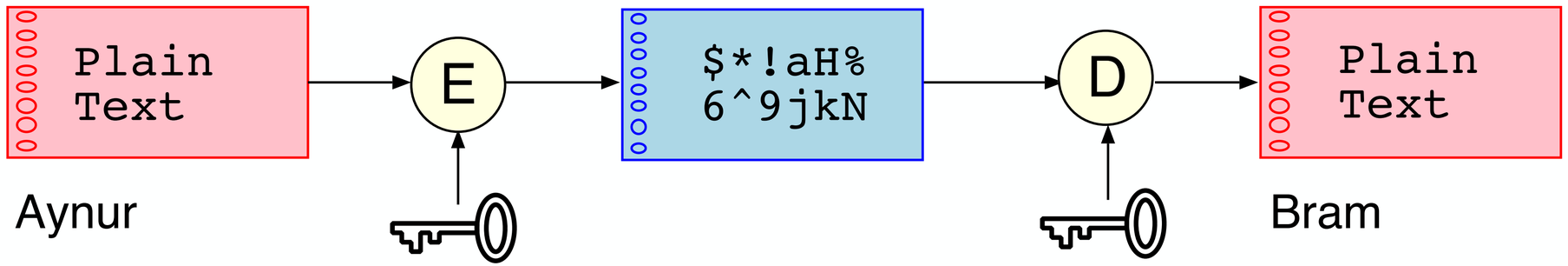
Symmetrische versleuteling

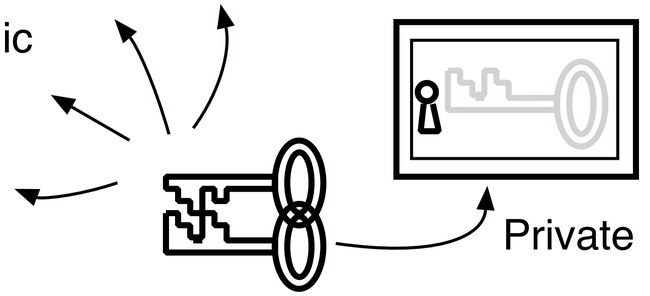
- Zender en ontvanger spreken met elkaar één geheime sleutel af.

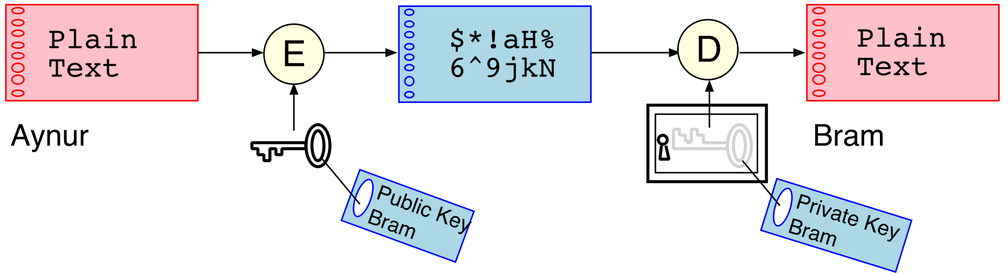


- Bekendste: Rijndael/AES256
- Snel maar probleem: distributie van de sleutels
- Sleutellengte van minstens 512 bits vereist
- Bijvoorbeeld: 7zip, GPG

Asymmetrische versleuteling

- Public key encryptie *gebaseerd op grote priemgetallen*
  - RSA, Diffie-Hellman, ...
  - Relatief langzaam
  - Sleuteluitwisseling is geen probleem:
    - public key mag iedereen weten
  - Wat is versleuteld met de public key kan alleen worden ontcijfert met de private (secret) key
  - Gebruikt in TLS (HTTPS)





Probleem

- Asymetrische versleuteling steunt op vermenigvuldiging van grote priemgetallen: p1 * p2
- Zelfs supercomputers doen miljoenen jaren om het product daarvan te ontleden in p1 en p2
- New kid on the block: Quantum Computers
  - Uren in plaats van miljoenen jaren
  - Groot risico voor HTTPS (TLS)!

