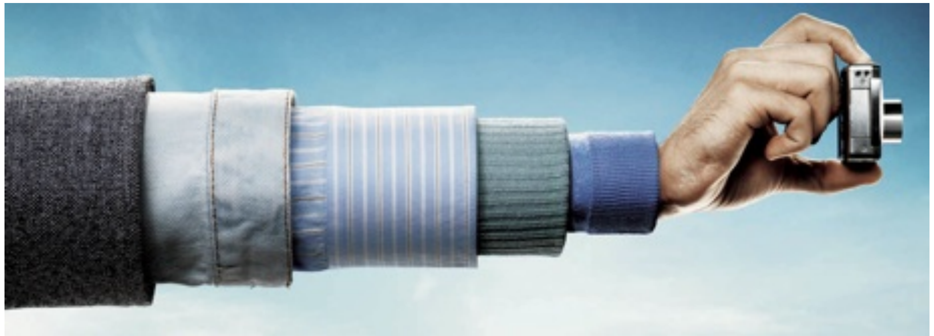
• Key recycling protocols
• Quantum Readout of Physical Unclonable Functions



1 Dec 2020

Boris Škorić

IDIC mini-symposium
on quantum technology and 5G

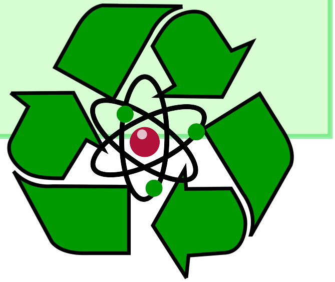
QT/e CENTER FOR QUANTUM MATERIALS AND TECHNOLOGY EINDHOVEN

Beyond Quantum Key Distribution

QKD is already "perfect". What is left to improve?

- Communication efficiency
  - number of qubits
  - number of rounds
  - size of classical messages
- Resilience to leaks & security breaches
- Additional authentication factors
  - hard-to-clone physical objects

Quantum Key Recycling



Alice and Bob already have shared secrets

- Basis choices, hash seed, authentication keys

Reduced need for communication

- no basis-mismatch losses (minor advantage)
- #qubits: same as best-known-QKD
- only two rounds
- option: put entire message in the qubits

} for channels with little photon loss

Keys are re-used in case of no disturbance!

[BBB 1982, Fehr+Salvail 2017, Leermakers+Škorić 2019-2020]

Resilience to leakage & breaches

"Unclonable Encryption"

[Gottesman 2003]

- message encrypted in qubits; basis is shared secret
- after successful decryption, all keys are allowed to leak!

"Vulnerable Sender Unclonable Encryption"

[Leermakers+BŠ 2020]

- Even if cipherstate gets intercepted, sender's keys are allowed to leak.

Option: keys are re-used in case of no disturbance

Disclaimer
Low-loss channels only

Authentication factors

- Digital credential
  - theft may remain unnoticed

- Physical credential
  - theft of object is noticed

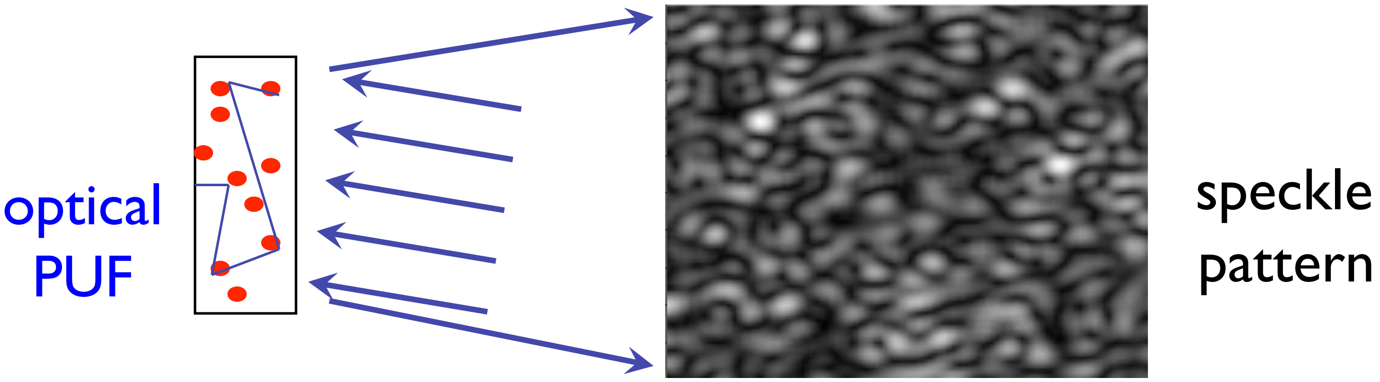
physical object ≠ dongle containing digital key

Unclonable Physical Function

[Pappu et al. 2001]

PUF:

- physical object
- challenge & response
- behaves like a keyed hash function
- making physical clone is difficult



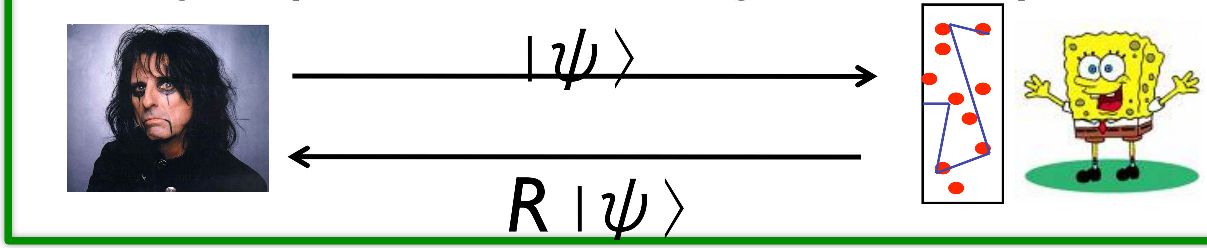
optical PUF

speckle pattern

Quantum protocols with PUFs

[TU Eindhoven + Univ. Twente + Utrecht Univ.]

Single-quantum challenge and response



[Škorić 2009]

Public PUF!

Experimental realisation:
"Quantum Secure Authentication"

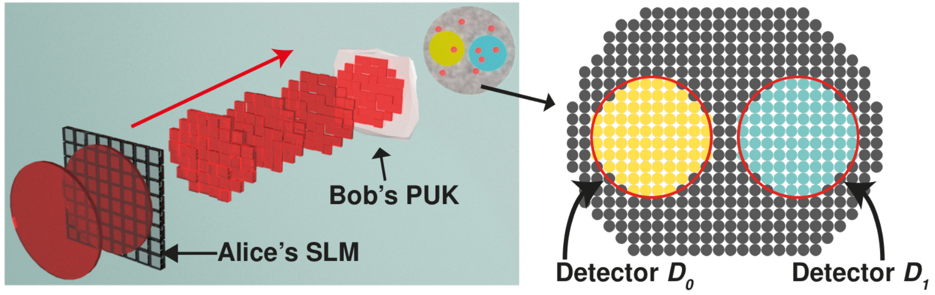
[Goorden et al. 2013]

