Behaviour Analysis and Improvement of the Proposed PUF on FPGA
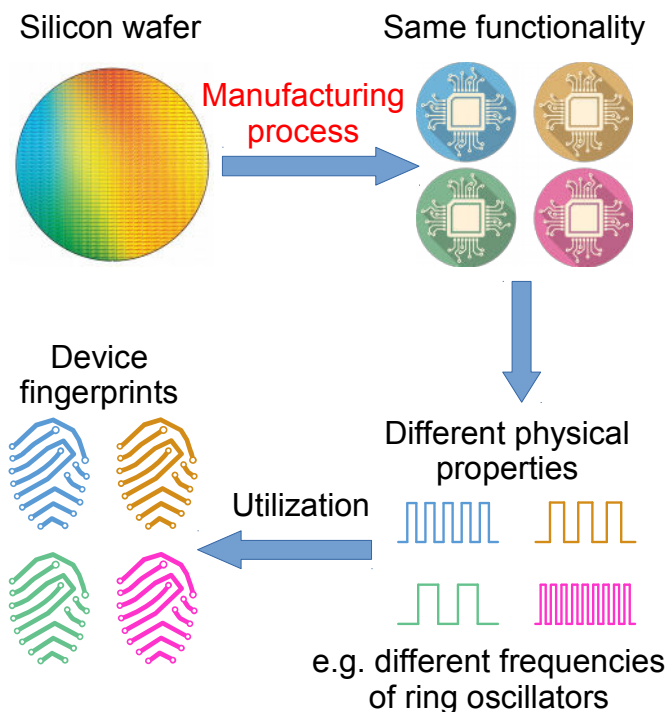
Filip Kodýtek   Supervised by Róbert Lórencz

Faculty of Information Technology, Czech Technical University in Prague

Physical Unclonable Function (PUF)

- Function based on physical system
- Each electronic device has unique physical properties
  - Arise due to random variations in the manufacturing process
    - Source of randomness for PUF
  - Forms a *"fingerprint"* of the device

Silicon wafer   Same functionality

Manufacturing process

Device fingerprints

Utilization   Different physical properties

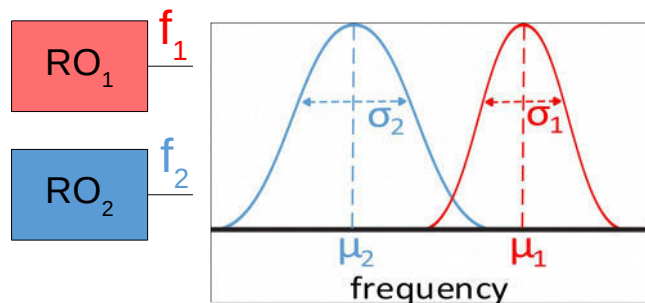e.g. different frequencies of ring oscillators

PUF's applications

- Device identification
- Authentication
- **Cryptographic key generation**
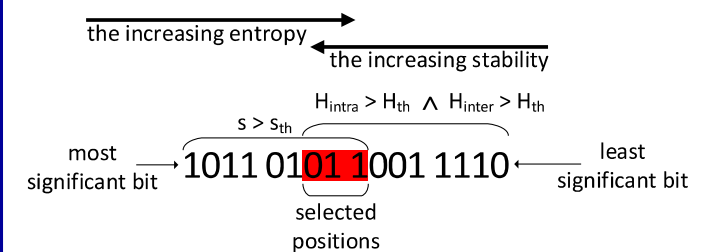 - Instead of storing the keys in memory

PUF proposal

- Delay-based PUF
  - Random variations in delays of logic gates and their interconnects
    - **Affects frequencies of ring oscillators (RO)**

RO$_1$ f$_1$

RO$_2$ f$_2$

σ_2 σ_1

μ_2 μ_1

frequency

- Pair of ROs is measured
- Result: binary counter value

$$Counter\ value = \frac{f_2}{f_1} \times 2^n$$

Selection of suitable positions for PUF

the increasing entropy

the increasing stability

$H_{intra} > H_{th} \wedge H_{inter} > H_{th}$

$s > s_{th}$

most significant bit → 1011 0101 01 1001 1110 ← least significant bit

selected positions

Results

Positions	7-8	7-9	7-10	8-9
w	2	3	4	2
HD$_{intra}$	1.37%	1.77%	2.71%	2.63%
HD$_{inter}$	48.49%	49.06%	49.32%	50%

- Easy to implement PUF design
- Multiple output bits from each RO pair
- Stable and unique PUF responses
- Influence of voltage and temperature on stability is investigated

Publications

- 2 articles in **impact journals**
  - Kodýtek, F.; Lórencz, R.: Proposal and Properties of Ring Oscillator-Based PUF on FPGA. In Journal of Circuits, Systems and Computers
  - Kodýtek, F.; Lórencz, R.; Buček, J. Improved ring oscillator PUF on FPGA and its properties. In Microprocessors and Microsystems
- 3 publications on **IEEE conferences**
- 5 publications on international workshops