Interceptive Side Channel Attack on AES-128 Wireless Communications for IoT Applications

Ali Akbar Pammu*, Kwen-Siong Chong and Bah-Hwee Gwee
School of Electrical and Electronic Engineering
Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798
Email: *ali1@e.ntu.edu.sg

***Abstract*–We propose a wireless interceptive side-channel attack (SCA) technique to reveal the secret key of the AES-128 encryption algorithm in wireless communications through correlation electromagnetic analysis (CEMA) for Internet of Things (IoT) applications. The encrypted wireless communication link is implemented using two ATmega processor based Arduino microcontrollers. There are two key features of our proposed wireless interceptive SCA technique. First, we analyze the physical leakage information, the correlated EM signals, of the processed data generated during the encryption process based on the circuit architecture of the ATmega processor. Therefore, our analysis is able to identify the particular module of the processor leaks the correlated EM signals. Second, we investigate the resistance of AES-128 encryption algorithm implemented on ATmega processor against CEMA based SCA. Thus, our investigation is able to evaluate the security level of AES implementation in ATmega processor against CEMA attack. Based on the experimental result, the correlated EM signals, corresponded with the processed data, noticeably leak out at data bus processor and SRAM module during the encryption process. In addition, we perform the CEMA attack against AES-128 algorithm based on ATmega processor implementation and the secret key is successfully revealed by 20,000 EM measurements. The result is significantly higher compared with other programmable circuit architectures, FPGA and ARM based processor, which are 20× and 6.67× more secured than FPGA and ARM based Processors implementations respectively.**

***Keywords*–Electromagnetic Attack, Arduino, ATmega, SCA**

I. INTRODUCTION

Advanced technology in Internet-of-Things (IoT) present enormous potential for connecting various smart objects through the wireless (i.e. Wi-Fi, Bluetooth and Radio Frequency), in real time with high quality of service (i.e. high bandwidth), as depicted in Fig. 1. The IoT has been employed for many system applications such as E-Healthcare system [1], Micro Energy Harvesting [2], Smart Building [3] and Vehicle-to-Vehicle (V2V) communication [4]. In the E-Healthcare system, information of patients is able to integrate with refrigerator to control stored food in such a way that it can filter the suitable food to consume. The information of the patient sent by doctor is updated in timely bases through online. In the smart building, the energy consumption can be smartly controlled by sensors and the IoT also enables the user to monitor the energy consumption through smart phone. In the V2V system, the traffic jam and accident can be prevented by gathering the information of the traffic, the position and the speed of other vehicles relative to the other.

The aformentioned examples on IoT application are highly dependent on online data availability. However, the online data is vulnerable against malicious attack. Unintended party (i.e. adversary) is able to intercept the communication system in IoT and abuse the necessary information. For instance, in E-Healthcare system, the adversary is able to acquire information of the patient and misuse it for other purpose and therefore the information of the patient is no longer be trustfully due to malicious attack.

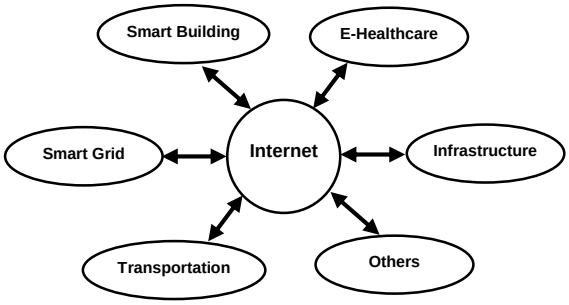

Fig. 1: IoT is a connection of multiple systems through internet

In order to address the aforementioned issues, the wireless communication system in IoT must be capable to communicate with other devices over an air interface and provide privacy and security capabilities. In this context, it is equipped with security module which can protect the necessary information sent to and received from an intended party. The security module is embedded with encryption algorithm such as Advanced Encryption Standard (AES) which is typically transform the information (i.e. plaintext) into encrypted information (i.e. ciphertext) using a secret key (known only by intended party). Therefore, any unauthorized party that intend to intercept the wireless signals is almost impossible to interpret it without the secret key.

