

Fluctuating Power Logic: SCA Protection By V_{DD} Randomization At The Cell-level

Fan Zhang, Bolin Yang, Bojie Yang, Yiran Zhang,

Shivam Bhasin, Kui Ren







Content

- 1. Introduction
- 2. FPL scheme
- 3. Simulation
- 4. Conclusion





1. Introduction

Side-Channel Attack

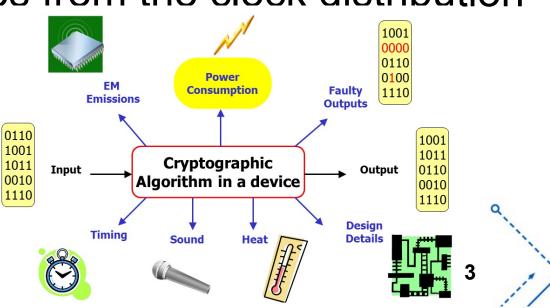
Power dissipation correlates to switching operations

Power models like hamming weight etc.

Major power consumption comes from the clock distribution

network and Flip-Flops

(FFs) (estimated 30%-60%)

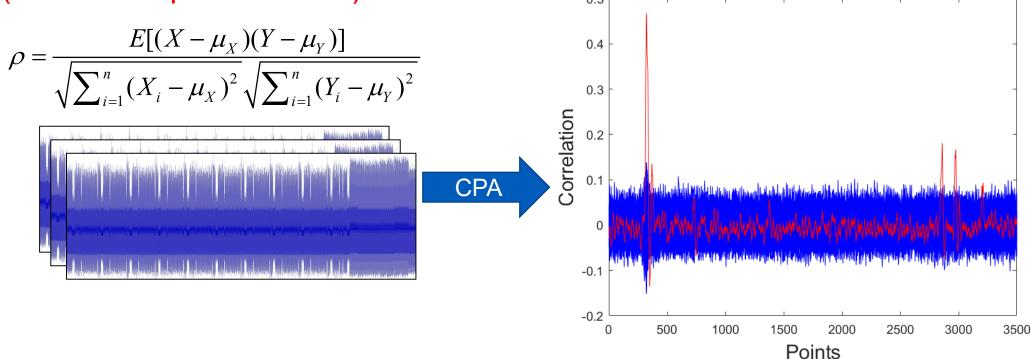






Side-Channel Attack Methods

- SPA(simple power attack), DPA(differential power attack)
- CPA(correlation power attack)

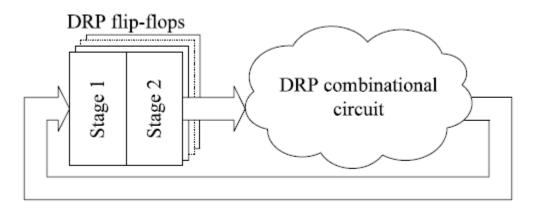






Mainstream SCA countermeasures

 Hiding :noise, clock randomizer, dual-rail precharge logics (DPL)



