Circuit-Variant Moving Target Defense for Side-Channel Attacks

Tristen Mullins, Brandon Baggett, Todd R. Andel and J. Todd McDonald
University of South Alabama, Mobile, USA
tah1323@jagmail.southalabama.edu
brb1323@jagmail.southalabama.edu
tandel@southalabama.edu
jtmcdonald@southalabama.edu

Abstract: The security of cryptosystems involves preventing an attacker's ability to obtain information about plaintext. Traditionally, this has been done by prioritizing secrecy of the key through complex key selection and secure key exchange. With the emergence of side-channel analysis (SCA) attacks, bits of a secret key may be derived by correlating key values with physical properties of cryptographic process execution. Information such as power consumption and electromagnetic (EM) radiation side-channel properties can be observed during encryption or decryption. These signals reflect data-dependent system behaviours that may reveal secret key information. Power and EM SCA attacks require several measurements of the target process to amplify the signal of interest, filter out noise, and derive the secret key through statistical analysis methods. Differential power and EM analysis attacks rely on correlating actual side-channel measurements to hypothetical models. The goal of this research is to increase the complexity of both power and EM SCA by introducing structural and spatial randomization of the target hardware. We propose a System-on-a-Chip (SOC) countermeasure that will periodically reconfigure an AES scheme using randomly located S-box circuit variants. We hypothesize that changing the location of the target modules between encryption runs will result in a nonconstant EM signal strength for any given point on the chip, increasing the number of traces needed to perform a localized EM SCA attack. Further, each of the S-box circuit variants will consist of functionally equivalent, structurally diverse hardware. By diversifying the implementations at the gate-level, we aim to vary the power behaviour observed by the attacker and disrupt the correlation between the hypothetical and actual power consumption, increasing the complexity of power SCA. This moving target defense aims to disrupt side-channel collection and correlation needed to successfully implement an attack.

Keywords: Side-Channel Analysis, Electromagnetic Analysis, Power Analysis, Countermeasure, Reconfigurable Hardware

1. Introduction

Several factors are considered when deciding on which platform to implement a cryptographic algorithm. There are many trade-offs between software and hardware implementations including cost, speed, and flexibility. While software implementations are often more flexible, easier to update, and have low development costs, they can have greater overhead costs and weaker security than their hardware counterparts. Reconfigurable hardware devices (e.g., field-programmable gate arrays, or FPGAs) feature characteristics that allow them comparable flexibility to software implementations while incorporating the benefits of hardware realization. Wollinger and Paar (2003) list some potential advantages reconfigurable hardware provides for cryptography including algorithm agility, algorithm upload, architecture efficiency, resource efficiency, algorithm modification, throughput, and cost efficiency. Not only do these improve algorithm performance, but they also ensure that the platform resources are used efficiently, and updates are easily made through reconfiguration. However, these advantages can only be exploited if security shortcomings are addressed.

The security of cryptosystems involves preventing an attacker's ability to obtain information about plaintext. Traditionally, this has been done by prioritizing secrecy of the key through complex key selection and secure key exchange (Meadows, 2003). With the emergence of side-channel analysis (SCA) attacks, bits of a secret key may be derived by correlating key values with physical properties of cryptographic process execution. Information such as timing (Kocher, 1995), power (Kocher *et al.*, 1999a), and electromagnetic (EM) radiation (Quisquater and Samyde, 2001) side-channel properties can all be observed during run-time of a cryptoprocess. These signals reflect data-dependent system behaviours that may be analysed by an attacker to derive secret key values.

The ability to obtain information about the system is dependent on the accessibility of a “usable” side-channel and does not “reflect inherent weaknesses” of the process being examined (Kelsey *et al.*, 1998). Therefore, countermeasures for SCA attacks should focus on reducing trace usability by minimizing behaviour-key correlation and information leakage within the signal.

Side-channel countermeasures are designed to increase the complexity of SCA attacks. This is often done through hiding and masking techniques such as random delay insertion, shuffling, masking, dual-rail logic, etc.

Increasing attack complexity does not necessarily mean that an attack is impossible, just more costly. Because there is currently no solution that eliminates all side-channel leakage, we must "accept that cryptographic implementations leak a certain amount of information," and avoid allowing the leakages to completely compromise security during use (Standaert *et al.*, 2010).