The AES algorithm has been proven to be more effective than Data Encryption Standard (DES) in protecting the plaintext [5]. In 1998, the key of DES (2^{56} possible keys) has been successfully broken by brute force attack. In addition, the AES algorithm can process large block size of plaintext such as 128-bit, 192-bit and 256-bit with dissipate low power (i.e. in FPGA, dissipate about 18mW), fast process (i.e. processing 128-bit requires only 50µs). Therefore, the AES is promising to be implemented in the future IoT system, particularly at sensor based application with battery powered system at high-end user.

A physical-attack approach which is known as side-channel attack (SCA) [5] has been reported to successfully extract the secret key of the encryption algorithm by analyzing the physical parameters such as power dissipation [6], electromagnetic interference [7] and timing [8] of electronic devices during the encryption process. Power analysis is the most common SCA where it analyzes the power dissipation profile to extract the secret key. However, power analysis is more invasive compared with electromagnetic analysis [9]. This is due the adversary is required to modify the circuit in order to obtain a valid power measurement (i.e. one should identify the V_{DD} of the circuit and measure the current across the resistor). Correlation Electromagnetic Analysis (CEMA) is one of the popular

techniques in EM based attack which is implemented to disclose the secret key of AES implementation.

The AES-128 algorithm, which processes 128-bit key size, requires 10 round of iterations to encrypt the plaintext into ciphertext. The 10 round of iterations make AES-128 highly effective when compared to other encryption algorithms such as DES. However, due to the leaking of physical parameters correlate with intermediate data, the AES-128 implementation may still be vulnerable against SCA, particularly against the CEMA attack, as depicted in Fig. 2.

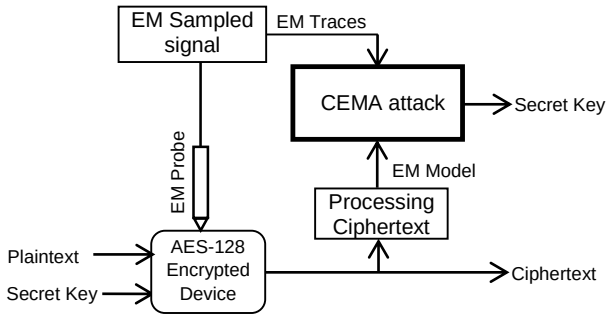

Fig. 2: General scheme of CEMA based SCA on AES-128

The SCA on small embedded devices, such as microcontrollers and cryptographic co-processors, are popular nowadays due to its ubiquitous application at high-end devices of IoT. However, there are only few literatures and studies of SCA on these systems (i.e. microcontroller and programmable chip) due to complexity on the program implementation. In the near future, there will be high chance to shift towards moving the cryptographic operation to the microcontroller, as proposed in mobile payments and host card emulation [9].

In this paper, we propose a wireless interceptive SCA technique to reveal the secret key of the AES-128 encryption algorithm. There are two key features of our proposed wireless interceptive SCA technique. First, we analyze the physical leakage information, the correlated EM signals, of the processed data generated during the encryption process based on the circuit architecture of the ATmega processor. Therefore, our analysis is able to identify the particular module of the processor leaks the correlated EM signals. Second, we investigate the resistance of AES-128 encryption algorithm in ATmega processor implementation against CEMA based SCA. Thus, our investigation is able to evaluate the security level of AES implementation in ATmega processor against CEMA attack. Based on the experimental result, the correlated EM signals, corresponded with the processed data, noticeably leak out at data bus processor and SRAM module during the encryption process. In addition, based on CEMA attack, the secret key is successfully revealed by 20,000 EM measurements.

This paper is organized as follows. Section II presents the ATmega structure in Arduino for high-end user application. Section III presents the proposed investigation of CEMA attack on Arduino ATmega based on AES-128 implementation. Section IV presents the measurement results and finally, conclusions are drawn in Section V.

II. ATMEGA ARCHITECTURE

The basic circuits design architecture of the processor can determine the robustness and resistance against SCA. Cell logic, switching activities, placement and routing of the modules and wiring structure are the key parameters which can potentially leak information out during the encryption process. In the cell logic perspective, the binary input (0 or 1) can be identified from variant of power dissipation measurement, hence the attacker can easily identify the internal processed data of the processor. For the switching activities, placement and wiring, its EM signal can be identified and measured during the transferred binary value (0 or 1) in the wire. The EM signal generated by the processor during the encryption is relatively easy to measure by placing the EM probe close to the chip.

