The Thesis Committee for Vishnuvardhan V Iyer
Certifies that this is the approved version of the following Thesis:

An Adaptive Measurement Protocol for Fine-Grained Electromagnetic Side-Channel Analysis of Cryptographic Modules

APPROVED BY
SUPERVISING COMMITTEE:

Ali Yilmaz, Supervisor

Mohit Tiwari

An Adaptive Measurement Protocol for Fine-Grained Electromagnetic Side-Channel Analysis of Cryptographic Modules

by

Vishnuvardhan Venkatramani Iyer

Thesis

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE IN ENGINEERING

The University of Texas at Austin

August 2019

Abstract

An Adaptive Measurement Protocol for Fine-Grained Electromagnetic Side-Channel Analysis of Cryptographic Modules

Vishnuvardhan Venkatramani Iyer, MSE

The University of Texas at Austin, 2019

Supervisor: Ali Yilmaz

An adaptive measurement protocol is presented to increase effectiveness of fine-grained electromagnetic side-channel analysis (EM SCA) attacks that attempt to extract the information that is unintentionally leaked from physical implementations of cryptographic modules. Because measured fields vary with probe parameters as well as the data being encrypted, identifying the optimal configurations requires searching among a large number of possible configurations. The proposed protocol is a multi-step acquisition that corresponds to a greedy search in a 4-D configuration space consisting of probe's on-chip coordinates, orientation, and number of signals acquired. This 4-D space can be extended to a 6-D space by repeating the protocol for different probe sizes and heights. This approach is presented as an alternative to current fine-grained EM SCA techniques that perform exhaustive full-chip scans to isolate information leaking locations. To demonstrate the feasibility of the approach, the protocol is tested by performing EM SCA attacks for different configurations and identifying the best attack configuration for two realizations of the advanced encryption standard (AES), subject to the precision of the measurement equipment. It is found that the protocol requires ~20× to ~25× less acquisition time compared to an exhaustive search for the optimal attack configuration.

Table of Contents

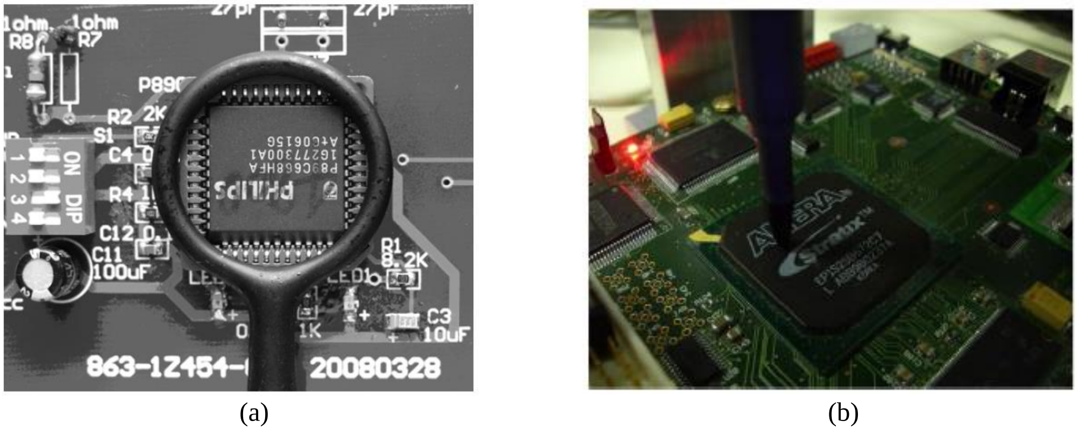
List of Tables

List of Figures

Chapter 1: Introduction

Physical implementations of cryptographic algorithms are prone to unintentional information leakage through observations of their EM emanations, dynamic power consumption, heat, vibrations, etc. In computer security, these are referred to as side channels; throughout this thesis, the analysis of side-channel signals to recover information is called a side-channel analysis (SCA) attack. The vulnerability of mathematically robust cryptographic algorithms to SCA attacks has been repeatedly demonstrated in the last two decades [1]-[6].

This thesis focuses on EM SCA attacks that are based on observing and analyzing EM emanations from cryptographic chips, which are closely related to power SCA attacks that monitor and analyze their power consumption. While the source of information leakage through both power and EM side channels is the data-dependent switching of



(a) (b)

Figure 1: (a) Coarse-grained attack on a microcontroller running Advanced Encryption Standard (AES) [7]. (b) fine-grained attack on an FPGA running Data Encryption Standard (DES) [4].

transistors in the CMOS logic [5], [6], the relative vulnerability of a chip to either type of attack depends on a large number of factors, including the measurement equipment, the chip's environment, and the availability of external connections. In general, near-field EM emanations provide an effective, non-invasive avenue to recover critical information from a chip and are difficult to counter without incurring significant overheads. This is partly because the location of on-chip leakages can be isolated and confounding signals from other sources be avoided by using EM probes. Moreover, the speed and potency of the EM SCA attacks can be increased by using scanning probes that automatically search for highly vulnerable configurations as in this thesis or by placing multiple sensors near the chip. The lack of direct sensor contact with the chip also complicates implementations of countermeasures and calls for novel countermeasures. For example, [8] proposed to integrate LC oscillators onto cryptographic chip designs and detect the presence of a nearby EM probe by the shifts in oscillation frequencies. This approach relies on inductive coupling between the probe and the oscillator coils, which can be rather weak depending on the probe orientation and size; e.g., the experiments in [8] could detect the probe only when it was less than 100 μm away from the die.

In contrast, power SCA attacks, which are more common in the literature [6], [11], are cheaper to implement and can be more effective (requiring fewer observations), especially when there is high information content in the observed signals, or equivalently, when the signal-to-noise-ratio (SNR) is high; e.g., when the target chip is dedicated to performing encryption operations and implements no countermeasures such as masking [9], [10] or hiding [11], [12] to obfuscate its power usage profile. Yet, power SCA attacks can be more easily countered and lose effectiveness while EM SCA attacks remain immune; e.g., when the encryption block is integrated in a chip with other modules that also consume power or if the chip's power usage is intentionally obfuscated. While both attack modalities are discussed and contrasted in this thesis, its main contribution is to increase the effectiveness of EM SCA attacks.

1.1 Granularity of EM SCA Attacks

Based on the type/amount/resolution of recovered information, EM SCA attacks can be grouped into two categories:

Coarse-grained EM SCA attacks aim to recover the minimal amount of information necessary to neutralize the cryptographic protection (e.g., a secret key); they generally use larger probes, typically hand-held or fixed at a single position [7], [13], [14]. The probe dimensions in such attacks are generally comparable to the chip's area such as the case in Fig. 1(a); occasionally, smaller probes are used [14]. Such EM SCA attacks are generally cheaper to implement and are similar to power SCA attacks as the signals detected by larger probes are a large aggregate of fields emanated from many sources distributed around the chip. As such, when the source of leakage is a small block of cells on a chip performing a critical computation, the information carrying signals emanated from such blocks can be below the sensor's detection threshold because of two reasons: (i) the generated fields can be small in magnitude and (ii) sources other than the blocks of interest will contribute uncorrelated noise signals to the analysis. As a result, a large, potentially infeasible, number of observations may have to be taken in order to extract the information within the noisy signal. Even when coarse-grained EM SCA attacks can neutralize cryptography; they provide little ability to reduce the costs of future attacks, e.g., by spatially localizing information leakage.

In contrast, *fine-grained EM SCA attacks* can not only neutralize cryptography, they provide additional information (such as best probe locations) that enable the marginal cost of measurements needed for future attacks on similar implementations to be reduced. They generally use smaller probes as shown in Fig. 1(b) to identify and isolate vulnerable locations [4], [15] especially when information is leaking through logic blocks in fixed locations rather than distributed sources. On the one hand, they may require far few measurements than alternatives when the probes are in the vicinity of such locations; on the other hand, when the probes are far away from these locations, they may become even less effective than coarse-grained EM SCA attacks because the EM fields emanated from relevant sources decay rapidly with distance, reducing the SNR. Although fine-grained EM SCA attacks can re-use best measurement configurations in future attacks and amortize the costs over multiple EM SCA attacks, identifying such configurations in the first place can require a prohibitively large number of measurements.

While a number of countermeasures can be deployed against EM SCA attacks, their effectiveness differ against the two categories of EM SCA attacks. Countermeasures for coarse-grained EM SCA attacks that modify aggregate signal values, such as masking [15], may not be able to withstand fine-grained EM SCA attacks; conversely, countermeasures for fine-grained EM SCA attacks, such as spatially randomized dataflow [16], may fail to defend against coarse-grained EM SCA attacks. In general, countermeasures for fine-grained EM SCA attacks are more difficult to implement and add major overheads to the design.

This thesis focuses on fine-grained EM SCA attacks. It presents a protocol to reduce the number of measurements needed for fine-grained EM SCA attacks; experiments on chips implementing the Advanced Encryption Standard (AES) algorithm achieve a reduction of ~20× to ~25× in measurement time. The algorithm also achieves a reduction of ~30× in total memory required for data storage. Although the proposed measurement protocol increases the effectiveness of fine-grained EM SCA attacks, the same protocol and the detailed explanations in this thesis can also be used to design better countermeasures against fine-grained EM SCA attacks or, at least, more rapidly test the effectiveness of existing countermeasures.

The thesis is divided into four chapters. Chapter 2 reviews AES and its vulnerability to various SCA attacks; it also presents the SCA attack flow and the instruments used to affect fine-grained EM SCA attacks in later chapters. Chapter 3 discusses the variation in information leakage with different parameters and presents a protocol to search for optimal attack configurations as a combination of these parameters. Chapter 4 details the procedure for one experiment based on the proposed protocol along with an analysis of costs and trade-offs. Chapter 5 presents experiments which cover a wide range of parameters and concludes by providing the ideal attack configurations for two target chips based on these experiments. Finally, Chapter 6 concludes with a summary of results and contribution of this thesis along with future work.

Chapter 2: Background

This chapter presents an overview of the AES algorithm, the principles of EM SCA attacks for recovering secret information, and the terminology that is used throughout the thesis. Section 2.1 details the operation of AES and its vulnerabilities to SCA attacks. Section 2.2 details an EM SCA attack that can recover the AES secret key by statistically analyzing observations of the ciphertext and the near-field EM emanations. Section 2.3 presents a binary search algorithm to reduce computation time for the statistical analysis needed to enable adaptive EM SCA attacks. Section 2.4 describes the equipment used for the experiments presented in this thesis.

2.1 The Advanced Encryption Standard

AES [17] is one of the most commonly used algorithms for symmetric cryptographic operations (encryption and decryption have the same key) in hardware

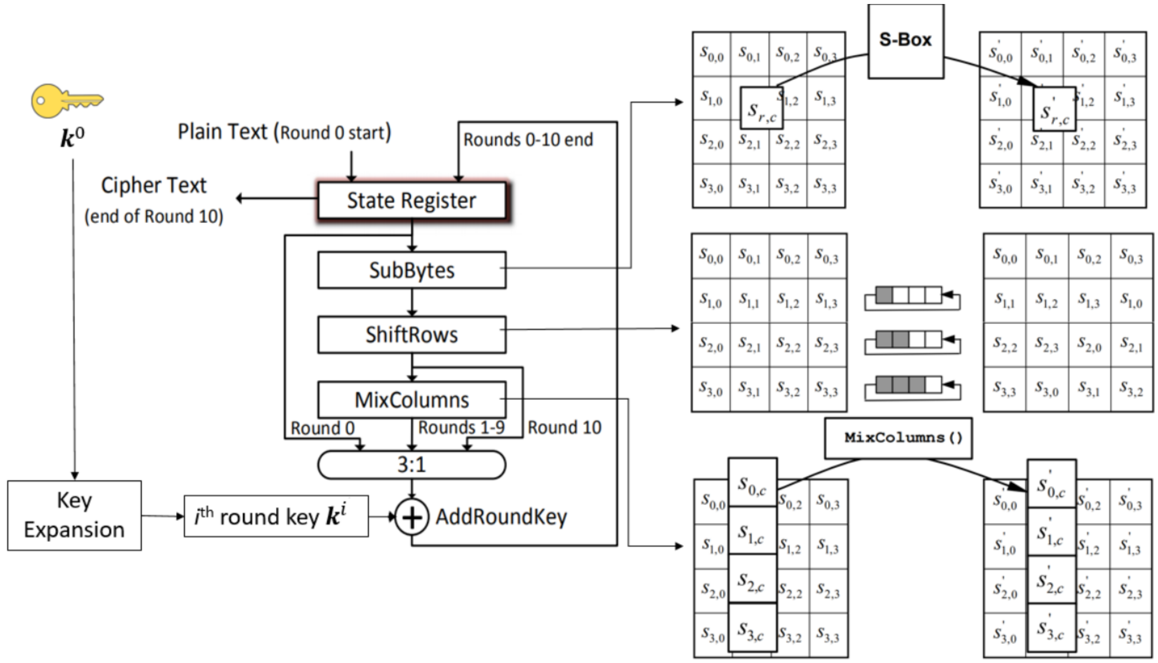


Figure 2: Flowchart of the AES algorithm adopted from [19].

security. It was established in 2001 by National Institute of Standards and Technology (NIST) [18]. The algorithm performs transformation operations on a given input (the "plaintext") to generate an output (the "ciphertext") using a secret key. There are 3 variants (AES-128, AES-192, AES-256) that use different length keys. All experiments in this thesis were performed on the 128-bit version of AES, where the key, plaintext, and ciphertext are 128 bits; the findings can be generalized to the more complex AES variants.

The AES-128 algorithm requires 11 rounds of transformations to generate the ciphertext. The algorithm splits the input plaintext into 16 bytes, reshapes these bytes into a 4 × 4 matrix on which it performs various transformations. Each element in the matrix is labeled as $S_{r,c}$ before transformation and $S'_{r,c}$ after transformation, where r is the row and c is the column index. The flowchart of AES-128 algorithm and a pictorial description of its transformations are shown in Fig. 2. Every round of AES uses a separate key; these are derived from the original secret key using Rijndael's key schedule [17] that involve the following steps.

- Split the original 16-byte secret key $\mathbf{k}^0 = [k^{0,1}, k^{0,2}, \dots, k^{0,16}]$ to four 32-bit words $\mathbf{w}^0$ to $\mathbf{w}^3$, where $\mathbf{w}^0 = [k^{0,1}, k^{0,2}, k^{0,3}, k^{0,4}]$, $\mathbf{w}^1 = [k^{0,5}, k^{0,6}, k^{0,7}, k^{0,8}]$, and so on. Since there are 11 rounds in the AES-128 algorithm (including round 0), a total of 44 words are generated in the key expansion. For the ith round, the 128-bit key $\mathbf{k}^i$ will consist of the words $\mathbf{w}^{4i}$ to $\mathbf{w}^{4i+3}$, where $0 \leq i \leq 10$.
- To derive the i+1th round's key $\mathbf{k}^{i+1}$ from the ith round's key $\mathbf{k}^i$, perform the following operations
  - ○ $\mathbf{w}^{4i+4} = g(\mathbf{w}^{4i+3}) \oplus \mathbf{w}^{4i}$; $\mathbf{w}^{4i+5} = \mathbf{w}^{4i+4} \oplus \mathbf{w}^{4i+1}$; $\mathbf{w}^{4i+6} = \mathbf{w}^{4i+5} \oplus \mathbf{w}^{4i+2}$; $\mathbf{w}^{4i+7} = \mathbf{w}^{4i+6} \oplus \mathbf{w}^{4i+3}$,

  where $\oplus$ is the XOR operator.
- The $g(\mathbf{w})$ function performs 3 steps
  - ○ Left circular rotate by one byte.

- Byte substitute each byte in the word using a 16×16 lookup table referred to as the substitution box or the S-box[1]. The S-box for AES is generated by first identifying multiplicative inverse of the input over Rijndael's Galois Field [17] and then using a fixed affine transform. The standard S-box generated for AES[2] [17] is shown in Fig. 3.
- XOR the word generated from the result of the S-box with a round constant *Rcon*[i] = (*RC*[*i*],00_{16},00_{16},00_{16}), which changes the first byte of the word. Here, *RC* follows the recursion *RC*[*i*] = 02_{16} × *RC*[*i* − 1] and *RC*[1] = 01_{16}.

Once all the keys $\mathbf{k}^0, \mathbf{k}^1, \cdots, \mathbf{k}^{10}$ are generated, the AES encryption can be performed. In the first step (round 0) of AES, the plaintext is loaded to the state register; this is followed by a bitwise XOR of the plaintext and the original secret key (Fig. 2). For the subsequent 9 rounds, four operations are performed:

- SubBytes – Each byte in the matrix is replaced by another byte using S-boxes for substitution. There are 16 S-boxes used for encryption operations in the AES implementation used in this thesis; each S-box is used to process one byte in parallel/in the same clock cycle. This step makes the algorithm non-linear, i.e., there is no algebraic relation between the ciphertext and the plaintext.
- ShiftRows – Each row of the 4×4 matrix undergoes a cyclic shift with a fixed offset. The first row does not shift, the second row shifts left by one position, the third row by two positions, and the fourth row by three positions.
- MixColumns – Byte entries of each column are mixed using a linear transformation. The resulting output column is a product of the input column and a fixed polynomial. ShiftRows and MixColumns provide diffusion to the cipher, i.e, they 'misplace' data in the matrix while the SubBytes step 'replaces' data in the matrix[3].

[1] S-boxes are generally used in cryptography for replacing data in the cipher and strengthening encryption.

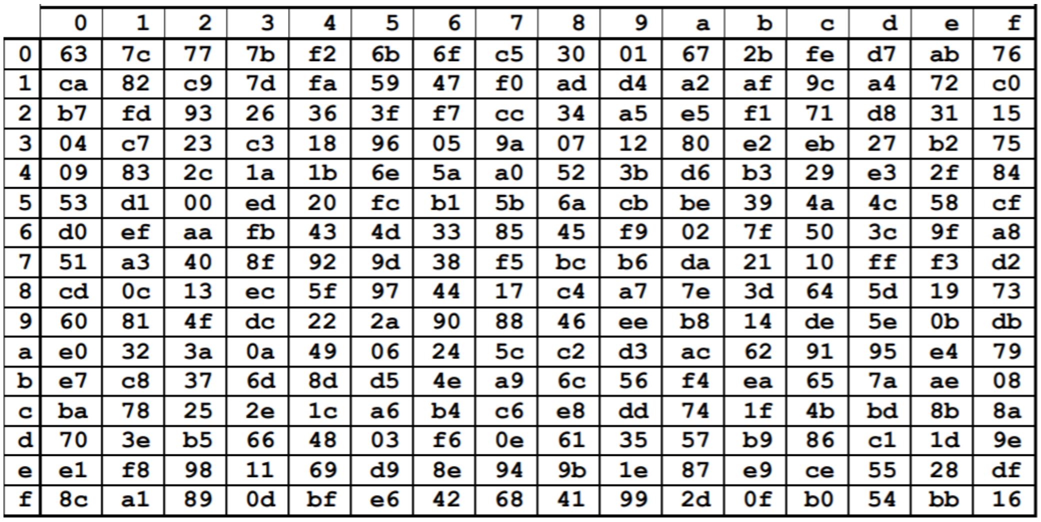
[2] Custom S-boxes may be generated by modifying affine transforms.

