Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

QUANTENCOMPUTING

Grundlagen, Anwendungen und Bedrohungen

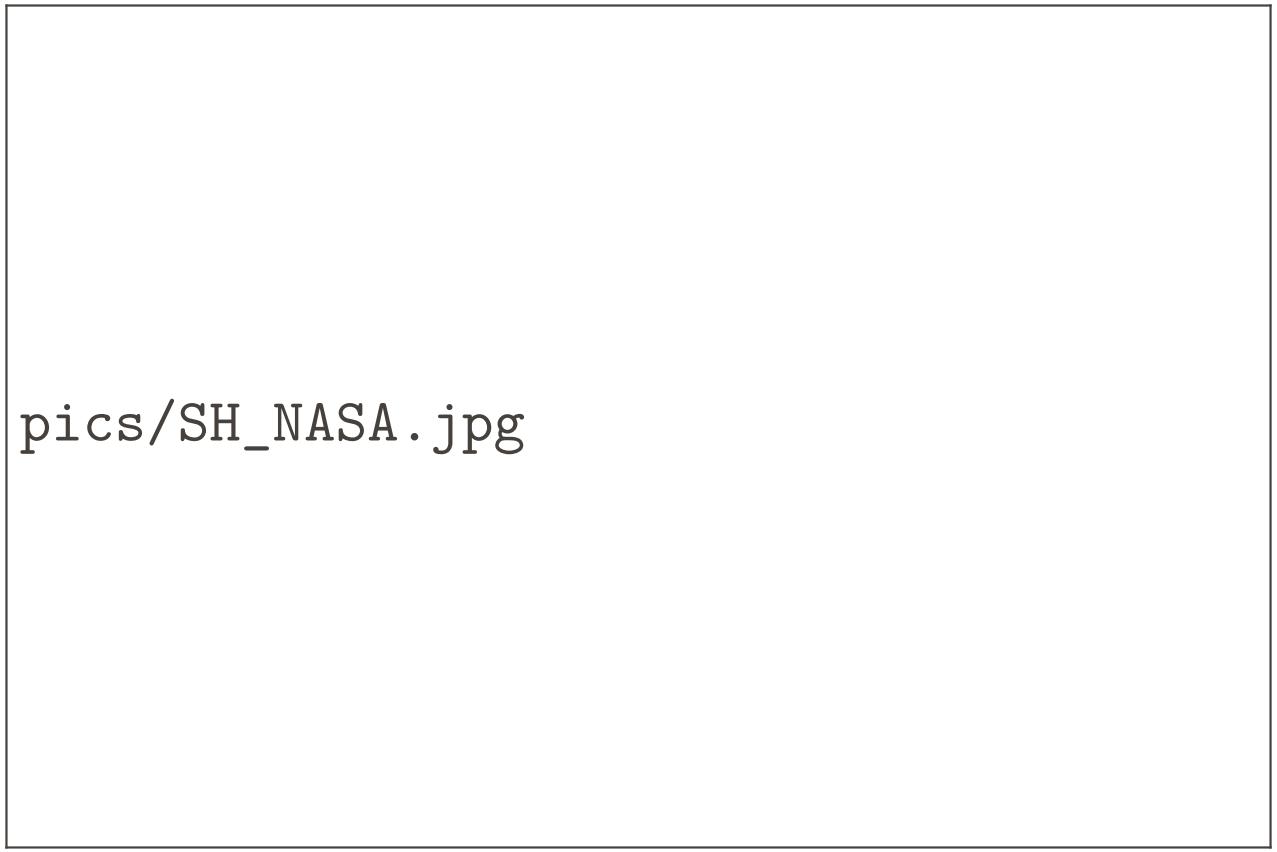
15. Feburar 2023

Steffen Reith
Steffen.Reith@hs-rm.de

Theoretische Informatik
Hochschule **RheinMain**

EINFÜHRUNG

ICH HAB DA EIN GANZ MIESES GEFÜHL



Jim Campbell/Aero-News Network - **https://www.flickr.com/photos/39735679@N00/475109138/**

„Jede mathematische Formel in einem Buch halbiert die Verkaufszahlen dieses Buches.“

Stephen Hawking

KURZE VORSTELLUNG

- → Seit Sommer 2006 Professor für **Theoretische Informatik** Hochschule RheinMain (ursprünglich FH Wiesbaden)
- → Vorher: Softwareentwickler für **kyptographische und mathematische Algorithmen** für tief eingebettete Systeme im KFZ-Bereich bei ElektroBit in Erlangen.
- → Arbeitsgebiete: **Kryptographie**, **eingebettete Systeme**, **Hardware** Design für **PQC**, Komplexitätstheorie, Logik und computational number theory

