Quantum Computers & Implications for IT-Security

Alexander May
Ruhr-University Bochum
Horst-Görtz Institut for IT Security

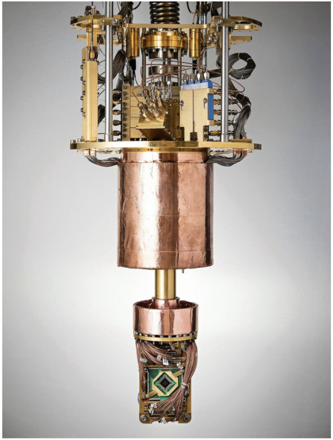
Summer School Kaliningrad – July 2019

Agenda

1. Basics of quantum computation
2. How quantum computers influence asym/sym crypto
3. Grover's search algorithm
4. Development of quantum computer

Spiegel on 18.05.2019

SPIEGEL ONLINE



D-Wave Systems

Quantenprozessor mit Kühlaggregat: "Die Fortschritte zuletzt waren geradezu fantastisch"

Quantencomputer

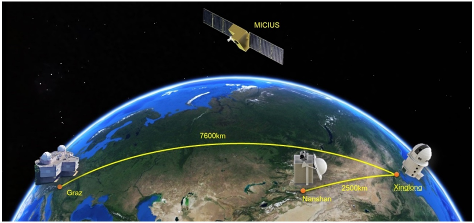
Diese Maschine wird unser Leben ändern

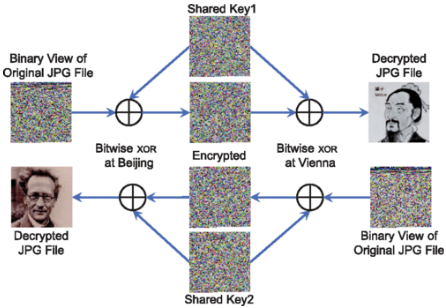
SPIEGEL+ Exklusiv für Abonnenten

Die Welt steht vor einer technischen Revolution: Quantencomputer - Millionen Mal schneller als moderne Superrechner. Sie könnten die großen Probleme der Menschheit lösen. *Von Thomas Schulz*

Picture from: *https://www.spiegel.de/plus*

Quantum Key Distribution (QKD)





Pictures: *https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html*

1-qubit system and superposition

1-qubit

$$|z\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \in \mathbb{C}^2$$

with $|0\rangle = (10), |1\rangle = (01)$, $\alpha_0, \alpha_1 \in \mathbb{C}$ and

$$||\alpha_0||^2 + ||\alpha_1||^2 = 1.$$

Example: $|z\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$

- We measure $|0\rangle$ with probability $||\alpha_0||^2 = \frac{1}{2}$.
- We measure $|1\rangle$ with probability $||\alpha_1||^2 = \frac{1}{2}$.

Observation

Measurement of $|z\rangle$ yields real **random bit.**

Positive und negative interference

Hadamard gate

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Application:

$$\begin{aligned} |0\rangle &\mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ &\mapsto \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \left(\frac{1}{2} + \frac{1}{2}\right)|0\rangle + \left(\frac{1}{2} - \frac{1}{2}\right)|1\rangle = |0\rangle \end{aligned}$$

2-qubit system and entanglement

2-qubit

$$|z\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle \in \mathbb{C}^4,$$

with $|00\rangle = (1000), \ldots, |11\rangle = (0001)$, $\alpha_0, \ldots, \alpha_3 \in \mathbb{C}$ and

$$||\alpha_0||^2 + ||\alpha_1||^2 + ||\alpha_2||^2 + ||\alpha_3||^2 = 1.$$

Example: Application of $H \otimes H$:

$$\begin{aligned} |00\rangle \mapsto & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle . \end{aligned}$$

Entanglement: $|z\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ (Einstein, Podolsky, Rosen)

- We measure $|0\rangle$ in first qubit with probability $||\alpha_0||^2 = \frac{1}{2}$.
- Then we always measure $|0\rangle$ in the second qubit (entanglement).

Some facts about quantum computation

n-qubit

An n-qubit system has 2^n many states $|0^n\rangle, \ldots, |1^n\rangle$.

