

Practical Instantaneous Frequency Analysis Experiments

Roman Korkikian^{1,2}, David Naccache^{2,3(✉)}, Guilherme Ozari de Almeida^{1,2},
and Rodrigo Portella do Canto^{1,2}

¹ Altis Semiconductor, 224, Bd. John Kennedy, 91105 Corbeil Essonnes, France
{roman.korkikian,guilherme.ozari-de-almeida}@altissemiconductor.com,
{roman.korkikian,guilherme.ozari-de-almeida}@etudiants.u-paris2.fr

² Sorbonne Universités – Université Paris II,
12 Place du Panthéon, 75231 Paris, France

david.naccache@u-paris2.fr, david.naccache@ens.fr

³ Département d’Informatique, École Normale Supérieure,
45, rue d’Ulm, 75230 Paris Cedex 05, France

Abstract. This paper investigated the use of instantaneous frequency (IF) instead of power amplitude and power spectrum in side-channel analysis. By opposition to the constant frequency used in Fourier Transform, instantaneous frequency reflects local phase differences and allows detecting frequency variations. These variations reflect the processed binary data and are hence cryptanalytically useful. IF exploits the fact that after higher power drops more time is required to restore power back to its nominal value. Whilst our experiments reveal IF does not bring specific benefits over usual power attacks when applied to unprotected designs, IF allows to obtain much better results in the presence of amplitude modification countermeasures.

Keywords: AES · CPA · CSBA · Instantaneous frequency · Side-channel attacks

1 Introduction

The physical interpretation of data processing (a discipline named the *physics of computational systems* [20]) draws fundamental comparisons between computing technologies and provides physical lower bounds on the area, time and energy required for computation [5, 14]. In this framework, a corollary of the second law of thermodynamics states that in order to perform a transition between states, energy must be lost irreversibly. A system that conserves energy cannot make a transition to a definite state and thus cannot make a decision (compute) ([20], 9.5).

At any given point in the evolution of a technology, the smallest logic devices must have a definite physical extent, require a certain minimum time to perform their function and dissipate a minimal switching energy when transiting from one state to another.

Because CMOS state transition energy is essentially proportional to the number of switched bits, transition energy leakage is the most popular side-channel attack vector. Because commuting also requires time, transition time and processed data might be also related.

Historically, timing attacks were developed to extract secrets from software algorithms [15] while hardware algorithms were usually assumed to run in constant time and hence be immune to timing attacks. The constant hardware execution time assumption is supported by the fact that usual block-cipher hardware implementations require an identical number of clock cycles to process any data. This article shows that this intuition is not always true, *i.e.* two different inputs may require distinct processing time and can hence be distinguishable.

Energy consumed during each clock cycle creates a waveform in the power domain. A duty cycle, *i.e.* the time during which the power wave is not equal to its nominal value, can be considered as the execution time of a hardware implemented algorithm. As shown later the duty cycle may depend on the processed data. Fourier transform can not determine local duty cycles since frequency is defined for the sine or cosine function spanning the whole data length with constant period and amplitude. However, recent techniques described in this paper that can detect local frequencies and hence determine wave duty cycle.

In 2005 it was observed that not only signal amplitude, but also power spectrum, can leak secret information [8]. Following the introduction of Differential Frequency Analysis (DFA) [9], power analysis on frequency domain was investigated on a series of papers [18, 19, 21, 22]. DFA applies Fourier transform to map a time-series into the frequency domain. Since each Fourier point is a linear combination of all other sample points, a spectrum is a direct function of the initial signal amplitude and hence, power spectra can also be used in side-channel attacks.

Reference [18] rightly noted that the term Differential Spectral Based Analysis (DSBA) is semantically preferable because DFA does not exploit variations in frequencies, but *differences in spectra*. As the matter of fact all time-domain power models and distinguishers remain in principle fully applicable in the frequency domain.

Dynamic Voltage Scrambling (DVS) is a particular side-channel countermeasure that triggers random power supply changes aiming to decorrelate the signal's amplitude from the processed data [2, 17]. While DVS degrades DPA's and DSBA's performances, nothing prevents the existence of more subtle side-channel attacks exploiting DVS-resistant die-hard information present in the signal. This paper successfully exhibits and exploits such DVS-resistant information.

Our Contribution. We show that, in addition to the signal's amplitude and spectrum, traditionally used for side-channel analysis, instantaneous frequency variations may also leak secret data. To the authors' best knowledge, "pure" frequency leakage has not been considered as a side-channel vector so far. Hence a re-assessment of several countermeasures, especially, these based on amplitude alterations, seems in order. As an example this paper examines DVS, which makes AES implementation impervious to power and spectrum attacks while

leaving it vulnerable to Correlation Instantaneous Frequency Analysis (CIFA), a new attack described in this paper.

Organization. This paper is organized as follows. Section 2 turns a signal processing algorithm called *Hilbert Huang Transform* (HHT) into an attack process. Section 3 illustrates an HHT performed on a real power signal and motivates the exploration of instantaneous frequency as a side-channel carrier. Section 4 compares the cryptanalytic effectiveness of Correlation Instantaneous Frequency Analysis, Correlation Power Analysis and Correlation Spectrum Based Analysis on an unprotected AES FPGA implementation and on AES FPGA power traces with a simulated DVS. Section 5 concludes the paper.

2 Preliminaries

The notion of *instantaneous frequency*, computable by the HHT, was introduced in [12]. During the last decade, HHT has found many practical applications including oceanographic exploration and medical research [11]. This section recalls HHT's main mathematical features and describes the hardware setup used for evaluating the attacks introduced in this paper.

2.1 Hilbert Huang Transform

The HHT represents the analysed signal in the time-frequency domain by combining the *Empirical Mode Decomposition* (EMD) with the *Discrete Hilbert Transform* (DHT).

