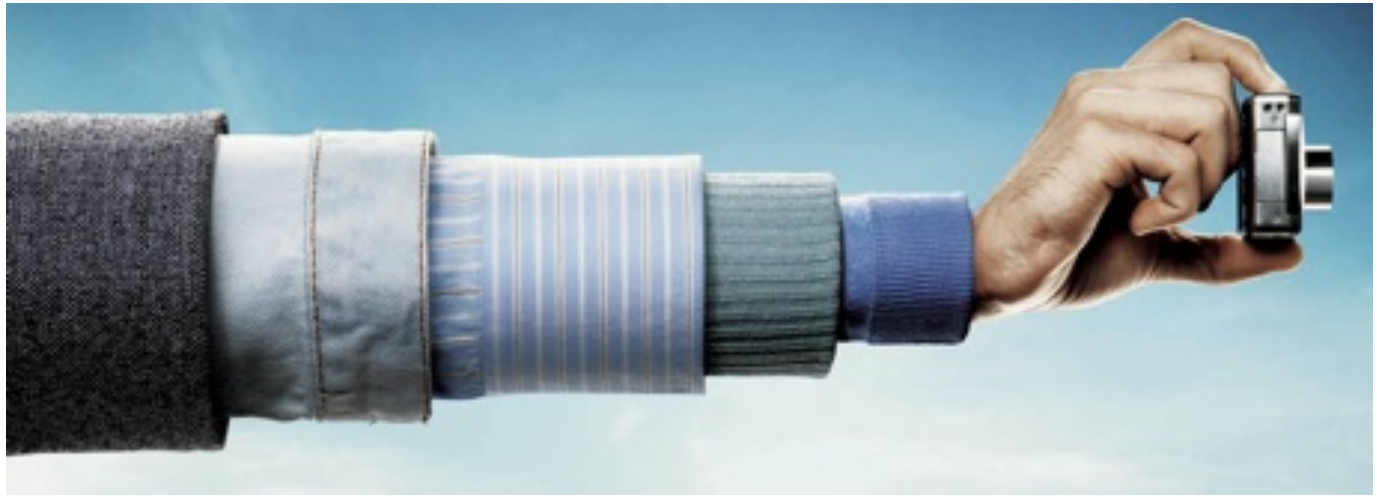
Quantum stuff with optical PUFs



25 May 2018
Crypto Working Group

Boris Škorić
TU/e

Outline

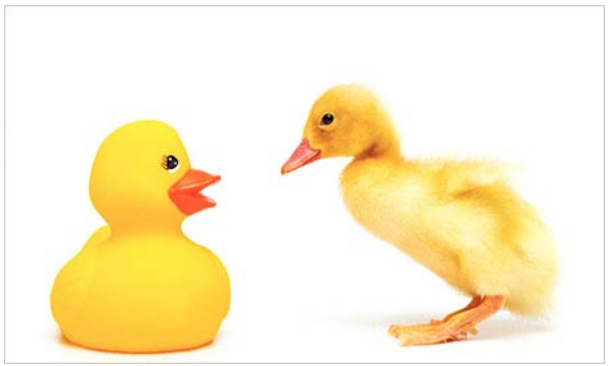
- Remote authentication of objects
- Unclonable Physical Functions (PUFs)
- Quantum readout of PUFs
  - theory
  - physical realization
  - security analysis
- Authentication of messages
- 1-way channel vs 2-way channel

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: PUFs (classical objects)

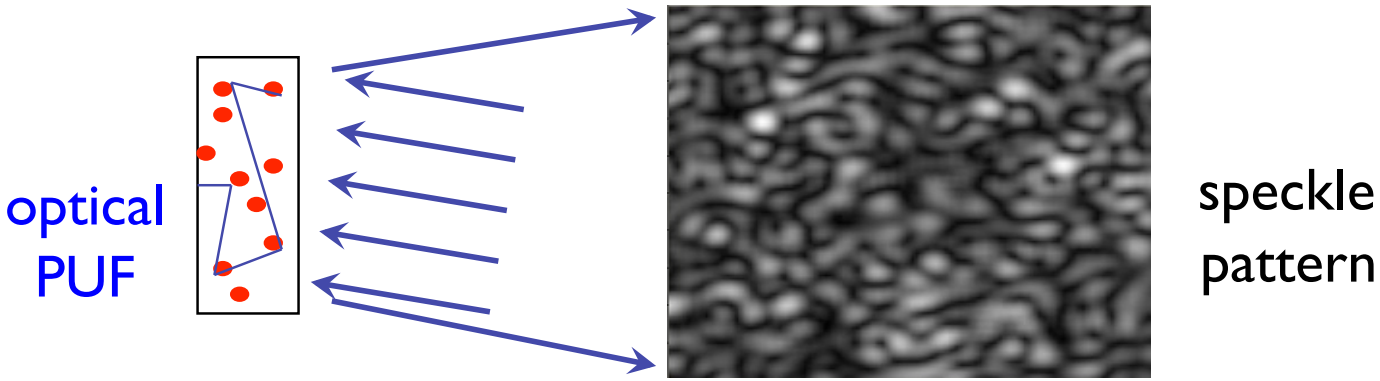


Unclonable Physical Function

[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

"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 ⇒ **can be digitally emulated!**

(Classical) solution:

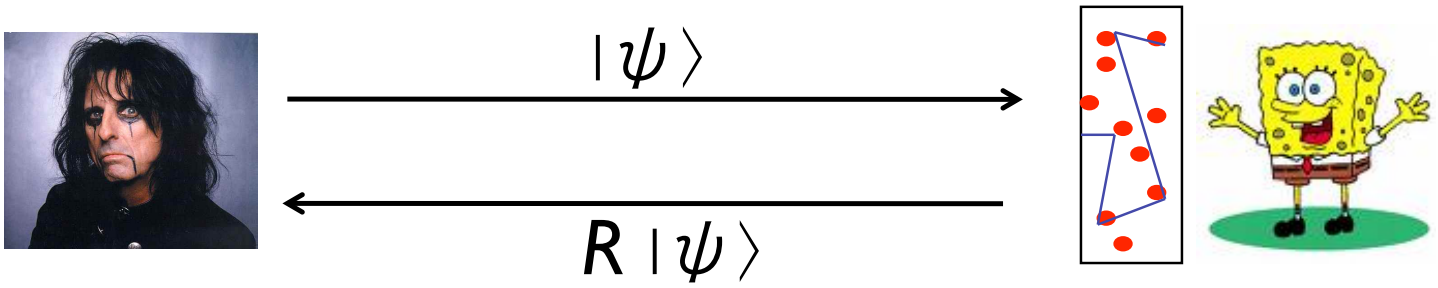
- *a **trusted device** in hostile territory*

