A Probe Placement Method for Efficient Electromagnetic Attacks

A Probe Placement Method for Efficient Electromagnetic Attacks

***Abstract*—Electromagnetic (EM) emissions have been explored as an effective means for non-invasive side-channel attacks. The leaked EM field from the memory bus when the data is loaded from the on-chip memory has received considerable attention in literature. Meanwhile, off-chip memory buses gradually become the new attack target due to the relative ease of access in the modern system in package technologies, such as 2.5-D integration where processing and memory chips are integrated, for example, on a silicon interposer. This paper, therefore, investigates EM snooping attacks on interposer-based off-chip memory buses. A gradient-search algorithm is proposed to locate fast (i.e. $O(N)$) the most efficient attack point. The effectiveness of the search algorithm and attack efficiency is evaluated on a 64-bit bus. It is demonstrated that at the optimal attack point, EM attacks can succeed with more than $10\times$ fewer traces, compared to placing the probe to sub-optimal locations.**

***Index Terms*—interposer, electromagnetic emission, side-channel attack, near-field probing, pearson correlation**

I. Introduction

A side channel is a physical communication channel which allows attackers to infer secret information from a system, for instance, power supply lines, EM leaks, timing or acoustic noise [1]. Among these side channels, the power side-channel attacks (SCAs) have greatly been explored, and are therefore regarded as the major threat to the security of integrated circuits (ICs) [2]. Compared to the semi-invasive characteristic of the power SCA, such as modifying or intervening with the circuits to measure power, the EM SCA is regarded as non-invasive and, hence, easier to launch an attack. Furthermore, EM SCAs utilize a probe to couple the EM field, and can attack the system faster than power SCAs [3].

The noise generated by the switching activity of the logic cells during the encryption process can also be leaked from an EM side channel. The fluctuations of the EM field can be received by near-field probing. By analyzing the spatial localized emanations, the EM emissions originating from the encryption modules rather than the non-encryption modules are mainly captured. Furthermore, there is another EM SCA called far-field EM attack. In this type of attack, the switching noise can also couple into the analog part of the chip through the substrate [4]. This noise can be amplified and transmitted by the analog wireless communication circuits along with the useful radio frequency. By intercepting it with a radio receiver, the attackers can recover the sensitive messages.

EM attacks on memory blocks on-chip have also been performed. In this case, the adversary can not physically access the internals of the memory circuit, and, thus, has to rely on EM emissions for extracting the desired information (e.g., secret key). However, EM emissions in this scenario are also produced from adjacent circuit blocks, hindering significantly the efficiency of an on-chip EM attack. On the other hand, the large physical size of the off-chip memory buses facilitates EM attacks as EM emissions from neighbouring components can be weaker due to the larger physical distance. Dayeol *et al.* [5] perform an off-chip side channel attack *MEMBUSTER* on the memory bus between the CPU and the off-chip DRAM. A Dual In-line Memory Module (DIMM) interposer, as stated in [5], inserted between the processor and the DRAM, captures the memory bus signals and finally sends the signals to an analyzer for the attack. However, with the development of new packaging solutions, the processor and memory chips can be integrated on the same substrate, which enables improved interconnections among these components [6]. To the best of our knowledge, no exploration has been performed to show how best to attack the interconnections implemented in such an interposer. A gradient-search algorithm [7], adapted in this paper, helps to determine the optimal probe position and retrieve the sensitive message on the memory bus with the minimal measurements to disclosure (MTD).

This paper is structured as follows. Preliminaries about the AES algorithm and EM correlation attack are presented in Section II and the investigated system is discussed in Section III. The algorithm used for the probe position search is described in Section IV. The simulation results are analyzed in Section V. Finally, conclusions are drawn in Section VI.

II. Preliminaries

In this section, a description of the targeted encryption algorithm (AES), the correlation based EM attack, and SNR, commonly used to evaluate information leakage, are introduced.

