Using the ANOVA F-Statistic to Rapidly Identify Near-Field Vulnerabilities of Cryptographic Modules

Vishnuvardhan V. Iyer[#1], Ali E. Yilmaz[#2]
[#]Department of Electrical and Computer Engineering, The University of Texas at Austin, USA
[1]vishnuv.iyer@utexas.edu, [2]ayilmaz@utexas.edu

***Abstract*—The analysis of variance (ANOVA) F-statistic is proposed as an indicator to accelerate the identification of near-field vulnerabilities of cryptographic modules to electromagnetic side-channel analysis (EM SCA) attacks. It is hypothesized that optimal measurement configurations that require collecting the fewest measurements to disclosure have high F-values; i.e., in these configurations, the measured signals exhibit high variability when the encryption changes and low variability when the encryption is repeated. The concept is demonstrated for an EM SCA attack to disclose the secret key used in an open-source implementation of the Advanced Encryption Standard (AES). It is shown that the F-statistic reduces the search space to identify optimal measurement configurations 6× to 17× depending on the probe height and orientation.**

***Keywords*—electromagnetic measurements, side-channel attacks, measurement uncertainty, electromagnetic interference.**

I. Introduction

Electromagnetic (EM) fields unintentionally emanated by embedded crypto-systems can be measured and statistically exploited to recover critical information about on-chip operations [1]-[3]. For example, the secret key used in the Advanced Encryption Standard (AES) algorithm was recovered in [2],[3] using automated near-field scanning systems similar to Fig. 1 to implement so-called side-channel analysis (SCA) attacks. Such EM SCA attacks collect large datasets from measurements of a device under test; in particular, they observe signals—sum of fields emanated by exploitable and un-correlated on- and off-chip sources and measurement noise—for many input plaintexts/output ciphertexts and correlate these using hypothetical leakage models to reveal the secret key.

Using high-resolution scans of the chip, EM SCA attacks can identify optimal configurations that require few measurements to disclose information [2],[3]. Uncertainties in such near-field measurements, however, can degrade correlations and increase the number of measurements needed to recover the key, potentially making the attacks infeasible. These measurement uncertainties may be attributed to variations in probe configurations, equipment sensitivity, cable-bending, drift, jitter, thermal noise, etc. [4]. Repeatability tests can be used to characterize various sources of uncertainty in a measurement setup and its environment [5]-[7]. Even if the measurements are well within the bandwidth and sensitivity range of test instruments and even if environmental variables such as temperature and vibration are controlled to vary only marginally, uncertainty arises from the measured quantity itself; e.g., the current drawn by on-chip logic blocks can vary when repeating the same operation.

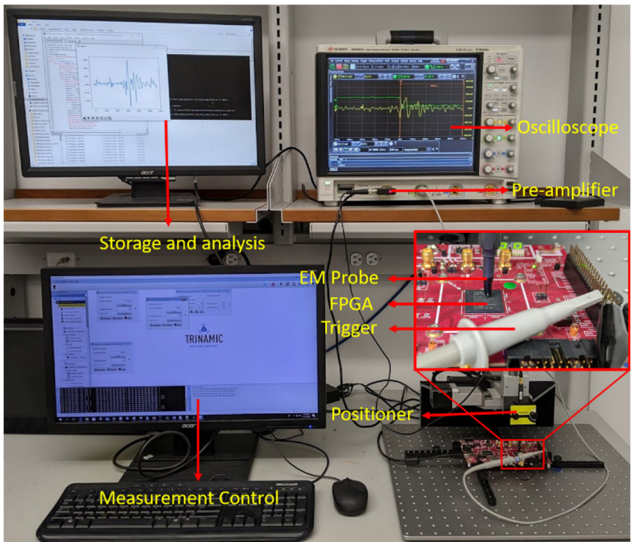

Fig. 1. An automated, high-fidelity EM measurement setup with separate measurement control and analysis units for near-field measurements.

The repeatability of near-field measurements for embedded crypto-systems can be quantified by computing the variance in observed fields for repeated encryptions. Such repeatability characterizations can identify probe configurations—such as transverse location, height, and orientation—that yield low-noise signals. Moreover, as shown in this article, when combined with configurations that yield signals exhibiting high variability with changing encryptions, they can indicate a higher likelihood of key recovery, potentially speeding up EM SCA attacks.