[3] In cryptographic terms, 'misplacing' shuffles the existing data while 'replacing' substitutes existing data.

- AddRoundKey – Bitwise XOR operation are performed between the key generated by the key expansion for that round and output from the MixColumns stage.

The final step (round 10) performs SubBytes, ShiftRows, and AddRoundKey operations and skips the MixColumns operation. After the final round, the ciphertext is available in the state register from which it is read out and replaced by the next plaintext. Attackers are assumed to have access to the ciphertexts and aim to extract the plaintexts.

A well-known vulnerability of AES is the data-dependency of side-channel signals during the last round; as discussed in the next section, SCA attacks can exploit this vulnerability to recover the final key $\mathbf{k}^{10}$. Using inverse operations of the key schedule, the first key $\mathbf{k}^{0}$, which is also the key used for decryption, can be recovered from $\mathbf{k}^{10}$. Therefore, all the observed ciphertexts can be decrypted to extract the protected plaintexts.



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 3: The standard S-box used in AES-128 [17] is a 16 × 16 lookup table. To replace the byte $1b_{16}$, the byte at row 1 and column b (the byte af_{16}) is selected.

2.2 SIDE-CHANNEL ANALYSIS ATTACK MECHANISM

SCA attacks extract keys by establishing statistical relations between the observed output of the encryption and measured physical signals (henceforth referred to as traces) using a hypothetical model [19]. Correlation-based attacks typically use one of three models [11]: Zero Value[4], Hamming Weight[5], and Hamming Distance[6] models. The Zero Value model assumes the power consumption for evaluating '0' valued data is less than that for other data values. The Hamming Weight model assumes that circuits evaluating more '1's than '0's draw more power. The Hamming Distance model requires knowledge of the preceding and current state of a circuit; it evaluates the power based on the number of transitions between them. Hamming Distance between the outputs of the last two stages of AES represents switching in the CMOS logic, which can be tied to dynamic power consumption and emanated fields. Therefore, SCA attacks on AES performed in this thesis use the Hamming Distance model.

In the final round of AES, apart from the ShiftRows operation, the byte locations in the 4×4 matrix do not change. ShiftRows employs fixed rotations and can be easily inverted by performing a rotate in the opposite direction. As a result, after accounting for the ShiftRows step, each element in the matrix can be processed separately and the SCA attack can be split into 16 individual attacks, one for each byte. With 256 possible guesses per byte, the final key $\mathbf{k}^{10} = [k^{10,1}, k^{10,2}, \dots, k^{10,16}]$ can be searched byte-by-byte within a space of 2^{12} possible values in sharp contrast to the 2^{128} values that a brute-force attack on the entire 16-byte key would have to evaluate. A detailed description of the attack follows.

The attack flow used throughout this thesis is shown in Fig. 4. Given a ciphertext, the output of the penultimate stage of AES can be deduced correctly by inverting the operations in the final AES round—provided the correct final key value $\mathbf{k}^{10}$ is used in the inversion. Because there are 2^8 possible values for each byte $b \in \{1, \cdots, 16\}$ of the final key, 256 guesses $k_0^{10,b}, \cdots, k_{255}^{10,b}$ are made and 256 possible values are generated for each byte b of the penultimate round's output (the previous state of the register in Fig. 3). Then, the Hamming Distances between the guessed output of the penultimate round and the

[4] Zero Value assigns zero to '0' valued results and one to all other values. It is useful to discern data values protected by multiplicative operations, as '0' multiplied by any number would give '0'.

[5] Hamming Weight is the number of '1's in a binary number; e.g., Hamming Weight of 1100_2 is 2.

[6] Hamming Distance is the number of transitions between 0s and 1s in two binary numbers; e.g., the Hamming Distance between 1001_2 and 0111_2 is 3.

ciphertext are calculated[7]. The calculation is repeated for each of the N_{e} ciphertexts[8], forming 256 sets that each contain N_{e} Hamming Distances.

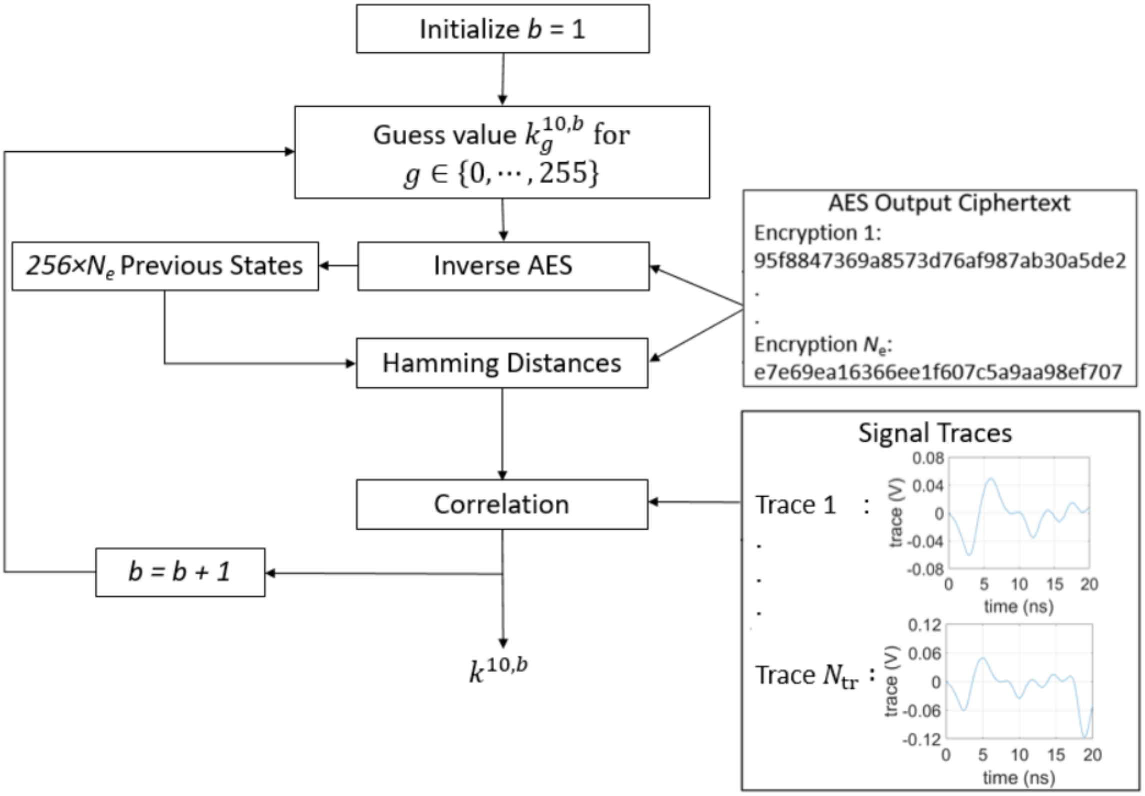


Figure 4: Side-channel analysis (SCA) attack flow [20].

To identify which of the 256 guessed keys $k_g^{10,b}$ is the correct guess for byte b of the final key, each set of Hamming distances is correlated with the set of measured signals (traces) that contains N_{tr} traces recorded during AES. Specifically, the Pearson Correlation

[7] It is important to note that this calculation is performed using only one byte of the ciphertext and guessed output. Accounting for the ShiftRows operation, byte b of the key encrypts one byte of the ciphertext following a one-to-one relation with the set {1,6,11,16,5,10,15,4,9,14,3,8,13,2,7,12}, e.g., bytes b=1, b=2, and b=3 of the key encrypt bytes 1, 6, and 11 of the ciphertext.

[8] For simplicity, encryptions/decryptions were always performed on the same group of N_{e} plaintexts throughout the thesis; these were generated using a pseudorandom generator.

Distinguisher is used with n_{tr} of these traces (for $1 \le n_{\mathrm{tr}} \le N_{\mathrm{e}}$)[9]. Let $\rho_g^b(t, n_{\mathrm{tr}})$ denote the correlation computed using set $g \in \{0, \cdots, 255\}$ of Hamming Distances, which corresponds to the guess $k_g^{10,b}$ for the key byte $k^{10,b}$; the correlation is a function of time and the number of traces used. The maximum value of the correlation over all time instants is denoted as

$$\rho_g^{b,\max}(n_{\mathrm{tr}}) = \max_t \rho_g^b(t, n_{\mathrm{tr}})$$

It should be noted that the measured signals are discrete samples of the underlying functions; thus, ρ_g^b are computed at N_{pts} time instances $t_0 + \{0, \Delta t, \cdots, (N_{\mathrm{pts}} - 1)\Delta t\}$, where t_0 represents the start time of the final AES round, $\Delta t = 1/f_{\mathrm{s}}$ is the time-step size, and f_{s} is the sampling rate used by the oscilloscope. An example of the correlation coefficients are shown in Fig. 5 for the scenario detailed in Section 3.1 with the probe located at (10.8,9,0) mm.

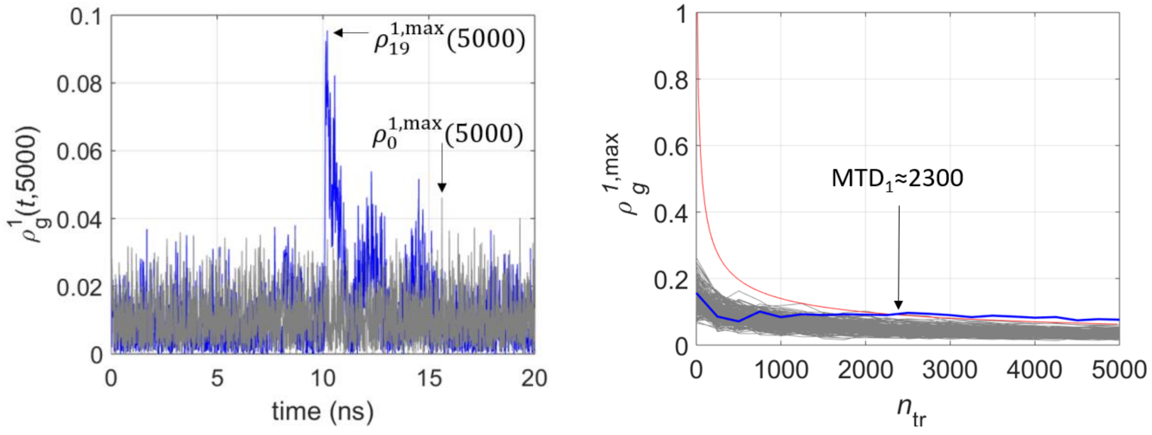


Figure 5: Correlation coefficients for byte 1. Left: The coefficient for the correct guess ($\boldsymbol{k}^{10,1} = 19$) and an incorrect guess ($\boldsymbol{k}^{10,1} = 0$) found using $n_{\mathrm{tr}} = 5000$ traces. Right: Maximum value of the coefficient for all 256 guesses when using different number of traces. Coefficients for the 255 incorrect guesses (gray) and the correct guess (blue) are shown along with the confidence threshold (red). Extracting byte 1 of the final key required at least ~2300 encryptions to be observed in this measurement configuration.

[9] It is common to observe multiple traces in fine-grained EM SCA attacks for each encryption using different measurement configurations; e.g., using different probe locations or orientations. In these cases, the total number of traces observed is often much larger than the number of encryptions, i.e., $N_{\mathrm{tr}} \gg N_{\mathrm{e}}$. Here, it is assumed that exactly one trace is collected in each measurement configuration per encryption (N_{e} traces per configuration) and that these sub-sets of N_{e} traces are used independently (one sub-set at a time) in the Pearson Correlation Distinguisher; thus, at most N_{e} traces are used to compute correlation.

When the maximum correlation coefficient for one of the 256 sets differs from those of the other sets beyond a threshold value, the guessed value of the key byte that was used to generate the outlier set is considered to be $k^{10,b}$, the correct value of byte b of the final key. In this thesis, the specific criteria used to identify the outlier set is that the null hypothesis

$$\rho_g^{b,\max}(n_{\text{tr}}) = 0, \tag{2.1}$$

must be valid with a confidence, α, of 99.99% [21] and the set for which this hypothesis is rejected is the outlier set (Fig. 5). A threshold is used to perform hypothesis testing and identify the correct guess; specifically

$$Threshold\ (n_{\text{tr}}) = \frac{t_{inv}(1-\alpha, n_{\text{tr}})}{\sqrt{n_{\text{tr}} - 3}}\ , \tag{2.2}$$

where t_{inv} function denotes the inverse t-distribution function used for statistical analysis [11]. The minimum number of traces for which the correlation is above this threshold, is denoted as the measurements to disclosure (MTD), which is the metric used in this thesis for judging SCA attacks. The MTD for byte b of the final key ($k^{10,b}$) is given by

$$[MTD_b, g] = \min_{n_{\text{tr}}}\ [n_{\text{tr}}, g]\ \text{s.t.}\ \rho_g^{b,\max}(n_{\text{tr}}) > \ Threshold\ (n_{\text{tr}}), \tag{2.3}$$

MTD is dictated by the measurement configuration as detailed in Chapter 3.

Once the first byte $k^{10,0}$ of the final key is recovered, the procedure is repeated until all 16 bytes of the final key $\mathbf{k}^{10}$ are decoded. Then, the first key $\mathbf{k}^0$ is found by inverting Rijndael's key schedule. This method for breaking AES is commonly used for power, coarse-grained, and fine-grained EM SCA attacks. To differentiate between the power and EM side-channels, the terms Correlation Power Analysis (CPA) and Correlation EM Analysis (CEMA) are used. Power SCA and coarse-grained EM SCA attacks generally recover all bytes using a single set of $N_{\text{tr}} = N_{\text{e}}$ observed traces; each trace is an aggregate of signals generated by all sources on the chip. In contrast, fine-grained EM SCA attacks can collect multiple sets of traces using different probe positions/orientations and can use a different sub-set of traces to extract each byte of the final key. Indeed, previous research on fine-grained EM SCA attacks shows that information leakage in AES can be localized near S-boxes [15], [22]; more specifically, the traces observed near an S-box processing a particular byte correlate strongly with the key byte used for encrypting it. As such, when EM probes are positioned close to these information leaking locations, the final key bytes can be recovered by observing fewer encryptions, i.e., such measurement configurations have smaller MTDs. Identifying measurement configurations that yield a small MTD for each byte reduces the cost of future attacks. Various methods to identify these configurations, including their costs, are detailed in Chapter 3

2.3 Binary Search Algorithm for Finding MTD

Computing the Pearson correlation coefficient $\rho_g^{b,max}(n_{\mathrm{tr}})$ requires $O\big(N_{\mathrm{pts}}n_{\mathrm{tr}}\big)$ operations. The direct method to identify MTD_b, using (2.3), is to re-compute the correlation coefficients as the number of traces n_{tr} decreases from N_{e} to MTD_b; this can require anywhere from $O\big(N_{\mathrm{pts}}N_{\mathrm{e}}\big)$ to $O\big(N_{\mathrm{pts}}N_{\mathrm{e}}^2\big)$ operations depending on MTD_b. Clearly, this naïve approach to finding MTD_b can quickly become a computational bottleneck and handicap the adaptive acquisition protocol in Chapter 3 that requires finding MTD_b at each scan.

To accelerate the search for MTD_b a binary search algorithm is used:

1. Compute $\rho_g^{b,\max}(N_{\mathrm{e}})$ using all N_{e} traces. If the threshold for null hypothesis $threshold(N_{\mathrm{e}})$ is crossed, then $MTD_b \leq N_{\mathrm{e}}$ and step 2 is performed; otherwise, $MTD_b > N_{\mathrm{e}}$ and more encryptions must be observed to be able to extract byte b.
2. Set $n_{\mathrm{tr}}^{\mathrm{start}} = 1$ and $n_{\mathrm{tr}}^{\mathrm{end}} = N_{\mathrm{e}}$; repeat the following until the stopping criterion is met.
   - Calculate the correlation $\rho_g^{b,\max}(n_{\mathrm{tr}}^{\mathrm{middle}})$ using only the traces $1,2,\cdots,n_{\mathrm{tr}}^{\mathrm{middle}}$, where $n_{\mathrm{tr}}^{\mathrm{middle}} = \big\lfloor (n_{\mathrm{tr}}^{\mathrm{start}} + n_{\mathrm{tr}}^{\mathrm{end}})/2 \big\rfloor$ and $\lfloor x \rfloor$ is the largest integer less than or equal to x.
   - If $\rho_g^{b,\max}(n_{\mathrm{tr}}^{\mathrm{middle}}) > threshold(n_{\mathrm{tr}}^{middle})$, then $MTD_b \leq n_{\mathrm{tr}}^{\mathrm{middle}}$; set $n_{\mathrm{tr}}^{\mathrm{start}} = n_{\mathrm{tr}}^{\mathrm{start}}$ and $n_{\mathrm{tr}}^{\mathrm{end}} = n_{\mathrm{tr}}^{\mathrm{middle}}$. Otherwise, $MTD_b \geq n_{\mathrm{tr}}^{\mathrm{middle}}$; set $n_{\mathrm{tr}}^{\mathrm{start}} = n_{\mathrm{tr}}^{\mathrm{middle}}$ and $n_{\mathrm{tr}}^{\mathrm{end}} = n_{\mathrm{tr}}^{\mathrm{end}}$.

- If $n_{\mathrm{tr}}^{\mathrm{end}} - n_{\mathrm{tr}}^{\mathrm{start}} \leq 10$, set MTD_b=$\lfloor (n_{\mathrm{tr}}^{\mathrm{start}} + n_{\mathrm{tr}}^{\mathrm{end}})/2 \rfloor$ and stop; otherwise, repeat the above steps.

For example, in Fig. 5, $MTD_b = 2300$ and N_{e}= 5000 encryptions are observed, the correlation for the correct guess will be evaluated for 5000 (pass), 2500 (pass), 1250 (fail), 1875 (fail), 2187 (fail), 2343 (pass), 2265 (fail), 2304 (pass), 2285 (fail), and 2294 (fail); the method yields $MTD_b =$ 2299. This algorithm finds MTD_b within ∓ 5 in $O(N_{\mathrm{pts}} N_{\mathrm{e}} \log_2 N_{\mathrm{e}})$ operations.

2.4 MEASUREMENT EQUIPMENT

Performing fine-grained EM SCA attacks requires the use of precise equipment for recording traces and positioning probes. Choice of equipment plays an important role in the time required to perform the attacks as shown in Section 5.1. This section describes the equipment used in the experimental setup – EM probes, an oscilloscope, target chips, and a probe positioner. Various properties of these components that impact EM SCA attacks are presented.