DHT is a classical linear operator that transforms a signal $u(1), \dots, u(N)$ into a time series $H_u(1), \dots, H_u(N)$ as follows:

$$H_u(t) = \frac{2}{\pi} \sum_{k \neq t \bmod 2} \frac{u(k)}{t - k} \quad (1)$$

DHT can be used to derive an *analytical representation* $u_a(1), \dots, u_a(N)$ of the real-valued signal $u(t)$:

$$u_a(t) = u(t) + iH_u(t) \text{ for } 1 \leq t \leq N \quad (2)$$

Equation (2) can be rewritten in polar coordinates as

$$u_a(t) = a(t)e^{i\phi(t)} \quad (3)$$

where

$$a(t) = \sqrt{(u^2(t) + H_u^2(t))} \text{ and } \phi(t) = \arctan\left(\frac{H_u(t)}{u(t)}\right) \quad (4)$$

represent the *instantaneous amplitude* and the *instantaneous phase* of the analytical signal, respectively.

The *phase change rate* $w(t)$ defined in Eq. (5) can be interpreted as an *instantaneous frequency* (IF):

$$w(t) = \phi'(t) = \frac{d}{dt}\phi(t) \quad (5)$$

For a real-valued time-series the definition of $w(t)$ becomes:

$$w(t) = \phi(t) - \phi(t - 1) \quad (6)$$

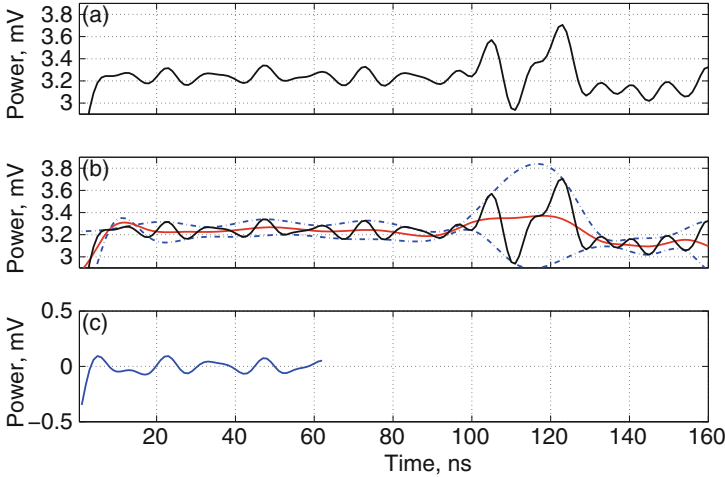


Fig. 1. Illustration of the EMD: (a) is the original signal $u(t)$; (b) $u(t)$ in thin solid black line, upper and lower envelopes are dot-dashed with their mean $m_{i,j}$ in thick solid red line; (c) shows the difference between $u(t)$ and the envelope's mean (Color figure online).

The derivative must be well defined since physically there can be only one instantaneous frequency value $w(t)$ at any given time t . This is insured by the *narrow band condition*: the signal's frequency must be uniform [13]. Further, the physical meaningfulness of DHT's output is closely related to the input's fitness into a narrow frequency band [6]. However, we wish to work with non-stationary signals having more than one frequency. This is achieved by de-composing these signals into several components, called *Intrinsic Mode Functions*, such that each component has nearly the same frequency.

Definition 1 (Intrinsic Mode Function). *An Intrinsic Mode Function (IMF) is a function satisfying the following conditions:*

1. the number of extrema and the number of zero crossings in the considered data set must be either equal or differ by at most one;
2. the mean value of the curve specified as a sum of the envelope defined by the local maxima and the envelope defined by the local minima is zero.

First Step: Empirical Mode Decomposition (EMD). EMD, the HHT's first step, is a systematic way of extracting IMFs from a signal. EMD involves approximation with splines. By Definition 1, EMD uses local maxima and minima separately. All the local signal's maxima are connected by a cubic spline to define an upper envelope. The same procedure is repeated for the local minima to yield a lower envelope. The first EMD component $h_{1,0}(t)$ is obtained by subtraction from $u(t)$ the envelopes' mean $m_{1,0}(t)$ (see Fig. 1):

$$h_{1,0}(t) = u(t) - m_{1,0}(t) \quad (7)$$

Ideally, $h_{1,0}(t)$ should be an IMF. In reality this is not always the case and EMD has to be applied to $h_{1,0}(t)$ as well:

$$h_{1,1}(t) = h_{1,0}(t) - m_{1,1}(t) \quad (8)$$

EMD is iterated k times, until an IMF $h_{1,k}(t)$ is reached, that is

$$h_{1,k}(t) = h_{1,k-1}(t) - m_{1,k}(t) \quad (9)$$

Then, $h_{1,k}(t)$ is defined as the first IMF component $c_1(t)$.

$$c_1(t) \stackrel{\text{def}}{=} h_{1,k}(t) \quad (10)$$

Next, the IMF component $c_1(t)$ is removed from $u(t)$

$$r_1(t) = u(t) - c_1(t) \quad (11)$$

and the procedure is iterated on all the subsequent residues, until the residue $r_n(t)$ becomes a monotonic function from which no further IMFs can be extracted.

$$\begin{cases} r_2(t) = r_1(t) - c_2(t) \\ \dots \\ r_n(t) = r_{n-1}(t) - c_n(t) \end{cases} \quad (12)$$

Finally, the initial signal $u(t)$ is re-written as a sum:

$$u(t) = \sum_{j=1}^n c_j(t) + r_n(t), \quad \text{for } 1 \leq t \leq N \quad (13)$$

where, $c_j(t)$ are IMFs and $r_n(t)$ is a constant or a monotonic residue.

Second Step: Representation. The second HHT step is the representation of the initial signal in the time-frequency domain. All components $c_j(t)$, $j \in [1, n]$ obtained during the first step are transformed into analytical functions $c_j(t) + iH_{c_j}(t)$, allowing the computation of instantaneous frequencies by formula (6). The final transform $U(t, w)$ of $u(t)$ is:

$$U(t, w) = \sum_{j=1}^n a_j(t) \exp \left(i \sum_{\ell=1}^t w_j(\ell) \right) \quad (14)$$

