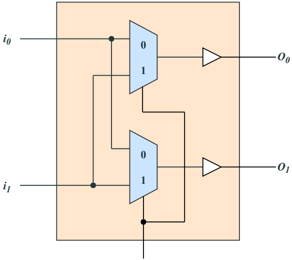
# On Statistical Properties of Arbiter Physical Unclonable Functions

Phillip Gajland



Examiner: Prof. Dr. Elena Dubrova
Supervisor: Dr. Felipe Marranghello

# TODAY

| | | |
|---|---|---|
| Motivation | - | Why should you care? |
| Background | - | What do you need to know? |
| Arbiter PUFs | - | What are they? |
| Example | - | How does it work? |
| Proof of Conflict | - | What’s the problem? |
| Solution | - | How do we fix it? |
| Simulation | - | What did we do? |
| Results | - | What did we find? |
| Summary | - | In short? |
| Conclusion | - | And what? |

# MOTIVATION

# MOTIVATION

50 billion IoT devices by 2020

# MOTIVATION

50 billion IoT devices by 2020:

- DDoS attacks e.g. Dyn cyberattack 2016

Intellectual property theft:

- Unique device identifiers
- Secure key storage (not battery backed SRAM or eFuses)

Devices using PUFs:

- Xilinx Zynq Ultrascale+
- Altera Stratix 10 FPGAs

# MOTIVATION

Figure: Altera Stratix 10 FPGA

# BACKGROUND

# BOOLEAN FUNCTIONS

**Table:** There are $2^{2^n}$ different n-variable Boolean functions.

| No. of variables (n) | Number of different functions (f) |
|---|---|
| 1 | 4 $(0, 1, x, \overline{x})$ |
| 2 | 16 $(0, 1, x_1, x_2, \overline{x_1}, \overline{x_2}, x_1 \oplus x_2,$ etc) |
| 3 | 256 $(0, 1, x_1, x_3, \overline{x_1}, \overline{x_2}, x_2 \oplus x_3,$ etc) |
| 4 | 65,536 $(0, 1, x_1, x_4, \overline{x_1}, \overline{x_2}, x_3 \oplus x_4,$ etc) |
| $\vdots$ | $\vdots$ |
| n | $2^{2^n}$ $(0, 1, x_1, x_n, \overline{x_1}, \overline{x_2}, x_3 \oplus x_n,$ etc) |

# PHYSICAL UNCLONABLE FUNCTIONS

Digital fingerprint for Integrated circuits

Manufacturing differences give rise to a race condition

Mapping between challenges and responses

Challenge Response Pair (CRP) can be evaluated in the form of a Boolean Function

# ARBITER PUFS

# SWITCH BLOCK

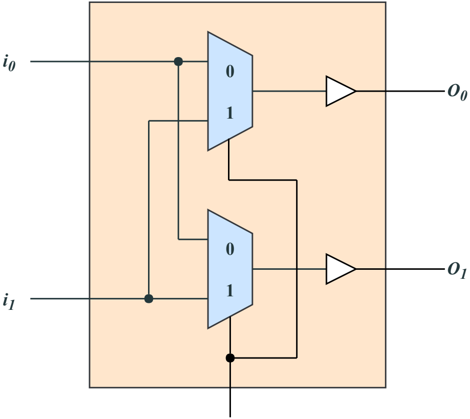


Figure: Schematic of a switch block

# ARBITER PUFS

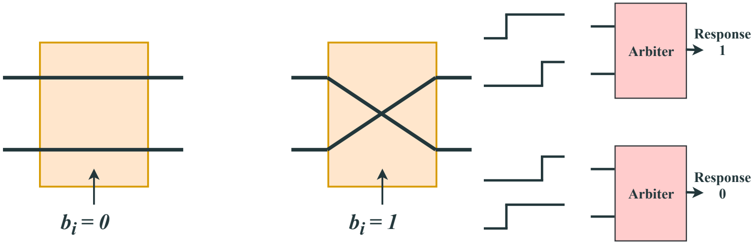


Figure: Arbiter PUF operations

# ARBITER PUFS

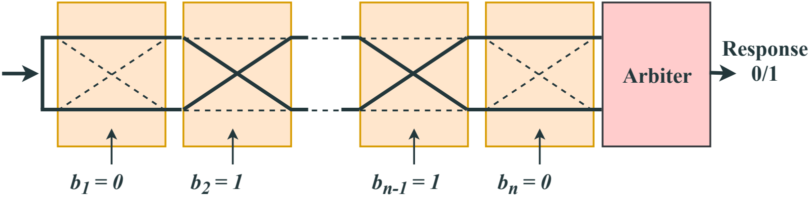


Figure: Multiple switch blocks in series form a PUF

# EXAMPLE

# EXAMPLE

|  |  |  |  |
|---|---|---|---|
| $d_{11}$ = 1.1 ns | $d_{13}$ = 1.0 ns | $d_{21}$ = 1.2 ns | $d_{23}$ = 0.8 ns |
| $d_{12}$ = 1.3 ns | $d_{14}$ = 1.5 ns | $d_{22}$ = 1.4 ns | $d_{24}$ = 0.9 ns |