In this section, feature of Arduino based on ATmega processor (specifically on ATmega328P) is discussed to investigate the possibility of leaking the SCA information. The processor technology is based on 8-bit AVR in which embed on-chip flash memory for program storage. As tabulated in Table I, size of the flash memory is 32KB used to store the program such as AES which occupies only 4KB. Temporary state of 16-byte of each rounds AES (totally 10 rounds iteration) is stored in data SRAM. The changes of the value for each state transitions in data SRAM is possible to be corresponded with the Hamming Distance (HD), EM model, which is derived from ciphertext. The switching activities with frequency of 20MHz generates EM signals which depends on the value of the processed information.

TABLE I. SPECIFICATION OF ATMEGA PROCESSOR BASED ARDUINO

ATmega328P	
Processor Technology	8-bit AVR
Operating Voltage	1.8 – 5.5 V
Switching Frequency	20MHz
Power Dissipation*	0.36mW
Flash Memory	32Kbyte
EEPROM	1Kbyte
SRAM	2Kbyte

*at voltage 1.8V and Frequency 1MHz

In order to protect the sensitive information, the 8-bit AVR microcontroller is implemented for high-performance encryption and decryption engine which can support 128-bit, 192-bit and 256-bit as lengths size key for AES. All AVR microcontrollers contain lock mechanisms to prevent reading and copying the program stored in on-chip Flash memory [10]. The lock mechanism program is stored in EEPROM. The intermediate result of AES which is the output of each round is stored in data SRAM before sending to I/O lines and I/O modules as depicted in Fig. 3.

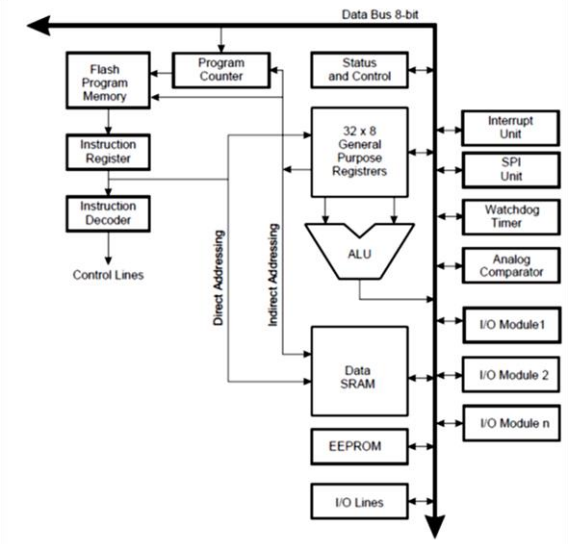

Fig. 3: Block diagram of 8-bit AVR architecture ATmega328P

The instruction from Flash memory during the encryption is sent to 32×8 General Purpose Register (GPR) and Arithmetic Logic Unit (ALU) to process the temporary stored information (i.e. plaintext) in the data SRAM. The result of the encryption is sent back to data SRAM by overwriting the previous result. The interface from GPU and ALU to SRAM is using data bus 8-bit as well as to the I/O modules. The EM of data flowing in data bus is emitted can be corresponded with processed data. In this context, the processed data is derived from ciphertext by employing HD EM model. The HD EM model is correlated with EM measurement and analyze the correct key. Since the ciphertext is more accessible than plaintext in practice, the HD model in this context is the changes between input and output of the last round. The key obtained at this round is reversed back using reverse expansion key AES to get the original key.

III. CEMA ON AES-128 BASED ARDUINO IMPLEMENTATION

The CEMA is the most prevalent type of EM analysis attack against encrypted devices [7] based on the EM model. An attacker exploits the correlation between the EM emanation by the device and the intermediate data (EM model) generated during the encryption process. In the AES-128 encryption process, there are 10 rounds of operations and at the last round consists of three operations such as S-Box, ShiftRow and AddRoundKey (XOR). As depicted in Fig. 4, the HD of the input (output of round 9) and the output (ciphertext) of the last round (round 10) is obtained to generate the HD EM model. The correlation coefficient based on the correlation between the EM model and the EM traces can then be determined to reveal the secrete key.