Many researchers suggest implementing countermeasures in combination to compensate for the shortcomings of individual designs and improve overall security (Güneysu and Moradi, 2011; Moradi, Mischke and Paar, 2011). This method of layering side-channel resistance may also be useful in scenarios where an attacker could perform multiple types of SCA on a target. With physical access to a device, both power and electromagnetic analysis (EMA) attacks may be conducted with simple equipment. Though many power countermeasures are assumed to protect against EMA, it has been shown that power countermeasures may still be vulnerable to localized EMA attacks (Agrawal *et al.*, 2002; Immler, Specht and Unterstein, 2017; Specht *et al.*, 2018). This creates a need for both power and EMA attack prevention methods on a device.

This research focuses on increasing the complexity of both power and localized EM SCA by introducing structural and spatial randomization of the target hardware. The proposed design utilizes the device's dynamic reconfiguration capabilities to enable a varying attack surface for a parallelized version of AES-128. Our countermeasure intends to reduce the usable trace set for an attack by incorporating circuit variants of the encryption hardware and limit EM hotspots by randomizing the hardware location.

The remainder of this paper is organized as follows. In Section 2, we outline the side-channel attacks our countermeasure is designed to prevent including differential power analysis, localized EM analysis, and exploitable leakage present in AES. Our proposed countermeasure is described in Section 3 and related works are presented in Section 4. The paper concludes in Section 5.

2. Side-Channel Analysis

2.1 Power Side-Channel Analysis

Kocher et al. (1998) first demonstrated how power consumption measurements could be correlated to secret key values. These power analysis attacks are based the behaviour of semiconductor logic. When charge is applied to or removed from transistors, a current is induced that consumes power and emits EM radiation. This switching activity may vary depending on which operations are being executed and even the data values being processed. These trends in power consumption may be measured by an attacker and used to determine runtime information that may otherwise be assumed to be private. If the device under observation is executing cryptographic processes, the data-dependent power usage may expose the secret key.

Differential power analysis (DPA) attacks use algorithm-specific statistical methods to identify data-dependent correlations in power traces. This type of attack requires little knowledge about the target device, requiring only the target cryptographic algorithm to be known. The strength of DPA attacks depends on the power model the attacker chooses. Hamming-distance and Hamming-weight models are the most common power models used in DPA attacks due to their ease of application (Mangard *et al.*, 2007). Customized power models increase the effectiveness of the attack but are up to the attacker to derive using their knowledge of the device.

DPA attacks all follow a general 5-step procedure (Mangard *et al.*, 2007). In step 1, an intermediate value is selected on which the attack will be based. This value must be a function of the plaintext and the key. Step 2 consists of measuring actual power traces from the target device. In step 3, a set of hypothetical intermediate values are calculated using a set of key hypotheses for the target cryptographic algorithm. The values from step 3 are then mapped to their hypothetical power consumption using the power model the attacker has selected as step 4. The hypothetical power consumption is then compared to the actual power consumption in step 5. The attacker assumes there is 1 hypothetical power consumption "trace" that corresponds to the correct key and 1 time period in the actual trace set where the selected intermediate value was processed. High correlation between hypothetical and actual power consumption values are indicative of a correct key hypothesis.

For DPA to be mounted efficiently, the captured power traces must be aligned in time (Mangard *et al.*, 2007). This ensures that each cryptographic operation corresponds to the same location throughout the trace set which is necessary for comparing the hypothetical power consumption to the actual trace set. Several countermeasures have been shown to be effective against DPA by misaligning traces including operation

shuffling, insertion of dummy rounds, and random delay insertion (Clavier, Coron and Dabbous, 2000; Korak, Plos and Hutter, 2012; Bogdanov *et al.*, 2019). These types of countermeasures increase the cost of performing an attack by reducing the number of usable traces that can be collected in a given amount of time.