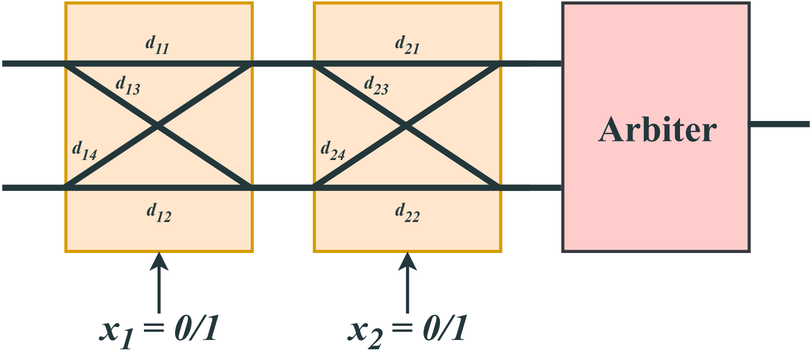
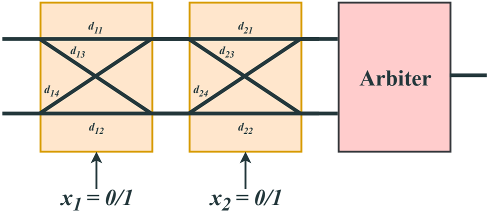


Figure: Delay Paths

# EXAMPLE

$d_{11}$ = 1.1 ns  $d_{13}$ = 1.0 ns  $d_{21}$ = 1.2 ns  $d_{23}$ = 0.8 ns
$d_{12}$ = 1.3 ns  $d_{14}$ = 1.5 ns  $d_{22}$ = 1.4 ns  $d_{24}$ = 0.9 ns



$$(x_1, x_2) = (0, 0) : d_{11} + d_{21} < d_{12} + d_{22} \rightarrow 0$$

$$(x_1, x_2) = (0, 1) : d_{12} + d_{24} > d_{11} + d_{23} \rightarrow 1$$

$$(x_1, x_2) = (1, 0) : d_{14} + d_{21} > d_{13} + d_{22} \rightarrow 1$$

$$(x_1, x_2) = (1, 1) : d_{13} + d_{24} > d_{14} + d_{23} \rightarrow 0$$

| $x_1$ | $x_2$ | f |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

The Boolean function induced by the PUF is $f(x_1, x_2) = x_1 \oplus x_2$, where "$\oplus$" denotes XOR.

# TRUTH TABLE

Table: 4 Boolean functions induced by an arbiter PUF with one switch block.

|  | Challenge |  |  |
|---|---|---|---|
|  | $x_1 = 0$ | $x_1 = 1$ | $f(x_1)$ |
| 00 | $d_{11} < d_{12}$ | $d_{13} > d_{14}$ | 0 |
| 01 | $d_{11} > d_{12}$ | $d_{13} < d_{14}$ | 1 |
| 10 | $d_{11} < d_{12}$ | $d_{13} < d_{14}$ | $x_1$ |
| 11 | $d_{11} > d_{12}$ | $d_{13} > d_{14}$ | $\overline{x_1}$ |

# TRUTH TABLE

**Table:** 16 functions induced by an arbiter PUF with two switch blocks.

| | Challenge | | | | |
|---|---|---|---|---|---|
| | $x_2x_1 = 00$ | $x_2x_1 = 01$ | $x_2x_1 = 10$ | $x_2x_1 = 11$ | $f(x_1, x_2)$ |
| 0000 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | 0 |
| 0001 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | $x_1x_2$ |
| 0010 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | $\overline{x_1}x_2$ |
| 0011 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | $x_2$ |
| 0100 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | $x_1\overline{x_2}$ |
| 0101 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | $x_1$ |
| 0110 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | $x_1 \oplus x_2$ |
| 0111 | $d_{11} + d_{21} < d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | $x_1 + x_2$ |
| 1000 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | $\overline{x_1 + x_2}$ |
| 1001 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | $\overline{x_1 \oplus x_2}$ |
| 1010 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | $\overline{x_1}$ |
| 1011 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} < d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | $\overline{x_1} + x_2$ |
| 1100 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | $\overline{x_2}$ |
| 1101 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} < d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | $x_1 + \overline{x_2}$ |
| 1110 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} < d_{14} + d_{23}$ | $\overline{x_1x_2}$ |
| 1111 | $d_{11} + d_{21} > d_{12} + d_{22}$ | $d_{14} + d_{21} > d_{13} + d_{22}$ | $d_{12} + d_{24} > d_{11} + d_{23}$ | $d_{13} + d_{24} > d_{14} + d_{23}$ | 1 |

# PROOF OF CONFLICT

For $f(x_1, x_2) = x_1$

$$d_{11} + d_{21} < d_{12} + d_{22}$$

$$d_{14} + d_{21} > d_{13} + d_{22}$$

$$d_{12} + d_{24} < d_{11} + d_{23}$$

$$d_{13} + d_{24} > d_{14} + d_{23}$$

$$-\Delta_{11-12} < \Delta_{13-14} < -\Delta_{11-12}$$

Hence, $f(x_1, x_2) = x_1$ can NOT be induced by a single arbiter PUF!

# SOLUTION

# XORED PUFS

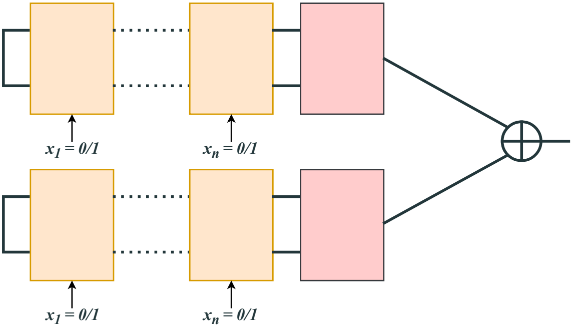


**Figure:** Setup for two XORed arbiter PUFs

# EXAMPLE

Two functions that can be induced by a single arbiter PUF:

$$f(x_1, x_2) = x_1 \oplus x_2$$

$$f(x_1, x_2) = x_2$$

$$(x_1 \oplus x_2) \oplus x_2 = x_1 \oplus x_2 \oplus x_1 = x_1$$

“Et Voilà!”