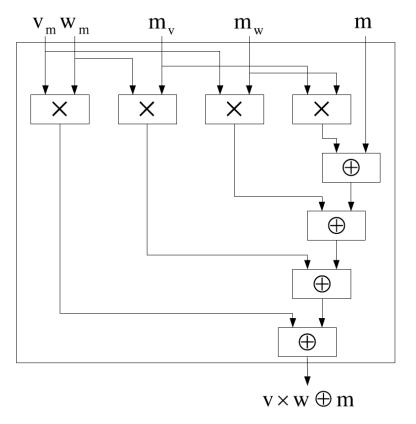


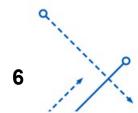


Mainstream SCA countermeasures

Masking: algorithm level, hardware level

$$a' = a \oplus m$$









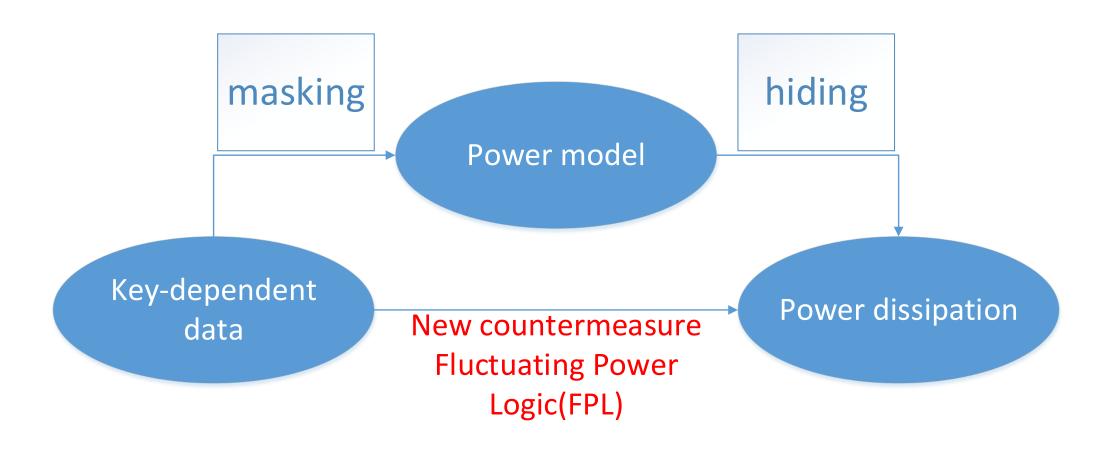
Wave Dynamic Differential Logic (WDDL)

- One of the dual-rail precharge logic based on standard cell flow, proposed by K. Tiri
- require a very strict complementary capacitive balance, making it difficult to implement in practice





New countermeasure: FPL





Our contributions

- We propose a novel cell-level logic: Fluctuating power logic(FPL)
- We compared FPL with standard-cell-based and WDDL-based implementation
- We analyzed side-channel security of FPL on PRESENT/AES implementation





Content

- 1. Introduction
- 2. FPL scheme
- 3. Simulation
- 4. Conclusion



2. FPL scheme

- The proposed logic is highlighted with a modified secure FF.
- This scheme is based on a cascade voltage logic(CVL) and further enhanced with a compensatory unit (CU).

