MOSFET - Metal Oxide Semiconductor Field Effect Transistor
QC - Quantum Computer
RSFQ - Rapid Single Flux Quantum
SET - Single Electron Tunneling

Zum Rechnen $[x, y \in \{0,1\}]$:
$x \,\text{AND}\, y = x \cdot y$,
$x \,\text{OR}\, y = x + y - x \cdot y$,
$\text{NOT}\, x = 1 - x$.

Qubit: beliebiges, quantenmechanisches Zwei-Zustands-System $[\,|0\rangle\,,\ |1\rangle\,]$.

Komplexitätsklassen von Algorithmen: P [polynomial], NP [nichtdeterministisch polynomial], NP-C [NP-vollständig]

QC: Parallelismus durch Superposition mehrer Qubits; Algorithmen mittels unitärer Transformationen U $[UU^\dagger = \mathbb{1}]$.

klassische Informatik:

Zur Verknüpfung von E Eingängen mit jeweils e verschiedenen möglichen Zuständen mit A Ausgängen mit jeweils a verschiedenen möglichen Zuständen ergeben sich $\left[a^A\right]^{\left[e^E\right]}$ paarweise unterschiedliche Möglichkeiten. a^A ist dabei die Anzahl unterschiedlicher Ausgangs- und e^E die Anzahl unterschiedlicher Eingangszustände.

[Für Bits $a = e = 2$.]

Für klassische Gatter muss man Werte kopieren können und braucht NAND-Gatter.
$x \,\text{AND}\, y = [x \,\text{NAND}\, y] \,\text{NAND}[x \,\text{NAND}\, y]$, $x \,\text{OR}\, y = [x \,\text{NAND}\, x] \,\text{NAND}[y \,\text{NAND}\, y]$, $\text{NOT}\, x = x \,\text{NAND}\, x$.

Zur Erstellung eines Algorithmus' aus seinen Funktionswerten:
- Kanonisch disjunktive Normalform (KDNF): Disjunktion von Konjunktionsthermen $[\ \bigvee_i \bigwedge_j (\neg) x_{ij}\ ]$.
- Kanonisch konjunktive Normalform (KKNF): Konjunktion von Disjunktionsthermen $[\ \bigwedge_i \bigvee_j (\neg) x_{ij}\ ]$.

reversible Gatter: eindeutig von Ausgabe auf Eingabe schließbar. [→ injektiv]

Nach Landauers Prinzip setzt jede irreversible Operation [Entropieverringerung] Energie frei [Größenordnung mindestens $k_B T \ln(2)$]. Jede irreversible Funktion kann reversibel gemacht werden $[(\underbrace{x}_{n-\text{bit}}, \underbrace{00\ldots0}_{m-\text{bit}}) \to (\underbrace{x}_{n-\text{bit}}, \underbrace{f(x)}_{m-\text{bit}})]$.

Von den $[2^n]^{2^n}$ unterschiedlichen n- zu n-bit Funktionen sind nur $[2^n]!$ reversibel.

(c) - control-Bit, (t) - target-Bit

CNOT - 2 Bits [1 (c), 1 (t)] und (t) flippt nur, wenn (c) 1 ist.

$[(x, y) \to (x, x \,\text{XOR}\, y)]$

Toffoli-Gatter: C^{2}NOT - 3 Bits [2 (c), 1 (t)] und (t) flippt nur, wenn beide (c) 1 sind.

$[(x, y, z) \to (x, y, [x \,\text{AND}\, y] \,\text{XOR}\, z)]$

Fredkin-Gatter: CEXCHANGE - 3 Bits [1(c), 2 (t)] und (t) tauschen nur, wenn (c) 1 ist.

