[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

Frequency Domain Horizontal Cross Correlation Analysis of RSA

Ebru AKALP KUZU[1], Ali TANGEL[2], Sıddıka Berna ÖRS YALÇIN[3]
[1]*TÜBİTAK-BİLGEM Gebze, Kocaeli, Turkey*
[2]*Kocaeli Üniversitesi, Elektronik ve Haberleşme Mühendisliği, Kocaeli, Turkey*
[3]*İstanbul Teknik Üniversitesi, Elektronik ve Haberleşme Mühendisliği, Istanbul, Turkey*
ebru.kuzu@tubitak.gov.tr

***Abstract*—This study shows that a previously published cross correlation based power analysis (CCPA) attack applied to the Montgomery Ladder exponentiation steps of a Rivest Shamir Adleman (RSA) implementation can be improved by working in frequency domain. It is shown that utilizing cross correlation values of discrete Fourier transform (DFT) coefficients instead of time samples, requires lesser power traces to retrieve the key bits of the target implementation. In addition, instead of using DFT coefficients corresponding to the whole measured frequency band, using a few DFT coefficients corresponding to lower bands, even under the first harmonic of the target clock is also an improving factor on the performance of the CCPA. Practical and theoretical results are also compared to both domains. To the best of our knowledge, this is the first study to show the frequency domain applicability and superiorities in terms of horizontal CCPA type attacks.**

***Index Terms*—ciphers, classification algorithms, data security, leakage currents, public key cryptography.**

I. INTRODUCTION

Side channel analysis (SCA) [1] is a family of physical attacks that enables to break mathematically strong cryptographic algorithms if appropriate countermeasures are ignored on the target devices. Today, most of the digital cryptographic devices are based on complementary metal-oxide semiconductor (CMOS) technology. The instantaneous power consumption of CMOS devices varies according to the processes carried out or the data processed [1]. Power analysis is a SCA family, which employs the power leakage of devices when executing cryptographic algorithms. Simple power analysis (SPA) [1], differential power analysis (DPA) [1-6], correlation power analysis (CPA) [7-8], collision power analysis [9-12] are power analysis types. In a cryptographic algorithm implementation, main vulnerability used by SPA [1] is process differences performed depending on the partial key values. Because different operations create different shaped power trace regions, SPA attacks are performed by visual inspection of these regions on a single or several power traces. On the other hand, the main vulnerability used by DPA [1-6] is that processing of partial key related intermediate values produces power trace regions with different amplitudes associated with their Hamming weight (HW) or Hamming distance (HD). DPA attacks are performed by statistical analysis of these regions on the power traces collected during the algorithm execution with the same key and different plaintext values.

"Distance of means" test is a classical tool for DPA attacks. Correlation power analysis (CPA) [7-8] is a variant of DPA and uses correlation analysis of the power traces with the predicted power consumption models. These models are created by calculating HW or HD of the partial key dependent intermediate values. Collision type SCA [9-22] is another power analysis family and based on the detection of the similar power trace regions produced by usage of same operand when a specified operation related with the key parts takes place. If a collision is detected, the related partial key value is classified as the same type with the collided one. Collision based SCA can use DPA [8], CPA [11-14], CCPA [7], [10], [13], [15-19] or combination of all these method with various clustering algorithms [20-22] to compare the respective power trace regions. If collision detection is performed by comparing different time instants on a power trace of a single run, it is called as the horizontal analysis [9-13], [15-17]. Otherwise, if comparisons are made between the regions belonging to the same time instants of the one more power traces, produced by algorithm execution with different inputs, this is called as vertical collision analysis [10], [14], [18].

This study introduces frequency domain counterpart of a previously published cross correlation based collision attack [15]. Both attacks are applied to the Montgomery ladder exponentiation steps of a RSA [24] implementation. CCPA attacks are commonly utilized for exponentiation or double-add steps of asymmetric algorithms such as RSA and elliptic curve (EC) cryptography. In [4], horizontal CCPA is applied to determine the locations of the double and add operations in the binary exponentiation steps of the RSA implementation. In [18], vertical CCPA is utilized for attacking to exponentiation steps of a RSA implementation having the binary-with-random-initial-point (BRIP) message blinding countermeasure. In [18], vertical correlation values are combined by summing up them in horizontal directions. In [14], vertical CCPA is used against a multiply always exponentiation steps of a RSA implementation to distinguish power trace regions of consecutive modular operations. In [15] which is the time domain counterpart of our proposed attack, CCPA is utilized against the Montgomery ladder (ML) exponentiation steps of an application specific integrated circuits (ASIC) RSA implementation, in which multiplication operands are retrieved from different locations according to the key bit types. In [15], a single constant reference bit power trace region is compared to the regions belonging to all other bits to classify them. In [16] attack in [15] is improved using all the secret key bit regions as reference. In [19], it is shown that the attack in [15] can

Digital Object Identifier 10.4316/AECE.2022.02001

1582-7445 © 2022 AECE

[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

be improved by selecting more correlative power trace points. In [20], it is shown that the attack in [15] can be improved by using "selected message" values.