A. Advanced encryption standard

AES is the most commonly targeted algorithm in side-channel attacks due to its widespread application. It is a symmetric block cipher, which encrypts messages segmented into blocks [8]. The encryption is symmetric because the key used for decryption is the same as that used for the encryption.

When implemented for blocks of 128 bits and a 128-bit (or 256-bit) key, the algorithm normally has ten rounds of processing. Within each round processing module except for the last one, there is a combination of 4 processes: substitution, transposition, substitution, and XORing with the sub-key.

This work is funded by European Commission under the Horizon 2020 Framework Programme for Research and Innovation through the EuroExa project under Grant 754337.

B. Correlation based EM attack

Correlation based EM attacks use Pearson's correlation coefficient to recover the most probable key by collecting a sufficient number of EM traces [3]. By linking the measured EM traces with a leakage model, the correlation coefficients of the traces are calculated to extract the key. The Hamming Distance (HD) model is employed as the leakage model, which assumes that the number of transitions ($0 \rightarrow 1$ or $1 \rightarrow 0$) predicts the magnitude of EM field.

If AES encryption is repeated N times with known plaintexts and a fixed unknown key, the collected magnetic traces are denoted as $\mathcal{L} = \{l_1, ..., l_N\}$, where l_m $(m = 1, ..., N)$ is a magnetic trace generated by a certain plaintext. Each trace is a time series with s sampling points, $l_m = \{l_{m,1}, ..., l_{m,s}\}$. $\mathcal{F}$ is a function of an intermediate value χ, which depends on the plaintext p and the key k, denoted as $\mathcal{F} = \psi(\chi) = \psi(p, k)$. $\mathcal{F}$ is a subset of m-bit χ, whose value is the Hamming Weight of χ. The correlation between the traces $\mathcal{L}$ and the function $\mathcal{F}$ for each guessed key is calculated as

$$\rho = \frac{E\left[\left(\mathcal{F} - E\left(\mathcal{F}\right)\right)\left(\mathcal{L} - E\left(\mathcal{L}\right)\right)\right]}{\sqrt{D\left(\mathcal{F}\right) D\left(\mathcal{L}\right)}}, \tag{1}$$

where $E\left[\left(\mathcal{F} - E\left(\mathcal{F}\right)\right)\left(\mathcal{L} - E\left(\mathcal{L}\right)\right)\right]$ is the co-variance between them, and $D\left(\mathcal{F}\right)$, $D\left(\mathcal{L}\right)$ are, respectively, their individual variances. The position where the highest ρ appears is the best sub-key candidate.

C. Signal-to-noise ratio (SNR)

In side-channel attacks, SNR is characterized as an essential parameter to describe the leakage in side channels, which affects the attack capability. The greater the SNR, the fewer traces are needed to disclose the secret key [9]. In side-channel measurements, the SNR of the gathered traces is [9]

$$SNR = \frac{D\left(V_{data}\right)}{D\left(V_{noise}\right)}, \tag{2}$$

where $D\left(V_{data}\right)$, $D\left(V_{noise}\right)$ is the variance of coupled voltages originating from the useful data and noise, respectively.

III. System under EM attack

S-box is a critical non-linear operation of substitution of AES. It is typically implemented on hardware by complex logic gates or a look-up table (LUT). In 2.5-D ICs, to reduce the dynamic power of the encryption chip, a LUT based S-box can be implemented on a custom-designed off-chip read-only ROM [10], as shown in Fig. 1. The ROM receives the address and sends the substitution data through the memory bus routed with the redistribution layers (RDL) of the interposer.

