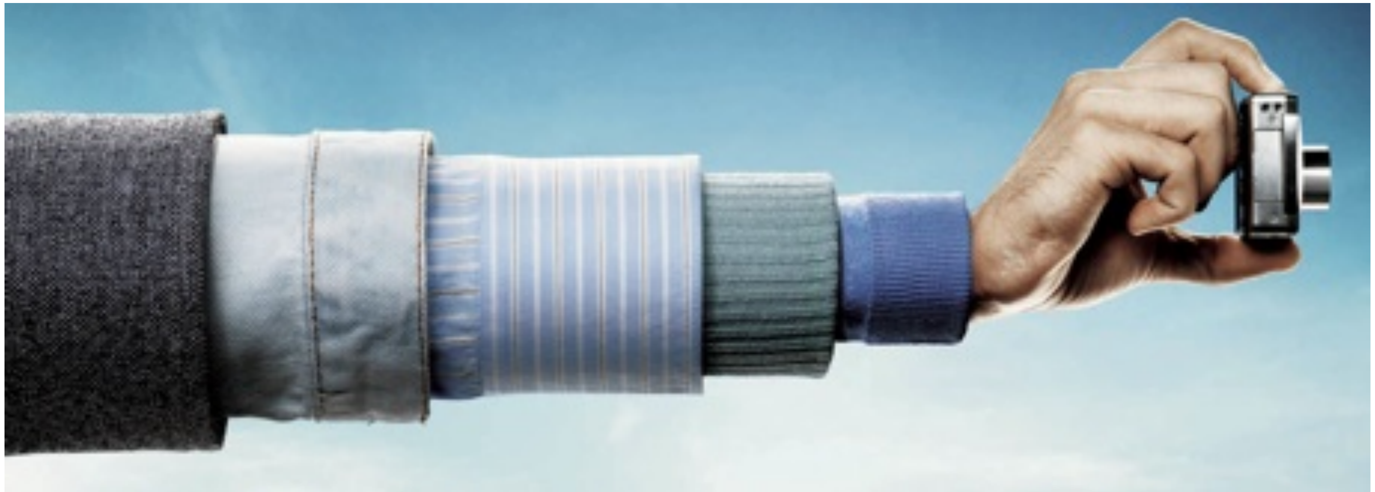
Quantum-Secure Authentication



Boris Škorić

TU/e

Outline

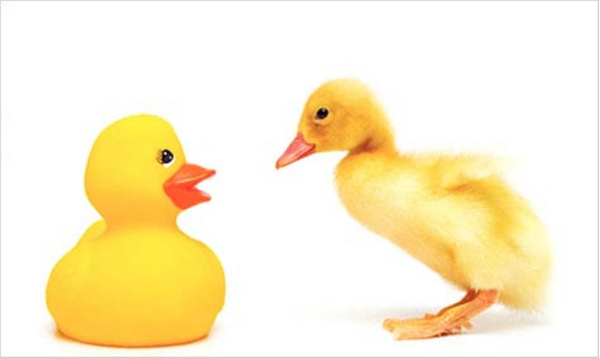
- Remote authentication of objects
- Unclonable Physical Functions (PUFs)
- Quantum readout of PUFs
  - theory
  - physical realization
- Security analysis

Authentication of Objects

How do you verify if an object is authentic?

- Step 1: registration / enrollment
- Step 2: check if fresh observation matches enrolled data

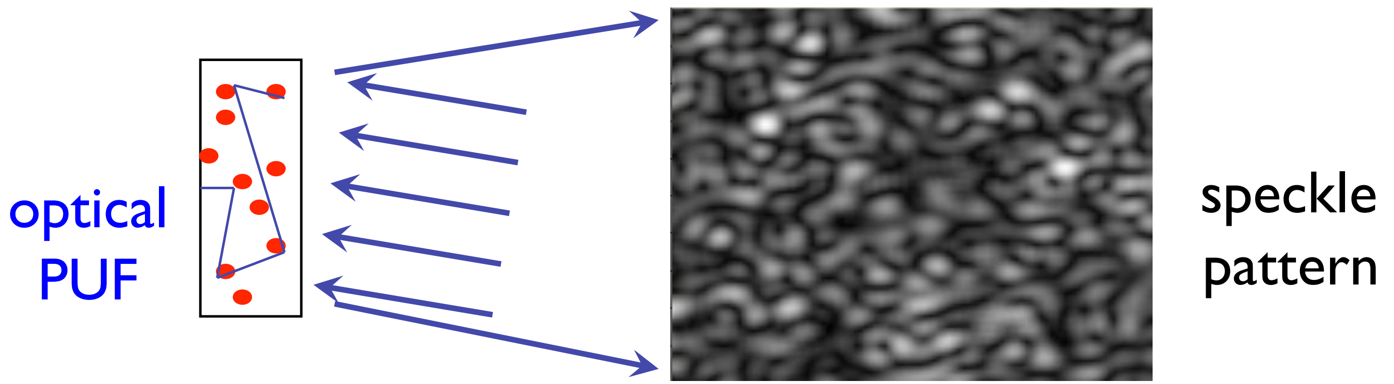
State of the art: <u>PUFs</u> (classical objects)



Unclonable Physical Function [Pappu et al. 2001]

PUF:

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



Attacks on PUF authentication

Attack #1: exact physical cloning

Attack #2: physical emulation

- build a *different* system that produces correct responses

Possible in theory;

Infeasible with current technology;

Arms race!