This article introduces an analysis of variance (ANOVA) Fischer statistic (F-statistic) indicator to rapidly identify effective probe configurations for EM SCA attacks. The ability of the proposed indicator to speedup EM SCA attacks is investigated by recovering the secret key from an FPGA implementation of AES-128 using various probes with different orientations, heights, and sizes.

II. Repeatability Characterizations Using ANOVA

A. Correlation-based EM SCA Attacks on AES

Information about the secret key used in AES leaks through fields emanated in its physical implementations because of data-dependent switching in CMOS logic during AES operations [1]. Such switching can be categorized using hypothetical leakage models to correlate observed fields

generated during encryption to bit transitions from observed inputs to intermediate values (or from intermediate values to observed outputs). Here, the Hamming-distance model is used: The AES output ciphertext and probed signals are observed for N_e encryptions, the previous state of the ciphertext is generated for each encryption by guessing the encryption key, and the guessed value maximizing the correlation of observed signals to Hamming distances (between the output ciphertexts and their penultimate round values) is chosen as the correct key [3]. Since final round of operations in AES involves independent byte-wise transformations, each of the 16 key-bytes in the 128-bit AES key can be recovered separately.

The potency of such EM SCA attacks depends on the number of observed encryptions N_e, the probe configuration pc (which includes the probe's transverse location l, height h, orientation o), and the measurement instant t. Assume that a near-field probe collects $N_x N_y N_h N_o$ different signals $V_e^{pc,t}$ for each encryption e above an $l_x \times l_y$ chip at transverse locations

$$\left(x_{n_x}, y_{n_y}\right) = \left(\frac{n_x l_x}{N_x - 1}, \frac{n_y l_y}{N_y - 1}\right), \text{for } n_{x/y} = 0,1,\cdots, N_{x/y} - 1. \quad (1)$$

Let these be stored in an array $\mathbf{V}^{pc,t} = [V_1^{pc,t}, V_2^{pc,t}, \cdots, V_{N_e}^{pc,t}]$.

Elements in $\mathbf{V}^{pc,t}$ can be expressed as a sum of exploitable signals in array $\mathbf{T}^{pc,t}$, uncorrelated algorithmic noise in $\mathbf{B}^{pc,t}$, and measurement noise in $\mathbf{N}^{pc,t}$. For each key-byte b, if $\mathbf{H}^b = [H_1^b, H_2^b, \cdots, H_{N_e}^b]$ denotes the Hamming distances, the observed correlation coefficient $\rho_{V,H}^{b,pc,t}$ can be decomposed as [1]

$$\rho_{V,H}^{b,pc,t} = \underbrace{\frac{\mathrm{Cov}(\mathbf{T}^{pc,t}, \mathbf{H}^b)}{\sqrt{\mathrm{Var}(\mathbf{T}^{pc,t}) \times \mathrm{Var}(\mathbf{H}^b)}}}_{\rho_{T,H}^{b,pc,t}} \times \frac{1}{\sqrt{1 + \underbrace{\frac{\mathrm{Var}(\mathbf{B}^{pc,t})}{\mathrm{Var}(\mathbf{T}^{pc,t})}}_{1/F_B^{pc,t}} + \underbrace{\frac{\mathrm{Var}(\mathbf{N}^{pc,t})}{\mathrm{Var}(\mathbf{T}^{pc,t})}}_{1/F_N^{pc,t}}}} \quad (2)$$

The decomposition shows that the ideal correlation coefficient $\rho_{T,H}^{b,pc,t}$ is degraded by algorithmic and measurement noise; this degradation is quantified by $F_B^{pc,t}$ and $F_N^{pc,t}$, which are the ratios of signal variability to algorithmic and measurement noise, respectively. The F-statistic $F_B^{pc,t}$ is often used to evaluate countermeasures that utilize obfuscating operations, i.e., measures that increase algorithmic noise, against SCA attacks [2]. The F-statistic $F_N^{pc,t}$ can similarly be used to evaluate information leakage in the presence of measurement uncertainty: Probe configurations that maximize $F_N^{pc,t}$ can potentially measure highly correlated signals, requiring fewer encryptions to be observed for key recovery, subject to other terms in (2).