For time-domain DPA, CPA and CCPA attacks, power trace regions of each separate algorithm execution should be well-aligned around the interested operation. However, timing variations between algorithm steps, several countermeasures such as adding dummy operations or triggering properties of the measurement setups can cause the misalignment of these regions. In addition, switching noise introduced by the other operations executed in parallel and the natural noise of the electronic circuit have a negative effect on the attacks performance. Recently, frequency-domain attacks are becoming an alternative to the time-domain counterparts because of their possible noise and jitter resistance [25-27]. If noise and actual leakages present in different frequency bands, noise can be isolated from the leakages, thus its effects can be mitigated in the frequency-domain [25]. Another advantage of the frequency-domain power analysis is that in frequency-domain, misalignment appears as a phase shift and its negative effects are less important compared to the time-domain. Frequency-domain CPA and DPA were first time proposed in [25-27] and efficiency of frequency-domain is verified by these works. Also, in [25], it is experimentally shown that power leakage in frequency-domain is not dependent on the clock frequency of the target device. In [28] it is shown that beside the amplitude, the shape of traces can also be considered for attacks in frequency domain. In [29-30], to enhance CPA or DPA, filtering was applied around clock signals of the algorithm execution and its harmonics. Furthermore, in [31], a mathematical model for power and electro-magnetic (EM) leakage in the frequency-domain are presented. This model also shows that actual leakage is not dependent on the operating clock frequency but it is only dependent indirectly on the maximum clock frequency, in which the circuit can operate. In [32], processing of traces in frequency domain is used for second-order CPA type attacks. In [33], CPA analysis in frequency domain applied to the EM radiation of RSA algorithm is implemented on Raspberry Pi platform. The theoretical results in [31] show that, in line with the practical studies presented in [26], the actual leakage does not need to be found around operating clock harmonics.

Unlike previous studies, this study suggests a CCPA attack in the frequency domain. It is called as Frequency-domain Cross Correlation Power Analysis (FCCPA). The proposed method uses amplitude of Discrete Fourier Transform (DFT) coefficients for the cross correlation analysis instead of time samples. The method is successfully applied to the Montgomery Ladder (ML) exponentiation steps of a RSA implementation. The proposed frequency domain CCPA has been shown to have advantages over time domain in two respects. The first one is that using all DFT coefficients representing the entire measured band, the FCCPA attack succeeded with lesser power traces compared to the CCPA attack. This result can be explained by the fact that the frequency domain is more immune to alignment problems as mentioned in previous DPA and CPA attacks [25-27], [31]. This property is also a healing factor for CCPA attack in this domain. The second one is that, rather than the entire measured frequency band, the use of DFT coefficients corresponding to the lower bands even under the first clock harmonic of the target, also improves the performance of the FCCPA. This result can be explained by the frequency domain leakage model given in [31] and frequency domain DPA or CPA attacks in [25-27], [31], which show that lower frequency bands can be more important because of their better leakage SNR. As a result, experimental results in this study show that, advantages of working in frequency domain for DPA and CPA attacks mentioned in [25-27], [31] are also valid for our frequency-domain CCPA.

Remaining outline of this paper is as follows: Section 2 gives information about RSA cryptosystem and its implementation types. Section 3 and Section 4 details the previous CCPA method and the FCCPA methods we propose as a frequency domain adaptation of this method. Section 5 presents the experimental results of FCCPA and their comparisons to CCPA. Section 6 is the conclusion.

II. RSA Cryptosystem Implementations

RSA is the first known "Public Key" asymmetric encryption algorithm. An algorithm being asymmetrical means using separate keys for encryption and decryption. Data encrypted with the public key must be decrypted with a private key. Although it is possible to encrypt and decrypt the communication using the RSA, normally symmetrical algorithms are preferred for this work. Symmetric algorithms such as data encryption standard (DES) and advanced encryption standard (AES) use same key for encryption and decryption operations and the key values must be kept secret. Secure key sharing, which is one of the most important problems in the use of these symmetric algorithms is provided by "Diffie-Helman Key Distribution" [34] type protocols that use asymmetric algorithms such as RSA and EC encryption. In addition, signing and signature verification protocols such as digital signature algorithm (DSA) [35], which are used to understand that a data comes from the right source, also work with these asymmetric algorithms.

RSA algorithm mathematically consists of a modular exponentiation loop. Let "M" is a large n-bit sized value and used as modulus. "M" is obtained by multiplying the two n/2 bit sized prime values p and q. The function Φ(M) is defined as (1).

$$\Phi(M) = (p-1)(q-1) \tag{1}$$

Let "e" and "d" be two integers satisfying the condition (2).

$$e.d = 1 \bmod \Phi(M) \tag{2}$$

The "e" value with the modulus value "M" is called as the public key and the "d" value is called as the private key. The encryption, and the decryption operations are performed as in (3) by using secret exponent "d" and public exponent "e".

$$S = Y^d \bmod M,\ Y = S^e \bmod M \tag{3}$$

The security of the RSA algorithm is based on the fact that factoring the large modulus M into its prime factors p and q is as difficult as finding the private key "d" when the public key pair "e" and "M" are known. Bit size of the modulus is called as the bit size of the RSA algorithm. This size can be in the range of 256-4096. Exponentiation loop of RSA algorithm includes hundreds of modular multiplication

[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

or squaring operations. There are some exponentiation algorithms to make these calculations efficiently. A practical and simple solution is "binary square-multiply" algorithm. This algorithm has SPA vulnerability, as it includes a conditional branch state depending on the secret key bit values. Coron [36] proposed a modified square-multiply always exponentiation algorithm to defeat this vulnerability. While the added dummy operations provide resistance to SPA-type attacks, they make the implementations vulnerable to other SCA types such as Safe-Error attack [37]. Joe and Yen [38] proposed an enhanced SPA countermeasure based on another modular exponentiation algorithm known as Montgomery ladder (ML) [23]. This algorithm has no conditional branches and no dummy operations. It performs both of the regular square and multiply operations for each bit of the secret exponent. The target RSA implementation in this study also uses the ML algorithm as the exponentiation method. Although ML is resistant against SPA type attacks because of its redundancy in terms of executed multiply-square operations, it is still vulnerable to DPA-CPA-and Collision type SCA methods as shown in this study.

III. BENCHMARK TCCPA

Before explaining the FCCPA attack, it is important to understand the time-domain counterpart TCCPA attack [15] which is applied to the ML exponentiation steps of a RSA implementation. It is a [15] cross correlation based collision type attack which tries to catch the similar power trace regions related with the secret bit operations in the ML loop. Source of the similarities can be explained as operand usage from similar location. To perform the CCPA attack, power trace regions of each key bit is correlated with the region of a known fixed reference bit. Here, the reference region is used as a template and cross correlation between this template and others are used as a measure of their similarity. In particular, by using these correlation values, each of the key bits are classified as the same (called type0) or different type (called type1) with the reference bit. An exponent bit is called as type0 bit if its value is same with the preceding bit, otherwise it is called as type1 bit.