2.2 Electromagnetic Side-Channel Analysis

While data-dependent current flow serves as the basis for power analysis attacks, it also emits electromagnetic fields that can contain key-revealing information. Differential Electromagnetic Analysis (DEMA) attacks follow similar statistical analysis methods to DPA using signals collected from EM field probes (Kocher et al., 2011, 1999b; Quisquater & Samyde, 2001). Using EM rather than current-based power measurements for attacks does have its advantages. EM measurements offer a desirable alternative to power consumption when access to the power and ground lines are limited, when the power signal contains too much noise, or when power analysis countermeasures are implemented (DeBeer et al., 2011; Gandolfi et al., 2001; Quisquater & Samyde, 2001).

When using a high-resolution EM probe, attackers may perform localized attacks using traces collected from a specific area on the chip (Gandolfi, Mourtel and Olivier, 2001). Localized EM attacks are particularly powerful in that they allow leakage from individual subcircuits to be isolated (Li, Iyer and Orshansky, 2019a). This may be leveraged by attackers to weaken countermeasures that are effective against DPA. Specht et al. (2018) use localized EMA to isolate the leakage from separate shares in a threshold implementation countermeasure. Their attack combines leakage from multiple probes to break the scheme. Localized EM attacks have also been used to break dual-rail logic countermeasures by leveraging placement and routing imbalances (Immler, Specht and Unterstein, 2017).

These types of attacks are most successful when the probe is placed above the area of the chip where the side-channel leakage of interest is strongest (Heyszl *et al.*, 2012). To determine the optimal probe position, measurements are taken across the surface of the chip during the execution of the target process. If the chip hosts a variety of processes with distinct clock frequencies, the EM signal should be filtered to reduce components that are not related to the target operations. The location with the greatest signal strength for the target process or the highest correlation to the hypothetical model indicates the optimal probe position. These points of interest may be visualized as “hotspots” using a spectralintensity plot or a correlation heat map. Once a target hotspot is selected, the probe is then placed, and an attack trace set is collected. Like the traces used for DPA, traces used for DEMA also need to be aligned during pre-processing.

2.3 Side-Channel Leakage in AES

The Advanced Encryption Standard (AES) is the current standard for encrypting electronic data (Standard, 2001). This symmetric block cipher is a form of the Rijndael cipher (Daemen and Rijmen, 1998) that processes 128-bit blocks with variable key length.

Figure 1 shows a block diagram for AES encryption. After the initial round key addition, a round function is implemented either 10, 12, or 14 times depending on the key length. Each round, excluding the final, consists of four transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. For a parallelized version of AES, 16 copies of the S-box are used so that all 16 bytes of a data block may be substituted at once.

The SubBytes transformation is a non-linear byte substitution that operates on each byte independently using a substitution table, or S-box. S-boxes are of particular interest to attackers due to their output being a function of the plaintext and the key in the first round of AES (Mangard *et al.*, 2007). Therefore, this value is often the intermediate value on which DPA and DEMA attacks on AES are based. While simple countermeasures may be used to mask the leakage of other intermediate values for the algorithm, the non-linearity of the SubBytes transformation makes it difficult to mask (Oswald *et al.*, 2005). Masked S-box implementations may still leak information via glitches when realized in hardware, requiring the inclusion of additional countermeasures (Mangard and Schramm, 2006). Localized EM attacks are also a significant threat to AES implementations since they allow leakage from a particular S-box to be isolated (Unterstein *et al.*, 2017).

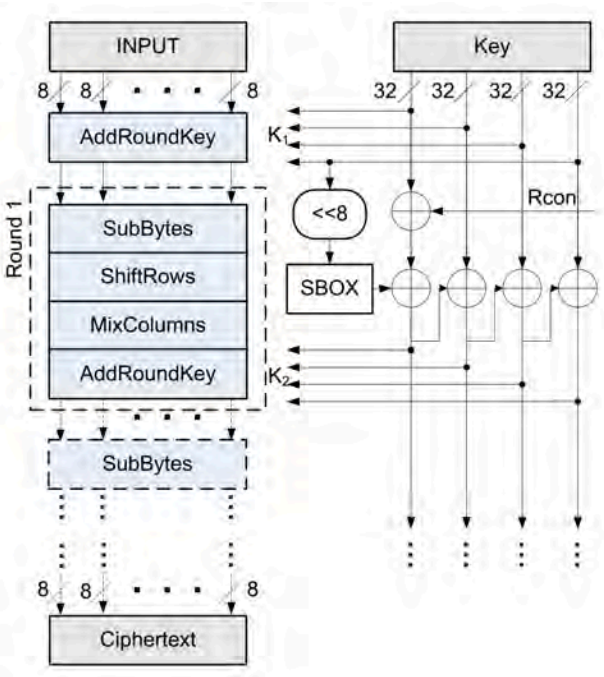

Figure 1: AES Encryption Block Diagram (Ambrose, Parameswaran and Ignjatovic, 2008)