B. Estimating $F_N^{pc,t}$ with Pre-characterization

The F-statistic $F_N^{pc,t}$, which cannot be observed directly, is estimated by adopting the ANOVA methodology used to estimate $F_B^{pc,t}$ in [2]: N_p different pre-characterization encryptions are observed and each encryption is repeated N_r times. Ideally, $F_N^{pc,t}$ should be found byte-wise by only varying the target byte and fixing the remaining 15 bytes in output ciphertexts. Instead, to reduce measurement costs, a single pre-characterization is performed by varying all 16 output bytes. One way to ensure inter-encryption independence and maximize variation in observed signals, is to enforce that none

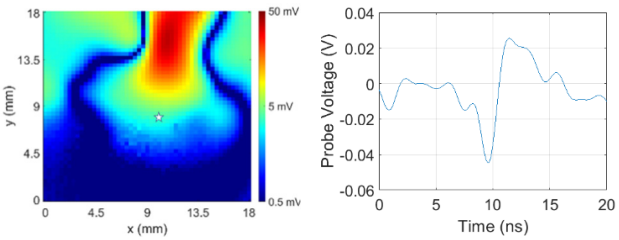

Fig. 2. Spatio-temporal distribution of measured signals for an encryption. The spatial map was plotted at time 10 ns and the time plot was recorded at the position (9, 9) mm. The star at (9.7, 8) mm marks the optimal location for recovering the key-byte $b = 1$ [3].

of the 16 byte values repeat among the N_p encryptions. For each encryption p, the sample mean $\bar{x}_p^{pc,t}$, variance $s_p^{pc,t}$, and standard deviation $sd_p^{pc,t}$ are found using the N_r samples. In this article, the mean value of the sample standard deviation $\overline{sd}^{pc,t}$, computed across N_p encryptions, is used to quantify measurement repeatability [7] (standard deviation is related inversely to repeatability) and the F-statistic $F_N^{pc,t}$ is used to quantify the effect of repeatability on observed information leakage. The F-statistic $F_N^{pc,t}$ can be estimated as a ratio of inter-group and intra-group variability, scaled by the number of repetitions [1], [2]:

$$F_N^{pc,t} \approx \frac{N_r \times \mathrm{Var}(\bar{x}_1^{pc,t}, \bar{x}_2^{pc,t}, \ldots, \bar{x}_{N_p}^{pc,t})}{\mathrm{Mean}(s_1^{pc,t}, s_2^{pc,t}, \ldots, s_{N_p}^{pc,t})} \quad (3)$$

High $F_N^{pc,t}$ is a necessary but not sufficient condition for key recovery, since the correlation coefficients also depend on $F_B^{pc,t}$ and the leakage model used. Furthermore, configurations with high $F_N^{pc,t}$ can be sensitive to any of the 16 bytes, and all such configurations must be analysed for byte-wise key recovery.

C. Using $F_N^{pc,t}$ as a Leakage Indicator

A critical threshold $F_{N,c}$ can be set for $F_N^{pc,t}$ to indicate high likelihood of key recovery, isolate regions of interest for correlation analysis, and significantly reduce measurement and analysis costs. Let

$$Indicator^{pc} = \begin{cases} 0 & \text{if } \max_t F_N^{pc,t} < F_{N,c} \\ 1 & \text{if } \max_t F_N^{pc,t} \geq F_{N,c} \end{cases} \quad (4)$$

In this article, the threshold is chosen from F-distributions and depends on N_r, N_p, and the confidence ratio selected. If the probe's orientation o and height above the chip surface h are fixed, the indicator can reduce the search-space of probe transverse locations l by a factor of

$$N_{\mathrm{red}}^{h,o} = \frac{N_x N_y}{\sum_l Indicator^{pc}} \quad (5)$$

The proposed indicator is more useful for noisy measurement setups where fewer locations have high $F_N^{pc,t}$.

