Security Vulnerabilities of Smart Meters in Smart Grid

Yutian Gui
University of North Carolina at Charlotte
Charlotte, USA
ygui@uncc.edu

Ali Shuja Siddiqui
University of North Carolina at Charlotte
Charlotte, USA
asiddiq6@uncc.edu

Suyash Mohan Tamore
University of North Carolina at Charlotte
Charlotte, USA
stamore@uncc.edu

Fareena Saqib
University of North Carolina at Charlotte
Charlotte, USA
fsaqib@uncc.edu

***Abstract*—Integration of complex and high-speed electronic components in the state of art electric power system enhances the need for improved security infrastructure and resilience against invasive and non-invasive attacks on the smart grid. A modern smart grid system integrates a variety of instruments and standards to achieve cost-effective and time-effective energy measurement and management. As the fundamental component in the smart grid, the smart meter supports real-time monitoring, automatic control, and high-speed communication along with power consumption recording. However, the wide use of smart meters also increases privacy and security concerns. In this paper, we demonstrate the vulnerability of side-channel attacks on secure communication in smart grids for software-based and hardware-based implementations.**

Keywords—smart grid, smart meter, AES, side-channel attack, correlation power analysis, electromagnetic attack

I. INTRODUCTION

The demand for electricity supply is rising rapidly. The integration of renewable power supply facilitates the production on the expense of complexity of the infrastructure with several electronic components, coordination of endpoints and data communication between the utility and its customers. Integration of infrastructure with renewable energy sources with power converters and smart grid initiatives improve power production and infrastructure. Compared to the traditional power system, the smart grid allows the utility to monitor the power generation and consumption for each customer individually and allocate resource uniformly and dynamically. The Advanced Metering Infrastructure (AMI), a.k.a. the smart meter takes charge of power measurement, automatic control and data communication for every customer.

The data exchange between the plant and each endpoint has become a security and safety threat, the risk of malicious attacks such as phishing attacks and social engineering attacks has also raised. To mitigate the risk, the Advanced Encryption Standard (AES) is implemented for protecting the communication between different nodes in the smart grid, but it is still vulnerable to attacks, such as side-channel attacks.

In this paper, the effectiveness of the side-channel attacks on AES encryption used in smart meters is explored. Our experiments include power analysis and electromagnetic analysis on software-based and hardware-based implementations.

Contribution: This paper makes the following contributions:

1. We present the threat model of non-invasive attacks on AMI security.

2. We demonstrate a successful attack on the key of software-based and hardware-based AES-128 using correlation Power Analysis (CPA).

3. We apply the Correlation EM Analysis (CEMA) attack on the key of AES-128 successfully.

4. A discussion of security analysis and countermeasures.

Paper organization: The paper is organized as follows. The related work is discussed in section II. Section III explains the attack model used in this work. Section IV and section V demonstrate the experimental setup and results. The security analysis is given in section VI.

II. RELATED WORKS

A. Smart Grid

The modern digital technology and high-speed interactive network allow two-way communication between the utility and its customers to make the grid "smart". By applying new techniques of sensing, controlling and real-time communication on electronic meters and connecting them with the utility, the time-efficiency and the cost-efficiency of the whole power grid have been increased significantly. The communication between the utility and smart meters in the smart grid supports several protocols defined by the American National Standard Institute (ANSI), such as C12.18 [1], C12.21 [2], and C12.22 [3]. Specifically, C12.18, C12.21, and C12.22 describe the communication over the optical port, the telephone modem, and the network, respectively. Depending on different applicable conditions, the smart meter might support different protocols or multiple protocols.

The boom of the smart device market and electric car market results in high demand for the electricity. C12.22 accommodates the network requirements of metering infrastructures and makes the centralized management of power system possible. The protocol specifies roles of all Utility AMI network assets in the distributed power system and defines the network management service to provide a universal global framework which can communicate with all the nodes bidirectionally.

978-1-7281-4878-6/19/$31.00 ©2019 IEEE

Meanwhile, to protect the confidentiality and data integrity, C12.22 supports the EAX' cryptographic mode to enable strong secure communication between the smart meter and the power plant. EAX' encrypts all the messages with AES-128 encryption standard using the key generated by a built-in function. The encryption engine in the smart meter can be implemented at the software level [4], or the hardware level [5] [6].