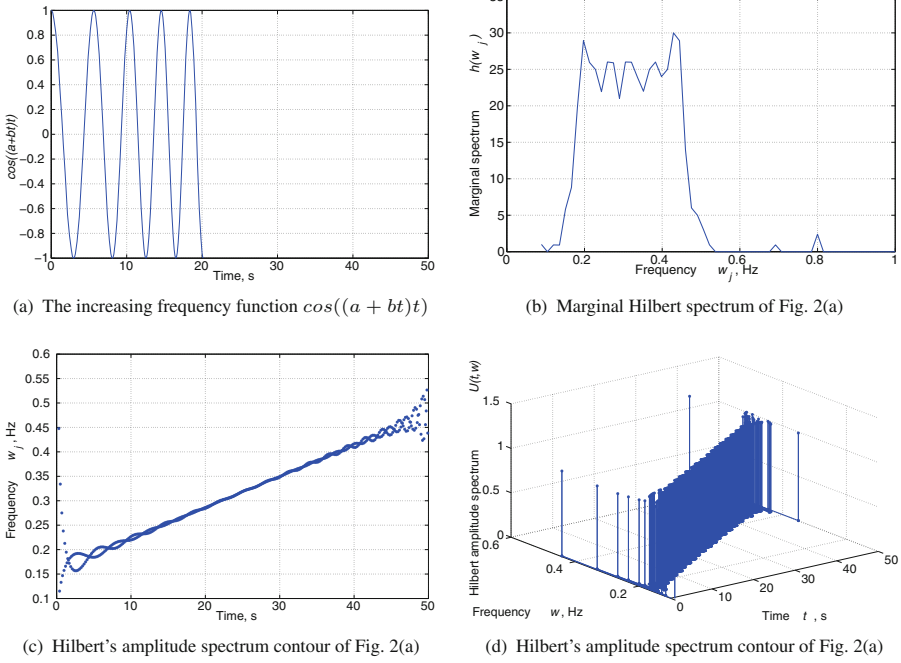


Fig. 2. Analysis of the function $\cos((a + bt)t)$.

where $j \in [1, n]$ is indexing components, $t \in [1, N]$ represents time and:

$$a_j(t) = \sqrt{c_j^2(t) + H_{c_j}^2(t)} \quad \text{is the instantaneous amplitude;}$$

$$w_j(t) = \arctan\left(\frac{H_{c_j}(t+1)}{c_j(t+1)}\right) - \arctan\left(\frac{H_{c_j}(t)}{c_j(t)}\right) \quad \text{is the instantaneous frequency;}$$

Equation (14) represents the amplitude and the instantaneous frequency as a function of time in a three-dimensional plot, in which amplitude can be contoured on the frequency-time plane. This frequency-time amplitude distribution is called the *Hilbert amplitude spectrum* $U(t, w)$, or simply the *Hilbert spectrum* [12]. In addition to the Hilbert spectrum, we define the *marginal spectrum* or *HTT power spectral density* $h(w)$, as

$$h(w_j) = \sum_{t=1}^T U(t, w_j) \quad (15)$$

The marginal spectrum measures the total amplitude (or energy) contributed by each frequency value. To illustrate HHT decomposition consider the function $u(t) = \cos(t(a + bt))$. In Fig. 2(a) parameters a and b were arbitrarily set to $a = 1$ and $b = 0.02$. Figure 2(a) shows that the cosine's frequency increases progressively. Figure 2(b) presents the Hilbert marginal spectrum of the signal

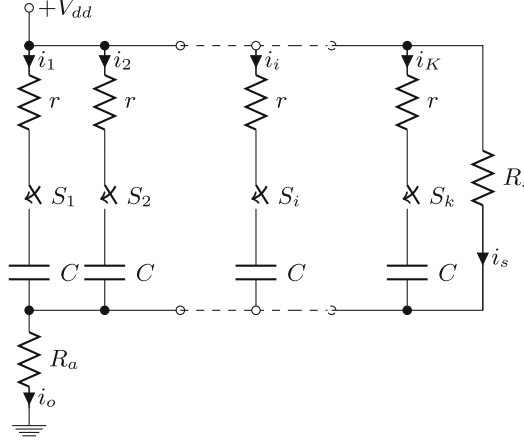


Fig. 3. Inverters switch simulation.

$u(t) = \cos((1 + 0.02t)t)$. Figure 2(c) shows the contour of Hilbert’s amplitude spectrum, i.e. frequency evolution in time, and this evolution is indeed nearly linear. The 3D Hilbert amplitude spectrum is illustrated in Fig. 2(d).

2.2 AES Hardware Implementation

The AES-128 implementation used for our experiments runs on an Altera Cyclone II FPGA development board clocked by an external 50 MHz oscillator. The AES architecture uses a 128-bit datapath. Each AES round is completed in one clock cycle and key schedule is performed during encryption. The substitution box is described as a VHDL table mapped into combinational logic after FPGA synthesis. Encryption is triggered by a high `start` signal. After completing the rounds the device halts and drives a `done` signal high.

The implementation has no side-channel countermeasures. To simulate DVS, 200,000 physically acquired power consumption traces were processed by Algorithm 1. Algorithm 1 splits a time-series into segments and adds a uniformly distributed random voltage offset to each segment.

The rationale for simulating a DVS by processing a real signal (rather than adding a simple DVS module to the FPGA) is the desire to work with a rigorously modelled signal, free of the power consumption artefacts created by the DVS module itself.

3 Hilbert Huang Transform and Frequency Leakage

3.1 Why Should Instantaneous Frequency Variations Leak Information?

Most of the power consumed by a digital circuit is dissipated during rising or falling clock edges when registers are rewritten with new values. This activity

is typically reflected in the power consumption trace as spikes occurring exactly during clock rising edges. Spike frequency, computed by the Fourier transform, is usually assumed to be constant because clock frequency is stable. In reality, this assumption is incorrect since each spike has its own duty cycle and consequently its own assortment of frequencies.

Differences in duty cycle come from the fact that the circuit's power supply must be restored to its nominal value after switching. Bigger amplitude spikes take more time to resorb than smaller amplitude ones.

To illustrate these spike differences, consider the simple circuit in Fig. 3. Each parallel branch has a resistor r , a switch S_i and a capacitor C that simulate a single inverter when switched from low to high. Resistor R_s and the current i_s represent the circuit's static current and R_a is the resistor used for acquisition. Initially all the switches $S_1 \dots S_k$ are open, so the current flowing through R_a is simply i_s .

