Design for EM Side-Channel Security through Quantitative Assessment of RTL Implementations

Jiaji He[1], Haocheng Ma[2], Xiaolong Guo[3], Yiqiang Zhao[2] and Yier Jin[4]
[1]Institute of Microelectronics, Tsinghua University, China
[2]School of Microelectronics, Tianjin University, China
[3]Department of Electrical and Computer Engineering, Kansas State University, USA
[4]Department of Electrical and Computer Engineering, University of Florida, USA
e-mail: [1]jiaji_he@mail.tsinghua.edu.cn, [2]{hc_ma, yq_zhao}@tju.edu.cn, [3]guoxiaolong@ksu.edu, [4]yier.jin@ece.ufl.edu

Abstract— Electromagnetic (EM) side-channel attacks aim at extracting secret information from cryptographic hardware implementations. Countermeasures have been proposed at device level, register-transfer level (RTL) and layout level, though efficient, there are still requirements for quantitative assessment of the hardware implementations' resistance against EM side-channel attacks. In this paper, we propose a design for EM side-channel security evaluation and optimization framework based on the *t*-test evaluation results derived from RTL hardware implementations. Different implementations of the same cryptographic algorithm are evaluated under different hypothesis leakage models considering the driven capabilities of logic components, and the evaluation results are validated with side-channel attacks on FPGA platform. Experimental results prove the feasibility of the proposed side-channel leakage evaluation method at pre-silicon stage. The remedies and suggested security design rules are also discussed.

I. Introduction

The fast growth of the hardware devices results in increased demand for intellectual property (IP) cores and complex connectivity, which brings on more potential vulnerabilities. The impact of cyber attack and design flaws in IP cores threatens to overturn the credibility of 3rd-party vendors as well as increases security risks on the customers and end users. Although previous solutions, like cryptographic algorithms, were proposed to protect the confidentiality, the sensitive information in implementations are still vulnerable to various attacks, such as side-channel attacks.

Side-channel attacks aim at recovering the information processed in devices by monitoring physical manifestations, including timing differences, power consumption, EM radiation, etc. Comparing with other physical measurements, the EM based side-channel attack has significant advantages, including non-contact detection, location awareness, and rich frequency information. EM radiations can be generally categorized into two types: direct radiation and modulated radiation [1]. *Direct radiations* are caused directly by current flow with sharp rising/falling edges, while *modulated radiations* occur when a signal modulates carrier signals which then generate EM radiations propagating into the space. The direct EM radiations arise as a consequence of current flows within logic gates or other logical parts inside a circuit, where the currents have a correlation with logical operations performed in the design.

There are different ways of implementing arithmetical operations on hardware, including instruction- or circuit-based operations [2], [3]. For instruction-based operations, side-channel attacks aim at extracting keys from the differences of the pipelined execution of instructions in microprocessors. For circuit-based operations, the side-channel information is leaked from the differences of the logical changes conducted by physical logic components. Countermeasures for the side-channel attacks have been proposed at device (logical) level, register-transfer (transistor) level and layout (physical) level, however, the resistance of hardware implementations against side-channel attacks has not been systematically studied.

Furthermore, most of the hardware vulnerabilities, which are explored to perform the attack, are the result that designers do not address security problems adequately [4]. With growing complexity of hardware system designs, the workload is overwhelming for the designers to manually diagnose security vulnerabilities. In addition, mitigating vulnerabilities after the design stage results in increased costs and delayed time-to-market (TTM). Therefore, an efficient pre-silicon evaluation mechanism at the register-transfer level is needed to assess the capability of hardware implementations against EM side-channel attacks and instruct designers to produce more secure hardware. Previous works in [5], [6] established RTL power models to evaluate the side-channel vulnerabilities at pre-silicon stage of a design. However, they do not enhance the vulnerable hardware implementations and only resist the power-based side-channel attack.

In this paper, we propose an EM side-channel security evaluation and optimization framework to perform quantitative assessment of the RTL implementations. Among different implementations or instances for the same specification, the ranking of the capabilities against EM side-channel attack will be given along with quantitative evaluation values by the framework. Besides, security design rules that can be utilized to optimize the implementations are discussed. In the working procedure of the framework, for the first step, an EM radiation information leakage model is established utilizing the RTL code of a design considering the circuit's structural and functional parameters, including logical components, driven capabilities, switching activities and logical status. Note that these simulated EM radiation traces, referred to as *L-traces*, are not real side-channel radiation. *L-traces* represent the chip's side-channel behaviors [7], which can be utilized to evaluate the EM side-channel information leakage. *t*-test [8] together with Test Vector Leakage Assessment (TVLA) [9] are introduced to quantify the information leakage according to various operating statistical moments. The contributions of

978-1-7281-4123-7/20/$31.00 © 2020 IEEE

our paper are listed as follows.