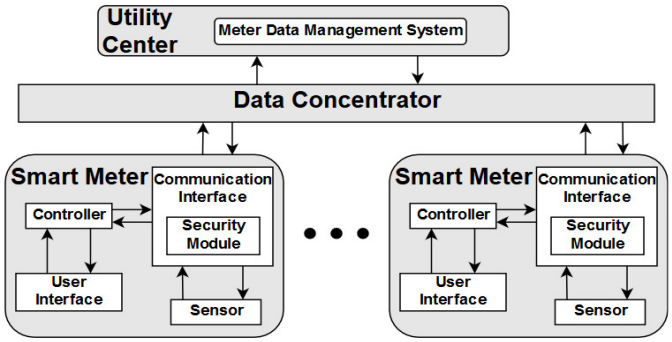

Figure 1. Smart metering architecture

Figure 1 shows the architecture of a smart grid. The customer is equipped with the smart meter that collects time-based data of power consumption. All the data in smart meters are collected and encrypted with AES-128 in the security module and sent to the Meter Data Management System (MDMS) in the utility center via the network for analysis and management.

B. AES Encryption

The Advanced Encryption Standard (AES) was established in 2001 by the U.S. National Institute of Standards and Technology (NIST) and adopted as the encryption standard of the U.S. government to replace Data Encryption Standard (DES). In past years, the AES standard has been developed fully to enhance the strength of security widely applied in the communication area and data storage to protect the confidential data and provide the function of authentication.

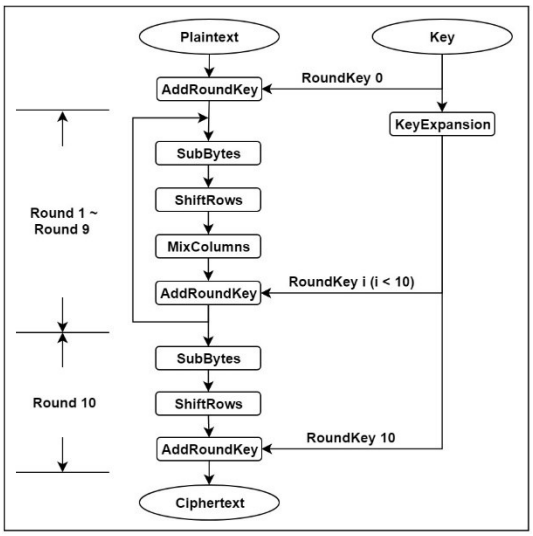

Figure 2. The encryption process of AES-128

In this paper, we implemented AES-128 as victim target. Figure 2 shows the full encryption process of AES-128. The AES-128 encryption is a streaming cipher that takes a 128-bit key and divides the data into 128-bit blocks and encrypts the data as follows:

1. KeyExpansion: Generate different round keys for each round based on the cipher key following Rijndael's key schedule.

2. AddRoundKey: Combine each byte of the state with the corresponding byte of the round key by using bitwise XOR.

3. Iterative round: Consist of 9 same iterative rounds. Each round has four operations: SubBytes (a non-linear substitution based on look-up table named S-box), ShiftRows (a cyclic shifting in each row by a certain offset), MixColumns (an invertible linear transformation combing the bytes in each column), AddRoundKey.

4. Final round: Similar to iterative round but only has 3 operations: SubBytes, ShiftRows, and AddRoundKey.

C. Side-channel Attack

In contrast to other attack models, the Side-Channel Attack (SCA) utilizes various physical parameters to steal information. As a typical form of reverse engineering, SCA steals keys using the leaked information from the implementation of the system rather than the weakness in the algorithm itself.

During execution, the leakage of physical information is inevitable, such as time delay, power consumption, electromagnetic radiation, and sound. The key concept of SCA is to find the relationship between the dynamic variation of physical parameters and operations being executed on the hardware thereby steal the secret information. Side-channel attacks can not only exfiltrate information from the communication process but also break encryption based on analyzing the variation of parameters during the runtime.