Meaning of type0 and type1 bits are arise from implementation details of the target implementation. The target Montgomery Ladder steps are given in Table I. Here "M" is p bit wide modulus, "Y" is the base value and "d" is the binary representation of the secret key. In target implementation as a modular multiplication, "Montgomery Modular Multiplication" algorithm is used and "MontMul" abbreviation stands for this. By looking at the exponentiation steps of the target ML, it is seen that one of the two registers named as A0 and A1 are used for the first operands and another register named as B is used for the second operands of the multiplication and squaring operations. After multiplication and squaring operations for each secret bit, current bit and preceding bit values are compared to check that if they have same or different values. If the processed bit is same as with the preceding one, the content of register B is directly generated by the previous multiplication operation result and these kind of bits are called as type0. Otherwise B register content is read from either registers A0 or A1 and these bits are called as type1. By looking at these operation steps, it can be seen that type0 bits have more common operations with each other and their leakage signals should have more similarities compared to the type1 bits. In the CCPA method [15] time instants corresponding these operation steps are selected as attacking point and cross correlation values are used to classify the leakage signals. Cross correlation values between the leakage signals of a type0 reference bit and with the signals of all the other type0 bit, should have higher values compared to the one between the reference and all the other type1 bits. The values calculated for each bit are used in two different ways to decide to its type. In the first approach, the correlation values obtained from each run of the algorithm for a given bit are summed and compared with a threshold value. If the correlation sum is greater than the threshold, the type of this bit is decided as the same as the reference, ie type0 otherwise, different from the reference, ie type1 bit.

For the second approach, if correlation values for each power traces are greater than the threshold, an estimation counter for type0 bit, otherwise an estimation counter for type1 bit is increased. When correlation values of all of the traces are evaluated, type of the bit is decided according to the corresponding counter. It is shown in [15] that the first approach works better. In this proposed FCCPA method, also first approach is preferred.

TABLE I. ATTACKED MONTGOMERY LADDER IMPLEMENTATION

Inputs
$M=m_p m_{p-1}..m_1 m_0$
$R=2^p$
$R^{-1}=2^{-p}$
$Y=y_p m_{yp-1}..y_1 y_0$
$d=d_p d_{p-1}..d_1 d_0$
Outputs:
$S=Y^d \bmod M$

```
A0=MontMul (Y,R^2 )
A1=MontMul (A0,A0)
For i=p-1 to p
 If(d_i=0  & d_{i+1}=0)
   A1=MontMul(A1,B)
   A0=MontMul(A0,B)
   Write square result to B
 Else If(d_i=0&d_{i+1}=1)
   A1=MontMul(A1,B)
   A0=MontMul(A0,B)
   B=A1
 Else If(d_i=1 & d_{i+1}=0)
   A0=MontMul(A0,B)
   A1=MontMul(A1,B),
   B=A0
 Else If(d_i=1 & d_{i+1}=1)
   A0=MontMul(A0,B)
   A1=MontMul(A1,B),
   Write square result to B
S=MontMul(A0,1)
Return S
```

[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

IV. The Proposed FCCPA Method

In this study, FCCPA method is applied to the Montgomery Ladder (ML) exponentiation steps of a RSA implementation like the previous time domain CCPA attack [15]. In contrary to the previous CCPA [15-19], the proposed FCCPA method uses selected DFT coefficients of per time regions. DFT transform decomposes a time-domain signal into sinuses and cosines of different frequencies. It represents a signal by how much each frequency contributes to the construction of the signal. Because at a given frequency, absolute values of DFT coefficients include most of the information that the signal contains, it is expected that FCCPA analysis in the frequency-domain works in a similar way to the time-domain CCPA method. FCCPA uses cross correlation analysis to determine the measure of the similarity between Discrete Fourier Transform (DFT) coefficients of power trace regions belonging to the each of the key bits.