- For the first time, a quantitative radiation model is established from a given RTL code for systematically evaluating the EM side-channel vulnerability.
- Bit level fine-grained information leakage vulnerabilities are identified and localized in the RTL implementations based on *t*-test evaluation results.
- Generic security design rules are outlined for designing EM side channel attack resistant hardware implementations by given an arbitrary specification at RTL designs.

The rest of the paper is organized as below. The proposed framework is presented in Section II. Section III demonstrates our framework by evaluating representative AES benchmarks. Limitations are discussed with proposed security design rules in Section IV. Conclusions are drawn in Section V.

II. EM Side-Channel Security Framework

The proposed framework involves two parts - evaluation and optimization. Fig. 1 outlines the EM side-channel security quantitative evaluation part in the framework by evaluating cryptographic algorithms as an example. It mainly includes three parts: the analysis of the RTL implementation shown in ①, the EM radiation simulation and the generation of *L-traces* shown in ②, and the leakage quantitative assessment shown in ③. In ①, the RTL implementations are analyzed to extract the logical components and the corresponding driven capabilities, because the logic gates and other logical parts inside a circuit contribute directly as the source of EM radiation. The detailed derivation is presented in Section II-A. In ②, the stimuli are applied to motivate the circuits, and the switching activities of the logical components as well as the logical status of the internal signals are extracted. With all the data collected above, the *L-traces* are calculated with different leakage models. Details are introduced in Section II-B. In ③, the quantitative assessment is performed, where *t*-test results and univariate TVLA results are analyzed. Details about the assessment metrics can be found in Section II-C.

A. RTL Implementation and EM Radiation Modeling

To evaluate the circuit's EM information leakage at pre-silicon stage, there are several levels of EM radiation modeling and simulation, including layout level, gate level and register-transfer level. At layout level, the most popular method is to calculate the EM radiation using a 3D or planar EM simulator. Although this process is proved accurate, it requires massive computation resources and is time-consuming. This calculation is not practical for IC designers. At gate and register-transfer level, the EM radiation simulations follow a similar theory, where a specific leakage model is utilized in the simulation process. Hamming Distance (HD) model, Hamming Weight (HW) model and other improved HD, HW models are used to simulate EM radiation at gate and register-transfer levels. As for the EM radiation modeling, Peeters et al. [10] present an improved EM leakage model called switching distance model based on the hypothesis that charging (respectively, discharging) the capacitance involves a leakage of +1 (respectively, -1). However, the simulation using this model can only obtain a single aggregated view of global EM radiation, and the weight allocation limits

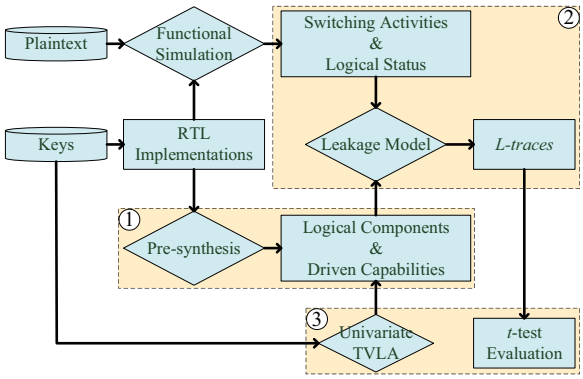


Fig. 1. The security evaluation on a cryptographic algorithm implementation

simulation precision. The framework proposed in [11] utilizes design data from RTL to generate circuit's EM radiation. Considering the FPGA implementation, the fan-out numbers of registers and look-up tables (LUTs) have been taken into account. Although the method can quickly acquire EM traces generated from cryptographic devices, the authors did not validate the simulated traces' consistency with chip measurement under different leakage models. Furthermore, all the above EM radiation simulation and side-channel information leakage evaluation methods are not able to provide specific feedback on how to design a more side-channel resistant implementations.