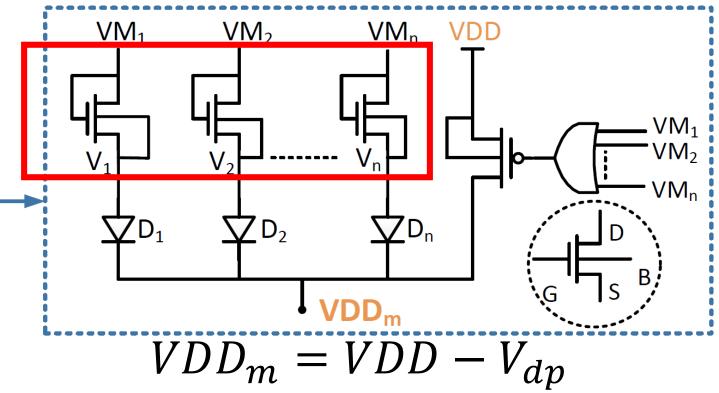




PRNG

CVL unit-

- n NMOS,
- n diodes
- one PMOS
- one "n-input" OR-gate.
- V_{dp}: voltage drop



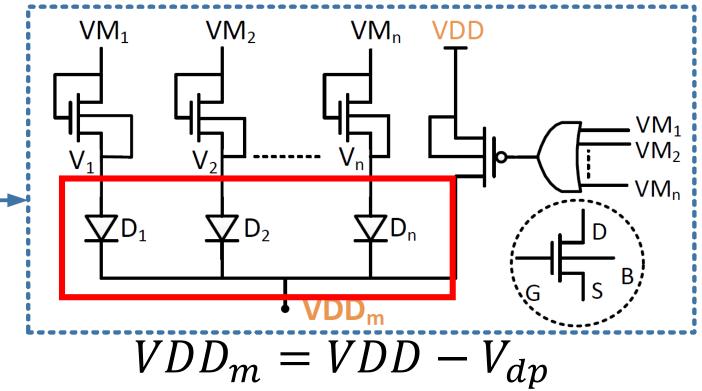






CVL unit-

- n NMOS,
- n diodes
- one PMOS
- one "n-input" OR-gate.
- V_{dp}: voltage drop



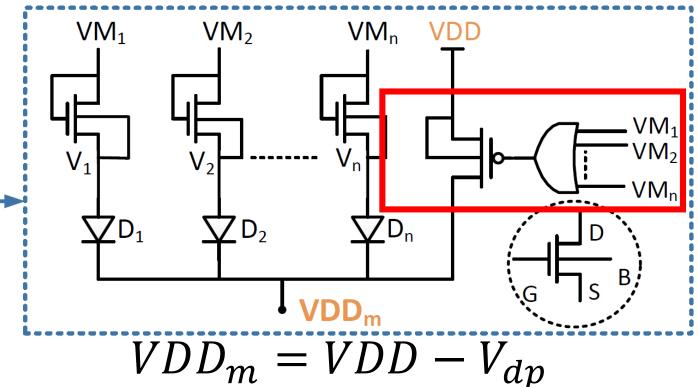






CVL unit-

- n NMOS,
- n diodes
- one PMOS
- one "n-input" OR-gate.
- V_{dp}: voltage drop

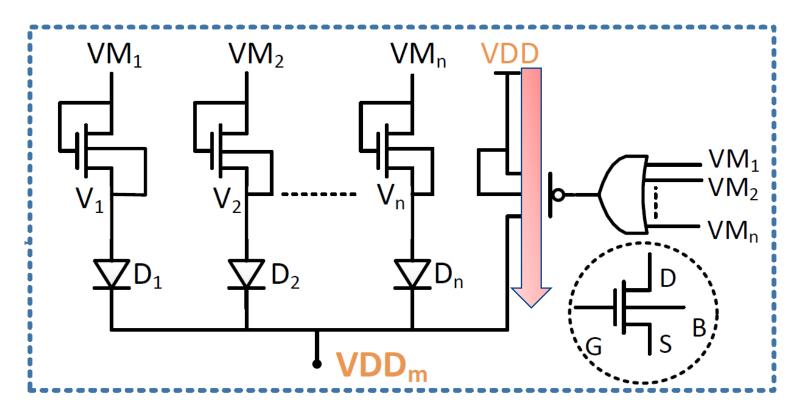






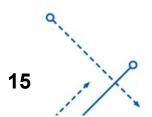
• $K=0, V_{dp}=0$

- K=1, $V_{dp}=V_{th0}$
- K>1, 0<V_{dp}<V_{th0}



K denotes the total number of VM_i whose logic value is "1"

V_{th0} denotes the threshold voltage of NMOS and diode

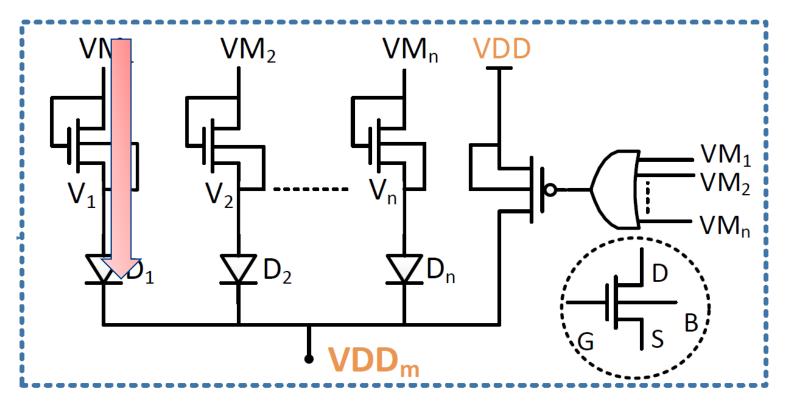






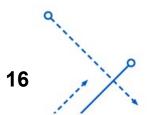
•
$$K=0, V_{dp}=0$$

• K>1, 0<V_{dp}<V_{th0}



K denotes the total number of VM_i whose logic value is "1"