3. Proposed Design

3.1 Equipment and Resources

This research will use a Digilent ZedBoard evaluation and development platform, which features a Zynq-7000 SoC (Xilinx, 2019). To design and program the system, we will use Xilinx Vivado Design Suite. With this software, we can synthesize designs from behavioural descriptions (e.g., VHDL code), add and configure specialized IP cores, specify placement and route (P&R) details, simulate execution, and generate then export bitstreams to the device. A Java software package called the Program Encryption Toolkit (PET) (Forbes, 2017) will be used to generate circuit variants of AES S-box structures that will be used to modify the design in Vivado.

To collect power and EM traces for our analysis we will use a Riscure Side-Channel analysis Suite including an EM Probe station, PicoScope 3000 Series oscilloscope, and Inspector software. The probe station consists of a high-resolution EM probe and a motorized XYZ table which are integrated with the Inspector software for configuration and measurement. The station can be setup to automatically scan the surface of the chip with a step size as small as 2.5 µm. The Inspector software will be used to configure the equipment for trace collection, send plaintext to the target device, receive ciphertext output, store traces, perform pre-processing on traces (e.g., filtering and resampling), and statistically analyse the samples during the attack.

For this research, we will implement a parallelized hardware version of AES-128. This will limit the algorithm to ten encryption rounds for a 128-bit block of plaintext which will be randomly generated by the Inspector software during analysis.

3.2 System Overview

The goal of this research is to increase the complexity of both power and localized EM SCA by introducing structural and spatial randomization of the target hardware. We propose a countermeasure that will periodically reconfigure an AES scheme using randomly located circuit variants of the S-boxes. The focus of this moving target defense (MTD) approach is limiting the presence of EM “hotspots” that indicate favourable candidates for high-resolution probe placement. Changing the location of the target components between encryption runs will result in a nonconstant signal strength for any given point on the chip, increasing the number of traces needed to perform a localized EMA attack. To implement this feature, an additional IP core will be configured that will serve as a Partial Reconfiguration Controller (PRC). Upon the occurrence of a trigger event, the PRC will fetch a partial bitstream from memory that will be used to reconfigure the FPGA. An interval on which reconfiguration should occur will need to be determined as well as what portions of the programmable logic (PL) will be reserved for reconfigurable area.

Power analysis resistance will be introduced to the design through the partial bitstreams used for reconfiguration. Each of the S-box bitstreams stored in memory will consist of functionally equivalent, structurally varied implementations. By diversifying the implementations at the gate-level, we aim to vary the power behaviour observed by the attacker and disrupt the correlation between the hypothetical and actual power consumption.

A Program Encryption Toolkit (PET) will be used to generate circuit variants for each S-box. This is a customized Java application that was used in the research presented by Forbes et al. (2017). It includes a feature to generate random equivalent circuits based on a ISCAS format netlist. After selecting an original circuit, the user specifies the number of gates, gate types, and maximum fan in for the variant. For the merged signature method, a circuit is generated for each output of the original and then merged to form a single circuit. The resulting circuits may be exported in several formats including BENCH netlist and VHDL. A tool is also included to compare BENCH netlists to verify that they are semantically equivalent. Figure 2 provides an example of the variants generated by PET using merged signature circuit generation.

