Leidsche Flesch lunchlezing, 10 febr. 2016. 1.

Bas Edixhoven.

<u>Wat kunnen quantumcomputers</u>?

Kijk eens hier: www.onderzoeksgebieden.leidenuniv.nl/de-kwantumcomputer

Kortste route? Langs alle steden ("TSP" handelsreizigersprobleem) of van zeg A naar B? Voor het eerste is geen polynomiale tijd algoritme voor quantumcomputers bekend (TSP is NP-hard). Voor het tweede hebben we Dijkstra's kortstepad algoritme, polynomiale tijd. Eigenlijk is bijna alles wat onder "Barrière voor de klassieke computer" staat onzin.

Onder "Kraken van geheimschriften": ja het is waar dat RSA te breken is voor quantumcomputers (wel met een paar duizend qubits dan, voor sleutels van zeg 1000 bits). Maar zie ook op wikipedia de pagina "post-quantum cryptography". Daar staan wel 6 alternatieve methoden voor cryptografie met klassieke computers ~~[illegible]~~ die voor zover bekend en ook voor zover verwacht niet door quantumcomputers te kraken zijn.

Wat doet een quantumcomputer?
Voor details, zie http://homepages.cwi.nl/~rdewolf/qcnotes.pdf
Ik zal proberen de belangrijkste ideeën uit te leggen.

Klassieke computer	Quantumcomputer
toestandsruimte één bit: $\{0,1\}$	één qubit: $\{f : \{0,1\} \to \mathbb{C} : \underbrace{\lVert f \rVert_2}_{= \sqrt{\lvert f(0)\rvert^2 + \lvert f(1)\rvert^2}} = 1\}$ $f \leftrightarrow f(0)\cdot\lvert 0\rangle + f(1)\cdot\lvert 1\rangle$, $\lvert 0\rangle, \lvert 1\rangle$ orthon.
n bits: $\{0,1\}^n = \{0,1,\ldots,2^n-1\}$	n qubits: $\{f : \{0,1,\ldots,2^n-1\} \to \mathbb{C} : \lVert f \rVert_2 = 1\}$. basis. $f \leftrightarrow f(0)\cdot\lvert 0\rangle + f(1)\cdot\lvert 1\rangle + \cdots + f(2^n-1)\cdot\lvert 2^n-1\rangle$
uitlezen: je ziet de enen en nullen die er staan	je vindt $a \in \{0,1,\ldots,2^n-1\}$ met kans $\lvert f(a)\rvert^2$, en dan is de toestand die $\lvert a\rangle$.
rekenen: $\wedge, \vee, \neg$ poorten	unitaire lin. transformaties $f \mapsto U(f)$, dus met $\lVert U(f)\rVert_2 = \lVert f \rVert_2$. maak elementaire quantumpoorten waarmee je snel die U mee kan benaderen.

Shor's factorisatie algoritme. Laat $m \in \mathbb{N}$, oneven, deelbaar door tenminste 2 verschillende priemgetallen. Neem n zodat $2^n/m$ groot genoeg.
Kies ~~[illegible]~~ $a \in \{1,\ldots,m-1\}$ random.
Laat $g : \{0,1,\ldots,2^n-1\} \to \{0,1,\ldots,2^n-1\} : x \mapsto a^x \bmod m$
Zet je 2n qubit register in toestand $2^{-n} \cdot \sum_{0 \le x < 2^n} \lvert x\rangle \lvert 0^n\rangle \xrightarrow{\text{unitair}}$

$$2^{-n} \cdot \sum_{x} \lvert x\rangle \lvert g(x)\rangle \longrightarrow \text{de periode } p \text{ vang} \xrightarrow{\text{elem. getaltheorie}} m = m_1 \cdot m_2 .$$

meet 2-e deel, doe FT op 1e deel

meten 2e deel: $\sqrt{2^{-n} \cdot p} \sum_{x : g(x) = a} \lvert x\rangle \xmapsto{FT}$ piek bij p.

Dat is de truuk: periodiciteit vinden is zo ongeveer het enige dat de quantumcomputer echt goed kan (en quantumsystemen simuleren, ~~deze~~ ook).

Lattice based crypto: Zie wikipedia "Lattice reduction" en bijvoorbeeld: www.latticechallenge.org/svp-challenge/