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

Quantum Readout of PUFs

[Škorić 2009]

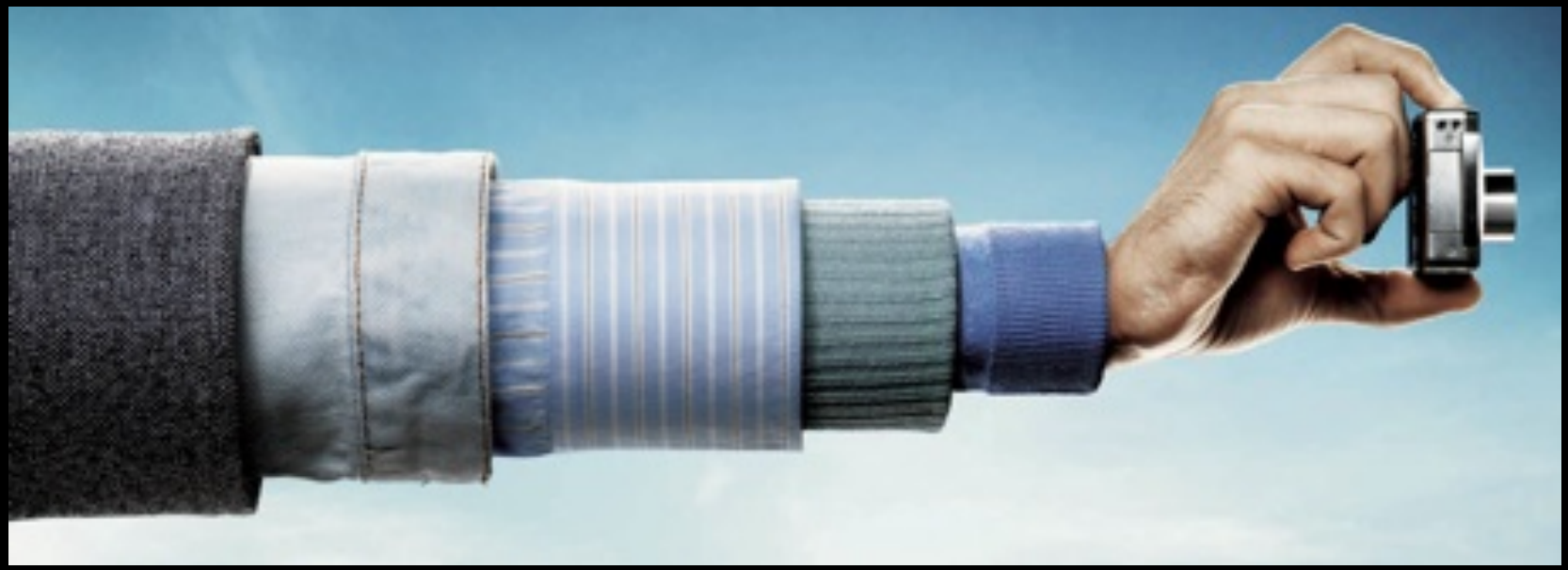
Single-quantum challenge and response



Why is this secure without trusted reader?

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

⇒ Attacker cannot figure out what the challenge is



The long arm of quantum physics

Implementation is not trivial!

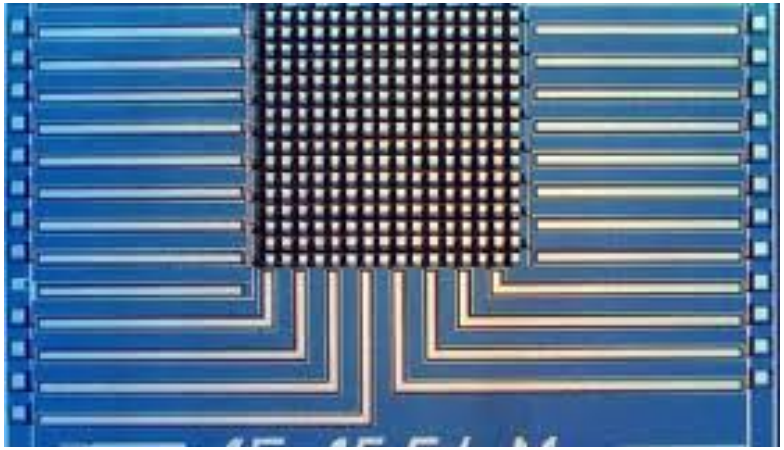
Problem:

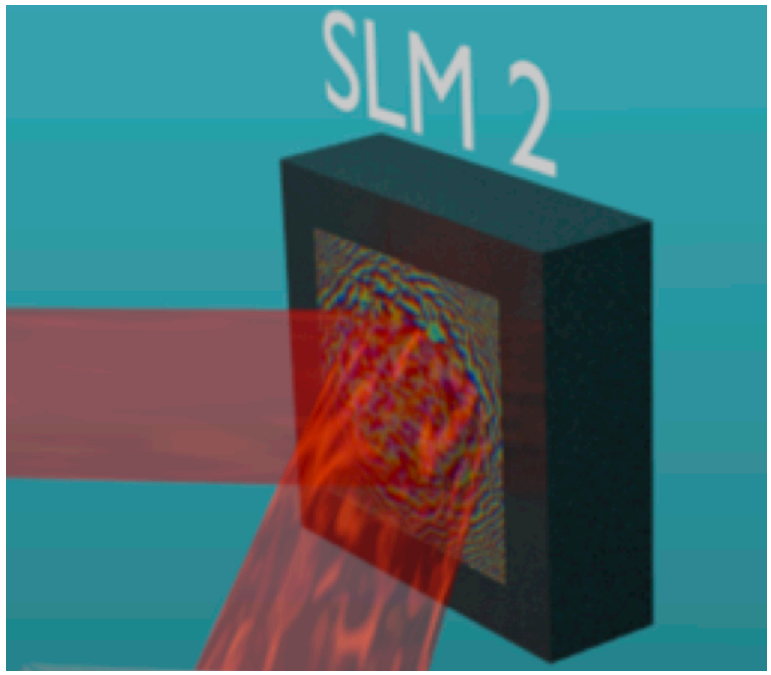
- measurement reveals little info about photon
- how to verify a complex photon state?