The countermeasures consist of morphing techniques and masking techniques and will be discussed in the security analysis.

D. Power Analysis

This form of attack uses the power traces to capture the variations in power consumption and correlate it with computational engine operations. The power consumption of an integrated circuit or a larger device reflects the aggregate activity of its individual elements, as well as the capacitance and other electrical properties of the system. By collecting power traces and modeling analysis, the hidden information can be extracted non-invasively.

Simple Power Analysis (SPA) is a type of SCA [7]. The attacker measures variations in the power consumption of a device and reveals the sequence of instructions or data executed and correlated to the fluctuation of power [8]. However, the SPA doesn't work effectively on hardware-based implementations of cryptographic algorithms because hardware-based implementations are using concurrent processing model and have smaller power consumption variations. As an advanced attack, Differential Power Analysis (DPA) uses a statistical method to analyze sets of measurements to identify data-dependent correlations. This process can reduce noise and extract the relationship between the dynamic power consumption and the secret key even the power variation is very small. [7]

Correlation Power Analysis (CPA) [9] uses hamming weight or hamming distance to model the consumption of power in the device based on the assumption that the number of bits set to 0 or 1 of output is correlated with the power consumption of the device. The correlation is quantified by Pearson Correlation Coefficient between the guessed model and actual power consumption traces in sequence until the correct information is extracted. Compared to DPA, CPA has higher efficiency and it normally requires fewer power traces than DPA [9].

E. ElectroMagnetic (EM) Analysis

For the power analysis, the attacker is required to have physical access to the Device Under Attack (DUA). To capture the real-time power trace of the device, the prerequisite is to find an attack point or to probe the device. For example, adding a resistor between power and ground line. However, EM analysis doesn't require to make any physical changes to the device. Electromagnetic radiations are captured, without touching the cryptographic device chip, by placing the EM sensor within a distance of few millimeters or even few feet in some cases. Such non-contact nature of the EM side-channel attack makes it more feasible and dangerous than power-based side-channel attacks.

EM emanations are the result of the flow of current through the different components and elements on the circuit or the microchip. Each electronic components on the circuit and data paths create their own EM radiations as well as coupled EM radiation by interfering with the nearby components EM field. This feature makes the attack based on EM radiation possible. By collecting EM radiation and performing signal analysis, the operation on the device and the information can be revealed. [10] and [11] presents EM side-channel attack on a smart card chip implementing DES encryption. [12] modifies the EM attack to decrease the number of total traces required to extract key information using a pre-processing technique which reduces noise levels.

III. Attack Model

In this work, we investigated side-channel attacks on different implementations of AES-128 encryption which is implemented on the smart meter for secure communication.

A. Power Analysis

The security of data communication in the smart grid system is provided by EAX' mechanism which supports message encryption/decryption with AES-128. The EAX' mechanism is specified by the ANSI C12.22 protocol and implemented at the software level. The power analysis can break the key used in the encryption engine by measuring and analyzing the run-time power consumption of the device. In this work, we demonstrate the Correlation Power Analysis (CPA) attack on different targets, that are used in the smart grid infrastructure. Following are steps to perform the CPA attack:

1. Collect power traces using the passive probe and EM probe for several different plaintexts. The attacks can be launched from the first round or the last round of AES. In this work, we attacked the AES from the first round for both software-based and hardware-based implementations.

2. Key guessing. The original key is divided into 16 subkeys. For each subkey, guess all the possible values. Each subkey is 8 bits long, so there are 256 possible values for each subkey.

3. Build the leakage model using hamming weight with all the guessed key values. The power trace of the device leaks the data transitions in the computational extensive cryptographic functions. Specifically, most of the energy is consumed by the operation of SubBytes [13], so the output of the S-Box is what we'll use to check the guessed value of the key.