The primary goal of the EM radiation modeling in this paper is to assess the EM side-channel information leakage of RTL implementations. In order to establish the correlations between the EM information leakage and RTL code, we assume the *partial Boolean difference* [12] of $f(x_0, x_1, \ldots, x_{n-1})$ with respect to one variable or a subset of variables is defined in Equation (1):

$$\frac{\partial f}{\partial x_i} = f_{x_i} \oplus f_{x_i'} \tag{1}$$

where $f_{x_i} = f(x_0, x_1, \ldots, 1, \ldots, x_{n-1})$ and $f_{x_i'} = f(x_0, x_1, \ldots, 0, \ldots, x_{n-1})$. The *total Boolean difference* of $f(x_0, x_1, \ldots, x_i, \ldots, x_{n-1})$ with respect to a k-variable subset of its inputs is defined as Equation (2):

$$\frac{\mathrm{d}f}{\mathrm{d}(x_{i1}x_{i2}\ldots x_{ik})} = \sum_{j=0}^{2^{k-1}-1} \frac{\partial f}{\partial \overrightarrow{x}}|_{m_j}(m_j + m_{2^k-j-1}) \tag{2}$$

where m_j's are defined in Equation (3) and Equation (4):

$$\begin{aligned} m_0 &= x_{i1}^{'}x_{i2}^{'}\ldots x_{in-1}^{'}x_{ik}^{'} \\ m_1 &= x_{i1}^{'}x_{i2}^{'}\ldots x_{in-1}^{'}x_{ik} \\ &\ldots \\ m_{2^k-1} &= x_{i1}x_{i2}\ldots x_{in-1}x_{ik} \end{aligned} \tag{3}$$

$$\frac{\partial f}{\partial \overrightarrow{x}}|_{m_j} = \frac{\partial f}{\partial(x_{i1}^{*}x_{i2}^{*}\ldots x_{ik}^{*})} \tag{4}$$

The logic gates in the circuits can be roughly classified into sequential logic and combinational logic. It has been demonstrated in [11] that the simulated EM traces, which are obtained through calculating the signal switching operations and fan-outs within the circuits, have a good correlation with

FPGA measurements. However, according to the theory presented in Equation (1), different variables are also important for the assessment of side-channel leakage.

In the proposed framework, both HD and HW models are utilized to simulate the EM radiation. The HD model is more applicable to evaluate the differences between sequential states, while the HW model is more suitable to evaluate the status of every single state. Except for the EM information leakage model, several papers have focused on the source from the perspective of the hardware that is responsible for generating the EM radiation. In [13], the authors provided an important observation that signal leakage is exclusively restricted to a time-span as short as the combinational path after the active clock edge when analyzing local EM measurements close to the source of leakage. An interpretation of this observation is that the EM leakage is related with registers that are driven by clock signals and are processing the information. Depending on this observation, the EM leakage is related with registers that are driven by clock signals and are processing the information. Considering the Equation (2), the HD model is more suitable to assess the EM information leakage, nevertheless, the HW model is also evaluated as a comparison in this paper. The modeling method can be applied to both ASIC and FPGA applications. Information on the implementations, including registers and driven capabilities, of the RTL code is required. EDA tools are utilized to map RTL code to registers and other logic components. Note that even if different users apply different synthesis strategies, the logical components and driven capabilities are still determined by the RTL code, therefore, the modeling method is still valid. In the ASIC design flow, however, the implementations of RTL code are influenced by both technology libraries and synthesis strategies. In contrast, the modeling method suits FPGA applications better because the basic logic components in FPGA are only look-up-tables (LUTs) and registers.

B. RTL EM Information Leakage Calculation

As indicated by Equation (1) and (2), the variables are also required. For the hardware implementations, the variables are the stimuli that are provided to the RTL implementations of the circuits to extract the fine-grained switching activities and logical status of every logical components. The simulation of the *L-traces* is illustrated in Algorithm 1. The *RTL_imp* is the RTL implementations of the circuits, and the $iv(t)$ represents the plaintext and other stimuli needed to motivate the circuits. The final output *L-traces*(iv, t) will be the EM radiation information with leakage models. Firstly, the RTL implementations are synthesized to extract the logical components and driven capabilities information as discussed in Section II-A. Then, under different stimuli, the RTL code is simulated to collect basic parameters, including the switching activities and logical status. The switching activities within current paths of a circuit's implementation will cause changes in register status. In each clock cycle, the states of signals under evaluation and these corresponding driven capabilities are recorded. With all information collected, *L-traces* are generated simultaneously for the evaluation of side-channel vulnerabilities with leakage models.