In this paper, the register value is selected as χ, and the first round of AES is preferred to be attacked. This choice is because the intermediate result of AES is stored in χ at the end of each round. Thus, the sub-key used in the first round can be revealed by the EM leakage generated at the edge of the clock when χ updates its value. Meanwhile, χ is the memory

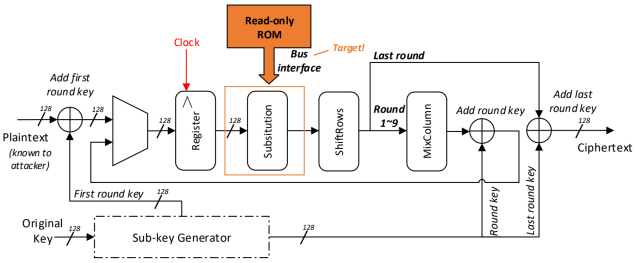


Fig. 1. Block diagram of AES encryption with ROM LUT based S-box.

address, being sent to ROM to find the correct swapped data. The leakage generated by the memory address (L_a) is

$$L_a = \psi(\chi) = \psi(PT, k_1) = HW(PT \oplus k_1), \tag{3}$$

where PT is the plaintext, k_1 is the sub-key byte used in the first round, and HW represents the Hamming Weight. Based on (1) and (3), the off-chip memory address can be snooped to recover the sensitive key.

IV. Gradient-search Algorithm

High spatial resolution can help maximize the coupling for near-field probing [11]. However, this high resolution leads to an extremely large space that must be searched to determine the best probe location for the attack. When the most effective probe location is determined, the target system is attacked fast. If the probe is positioned far from optimal places, MTD can require 4.3 times more traces or fail to attack [12]. Consequently, a gradient-search approach is introduced to facilitate the attack over brute-force search across the overall system area. SNR is used to evaluate the search efficiency of the algorithm in this paper.

A. Probe location algorithm

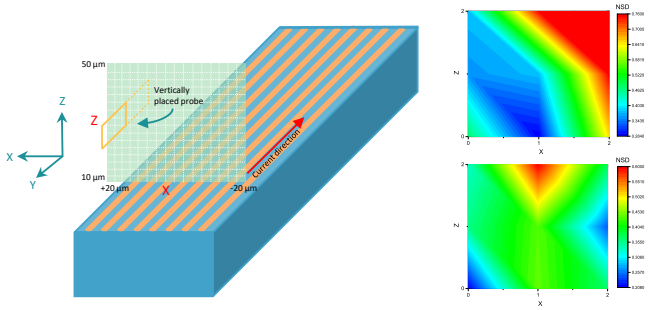
When the signal current flows along the bus lines, the amplitude of the magnetic emissions in different y positions has negligible differences due to the voltage drop. However, the EM field varies significantly along x and z directions. Consequently, the search space reduces from three dimensions (x,y,z) to two dimensions (x-z plane). In the search across the x-z plane, the normalized standard deviation (NSD) of the emissions is selected to evaluate information leakage.

The evaluation function f of the gradient-search algorithm is denoted as $f(x, y, z) = h_{NSD}$, where h_{NSD} is the value of normalized standard deviation at each point. The search starts from a random position (x_1,y_1,z_1), where NSD value is measured at the closest grid cell corresponding to this position. Next, NSD is measured, separately, in four adjacent grid cells to the location (x_1,y_1,z_1). The difference of measured NSD value between the tested cell and the current cell is regarded as the magnitude of the vector, and the direction of search is pointing from the tested cell to the current cell. The combination of the four vectors is the gradient. In that case, the next location to be measured is $(x_1 - \Delta \cdot \nabla f,\ y_1,\ z_1 - \Delta \cdot \nabla f)$, where Δ is the step size and ∇f is the calculated gradient. NSD can be measured in the new grid cell which is mapped at

the new position. In the next iteration, the monitored grid cell is shifted between adjacent grid cells until NSD value reaches the maximum or the edge of x-z plane.

B. Search area reduction

In this section, the 8-bit bus described in Fig. 2(a), is taken as an example to verify the quality of gradient-search algorithm. As shown in Fig. 2(a), the sweeping range for x-z plane is 40 μm × 40 μm and the probe is assumed to be placed vertically over the y-z plane of the bus, depicted in Fig. 2(b). When the x-z plane is divided into a 8 × 8 grid, the NSD map is shown in Fig. 3(a). MTD is normally inversely proportional to SNR^2, denoted as $MTD = \frac{k1}{SNR^2} = \frac{k2}{NSD^4}$ [13], where k_1 and k_2 are empirical values chosen to match the experiment result. In this 8-bit bus model, when NSD equals 1.112, MTD is 30, in that case, k_2 is taken as 45.87. As depicted in Fig. 3(b), as the NSD increases, the minimal number of traces needed for the EM attack decreases.



