Practical security analysis of PUF-based two-player protocols

CHES, September 11, 2012

Ulrich Rührmair [(1)], Marten van Dijk [(2)]

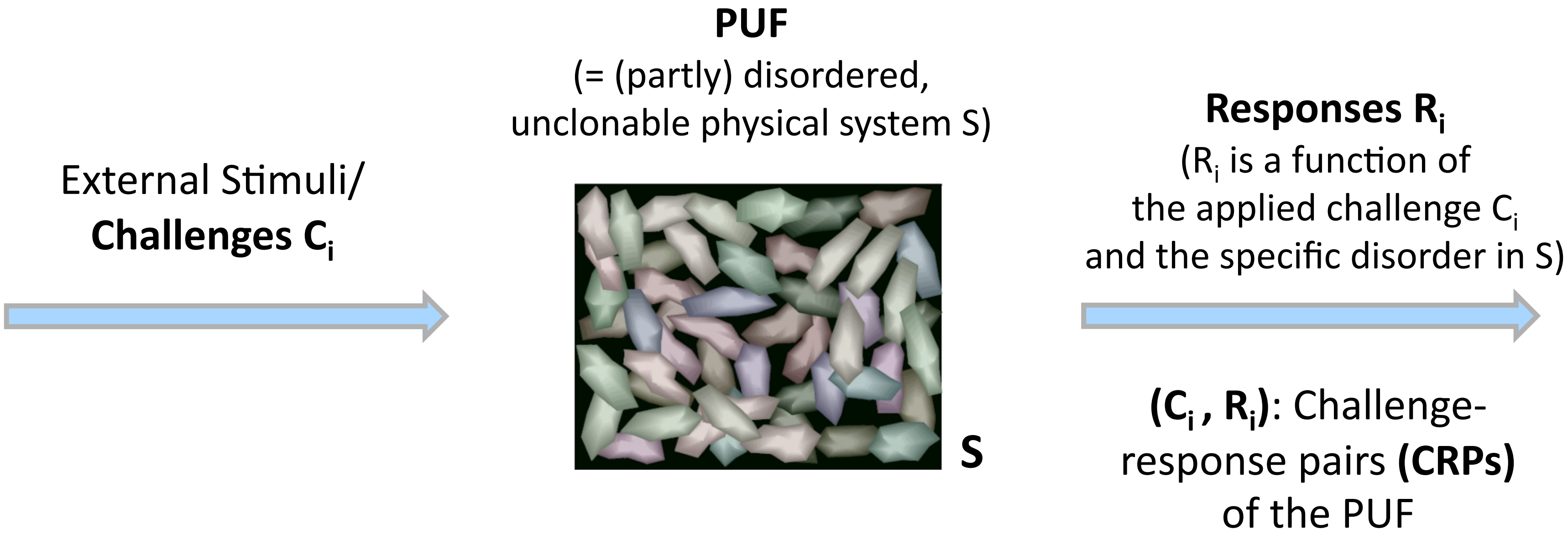
[(1)] Technische Universität München, Germany

[(2)] RSA Laboratories, Cambridge, MA, USA

Outline

1. **Background: PUFs and Oblivious Transfer**
2. Attack on a Recent PUF-based Oblivious Transfer Protocol (CRYPTO'11)
3. Practical Effect of the Attack
4. Countermeasures?
5. Summary

Physical Unclonable Functions (PUFs)



PUF
(= (partly) disordered,
unclonable physical system S)

