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

WENN QUANTEN RECHNEN LERNEN

Der Wettlauf um die Zukunft der Kryptographie

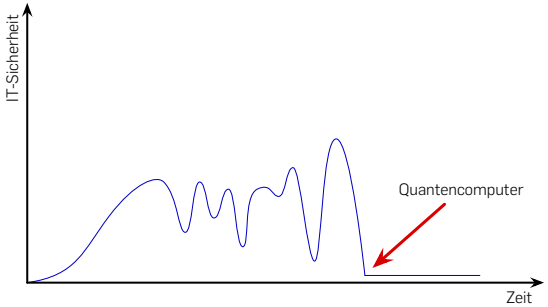
18. Dezember 2025

Steffen Reith
Steffen.Reith@hs-rm.de

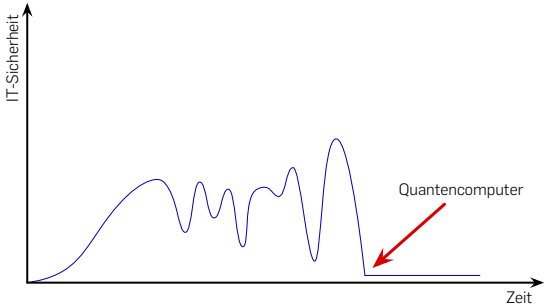
Computer Science
Hochschule **RheinMain**

EINLEITUNG

Wahrnehmung: Quantencomputern machen IT-Sicherheit unmöglich:



Wahrnehmung: Quantencomputern machen IT-Sicherheit unmöglich:



Fragen:

- Was sind Quantencomputer?
- Warum haben diese einen so starken Einfluss?
- Was könnnen / müssen wir tun?

DIE WELT DIE WIR KENNEN HÄNGT AN DER KRYPTOGRAPHIE

Klassische Gebiete

- **Vertraulichkeit** (Verschlüsselung)
- **Integrität** (Hashfunktionen)
- **Authentizität** / Nichtabstreitbarkeit (digitale Signaturen)
- **Authentifizierung** (Challenge-Response, Zero-Knowledge-Proofs)

DIE WELT DIE WIR KENNEN HÄNGT AN DER KRYPTOGRAPHIE

Klassische Gebiete

- **Vertraulichkeit** (Verschlüsselung)
- **Integrität** (Hashfunktionen)
- **Authentizität** / Nichtabstreitbarkeit (digitale Signaturen)
- **Authentifizierung** (Challenge-Response, Zero-Knowledge-Proofs)

Finanzsektor:	Manipulation von Zahlungen, hohe Verluste, Marktzusammenbrüche
Infrastrukturen:	Sabotage / Manipulation von Energie-, Verkehrs- und Versorgungssystemen, großflächige Ausfälle
Demokratie:	Militär- und Wahldaten, Gefährdung nationaler Sicherheit, demokratische Legitimität
Privatpersonen:	Massiver Identitätsdiebstahl, finanzielle Verluste, Erpressung durch veröffentlichte sensible Daten
Digitale Dienste:	Gefälschte Software-Updates, manipulierte Verträge, Haftungs- und Rechtskosten.

KRYPTOGRAPHIE

AM ANFANG WAR DAS LICHT

AM ANFANG WAR DAS LICHT

Für eine Verschlüsselung benötigen wir:

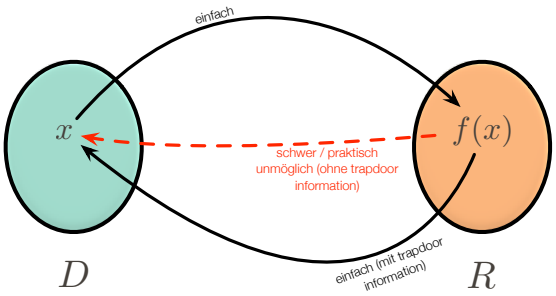
Sender: Eine **effiziente Methode** (Wissen) die **Nachricht** zu **verbergen** / verschlüsseln

Empfänger: Eine **effiziente Methode** (mit Wissen!) die Nachricht zurückzugewinnen.

Angreifer: **Keine praktische Chance** ohne Wissen die Nachricht zu erhalten.

