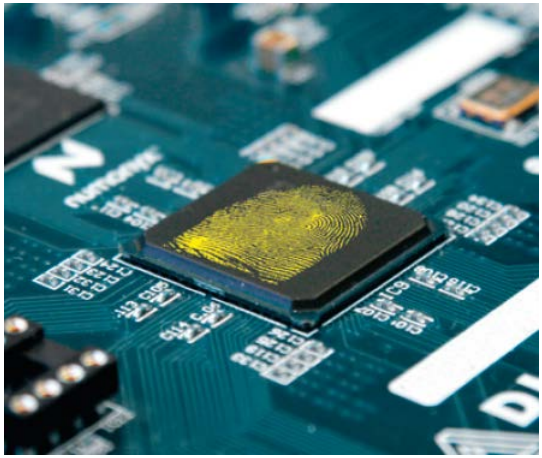
SMART GRID PROTECTION AGAINST CYBER ATTACKS

SPARKS Smart Grids Week Stakeholder Workshop

Smart meter (gateway) authentication and key management using hardware PUFs

EU FP7 Programme Contract No. 608224

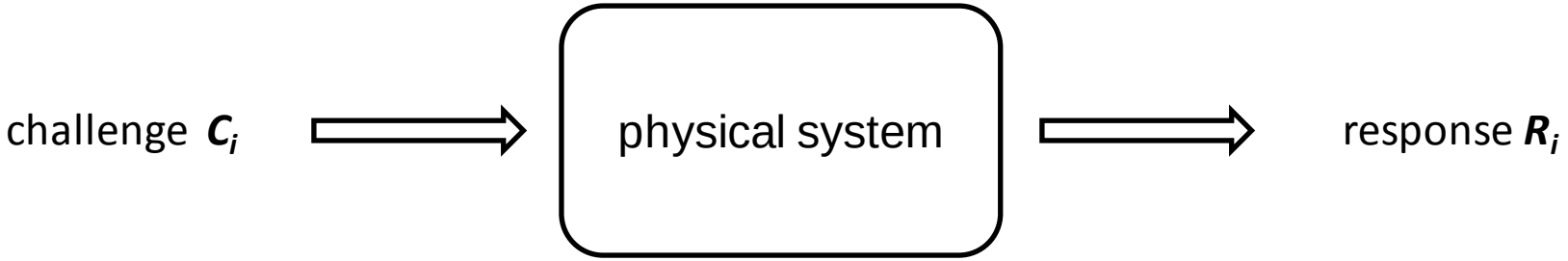
Physical structures are unique



- every physical object is unique, has a specific “fingerprint”
- fingerprint enables **identification**
- challenge-response-behaviour of physical structure enables **authentication**
- keeping the fingerprint secret enables **cryptographic key generation**
- however, measuring physical properties inevitably involves noise