External Stimuli/
Challenges C_i

S

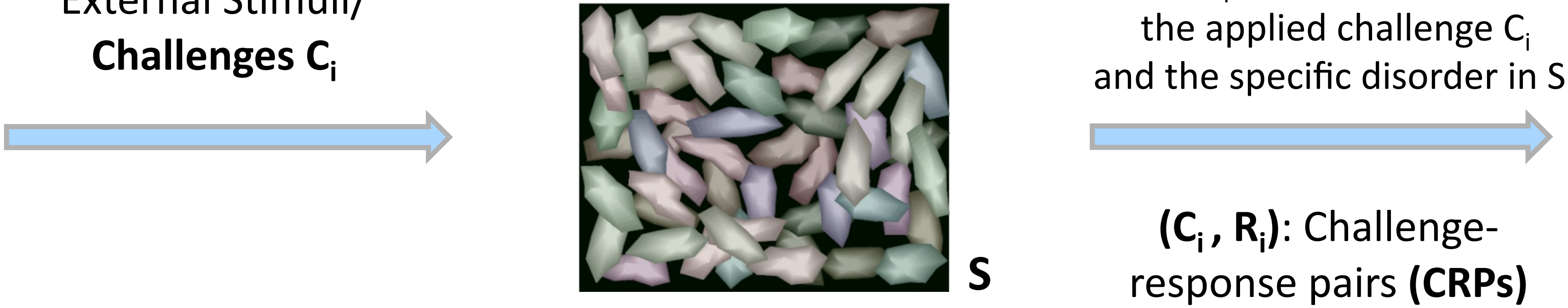
Responses R_i
(R_i is a function of
the applied challenge C_i
and the specific disorder in S)

(C_i , R_i): Challenge-response pairs **(CRPs)** of the PUF

- **„Zoo“ of PUFs [(1)]:** Physically Obfuscated Keys, Weak PUFs, Controlled PUFs, Physical Random Functions, Strong PUFs, Public PUFs, SIMPL Systems, **etc.**
- **This work:** Strong PUFs
(and their use in fundamental cryptographic protocols)

(1) U. Rührmair, S. Devadas, F. Koushanfar: *Security based on Physical Unclonability and Disorder*.
In M. Tehranipoor and C. Wang (Editors): Introduction to Hardware Security and Trust. Springer, 2011.

Physical Unclonable Functions (PUFs)



PUF
(= (partly) disordered,
unclonable physical system S)

External Stimuli/
Challenges C_i

S

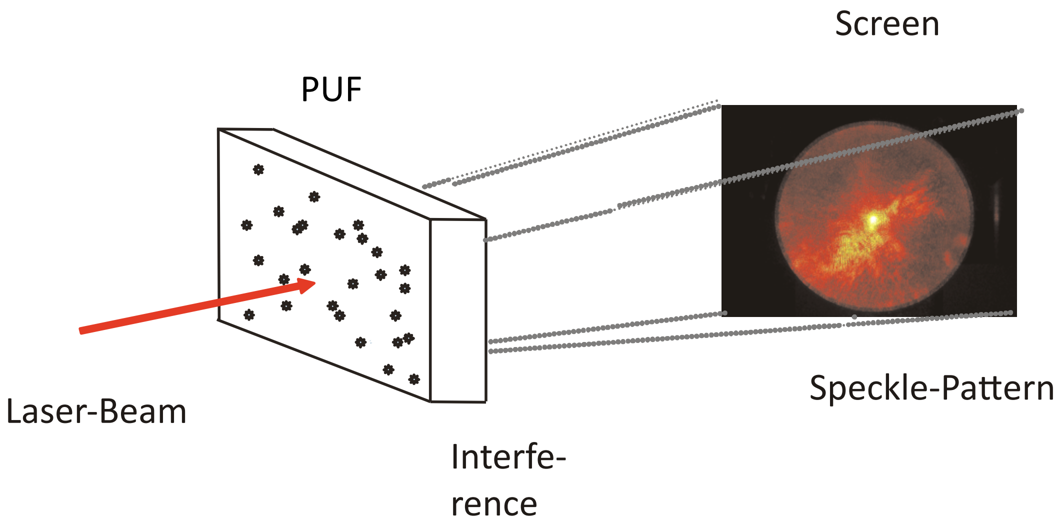
Responses R_i
(R_i is a function of
the applied challenge C_i
and the specific disorder in S)

