Analysis of Side-Channel Attack AES Hardware Trojan Benchmarks against Countermeasures

Sudeendra kumar K, Sauvagya Sahoo, Abhishek Mahapatra, Ayas Kanta Swain, K.K.Mahapatra
ECE Dept., NIT Rourkela, India
kkm@nitrkl.ac.in

***Abstract*- Hardware Trojan (HT) is one of the well known hardware security issue in research community in last one decade. HT research is mainly focused on HT detection, HT defense and designing novel HT's. HT's are inserted by an adversary for leaking secret data, denial of service attacks etc. Trojan benchmark circuits for processors, cryptography and communication protocols from Trust-hub are widely used in HT research. And power analysis based side channel attacks and designing countermeasures against side channel attacks is a well established research area. Trust-Hub provides a power based side-channel attack promoting Advanced Encryption Standard (AES) HT benchmarks for research. In this work, we analyze the strength of AES HT benchmarks in the presence well known side-channel attack countermeasures. Masking, Random delay insertion and tweaking the operating frequency of clock used in sensitive operations are applied on AES benchmarks. Simulation and power profiling studies confirm that side-channel promoting HT benchmarks are resilient against these selected countermeasures and even in the presence of these countermeasures; an adversary can get the sensitive data by triggering the HT.**

Keywords: **Hardware Trojan, Hardware Security, Side-channel attack.**

I. INTRODUCTION

The idea of Internet of Things (IoT) is to connect the digital and physical worlds seamlessly to create a network of objects which communicate with each other. There can be millions of objects in the network with a capability to take intelligent decisions. The complete IoT ecosystem consists of sensor and actuators, microcontrollers with modest processing and connectivity capabilities, network gateways and cloud computing. The known challenges in an IoT ecosystem are: - identification or authentication for addressing an IoT node, choosing a right connectivity technique, maintaining data compliance across network and security. The core tenets to follow in the IoT design are: - agility, scalability, cost and security. Security is of a prime importance because it is a part of challenge and also it is one of the core tenets in the IoT design. The end node in an IoT ecosystem is generally an embedded system in most of the application areas. Security is more important design metric in IoT era [1]. Most of the embedded systems today incorporate cryptographic modules to process the secure data. Different side channel analysis (SCA) methods can be employed to extract the secret key used for encryption in cryptographic modules is well known to security community. SCA are generally performed using power analysis, timing analysis, using design for testability (DFT), electromagnetic analysis and by inducing different types of faults. SCA and designing countermeasures against different types of SCA is a well established research area. The semiconductor design process and manufacturing is fragmented across geographies due to globalization. The fragmented business model in both design and supply chain raise a few serious security issues like counterfeit chips coming out from un-trusted foundries and test centres and Hardware Trojans (HT) [2]. HT is malicious inclusions in the design, which are inserted by an adversary in-house designer or there may be HT in the IP core sourced from 3rd party vendor. The intentions of adversary depend upon the functionality of the circuit. Leaking secret key used in cryptographic cores and denial of service (DoS) in processors can be the intensions of adversary [3]. The research in HT can be classified as: - HT benchmark design, HT detection techniques and run-time defence against HT. HT benchmark circuits are required to validate the strength of HT detection schemes. Trust-hub provides the HT benchmarks for cryptographic cores, processors and communication protocols [4]. There are different types of Advanced Encryption Standard (AES) HT benchmarks available in Trust-hub. The side channel attack promoting HT benchmarks are classified into two categories: - CDMA based side channel attack HT and power analysis based side channel attack HT benchmarks. Further SCA promoting benchmarks are classified as: - leakage current benchmarks and dynamic power benchmarks. The classification of Power SCA AES benchmarks from Trust-hub is shown in Table I. There are total 21 benchmarks available from Trust-hub and more detail description of other AES HT benchmarks can be found in [3] and [4].

