Side-channel Attack Countermeasure Based on Power Supply Modulation

Ruzica Jevtic, Pablo Perez-Tirador, Carmen Cabezaolias, Pablo Carnero, Gabriel Caffarena
Escuela Politecnica Superior
Universidad San Pablo-CEU
CEU Universities
28003 Madrid, Spain
Email: {ruzica.jevtic,pablo.pereztirador,gabriel.caffarena}@ceu.es
{cm.cabezaolias, p.carnero1}@usp.ceu.es

***Abstract*—As the number of IoT devices grows exponentially every year, so do the security threats. Due to their mobility and limited size, power and performance, these devices are particularly vulnerable to side-channel attacks that are based on device physical leaks. In this paper, we modulate the power supply voltage to secure the devices against two types of side-channel attacks: differential and correlation power analysis attacks (DPA and CPA) that aim to reveal cryptographic secret key and attacks that process the leaked signal to obtain the information on the activity inside the device (e.g. identify the keystrokes when typing a password). We perform both types of attacks on a low-cost microcontroller used in a variety of IoT devices and find the most effective voltage modulation for both of the targeted attacks. The proposed countermeasure is easy to implement and does not require re-designing the microcontroller, thereby avoiding high costs of fabrication and testing. It is extremely effective against cryptographic attacks as it increases the minimum number of traces required to disclose (MTD) by two orders of magnitude. For non-cryptographic attacks the correlation coefficient between the leaked signal and the sensitive information is lowered by 33%.**

I. Introduction

The rapid expansion of Internet-of-Things has made security a major concern. The IoT nodes are small devices with limited processing and storage capabilities that restrict the implementation of power hungry cryptographic algorithms. Suddenly, the side-channel attacks that have been known for several decades but have had mostly academic importance, have become a real threat. Their practical implementation was first reported for the smart card pin retrieval, and it has evolved since towards attacks on a wide variety of IoT devices.

Side-channel attacks extract the sensitive data by measuring device physical leaks such as time, power or electro-magnetic radiations. They can be classified into passive and active attacks. Passive attacks can be further classified into attacks that target the cryptographic algorithm secret key and non-cryptographic TEMPEST attacks. The former ones are known as differential and correlation attacks that are based on passive recollection of data and signal statistics applied on data afterwards to retrieve the key [1]–[10], [12]–[14]. The latter ones take advantage of leaked signals, generally electro-magnetic radiations of high-frequency signals such as CPU, memory or voltage regulator clocks that contain amplitude modulated sensitive data. They are then used for example to retrieve passwords by identifying keystrokes or obtain the information that is displayed on a screen. Active attacks are based on running a small program inside the device to create patterns in the leaked signal that disclose sensitive data [15]–[18] and are used for similar purposes as the TEMPEST attacks.

The signals that are routed throughout the entire chip such as power supply and clock, are the strongest signals and hence, the ones that leak the most of sensitive information [1]. Therefore it is of utmost importance to protect the leaks coming from these signals.

In this paper we focus on the power attacks. The leaked signal used in the power attacks is the current going to a device and is usually measured as a voltage over the shunt resistance that is placed in series with the power supply, divided by the resistance value. The current depends on both the power supply voltage and the activity in the chip and can be expressed mathematically as the load transductance amplitude modulated by the power supply voltage. We propose to modify the power supply voltage to create aliasing of the load signal to protect the device from TEMPEST and active attacks. Aliasing in the measured spectrum lowers the correlation between the leaked signal and the sensitive data as the original load spectrum is obscured. Additionally, the modified power supply voltage introduces variations in the power traces making the CPA and DPA attacks more difficult as well.

To test this, we use real on-board power measurements performed on an Arduino platform and change the power supply voltage externally. The proposed countermeasure is easy to implement and thereby avoids high costs of circuit design, fabrication and testing. We prove that it is capable of increasing the minimum number of traces to disclose by a factor of 100, and it lowers the correlation coefficient to 0.67.

II. Related work

The best method for evaluating the effectiveness of the countermeasures is by performing an actual attack.

