Quantum Computers en Cryptografie

Sebastian R. Verschoor

Instituut voor Informatica (IvI), Universiteit van Amsterdam

QuSoft

Gastcollege—Privacy Seminars
AI & Cybersecurity

2026-03-16

UvA

QuSoft
Research Center for Quantum Software

Waarschuwing

In deze presentatie heb ik veel versimpeld.

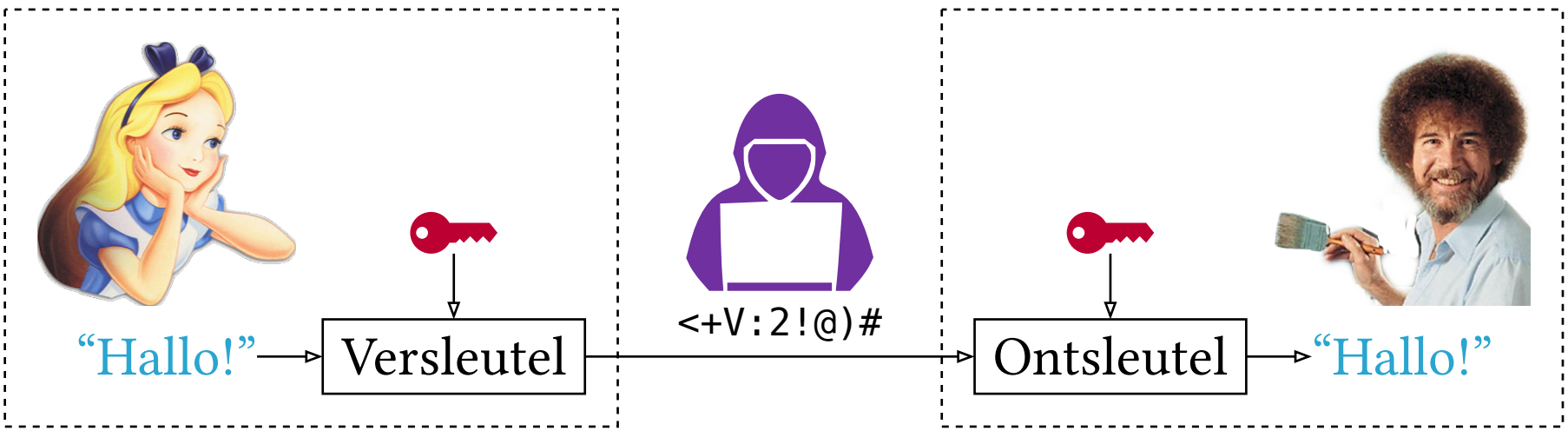
Verifieer altijd details met behulp van andere bronnen, zeker als het om veiligheid gaat.

1. Cryptografie
2. Quantum Informatie
3. Quantum Computers
4. Post-Quantum Cryptografie
5. Quantum Cryptografie

Cryptografie is overal

Symmetrische versleuteling

Alice en Bob delen een geheime **sleutel**



leert niets over het bericht

Bijvoorbeeld: AES, ChaCha20, one-time pad

One-time pad

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

$$\begin{array}{rr} m = & 0100\ 0111 \\ k = & 1000\ 1101 \quad \oplus \\ \hline c = & 1100\ 1010 \end{array} \qquad \begin{array}{rr} c = & 1100\ 1010 \\ k = & 1000\ 1101 \quad \oplus \\ \hline m = & 0100\ 0111 \end{array}$$

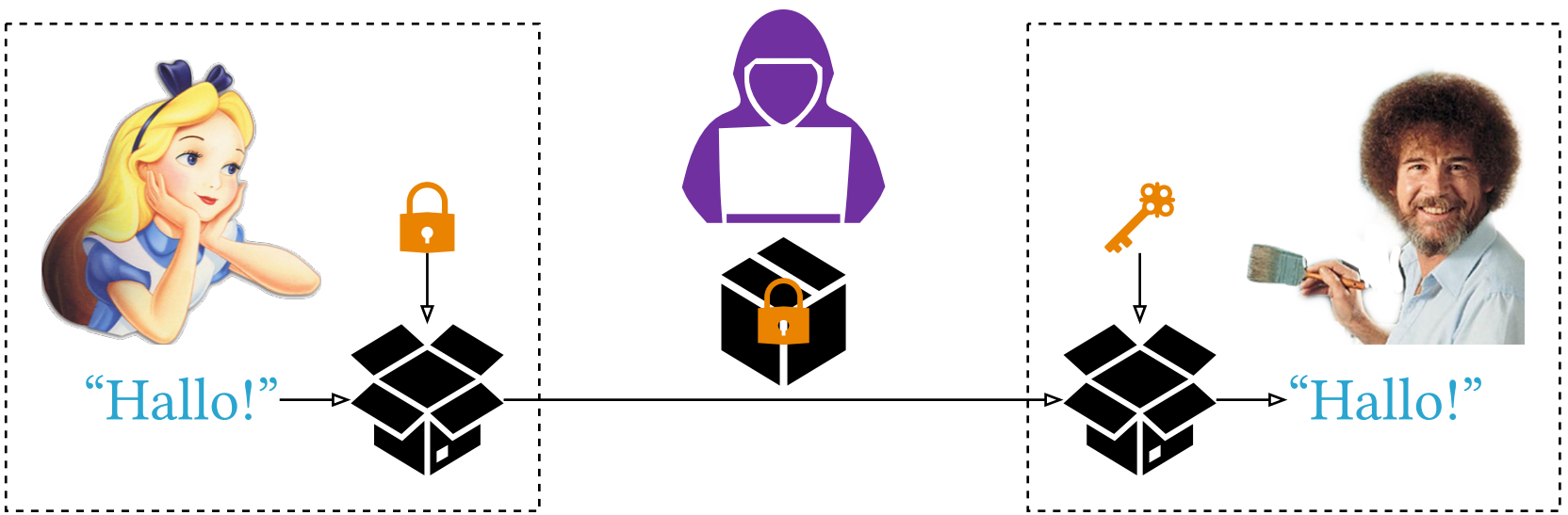
m: message (plaintext) c: ciphertext k: key

 ziet c, maar dit zegt niets over m.

Bewijs: voor elke mogelijke m' is er een k' zodat $c = m' \oplus k'$ (namelijk $k' = c \oplus m'$)

Asymmetrische cryptografie

Bob genereert een sleutelpaar: publieke sleutel 🔒 en geheime sleutel 🔑

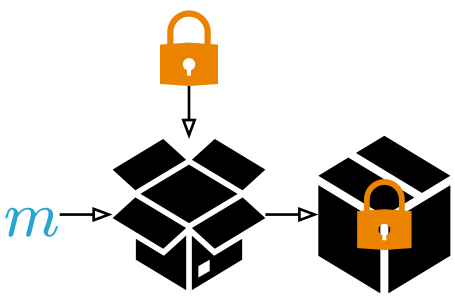


Bijvoorbeeld: Rivest-Adleman-Shamir (RSA)

RSA

Neem twee willekeurige priemgetallen, p en q, en hun product $N = pq$.

$$\text{🔒} = N \quad \text{🔑} = (p, q)$$

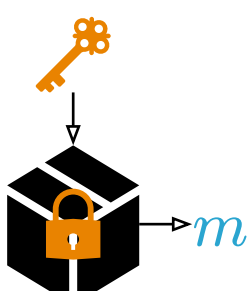


Versleutelen, met $e = 65\,537$:

$$c = m^e \mod N$$

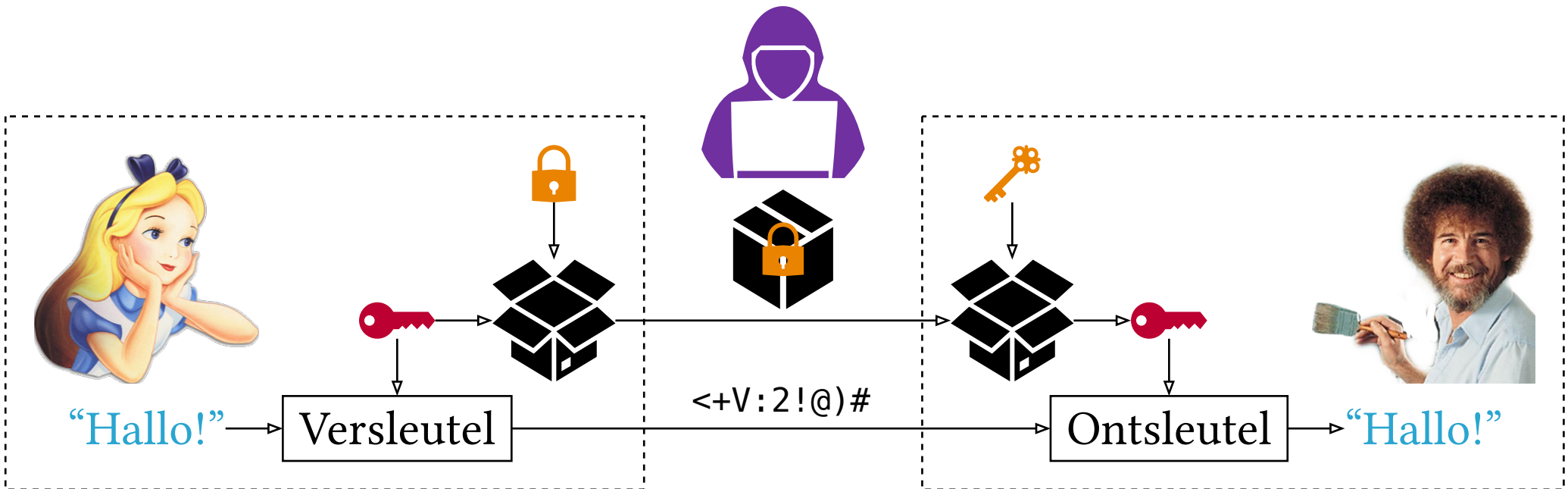
Ontsleutelen, met $d = e^{-1} \bmod (p-1)(q-1)$:

$$m = c^d \mod N$$



🕵 kan RSA breken door N te **ontbinden** in (p, q)