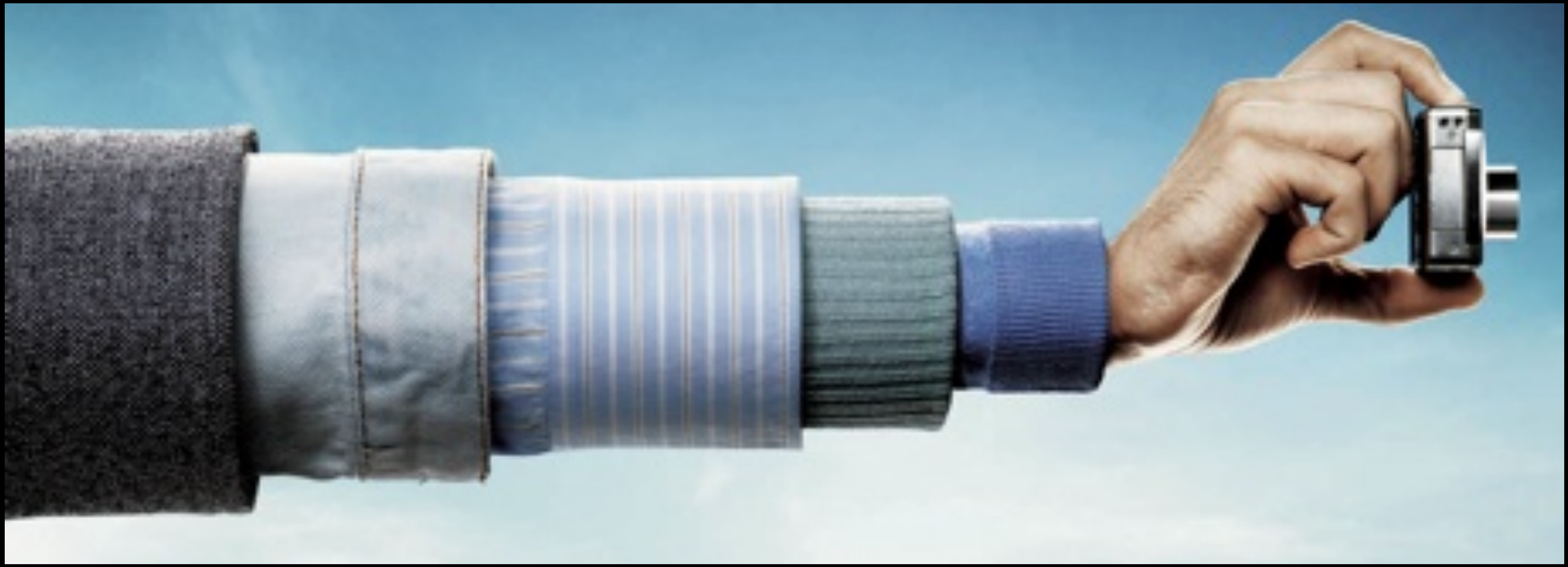
PEAC

PUF-Enabled Asymmetric Communication

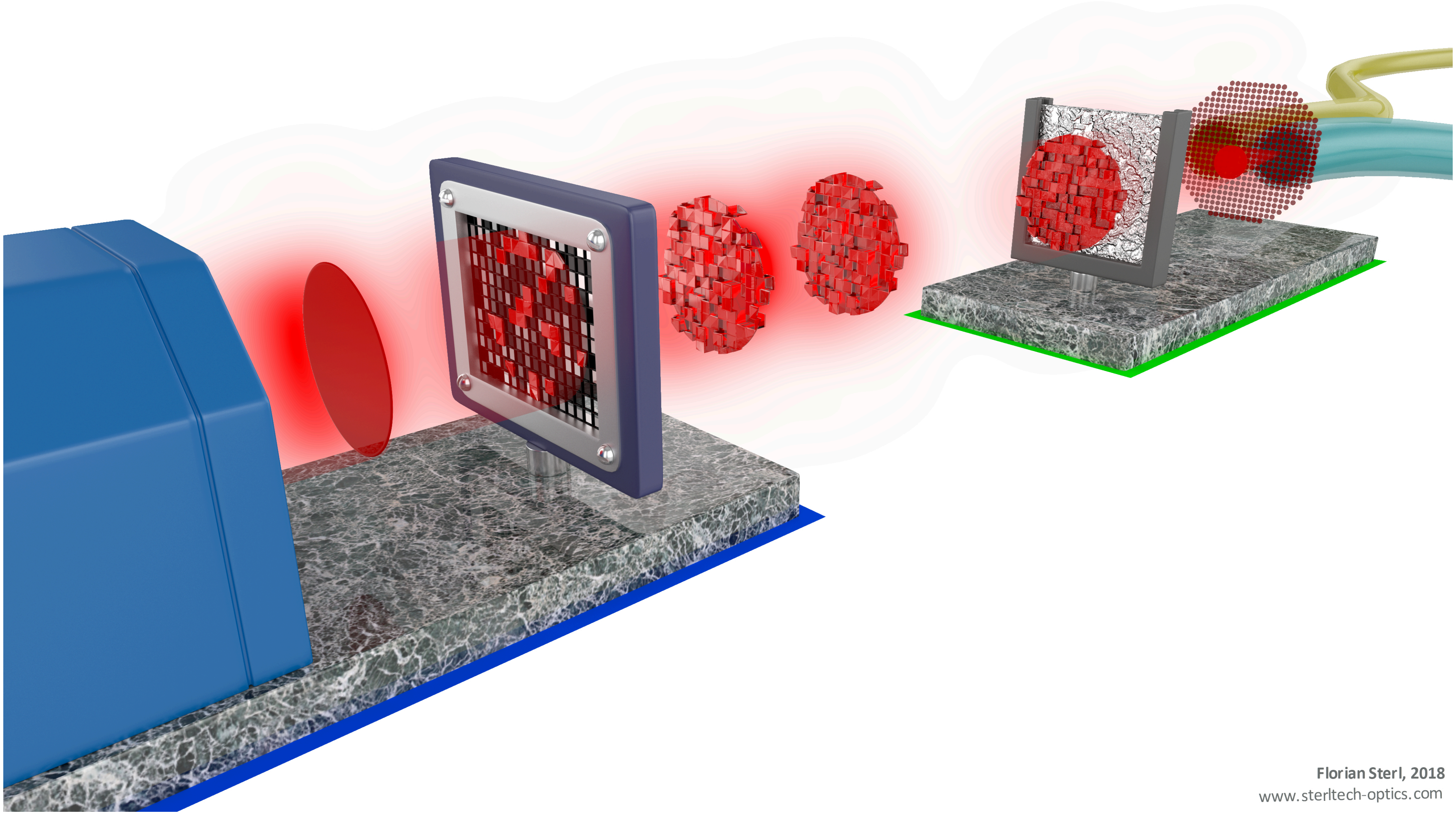
[Uppu et al 2018]
export.arxiv.org/abs/1802.07573

One-way use of the quantum channel





The long arm of quantum physics



Florian Sterl, 2018
www.sterltech-optics.com

Outlook

Research on quantum protocols at QT/e

- Key recycling / unclonable encryption
  - further optimisations
- PUFs
  - single-mode fiber

Starting up new project with Univ. Twente.

Open for other collaborations.