Differential Power Analysis and Correlation Power Analysis are the most commonly used attacks for retrieving the secret key of the cryptographic algorithm [20], [21]. They are based on collecting a large number of power traces for different

inputs. The traces are grouped according to a value of a bit in a particular position (DPA) or correlation model (CPA) for a certain secret key guess. The correct key produces a clear difference in signal statistics of the different groups in a DPA and high correlation values in a CPA attack.

Several implementations have been reported to perform DPA and CPA attacks on Arduino [22]–[25]. Neither of them considers non-cryptographic attacks based on data correlation. The work in [23] considers the CPA attack only on AddRoundKey, one operation inside an AES round that is executed separately from the rest of the algorithm. The work in [22] presents a test bench for remote power attacks on Arduino Uno and Arduino Due platforms. They use an EM probe to capture the radiations from the chip and calculate their power. Their goal is to demonstrate that the attacks on IoT nodes are easily achieved and available at low cost, effort and knowledge on targets and should be taken seriously.

The work in [24] presents a testbed for power attacks on microcontrollers PIC and Atmega, and explores the effectiveness of several hardware and software countermeasures. The hardware techniques such as adding a constant current source, voltage regulator or another microcontroller in parallel with the attacked one, are not effective. Adding an operational amplifier to introduce non-linear relationship between the current and the voltage and building a low-pass filter with capacitors and inductances increase the number of traces needed for the attack, but at the high cost of power and area overhead. Software techniques such as injecting random instructions and shuffling the S-boxes randomly also improve the security, but the number of injected instructions needs to be very large, leading again to a significant power overhead. The tutorial in [25] describes a hardware and software setup for performing side-channel attacks and briefly presents the changes that need to be done to Arduino's board connections in order to capture the power traces. However, experimental results regarding the number of traces to perform a successful attack are not reported.

Several countermeasures have been reported for voltage regulators [2]–[9]. However, their implementation is expensive as they all require re-design of the device's power supply that includes chip design, verification and fabrication.

There is very little work on countermeasures against active attacks and TEMPEST attacks. Most of the work in the literature describes different methods for attacking [1], [15], [19], but neither one of them offers a protection against these attacks. TEMPEST attacks take advantage of the amplitude modulation of the sensitive information (the so-called red signal) that is either done by periodic signals inside the device such as CPU clock, voltage regulator clock or memory controller clock, or by a crosstalk of data buses (the so-called black signals).

Active attacks manipulate peripherals [15], memory [16], [17] or power management unit [18] by infiltrating a small program in the device that creates certain patterns in the leaked signal and thereby, reveals information on the device's activity. These attacks are very dangerous as they can hack the device from large distances and even through obstacles such as wall separation.

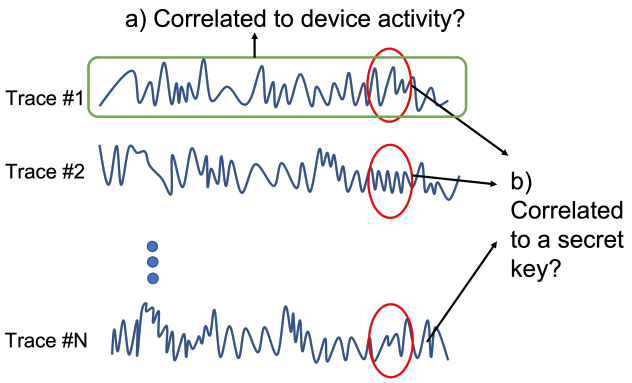

Fig. 1. Illustration for a) non-cryptographic and b) cryptographic attacks.

III. Power Attacks

In this work we evaluate voltage modulation as a method for securing the device against both type of attacks.

There is a fundamental difference in the nature of both types of attacks. The non-cryptographic attacks search for correlation between the leaked signal and the activity inside the device. The correlation is calculated for each program execution and takes into account the change in power during time. CPA and DPA attacks are based on many power traces and search for correlation between the power samples at the same time moments. In other words, while active and TEMPEST attacks exploit the behaviour of the power trace sequence in time, CPA and DPA attacks exploit the relationship between different power traces sample-wise. This is illustrated in Fig. 1.

