Quantum Readout of PUFs

TU/e

Boris Škorić  
Physical Aspects of Digital Security  
chapter 10
Outline

- Remote authentication of objects
- Unclonable Physical Functions (PUFs)
- Quantum readout of PUFs
  - theory
  - physical realization
- Security analysis
How do you verify authenticity of an object?

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

State of the art: PUFs (classical objects)
Unclonable Physical Function

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

[Pappu et al. 2001]
Attacks on PUF authentication

Attack #1: exact physical cloning

Possible in theory;

Attack #2: physical emulation

Infeasible with current technology;

• build a different system that produces correct responses

Arms race!

Attack #3: digital emulation

Topic of this lecture

• 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

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
Technical difficulty:
• 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 $\rightarrow$ photon detection
- incorrect PUF response $\rightarrow$ no detection

Accept prob. $|\langle \text{response} | R | \psi \rangle |^2$
Experimental setup

- Weak laser pulse: 230 photons
- 1000 SLM pixels

[Goorden et al. 2013]
[Same thing, more fancy picture]
Experimental results

Clear distinction between correct and incorrect response
Dutch physicists develop first fraud-proof credit card

Fraud-proof Credit Cards Possible with Quantum Physics
Security analysis

Attack model:
• All PUF properties are publicly known
• Attacker does measurements on challenge $\ket{\psi}$
  – thousands of detectors; ideal equipment
  – best choice of measurements
  – guess: $\ket{\psi'}$
• Table lookup / emulation based on guess
  – Attacker sends response state $R \ket{\psi'}$

False Accept prob. $|\langle \psi' | R^\dagger R | \psi \rangle|^2 = |\langle \psi' | \psi \rangle|^2$

"fidelity"
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

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

Prob[False Accept] $\leq \frac{n}{K}$

n= #photons
K = #modes
Theorem by Bruss and Macchiavello (1999):

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

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

Fidelity $\overset{\text{def}}{=} | \langle \text{estimate} | \text{real} \rangle |^2$

$= \text{precisely the false accept probability!}$
Summary

• Remote object authentication: Quantum Readout of PUFs
  - Best that can theoretically be achieved for classical objects.

• Unconditionally secure against digital emulation
  Analysis based on optimal challenge estimation
  ⇒ formula for False Accept prob: \( \frac{n+1}{n+K} \)

• Physical realization (2012–2013)
  Spatial Light Modulator + photon detector

• Future work
  – "formal" security proof for generic attacks
  – other physical realizations
Message authentication

Trivial construction

- Bob has two PUFs: "PUF(0)" and "PUF(1)"
- Bob broadcasts message $x \in \{0, 1\}^L$.
- For $i=1 \ldots L$
  - Run QSA using $PUF(x_i)$