QUANTUM AUTHENTICATION AND COMMUNICATION

PEPIJN PINKSE

Symposium Quantum Technology 13 May 2024

Quant Quantum Nanotechnology Twente

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

OUTLINE

Quantum Authentication

Quantum Communication

Secure Quantum Information Processing

Quant Quantum Nanotechnology Twente

Two ways to secure access:

1) Code keys

Risc of leaking out

2) Physical keys

Risc of copying

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Physical Unclonable Functions

Quantum Nanotechnology Twente

Properties of PUFs

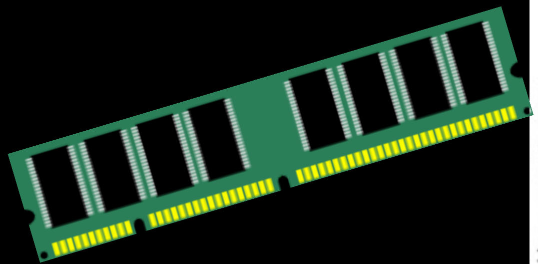
1) Easy to evaluate
2) Unclonable: manufacturing has uncontrollable aspects
3) Quantum Readout* → Properties can be made public; it can still not be copied!

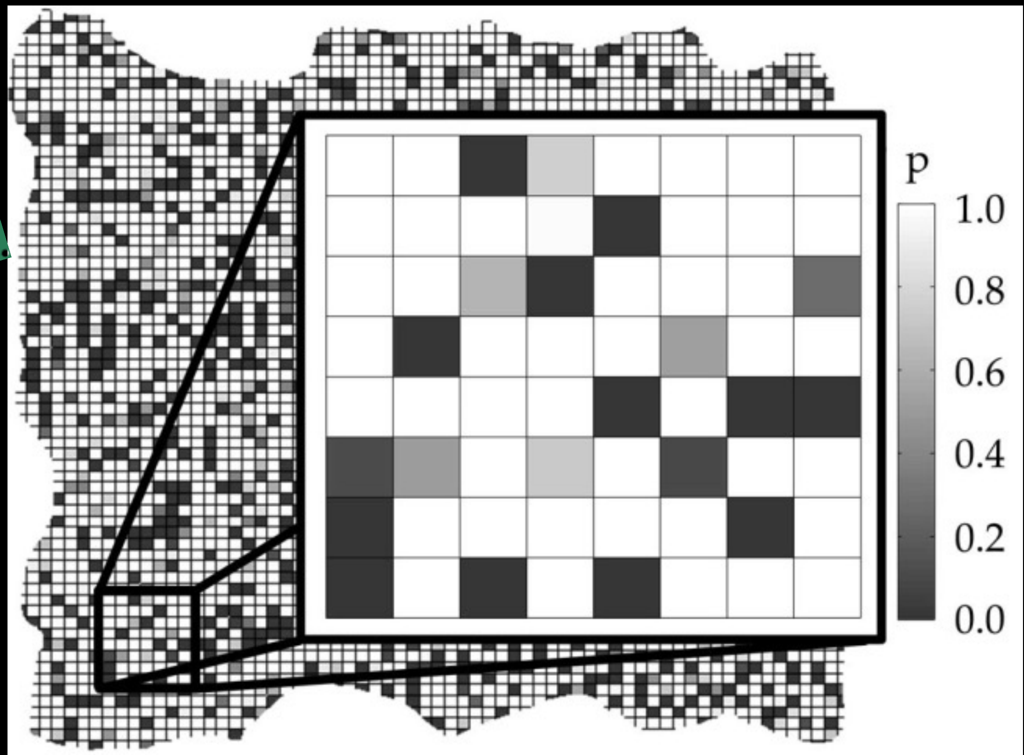
*proposed by Boris Skoric

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Example: SRAM Fingerprint

Quantum Nanotechnology Twente





Weakness: emulation

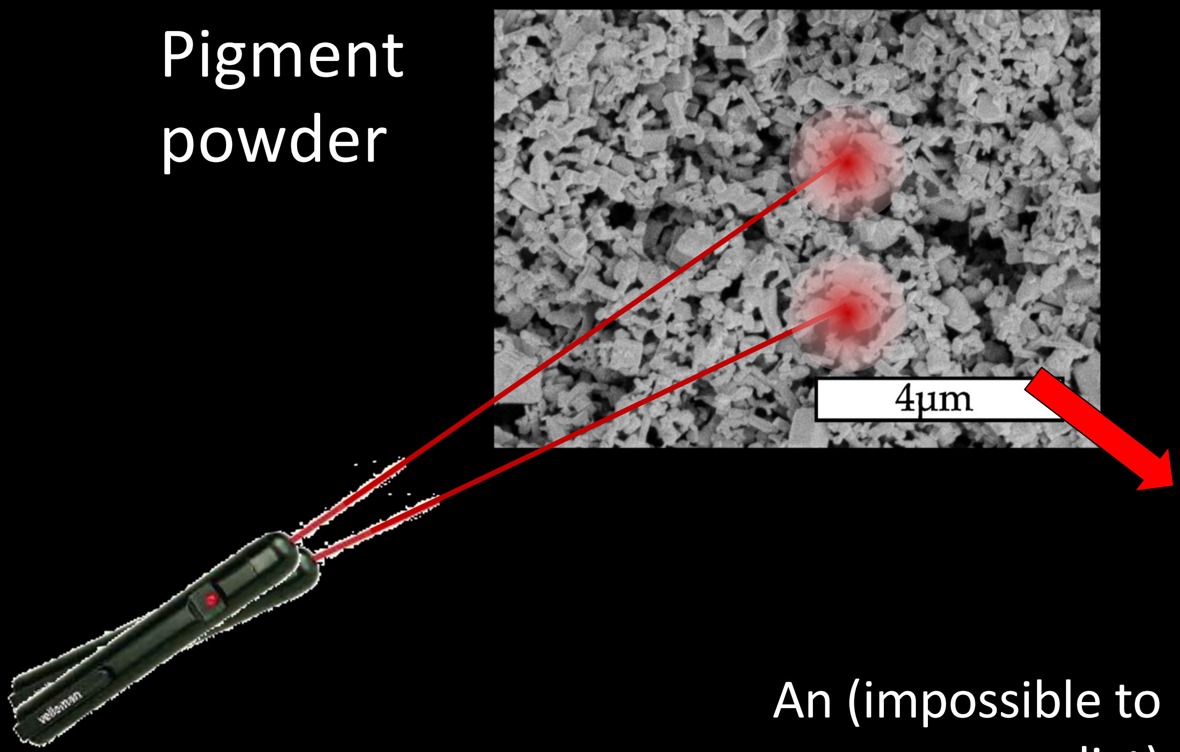
Holcomb *et al.*, IEEE Trans. Comp. **57** (2008)

