

Quantum Readout of Physical Unclonable Functions

Boris Škorić

TU Eindhoven

Dept. of Math. & Comp. Science

Africacrypt 2010

5 May 2010

Outline

Part I

- Unclonable Physical Functions (PUFs)
- Quantum no-cloning theorem
- Quantum readout of PUFs

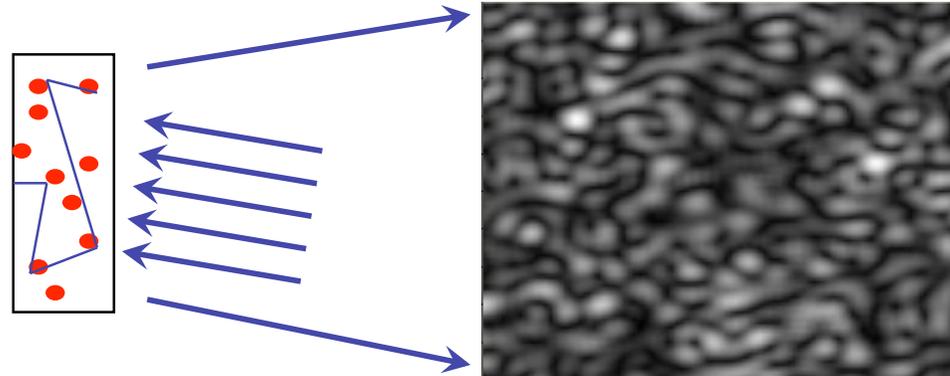
Part II

- Authenticated quantum channel
- Quantum Key Distribution
 - BB84 protocol
 - QKD through a PUF

- There are (too) many definitions of a PUF
- Today's definition:
 - physical object
 - behaves like a function
 - unique
 - hard to make physical clone
- Examples of security applications:
 - authentication token
 - anti-counterfeiting
 - [more if you beef up the definition:
key storage, tamper evidence, trusted platform]

Example: Optical PUF

Transmission
or reflection,
or both



- Transparent medium with light-scattering particles at random positions
- Coherent multiple scattering
- Challenge = angle of laser beam
- Response = unique speckle pattern
- Object is difficult to replicate

Enrollment and verification

Enrollment:

- Characterize the PUF
 - measure its unique responses to challenges
- Store enrollment data in tamper-proof way
 - e.g. own storage / trusted party database
 - can be done publicly; no secrets!

Verification:

- Measure the PUF again
- Compare to enrolled data
 - no crypto / hashes / fuzzy extractors

Remote PUF authentication

What if:

- we want to authenticate a PUF by challenge-response
- it has little entropy \Rightarrow emulatable
- it is in hostile territory

Answer:

- must be sure that *right type of object* is probed
- *we need a trusted device in hostile territory*

Quantum physics for mathematicians

Formalism:

- quantum state is vector in Hilbert space
 - contains all physical information
 - denoted as $|\text{parameters}\rangle$
 - unit length
- real-valued observable \leftrightarrow Hermitian operator
 - eigenvalues $\lambda_i =$ possible measurement outcomes
 - basis of orthogonal eigenvectors $|\lambda_i\rangle$
- "superpositions", e.g. $|\psi\rangle = (|1\rangle + |2\rangle) / \sqrt{2}$
- measurement of A projects the state onto eigenstate of A
 - non-deterministic: $\text{Prob}[\text{outcome } \lambda] = |\langle \lambda | \psi \rangle|^2$.
 - destruction of state information!

The no cloning theorem

Wootters+Zurek 1982, Dieks 1982

- Time evolution = unitary operator acting on state.
- There is no generic evolution operator U that achieves

$$U |\psi\rangle \otimes |e\rangle = |\psi\rangle \otimes |\psi\rangle \quad \text{for all } \psi$$

Executive summary for cryptographers:

- **measuring kills info**
- **no cloning**

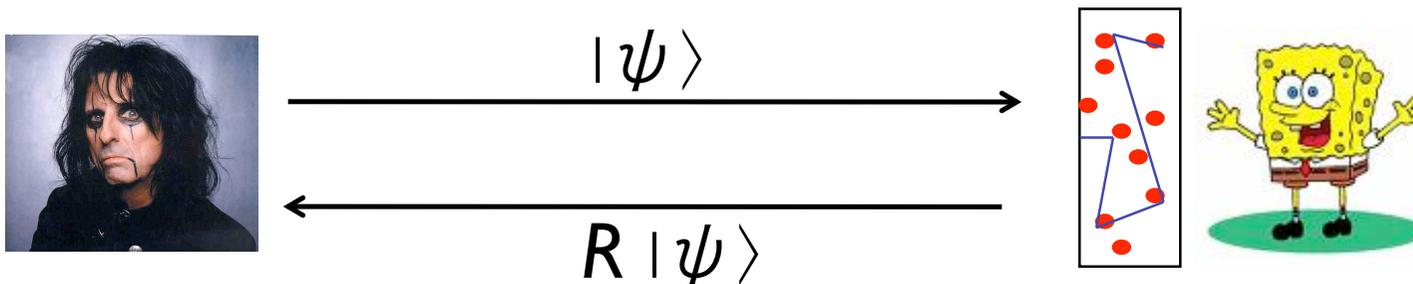


Quantum-readout PUF

New insight:

- combine classical unclonability with quantum no-cloning
- challenge a PUF with unclonable quantum states
 - response is also unclonable quantum state
 - eavesdropping on challenge/response is detected
 - **no more need for remote trusted device !**

Example: Optical PUF challenged with single photons



Assumptions

- Known physics is correct.
- Attacker has full knowledge of the PUF.
- Physical cloning is infeasible
- Quantum emulation is infeasible
 - large quantum computer
 - two quantum teleports

Security of quantum readout

Assume:

- n-dimensional Hilbert space
- arbitrary state preparation
- arbitrary measurements

Send $|\psi\rangle$, measure projection on $R|\psi\rangle$

Prob[correct response]
without having the PUF:

$$p_1 \leq \frac{3}{n+2}$$

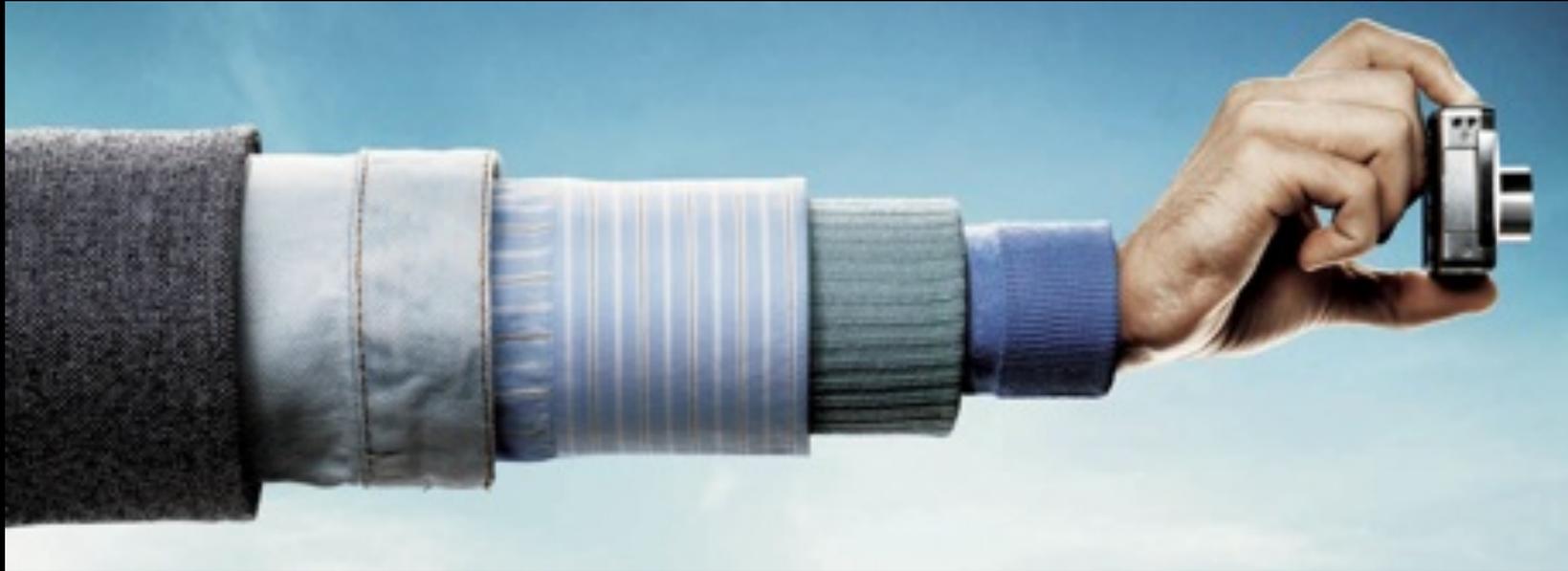
Attack with imperfect clone

Theorem 2. *Let $\delta > 0$ be a constant. Let the imperfect clone have a unitary reflection matrix R' . Let the eigenvalues of $R^{-1}R'$ be denoted as $\{e^{i\varphi_k}\}_{k \in [n]}$. Let these eigenvalues satisfy*

$$\left| \sum_{k \in [n]} e^{i\varphi_k} \right|^2 \leq n^2(1 - \delta). \quad (6)$$

Then the impostor's per-round probability of success is bounded by

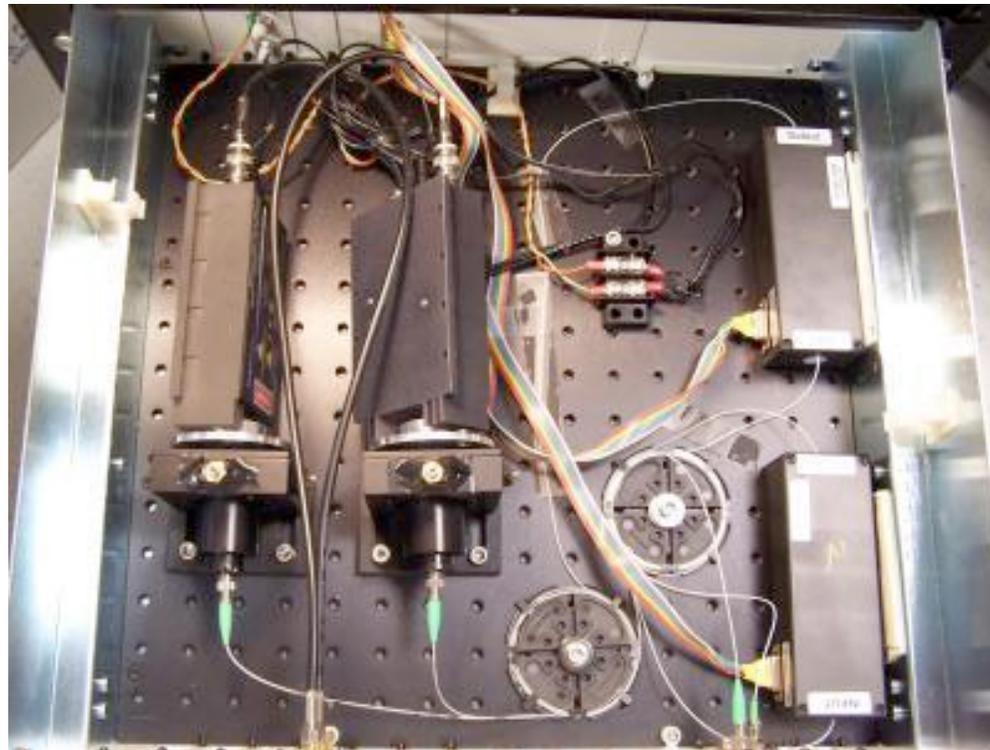
$$p_1 \leq 1 - \frac{n}{n+2}\delta. \quad (7)$$



The long arm of quantum physics

Part 2

Quantum Key Distribution



Quantum Key Distribution: bird's eye view

What is achieved:

- Alice and Bob generate a random shared key from scratch
- Eavesdropping gets detected
- *Unconditional* secrecy of key
- Requirement: authenticated classical channel

How is this possible?