4. Correlation analysis. Evaluate the similarity between the modeled leakage model and each collected power trace. The correlation is quantified by calculating the Pearson correlation coefficient in this work. The Pearson correlation coefficient ρ is defined as:

$$\rho(A,B) = \frac{cov(A,B)}{\sigma_A \sigma_B} = \frac{\mathrm{E}[(A-\mu_A)(B-\mu_B)]}{\sqrt{\mathrm{E}[(A-\mu_A)^2]}\sqrt{\mathrm{E}[(B-\mu_B)^2]}} \quad (1)$$

where A and B are variables, cov denotes the covariance, σ denotes the standard deviation, μ is the mean value and E is the expectation value. In this work, we collected multiple power traces for a more accurate result, so the objective of CPA attack is to calculate the coefficient as follows:

$$C(h,t) = \frac{\sum_{d=1}^{D}[(h_d-\bar{h})(t_d-\bar{t})]}{\sqrt{\sum_{d=1}^{D}(h_d-\bar{h})^2 \sum_{d=1}^{D}(t_d-\bar{t})^2}} \quad (2)$$

where h is the hypothetical value, t is the power trace, D is the total number of collected power traces.

5. Key obtainment: The guessed subkey with the highest coefficient is considered as most likely the correct subkey used in the encryption.

B. EM Analysis

In this work, the Correlation ElectroMagnetic Analysis (CEMA) attack is also explored. The attack flow of CEMA is similar to CPA except for two aspects:

1. The process of EM capture requires a specialized EM probe and the amplification factor of the signal is higher than CPA because the EM signal is more susceptible to the environmental noise.

2. Different from power capture, even the trigger signal is implemented on an independent Spartan-6 chip, the EM radiation caused by the trigger is also captured by the EM probe inevitably (The first peak and the second peak in Figure 8). To remove this noise, the EM analysis starts from the third clock cycle.

IV. Experimental Setup

In this work, we applied side-channel attacks on different targets, using power analysis and EM analysis. The key of AES we used in all the experiments is 97 45 C3 73 1D AD 77 B1 17 B5 76 F4 5B 4C 1E E0.

A. Power Analysis on Software-based AES Implementation

In the up-to-date smart meter, a software-based framework is implemented which provides multiple functionalities, including real-time monitoring, power consumption recording,

intelligent regulation, and secure data communication based on AES encryption.

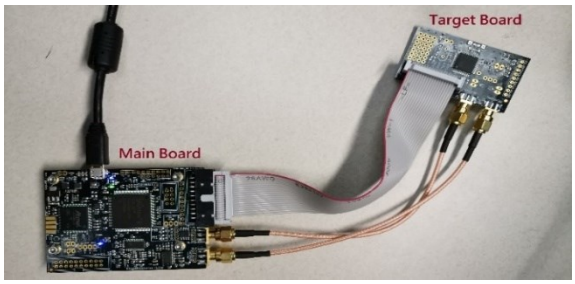

Figure 3. Chipwhipserer toolkit

As shown in figure 3, the AES-128 engine is implemented on the XMEGA 128D4 microcontroller on the target board, and the capture module is implemented on the motherboard which has a USB controller (in C) and an FPGA for high-speed captures (in Verilog) [14]. AES encryption takes different random plaintexts on the target board and for each operation, power traces are collected. Figure 4 shows an example of a collected power trace of a full AES encryption process.

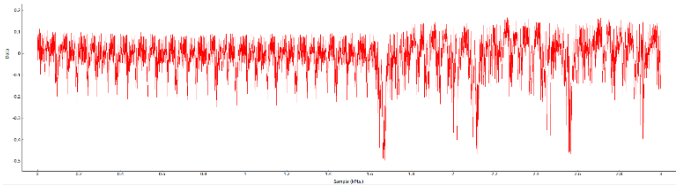

Figure 4. Power trace of AES encryption on XMEGA chip

B. Power Analysis on Hardware-based AES Implementation

According to the research presented in [6], the implementation on the microprocessor has a significant drawback of time delay due to the sequential processing model. The hardware-based implementation of AES engine on AMI meter has benefits in terms of low latency and reconfigurability. Moreover, the hardware-based implementation has a better tolerance to side-channel attack because of low power variation and its parallel nature [7].

