Physical Aspects of Digital Security

2IMS10

Lecturer: Boris Škorić

b.skoric@tue.nl
https://oncourse.tue.nl/2015/course/view.php?id=71

What is this course about?

- Digital security
- Interaction with physical environment
- Algorithms

Not: side channels
Not: physics

Topics covered

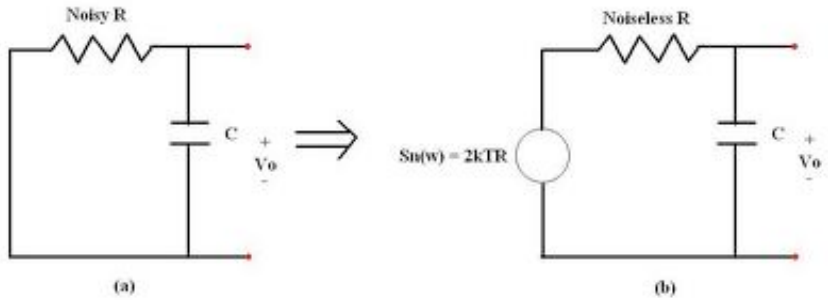
- Physical randomness
  - how to make it uniform (TRNG)
  - how to exploit it (key generation)
- Physical Unclonable Functions (PUFs)
  - anti-counterfeiting & authentication
  - key storage
  - software-to-hardware binding
- Distance bounding
- Quantum Key Exchange
- Quantum Readout of PUFs
- Quantum Computing

Organisational matters

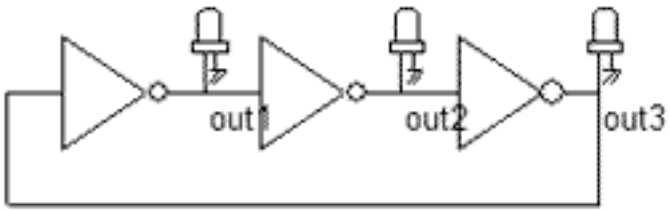
- Lectures
  - 4 hours per week
  - English
  - no separate instruction classes
  - ask questions!
- All slides etc. are online
- Printed lecture notes
- Grading
  - written exam
  - homework problems (not mandatory):

    whole point extra if good enough!

Bird's eye view: True Random Numbers



Noisy resistor: thermal noise



Ring oscillator

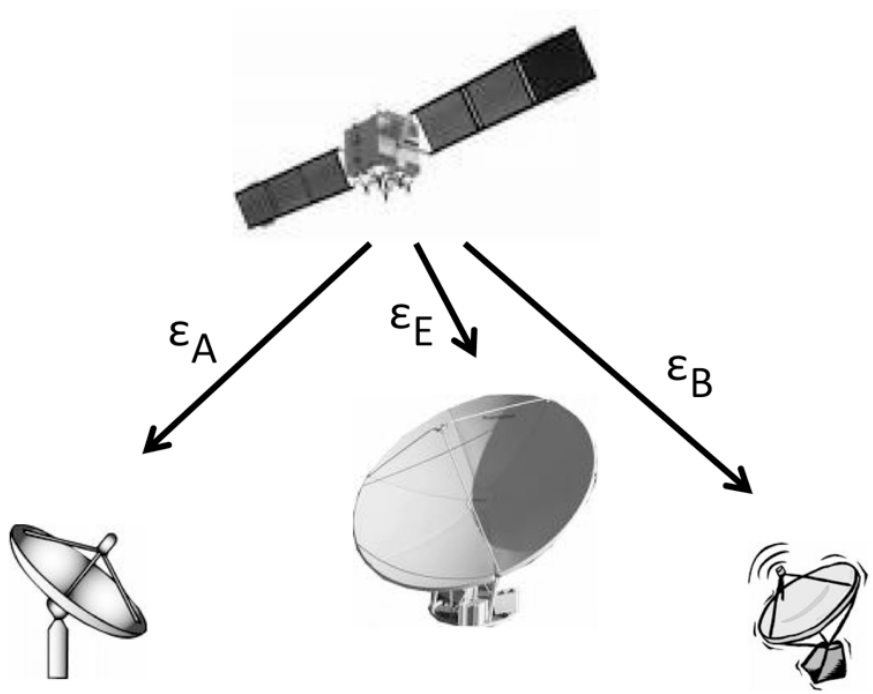
Radio-active decay

- Physical sources of randomness
  - true random number generation
  - data not uniformly distributed
  - *algorithms for making it uniform*