ARBEITSGRUPPE THEORETISCHE INFORMATIK

Forschungsgebiete:

- → **OpenSource Hardware** (kryptographische Beschleuniger)
- → **Post Quantum Kryptographie** (PQC)
- → (tief) eingebettete Systeme (μC, FPGAs and ASICs) (Fokus: **Automotive** und IoT)
- → Kryptographische Algorithmen & Zahlentheorie

Das Team:

- → Vier Doktoranden **Open-Source Hardware** vom BMBF & Innenminsterium Hessen (QuantumRISC / VE-HEP / Progenitor) finanziert
- → Zwei Doktoranden für **PQC** interne Mittel
- → Ein externer Doktorand **Intrusion Detection for CAN-networks**, aus der Automobilindustrie finanziert
- → Ein externer Doktorand **Forensics for Smart-Phones** durch Bundesbehörde finanziert

BERECHENBARKEIT

WAS BEDEUTET BERECHENBARKEIT EIGENTLICH?

Intuitiv:

1. Es gibt eine **Berechnungsanweisung** (Programm / Algorithmus)
2. Die Berechnungsanweisung bekommt **Eingaben**
3. Nach Abarbeitung der Anweisungen bekommen wir eine **Ausgabe**

WAS BEDEUTET BERECHENBARKEIT EIGENTLICH?

Intuitiv:

1. Es gibt eine **Berechnungsanweisung** (Programm / Algorithmus)
2. Die Berechnungsanweisung bekommt **Eingaben**
3. Nach Abarbeitung der Anweisungen bekommen wir eine **Ausgabe**

In der Informatik sind eine **Vielzahl** von solchen **Berechenbarkeitsmodellen** bekannt (Webstühle, Turing-Maschinen, C/C++, Python, μ-Rekursion, λ-Kalkül, WHILE-Programme, Zweikellerautomaten, DNA-Computer, **Quantencomputer**, . . .)

WAS BEDEUTET BERECHENBARKEIT EIGENTLICH?

Intuitiv:

1. Es gibt eine **Berechnungsanweisung** (Programm / Algorithmus)
2. Die Berechnungsanweisung bekommt **Eingaben**
3. Nach Abarbeitung der Anweisungen bekommen wir eine **Ausgabe**

In der Informatik sind eine **Vielzahl** von solchen **Berechenbarkeitsmodellen** bekannt (Webstühle, Turing-Maschinen, C/C++, Python, μ-Rekursion, λ-Kalkül, WHILE-Programme, Zweikellerautomaten, DNA-Computer, **Quantencomputer**, . . .)

Wir **berechnen eine (mathematische) Funktion**, wenn für Sie ein **Algorithmus formuliert** werden kann, die Art des Algorithmus wird durch das Berechenbarkeitsmodell festgelegt.

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (und allen genannten Berechenbarkeitsmodellen) **berechenbar**.

Alonzo Church

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (und allen genannten Berechenbarkeitsmodellen) **berechenbar**.

Alonzo Church

Wichtige Fragestellungen für die Praxis:

→ Kann das Berechenbarkeitsmodell manche Dinge besser?

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (und allen genannten Berechenbarkeitsmodellen) **berechenbar**.

Alonzo Church

Wichtige Fragestellungen für die Praxis:

- → Kann das Berechenbarkeitsmodell manche Dinge besser?
- → Kann das Berechenbarkeitsmodell (technisch) realisiert werden?

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (und allen genannten Berechenbarkeitsmodellen) **berechenbar**.

Alonzo Church

Wichtige Fragestellungen für die Praxis:

- → Kann das Berechenbarkeitsmodell manche Dinge besser?
- → Kann das Berechenbarkeitsmodell (technisch) realisiert werden?
- → Löst das Berechenbarkeitsmodell (technisch) wichtige Probleme?

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (und allen genannten Berechenbarkeitsmodellen) **berechenbar**.

Alonzo Church

Wichtige Fragestellungen für die Praxis:

- → Kann das Berechenbarkeitsmodell manche Dinge besser?
- → Kann das Berechenbarkeitsmodell (technisch) realisiert werden?
- → Löst das Berechenbarkeitsmodell (technisch) wichtige Probleme?