- Classical computers can be simulated with quantum computers.
- Therefore quantum computers are at least as mighty.
- Quantum computers offer an amazing parallelism.
- **Example:** Evaluate function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$

$$|z\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \, |f(x)\rangle \, .$$

Good question

Does that help? Are quantum computers strictly more powerful?

Topic Post-Quantum Crypto

Better: Finding a period s, i.e. $f(x) = f(x + s)$ for all x.

Post-Quantum Crypto: Public key

- Breaks factoring/discrete log based crypto.
  - RSA
  - Diffie-Hellman
  - ElGamal
  - DSA
  - ECDSA
- Factoring/discrete log as efficient as encryption/decryption.

Rule of thumb

We have to replace our currently used public key crypto.
(when having robust quantum computers with sufficiently many qubits)

Best quantum algorithm: **Shor (1994)**

Symmetric world

Post-Quantum Crypto: Secret Key

Rule of thumb for symmetric crypto

- Doppel key lengths for
  - encryption,
  - authentication.
- Increase hash length bei factor $\frac{3}{2}$.

Best quantum algorithm: **Grover (1996)**

Question

Why factor 2?

Grover's algorithm (1996)

Grover function

Given $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with $f(x) = \begin{cases} 1 & \text{if} \quad x = x_0 \\ 0 & \text{if} \quad x \neq x_0 \end{cases}$. Find x_0.

- Classically, we need $\Theta(2^n)$ evaluations of f.

Grover's algorithm

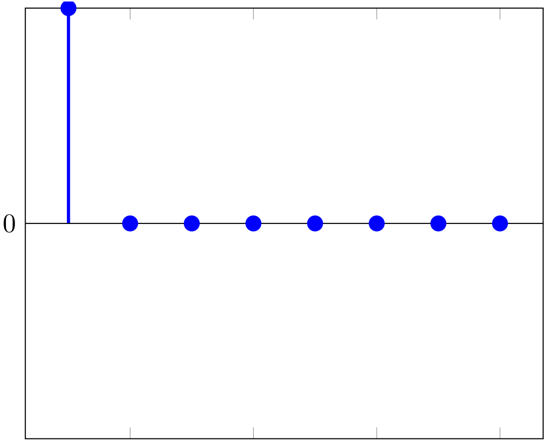
On a quantum computer we only need $\Theta(2^{n/2})$ evaluations.

- We gain (only) a square root.
- But has many applications.

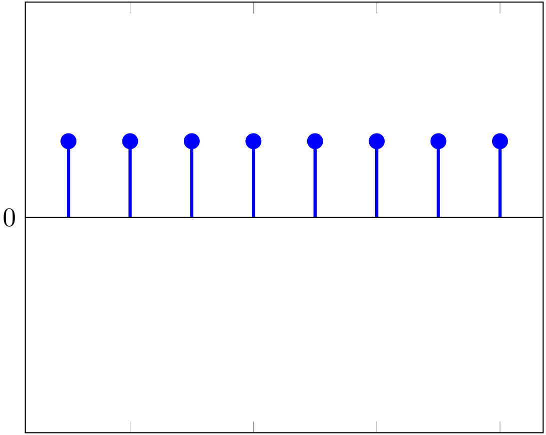
Example: Grover with 3 qubits

Consider $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ with $f(x) = 1 \Leftrightarrow x = 011$.