Bird's eye view: exploiting noise

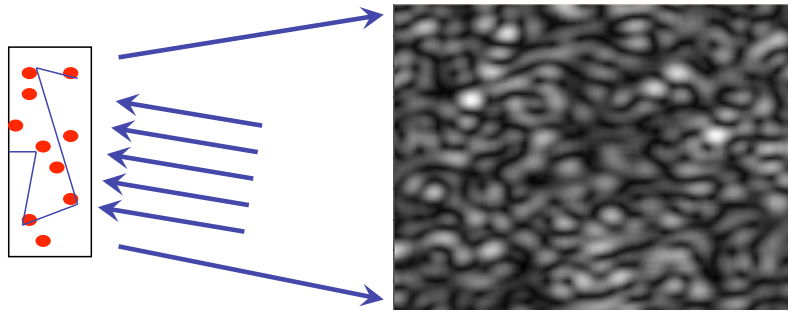
Noise as a <u>resource</u> instead of a nuisance

Secret key generation in an "impossible" setting



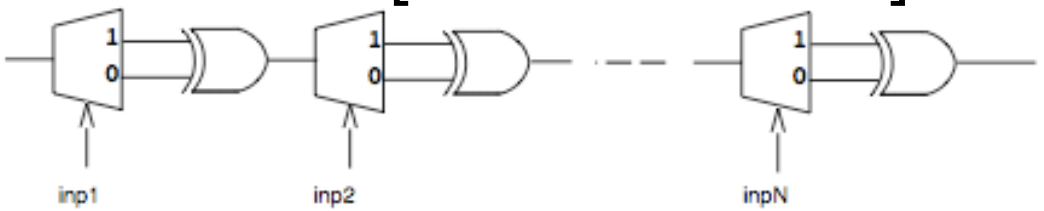
Bird's eye view: PUFs

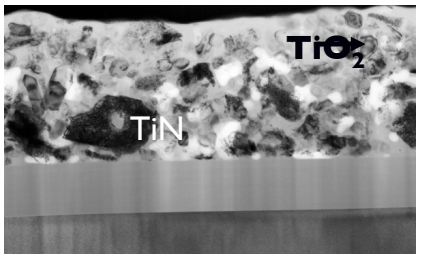
- Relatively new security primitive (2001)
- Physical Unclonable Function
  - complex piece of material
  - challenge-response behaviour
  - difficult to characterize
  - difficult to clone physically
  - difficult to emulate
- Various applications
  - anti-counterfeiting
  - authentication token
  - secure key storage
  - software to hardware binding
  - tamper evidence



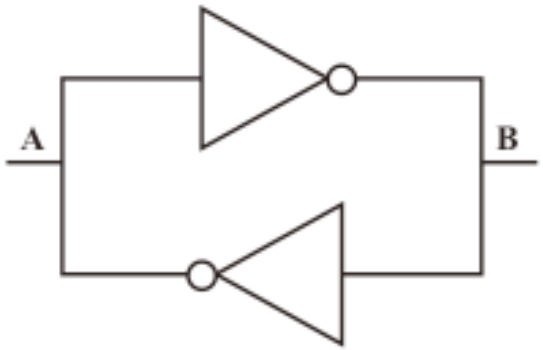
Optical PUF
Pappu 2001

Silicon PUF [Gassend et al. 2002]