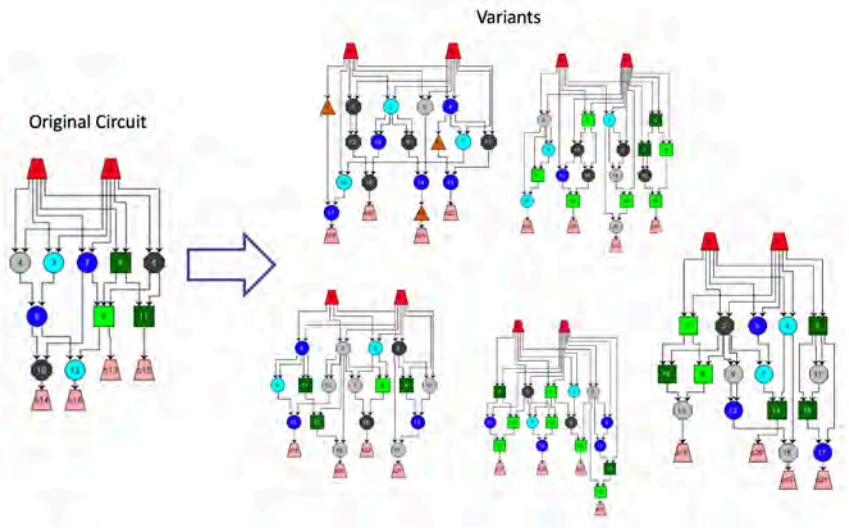

Figure 2: Merged Signature Circuit Generation. 5 Gates with a Max Fan In of 2

A practical countermeasure evaluation will be conducted to determine the implementation's resistance to power and localize EM analysis. DPA and DEMA attacks will be performed on a static, unprotected target as a control. The number of traces to break this AES version will indicate the worst-case resistance to each attack. The DPA and DEMA resistance of the countermeasure will be assessed by comparing the number of traces to key disclosure (NTD) for each attack to that of the unprotected version. During the acquisition step of the DEMA attacks, the optimal probe placement will be determined as well as any leakage hotspots identified. These characteristics will be used to investigate the level of hotspot obfuscation provided by the countermeasure.

Figure 3 shows a block diagram for the proposed design. The Zynq System on a Chip (SOC) features a processing system (PS) and FPGA programmable logic (PL). Though the AES implementation is hardware based, the input and output are handled by the PS side of the SOC. Interfacing applications will be hosted on the PS side that will be used to communicate to the device with the Inspector software (i.e., send and receive data blocks). During each execution of the algorithm, a 128-bit block of random data will be sent from the Inspector software to be encrypted by the AES scheme.

The entire AES core will be designed using a behavioural VHDL description and the Xilinx Vivado software. Excluding the S-boxes, the AES core will be placed in a designated area in the PL. This area is near the reconfiguration region to avoid having to make connections over long distances which can be more prone to leakage. The static AES modules will include a signal that will be used to indicate to the oscilloscope when to start and stop trace collection during analysis. This trigger will correspond to the receiving of plaintext and sending of ciphertext to the PS side of the SOC.