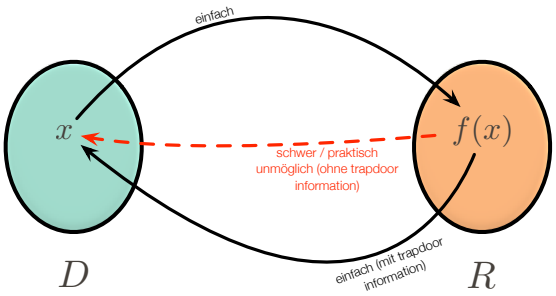
IT'S A TRAP!

Für die Konstruktion von (asymmetrischen) Kryptosystemen verwenden wir **Trapdoorfunktionen**:



IT'S A TRAP!

Für die Konstruktion von (asymmetrischen) Kryptosystemen verwenden wir **Trapdoorfunktionen**:



Frage: Was bedeuten die Begriffe **einfach** und **schwer / praktisch unmöglich**?

DU KANNST NICHT VORBEI!

Laufzeiten von Algorithmen auf einen Rechner mit 1 PIPS (10^{15} Instruktionen pro Sekunde)

Anzahl der Takte	Eingabelänge n = 10	30	50	70	90
n	10 fs	30 fs	50 fs	70 fs	90 fs
n^2	0.1 ps	0.9 ps	2.5 ps	4.9 ps	8.1 ps
n^3	0.001 ns	0.027 ns	0.125 ns	0.343 ns	0.729 ns
n^5	0.1 ns	24.3 ns	312.5 ns	1680.7 ns	5904.9 ns
2^n	0.001 ns	1074 ns	1.13 s	13.66 Tage	39320 Jahre
3^n	0.059 ns	0.206 s	22.76 Jahre	$7.93 \cdot 10^{10}$ Jahre	$2.77 \cdot 10^{20}$ Jahre

DU KANNST NICHT VORBEI!

Laufzeiten von Algorithmen auf einen Rechner mit 1 PIPS (10^{15} Instruktionen pro Sekunde)

Anzahl der Takte	Eingabelänge n = 10	30	50	70	90
n	10 fs	30 fs	50 fs	70 fs	90 fs
n^2	0.1 ps	0.9 ps	2.5 ps	4.9 ps	8.1 ps
n^3	0.001 ns	0.027 ns	0.125 ns	0.343 ns	0.729 ns
n^5	0.1 ns	24.3 ns	312.5 ns	1680.7 ns	5904.9 ns
2^n	0.001 ns	1074 ns	1.13 s	13.66 Tage	39320 Jahre
3^n	0.059 ns	0.206 s	22.76 Jahre	$7.93 \cdot 10^{10}$ Jahre	$2.77 \cdot 10^{20}$ Jahre

Fazit: Es gibt Berechnungprobleme die auch mit extrem mächtigen Computern (vermutlich) **nicht gelöst** werden können.

SCHWIERIGE PROBLEME

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 $N = p_1 \cdot p_2 \cdot \ldots \cdot p_l$

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

Alle aktuell (technisch) verwendeten asymmetrischen Verfahren und der Diffie-Hellman Schlüsselaustausch **verwenden** FACTORING oder (Varianten) von DLOG!

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (oder C-Programmen) **berechenbar**.

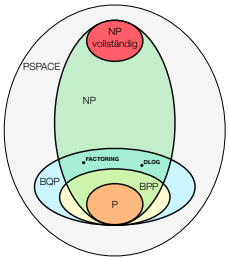
Alonzo Church

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (oder C-Programmen) **berechenbar**.

Alonzo Church



In der Praxis:

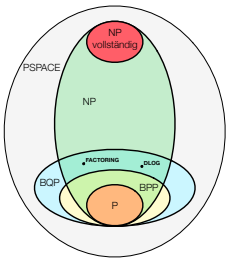
- Kann ein Maschinentyp manche **Dinge besser**?
- Kann das Modell **realisiert** werden?
- Löst das Modell (technisch) **wichtige Probleme**?

GIBT ES UNTERSCHIEDE?

These (These von Church (1936))

Alle im **intuitiven Sinn** berechenbaren Funktionen sind schon durch eine **Turing-Maschine** (oder C-Programmen) **berechenbar**.