# SIMULATION

# SIMULATION

1. Select n and number of trials
2. For each trial:
    - Assign random values to the delays (Gaussian Distribution)
    - Evaluate the resulting truth table

# GOAL

We want uniform distribution!

# RESULTS

# RESULTS

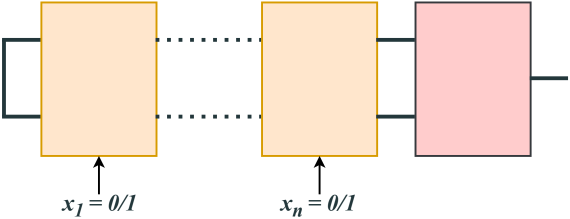


Figure: Single Arbiter PUF

# SINGLE ARBITER PUF

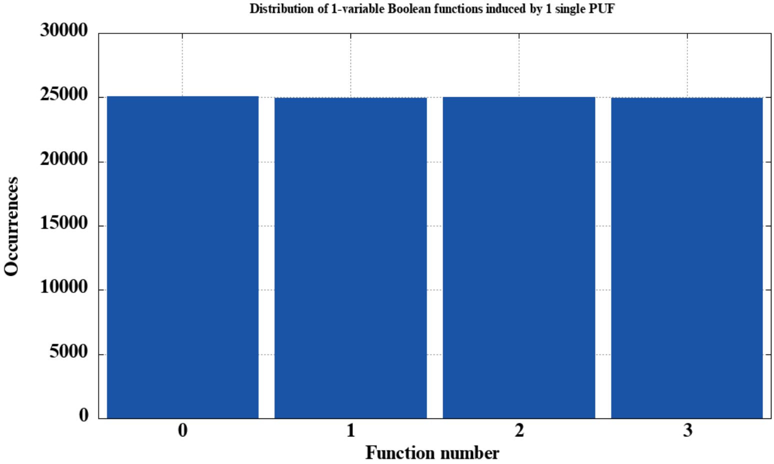


Figure: All functions are equally probable.