We first analyze non-cryptographic attacks. The leaked signal is the current $I(t)$ going to the device. The activity of the device is the load for the power supply voltage regulator and can be represented as the equivalent resistance $R(t)$ that changes in time. The current can then be expressed as $I(t) = V(t)/R(t) = V(t) \cdot G(t)$, where $V(t)$ is the voltage power supply of the device and $G(t)$ is the equivalent load transconductance. It can be seen that the leaked signal $I(t)$ is the load transconductance amplitude modulated by the voltage power supply $V(t)$.

In the frequency domain, the current spectrum is obtained as convolution of the voltage spectrum and load transductance spectrum. Therefore, we propose to modulate the voltage to create aliasing in the current spectrum and, as a result, lower the correlation coefficient between the load and the leaked signal.

The voltage is modulated as $V(t) = V_m + V_a \cdot \sin(\omega \cdot t)$, where V_m is the mean and V_a the amplitude of the voltage. Since the voltage is modulated as a sine wave, another replica of the load spectrum is created around the sine frequency. If the load spectrum at the DC frequency and the replica overlap, aliasing is produced, and the original load spectrum is more difficult to retrieve (see Fig. 2).

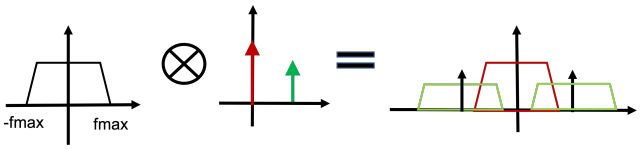

Fig. 2. Aliasing

A similar idea has been reported in [2] for switched capacitor dc-dc converters. However, their methodology is applied to flying capacitors in the voltage regulators and has not been tested on a real device, contrary to this work where the actual attacks are performed on a popular microcontroller used in IoT devices to assess the effectiveness of the proposed voltage modulation.

IV. Experimental results

To test the proposed countermeasure, we perform two experiments: one for non-cryptographic attacks and the other for the cryptographic attacks. For both experiments, we attack the execution of the AES-128 algorithm.

AES is the most widely used encryption algorithm for IoT devices and is based on laborious steps such as permutations, shuffling, and linear transformations that involve the input data and the encryption key. Ideally, these operations ensure that the relationship between the input and the output data is random. Although AES is considered to be quite secure, side-channel attacks such as Differential and Correlation Power Analysis (DPA and CPA respectively) can break the algorithm and obtain its encryption key. For non-cryptographic attacks, any application can be chosen to be attacked instead since we are looking for the correlation between the leaked signal and the device activity. However, we use AES-128 as well for the sake of simplicity.

A. Experimental setup

Several board modifications are necessary to perform the attacks and modulate the voltage on Arduino board.

To record dynamic changes in the current that are needed for the attacks: for the correlation power analysis and to obtain the information on the activity inside the device, a shunt resistor needs to be inserted as close as possible to the Arduino's microcontroller. The farther away the resistance is, the more filtrated are the high frequency components of the current. With this in mind, we have placed a 120 Ohm resistance between the 5V power supply pin of the Atmega328P chip and the power trace on the PCB that connects that pin to the ouput of the voltage regulator (see Fig.3). As a result, we have bypassed the voltage regulator that acts as a low-pass filter.

The power supply for Arduino is connected directly via 5V pin as all voltage variations are filtered by the voltage regulator if the power supply is connected to Vin pin. We use a PeakTech 4046 function generator as a power supply that can be modulated (see Fig. 4).

As explained in section III, we use a sine function for the voltage. To make sure that Arduino is not damaged, we vary

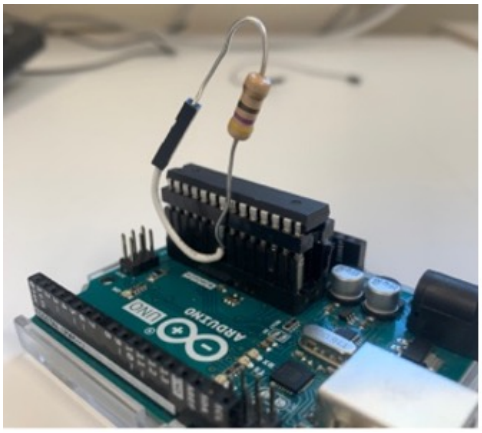

Fig. 3. Shunt resistance inserted in series with the power supply

Fig. 4. Voltage modulation with PeakTech 4046 function generator

the voltage between 5V and 6V. Since there is a voltage drop over the shunt resistance, the voltage on the microcontroller side is even lower than these limits. The frequency for the sine function is varied across a broad range of [0, 100MHz].