2.4.1 EM Probes

EM probes (shown in Fig. 6) used in the experiments described in this thesis are H-field probes from Langer (LF-R and LF-U probe set) [23] of 1 mm, 10 mm, and 25 mm diameters. The voltage detected by a probe p of surface S_p that is oriented in $\hat{o}$ direction is given by Faraday's Law:

$$V_p^o(t) = -\frac{d}{dt} \iint_{S_p} \mu \vec{H}(\vec{r}, t) \cdot \hat{o} ds \qquad (2.4)$$

which shows the dependence of observed voltages (traces) on probe size, orientation, and position. The voltages detected near the target chips in this thesis by the smallest probe had magnitudes ~100 μV. Typical oscilloscopes (Fig. 7) can detect down to a minimum of ~400 μV and signals must be on the order of ~1 mV to limit the effect of quantization error. A 30-dB pre-amplifier [24] (Fig. 6) was used in conjunction with all probes to ameliorate this issue but using an amplifier adds extra noise that degrades SNR.

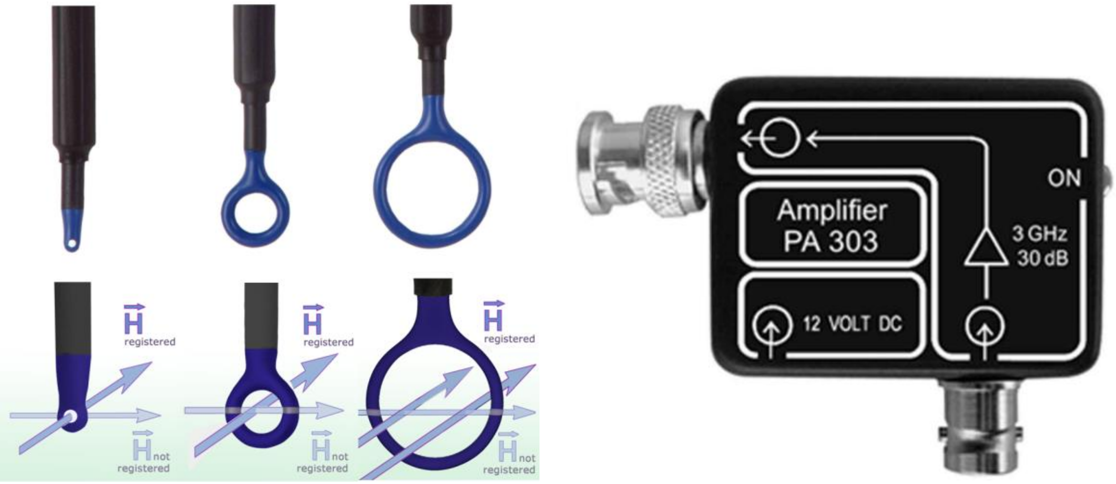


Figure 6: H-field probes of different sizes from Langer [23] (left) and a 30-dB pre-amplifier [24] (right).

2.4.2 Oscilloscopes

Keysight Infiniivision X-series (MSO-X 3024A) [25] and Infiniium S-series (MSO-S104A) [26] oscilloscopes (Fig. 7) were used for data collection. Data capture by the oscilloscope and transferring it to a computer is a major component of the measurement cost (see Section 3.7) for EM SCA attacks. The oscilloscopes and computer communicate through a USB interface controlled using Python's virtual instrumentation library.

Figure 7: Keysight's Infiniivision scope [25] (left) performs a single measurement in every acquisition cycle while the Infiniium scope [26] (right) captures upto 4096 signals per acquisition cycle making experiments significantly faster.

Most modern oscilloscopes have a feature called segmented memory to capture multiple traces in a single acquisition; e.g., an Infiniium S-series oscilloscope can collect up to 4096 segments before data needs to be saved. Older oscilloscopes, such as the Infiniivision X-series, may not have this feature resulting in capture and transfer of a single trace at a time. Typically, the time required to transfer the data is a major bottleneck in acquisition compared to the time required to capture it; thus, having to perform many transfers increases the measurement time significantly; see Section 3.7.

2.4.3 Target Chips and Boards

The experiments reported in this thesis were performed on a ChipWhisperer [27] board with an Artix-7 chip and a Sakura-G [28] board that has a Spartan-6 chip (Fig. 8). Opensource Verilog implementations of AES [28], [29] were deployed on these chips and Python's serial interface library was used to control their USB interface. The Sakura-G and ChipWhisperer were operated at a clock frequency (denoted as f_{clk}) of 6 MHz and 50 MHz in all the reported experiments, respectively. Both boards have start and end signals mapped to the IO pins to trigger the oscilloscope for data capture.

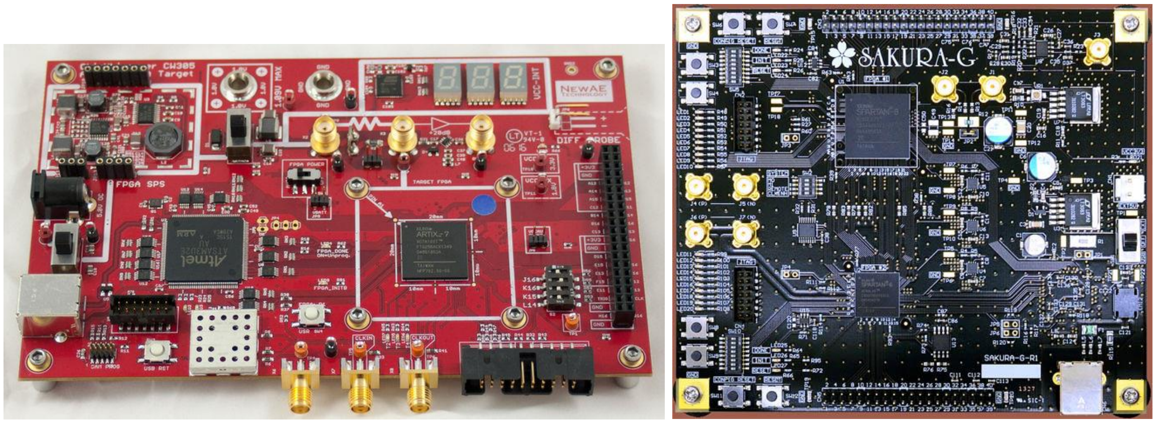


Figure 8: The target boards. CW305 from ChipWhisperer [27] (left) with an Artix-7 chip and the Sakura-G board [28] (right) with a Spartan 6 chip.

2.4.4 Probe Positioner

A 3-D probe station from Riscure [30] was used to position the probes within a ±2.5 µm tolerance above target chips. The station can be controlled through a USB interface and Python's Trinamic Motor Control Library (TMCL), which can access the motors responsible for positioning. The probe can be moved within a range of 40 mm in 3 directions. The station has a mounting apparatus to keep the target affixed (Fig. 9).

All the equipment used in the measurements and a typical measurement setup used to perform the experiments in this thesis are shown in Fig. 9.

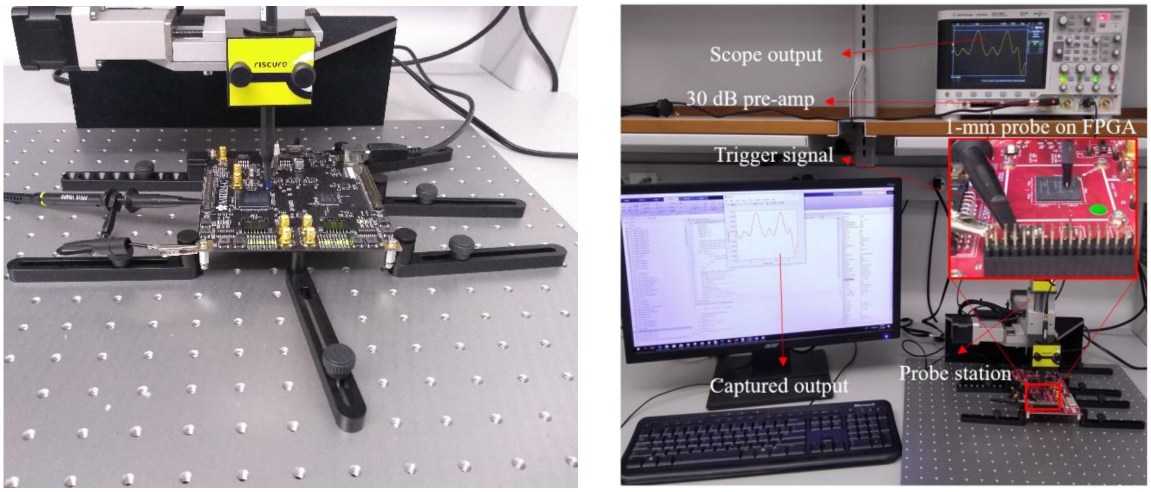


Figure 9: Probe positioner along with mounting apparatus from Riscure [30] (left) and the experiment setup with all components connected [20].

Chapter 3: Acquisition Protocols for Fine-Grained EM SCA Attacks

Information recovery in EM SCA attacks depends on a number of measurement parameters; in particular, as shown in (2.4), the probe voltage depends on the probe's size as well as its location and orientation relative to the chip. The impact of these parameters on information recovery is discussed in Section 3.1. Section 3.2 discusses the search space of configurations for EM SCA attacks. Sections 3.3 and 3.4 present two possible methods for performing fine-grained EM SCA attacks within this search space. Sections 3.5 details the associated costs and trade-offs for the presented methods while Sections 3.6–3.8 focus on time taken to perform measurements. Section 3.9 details storage requirements for collecting the data.

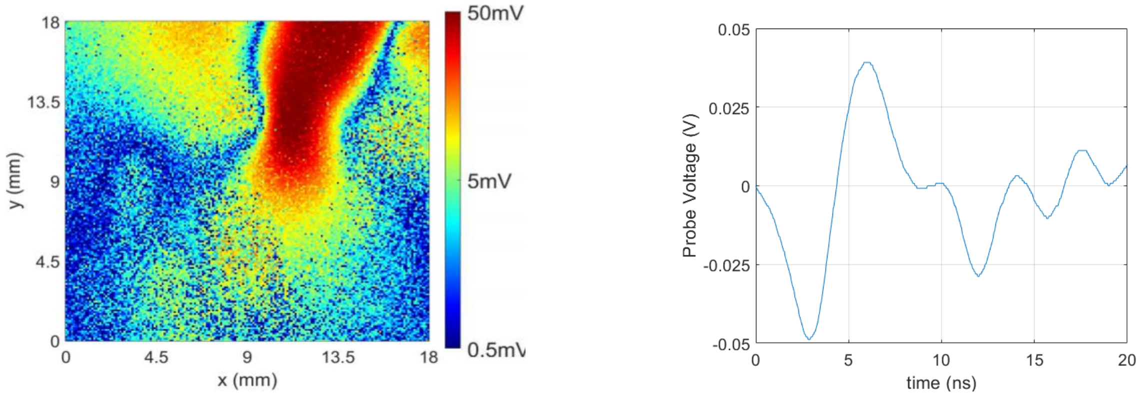


Figure 10: Spatial distribution of the probe voltage observed at time 6 ns during the final round of AES (left) and the temporal distribution (right) observed at position (9.7,7.95,0) mm. Here, an *x*-oriented probe of 1-mm radius was used to scan 181×181 locations just above the ChipWhisperer target chip.

3.1 Impact of Probe Parameters on Information Recovery

This section details the dependence of information recovery on various probe parameters; specifically, the probe’s location, height, size, and orientation. In the following, the case shown in Fig. 10 is chosen as a reference scenario[10] for recovering byte $b = 1$ of the final key of AES. Then, the impact of probe parameters on information recovery is studied by changing one probe parameter at a time.

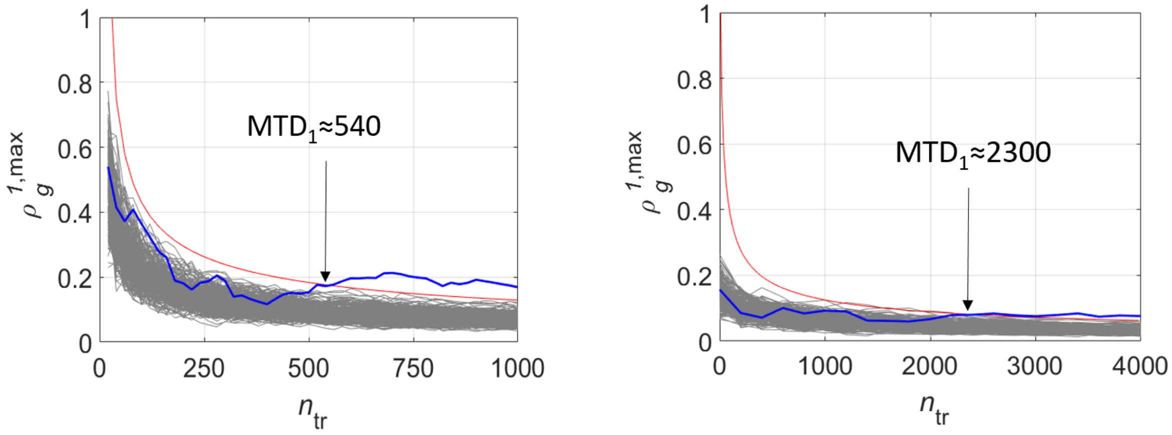
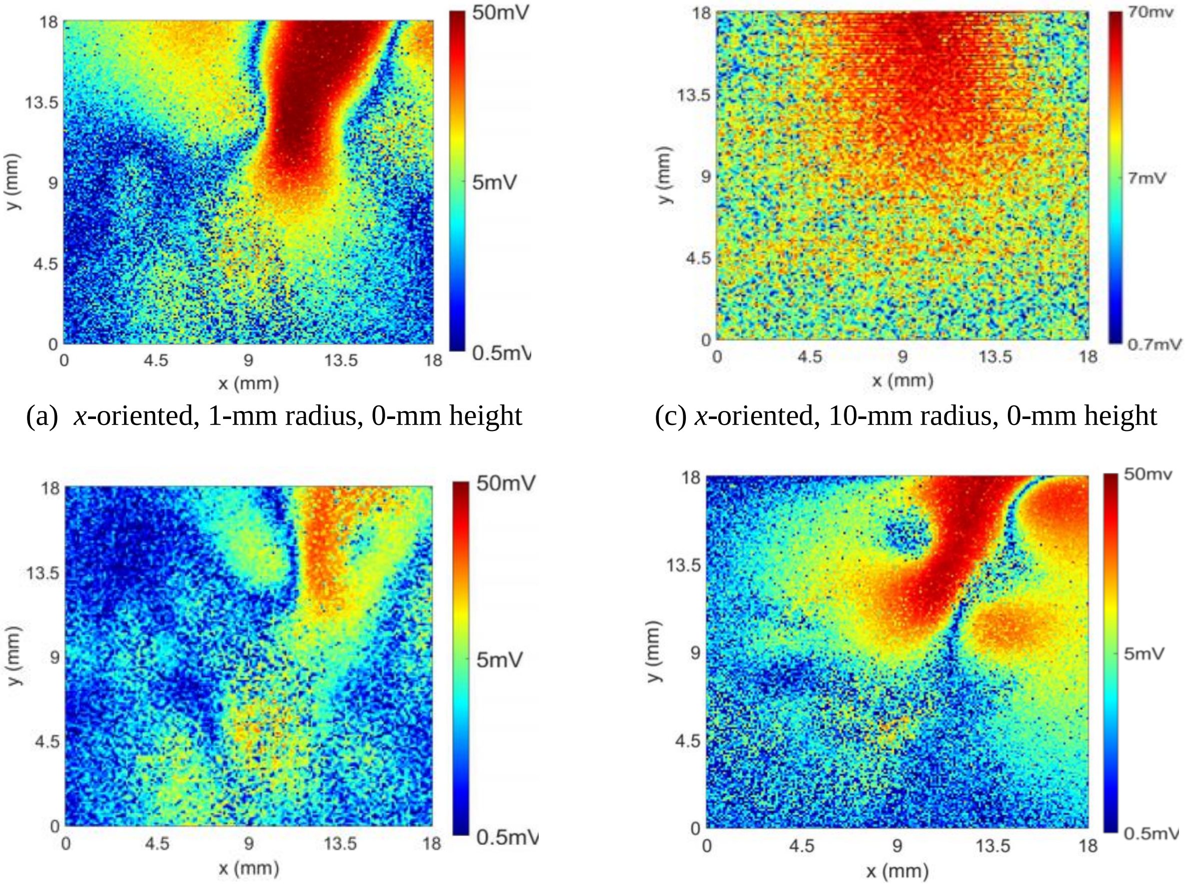


Figure 11: CEMA results for key byte b = 1 using an x- oriented probe. Left: The probe is centered at (9.7,7.95,0) mm (the reference scenario). Right: The probe is centered at (10.8,9,0) mm.

First, the EM SCA attack detailed in Chapter 2 was performed at two probe locations separated by a distance of ~2 mm; the analysis results are shown in Fig. 11. While the EM SCA attack successfully found the correct value of the key byte in both cases, *~4.3× more encryptions had to be observed compared to the baseline case when the probe was shifted ~2 mm in the x-y plane*, demonstrating the sensitivity of information recovery to probe positioning. It is also worth observing that probe locations that result in higher magnitudes of EM traces do not necessarily recover information fastest. For this example, the baseline case had a peak-to-peak probe voltage of ~80 mV, whereas the second location had a peak-to-peak probe voltage of ~100 mV. This demonstrates that the MTD using a given measurement configuration depends on not the magnitudes of the traces but their SNR, i.e., how strongly the traces are correlated to the Hamming Distances between the ciphertext and the penultimate round’s output.

[10] The case with the probe at (9.7,7.95,0) mm is an optimal configuration to recover $\boldsymbol{k}^{10,1}$ for the ChipWhisperer board [20] (see Section 5.6).

Next, the probe was shifted above the chip surface. The observed probe voltages at time 6 ns are plotted as a function of probe position in Fig. 12(b) when the probe was 2.5 mm above the chip surface. Comparing to Fig. 12(a) shows that the magnitudes of probe voltages were generally lower when the probe was farther away from the chip, as should be expected because EM fields decay with distance. The EM SCA attack when the probe was at the same *x*-*y* position as the baseline case succeeded; yet, *~4.5× more encryptions had to be observed compared to the baseline case when the probe was shifted 2.5 mm above the chip surface*, once again demonstrating the sensitivity of information recovery to probe



(a) *x*-oriented, 1-mm radius, 0-mm height

(c) *x*-oriented, 10-mm radius, 0-mm height

(b) *x*-oriented, 1-mm radius, 2.5-mm height

(d) *y*-oriented, 1-mm radius, 0-mm height

Figure 12: Spatial distribution of probe voltage at 6 ns during the final round of AES for various configurations. EM SCA results for these configurations resulted in MTD_1 of (a) 540 at (9.7,7.95,0) mm (the reference scenario), (b) 2400 at (9.7,7.95,2.5) mm, (c) 3000 at (9.7,7.95,0) mm, and (d) greater than 5000 at (9.7,7.95,0) mm.

positioning.