V_{th0} denotes the threshold voltage of NMOS and diode

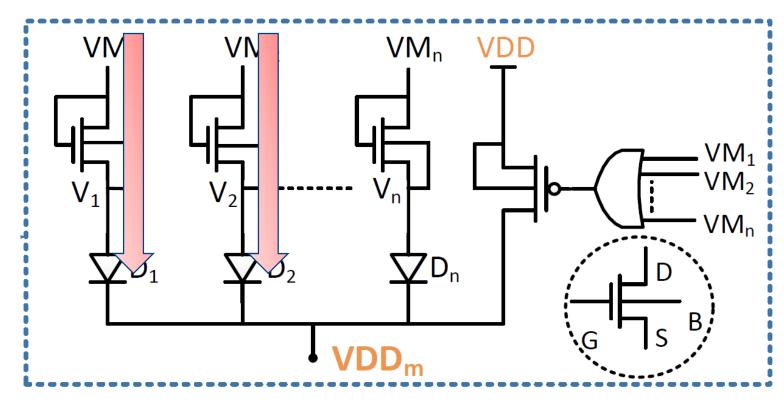






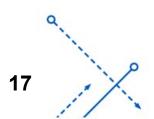
•
$$K=0, V_{dp}=0$$

• K>1, 0<V_{dp}<V_{th0}



K denotes the total number of VM_i whose logic value is "1"

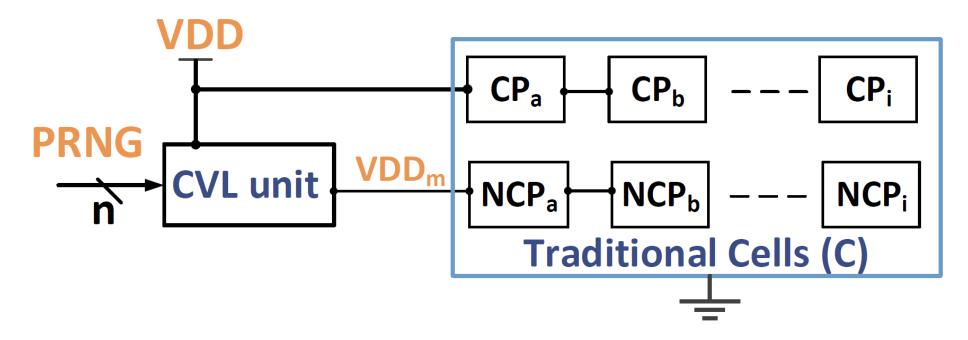
V_{th0} denotes the threshold voltage of NMOS and diode







- CP: circuit on critical path
- NCP: circuit on non-critical path

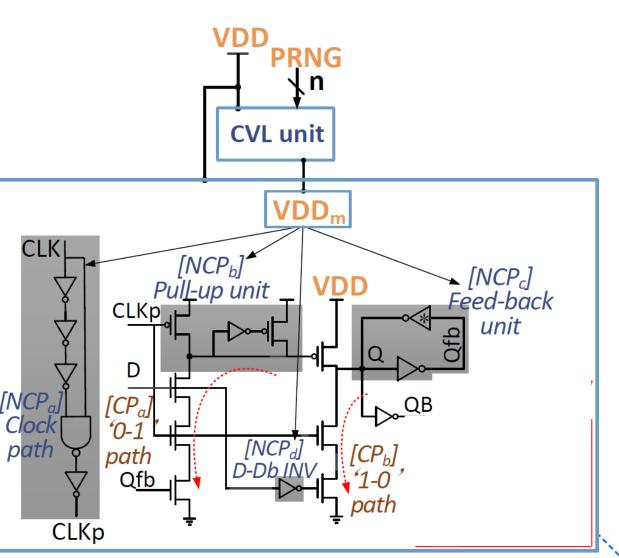






Modified FF with FPL

- Critical paths marked in brown
- Non-critical paths marked in blue
- Transistors connected with VDD_m
 marked in grey





compensatory unit (CU)

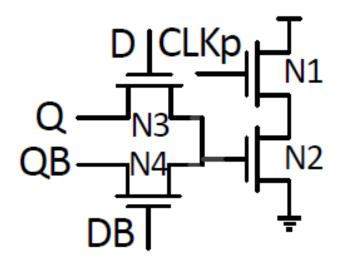
- The power consumption for variant data transitions (0 →1 and 1→0) is larger than that for invariant ones (0→0 and 1→1)
- The compensatory unit make up the power consumption during invariant data transition





compensatory unit (CU)

- When the FF makes a 0→1 or 1→0 the CU is off
- when the inputs of FF keep unchanged the CU is turned on