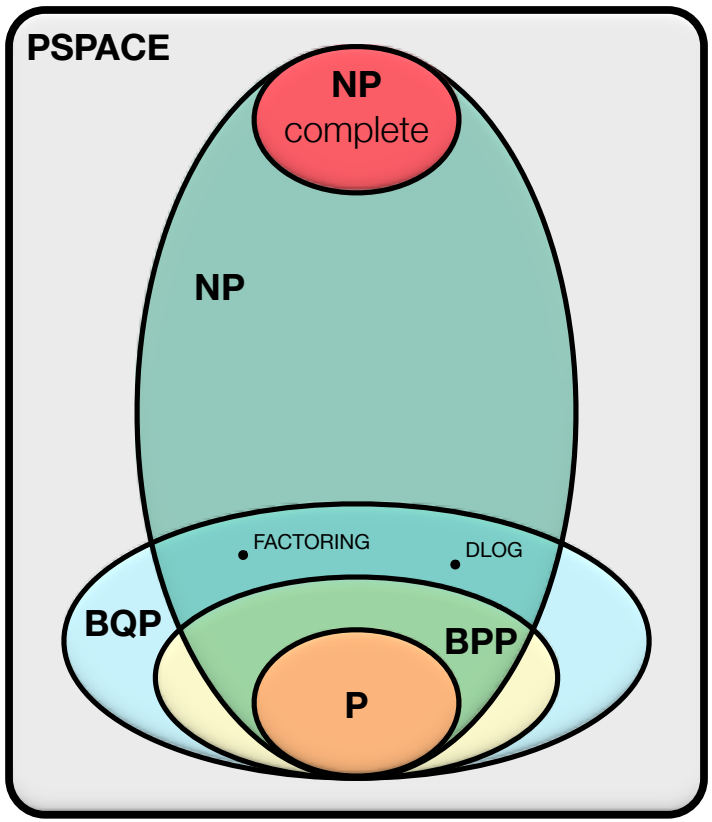
Von Quantencomputer **glauben** wir, dass alle drei **Fragen positiv beantwortet** werden können

QUANTENCOMPUTER

ERZÄHLE MIR NICHT, WIE MEINE CHANCEN STEHEN!

Man glaubt, dass **Quantencomputer** bestimmte Probleme **schneller lösen** können als “klassische” Computer.

Eine aktuell akzeptierte “Landkarte” aus der Komplexitätstheorie:



EINE ERSTE IDEE

Ein Computer besteht aus einem **gespeicherten Zustand** und (einer Folge von) **Befehlen** die den Zustand ändern, um aus der Eingabe die Ausgabe zu machen.

Klassische Computer verwenden **Bits**, die entweder 0 (falsch) oder 1 (wahr) speichern.

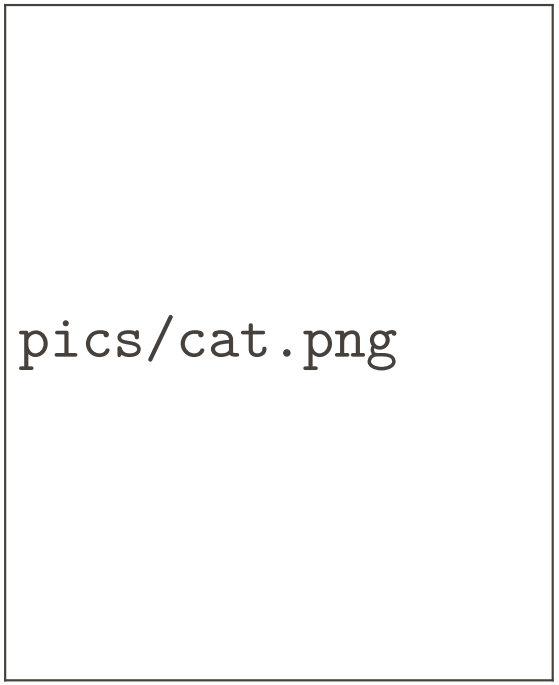
EINE ERSTE IDEE

Ein Computer besteht aus einem **gespeicherten Zustand** und (einer Folge von) **Befehlen** die den Zustand ändern, um aus der Eingabe die Ausgabe zu machen.

Klassische Computer verwenden **Bits**, die entweder 0 (falsch) oder 1 (wahr) speichern.

Unter **Superposition** versteht man die Fähigkeit eines Quantensystems sich in **mehreren Zuständen gleichzeitig** zu befinden bis es **gemessen** wird.

Mit dieser Idee können sogenannte **QuBits** realisiert werden, die sich gleichzeitig im Zustand 0 und 1 befinden.