III. Measurement Results

The fields emanated by an open-source implementation of AES-128 [8] on a Xilinx Artix-7 FPGA (18 mm × 18 mm size) were measured using a 1-mm diameter H-field probe from

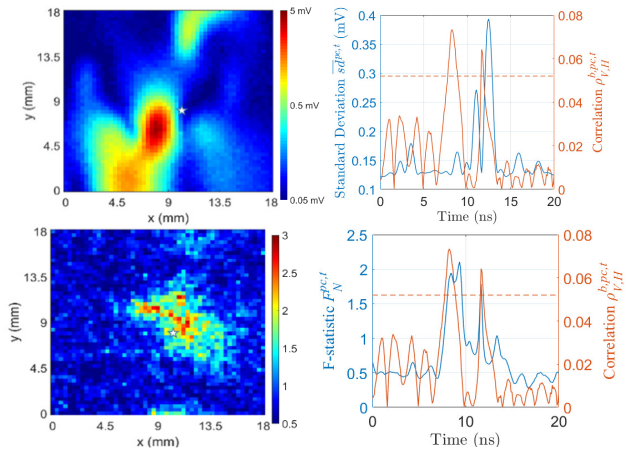

Fig. 3. Spatial maps at time 8 ns and time plots of $\overline{sd}^{pc,t}$ (top) and $F_N^{pc,t}$ (bottom) at the optimal location for recovering the key-byte $b = 1$. Key bytes can be recovered where the correlation crosses a null hypothesis threshold (dashed red line) [3]. The optimal location exhibited small $\overline{sd}^{pc,t}$ (high repeatability) and large $F_N^{pc,t}$.

Langer in conjunction with a 30-dB amplifier. A Keysight DSOS054A oscilloscope was used for experiments due to its high sampling rate (20 GS/s) and sufficient storage and analysis capabilities. The probe was positioned using Riscure's EM probe station which has a resolution of 2.5 µm. The chip operated at a clock speed of 50 MHz. To characterize repeatability, measurements for $N_\mathrm{p} = 20$ encryptions were repeated $N_\mathrm{r} = 50$ times and signals were recorded at $N_\mathrm{x} \times N_\mathrm{y} = 51 \times 51$ locations; the total acquisition time needed was ~ 4 hrs per probe configuration.

Fig. 2 shows a space-time map of measured signals for an *x*-oriented, 1-mm diameter probe at height 0.5 mm and marks

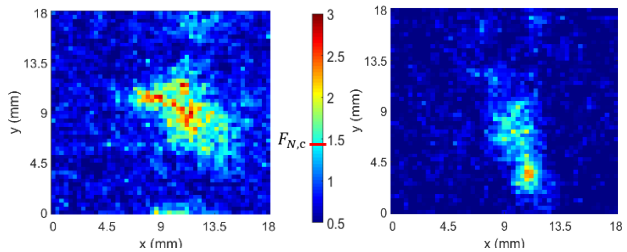

Fig. 4. Spatial maps of $F_N^{pc,t}$ at 8 ns when the 1-mm probe was 0.5 mm above the chip surface and *x*- (left) or *y*- (right) oriented. The F-statistic depended strongly on the probe orientation.

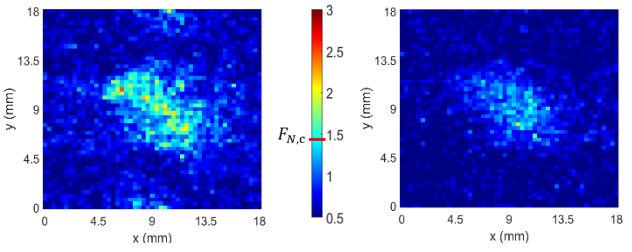

Fig. 5. The spatial maps of $F_N^{pc,t}$ as the *x*-oriented 1-mm probe was raised to 1 mm (left) and 2 mm (right) above the chip surface. The F-statistic indicated that the number of positions where the EM SCA attack can reveal the key reduced significantly with probe distance.