Magical ingredient: Spatial Light Modulator (SLM)

- Extract *one* strategically chosen bit of info:

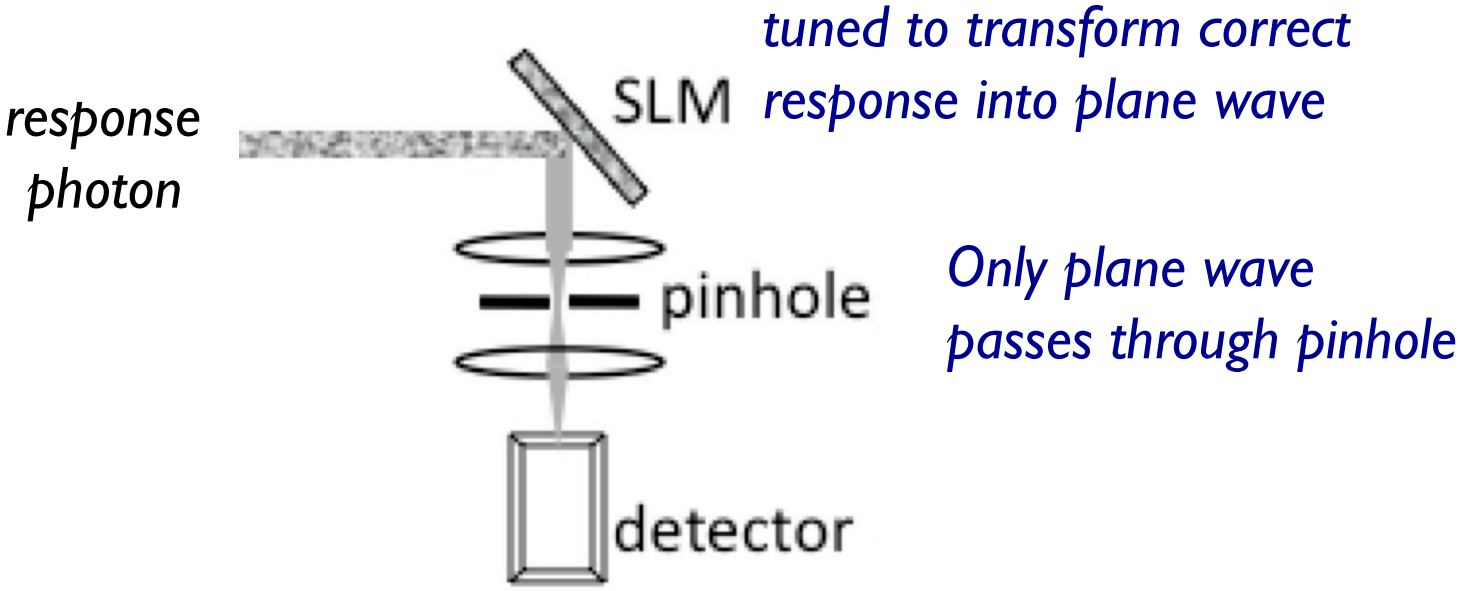
  correct speckle pattern or not?





Verifying single-photon speckle

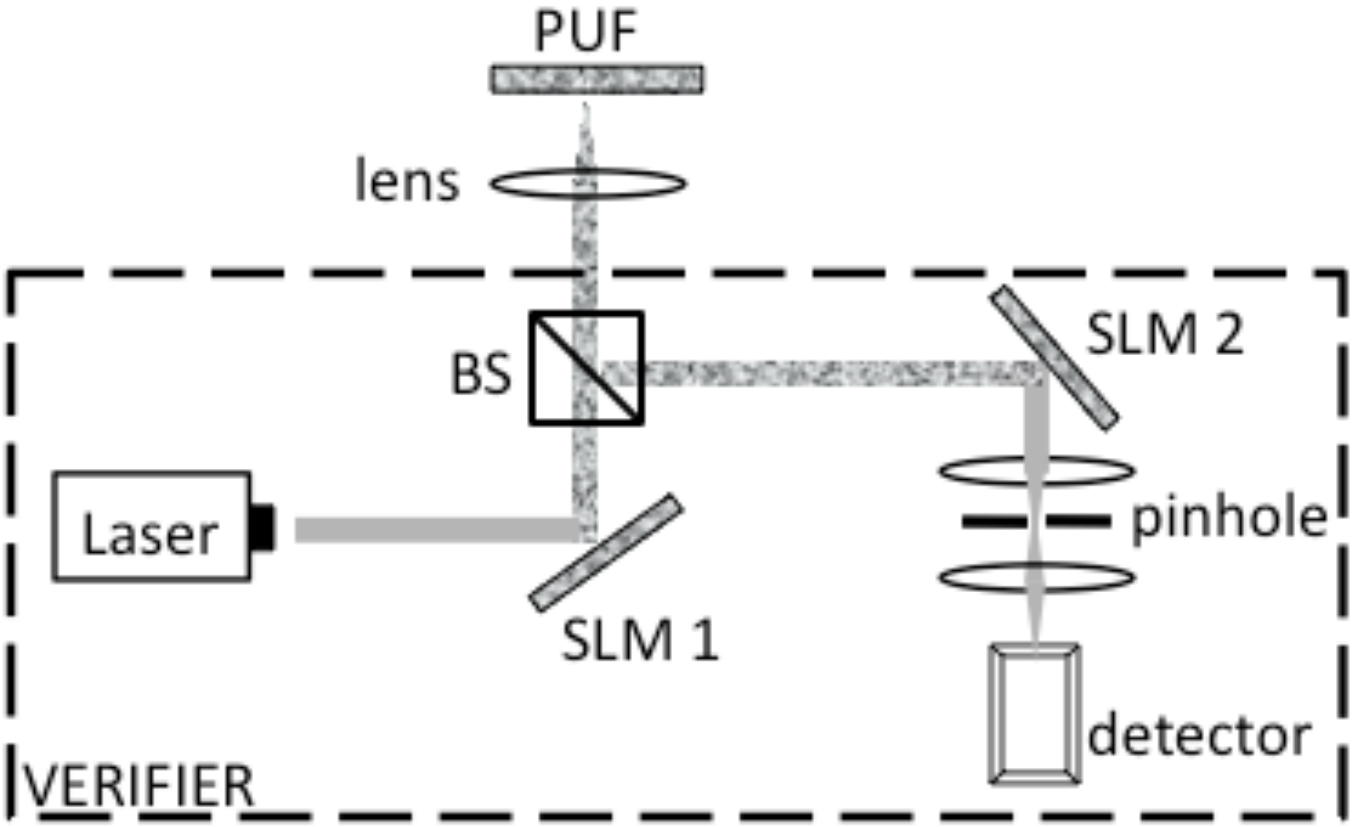
[Goorden et al. 2013]