Researchers have proposed different SCA methods and countermeasures in last two decades. In this paper, we focus mainly on power analysis based SCA and power based SCA promoting HT benchmarks. Most of the research is focused on development of HT detection schemes [5]. And the amount of research on new HT benchmarks design or analysis of existing HT benchmarks is relatively less in comparison with HT detection schemes. An investigation of side channel attack promoting HT benchmarks (Trust-hub) in the presence of standard SCA countermeasures is an unexplored area. This work mainly focuses verifying the behaviour of AES HT benchmarks in the presence of standard SCA countermeasures. The next section describes the power analysis based SCA and generally used standard countermeasures, section III discuss Hardware Trojans, HT benchmarks and different SCA promoting HT benchmarks from Trust-hub. Section IV discusses analysis of HT benchmarks in the presence of countermeasures and finally section V concludes the paper.

978-1-5090-6762-6/17/$31.00 ©2017 IEEE

TABLE I
DESCRIPTION OF POWER SCA PROMOTING HARDWARE TROJAN BENCHMARKS FROM TRUST-HUB

AES Hardware Trojan Benchmarks	Malicious Activity
Dynamic Power based SCA promoting HT Benchmarks	
AES-T300	This HT introduces leaking states in the key for known input bits and key bits. The HT leaks one byte of the AES round key for every round of the key schedule. The leakage circuit consists of 16-bit shift register, which is loaded with an alternating sequence of zeros and ones. Shift register is enabled only when input to the leakage circuit is one. When shift register is enabled, it results in additional dynamic power consumption. This is an 'always on' Trojan.
AES-T1300, AES-T1400	This HT is similar to AES-T300, but this is not an 'always on' Trojan. Trojan is triggered when a predefined input is observed.
AES-T1500	This HT is similar to AES-T300, but this is not an 'always on' Trojan. Trojan is triggered after 128'hFFFF_FFFF_FFFF_FFFF_FFFF_FFFF_FFFF_FFFF encryptions.
Leakage Current based SCA promoting HT Benchmarks	
AES-T600	The Trojan leaks the secret key of AES-128 through the leakage current, when a specific input is detected on data to be encrypted. Leakage circuit consists of a shift register holding the secret key and two inverters. The LSB is connected to one inverter whose output connected to the input of the other inverter. When the LSB of the shift register is '0', a direct path between power and ground is established through the PMOS of the first inverter and NMOS of the second inverter. The secret key can be retrieved by measuring the leakage current.
AES-T2000	Similar to AES-T600.
AES-T2100	Similar to AES-T600 and Trojan is triggered after pre-defined number of encryptions.

II. PRIOR WORK

A. Power Analysis Attacks on Cryptographic Circuits: - In 1999, Kocher demonstrated the successful extraction of secret key using power analysis based side channel attack [6]. There are different types of power SCA: - differential power analysis (DPA), simple power analysis (SPA) and correlation power analysis (CPA). Side-channel Attack is a process of extracting the secret key through passive and non-invasive methods, typically using statistical analysis on leaked information collected from measurements in real time during processing of secret information [6].

The first step is collection of power traces from the device used in encryption process. The power traces are collected on the power supply line near to the device. The adversary chooses an internal signal related to the target operation. The selected signal should represent the operation that connects known input data and secret key used in encryption. And selected signal should show the correlation with measured traces when the secret key is guessed correctly. This will help adversary to extract the secret key.

The final phase of any SCA scheme is the evaluation of the collected power traces. In the case of DPA, the adversary will use the selection function to partition the power traces based on the expected value of the target signal for every valid secret key guess. The choosing of partition function is very important. The success of DPA attack mainly depends on choosing appropriate partition function. The average power consumption for each partition is calculated. A differential spike can be generated on calculating the difference between the given two selected partitions. The two common power consumption models used are Hamming distance and Hamming weight depending on the type of the attack. A large magnitude spike should be observed for the correct guess of secret key guess. The detailed description of DPA and CPA can be found in [6] and [7].

B. Countermeasures against power analysis attacks: - The countermeasures against power analysis based SCA can be categorized into three types: - Power Analysis Attack (PAA) resistant logic styles, module modification methods and Adding additional modules to mitigate the power based SCA attacks [8].

AES benchmarks from Trust-hub are represented in Verilog HDL. The different countermeasures mentioned above are targeted to ASIC and FPGA implementation of cryptographic circuits. Few countermeasures are purely at circuit level (ex: few PAA resistant logic styles), which can't be applied on RTL benchmarks for investigation. Similarly, all module modification and adding extra modules as countermeasure also can't fit with RTL benchmarks for investigation. In this work, we select the countermeasure schemes that can be used with AES benchmarks for the analysis. The detailed description on selection of countermeasure techniques for analysis is presented in Table II.