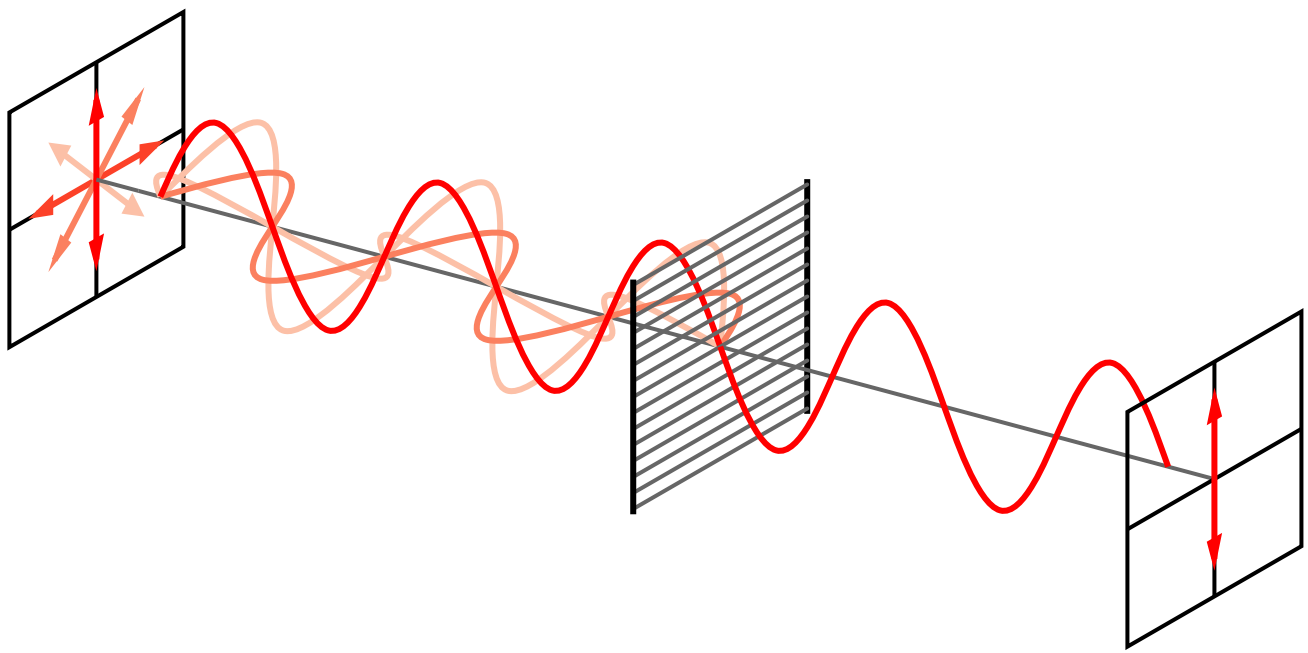
Hybride versleuteling



Bijvoorbeeld*: Diffie-Hellman, Module-Lattice-Based KEM (ML-KEM)