We use the NewAE ChipWhisperer platform to perform the power attacks on Arduino as well as to record and analyze current traces. Chipwhisperer platform is designed to perform CPA attacks. It connects to the target board via four digital connections and one analog measurement port and communicates with the target board via SimpleSerial protocol. Only the AC value of the current is recorded since both attacks extract information from the dynamic changes in the current.

B. Non-cryptographic attacks

The first experiment is designed to assess the effectiveness of the countermeasure to protect against active and TEMPEST attacks.

Fig. 5 shows the spectrum of the device current when Arduino is operating out of fixed 5V (up) and the spectrum of the device current when the voltage is modulated with frequencies of 10 MHz (middle) and 20 MHz (bottom). There is a dominant frequency component at 16 MHz in the original spectrum, that corresponds to the Arduino clock frequency. The spectra obtained with the modulated voltage show additional frequency components as a consequence of

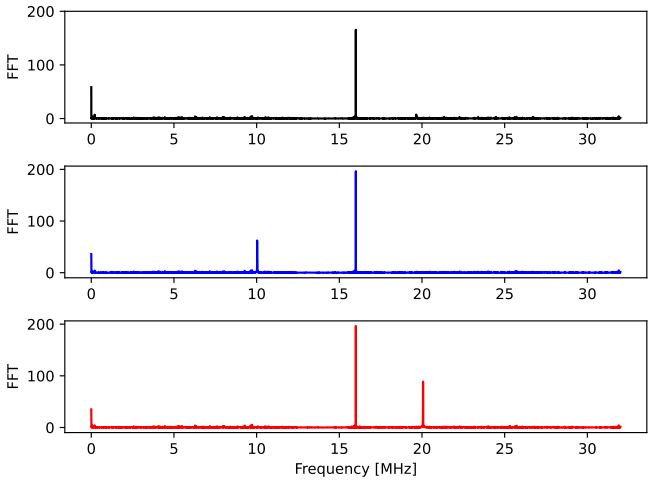

Fig. 5. Current spectrum for fixed voltage (up), 10 MHz modulation (middle) and 20 MHz (bottom)

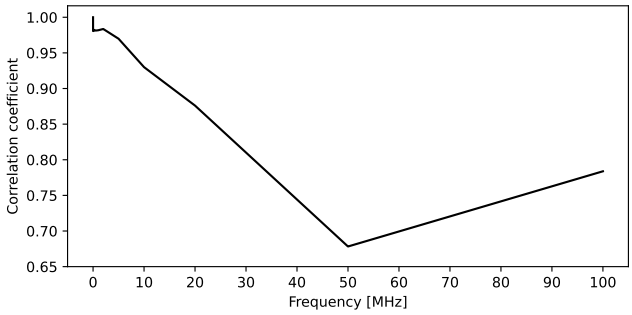

Fig. 6. Correlation coefficient vs. voltage sine frequency

voltage modulation. Due to the low voltage swing of the modulation and possibly due to sampling frequency limitations of the ChipWhisperer platform, the additional components from the modulated signal are difficult to distinguish in the spectrum.

We calculate the correlation between the power trace recorded for one execution of the AES algorithm when Arduino is operating out of a fixed 5V voltage and the power trace recorded when the voltage is modulated at many different frequencies from [0, 100MHz] range. Fig. 6 shows the correlation coefficient against voltage frequency. It can be seen that the largest decrease in the correlation coefficient of 33% is observed for a frequency of 50MHz.