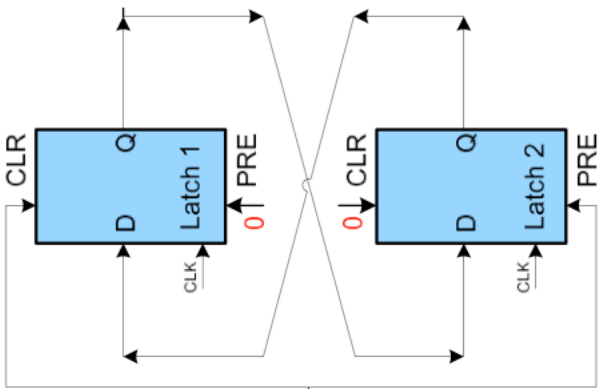




Coating PUF
Posch 1998; Tuyls et al. 2006



SRAM PUF
Guajardo et al.
Su et al. 2007

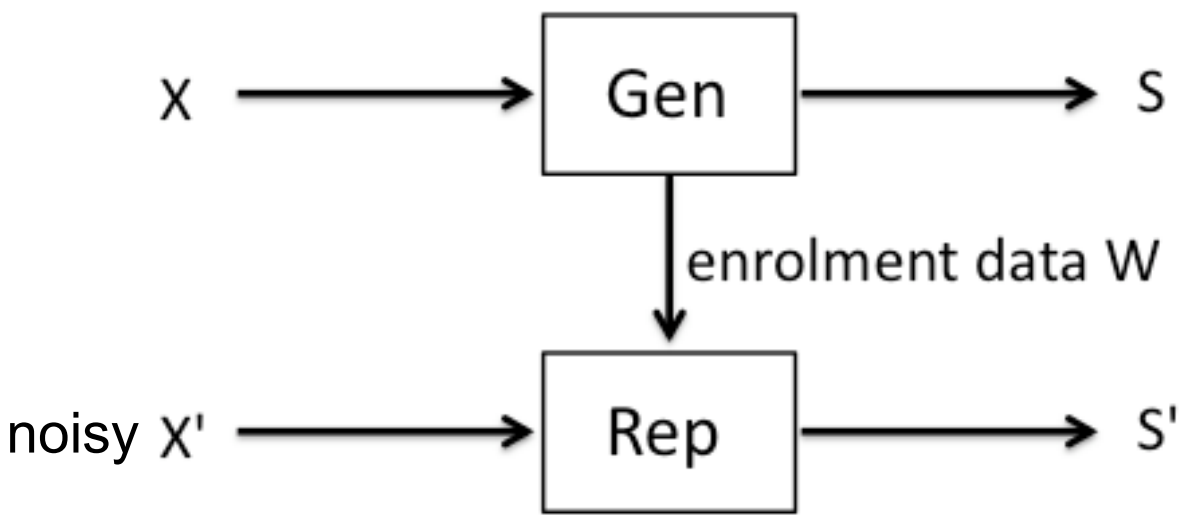


FPGA 'butterfly' PUF
Guajardo et al.
Su et al. 2007

Bird's eye view: Fuzzy Extractors

Secret key generation from common randomness

- error correction
- redundancy data must not leak about secret!
- secret must be uniform

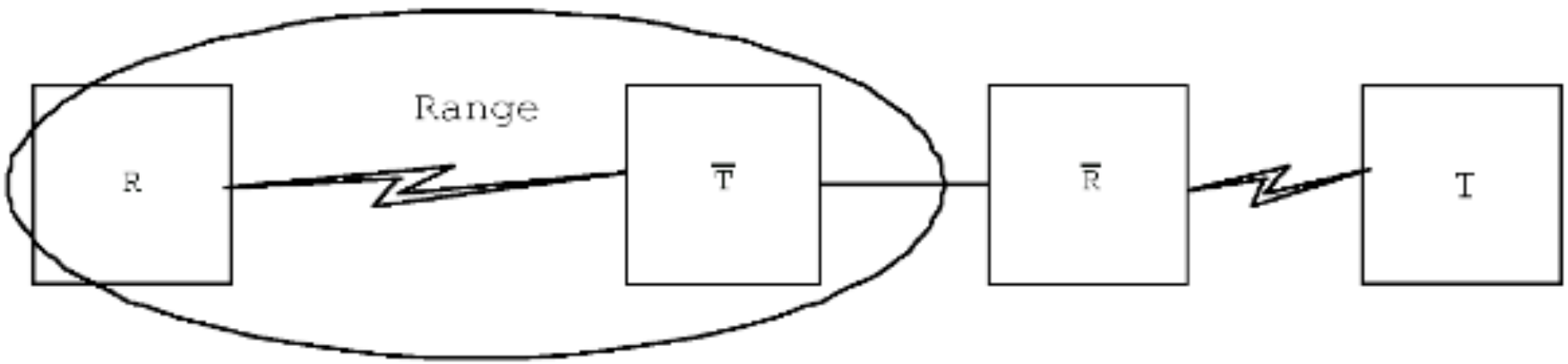


Bird's eye view: Distance bounding

Some protocols are vulnerable to relay attacks

- "mafia fraud"
- "terrorist fraud"

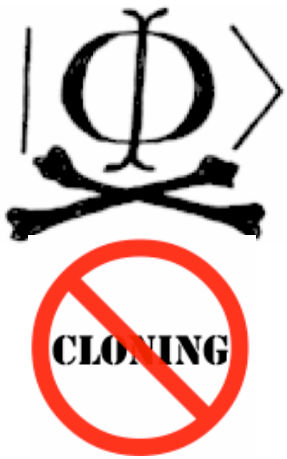
How to verify distance reliably and efficiently



Bird's eye view: Quantum Key Exchange

Exploit special properties of quantum physics

- measuring destroys information
- no cloning theorem



Alice and Bob generate a secret key

- insecure (but authentic) classical channel
- quantum channel
- error correction & privacy amplification
- eavesdropping is detected
- *unconditional security* of the key

Bird's eye view: Quantum Readout

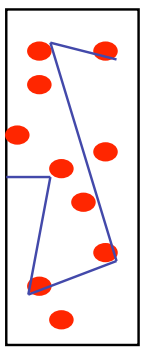
Remote authentication of "public" PUF

- Impossible with classical physics.
- Quantum physics can hide the challenge.

Single-quantum challenge and response

$|\psi\rangle$

$R\,|\psi\rangle$



Bird's eye view: Quantum Computing

Quantum parallel computation

- superposition of logical states
- operate on all states simultaneously
- interference of all these computations

Special algorithms

- Shor 1994: factorization (**breaking RSA**)
- 1999: discrete logs (breaking ECC)
- Grover 1996: searching unordered lists