TABLE II
SCA COUNTERMEASURES AND THEIR SELECTION FOR AES HT BENCHMARK ANALYSIS

Name of the technique	Description	Applicability to AES HT Benchmarks
PAA Resistant Logic Styles		
DWDDL [9]	Divided Wave Dynamic Differential Logic (DWDDL) is based on sense amplifier based logic (SABL). The standard cells for all logic gates used in digital implementation of cryptographic core are created with a dynamic and differential behavior using De-Morgan's law, by expressing the false output of any logic function using the false input of original logic function and AND-ing the differential output with a pre-charge signal. The construction of gates using this technique exhibit a constant amount of power consumption for every clock cycle, irrespective of inputs. WDDL technique is one of the primitive PAA resistant logic style on which many other similar logic styles are proposed. This technique can be implemented in both FPGA and ASIC.	All three PAA resistant logic styles are discussed here are generic and applicable to any cryptographic algorithm. All AES benchmarks are algorithmic level implementations and it is difficult to build complete secure standard cell library for synthesis of the circuit. The PAA resistant logic styles proposed for FPGA designs are very specific to target device and vendor specific. It is very difficult to validate the AES benchmarks for PAA resistant logic styles.
BCDL [10]	Balanced –Cell based Dual Rail Logic (BCDL) is designed for FPGA implementation of crypto cores, which address both global and local synchronization of signals are taken care to avoid glitches during circuit operation. This work is also extension of WDDL.	
SDDL [11]	Separated Dynamic Differential Logic (SDDL) is an extension to WDDL technique, which does not require cross coupling between true and complementary paths to implement negative logic. The idea of SDDL is to implement true and complimentary network on two different sections of FPGA.	
Masking Techniques		
Generic Boolean Masking Techniques [12]	In [12], the author proposes masking schemes based on Boolean masking techniques, rather than pre-computed table. Boolean masking technique in [12] identifies common operations in crypto algorithms require masking and propose suitable circuits for applying the mask in a secure procedure. Random Boolean masking circuits for an AND operations, to convert between Boolean and arithmetic operations and integer addition and comparison. The mask design approaches discussed in the paper are based on XORs and MUXs. The use of basic elements in designing the mask operations makes this technique applicable to all types of cryptographic implementations.	Both the masking techniques discussed are suitable for this experiment. Boolean masking and Split datapath technique can be implemented at algorithmic level. The AES benchmarks are described in Verilog HDL at algorithmic level. Generic Boolean Masking technique can be implemented without much difficulty. The split datapath technique need implementation changes in AES benchmark circuits which changes the basic characteristic of AES benchmarks. In this experiment only Boolean masking technique is used with AES benchmarks.
Splitting datapath into separate halves [13]	This technique split the datapath as two separate halves which process the masked data and mask. The two input registers will hold the intermediate result and the updated mask separately. The leakage of data can be prevented by implementing the masking as ROM in datapath [13]. The registers storing the mask and intermediate values can become the primary source for SCA [13]. The masking is designed through series of bijections of mask update operation. This will lead to splitting of sensitive data and leakage of split data through SCA will make less or no significance. The adversary cannot reveal with the knowledge of split data.	
Countermeasures through addition of extra modules		
Separate Clock for Sensitive Operations [14]	Using separate isolated clock for sensitive operations which is not derived from external clock is a countermeasure against SCA described in [14]. The internal clock used for sensitive operations should be faster than external clock and it should be dedicated to the module performing sensitive operations and not used for any other module. This limits the options for adversary to it needs a invasive attacks to understand timing information. This technique does not need any changes to encryption module.	This countermeasure fit into the algorithmic implementation of AES benchmarks and can be used in this investigation.
Random Delay Insertion [15]	Another timing obfuscation approach called Random Delay Insertion (RDI) is proposed in [15]. The basic idea of RDI is to randomly introduce the delay operations on secret key to shift the position of information on sensitive data in the collected traces. The randomization of delays is controlled through control signals. But this countermeasure is considered weak and close observation of collected traces, an intelligent adversary can get sensitive information.	This countermeasure fit into the algorithmic implementation of AES benchmarks and can be used in this investigation.
DVFS (Dynamic Voltage and Frequency Scaling) [16]	DVFS technique is originally intended to reduce the dynamic power consumption of the design. This technique can be extended to randomize the current and voltage profiles through varying the system's frequency and operating voltage and to confuse the adversary.	This countermeasure need a large separate feedback circuits to control DVFS and changes the structure of benchmark to some extent.
Decoupling Power supply [17]	The decoupling the power supply from the encryption modules handling sensitive data as a countermeasure against SCA is proposed in [17]. The basic idea of decoupling is disconnect the power source from modules handling secret data rather than performing modifications in the circuit to balance the dynamic power consumption. A variety of decoupling architectures are proposed in [17].	Verilog models of AES benchmarks are available with Trust-hub. It is difficult to analyze the benchmarks with this set of countermeasures.