(C_i , R_i): Challenge-
response pairs **(CRPs)**
of the PUF

Security features of Strong PUFs:

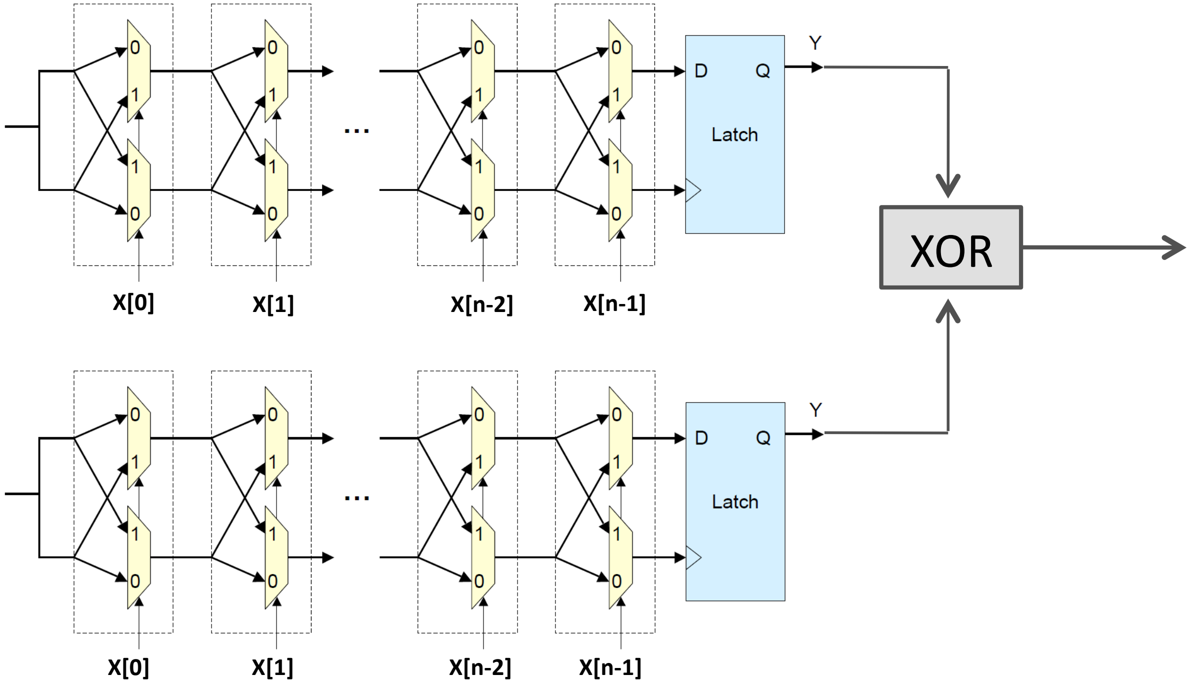
- Challenge-response interface is publicly accessible
  - **Everyone** who holds physical possession of the Strong PUF can freely apply challenges and read out responses
- Very many possible challenges *(ideally exponentially many)*
- No model building/numerical prediction of unknown responses