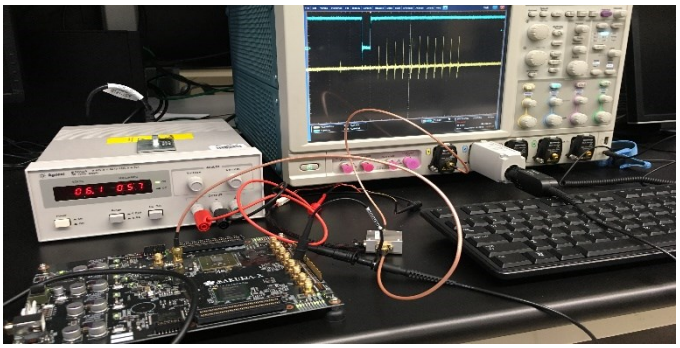

Figure 5. Setup of power capture.

In this work, the tolerance to side-channel attack on hardware-based implementation is explored. The target device used is Sakura-X experimental board which has two on-board FPGA chips. The AES engine is implemented on the Kintex-7 160T FPGA chip based on 28nm technology (in Verilog), while the controller and the trigger are implemented on the Spartan-6 FPGA chip. The power consumption is amplified by YKS 1000 low noise amplifier and captured by the oscilloscope at a sampling rate of 6.25 GS/s. Figure 5 shows the detail of the setup for capturing power consumption.

In this experiment, we collected 15000 power traces with random plaintexts considering the better tolerance of hardware-based implementation. Figure 6 shows an example of a power trace of the first 3 rounds in the encryption process.

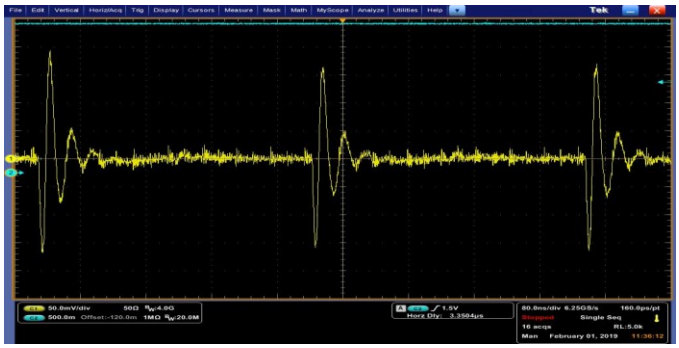

Figure 6. Power trace of first 3 rounds in encryption on Kintex-7

C. EM Analysis on Hardware-based AES Implementation

We also measured EM traces of the encryption process. To capture EM traces, we used CW505 Planar H-field probe manufactured by NewAE Technology. The setup of EM capture is shown in Figure 7.

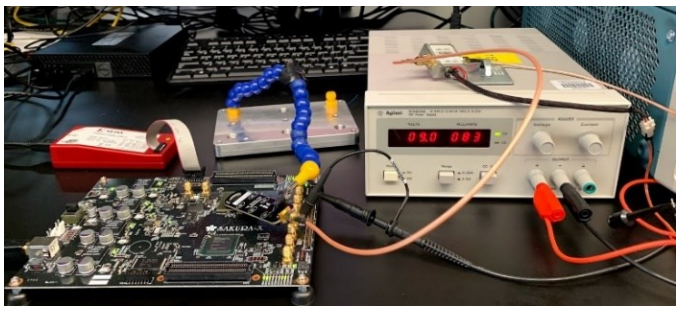

Figure 7. Setup of EM capture.

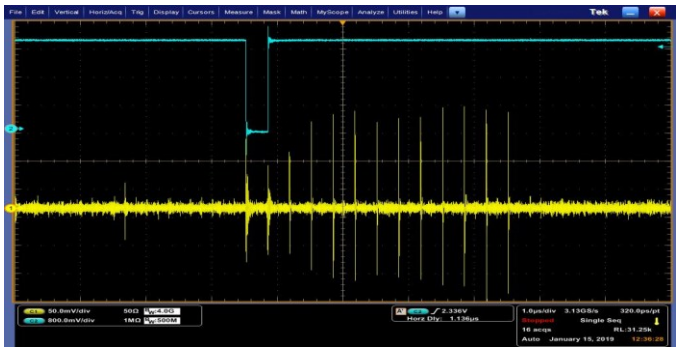

Figure 8. EM trace of AES encryption on Kintex-7. The yellow line is EM radiation of the chip and the blue line is the trigger signal.

