, 2018]
How many qubits are required to see quantum improvement?

Estimate of the number of “good” qubits required before quantum computing shows advantage over conventional:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Type of Quantum Computer</th>
<th># Qubits for advantage (est)</th>
<th>Years to advantage (est)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum Chemistry</td>
<td>NISQ/Approximate QC</td>
<td>$10^2 \sim 10^3$</td>
<td>&lt; 5 ?</td>
</tr>
<tr>
<td>Optimization (specific)</td>
<td>NISQ/Approximate QC</td>
<td>$10^2 \sim 10^3$</td>
<td>&lt; 5 ?</td>
</tr>
<tr>
<td>Heuristic machine learning</td>
<td>NISQ/Approximate QC</td>
<td>$10^2 \sim 10^3$</td>
<td>&lt; 5 ?</td>
</tr>
<tr>
<td>Shor’s algorithm</td>
<td>Universal fault-tolerant QC</td>
<td>&gt; $10^8$</td>
<td>&gt; 10~15 if possible</td>
</tr>
<tr>
<td>Big Linear Algebra Programs (FEM)</td>
<td>Universal fault-tolerant QC</td>
<td>&gt; $10^8$</td>
<td>&gt; 10~15 if possible</td>
</tr>
</tbody>
</table>

[Sutor, 2018]
Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade.
“Quantum Computing: Progress and Prospects”

Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster.

— http://nap.edu/25196
Conclusions

• Quantum computers are not an immediate threat, they are rather a big opportunity for other areas, such as e.g. chemistry, optimisation tasks, and financial mathematics, now

• However, they are mid / long-term threat, so **be careful about retroactive cryptanalysis**

• Follow upcoming recommendation of cryptologists

• Be careful when implementing symmetric encryption on quantum hardware

• When appropriate, migrate to a quantum resistant public key cryptosystem
Physics is like sex: sure, it may give some practical results, but that's not why we do it.

Richard Phillips Feynman
(1918 - 1988, Nobel Prize in Physics 1965)