

SoC Security: A Logic Level Methodology to Prevent Differential Power Analysis

- Hemanth Sabbella
- Diljyot Singh

Motivation

Researchers demonstrated a new side channel attack which allow them to steal encryption keys by simply touching a laptop.

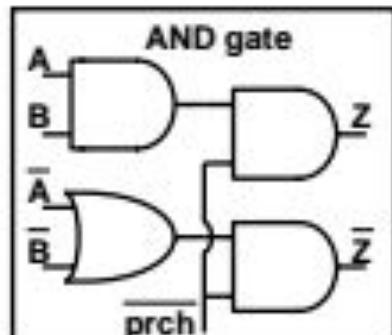
-Workshop on Cryptographic Hardware and Embedded Systems 2014 ([CHES](#) 2014) in Korea, on September 23th

Showed that the “ground” electric potential deviates in a computation-dependent way.

They further showed that the signal can also be measured at remote ends of ethernet, USB and VGA cables.

Proposed Methodology

- SDDL(Simple Dynamic Differential Logic)



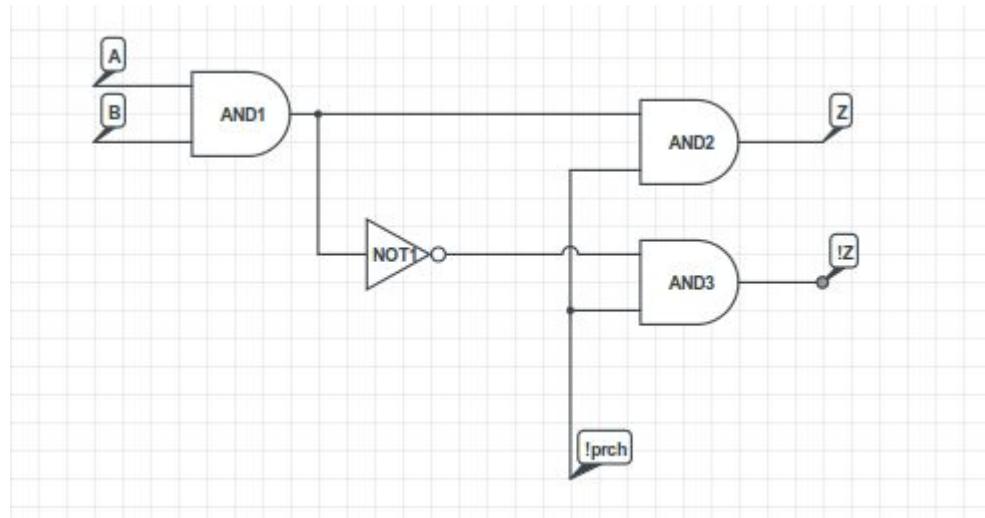
$$(A \cdot B) \cdot \overline{\text{prch}} \leftrightarrow (\overline{A} + \overline{B}) \cdot \overline{\overline{\text{prch}}}$$

A	B	\overline{A}	\overline{B}	prch	Z	\overline{Z}
0	0	1	1	0	0	1
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	0	0	0	1	0
X	X	X	X	1	0	0

Source[1]

Modified Methodology

- IDL(Inversion Dynamic Logic)

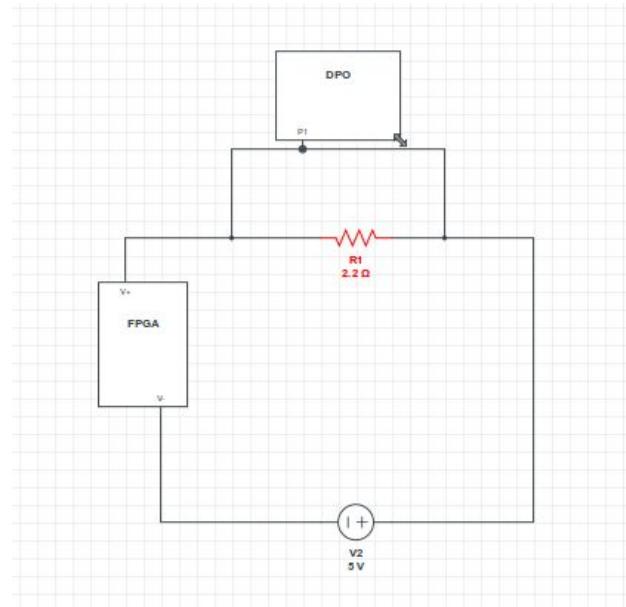


FPGA Implementation

- The power consumption of the device/hardware changes for every logic transition since the amount of current consumption changes.
- The power consumption can be measured by the doing the side channel attack or connecting a resistor in series with the power supply of the FPGA and probing the voltage across the resistor using a DPO/DSO since power is directly proportional to V_{series} .