$[(x, y, z) \to (x, [[\text{NOT}\, x] \,\text{AND}\, y] \,\text{OR}[x \,\text{AND}\, z], [[\text{NOT}\, x] \,\text{AND}\, z] \,\text{OR}[x \,\text{AND}\, y])]$

Quantenmechanik:

wichtigste Begriffe:
Hilbert-Raum $\mathcal{H}_d$, Dimension d, Zustände $|\Psi\rangle$ [ket], $\langle\Psi|$ [bra], Normierung $\langle\Psi\,|\,\Psi\rangle = 1$, orthonormierte Basis [ONB] $\{\,|q\rangle\,\}$ mit $\langle q\,|\,q'\rangle = \delta_{qq'}$ und $\mathcal{H}_d = \text{span}(\{\,|q\rangle\,\})$, Normaloperator Q mit $Q\,|q\rangle = q\,|q\rangle$, hermitescher Operator $H = H^\dagger$, Projektor $P_q = |q\rangle\,\langle q|$, Vollständigkeit $\mathbb{1}_d = \sum_q P_q$, unitärer Operator $U^\dagger = U^{-1}$.

Dynamik eines QM-Systems:
Schrödinger-Gleichung $\mathrm{i}\,\hbar \frac{\partial}{\partial t}\,|\Psi\rangle = H\,|\Psi\rangle$, für $\partial_t H = 0$ und Eigenwerten ε_i von H ist der unitäre Zeitentwicklungsoperator $U = \mathrm{e}^{\frac{1}{\mathrm{i}\hbar} H t}$ und $|\Psi(t)\rangle = U\,|\Psi(0)\rangle$.

Messung:
$Q\,|\Psi\rangle = \sum_q Q P_q\,|\Psi\rangle = \sum_q q \underbrace{\langle q\,|\,\Psi\rangle}_{\alpha_q}\,|q\rangle$ mit der Wahrscheinlichkeit der Messung des Zustandes $|q\rangle$ $|\alpha_q|^2$, Mittelwert $\langle A\rangle = \langle\Psi\,|\,A\,|\,\Psi\rangle = \sum_q q\,|\alpha_q|^2$, Varianz $\langle[A - \langle A\rangle\,]^2\rangle \geq 0$.

Kommutator $[a, b] = ab - ba$; Antikommutator $[a, b]_+ = ab + ba$

1 Qubit-System:

2-Niveau Quantensystem [z.B. Spin-$\frac{1}{2}$-Teilchen], Hilbertraum $\mathcal{H}_2$ mit ONB $\{|0\rangle, |1\rangle\}$.

Matrixdarstellung: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

$\sigma_x \hat{=}$ NOT, Hadamart-Gatter $H = \frac{1}{\sqrt{2}}[\sigma_x + \sigma_z]$

wichtige Operatoren:

elementar: $P_0 = |0\rangle\langle 0| = \begin{pmatrix}1&0\\0&0\end{pmatrix}$, $P_1 = |1\rangle\langle 1| = \begin{pmatrix}0&0\\0&1\end{pmatrix}$, $\sigma_+ = |0\rangle\langle 1| = \begin{pmatrix}0&1\\0&0\end{pmatrix}$, $\sigma_- = |1\rangle\langle 0| = \begin{pmatrix}0&0\\1&0\end{pmatrix}$.

kombiniert: $\mathbb{1} = P_0 + P_1 = \underbrace{\begin{pmatrix}1&0\\0&1\end{pmatrix}}_{\text{copy}}$, $\sigma_x = \sigma_+ + \sigma_- = \underbrace{\begin{pmatrix}0&1\\1&0\end{pmatrix}}_{\text{bit-flip}}$, $\sigma_y = \mathrm{i}[\sigma_- - \sigma_+] = \underbrace{\begin{pmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{pmatrix}}_{\text{bit-flip mit phase-spread}}$, $\sigma_z = P_0 - P_1 = \underbrace{\begin{pmatrix}1&0\\0&-1\end{pmatrix}}_{\text{phase-spread}}$.

Mit dem Spin-Hamiltonian $H_s = -\vec{B}\vec{s} = -\frac{\hbar}{2}B_{\underline{\alpha}}\sigma_{\underline{\alpha}}$ ist dann $U(t) = \mathrm{e}^{\mathrm{i}B_{\underline{\alpha}}\sigma_{\underline{\alpha}}\frac{t}{2}} = \mathbb{1}\cos(B_{\underline{\alpha}}\frac{t}{2}) + \sigma_{\underline{\alpha}}\,\mathrm{i}\sin(B_{\underline{\alpha}}\frac{t}{2})$.

