

# Demonstratie: quantum beveiligde videoverbinding

29 JUNI 2023 - WAALRE

Dr. Sebastian Verschoor

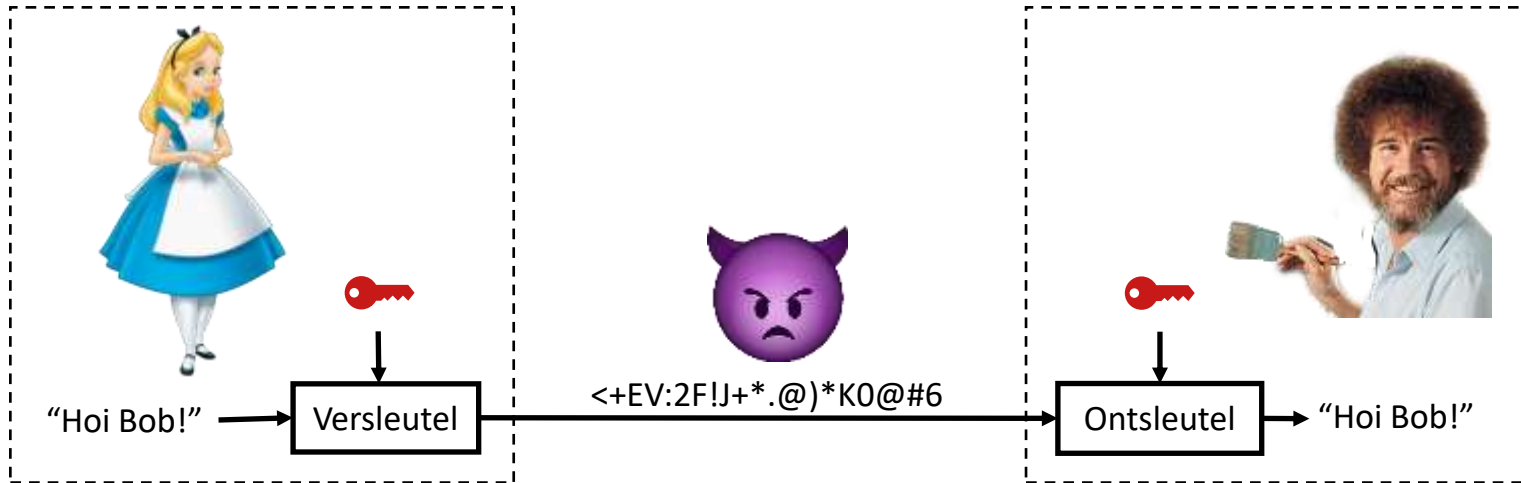


# Cryptografie

Het versleutelen van berichten

