Leakage Evaluation on Power Balance Countermeasure Against Side-Channel Attack on FPGAs

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

***Abstract*—Power leakage through side-channels has been utilized by attackers to recover secret information in embedded cryptographic systems, and various countermeasures have been devised to mitigate this kind of leakage. In hardware systems, examples of such countermeasures include power balance circuits and masked gates. Power balance technologies such as Wave Dynamic Differential Logic (WDDL) aim to balance the power by introducing differential logic. However, the early evaluation effect, which can take advantage of the possible different arrival times for a pair of differential input signals, hampers the strength of the power balance countermeasure. In this paper, we provide a new method to further balance the power of differential signals by manipulating the lower level primitives and applying placement constraints on a Field Programmable Gate Array (FPGA). We use the Advanced Encryption Standard (AES) encryption algorithm as an example to demonstrate the amount of leakage for different implementations. Results show that constraining the differential pair in one LUT does not guarantee power leakage reduction, and placement constraints on state registers are necessary.**

I. Introduction

Side-channel attacks have been a serious threat to the security of embedded cryptographic systems since their introduction [1]. Different attack methods such as Correlation Power Analysis (CPA) [2], Differential Power Analysis (DPA) [1], and template attacks [3] have been widely used to defeat cryptographic systems.

To protect cryptosystems from such attacks, different kinds of protection schemes have been proposed, either at the algorithmic level or at the gate level. For hardware systems like FPGAs and ASICs, power balance circuits are widely used to mitigate side-channel power leakage at the gate level [4], [5]. Wave Dynamic Differential Logic (WDDL) is one such technique and it is effective at mitigating side-channel power leakage. However, techniques such as WDDL suffer from unbalanced power consumption and the early propagation phenomenon which still incurs side-channel power leakage [6].

Different methods have been proposed to mitigate early propagation problems [7], [8]. Researchers are able to configure one single Look-Up Table (LUT) primitive in an FPGA to fit a pair of complementary output signal bits for more balanced circuits. In [7], the authors also propose a method named Dual Rail Precharge Logic without Early Evaluation (DPL-noEE), which can further decrease the power leakage of an AND gate in FPGA implementations. Other researchers aim to balance the routing length to avoid different arrival time for differential signals. In [8], to further reduce the power leakage, an SAT solver and RapidSmith [9] are exploited which can provide feedback to designers about the length of the differential wires.

In this paper, we first map each pair of differential signals into a single LUT and then introduce innovative, interleaved placement constraints for register placement in FPGAs. Results show that AES countermeasure only with LUT constraints cannot achieve the expected results of reducing power leakage and adding the placement constraints will contribute to much lower information leakage in the power side-channel.

We also adopt DPL-noEE which uses different LUT initialization values for the countermeasure against early propagation leakage. Evaluated at three time points for correlation, DPL-noEE does not provide significant improvement when combined with our approach. This demonstrates that mapping two complementary signal bits into one LUT and at the same time ensuring specific register placement will substantially improve WDDL.

The rest of this paper is organized as follows. Section II covers background about WDDL and related work. Details of the implementation of our method at the gate level are discussed in section III. Section IV presents the power correlation analysis using two Hamming weight models. Finally, conclusions and future work are presented in section V.

II. Background and Related Work

For hardware cryptographic systems, there are two popular methods for protecting the crypto module against side-channel analysis at the gate level. One method is power balancing which is to balance the power consumption no matter what operations are being performed; the other is to mask the secret information by introducing random bits to the intermediate state.

Masking introduces random bits to the hardware circuit in order to cover secret information [10], [11]. These methods are effective against first-order attacks, but the overhead is very high. Results show that the area consumption of implementations based on masked gates can be ten times that of the original circuits [11]. Since masking incurs much larger overhead than pure differential circuits, it is reasonable to place more effort on decreasing the leakage in balanced circuits.