Next, a larger probe was used. The observed probe voltages at time 6 ns are plotted in Fig. 12(c) for a 10-mm radius probe. Compared to Fig. 12(a), which was generated by a 1-mm radius probe, the sensitivity to probe position/resolution were reduced, as should be expected: the 10-mm probe integrates fields over a larger area. The EM SCA attack when the probe was at the same *x-y* position as the baseline case succeeded but *using the 10-mm radius probe required ~5.5× more encryptions to be observed compared to the 1-mm radius case*, indicating the differences between coarse-grained and fine-grained EM SCA attacks.

3.2 The 4-Dimensional Space of Configurations

As Section 3.1 demonstrates, fine-grained EM SCA attacks have *a multi-dimensional space of configurations* that strongly impact their potency. This space of configurations must be searched to identify vulnerabilities of a cryptographic implementation and to find optimal EM SCA attack configurations. Assuming various probe parameters are pre-determined[11], the space of configurations can be narrowed down to a 4-D space: the 2-D location of the probe on the plane of the chip, the probe orientation, and, importantly, the number of encryptions that should be observed at each position.

3.3 Exhaustive 4-D Acquisition

Current techniques employ full-chip scans [15], [21], [22]—typically with a small probe placed in single or multiple orientations searching in the *x-y* plane above the chip—to identify configurations that minimize information recovery time. Such techniques can be considered exhaustive scans. For example, the encryption key leakage from an FPGA implementing AES was localized to a resolution of ~1 mm with a full-chip scan of the chip surface after de-capsulating the FPGA in [21]; this required collecting a total of ~1.7×10^6 traces (27 × 27 locations, 3 orientations, and 800 traces per position).

[11] The size, bandwidth, electric- or magnetic-field type, maker, and model of a probe can be pre-determined. This thesis also assumes that the probe-height is also pre-determined and fixed; in particular, probe location is assumed to be just above the chip's surface, denoted as 0 mm height.

Because information recovery in fine-grained EM SCA attacks is sensitive to minor changes in probe position, a large number of locations must be probed in order to find the best location for the attack. For example, consider an exhaustive scan of the ChipWhisperer target chip similar to that shown in Fig. 10, which shows results for one probe orientation and one encryption. Probing 181×181 locations (it is an 18 mm×18 mm chip) using 100-µm spatial resolution, with two vertical orientations (probe face perpendicular to the chip), and observing 5000 encryptions per position would require the collection of $\sim 3.3\times 10^{8}$ traces. Although it would yield the best EM SCA attack configuration, the exhaustive scan would be prohibitively time consuming to implement; e.g., using the equipment available for this thesis, it would require ~1 month to perform the search (see Section 4.4). Techniques are needed to more rapidly search this space and find optimal solutions.

3.4 Adaptive Acquisition Protocol

One possible approach to explore the space of configurations is to use an adaptive search algorithm: perform multiple (increasingly localized) scans of the EM fields on the chip surface and make a locally optimal choice based on the EM SCA attack results to determine the next scan. Each scan can reduce the total MTD and thus the marginal cost of attacking similar implementations; in return for increasing the total cost of the search with that of the latest scan.

The proposed algorithm divides the search into 2 phases. Phase I is a full-chip scan that aims to provide a reasonable starting point for subsequent scans. Phase II initially uses the best configurations provided by phase I—probe locations and orientations with the least MTD—and improves upon them by performing localized scans. It places constraints on the area and number of measurements per position to reduce number of measurements. This phase is performed for each of the 16 bytes independently. The two phases of the scan are detailed next.

3.4.1 Phase I : Full-Chip Scans

In this phase, $N_{\text{scan}}^{\text{I}}$ scans are performed over the entire area A of the chip as the number of encryptions observed per position or the spatial resolution increases. In each scan $s = 1, \ldots, N_{\text{scan}}^{\text{I}}$, $N_{\text{e}}^{s,\text{I}}$ encryptions are observed at $N_{\text{obs}}^{s,\text{I}}$ probe locations above the chip using two (or if possible, three) orthogonal probe orientations. The probe locations are distributed uniformly over the chip surface; thus,

$$N_{\text{obs}}^{s,\text{I}} = A/(\Delta^{s,\text{I}})^2 \ , \tag{3.1}$$

where $\Delta^{s,\text{I}}$ denotes the scan's spatial resolution. The increasingly more costly scans are performed until CEMA can extract all 16 bytes of the secret key using the acquired signal traces. The extraction in early scans may fail for one or more bytes due to insufficient number of probe locations ($N_{\text{obs}}^{s,\text{I}}$) or encryptions observed per position ($N_{\text{e}}^{s,\text{I}}$); either one of these two parameters may be incremented from one scan to the next during phase I. The next phase of the protocol assumes that at the end of phase I each byte of the secret key can be extracted via CEMA of the signal traces from at least one probe position with at least one probe orientation. Phase I ends by identifying

$$mMTD_b^0 = \min_l \min_o MTD_b^{N_{\text{scan}}^{\text{I}},\text{I}}(o,l), \tag{3.2}$$

the minimum MTD over all measurement configurations from the last scan in phase I for each key byte b. Here and in the following, $MTD_b^{s,\text{I/II}}(o,l)$ denotes the MTD for key byte b when the traces are collected using probe orientation o at location l in scan s of phase I/II. The optimal probe location $(x_b^{\text{opt},0}, y_b^{\text{opt},0}, 0)$ and orientation $o_b^{\text{opt},0}$ that corresponds to $mMTD_b^0$ is recorded for each byte $b = 1, \cdots, 16$.

3.4.2 Phase II : Byte-by-byte Optimization

In this phase, $N_{\text{scan}}^{\text{II}}$ scans are performed over progressively smaller areas of the chip as the number of encryptions observed per position decreases and the spatial resolution increases. Importantly, the localization is performed separately for each byte of the key, i.e., 16 different localizations are performed. In the following, $\Delta^{s,\text{II}}$ denotes the scan's spatial resolution (as the last scan of phase I is the starting resolution in phase II, $\Delta^{0,\text{II}}$=$\Delta^{N_{\text{scan}}^{\text{I}},\text{I}}$).

All the scans in phase II are performed independently for each key byte b using a single probe orientation based on the results of Phase I ($o_b^{\text{opt},0}$); the scans are progressively constrained to within the $3\Delta^{0,\text{II}}$×$3\Delta^{0,\text{II}}$ square region centered at $\left(x_b^{\text{opt},0}, y_b^{\text{opt},0}\right)$. Each scan ($s$=1,…,$N_{\text{scan}}^{\text{II}}$) is performed over the $3\Delta^{s-1,\text{II}} \times 3\Delta^{s-1,\text{II}}$ area between the four corners ($x_b^{\text{opt},s-1} \pm \Delta^{s-1,\text{II}}, y_b^{\text{opt},s-1} \pm \Delta^{s-1,\text{II}}$), i.e., the encryptions are observed at

$$N_{\text{obs}}^{s,\text{II}} = (3\Delta^{s-1,\text{II}}/\Delta^{s,\text{II}})^2 \tag{3.3}$$

locations. It is important to emphasize that *only $mMTD_b^{s-1}$ encryptions are observed at each location during scan s of phase II*. To prepare for the next scan, the measurement configuration with the minimum MTD

$$mMTD_b^s = \min_l MTD_b^{s,\text{II}}(o_b^{\text{opt},0}, l) \tag{3.4}$$

is found and the corresponding optimal location ($x_b^{\text{opt},s}, y_b^{\text{opt},s}$, 0) is identified and the next scan is performed. At the end of the last scan, a near-field measurement configuration $\{x_b^{\text{opt},N_{\text{scan}}^{\text{II}}}, y_b^{\text{opt},N_{\text{scan}}^{\text{II}}},\ o_b^{\text{opt},0}\}$ is identified for each byte b. Using these configurations, the 16 bytes of the final key of AES can be extracted from an identical chip by collecting only

$$Marginal\ Cost = \sum_{b=1}^{16} mMTD_b^{N_{\text{scan}}^{\text{II}}} \tag{3.5}$$

signal traces. In other words, once the measurement configurations are identified at the end of phase II by the proposed approach, the additional cost of extracting AES keys from the same implementation is given by (3.5).

3.5 Acquisition Cost

The costs of the exhaustive and adaptive acquisition protocols are detailed next.

3.5.1 Exhaustive Acquisition

The cost of exhaustive acquisition is simply the number of traces recorded, which is the product of number of measurements per position N_{e}, the number of observer positions N_{obs}, and the number of orientations for which the measurements were taken. The acquisition cost for this approach is

$$Acquisition\ Cost = 2N_{\mathrm{e}}N_{\mathrm{obs}} \tag{3.6}$$

Here and throughout this thesis, only 2 probe orientations (*x* and *y*) are considered because of equipment limitations.

3.5.2 Adaptive Acquisition

The cost for the adaptive protocol is the sum of the acquisition costs of the phase I scans (over the entire chip with all probe orientations) and phase II scans (focused on optimal locations for each byte). The cost of each scan is the number of traces recorded in that scan; thus, the total cost of the proposed adaptive acquisition approach is

$$Acquisition\ Cost = \underbrace{\sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{I}}} 2N_{\mathrm{e}}^{s,\mathrm{I}}N_{\mathrm{obs}}^{s,\mathrm{I}}}_{\text{phase I}} + \underbrace{\sum_{b=1}^{16}\sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{II}}} mMTD_b^{s-1}N_{\mathrm{obs}}^{s,\mathrm{II}}}_{\text{phase II}} \tag{3.7}$$

The first term is similar to the cost of the exhaustive scan in (3.6) as phase I also performs full-chip scans. The second term reflects the fact phase II scans use fixed probe orientations for each byte and observes fewer encryptions per position as the scans progress.

3.6 Acquisition Time

The expressions in (3.6) and (3.7) give the number of traces collected for analysis. Depending on the measurement equipment, however, the acquisition times for collecting the same exact data may differ significantly. The acquisition time can be calculated from the number of traces recorded (given by equations (3.6) and (3.7)) by using six variables:

(i) v_{pos}: the speed of the probe positioner.

(ii) N_{pts}: the number of samples/datapoints collected per trace, which is dictated by f_{s} the sampling rate used by the oscilloscope and f_{clk} the clock frequency of the chip. As only the probe voltage during the final round of AES is stored, $N_{\mathrm{pts}} = f_{\mathrm{s}}\ /f_{\mathrm{clk}}$.

(iii) N_{seg}; the number of traces that the oscilloscope can capture/store in local storage (also known as deep memory) in a single acquisition. This depends on the available local memory[12], the file format, and how many samples are collected per trace.

(iv)T_{cap}: the time needed to capture each trace and store it locally, which is dictated by the time it takes to perform the encryption (the 11 rounds of AES) and the time needed to load the plaintext, trigger the oscilloscope capture, and control the measurement equipment remotely from a computer.

(v) The time needed to save the data remotely by storing it to an attached device or communicating it to a computer. For storing N bytes of data, this time can be expressed as $t_{\text{lat}} + Nt_{bw}$, where t_{lat} is the latency and t_{bw} the inverse of the data transfer rate. In practice, t_{lat} is orders of magnitude larger than t_{bw}.

In the measurement setup used in this thesis, typical values of these parameters are in the range: $v_{\text{pos}} = 1.3\, mm/s, N_{\text{pts}} = 150\ to\ 600, N_{\text{seg}} = 1\ or\ 4096,\ \ T_{\text{cap}} = 0.7\, ms,\ \ t_{\text{lat}} = 3.5\, ms$ to $70\, ms$, and $t_{bw} = 4\, \mu s\ to\ 40\, \mu s$

3.6.1 Exhaustive Acquisition

The acquisition time required to perform exhaustive acquisition can be expressed as

$$Acquisition\ Time = \underbrace{2\left\lceil \frac{N_{\text{e}}}{N_{\text{seg}}} \right\rceil N_{\text{obs}} t_{\text{lat}}}_{T_{\text{save}}} + \underbrace{\left(2N_{\text{e}}\left(N_{\text{pts}} t_{\text{bw}} + T_{\text{cap}}\right) + \frac{\Delta^{exh}}{v_{\text{pos}}}\right) N_{\text{obs}}}_{T_{\text{collect}}} \qquad (3.8)$$

where $\lceil x \rceil$ is the smallest integer greater than or equal to x and Δ^{exh} is the exhaustive scan's spatial resolution. This expression follows from (3.6) and the above definitions. The first term is the bottleneck in the measurement setup used for this thesis; to emphasize this, it is denoted as T_{save} and remainder is referred to as T_{collect} in the following. The acquisition time is impacted by the oscilloscope model: Older models may not have the option of

[12] Some oscilloscope models have no local storage space on the equipment and each measured trace replaces the previously measured trace; see Section 2.3.3. In this case, $N_{\text{seg}} = 1$.

saving multiple traces and $N_{\mathrm{seg}} = 1$ in these cases. Therefore, 5000 measurements require 5000 data transfers. Newer models can store multiple segments of data as they have larger memory storage. For example, if an oscilloscope can store $N_{\mathrm{seg}} = 1000$ segments and $N_{\mathrm{e}} = 5000$ encryptions must be observed, then only 5 data transfers would be required. Section 5.1 shows a sample comparison of the two oscilloscopes models for a measurement. The last term in (3.8) is the total distance traversed during the scan divided by speed of the positioner. The formula is valid if the scan pattern ensures a single step-size movement between each position.

3.6.2 Adaptive Acquisition

The total acquisition time for the adaptive acquisition is the sum of phase I and phase II acquisition times, which can be derived from (3.7). The time required to perform phase I can be expressed as

$$Acquisition\ Time^{\mathrm{I}} = \sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{I}}} \underbrace{2\left\lceil \frac{N_{\mathrm{e}}^{s,\mathrm{I}}}{N_{\mathrm{seg}}} \right\rceil N_{\mathrm{obs}}^{s,\mathrm{I}} t_{\mathrm{lat}}}_{T_{\mathrm{save}}} + \underbrace{\left(2N_{\mathrm{e}}^{s,\mathrm{I}}\left(N_{\mathrm{pts}} t_{\mathrm{bw}} + T_{\mathrm{cap}}\right) + \frac{\Delta^{s,\mathrm{I}}}{v_{\mathrm{pos}}}\right) N_{\mathrm{obs}}^{s,\mathrm{I}}}_{T_{\mathrm{collect}}}, \quad (3.9)$$

and the time required for phase II is given by

$$Acquisition\ Time^{\mathrm{II}} = \sum_{b=1}^{16} \sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{II}}} \underbrace{\left\lceil \frac{mMTD_b^{s-1}}{N_{\mathrm{seg}}} \right\rceil N_{\mathrm{obs}}^{s,\mathrm{II}} t_{\mathrm{lat}}}_{T_{\mathrm{save}}} + \underbrace{\left(mMTD_b^{s-1}\left(N_{\mathrm{pts}} t_{\mathrm{bw}} + T_{\mathrm{cap}}\right) + \frac{\Delta^{s,\mathrm{II}}}{v_{\mathrm{pos}}}\right) N_{\mathrm{obs}}^{s,\mathrm{II}}}_{T_{\mathrm{collect}}} \quad (3.10)$$

3.7 Analysis Time

It is important to consider the time required for the correlation analysis in EM SCA attacks as MTD calculations can be expensive; see Section 2.3. Let T_{anl} denote the time needed for these computations; using the binary search algorithm in Section 2.3,

$$T_{\mathrm{an}l} = 2N_{\mathrm{obs}} N_{\mathrm{pts}} N_{\mathrm{e}} \log_2 N_{\mathrm{e}} \times T_{\mathrm{flop}}, \quad (3.11)$$

for the exhaustive acquisition and

$$T_{\mathrm{anl}} = \left(\begin{array}{c} \underbrace{\sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{I}}} 2N_{\mathrm{obs}}^{s,\mathrm{I}} N_{\mathrm{pts}} N_{\mathrm{e}}^{s,\mathrm{I}} \log_2 N_{\mathrm{e}}^{s,\mathrm{I}}}_{\text{phase I}} \\ + \underbrace{\sum_{b=1}^{16} \sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{II}}} N_{\mathrm{obs}}^{s,\mathrm{II}} N_{\mathrm{pts}} mMTD_b^{s-1} \log_2 mMTD_b^{s-1}}_{\text{phase II}} \end{array} \right) T_{\mathrm{flop}} \tag{3.12}$$

for the adaptive acquisition. Here, T_{flop} denotes the time needed for 1 floating point operation.

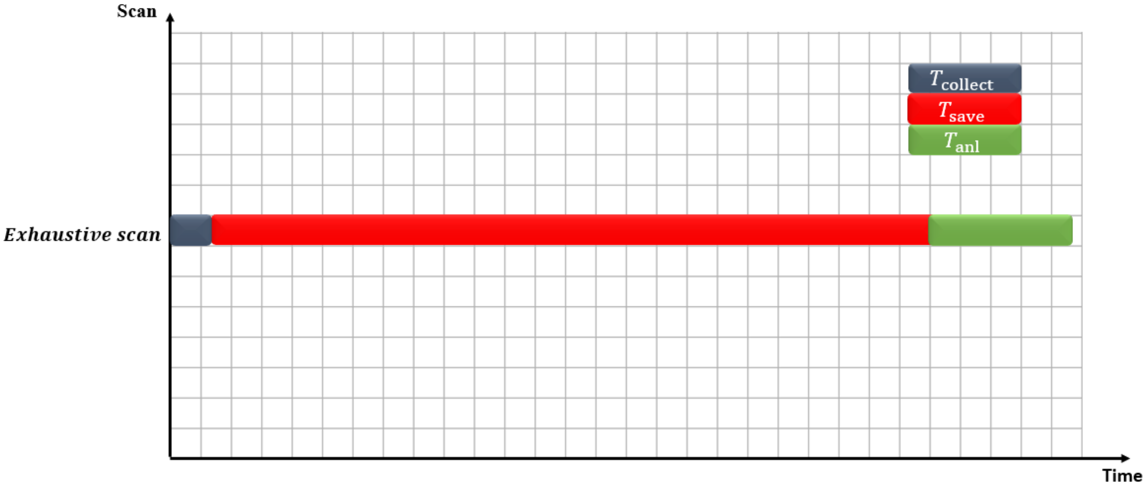


Figure 13: Timeline of steps for the exhaustive acquisition. Measurement, data transfer, and analysis steps are performed sequentially.

3.8 Timeline

The various steps of the measurements are visualized next by constructing timelines.

3.8.1 Exhaustive Acquisition

A sample timeline for the exhaustive acquisition approach is shown in Fig. 13. The capture, transfer, and analysis steps are performed sequentially. Typically, the latency in transferring data from local memory of the oscilloscope to remote storage the computer

(T_{save}) takes the longest time, whereas the rest of the time needed to collect the signals (T_{collect}) as well as the time needed to compute correlations, identify the outlier guess, and find MTD (T_{anl}) once the data is transferred to the computer are shorter.