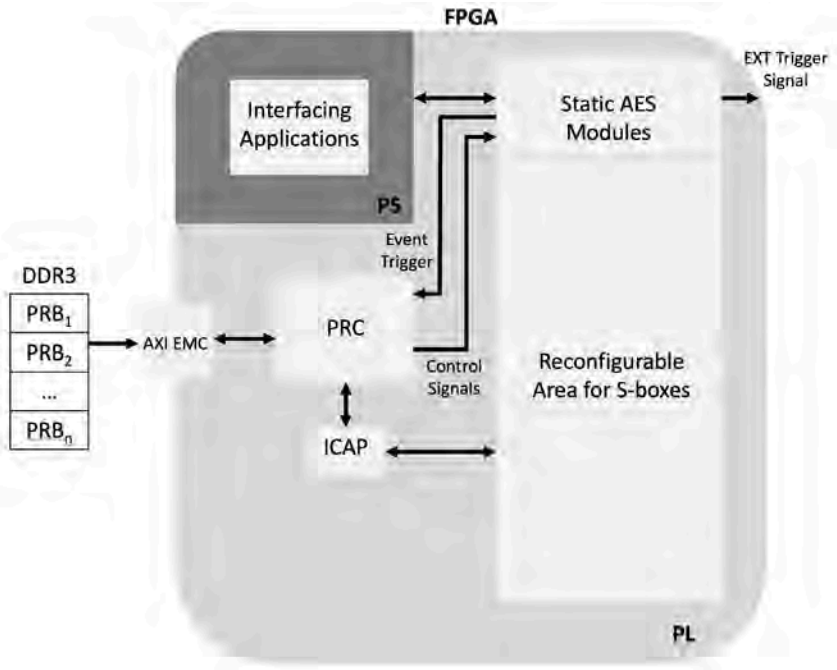

Figure 3: System Block Diagram

The target device supports the inclusion of a Partial Reconfiguration Controller (PRC) IP core (Xilinx, 2018). Upon the occurrence of a trigger event, the PRC fetches a partial bitstream from memory for reconfiguration. In this design, the PRC will be triggered after a certain number of encryptions have been performed. This number will be based on the minimum number of traces needed to break a single configuration. The PRC delivers the PRB to an internal configuration access port (ICAP) which performs the partial reconfiguration. Any control signals needed to disable existing reconfigurable modules or protect static modules are handled by the PRC. Due to the limited size of available BRAM on the FPGA, it is likely that PRBs will need to be stored in external flash memory, DDR3. The PRC can access the PRBs using and AXI External Memory Controller (AXI_EMC).

4. Related Works

Diversity for obfuscation was first presented by Cohen to protect operating systems (1993). In their work, several methods for increasing attack complexity via program evolution are discussed. This concept of implementation diversity has since grown to include schemes for hardware security.

In their work, Li et al. (2019) propose a spatial randomization technique to minimize leakage that may be exploited through localized EM attacks. In this MTD countermeasure, a permutation network is used to randomly assign data bytes to 16 AES S-boxes and a second permutation network restores the order of the bytes. Unlike the design we have proposed which uses dynamic partial reconfiguration (DPR) to randomize the target location, the countermeasure presented by Li et al. utilizes dynamic logic reconfiguration (DLR) which selects among components that remain static in the logic of the FPGA.

Hettwer et al. (2019) demonstrate that randomized hardware location may be used to minimize observable EM leakage hotspots. In their work, the entire AES core is replaced between encryption runs and placed in a different location in the FPGA fabric. The authors also introduce implementation diversity by setting minimum and maximum path delay restrictions to randomize the dynamic power consumption. Their results showed an increase in localized EMA and fault injection resistance; however, resistance to power analysis was only increased by a factor of 3. Additional countermeasures would be needed to further increase resistance to power analysis attacks.

In their work, Bow et al. (2020) present Side-Channel Power Resistance for Encryption Algorithms Using Implementation Diversity (SPREAD). This paper is a power countermeasure proof-of-concept that shows that input-to-output delays are distinct for each circuit structure used. The authors use two methods for varying S-box behavior: synthesis and circuit-directed variation. The synthesis-directed method creates diversity by excluding specific gate types from netlists and the circuit-directed introduces random delays on paths.

This research differs from related works in both the circuit variant generation specifications and the increased resistance to localized EM attacks. By limiting the design to only reconfigure S-boxes, we expect to reduce the storage overhead of the scheme proposed by Hettwer et al. (2019). The criteria for generating variants in our proposal focuses on gate-level diversity as well as P&R constraints which is expected to further increase resistance to power attacks. The bitstreams that will be used in this research include the P&R configurations for the netlist where the SPREAD (2020) scheme utilizes a custom synthesis tool flow to create relocatable bitstreams. Though this may result in less storage overhead for SPREAD, it is likely that our reconfiguration controller will be simpler, leaving more FPGA area to dedicate to the S-box reconfigurations. This research will also only utilize a synthesis-directed circuit variant generation method as opposed to SPREAD which also includes additional hardware for a circuit-directed approach. To introduce gate-level diversity, we will use a program encryption toolkit (Forbes, 2017) to generate equivalent circuits that vary in size and composition where the method in (Bow *et al.*, 2020) exclude specific gate types when generating netlists for each version. Lastly, the proposed countermeasure will be not only be assessed for power analysis resistance but for localized EM analysis resistance as well.