Total Power dissipation

$$P_{\text{total}} = P_{FF} + P_{CVL} + P_{CU}$$





Content

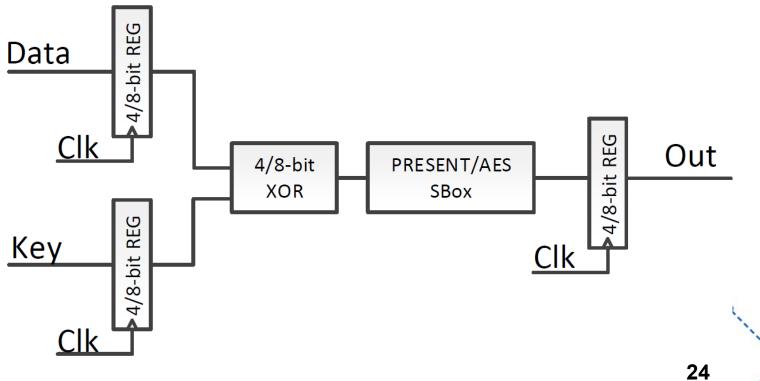
- 1. Introduction
- 2. FPL scheme
- 3. Simulation
- 4. Conclusion





3. Simulation

- Testbench
- compiling and synthesis by Design Compiler
- n=4
- HSPICE







Simulation results

- (GE) Gate equivalents
- (SC-FF) standard-cell-based FF
- (WDDL) dynamic differential logic

Testbench	PRESENT encryption circuit			AES encryption circuit		
	SC-based	FPL-based	WDDL-based	SC-based	FPL-based	WDDL-based
Area[GE]	152	221 (× 1.45)	520 (×3.42)	1340	1478 (×1.10)	3111 (×2.32)
$P_{max}[fJ]$	2212.2	2335.9	7097.0	2590.9	3664.6	21249.0
$P_{min}[fJ]$	769.6	1132.2	6829.0	1301.0	2595.4	20842.0
$P_{avg}[fJ]$	1299.3	1532.3 (× 1.18)	6958.0 (×5.36)	2249.6	3307.6 (×1.47)	21083.1 (×9.37)
σ_P	362.2	281.6	80.6	219.0	181.2	79.0

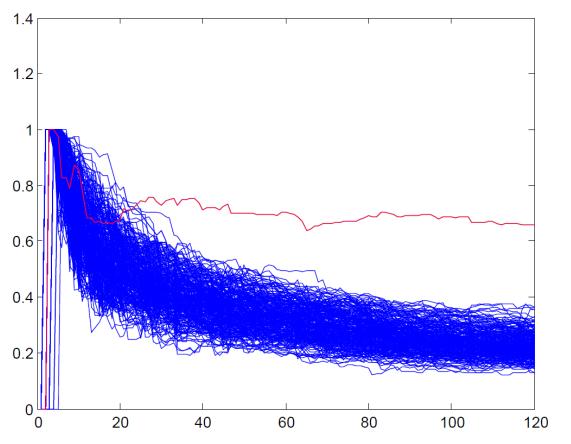


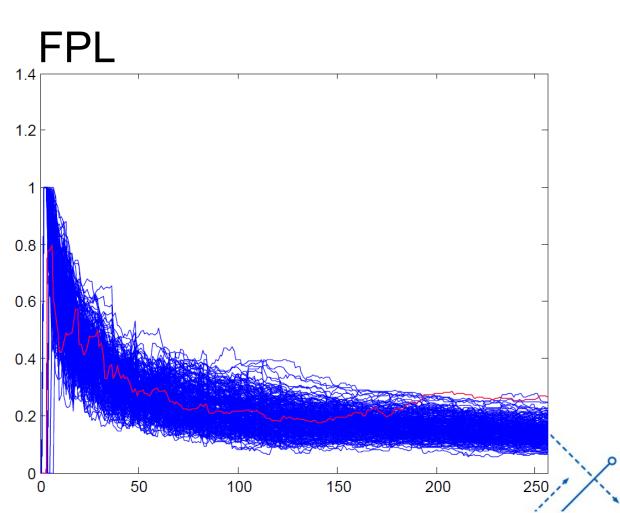


Comparation(AES)

