# Balance Power Leakage to Fight Against Side-Channel Analysis at Gate Level in FPGAs

Xin Fang, Pei Luo, Yunsi Fei, and Miriam Leeser
Electrical & Computer Engineering Department, Northeastern University, Boston, MA 02115 USA
fang.xi@husky.neu.edu, silenceluo@coe.neu.edu, yfei@ece.neu.edu, mel@ece.neu.edu

***Abstract*—Side-channel attacks have been a serious threat to the security of embedded cryptographic systems, and various countermeasures have been devised to mitigate the leakages. Power balance technologies such as wave dynamic differential logic (WDDL) aim to balance the power by introducing differential logic. However, different routing length leads to different capacitance of wire, and this hampers the strength of the power balance countermeasure. In this paper, we further balance the power of differential signals by manipulating the lower level primitives and placement constraints on a Field Programmable Gate Array (FPGA). We choose Advanced Encryption Standard (AES) as the encryption algorithm and apply Hamming weight model to demonstrate the amount of leakage for different implementations. Results show that our method not only efficiently mitigates the side-channel leakage but also saves FPGA logic block resources and dynamic power consumption.**

## I. Introduction

Power analysis attack [1] is one kind of side-channel attack against hardware cryptographic systems. Two countermeasures are widely used at the gate level; one is to balance the power consumption in order to decrease its correlation with the sensitive inner state, and the other is to mask secret information by introducing random bits to the system. WDDL [2] is widely used for mitigating side-channel leakage by balancing the power consumption. At the left side of Fig. 1, both input and output ports are complementary signals and there are two stages which are called pre-charge and evaluation. In the pre-charge stage, the differential input and output signals will both be 0 and in the evaluation stage, the output will contain complementary values. The number of bitwise transitions based on WDDL during an operation cycle is constant, independent of the values of the inputs.

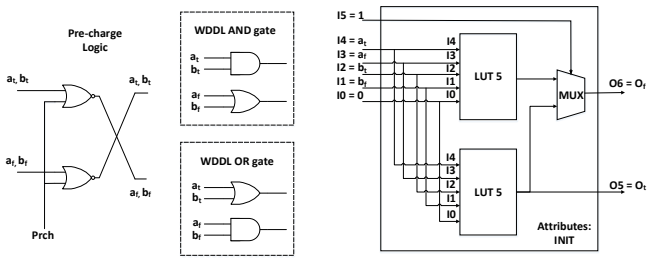


Fig. 1: Components of WDDL

However, WDDL can still leak information for two reasons. First, the difference in loading capacitance between two complementary wires in WDDL may cause unbalanced power leakage. Second, early evaluation incurs leakage when there are differences in arrival time between input signals of WDDL gates. Researchers have proposed methods to balance the routing in hardware implementations. While circuit components are completely defined by designers in ASICs, logic can only be mapped to existing resources in an FPGA, making it more difficult. Others [3] have placed a pair of complementary signals into a single LUT6_2 primitive. The right side of Fig. 1 shows the mapping of logic using LUT6_2 which, for Xilinx FPGAs, contains two 5-input LUTs within one slice. This ensures that each complementary signal pair of the combinational logic operations in WDDL implementation is in the same location in the FPGA. In section II, we show how we constrain register placement, which when combined with mapping LUT6_2 primitives in an FPGA, further enhances the level of countermeasure against power analysis attack.

## II. Implementation

Fig. 2 is a standard WDDL implementation of AES. It has two groups of registers instead of one because of the pre-charge and evaluation steps for WDDL. Besides the LUT primitives, we constrain the register placement to specific locations in an FPGA to ensure a better countermeasure. Without any constraints, the location of flip-flops after placement will incur significant loss of security strength due to routing length differences even though the LUTs define the location of the complementary signal pairs.

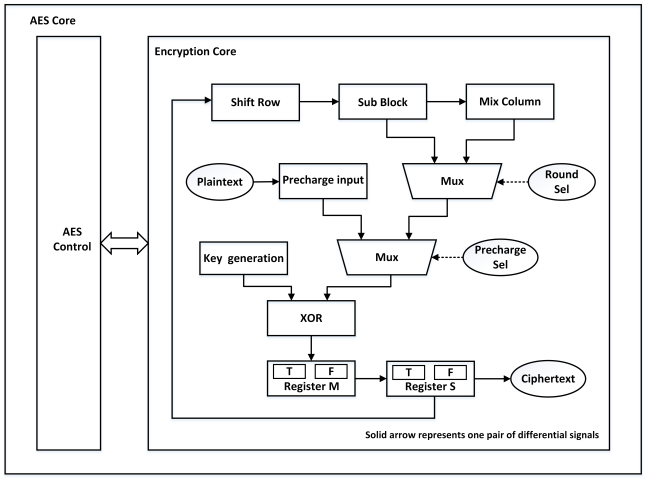


Fig. 2: WDDL Implementation of AES

Fig. 3 shows how registers are placed and organized in FPGAs. For registers $M$ and $S$ in AES, each register contains

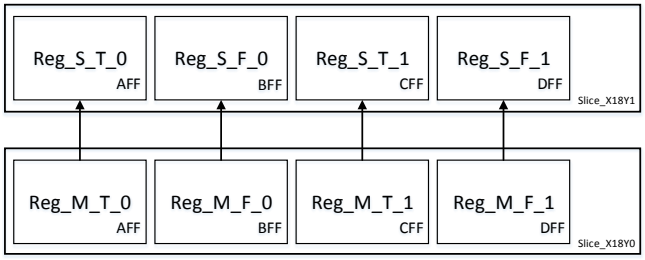


Fig. 3: Placement Example

128 pairs of bitwise complementary signals, and two pairs can fit in one slice which contains 4 flip-flops. To equalize and minimize the wiring length between register $M$ and register $S$, the two corresponding signal pairs for register $S$ will be placed in the next slice. Fig. 3 shows placement of the first two indices of registers $M$ and $S$. In total, 128 slices are required to accommodate all 128 bits.