2 Qubit-System:

Zustände aus zwei Hilberträumen $\mathcal{H}^A, \mathcal{H}^B$ mit ONB $\{|\Psi_i^A\rangle\}, \{|\Psi_i^B\rangle\}$ sind separabel, falls $|\Psi_{AB}\rangle$ als Produktzustand $|\Psi_{AB}\rangle = \sum_{i,j}[\alpha_i|\Psi_i^A\rangle] \oplus [\beta_j|\Psi_j^B\rangle]$ darstellbar ist. Sonst heißt der Zustand verschränkt.

Bei separablen Systemen gilt $\langle M\rangle = \mathrm{tr}(M\rho)$ mit dem Dichteoperator $\rho = |\Psi\rangle\langle\Psi|$; dabei ist ρ positiv [hermitesch, $\langle\varphi|\rho|\varphi\rangle \geq 0$], $\mathrm{tr}(\rho) = 1$, $\rho^2 = \rho$

$\rho^2 \begin{cases} = \rho & \text{, reiner Zustand} \\ \neq \rho & \text{, verschränkter Zustand} \end{cases}$

Bei verschränkten Systemen ist ρ positiv [also hermitesch], $\mathrm{tr}(\rho) = 1$ aber $\rho^2 \neq \rho$ und $\mathrm{tr}(\rho^2) \leq 1$.

Konkurrenz:
Für $|\chi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ [normiert auf 1] definiert man $C = 2|\alpha\delta - \beta\gamma|$. Es ist $0 \leq C \leq 1$ und für separable Zustände $C = 0$ und für „maximal verschränkte“ Zustände $C = 1$.

Bell-Zustände:
$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle]$
$|\psi_\pm\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$

Blochkugel:

Bloch-Vektor $\vec{P} \in \mathbb{R}^3$ für ein 1-Qubit-System; es ist $|\vec{P}| \leq 1$; Dichteop. $\rho = \frac{1}{2}[\mathbb{1} + \vec{P}\vec{\sigma}]$.

Die EW von $\rho|\pm\rangle = \lambda|\pm\rangle$ sind $\lambda_\pm = \frac{1}{2}[1 \pm |\vec{P}|]$.

Für einen *reinen* Zustand ist $\vec{P} = \begin{pmatrix}\sin(\theta)\cos(\varphi)\\\sin(\theta)\sin(\varphi)\\\cos(\theta)\end{pmatrix}$, $|\vec{P}| = 1$ und die Eigenwerte und Eigenvektoren sind $[\rho|\pm\rangle = \mu_\pm|\pm\rangle]$:

$$\mu_+ = 1,\ |+\rangle = \begin{pmatrix}\cos(\frac{\theta}{2})\,\mathrm{e}^{-\mathrm{i}\frac{\varphi}{2}}\\\sin(\frac{\theta}{2})\,\mathrm{e}^{\mathrm{i}\frac{\varphi}{2}}\end{pmatrix} \quad \text{bzw.} \quad \mu_- = -1,\ |-\rangle = \begin{pmatrix}-\sin(\frac{\theta}{2})\,\mathrm{e}^{-\mathrm{i}\frac{\varphi}{2}}\\\cos(\frac{\theta}{2})\,\mathrm{e}^{\mathrm{i}\frac{\varphi}{2}}\end{pmatrix}$$

Bei maximaler Verschränkung [für alle Bell-Zustände] ist $\rho_A = \mathrm{tr}_B(|\Psi\rangle\langle\Psi|) = \frac{1}{2}\mathbb{1} = \rho_B$.

Reinheit: $\eta = 2\,\mathrm{tr}(\rho^2) - 1 = |\vec{P}|^2 \begin{cases} = 0 & \text{, maximal gemischter Z.} \\ = 1 & \text{, reiner/separabler Z.} \end{cases}$ $\Rightarrow C = 1 - \eta$.