Attack #3: digital emulation

- build challenge-response table
- determine the challenge
- find the response in the table

Topic of this talk

"Hands-off" authentication of PUFs

Attacker model:

- We want to authenticate a PUF
- It is in hostile territory
- No phys. cloning
- No phys. emulation (no arbitrary unitaries)
- PUF has limited entropy $\Rightarrow$ **can be digitally emulated!**

(Classical) solution:

- *a **trusted device** in hostile territory*

Problem: unknown security, and expensive;
"arms race" situation

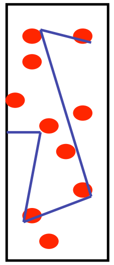
Quantum Readout of PUFs

[Škorić 2009]

Single-quantum challenge and response

$$|\psi\rangle \longrightarrow$$

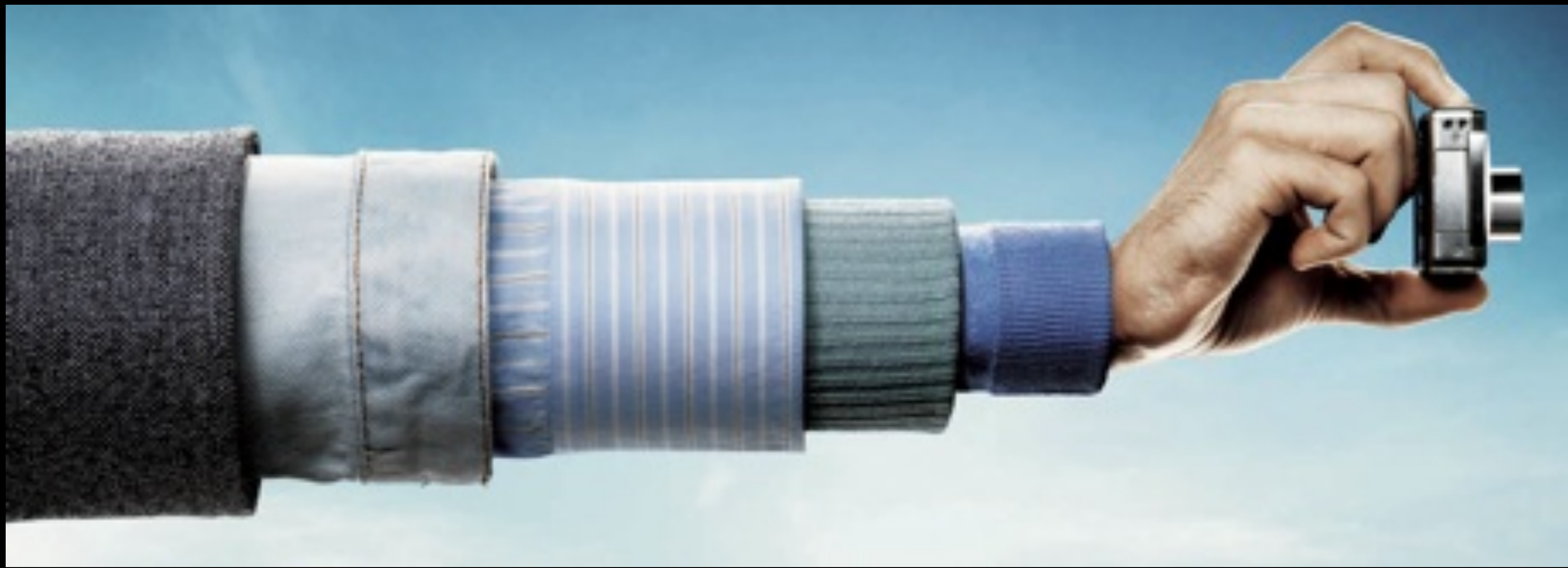
$$\longleftarrow R\,|\psi\rangle$$



Why is this secure without trusted reader?

- Measuring destroys state information
- No-cloning theorem: unknown quantum cannot be copied

$\Rightarrow$ Attacker cannot figure out what the challenge is



The long arm of quantum physics

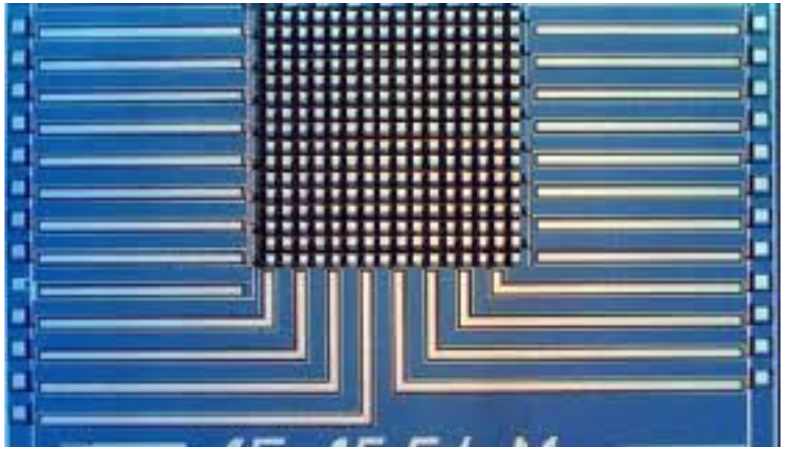
Implementation is not trivial!