EINE ERSTE IDEE

Ein Computer besteht aus einem **gespeicherten Zustand** und (einer Folge von) **Befehlen** die den Zustand ändern, um aus der Eingabe die Ausgabe zu machen.

Klassische Computer verwenden **Bits**, die entweder 0 (falsch) oder 1 (wahr) speichern.

Unter **Superposition** versteht man die Fähigkeit eines Quantensystems sich in **mehreren Zuständen gleichzeitig** zu befinden bis es **gemessen** wird.

Mit dieser Idee können sogenannte **QuBits** realisiert werden, die sich gleichzeitig im Zustand 0 und 1 befinden.

pics/cat.png

Hoffnung: Damit kann man bestimmt schneller rechnen!?

QUBITS

Definition (Qubit)

Ein **Quantenbit** (kurz: QuBit) ist eine Linearkombination der Form

$$\alpha |0\rangle + \beta |1\rangle$$

Es gilt $\alpha, \beta \in \mathbb{C}$ und $|\alpha|^2 + |\beta|^2 = 1$

Die Wert α und β werden als **Amplitude** bezeichnet.

QUBITS

Definition (Qubit)

Ein **Quantenbit** (kurz: QuBit) ist eine Linearkombination der Form

$$\alpha |0\rangle + \beta |1\rangle$$

Es gilt $\alpha, \beta \in \mathbb{C}$ und $|\alpha|^2 + |\beta|^2 = 1$

Die Wert α und β werden als **Amplitude** bezeichnet.

Ist $\alpha \neq 0$ oder $\beta \neq 0$, dann befindet sich das QuBit gleichzeitig in beiden Zuständen (**Superposition**).

Beispiel (zulässige Zustände eines QuBits)

- → $|0\rangle$ und $|1\rangle$ (klassische Zustände)
- → $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$, da $\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 1$

MAKE IT SO!

Messen wir ein Qubit, so tritt der

→ **Zustand** $|0\rangle$ mit **Wahrscheinlichkeit** $|\alpha|^2$ auf und der

→ **Zustand** $|1\rangle$ mit **Wahrscheinlichkeit** $|\beta|^2$.

MAKE IT SO!

Messen wir ein Qubit, so tritt der

→ **Zustand** $|0\rangle$ mit **Wahrscheinlichkeit** $|\alpha|^2$ auf und der

→ **Zustand** $|1\rangle$ mit **Wahrscheinlichkeit** $|\beta|^2$.

Die **Wahrscheinlichkeiten** hängen vom **Quadrat des Betrags der Amplituden** ab!

MAKE IT SO!

Messen wir ein Qubit, so tritt der

- → **Zustand** $|0\rangle$ mit **Wahrscheinlichkeit** $|\alpha|^2$ auf und der
- → **Zustand** $|1\rangle$ mit **Wahrscheinlichkeit** $|\beta|^2$.

Die **Wahrscheinlichkeiten** hängen vom **Quadrat des Betrags der Amplituden** ab!

Beispiel

Messung von $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ergibt

- → $|0\rangle$ mit Wahrscheinlichkeit $\frac{1}{2}$
- → $|1\rangle$ mit Wahrscheinlichkeit $\frac{1}{2}$

THINGS ARE ONLY IMPOSSIBLE UNTIL THEY'RE NOT

QuBits können auch ganz klassisch als **Linearkombination von Vektoren** geschrieben werden:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Ein **Rechenschritt** eines Quantencomputers ist die Anwendung / **Multiplikation** einer (quadratischen) **Matrix** auf den Speicher (aus QuBits gebaut). Also gilt für einen Rechenschritt:

$$M: \mathbb{C}^n \to \mathbb{C}^n, \vec{v} \mapsto M \cdot \vec{v}$$

Beispiel (No Operation (NOP) eines Quantencomputers)

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

HASTA LA VISTA, BABY!

Sei $x + iy$ mit $i = \sqrt{-1}$ eine komplexe Zahl, so heißt $x - iy$ die **konjugierte** Zahl.

→ **Spiegeln** einer Matrix M: **transponierte** Matrix M^T

→ Alle Einträge konjugieren: **konjugierte** Matrix $\overline{M}$

$$M = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

Eine Matrix heißt **unitär**, wenn gilt

$$\overline{M}^T \cdot M = 1$$

NEED FOR SPEED

Die **Quantenmechanik verlangt**, dass eine Matrix für einen Quantencomputer ($\widehat{=}$) Programmbefehl) **unitär sein muss**!

Beispiel (Hadamard-Matrix)

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

H ist **unitär**!