Two Examples of Strong PUFs



Optical PUF

R. Pappu et al,
Science 2002

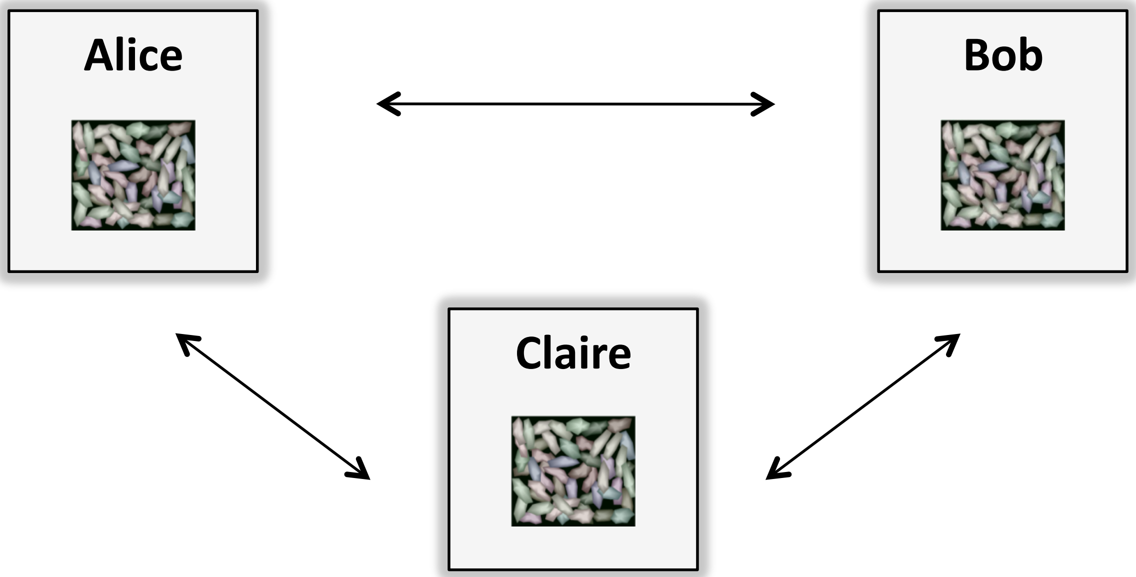


XOR Arbiter PUF
(with at least 6 XORs)

B. Gassend et al,
E. Suh et al
2003/ 2007

Strong PUFs in Cryptographic Protocols

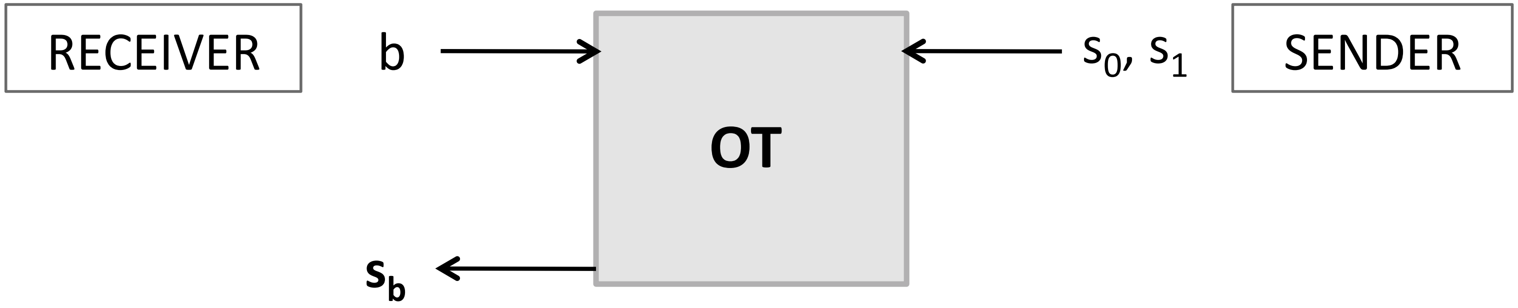
- **Idea:**



- Due to the security features of Strong PUFs:
  *Only the party **currently** in possession of the PUF can determine CRPs.*
- ***Which cryptographic protocols can we build on this simple fact?***

Oblivious Transfer (OT)

- Two-party protocol with the following functionality:
  - *Beginning of Protocol:* **Sender** holds two strings $\boldsymbol{s_0}$ and $\boldsymbol{s_1}$, and **Receiver** holds a choice bit ***b***.
  - *End of Protocol:* **Receiver** has learned the string $\boldsymbol{s_b}$, i.e. the string that he selected by his choice bit ***b***.



- Security requirements:
  - If Sender follows protocol, **Receiver cannot** learn **both** $\boldsymbol{s_0}$ and $\boldsymbol{s_1}$.
  - If Receiver follows protocol, **Sender cannot** learn choice bit ***b***.