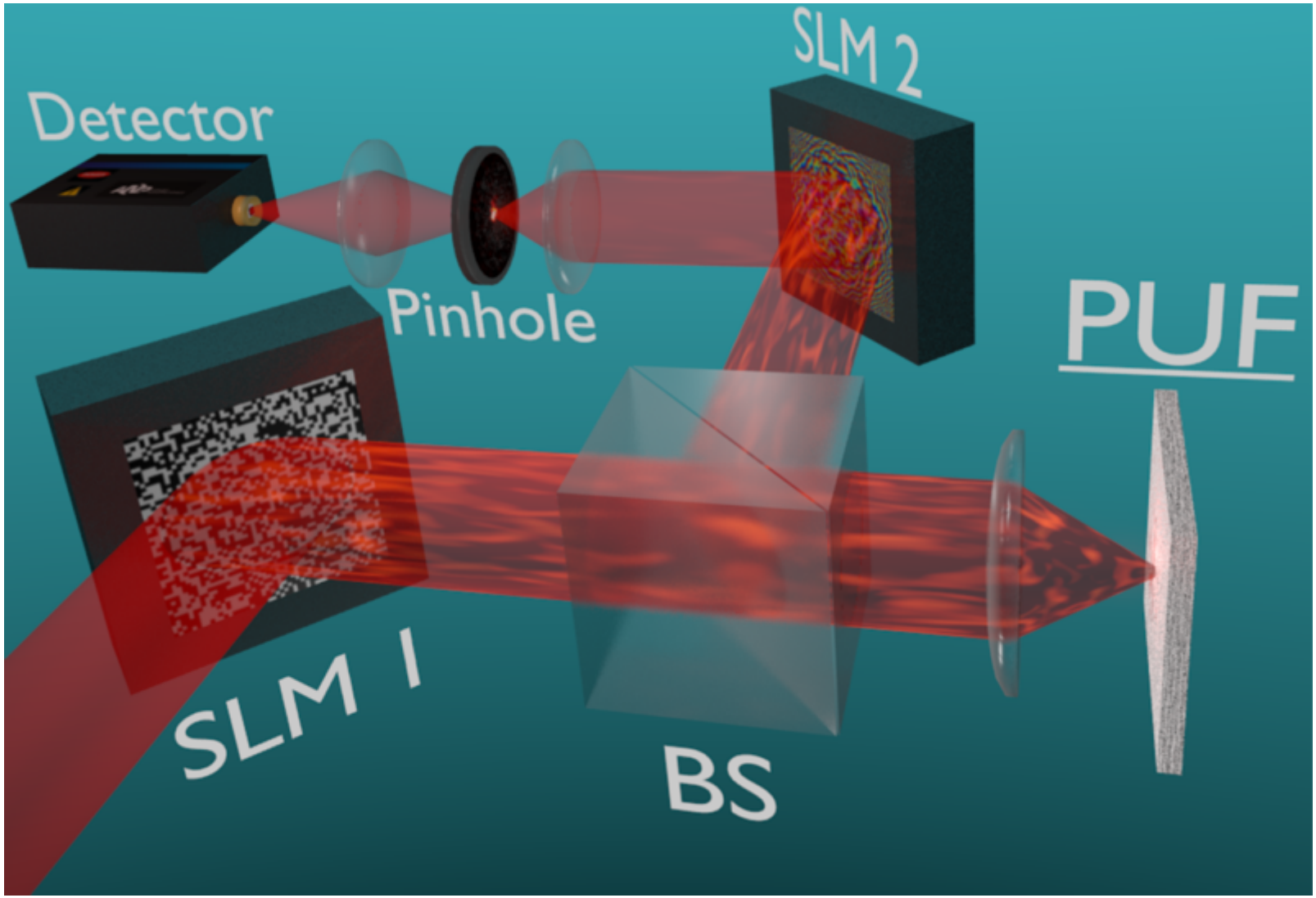
- correct PUF response $\Longrightarrow$ photon detection
- incorrect PUF response $\Longrightarrow$ no detection

Experimental setup

[Goorden et al. 2013]