[Beim Übergang $\vec{P} \to -\vec{P}$ gehen auch die EV gemäß $|\pm\rangle \to |\mp\rangle$ über.]

Zustände auf der Oberfläche der Blochkugel sind rein, Zustände im Innern verchränkt. Zustände im Ursprung sind maximal verschränkt.

Paritätsoperator: $\sigma_{A_z}\sigma_{B_z}$ $[\sigma_{A_z}\sigma_{B_z}|\Phi_\pm\rangle = |\Phi_\pm\rangle,\ \sigma_{A_z}\sigma_{B_z}|\Psi_\pm\rangle = -|\Psi_\pm\rangle]$

Vorzeichenoperator: $\sigma_{A_x}\sigma_{B_x}$ $[\sigma_{A_x}\sigma_{B_x}|\Phi_\pm\rangle = \pm|\Phi_\pm\rangle,\ \sigma_{A_x}\sigma_{B_x}|\Psi_\pm\rangle = \pm|\Psi_\pm\rangle]$

$\sigma_j\sigma_k = \delta_{jk}\mathbb{1} + \mathrm{i}\varepsilon_{jkl}\sigma_l$, $[\sigma_j, \sigma_k] = 2\,\mathrm{i}\varepsilon_{jkl}\sigma_l$, $\cos(x) = \sum_{k=0}^{\infty}[-1]^k\frac{x^{2k}}{[2k]!}$, $\sin(x) = \sum_{k=0}^{\infty}[-1]^k\frac{x^{2k+1}}{[2k+1]!}$, $\mathrm{tr}(ab) = \mathrm{tr}(ba)$.

Bellsche Ungleichung:

Es sei $[|\vec{n}| = |\vec{m}| = 1]$ $P(\vec{n},\pm) = \frac{1}{2}[1 \pm \vec{n}\vec{\sigma}]$ und $|\Psi_-\rangle$ der entsprechende Bell-Zustand. Dann ist $\langle\Psi_-|\,\vec{n}\vec{\sigma}\,|\Psi_-\rangle = 0$, $\sigma_B|\Psi_-\rangle = -\sigma_A|\Psi_-\rangle$ und $\langle\Psi_-|\,P_A(\vec{n},+)P_B(\vec{m},+)\,|\Psi_-\rangle = \frac{1}{4}[1-\vec{n}\vec{m}]$. [Es ist $P(\vec{n},+) = P(-\vec{n},-)$!]

Wählt man als Messachsen $\vec{n}_1 = \begin{pmatrix}0\\0\\1\end{pmatrix} = -m_1$, $\vec{n}_2 = \begin{pmatrix}\frac{\sqrt{3}}{2}\\0\\-\frac{1}{2}\end{pmatrix} = -m_2$ und $\vec{n}_3 = \begin{pmatrix}-\frac{\sqrt{3}}{2}\\0\\-\frac{1}{2}\end{pmatrix} = -m_3$ und bestimmt die Wahrscheinlichkeit der gleichzeitigen Messung in 2 Achsen $p(i,j) = \langle\Psi_-|\,P_A(\vec{n}_i,+)P_A(\vec{m}_j,-)\,|\Psi_-\rangle + \langle\Psi_-|\,P_A(\vec{n}_i,-)P_A(\vec{m}_j,+)\,|\Psi_-\rangle$, so sieht man, dass $p(1,2)+p(2,3)+p(3,1) = \frac{3}{4}$ [?] .
Klassisch wäre $p(1,2)+p(2,3)+p(3,1) = 2$ [?]; mit Experiment jedoch ersteres bestätigt!