The most widely used power balance methods are Simple Dynamic Differential Logic (SDDL) [4] and WDDL [5]. The basic component structure of WDDL is shown in Fig. 1. It has

978-1-4673-9286-0/15/$31.00 ©2015 IEEE

several features to balance the power consumption for different input signals. First, each gate of WDDL has differential input and output ports. Second, there are two fundamental steps for WDDL; one is the pre-charge step when the pre-charge signal is 1, and the other is the evaluation step. During pre-charge, two complementary input signal bits in each pair will both be 0, and this zero value will propagate from input ports to output ports. During the evaluation phase, the calculated signal pair will either be $(0, 1)$ or $(1, 0)$ representing the real value. Third, the Hamming weight of the state register, which represents the number of bit-flips generated during a pre-charge or evaluation cycle in hardware is constant, independent of the values of input signal and inner operation [5], [6].

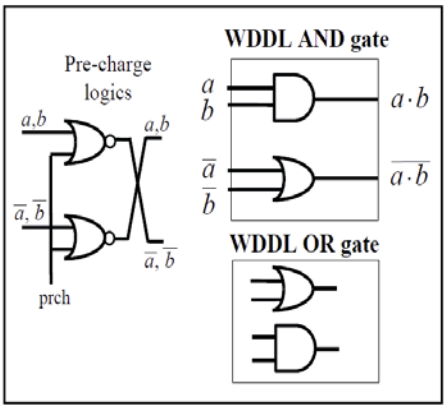

Fig. 1: Components of WDDL

However, researchers have pointed out that WDDL can still leak secret information in practice for two reasons. First, the difference in the loading capacitance between two complementary logic gates in WDDL may cause unbalanced power leakage for different input values, which can be taken advantage of by attackers. The second problem with WDDL is the early evaluation phenomenon, where different arrival times for differential signals incurs information leakage [12], [13].

To mitigate the power leakage problems with WDDL implementations, countermeasures have been proposed to balance the routing path for encryption circuits. Unlike ASICs, where circuit components are completely defined by the designer, combinational and sequential logic can only be mapped into existing resources in FPGAs. It has been shown that it is difficult to balance the routing in FPGAs after the design has been mapped and thus crypto hardware based on WDDL is still vulnerable [8]. Others attempt to make the total length of differential signals equal, while each small signal pair within those signals may still be unbalanced.

Finding a method to make the routing path balanced between each and every pair of complementary signals is the objective of this paper. In section III, we describe mapping every logic gate pair of differential signals to the same slice LUT as well as placing registers on flip-flops in order to balance the routing and minimize the power leakge.

III. Implementation of Gate Level Countermeasure

FPGAs are widely used platforms for cryptographic algorithm implementation. Compared to ASICs, FPGAs are easier to modify, have faster development times and lower cost. Compared to software, FPGAs have faster run time, lower energy consumption, and are less likely to leak information from a cryptanalysis point of view. Also, FPGAs provide a good platform to evaluate prototype designs for encryption algorithms. The development board used in this research is SASEBO-GII [14], which is designed specifically for side-channel attack and security evaluation of countermeasures. Users can acquire the power comsumption waveform of any running operation by a designated port. The board contains two Xilinx FPGAs, one is a cryptographic core using a Virtex-5 series FPGA and the other is a Spartan-3A series acting as the control FPGA. The basic logic unit of a Xilinx FPGA is Configurable Logic Block (CLB). In Virtex-5 FPGAs, one CLB contains a pair of slices where each slice contains 4 LUTs and 4 flip-flops.

A 38 bit general purpose input and output bus connects these two FPGAs for control signal and data transfer. The on-board oscillator is 24 MHz and users can customize the frequency of the input clock signal which determines the speed of the encryption step. For better power acquisition and attack accuracy, we divide the clock frequency by 8 to 3 MHz. This benefits the data acquisition step by providing high quality precise power traces.

A. Standard WDDL Implementation for AES

Fig. 2 shows the hardware architecture of the WDDL implementation of AES [15]. The total key length for AES is 128 bits. Within the design, there is an encryption core which performs the AES operation and a controller which transmits plaintext, ciphertext and control signals to the encryption core. Since WDDL uses differential logic to balance the power, the routing wires that connect each module consists of one pair of signals with bitwise complementary positive and negative values. In Fig. 2, a solid arrow represents one pair of these differential signals.

The precharge signal will first pass precharge input to flush the two registers M and S with all zero values, then let the plaintext go through. For the following clock cycles, one of the registers M and S will be all zero, and the other will store the intermediate state value. Register M has 128 positive and 128 negative bits, and the same applies to register S. After a clock cycle, the value of one register will flush to zero and the other will store the round output value. Due to the existence of complementary bit values in each register, the total Hamming distance for each register is also the total Hamming weight, 128. This means that no matter what plaintext and secret key are applied to the datapath, the power consumption contributed by the register bit-flips from every register is always constant. Finally, the latency of AES encryption with WDDL is doubled to 20 clock cycles, due to the two steps of precharge and evaluation.