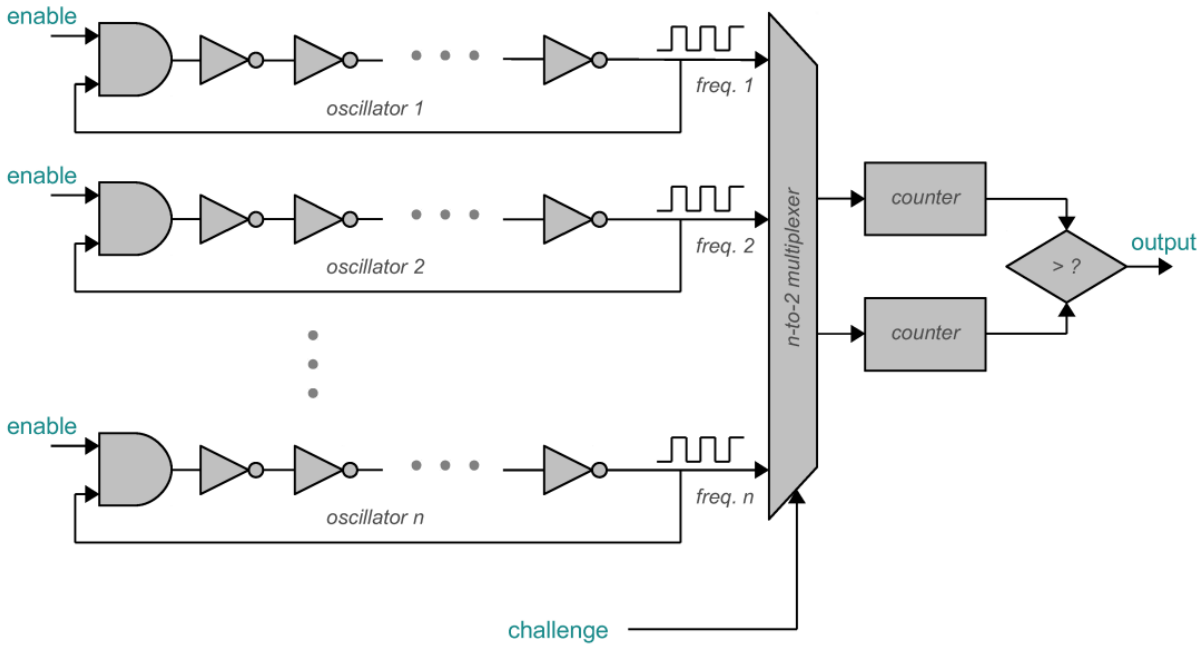
EU FP7 Programme Contract No. 608224

What is a PUF?



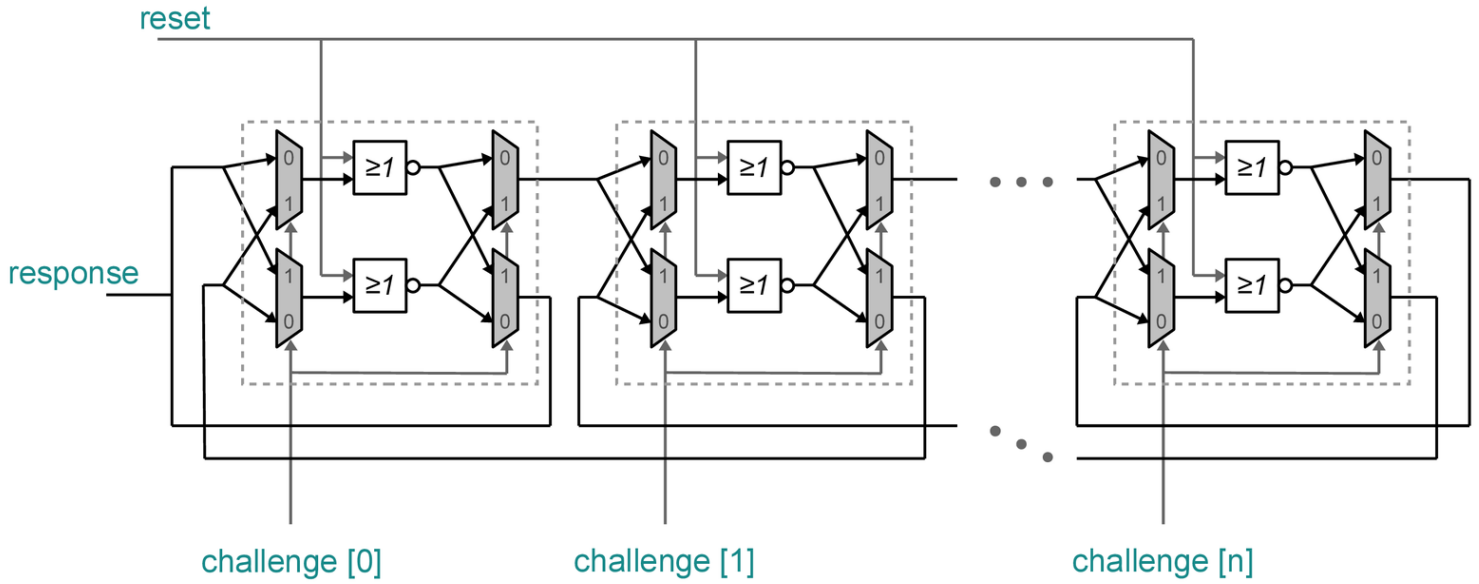
- Physical Unclonable Function (PUF)
  - physical information storage system
  - challenges (addresses) lead to responses (data), similar to a memory
  - physical properties influence challenge-response mapping