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

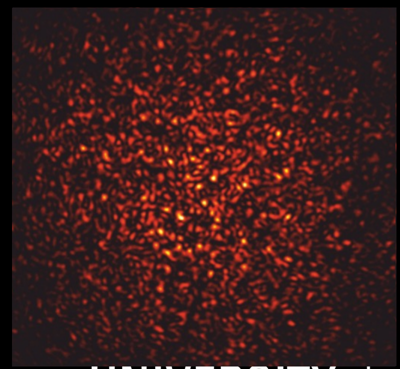
Speckle Authentication

Quant Quantum Nanotechnology Twente

Pigment powder



An (impossible to predict) speckle pattern

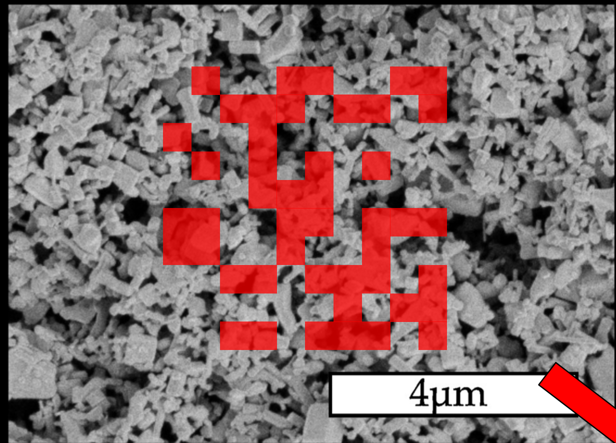


UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

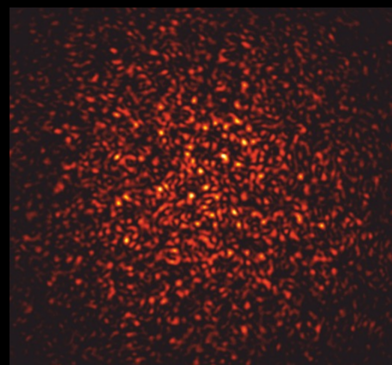
Speckle Authentication

Quant Quantum Nanotechnology Twente

Pigment powder



Yet another impossible to predict speckle pattern

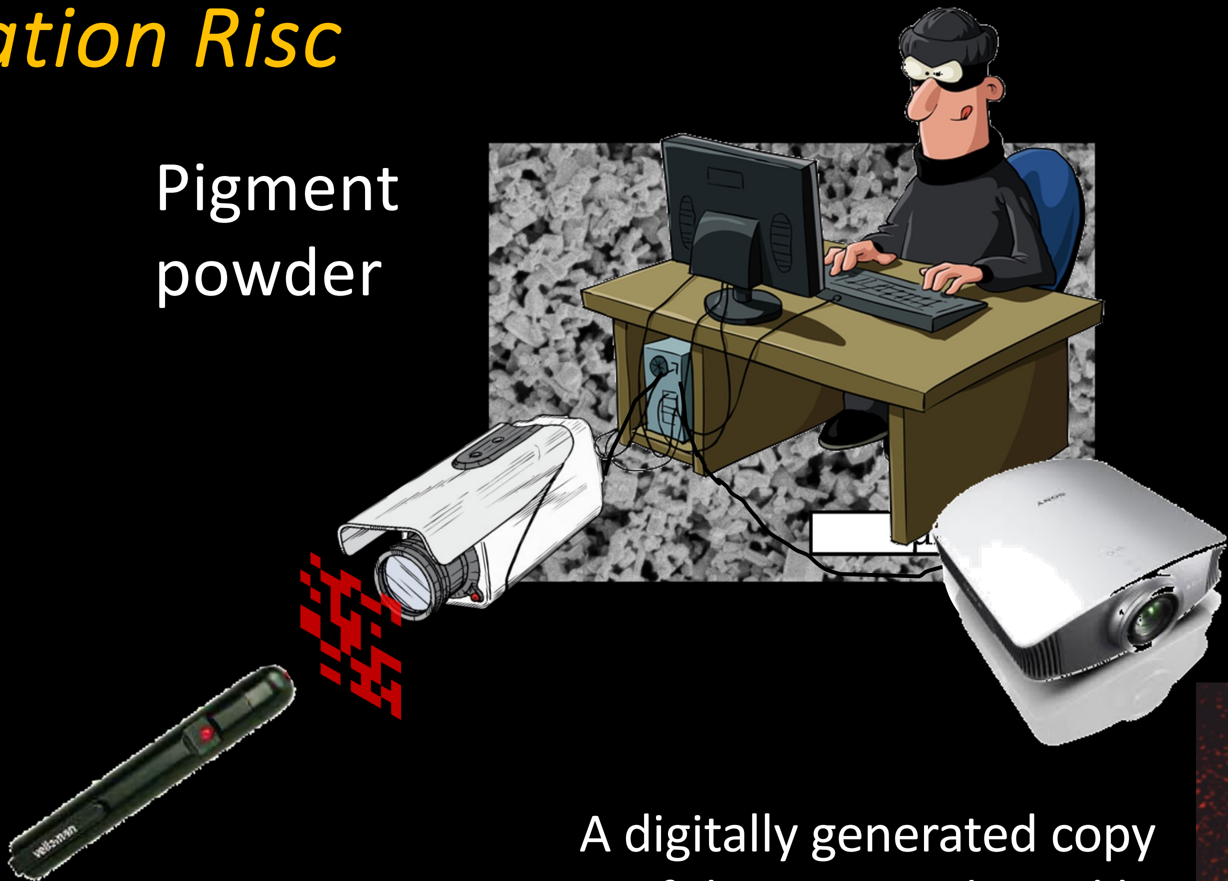


UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

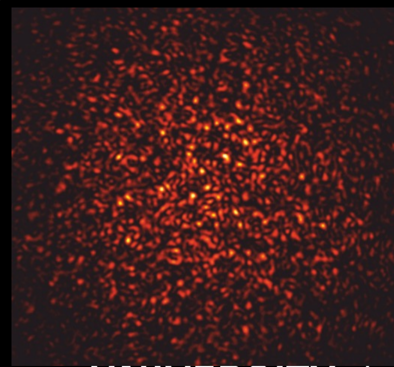
Emulation Risc

Quant Quantum Nanotechnology Twente

Pigment powder

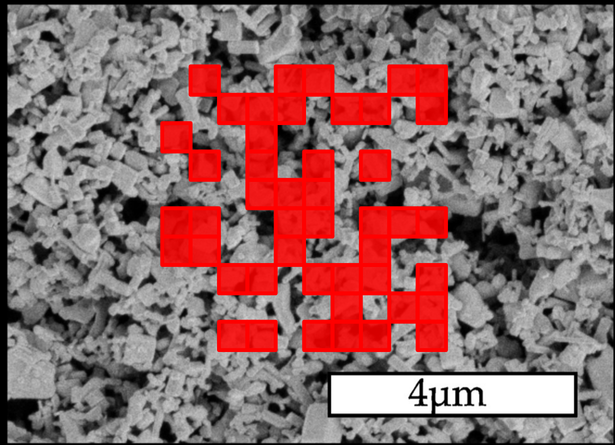


A digitally generated copy of the expected speckle pattern



UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Speckle Authentication with little Light

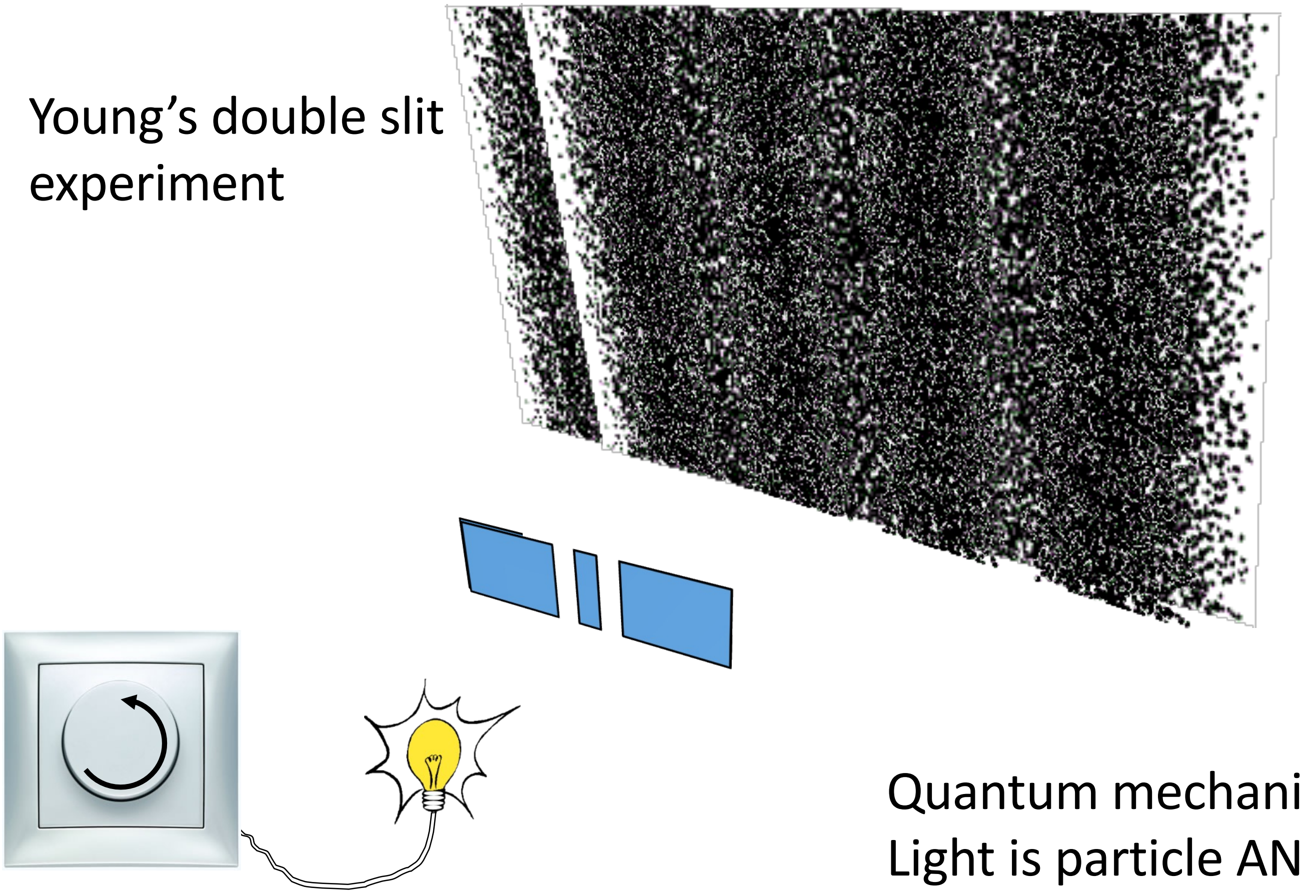


A small number of photons yields only little information about an illumination pattern

Yet every photon is spatially distributed in the same illumination pattern

Wave-Particle Duality

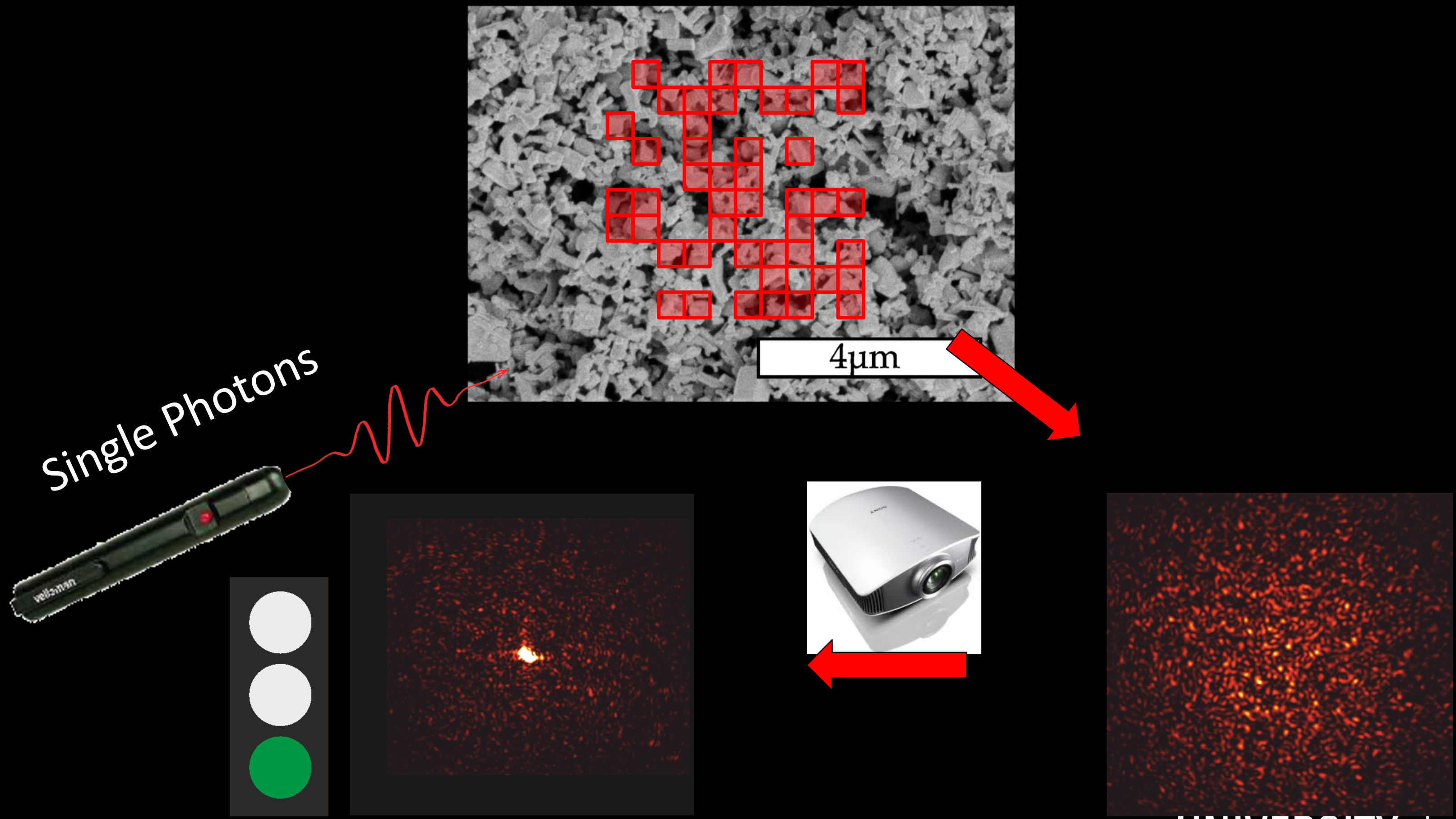
Young’s double slit experiment



Quantum mechanics:
Light is particle AND wave

Reverse Projection

Quant Quantum Nanotechnology Twente



UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Quantum-Secure Authentication