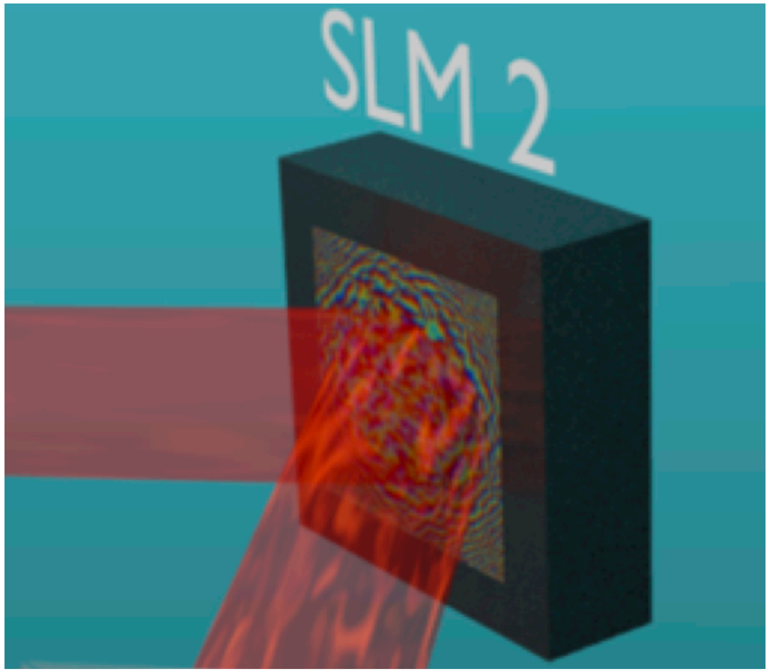
Problem:

- measurement reveals little info about photon
- how to verify a complex photon state?

Magical ingredient: Spatial Light Modulator (SLM)

- Extract *one* strategically chosen bit of info:
  correct speckle pattern or not?



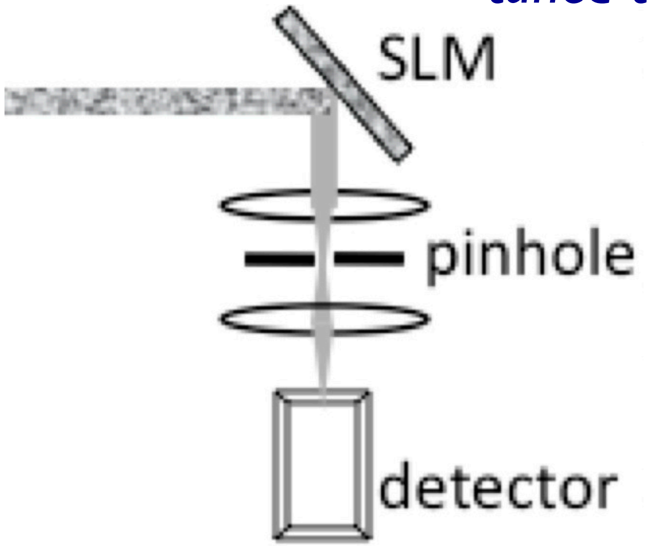


Verifying single-photon speckle

[Gooorden et al. 2013]

