(VL vom 22.6.22) 22.8.22

Eigenes „Gesamtbild" CRYPTO1 – Quantencomp. (I)

- Normaler Computer: Bit: 2 Basiszustände: 0 und 1 (sonst nix)
- Quantencomputer: Qubit: 2 Basiszustände $|0\rangle := \binom{1}{0}$ und $|1\rangle := \binom{0}{1} \in \mathbb{C}^2$
  sowie Überlagerung dieser $\Rightarrow$ VR $\mathbb{C}^2$:
  Status Qubit: (= Vektor der Länge 1 in $\mathbb{C}^2$) $\alpha \cdot |0\rangle + \beta \cdot |1\rangle = \binom{\alpha}{\beta}$; $|\alpha|^2 + |\beta|^2 = 1$; $\alpha, \beta \in \mathbb{C}$
  $\Rightarrow$ kann man n. sehen; Messen: $|0\rangle$ mit Wk. $|\alpha|^2$, $|1\rangle$ mit Wk. $|\beta|^2$
  de.wiki: „Qubit ist Zstd. $|0\rangle$ mit Wk. $|\alpha|^2$ u. in $|1\rangle$ Wk. $|\beta|^2$".
  ↳ das könnte auch ein klassischer Computer.

- Nun mehrere Qubits: auch durch VR beschrieben: $\mathbb{C}_2 \otimes \mathbb{C}_2 \otimes \mathbb{C}_2 \otimes \dots$

en.wiki:
> Seien V, W 2 VR über demselben Körper F.
> Das Tensorprodukt $V \otimes W$ ist ein VR mit Basis $\{v \otimes w \mid v \in B_V, w \in B_W\}$.
> Das Tensorprodukt $x \otimes y$ zweier Vektoren $x \in V$, $y \in W$ ist definiert als:
> $x \otimes y := \sum_{b \in B_V} \sum_{c \in B_W} x_b y_c \, b \otimes c$
> Damit ist das Tensorprodukt eine bilineare Abb. $V \times W \to V \otimes W$.

2 Qubits: $\mathbb{C}^2 \otimes \mathbb{C}^2$ mit Basis $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$
bzw. $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
bzw. $|0\rangle, |1\rangle, |2\rangle, |3\rangle$ (kennt Dim. n. mehr)

Schreibe auch: $v \in \bigotimes^n \mathbb{C}^2$ = Zustand & hat Länge 1

3 Qubits: $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ mit Basis $|0\rangle \otimes |0\rangle \otimes |0\rangle, \dots, |1\rangle \otimes |1\rangle \otimes |1\rangle$
$\Rightarrow$ Der VR für n Qubits hat 2^n Dimensionen a. Basis $|0\rangle, \dots, |2^n - 1\rangle$
Man kann leicht nachrechnen, dass sich die Normierung auf 1 auf $\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$ überträgt!

- Nun operiere auf einem solchen System von n Qubits:
  Dies geschieht mit einer $2^n \times 2^n$ Matrix U. (bei Multiplikation)
  *=konjugiert, T=transponiert
  Diese ist unitär, d.h. $U^{*T} = U^{-1}$. Sie erhält damit sowohl Norm als auch Skalarprod.
  siehe auch Wiki: Liste der Quantengatter

Auf 1 Qubit: NOT: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $|0\rangle \mapsto |1\rangle$, $|1\rangle \mapsto |0\rangle$ — q_0 — X — („Pauli-X-Gatter") (Notation VL)

HADAMARD: $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ (Konst. in = gem. gemischten Zstd.) — A — H — A' (Notation de.wiki)

T-Gatter („Phasengatter"): $\begin{pmatrix} 1 & 0 \\ 0 & e^{\pi \cdot i/4} \end{pmatrix}$ — A — T — A'

$|0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $|1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Auf 2 Qubits: CNOT: q_0 — •, q_1 — X — $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ d.h. $|00\rangle \mapsto |00\rangle$, $|10\rangle \mapsto |10\rangle$, $|01\rangle \mapsto |11\rangle$, $|11\rangle \mapsto |01\rangle$ ($q_1 \to q_0$)

Kontrolliertes T-Gatter: q_0 — •, q_1 — T — $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\pi i/4} \end{pmatrix}$ $|11\rangle \mapsto e^{\pi i/4} \cdot |11\rangle$, $|00\rangle \mapsto |00\rangle$, etc...

- **Die Quanten-Fourier-Transformation:** = ein wesentlicher Bestandteil des Shor-Algo
  de.wiki: = eine Zerlegung der diskreten Fourier-Trafo in unitäre Matrizen, sodass als Q.schaltkreis impl.bar
  en.wiki: = Quanten-Analog der diskreten Fourier-Trafo
  $\Rightarrow$ kann effizient auf Q.comp. durchgeführt werden mit $O(n^2)$ (Hadamard-) Gattern (n = # Qubits)
  ↳ die klassische diskrete Fourier-Trafo braucht $O(n \cdot 2^n)$ Gatter, exp. mehr.
  n Qubits, $N = 2^n$, $w_N = e^{(2\pi i)/N}$ (× als Zahlen multipliziert!)
  QFT als Abb. auf Basisvektoren: $|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} w_N^{xy} |y\rangle$
  QFT als Matrix: $\frac{1}{\sqrt{N}} \begin{pmatrix} w_N^{0,0} & w_N^{1,0} & \dots & w_N^{N-1,0} \\ w_N^{0,1} & w_N^{1,1} & \dots & w_N^{N-1,1} \\ \vdots & \vdots & & \vdots \\ w_N^{0,N-1} & w_N^{1,N-1} & \dots & w_N^{N-1,N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{N-1} \\ 1 & w^2 & w^4 & \dots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \dots & w^{(N-1)^2} \end{pmatrix}$ (en.wiki)
  Inverse QFT als Abb.: $|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} w_N^{-yx} |y\rangle$

- **Idee/Intro Shor-Algorithmus:** Sei $a \in_R \mathbb{Z}_{p \cdot q}$ mit $ggT(a, p \cdot q) = 1$.
  Iteriere die Abb. $f_a: \mathbb{Z}_{pq} \to \mathbb{Z}_{pq}$, $x \mapsto ax$: $f_a^k : a \mapsto a^k \cdot x$
  $k = ord(a) \Rightarrow f_a^k = id$ $\to$ ist eine Schwingung mit Basisfrequenz $= ord(a)$
  $\to$ analysiere mit Fourier-Trafo, die Freq.anteile rauszieht
  Ziel = „analysiere Harmonie der Zahl a"
  Habe $a^k \equiv 1 \pmod N$ gefunden $\Rightarrow N \mid (a^k - 1) \Rightarrow N \mid (a^{k/2} - 1)(a^{k/2} + 1) \Rightarrow p = ggT(N, a^{k/2} - 1)$