# SINGLE ARBITER PUF

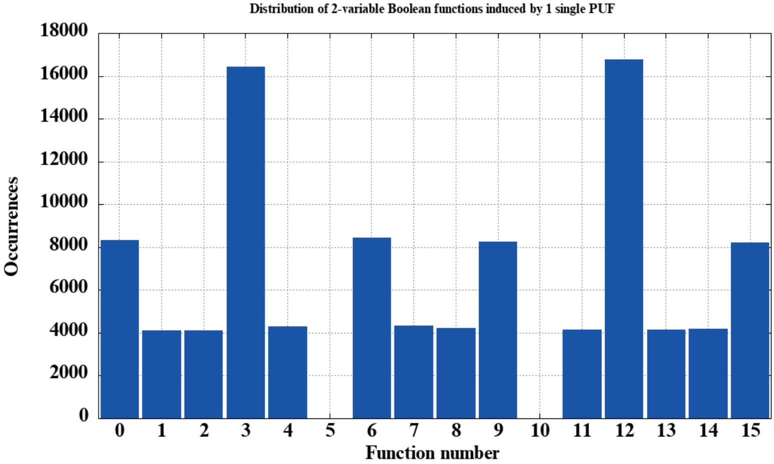


**Figure:** $x_1$ and $\overline{x_1}$ are not induced (100,000 trials).

# SINGLE ARBITER PUF

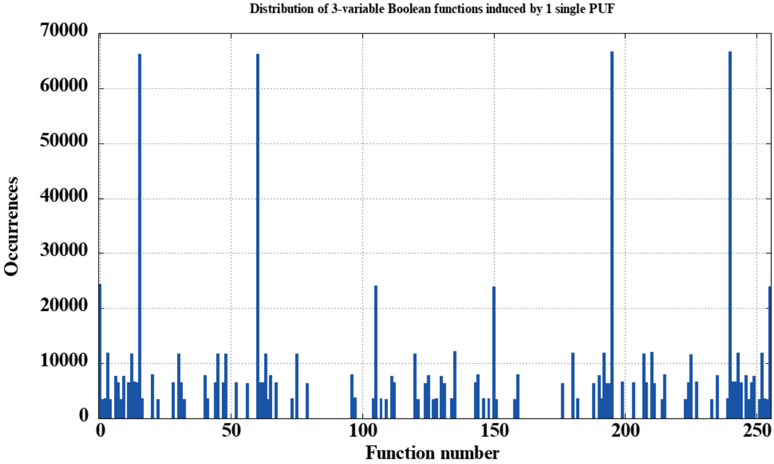


**Figure:** 152 functions are not induced (1 million trials).

# SINGLE ARBITER PUF

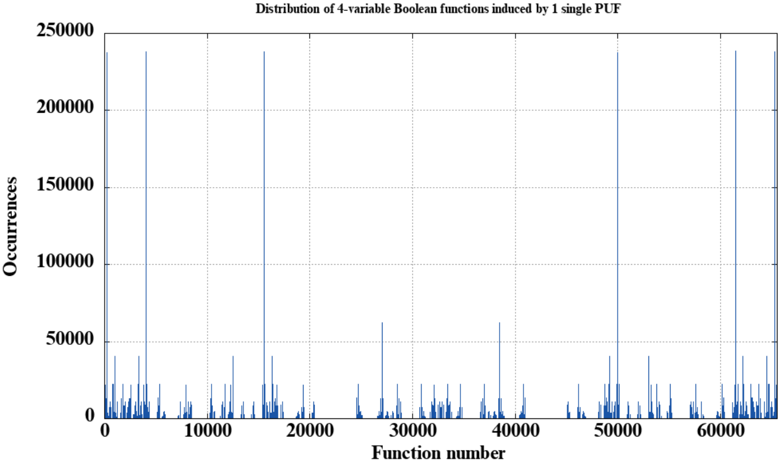
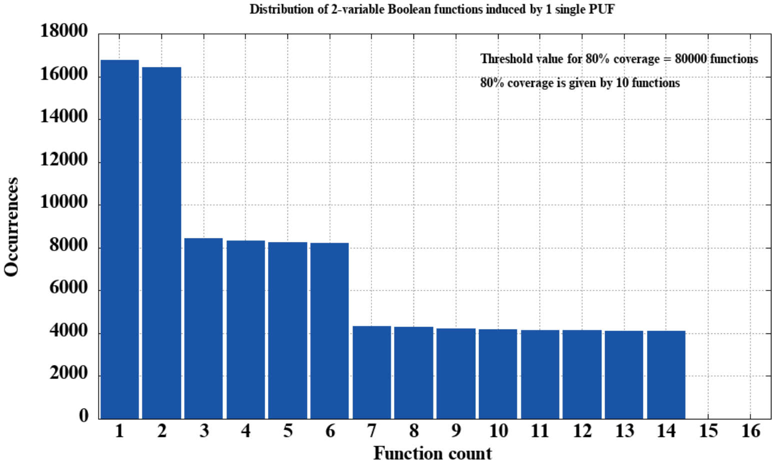


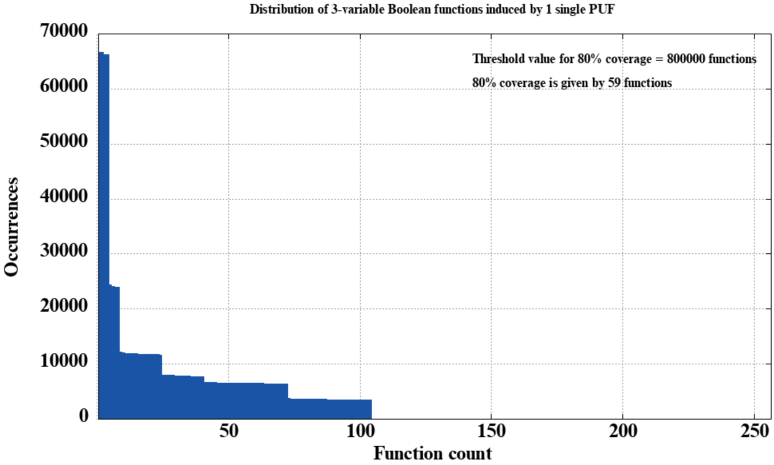
**Figure:** 63,654 functions are not induced (10 million trials).

# COVERAGE

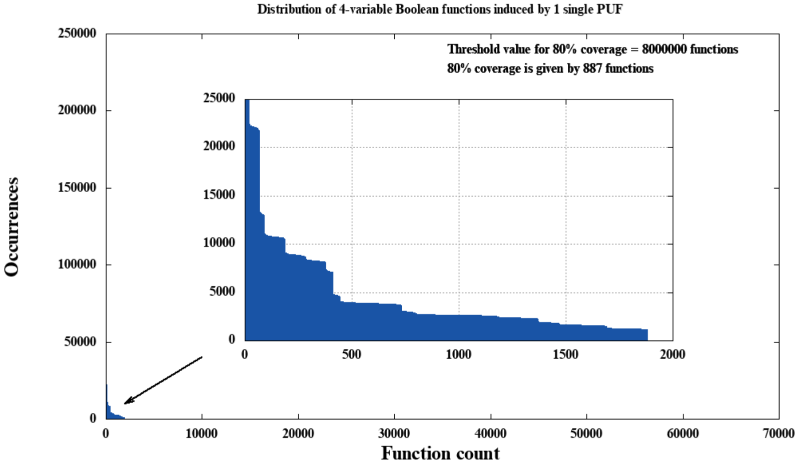
# SINGLE ARBITER PUF



# SINGLE ARBITER PUF



# SINGLE ARBITER PUF



# RESULTS

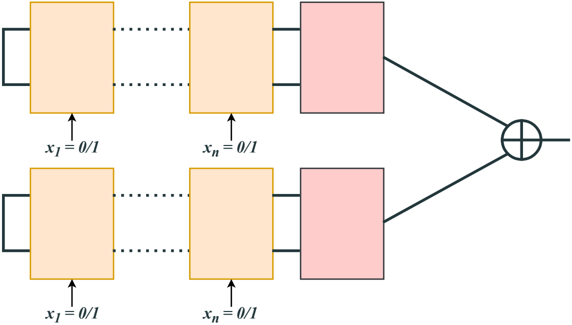


**Figure:** Two XORed PUFs

# TWO XORED PUFS

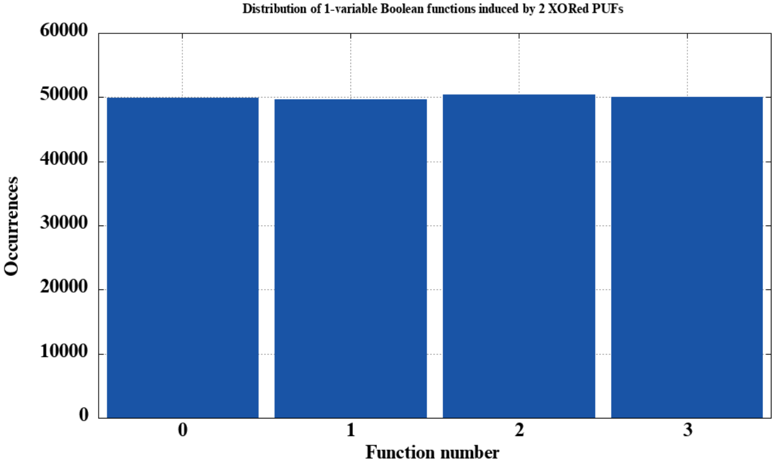


Figure: All functions are equally probable.