PAA resistant logic styles: - The significant amount of research literature is found on PAA resistant logic styles. The basic idea is designing a secure logic style which will leak the less amount of side-channel information. The standard cells are designed using secure logic style, which are used as building blocks in the construction of cryptographic circuits. The secure logic style methods result in secure cryptographic

implementations, but there are few demerits in terms of area and power consumption and complexities in physical design. Few logic styles need special care during placement and routing of design to mitigate the leakage of side-channel information.

The few PAA logic styles are not generic and not suitable for semi-custom design. In this paper we discuss more versatile and generic PAA logic styles which are discussed widely in the SCA literature. The WDDL, BCDL and STTL logic styles are discussed in Table II. In this work, it is difficult to validate the AES benchmarks for PAA resistant logic styles. All AES benchmarks are algorithmic level implementations and it is difficult to build complete secure library and standard cells for synthesis of the circuit. The PAA resistant logic styles proposed for FPGA designs are very specific to target device and vendor specific.

Module modification methods: - The cryptographic circuit implementations are modified to prevent leakage of sensitive data through SCA. The module modification schemes can be classified as: - Masking, Isomorphism and data transform techniques. Most of the Isomorphism and data transform techniques proposed are very specific to the cryptographic algorithm and implementation methods. Some of the masking techniques are also tailored for specific algorithms and implementations. Masking techniques proposed in [12] [13] are generic techniques and can fit into any cryptographic algorithm and implementation. The technique proposed in [] is applied on AES benchmarks in this paper to investigate the behavior of Trust-hub benchmarks. The masking is easy to implement countermeasure technique against SCA at algorithmic level [14].

The two important generic masking techniques are discussed in Table II. The principle behind the masking in [13] is to split all the variables in the algorithm randomly into at least two parts to avoid the leakage of sensitive data. With the knowledge of split part, adversary should not be able to derive any information on sensitive data. The efficient masking technique will reveal less information during SCA. Another generic technique proposed is based on Boolean equations is also discussed and investigated on AES benchmarks.

Countermeasures through addition of extra modules: - Another important countermeasure against power based SCA is through incorporating an additional circuitry. The benefit of this method is that, these techniques can be applied without modification of the functional implementation of cryptographic algorithm. The extra area overhead and power consumption due to addition of extra modules is one disadvantage of this category of countermeasures. The resistance against SCA is achieved by adding a module which cause random changes in timing of sensitive operations, randomization of power consumption and disconnect the power supply from the cryptographic modules during sensitive operations. The Table II discusses the widely discussed techniques of this type and their applicability to AES benchmarks.

General Observation on Power based SCA countermeasures: - There is no standard procedure or tests to evaluate the strength and weakness of different types of countermeasures against SCA. It is difficult to compare the different countermeasures and their performances. The PAA resistant logic styles are generally assumed robust against SCA. This technique comes with large design complexity and also difficult to implement the security enhancing constraints in placement, routing etc. Most of the masking techniques are not sufficient against advanced SCA attacks and masking alone may not provide complete security. The control complexity in decoupling circuits is difficult to implement accurately. There will be some amount of leakage power, which may give out the sufficient information on secret key. In this work, we present the analysis of AES benchmarks in the presence of few widely discussed countermeasures like masking and timing obfuscation schemes found appropriate for investigation with Trust-hub AES benchmarks.