KWANTUM mechanica in 5 minuten

- Gaat over gedrag van deeltjes zo klein als een elektron en kleiner
- Bij observeren van zulke deeltjes:
  - Je kunt meten waar ze zijn maar dan kun je hun snelheid niet meten…..
  - …..of je meet hun snelheid maar dan weet je niet waar ze zijn…..
  - Ze kunnen in 2 toestanden bestaan:
    - elektron: draait linksom of rechtsom
    - foton: staande of liggende polarisatie
    - en nog meer deeltjes: bosonen, …
  - In “paren” kun je bij één de toestand meten, dan weet je zonder te meten ook de toestand van de ander
  - Je kunt er mee rekenen met met golfwiskunde maar ook met deeltjeswiskunde
  - Als je uitzoomt naar “onze” wereld (atomen, tennisballen en planeten) *lijken* deze rare eigenschappen verdwenen

“superposition”

“entanglement”

KWANTUM mechanica in 5 minuten

Mocht je het niet snappen, je bent in goed gezelschap.

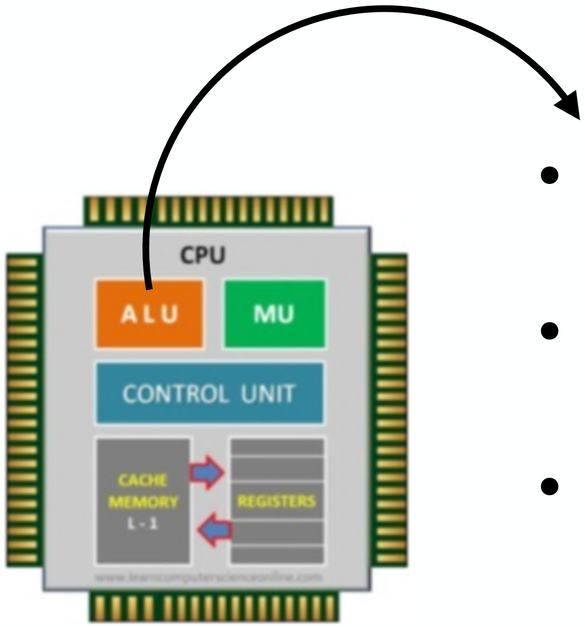
Quotes van de grondlegger van Quantum Mechanics, Niels Bohr:

“Those who are not shocked when they first come across quantum theory cannot possibly have understood it.”

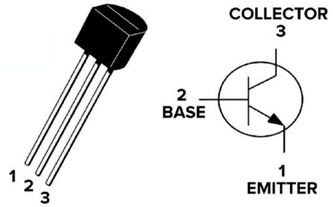
Student: ‘Professor, I do not understand your Quantum Mathematics.’
Bohr: ‘Son, you can not *understand* it. You only can *get used* to it.’

KWANTUM

Normale computer



- De Arithmetic Logic Unit (ALU) is het rekenregister
- Bij moderne CPU’s is de ALU 64 bits
- Elk bit is 0 óf 1
- Een bit wordt opgeslagen in een transistor*

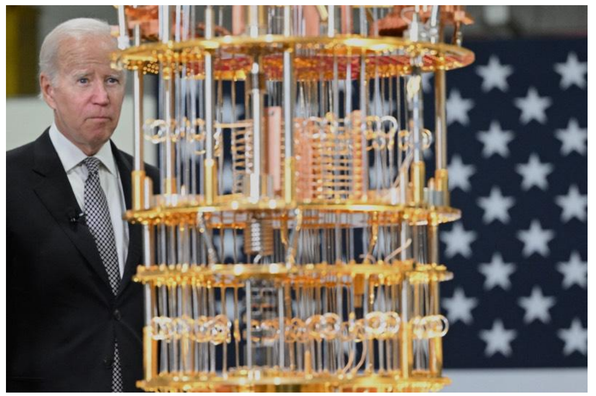


* Vanwege error correcties eigenlijk 6 transistoren per bit

KWANTUM

Quantum Computer

- Het rekenregister (ALU) van een Quantum Computer bevat (anno 2023) 50 qubits
  - elke qubit is 0 én 1 *tegelijkertijd* (door die rare quantum eigenschappen) en pas bij uitlezen wordt de waarde bepaald
  - een qubit bestaat uit 2 quantum-deeltjes in superpositie in een extreem super gekoeld containertje
    - een quantum computer is lomp groot en duur
    - met 50 qubits kun je geen echte problemen oplossen