FPGA Implementation

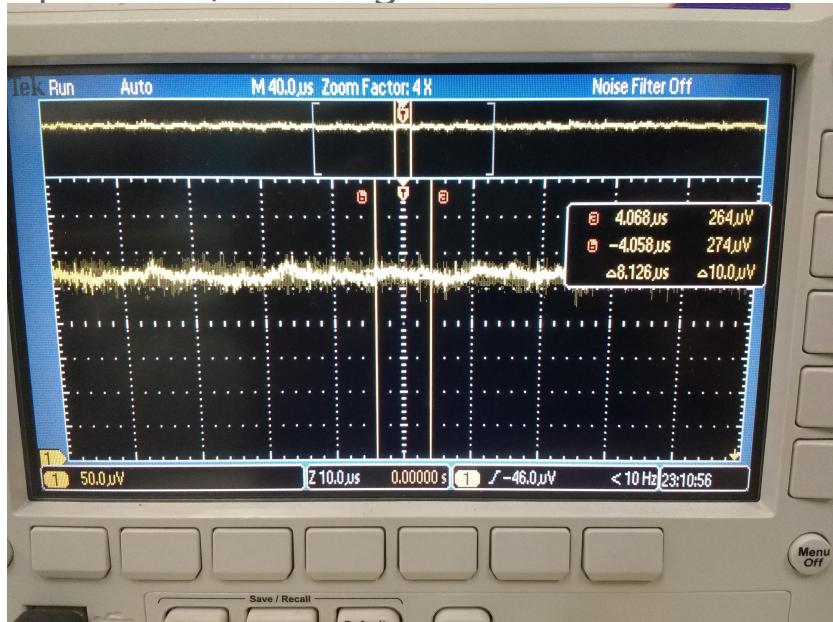
- Side channel attack on FPGA:



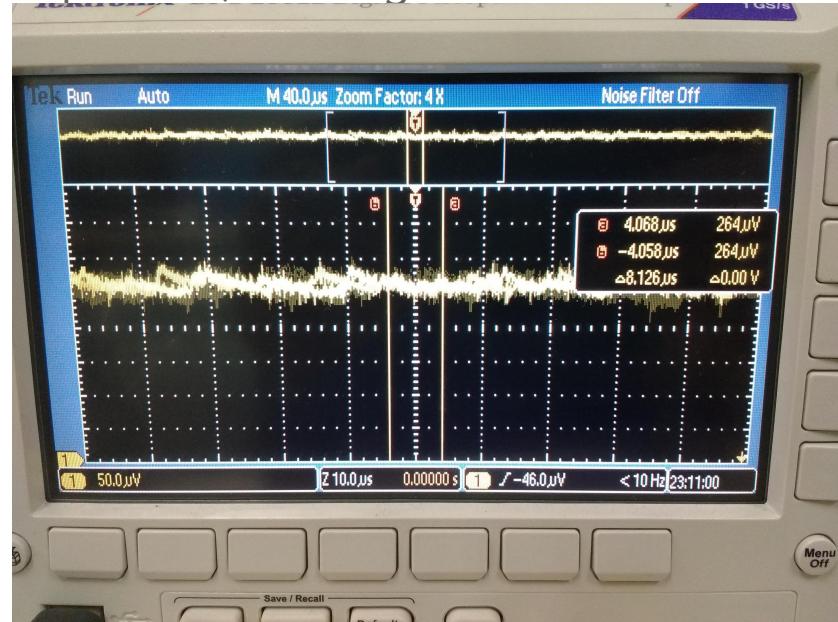
Results

Proposed Methodology:

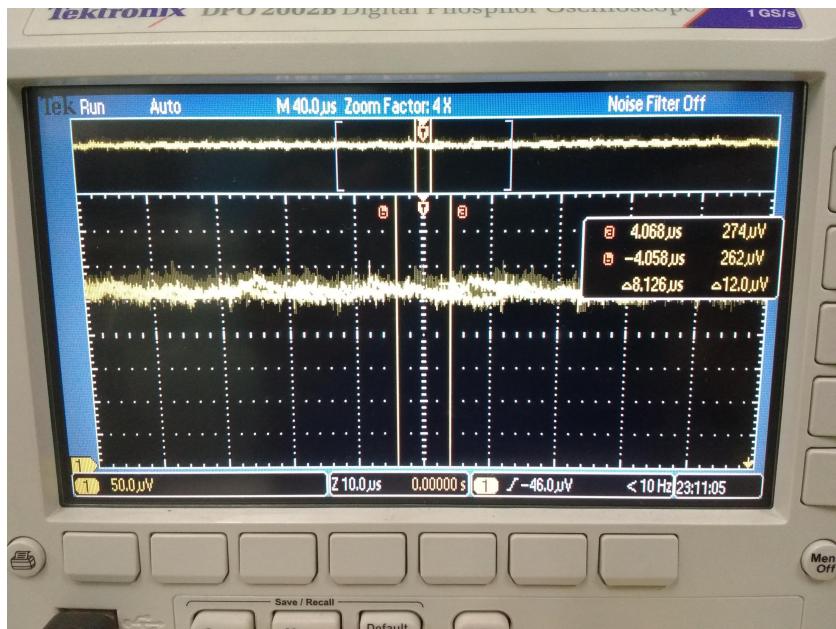
Inputs: 00, Precharge: 0



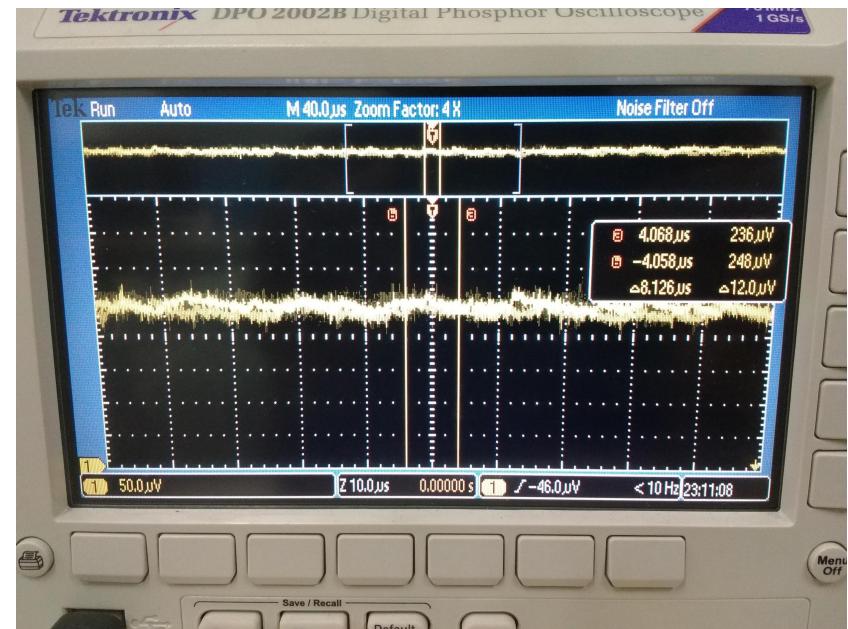
Inputs: 01, Precharge: 0