III. Implementation of Countermeasures in AES Benchmarks

A. Boolean Masking Technique: - In this technique, a logic circuit composed of basic gates can be masked. The AND and OR gates in the circuit should be masked. In the case of XOR and NOT gates related to affine parts of circuits are kept untouched. The circuit is structured in such a way that output of operation exhibits an even probability distribution for most of the input combinations. The non-linear gates like AND gate are reconstructed using XOR's and MUXs [12]. These techniques applied for the masking of AES (S-box and key scheduling) circuit composed of basic logic gates. The MUX based masking technique is more efficient in terms of area overhead [12] as it requires the less number of gates. The MUX based implementation of secure masked AND gate operation is shown in fig.1. The X' is the result of masking: X' = X XOR r_x and Y' is the result of masking operation Y' = Y XOR r_y. The more detailed implementation of this technique can be found in [12]. MUX based Boolean masking technique is applied on all SCA promoting AES benchmarks listed in Table I.

B. Separate Clock for Sensitive Operations: - The patent [14] proposes the using faster and isolated clock for secret key handling operations to prevent leaking of sensitive data during SCA. In this experiment, the normal operating frequency of all benchmarks is 20MHz. The architecture of benchmarks are modified to operate the round key module (which adds key to input) operates at 50MHz.

C. Random Delay Insertion (RDI) Technique: - The basic principle in this countermeasure is inserting the random delays before and after the sensitive operations. The model circuit diagram is shown in figure 2. The control signals will select the amount delay inserted during operation. The control signals are randomized [15]. The control signals are part of input data for encryption. In this work, modifications to AES benchmarks are performed to insert eight different

TABLE III
DYNAMIC POWER ANALYSIS OF AES BENCHMARKS WITH AND WITHOUT COUNTERMEASURES

HT Benchmarks	Dynamic Power for HT without countermeasures (power in milliwatt) (for 10000 cycles)		Dynamic Power with Countermeasures (power in milliwatt) (for 10000 cycles)					
	HT is not Triggered	HT is Active	Boolean masking Technique [12]		Separate Clock for Sensitive Operations [14]		Random Delay Insertion (RDI) [15]	
			HT is not Triggered	HT is Active	HT is not Triggered	HT is Active	HT is not Triggered	HT is Active
AES-T300	184.5204	198.4543	189.6543	203.9123	204.5201	218.2838	185.3720	201.2912
AES-T1300	184.5068	198.5671	191.4307	202.4136	203.3476	219.4821	184.4921	202.2492
AES-T1400	186.4748	199.5678	190.1237	203.6028	202.2038	217.9248	186.1527	202.1905
AES-T1500	184.5225	198.8765	190.7650	202.8244	203.2848	218.2581	185.2731	202.4211
AES-T600	184.5315	198.6122	191.9876	201.9220	204.1203	218.6291	185.2017	203.2367
AES-T2000	184.5574	198.3245	191.2335	202.5609	203.2988	218.8238	185.2937	203.7129
AES-T2100	184.5159	198.6574	192.8745	202.3496	203.3499	218.2732	185.2901	203.2841

combinations of delays can be inserted. The three bit random control signals are derived from the specific section of input data. Based on the input data, corresponding delay loop will get selected.