5. Conclusion

Related work has shown that individually, spatial randomization and circuit variance may be used to obfuscate optimal EM probe positions and increase resistance to power analysis attacks, respectively. However, countermeasures that have attempted to combine these concepts have yet to display resistance to both power analysis and localized EMA attacks in an efficient manner. A spatially randomized implementation may hinder an attacker using a high-resolution EM probe, but if the power consumption behaviour does not vary between implementations, an attacker may still perform a side-channel attack that is not location-dependent (i.e., a power analysis attack). This scenario is unfavourable since the equipment to perform a power analysis attack is simpler and more affordable than that of a localized EM attack (Mangard *et al.*, 2007; Heyszl *et al.*, 2012). Therefore, it is in the researcher's best interest to ensure that defenses against localized EM attacks are also resistant to power attacks.

This research proposes a countermeasure design to resist DPA and DEMA attacks by structurally and spatially randomizing a design. It is hypothesized that reconfiguring an AES implementation with S-box circuit variants will result in a randomized power profile that will disrupt the correlation between actual and hypothetical power consumption, hindering DPA attacks. It is also hypothesized that shuffling the location of S-boxes will obfuscate candidates for optimal probe placement, increasing resistance to localized DEMA attacks.

Reconfiguring the S-box area between encryption runs is expected to increase the execution time of our implementation. Further, the inclusion of control logic for reconfiguration is expected to increase the area of the design. This cost as well as the need for external storage for bitstreams may limit the applicability of our countermeasure to other devices that do not have such resources available. Future work will focus on improving these timing costs as well as determining the minimum number of bitstreams needed for power analysis resistance to reduce storage overhead costs.

References

Aerts, W. *et al.* (2006) 'Matching shielded loops for cryptographic analysis', in *1st European Conference on Antennas and Propagation-EuCAP 2006*, pp. 1–6.

Agrawal, D. *et al.* (2002) 'The EM side—channel (s)', in *International workshop on cryptographic hardware and embedded systems*, pp. 29–45.

Ambrose, J. A., Parameswaran, S. and Ignjatovic, A. (2008) 'MUTE-AES: A multiprocessor architecture to prevent power analysis based side channel attack of the AES algorithm', in *2008 IEEE/ACM International Conference on Computer-Aided Design*, pp. 678–684.

Bogdanov, A. *et al.* (2019) 'Higher-order DCA against standard side-channel countermeasures', in *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pp. 118–141.

Bow, I. *et al.* (2020) 'Side-Channel Power Resistance for Encryption Algorithms Using Implementation Diversity', *Cryptography*, 4(2), p. 13.

Clavier, C., Coron, J.-S. and Dabbous, N. (2000) 'Differential power analysis in the presence of hardware countermeasures', in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 252–263.

Cohen, F. B. (1993) 'Operating system protection through program evolution', *Computers and Security*, 12(6), pp. 565–584. doi: 10.1016/0167-4048(93)90054-9.

Daemen, J. and Rijmen, V. (1998) 'The block cipher Rijndael', in *International Conference on Smart Card Research and Advanced Applications*, pp. 277–284.