1. Cryptografie
2. **Quantum Informatie**
3. Quantum Computers
4. Post-Quantum Cryptografie
5. Quantum Cryptografie

Polarisatie van licht

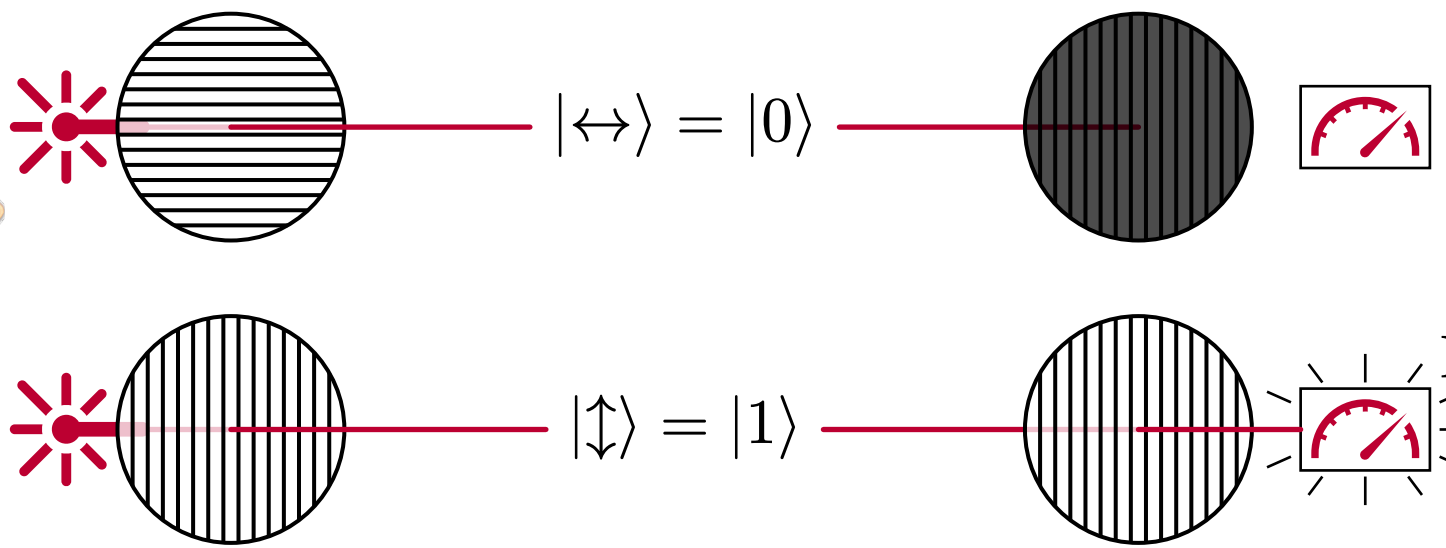


Polarisatie is de richting van een golf

Een polarisatiefilter laat maar één richting door*

Klassieke informatie als gepolariseerd licht

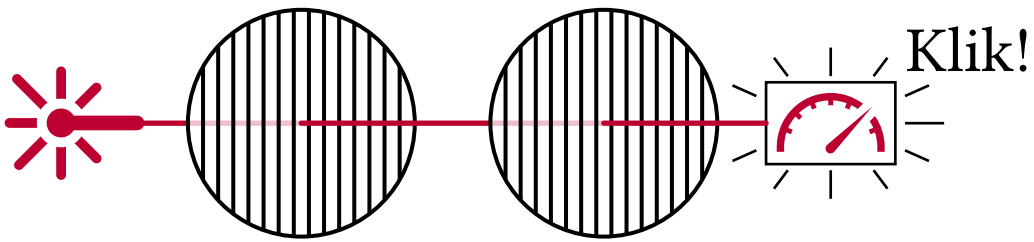
Alice stuurt de bits 01

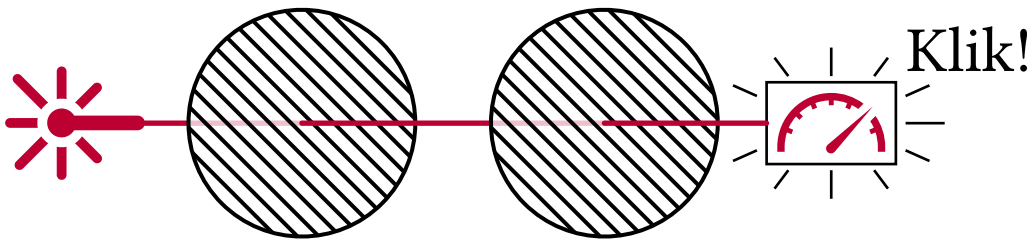


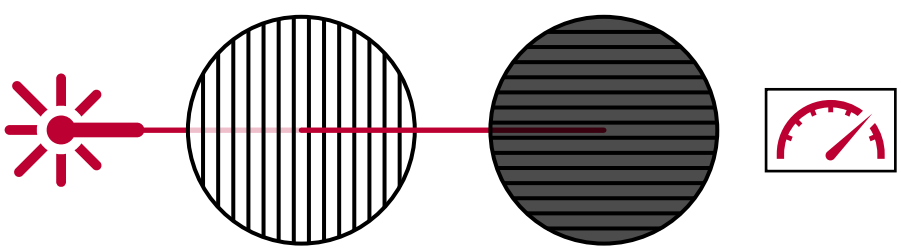
Bob ontvangt de bits 01

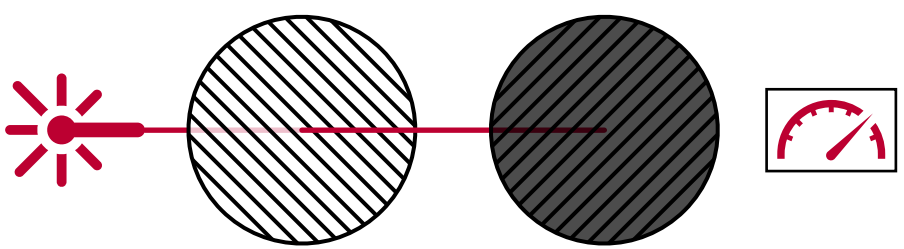
Demonstratie

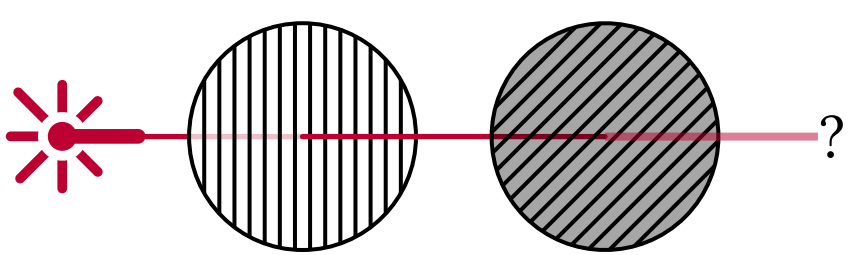
Informatie als gepolariseerd licht





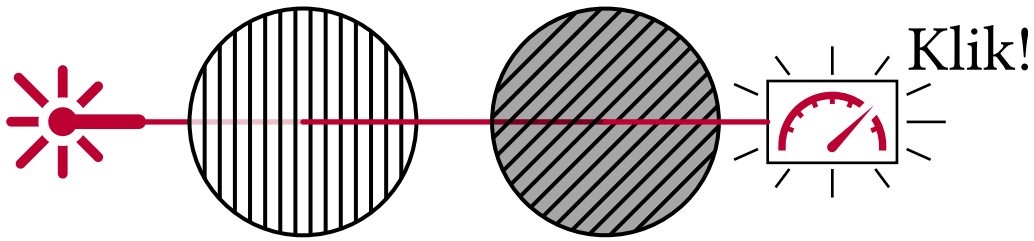




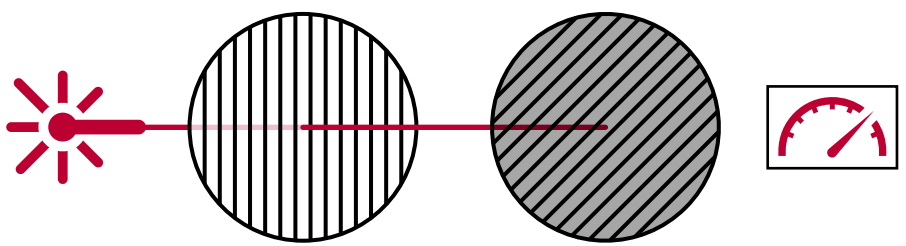


Metingen

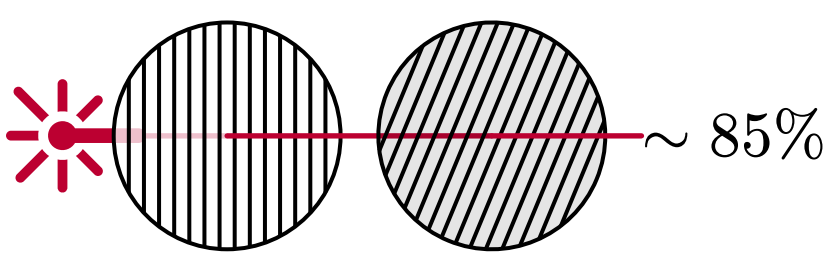
met 50% kans:

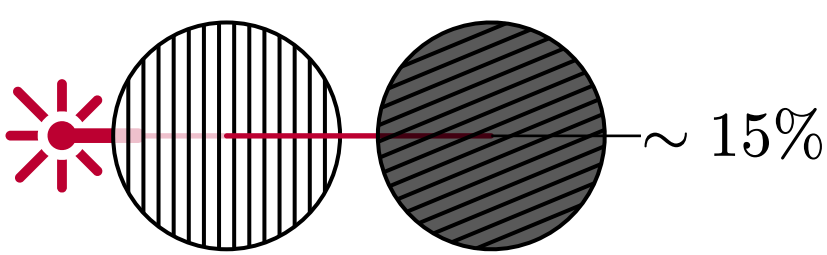


met 50% kans:



Hoe kleiner de hoek, des te groter de kans

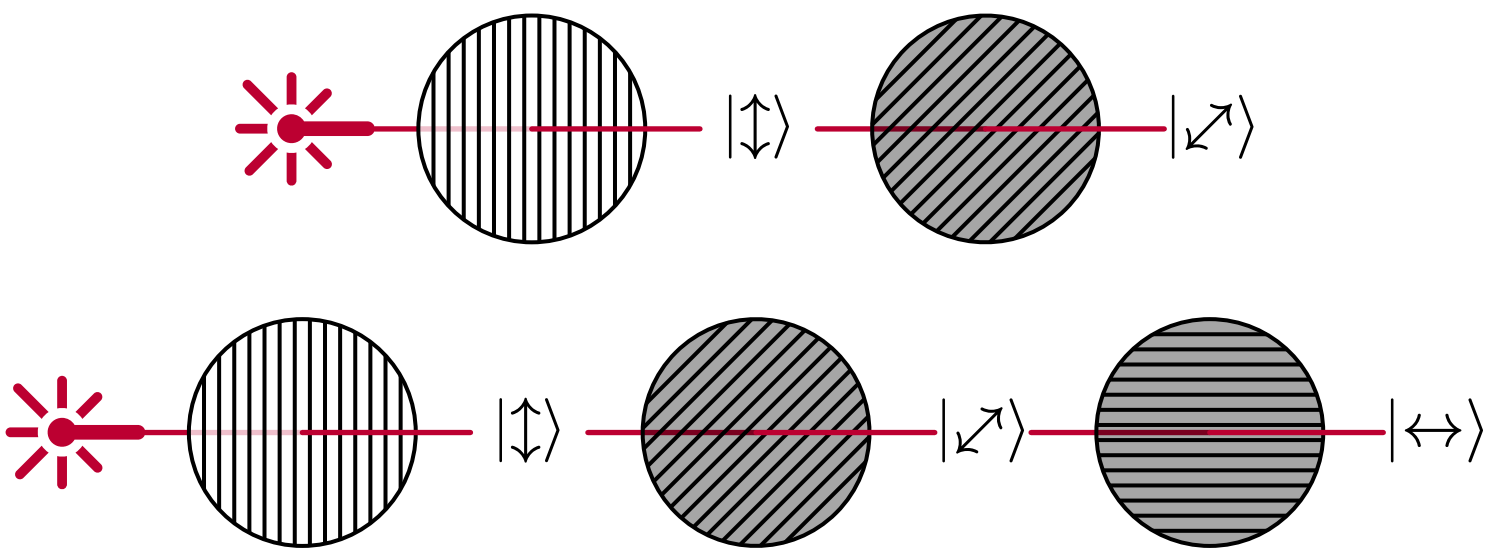




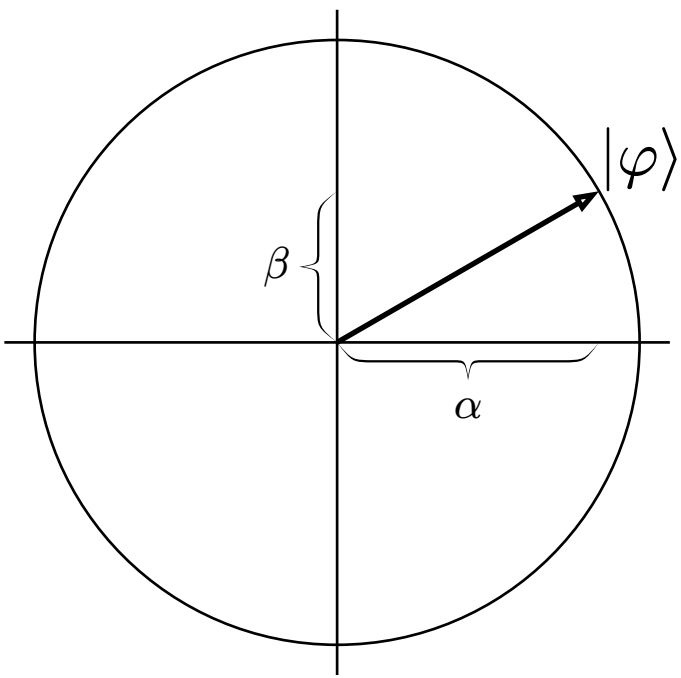
Demonstratie

Meting verandert de toestand

De filters blokkeren niet alleen licht, ze veranderen ook de polarisatie van de doorgelaten fotonen



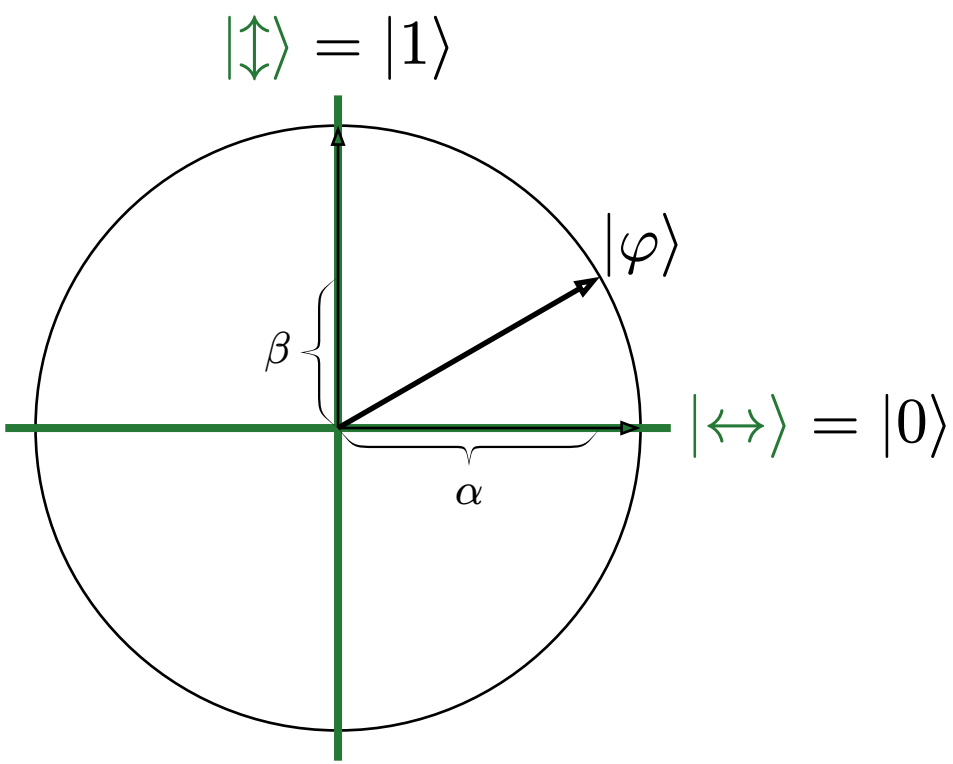
Qubit



Een qubit is een vector $|\varphi\rangle$ met **amplitudes** α en β zodat

$$|\alpha|^2 + |\beta|^2 = 1$$

Standaard basis



De amplitudes zijn t.o.v. een **basis**

Standaard basis $+$

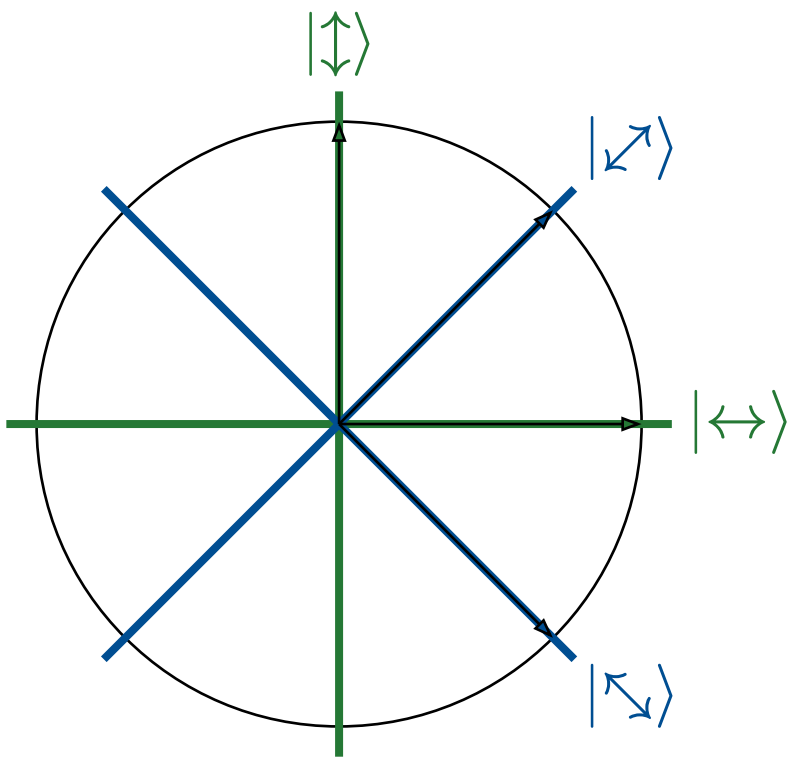
Qubit $|\varphi\rangle$ is een lineaire **superpositie** van $|0\rangle$ en $|1\rangle$:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Meting van $|\varphi\rangle$ in basis $+$ geeft:

- uitkomst $|0\rangle$ met kans $|\alpha|^2$
- uitkomst $|1\rangle$ met kans $|\beta|^2$

Hadamard basis



De **Hadamard** basis $\times$:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

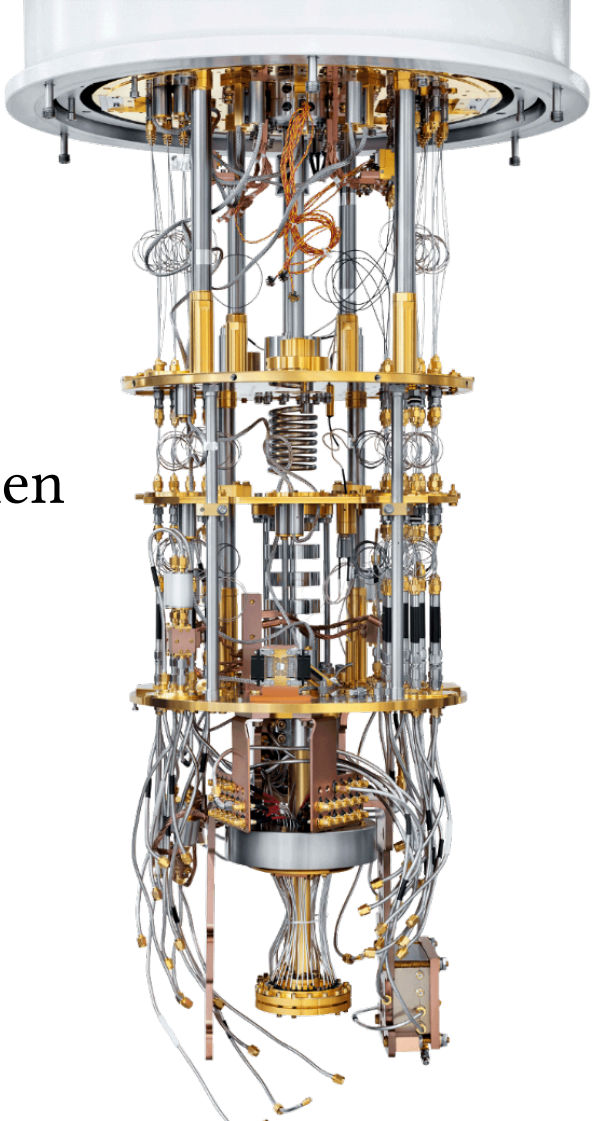
Meting van $|\nearrow\rangle$ of $|\nwarrow\rangle$ in basis $+$

- uitkomst $|\leftrightarrow\rangle$ met kans 50%
- uitkomst $|\updownarrow\rangle$ met kans 50%

Meting van $|\leftrightarrow\rangle$ of $|\updownarrow\rangle$ in basis $\times$
geeft $|\nearrow\rangle$ of $|\nwarrow\rangle$ met 50%

1. Cryptografie
2. Quantum Informatie
3. **Quantum Computers**
4. Post-Quantum Cryptografie
5. Quantum Cryptografie

Quantum computers



Bestaan al op kleine schaal

- kan berekeningen die klassieke computers niet kunnen
- maar lost nog geen “echte” problemen op

Ruis is een limiterende factor voor groei

- decoherentie verstoort quantum toestanden

Foutcorrectie biedt een oplossing

- meerdere fysieke qubits vormen één logisch qubit

Meerdere qubits

- 1 qubit: superpositie van 2 toestanden $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
- 2 qubits: superpositie van 4 toestanden

$$\frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{\sqrt{4}}$$

- 3 qubits: superpositie van 8 toestanden

$$\frac{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle}{\sqrt{8}}$$

- ...
- n qubits: superpositie van 2^n toestanden

Quantum parallelisme

We kunnen een functie f berekenen op een superpositie van invoer: dit resulteert in een superpositie van uitvoer

Neem bijvoorbeeld vermenigvuldiging $f(x, y) = x \cdot y$

Geef de quantum computer een superpositie als invoer

$$|x, y\rangle = \Big(|1, 1\rangle + |1, 2\rangle + ... + |N, N-1\rangle + |N, N\rangle\Big)/N$$

De quantum computer berekent dan

$$|x, y, f(x, y)\rangle$$

$$= \Big(|1, 1, 1\rangle + |1, 2, 2\rangle + ... + \big|N, N-1, N^2 - N\big\rangle + \big|N, N, N^2\big\rangle\Big)/N$$

Het is **alsof** we N^2 vermenigvuldigingen hebben gedaan, met 1 evalatie van f

Was dit nuttig?

Als we nu meten krijgen we slechts één uitvoer, bijvoorbeeld $(3, 5, 15)$

- Elke toestand heeft dezelfde amplitude, dus elke uitvoer heeft kans: $1/N^2$
- Kans is verwaarloosbaar dat dit het getal is dat we wilden ontbinden

Nuttige quantum berekeningen

De kunst is om de amplitudes te manipuleren

- constructieve interferentie voor “gewilde” toestanden
- destructieve interferentie voor “ongewilde” toestanden

We kennen zeer weinig nuttige quantum berekeningen

Bekende quantum algoritmes

Het algoritme van **Shor**

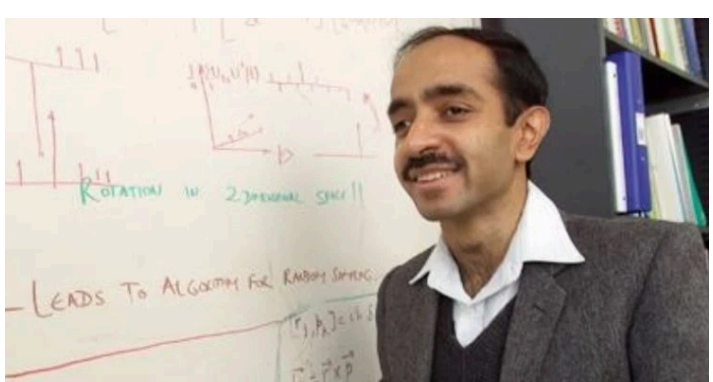
- Kan getallen ontbinden in priemfactoren

   RSA gebroken!
- Kan discrete logaritmes berekenen

   (EC)DH gebroken!
- Zeer efficient!

Het algoritme van **Grover**

- Zeer algemeen zoek-algoritme: vind een speld in een hooiberg (ter grootte n) in $\sqrt{n}$ stappen.
- Bijv. vind  uit 2^n totaal, in $2^{n/2}$ stappen
- Sequentieel: supercomputers met klassiek parallelisme kunnen sneller zijn



1. Cryptografie
2. Quantum Informatie
3. Quantum Computers
4. **Post-Quantum Cryptografie**
5. Quantum Cryptografie

Post-Quantum Cryptografie

Alice en Bob hebben een klassieke computer

- maar zijn veilig tegen hackers met een quantum computer

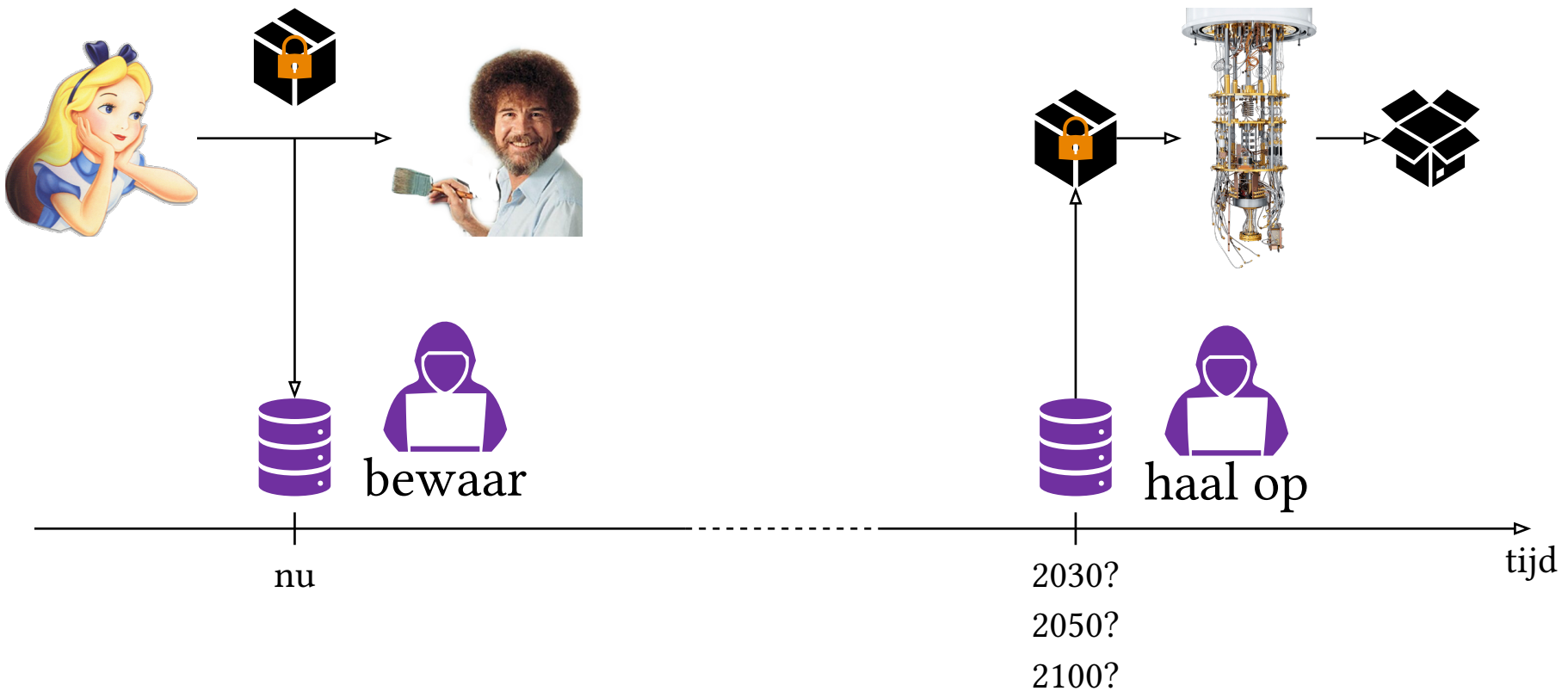
Andere wiskundige problemen voor ( , )