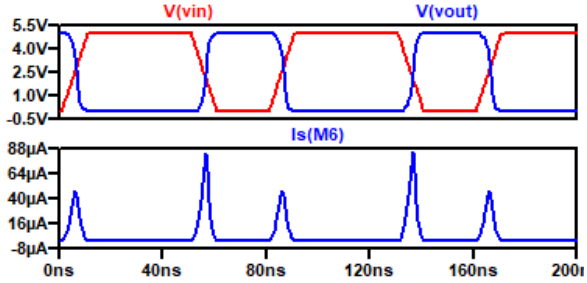

Figure 1. CMOS inverter leakage currents with changing input output states

In general, like other passive SCA types, frequency domain has several advantages for FCCPA attacks. One of the advantages is that, misalignments of the traces regions have a lesser negative effect on the corresponding DFT coefficients. To apply the CCPA [12], [11] trace regions belonging to the interested operations are extracted from power traces. It is important that these trace segments must be well aligned around the focused operation. Because there are time deviations for each execution of the target algorithm steps and also non-ideal triggering, due to the unstable conditions of measurement setups, displacement errors along with the trace regions occur. As with CPA and DPA attacks, if the errors are significant, the performance of CCPA-type attacks in the time domain suffers and requires much more traces. However, as the frequency spectrum is more resistant to time drift, misalignment becomes less significant, which gives the FCCPA method an advantage. Another advantage of operating in frequency-domain is that the correlation values are computed independently for each frequency component. This enables the attacker to eliminate the information that is not related to the key-dependent operations. To understand which frequency band may include more information, it will be useful to look at the models explaining the source of leakage which is used by DPA and CPA type attacks. The source of the operand dependent power leakage in CMOS based digital circuits is explained by the switching current behavior of the inverters. When a CMOS circuit output state is changed, there are two main source of the leakage: One of them is the charging current drawn by the output load capacitance. The other one is the temporary short circuit current of instant Gnd-Vdd connection. At the logic level, dynamic power consumption behavior is approximated by HW/HD modeling. These models assume that all of the cells and all of the 0-1and 1-0 transitions consume equal amount of power. DPA and CPA attacks use this simplified logic level behavior [29]. When HW or HD approaches are used, transient behavior of the leakage during the switching of the output of an inverter is disregarded [26]. For time based and frequency based CCPA analysis, time slots or DFT coefficients belonging to these time slots are correlated to each other. Therefore, for CCPA and FCCPA, instead of HW or HD models, which represent a single time instant, transient leakage behavior of the inverter is more important. For the transient behavior simulation of a CMOS inverter at the analog level, lumped-C model can be used as a simplification [30]. In this model, all of the intrinsic parasitic capacitance of the transistor and the capacitance of the wires and subsequent cells are modeled as a common capacitance C_L at the output of the inverter. The effect of the number of subsequent cells and effect of difference for the capacitance of wires bounded to the inverter can be modeled by this C_L. In Fig. 1, SPICE simulation of the lumped-C model of a CMOS inverter is given. As can be seen for 1-0 and 0-1 transitions, approximately triangular shaped currents with different maximum amplitudes during different time duration are driven. The 1-0 transition of the output contains only direct path or short circuit current. However the 0-1 transition contain both direct path current and charging current of the C_L, and as a result, its amplitude is bigger.

In Fig. 2 (a), direct path current of the 0-1 state change of a CMOS inverter for two different C_L values are given. When C_L is changed, amplitude and duration of the currents also changes. In Fig. 2(b), DFT coefficients of these leakage currents are given. It is seen that the amplitude of the DFT coefficients decreases and eventually disappears towards the higher frequency bands. By using a similar approach with [26], spreading of the power leakages in frequency domain can be represented by taking the Fourier Transform of these triangular shaped currents. Suppose that direct path current occurs within the time duration of t_{sc} and peak current value I_t is reached at the time at_{sc}. In that case the Fourier transform of two triangular shaped pulses with the base values of at_{sc} and t_{sc}-at_{sc} with the height of I_t can be calculated by using (4). Here, t_{sc} value is dependent on the maximum clock frequency at which the circuit can operate and is only indirectly related to the actual operating clock frequency [27]. The other parameter "a" represents the rise time of the current and it is related to the operating clock rise time [40], [41].

$$P(f)=\int_0^{at_{sc}}\frac{I_t}{a.t_{sc}}te^{-j2\delta ft}d_t+\int_{at_{sc}}^{t_{sc}}\frac{I_t}{a.t_{sc}}te^{-j2\pi ft}d_t$$

$$=\frac{-jI_t}{2\pi^2f^2.t_{sc}}\times \tag{4}$$

$$\left[\frac{1}{a}\sin(a\pi ft_{sc})e^{-j\pi fat_{sc}}\frac{1}{a-1}\sin((1-a)\pi ft_{sc})e^{-j\pi f(at+1)_{sc}}\right]$$

Frequency model formulation given in (4) indicates the presence of leakage power in the entire frequency band, and its practical upper limit is the bandwidth of the acquisition system. However, its value changes inversely with the frequency. Especially in a noisy measurement environment,

[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

it is expected that for higher frequencies, signal to noise ratio (SNR) of the leakages get worse. As a result, choosing most important few low frequency components of the DFT values, even under the operating clock frequency of the target device may increase the performance of the frequency-domain CCPA attack.

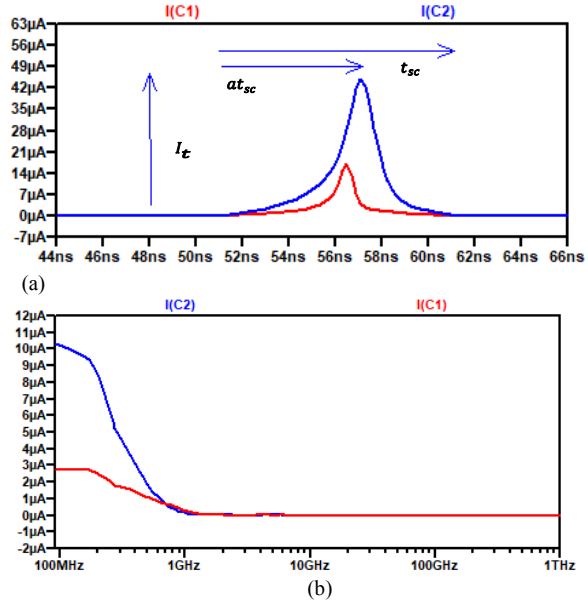

Figure 2. CMOS inverter simulations: (a) 0-1 state change leakage currents for 2 different C_L values. (b) Corresponding frequency components of these leakage currents

First step of the FCCPA analysis is the extraction of the trace segments corresponding to the operations of the each key bit. From each power trace Pi, the regions Pi_1, Pi_2, …, Pi_{1w-1} of a key bit "jϵ1, 2,…, w" are extracted. Here w=1024 is the bit size of the target RSA operation. Each extracted region Pi_j contains whole of the acquired N time samples $Pi_j=\{x_{N-1}, x_{N-2},\ldots, x_0\}$. The regions to be extracted on a typical leakage signal are shown in Fig. 3 within the rectangles. For each measurement, the trace segments corresponding to a chosen reference bit "r" is labeled as the reference region.