ALU van 50 qubits

KWANTUM

Quantum Computer

- Niet geschikt voor gewoon rekenwerk, daar zijn gewone computers sneller en goedkoper voor
- Wel geschikt voor wiskundige bewerkingen op matrix-achtige patronen:
  - bewerk het complete patroon in de qubits in één stap — Met Quantum Comp.
    - bevalt de uitkomst: ga verder met gewoon rekenen — Met gewone PC
    - bevalt de uitkomst niet: laadt qubits met nieuw patroon — Met gewone PC
  - Geschikt voor priemgetallen kraken, chemische berekeningen, AI(?)

KWANTUM

Voorbeeld: priemgetallen

- Makkelijk: 2 priemgetallen vermenigvuldigen:
  - 3 x 5 = 15
- Moeilijk: groot getal ontleden in priemgetallen:
  - 85952123 = 9733 * 8831
  - 32317006071311007300714876688669951960444102669715484032130345427524655138867890
    89319720141152291346368871796092189801949411955915049092109508815238644828312063
    08773673009960917501977503896521067960576383840675682767922186426197561618380943
    38476170470581645852036305042887575891541065808607552399123930385521914333389668
    34242068497478656456949485617603532632205807780565933102619270846031415025859286
    41771167259436037184618573575983511523016459044036976132332872312271256847108202
    09725157101726931323469678542580656697935045997268352998638215525166389647960126
    93924980662544070068581946958993838435695183356821818866 3

4096 bits getal

bereken: priem1 en priem2

kost een supercomputer een miljoen jaar

KWANTUM

Shor’s algoritme

https://www.youtube.com/watch?v=-UrdExQW0cs

- Shor bedacht een algoritme (speciaal voor quantum computer) in 7 stappen om groot getal te ontleden in p1 en p2:
  - Stap 1-3: kan gedaan worden met gewone PC,
  - Stap 4: gebruik getal om repeterende patronen te genereren
    - dit is een lus die triljarden keren moet wordt uitgevoerd op een gewone computer
      - bij een quantum computer bestaan alle patronen tegelijkertijd
  - Stap 5-7: kan weer op gewone PC, p1 en p2 zijn nu bekend