3.8.2 Adaptive Acquisition

Fig. 14 shows a sample timeline for the adaptive acquisition method: In phase I, every scan depends on the analysis of the previous scan; the steps of each scan are performed sequentially and get progressively more expensive. In contrast, the data collection and transfer may run in parallel to the analysis for phase II because the correlation analysis for a byte can be performed independently from the same scan for another byte. Using the binary search algorithm in Section 2.3 to accelerate the analysis ensures that there is no lag between scans. Moreover, the acquisition times for each scan decrease in phase II because the number of encryptions observed decreases progressively.

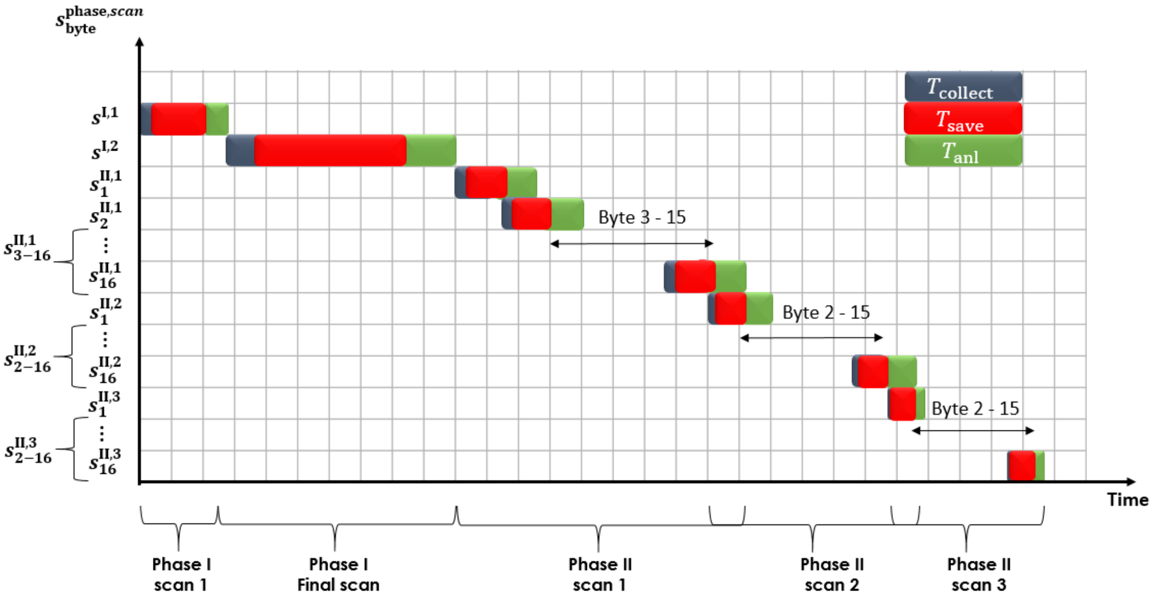


Figure 14: Timeline of steps for the adaptive acquisition approach. Measurement, data transfer, and analysis steps are performed in parallel for the byte-by-byte scans in phase II: The analysis needed before the next scan for each byte is performed while the signal capture and transfer is happening for the next byte.

3.9 Storage Requirements

The data transfer time T_{save} and the analysis time T_{anl} depend on the data size and storage formats. Typically, single precision floating point numbers in binary files are used to store the data. Apart from the acquired data, every such file has a 140 byte-length header storing information on sampling, ranges, resolution. etc.; moreover, 140 byte-length headers are also attached before every trace. While these have to be carefully parsed, they may be neglected for estimating storage requirements if N_{pts} is sufficiently large, as is done next.

To store all the data, the exhaustive scan uses files of size

$$Total\ \ File\ Size =\ 2N_{\mathrm{obs}}N_{\mathrm{pts}}N_{\mathrm{e}} \times 4\ \mathrm{bytes} \tag{3.13}$$

The adaptive acquisition does not require the data from the all the scans to be stored as the files for the previous scan can be discarded when the next scan is completed. Thus, the adaptive scan can use files that are at most of size

$$Max\ File\ Size = \max\left(\underbrace{2N_{\mathrm{obs}}^{N_{\mathrm{scan}}^{\mathrm{I}},\mathrm{I}}N_{\mathrm{e}}^{N_{\mathrm{scan}}^{\mathrm{I}},\mathrm{I}}}_{\text{phase I last scan}},\underbrace{\sum_{b=1}^{16} N_{\mathrm{obs}}^{1,\mathrm{II}} mMTD_b^0}_{\text{phase II first scan}}\right) N_{\mathrm{pts}} \times 4\ \mathrm{bytes} \tag{3.14}$$

If all the data collected in all the scans were to be stored, the adaptive scan would require

$$Total\ File\ Size = \left(\underbrace{\sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{I}}} 2N_{\mathrm{e}}^{s,\mathrm{I}}N_{\mathrm{obs}}^{s,\mathrm{I}}}_{\text{phase I}} + \underbrace{\sum_{b=1}^{16}\sum_{s=1}^{N_{\mathrm{scan}}^{\mathrm{II}}} mMTD_b^{s-1}N_{\mathrm{obs}}^{s,\mathrm{II}}}_{\text{phase II}}\right) N_{\mathrm{pts}} \times 4\ \mathrm{bytes} \tag{3.15}$$

Chapter 4: Measurement Results—Baseline Scenario

This chapter shows the data collected and analyzed at the various steps of the measurement protocol for a baseline scenario. Section 4.1 describes the measurement setup. Sections 4.2 and 4.3 show scan results for the two phases of the adaptive scan protocol. Section 4.4 details the acquisition cost and timeline for the measurement and compares it to the exhaustive acquisition approach.

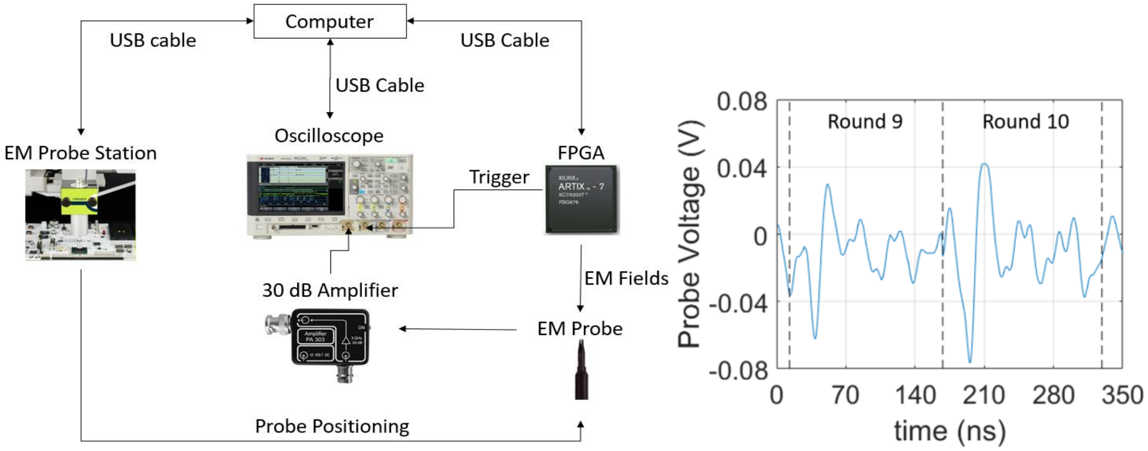


Figure 15: A diagram of the setup used for the measurements [20] and probe voltage observed at the center of the chip (9,9,0) mm, using this setup, in the last 2 rounds of AES. Each round begins at rising edge of clock (dashed) and the traces used in CEMA are only the ~166-ns wide signals that are captured during the 10th round.

4.1 Setup

The measurements described in this chapter were performed on the Sakura board clocked at $f_{\text{clk}} = 6$ MHz. The probe size is 1 mm and the probe's tip touches the surface of the chip (Model no. LF-R 3). The Infiniium oscilloscope was used for measurements and the entire setup was controlled and automated with a Python script. The sampling rate $f_s = 4$ giga-samples/second $(\Delta t = 0.25\ \text{ns})$. Fig. 15 shows a block diagram for the setup and the probe voltage, corresponding to one encryption, in the penultimate and final rounds of AES.

4.2 Phase I

Phase I starts with an initial guess of resolution and the number of encryptions that should be observed at each position. Here, one of two approaches, termed as the Fewer Encryptions High Resolution (FEHR) approach and the Many Encryptions Low Resolution (MELR) approach, may be adopted. For the FEHR approach, the higher initial resolution can help identify good attack locations with fewer traces, but at a higher phase I acquisition cost. A significant reduction in search area resulting from phase I, however, would mean fewer phase II scans, which may reduce the overall acquisition cost. On the other hand, the lower initial resolution scans in the MELR approach, with more measurements per

Byte	Orientation (o)	$x_b^{\text{opt},0}, y_b^{\text{opt},0}$(mm)	$mMTD_b^0$	Byte	Orientation (o)	$x_b^{\text{opt},0}, y_b^{\text{opt},0}$(mm)	$mMTD_b^0$
1	x	7.2,7.2	3120	9	x	3.2,14.4	2370
	y	7.2,7.2	2480		y	10.8,10.8	1240
2	x	7.2,10.8	3430	10	x	7.2,7.2	2460
	y	No Location Detected	>5000		y	3.6,7.2	4220
3	x	7.2,7.2	2010	11	x	7.2,3.6	3100
	y	3.6,3.6	3180		y	No Location Detected	>5000
4	x	7.2,7.2	2320	12	x	7.2,7.2	2640
	y	7.2,3.6	3220		y	7.2,3.6	3440
5	x	3.2,10.8	1640	13	x	7.2,14.4	2120
	y	3.2,10.8	2040		y	No location Detected	>5000
6	x	7.2,10.8	2480	14	x	7.2,3.6	3990
	y	10.8,7.2	2980		y	3.6,7.2	3220
7	x	7.2,10.8	4460	15	x	No location Detected	>5000
	y	7.2,3.6	3680		y	7.2,10.8	4660
8	x	7.2,7.2	2300	16	x	No location Detected	>5000
	y	7.2,3.6	2620		y	3.6,7.2	3920

Table 1: Phase I Results

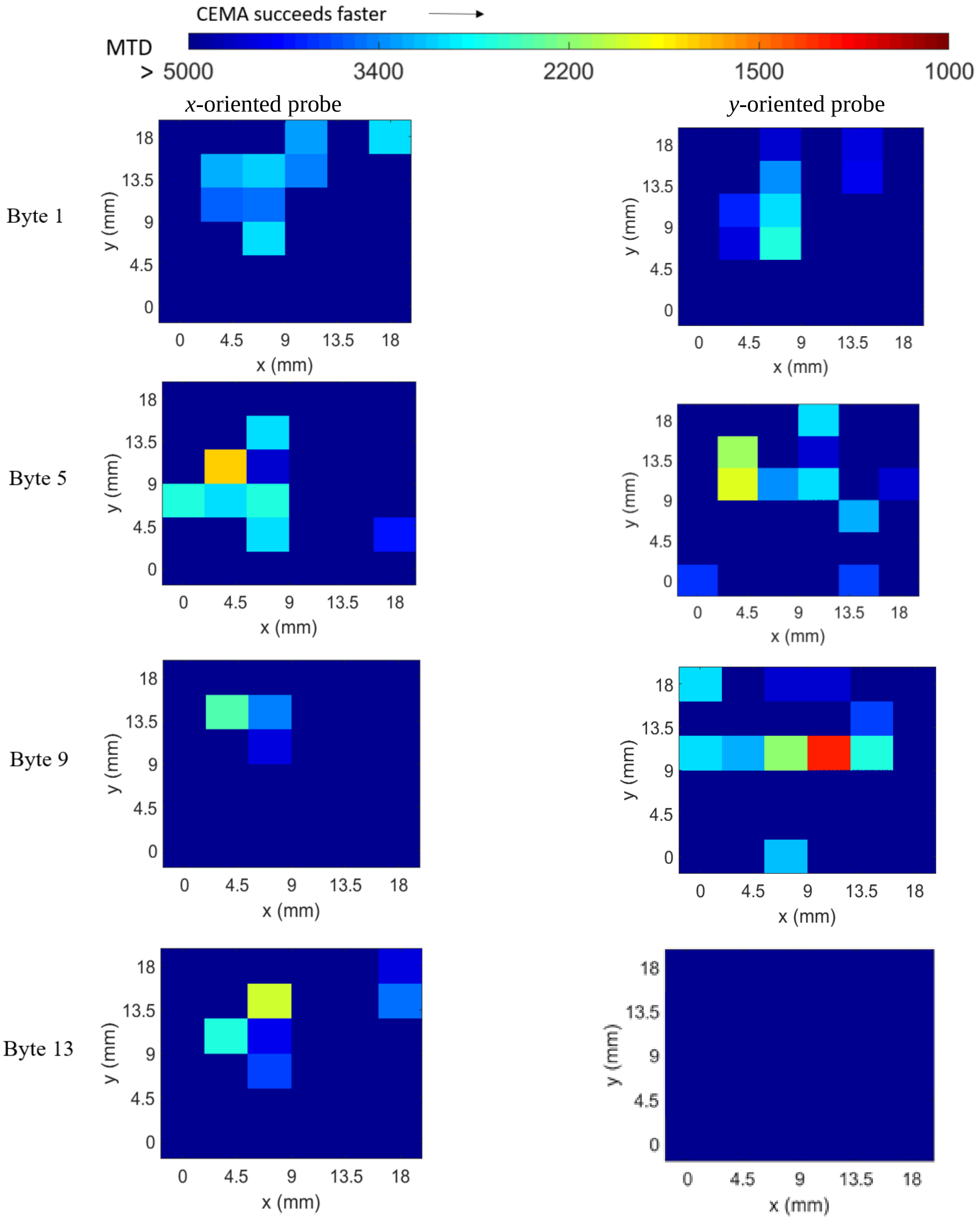


Figure 16: Maps of MTD_b results in phase I for bytes $b \in \{1,5,9,13\}$ when the probe is *x* or *y* oriented. The most effective location above the chip and orientation for the probe is different for the different bytes of the AES key. Colorbars are logarithmic and limits are chosen such that the maximum and minimum values of MTD across all compared scans are covered and the variation between location with best MTD and surrounding locations are observed clearly.

.

position, are cheaper[13] and likely to complete phase I with lower acquisition cost than the FEHR approach. The measurements reported in this chapter used the MELR approach for phase I. A FEHR version was also performed (Section 5.2).

An initial resolution with $N_{\mathrm{obs}}^{1,\mathrm{I}} = 6 \times 6$ locations on the chip area ($\Delta^{1,\mathrm{I}} = 3$ mm) and $N_{\mathrm{e}}^{1,\mathrm{I}}$=5000 measurements per position were chosen to perform the attack. Two scans (one with *x*- and one with *y*-oriented probe) were performed using these parameters. After the first scan, all bytes could be recovered for some combination of location and probe orientation, i.e., phase I could terminate with $N_{\mathrm{scan}}^{\mathrm{I}} = 1$ scan. The optimal location $(x_b^{\mathrm{opt},1}, y_b^{\mathrm{opt},1}, 0)$ and minimum MTD for every byte in phase I are shown in Table 1, which highlights the probe orientation used in phase II. Results of phase I scans for select bytes are shown in Fig. 16. At the end of phase I, the marginal cost of breaking an identical implementation was ~4.4×10^4 measurements. Phase I required a total of 1.8×10^5 measurements, ~3.5 hours acquisition time, and ~ 432 MB storage space.

4.3 PHASE II

Phase II starts with the optimal configurations identified in phase I, performs progressively constrained scans to refine the results, and reduces the number of traces observed in each scan as localization improves. Every scan of phase II observes the encryptions at $N_{\mathrm{obs}}^{s,\mathrm{II}} = 11{\times}11$ locations; thus, the resolution increases 3× in each scan. Fig. 17 shows the localization of the scans and the change in MTD as phase II progresses. It was found that the 3rd scan of phase II did not significantly improvement MTD and multiple locations with similar MTDs were observed for some bytes. Therefore, phase II was terminated $N_{\mathrm{scan}}^{\mathrm{II}} = 3$ scans. Table 2 shows the optimal location and MTD after every scan for each bytes. Most bytes are found to be clustered in similar areas if the probe orientation used for attack is the same. At the end of phase II, the final marginal cost of breaking a

[13] Phase I cost increases quadratically with increasing resolution; see (3.7).

similar implementation was ~10^4 measurements. Phase II required a total of ~10^7 measurements, ~24 hours acquisition time, and ~12 GB storage space for the first scan.