Next step is the calculation of DFT coefficients for each segment. For the sampling frequency $f_s=1/T_s$, with the resolution frequency of $f_0=2\Pi f_s/N$, the DFT coefficients $Xi_j(f_n)$ corresponding to the frequencies $f_n=n.f_0$, n ϵ [0, N-1] are calculated as given in (5).

$$Xi_j(f_n)=\sum_{k=0}^{N} x_k.e^{(-i2\pi nk/N)} \tag{5}$$

Because DFT transform is symmetrical, only absolute values of one half of the DFT coefficients $Fi_j(f_n)=abs(Xi_j(f_n))$ are stored into a N/2 dimensional vector Fi_j as described in (6) and used for cross correlation calculations.

$$Fi_j=\{Fi_j(f_0),Fi_j(f_1),\ldots Fi_j(f_{(N-1)/2}))\} \tag{6}$$

In this step, it is important finding the range of the current. As emphasized in [31] the low frequency components are more important in terms of SNR. For our case also, it is expected that, using only the most important lower frequency regions gives better results. First n1 coefficients in vector Fi_j corresponding to the lower frequency band $0\ldots f_{n1}$ are extracted and named as Fi'_j. The next step is the calculation of cross correlation values between DFT vectors. For i-th execution of the algorithm, frequency vectors Fi'_j containing the selected n1 DFT coefficients corresponding j.th bit of the secret key are correlated with the vector Fi'_r which is the reference DFT vector of the same execution. By using absolute values of selected DFT coefficients, for each exponent bit, cross correlation vectors $FCi'_{rj}=\{FCi'_{r1}, FCi'_{r2}, \ldots, FCi'_{rw-1}\}$ are generated. Calculation of these correlation values are described in (7). Here, the frequency vector of the j.th secret bit and reference bit r of the i.th power trace have mean values of $\mu i'_r$, $\mu i'_j$ and variance $\sigma i'_r$, $\sigma i'_j$ respectively.

$$FCi'_{rj}=CorrCoeff\left(Fi'_j,Fi'_r\right)=\frac{Cov\left(Fi'_j,Fi'_r\right)}{\sigma i'_j.\sigma i'_r}$$

$$=\frac{\sum_{n=1}^{n1}\left(Fi_j(f_n)'-\mu i_j\right)\left(Fi_r(f_n)'-\mu i_r\right)}{\sqrt{\sum_{n=1}^{n1}\left(Fi_j(f_n)'-\mu i_j\right)^2\left(Fi_r(f_n)'-\mu i_r\right)^2}} \tag{7}$$

The last step of the FCCPA analysis is the estimation of each secret bit types. In order the attack to be successful, it is necessary to use many power traces in which different base values are treated with the same secret exponent "d" and combine calculated correlation coefficients from each trace. Otherwise the method does not work or its performance decreases too much.

One of the reasons to calculate better common correlation coefficient is the switching noise present in each interested leakage region. As detailed above, the implementation weaknesses used by the presented frequency domain and previous time domain cross-correlation-based attacks are reading data from different memory locations depending on the type of the key bits. During the execution of such interested operations, HW or HD changes of the data carried from a certain memory location also causes a "data dependent" power leakage. This power leakage adds a "switching noise" component to the power measurements as it has no part that can be used by the attack and happens simultaneously with the interested operations. It is aimed to decrease this noise by using many curves measured during the transport of random HW or HD values.

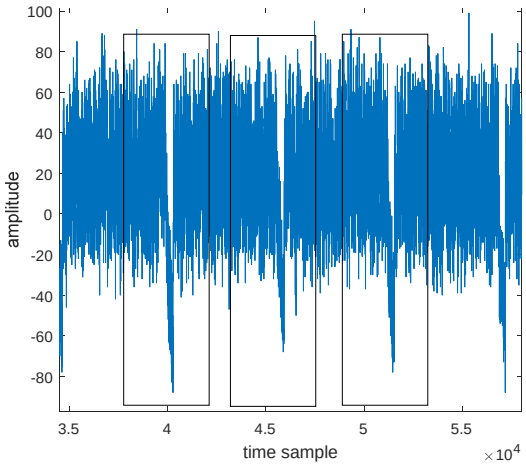

Figure 3. Extracted areas on a typical leakage signal

Another reason for using many curves is the existence of electronic noise in each power leakage measurement. By using multiple curves, it is aimed to reduce the components

[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

from this noise just like those from switching noise. Thus, while a common correlation value is generated from all of the calculated correlation values, only key bit dependent effects strengthen each other and others diminish. As a result, required correlation values are obtained.

TABLE II. CALCULATION OF BIT TYPES

Inputs
$FCi_{rj}'=\{ FCi_{r1}', FCi_{r2}', ..., FCi_{rw-1}' \}$

Outputs:
$dt=\{dt_{w-1}, dt_1, dt_0\}$

$FCi_{rjsum}'=0$
trsehold=0
For i=1 to M do
 For j=w-1 to 1 do
  $FCi_{rjsum}'= FCi_{rjsum}'+FCi_{rj}'$
  If ($FCi_{rjsum}'+FCi_{rj}'$>treshold)
   dt_j=type0
  Else
   dt_j=type1
  update treshold
 Return $dt=\{dt_{w-1}, dt_1, dt_0\}$

Algorithm given in Table II describes the estimation procedure for the type of the secret bits, based on the sum of correlations of DFT coefficients. As explained before, the "FCi'$_{rj}$" vectors contain the cross correlation values of DFT coefficients between the leakage regions of reference bit and the regions of the other secret bits. Here "dt" is the binary type vector representation of the secret exponent "d", "w" is the number of the secret bit values. For each power trace i, FCi'$_{rjsum}$ value, which is the sum of the correlation alues of j.th bit, are updated and compared to an updated threshold value. According to this comparison, type dt_j of each of the bit d_j is decided. If the calculated mean correlation value is greater than the threshold, type of the target bit is decided as type0 which is the same with the reference bit. As explained before, type0 bit means that the bit d_w has the same value with the preceding bit. Otherwise, the type of the bit is judged to be type1, meaning it has a different value from the previous bit. As the threshold value, averages of the sum of the neighboring 50 bits cross correlation coefficients are used.