Motivation for Studying OT with PUFs

- OT is a fundamental, very powerful cryptographic tool
  - A large number of cryptographic tasks can be reduced to OT:

    Bit commitment, zero-knowledge proofs, key exchange, **any** secure two-party computation [Kilian, STOC 1988]

- Usually, the (im)possibility of OT is studied in order to illustrate the potential of a new cryptographic model
  - Bounded storage model *(yes ✓)*
  - Quantum crypto *(no ✗)*
  - Noise-based crypto *(yes ✓)*
  - PUFs *(yes ✓)* [Rührmair, TRUST 2010; Brzuska, Fischlin, Schröder, Katzenbeisser, CRYPTO 2011]

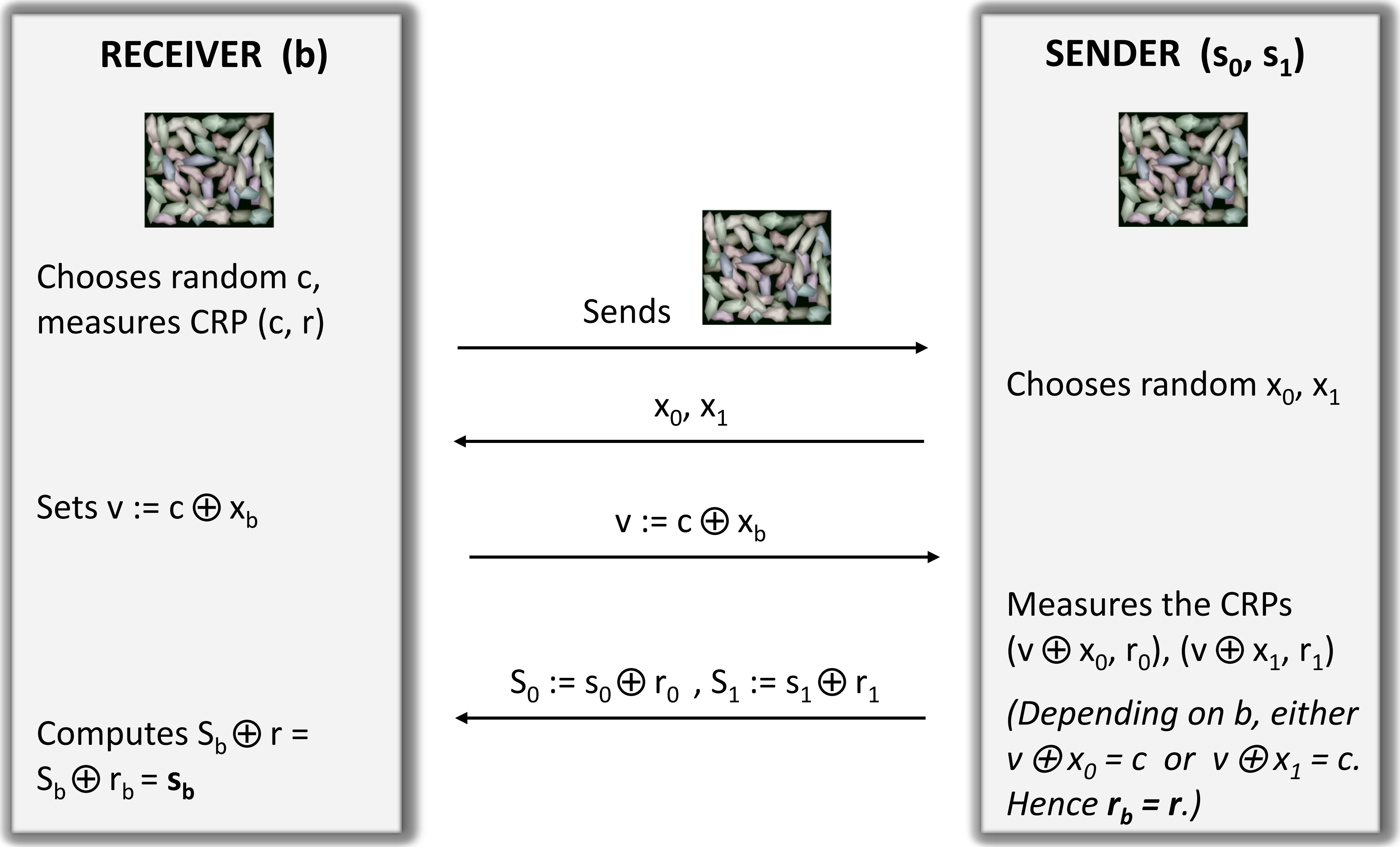
[TRUST '10] U. Rührmair, *Oblivious Transfer based on Physical Unclonable Functions.* TRUST 2010.