tuned to transform correct response into plane wave

response photon

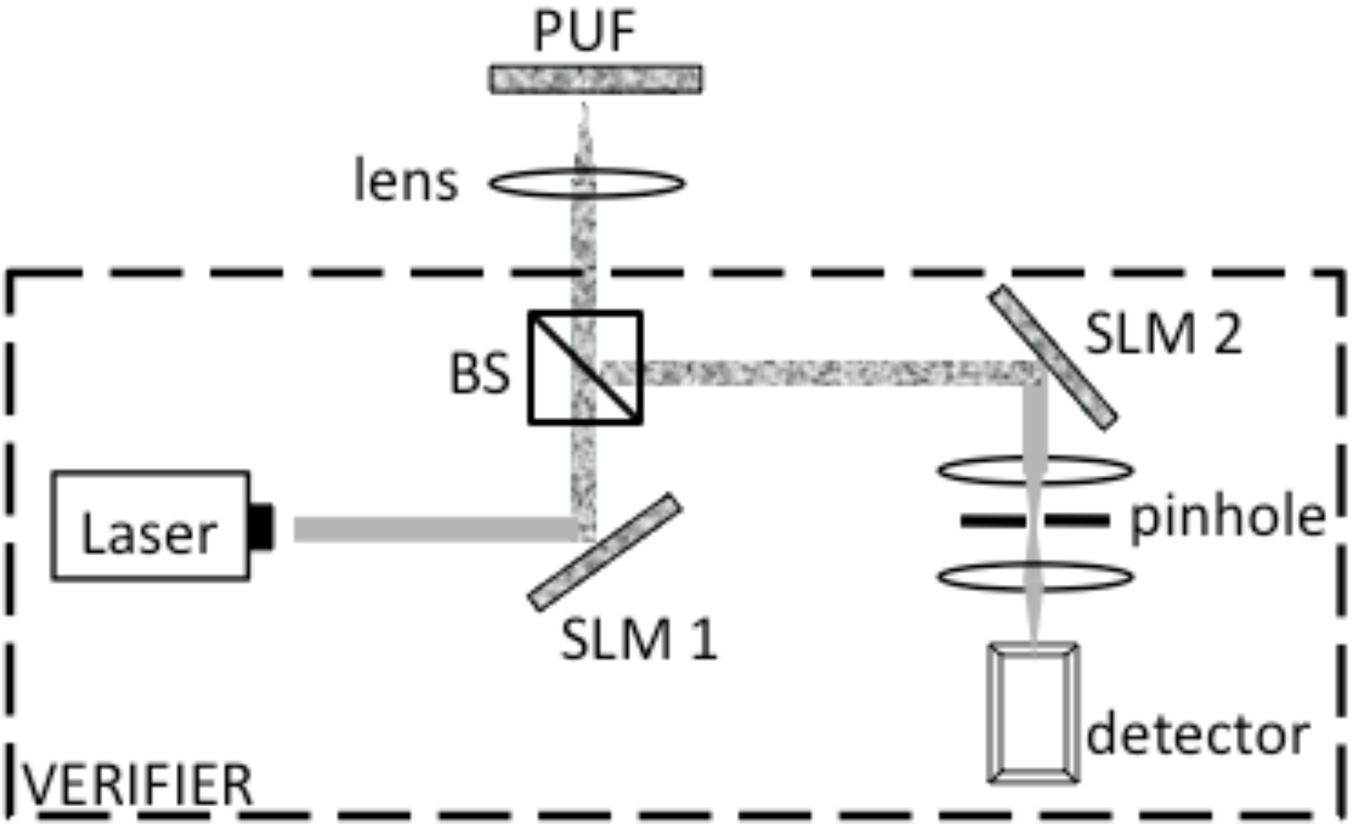


Only plane wave passes through pinhole

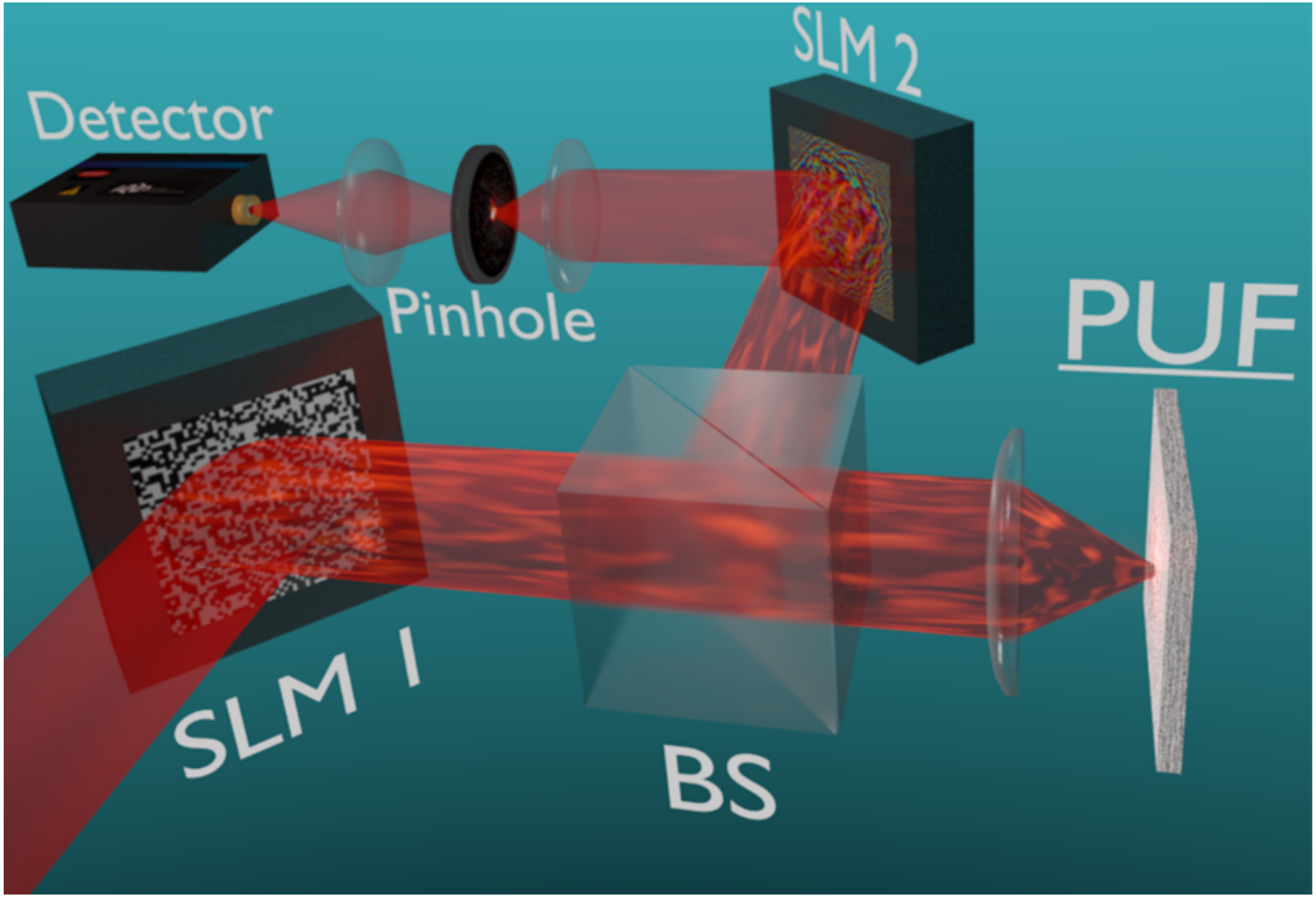
- correct PUF response $\Longrightarrow$ photon detection
- incorrect PUF response $\Longrightarrow$ no detection