V. EXPERIMENTAL RESULTS

Measurements are recorded by using a Tektronix digital phosphor oscilloscope as the chip making calculations for random messages with the same private key. Measurements are taken using a differential probe connected across a 1-ohm resistor tied in series to the power line of the target circuit. The acquisition sampling rate was 100 Msample/sec.

As a preprocessing step of the attack, power trace regions corresponding to the interested operations of each bit in the exponentiation steps are extracted and DFT coefficients are calculated. In Fig. 4, single-sided amplitudes of DFT coefficients of a sample trace region are given.

As the final step of the attack, cross correlation values of a bit calculated for each traces are summed and divided by trace number and compared to a threshold value. As shown theoretically in [42] it is possible to calculate a better common correlation value simply by averaging correlation coefficients. Mean cross correlation values of DFT coefficients of each of the key bits with a chosen type0 reference bit (bit 500) is given in Fig. 5 (a). Here all off the DFT coefficients represents 0-50 MHz frequency band which correspond to the half of the sampling frequency band. For the analysis, 28.000 power traces are used. The green line shows the used threshold value.

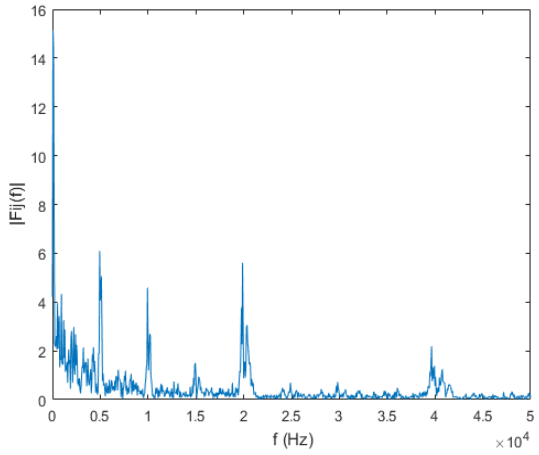

Figure 4. Single sided amplitude spectrum of a sample trace region for 0-50 MHz frequency band

In Fig. 5(b), same results are given for only those DFT coefficients representing 0-0.5 MHz frequency bands. This band is selected because it contains the DFT component having the highest amplitude.

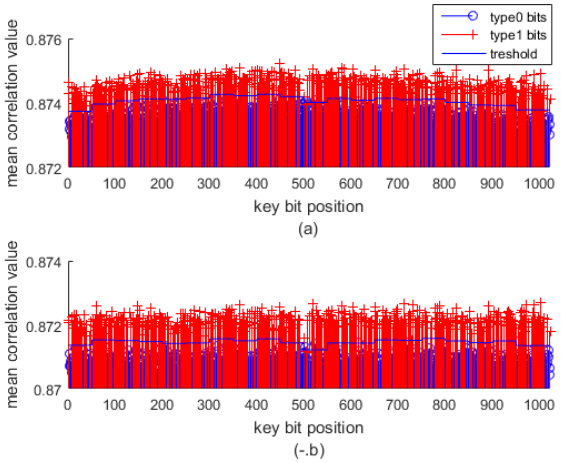

Figure 5. Mean correlation values of DFT coefficients for 0-05 and 0-50 MHz frequency bands

It can be seen that when all of the DFT coefficients representing the whole measured band is used, mean cross correlation values have a rising amplitude as the corresponding bit positions are approached to the reference. This behavior indicates that trace segments as well as their DFT coefficients are not statistically independent over time. Because noise founding in a power trace have more dependency at the neighboring points [40], the noise included in each trace segment make more contribution to the calculated correlation values when the segments approach to the reference. Because this behavior is due to the noise and independent from the corresponding bit types, it also negatively affects the attack performance. However,

[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

this appearance in the correlation curve reduces and even disappears when lower frequency band is used as shown in Fig. 5(b). The choice of lower band DFT components which have better SNR values, exhibits less statistical dependency between represented trace segments because of their locations. These make the threshold calculation and key bit dependent correlation calculations better. By this way, separations of the different bit types and the performance of the attack increases.

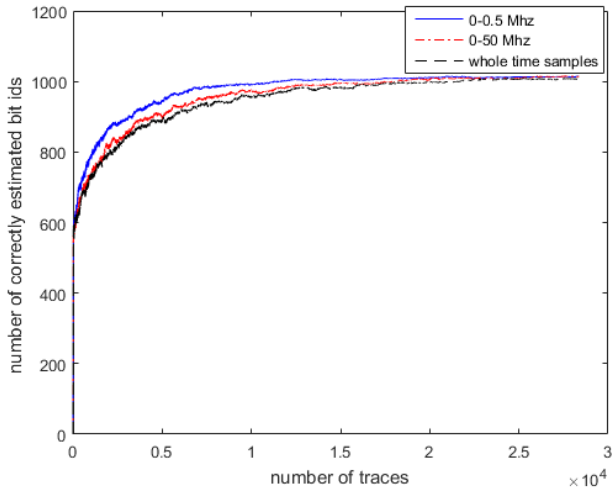

Figure 6. Number of correctly found bit types with increasing number of traces

In Fig. 6, the number of correctly found bit types with increasing number of power traces is given. Here, black line shows the results when all of the time-domain samples are used for time-domain CCPA. Red line shows the results when half of the frequency-domain samples representing the whole of the 0-50 MHz measured interval for FCCPA. Blue line shows the results when DFT coefficients representing 0-0.5 MHz frequency band interval are used. It is clear that FCCPA works better compared to the CCPA when DFT components corresponding to the whole of the measured frequency band are used. Also, when the lower frequency components are chosen, FCCPA gives much better results.