978-1-4673-9286-0/15/$31.00 ©2015 IEEE

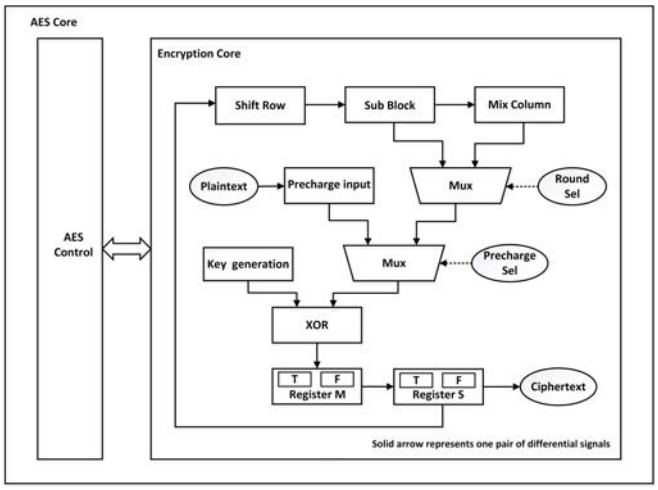

Fig. 2: WDDL implementation of AES Core

B. Logic Mapping in LUTs

A standard FPGA design process includes steps to synthesize, translate, map, place and route, and generate the programming file for the implementation. Every design step has to be considered for a good countermeasure against power analysis attacks. For example, different positive and negative port locations can lead to routing length differences for a specific pair of complementary signals and the parasitic capacitance of the complementary wire can vary due to the unbalanced wiring capacitance. The unbalanced power leakage will lower the security level of the WDDL implementation.

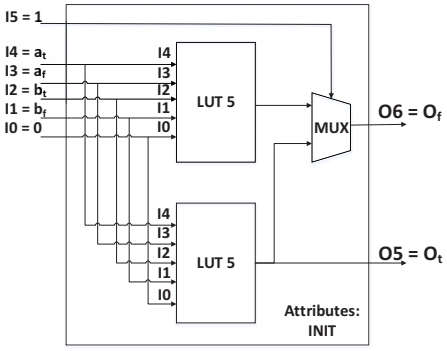

Fig. 3: LUT6_2 Primitive Structure

To mitigate the difference in routing, researchers use the primitive LUT6_2 to ensure that complementary signals of a logic gate are located in the same slice. Fig. 3 shows the LUT6_2 primitive, a type of Xilinx resource that contains two 5-input LUTs and one multiplexor. There are 6 input ports with I_5 connected to a multiplexor; I_0 to I_4 are the inputs of the two 5-input LUTs. Output is produced on ports O_5 and O_6.

Fig. 3 shows the assignment of input and output ports. The input ports are two signals a_t b_t and their complement a_f b_f. O_5 and O_6 are the output ports for complementary results. Logic modules such as AND gate, XOR gate, precharge input module and multiplexor can be mapped to a Virtex-5 FPGA using LUT6_2. This will ensure each complementary signal pair of the combinational logic operations in WDDL implementation is in the same slice.

C. Interleaved Register Placement

To improve the WDDL implementation in FPGAs, we propose a countermeasure of constraining the location of flip-flops for registers M and S in Fig. 2 for the placement and route step in addition to the LUT primitives. Registers are mapped to an FPGA in the form of flip-flops where each slice contains 4 flip-flops in the Virtex-5 series. If placement is done without any constraints, the location of flip-flops after placement will vary, incurring significant loss of security strength due to routing length differences even though the LUTs define the location of the complementary signal pairs.

There are two aspects to consider in register placement: the first is how to place the complementary pair within each registers M and S; the other is how to place the register M and S so that the wiring between them can also be determined.