- vervanging van RSA en (EC)DH

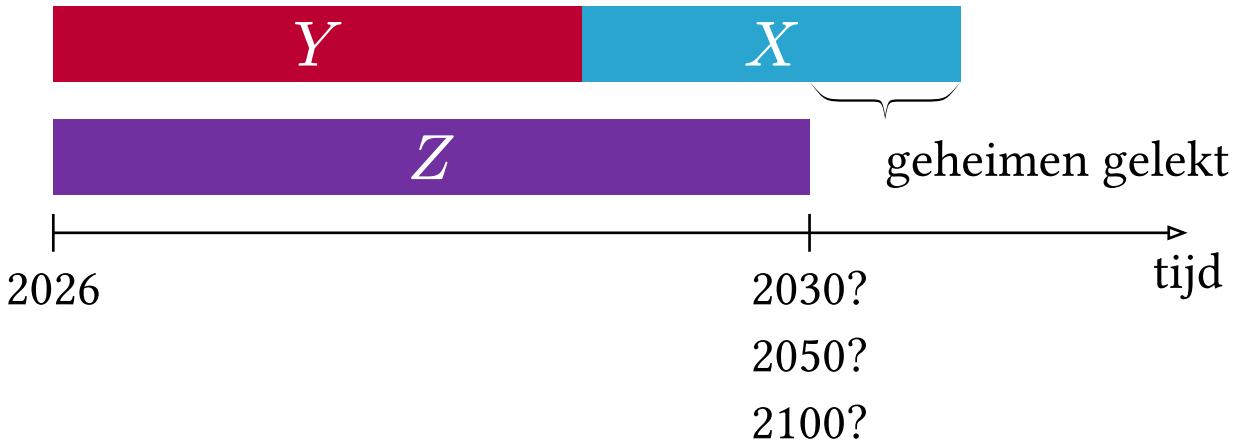
Verdubbel de grootte van 

- “slechts” een update van AES-128 naar AES-256

Nu bewaren, later kraken



Stelling van Mosca



- X: hoe lang moet je data veilig blijven?
- Y: hoe lang duurt je migratie naar PQC?
- Z: hoe lang voor er quantum computers zijn?

Je moet je zorgen maken als

$$X + Y > Z$$

PQC - wiskundige problemen

Gebaseerd op andere (wiskundige) problemen

- **Roosters**: vind de kortste vector in een hoogdimensionaal rooster
- **Foutcorrectie**: decodeer zonder kennis van de structuur van de code
- **Hash**-gebaseerd: vind twee invoeren met dezelfde uitvoer van een cryptografische hash functie
- … en andere kandidaten

Geen bewijs van veiligheid, maar er is geen aanval bekend

https://cryptography101.ca/

PQC - huidige status

Gestandaardiseerd:

ML-KEM (Kyber, FIPS 203): KEM gebaseerd op roosters

ML-DSA (Dilithium, FIPS 204): handtekening gebaseerd op roosters

SLH-DSA (SPHINCS+, FIPS 205): handtekening gebaseerd op hash functies

Concept standaard:

FN-DSA (FALCON, FIPS 206): handtekening gebaseerd op roosters

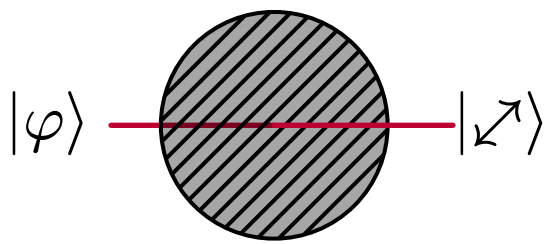
HQC-KEM (HQC, FIPS 207): KEM gebaseerd op foutcorrectie

1. Cryptografie
2. Quantum Informatie
3. Quantum Computers
4. Post-Quantum Cryptografie
5. **Quantum Cryptografie**

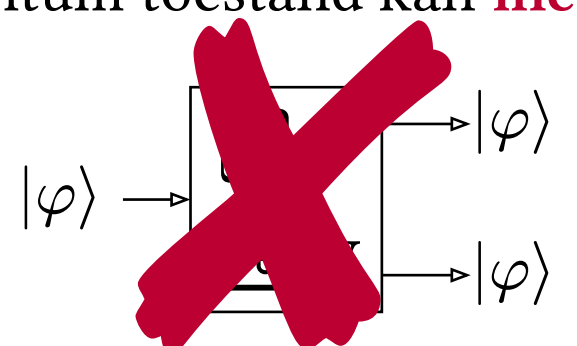
Quantum Cryptografie

Gebruik de wetten van quantum informatie

1. Meting verstoort de toestand



2. Een onbekende quantum toestand kan **niet gekloond** worden

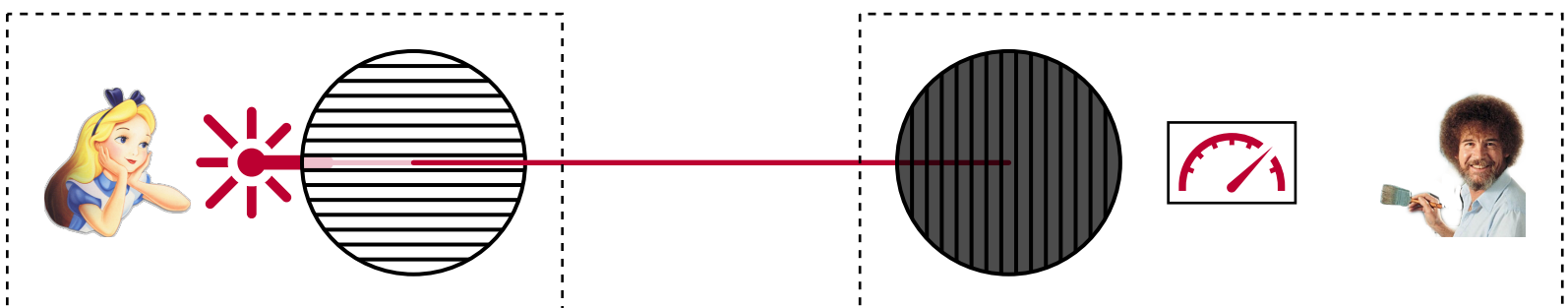


Veiligheid is onafhankelijk van de rekenkracht van  !!!

Quantum Key Distribution (QKD) 1/3

Maak een nieuwe 🔑 met quantum informatie

Alice en Bob kiezen beiden willekeurig een basis: $+$ of $\times$
Alice kiest willekeurig een bit ($0 = |\leftrightarrow\rangle$ of $1 = |\updownarrow\rangle$)



"Mijn basis was $+$"

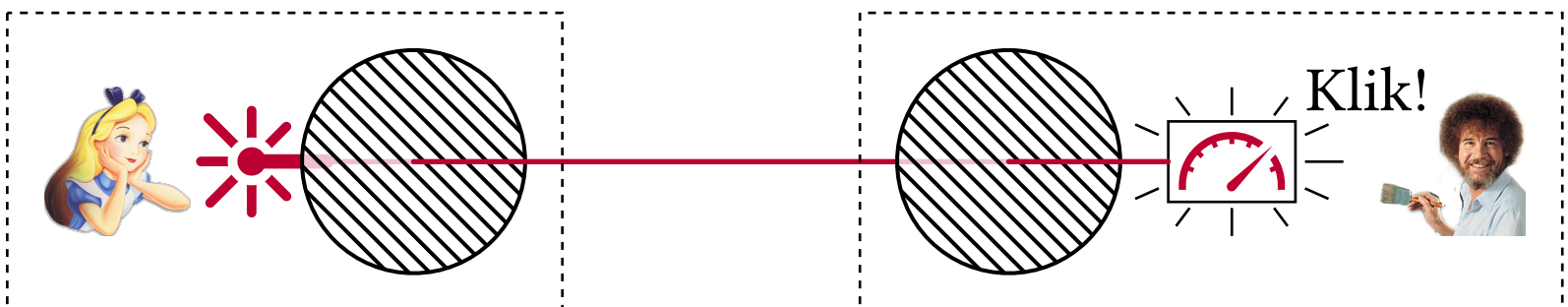
"Mijn basis was $+$"

Alice en Bob delen bit 0

Quantum Key Distribution (QKD) 2/3

Alice en Bob kiezen beiden willekeurig een basis: $+$ of $\times$

Alice kiest een bit ($0 = |\nearrow\rangle$ of $1 = |\nwarrow\rangle$)



"Mijn basis was $\times$"