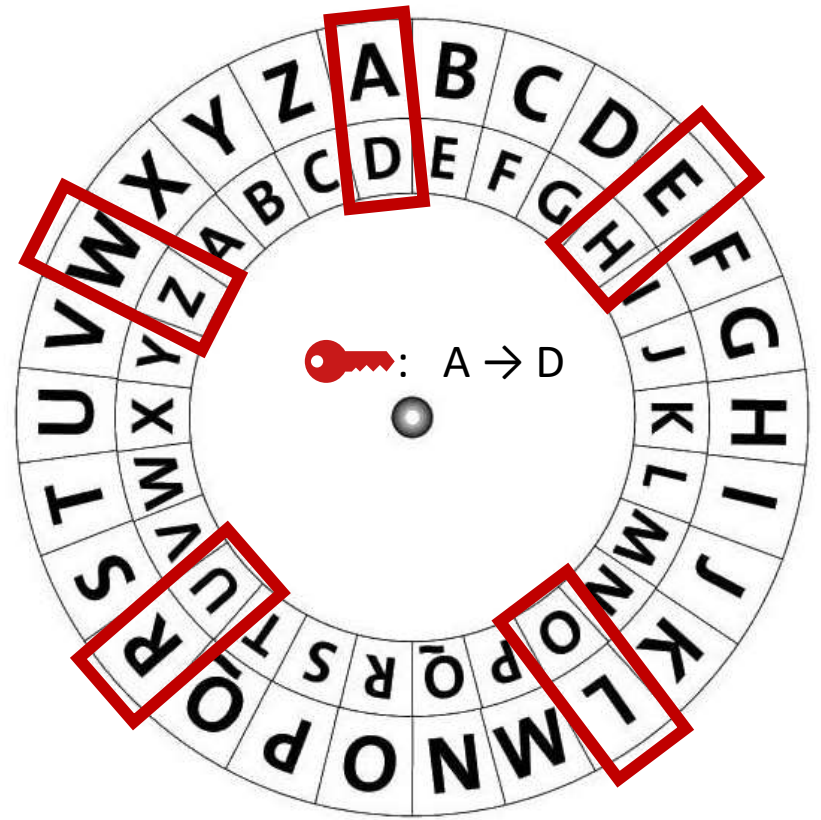
# Geheime berichten

Alice en Bob hebben een geheime sleutel 



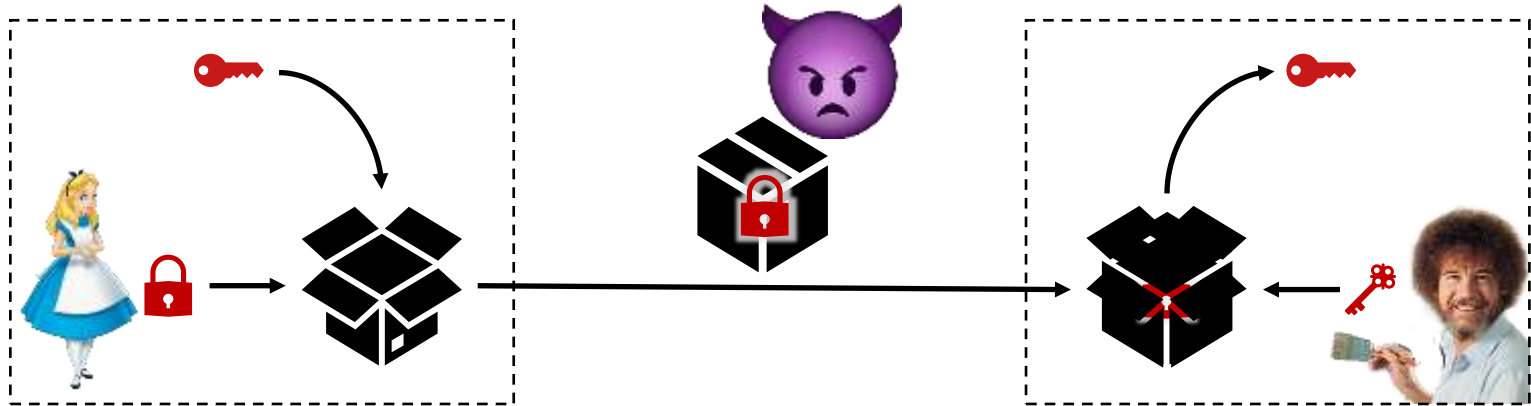
# Ontsleutelen

Z	D	D	O	U	H



# Hoe delen Alice en Bob hun sleutel?