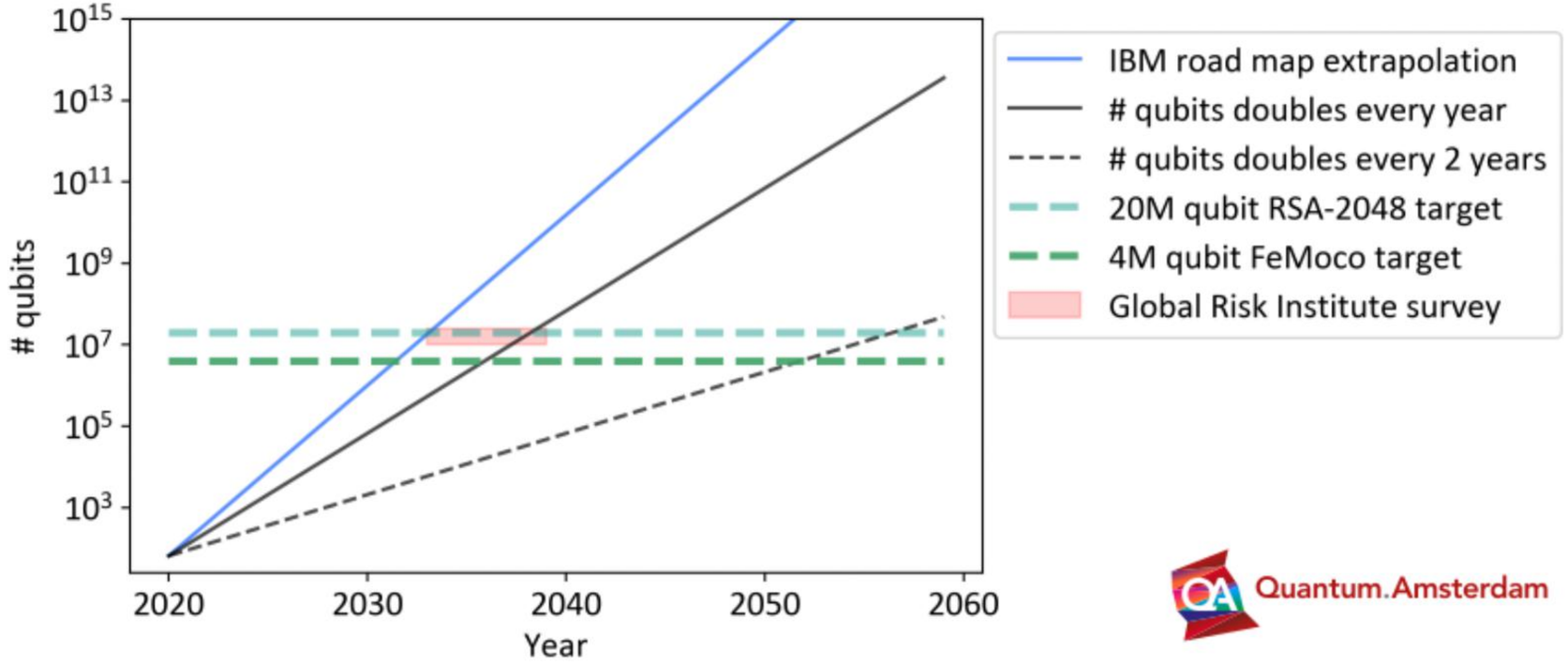
Met gewone computer miljoen jaar

Met quantum computer van 20.000 qubits kwestie van uren

KWANTUM

Probleempje

- Op dit moment zitten we pas op ca. 50 qubits i.p.v. 20.000 qubits
- Elke qubit heeft 1000 extra qubits nodig voor error correctie



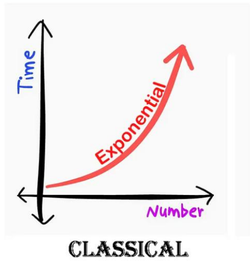
Quantum.Amsterdam

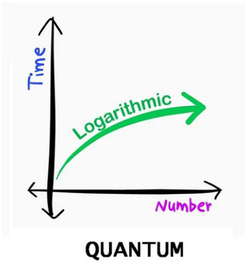
- Pas ergens tussen 2030 en 2040 wordt kraken 2048 RSA key mogelijk

KWANTUM

Oplossingen

- Grotere sleutels: 4096 bits?
  - helaas: dan na 4 á 5 jaar alsnog gekraakt: qubits werken logaritmisch in de tijd





- Symmetrische versleuteling is quantum proof!
- Post Quantum Crypto: ongevoelig voor quantum aanvallen
  - NIST heeft 4 PQC algoritmes vrijgegeven, binnenkort nog 4
    - TLS 1.3 proposed standard krijgt PQC support
    - moet nog wel geïmplementeerd worden: *industrie is aan zet*

KWANTUM

Store now - Decrypt later

- Tot 2030/2040 kan een hacker dus niets met een afgeluisterde TLS-sessie.
- Het aanpassen van apparatuur en software zal jaren kosten.
- Overheden slaan nu al op enorme schaal afgeluisterd netwerkverkeer op om het in de toekomst alsnog te kunnen ontsleutelen.
  - “Store now, decrypt later”.
- Dat is voor gegevens die lang geheim moeten blijven dus een probleem:
  - Bijvoorbeeld medische gegevens met een lange archiveringsverplichting.

KWANTUM

AIVD Handleiding

- De AIVD heeft een handleiding uitgegeven met tevens een migratie-leidraad voor drie soorten organisaties:
  - Reguliere adopters
    - Deze hoeven nog niet in actie te komen.
  - Urgente adopters
    - Deze dienen nu al in actie te komen (wegens store now decrypt later risico voor langdurig te beschermen gegevens).
  - Cryptografie-experts
    - Deze dienen nu al in actie te komen om de PQC implementies te realiseren.