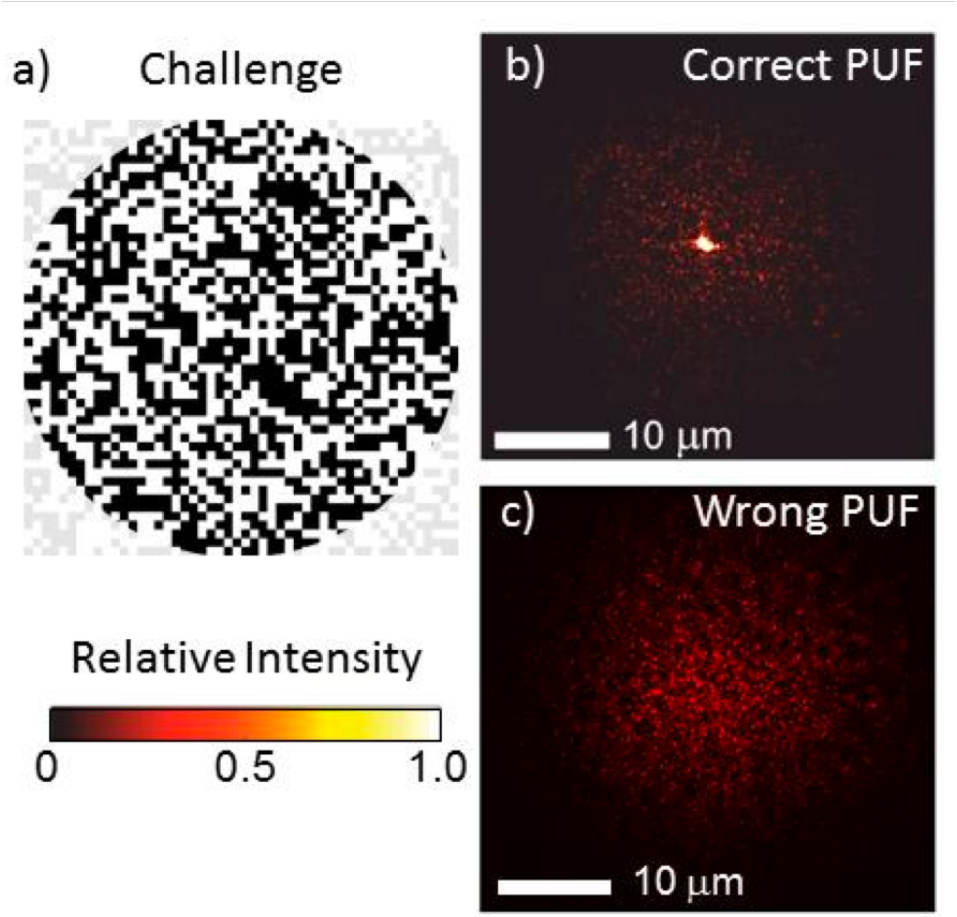


- Weak laser pulse: 230 photons
- 1000 SLM pixels

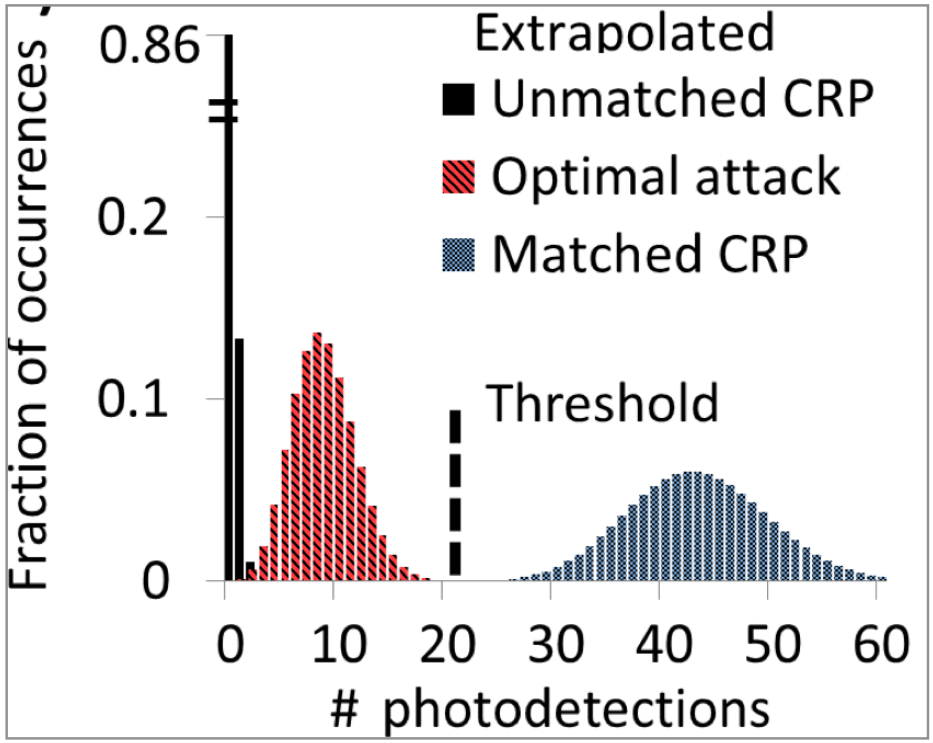


(Same thing, more fancy picture)

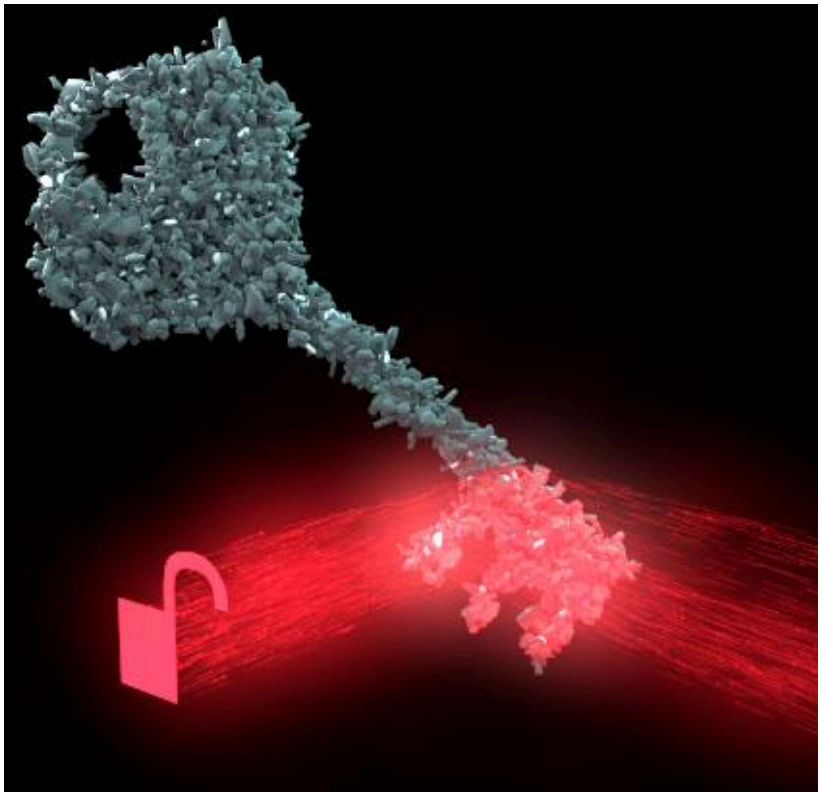
Experimental results



pattern after SLM2



Clear distinction between correct and incorrect response



QSA

Quantum Secure Authentication

Cover page, Dec. 2014

Dutch physicists develop first fraud-proof credit card

Fraud-proof Credit Cards Possible with Quantum Physics

Security of QSA

Attacker model:

- Attacker wants to authenticate without PUF
- All PUF properties are publicly known
- Attacker measures challenge state
  - ideal equipment
- Table Lookup based on best guess for challenge
- Attacker creates response state and sends it

Result for one round:

$$\text{Prob[False Accept]} \approx \frac{n+1}{n+K}$$

n= #photons
K = #modes

Security of QSA (2/3)

Theorem by Bruss and Macchiavello (1999):

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

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

Security of QSA (3/3)

QSA security assumption:

Attacker cannot do PUF transform as efficiently as the PUF

- *correctness*
- *photon losses*
- *speed*

QSA engineering requirement:

Side channel resistance

- *don't allow Eve to probe SLM states*
- *optical isolator at SLM1*
- *short (random) time windows*
- *open SLM2 path as late as possible*
- *detect flooding*
- *decoy challenges*

QSA summary

Hands-off authentication of an object.

False Accept per round is approx n/K.
Proof based on quantum physics.

Security depends on the "QSA assumption":
difficult to perform PUF transform efficiently

QSA requires two-way quantum channel.