Jacques Hadamard

Die **Hadamard-Matrix** kann technisch **realisiert werden** und führt zu einem einfachen Quantenalgorithmus!

EIN EINFACHER ALGORITHMUS

random.slq

```
1  // Example random-number generation
2  def main(){
3      x:=0:B;
4      x:=H(x);
5      return measure(x);
6  }
7
```

Es gilt: $|0\rangle \xmapsto{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

Die **Messung in Zeile 5** liefert also einen **fairen Münzwurf**!

DEMO

ALGORITHMEN

BERECHNUNGSPROBLEME

PROBLEM: SEARCH
INPUT: Funktion/Datenbank f mit $N = 2^n$ Einträgen, Element $\hat{x}$
OUTPUT: Position von $\hat{x}$ in der Datenbank

PROBLEM: FACTORING
INPUT: Natürliche Zahl N
OUTPUT: Primfaktorzerlegung $N = p_1 \cdot p_2 \cdot \cdots \cdot p_l$

PROBLEM: DLOG(G)
INPUT: Gruppe G, Element $g \in G$ und $b = g^x$
OUTPUT: Exponent x

BERECHNUNGSPROBLEME

Algorithmus (Grover's Algorithmus)

Das Problem SEARCH kann

→ mit **klassischen** Computern in $N - 1$ **Schritten** und mit

→ **Quantencomputern in** $O(\sqrt{N})$ Schritten gelöst werden.

BERECHNUNGSPROBLEME

Algorithmus (Grover's Algorithmus)

Das Problem SEARCH kann

→ mit **klassischen** Computern in $N - 1$ **Schritten** und mit

→ **Quantencomputern in** $O(\sqrt{N})$ Schritten gelöst werden.

Algorithmus (Shor's Algorithmus)

Das Problem FACTORING (DLOG(G)) kann

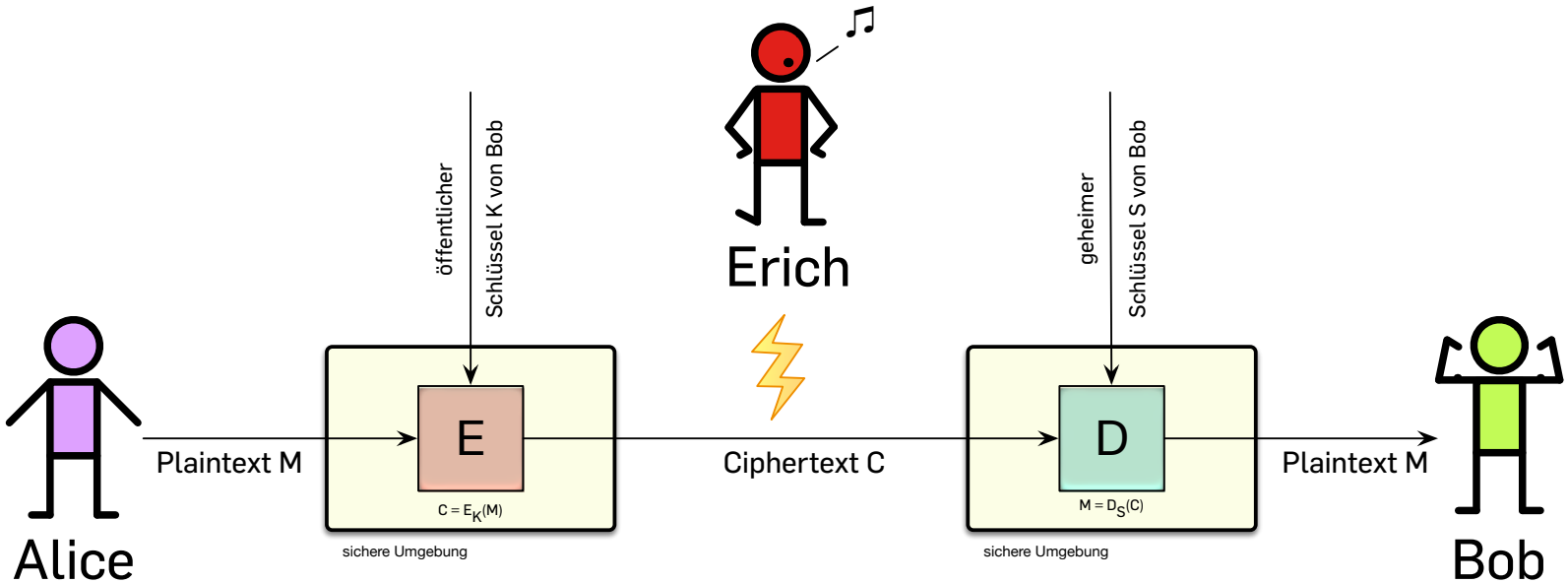
→ im **klassischen** Fall in $e^{\sqrt[3]{\frac{64}{9}+o(1)}\sqrt[3]{\log N}\sqrt[3]{(\log\log N)^2}}$ **Schritten** (Zahlkörpersieb) und mit

→ **Quantencomputern in** $O(\log N^3)$ Schritten gelöst werden.