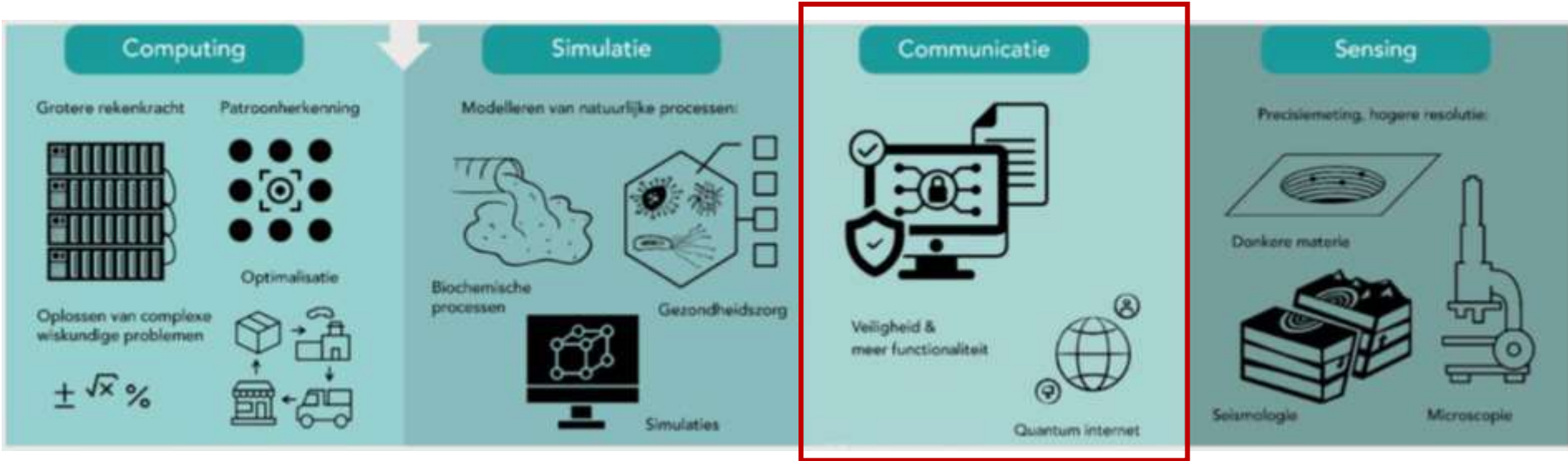
- Bob heeft een speciale sleutel , met bijbehorend slot 



# Quantumcomputers

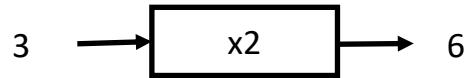
Extra rekenkracht (voor sommige problemen)