Authentication of data

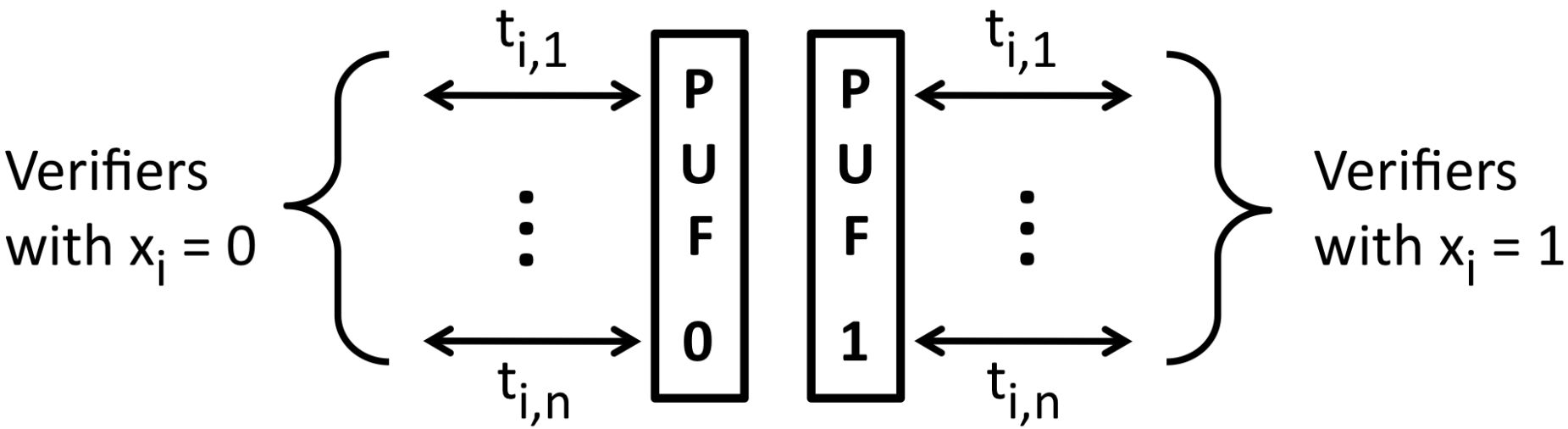
[Škorić, Pinkse, Mosk 2016]
eprint.iacr.org/2016/971

QSA authenticates an object. But what about messages?

New protocol variant called QSA-d

- Bob has PUF(0) and PUF(1)
- Bob broadcasts L-bit string x
- L rounds of QSA
  - in round i Bob presents PUF(x_i)
  - Alice knows x beforehand ⇒ knows how to prepare SLMs
- Alice now knows that PUF holder agrees with x
- Security identical to QSA

Parallel QSA-d



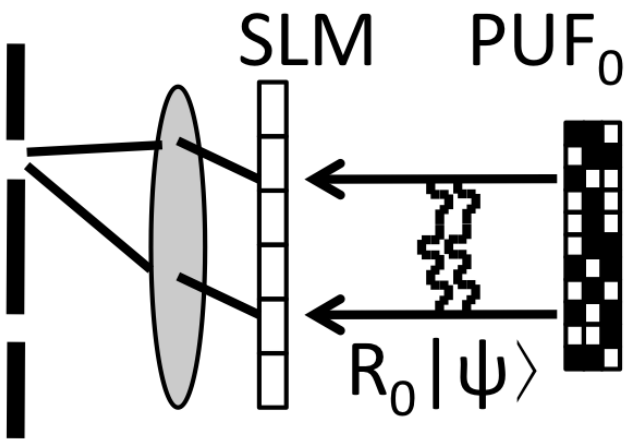
Parallel operation

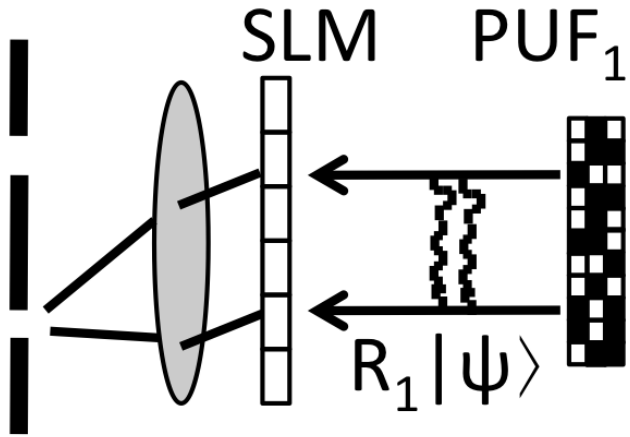
- multiple verifiers
- multiple messages

QSA-d with quantum information

SLM config that can handle *two different wavefronts*

- [more photon losses]
- responses from PUF(0) and PUF(1)
- Alice does <u>not</u> know x_i beforehand





Trick: Bob sends superposition $\alpha R_0|\psi\rangle + \beta R_1|\psi\rangle$.
Alice receives authenticated (α,β) state without knowing α,β.

QSA-d summary

Verification that PUF holder agrees with message x.

Security exactly the same as QSA.

Allows for authenticated quantum information.

QSA-d too requires two-way quantum channel.

One-way quantum channel

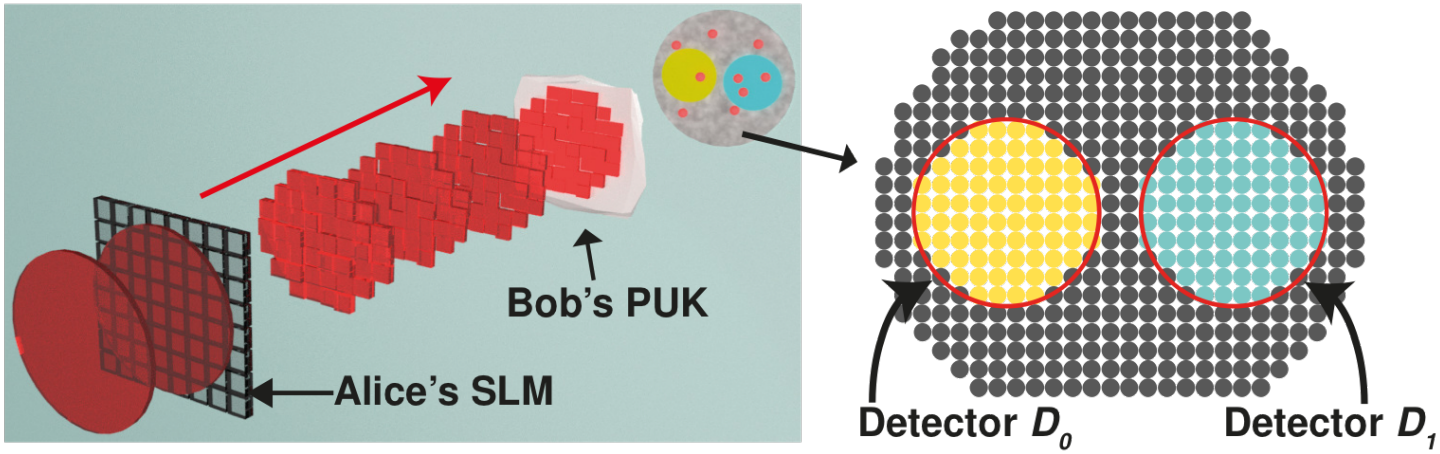
[Uppu et al 2018]
export.arxiv.org/abs/1802.07573