Assume that at $t_0 = 0$ all the switches $S_1 \dots S_k$ are suddenly closed. All capacitors start charging and current flowing through R_a rises according to the following equation:

$$i_o(t) = i_s + k \left(\frac{V_{dd}}{r} e^{-\frac{t}{rC}} \right) \quad (16)$$

Equation (16) shows that current amplitude depends on the number of closed switches. However, there is one more parameter in the equation, namely the time t that characterizes the switching spike. The current i_o needs some time to “practically” reach an asymptotic nominal value i_s and this time depends on the number of closed switches k . Consider the time T_k required by $i_o(t)$ to reach $\Gamma\%$ of its asymptotic value, i.e. $\frac{\Gamma}{100}i_s$:

$$i_o(T_k) = i_s - k \left(\frac{V_{dd}}{r} e^{-\frac{T_k}{rC}} \right) = \frac{\Gamma}{100} i_s \quad (17)$$

This is equivalent to:

$$T_k = rC \ln \left(\frac{100}{100 - \Gamma} \frac{V_{dd}}{i_s r} \right) + rC \ln(k) = \alpha + \beta \ln(k) \quad (18)$$

Equation (18) shows that convergence time has a constant part α and a variable part $\beta \ln(k)$ that depends on the number of closed switches k . Equation (18) shows that both spike period and spike frequency depend on the processed data and could hence in principle be used as side-channel carriers. Nevertheless, power consumption is a non-stationary signal, which justifies the use of HHT.

The dependency between the number of switches and spike period in Eq. (18) is non-linear and hard to formalize as a simple formula for a real circuit. Section 3.2 shows that the standard Hamming distance model can be used in conjunction with instantaneous frequency.

3.2 Power Consumption of One AES Round

The relationship between processed data and power amplitude is a well understood phenomenon [1, 7, 10, 16]. However, to the best of our knowledge the dependency

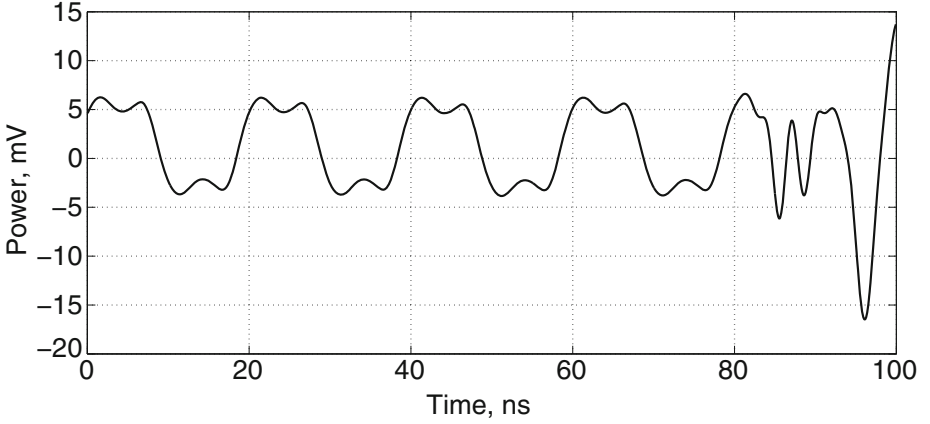


Fig. 4. Four AES last rounds.

of instantaneous frequency on processed data has not been explored so far. This may be partially explained by the fact that Fourier Transform, previously used in some papers, is not inherently adapted to non-stationary and non-linear signals. Fourier analysis cannot extract frequency variations from a signal because frequency is defined as a constant parameter of the underlying sine function spanning the whole data-set $u(t)$. By opposition, HHT allows extracting instantaneous frequencies and exploiting them for subsequent cryptanalytic purposes.

To illustrate information leakage through frequency variation, the AES last rounds' power consumption was measured using a Picoscope 3207 A with 250 MHz bandwidth at 10 G/s equivalent time sampling rate. Every signal had 1,000 samples and 100,000 traces were acquired for various input plaintexts. A power consumption example of the 4 last rounds is shown on the Fig. 4.

The AES last round was extracted from each power trace as shown on Fig. 5(a). The number of bits switches in the AES last round was computed with the known key. Afterwards the traces with the same number of bits switches were averaged.

In classic side-channel models [7], flipping more bits would consume more energy. Figure 5 shows that such is indeed the case for power consumption of 55, 65 and 75 bit flips where $v_{75} > v_{65} > v_{55}$. As per our assumption, the *frequency signatures of these three operations are also different*.

To show that HHT can detect frequency differences consider the power spectral density (PSD) of signals during 55, 65 and 75 bits switchings (Fig. 5(c)). The maximal spectral amplitude of the 55 bit change is located at 51.18 MHz (point f_{55}), that of the 65 bit change is at 51.12 MHz (point f_{65}) and that of the 75 bit change is at 50.73 MHz (point f_{75}) which is supportive of the hypothesis that HHT can distinguish frequency variations even in non-stationary signals because $f_{55} > f_{65} > f_{75}$.