Quant Quantum Nanotechnology Twente

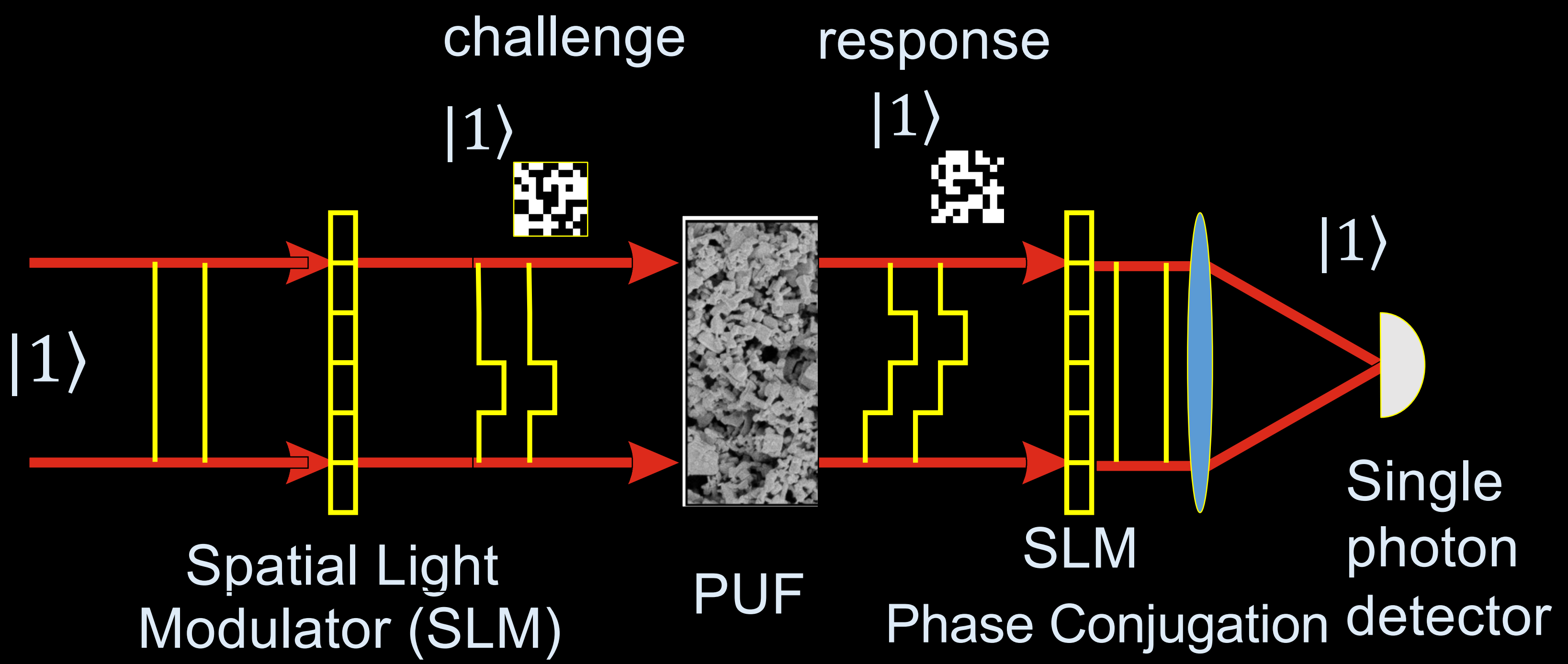
UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Quantum-Secure Authentication

https://vimeo.com/145129613

Goorden *et al.*, *Quantum-Secure Authentication*, Optica **1,** 421 (2014)

Quantum Readout of hardware keys (PUFs)

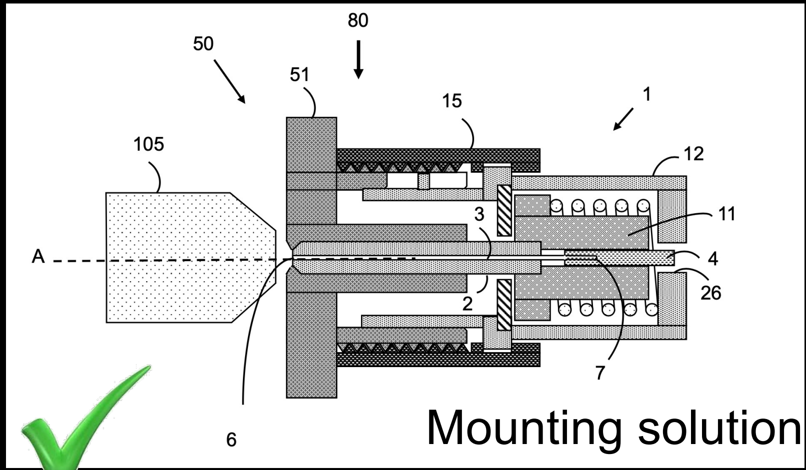


Goorden *et al.*, *Quantum-Secure Authentication*, Optica **1,** 421 (2014)

MESA+ INSTITUTE

Quantum-Secure Authentication

Temperature - insensitive materials



Proof-of-principle demonstration

Applications?

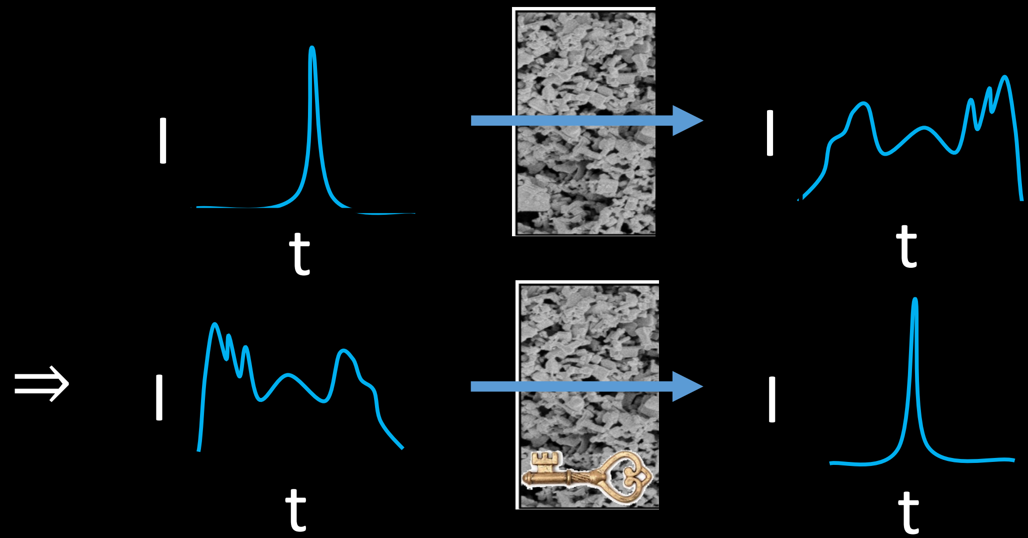
Goorden *et al.*, Optica **1,** 421 (2014); https://vimeo.com/145129613

MESA+ INSTITUTE

Remote Key Readout

Quant Quantum Nanotechnology Twente

Pulse shaping to temporally focus through a medium that distorts temporal wavefronts.

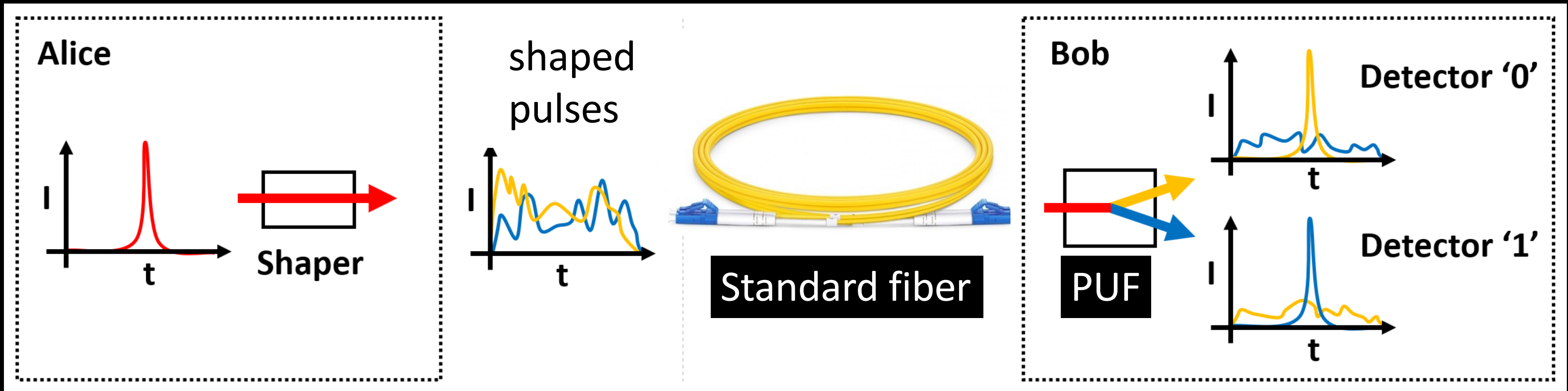


UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Quantum Nanotechnology Twente