Take register M in Fig. 2 as an example. Register M contains a pair of registers: register_M_T and register_M_F. Each contains 128 bits and the contents stored are bitwise complementary at each location index. The same applies to register S. First, we guarantee that complementary signal pairs within register M will be located in the same slice. Since each slice contains 4 flip-flops, 2 pairs of signal bits can fit. The routing for the WDDL implementation will benefit significantly from the same location of complementary signals and LUT primitives.

Second, registers M and S are two cascading registers, where the output of register M is the input of register S. It is helpful to shorten the length between these two registers to minimize power leakage and the idea is to interleave them bitwise. The slice location is in the form of "$Slice\_X_iY_j$" and thus the nearest slices are "$Slice\_X_iY_{j+1}$", "$Slice\_X_{i+1}Y_j$", "$Slice\_X_iY_{j-1}$" and "$Slice\_X_{i-1}Y_j$". Assume after placement that two pairs of complementary signals for register M are located in "$Slice\_X_iY_j$". Without loss of generality, we use "$Slice\_X_iY_{j+1}$" as the location of the two signal pairs in register S, which connect to the corresponding two pairs in register M in "$Slice\_X_iY_j$". This approach can be applied to all 128 bit pairs of registers M and S and the wiring length will be the shortest possible between them.

Fig. 4 shows where registers are placed as flip-flops in a Virtex-5 FPGA. Each large frame represents a slice, and the figure only shows the flip-flops in each slice for clarity. Two pairs of complementary register bits can be fit into the four flip-flops AFF, BFF, CFF and DFF. The neighboring slices contain the corresponding register index from another register. In the Virtex-5 FPGA on Sasebo board, since the Y direction cannot contain 128 slices, there registers are divided in half and mapped to $Slice\_X_{18}$ and $Slice\_X_{19}$. The actual location of flip-flops resides in "$Slice\_X_{18}Y_0$" to "$Slice\_X_{18}Y_{63}$" and "$Slice\_X_{19}Y_0$" to "$Slice\_X_{19}Y_{63}$" in this AES implementation. Each slice contains 4 flip-flops and the total number of flip-flops required is $4 * (64 + 64) = 512$.

For register placement, these two aspects of techniques are combined in our improved implementation of WDDL.

978-1-4673-9286-0/15/$31.00 ©2015 IEEE

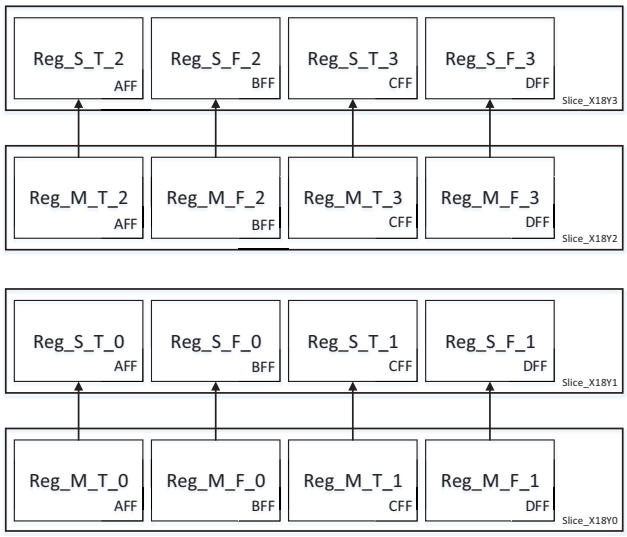

Fig. 4: Part of Placement Constraints in Virtex-5 FPGA

D. DPL-noEE Implementation

The LUT initialization method DPL-noEE [7] is applied as a countermeasure to improve on our proposed WDDL implementation. Assume inputs a, b and their complementary signal are named a_t a_f b_t b_f respectively. The possible input combinations range from "0, 0, 0, 0" to "1, 1, 1, 1". A standard DPL AND gate will perform the operation $O_t = a_t AND b_t$, $O_f = a_f OR b_f$. In [7], 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. Take $a_T, a_F, b_T, b_F = 0, 0, 0, 1$ as an example, its state is Null 0. This means that input combination "0, 0, 0, 1" is an early propagation state transformed from state "0 0 0 0". Compared with standard DPL, the negative output will stay 0 instead of 1. Glitches of early evaluation introduced by unbalanced routing will be mitigated.