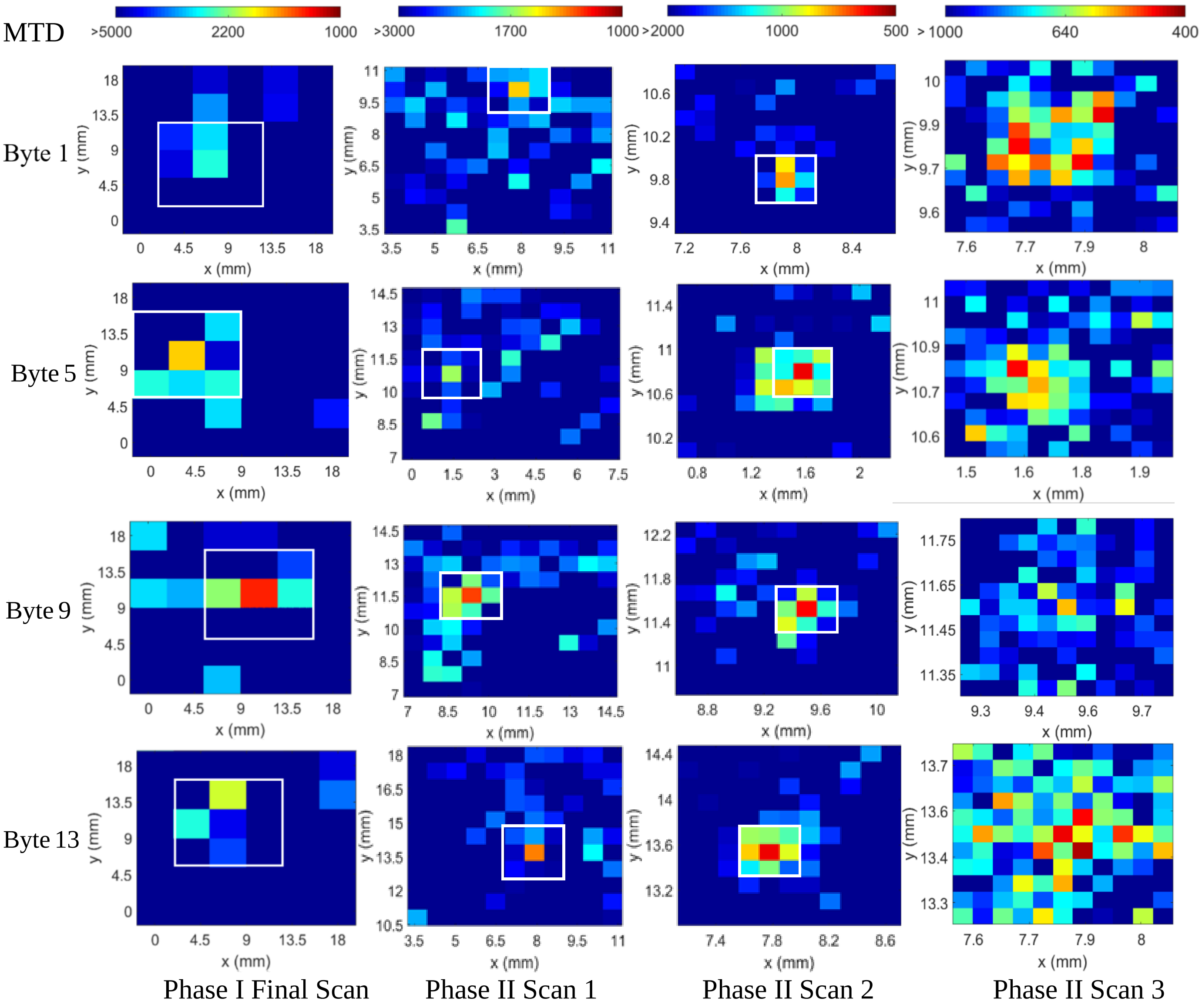
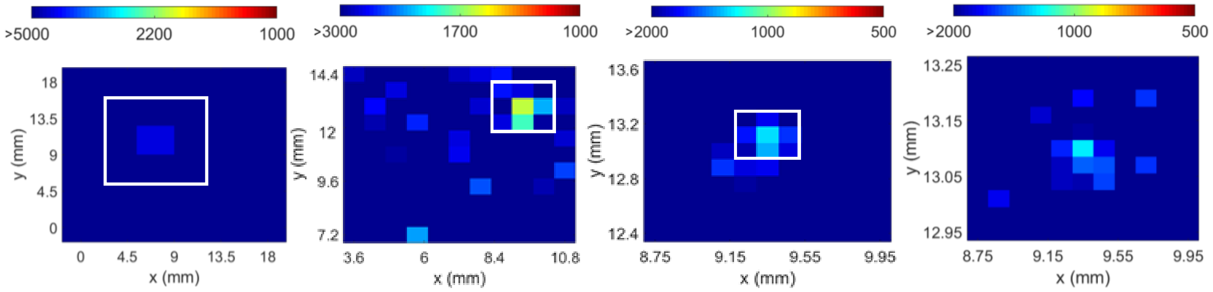


Figure 17: Progression of MTD_b in phase II for byte $b \in \{1,5,9,13\}$. The square region represents the area probed in the next scan. The final scan does not significantly reduce the MTD further and multiple locations may have similar MTDs.

Byte	Orientation	Scan 1		Scan 2		Scan 3	
		$x_b^{\text{opt},1}, y_b^{\text{opt},1}$ (mm)	$mMTD_b^1$	$x_b^{\text{opt},2}, y_b^{\text{opt},2}$ (mm)	$mMTD_b^2$	$x_b^{\text{opt},3}, y_b^{\text{opt},3}$ (mm)	$mMTD_b^3$
1	y	7.92,10.08	1440	7.9,9.78	780	7.68,9.78	480
2	x	8.64,10.8	1820	8.84,10.8	910	8.9,10.8	850
3	x	8.64,7.2	900	9.04,7.6	640	8.98,7.6	600
4	x	8.64,7.92	1280	9.04,7.92	680	9.04,7.8	640
5	x	1.44,10.8	1870	1.64,10.8	610	1.58,10.8	500
6	x	9.36,7.92	820	9.16,7.92	620	9.16,7.92	610
7	y	5.04,5.76	2200	5.44,5.56	950	5.56,5.56	490
8	x	7.92,7.92	1000	8.32,7.92	800	8.32,7.92	800
9	y	8.64,11.52	1240	9.36,11.52	590	9.36,11.52	600
10	x	7.92,7.92	1920	8.12,7.92	540	8.12,7.98	510
11	x	5.04,5.04	1440	5.44,5.44	920	5.44,5.56	740
12	x	9.36,6.48	1560	9.36,6.88	920	9.36,7.02	710
13	x	7.92,13.68	1590	7.72,13.48	580	7.9,13.42	420
14	y	5.04,7.2	1700	5.44,7.6	630	5.5,7.36	460
15	y	9.36,12.96	1550	9.36,13.08	1220	9.36,13.08	1220
16	y	5.04,6.48	940	5.24,7.08	610	5.48,7.14	540

Table 2: Phase II Results

The configurations identified by this experiment may not represent the most optimal result, e.g., byte 15 did not show improved MTD after the 2nd scan of phase II (Fig. 18), implying that the best attack location or orientation may be different.



Phase I Final Scan Phase II Scan 1 Phase II Scan 2 Phase II Scan 3

Figure 18: Analysis for byte 15 shows minimal improvement in phase II

4.4 Cost Analysis and Timeline

Marginal cost and acquisition cost are calculated using the MTD values in Tables 1 and 2 and (3.5) and (3.7); they are plotted in Fig. 19 with respect to the scan round. Fig. 18 shows that the first scan of phase II is the costliest scan since it is performed for all 16 bytes in contrast to phase I where a full-chip scan is performed for all bytes. Subsequent scans in phase II have lower costs due to the decrease in the encryptions observed/measurements recorded per position. Marginal cost reduces sharply after the first phase II scan and then converges after the second scan to ~10^4 measurements.

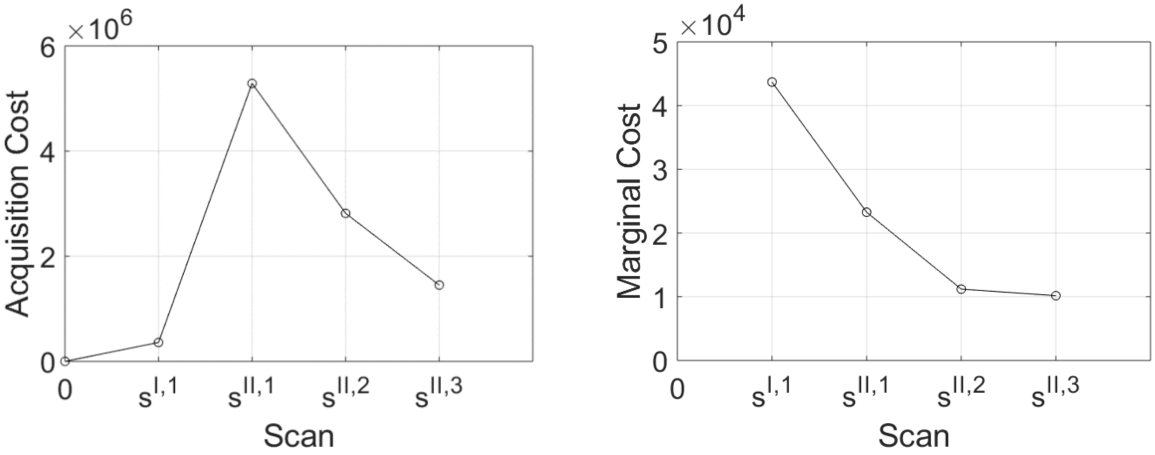


Figure 19: Acquisition cost and marginal cost of the adaptive protocol as scans progress. The final marginal cost is ~4× lower than the initial marginal cost.

Fig. 20 shows trade-off between marginal and acquisition cost. It also shows the expected cost of the exhaustive scan, which corresponds to the number of measurements required for probing 181 × 181 locations for 5000 encryptions and 2 orientations. Because this scan is impractical to implement, the marginal cost and the configurations that would be identified by the exhaustive scan are unknown and the exhaustive scan can potentially decrease the marginal cost further, but the gains are expected to be minor. The adaptive search acquired ~10^7 traces, which was ~30× fewer traces compared to the exhaustive scan.

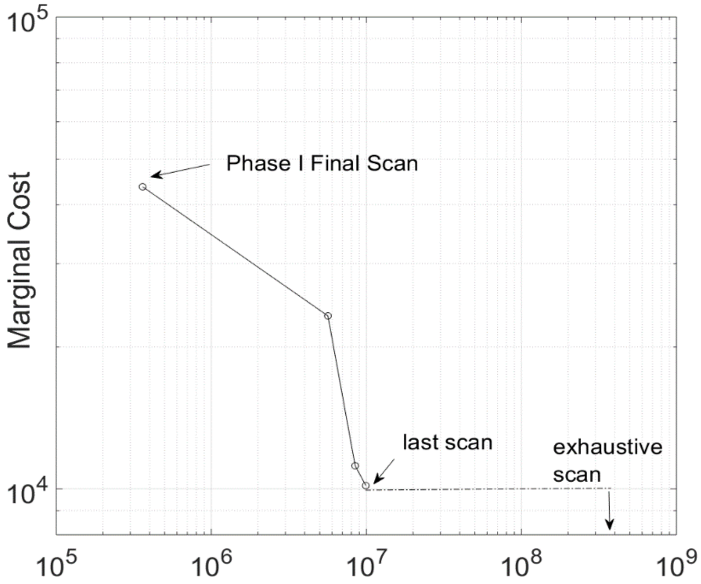


Figure 20: Trade-off between the acquisition cost and the marginal cost of extracting AES key from an identical implementation.

Timelines for both the adaptive and exhaustive acquisition can be constructed using (3.8)-(3.11). Phase I acquisition time was ~3.5 hrs. In phase II, measurements and analysis were performed simultaneously till byte 15 in the last scan. T_{save} for the oscilloscope scales with the number of traces observed and therefore acquisition time decreases with every scan. Total acquisition time for this experiment was ~ 28 hrs (Fig. 21). The expected timeline of the exhaustive acquisition (Fig. 22) shows the total acquisition time to be ~25× more, which is nearly a month. The maximum file-size requirement for the adaptive acquisition method is close to 12 GB for this experiment compared to the 750 GB that would be required by the exhaustive search. Storage with each scan is shown in Fig. 23.

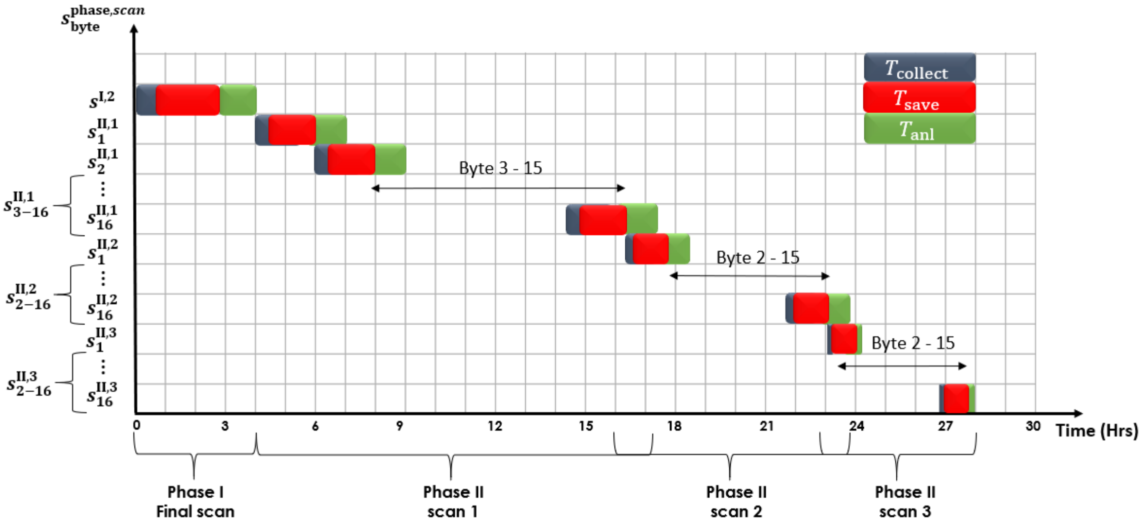


Figure 21: Timeline of the adaptive acquisition. The total time taken for the experiment was ~28 hrs; about half of which was spent in the first scan of phase II..

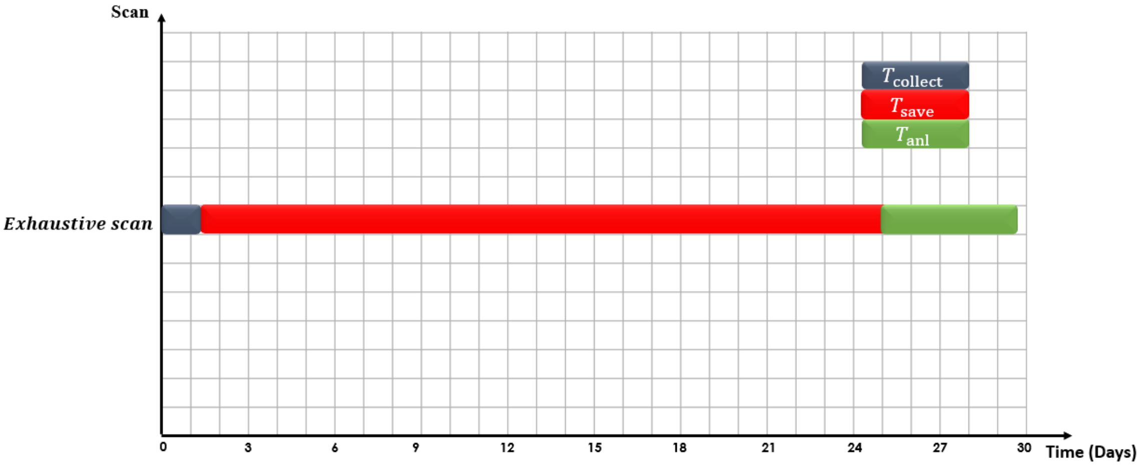


Figure 22: Timeline of the exhaustive scan with expected acquisition time close to 30 days.

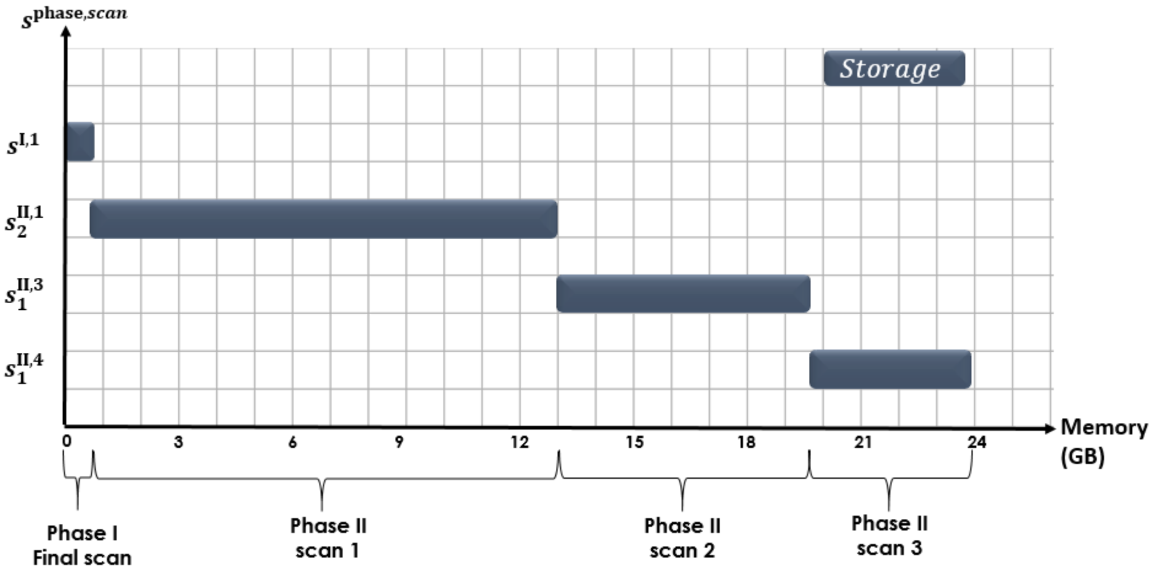


Figure 23: Storage with each scan shows phase II scan 1 requiring maximum storage of ~12 GB.

Chapter 5: Analyses of Attack Configurations

This chapter presents a comparison of attack configurations with different oscilloscopes, different targets, approaches and configurations, and selects low-cost configurations for performing EM SCA attacks. Each section in this chapter observes the variation in information recovery by changing one parameter with respect to the baseline scenario in Chapter 4. Section 5.6 presents the best configurations to attack the target chips based on the experiments. Section 5.7 concludes with a comparison of the lowest cost needed to perform EM SCA attack and power SCA attack.

5.1 Infiniivision vs Infiniium Oscilloscopes

As discussed in Section 3.6, an oscilloscope's save time and capture time have major influence on the total acquisition time for a measurement. The experiment performed in Chapter 4 used the Infiniium model; here, the experiment is repeated with the Infiniivision model. The Infiniivision oscilloscope cannot store more than one trace at a given time and therefore data needs to be transferred to the computer before the next encryption can be performed. This creates a major bottleneck because $T_{\text{save}} \gg T_{\text{collect}}$. Table 3 compares the differences in acquisition time for phase I and phase II using these two oscilloscopes for 5000 measurements with $N_{\text{pts}} = 600$.

Oscilloscope	T_{cap} (ms)	t_{bw} (μs)	t_{lat} (ms)	Max (N_{seg})	v_{pos} (mm/sec)	Phase I time (hrs)	Phase II time (hrs)	Total time (hrs)
Infiniivision	0.7	40	70	1	1.33	30.6	176.9	207.5
Infiniium	0.7	4	3.5	4096	1.33	3.7	24.1	27.8

Table 3: Times Required to Perform the Experiments

t_{lat} for the Infiniium oscilloscope, which is a major component of T_{save}, is ~20× lower than the Infiniivision oscilloscope for the baseline case. However, since analysis time for both oscilloscopes are equal, using the Infiniium model requires ~8× less time than the Infiniivision model. Unless otherwise noted, the Infiniium model was used to collect the data in the following.

5.2 Sakura vs Chipwhesperer Targets

It is necessary to ensure that the presented protocol can scale with shrinking technology nodes. The experiment performed in Chapter 4 is repeated for the ChipWhisperer board, which has a target chip manufactured at the 28 nm technology node (Sakura board has a 45 nm FPGA chip).