Spatial-Temporal Quantum Authentication

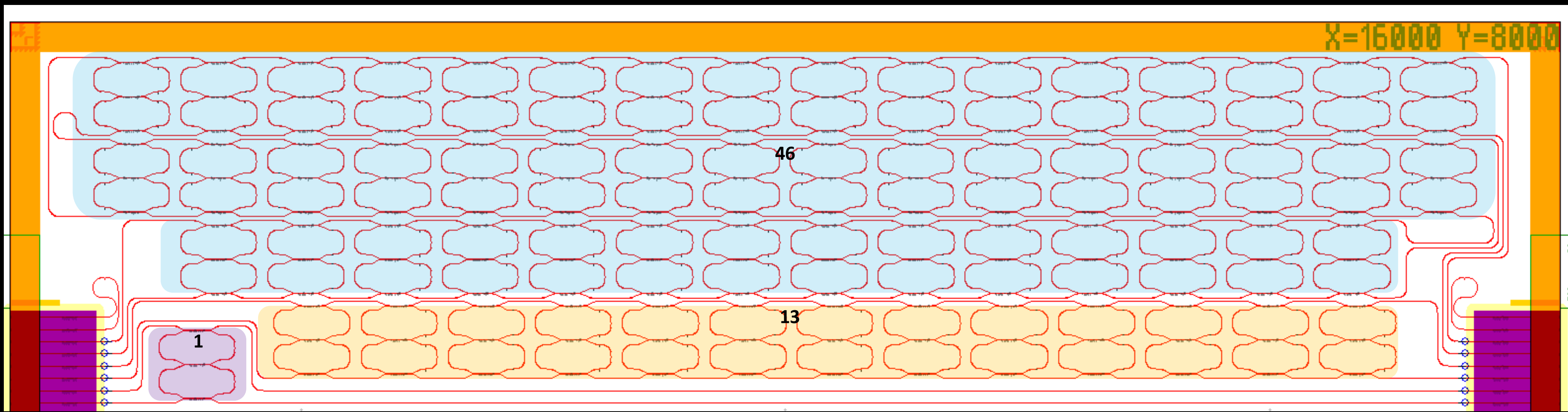
- PUF with two outputs: binary communication.
- Only PUF owner can decipher communication.
- Eavesdropping not possible with weak light

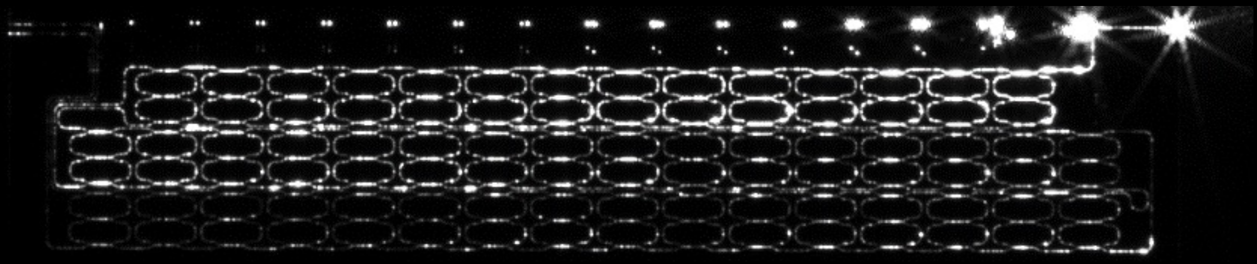


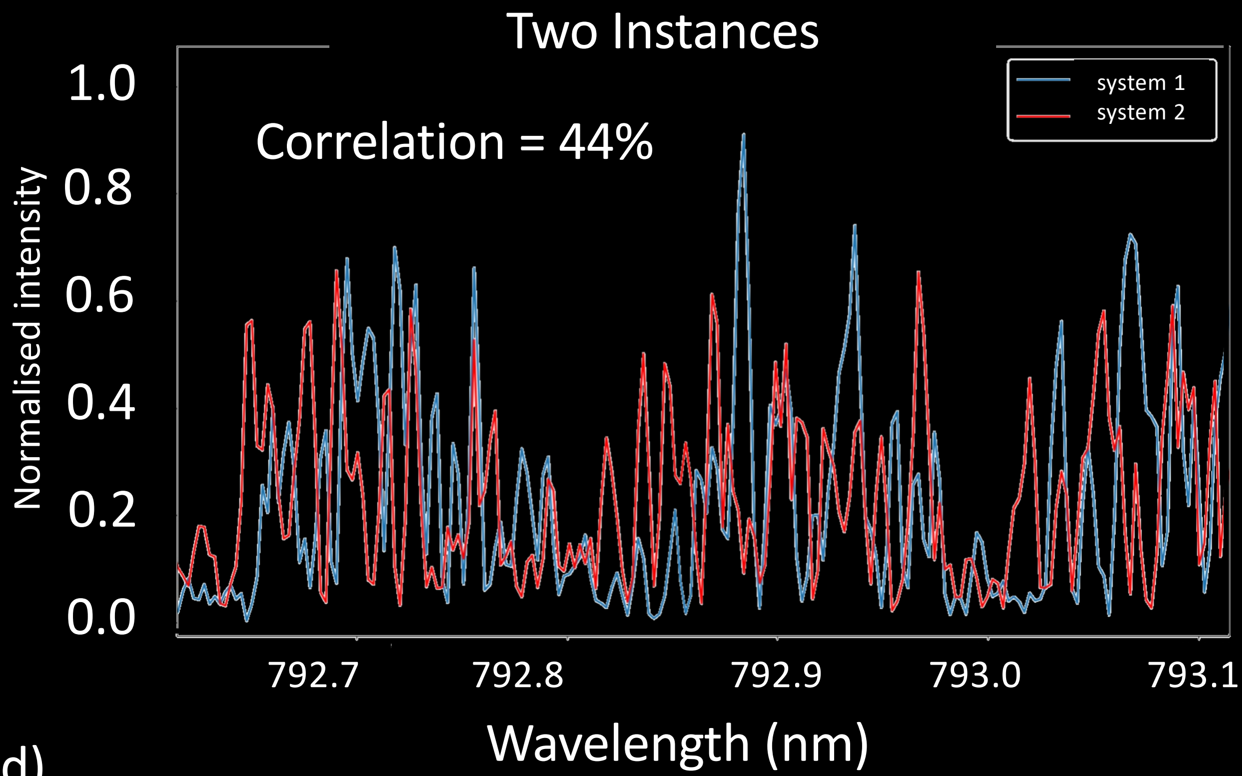
UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Physical-Key-based Quantum Authentication

The ring resonators are designed with different sizes
➔ Rings all have different sets of resonant frequencies







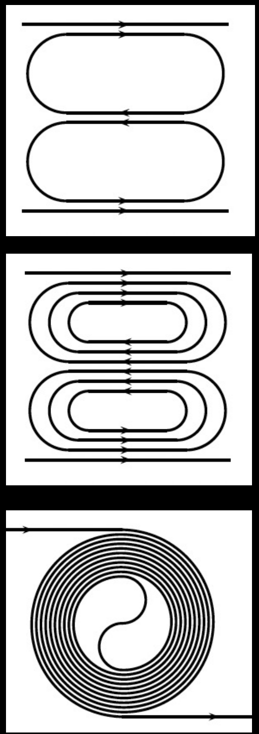
Quant Quantum Nanotechnology Twente

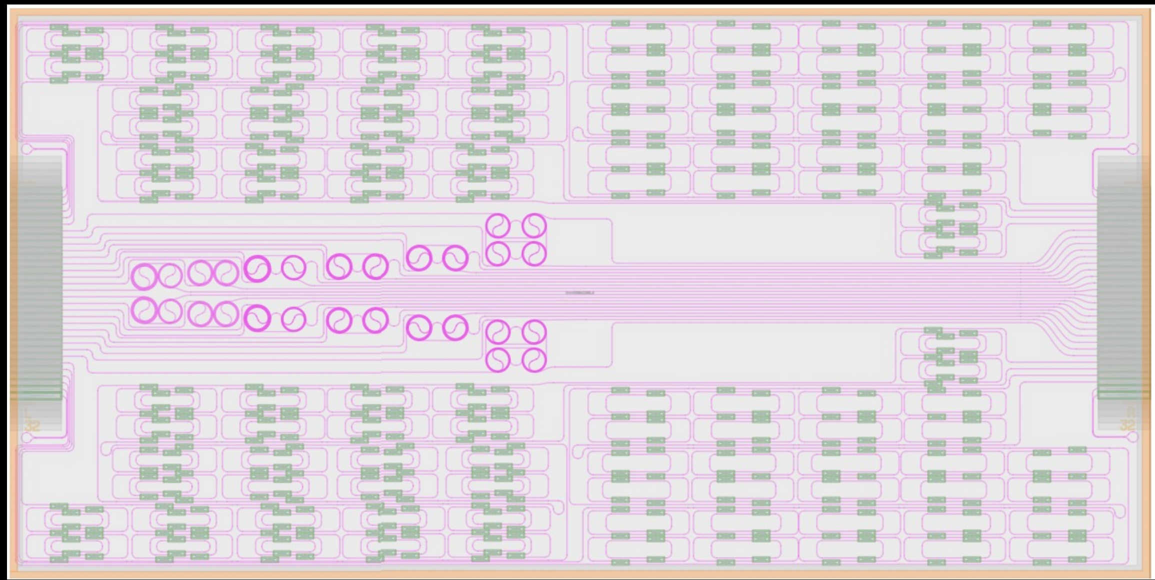
(unpublished)

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Temporal PUFs

Quantum Nanotechnology Twente





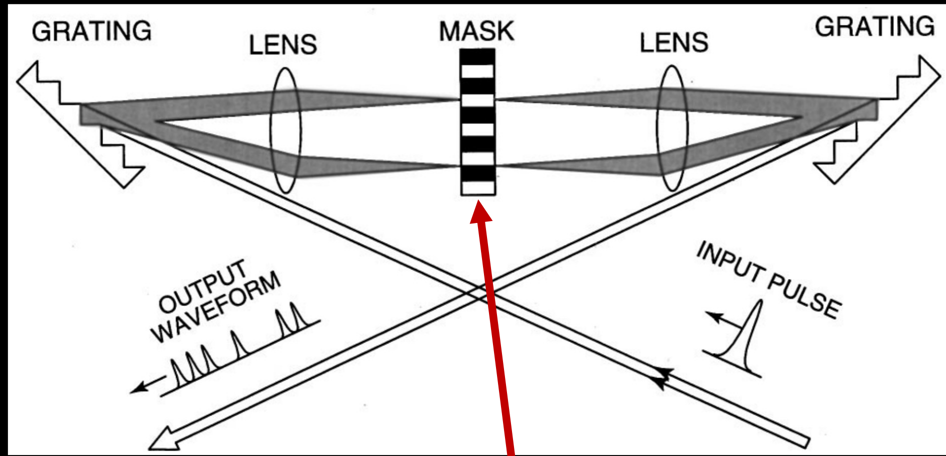
New Chip - PUF designs targeted to give more complexity using a smaller footprint