After modifying the AND gate using different LUT initialization values, the DPL-noEE countermeasure is evaluated. In section IV, there will be four candidates for comparison: the standard WDDL implementation, WDDL method using only LUT constraints, with both LUT and placement constraints, and additional DPL-noEE modification with both types of constraints. The process properties the synthesis, translate,map, and place and route steps in the Xilinx ISE design tools all use the default settings.

IV. Results and Comparison

In this section, we sample power traces of four different implementations and show the results of power correlation using Hamming weight models targeting three attack points.

A. Power Trace Acquisition Setup

Power trace acquisition is done with a LeCroy WaveRunner 640Zi oscilloscope. The host computer generates and sends 128-bit plaintext and 128-bit secret key to the SASEBO-GII board as the input for every AES operation. The key value is the same for all AES operations and the plaintext is generated by a Pseudo-Random Number Generator (PRNG). Trigger signals will be generated on-board for the oscilloscope to sample all the power traces. In this work, we sample $100,000$ traces for each implementation. One power trace waveform sample is shown in Fig. 5. There are 20 clock cycles latency in the WDDL implementation of AES instead of 10 cycles because of the extra pre-charge stages, and there are $10,000$ points in each power trace.

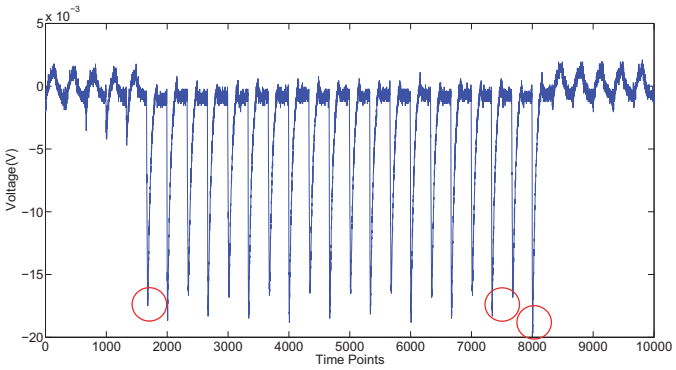

Fig. 5: Power Trace of one AES Encryption

B. Correlation Power Analysis Results

Data changes in registers are reflected in power traces. Generally, there are two models to quantify the influence of the register data changes on power consumption. One is the Hamming weight model, and the other is the Hamming distance model. For WDDL circuits, state registers are cleared to zero before each round, thus the Hamming weight model is used for WDDL implementations and it can also be treated as a special case of the Hamming distance model containing the time point when all register bits are zero. The correlation between the Hamming weight of the register and the power trace is an indication of the security level of the countermeasure.

For side-channel leakage analysis, we focus on the first round, the 9th round and the last round of AES operation, which can all be used for side-channel analysis and evaluation. The corresponding points are represented by three circles in Fig. 5. Since the leakage of WDDL is much smaller than that of the unprotected implementations, we use all the 128 bits of the state register for evaluation. The first leakage point happens at the first clock cycle, and the correlation is:

$$correlation(HW(P \oplus K), power).$$

in which P is the 128 bit plaintext and K is the 128 bit secret key. When $P \oplus K$ is loaded into the register, the register will consume more power which is correlated to $HW(P \oplus K)$. Thus there is a time point in the power trace where the voltage has a strong correlation with $HW(P \oplus K)$.

The second attack point is C_9 which is the output state of the 9^{th} round of AES. The correlation between $HW(C_9)$ and power has been used for leakage assessment:

$$correlation(HW(C_9), power).$$

Similarly, we use the Hamming weight of ciphertext C to run correlation to evaluate the leakage. This third time point