VI. Conclusion

In this study, it is shown that a previously published cross correlation based power analysis method, which is applied to the Montgomery Ladder exponentiation steps of a RSA implementation can be improved by working in frequency domain. The proposed attack utilizes cross correlation values of DFT coefficients instead of time-domain samples. Like in previous time-domain counterpart, this attack needs to use fixed known reference bit. It is experimentally shown that frequency-domain attack works faster than time-domain attack when all of the DFT coefficients corresponding to the whole of the measured frequency band are used. As a result, it is shown that, as mentioned in previous frequency domain DPA and CPA type attacks, noise and jitter robustness of frequency domain compared to the time domain is also a healing factor for the CCPA type attacks in this domain.

In addition, instead of using whole of the DFT coefficients which includes several harmonics of the operating clock frequency of the target circuit, using a few DFT coefficients corresponding to a lower band, even under the first clock harmonic of the target is also an improving factor on the performance of the FCCA. The reason behind the better performance of the lower frequency bands can be explained because of their better SNR values, like other DPA and CPA attacks. It is clear that frequency domain enables the attacker to choose the components that having better leakage SNR and by this way it can improve the attack performance of the FCCPA.

It is also shown that dependency of DFT coefficients corresponding to the time samples in the trace regions are increasing when these regions are getting closer to each other. One reason behind this behavior is that, electronic noise of neighboring points on a trace are more related and as a result, more correlated to each other. However, in lower frequency band, SNR values of DFT coefficients of each segments are getting better and effect of this dependency diminishes. As a result, the steepness of these lower band correlation values provides better threshold calculations and better separation of target bits.

As a disadvantage of frequency-domain, it can be said that some extra computing power is needed for calculations of DFT coefficients. However, FCCPA requires lesser number of power traces and much lesser number of points for cross correlation calculations. Showing this advantageous property of FCCPA is the main contribution of this study.

Acknowledgment

The authors would like to thank to TUBİTAK BİLGEM for providing measurement environment for this study.

References

[1] P. C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” Annual International Cryptology Conference, pp. 104-113, August 1996. doi:10.1007/3-540-68697-5_9

[2] P. C. Kocher, J. Jaffe, B. Jun, P. Rohatgi, “Introduction to differential power analysis,” J Cryptogr Eng 1, 5–27, 2011. doi:10.1007/s13389-011-0006-y

[3] T. S. Messerges, E. A. Dabbish, R. H. Sloan, “Investigations of power analysis attacks on smartcards,” Smartcard 99, 151-161, 1999. doi:10.1.1.137.8671

[4] T. S. Messerges, E. A. Dabbish, R. H. Sloan, “Power analysis attacks of modular exponentiation in smartcards,” International Workshop on Cryptographic Hardware and Embedded Systems, pp. 144-157, August 1999. doi:10.1007/3-540-48059-5_14

[5] K. Itoh, T. Izu, M. Takenaka, “A Practical countermeasure against address-bit differential power analysis,” Cryptographic Hardware and Embedded Systems 2003. doi:10.1007/978-3-540-45238-6_30

[6] E. De Mulder, S. B. Örs, B. Preneel, I. Verbauwhede, “Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems,” Computers & Electrical Engineering, 33(5-6), 367-382, 2007. doi:10.1109/EURCON.2005.1630348

[7] E. Brier, C. Clavier, F. Olivier, “Correlation Power Analysis with a Leakage Model,” Cryptographic Hardware and Embedded Systems – CHES, 2004. doi:10.1007/978-3-540-28632-5_2

[8] F. Amiel, B. Feix, K. Villegas, “Power analysis for secret recovering and reverse engineering of public key algorithms,” International Workshop on Selected Areas in Cryptography, pp. 110-125, August 2007. doi:10.1007/978-3-540-77360-3_8

[9] C. D. Walter, “Sliding windows succumbs to big mac attack,” International Workshop on Cryptographic Hardware and Embedded Systems, pp. 286-299, May 2001. doi:10.1007/978-3-540-77360-3_8

[10] P. A. Fouque, F. Valette, “The doubling attack–why upwards is better than downwards,” International Workshop on Cryptographic Hardware and Embedded Systems, pp. 269-280, September 2003. doi:10.1007/978-3-540-45238-6_22

[11] E. Akalp Kuzu, A. Tangel, “A new style CPA attack on the ML implementation of RSA,” International Computer Science and Engineering Conference, pp. 323-328, July 2014. doi:10.1109/ICSEC.2014.6978216

[Downloaded from www.aece.ro on Thursday, July 03, 2025 at 19:26:57 (UTC) by 172.69.130.184. Redistribution subject to AECE license or copyright.]

[12] E. Akalp Kuzu, A. Tangel, "Correlation template matching CPA method," Electronics Letters, 52(15), 1306-1308, 2016. doi:10.1049/el.2016.0415

[13] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, V. Verneuil, "Horizontal correlation analysis on exponentiation," Information and Communications Security, ICICS, 2010. doi:10.1007/978-3-642-17650-0_5

[14] M. F. Witteman, J. G. J. van Woudenberg, F. Menarini, "Defeating RSA multiply-always and message blinding countermeasures," Topics in Cryptology, 2011. doi:10.1007/978-3-642-19074-2_6

[15] E. Akalp Kuzu, B. Soysal, M. Şahinoğlu, U. Güvenç, A. Tangel, "New cross correlation attack methods on the Montgomery Ladder implementation of RSA," IEEE International Advance Computing Conference- IACC, pp. 138-142, 2013. doi:10.1109/IAdCC.2013.6514209

[16] E. Akalp Kuzu, A. Tangel, "All bits cross correlation attack on the Montgomery Ladder implementation of RSA," Digital Signal Processing, pp. 1-5, 2013. doi:10.81043/aperta.91871

[17] A. Bauer, E. Jaulmes, E. Prouff, J. R. Reinhard, J. Wild, "Horizontal collision correlation attack on elliptic curves," Cryptography and Communications", pp:7(1), 91-119, 2015, doi:10.1007/s12095-014-0111-8

[18] H. Kim, T. H. Kim, J. C. Yoon, S. Hong, "Practical second-order correlation power analysis on the message blinding method and its novel countermeasure for RSA," ETRI Journal, 32(1):102–111, February 2010. doi:10.4218/etrij.10.0109.0249