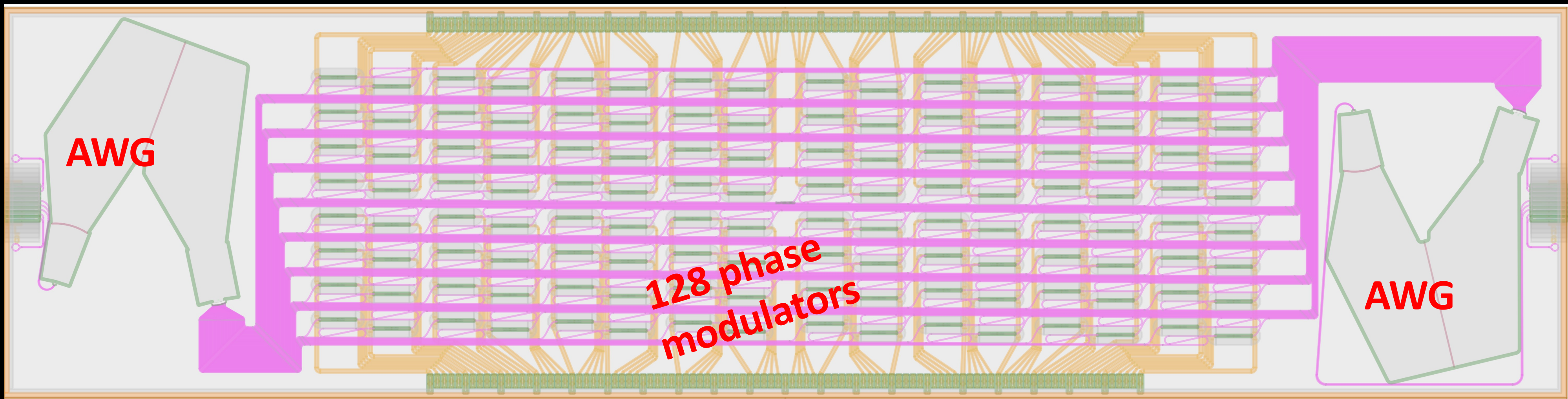
UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Integrated Pulse Shaper Design

Quantum Nanotechnology Twente

Standard bench top configuration:





OUTLINE

Quantum Authentication

Quantum Communication

Secure Quantum Information Processing

Quantum Communication

Quant Quantum Nanotechnology Twente

Motivation: A sufficiently powerful quantum computer can break most standard asymmetric key systems (via Shor algorithm that can efficiently find prime factors on a Quantum Computer)

Basis principle: No-cloning theorem

<u>Post-Quantum Crypto</u>
(TRL 5 now)

<u>Issues:</u>
- Not provable secure
- Prone to backdoors
- Computational overhead
- Key size

<u>Quantum Communication</u>
-> Quantum Key Distribution (TRL 5 in 2024)

<u>Issues:</u>
- Only key exchange
- Authenticated channels needed
- New infrastructure (dark fibers)
- Scalability and resilience
- Prone to implemenation attacks

Measurement-Device-independent Quantum Communication needs quantum internet

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Post Quantum Crypto

Quantum
Nanotechnology
Twente

Lattice-based cryptography
(e.g. Dilithium, Kyber)

- Efficient, public key, digital signatures
- Large keys needed

Multivariate cryptography
(e.g. SPHINCS+, XMSS, LMS)

- Multipurpose, very efficient for signatures
- Most public-key schemes broken

Hash-based cryptography
(e.g. Rainbow)

- Very efficient, based on hash-functions
- No encryption schemes

Code-based cryptography
(e.g. McEliece, Bike)

- Fast, multipurpose
- Large keys needed

Isogeny-based cryptography
(e.g. SIKE)

- Elliptic-based, smallest key sizes
- Low efficiency

Symmetric-key quantum resistance (e.g. AES, SNOW 3G)

- Already widespread use
- Bigger keys needed

NIST Post-Quantum Cryptography Candidate Cracked
Posted January 24 2023

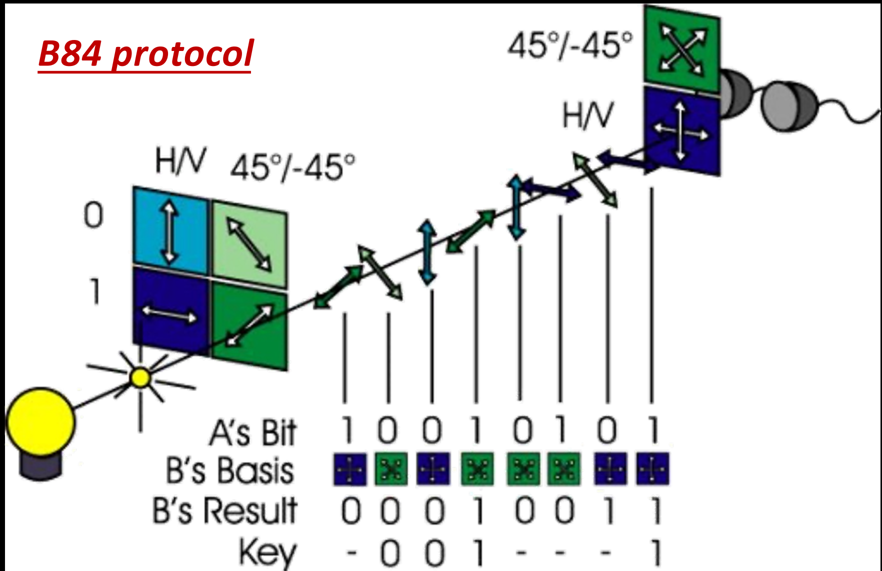
Belgian researchers have cracked the SIKE cryptographic algorithm, a fourth and final-round candidate that the U.S. National Institute of Standards and Technology (NIST) was evaluating for its Post-Quantum Cryptography (PQC) standard.
Wouter Castryck and Thomas Decru, research experts at the KU Leuven research university in Leuven, Belgium, broke the SIKE algorithm in about 62 minutes. They did it using a single core on a six-core Intel Xeon CPU E5-2630v2 at 2.60GHz.

→ PQC is important but has its limitations

→ Quantum Communication offers a solution!

Quantum Key Distribution

Quant Quantum Nanotechnology Twente



After Bennard & Brassard, 1984

1. Alice sends bits according to table, randomly switching basis
2. Bob measures clicks in D1 or D2 choosing a random basis
3. Bob tells Alice his choice of basis (w/o giving the result) over a public channel
4. Alice compares these choices and tells Bob which ones to discard
5. Bob transmits over a public channel a subset of his bits. Alice compares them with her own and performs error analysis
6. If error<25% then there was no eavesdropper, Bob can use the key.

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

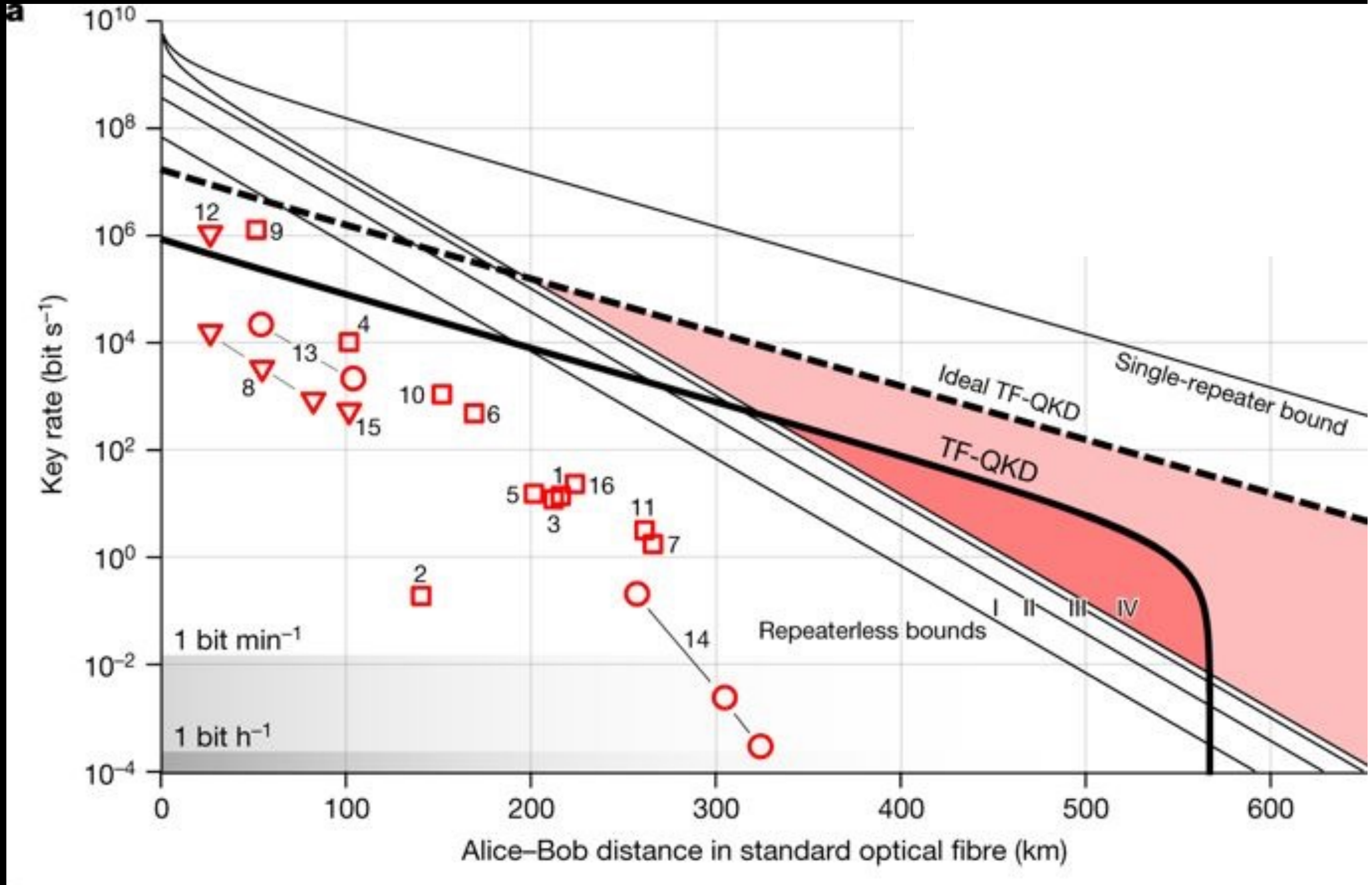
State of the Art Fiber-Based ~~Experiments~~ Products