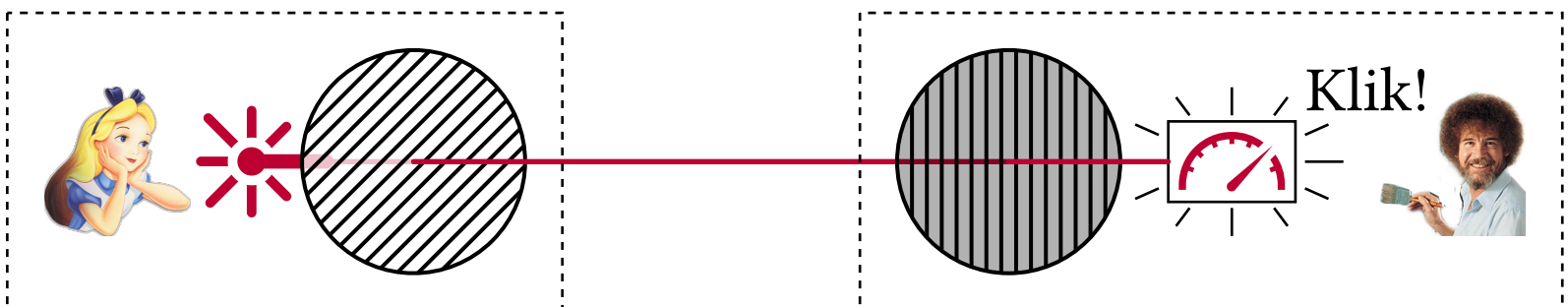
"Mijn basis was $\times$"

Alice en Bob delen bit 1

Quantum Key Distribution (QKD) 3/3

Alice en Bob kiezen beiden willekeurig een basis: $+$ of $\times$

Alice kiest een bit ($0 = |\nearrow\rangle$ of $1 = |\searrow\rangle$)



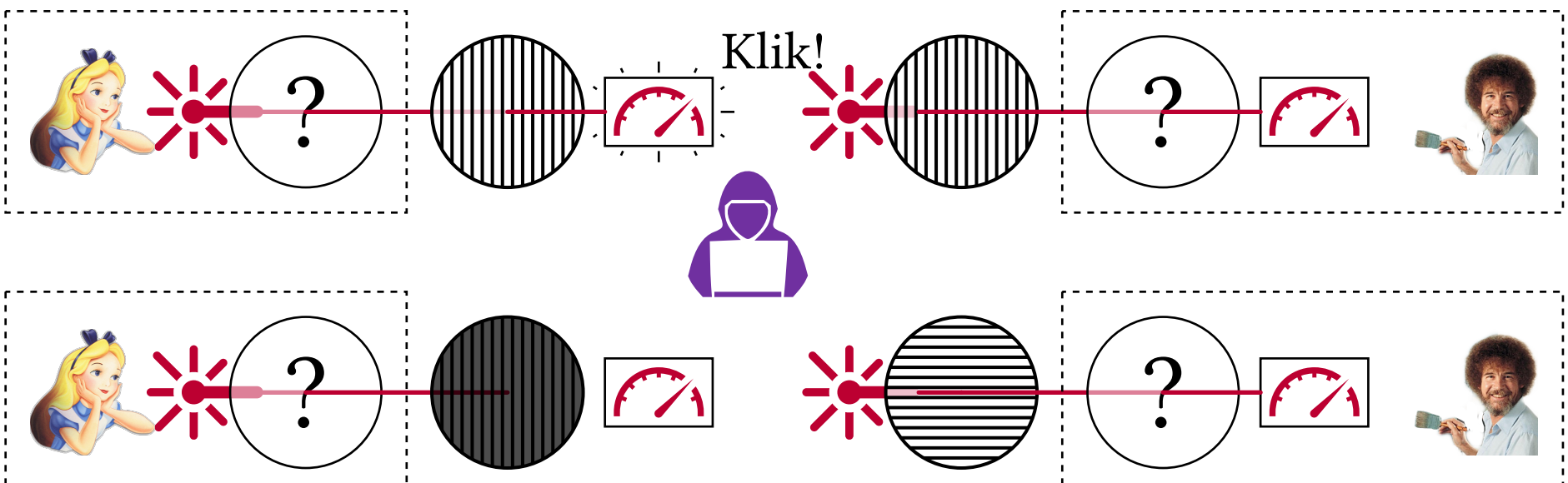
"Mijn basis was $+$"

"Mijn basis was $\times$"

Bob's resultaat is willekeurig: Alice en Bob negeren deze ronde

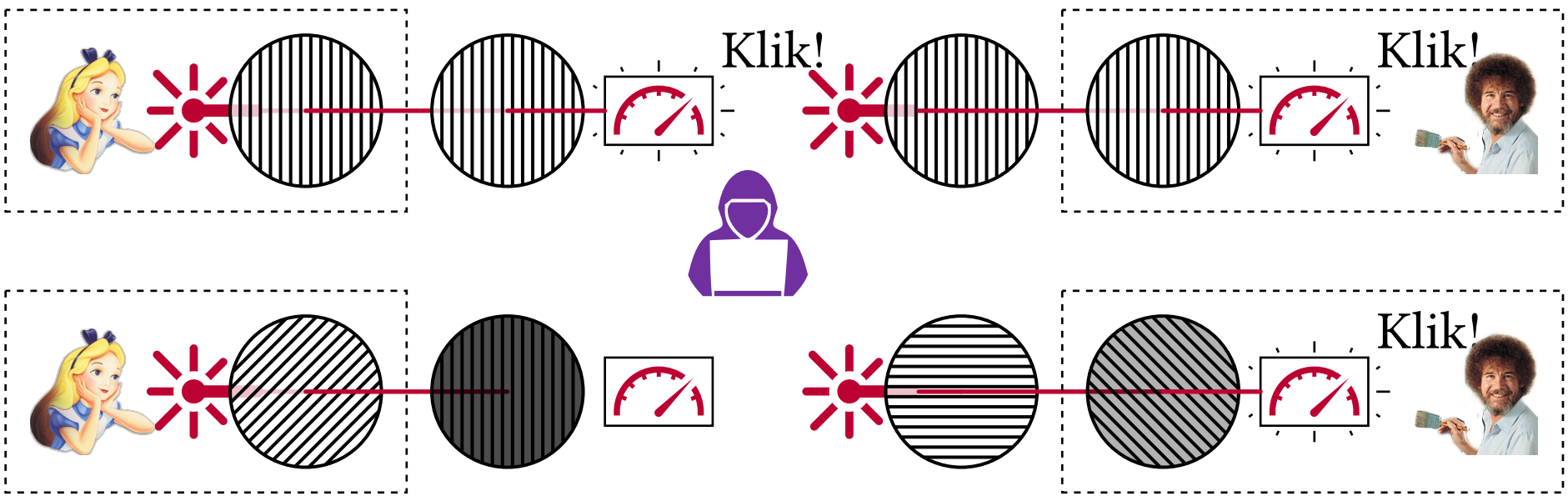
Aanval op QKD

wil afluisteren, maar weet de basis niet



Aanval op QKD

De eerste gok was goed: heeft een geheim bit (1) geleerd!

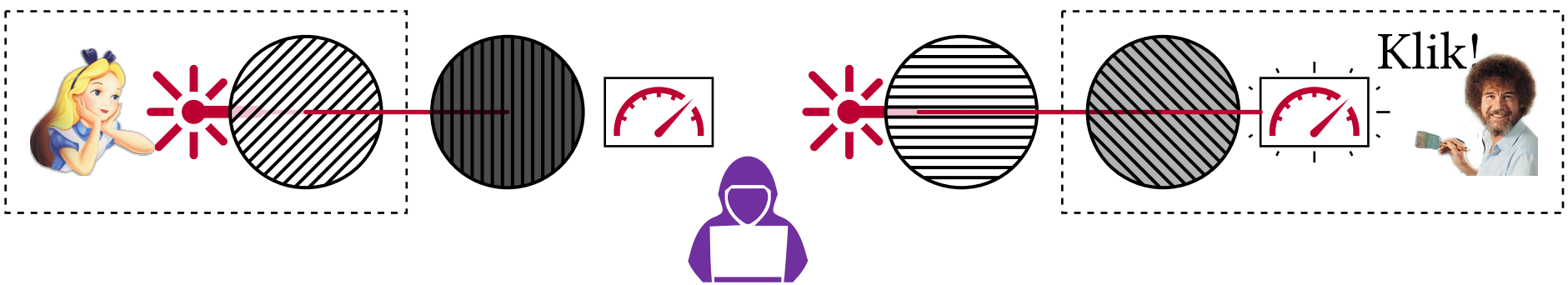


Tweede gok was fout: Alice heeft 0 en Bob heeft 1!

Bescherming tegen de aanval

Alice en Bob kiezen willekeurig een aantal rondes

- ze onthullen de bits van die rondes (en gebruiken die dus niet voor 🔑)
- bij een foute gok wordt 🕵 waarschijnlijk gedetecteerd



"Mijn basis was $\times$, en ik zag $|\nwarrow\rangle$"

"Mijn basis was $\times$, en ik stuurde $|\nearrow\rangle$"

Alice en Bob concluderen dat ze afgeluisterd worden!

QKD: nabewerking

Fouten in dezelfde basis kunnen ook optreden door ruis

- Alice en Bob tolereren een maximaal aantal fouten
- Na **foutcorrectie** delen Alice en Bob dezelfde bits

Een deel van deze bits kan bekend zijn bij de aanvaller

- een sterke sleutel wordt **gedistileerd** uit de gedeelde bits
  - dit is veilig, zelfs als **alle** getoleerde ruis door  veroorzaakt was

Alice en Bob moeten zeker weten dat ze met elkaar spreken (**authenticatie**)

Praktische bezwaren

1. Authenticatie nodig
   (dit kan met 🔑, maar dan is QKD geen alternatief voor PQC)
2. Speciale hardware nodig
3. Gelimiteerd in afstand (~100km)
   (quantum repeaters zijn een oplossing, maar nog onpraktisch)
4. Side-channels
   (QKD is theoretisch veilig, maar is in de praktijk al vaker gebroken)
5. Langzaam

Mijn onderzoek

Wanneer heeft QKD toegevoegde waarde?