Algorithm 1 L-traces simulation

Input:
RTL_{imp} ▷ Original circuit implementations.
$iv(t)$ ▷ Input vectors at time point t.
Output: $L\text{-}traces(iv, t)$ ▷ The simulated EM radiation at time point t under the stimuli iv.
$LogicalComponents \leftarrow RTL_{imp}$;
$DrivenCapabilities \leftarrow LogicalComponents$;
for Each t **do**
  $List_{SwitchingActivities} \leftarrow RTL_{imp}|iv(t)$;
  $List_{LogicalStatus} \leftarrow RTL_{imp}|iv(t)$;
end for
$H(A_i)$, $F_i \leftarrow list_{SwitchingActivities}$; ▷ HW model
A_i, B_i $F_i \leftarrow list_{LogicalStatus}$; ▷ HD model
$L\text{-}traces(iv, t) \leftarrow H(Ai), A_i, B_i, F_i$;

For the HW model, the input vector of the circuit is denoted as iv. The EM radiation R of the target logic component in the circuit under test is modeled in Equation (5) where A_i denotes the logical states of the i_{th} register, t denotes the time of simulation, and $H(A_i)$ means the HW of A_i. Based on the RTL code, a script is developed to calculate registers and driven capabilities. The fan-out number of the i_{th} register is denoted as F_i, and simulated EM side-channel leakage *L-traces* is modeled in Equation (6). A $N \times L$ matrix T is generated where N denotes the number of different plaintexts and L means the number of sampling points in simulation.

$$R(iv, t) = \sum_{i=1}^{n} H(A_i)|_{iv} \tag{5}$$

$$\textit{L-traces}(iv, t)_{HW} = \sum_{i=1}^{n} F_i \times H(A_i)|_{iv} \tag{6}$$

For HD model, the initial and final states of the i_{th} register/LUT are denoted as A_i and B_i respectively, and t represents the moment of the transition under the input vector iv. The transitions of all registers/LUTs in the circuit under test are modeled in Equation (7), where $\oplus$ denotes the exclusive-OR operation. Then a TCL script is utilized to calculate registers, LUTs and driving capabilities. The fan-out number of the i_{th} register or LUT is denoted as F_i, then the simulated EM side-channel trace is modeled in Equation (8).

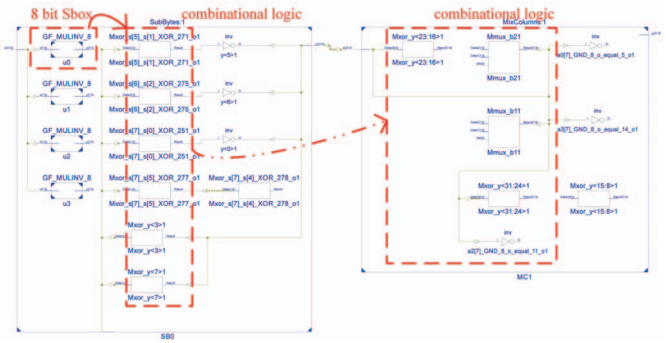
$$D(t) = \sum_{i=1}^{n} (A_i \oplus B_i)|_{iv} \tag{7}$$

$$\textit{L-traces}(iv, t)_{HD} = \sum_{i=1}^{n} F_i \times (A_i \oplus B_i)|_{iv} \tag{8}$$

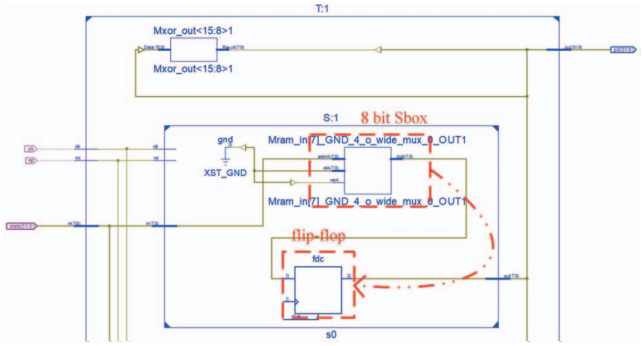
C. T-test Leakage Evaluation Metric

To quantitatively evaluate the level of information leakage, there are basically two main metrics, which are the measurements to disclosure (MtD) and Welch's *t*-test. The number of MtD represents the beginning of the first sequence of a certain number of successive correct guesses of the secret key along with the increasing of the number of *L-traces*. The MtD is usually applied in correlation side-channel attack [14] that calculates the Pearson correlation function between each measured EM trace and a hypothetical EM value, and then recovers the secret key from a large number of correlation computations. The Welch's *t*-test is the most