The drop in the correlation coefficient is limited due to the DC component of the modulated voltage. Since the voltage mean is 5.5V and the amplitude is 0.5V, the zero-frequency component in the voltage spectrum is much larger than the spectrum component at the sine frequency. The replica of the load spectrum is therefore multiplied by the voltage amplitude, and the original spectrum is multiplied by the voltage mean. When the two of them are overlapped, the frequency components of the original spectrum are not affected enough by the frequency components of the replica. To remedy this situation, some other type of voltage modulation capable of creating more aliasing should be applied instead.

Frequency	Number of traces
0 (fixed 5V)	1K
10 KHz	1K
10 MHz	10K
30 MHz	40K
50 MHz	+130K

TABLE I
MTD FOR DIFFERENT VOLTAGE SINE FREQUENCIES

C. Cryptographic attacks

The second experiment is designed to assess the effectiveness of the countermeasure for CPA and DPA attacks on AES-128.

First, we deliver 5V constant voltage to program the Arduino. Then, we perform a CPA attacks for a constant 5V voltage and record the number of traces needed for the attack. Afterwards, we modulate the voltage as in the first experiment. We perform a CPA attack for several different frequencies and observe a huge increase in the number of traces needed for the successful attack at 50MHz, the same frequency that resulted in the smallest correlation coefficient. Table I shows the number of traces needed for the successful attack at different frequencies. MTD for an 80% success rate where 13 secret key bytes are recovered out of 16, is 130K traces.

The presented methodology uses only off-the-shelf components without any security measures integrated with the processor and increases the minimum number of traces to disclose similar to the previous work in [10] (100X) where the inductive voltage regulator was integrated together with the AES core and fabricated in 130nm technology. The achieved MTD is also three times larger MTD than the one reported in [11] (30X) where the specialized co-processor was implemented by using logic style and layout techniques different than the standard ones and therefore, not available to everyone. The increase in MTD reported here is several times smaller than the MTD reported in [12] (692X), [7] (4000X) and [13] (4210X). However, their increase in MTD comes at the expense of high design complexity and high fabrication cost. Additionally, the proposed methodology can be used on devices that already have security countermeasures applied to them, to achieve even better device protection against cryptographic attacks.

V. Conclusion

We evaluate the effectiveness of the countermeasure based on voltage modulation against both, cryptographic and non-cryptographic side-channel attacks. The voltage is modulated as a sine function to create aliasing in the spectrum of the leaked signal and therefore obscure the spectrum of the device activity. The variations in voltage also introduce variations in the device current during CPA and DPA attacks making it more difficult for the attacker to find the secret key. We

implement the countermeasure on Arduino platform and test it for several different voltage sine frequencies. The results show that the proposed countermeasure is extremely effective against cryptographic attacks as it increases the mean time to disclose by several orders of magnitude. The effectiveness of the technique is limited for the non-cryptographic attacks due to the limited amplitude for the voltage variations. The sine frequency that achieves the best security protection for both types of attacks is the same, making the proposed counteremasure a promising approach for increased security in the electronic devices.

ACKNOWLEDGMENT

This work was supported by the Spanish Ministry of Science, Innovation and Universities and the European Regional Development Fund of the European Commission under project RTI2018-095324-B-I00 and project FLYINGDRONES IDI-20210468.

REFERENCES

[1] R. Callan, et. al., "FASE: Finding Amplitude-Modulated Side-Channel Emanations", *In Proc. 42nd Annu. Int. Symp. Comput. Archit. (ISCA)*, Jun. 2015, pp. 592-603.

[2] R. Jevtic, et. al., "EM Side-Channel Countermeasures for Switched-Capacitor DC-DC Converters based on Amplitude Modulation", *IEEE Transactions on VLSI Systems*, vol. 29 (7), pp. 1061-1072, June 2021.

[3] R. Jevtic, et. al., "Methodology for complete decorrelation of power supply EM side-channel signal and sensitive data", *IEEE Transactions on Circuits and Systems II: Express Briefs*, January 2022.

[4] O.A. Uzun and S. Kose, "Converter gating: A power efficient and secure on-chip power delivery system", *IEEE J. Emerging Sel. Topics Circuits Syst.*, vol. 4, no. 2, pp. 169179, Jun. 2014.