ICH BRAUCH MAL URLAUB

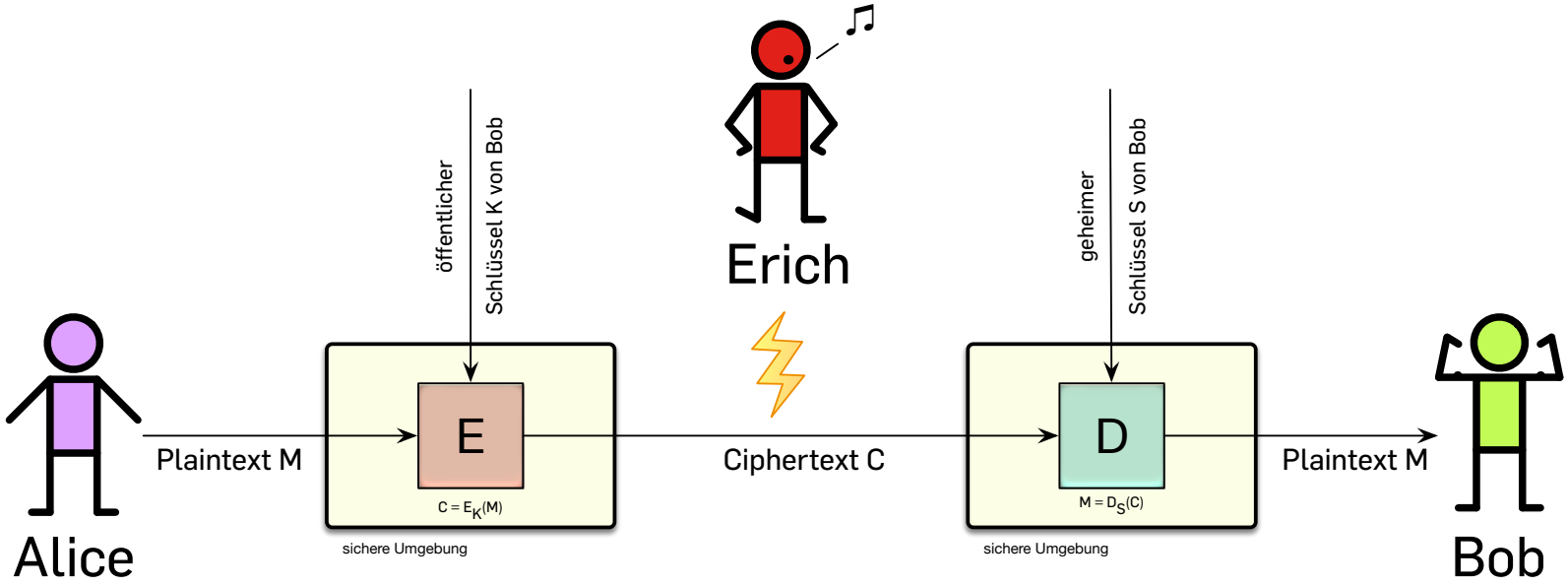
Massive Auswirkungen auf die Kryptographie, Internet, Banking und IT-Sicherheit.

Grover's Algorithmus bedingt eine **Verdopplung der Schlüssellängen** von **symmetrischen** Verfahren.



SETEC ASTRONOMY - NO MORE SECRETS

Shor's Algorithmus macht **ALLE** gebräuchlichen **asymmetrischen** Verfahren **unbrauchbar**!



Keine digitalen Unterschriften, keine Zertifikate (z.B. `https`), kein TLS, keine sichere EMail / Messenger, kein Streaming, kein Update over the Air . . .

POST QUANTUM KRYPTOGRAPHIE

Asymmetrische Kryptographie funktioniert nicht mehr, wenn Physiker **leistungsfähige Quantencomputer** bauen können.

Idee: Suche **Verfahren für klassische Computer**, die noch **sicher** sind, wenn der **Angreifer** einen **Quantencomputer hat**.