- Ingenious use of quantum physics
 - unpredictable outcome of measurements
 - inbuilt tamper evidence
- ... and some classical crypto tricks

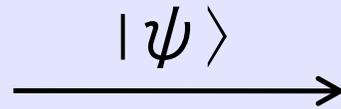
The BB84 protocol

(Bennett+Brassard 1984)

basis	b	ψ
x	0	\swarrow
x	1	\nearrow
+	0	\leftrightarrow
+	1	\updownarrow



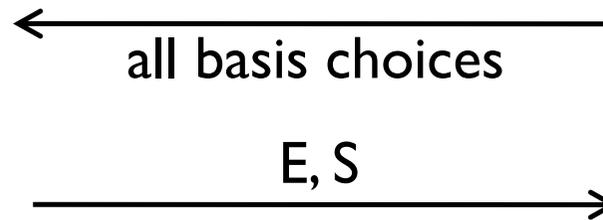
Random basis.
Random bit b.



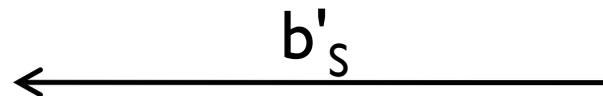
Random basis.
Measure b'.

repeat
n times

Keep events with equal basis:
subset E.
Small random set $S \subset E$.



Check if $b_S \approx b'_S$.



Shared secret $b_{E \setminus S} \approx b'_{E \setminus S}$.

- Error correction
- Privacy amplification

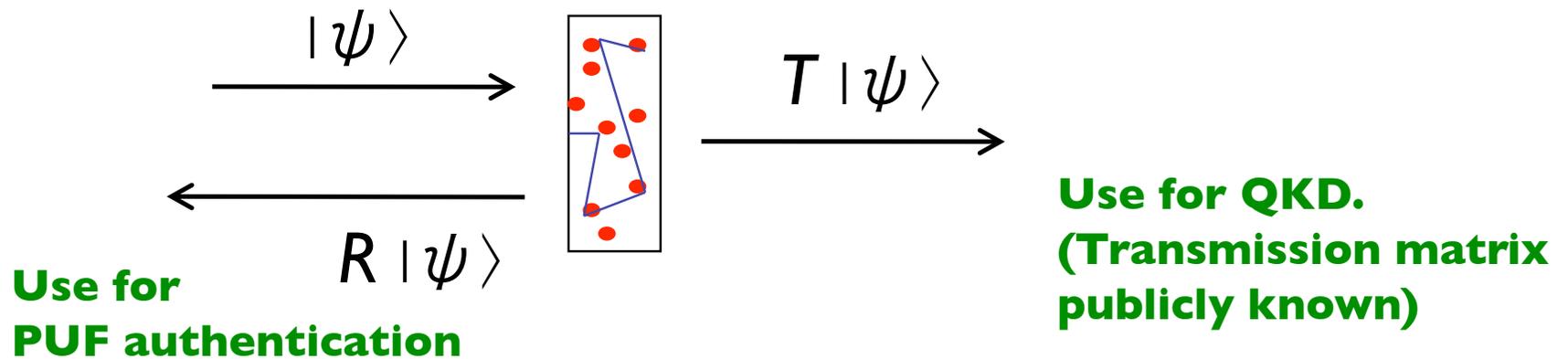
QKD: authentication

So you generate an unconditionally secure key
... but with whom?

Authenticated QKD

- Usually with short MAC key
 - unconditionally secure authentication
 - a priori shared secret
- Is that cheating?
 - No, QKD indefinitely lengthens short initial secret
- Alternative method: shared entangled state
 - practical difficulties