Considering the EM is more susceptible to the environmental noise, we collected 30000 EM traces with random plaintexts for performing the CEMA attack. Figure 8

shows an example of EM trace of the whole AES encryption process.

V. Experimental Result

A. Power Analysis on Software-based AES Implementation

To perform the CPA attack, the AES 128-bit key is divided into 16 subkeys and each byte is attacked independently. After applying the attack, guessed subkey with the highest coefficient is considered as the correct subkey used in the AES encryption.

The result of CPA attack with different numbers of collected power traces on software-based implementation is shown in Figure 9. The x-axis represents the quantity of power traces used in the CPA attack, and the y-axis represents the number of revealed subkeys. All the subkeys are extracted successfully after applying the CPA attack with only 40 power traces.

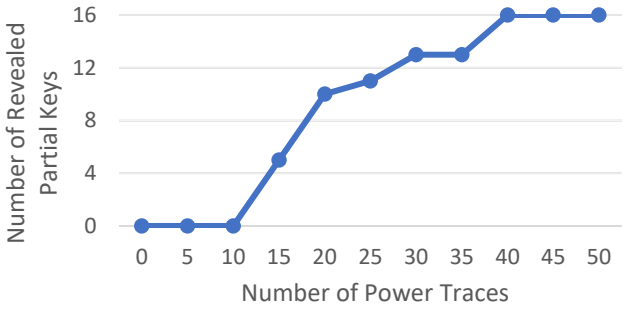

Figure 9. The result of CPA attack on software-based AES implementation.

B. Power Analysis on Hardware-based AES Implementation

Figure 10 shows the result of CPA attack on the first subkey. The value of the first subkey used in the encryption is 97 (151 in decimal), and it takes around 6000 power traces to extract it successfully. The graph shows that as more traces are included, the correlation coefficient of the correct key combination is obviously higher than other combinations.

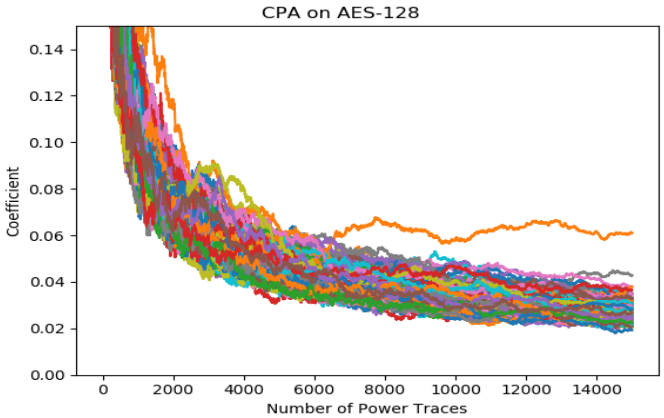

Figure 10. The result of CPA attack on the first subkey on hardware-based AES implementation with 15000 power traces.

Even the required number of power traces is more than the attack on the software-based implementation, the hardware-based AES implementation is still unsecure to CPA attack.

C. EM Analysis on Hardware-based AES Implementation

The result of the CEMA attack on the first subkey of AES encryption is shown in Figure 11. The attack needs around 12000 traces to reveal the first subkey.

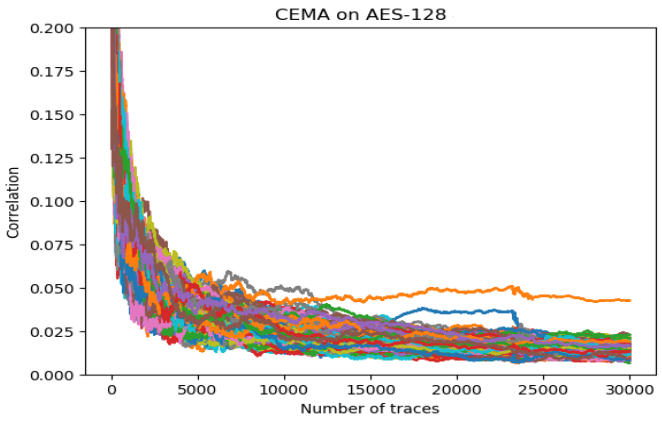

Figure 11. The result of CEMA attack on the first subkey on hardware-based implementation with 30000 EM traces.