DPL-noEE is a LUT initialization method which can be added to the implementation mentioned above. In [4], the authors divide the combination of 16 input values into four groups: Null 0, Null 1, Valid and Fault. These represent the states from which the input bits are produced. Compared with standard DPL, glitches of early evaluation introduced by unbalanced routing will be mitigated.

In section III, we compare the side-channel leakages of (1) standard WDDL implementation, (2) WDDL method with LUT and register placement constraints and (3) with additional DPL-noEE countermeasure.

## III. Results and Comparison

Power trace acquisition is conducted with a LeCroy WaveRunner 640Zi oscilloscope on a SASEBO-GII board [5]. For each implementation, $100,000$ traces are acquired. Data changes in registers can be reflected in power traces. In WDDL circuits, state registers are cleared to zero before each round and the Hamming weight of each register represents the power change of each clock cycle. The correlation between the Hamming weight and the power trace reflects the security level of the countermeasure.

Outputs of the first round, the ninth round and the last round of AES operation are analyzed. All 128 bits of the state registers are used for leakage evaluation. The correlation value is calculated as follows respectively for these three rounds: $correlation(HW(P \oplus K), power)$, $correlation(HW(C_9), power)$ and $correlation(HW(C), power)$. Table I shows the largest correlation for each implementation. Table I shows that the design based on our proposed scheme has much lower leakage than the reference WDDL design. There is a $31.9\%$ decrease for the first round, $22.5\%$ decrease for the ninth round, and $32.8\%$ for the last round. In addition, as long as the wiring length of complementary signals are the same, the DPL-noEE scheme will not provide an advantage.

FPGA resource consumption and power dissipation are important for embedded cryptographic systems. The resource utilization for Xilinx Virtex-5 LX30 FPGA is shown in Table II. Our method not only increases the security level but also decreases the number of slice LUTs from the original's 7031 to 4763. Also, changing initialization values inside the LUT as done in the DPL-noEE countermeasure will not incur any FPGA resource utilization difference. Table III shows the power estimation by XPower Analysis in Virtex-5. The quiescent power is the same among all three. For dynamic power, our method either with or without DPL-noEE has lower dynamic power dissipation, about $18.2\%$ lower than the reference WDDL countermeasure.

TABLE I: Correlation Comparison

| Attack Point | Original WDDL | Proposed WDDL | Proposed WDDL with DPL-noEE |
|---|---|---|---|
| First Round | -0.091 | -0.062 | -0.064 |
| Ninth Round | -0.080 | -0.062 | -0.063 |
| Last Round | -0.061 | -0.041 | -0.040 |

TABLE II: FPGA Resource Utilization in Virtex-5

| Resources | Original WDDL | Proposed WDDL | Proposed WDDL with DPL-noEE |
|---|---|---|---|
| Slice Register | 1495 | 1495 | 1495 |
| Slice LUTs | 7031 | 4763 | 4763 |

TABLE III: Power Consumption Comparison in Virtex-5

| Power | Original WDDL | Proposed WDDL | Proposed WDDL with DPL-noEE |
|---|---|---|---|
| Dynamic | 0.022w | 0.018w | 0.018w |
| Quiescent | 0.380w | 0.380w | 0.380w |
| Total | 0.402w | 0.398w | 0.398w |

## IV. Conclusion

We present a gate level methodology for mapping and placing WDDL implementation of AES in FPGAs. Hamming weight models are adopted to evaluate power leakage on a SASEBO-GII board. The proposed method can reduce more than $20\%$-$30\%$ of the correlation at the evaluated time points. At the same time, FPGA resources and power dissipation are significantly reduced.

## References

[1] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems*, 2004, pp. 16–29.

[2] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," in *Design, Automation and Test in Europe Conference and Exhibition*, vol. 1, 2004, pp. 246–251.

[3] A. Moradi and V. Immler, "Early propagation and imbalanced routing, how to diminish in FPGAs," in *Cryptographic Hardware and Embedded Systems*, 2014, pp. 598–615.

[4] S. Bhasin, S. Guilley, F. Flament, N. Selmane, and J.-L. Danger, "Countering early evaluation: an approach towards robust dual-rail precharge logic," in *Proceedings of the 5th Workshop on Embedded Systems Security*. ACM, 2010, p. 6.

[5] Satoh Laboratory in UEC, "Side-channel attack standard evaluation board SASEBO-GII," http://satoh.cs.uec.ac.jp/SAKURA/hardware/SASEBO-GII.html.