DeBeer, F. *et al.* (2011) 'Practical electromagnetic analysis', in *Proc. Non-Invasive Attack Testing Workshop NIAT*.
Forbes, M. A. (2017) *Digital Logic Protection Using Functional Polymorphism and Topology Hiding*. University of South Alabama.
Gandolfi, K., Mourtel, C. and Olivier, F. (2001) 'Electromagnetic analysis: Concrete results', in *International workshop on cryptographic hardware and embedded systems*, pp. 251–261.
Güneysu, T. and Moradi, A. (2011) 'Generic Side-Channel Countermeasures for Reconfigurable Devices', *CHES 2011*, pp. 33–48.
Hettwer, B. *et al.* (2019) 'Securing cryptographic circuits by exploiting implementation diversity and partial reconfiguration on FPGAs', in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 260–263.
Heyszl, J. *et al.* (2012) 'Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis', in *International Conference on Smart Card Research and Advanced Applications*, pp. 248–262.
Immler, V., Specht, R. and Unterstein, F. (2017) 'Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs', in *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 403–424.
Kelsey, J. *et al.* (1998) 'Side channel cryptanalysis of product ciphers', in *European Symposium on Research in Computer Security*, pp. 97–110.
Kocher, P. *et al.* (1998) 'Introduction to differential power analysis and related attacks', 4(1), pp. 64–75.
Kocher, P. *et al.* (1999a) 'Differential power analysis', in *Annual International Cryptology Conference*, pp. 388–397. doi: 10.1007/978-1-4419-5906-5_196.
Kocher, P. *et al.* (1999b) 'Differential power analysis', in *Annual International Cryptology Conference*, pp. 388–397. doi: 10.1007/978-1-4419-5906-5_196.
Kocher, P. *et al.* (2011) 'Introduction to differential power analysis', *Journal of Cryptographic Engineering*, 1(1), pp. 5–27. doi: 10.1007/s13389-011-0006-y.
Kocher, P. C. (1995) 'Cryptanalysis of Diffie-Hellman, RSA, DSS, and other systems using timing attacks', in *Extended abstract*.
Korak, T., Plos, T. and Hutter, M. (2012) 'Attacking an AES-enabled NFC tag: Implications from design to a real-world scenario', in *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pp. 17–32.
Li, G., Iyer, V. and Orshansky, M. (2019a) 'Securing AES against Localized em Attacks through Spatial Randomization of Dataflow', *HOST 2019*, pp. 191–197. doi: 10.1109/HST.2019.8741026.
Li, G., Iyer, V. and Orshansky, M. (2019b) 'Securing AES against Localized em Attacks through Spatial Randomization of Dataflow', *HOST 2019*, pp. 191–197. doi: 10.1109/HST.2019.8741026.
Mangard, S. *et al.* (2007) *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*, *Power Analysis Attacks*. Available at: http://gen.lib.rus.ec/book/index.php?md5=16648344AC0BC386A97D0ADACC9F9F78.
Mangard, S. and Schramm, K. (2006) 'Pinpointing the side-channel leakage of masked AES hardware implementations', *CHES 2006*, 4249 LNCS, pp. 76–90. doi: 10.1007/11894063_7.
Meadows, C. (2003) 'What makes a cryptographic protocol secure? the evolution of requirements specification in formal cryptographic protocol analysis', in *European Symposium on Programming*, pp. 10–21.
Moradi, A., Mischke, O. and Paar, C. (2011) 'Practical evaluation of DPA countermeasures on reconfigurable hardware', *HOST 2011*, pp. 154–160. doi: 10.1109/HST.2011.5955014.
Oswald, E. *et al.* (2005) 'A side-channel analysis resistant description of the AES S-box', in *International workshop on fast software encryption*, pp. 413–423.
Quisquater, J.-J. J. and Samyde, D. (2001) 'Electromagnetic analysis (Ema): Measures and countermeasures for smart cards', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2140, pp. 200–210. doi: 10.1007/3-540-45418-7_17.
Quisquater, J.-J. and Samyde, D. (2001) 'Electromagnetic analysis (ema): Measures and counter-measures for smart cards', in *International Conference on Research in Smart Cards*, pp. 200–210.
Specht, R. *et al.* (2018) 'Dividing the threshold: Multi-probe localized em analysis on threshold implementations', in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 33–40.
Standaert, F.-X. *et al.* (2010) 'Leakage resilient cryptography in practice', in *Towards Hardware-Intrinsic Security*. Springer, pp. 99–134.
Standard, N.-F. (2001) 'Announcing the advanced encryption standard (AES)', *Federal Information Processing Standards Publication*, 197(1–51), p. 3.
Unterstein, F. *et al.* (2017) 'Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks A Practical Security Evaluation on FPGA', *COSADE 2017*, 2, pp. 120–137. doi: 10.1007/978-3-319-64647-3.
Wollinger, T. and Paar, C. (2003) 'How secure are FPGAs in cryptographic applications?', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2778, pp. 91–100. doi: 10.1007/978-3-540-45234-8_10.
Xilinx (2018) 'Partial Reconfiguration Controller', *Xilinx*. Available at: https://www.xilinx.com/support/documentation/ip_documentation/prc/v1_3/pg193-partial-reconfiguration-controller.pdf.
Xilinx (2019) 'Zynq-7000 SoC product selection guide', *Xilinx*. Available at: https://www.xilinx.com/support/documentation/selection-guides/zynq-7000-product-selection-guide.pdf.