EMA attack requires more traces than CPA attack, and the result proves that attacking the encryption engine on the hardware-based implementation by CEMA is possible and even more threatening because it is a non-contact attack.

VI. Security Analysis

Electronic devices in smart meters are vulnerable to invasive and non-invasive attacks. These devices are in the untrusted field, and in physical proximity that can be used as the point of attack to bring the grid down. In this work, we evaluated the resilience of smart meters AMIs to different side-channel attacks on software-based and hardware-based implementations.

According to the result of experiments, the key of software-based AES implementation can be extracted correctly by CPA attack with less than 40 power traces, it means that implementing AES encryption at the software level is the most vulnerable to side-channel attacks. The main reason is that the software-based implementation works sequentially, the real-time power trace leaks more information which makes the process of finding the statistical relationship between the measured signal and the hypothetical model faster and easier.

In contrast to the software-based implementation, the hardware-based (FPGA in this work) implementation shows better resilience. To extract the correct value of the first subkey, around 6000 power traces are used. There are two main reasons:

1. The parallel nature of the hardware-based implementation. The parallel processing model decreases the variation of power consumption significantly, thereby increases the difficulty of side-channel attack on it.

2. The use of the state-of-the-art lithography process. The Kintex-7 160T chip on the Sakura-X board used in this work is using the 28nm technology which makes the dynamic range very small [15].

The CEMA attack on the FPGA-based AES implementation is also feasible but takes around 12000 traces to extract the same

key value which is more than CPA attack. This is because the noise disturbance from the environment in EM trace is higher than in power trace. In general, implementing AES on hardware is helpful for enhancing the resilience of smart device to side-channel attacks, but even the implementation on the most advanced hardware platform is still vulnerable to CPA attack and CEMA attack.

To mitigate the risk of side-channel attacks, [16] proposes a code morphing based countermeasures for software-based implementation which can change the implementation of a block cipher at runtime. Applying the proposed dynamic re-compiler increases the Measurements To Disclose (MTD) time, but the overhead of time delay is not negligible.

The parallel nature makes hardware-based implementation more resilient to side-channel attack, so applying countermeasures on the hardware-based implementation is more efficient and practical. One common countermeasure is masking which randomly splits every sensitive intermediate variable occurring in the computation into shares to hide the secure information. This method has been proved as an efficient countermeasure by previous works, such as [17] and [18].

Another feasible countermeasure to defend side-channel attacks is key update scheme. The key update mechanism sets a module on both sender side and receiver side and updates the key value before the current key can be extracted by the side-channel attack synchronically. This mechanism increases the difficulty of side-channel attacks but requires synchronization of all the nodes in the network and additional space for key storage or new key generation scheme such as the embedded Physical Unclonable Function (PUF) as discussed in [19].

VII. Conclusion

The widespread use of AMI devices in the smart grid has improved the efficiency of power measurement and management, but also brings a critical concern of security due to data leakage. In this paper, we showed that the AES encryption used for protecting communication in the smart grid is vulnerable to side-channel attacks by performing CPA attack and CEMA attack on both software-based implementation and hardware-based implementation successfully. The result indicates that side-channel attacks can extract the secret key used in encryption non-invasively even without physical proximity. To address the degree of vulnerability of different implementations to power analysis and EM analysis, we analyzed the result and discussed some feasible countermeasures for mitigating side-channel attacks.

Acknowledgment

This research was supported by the National Science Foundation under Grant No.1819687 and No.1819694.