# TWO XORED PUFS

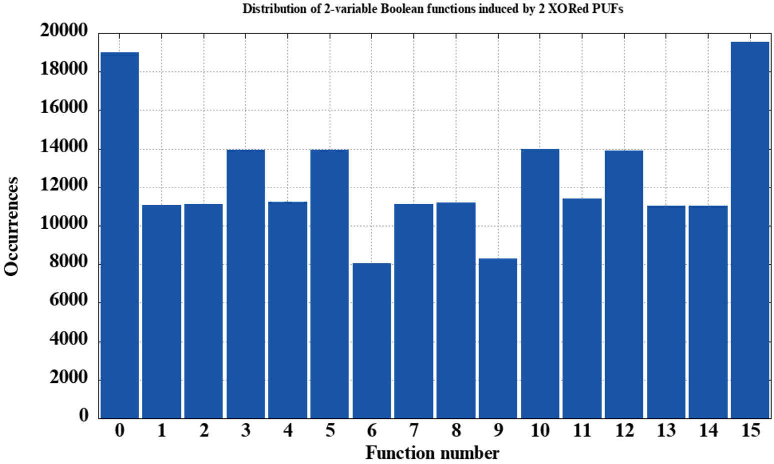


**Figure:** All functions are induced (100,000 trials).

# TWO XORED PUFS

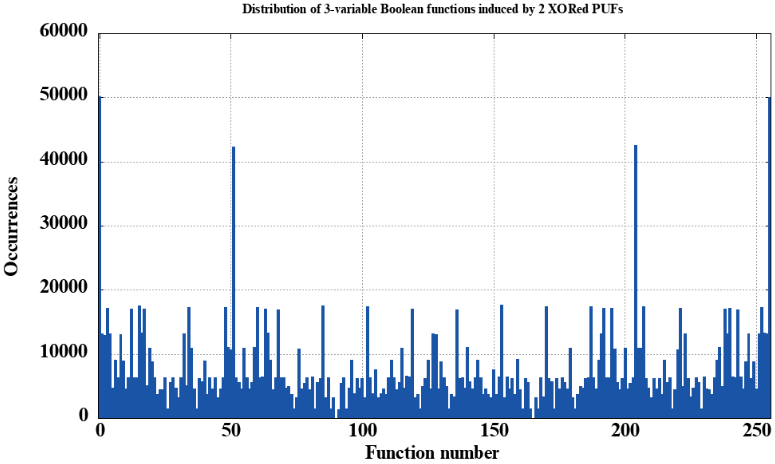


**Figure:** All functions excl. $x_1 \oplus x_2$ and $\overline{x_1 \oplus x_2}$ are induced (1 million trials).

# TWO XORED PUFS

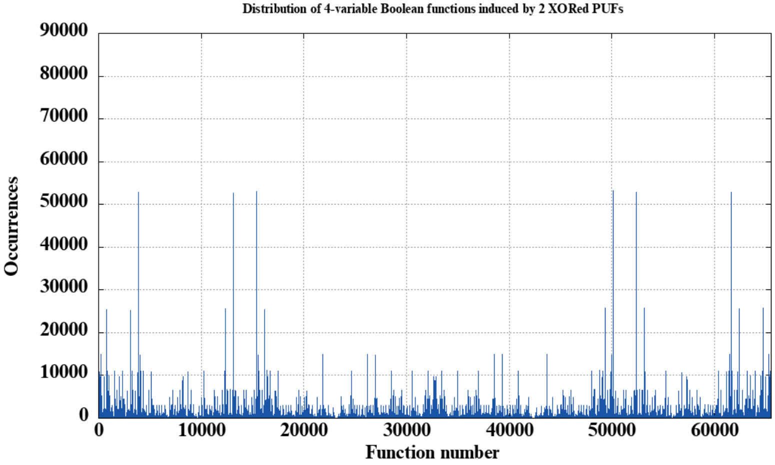
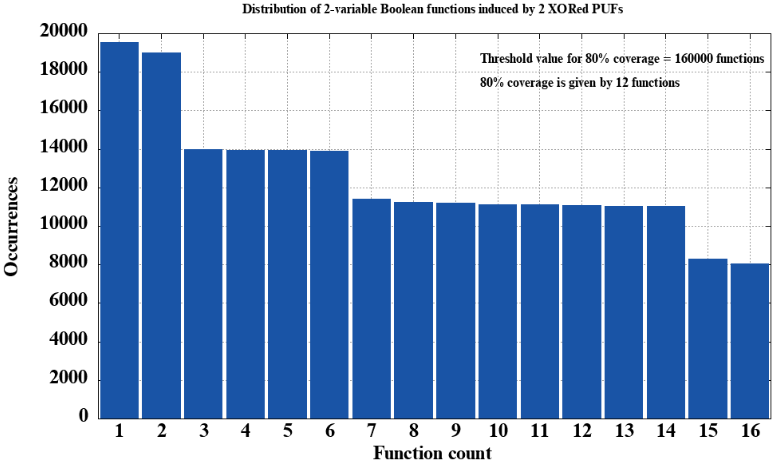


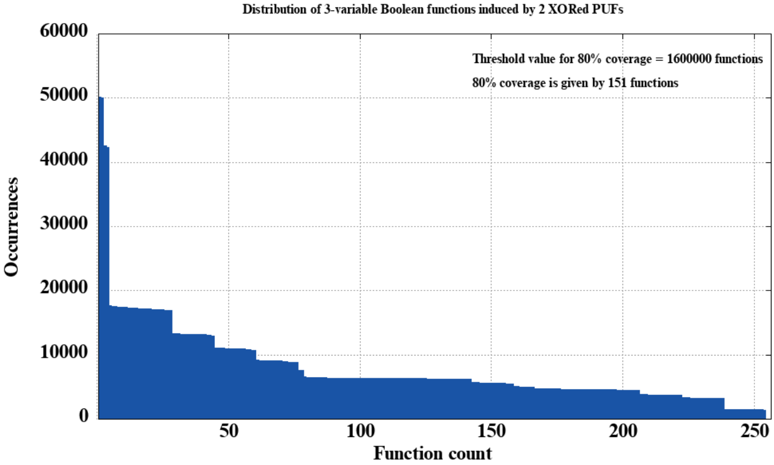
**Figure:** 11,226 functions are not induced (100 million trials).