- In welke context zijn de (huidige) praktische bezwaren geen probleem?
- Als we de praktische bezwaren oplossen met PQC, behouden we dan nog voordelen van QKD?
- Hoe kunnen we PQC en QKD combineren om 🔑 te genereren?
  - zodat 🔑 veilig is, zelfs als PQC of QKD gebroken is

Samenvatting

- **Cryptografie** is overal
  - gedeelde sleutels (🔑) versleutelen onze data
  - (🔒, 🔑) genereert 🔑: gebaseerd op wiskundige problemen
- **Quantum computers** lossen sommige van deze problemen zeer efficiënt op
- **Post-Quantum Cryptografie** introduceert nieuwe wiskundige problemen
  - geen efficiënte (quantum) oplossingen
- **Quantum cryptografie** baseert veiligheid op quantum informatie
  - **QKD** kan 🔑 genereren
    - maar heeft praktische bezwaren

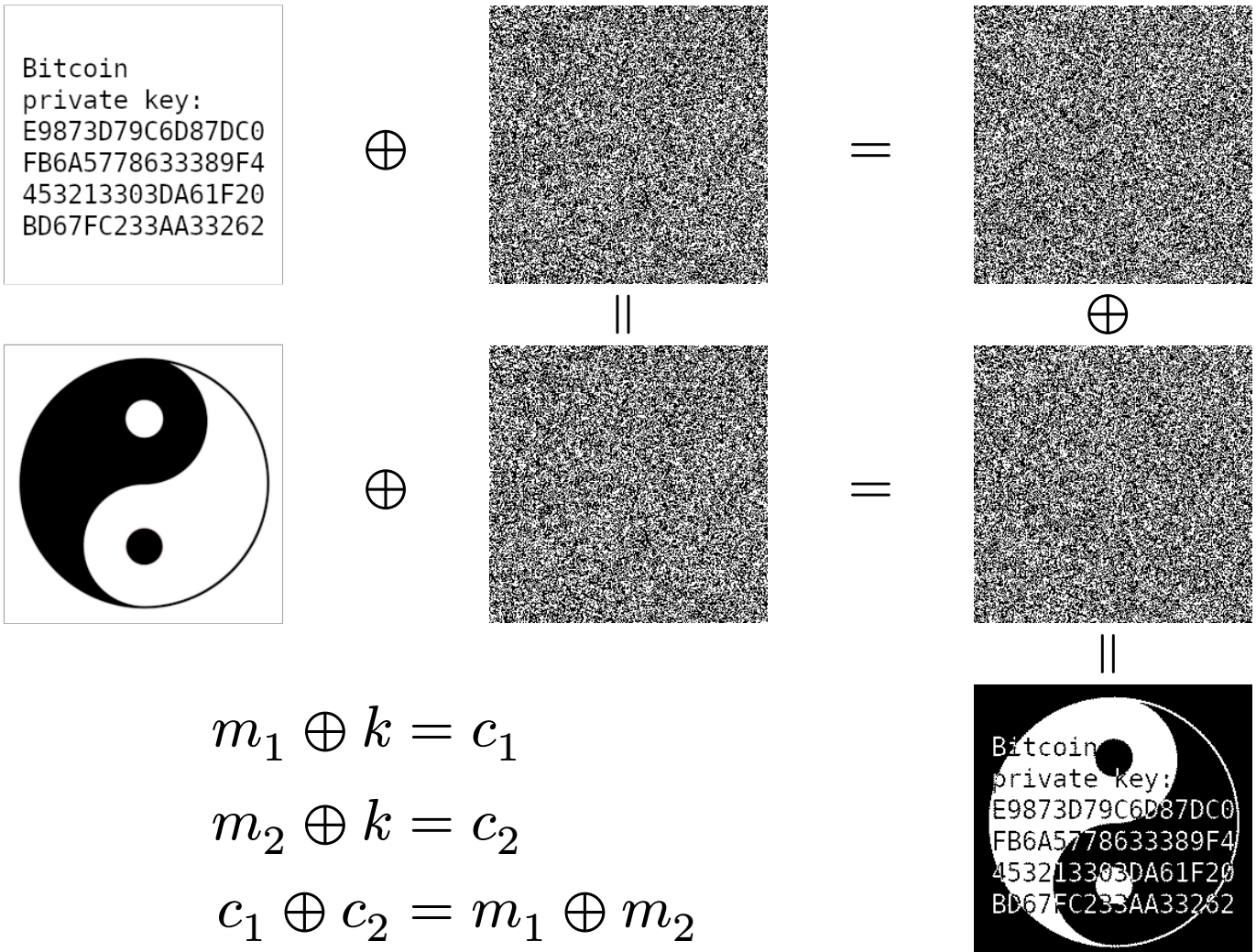
Meer informatie

- Simon Singh - The Code Book
- P. Kaye, R. Laflamme, M. Mosca - An Introduction to Quantum Computing
- Mike Rosulek: The Joy of Cryptography (https://joyofcryptography.com/)
- Het PQC-migratie handboek (https://ir.cwi.nl/pub/34603)
- QuSoft (https://qusoft.org/)
- IBM quantum (https://quantum.cloud.ibm.com/)
  - John Watrous: Quantum Information & Computation
  - Qiskit tutorials
- Tiq Taq Toe (https://www.tiqtaqtoe.com/)
- “The talk” (https://www.smbc-comics.com/comic/the-talk-3)
- Uitleg algoritme van Shor (https://scottaaronson.blog/?p=208)

zeroknowledge.me

s.r.verschoor -at-
uva.nl

Two-time pad is onveilig



$$m_1 \oplus k = c_1$$

$$m_2 \oplus k = c_2$$

$$c_1 \oplus c_2 = m_1 \oplus m_2$$

Two-time pad is onveilig

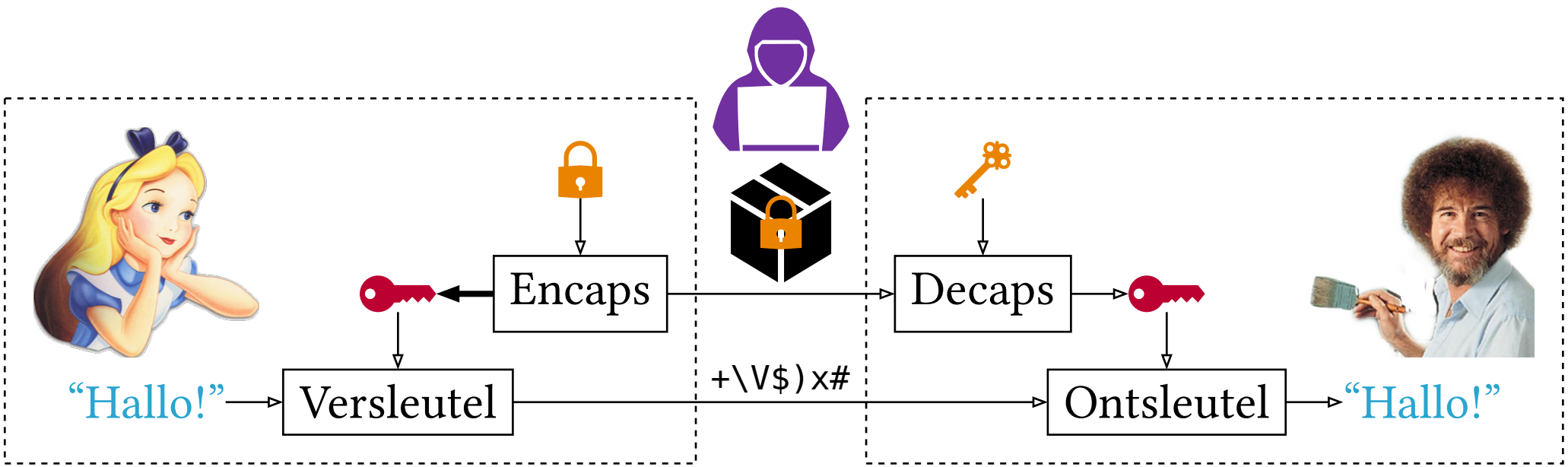
```
import PIL.Image, numpy as np

m1 = np.array(PIL.Image.open("m1.png").convert("1"))
m2 = np.array(PIL.Image.open("m2.png").convert("1"))
k = np.random.randint(2, size=m1.shape, dtype=bool)
c1 = m1 ^ k
c2 = m2 ^ k
m12 = c1 ^ c2

PIL.Image.fromarray(k).save("k.png")
PIL.Image.fromarray(c1).save("c1.png")
PIL.Image.fromarray(c2).save("c2.png")
PIL.Image.fromarray(m12).save("m12.png")
```

Key/Data Encapsulation Mechanism (KEM/DEM)

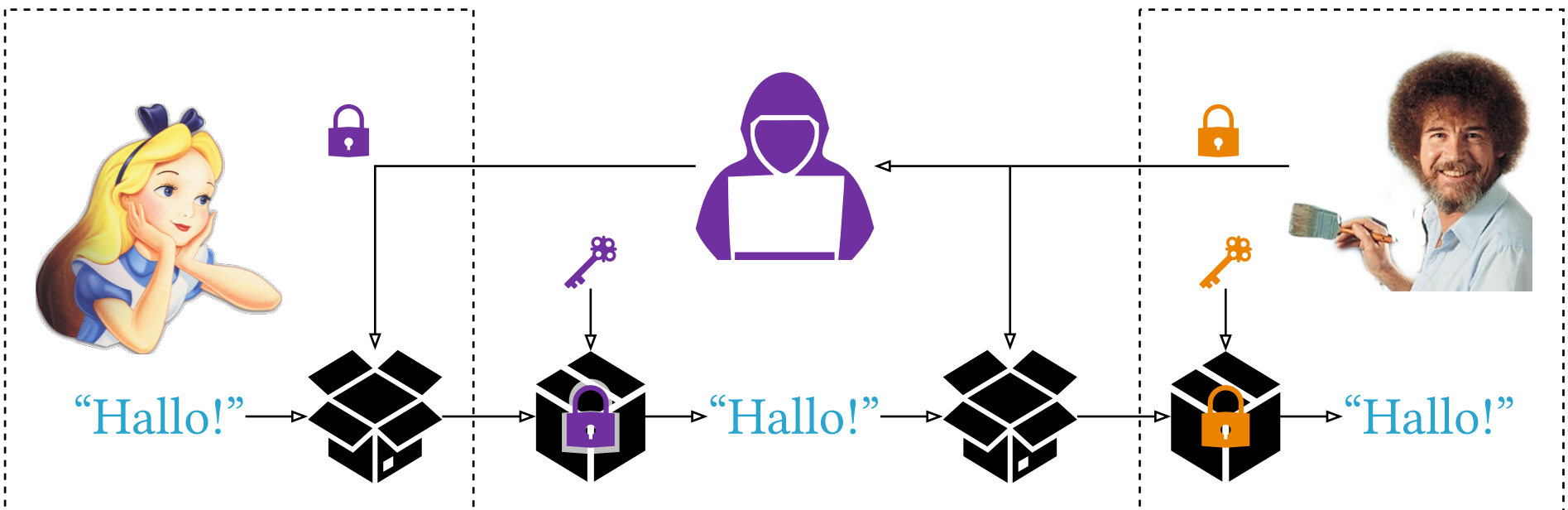
Moderne variant van hybride versleuteling (is een uitvoer van Encaps)