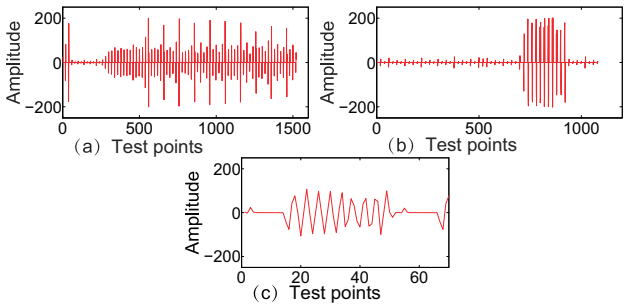
(a) RTL schematic of AES_NIST.



(b) RTL schematic of AES_LUT.



(c) RTL schematic of AES_CEP.



(d) Simulation of (a) AES_NIST, (b) AES_LUT and (c)AES_CEP

Fig. 2. RTL schematics of AES_NIST, AES_LUT, AES_CEP, and their respective simulation traces.

common approach to assess if two sets of data are significantly different from each other. For the assessment of the information leakage in the proposed framework, the *t*-test is more applicable because different variables and stimuli are applied in the evaluation process. Furthermore, the test vector leakage assessment (TVLA) methodology [9] is utilized together with the *t*-test distinguisher to detect statistical dependencies between sensitive data and side-channel information, where two sets of measurements partitioned are analyzed according to sensitive information.

Assume μ_i, s_i^2 and n_i to be sample mean, variance, and cardinality of set i, respectively, where $i \in \{1, 2\}$. Then, the t value is computed in Equation (9). If the t value is outside the ± 4.5 range, the test rejects the null-hypothesis with confidence greater than 99.999% for large numbers of measurements, i.e. indicating that the mean of the sets at a particular sample is distinguishable and thus highlighting the existence of side-channel leakage [15]. However, a higher $|t|$ does not guarantee success of side-channel attacks.

$$t = \frac{\mu_2 - \mu_1}{\sqrt{\frac{s_1^2}{n_2} + \frac{s_1^2}{n_1}}} \tag{9}$$

For instance, in the side-channel information leakage assessment of modern cryptographic block ciphers, cipher texts are of 64, 128, or more bits. Treating the texts as a single entity cannot guarantee the fine-grained information leakage evaluation. Therefore, the *t*-test should be applied in an univariate manner to each variable of the ciphertext, and the univariate setting enables the tracking of every single bit of the cipher texts. Although the information leakage may not be manifested in the univariate setting, the *t*-test results can still serve as an indicator of the level of differentials that can be utilized to extract sensitive information.

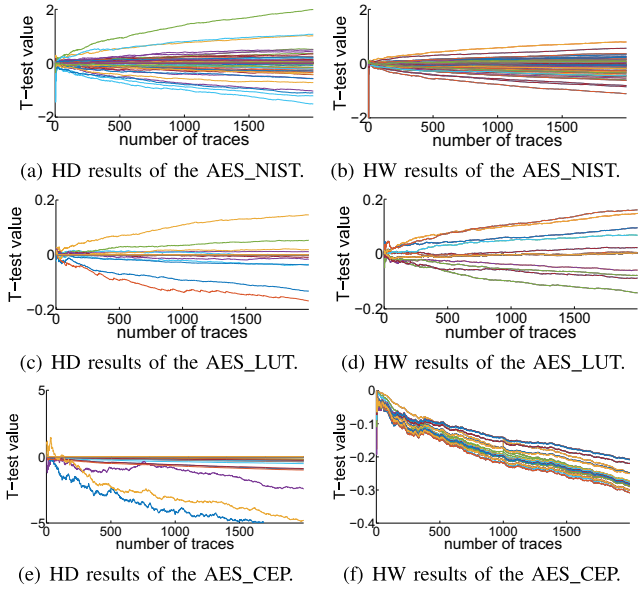
III. Experimentation

To demonstrate the feasibility of the proposed framework, three representative AES hardware implementations are evaluated from the perspective of information leakage. The practicality of the proposed leakage evaluation framework is also validated with actual FPGA measurements, where those benchmarks are configured into FPGAs and correlation side-channel attacks are performed. Proof-of-concept experiments are carried out to demonstrate the effectiveness of the security design rules countering EM side-channel attacks.