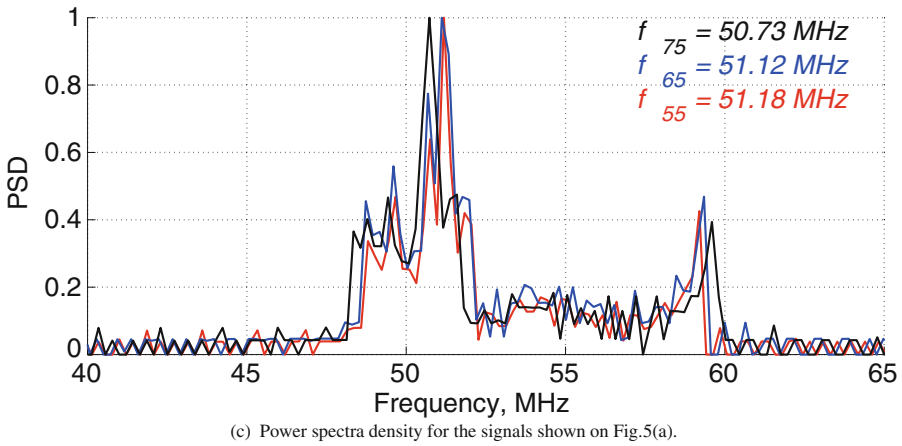
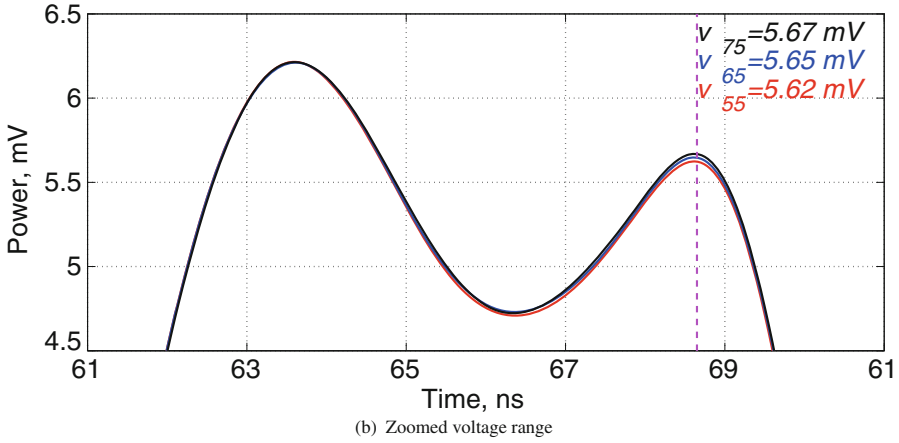
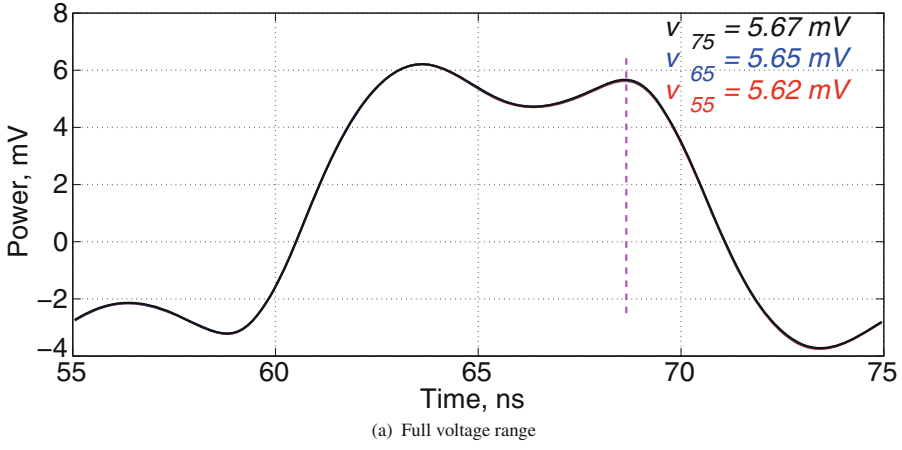


Fig. 5. AES last round power consumption for 55 (red), 65 (blue) and 75 (black) register's flip-flops (Color figure online).

This shows that not only amplitude but also frequency varies during register switch. Logically, power consumption increases as more bits are flipped. However, HHT was previously applied only for one AES round and HHT's applicability for the entire AES power traces must be verified. That is why the next section carefully examines the effect of register alteration on IF when AES FPGA implementation is sampled at a smaller rate.

3.3 Hilbert Huang Transform of an AES Power Consumption Signal

We start by performing a Hilbert Huang decomposition of a real signal. The analysis was performed on the power trace of the previously described AES-128 implementation. The acquisition was performed 1 G/s real time rate with 1 GHz differential probe. Signals were averaged 10 times and had 1,000 samples (Fig. 6(a)).

EMD decomposed the power trace to five IMFs and a residue, shown in Fig. 6(b). After decomposition, each IMF was Hilbert Transformed to derive the power signal's time-frequency representation.

Figure 6(c) is an IF distribution of Fig. 6(a).

Amplitude combination over frequency gave the power spectral density plot shown in blue on Fig. 7. An important observation in Fig. 7 is that HHT spectrum shows the distribution of a periodic variable over the main peak frequencies. Notably, the peak near 50 MHz that corresponds to the board's oscillator is not represented by a single point, but by a set of points. This data scatter can be explained by the fact that the IF of AES rounds varies, and HHT distinguishes this variation.

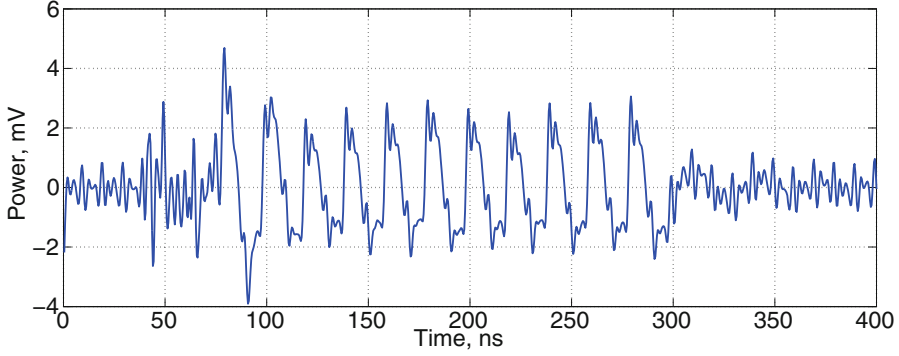
The main difference between HHT and FFT spectra (see plot shown in red on Fig. 7) is that HHT defines frequency as the speed of phase change and can hence detect intra-time-series deviations from the carrier's oscillation, whereas FFT frequency stems from the sine function, which is independent of the signals' shape.

So far, it was shown that IF varies for different rounds even within a given trace. However, an attack is only possible when IF depends on the data's Hamming weight.

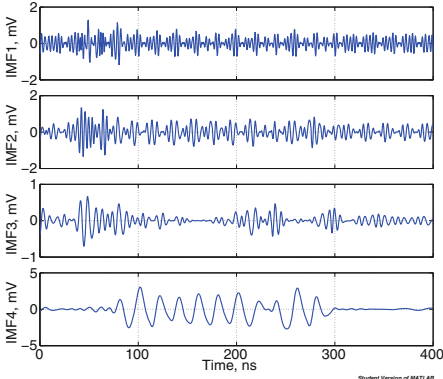
The dependency is apparent in Fig. 8 showing the relationship between Hamming distance of the 9-th and 10-th AES round states and IF, taken from the first IMF component at the beginning of the 10-th round. Figure 8 was drawn using 200,000 HHT-processed power traces. The thin solid line in Fig. 8 represents the mean IF value, obtained from the first IMF component, as a function of Hamming distance.

