

Demonstratie: quantum beveiligde videoverbinding

29 JUNI 2023 - WAALRE

Dr. Sebastian Verschoor



Cryptografie

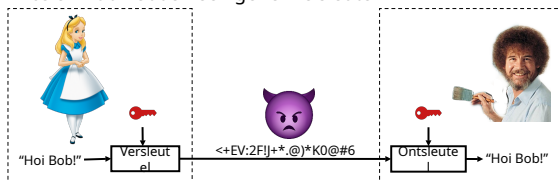
Het versleutelen van berichten

2



Geheime berichten

Alice en Bob hebben een geheime sleutel



3



Ontslutelen

Z D D O U H

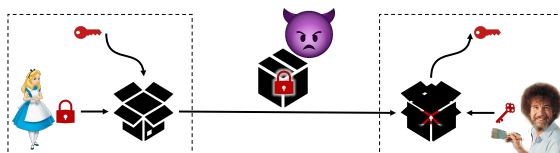


4



Hoe delen Alice en Bob hun sleutel?

- Bob heeft een speciale sleutel, met bijbehorende slot



5



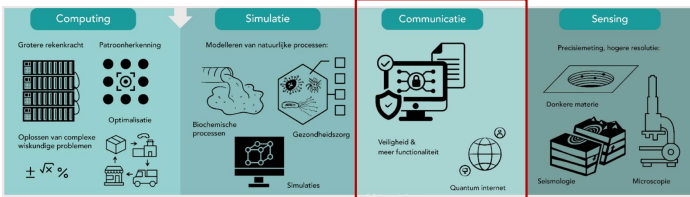
Quantumcomputers

Extra rekenkracht (voor sommige problemen)

6



Toepassingen van quantum technologie



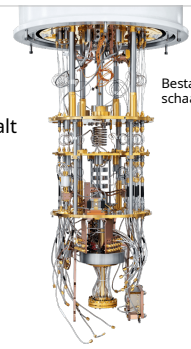
7

Quantumcomputer

- Elk computerprogramma vertaalt invoer naar uitvoer

$$3 \rightarrow \boxed{\times 2} \rightarrow 6$$

- Quantumcomputers hebben quantum invoer/uitvoer:
- dit geeft extra rekenkracht



Bestaan al op kleine schaal

8

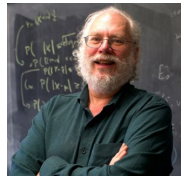
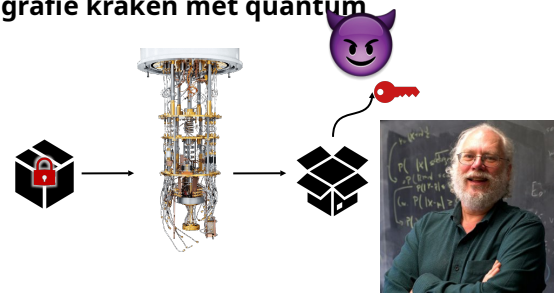
Maar hoe werkt dat dan?

- **Superpositie:** alsof het deeltje in meerdere staten tegelijk
- Een berekening hierop is alsof je alle mogelijke oplossingen voor een probleem tegelijk kan proberen
- **Maar:** je krijgt ook alle antwoorden in superpositie
- Een goed quantum algoritme zorgt ervoor dat goede oplossingen elkaar versterken en slechte oplossingen elkaar verzwakken



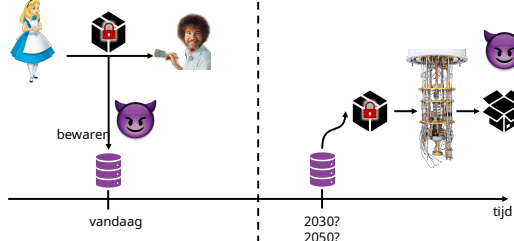
9

Cryptografie kraken met quantum



10

Nu bewaren, later kraken



11

Quantum communicatie

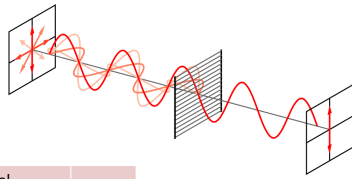
Detectie van afluisteraars

12

Gepolariseerd licht

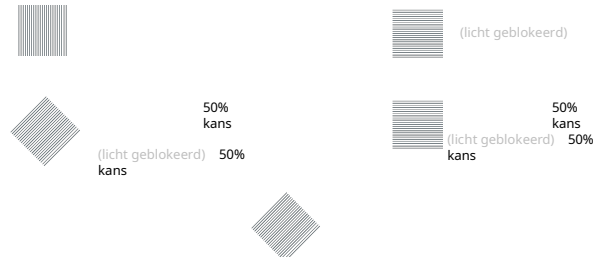
- Licht heeft polarisatie: dit is een quantum effect