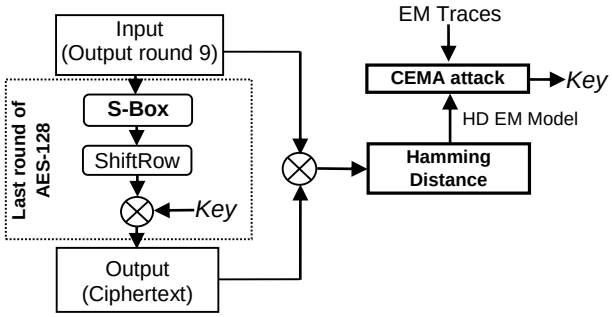

Fig. 4: CEMA attack is based on HD EM model of the last round AES

The CEMA attack is performed based on the analysis of correlation coefficient. The highest value of correlation coefficient occurs at the highest variance (σ^2) of EM traces [5]. The variance of EM traces is defined as the distribution of the EM emanation generated from different values of the processed intermediate data. Highest variance corresponds to sampled EM traces (sampling points) which have highest probability of leaking the information of the secret key.

The AES-128 algorithm is implemented on Arduino microcontroller which are the random plaintext and key pre-programmed in the flash memory. In this context, the AES-128 is based on *T-Table* approach [9], where the internal operations (i.e. S-Box, MixColumn and ShiftRow) are merged in one Look-Up-Table (LUT), hence the implementation dissipates low power and compatible with high-end user (i.e. IoT application). There are two Arduinos employed in this experiment which are Arduino_1 to encrypt the plaintext and send it in the form of ciphertext and Arduino_2 to intercept the ciphertext from Arduino_1.

Our main objective is to reveal the stored and programmed key on unprotected Arduino_1 by analyzing the ciphertext and the EM signals. In Arduino_1, it requires two sub-modules, AES-128 and Radio Frequency (RF) with antenna A_1, which are processing the plaintext and the key into a form of ciphertext and send it through wireless channel. In Arduino_2, the ciphertext is received by RF antenna A_2 and convert the analog signal into digital by means of Analog to digital converter (ADC) module. The EM signal is measured together with ciphertext during the encryption process and analyzed both parameters in Personal Computer (PC) as depicted in Fig. 5.

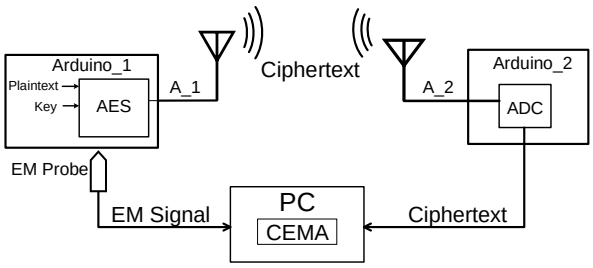

Fig. 5: CEMA attack scenario on Arduino

The CEMA attack is a byte-based EM analysis attack. Each byte of key (sub-key) is estimated by means of 256 possible values (1 byte = 8 bits and possibility is 2^8 = 256), hence the correct sub-key is one of the 256 sub-key candidates. The CEMA attack is performed by analyzing the correlation coefficient ($r_{i,j,t}$) of two variables, EM model ($X_{i,j,m}$) and EM traces ($Y_{t,m}$), for i = 1, ⋯, 16 sub-keys, j = 1, ⋯, 256 sub-key candidates, t = 1, ⋯, 1000 sampling points, as follows:

$$r_{i,j,t} = \frac{\sum_{m=1}^{n}(X_{i,j,m}-\bar{X}_{i,j})(Y_{t,m}-\bar{Y}_t)}{\sqrt{\sum_{m=1}^{n}(X_{i,j,m}-\bar{X}_{i,j})^2}\cdot\sqrt{\sum_{m=1}^{n}(Y_{t,m}-\bar{Y}_t)^2}} \quad (1)$$

The correct sub-key, i, corresponds to the highest $r_{i,j,t}$ at particular sub-key candidate, j, and sampling point of power traces, t. For instance, in attacking the first sub-key (i =1), with 1,000 EM traces (n = 1,000), the highest correlation coefficient ($r_{i,j,t}$ = 0.9) occurs at sampling point 61 (t = 61) for sub-key candidate 45 (j = 45), thus the correct first sub-key is 45.