(a) (b)

Fig. 2. (a) Grid division in x-z plane where leakage measurements are performed, and (b) a rough scan (3 × 3) of NSD distribution in x-z plane when probe is placed vertically (above) and horizontally (below). In the maps, vertical orientation shows a more significant signal clutter than the other.

Different grid scales are used to verify the algorithm. As shown in Fig. 3(c), for a grid of N × N, the gradient-search algorithm can reduce the NSD measurements needed to reach minimal MTD from N^2 (brute-force measurements) to approximate N. Furthermore, for the 16×16 grid, the effect of step size Δ on the number of iterations is demonstrated in Fig. 3(d). If the step size is too small, for example one grid cell (2.5 μm), the search can be trapped at local minimum. If the step size is too large, for example 4 grid cells (10 μm), the search might miss the optimal location. Thus, given a reasonable step size, the algorithm can achieve a reduced search space over the exhaustive brute-force search.

V. Effectiveness of the Algorithm

The side view of the fabricated stacking structure of the 8-bit bus on an interposer is shown in Fig. 4(a) along with the geometry parameters. The data rate of the bus is 1 $Gbps$ and the sampling rate is set to 10 $Gbps$. In EM simulations, the probe is modeled as a single turn rectangle coil with 200 μm length and width equal to a quarter of the length, which exhibits the maximum NSD, and is placed vertically over the bus. The step size is set to 5 μm.

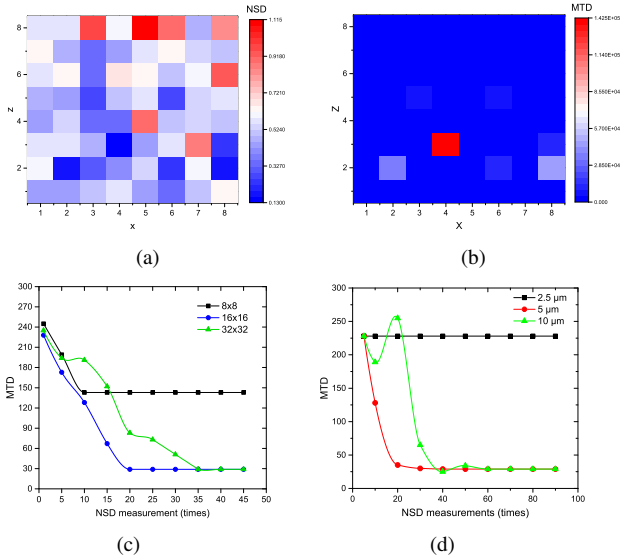


Fig. 3. (a) NSD map for an 8 × 8 scan, (b) Heatmap of MTD. Higher NSD means fewer traces are needed for a successful attack, (c) Gradient-search algorithm reduces the search time complexity from $O(N^2)$ to $O(N)$, and (d) Effect of step size on the convergence of the search.

Based on the gradient-search algorithm presented in Section IV-A, the optimal EM attack location for the interposer based 8-bit bus is found at $(-2.5, 700, 45)$, where the value for y-axis can be randomly chosen as close as possible to the near-end of the bus. When the probe is placed at this point, frequency sweeping is performed with $ANSYS\ HFSS$ [14]. The S-parameters generated at the frequency domain are exported from $HFSS$ and imported into $Spectre$ for the transient analysis in time domain. When the plaintext is swept from 0 to 255, 256 HD values are recorded in addition to the coupled voltage on the probe. When plotting all 256 peak voltage values for the 256 different plaintexts according to their HD values (0 to 8), as in Fig. 4(b), the captured EM trace demonstrates a very good linear correlation with the Hamming Distance that depends on the plaintext and the key.