And many more (>10)

Quantum Key Distribution

Quantum Nanotechnology Twente

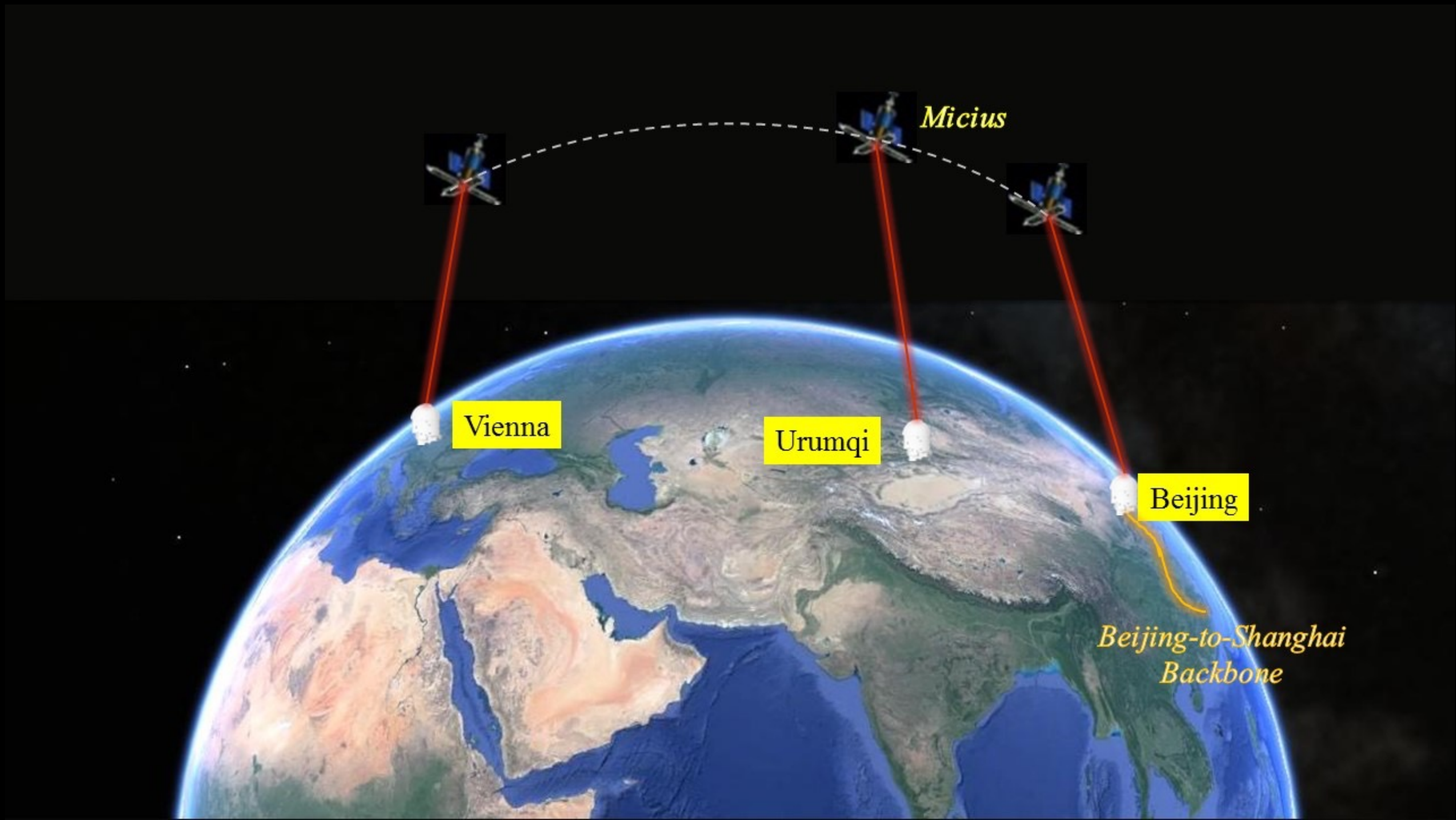
Problem: exponential transmission with distance
How do you compensate for losses?



UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Lucamarini *et al.,* Nature **557**, 400 (2018)

Quantum Key Distribution: in space



Liao *et al.*, Nature 549, 43 (2017)

Quant Quantum Nanotechnology Twente

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Long-Distance Quantum Key Distribution

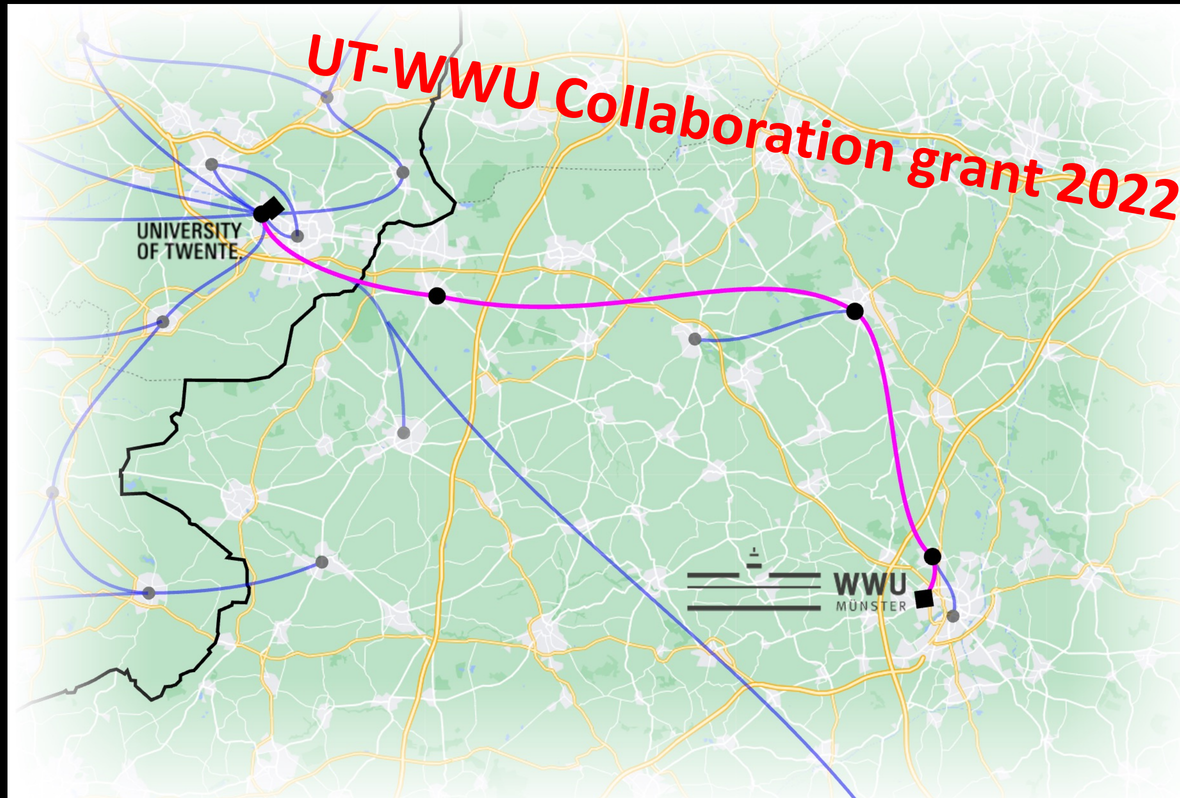
Simplest solution:
'trusted nodes'

Classically store +
repeat the message

The Twente-Münster high-speed Quantum Key Distribution link

Carsten Schuck
(WWU)
Pepijn Pinkse
(UT-MESA+)

WWU
MÜNSTER
UNIVERSITY
OF TWENTE.



The Challenge

Quant Quantum Nanotechnology Twente

UT-WWU Collaboration grant 2022

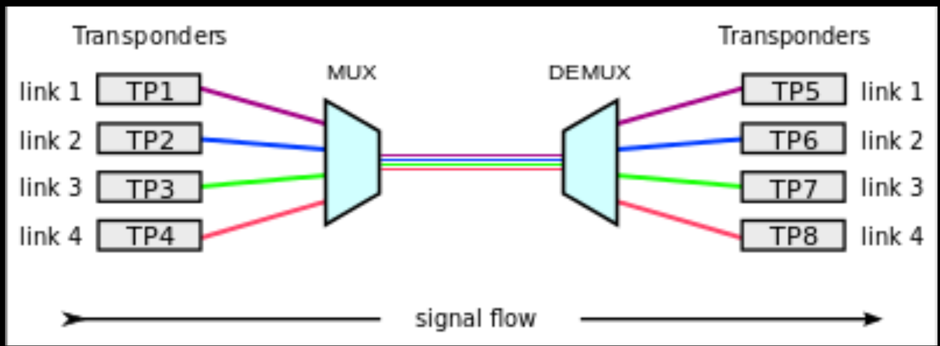
- Provably secure
- Commercial potential
- Slow
- Limited in Range

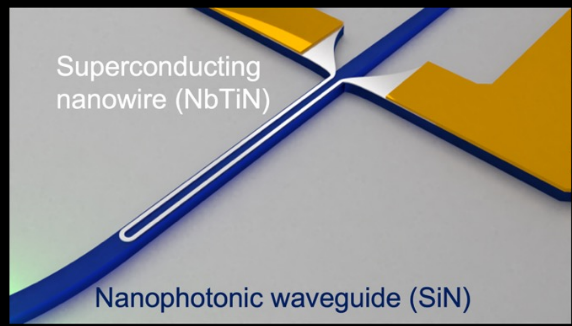
UT

Wavelength Division Multiplexing (WDM)

WWU

Superconducting Single-photon detectors (SNSPD)