Experimental setup

[Goorden et al. 2013]

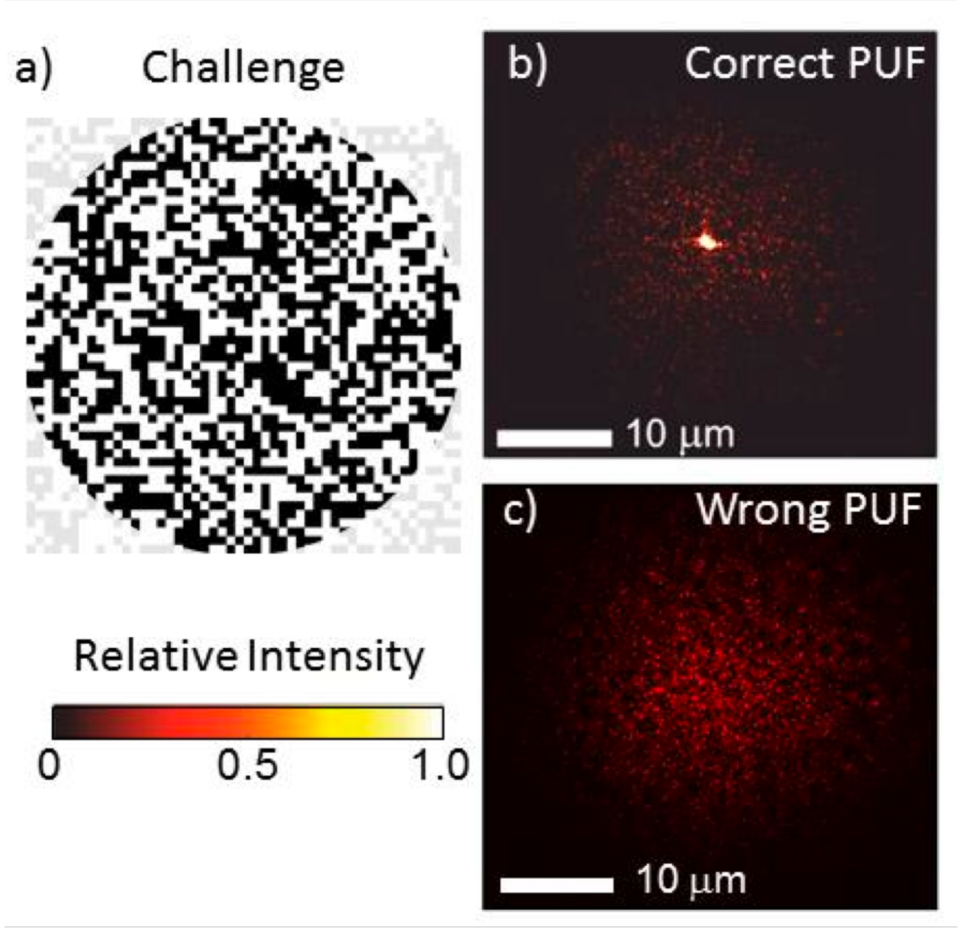


- Weak laser pulse: 230 photons
- 1000 SLM pixels

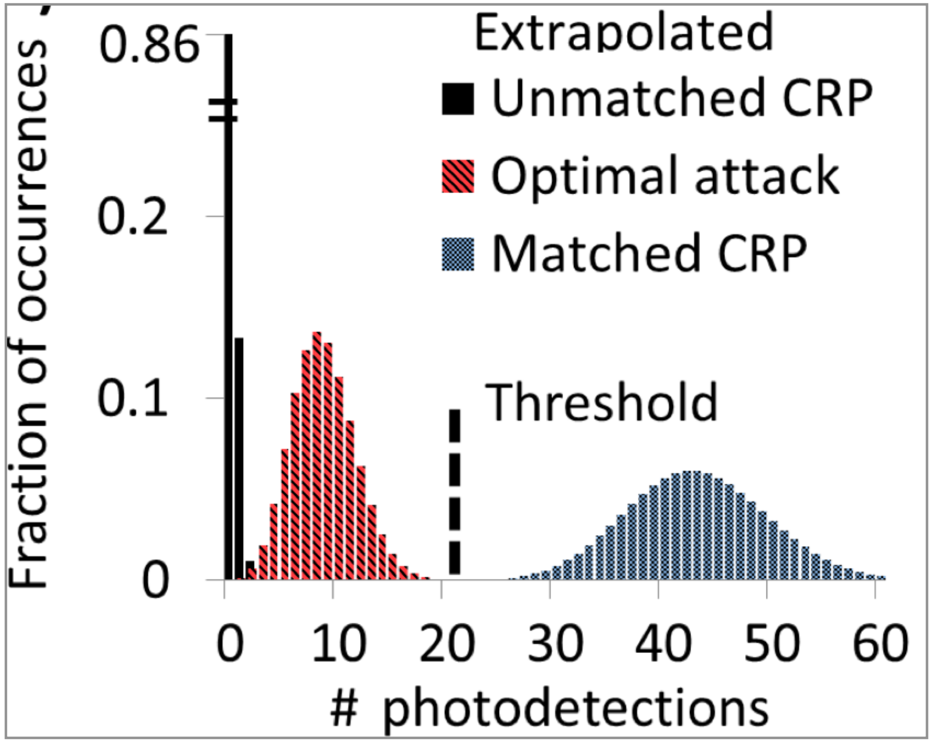


[Same thing, more fancy picture]

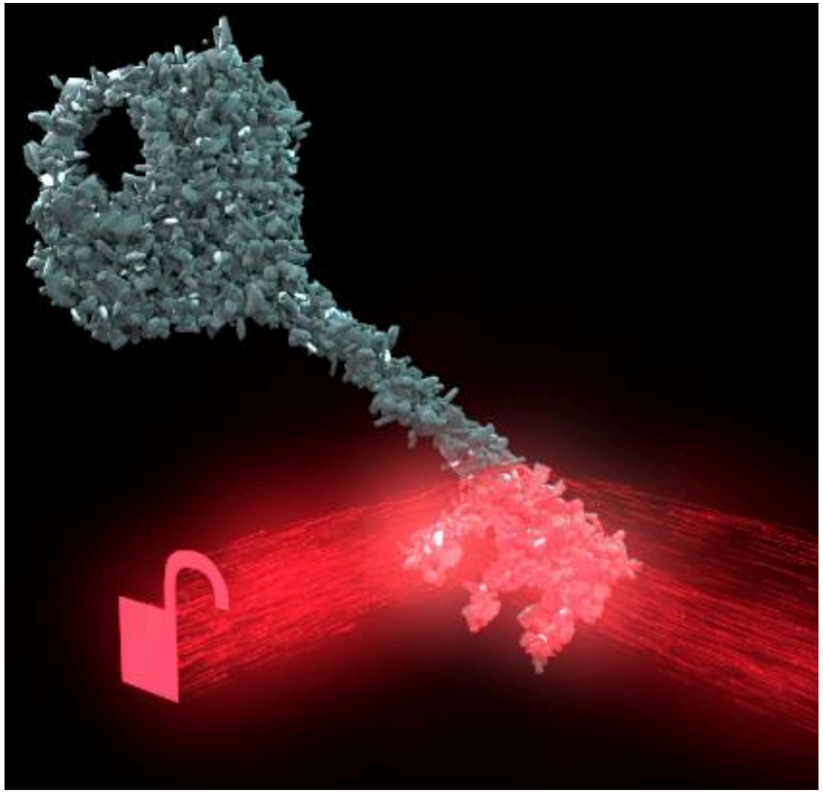
Experimental results



pattern after SLM2



Clear distinction between correct and incorrect response



Cover page, Dec. 2014

Dutch physicists develop first fraud-proof credit card

Like 2

Fraud-proof Credit Cards Possible with Quantum Physics

Security analysis: quadratures

Attack model:

- All PUF properties are publicly known
- Attacker does measurements on challenge
  - thousands of detectors; ideal equipment
  - best choice of measurements ("quadrature")
- Table Lookup based on best guess for challenge
- Attacker creates response state and sends it