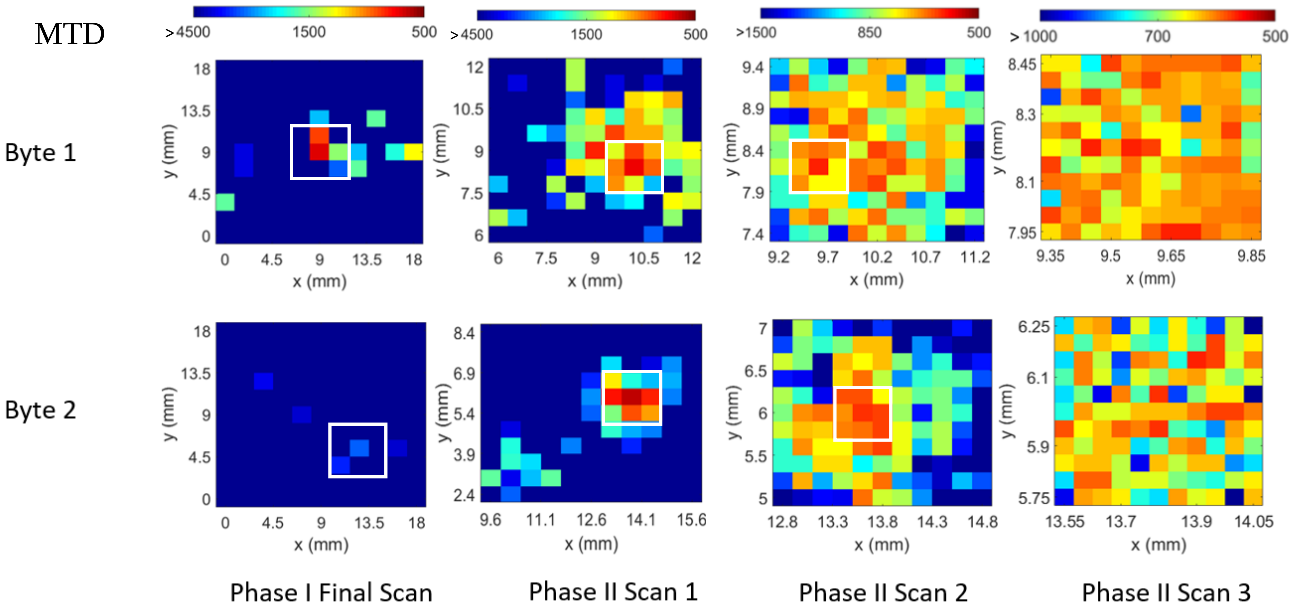


Figure 24: Phase I and phase II analysis for byte 1 and 2 for the ChipWhisperer board..

Here, phase I started with the same initial condition used in the baseline case, i.e. resolution of $N_{\text{obs}}^{1,\text{I}}$ = 6 × 6 divisions of the entire chip area and $N_{\text{e}}^{1,\text{I}}$=5000 measurements per position. However, this configuration failed to yield $MTD_b < N_{\text{e}}^{1,\text{I}}$ for a few bytes. The number of locations was then increased to $N_{\text{obs}}^{2,\text{I}}$ = 11 × 11 keeping the measurements per positions at $N_{\text{e}}^{2,\text{I}}$=5000. This configuration succeeded for all bytes and phase I finished with $N_{\text{scan}}^{\text{I}} = 2$ scans. Analysis for bytes 1 and 2 are shown in Fig. 24. After identifying optimal configurations for all bytes, phase II was performed. The marginal cost of phase I was ~7 × 10^4 measurements. Time taken to perform phase I was ~ 12 hours and the storage space required was ~ 3 GB.

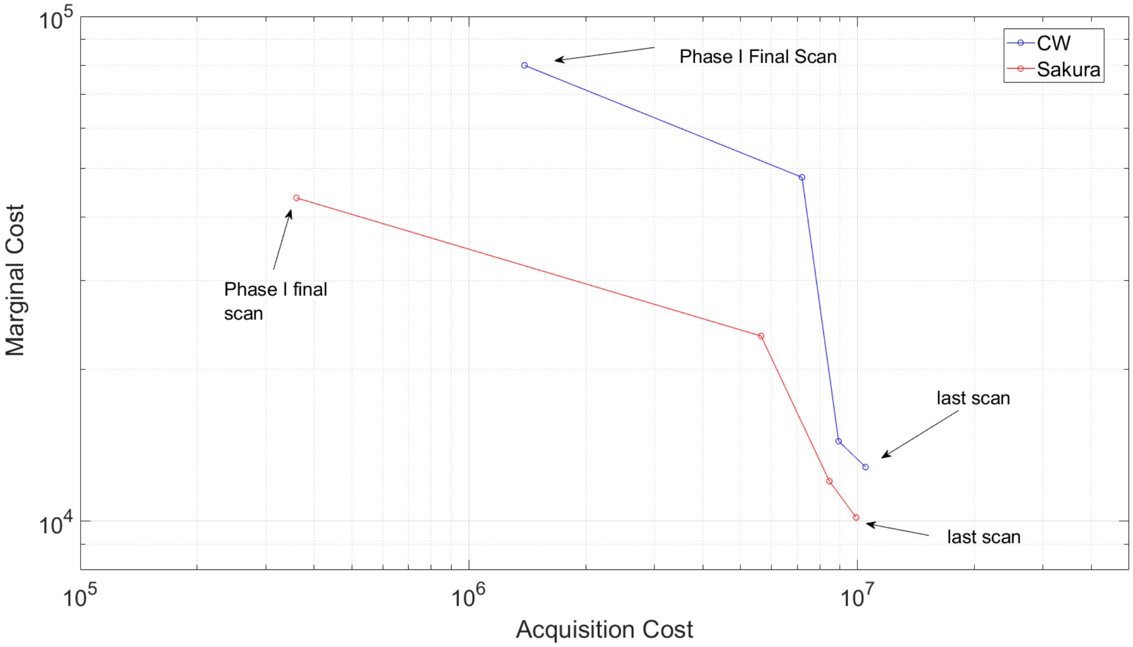


Figure 25: Comparison of marginal cost and acquisition cost of two targets. The Sakura board has lower marginal cost at a lower acquisition cost.

Every scan of phase II observed the encryptions at $N_{\text{obs}}^{s,\text{II}} = 11 \times 11$ locations. Phase II terminated at $N_{\text{scan}}^{\text{II}} = 3$ scans and finished with a final marginal cost of ~ 1.2×10^4 measurements at a total acquisition cost of ~10^7 measurements. The trade-off curves for the two targets is shown in Fig. 25. Phase I acquisition cost was significantly higher for the Chipwhisperer target which also had a much higher marginal cost at the end of phase I compared to the Sakura target. At the end of phase II, the Chipwhisperer target had ~1.2× higher marginal cost and ~1.5× higher overall acquisition cost. The timeline for this experiment (Fig. 26) shows that total acquisition time was ~38 hrs. The maximum storage required for analysis is ~14 GB which is required for first scan of phase II.

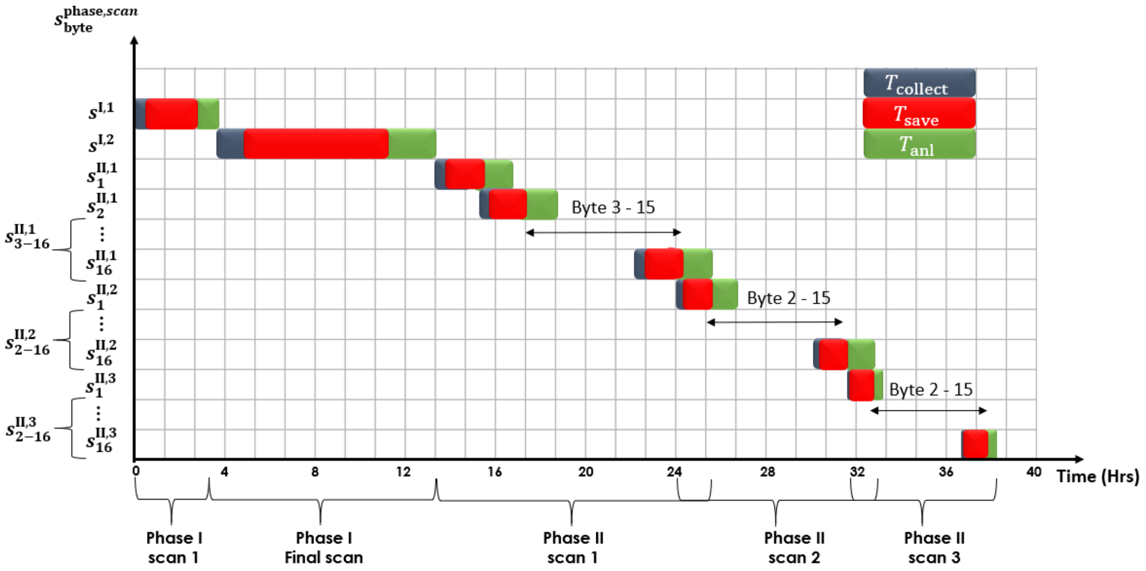
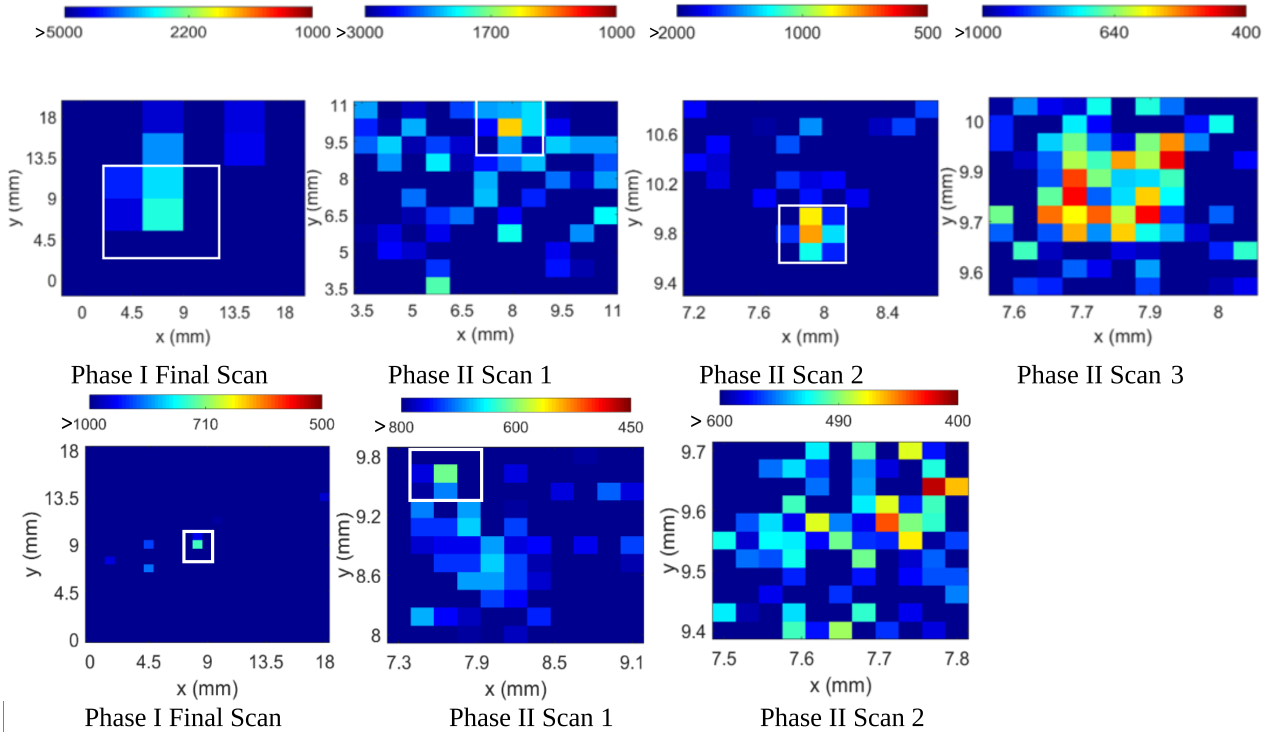


Figure 26: Timeline for the experiment on Chipwhisperer board.

5.3 MELR Approach vs FEHR Approach

As discussed in Section 4.2, there are two possible initial acquisition approaches—MELR and FEHR. The MELR approach was used in the baseline scenario and the FEHR approach is presented here. The FEHR approach started with an initial guess of $N_{\text{obs}}^{1,\text{I}} = 21 \times 21$ divisions of chip area and $N_{\text{e}}^{1,\text{I}}$ =500 measurements per probe position. The attack failed to extract the secret key for this scan and also the second scan with $N_{\text{obs}}^{2,\text{I}}$ =25×25 locations. Following this, the number of measurements per position was increased by 500 ($N_{\text{e}}^{3,\text{I}} = 1000$) and the third scan was performed using the same resolution as the second scan. This configuration yielded a successful acquisition and phase I terminated at $N_{\text{scan}}^{\text{I}} = 3$ scans. Storage needed to complete phase I is ~ 3 GB. Although this approach is more likely to encounter locations with faster information recovery in phase I, it is also more expensive: The phase I acquisition cost for the FEHR scan was ~7× that of the MELR scan for this target. At the end of phase I, the marginal cost was found to be ~1.3×10^4. For the FEHR approach, the area for first scan in phase II was ~6× smaller than the first scan of



Phase I Final Scan

Phase II Scan 1

Phase II Scan 2

Phase II Scan 3

Phase I Final Scan

Phase II Scan 1

Phase II Scan 2

Figure 27: Phase I and phase II analysis for byte 1 for the MELR and FEHR.

MELR approach. Therefore, the FEHR approach required only $N_{\text{scan}}^{\text{II}} = 2$ scans to identify optimal configurations. Phase II analysis for byte 1 for both the approaches are shown in Fig. 27. The final configuration for byte 1 using both these approaches yield similar results, although this is not true for all bytes [20]. Finally, both approaches finished with a similar marginal cost: ~10^4 signal traces to extract the AES-128 key from this implementation as shown in Fig. 28, although the FEHR approach reached this marginal cost with ~1.25× fewer measurements. Total acquisition time for the FEHR approach was found to be ~ 22 hours and the maximum file storage needed for first scan of phase II is ~3.7 GB which is ~4× lower than the MELR approach.

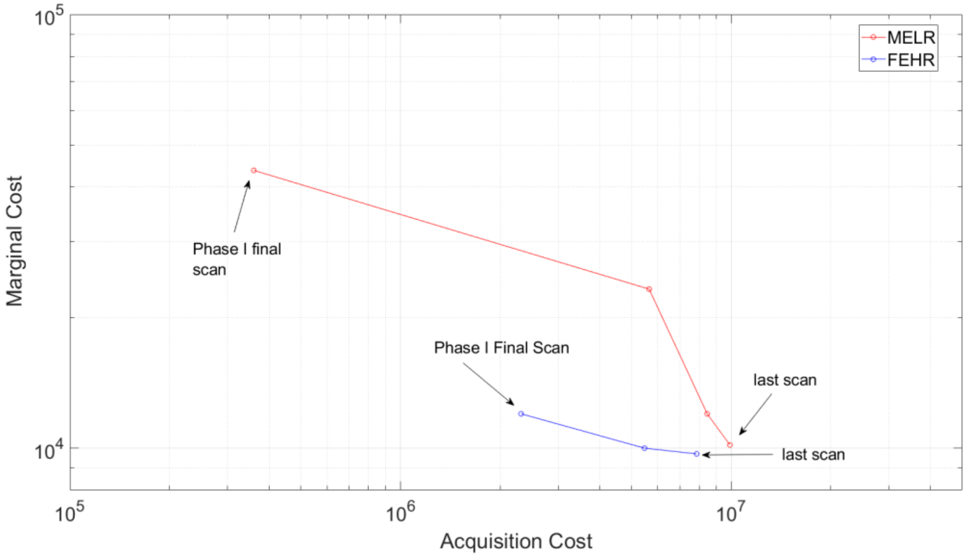


Figure 28: The cost tradeoff for the two different approaches used in phase I scan.

5.4 Variation with Probe Height

This experiment was performed by raising the probe to– 2.5 mm and 5 mm above the chip surface. All heights were measured from probe tip to the surface. For distances greater than 5 mm, detected voltage levels are lower than the oscilloscope's minimum resolution making it infeasible to perform the fine-grained EM SCA attack. Phase I configurations identified for the 0-mm height case, with $N_{\mathrm{e}}^{1,\mathrm{I}} = 5000$ measurements and $N_{\mathrm{obs}}^{1,\mathrm{I}}$ = 5 × 5 divisions of the entire chip area, succeeded for the 2.5 mm case but failed for the 5 mm case. The 5 mm case required increasing both number of traces to $N_{\mathrm{e}}^{3,\mathrm{I}}$=10000 and resolution to $N_{\mathrm{obs}}^{3,\mathrm{I}} = 11 \times 11$. Therefore, phase I acquisition costs for the 2.5 mm case and 0 mm case were the same, whereas that for the 5 mm case was higher.

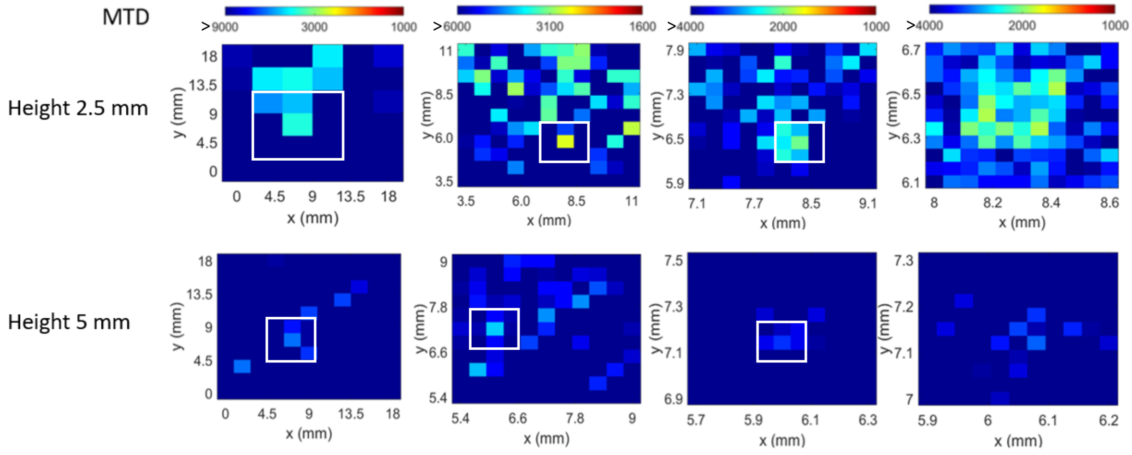


Figure 29: Analysis shows difficulty in isolating information leaking locations as probe shifts further away.

Phase II analysis (shown in Fig. 29) showed minimal improvement in MTD over phase I as the height increased. The scans also yielded different optimal locations for the EM SCA attack for different heights. The trade-off curves for the 3 heights (Fig. 30) show that both acquisition cost and marginal cost increase as the probe height increased.