IV. MEASUREMENT RESULTS

The experiment is conducted based on two Arduino microcontrollers which are implementing AES-128 algorithm. The EM emanation signal of Arduino_1 generated during the encryption process is measured and recorded in oscilloscope (2.5GS/sec) as depicted in Fig. 6. The encrypted data, ciphertext, intercepted by Arduino_2 which is sent from Arduino_1 through wireless communication (i.e. RF).

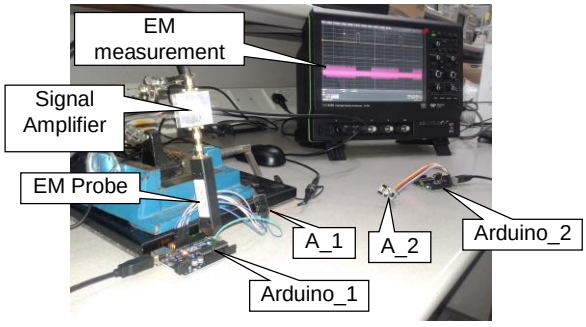

Fig. 6: EM measurement of AES-128 based Arduino implementation

The encryption process is initiated by loading the plaintex from I/O module to SRAM through data bus 8-bit. Subsequently, the data in SRAM is processed in 10 round iterations with the instruction from flash memory to GPR and ALU through data bus 8-bit. During the iteration process, the EM signals is increased due to processed data and intruction are contributing the EM signals through data bus 8-bit as depicted in Fig. 7. EM noise of 0.25V/m is due to clock frequency of the processor generates uniform EM.

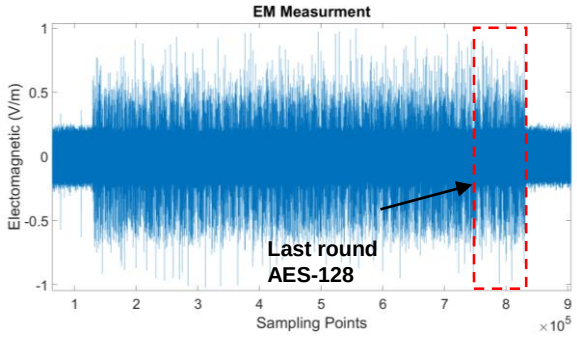

Fig. 7: EM measurement of AES-128 based Arduino implementation

The focus of the CEMA attack is at the last round of AES-128 which is the measurement indicated in the Fig. 7. The HD EM model is employed in this experiment, measuring the changes of input and output of the last round in SRAM of the AES-128 implementation. The 30,000 EM emanation (EM traces) is measured and plotted with Correlation coefficient. The result shows that the secret key is start to reveal at 20,647 EM traces as depicted in Fig. 8, where the black and grey color denoted as correct and the wrong key respectively. The investigation result is compared with FPGA [7] and ARM cortex A-8 processor [9] implementation and require only 1,000 and 3,000 EM traces respectively to reveal the secret key. Hence, the AES-128 implementation on Arduino is 20× and 6.67× more secured than FPGA and ARM based Processors implementation respectively. The comparison result of the performance resistance against CPA without countermeasure is tabulated in Table. II.