A. AES Benchmarks

All three AES benchmarks are open source designs realizing the AES algorithm by different developers. The first AES implementation is designed in the light of NIST standard [16], denoted as AES_NIST. The second AES implementation is designed by the developers with Satoh Lab. [17], denoted as AES_LUT. The third AES implementation is extracted from the release of a common evaluation platform by MIT Lincoln Lab. supported by DARPA [18], denoted as AES_CEP. The AES_NIST is the official version of AES hardware implementations, the AES_LUT is a commercial version, and the AES_CEP is an IP module in a system on chip (SoC).

Different RTL implementations can lead to diverse circuit structures and finally result in different side-channel leakages. The corresponding RTL schematics are shown in Fig. 2. In order to demonstrated the key related RTL implementations, we focused on the lower 8 bits output of S-box and the related signal processing units. As shown in AES_NIST schematic, the signals from S-box block are stored in the registers of



(a) HD results of the AES_NIST. (b) HW results of the AES_NIST.

(c) HD results of the AES_LUT. (d) HW results of the AES_LUT.

(e) HD results of the AES_CEP. (f) HW results of the AES_CEP.

Fig. 3. *t*-test evaluation results of different AES implementations.

a cipher block first and then passed through the following encryption operations. In AES_LUT schematic, the signals from S-box block are passed to mixcolumn operation directly, and in AES_CEP schematic, the signals from S-box are passed directly to an internal flip-flop. The AES_CEP has a similar schematic with the AES_NIST, but each of the encryption rounds are instantiated, thus the circuit area of AES_CEP is much bigger and the operation of the AES_CEP is in a pipelined style, resulting in a faster encryption.

B. Leakage Evaluation of Different AES Implementations

The corresponding EM traces under the same secret keys and plaintexts are simulated in MATLAB according to Equation (6) and (8), and the simulation results are shown in Fig. 2(d). The EM radiation emanated by three AES implementations on FPGAs are diverse due to their different RTL schematics. It is clear that compared with AES_LUT, extra EM leakages are generated between adjacent encryption rounds of AES_NIST circuit due to the data storage in the registers. Under the same circumstances and sampling rate, the AES_CEP takes much less time to perform the encryption operation, and the reason for this is the pipelined execution feature of the RTL implementation.

To quantitatively evaluate the level of information leakage, *t*-test results are also calculated, and the *t*-test evaluation results are demonstrated in Fig. 3, and the comprehensive information is shown in Table I. Overall, the *t*-test evaluation results match well with the time domain simulation results, and the HD model is more suitable for the evaluation framework as the *t*-test results utilizing HD model is higher than that with HW model. More specifically, from the simulation results, the AES_CEP has the most obvious information leakage as the *t*-test value with HD model exceeds 4.5 within the 2000 traces. Although the *t*-test results of AES_NIST and AES_LUT do not reach 4.5 with only 2000 traces, the AES_NIST has more obvious information leakage than the AES_LUT. Overall, the leakage evaluation of three AES implementations validates that the implementations with more registers and clock varieties have higher level of information leakage.

TABLE I
AES IMPLEMENTATION VALIDATION

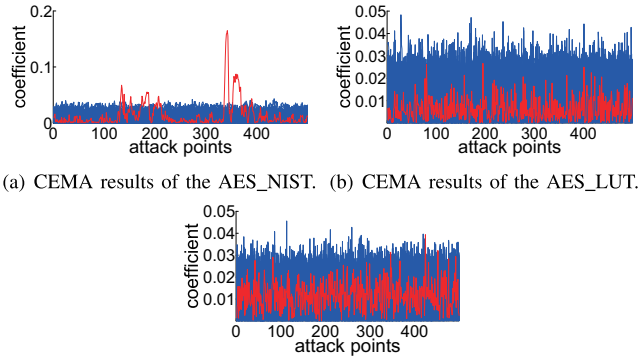
	AES_NIST	AES_LUT	AES_CEP
Total registers	1595	649	6566
High fan-out registers	13	26	872
Clock varieties	28	8	119