978-1-4673-9286-0/15/$31.00 ©2015 IEEE

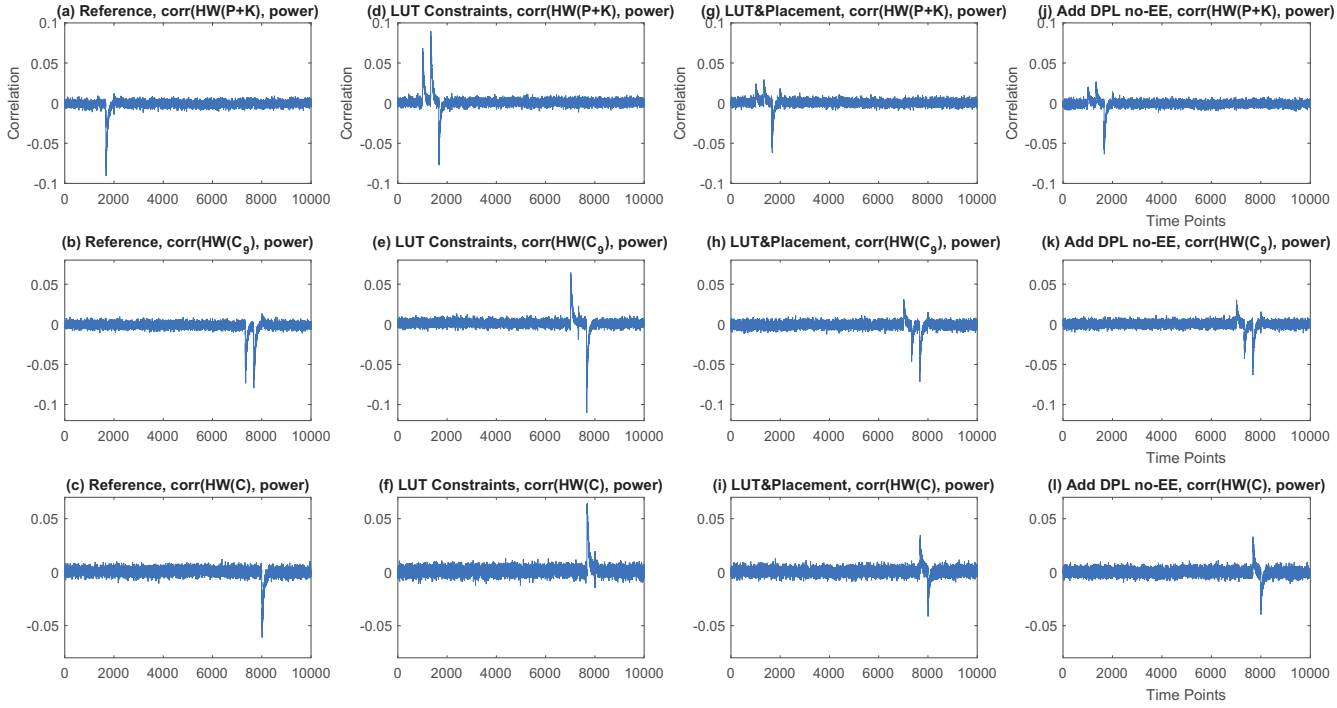

Fig. 6: Correlation Waveform at the First, 9th and Last Round

is at the last round, and the correlation is:

$$correlation(HW(C), power).$$

As stated previously, for WDDL implementation at each rising clock edge, one register is cleared while the other is loaded. While these two registers load the same value at two different times, there should be more than one time point with strong correlation for each CPA result. In addition, clearing and loading registers will cause the same Hamming weight value but in different directions, thus the correlation should contain both positive and negative values. The strongest information leakage happens when the absolute value of the correlation value is the largest.

For leakage assessment, we assume the key value is known for each time point where the correlation value is calculated. Fig. 6(a)(b)(c) provide the correlation results for the first, 9th and last round of the standard WDDL implementation. For this implementation, we use the default mapping and routing constraints, thus the unbalanced routing will incur unbalanced power consumption. To better compare the leakage result among these three designs, we show the correlation results at the three attack time points in Table I. Our results show that the correlation between $HW(P \oplus K)$ and power is about -0.091 for the first time point, correlation between $HW(C_9)$ and power is about -0.080, and the last round leakage is about -0.061 between $HW(C)$ and power. Although this leakage is much smaller than that of unprotected implementations [16], it is still large enough for an attacker to extract the secret information.

As the second implementation, we implement the WDDL with only LUT primitives and the correlation results are shown in Fig. 6(d)(e)(f) for the first, 9th and the last round. Correlation results are shown in Table I. For the first round input and last round output, the values of correlation are both the positive correlation, 0.090 and 0.064 respectively. Interestingly, the correlation value of the 9th round and the last round give an even higher correlation compared with the standard WDDL implementation. Since the experiments use the default settings of the Xilinx ISE tools, this confirms that applying LUTs alone cannot decrease the correlation, and sometimes even has the negative effect.