QKD through a PUF

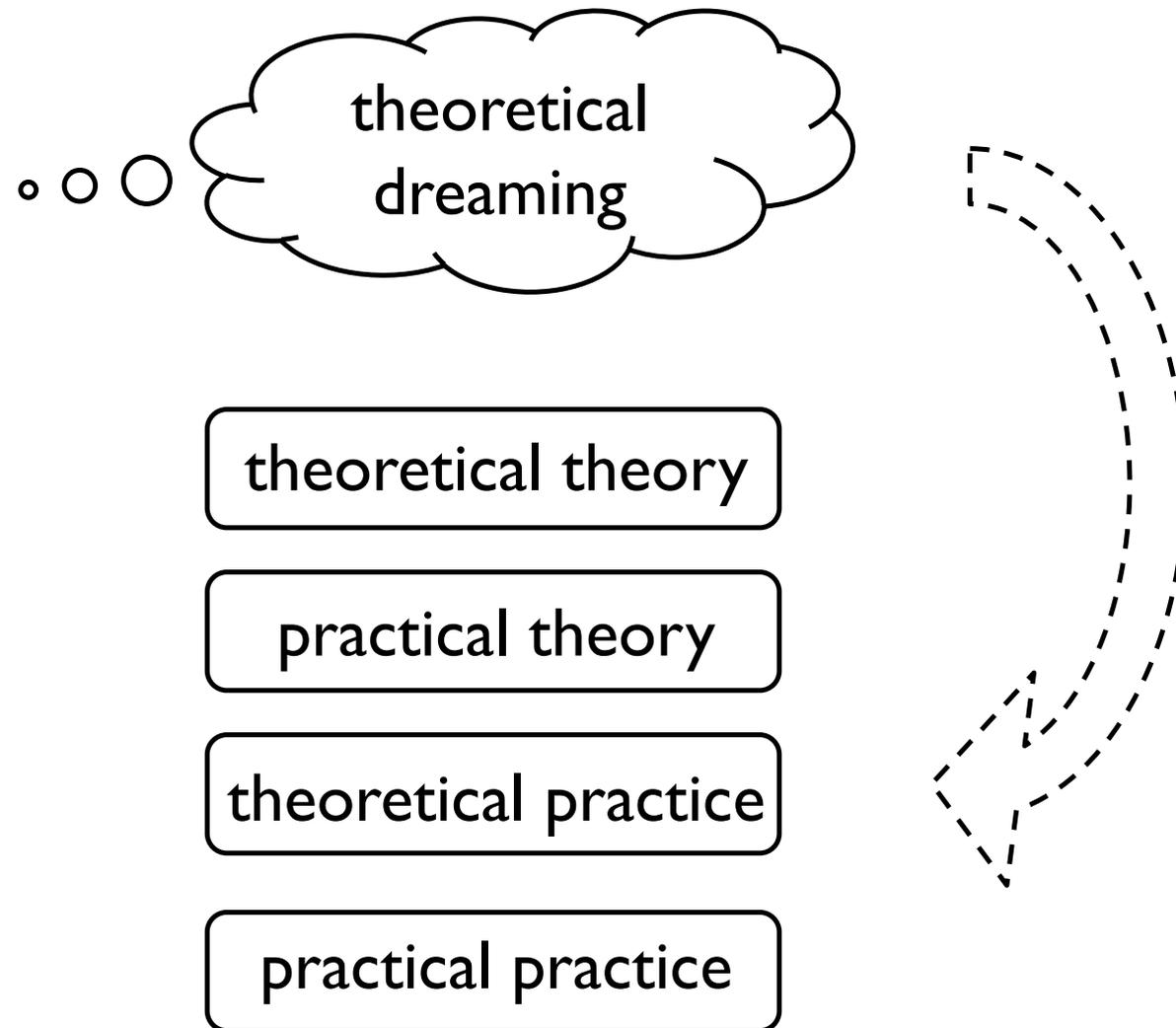


Security

- QKD unconditionally secure
- Authentication is *not unconditional*
 - needs phys. unclonability assumption
 - also exclude emulation by quantum computer + teleport
- MAC key replaced by physical assumptions
 - **authenticated quantum channel !**

Quantum readout of PUFs: practice?

Where do we stand?



Summary

1. PUF with quantum challenge & response
⇒ *no trusted device required!*
2. You can run QKD through a PUF
and at the same time authenticate it.
➤ *authentication of quantum channel vs. classical channel*

	Standard QKD	QKD through PUF
<i>security of key:</i>	identical (unconditional)	
<i>auth. method:</i>	a priori shared key	PUF, no secrets
<i>auth. security:</i>	unconditional	Physical assumptions: - physical unclonability - no quantum emu+teleport