Inputs: 11, Precharge: 0

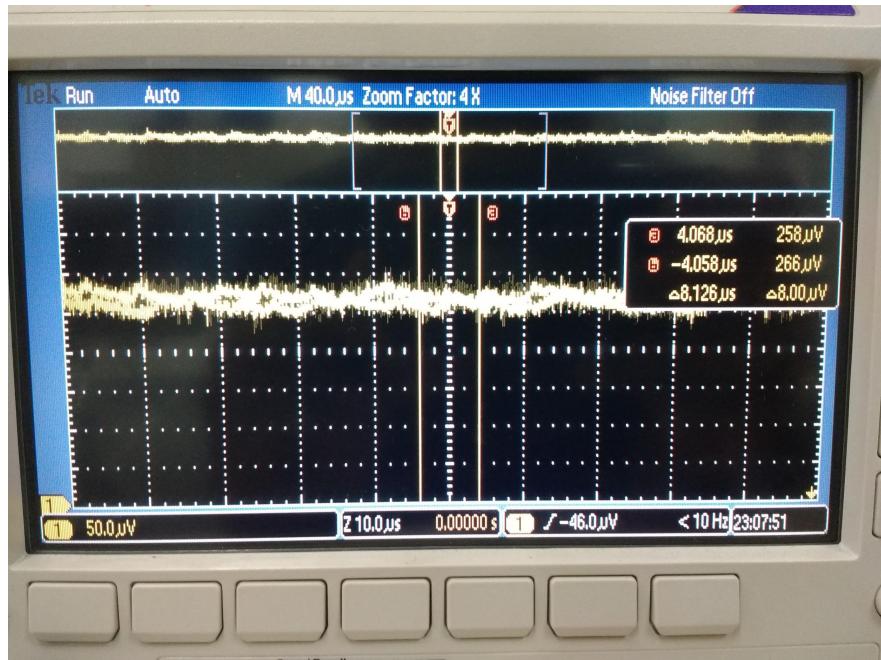


Inputs: 11, Precharge: 1

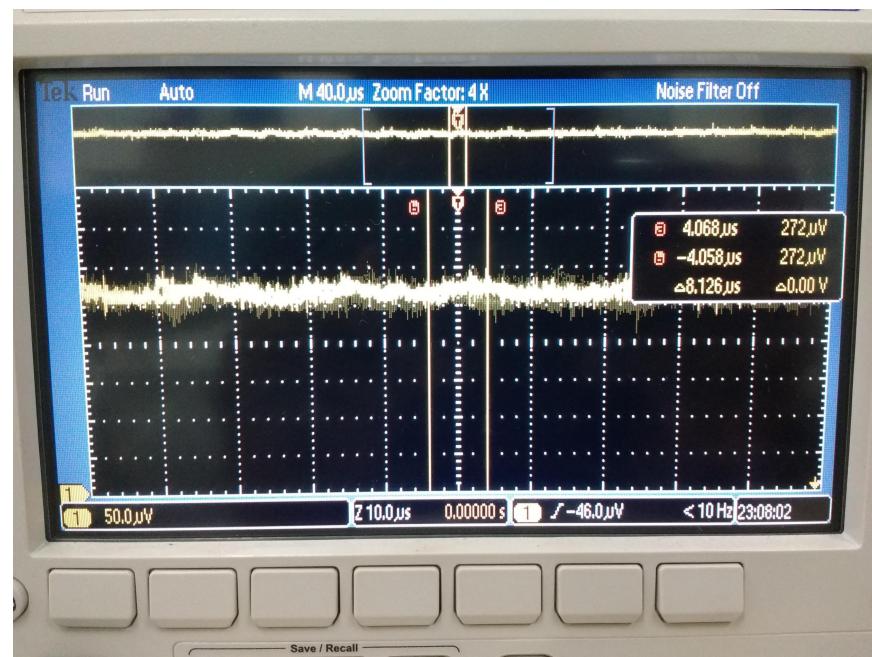


Modified Methodology:

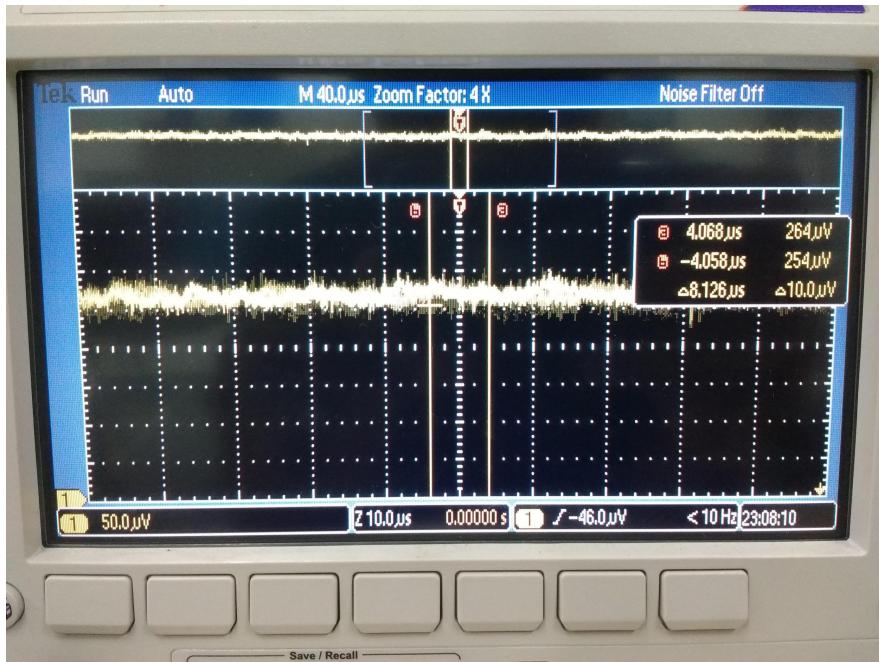
Inputs: 00, Precharge: 0



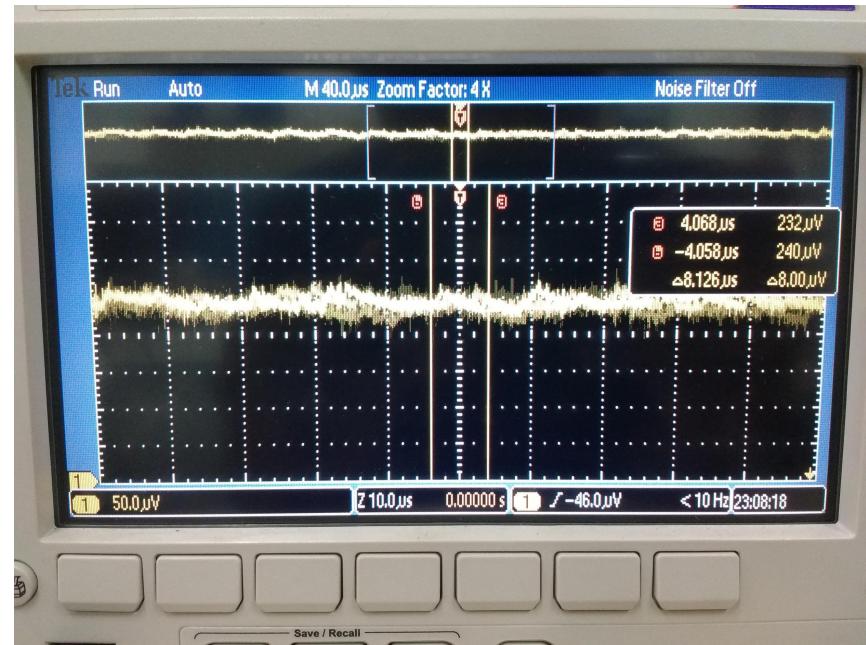
Inputs: 01, Precharge: 0



Inputs: 11, Precharge: 0



Inputs: 11, Precharge: 1



Evaluation

Power:

Proposed Methodology:

Design Vision - TopLevel.1 (ckt1) - [Report.1 - Power]

```
Cell Internal Power = 0.0000 mW (0%)
Net Switching Power = 206.6544 nW (100%)
-----
Total Dynamic Power = 206.6544 nW (100%)
Cell Leakage Power = 0.0000 pW

Information: report power power group summary does not include estimated clock tree power. (PWR-789)

Power Group      Internal Power      Switching Power      Leakage Power      Total Power ( % ) Attrs
-----           0.0000             0.0000              0.0000          0.0000 ( 0.00% )
io pad           0.0000             0.0000              0.0000          0.0000 ( 0.00% )
memory          0.0000             0.0000              0.0000          0.0000 ( 0.00% )
black box        0.0000             0.0000              0.0000          0.0000 ( 0.00% )
clock network   0.0000             0.0000              0.0000          0.0000 ( 0.00% )
register         0.0000             0.0000              0.0000          0.0000 ( 0.00% )
sequential       0.0000             1.0541e-05          0.0000          1.0541e-05 ( 5.10% )
combinational   0.0000             1.9611e-04          0.0000          1.9611e-04 ( 94.90% )
-----
Total           0.0000 mW           2.0665e-04 mW       0.0000 pW       2.0665e-04 mW

***** End Of Report *****
```

Hier.1 Report.1

```
Total           0.0000 mW           2.0665e-04 mW       0.0000 pW       2.0665e-04 mW
design_vision>
```

Log History design_vision>

Ready

or gate in ... [1] iiitd@local... [1] iiitd@local... [1] VCS_tutor... design_co... lab2_syno...