Attack Point	Standard WDDL	LUT Primitive	LUT and Placement	Add DPL noEE
First	-0.091	0.090	-0.062	-0.064
9th	-0.080	-0.110	-0.062	-0.063
Last	-0.061	0.064	-0.041	-0.040

TABLE I: Correlation Comparison

Next, LUT primitives are combined with placement constraints in the third countermeasure experiments. From Table I and Fig. 6(g)(h)(i), it can be seen that the correlation values based on all three attack modules are decreased significantly. In particular, first round correlation decreases by about 32% compared with the standard and LUT primitive approaches. For the 9th round output, correlations decrease by about 22.5% and 44% respectively and for output of the last round, 33% and 36%.

We also implement our proposed scheme together with the DPL-noEE LUT design [7]. The corresponding correlation results are shown respectively in Fig. 6(j)(k)(l). The correlation

978-1-4673-9286-0/15/$31.00 ©2015 IEEE

result is similar to our proposed implementation without DPL-noEE. We find that whether or not we add DPL-noEE to our design, the leakage is almost the same. This proves that our method helps to eliminate the unbalanced routing problem, and as long as the wiring length of complementary signals are the same, the DPL-noEE scheme will not provide an advantage.

V. Conclusions and Future Work

In this paper, we present a gate level methodology for mapping and placing WDDL implementation of AES on FPGAs. Hamming weight models are adopted to evaluate power leakage on a SASEBO-GII board. Results show that the LUT primitive method alone does not guarantee countermeasure improvement against power analysis attack. When combined with the placement constraints and LUT primitives, we can largely reduce the correlation at all attack points. For future work, this methodology should improve the resistance against the ElectroMagnetic attacks, which is worth evaluating. Other cryptographic primitives with countermeasures implemented on different FPGA families and their resilience against side-channel power analysis will be evaluated.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology – CRYPTO 99*, 1999, pp. 388–397.

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

[3] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems – CHES 2002*, 2002, pp. 13–28.

[4] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Solid-State Circuits Conference, 2002. ESSCIRC 2002. Proceedings of the 28th European*. IEEE, 2002, pp. 403–406.

[5] 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, 2004. Proceedings*, vol. 1, Feb 2004, pp. 246–251 Vol.1.

[6] D. Suzuki and M. Saeki, "Security evaluation of DPA countermeasures using dual-rail pre-charge logic style," in *Cryptographic Hardware and Embedded Systems – CHES 2006*, 2006, pp. 255–269.

[7] 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.

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

[9] C. Lavin, M. Padilla, J. Lamprecht, P. Lundrigan, B. Nelson, B. Hutchings, and M. Wirthlin, "A library for low-level manipulation of partially placed-and-routed fpga designs," Technical report, Brigham Young University, 2014.

[10] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *Cryptographic Hardware and Embedded Systems – CHES 2005*, 2005, pp. 172–186.

[11] A. J. Leiserson, M. E. Marson, and M. A. Wachs, "Gate-level masking under a path-based leakage metric," in *Cryptographic Hardware and Embedded Systems – CHES 2014*, 2014, pp. 580–597.

[12] D. Suzuki, M. Saeki, and T. Ichikawa, "DPA leakage models for CMOS logic circuits," in *Cryptographic Hardware and Embedded Systems – CHES 2005*, 2005, pp. 366–382.

[13] K. Tiri and I. Verbauwhede, "Place and route for secure standard cell design," in *Smart Card Research and Advanced Applications VI*, ser. IFIP International Federation for Information Processing, 2004, vol. 153, pp. 143–158.

[14] National Inst. of Advanced Industrial Science and Technology of Japan, "Side-channel attack standard evaluation board SASEBO-GII," http://satoh.cs.uec.ac.jp/SAKURA/hardware/SASEBO-GII.html.

[15] Information Physical Security Research Group in YNU, "An AES encryption circuit with DPA countermeasure WDDL," http://ipsr.ynu.ac.jp/circuit/.

[16] P. Luo, Y. Fei, L. Zhang, and A. Ding, "Side-channel power analysis of different protection schemes against fault attacks on AES," in *ReConFigurable Computing and FPGAs (ReConFig), 2014 International Conference on*, Dec 2014, pp. 1–6.

978-1-4673-9286-0/15/$31.00 ©2015 IEEE