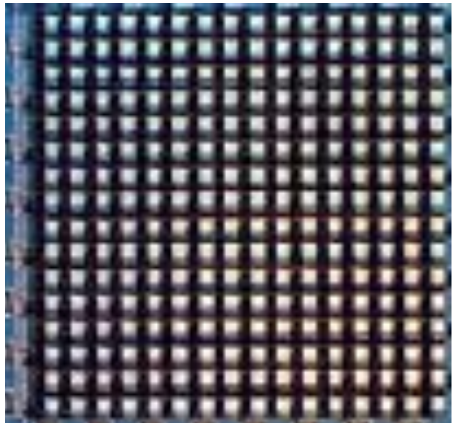
Analysis:

- Compute Prob[False Accept]
  - waveguide model
  - average over challenge space and meas. outcomes

$$\text{Prob[False Accept]} \approx \frac{n}{K+n}$$

n= #photons
K = #modes

Handwaving analysis



Intuition:

- Each photon gives a click in 1 of K modes
  - ➢ attacker gets n log(K) bits of info
- Challenge is spread out over K modes
  - ➢ K log(K) bits of entropy
- Known fraction = n/K
- Apply Fano inequality

$$P_{\text{err}} \geq \frac{\text{ignorance}}{\log(\text{space})} = \frac{K \log K - n \log K}{K \log K} = 1 - \frac{n}{K}$$

Prob[False Accept] $\leq$ n/K

Security analysis: fixed photon number

Theorem by Bruss and Macchiavello (1999):

The maximum achievable fidelity for state estimation from n identical copies of a K-dimensional quantum system is

$$\frac{n+1}{n+K}$$

Summary

- Remote object authentication: Quantum Readout of PUFs

  - Theoretical optimum.

- Unconditionally secure against digital emulation

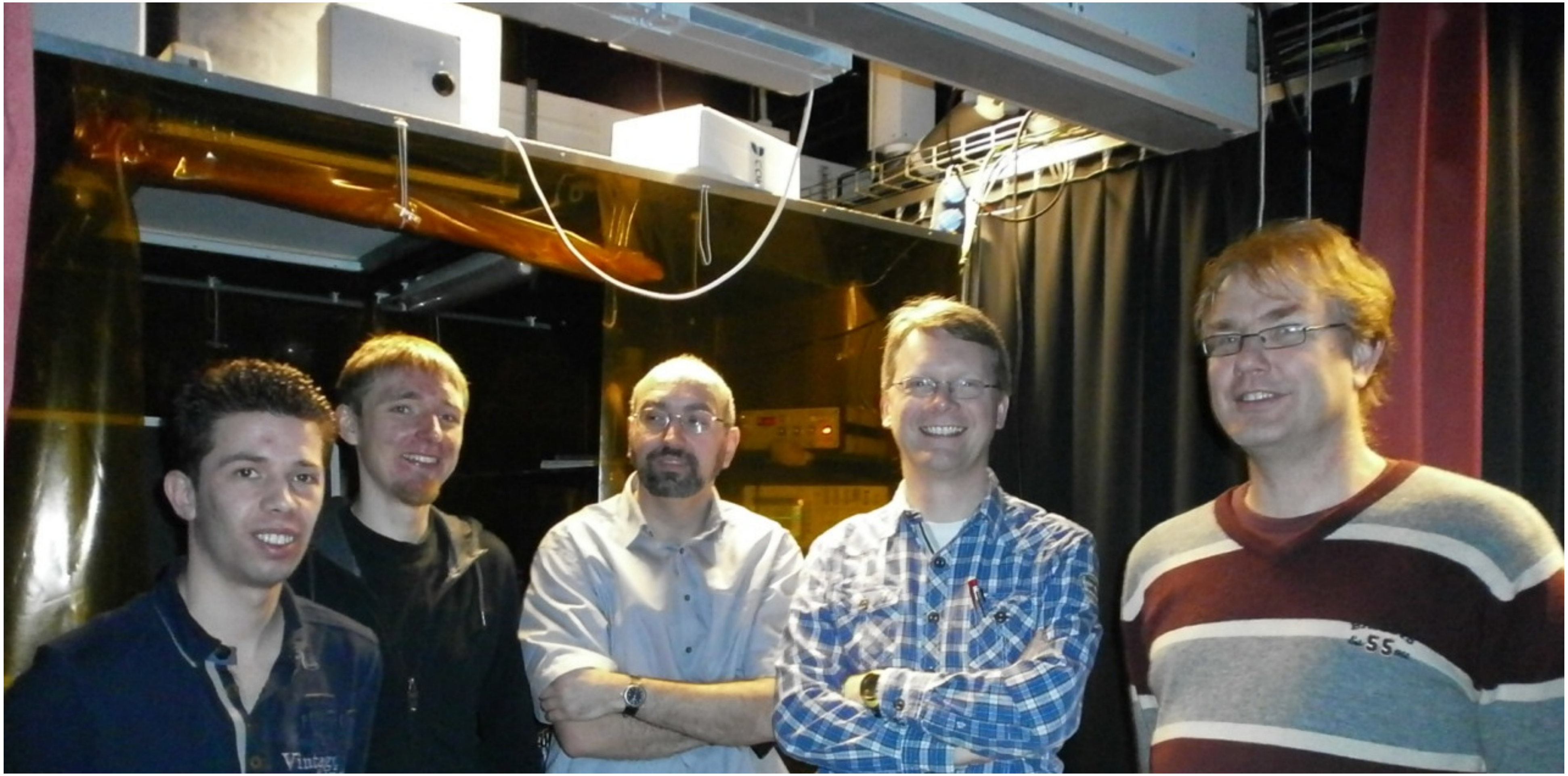
  analysis based on optimal challenge estimation