# Toepassingen van quantum technologie

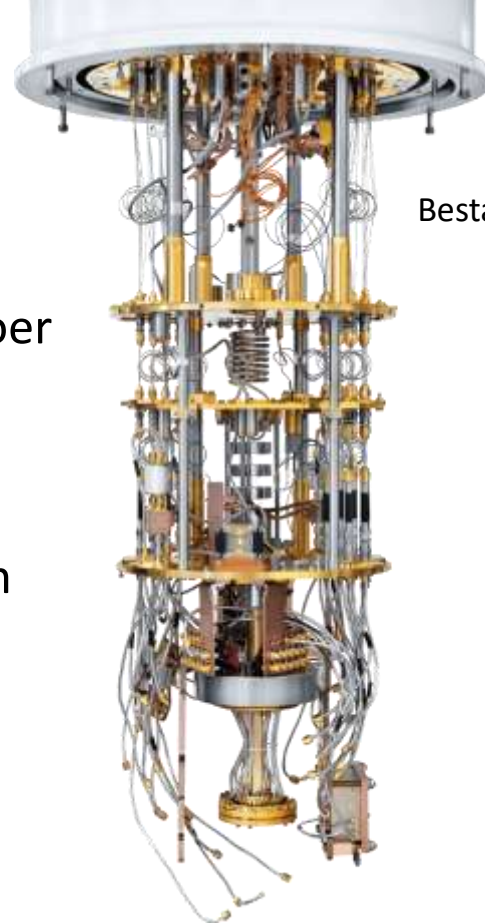


# Quantumcomputer

- Elk computerprogramma vertaalt invoer naar uitvoer



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



Bestaan al op kleine schaal

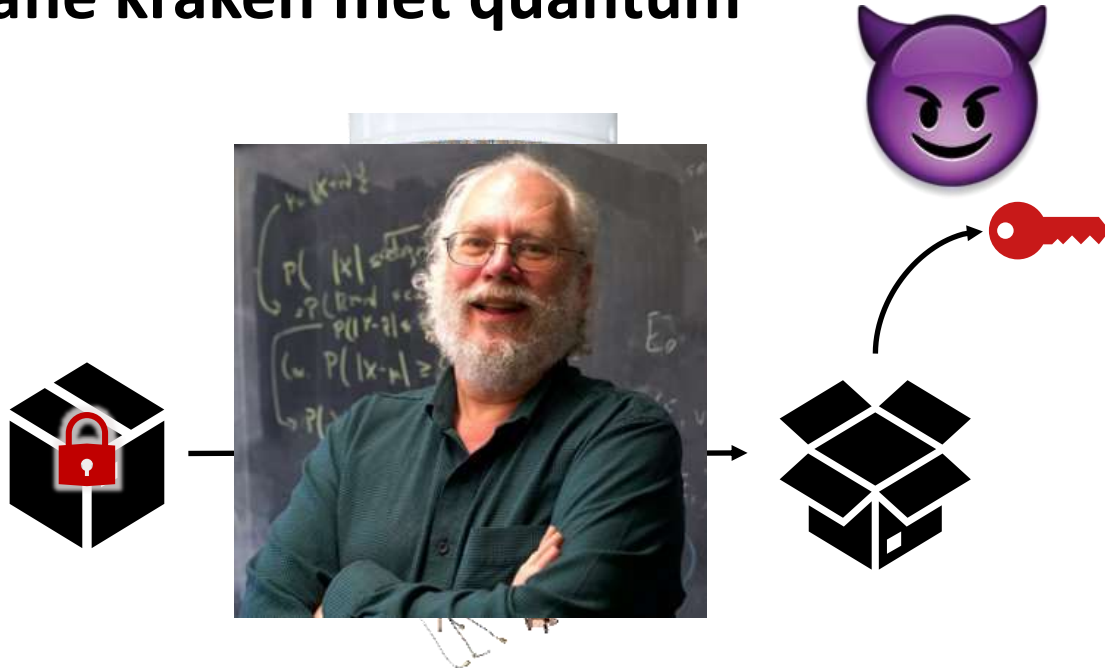


# Maar hoe werkt dat dan?

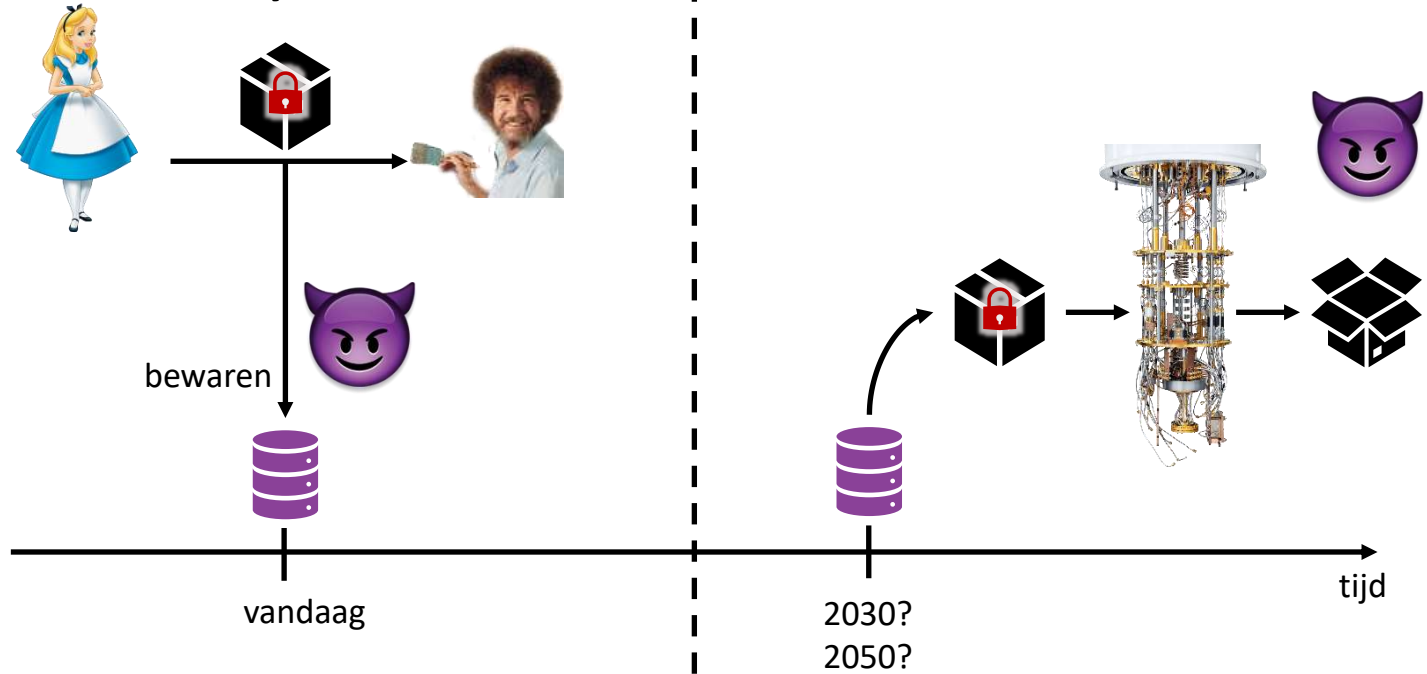
- *Superpositie*: alsof het deeltje in meerdere staten tegelijk is
- Een berekening hierop is alsof je alle mogelijke oplossingen voor een probleem tegelijk kan proberen
- **Maar**: je krijgt ook alle antwoorden in superpositie
- Een goed quantum algoritme zorgt ervoor dat goede oplossingen elkaar versterken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