# COVERAGE

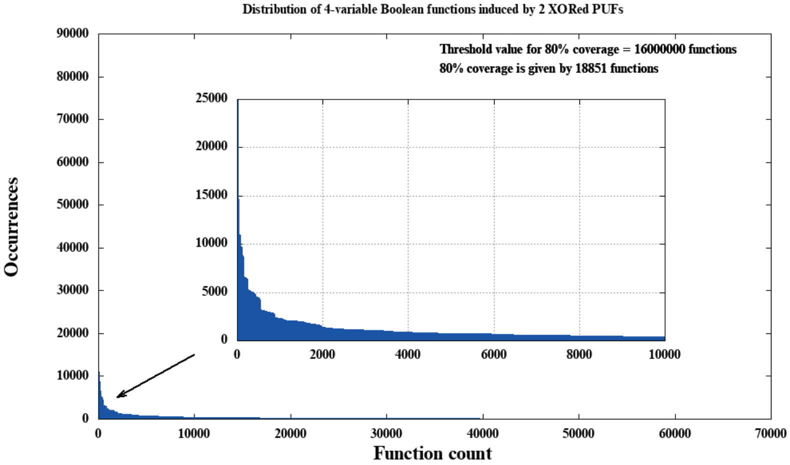
# TWO XORED PUFS



# TWO XORED PUFS



# TWO XORED PUFS



# RESULTS

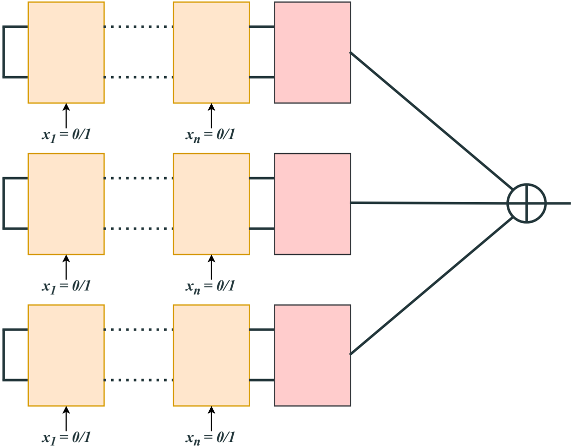


**Figure:** Three XORed PUFs

# THREE XORED PUFS

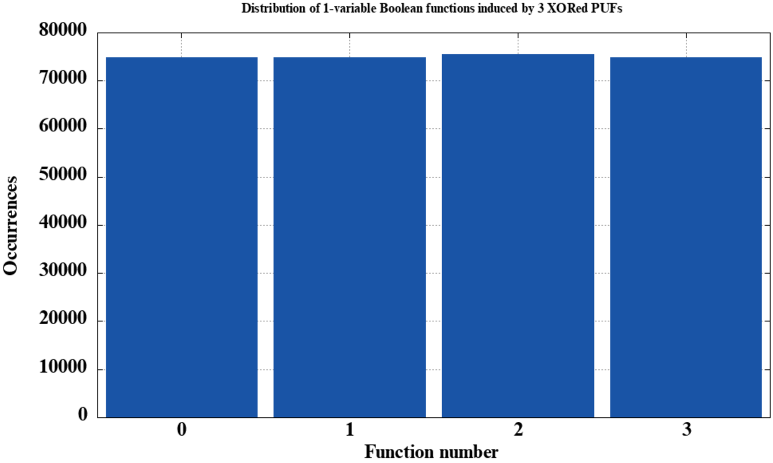


Figure: All functions are equally probable

# THREE XORED PUFS

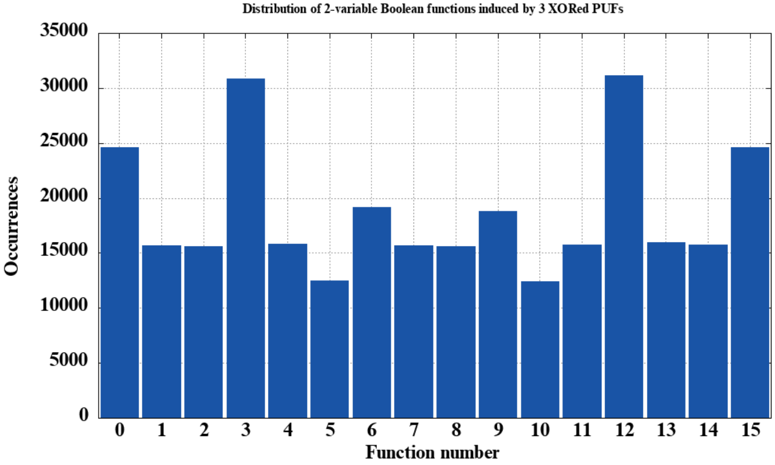