verticaal	
horizontaal	
diagonaal	↗
anti-diagonaal	↘



13

Polariserende filters



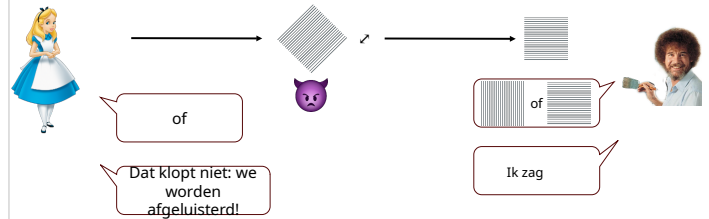
14

Afluisteraars detecteren



15

Afluisteraars detecteren



16

Quantum Key Distribution (quantum sleutel uitwisseling)

- Alice stuurt fotonen naar Bob
- Een (willekeurig) deel wordt gebruikt om af te luisteren te detecteren
- Zo niet: dan wordt de rest gebruikt voor een geheime sleutel

17

Waalre

De huidige opstelling

18

De opstelling



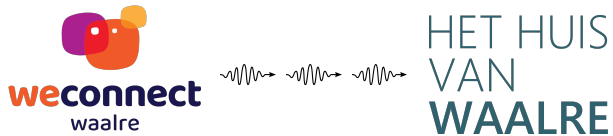
19

De opstelling



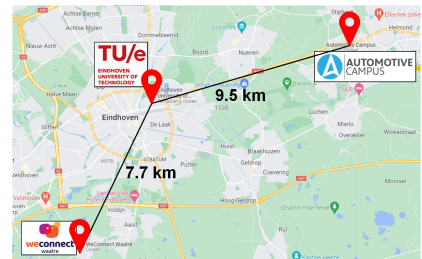
20

De opstelling



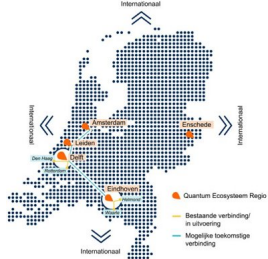
21

Eindhoven testomgeving - fase 2



22

Eindhoven testomgeving - fase 3



23

Phase 4?



24

Quantum communicatie team TU/e



Simon Rommel
Quantum Secure Comms.
Quantum Testbed



Chigo Okonkwo
Quantum Secure Opt.
CV QKD Systems



Melfares Tolu Maenry
Quantum Secure Comms.
DV QKD Systems



Boris Stanc
Theory and
Security proofs



Andreea Hiding
Post-Quantum
Cryptography



Kathrin Hovelmanns
Post-Quantum
Cryptography



Dana Patterson
Project Management



Gijb Hiphans
Program Manager
Quantum Technologies



Sebastian Verschoor
QKD testbed
KMS & Key Relay



Bruno Cmolli
Quantum Testbed
Systems Engineering



Hui Liu
Quantum Secure Comms.
DV/MDI-QKD Systems



Aaron Albrechts-Majaj
Integrated QKD
Systems Engineering



Sjoerd van der Heide
QKD Systems
Systems Engineering



Alexander Gribchenchikov
DV-QKD Systems



Mehmet Temel
Quantum Information Security



Jolo Frazzlo
CV-QKD Systems



Denis Farkhov
On-Chip QKD



Gleb Nazarikov
DV-QKD On-Chip



Arpan Ray
Quantum cryptography



Catalina Stan
Quantum Testbed
Monitoring & Control Layer



Carlos Rubio Garcia
Quantum Testbed
Control Plane



Omerayma Isoucheimal
Quantum Secure Comms.
Quantum ML



Daniel Livan
Quantum Secure Comms.



Abraham Cano Aguilera
Quantum Secure Comms.



Xavi Arnal / Clemente
Quantum Secure Comms.



Raphael Frantz
Quantum Secure Comms.

Demonstratie: quantum beveiligde videoverbinding

Dr. Sebastian
Verschoor
s.r.verschoor@tue.nl