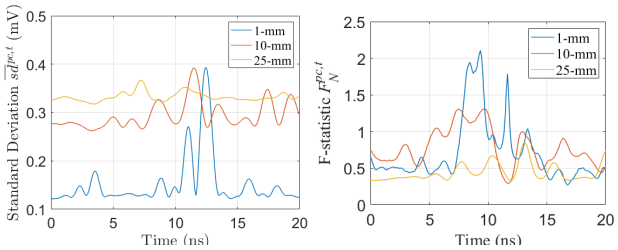

Fig. 6. Standard deviation and F-statistic for three probes of different sizes centred at (9.7, 8) mm. Measurements with the smallest probe had higher repeatability and were more likely to reveal the key between 7-12 ns.

the optimal location to reveal the first key-byte that was identified in [3]. Fig. 3 shows space-time maps of $F_N^{pc,t}$ and $\overline{sd}^{pc,t}$ for the same probe configuration. It was observed that the time instant with maximum correlation (~8 ns) was different from the time instant with maximum absolute value of the observed signal (~10 ns). This is because information leakage depends on the variations in observed signals with changing encryptions, rather than on the strength of the observed signal. In the following, the 1-mm probe was used to quantify $F_N^{pc,t}$ and $N_\mathrm{red}^{h,o}$ for different probe orientations and heights; measurement repeatability was also studied for larger probes of size 10-mm and 25-mm. To calculate $N_\mathrm{red}^{h,o}$, a 90% confidence ratio was used to set $F_{N,c} = 1.44$; the choice of confidence ratio depends inversely on the security of the design.

Fig. 4 shows that configurations with higher F-statistics can be isolated and the *x*-orientation of the probe showed more potentially leaking locations compared to *y*-orientation; here, $N_\mathrm{red}^{0.5\ \mathrm{mm,x}} \approx 6.5$ and $N_\mathrm{red}^{0.5\ \mathrm{mm,y}} \approx 10.2$. Fig. 5 shows results for different probe heights, where the search space was reduced by a factor of $N_\mathrm{red}^{0.5\ \mathrm{mm,x}} \approx 6.5$, $N_\mathrm{red}^{1\ \mathrm{mm,x}} \approx 8$, and $N_\mathrm{red}^{2\ \mathrm{mm,x}} \approx 17$. This is because signals from information-leaking components are attenuated and obfuscated with distance; repeatability suffers, and fewer locations are feasible for mounting an attack. Fig. 6 compares $\overline{sd}^{pc,t}$ and $F_N^{pc,t}$ for different probe sizes at a leaking location ($N_\mathrm{red}^{h,o}$ was not computed for larger probes because coarse-grained attacks with such probes are typically limited to single-location measurements). Because larger probes average fields spatially, they have a higher noise floor and stronger emanations from uncorrelated components mask any inter-encryption variance, which further degrades $F_N^{pc,t}$.

IV. Conclusion

The article characterized measurement repeatability of EM SCA attacks and introduced an F-statistic indicator to identify effective near-field measurement configurations for extracting information from cryptographic modules. By isolating configurations more sensitive to the key byte and less sensitive to measurement noise, the proposed indicator reduced the search space of potentially leaking probe configurations. The experiments on the AES implementation showed significant reductions in the search space for noisy measurement setups, thus helping designers rapidly test, validate, and rectify security vulnerabilities due to unintentional EM emissions.

REFERENCES

[1] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks*, Springer Science & Business Media, 2008.

[2] F. Unterstein, *et al.* "Dissecting leakage resilient prfs with multivariate localized em attacks," in *Proc. COSADE*, Jul. 2017.

[3] V. V. Iyer and A. E. Yilmaz, "An adaptive acquisition approach to localize electromagnetic information leakage from cryptographic modules," in *Proc. IEEE Texas Wireless Symp.*, Mar. 2019.

[4] K. A. Remley, *et al.* "Millimeter-wave modulated-signal and error-cector-magnitude measurement with uncertainty," *IEEE Trans. Microw. Theory Tech.*, vol. 63, no. 5, pp. 1710-1720, May 2015.

[5] B. F. Jamroz, *et al.* "Accurate monte carlo uncertainty analysis for multiple measurements of microwave systems," in *Proc. IEEE MTT-S Int. Microw. Symp.*, Jun. 2016.

[6] C. Fager and K. Andersson, "Improvement of oscilloscope-based RF measurements by statistical averaging techniques," in *Proc. IEEE MTT-S Int. Microw. Symp.,*Jun. 2006.

[7] S. Gu, K. Haddadi, A. El Fellahi, G. Dambrine and T. Lasri, "Measurement accuracy and repeatability in near-field scanning microwave microscopy," in *Proc. IEEE I2MTC*, May 2015.

[8] ChipWhisperer, Github Repository [online], available: https://github.com/newaetech/chipwhisperer