**Figure:** All functions are induced (100,000 trials).

# THREE XORED PUFS

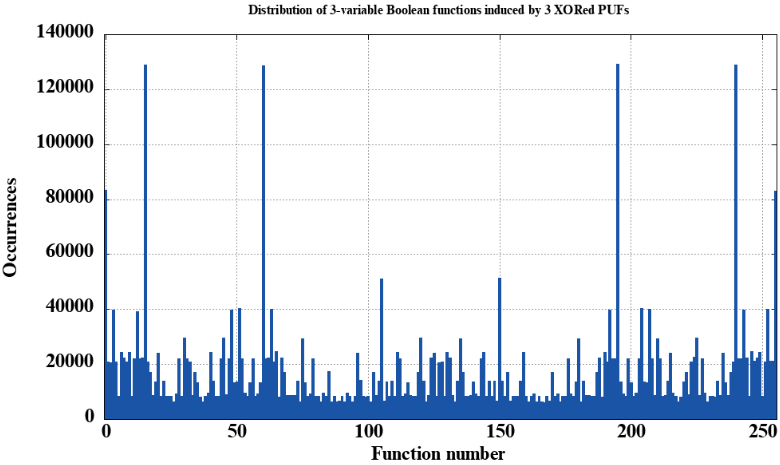


Figure: All functions are induced (1.5 million trials).

# THREE XORED PUFS

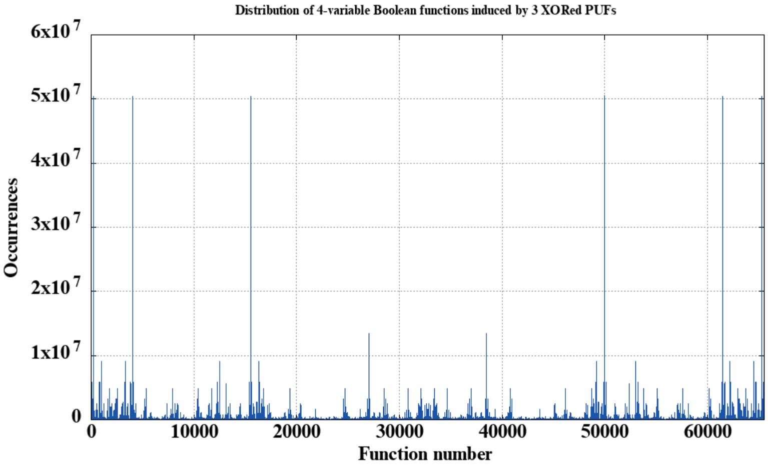
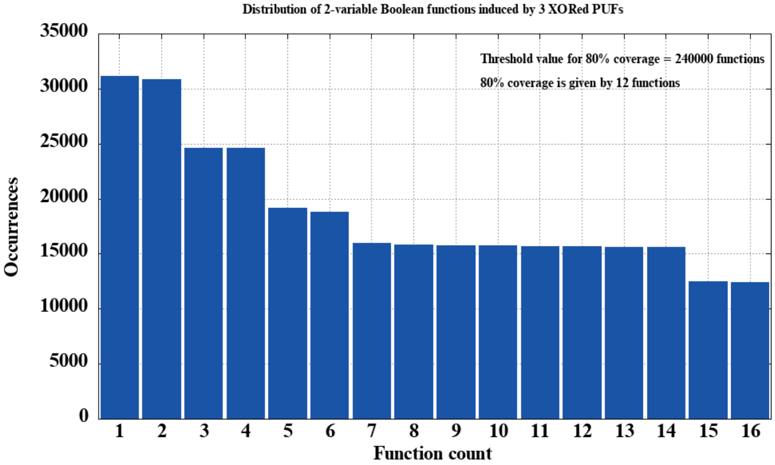


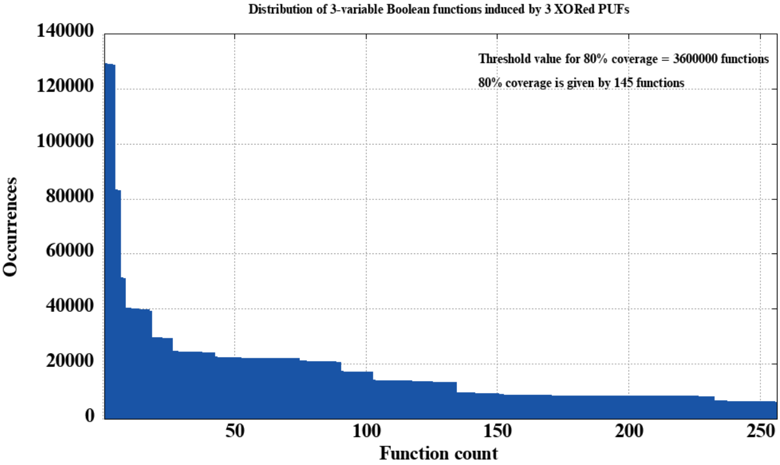
**Figure:** All functions excl. $x_1 \oplus x_3$ and $\overline{x_1 \oplus x_3}$ are induced (2 billion trials).