The principal trend is the ascending line. Figure 8 corresponds well to the simulation of a register's power consumption since frequency is decreasing due to the increase in Hamming distance. The relationship in Fig. 8 between Hamming distance and IF looks linear and therefore the Pearson correlation coefficient can be used as an SCA distinguisher.

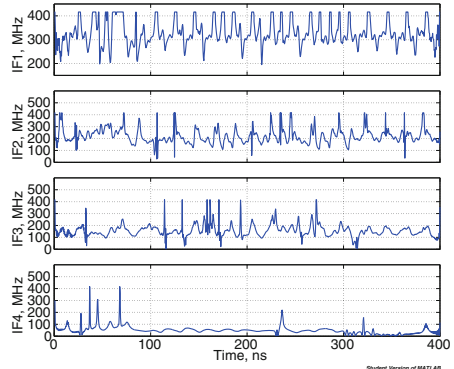
IF adoption for side-channel attacks presents some particularities. The disadvantage of the method is that data scatter is higher than in usual DPA and hence



(a) Initial signal $u(t)$



(b) The Empirical Mode Decomposition of signal $u(t)$



(c) IF distribution over time for the different IMFs of Fig. 6(b).

Fig. 6. Power consumption of our experimental AES-128 implementation.

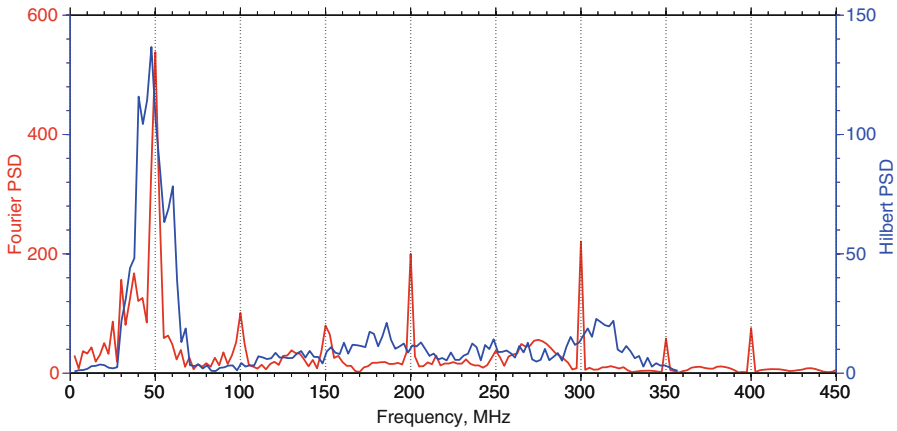


Fig. 7. Fourier and Hilbert power spectrum density of Fig. 6(a).

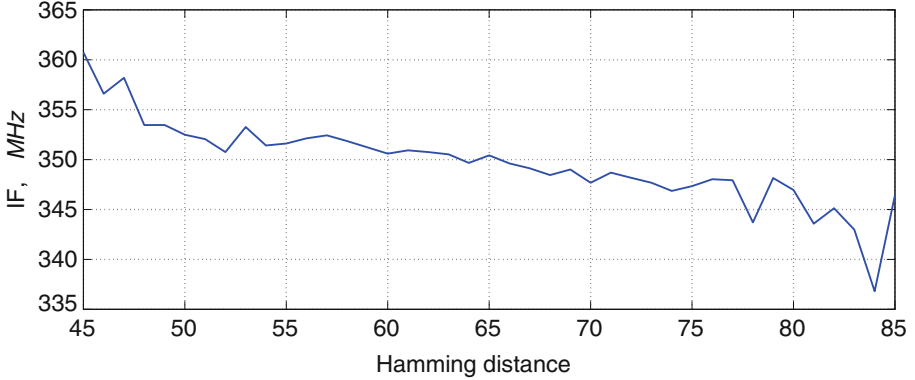


Fig. 8. Dependency between the Hamming distance of 9-th and 10-th AES round states and the IF of the first IMF component at time 276 ns (corresponding to the beginning of the last AES round).

the attack requires more power traces. Another issue is that each time-series will be decomposed into a set of IMFs, hence every sample will be wrapped-up with a set of IFs virtually multiplying the amount of data to be processed. However, the advantage is that because frequency based analysis is independent of local amplitude, CIFA can still be attempted in the presence of certain countermeasures.

4 Correlation Instantaneous Frequency Analysis

This section introduces Correlation Instantaneous Frequency Analysis (CIFA) and compares its performance with Correlation Power Analysis (CPA) and to Correlation Spectral Based Analysis (CSBA).

4.1 Correlation Instantaneous Frequency Analysis on Unprotected Hardware

During the acquisition step 200,000 power traces were acquired at a sampling rate of 2.5 GS/s. Each power signal was averaged 10 times to reduce noise. All traces were HHT-processed using the Matlab HHT code of [3,4]. Most traces were decomposed into 6 components, but 5 and 7 IMFs occurred as well. To reduce the amount of processed information only the first four IMFs were used.

Generally, each higher rank IMF carries information present in smaller instantaneous frequencies (Fig. 6(c)), this is why IMFs from different power traces were aligned index-wise, *i.e.* all first IMFs from every encryption were analyzed first, then all second IMFs and so on.

We chose the Hamming distance model and Pearson's correlation coefficient to investigate CIFA's properties and compare CIFA with other attacks.

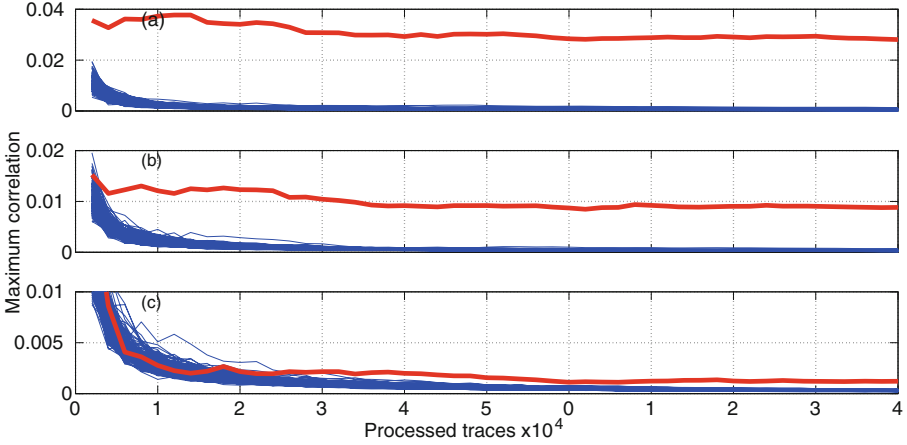


Fig. 9. Maximum correlation coefficients for a byte of the last round AES key in an unprotected implementation. Although the three attacks eventually succeed CPA>CSBA>CIFA. (a) CPA (b) CSBA (c) CIFA.