POST QUANTUM KRYPTOGRAPHIE

Asymmetrische Kryptographie funktioniert nicht mehr, wenn Physiker **leistungsfähige Quantencomputer** bauen können.

Idee: Suche **Verfahren für klassische Computer**, die noch **sicher** sind, wenn der **Angreifer** einen **Quantencomputer hat**.

Internationaler Wettbewerb (vom NIST organisiert) untersucht fünf Familien:

- → Verfahren mit multivariaten Polynome
- → **Verfahren mit kryptologischen Hashfunktionen** (vgl. SPHINCS$^+$)
- → Kryptographie mit fehlerkorrigierenden Codes (vgl. McEliece-Kryptosystem)
- → **Verfahren mit Isogenien zwischen supersingulären elliptische Kurven** (vgl. CSIDH)
- → Gitterbasierte Kryptografie (vgl. KYBER / DILITHIUM)

DIE ZUKUNFT

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE

Es stellt sich die Frage: "**Wann** brauchen wir Post Quantum Kryptographie?"

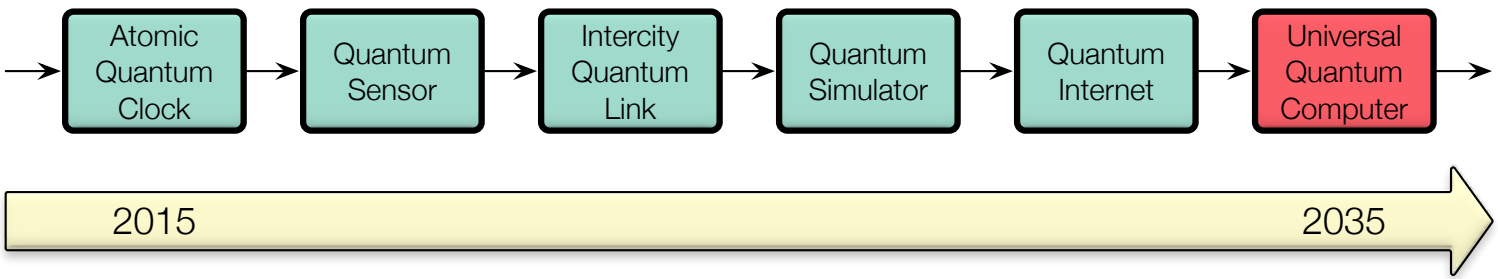
Klar: **Daten** müssen evtl. **lange beschützt werden** (z.B. Medizindaten oder Autos). Wenn es **noch 30 Jahre** dauert, dann sind wir schon **spät dran**!

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE

Es stellt sich die Frage: "**Wann** brauchen wir Post Quantum Kryptographie?"

Klar: **Daten** müssen evtl. **lange beschützt werden** (z.B. Medizindaten oder Autos). Wenn es **noch 30 Jahre** dauert, dann sind wir schon **spät dran**!

Pessimistische Sichtweise:

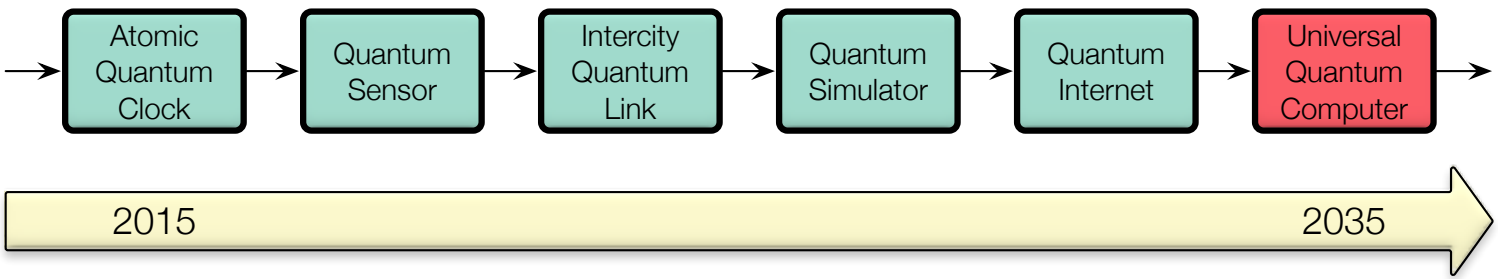


DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE

Es stellt sich die Frage: "**Wann** brauchen wir Post Quantum Kryptographie?"

Klar: **Daten** müssen evtl. **lange beschützt werden** (z.B. Medizindaten oder Autos). Wenn es **noch 30 Jahre** dauert, dann sind wir schon **spät dran**!