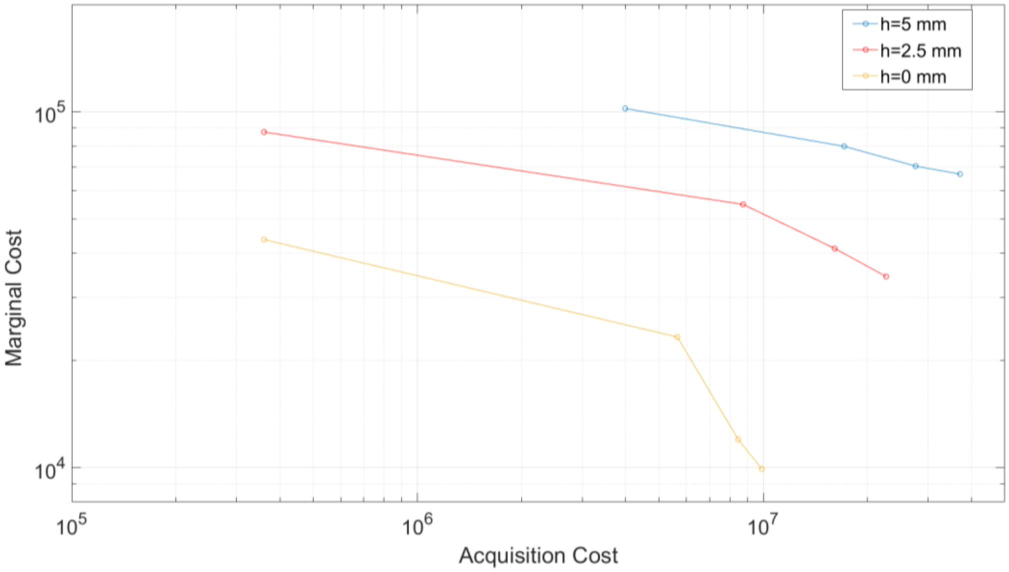
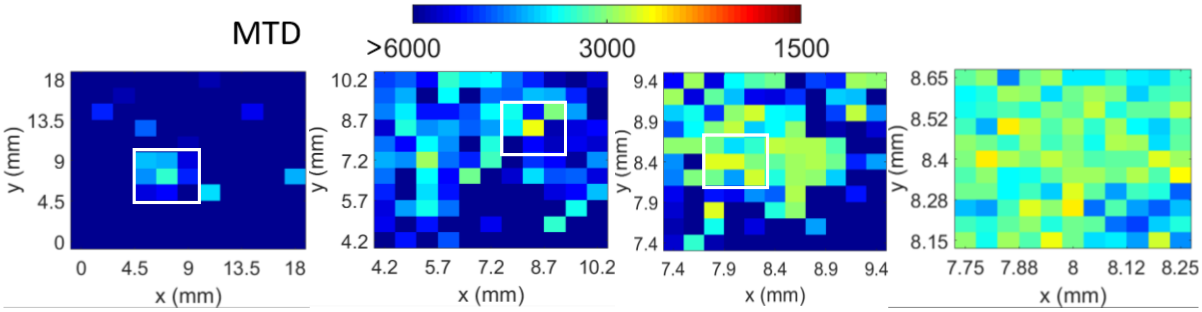


Figure 30: Marginal cost vs Acquisition cost for increasing probe height..

Although signal levels reduce, the main reason for degradation of marginal cost and increase in acquisition cost is the uncorrelated noise from background sources which have more influence as the probe shifts further away. In comparison with baseline, the acquisition time for the 2.5 mm case is ~2× slower and the 5 mm case is ~3× slower. Maximum file storage needed for the 2.5 mm case and the 5 mm case is found to be ~18 GB and ~22 GB.

5.5 Variation with Probe Size

This experiment used the probes with two probe sizes—10 mm and 25 mm with the tips of the probe touching the surface of the Sakura target. The largest probe could not complete phase I even after increasing the number of observers to $N_{\mathrm{obs}}^{4,\mathrm{I}} = 21 \times 21$ and measurements per position to $N_{\mathrm{e}}^{4,\mathrm{I}}$=10000. Scan results for byte 1 using the 10 mm probe is shown in Fig. 31. The MTD does not improve significantly with each scan in comparison with the baseline results shown in chapter 4 where the 1 mm probe was used. The trade-off curves comparing the two cases (Fig. 32) show the disadvantage of using larger probes for low resolution attacks, which is because of low SNR (See Section 3.1). Acquisition



Phase I Final Scan Phase II Scan 1 Phase II Scan 2 Phase II Scan 3

Figure 31: Scan results shown for byte 1 using a 10 mm probe for attack.

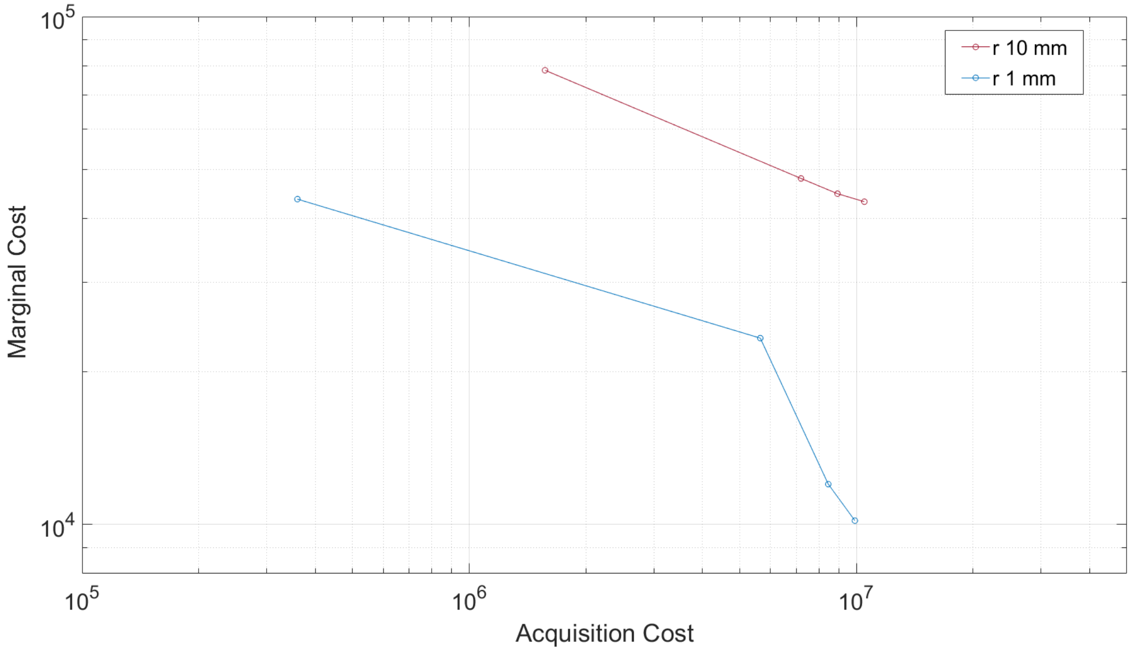


Figure 32: Trade-off curves show slower reduction in marginal cost with each scan for larger probe.

time to perform EM SCA attack for the larger probe ~ 32 hours. Maximum storage for performing this attack is ~16 GB.

5.6 Final Configuration for Fine-Grained EM SCA Attacks

From experiments performed in this thesis, the smallest probe with the probe touching the surface of the chip shows the fastest recovery of key bytes from AES. The final configurations for the 1 mm probe at 0 mm height which were obtained for both the target chips using a combination of MELR and FEHR approach are given in Table 4 and Table 5.

Byte	Orientation (o)	$x_b^{\text{opt},0}, y_b^{\text{opt},0}$(mm)	$mMTD_b^0$	Byte	Orientation (o)	$x_b^{\text{opt},0}, y_b^{\text{opt},0}$(mm)	$mMTD_b^0$
1	y	7.68,9.78	480	9	y	9.36,11.52	600
2	x	8.9,11	640	10	x	8.12,7.98	510
3	x	8.98,7.6	600	11	x	5.44,5.56	740
4	x	9.04,7.8	640	12	x	9.36,7.02	710
5	x	1.58,10.8	500	13	x	7.9,13.42	420
6	x	9.16,7.92	610	14	y	5.5,7.36	460
7	y	5.56,5.56	490	15	y	5.48,7.24	660
8	x	8.32,7.92	800	16	y	5.48,7.14	540

Table 4: Sakura Board Best EM SCA Attack Configurations

Byte	Orientation (o)	$x_b^{\text{opt},0}, y_b^{\text{opt},0}$(mm)	$mMTD_b^0$	Byte	Orientation (o)	$x_b^{\text{opt},0}, y_b^{\text{opt},0}$(mm)	$mMTD_b^0$
1	x	9.7,7.95	540	9	x	9.7,7.95	670
2	y	8.9,10.8	760	10	x	9.7,7.95	710
3	x	9.7,7.95	730	11	y	5.44,5.56	730
4	x	9.7,7.95	680	12	x	9.36,7.02	580
5	x	9.7,7.95	620	13	x	9.7,7.95	590
6	y	9.16,7.92	610	14	y	5.5,7.36	790
7	x	9.7,7.95	740	15	x	9.7,7.95	650
8	y	8.32,7.92	620	16	x	9.7,7.95	610

Table 5: Chipwhisperer Board Best EM SCA Attack Configurations

The final key $\boldsymbol{k}^{10}$ was identified as $\boldsymbol{k}^{10}$ =[19, 17, 29, 127, 227, 148, 74, 23, 243, 7, 167, 139, 77, 43, 48, 197]. Reversing the key schedule step, $\boldsymbol{k}^{0} = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]$ which is the original AES key.

5.7 EM SCA VS POWER SCA ATTACK

The power SCA attack followed the same procedure as the EM SCA attack except it is performed on a single set of 5000 traces collected by observing the V_{DD} to GND drop during the final AES cycle. This measurement is available through a port on the Sakura board [28], the power SCA recovered all bytes with less than 2500 measurements; thus, the marginal cost for the power SCA attack was 2500 and the acquisition cost was only 5000 measurements. Thus, the power SCA attack was ~2000× cheaper to implement with a marginal cost that was ~4× smaller compared to the fine-grained EM SCA attack described in this thesis. It is important to observe, however, that the chips were dedicated to performing only AES and no countermeasures were implemented; i.e., the best-case scenario for the power SCA attack. For example, the AES block can be integrated in a chip to encrypt data that is generated from other components and processes on the chip.

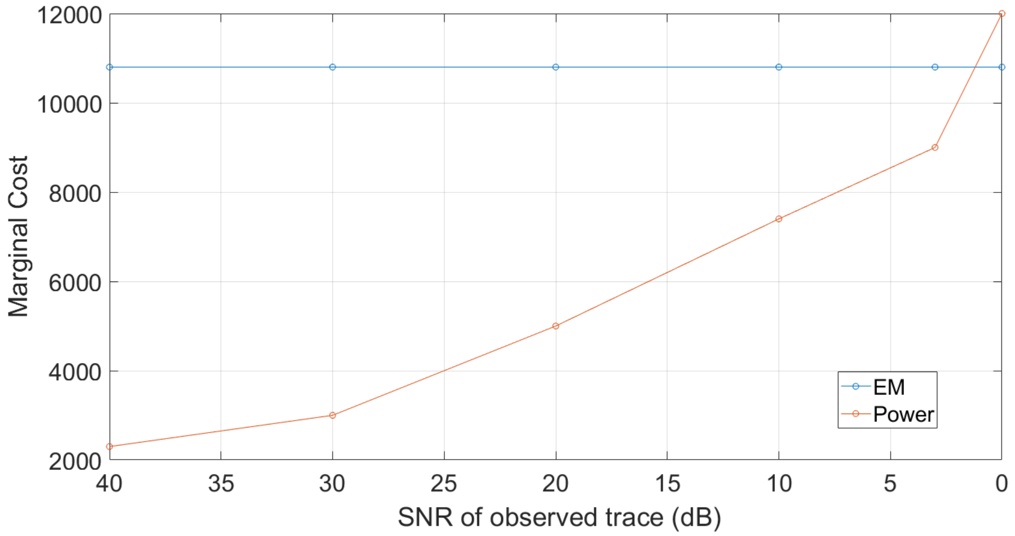


Figure 33: Change in the marginal cost of power analysis compared to EM analysis as random Gaussian noise is added to the system.

Therefore, any analysis of the total power drawn would also include noise from these additional components and processes. In contrast, fine-grained EM SCA attacks has the potential to be less affected by these.

To demonstrate the impact of the power drawn by background components on the effectiveness of the power SCA attack, a Gaussian random noise was added to the power trace and the marginal cost was observed as the noise signal's strength was increased from noise of magnitude 100× lower than signal to noise level equal to signal. The results are plotted with respect to the SNR in Fig. 33, which shows that if the power drawn by the AES component is less than half the total power, the fine-grained EM attack has a lower marginal cost.

Chapter 6: Conclusion and Future Work

The thesis presented a measurement protocol that increases the effectiveness of fine-grained EM SCA attacks. It presented a detailed description of the EM SCA attack procedure for AES and then presented an adaptive protocol to effectively implement fine-grained EM SCA attack. The proposed protocol is a greedy acquisition approach to search the space of possible configurations and identify optimal near-field measurement configurations for recovering AES keys. A baseline scenario using this measurement protocol was presented which showed significant speedup over the exhaustive acquisition approach in time and memory. Memory and cost would scale in proportion with key length for AES-192 and AES-256.

Further, the protocol was put to test for a variety of different scenarios, including changing the chip/board, probes, and probe heights, and the optimal configurations were identified. The EM SCA attack was compared to the power SCA attack; while it was found that the fine-grained EM SCA attack was less effective for the baseline scenario even with the proposed protocol, the thesis indicates that very different countermeasures are needed for countering the two types of attacks and performing intentional or unintentional obfuscating operations during AES encryption may not be sufficient countermeasures for fine-grained EM SCA attacks.

The proposed protocol is general enough to be used for other chips and boards implementing AES, and can also be adopted for other cryptographic algorithms. It can be improved further to reduce acquisition cost by reusing the data from previous scans to reduce the cost of each scan. The protocol will also be repeated with frequency domain analysis which may prove to be a more effective SCA attack.

References

[1] Genkin, D., Pachmanov, L., Pipman, I. and Tromer, E.,"ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in *Cryptographers' Track at the RSA Conference* Feb. 2016 ,pp. 219-235.

[2] Peeters, E., Standaert, F.X. and Quisquater, J.J.,"Power and electromagnetic analysis: Improved model, consequences and comparisons," in *Integration, the VLSI journal*, 40(1), 2007, pp.52-60.8.

[3] Genkin, D., Pachmanov, L., Pipman, I., Tromer, E. and Yarom, Y., "ECDSA key extraction from mobile devices via nonintrusive physical side channels," in Proc., *ACM SIGSAC Conference on Computer and Communications Security,* Oct 2016 ,pp. 1626-1638.

[4] Sauvage, L., Guilley, S. and Mathieu, Y., "Electromagnetic radiations of fpgas: High spatial resolution cartography and attack on a cryptographic module, in *TRETS* 2009, 2(1), p.4.

[5] Agrawal, D., Archambeult, B., Rao, J.R., and Rohatgi, P., "The EM side-channel (s): attacks and assessment methodologies", 2002.

[6] Kocher, P., Jaffe, J. and Jun, B., "Differential power analysis," in *Advances in cryptology—CRYPTO,* 1999 ,pp. 789-789

[7] G. Ding, Z. Li, X. Chang and Q. Zhao, "Differential electromagnetic analysis on AES cryptographic system," *2009 Second Pacific-Asia Conference on Web Mining and Web-based Application*, Wuhan, 2009, pp. 120-123.

[8] Homma N. et al., "EM Attack Is Non-invasive? - Design methodology and validity verification of EM attack sensor," in *proc. CHES,* 2014. Lecture Notes in Computer Science, vol 8731. Springer, Berlin, Heidelberg

[9] J. Coron and L. Goubin, "On boolean and arithmetic masking against differential power analysis, " in *Proc. CHES* 2000 , vol. 1965, pp. 231–237.

[10] Blomer, J., Merchan, J. G., and Krummel, V., "Provably secure masking of AES," in *SAC* , Springer, 2004, pp. 69–83

[11] Mangard, S., Oswald, E., and Popp, T., "Power analysis attacks: revealing the secrets of smart cards (Advances in Information Security)", Springer-Verlag New York,, 2007.

[12] Liu, P.-C., Chang, H.-C., and Lee, C.-Y., "A low overhead DPA countermeasure circuit based on ring oscillators,", in *IEEE Trans. on Circuits and Systems II: Express Briefs,* Vol. 57, July 2010, pp. 546–550.

[13] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom," ECDSA key extraction from mobile devices via nonintrusive physical side-channels," in *Proc. of the 2016 ACM SIGSAC CCS*, 2016, ACM, pp. 1626–1638

[14] M. Alam, H. Khan, M. Day, R. Callan, N. Sinha, A. Zajic, and M. Prvulovic, "One & done – A single-decryption EM-based attack on OpenSSL's Constant-Time Blinded RSA ," in *Proc. USENIX Security*, August 2018

[15] Unterstein, F., Heyszl, J., De Santis, F., Specht, R., "Dissecting leakage resilient PRFs with multivariate localized EM attacks - a practical security evaluation on FPGA," in *Proc. 8th*

International Workshop on Constructive SideChannel Analysis and Secure Design (COSADE 2017). Springer (2017)

[16] G. Li, V. Iyer and M. Orshansky, “Securing AES against localized EM attacks through spatial randomization of dataflow," in *Proc. HOST*, 2019, pp. 191-197.

[17] Pub, N.F., 2001. 197: Advanced encryption standard (AES). Federal information processing standards publication, 197(441), p.0311.

[18] www.nist.gov [Available online]

[19] A . Kumar, C. Scarborough, A. E. Yilmaz, and M. Orshansky, “Efficient simulation of EM side-channel attack resilience,” in *Proc. ICCAD*,2017, pp. 123 – 130.

[20] V. V. Iyer and A. E. Yilmaz, “An adaptive acquisition approach to localize electromagnetic information leakage from cryptographic modules,” *2019 IEEE Texas Symposium on Wireless and Microwave Circuits and Systems (WMCS)*, Waco, TX, USA, 2019, pp. 1-6.

[21] Heyszl J. *et al*., Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis”, Lecture Notes in Computer Science, Berlin, Germany: Springer, 2012, vol. 7771.

[22] R. Specht, J. Heyszl and G. Sigl, “Investigating measurement methods for high-resolution electromagnetic field side-channel analysis,” *2014 International Symposium on Integrated Circuits (ISIC)*, Singapore, 2014, pp. 21-24

[23] www.langer-emv.de/en/category/lf-passive-100-khz-50-mhz/36

[24] https://www.langer-emv.de/en/product/preamplifier/37/pa-303-bnc-set-preamplifier-100-khz-up-to-3-ghz/519

[25] www.keysight.com/en/pdx-x201844-pn-MSOX3024A/mixed-signal-oscilloscope-200-mhz-4-analog-plus-16-digital-channels?cc=EE&lc=eng

[26] https://www.keysight.com/us/en/products/oscilloscopes/infiniium-real-time-oscilloscopes/infiniium-s-series-oscilloscopes.html

[27] https://wiki.newae.com/CW305_Artix_FPGA_Target

[28] http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html

[29] https://github.com/newaetech/chipwhisperer

[30] https://www.riscure.com/product/em-probe-station/