# Cryptografie kraken met quantum



# Nu bewaren, later kraken

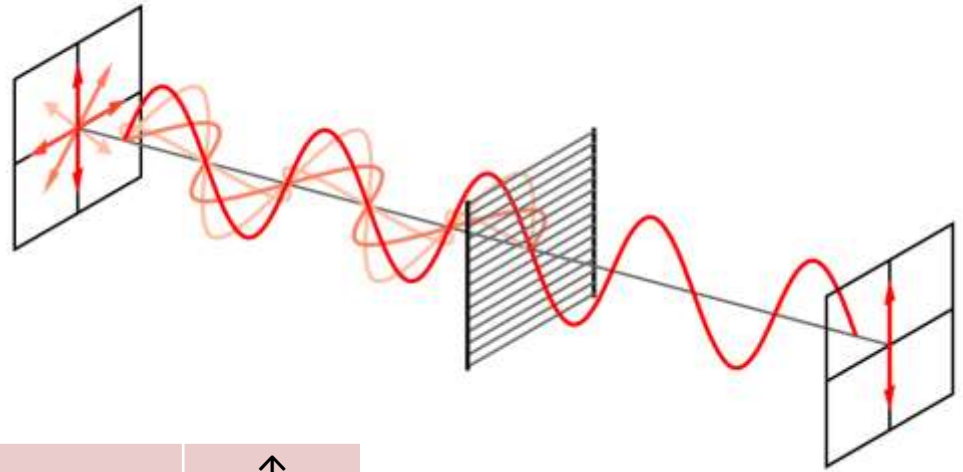


# Quantum communicatie

Detectie van afluisteraars

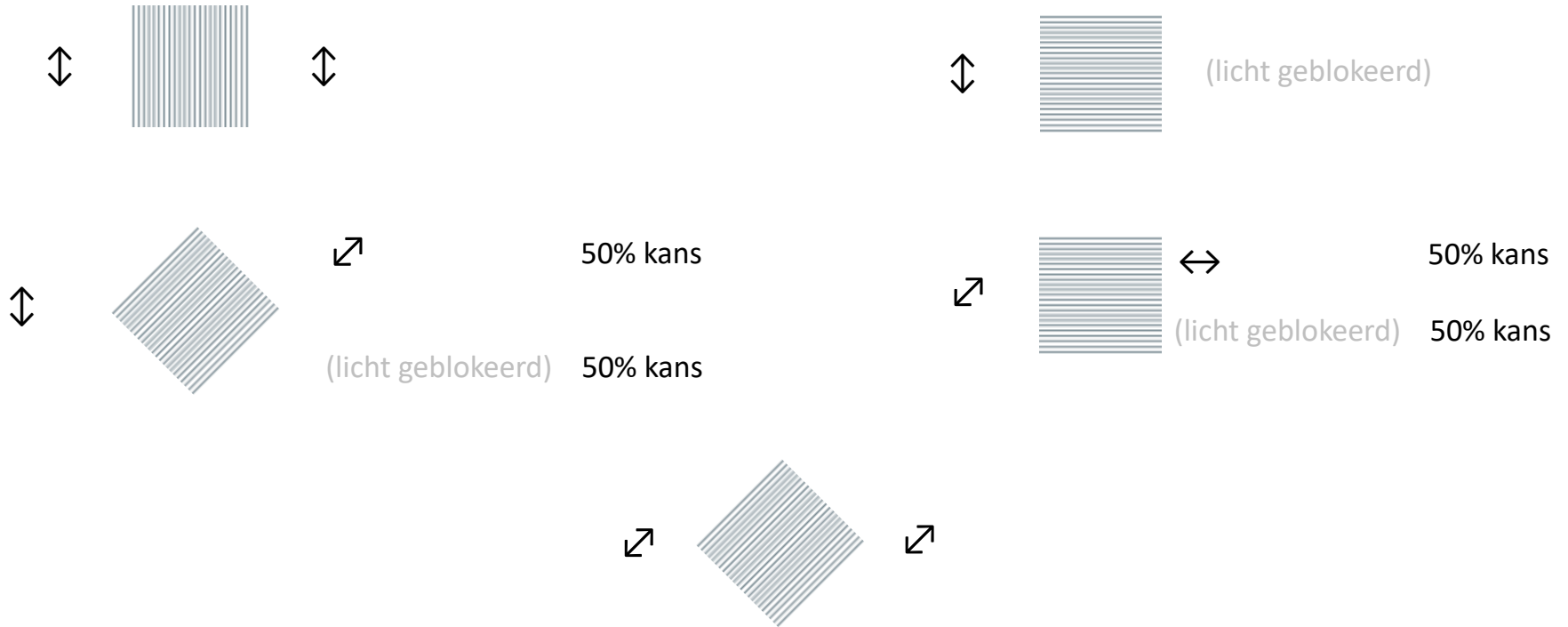
# Gepolariseerd licht

- Licht heeft polarisatie:  
dit is een quantum effect

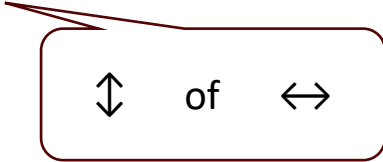


verticaal	$\updownarrow$
horizontaal	$\leftrightarrow$
diagonaal	$\nearrow$
anti-diagonaal	$\nwarrow$

# Polariserende filters



# Afluisteraars detecteren



# Afluisteraars detecteren



↕ of ↔

Dat klopt niet: we worden afgeluisterd!