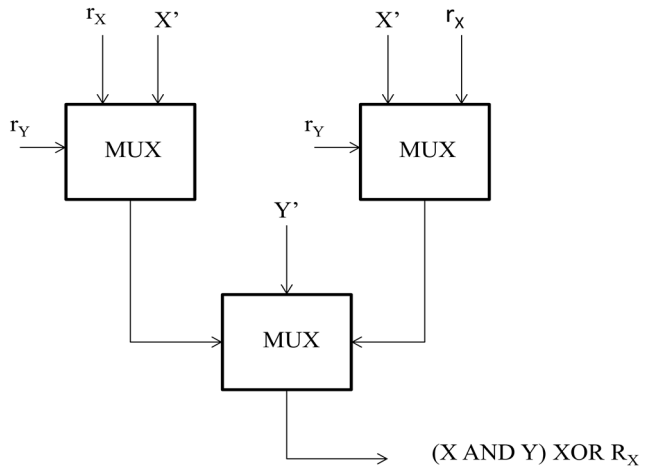

Figure 1 MUX based Boolean Masking Technique

IV. SIMULATION AND ANALYSIS OF AES BENCHMARKS WITH SCA COUNTERMEASURES

Power based side-channel attacks can be observed through dynamic power consumption of circuits. When HT promoting power based side-channel attack (SCA) is triggered, a variation/abnormality in dynamic power consumption should be observed. The dynamic power analysis is performed on HT benchmarks which are suspected for promoting power based SCA in the presence of possible countermeasures. The power analysis flow is shown in figure 3. The Value Change Dump (VCD) file is generated during testbench simulation of synthesized netlist. The VCD file captures the switching activity inside the design during simulation for the given input stimulus in the testbench. When HT is not triggered, for a normal operation dynamic power is recorded. The power values are measured in Synopsys Primetime PX tool [18]. The VCD from simulation and SPEF (standard parasitic extraction format) from layout is fed into Primetime PX along with gate-level netlist. The triggering of HT does not affect the encryption process of AES. During encryption, when active HT increases the dynamic power consumption to support power based SCA. The synthesis, place and route are performed using TSMC 65nm standard cell library. The amount of simulation time used to generate VCD file which capture switching activity is equal for the both HT triggered and HT un-triggered. The power analysis and dynamic power consumption is recorded for below possible combinations: -

- AES benchmarks without countermeasures without triggering the HT.
- AES benchmarks without countermeasures with triggering the HT.
- AES benchmarks with countermeasures without triggering the HT.
- AES benchmarks with countermeasures with triggering the HT.

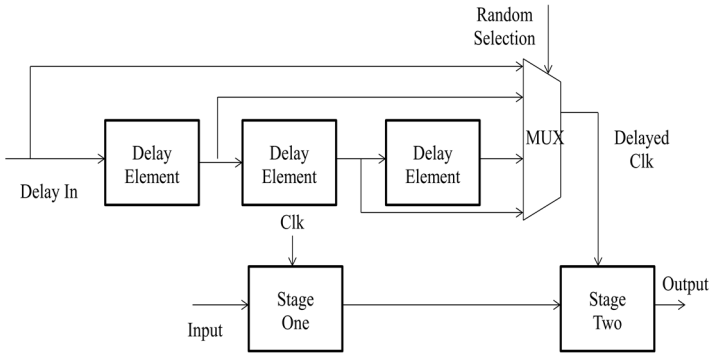

Figure 2 Random Delay Insertion Circuit

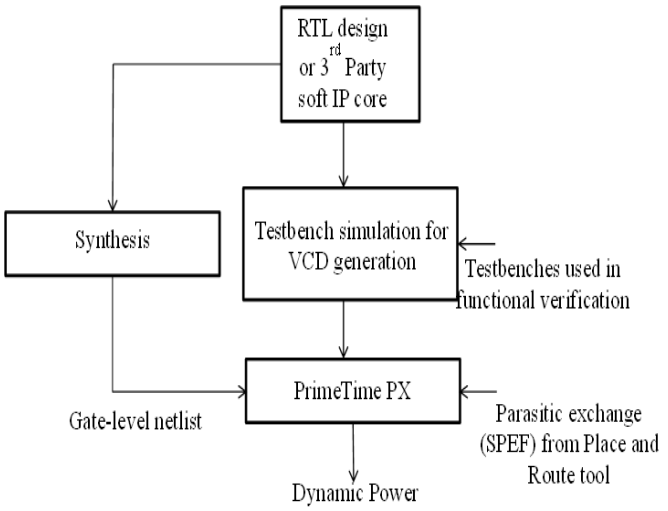

Figure 3 Dynamic Power Analysis flow

The dynamic power values presented for above combinations are presented in Table III.