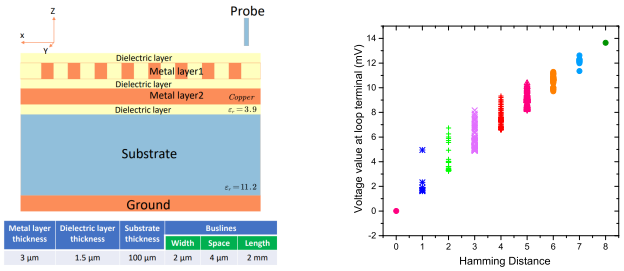
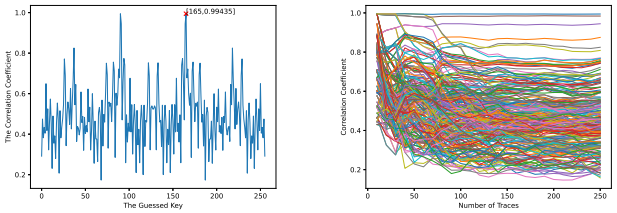


Fig. 4. (a) Stacking structure of the interposer-based bus, and (b) Correlation between the coupled voltage and HD at the optimal position.

In order to demonstrate that the key can be extracted with this method, the AES encryption process is repeated 256 times for each 8-bit plaintext value and an 8-bit fixed key. As shown in Fig. 5(a), among the correlation coefficients of

all the guessed keys (256 keys), the position with the highest correlation corresponds, indeed, to the right key (165). There is another similar peak obtained at the position where the symmetric key (90), called the "shadow key", appears. This is because the XOR operation is symmetric. Moreover, the number of traces needed for this successful attack is illustrated in Fig. 5(b), where each line represents the probability of each guessed key. The line that maintains the highest correlation compared to other lines is the correct key.



(a) (b)

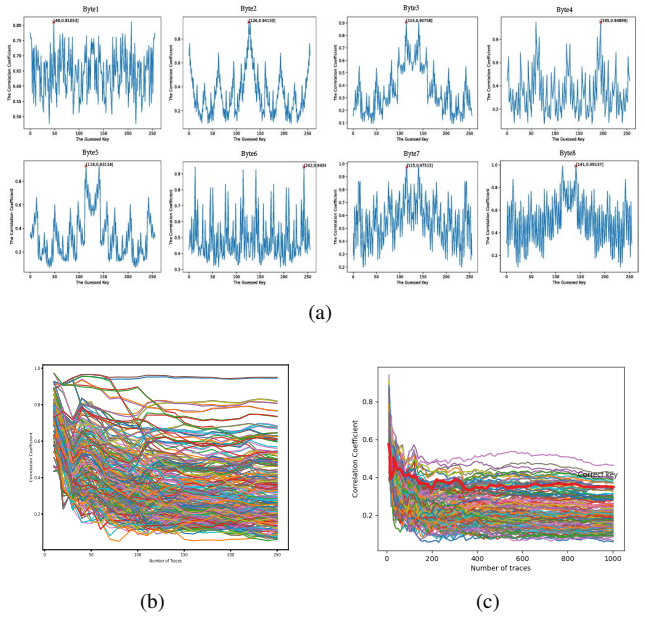
Fig. 5. Attack results of the 8-bit bus. (a) Correlation based EM attack uses a HD leakage model to attack the sub-key used in the first round of AES, and (b) the correct key is distinguished in less than 80 traces.

After the successful attack on 8-bit bus, the bus width is extended to 64 bits to verify the effectiveness of the algorithm in wider buses. If each byte of the 64-bit secret key can be attacked individually, the measurements for attacking the whole key can be highly reduced from $2^{64} = 1.84467 \times 10^{19}$ to $8 \times 2^8 = 2048$. This number can significantly increase (decrease) if the EM is sub-optimally (optimally) placed. Far from optimal probe locations completely fail to retrieve even a single sub-key. However, using the proposed algorithm, the correct 64-bit key is generated byte by byte with fewer than 256 traces by placing the EM probe at the optimal position as determined for attacking each byte. The results of the correlation attack for all the sub-keys are shown in Fig. 6(a).