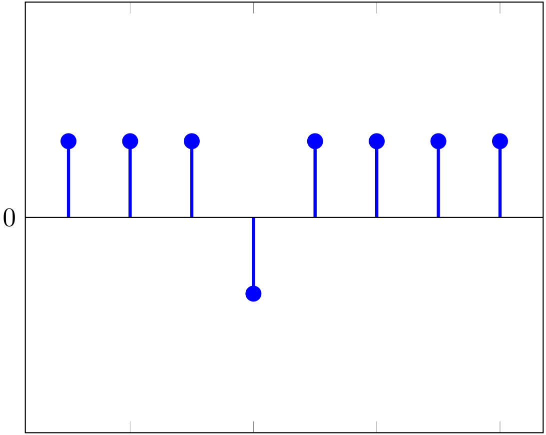
Grover's algorithm



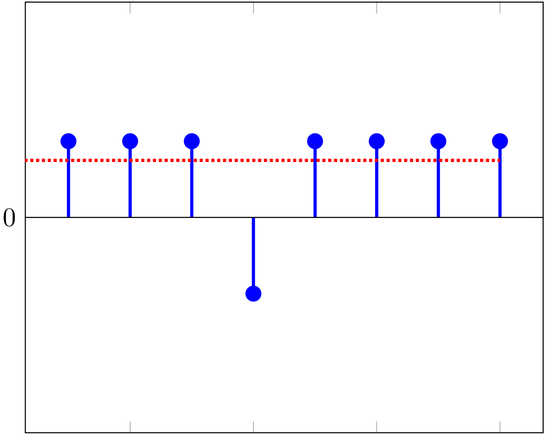
Grover's algorithm



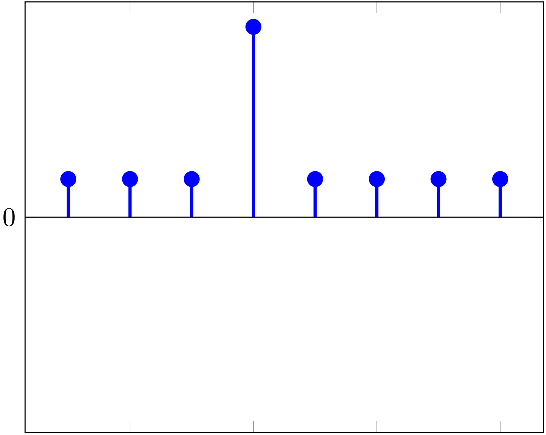
Grover's algorithm



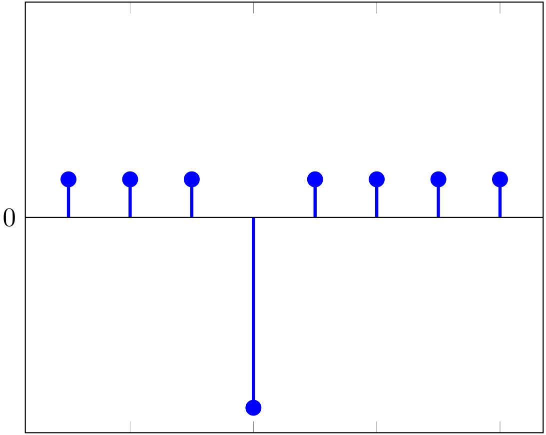
Grover's algorithm



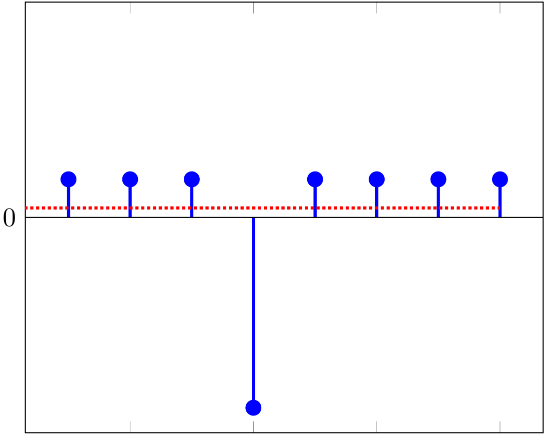
Grover's algorithm



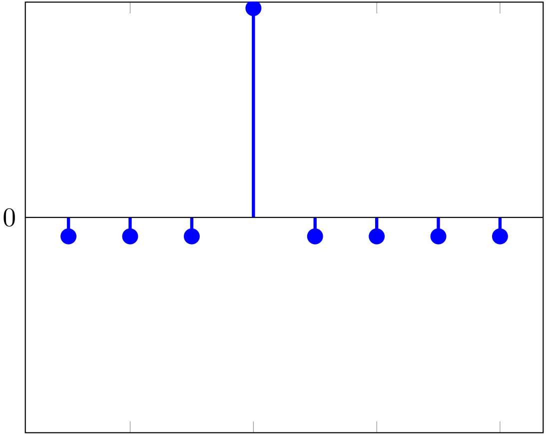
Grover's algorithm



Grover's algorithm



Grover's algorithm



Grover's algorithm applied to block ciphers

Block cipher

$$m \longrightarrow \boxed{E_k} \longrightarrow c$$

Define a Grover function

$$f(x) = \begin{cases} 1 & \text{is } E_x(m) = c \\ 0 & \text{else} \end{cases}.$$

Attack

Apply Grover's algorithm to f for finding k in time $\Theta(2^{n/2})$.