Correlation vs. number of traces

Standard



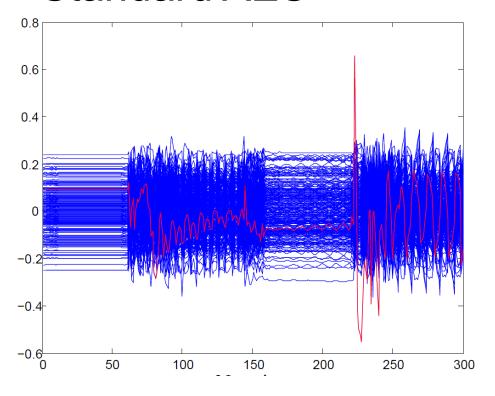




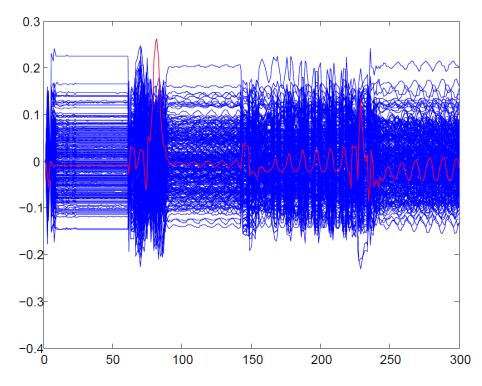


Comparation(AES)

- Correlation vs. length of a trace
- Standard AES



PFL AES



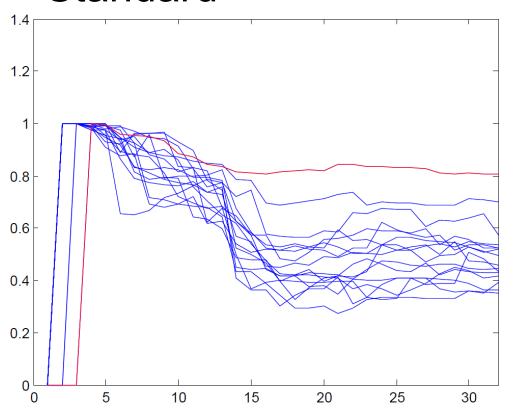




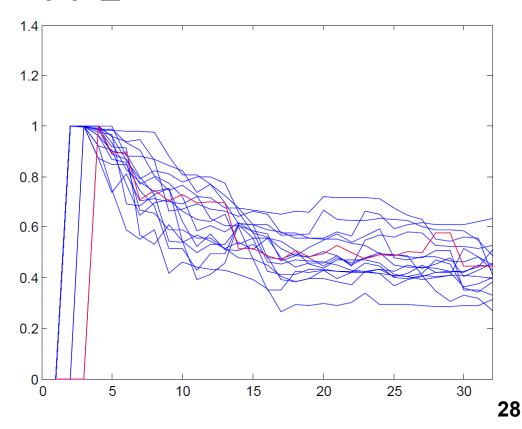
Comparation(PRESENT)

Correlation vs. number of traces

Standard



FPL



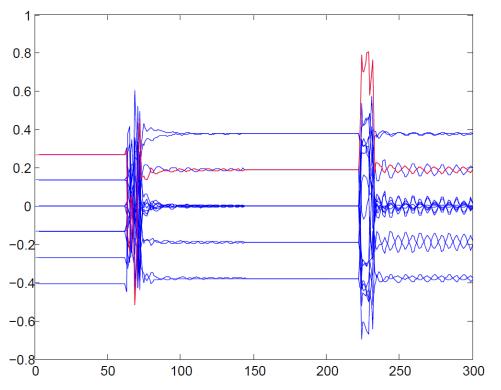




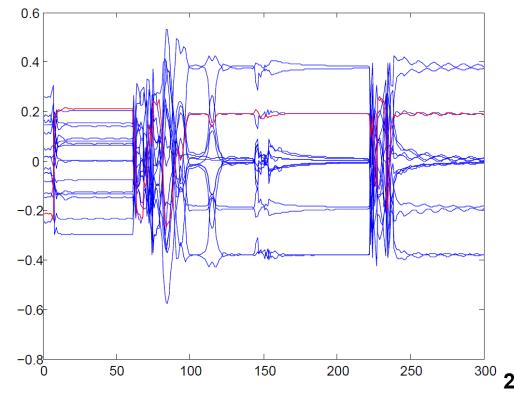
Comparation(PRESENT)

Correlation vs. length of a trace

Standard









Content

- 1. Introduction
- 2. FPL scheme
- 3. Simulation
- 4. Conclusion



Conclusion

- proposed a power-diffusing logic named as fluctuating power logic (FPL)
- analyzed side-channel security on PRESENT/AES implementation
- compared FPL with standard-cell-based and WDDLbased implementation



Thank you~