↕ of ↔

Ik zag ↔



# Quantum Key Distribution (quantum sleutel uitwisseling)

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

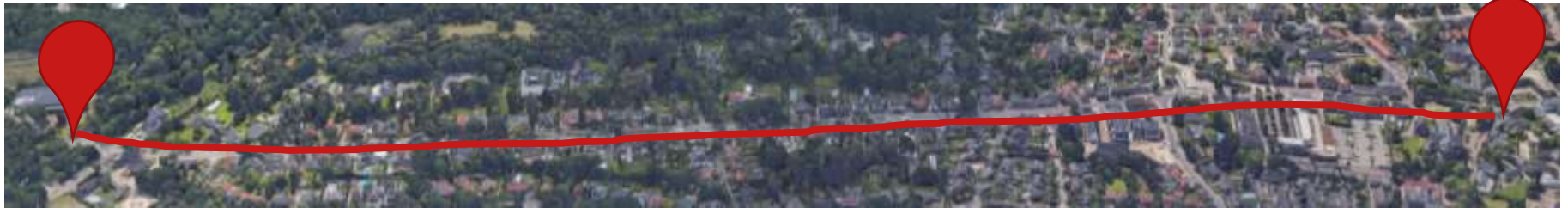
# Waalre

De huidige opstelling

# De opstelling



# De opstelling

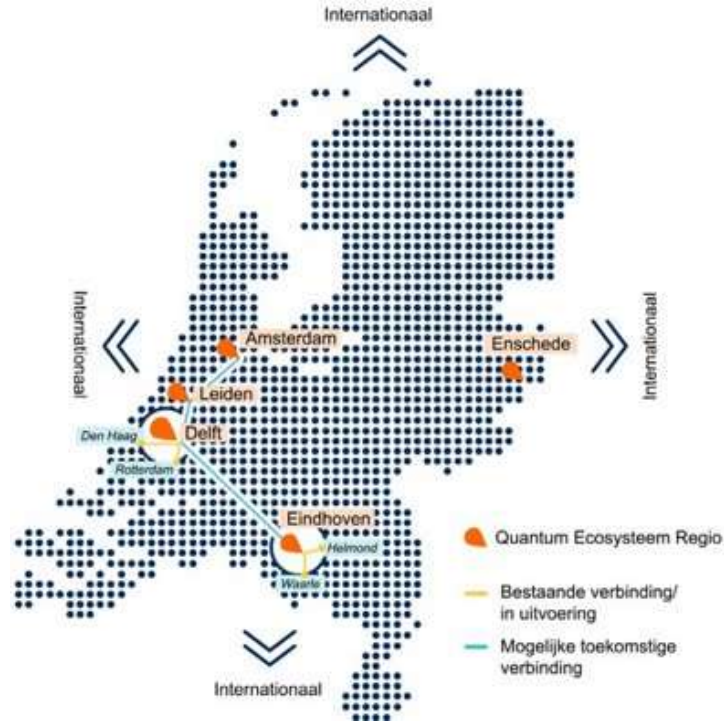


1.5 km

# Eindhoven testomgeving – fase 2



# Eindhoven testomgeving – fase 3



# Phase 4?



# Quantum communicatie team TU/e



**Simon Rommel**  
Quantum Secure Comms.  
Quantum Testbed



**Chigo Okonkwo**  
Quantum Secure Opt.  
CV QKD Systems



**Idelfonso Tafur Monroy**  
Quantum Secure Comms.  
DV QKD Systems



**Boris Škorić**  
Theory and  
Security proofs



**Andreas Hülsing**  
Post-Quantum  
Cryptography



**Kathrin Hövelmanns**  
Post-Quantum  
Cryptography



**Diana Patterson**  
Project Management



**Gijs Hijmans**  
Program Manager  
Quantum Technologies



**Sebastian Verschoor**  
QKD testbed  
KMS & Key Relay



**Bruno Cimoli**  
Quantum Testbed  
Systems Engineering



**Hui Lui**  
Quantum Secure Comms.  
DV/MDI-QKD Systems



**Aaron Albores-Mejia**  
Integrated QKD  
Systems Engineering



**Sjoerd van der Heide**  
QKD Systems  
Systems Engineering



**Alexander Grebenchukov**  
DV-QKD Systems



**Mehmet Temel**  
Quantum Information Security



**João Frazão**  
CV-QKD Systems



**Denis Fatkhiev**  
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



**Oumayma Bouchmal**  
Quantum Secure Comms.  
Quantum ML



**Daniel Lawo**  
Quantum Secure Comms.



**Abraham Cano Aguilera**  
Quantum Secure Comms.



**Xavi Arnal i Clemente**  
Quantum Secure Comms.



**Raphael Frantz**  
Quantum Secure Comms.



# Demonstratie: quantum beveiligde videoverbinding

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