Modified Methodology:

Design Vision - TopLevel.1 (ckt1) - [Report.1 - Power]

```
Cell Internal Power = 0.0000 mW (0%)
Net Switching Power = 181.0236 nW (100%)
-----
Total Dynamic Power = 181.0236 nW (100%)
Cell Leakage Power = 0.0000 pW

Information: report power power group summary does not include estimated clock tree power. (PWR-789)

Power Group      Internal Power      Switching Power      Leakage Power      Total Power ( % ) Attrs
-----           0.0000             0.0000              0.0000          0.0000 ( 0.00% )
io pad           0.0000             0.0000              0.0000          0.0000 ( 0.00% )
memory          0.0000             0.0000              0.0000          0.0000 ( 0.00% )
black box        0.0000             0.0000              0.0000          0.0000 ( 0.00% )
clock network   0.0000             0.0000              0.0000          0.0000 ( 0.00% )
register         0.0000             0.0000              0.0000          0.0000 ( 0.00% )
sequential       0.0000             1.0541e-05          0.0000          1.0541e-05 ( 5.82% )
combinational   0.0000             1.7048e-04          0.0000          1.7048e-04 ( 94.18% )
-----
Total           0.0000 mW           1.8102e-04 mW       0.0000 pW       1.8102e-04 mW

***** End Of Report *****
```

Hier.1 Report.1

```
Total           0.0000 mW           1.8102e-04 mW       0.0000 pW       1.8102e-04 mW
design_vision>
```

Log History design_vision>

Ready

Inbox (2) ... [1] iiitd@local... [1] iiitd@local... [1] VCS_tutor... design_co... lab2_syno...

Area:

Proposed Methodology:

Design Vision - TopLevel.1 (ckt1)

File Edit View Select Highlight List Hierarchy Design Attributes Schematic Timing Test

Library(s) Used:
gtech (File: /usr/synopsys/DesignCompiler/libraries/syn/gtech.db)

Number of ports: 6
Number of nets: 14
Number of cells: 8
Number of combinational cells: 6
Number of sequential cells: 2
Number of macros/black boxes: 0
Number of buf/inv: 2
Number of references: 4

Combinational area: 0.000000
Buf/Inv area: 0.000000
Noncombinational area: 0.000000
Macro/Black Box area: 0.000000
Net Interconnect area: 2.220489

Total cell area: 0.000000
Total area: 2.220489

Information: This design contains unmapped logic. (RPT-7)

***** End Of Report *****

Hier.1 Report.1

Information: This design contains unmapped logic (RPT-7)
design_vision>

Log History
design_vision>

Ready

or gate in ... [1] iiid@local... [1] iiid@local... [1] VCS_tutor... [1]

Modified Methodology:

Design Vision - TopLevel.1 (ckt1)

File Edit View Select Highlight List Hierarchy Design Attributes Schematic Timing Test

Library(s) Used:
gtech (File: /usr/synopsys/DesignCompiler/libraries/syn/gtech.db)

Number of ports: 6
Number of nets: 12
Number of cells: 6
Number of combinational cells: 4
Number of sequential cells: 2
Number of macros/black boxes: 0
Number of buf/inv: 1
Number of references: 3

Combinational area: 0.000000
Buf/Inv area: 0.000000
Noncombinational area: 0.000000
Macro/Black Box area: 0.000000
Net Interconnect area: 2.031397

Total cell area: 0.000000
Total area: 2.031397

Information: This design contains unmapped logic. (RPT-7)

***** End Of Report *****

Hier.1 Report.1

Information: This design contains unmapped logic (RPT-7)
design_vision>

Log History
design_vision>

Ready

Inbox (2) ... [1] iiid@local... [1] iiid@local... [1] VCS_tutor... [1]

Conclusion

- Implemented SDDL methodology.
- Optimized the methodology using the inversion logic.
- Implemented the above methodologies on FPGA and did a side channel attack to know the power consumption.
- Evaluated both the designs using Synopsys for power and area consumption.
- Future work:
 - This may be extended to implement on a larger environment and see how performance varies.

References

[1] A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation Kris Tiri and Ingrid Verbauwhede UCLA Electrical Engineering Department, 7440B Boelter Hall, P.O. Box 951594, Los Angeles, CA 90095-1594

Thank you!