  ⇒ formula for False Accept prob: $(n+1)/(n+K)$

- Physical realization (2012-2013)

  Spatial Light Modulator + photon detector

- Future work
  - "formal" security proof for generic challenges
  - other physical realizations

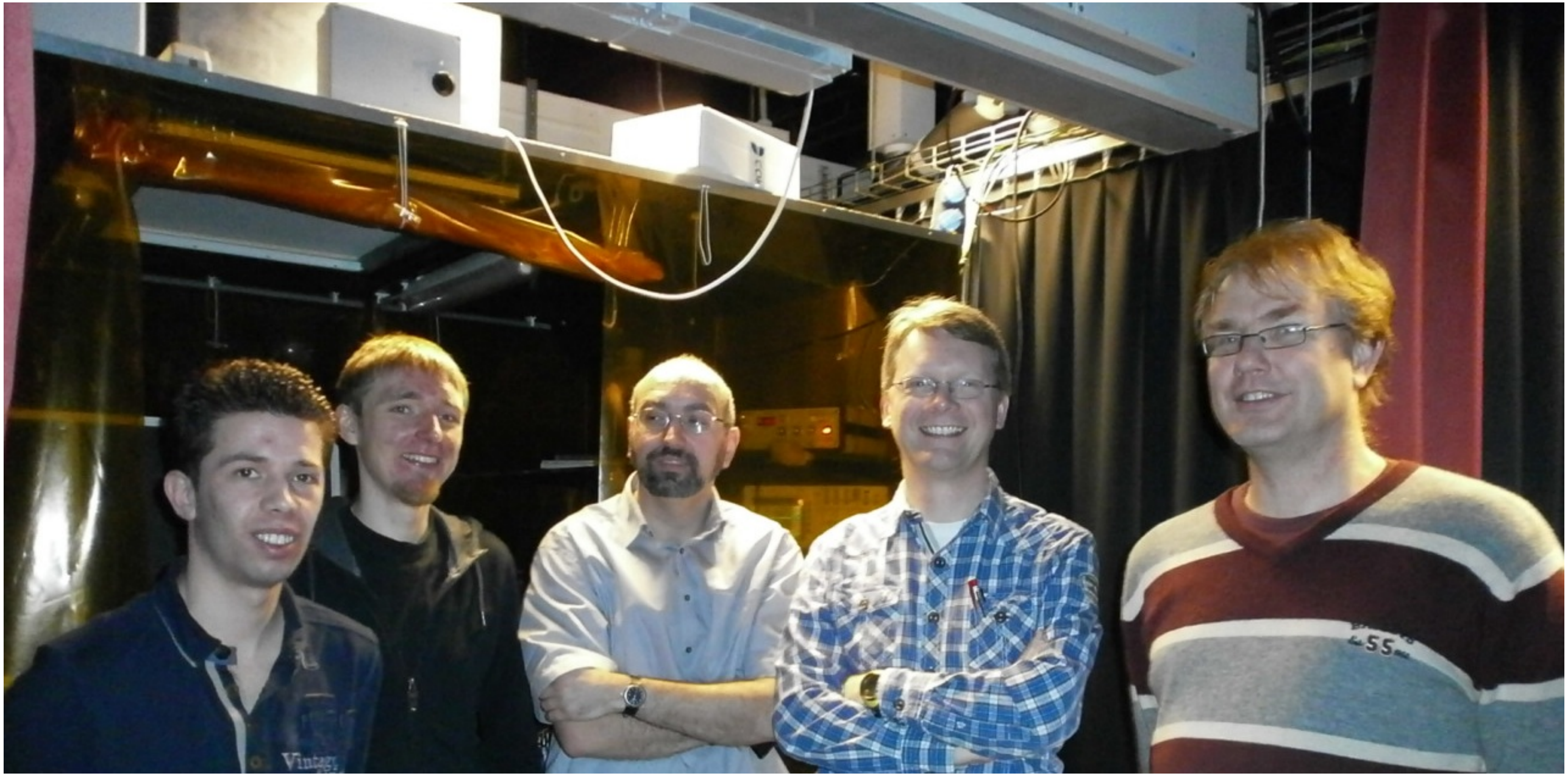


Bas Goorden	Marcel Horstmann	Boris Škorić	Pepijn Pinkse	Allard Mosk

MESA+ Institute for Nanotechnology

University of Twente COPS Complex Photonic Systems

TU/e EiΨ



Questions ?