CPA. CPA applied to power traces produces Fig. 9(a). Clearly, CPA outperforms CIFA. CIFA’s poorer performance can be partially attributed to the power model, because IF is not linearly dependent on the Hamming distance.

CSBA. Figure 9(b) presents CSBA applied against Fourier power trace spectra with the same power model and distinguisher. The correct key byte can be distinguished from 2000 power traces and on.

CIFA. The application of the selected power model and of the distinguisher to IFs yields Fig. 9(c) where the correct key byte emerges from 16,000 power traces and on.

The three experiments seem to suggest that CSBA is superior to CIFA but inferior to CPA. That is $\text{CIFA} < \text{CSBA} < \text{CPA}$.

While it appears that CPA and CSBA outperform CIFA in the absence of countermeasures, we will now see that CIFA survives countermeasures that derail CPA and CSBA.

4.2 Correlation Instantaneous Frequency Analysis in the Presence of DVS

As mentioned previously DVS alters power supply to reduce dependency between data and consumed power. According to [2, 17] DVS is cheap in terms of area overhead since only a voltage controller and a random number generator must be added to the protected design.

To simulate DVS all the traces of the unprotected AES were modified by Algorithm 1. Each power trace was partitioned into γ segments of normally

distributed lengths covering the whole dataset.¹ Each segment was lifted by a uniformly distributed random offset ℓ that did not exceed a predetermined value D set to $D = 12$ mV.

Algorithm 1. Dynamic Voltage Scrambling (DVS) Simulator.

Input:

A power trace $u(1), \dots, u(N)$;
 γ : the number of segments;
 m : mean value of segment length $m \stackrel{\text{def}}{=} N/\gamma$;
 σ : standard deviation of segment length;
 D : maximum offset for segment lifting;

Output:

a DVS-protected power trace $u'(1), \dots, u'(N)$;

▷ Split a trace to a set of segments of normally distributed random length chunks
 $\tau_0 \leftarrow 1$
 $\tau_\gamma \leftarrow N$
for $i = 1$ **to** $\gamma - 1$ **do**
 $\tau_i \leftarrow \tau_{i-1} + \mathcal{N}(m, \sigma)$
end for
 ▷ Lift each segment by a uniformly distributed random offset ℓ
for $s = 1$ **to** γ **do**
 $\ell_s \in_R [0, D]$
for $t = \tau_{s-1}$ **to** τ_s **do**
 $u'(t) \leftarrow u(t) + \ell_s$
end for
end for

A trace modification example is presented in Fig. 10, in which the trace of Fig. 6(a) was processed by Algorithm 1.

Logically, DVS decreases power analysis performance by reducing the attacker's SNR. We disposed of 200,000 DVS-modified power traces. All of which were used to mount power analysis attacks under the same conditions as before, *i.e.*, using Pearson's correlation coefficient and the Hamming distance model.

The same final round key byte used for attacks against the unprotected implementation was targeted. CPA and CSBA failed to detect the correct key byte even with 150,000 traces (Fig. 11(a), (b)). This confirms the intuition that DVS has a beneficial effect on the required number of power traces.

However CIFA was able to recover the byte from 60,000 traces and on (Fig. 11(c)). This illustrates that whilst CIFA is usually outperformed by CPA and CSBA, CIFA is much more resilient to DVS, to which CPA and CSBA are very sensitive.

¹ The mean m and the standard deviation σ were arbitrary set to $m = 40$ ns and $\sigma = 5$ ns in our experiment.

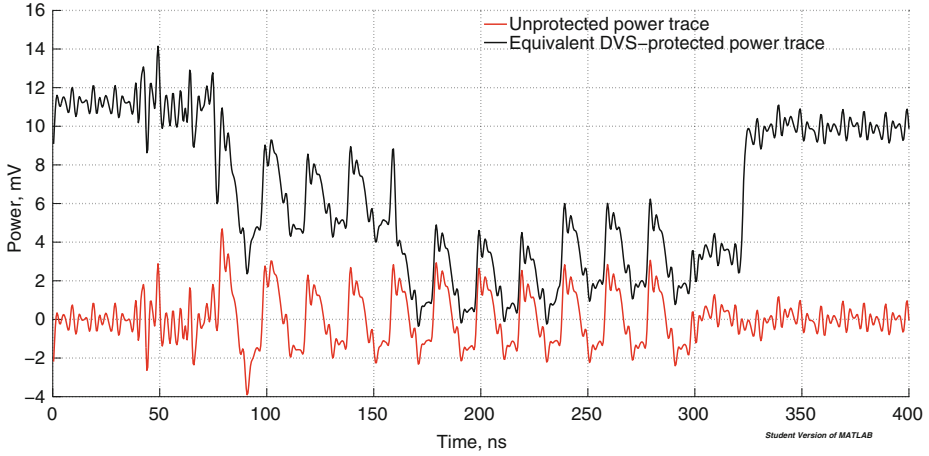


Fig. 10. Power traces of the FPGA AES implementation. The unprotected signal is shown in red. The DVS-protected signal is shown in black (Color figure online).