[5] Weize Yu and Selcuk Kose, "Charge-Witheld Converter Reshuffling: A Countermeasure Against Power Analysis Attacks", *IEEE Trans. Circuits and Systems II, Exp. Briefs*, vol.63, no. 5, pp. 438-442, May 2016.

[6] R. Jevtic, M. Ylitolva and L. Koskinen, "Reconfigurable Switched-Capacitor DC-DC converter for Improved Security in IoT devices", *In Proc. 28th Int. Symp. Power, Timing, Modeling, Optim. and Simulation (PATMOS)*, July 2018.

[7] A. Ghosh, et. al.,"Physical Time-Varying Transfer Functions as Generic Low-Overhead Power-SCA Countermeasure", *arXiv:2003.07440*, 2020.

[8] C. Wang, et.al, "Electromagnetic equalizer: an active countermeasure against EM side-channel attack", *ICCAD*, Nov. 2018.

[9] D. Das, et. al.,"EM and Power SCA-Resilient AES-256 in 65nm CMOS Through $>$ 350X Current-Domain Signature Attenuation", *In IEEE Int. Solid-State Circuits Conf. (ISSCC)*, Feb. 2020, pp. 424-426.

[10] M. Kar, et. al., "Improved Power-Side-Channel-Attack Resistance of an AES-128 core via a security-aware integrated buck voltage regulator", *IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2017.

[11] D. D. Hwang, et. al., "AES-Based Security Coprocessor IC in 0.18um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks", *IEEE J. Solid-State Circuits*, 2006.

[12] A. Singh, et. al., "Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering", *IEEE J. Solid-State Circuits*, 2018.

[13] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "A 128b AES Engine with Higher Resistance to Power and Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low-Dropout Regulator", In *IEEE Int. Solid-State Circuits Conf. (ISSCC)*, February 2019, pp. 404-406.

[14] Y. Xiang et al., "Open DNN Box by Power Side-Channel Attack," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 11, pp. 2717-2721, Nov. 2020.

[15] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations", in *International Workshop on Information Hiding*, 1998.

[16] M. Guri, et. al.,"Gsmem: Data exfiltration from air-gapped computers over gsm frequencies", In *USENIX Security Symposium*, 2015.

[17] C. Shen, T. Liu, J. Huang and R. Tan, "When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient," in *IEEE Symposium on Security and Privacy (SP)*, pp. 1304-1317, 2021 .

[18] N. Sehatbakhsh, B. B. Yilmaz, A. Zajic and M. Prvulovic, "A New Side-Channel Vulnerability on Modern Computers by Exploiting Electromagnetic Emanations from the Power Management Unit," In *IEEE International Symposium on High Performance Computer Architecture (HPCA)*, pp. 123-138, 2020.

[19] Corentin Lavaud, et al. "Whispering devices: A survey on how side-channels lead to compromised information", *Journal Hardware and Systems Security*, Springer, 2021.

[20] David Oswald, *Implementation Attacks: From Theory to Practice*, PhD Thesis, 2013.

[21] E. Brier, et. al., *Correlation Power Analysis with a Leakage Model*, CHES'04, vol. 3156, pp. 16-29, 2004.

[22] Franois Durvaux and Marc Durvaux, *SCA-Pitaya: A Practical and Affordable Side-Channel Attack Setup for Power Leakage Based Evaluations*. Digit. Threat.: Res. Pract. 1, 1, Article 3 (March 2020).

[23] Young Jin Kang, Tae Yong Kim, Jung Bok Jo and Hoon Jae Lee, *An Experimental CPA Attack for Arduino Cryptographic Module and Analysis in Software-based CPA Countermeasures*, Int. Journal of Security and Its Applications, Vol. 8, No. 2, pp. 261-270, 2014.

[24] Hasindu Gamaarachchi and Harsha Ganegoda, *Power Analysis Based Side Channel Attack*, arXiv:1801.00932, 2018.

[25] Colin O'Flynn, *Power Analysis for Cheapskates*, the White Paper at BlackHat USA conference, 2013.