PEAC

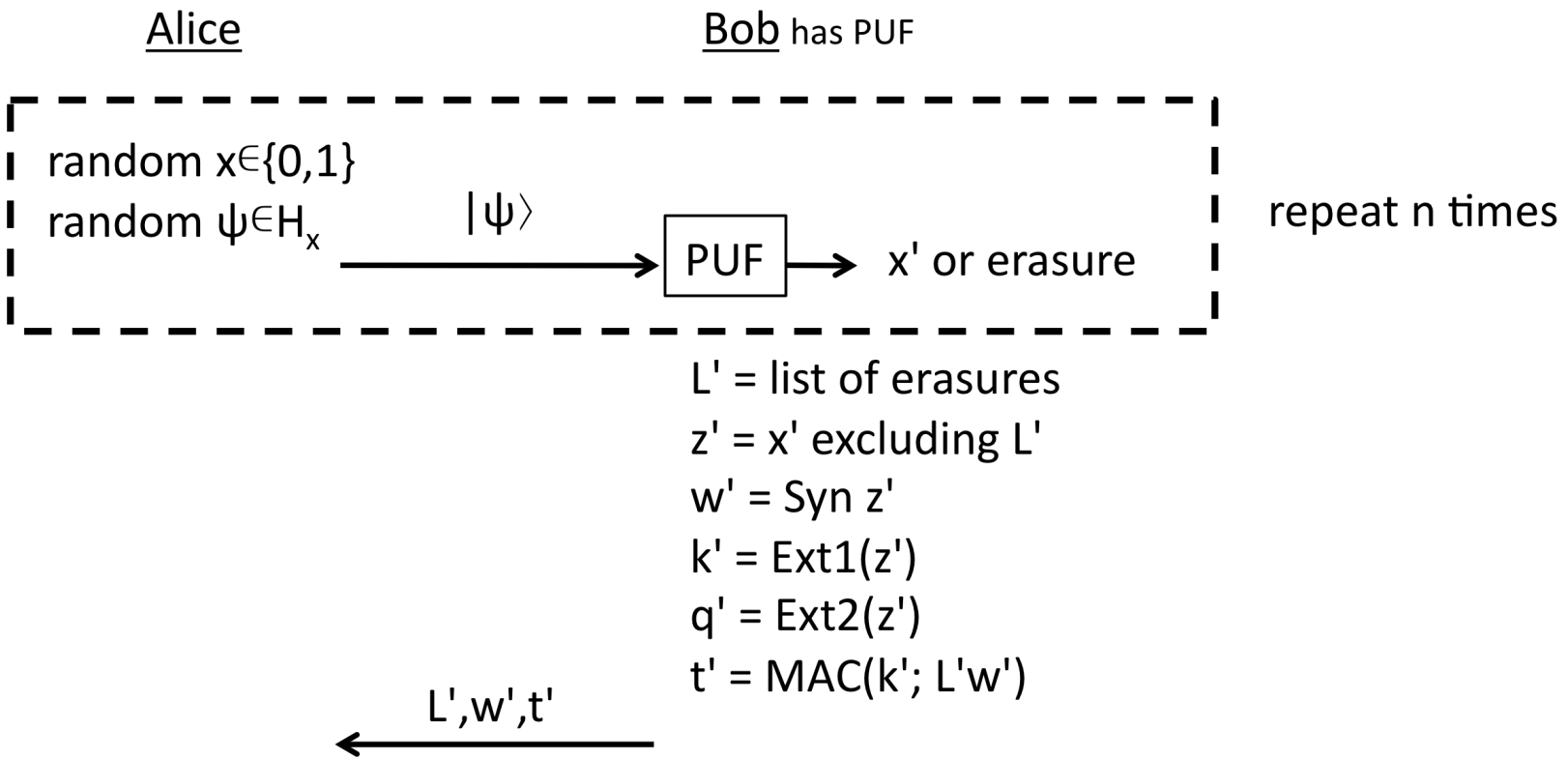
PUF-Enabled Asymmetric Communication

Alice sends quantum states that Bob's PUF will map onto detector D_0 or detector D_1.

- orthogonal Hilbert spaces H_0, H_1
- to communicate $x \in \{0,1\}$ send random $|\psi\rangle \in H_x$.

