Analysis of Ring Oscillator PUFs on 60nm FPGAs

30th of May 2013

Linus Feiten, Andreas Spilla, Matthias Sauer, Tobias Schubert, Bernd Becker
Physically Unclonable Functions (PUF)

- Should be **unique**. (different for different chips)
- Should be **reliable**. (the same for the same chip)
Ring-Oscillator Physically Unclonable Functions

**Challenge:** select two ROs for comparison

**Response:**
1, if $c_A > c_B$
0, else

Different frequencies

- $RO_1$
- $RO_2$
- $RO_m$
Implementation on Altera Cyclone IV FPGAs

- Altera Cyclone IV EP4CE22F17C6N (60 nm) on Terasic DE0-Nano Development Board
Implementation on Altera Cyclone IV FPGAs

**Logic Array Block (LAB)** holding 16 LEs

**Logic Element (LE)** containing LUTs to realise any 4-input function
Implementation on Altera Cyclone IV FPGAs

Logic Array Block (LAB) holding 16 LEs

Logic Element (LE) containing LUTs to realise any 4-input function

Ring Oscillator (RO)

enable  \[ \begin{array}{c}
\text{(one LE)} \\
\text{(one LE)} \\
\text{(one LE)} \\
\text{(one LE)} \\
\text{(one LE)} \\
\end{array} \]

output
Implementation on Altera Cyclone IV FPGAs

PUF implementation with Altera Quartus Software

(ardous but possible)

• Define “LogicLock regions” to be addressed in VHDL.
  (One LogicLock region per Ring Oscillator.)

• Use “LCELLs” as delay elements.
  (Not optimised away by compiler.)

• Manually reconfigure the routing within each LogicLock region.
  (Takes most time!!)
Experiments

- 20 FPGAs
- 64 ROs (2016 possible RO comparisons)
- Selected 128 RO comparisons (challenges) $\Rightarrow$ 128 response bits
Experiments

- 20 FPGAs
- 64 ROs (2016 possible RO comparisons)
- Selected 128 RO comparisons (challenges) ⇒ 128 response bits
- Quality measures:
  - Inter-Distance (**Uniqueness**)
    “Is the response of each FPGA unique?”
    ⇒ Hamming-distance between responses of all FPGAs.
    **Optimum**: 50%
  - Intra-Distance (**Un-reliability**)
    “Do the responses of one FPGA differ?”
    ⇒ Hamming-distance between 100 responses of one FPGA.
    **Optimum**: 0%
Experiments
Experiments

Ring Oscillator length

3 LEs  16 LEs  18 LEs
Experiments

Ring Oscillator length

Uniqueness (50% optimal)

Un-reliability (0% optimal)
Experiments

Ring Oscillator length

For remaining experiments: always length 16
Experiments

Ring Oscillator placement (1)
Experiments

Ring Oscillator placement (1)

Controller Logic

Ring Oscillators

Uniqueness (50% optimal)

Un-reliability (0% optimal)
Experiments

Ring Oscillator placement (2)

Controller Logic and Ring Oscillators

Uniqueness (50% optimal)

Un-reliability (0% optimal)
Experiments

Ring Oscillator
distribution structure

1  2  3
Experiments

Ring Oscillator distribution structure

1

2

3

Uniqueness (50% optimal)

Un-reliability (0% optimal)

Structure type

Structure type
Conclusion

- Demonstrated **feasibility** of RO-PUFs on *Altera* FPGAs.
- Identified **optimal RO length** to be 16 LEs (spanning one LAB).
- Discovered **anomalous** RO placement and structure **configurations**.

- Further results (not presented here):
  - Ambient temperature
  - On chip activity

  (Still good PUF quality!)