[19] W. Wunan, Y. Wei, C. Jun, "An optimized cross correlation power attack of message blinding exponentiation algorithms," China Communications, Volume 12, Issue 6, pp. 22–32, 2015. doi:10.32604/csse.2021.014460

[20] H. Wang, G. Wei, W. Jizeng, "Practical chosen-message CPA attack on message blinding exponentiation algorithm and its efficient countermeasure," World Wide Web 21.1, 201-217, 2018. doi:10.1007/s11280-017-0442-4

[21] W. Wan, J. Chen, S. Zhang, J. Xia, "A cluster correlation power analysis attack against modular exponentiation based on double masking scheme," Journal of University of Electronic Science and Technology of China, 47(4)588-594, 2018. doi:10.1016/j.jisa.2019.06.013

[22] M. Aftowicz, D. Klann, I. Kabin, Z. Dyka, P. Langendörfer, "Extended horizontal SCA attack using clustering algorithm. In: Gazdag, S.-L., Loebenberger, D. & Nüsken, M. (Hrsg.), crypto day matters 32. doi:10.18420/cdm-2021-32-25

[23] G. Perin, L. Chmielewski, Ł.Batina, S. Picek, "Keep it unsupervised: horizontal attacks meet deep learning," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 343-372, 2021. doi:10.46586/tches.v2021.i1.343-372

[24] P. L. Montgomery, "Montgomery. speeding the Pollard and elliptic curve methods of factorization," Mathematics of Computation, p. 48(177), 243-264, 1987. doi:10.1090/S0025-5718-1987-0866113-7

[25] R. L. Rivest, A.Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, pp:26(1), 96-99, 1983. doi:10.1145/359340.359342

[26] E. Mateos, C. H. Gebotys, "A new correlation frequency analysis of the side channel," Proceedings of the 5th Workshop on Embedded Systems Security, pp. 1-8, 2010. doi:10.1145/1873548.1873552

[27] E. Bohl, J. Hayek, O. Schimmel, P. Duplys, W. Rosenstiel, "Correlation power analysis in frequency-domain," COSADE, pp. 1–3, 2010. doi:10.1145/1873548.1873552

[28] C. H. Gebotys, S. Ho, C. C. Tiu, "EM analysis of Rijndael and ECC on a wireless java-based PDA," Lecture Notes in Computer Science, pp. 250–264, 2005. doi:10.1007/11545262_1

[29] S. Tiran, P. Maurine, "SCA with magnitude squared coherence," Smart Card Research and Advanced Applications, 2012. doi:10.1007/978-3-642-37288-9_16

[30] A. Barenghi, G. Pelosi, Y. Teglia, "Improving first order differential power attacks through digital signal processing," Proceedings of the 3rd international conference on Security of information and networks, pp. 124-133, September 2010. doi:10.1007/978-3-642-37288-9_16

[31] A. Barenghi, G. Pelosi, Y. Teglia, "Information leakage discovery techniques to enhance secure chip design," International Workshop on Information Security Theory and Practices, pp. 128-143, June 2011. doi:10.1007/978-3-642-21040-2_9

[32] S. Tiran, S. Ordas, Y. Teglia, M. Agoyan, P. Maurine, "A frequency leakage model and its application to CPA and DPA," IACR Cryptology ePrint Archive, p. 278, 2013. doi:10.1007/s13389-014-0074-x

[33] P. Belgarric, S. Bhasin, N. Bruneau, J. L. Danger, N. Debande, S. Guilley, O. Rioul, "Time-frequency analysis for second-order attacks," International Conference on Smart Card Research and Advanced Applications, pp. 108-122, November 2013. doi:10.1007/978-3-319-08302-5_8

[34] E. Hatun, G. Kaya, E. Buyukkaya, B. O. Yalcin, "Side channel analysis using EM radiation of RSA algorithm implemented on Raspberry Pi," International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6, June 2019. doi:10.1109/ISNCC.2019.8909185

[35] W. Diffie, M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, 22(6), 644–654, 1976. doi:10.1109/TIT.1976.1055638

[36] FIPS PUB 186-3. Digital Signature Standard, National Institute of Standards and Technology, Gaithersburg, October 2009. doi:10.6028/NIST.FIPS.186-5-draft

[37] J. S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," Cryptographic Hardware and Embedded Systems, August 1999. doi:10.1007/3-540-48059-5_25

[38] S. M. Yen, S. J. Kim, S. G. Lim and S. J. Moon, "A countermeasure against one physical cryptanalysis may benefit another attack," Proceedings of Information Security and Cryptology, 2288, 414-427, 2002. doi:10.1007/3-540-45861-1_31

[39] M. Joye, S.-M. Yen, "The Montgomery Powering Ladder," Cryptographic hardware and embedded systems CHES 2002, Lecture Notes in Computer Science, vol 2523, pp. 8-10, Berlin, September 2003. doi:org/10.1007/3-540-36400-5_22

[40] S. Mangard, E. Oswald, T. Popp, "Power analysis attacks, revealing secrets of the smart cards," pp. 20, 2006. doi:10.5555/1942228

[41] D. Pandini, G. A. Repetto, I. Sinisi, "Clock distribution techniques for low-EMI design," Lecture Notes in Computer Science, pp. 201–210, 2007. doi:10.1007978-3 - 540-74442-9_20

[42] P. Belgarric, S. Bhasin, N. Bruneau, J. L. Danger, N. Debande, S. Guilley, O. Rioul, "Time-frequency analysis for second-order attacks," International Conference on Smart Card Research and Advanced Applications, pp. 108-122, November 2013. doi:10.1007/978-3-319-08302-5_8

[43] A. Donner, B. Rosner, "On inferences concerning a common correlation coefficient," Journal of the Royal Statistical Society, 1980. 29(1), 69-76, doi:10.2307/2346412