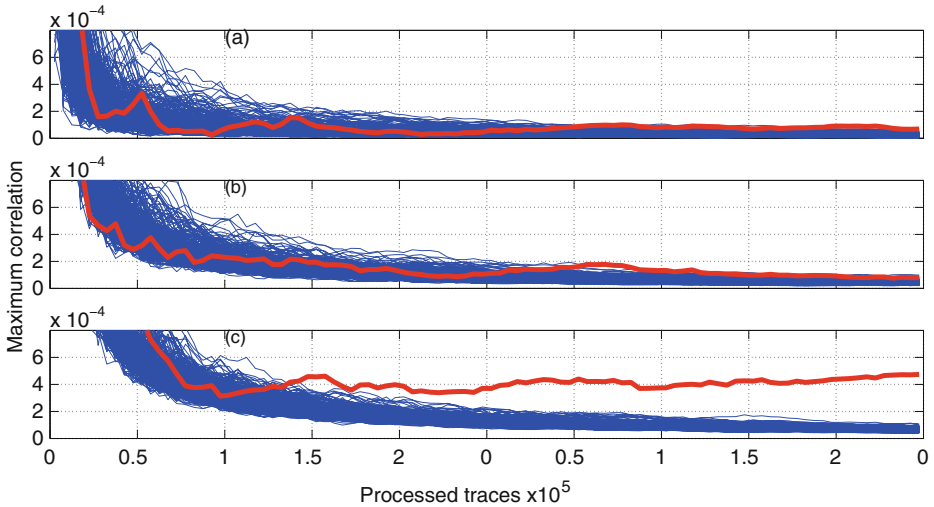


Fig. 11. Maximum correlation coefficient for a byte of the last round AES key with simulated DVS. (a) CPA (b) CSBA (c) CIFA.

5 Conclusions and Further Research

This paper investigated the use of instantaneous frequency instead of power amplitude and power spectrum in side-channel analysis. By opposition to the constant frequency used in Fourier Transform, instantaneous frequency reflects local phase differences and allows to detect frequency variations. These variations depend on the processed binary data and are hence cryptanalytically useful.

The relationship stems from the fact that after higher power drops more time is required to restore power back to its nominal value.

IF analysis does not bring specific benefits when applied to unprotected designs on which CPA and CSBA yield better results. However, CIFA allows to discard the effect of amplitude modification countermeasures, e.g. DVS, because CIFA extracts from signal features not exploited so far.

Acknowledgments. The authors thank Natacha Laniado for editing and proofreading this work.

References

1. Agrawal, D., Archambeault, B., Rao, J.R., Rohatg, P.: The EM Side-Channel(s). In: Kaliski, B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 29–45. Springer, Heidelberg (2003)
2. Baddam, K., Zwolinski, M.: Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure. In: Proceedings of the 20-th International Conference on VLSI Design Held Jointly with 6-th International Conference: Embedded Systems, VLSID '07, pp. 854–862. IEEE Computer Society (2007)
3. Battista, B., Knapp, C., McGee, T., Goebel, V.: Application of the empirical mode decomposition and Hilbert-Huang transform to seismic reflection data. In: Geophysics, vol. 72, pp. H29–H37. SEG (2007)
4. Battista, B., Knapp, C., McGee, T., Goebel, V.: Matlab program demonstrating performing the empirical mode decomposition and Hilbert-Huang transform on seismic reflection data, August 2012. <http://software.seg.org/2007/0003/mat/emd.zip>
5. Bennett, C.: Logical reversibility of computation. IBM J. Res. Dev. **17**, 525–532 (1973). IBM Corp.
6. Boashash, B.: Estimating and interpreting the instantaneous frequency of a signal. I. fundamentals. Proc. IEEE **80**, 520–538 (1992)
7. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
8. Gebotys, C.H., Ho, S., Tiu, C.C.: EM analysis of Rijndael and ECC on a wireless Java-based PDA. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 250–264. Springer, Heidelberg (2005)
9. Gebotys, C., Tiu, C., Chen, X.: A countermeasure for EM attack of a wireless PDA. In: International Conference on Information Technology: Coding and Computing, 2005, ITCC 2005, vol. 1, pp. 544–549, April 2005
10. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual Information Analysis - A Generic Side-Channel Distinguisher. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 426–442. Springer, Heidelberg (2008)
11. Huang, N., Shen, S.: The Hilbert-Huang Transform and its Applications. World Scientific Publishing Company, Singapore (2005)
12. Huang, N., Shen, Z., Long, S., Wu, M., Shih, S., Zheng, Q., Tung, C., Liu, H.: The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci. **454**, 903–995 (1998)

13. Kaslovsky, D., Meyer, F.: Noise Corruption of Empirical Mode Decomposition and Its Effect on Instantaneous Frequency. ArXiv e-prints, August 2010. <http://arxiv.org/pdf/1008.4176v1>
14. Keyes, R.: Physical limits in digital electronics. *IEEE Proc.* **63**, 740–767 (1975)
15. Kocher, P.C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, N. (ed.) *CRYPTO 1996*. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996)
16. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) *CRYPTO 1999*. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
17. Krieg, A., Grinschgl, J., Steger, C., Weiss, R., Haid, J.: A side channel attack countermeasure using system-on-chip power profile scrambling. In: *IEEE International On-Line Testing Symposium*, pp. 222–227. IEEE Computer Society (2011)
18. Luo, Q.: Enhance multi-bit spectral analysis on hiding in temporal dimension. In: Gollmann, D., Lanet, J.-L., Iguchi-Cartigny, J. (eds.) *CARDIS 2010*. LNCS, vol. 6035, pp. 13–23. Springer, Heidelberg (2010)
19. Mateos, E., Gebotys, C.: Side channel analysis using giant magneto-resistive (GMR) sensors. In: *2-nd International Workshop on Constructive Side-Channel Analysis and Secure Design - COSADE 2011*, pp. 42–49, February 2011
20. Mead, C., Conway, L.: *Introduction to VLSI Systems*. Addison-Wesley, Reading (1980)
21. Peng, Z., Gaoming, D., Qiang, Z., Kaiyan, C.: EM frequency domain correlation analysis on cipher chips. In: *2009 1-st International Conference on Information Science and Engineering (ICISE)*, pp. 1729–1732, December 2009
22. Schimmel, O., Duplys, P., Boehl, E., Hayek, J., Bosch, R., Rosenstiel, W.: Correlation power analysis in frequency domain. In: *First International Workshop on Constructive Side-Channel Analysis and Secure Design - COSADE 2010*, pp. 1–3 (2010)

E-Business and Telecommunications

International Joint Conference, ICETE 2013, Reykjavik,

Iceland, July 29-31, 2013, Revised Selected Papers

Obaidat, M.S.; Filipe, J. (Eds.)

2014, XVII, 419 p. 189 illus., Softcover

ISBN: 978-3-662-44787-1