Alonzo Church



In der Praxis:

- Kann ein Maschinentyp manche **Dinge besser**?
- Kann das Modell **realisiert** werden?
- Löst das Modell (technisch) **wichtige Probleme**?

Quantencomputer: alle **drei Fragen** sind (wohl) positiv zu beantworten

QUANTENCOMPUTING

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.

Klassisch: **Bits** (**entweder** 0 (falsch) oder 1 (wahr))

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.

Klassisch: **Bits** (**entweder** 0 (falsch) oder 1 (wahr))

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.

Klassisch: **Bits** (**entweder** 0 (falsch) oder 1 (wahr))

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.

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 $|\alpha|^2 + |\beta|^2 = 1$ (α und β heißen **Amplitude**)

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 $|\alpha|^2 + |\beta|^2 = 1$ (α und β heißen **Amplitude**)

Wenn $\alpha \neq 0$ und $\beta \neq 0$, dann ist ein 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** $|\beta|^2$.

Beispiel (Ein Zufallszahlengenerator)

Messung eines QuBits mit $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ ergibt

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

THAT'S ONE SMALL STEP FOR MAN . . .

Ein **Rechenschritt** eines Quantencomputers ist die Anwendung / **Multiplikation** einer (quadratischen) **Matrix** $\mathbb{C}^{n\times n}$ auf den Speicher (aus Qubits gebaut). Also gilt für einen Rechenschritt:

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

Beispiel (No Operation (NOP) eines Quantencomputers)

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

NEED FOR SPEED

Die **Quantenmechanik / Physik verlangt**, dass eine Matrix M für einen Quantencomputer ($\widehat{=}$ Programmbefehl) **unitär** (also $\overline{M}^T \cdot M = 1$) 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!

HASTA LA VISTA, BABY!

random.slq

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

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** (TRNG)!

[1] **https://silq.ethz.ch/**
[2] **https://www.qrisp.eu/**

HASTA LA VISTA, BABY!

random.slq

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

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

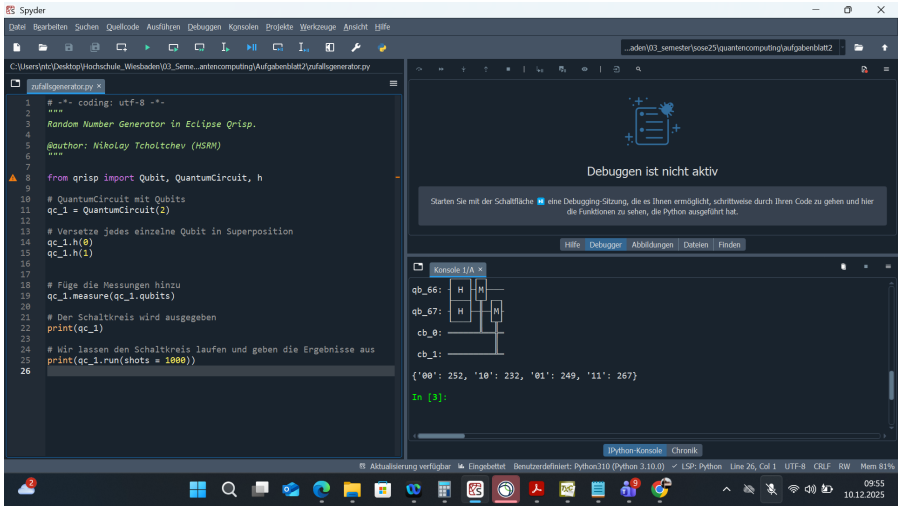
Die **Messung in Zeile 5** liefert also einen **fairen Münzwurf** (TRNG)!

Für `random.slq` wurde Silq[1] (ETHZ) verwendet. Eine **(bessere) Alternative ist QRISP**[2], das u.a. auch von der **HSRM mitentwickelt** wird (Prof. Nikolay Tcholtchev).

[1] **https://silq.ethz.ch/**

[2] **https://www.qrisp.eu/**

THERE'S NO PLACE LIKE HOME



POST QUANTEN KRYPTOGRAPHIE

. . . LIKE TEARS IN RAIN. TIME TO DIE!

(**Reale**) Quantencomputer haben massive Auswirkungen auf die Kryptographie, Internet, Banking und IT-Sicherheit.