Ring Oscillator PUF (RO PUF)



- unique ring oscillator frequencies
- one of the most non-biased PUF statistics
- implementable in CMOS chips and FPGAs

Twisted Bistable Ring



- unique oscillation/settling behavior
- more complex and ressource efficient than RO PUF
- implementable in CMOS chips and FPGAs

PUF Applications Possibilities (1)

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- Cryptographic key generation
  - noisy fingerprint can be used as device-specific bit string
  - helper data algorithms allow for reliable key generation
- Advantages
  - CMOS devices can extract secret keys without on-chip NVM
  - no binary key present in powered-off state
  - higher resilience against optical inspection compared to fuses and ROM
- Disadvantage
  - off-chip helper data storage and enrolment phase required

EU FP7 Programme Contract No. 608224

PUF Applications Possibilities (2)

- Authentication by external challenges
  - challenge-response behavior of a PUF is exploited
  - verifier authenticates PUF with precollected challenge-response pairs
  - requires a sufficiently complex PUF

- Advantages
  - Challenge-response authentication without binary key on device
  - Maybe even possible in pure CMOS devices, without NVM

EU FP7 Programme Contract No. 608224

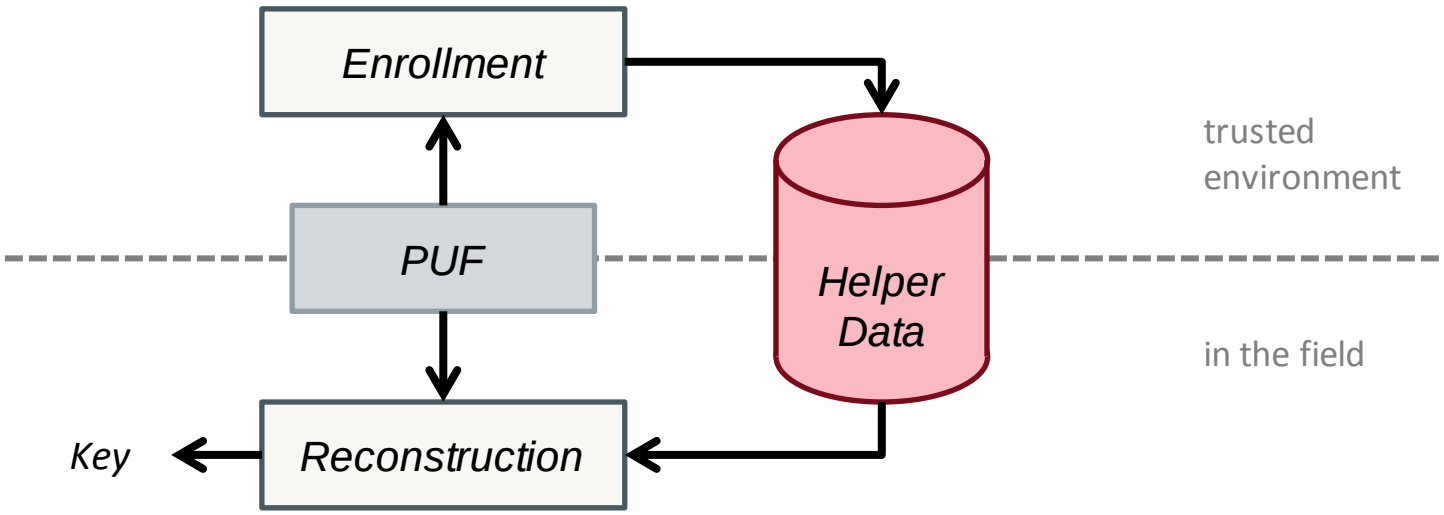
PUF Applications Possibilities (3)

- Authentication by external challenges and public models
  - Challenge-response behavior of a PUF is exploited
  - Verifier authenticates PUF responses with public simulation model
  - Security relies on PUF providing the response always faster than model
  - Time difference not proven yet

- Advantages
  - Device authentication without any secret information in device
  - Technology barrier hinders physical cloning