No-Cloning Theorem:

Kopierbare Zustände sind identisch oder orthogonal.

$$[|\Phi\rangle, |\Psi\rangle \in \mathcal{H},\ \forall|\Phi\rangle : U|\Phi,z\rangle = |\Phi,\Phi\rangle \Rightarrow \langle\Phi|\Psi\rangle = \langle\Phi,z|\Psi,z\rangle = \langle\Phi,z|U^\dagger U|\Psi,z\rangle = \langle\Phi,\Phi|\Psi,\Psi\rangle = [\langle\Phi|\Psi\rangle]^2 \in \{0,1\}]$$

Mehr-qubit-Operationen:

$\frac{\pi}{8}$-Gatter: $T = e^{i\frac{\pi}{8}[\mathbb{1}-\sigma_z]} = e^{i\frac{\pi}{8}}\begin{pmatrix}e^{-i\frac{\pi}{8}} & 0\\ 0 & e^{i\frac{\pi}{8}}\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix}$, unitär $[U^\dagger = U^{-1}]$.

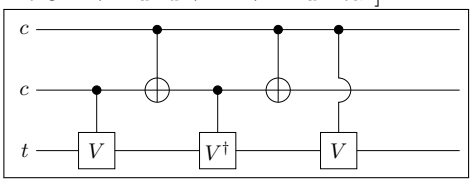
Allgemeine Rotation um eine Achse in Richtung $\vec{n}$ um den Winkel θ: $R_{\vec{n}}(\theta) = e^{i\theta\vec{n}\vec{\sigma}}$. [unitär]

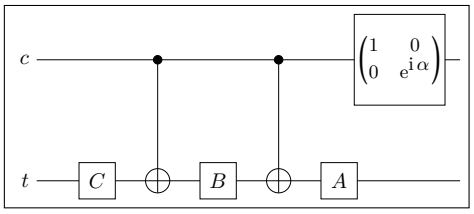
Blochvektor $\vec{P} = \langle\Psi|\,\vec{\sigma}\,|\Psi\rangle$, reiner Zustand auf Blochsphäre $|+,\theta,\varphi\rangle = \begin{pmatrix}e^{-i\frac{\varphi}{2}}\cos(\frac{\theta}{2})\\ e^{i\frac{\varphi}{2}}\sin(\frac{\theta}{2})\end{pmatrix}$ mit $\vec{P} = \begin{pmatrix}\sin(\theta)\cos(\varphi)\\ \sin(\theta)\sin(\varphi)\\ \cos(\theta)\end{pmatrix}$.

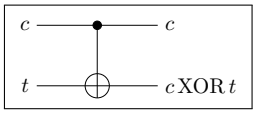
Allgemeine unitäre Matrix: $U = e^{i\alpha}R_{\vec{e}_z}(\beta)R_{\vec{e}_y}(\gamma)R_{\vec{e}_z}(\delta)$;
durch Berücksichtigung der Phase entspricht eine Drehung um φ auf der Blochkugel 2φ im Realraum.

Mit $A = R_{\vec{e}_z}(\beta)R_{\vec{e}_y}(\frac{\gamma}{2})$, $B = R_{\vec{e}_y}(-\frac{\gamma}{2})R_{\vec{e}_z}(-\frac{\delta}{2}-\frac{\beta}{2})$, $C = R_{\vec{e}_z}(\frac{\delta}{2}-\frac{\beta}{2})$ ist $U = e^{i\alpha}A\sigma_xB\sigma_xC$ und $ABC = \mathbb{1}$.

Oder z.B. C^2U [mit $U = V^2$ und $V^\dagger = V^{-1}$ unitär]:







Matrixexponential:

Sei $X \in \mathbb{C}^{n\times n}$, dann ist das Exponential von X $e^X = \sum_{k=0}^{\infty}\frac{X^k}{k!}$.

Dabei gilt $[a,b \in \mathbb{R}]$: $e^{0_{n\times n}} = 1_{n\times n}$, $e^{aX}e^{bX} = e^{[a+b]X}$, $\left[e^X\right]^T = e^{X^T}$, $\left[e^X\right]^* = e^{X^*}$, $\det\left(e^X\right) = e^{\mathrm{tr}\,(X)}$ und falls $[X,Y] = 0$ gilt $e^{X+Y} = e^Xe^Y$ [sonst Baker-Campbell-Hausdorff-Formel].