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

Shor's Algorithmus macht **ALLE** gebräuchlichen **asymmetrischen** Verfahren **unbrauchbar**, denn sie basieren auf FACTORING oder (Varianten von) DLOG!

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

SETEC ASTRONOMY - (NO) MORE SECRETS

Idee: Suche **Verfahren für klassische Computer**, die noch **sicher** sind, wenn der **Angreifer** einen **Quantencomputer hat**. Internationaler Wettbewerb (vom NIST organisiert) untersucht(e) fünf Familien:

SETEC ASTRONOMY - (NO) MORE SECRETS

Idee: Suche **Verfahren für klassische Computer**, die noch **sicher** sind, wenn der **Angreifer** einen **Quantencomputer hat**. Internationaler Wettbewerb (vom NIST organisiert) untersucht(e) fünf Familien:

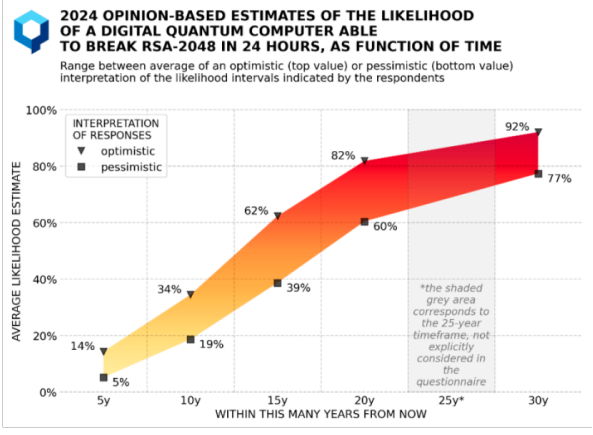
- Verfahren mit Systemen von multivariaten quadratischen Polynomen (vgl. Rainbow)
- **Verfahren mit kryptologischen Hashfunktionen** (vgl. SPHINCS$^+$)
- Kryptographie mit fehlerkorrigierenden Codes (vgl. McEliece-Kryptosystem)
- **Verfahren mit Isogenien zwischen supersingulären elliptische Kurven**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

Deutlich aufwändigere Verfahren! → brauchen Migrationsstrategie und bessere Hardware!

UMSETZUNG

QUANTENCOMPUTER - ENEMY MINE?

Ein Zeitplan ist aktuell nur schwer vorher zu sehen:



https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE.

Sei

- x die benötigte Zeit für die Umstellung auf PQC
- y der Zeitraum in dem Daten beschützt werden müssen
- z der Zeitraum für den Bau eines (starken) Quantencomputers

Mosca's Gesetz: Ist $x + y \geq z$, dann gibt es ein **ernstes** Problem!

[3] **https://magics.cs.hs-rm.de**

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE.

Sei

- x die benötigte Zeit für die Umstellung auf PQC
- y der Zeitraum in dem Daten beschützt werden müssen
- z der Zeitraum für den Bau eines (starken) Quantencomputers

Mosca's Gesetz: Ist $x + y \geq z$, dann gibt es ein **ernstes** Problem!

Persönliche Meinung: Wir haben ein **sehr** ernstes Problem!

[3] **https://magics.cs.hs-rm.de**

DIFFICULT TO SEE. ALWAYS IN MOTION IS THE FUTURE.

Sei

- x die benötigte Zeit für die Umstellung auf PQC
- y der Zeitraum in dem Daten beschützt werden müssen
- z der Zeitraum für den Bau eines (starken) Quantencomputers

Mosca's Gesetz: Ist $x + y \geq z$, dann gibt es ein **ernstes** Problem!

Persönliche Meinung: Wir haben ein **sehr** ernstes Problem!

Das BMFTR fördert die Erforschung von Migrationsthemen mit dem Projekt **PARFAIT** (Prof. Marc Stöttinger) und die HSRM startet **MAgiCS 2026 – Migration and Agility in Cryptographic Systems** auf der Eurocrypt 2026[3].

[3] **https://magics.cs.hs-rm.de**

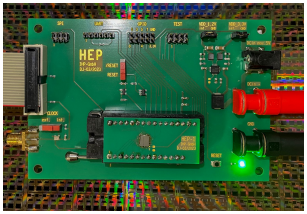
A MARTINI. SHAKEN, NOT STIRRED!