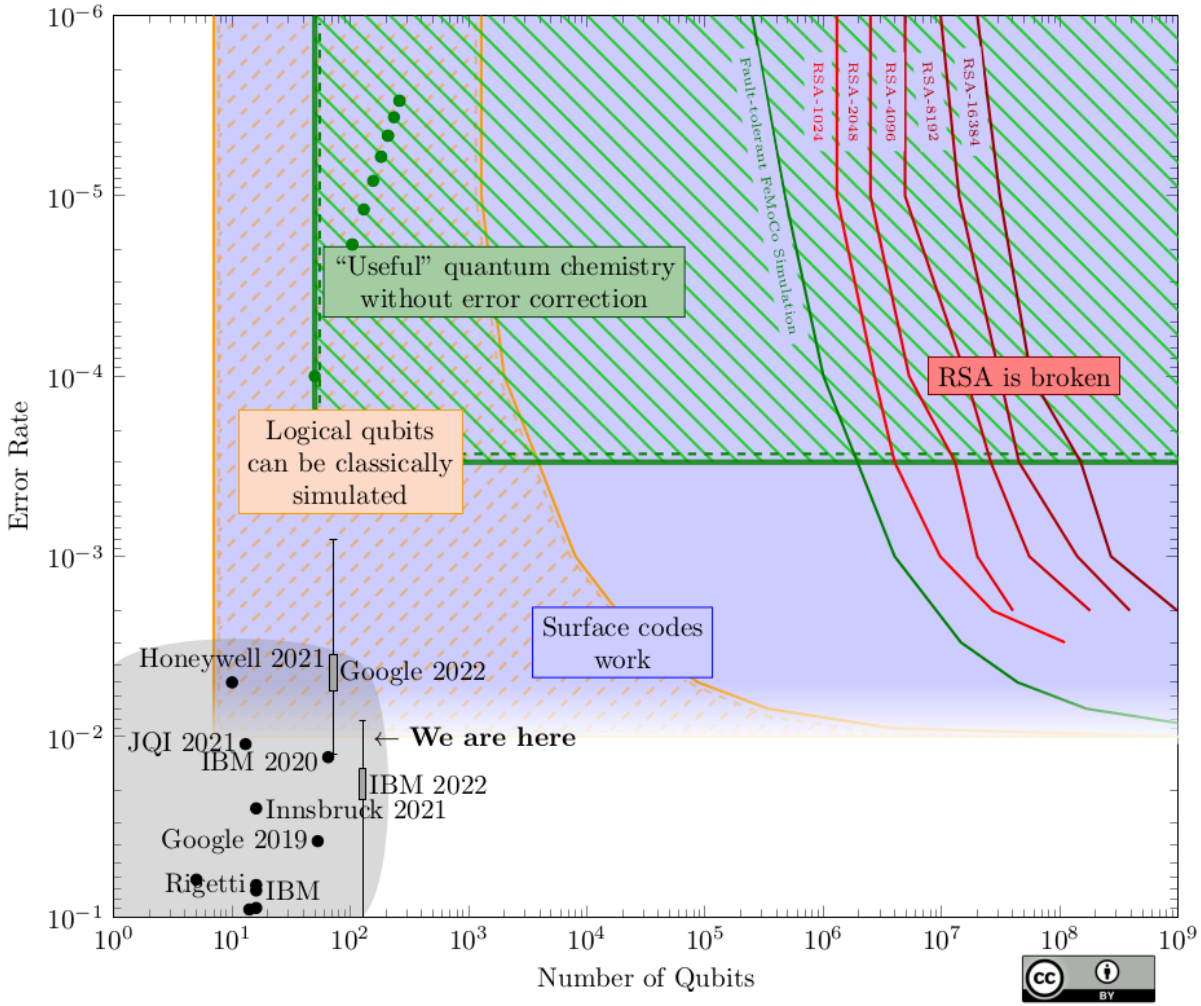
Pessimistische Sichtweise:



Optimistische (nicht ganz ernstgemeinte) Sichtweise:
Die Physiker versprechen seit **50 Jahren**, dass ein Fusionsreaktor **in 20 Jahren fertig** ist. Das ist bei Quantencomputern sicherlich auch so!

STANDORTBESTIMMUNG

Wirtschaftliche Interessen können Entwicklungen **beschleunigen**!



Samuel Jaques **https://sam-jaques.appspot.com/quantum_landscape_2022**

Vielen Dank!