E.g. breaking AES-128 requires only 2^{64} steps instead of 2^{128}.

Sym. Crypto: Encryption/Authentication

Table: Security (in bit) of block ciphers.

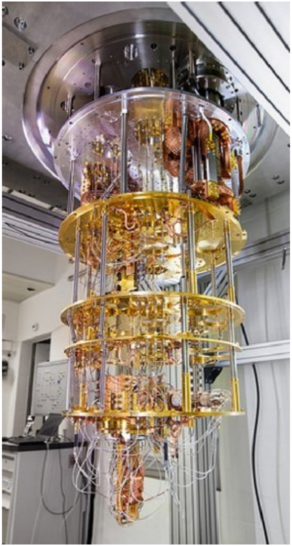
Scheme	classic	quantum
AES-128	128	64
AES-256	256	128

Sym. Krypto: hash functions

Table: Security (in bit) of hash functions.

Family	Scheme	Security	
		classic	quantum
SHA-3	SHA3-256	128	85
	SHA3-384	192	128

Quantum computer



Picture: *https://www.designnews.com/electronics-test/quantum-computing-101-5-key-concepts-understand/208209538060343*

Status of quantum computers

1. Google AI Quantum: 72-qubit computer
2. IBM Q: 50-qubit computer

IBM Q

- Network of 50-qubit computers.
- Freely available 5- und 16-qubit devices.
- Comfortable programming environment (quiskit).
- Quite error prone.

Breaking of RSA-1024

2048 qubits with Shor, 513 qubits with Ekera-Hastad & May-Schlieper.

$$|z\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_{\mathbb{N}}} |x\rangle \, |a^x \bmod N\rangle \, .$$

IBM Q

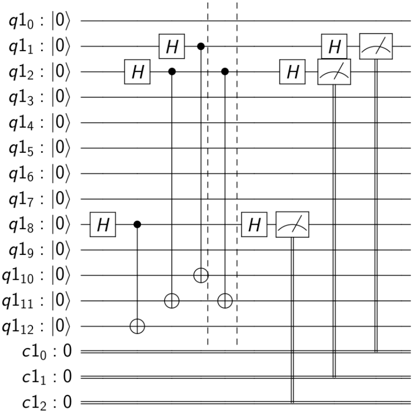


Figure: Implementation of period finding

IBM Q

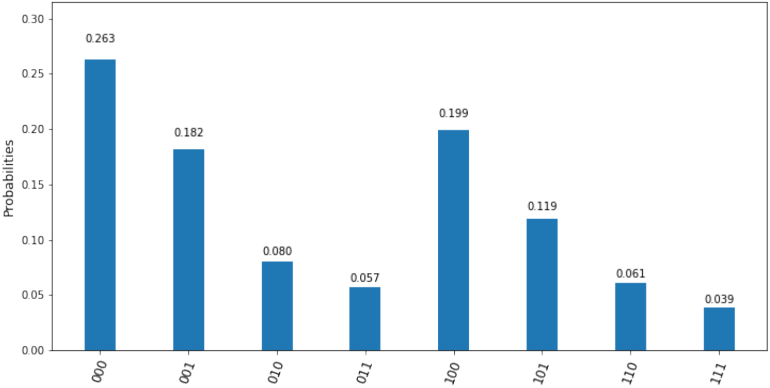


Figure: Period is $s = 010$.

Summary

Lessons learned

- Quantum algorithms solve some problems faster.
  - Speed-up is small for most problems.
  - May allow for efficient simulations of quantum systems.
  - Quantum crypto does not solve all problems in crypto!
- There is progress in constructing quantum computers.
- Tuning of secret key crypto quite easy.
- RSA/Dlog in this decade save, but substitution takes time.
- We will see a shift towards PQ crypto!