C. FPGA Experiments on AES Implementations

Correlation EM attack (CEMA) is a powerful evaluation method for evaluating the EM information leakage for cryptographic circuits. To demonstrate the effectiveness of the framework, FPGA measurements on the implementations of AES_NIST, AES_LUT and AES_CEP are carried out, and the correlation analysis is performed to check the correspondence of the *t*-test evaluation results with actual MtD values. Total 10000 traces of three AES implementations each are collected using SAKURA-G [19] board, and the RF2 probe from LANGER [20] is utilized for EM radiation measurement. The attack point selected is the last round of AES operation, where the S-box output of the last round is analyzed utilizing the collected EM traces. The CEMA results are illustrated in Fig. 4. From the CEMA results of the AES_NIST, the right key stands out indicating the attack is successful within 10000 traces, while the CEMA results of the AES_LUT and AES_CEP shows the right key guess is still mixed with the wrong key guesses, indicating the attack is failed within 10000 traces. The FPGA experiments of AES_NIST and AES_LUT validate the proposed EM side-channel security evaluation framework. However, according to the analysis in Section III-B, the AES_CEP should have more information leakage than AES_NIST, and the reason for this discrepancy is discussed in Section IV.

IV. DISCUSSIONS

From the theoretical analysis and experimentation above, the feasibility of the proposed framework is validated and three implementations of one representative encryption algorithm are analyzed and compared utilizing the framework. One exception is the FPGA experiments on the AES_CEP hardware implementations. For the AES_CEP, although the RTL assessment shows the most significant information leakage level, its hardware implementation is the most side-channel resistant one among three different AES implementations. The observations are as follows. In the AES_CEP implementation, although there are much more registers instantiated from the RTL code, the registers are implemented into RAM format in FPGA. In the AES_CEP, the designers adopted *case* statements among the clock controlled *always* block, and the segment of RTL code is shown in Fig. 5, while the AES_NIST and AES_LUT utilize *assign* statements and other logical operators. This coding style results in a single-port distributed read-only RAM in FPGA implementation. The sequential access feature of RAM will not cause much correlation between the operation of the data with the side-channel information.



(a) CEMA results of the AES_NIST. (b) CEMA results of the AES_LUT.

(c) CEMA results of the AES_CEP.

Fig. 4. FPGA CEMA results of (a) AES_NIST, (b) AES_LUT and (c) AES_CEP implementations.

Furthermore, although the circuit size of the AES_CEP is much bigger than the other two implementations, the pipelined execution actually reduces the toggling rate of the registers. There are total 10 key expansion and 10 encryption blocks in the AES_CEP implementation, however, only 1 block will be activated by the clock within the pipelined execution. Again, the AES_CEP RTL implementation validates the design for side channel security rules. The evaluation framework provides a circuit designer the foresight of EM information leakage level. However, the hardware instantiations are still vital to the level of information leakage.

RTL descriptions are high-level representations of a circuit, from which gate-level representations and ultimately logic gates and wiring are derived. There are usually two kinds of logical components in the circuits: sequential logic and combinational logic. Registers (usually implemented as D flip-flops) synchronize the circuit's operation to the edges of the clock signals, and are the only elements in the circuit that have memory properties. The registers' outputs are checked every clock cycle. Furthermore, the registers are utilized for latching the signals from the combinational logic. Combinational logic performs all the logical functions in the circuit and the computation result updates whenever the input signals are updated, so the output values of the combinational logic may remain constant for more than one clock cycle. According to the analysis above, to reduce the information leakage, the circuit's logical components need to be carefully designed. The registers' read and write operations are usually directly related with data operations, which have the most significant logical correlations with the EM radiation. Also, the clock signal and its varieties contribute directly to the EM radiation.