[CRYPTO '11] C. Brzuska, M. Fischlin, H. Schröder, S. Katzenbeisser: *Physical Unclonable Functions in the Universal Composition Framework.* CRYPTO 2011.

Outline

1. Background: PUFs and Oblivious Transfer
2. **Attack on a Recent PUF-based Oblivious Transfer Protocol (CRYPTO'11)**
3. Practical Effect of the Attack
4. Countermeasures?
5. Summary

OT-Protocol from CRYPTO'11 (slightly simplified)



RECEIVER (b)

Chooses random c, measures CRP (c, r)

Sets $v := c \oplus x_b$

Computes $S_b \oplus r = S_b \oplus r_b = \mathbf{s_b}$

Sends

x_0, x_1

$v := c \oplus x_b$

$S_0 := s_0 \oplus r_0$, $S_1 := s_1 \oplus r_1$

SENDER (s_0, s_1)

Chooses random x_0, x_1

Measures the CRPs $(v \oplus x_0, r_0)$, $(v \oplus x_1, r_1)$

(Depending on b, either $v \oplus x_0 = c$ or $v \oplus x_1 = c$. Hence $\boldsymbol{r_b = r}$.)

The Attack

WLOG we assume that PUF has challenge space $\mathbf{C} = \{0,1\}^{2n}$

RECEIVER (b)

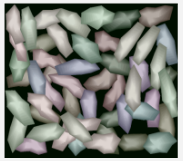
Read out CRPs whose challenges are in set $\mathbf{M}^* = \mathbf{A}^* \cup \mathbf{B}^*$ **, with**

$\mathbf{A}^* = \{\, 0^n || x : x \in \{0,1\}^n \,\},$

$\mathbf{B}^* = \{\, x || 0^n : x \in \{0,1\}^n \,\}.$

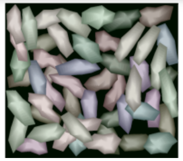
Then $\#M^* = 2^{n+1} << 2^{2n}$

SENDER $(\mathbf{s_0}, \mathbf{s_1})$



Chooses random c, measures CRP (c, r)

Sends



Chooses random x_0, x_1

x_0, x_1

Finds $\mathbf{c_0^* \in A^*}$, $\mathbf{c_1^* \in B^*}$ s.th. $\mathbf{c_0^* \oplus c_1^* = x_0 \oplus x_1}$. Sets $\mathbf{v} := \mathbf{c_0^* \oplus x_0}$

$\mathbf{v} := \mathbf{c_0^* \oplus x_0}$

Measures the CRPs $(\mathbf{v} \oplus x_0, r_0)$, $(\mathbf{v} \oplus x_1, r_1)$ $\mathbf{= (c_0^*, r_0), (c_1^*, r_1)}$ (known to RECEIVER)

$\mathbf{S_0} := \mathbf{s_0 \oplus r_0}$, $\mathbf{S_1} := \mathbf{s_1 \oplus r_1}$