Furthermore, the EM attack results on the subkey Byte4 for two different measurement configurations are shown in Fig. 6(b) and Fig. 6(c). When the probe is placed at the optimum location, the sub-key can be efficiently recovered in less than 100 traces ($MTD = 70$), while at the non-optimal position, more than $10\times$ traces are recorded and yet the correct key (the thick line) fails to be detected.

VI. Conclusion

In this paper, a fast and efficient side-channel attack on an interposer-based off-chip memory bus is introduced. The core idea is to exploit high spatial EM field resolution to determine the best attack location quickly. An algorithm based on gradient-search is developed to provide a scanning strategy, which reduces the brute-force search of $N \times N$ space to N. NSD is preferred as the leakage evaluation, such that the attack hotspot can be precisely determined for EM attacks with considerably low MTD. For the off-chip 64-bit bus scenario, $10\times$ fewer traces are needed for sub-key attacks where the probe is placed at the hot-spot. The proposed search algorithm is scalable as it is shown to apply to different bus widths.



(a)

(b) (c)

Fig. 6. (a) Attack results of the 64-bit bus. Results of EM attack for subkey Byte4 at (b) the optimal position detected by gradient-search algorithm, and (c) 10 μm away from the hot-spot.

References

[1] S. François-Xavier, "Introduction to side-channel attacks," *Proceedings of Secure integrated circuits and systems conference*. pp. 27–42, December 2010.

[2] K. Paul, J. Jaffe, and B. Jun, "Differential power analysis," *Proceedings of Advances in Cryptology conference*, pp. 388–397, December 1999.

[3] A. Dakshi, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—channel (s)," *International workshop on cryptographic hardware and embedded systems*, pp. 29–45, August, 2002.

[4] C. Giovanni, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels: When electromagnetic side channels meet radio transceivers," *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 163–177, October 2018.

[5] L. Dayeol, D. Jung, I. T. Fang, C. C Tsai, and R. A. Popa. "An off-chip attack on hardware enclaves via the memory bus," *Proceedings of 29th USENIX Security Symposium (USENIX Security 20)*, 2020.

[6] V. F. Pavlidis, I. Savidis, and E. G. Friedman, *Three-Dimensional integrated circuit design*, 2nd Edition, Morgan Kaufmann Publishers, 2017.

[7] R. Sebastian, "An overview of gradient descent optimization algorithms," arXiv, preprint, September 2016.

[8] D. Joan and V. Rijmen, "AES proposal: Rijndael," 1999.

[9] O. Changhai, S. K. Lam, D. Sun, X. Zhou, K. Qiao, and Q. Wang, "SNR-Centric Power Trace Extractors for Side-Channel Attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Early Access, June 2020.

[10] T. Craig, M. Bhargava, and K. Mai, "Side-channel attack resistant ROM-based AES S-Box," *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 124–129, June 2010.

[11] S. Laurent, S. Guilley, and Y. Mathieu, "Electromagnetic radiations of fpgas: High spatial resolution cartography and attack on a cryptographic module," *ACM Transactions on Reconfigurable Technology and Systems*, Vol. 2, No. 1, pp. 1–24, March 2009.

[12] I. Vishnuvardhan and A. E. Yilmaz, "An adaptive acquisition approach to localize electromagnetic information leakage from cryptographic modules," *IEEE Texas Symposium on Wireless and Microwave Circuits and Systems*, pp. 11-6, Marh 2019.

[13] M. Stefan, "Hardware countermeasures against DPA–a statistical analysis of their effectiveness," *Proceedings of In Cryptographers' Track at the RSA Conference*, pp. 222–235, February 2004.

[14] https://www.ansys.com/products/electronics/ansys-hfss