Bijvoorbeeld: Diffie-Hellman, Module-Lattice-Based KEM (ML-KEM)

Sleutel Authenticatie

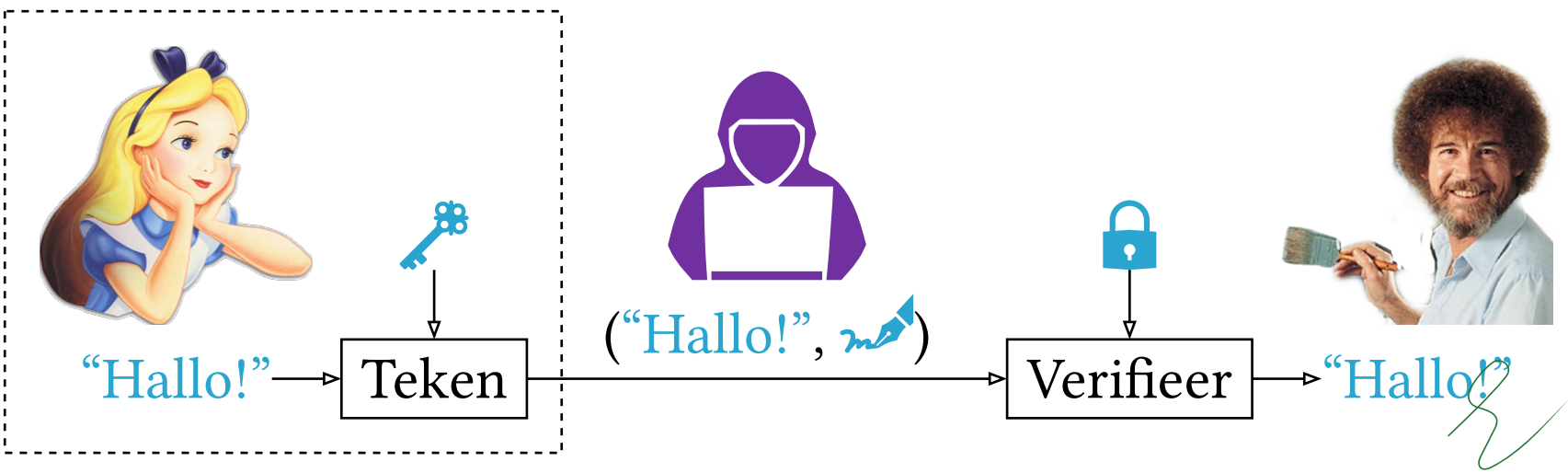
Hoe weet Alice dat 🔒 echt van Bob is?



Dit is een Monster-in-'t-Midden (MitM) aanval

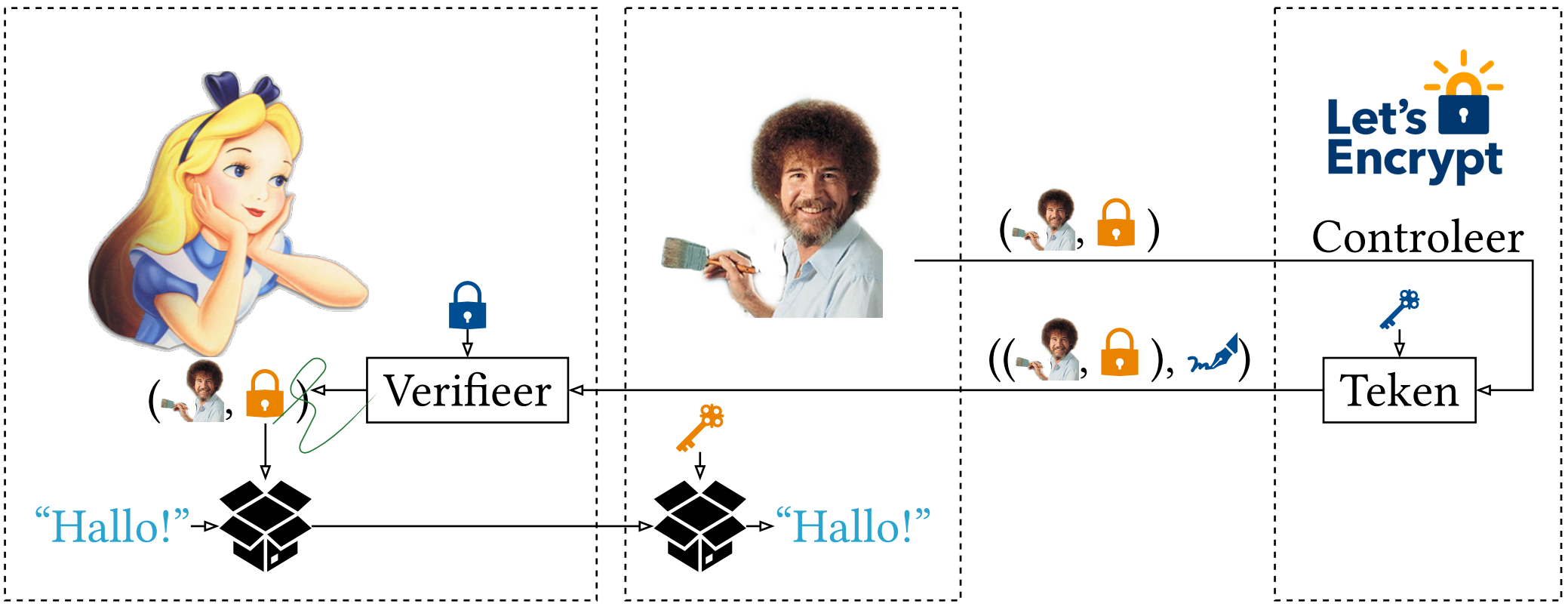
Digitale Handtekening

Authenticatie: het bericht komt van  en is niet veranderd door  .



Bijvoorbeeld: Rivest-Adleman-Shamir (RSA), Module-Lattice-Based Digital Signature Algorithm (ML-DSA)

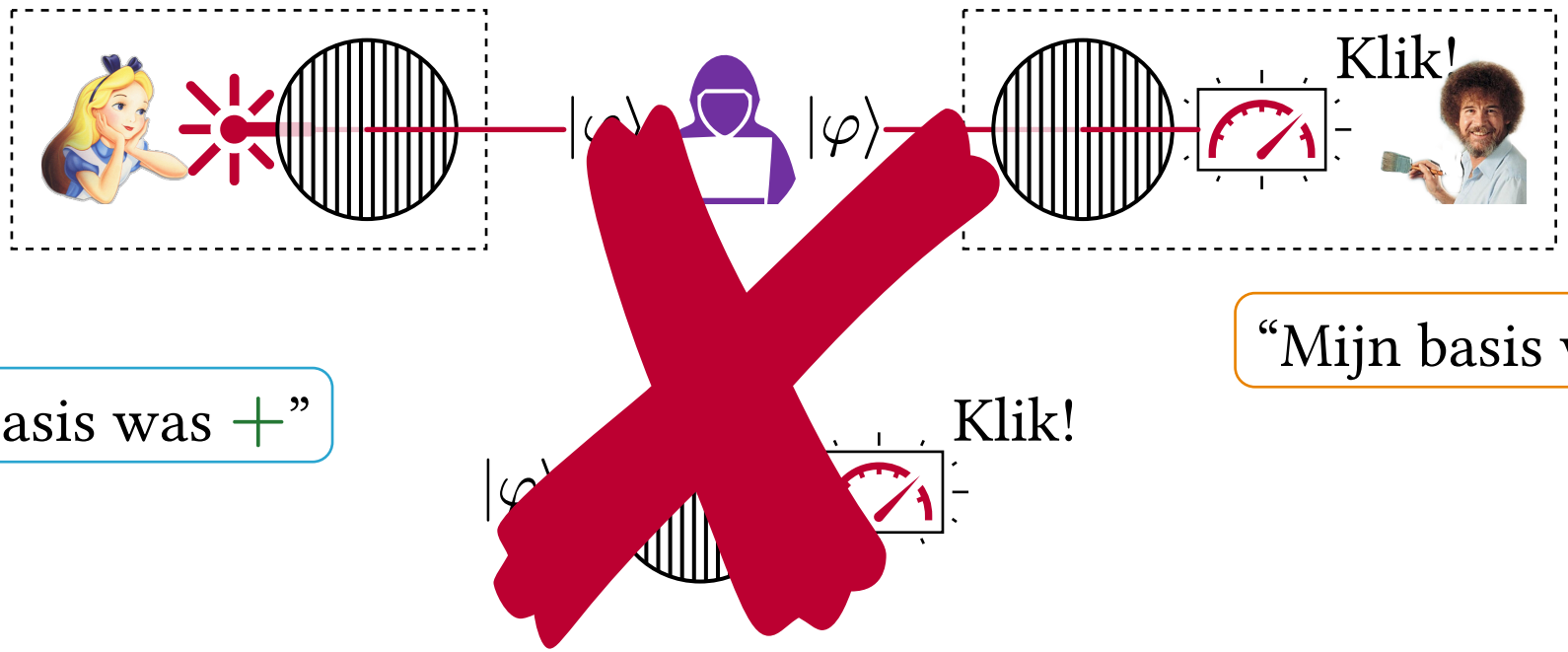
Certificaten



Meer info: https://letsencrypt.org/how-it-works/

Andere aanval op QKD?

wacht met meten van $|\varphi\rangle$ tot de basis bekend gemaakt wordt



heeft nu het geheime bit (1) geleerd!

heeft $|\varphi\rangle$ bewaard **en** doorgestuurd, oftewel: **gekloond**, en dat kan niet!