Obtains $\mathbf{s_0 = S_0 \oplus r_0}$ and $\mathbf{s_1 = S_1 \oplus r_1}$

Outline

1. Background: PUFs and Oblivious Transfer
2. Attack on a Recent PUF-based Oblivious Transfer Protocol (CRYPTO'11)
3. **Practical Effect of the Attack**
4. Countermeasures?
5. Summary

Practical Effect of our Attack

- Are quadratic attacks relevant at all?
  - *Example RSA:* Not very relevant
  - *Example SHA-1, single-round DES:* Highly relevant!
- We argue that PUFs are closer to SHA-1 or single-round DES
  - **Reason:** PUFs are finite physical systems;
    cannot be scaled indefinitely due to size, cost and stability issues
- Two examples:
  - Crypto‘11 protocols **+** Optical PUFs
    (suggested explicitly in extended version of CRYPTO’11)
  - Crypto‘11 protocols **+** electrical XOR Arbiter PUFs of bitlength 64
    (currently most popular electrical Strong PUFs)

Electrical PUFs

- XOR Arbiter PUF with challenge length 64 bits
  - 2^{64} challenges

- Reduced to $\mathbf{2^{33} = 8.58 \times 10^{9}}$ challenges by our attack, which malicious party must read out in order to cheat.

- This takes **144 min** *(at read-out rate of 1 MHz* [1]*)*

[1] Lee, J.-W., Lim, D., Gassend, B., Suh, G.E., van Dijk, M., Devadas, S.: *A technique to build a secret key in integrated circuits with identification and authentication applications.* In: Proceedings of the IEEE VLSI Circuits Symposium (June 2004)

Optical PUFs

- Pappu et al [Science2002]: Optical PUF of size **1 cm × 1 cm** possesses **2.37 × 10^{10}** independent, decorrelated CRPs
- Reduced to **5.2 × 10^{5}** CRPs by our attack,
  which malicious party must read out in order to cheat
- This takes: **14.4 hours** *(read-out rate of 10 CRPs/sec)*
  87 minutes *(read-out rate of 100 CRPs/sec)*
- If you want to increase these read-out times by a factor of 10, then you must use an optical PUF of size **10 cm × 10 cm**
  - Does not even fit onto a smart card! ☹

Outline

1. Background: PUFs and Oblivious Transfer

2. Attack on a PUF-based Oblivious Transfer Protocol (CRYPTO’11)

3. Practical Effect of the Attack

4. **Countermeasures?**

5. Summary

Countermeasures

- Use OT-protocol from TRUST‘10 (with interactive hashing step)
  - Better security, can be used safely with optical PUFs and 64-bit electrical PUFs
  - But leads to increased round complexity
  - ***Future work:*** interactive hashing variants with constant rounds [1]
- *Probably:* Use CRYPTO‘11 protocols with electrical PUFs with longer bitlength, e.g. 128 bits
  - *Still needs to be fully confirmed in future work;* requires security properties of the PUF that go beyond the usual unpredictability feature

[1] Marten van Dijk, Ulrich Rührmair: *Physical Unclonable Functions in Cryptographic Protocols: Security Proofs and Impossibility Results.* Cryptology ePrint Archive, 2012.

Outline

1. Introduction: PUFs and Cryptographic Protocols

2. Quadratic Attack on a PUF-based Oblivious Transfer Protocol (CRYPTO'11)

3. Practical Effect of the Attack

4. Countermeasures?

5. **Summary**

Summary

- Discussed work concerning the use of PUFs in fundamental cryptographic protocols
  - Relatively recent, emerging branch
- Devised quadratic attacks on recent OT- (and BC-) protocols from CRYPTO'11
- Attacks make protocols insecure when they are employed with optical PUFs, or with Arbiter PUFs of challenge length 64 bits
  - Special relevance of these two implementations
- Briefly discussed countermeasures
  - Use interactive hashing and OT-protocols from TRUST'10 *(✓)*
  - Electrical PUFs with longer challenge bit length *(?)*

Thanks!