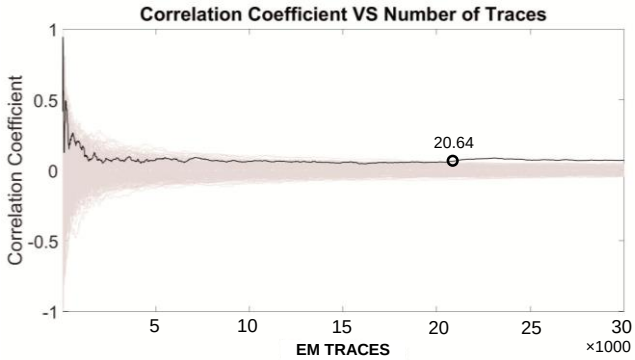

Fig. 8: Correlation coefficient vs EM Traces of AES-128 key based Arduino implementation

TABLE II. PERFORMANCE OF PROGRAMMABLE CHIP AGAINST SCA

Programmable processor	EM Traces	Crypto-Algorithm	SCA-Technique
FPGA (kintex-7) [7]	1,000	AES, DES	CPA, CEMA
ARM Cortex A-8 [9]	3,000	AES	CEMA
ATmega328P [Investigated]	20,000	AES, DES	CEMA

V. CONCLUSION

We have proposed a wireless interceptive SCA technique to reveal the secret key of the AES-128 encryption algorithm in wireless communications through CEMA for IoT applications. The physical leakage information, the correlated EM signals, of the processed data generated during the encryption process based on the circuit architecture of the ATmega processor has been analyzed. Therefore, our analysis is able to identify the particular module of the processor leaks the correlated EM signals. We have also investigated the resistance of AES-128 encryption algorithm implemented on ATmega processor against CEMA based SCA. Based on the experimental result, the correlated EM signals, corresponded with the processed data, noticeably leak out at data bus processor and SRAM module during the encryption process. In addition, we have performed the CEMA attack against AES-128 algorithm based on ATmega processor implementation and the secret key is successfully revealed by 20,000 EM measurements. The result is significantly higher compared with other programmable circuit architectures, FPGA and ARM based processor, which are 20× and 6.67× more secured than FPGA and ARM based Processors implementations respectively.

ACKNOWLEDGMENT

This research work was supported by Agency for Science, Technology and Research, Singapore, under SERC 2013 Public Sector Research Funding, Grant No: SERC1321202098. The authors thank A*STAR for the kind support in funding this research.

REFERENCES

[1] Boyi Xu, Li Da Xu, Hongming Cai, Cheng Xie, Jingyuan Hu and Fenglin Bu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1578-1586, May 2014.

[2] R. Gomez Cid-Fuentes, A. Cabellos-Aparicio and E. Alarcon, "Area Model and Dimensioning Guidelines of Multisource Energy Harvesting for Nano–Micro Interface," in *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 18-26, Feb. 2016.

[3] F. Zafari, I. Papapanagiotou and K. Christidis, "Microlocation for Internet-of-Things-Equipped Smart Buildings," in *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 96-112, Feb. 2016.

[4] L. Du and H. Dao, "Information Dissemination Delay in Vehicle-to-Vehicle Communication Networks in a Traffic Stream," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 1, pp. 66-80, Feb. 2015.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99*. vol. 1666, M. Wiener, Ed., ed: Springer Berlin Heidelberg, 1999, pp. 388-397.

[6] Kwen-Siong Chong *et al.*, "Counteracting differential power analysis: Hiding encrypted data from circuit cells," *Electron Devices and Solid-State Circuits (EDSSC), 2015 IEEE International Conference on*, Singapore, 2015, pp. 297-300.

[7] Y. Hori, T. Katashita, A. Sasaki, and A. Satoh, "SASEBO-GIII: A hardware security evaluation board equipped with a 28-nm FPGA," in *1st Global Conference on Consumer Electronics (GCCE), IEEE*, 2012, pp. 657-660.

[8] B. Coppens, I. Verbauwhede, K. De Bosschere and B. De Sutter, "Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors," *Security and Privacy, 2009 30th IEEE Symposium on*, Berkeley, CA, 2009, pp. 45-60.

[9] J. Balasch, B. Gierlichs, O. Reparaz, and I. Verbauwhede, "DPA, Bitslicing and Masking at 1 GHz," In *Cryptographic Hardware and Embedded Systems - CHES 2015*, Lecture Notes in Computer Science 9293, T. GÃneysu, and H. Handschuh (eds.), Springer-Verlag, pp. 599-619, 2015.

[10] Amel-8271J-AVR-ATmega-Datasheet_11/2015: ATmega48A/ PA/ 88A/ PA/ 168A/ PA/ 328/P