V. Conclusion and Future Work

In this paper, the vulnerabilities which can lead to the success of EM side-channel attack are detected and localized quantitatively in the early design stage. We validate the work in the practical scenario among various RTL benchmarks. For future work, security design rules will be summarized, and we will demonstrate how developers can optimize the vulnerable designs to improve the confidentiality following the proposed security design rules, also we will continually enhance the framework to cover more general hardware with more design rules delivered and validated.

```
module S (clk, rst, in, out);
    input clk;
    input rst;
    input [7:0] in;
    output reg [7:0] out;

    always @ (posedge clk or posedge rst)
        if (rst)
            out <= 8'd0;
        else
            case (in)
                8'h00:  out <= 8'h63;
                8'h01:  out <= 8'h7c;
                8'h02:  out <= 8'h77;
```

Total 256 lines of *case* statements

Fig. 5. Segment of RTL Code in AES_CEP

Acknowledgments

This work was supported in part by National Institute of Standards and Technology (NIST) under Grant 60NANB18D214. Dr. Jiaji He is supported by the China Postdoctoral Science Foundation under Grant 2019TQ0167.

References

[1] H. Li, A. T. Markettos, and S. Moore, "Security evaluation against electromagnetic analysis at design time," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2005, pp. 280–292.

[2] K. Atasu, L. Breveglieri, and M. Macchetti, "Efficient aes implementations for arm based platforms," in *Proceedings of the 2004 ACM Symposium on Applied Computing*, ser. SAC '04. New York, NY, USA: ACM, 2004, pp. 841–845. [Online]. Available: http://doi.acm.org/10.1145/967900.968073

[3] P. Chodowiec and K. Gaj, "Very compact fpga implementation of the aes algorithm," in *Cryptographic Hardware and Embedded Systems - CHES 2003*, C. D. Walter, Ç. K. Koç, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 319–333.

[4] L. Batina, N. Mentens, and I. Verbauwhede, "Side-channel issues for designing secure hardware implementations," in *11th IEEE International On-Line Testing Symposium*, July 2005, pp. 118–121.

[5] M. He, J. Park, A. Nahiyan, A. Vassilev, Y. Jin, and M. M. Tehranipoor, "Rtl-psc: Automated power side-channel leakage assessment at register-transfer level," *CoRR*, vol. abs/1901.05909, 2019.

[6] S. A. Huss, M. Stöttinger, and M. Zohner, "Amasive: an adaptable and modular autonomous side-channel vulnerability evaluation framework," in *Number Theory and Cryptography*. Springer, 2013, pp. 151–165.

[7] S. B. Rs, F. Grkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an asic aes implementation," in *International Conference on Information Technology: Coding and Computing*, 2004, p. 546.

[8] T. Schneider and A. Moradi, "Leakage assessment methodology - a clear roadmap for side-channel evaluations," 2015.

[9] G. C. Becker, J. Cooper, E. DeMulder, G. Goodwill, J. Jaffe, G. Kenworthy, T. Kouzminov, A. Leiserson, M. E. Marson, P. Rohatgi, and S. Saab, "Test vector leakage assessment (tvla) methodology in practice (extended abstract)," 2013.

[10] E. Peeters, F. X. Standaert, and J. J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration the Vlsi Journal*, vol. 40, no. 1, pp. 52–60, 2007.

[11] J. He, Y. Zhao, X. Guo, and Y. Jin, "Hardware trojan detection through chip-free electromagnetic side-channel statistical analysis," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 10, pp. 2939–2948, Oct 2017.

[12] N. Mohyuddin, E. Pakbaznia, and M. Pedram, *Probabilistic Error Propagation in a Logic Circuit Using the Boolean Difference Calculus*, 2011.

[13] J. Heyszl, D. Merli, B. Heinz, F. D. Santis, and G. Sigl, *Strengths and Limitations of High-Resolution Electromagnetic Field Measurements for Side-Channel Analysis*, 2013.

[14] T. Sugawara, Y.-i. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, and A. Satoh, "Spectrum analysis of cryptographic modules to counteract side-channel attacks," *EMC '09*, vol. 6, 01 2009.

[15] B. J. Gilbert Goodwill, J. Jaffe, P. Rohatgi *et al.*, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*, vol. 7, 2011, pp. 115–136.

[16] Secworks, "Nist document fips 197 based aes design," https://github.com/secworks/aes, 2014.

[17] S. Lab, "Lookup tabel based aes design," http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html, 2017.

[18] L. LABORATORY, "Cep aes design," https://github.com/mit-ll/CEP, 2018.

[19] SAKURA, *http://satoh.cs.uec.ac.jp/SAKURA/index.html*.

[20] LANGER, *https://www.langer-emv.com/en/index*.