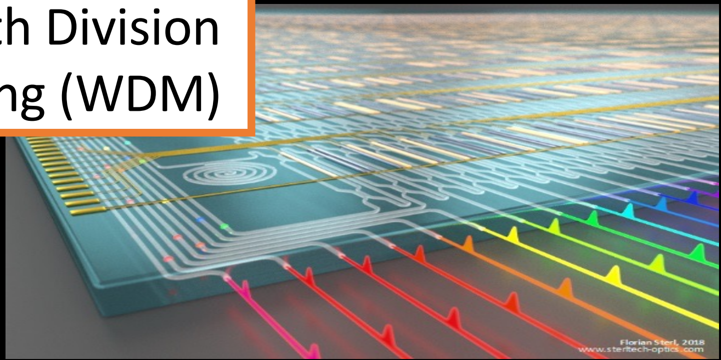


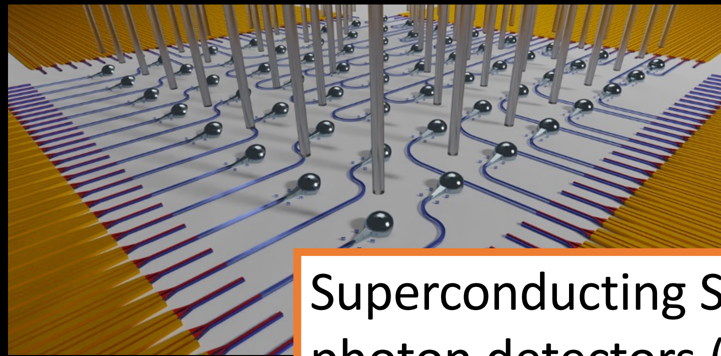
UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Quant Quantum Nanotechnology Twente

The Twente-Münster high-speed Quantum Key Distribution link

Wavelength Division Multiplexing (WDM)





Superconducting Single-photon detectors (SNSPD)

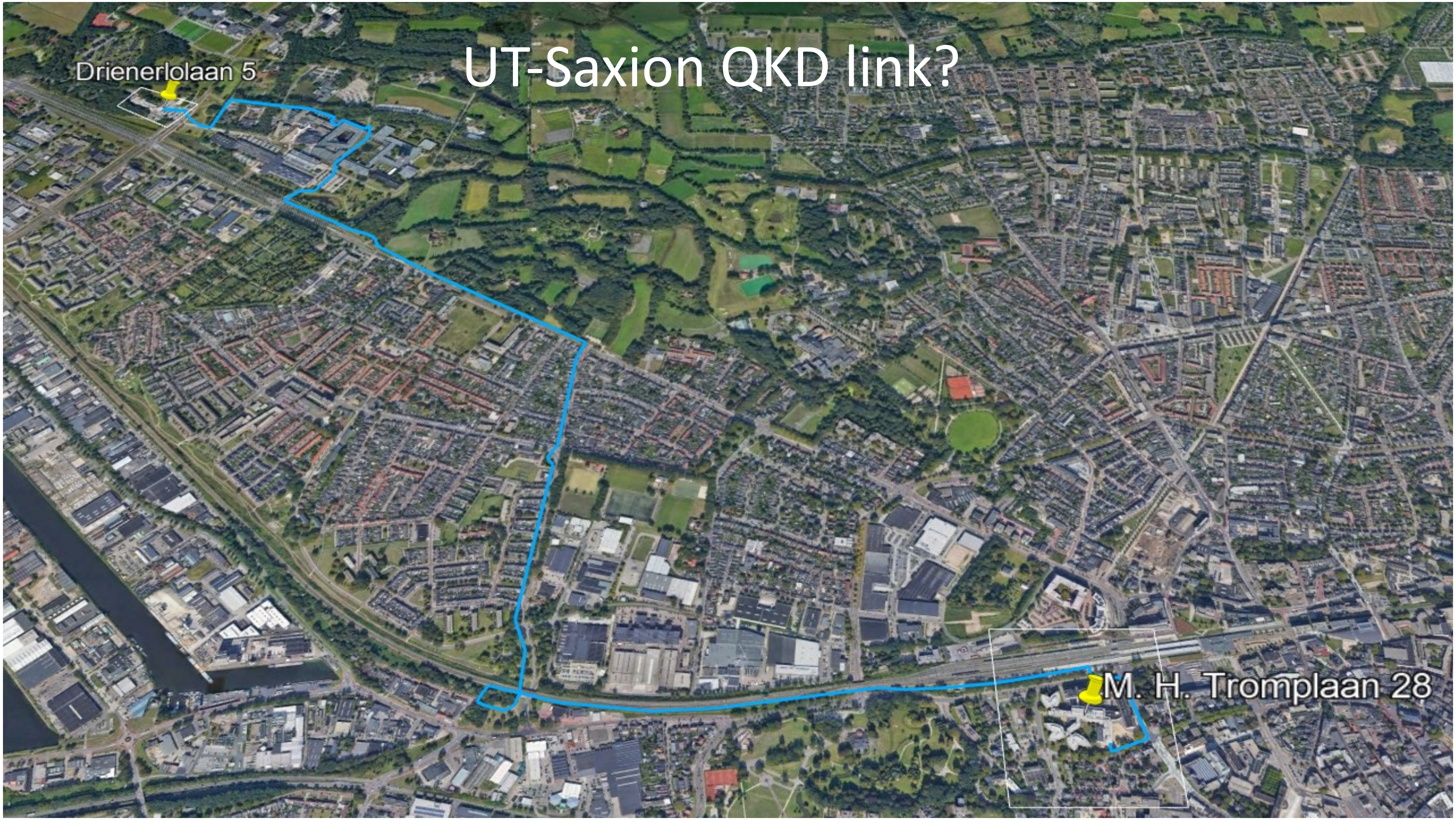
UNIVERSITY OF TWENTE.