References

[1] "ANSI C12.18-2006." [online]. Available: https://webstore.ansi.org/Standards/NEMA/ANSIC12182006R2016 [Accessd Feb. 10, 2019

[2] "ANSI C12.21-2006." [online]. Available: https://webstore.ansi.org/Standards/NEMA/ANSIC12212006R2016 [Accessd Feb. 10, 2019]

[3] "ANSI C12.22-2008". [online]. Available: https://webstore.ansi.org/Standards/NEMA/ANSIC12222008 [Accessd Feb. 10, 2019]

[4] Yujie Shi and Xinhui Du. "The Design of Smart Power Meter Based on ARM9 Microprocessor," in *2015 International Symposium on Computers and Informatics*, Beijing, China, January 17-18, 2015.

[5] Arockia Cecilia A and Sudrsanan K. "An Implementation of FPGA Based smart meter for Home Energy Management," *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 2, pp.1236-1239, February 2016.

[6] Kautilya Pachorie, Surabhi Agrawal, Varun Maheshwari, Bhagwan Das Devulapalli and A. K. Saxena. "Design and Development of Digital Energy Meter on FPGA," in *Muttoo S. (eds) System and Architecture*, vol 732, pp.261-273, 2015.

[7] Paul C. Kocher, Joshua Jaffe and Benjamin Jun. "Differential Power Analysis," in *CRYPTO '99 Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara, USA, August 1999.

[8] Yutian Gui, Ali Shuja Siddiqui, Suyash Mohan Tamore and Fareena Saqib. "Investigation of Vulnerabilities on Smart Grid End Devices," in *IEEE PELS CyberPELS Workshop 2019*, April 2019.

[9] E. Brier, C. Clavier and F. Olivier. "Correlation power analysis with a leakage model," in *Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004*. vol. 3156, pp.16-29, 2004.

[10] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao and Pankaj Rohatgi. "The EM Side-Channel(s): Attacks and Assessment Methodologies," *Kaliski B.S., Koç .K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2002*, vol. 2523, pp. 29-45, 2002.

[11] Karine Gandolfi, Christophe Mourtel and Francis Olivier. "Electromagnetic Analysis: Concrete Results," In *Koç Ç.K., Naccache D., Paar C. (eds) Cryptographic Hardware and Embedded Systems — CHES 2001*, vol. 2162, pp. 251-261, 2001.

[12] Aiguo Bu, Wentao Dai, Minyi Lu, Hao Cai and Weiwei Shan. "Correlation-Based Electromagnetic Analysis Attack Using Haar Wavelet Reconstruction with Low-Pass Filtering on an FPGA Implementation of AES," in *TrustCom/BigDataSE 2018*, New York, USA, August 2018.

[13] Sumio Morioka and Akashi Satoh. "An Optimized S-Box Circuit Architecture for Low PowerAES Design," in *In: Kaliski B.S., Koç .K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2002.*, vol 2523, pp. 172-186, 2018.

[14] "ChipWhisperer - the complete open-source toolchain for side-channel power analysis and glitching attacks." [online]. Available: https://github.com/newaetech/chipwhisperer [Accessd Feb. 15, 2019]

[15] Yu Nomata, Masato Matsubayashi, Kohei Sawada and Akashi Satoh. "Comparison of side-channel attack on cryptographic circuits between old and new technology FPGAs," in *2016 IEEE 5th Global Conference on Consumer Electronics*, Kyoto, Japan, October 2016, pp. 1-4.

[16] G. Agosta, A. Barenghi, and G. Pelosi, "A Code Morphing Methodology to Automate Power Analysis Countermeasures," in *The 49th Annual Design Automation Conference 2012*, San Francisco, USA, June 2012, pp. 77-82.

[17] Emmanuel Prouff and Matthieu Rivain. "Masking against Side-Channel Attacks: A Formal Security Proof," In *Johansson T., Nguyen P.Q. (eds) Advances in Cryptology – EUROCRYPT 2013*, vol 7881, pp. 142-159, 2013.

[18] Massoud Masoumi, Pouya Habibi and Mohammad Jadidi. "Efficient implementation of masked AES on Side-Channel Attack Standard Evaluation Board," In *2015 International Conference on Information Society (i-Society)*, London, UK, November 2015, pp. 151-156.

[19] Xiaodan Xi, Aydin Aysu and Michael Orshansky. "Fresh re-keying with strong PUFs: A new approach to side-channel security," *In 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Washington, USA, May 2018.