# COVERAGE

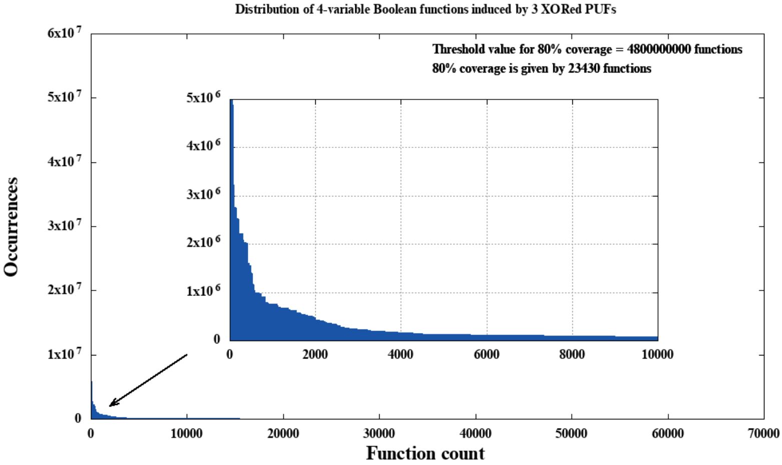
# THREE XORED PUFS



# THREE XORED PUFS

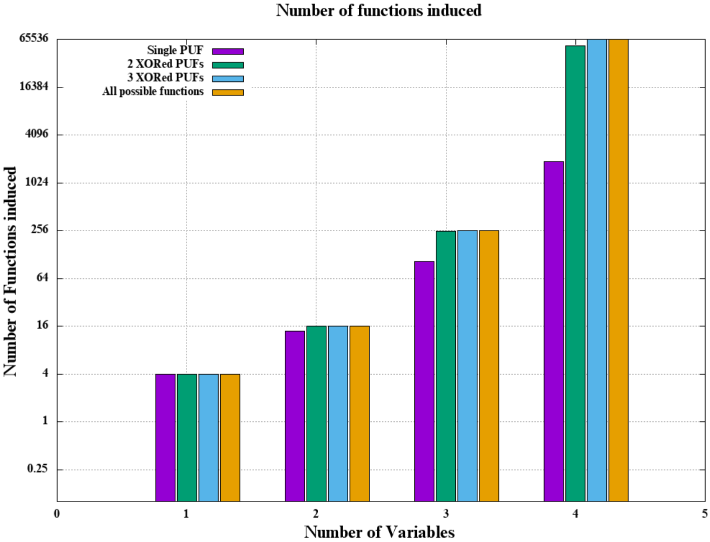


# THREE XORED PUFS



# SUMMARY

# SUMMARY



Number of functions induced
Single PUF
2 XORed PUFs
3 XORed PUFs
All possible functions
65536
16384
4096
1024
256
64
16
4
1
0.25
0
1
2
3
4
5
Number of Functions induced
Number of Variables

# OVERVIEW

Table: Number of Impossible Functions

| n | N | I |
|---|---|---|
| 1 | 4 | 0 |
| 2 | 16 | 2 |
| 3 | 256 | 152 |
| 4 | 65,536 | 63,654 |
| $\vdots$ | $\vdots$ | $\vdots$ |
| n | $2^{2^n}$ | $\geq 2^{2^{n-1}} - 2$ |

(a) One single PUF

| N | I |
|---|---|
| 4 | 0 |
| 16 | 0 |
| 256 | 2 |
| 65,536 | 11,226 |
| $\vdots$ | $\vdots$ |
| $2^{2^n}$ | ??? |

(b) 2 XORed PUFs

| N | I |
|---|---|
| 4 | 0 |
| 16 | 0 |
| 256 | 0 |
| 65,536 | 2 |
| $\vdots$ | $\vdots$ |
| $2^{2^n}$ | ??? |

(c) 3 XORed PUFs

# IMPOSSIBLE FUNCTIONS

$$f(x_1, x_2) = \begin{cases} \overline{x_1} \\ x_1 \end{cases}$$ for n = 2 using 1 single PUF

$$f(x_1, x_2, x_3) = \begin{cases} \overline{x_1 \oplus x_2} \\ x_1 \oplus x_2 \end{cases}$$ for n = 3 using 2 XORed PUFs

$$f(x_1, x_2, x_3, x_4) = \begin{cases} \overline{x_1 \oplus x_3} \\ x_1 \oplus x_3 \end{cases}$$ for n = 4 using 3 XORed PUFs

# HYPOTHESIS

n XORed arbiter PUFs can induce all $2^{2^n}$ n-variable Boolean functions.

# HYPOTHESIS

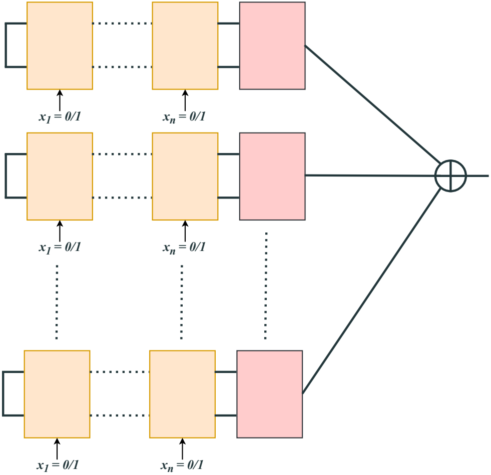


**Figure:** n XORed PUFs can induce all possible n-variable functions.

# CONCLUSION

# FUTURE WORK

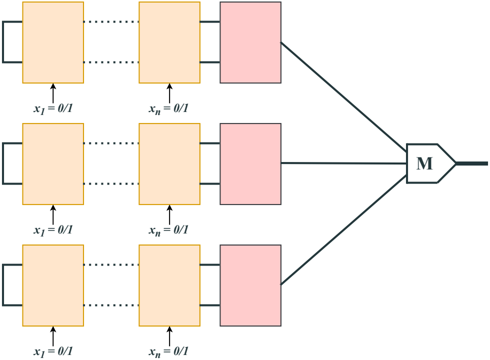


**Figure:** Three arbiter PUFs MAJed

# CONCLUSION

Functions induced by arbiter PUFs are **not uniformly** distributed

Potential **weakness** - could be used for targeted attacks

**XORing** PUFs can improve the distribution

# ACKNOWLEDGEMENTS

Latex Beamer:

`github.com/matze/mtheme`

Graphics:

`draw.io`

# Questions?

Prof. Dr. Elena Dubrova
Dr. Felipe Marranghello