WWU MÜNSTER

- Quantum Communication Testbed
- Integrated Photonics Ecosystem

UT-WWU Collaboration grant 2022

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE


UT-Saxion QKD link?
Drienerlolaan 5
M. H. Tromplaan 28

OUTLINE

Quantum Authentication

Quantum Communication

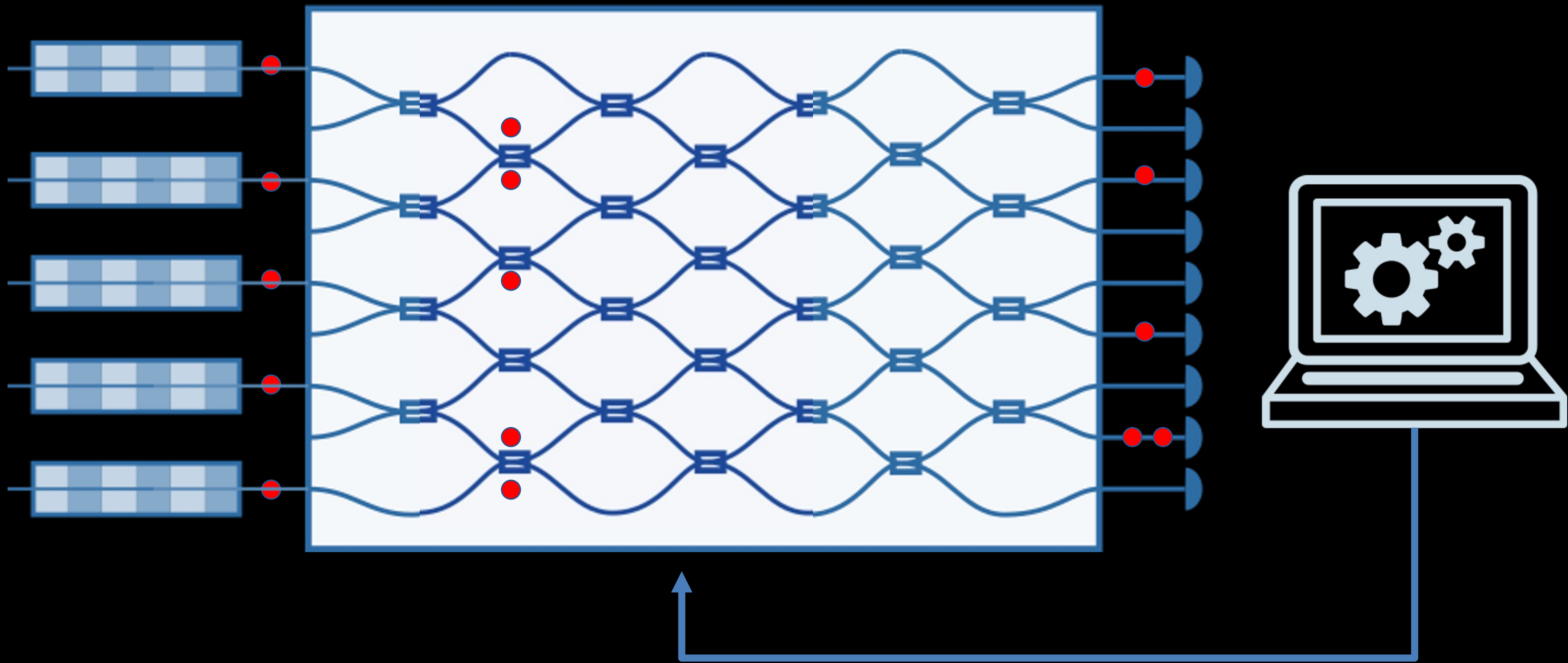
Secure Quantum Information Processing

Integrated Quantum Photonics

Quantum
Nanotechnology
Twente

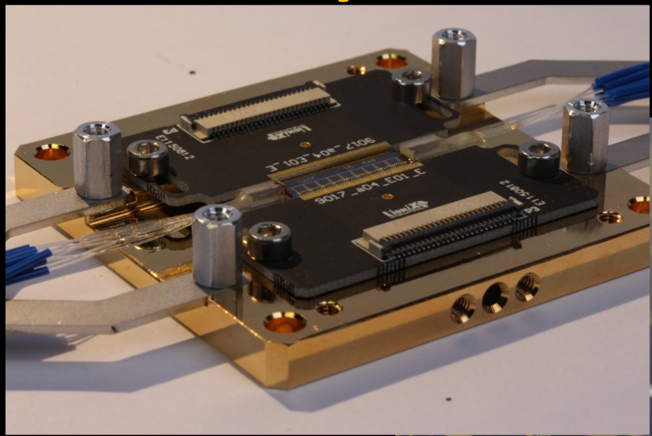
Single-photon
Sources

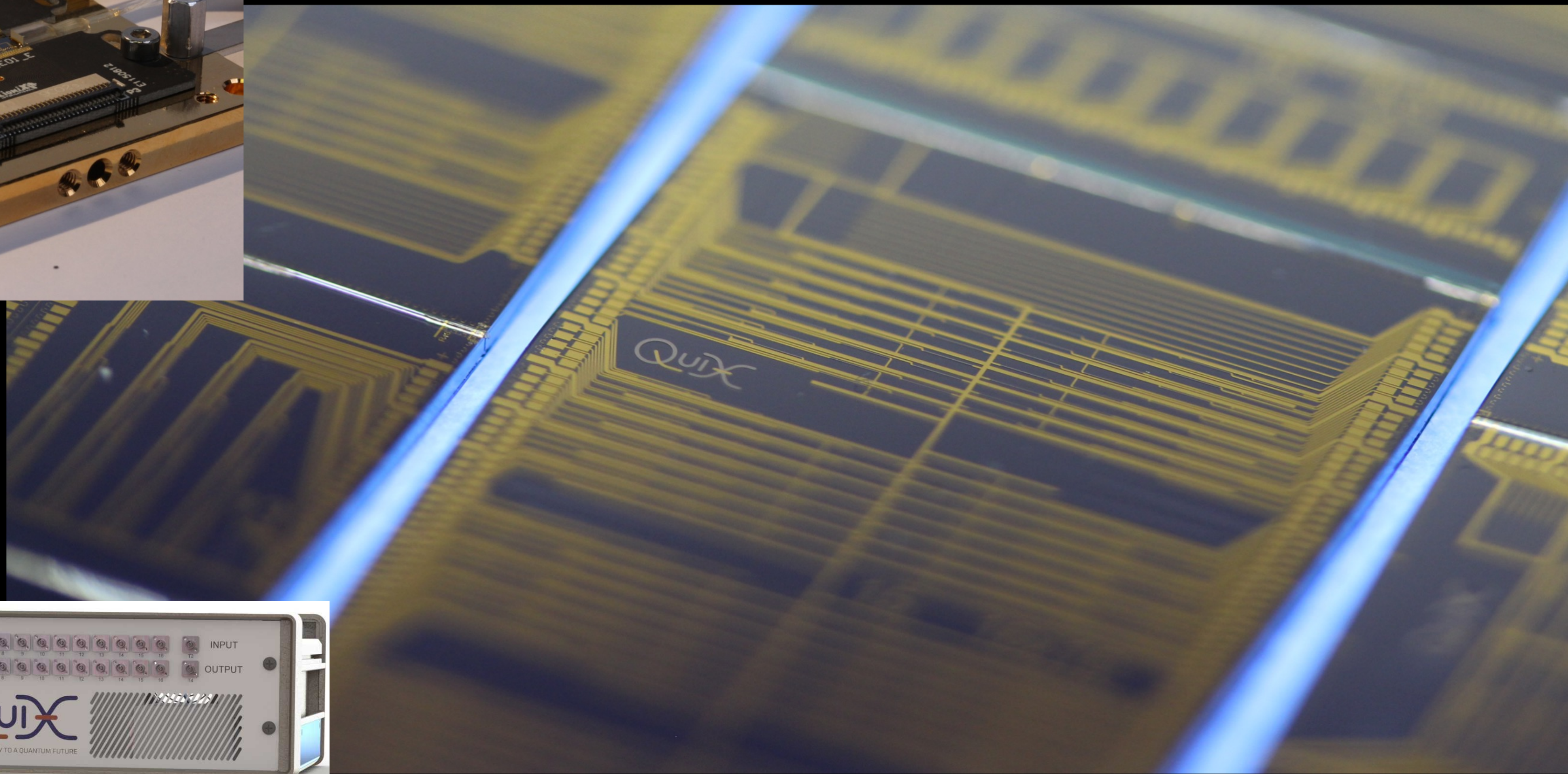
Single-photon
Detectors

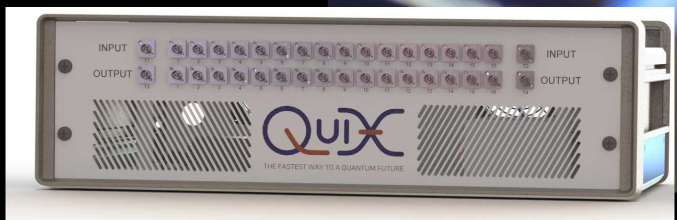


Our photonic quantum computer lab

Quant
Quantum
Nanotechnology
Twente





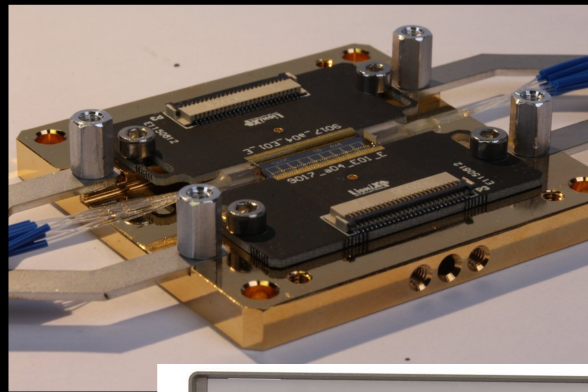


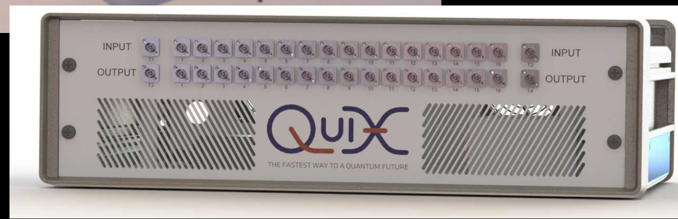
UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Optical Quantum Computing

Quant Quantum Nanotechnology Twente

A programmable multi-channel low-loss interferometer!





1. Quantum photo-thermodynamics (Nature Commun. 2023)
2. Entanglement witness (2112.00067)
3. Analog simulation of classical scattering (2110.04380)
4. Loop quantum gravity on a photonic chip. NPJ Q. Inf. (2023)
5. More to come…

A 20-mode Universal Quantum Photonic Processor: Taballione *et al.,* Quantum (2023)

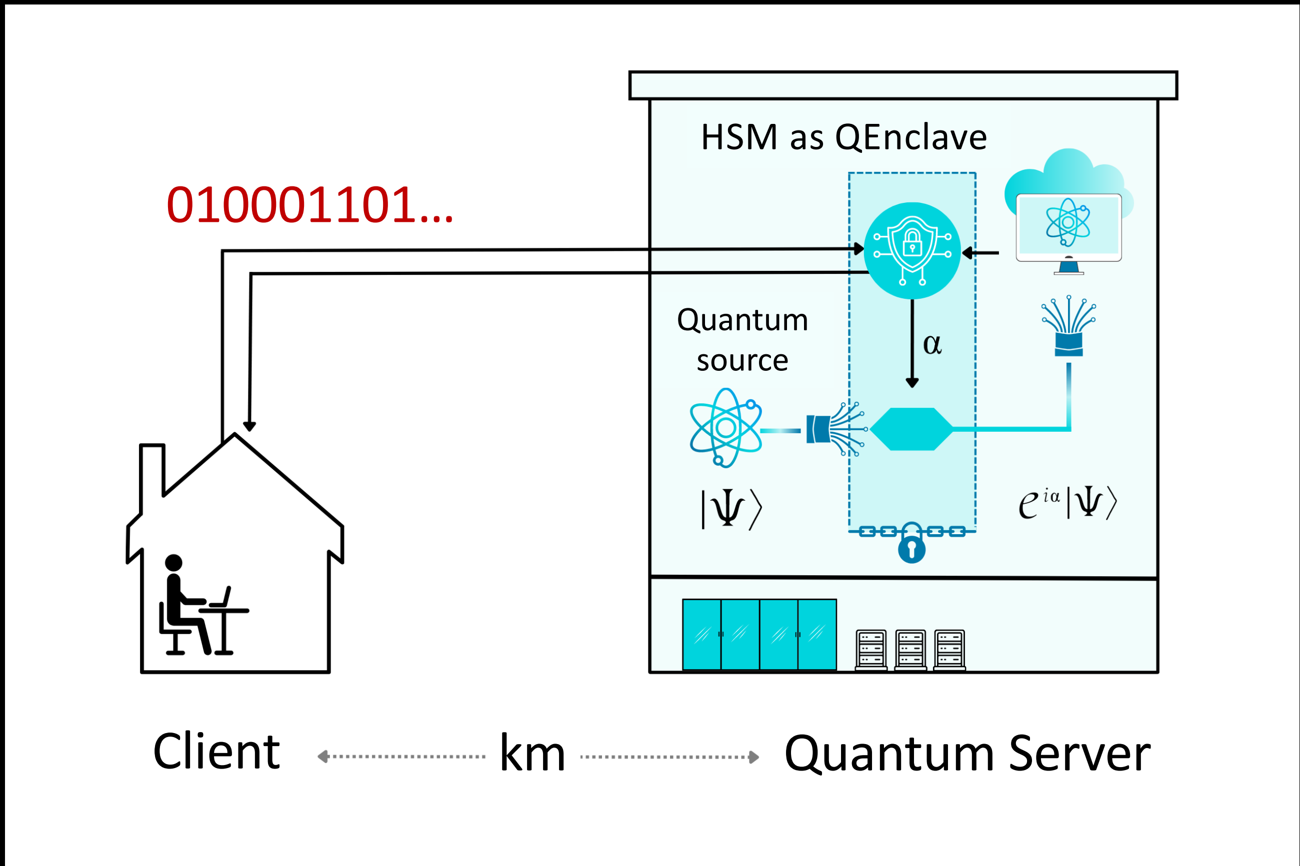
UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Quantum Computing

How to secure access to Quantum Cloud Computer?

Secure Quantum Cloud Computing using an Hardware Security Module (HSM)

Quant Quantum Nanotechnology Twente



QuantERA project by Kashefi, Kaplan, Arapinis, Doosti, Zimboras, ...Pinkse

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE

Summary

Quant Quantum Nanotechnology Twente

Quantum Authentication,
Communication
& Secure Computing!

PhD or Postdoc vacancies!

Thanks to

References

Quantum-Secure Authentication & Communication: Goorden *et al.*, Optica 1 (2014); Uppu *et al.*, QST (2019); Amitonova *et al.*, Opt. Expr. (2020); Škorić *et al.*, Quant. Inf. Proces. (2017); Marakis *et al.*, ArXiv 2212.12495

Integrated Quantum Photonics: Somhorst *et al.*, Nature Commun. 2023; Taballione *et al.*, Quantum 2023; Mater. Quant. Tech. **1**, 035002 ('21); ArXiv 2110.04380, 2110.05099, 2112.00067

UNIVERSITY OF TWENTE. | MESA+ INSTITUTE