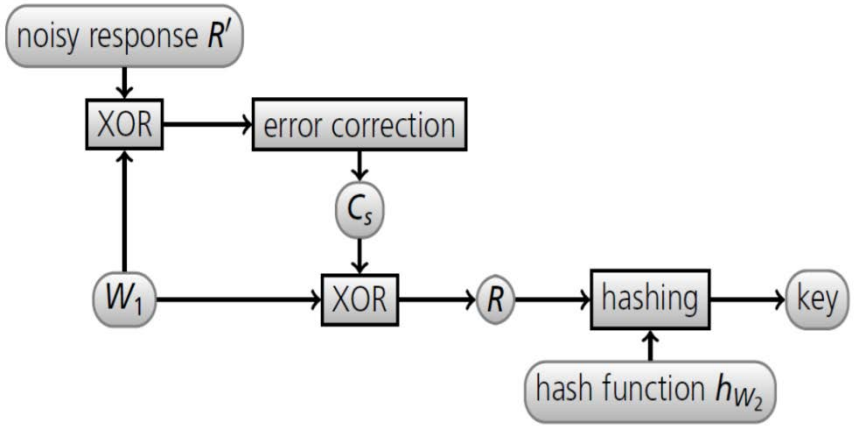
Key Generation Basics

- Two phases required
  - Enrollment: key is defined and helper data (HD) is generated
  - Reconstruction: key is recovered from noisy PUF response bits