Mit den Pauli-Matrizen σ_1, σ_2, σ_3 $[\vec{\sigma} = (\sigma_x,\sigma_y,\sigma_z)^T]$, mit $\sigma_0 = \mathbb{1}$, $\vec{n} \in \mathbb{R}^3$ $[|\vec{n}| = 1]$ und $a \in \mathbb{C}$ gilt somit:

$$e^{ia\vec{n}\vec{\sigma}} = \sum_{k=0}^{\infty}\frac{[ia\vec{n}\vec{\sigma}]^k}{k!} = \sum_{n=0}^{\infty}\left[\frac{[ia\vec{n}\vec{\sigma}]^{2n}}{[2n]!} + \frac{[ia\vec{n}\vec{\sigma}]^{2n+1}}{[2n+1]!}\right] = \mathbb{1}\sum_{n=0}^{\infty}[-1]^n\frac{a^{2n}}{[2n]!} + i\vec{n}\vec{\sigma}\sum_{n=0}^{\infty}[-1]^n\frac{a^{2n+1}}{[2n+1]!} = \cos(a)\mathbb{1} + i\sin(a)\vec{n}\vec{\sigma}$$

Universeller Satz von Quantengattern:

Jede unitäre Transformation kann auf folgende Quantengatter zurückgeführt werden: CNOT, $\frac{\pi}{8}$-Gatter, Hadamard-G.

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T = e^{i\frac{\pi}{8}[\mathbb{1} - \sigma_z]} = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}}[\sigma_x + \sigma_z] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Denn:

1. Jede unitäre Operation kann exakt als Produkt „einfacher“ unitärer Operationen dargestellt werden, die jeweils nur auf die Basiszustände des Hilbertraumes wirken.
2. Irgendein unitärer 2-Niveau-Operator kann durch Einzel-Qubit- und verallgemeinerte CNOT-Gatter ausgeführt werden.
3. Einzelqubitoperationen können mit beliebiger Genauigkeit durch H und T approximiert werdem.

Quantencomputer und -algorithmen

5 natürliche Grundsätze [nach DiVincenco, 2001]:

1. Wohldefinierte Qubits nötig. System skalierbar.
2. Initialisierung eines wohldefinierten Anfangszustands.
3. Lange Dekohärenzzeit des Gesamtsystems.
4. Universeller Satz von Quantengattern.
5. Qubit-selektives Auslesen.

Deutsch-Algorithmus:

Initialisieren $|01\rangle$ und nutzen U_f $[U_f|x,y\rangle = |x, y \oplus f(x)\rangle]$, dann ist

$$|\Psi\rangle = H_x U_f H_x H_y |01\rangle = \frac{1}{\sqrt{2}} |f(0) \oplus f(1)\rangle \otimes [\,|f(0)\rangle - |1 \oplus f(0)\rangle\,]$$

und somit mit $\langle 0|$ unterscheidbar, ob $f(x) = const.$ $[|\Psi\rangle = |0\rangle \otimes \ldots]$ oder balanciert $[|\Psi\rangle = |1\rangle \otimes \ldots]$.

Deutsch-Josza-Algorithmus:

Verallgemeinerung des Deutsch-Algorithmus auf n Dimensionen $[f(\vec{x})$, wobei $f : \mathbb{B}^d \to \mathbb{B}^1$ mit $\mathbb{B} = 0, 1]$, wobei $H_{\vec{x}} = \prod_{i=1}^{n} H_i$:

$$|\Psi\rangle = H_{\vec{x}} U_f H_{\vec{x}} H_y |\vec{0}, 1\rangle$$

und dann mit $\langle\vec{0}|\ f(\vec{x}) = const.$ $[[\langle\vec{0}| \otimes \frac{1}{\sqrt{2}}[\langle 0| - \langle 1|]]|\Psi\rangle = \pm 1]$ und $f(\vec{x})$ balanciert $[[\langle\vec{0}| \otimes \frac{1}{\sqrt{2}}[\langle 0| - \langle 1|]]|\Psi\rangle = 0]$ unterscheidbar.