Analysis of AES Benchmarks with countermeasures: - The Table III shows the dynamic power values for with and without countermeasures. Dynamic power consumption is higher when SCA countermeasures are implemented in AES benchmarks. The simulation environment consists of two types of stimulus, which carry out the simulation with and without triggering the Hardware Trojan. The MUX based Boolean masking technique is implemented into AES benchmarks, which increases the switching activity inside the circuit for the same stimulus applied. Similarly, higher dynamic power consumption values are recorded for RDI and using separate clock for sensitive operations. It is relatively easy for an adversary, in the presence of hardware Trojan. Adversary can get a secret key with less number of collected traces, which are accurate. The power consumption profile in the presence of countermeasures in AES benchmarks makes no much difference. Only simulation studies and profiling of power consumption is performed in this experiment. The better countermeasures like decoupling, advanced DVFS techniques and PAA resistant logic styles need to be tested with AES benchmarks to determine the strength and weakness of Benchmarks. The Trust-hub power based SCA promoting AES benchmarks are resilient against countermeasures like masking, delay insertion and higher operating speed for sensitive operations.

V. Conclusions

In this paper, we present the analysis of Trust-hub power based SCA promoting AES benchmarks in the presence of selected SCA countermeasures techniques. Simulation and power profiling studies are conducted on each side-channel promoting benchmark in the presence of countermeasures like masking, insertion of delay elements and tweaking operating frequency. In the presence of SCA countermeasures selected for analysis, AES benchmarks are resilient and adversary can still get good amount of secret information by triggering the hardware Trojan. The SCA countermeasure considered for analysis in this paper are relatively simple techniques. The AES benchmarks should be analyzed against much strong countermeasures like DVFS, decoupling and advanced masking techniques in future.

References

[1] Cognizant White Paper, “The Internet of Things: Impact and Applications in the High Tech Industry”, http:// www.cognizant.com/.

[2] M. Rostami, F.Koushanfar, J.Rajendran, R.Karri, “Hardware security: threat models and metrics”, International Conf. on CAD (ICCAD)-2013.

[3] M.Tehranipoor, Farinaz Koushanfar, A survey of Hardware Trojan Taxonomy and Detection, IEEE Design and Test of Computers-2010.

[4] https://www.trust-hub.org/benchmarks.php.

[5] K.Xiao et al, “Hardware Trojans: Lessons after one decade of research”, ACM Transactions on Design Automation of Electronic Systems (TODAES), Volume 22, Issue 1, December-2016.

[6] P.Kocher, J.Jaffe, B.Jun, “Differential Power Analysis”, 19th Annual International Cryptology, CRYPTO’99, pages 3880-397, Aug-1999.

[7] Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks, Revealing the Secrets of Smart Cards. Springer, New York (2007).

[8] Mayhew, Muresan, “An overview of hardware-level statistical power analysis attack countermeasures”, Journal of Cryptographic Engineering, Springer-2016.

[9] Baddam, K., Zwolinski, M.: “Divided backend duplication methodology for balanced dual rail routing”. In: Proceedings of the CHES-2008. LNCS, vol. 5154, pp. 396–410 (2008).

[10] Nassar, M., Bhasin, S., Danger, J.-L., Duc, G., Guilley, S.: BCDL: a high speed balanced DPL for FPGA with global precharge and no early evaluation. In: Proceedings of the DATE 2010, pp. 1–6 (2010).

[11] Velegalati, R., Kaps, J.-P.: Improving security of SDDL designs through interleaved placement on xilinx FPGAs. In: Proceedings of the FPL 2011, pp. 506–511 (2011).

[12] Golic, J.D.: Techniques for random masking in hardware. IEEE Trans. Circuits Syst. Regul. Pap **54**(2), 291–300 (2007).

[13] Maghrebi, H., Guilley, S., Danger, J.-L.: Leakage squeezing countermeasure against high-order attacks. In: WISTP 2011. LNCS, vol. 6633, pp. 208–223 (2011).

[14] Pedersen, B.B.: Programmable Logic Device with Improved Security. US Patent 8,255,702 (2012).

[15] Lu,Y., O’Neill,M., McCanny, J.:Evaluation of random delay insertion againstDPAon FPGAS.ACMTrans. Reconfigurable Technol. Syst **4**(1), 11:1–11:20 (2010).

[16] Baddam, K., Zwolinski, M.: Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure. In: Proceedings of the IEEE International Conference on VLSI Design 2007, pp. 854–859 (2007).

[17] Baddam, K., Zwolinski, M.: Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure. In: Proceedings of the IEEE International Conference on VLSI Design 2007, pp. 854–859 (2007).

[18] Synopsys PrimeTime manual, version 2016.1, www.synopsys.com.