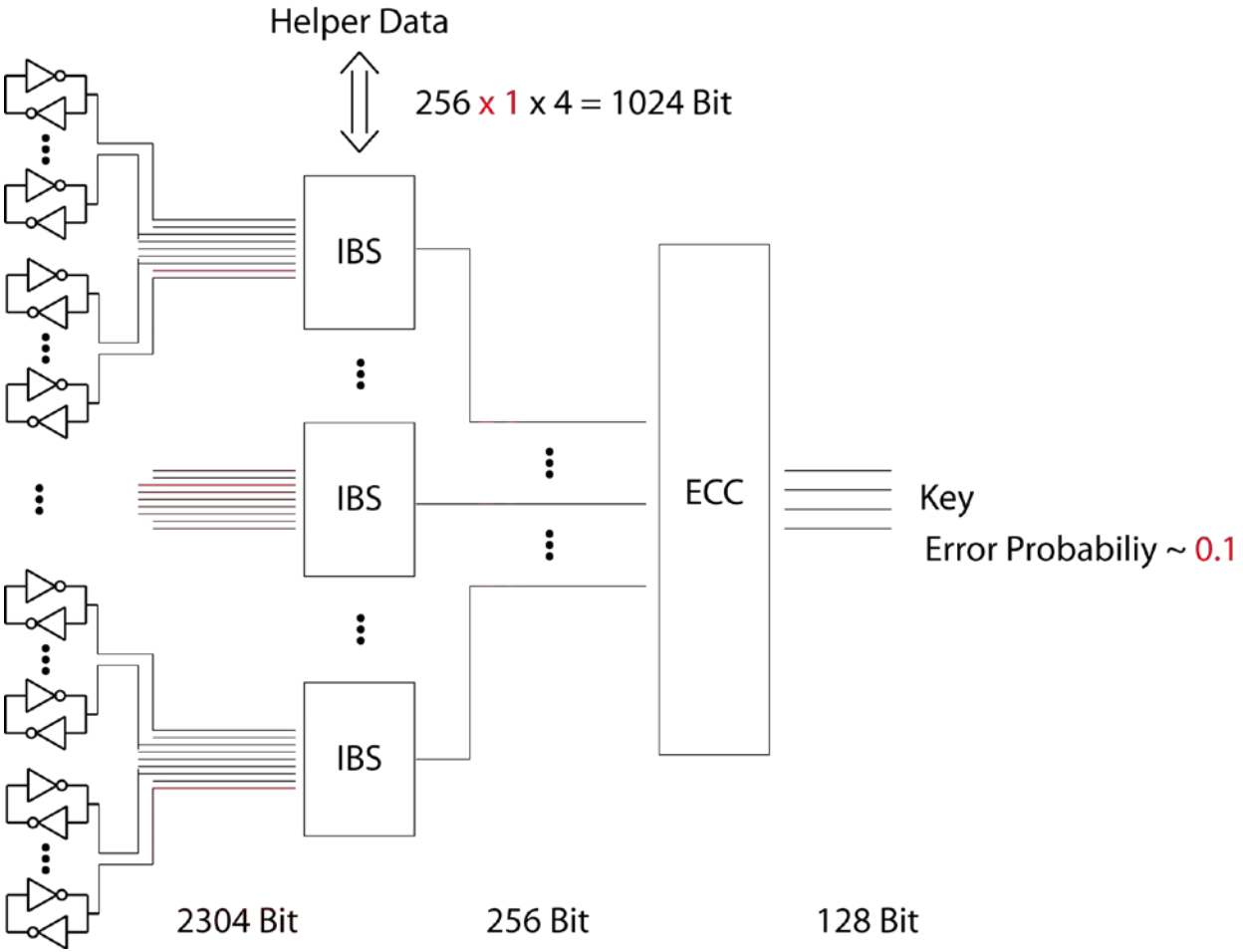
Code-Offset Fuzzy Extractor

- Enrollment
  - HD: XOR of PUF response bits and random codeword
  - Key extracted from PUF bits by extractor algorithm, e.g. Toeplitz hash



- Reconstruction
  - XOR of HD and noisy PUF response bits yields noisy codeword
  - Codeword can be corrected by error-correcting code
  - XOR of corrected codeword and HD yields original PUF response bits
  - Key can be extracted again by extractor algorithm

Complementary Index-Based Syndrome Coding (C-IBS)



Smart Meter Security

- exposed to physical attacks
  - at the premise of end-users
  - interest in manipulation
- interesting target
  - financial damage
  - entry point to the smart grid infrastructure
- PUFs have a high level of protection against physical attacks
  - not explicitly stored
  - opening the PUF destroys the information

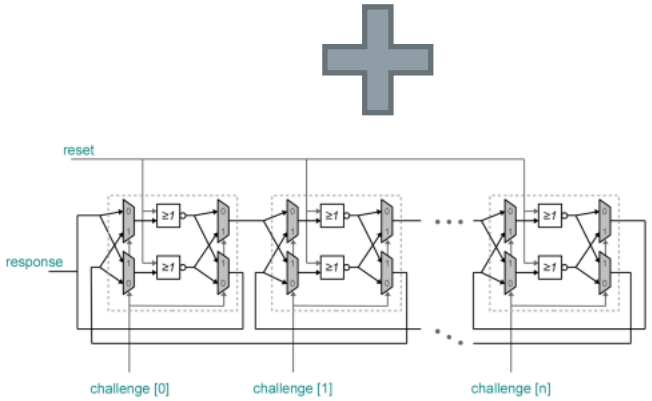
EU FP7 Programme Contract No. 608224

SPARKS mini-project

- Smart meter and gateway authentication and key management using hardware PUFs
  - novel smart meter authentication and key management based on PUFs
  - establish a smart meter hardware reference architecture
  - investigation into existing hardware PUF designs
  - selection of a PUF design for this mini-project
    - smart meter architecture
    - environmental conditions
    - lightweight PUF
  - integrated the PUF into a prototype smart meter using FPGA devices
  - develop a key generation facility based on the on-board PUF
  - lightweight authentication protocol
  - validate the smart meter PUF in a lab based test network
  - prepare an enhanced smart meter bill of materials, and an authentication/key management deployment architecture

Smart Meters with PUFS

- provides high level of security
- technologically and scientifically challenging
- in the long run: no extra hardware needed (costs!)
- smart meters are not only a good candidate but also a good showcase for PUF technologies



Questions

How are your smart meters connected to the business infrastructure? (public/private network, protocols, server side)

By which means is authenticity and integrity of the smart meter data ensured?

Where else could you imagine PUF technologies can be used a key generation and authentication facility?

What would be the requirements to use smart meters with PUFs in your infrastructure?

Thank you for your attention

Dr. Martin Hutle

Fraunhofer Institute for Applied and Integrated Security (AISEC)

Department for Product Protection and Industrial Security

+49 89 3229986-135

martin.hutle@aisec.fraunhofer.de

Fraunhofer AISEC
Parkring 4
85748 Garching
Germany

www.aisec.fraunhofer.de

EU FP7 Programme Contract No. 608224