Quantenfouriertransformation ist mit $\mathcal{O}(n^2)$ wesentlich schneller als die klassische diskrete FT mit $\mathcal{O}(2^n n)$.

RSA-Verschlüsselung wäre mit Quantencomputern wesentlich schneller zu knacken [→ Shor-Algorithmus].

Grover-Suchalgorithmus:

Zur Suche in unstrukturierter Datenbank [$N = 2^n$ Elemente, M Suchlösungen] mit Orakelfunktion $f(x) = \begin{cases} 1 & , x \text{ Lösung} \\ 0 & , \text{sonst} \end{cases}$
$[U_f|x,y\rangle = |x, y \oplus f(x)\rangle]$, $H_x = \prod_{i=1}^{n} H_i$ und $|q_0\rangle = \frac{1}{\sqrt{2}}[\,|0\rangle - |1\rangle\,] = H|1\rangle$:

Es gilt $U_f|x, q_0\rangle = [-1]^{f(x)}|x, q_0\rangle$.

Initialisierung des Systems zu

$$|\Psi\rangle = [H_x \otimes \mathbb{1}_1][\,|\vec{0}\rangle \otimes |q_0\rangle\,] = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x\rangle \otimes |q_0\rangle = \Big[\underbrace{\sqrt{\frac{N-M}{N}}}_{=:\cos(\frac{\theta}{2})} \underbrace{\frac{1}{\sqrt{N-M}} \sum_{x=0}^{N-1} [1-f(x)]\,|x\rangle}_{\text{ungesuchter Anteil} =:|\alpha\rangle} + \underbrace{\sqrt{\frac{M}{N}}}_{=:\sin(\frac{\theta}{2})} \underbrace{\frac{1}{\sqrt{M}} \sum_{x=0}^{N-1} f(x)\,|x\rangle}_{\text{gesuchter Anteil} =:|\beta\rangle} \Big] \otimes |q_0\rangle$$

$$= \Big[\underbrace{\cos(\tfrac{\theta}{2})\,|\alpha\rangle + \sin(\tfrac{\theta}{2})\,|\beta\rangle}_{=:|\Phi\rangle} \Big] \otimes |q_0\rangle$$

$$[\Rightarrow \theta = 2\arcsin(\sqrt{\tfrac{M}{N}}) \approx 2\sqrt{\tfrac{M}{N}}]$$

Mit dem Graver-Operator $G = [[H_x[-\mathbb{1} + 2\,|0\rangle\,\langle 0\,|\,]H_x] \otimes \mathbb{1}_1]U_f = [[2\,|\Phi\rangle\,\langle\Phi\,| - \mathbb{1}] \otimes \mathbb{1}_1]U_f$

$= [[\,|\Phi\rangle\,\langle\Phi\,| - [\mathbb{1}_n - |\Phi\rangle\,\langle\Phi\,|\,]] \otimes \mathbb{1}_1]U_f = [[P_{|\Phi\rangle} - P_{|\Phi\rangle^\perp}] \otimes \mathbb{1}_1]U_f$

sieht man nach k-facher Anwendung auf $|\Psi\rangle$ dann $|\Psi_k\rangle = G^k\,|\Psi\rangle = \big[\,\cos(\frac{2k+1}{2}\theta)\,|\alpha\rangle + \sin(\frac{2k+1}{2}\theta)\,|\beta\rangle\,\big] \otimes |q_0\rangle$.

Da bei $\frac{2k+1}{2}\theta = \frac{\pi}{2}$ einzig der gesuchte Teil überbleibt $[\,|\Psi_{k'}\rangle = |\beta\rangle \otimes |q_0\rangle\,]$, ergibt sich für $M \ll N$: $k' \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}$. $[\Rightarrow \mathcal{O}(2^{\frac{n}{2}})]$

Die Fehlerwahrscheinlichkeit beträgt $p = \cos^2(\frac{2k'+1}{2}\theta) \approx \frac{M}{N} \ll 1$ für $M \ll N$.