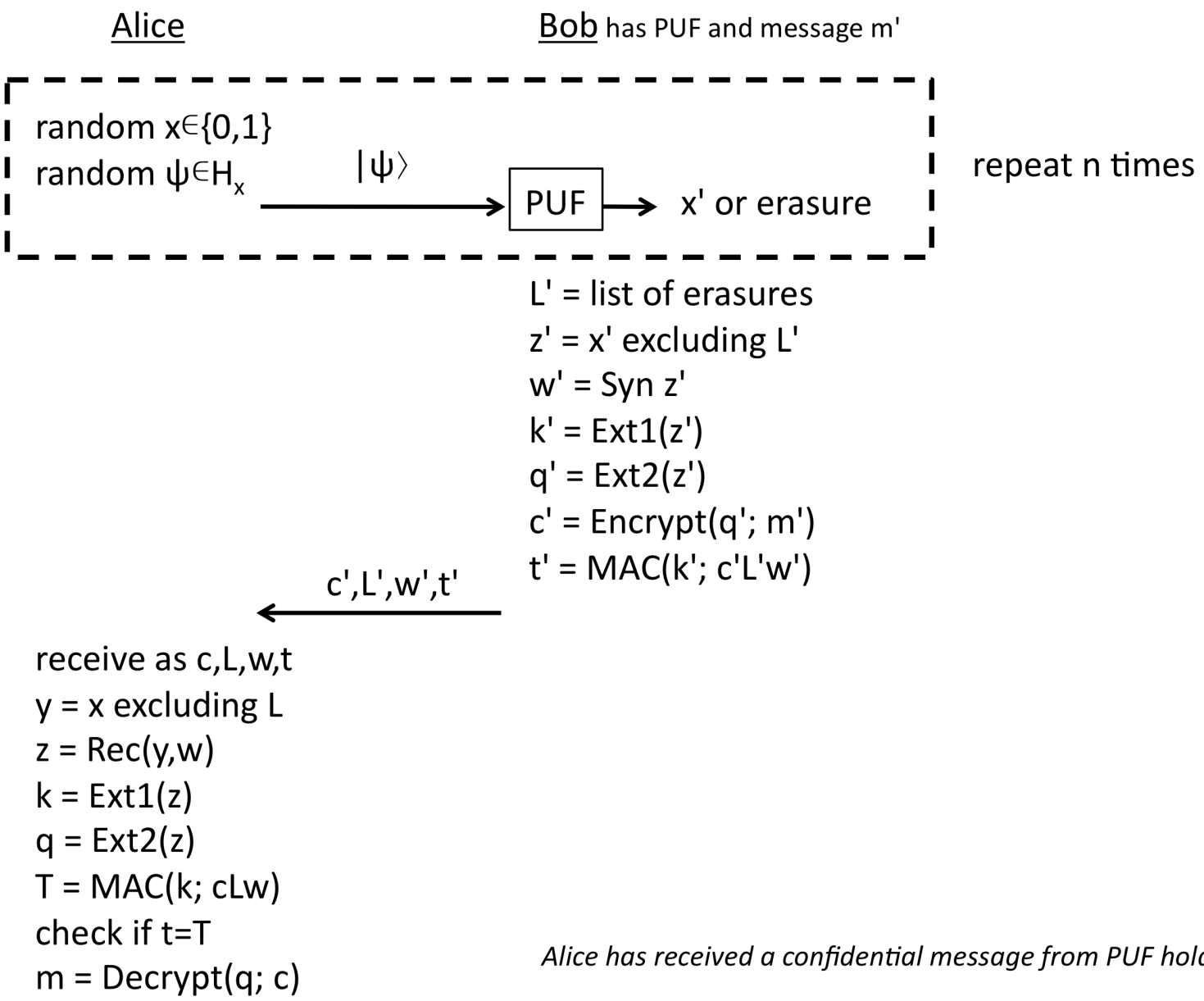


PEAC protocol #1



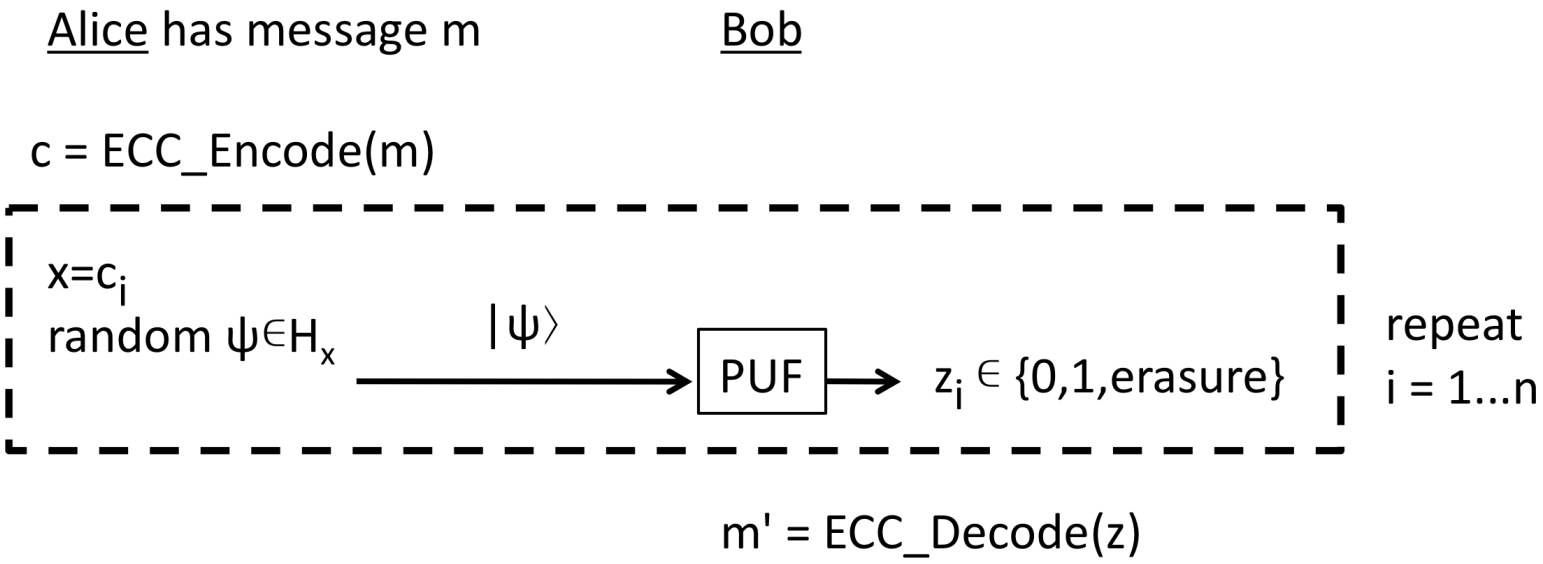
Alice has a shared key q with PUF holder.
They can do all kinds of protocol now.

PEAC protocol #2



Alice has received a confidential message from PUF holder.

PEAC protocol #3 (implemented)



Simple protocol but more difficult to implement

- code must correct erasures
- erasure rate 59%, bit flip rate 43%
- we used a Polar code, excluding the Alice=>Eve channel (low code rate, 0.002)

PEAC security

PEAC security assumption:

Attacker cannot distinguish H_0, H_1 as efficiently as the PUF

- *correctness*
- *photon losses*
- *speed*

Distinguishing orthog. subspaces trivial in theory, hard in practice

---

PEAC engineering requirement:

Side channel resistance

- *don't allow Eve to probe SLM states*
- *optical isolator*
- *short time windows*
- *decoy states*

PEAC security argument

Again based on
[Bruss+Macchiavello 1999]

$\hat{\psi}$ *is estimator for* ψ

$\{\psi, v_2, v_3, \ldots, v_{K/q}\}$ *is basis of correct Hilbert space*

q = alphabet size
n = #photons
K = #channels

$$P_{\text{Eve}} = |\langle\hat{\psi}|\psi\rangle|^2 + \sum_{j=2}^{K/q} |\langle\hat{\psi}|v_j\rangle|^2$$

fidelity F

$$= F + \sum_{j=2}^{K/q} |\langle\hat{\psi}|v_j\rangle|^2$$

directions are random

$$\leq F + \sum_{j=2}^{K/q} \frac{1}{K}$$

use [BM1999]

$$\leq \frac{1}{q} + \frac{\langle n\rangle}{K} \frac{1-\frac{1}{K}}{1+\frac{\langle n\rangle}{K}}.$$

PEAC vs QSA

PEAC is less secure than QSA.
Breaking QSA ⇒ breaking PEAC.

PEAC needs only one-way quantum channel.

QSA can yield confidentiality *indirectly*
(QKD+QSA).
PEAC can yield confidentiality *directly*.

Summary

- QSA: PUF-based quantum authentication of objects
  - remote / hands-off
- PUF-based quantum authentication of data
  - classical and quantum info
  - data approved by PUF holder
- Physical security assumptions. Difficulty of
  - two-way (QSA): doing the PUF transform
  - one-way (PEAC): distinguishing subspaces