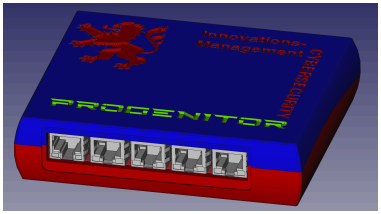
Das HMdI förderte PROGENITOR **Bau eines Open-Source VPN-Routers**. Das BMFTR fördert **DI-Sign-HEP**[4] (**RISC-V basiertes Sicherheitsmodul** (TPM) in 130nm mit Open-Source) und **POST** (Intelligenter Sensor mit PQC für Autos).

[4] **https://hep-alliance.org/**

A MARTINI. SHAKEN, NOT STIRRED!

Das HMdI förderte PROGENITOR **Bau eines Open-Source VPN-Routers**. Das BMFTR fördert **DI-Sign-HEP**[4] (**RISC-V basiertes Sicherheitsmodul** (TPM) in 130nm mit Open-Source) und **POST** (Intelligenter Sensor mit PQC für Autos).

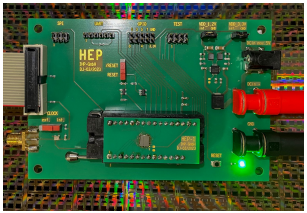


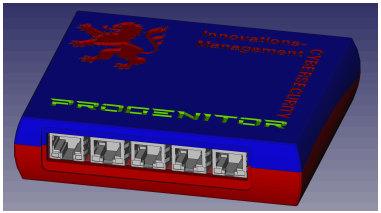


[4] **https://hep-alliance.org/**

A MARTINI. SHAKEN, NOT STIRRED!

Das HMdI förderte PROGENITOR **Bau eines Open-Source VPN-Routers**. Das BMFTR fördert **DI-Sign-HEP**[4] (**RISC-V basiertes Sicherheitsmodul** (TPM) in 130nm mit Open-Source) und **POST** (Intelligenter Sensor mit PQC für Autos).





Vergleich zu **Pentium III**: Launched February 28, 1999, Discontinued April 2004, Feature size 250 nm to 130 nm, Clock 400 MHz to 1.4 GHz

[4] **https://hep-alliance.org/**

FAZIT

THIS IS THE WAY

Takeaway 1

Ohne die vollständige **Kontrolle der Hardware** ist **digitale Souveränität** nicht möglich!

THIS IS THE WAY

Takeaway 1

Ohne die vollständige **Kontrolle der Hardware** ist **digitale Souveränität** nicht möglich!

Takeaway 2

Unterschiedliche Themen & Technologien verwenden die Quantenphysik (Quantencomputing, Quantenkryptografie, Post Quanten Kryptographie).

THIS IS THE WAY

Takeaway 1

Ohne die vollständige **Kontrolle der Hardware** ist **digitale Souveränität** nicht möglich!

Takeaway 2

Unterschiedliche Themen & Technologien verwenden die Quantenphysik (Quantencomputing, Quantenkryptografie, Post Quanten Kryptographie).

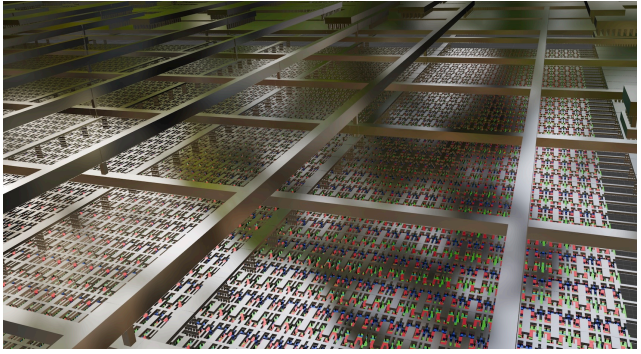
Takeaway 3

Die Entwicklungen rund um Quantencomputer sind schwer voraus zu sehen! Sie brauchen **jetzt(!)** eine **Migrationsstrategie**!

Q AND A

Vielen Dank!

Fragen ∧ Anmerkungen?



steffen.reith@hs-rm.de