Instantaneous Frequency Analysis

Roman Korkikian[1,2], David Naccache[2,3], Guilherme Ozari de Almeida[1,2]

[1] Altis Semiconductor
224, Bd. John Kennedy, F-91105, Corbeil Essonnes, France
roman.korkikian@altissemiconductor.com
guilherme.ozari-de-almeida@altissemiconductor.com
[2] Sorbonne Universités – Université Paris II
12 Place du Panthéon, F-75231, Paris, France
roman.korkikian@etudiants.u-paris2.fr
guilherme.ozari-de-almeida@etudiants.u-paris2.fr
david.naccache@u-paris2.fr
[3] École normale supérieure, Département d'informatique
45, rue d'Ulm, F-75230, Paris CEDEX 05, France
david.naccache@ens.fr

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.

1 Introduction

In addition to its usual complexity postulates, cryptography silently assumes that secrets can be physically protected in tamper-proof locations. All cryptographic operations are physical processes where data elements must be represented by physical quantities in physical structures. These physical quantities must be stored, sensed and combined by the elementary devices (gates) of any technology from which we build tamper-resistant machinery.

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.

The physical interpretation of data processing (a discipline named the *physics of computational systems* [23]) draws fundamental comparisons between computing technologies and provides physical lower bounds on the area, time and

energy required for computation [5,16]. In this framework, a corollary of the second law of thermodynamics states that in order to introduce direction into 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) ([23],9.5). In tamper-resistant devices this inescapable energy transfer must, in addition, at least appear to be independent of the machine's secret parameters.

In 2005 it was observed, that not only signal amplitude, but also power spectrum, can leak secret information [10]. Following the introduction of Differential Frequency Analysis (DFA) [11], frequency domain power analysis was investigated in a thread of research papers [20,22,24,25]. 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.

[20] rightly noted that the term Differential Spectral Based Analysis (DSBA) is semantically preferable to DFA 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 meant to decorrelate the signal's amplitude from the processed data [2,19]. While DVS significantly 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 the *Hilbert Huang Transform* (HHT, a signal processing algorithm), 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 conjectures the previsible effect of CIFA on other countermeasures and section 6 concludes the paper.

2 Preliminaries

The notion of *instantaneous frequency*, computable by the HHT, was introduced in [14]. During the last decade, HHT found many practical applications including oceanographic exploration and medical research [13]. 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 transforming a signal $u(1), \ldots, u(N)$ into a time series $H_u(1), \ldots, H_u(N)$ as follows:

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

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

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

Equation (2) can be rewritten in polar coordinates as

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

where

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

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

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

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

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

$$w(t) = \phi(t) - \phi(t-1) \tag{6}$$

The derivative must be well defined since physically there can only be 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 [15]. 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 to extract 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):

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

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:

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

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

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

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

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

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

$$r_1(t) = u(t) - c_1(t) \tag{11}$$

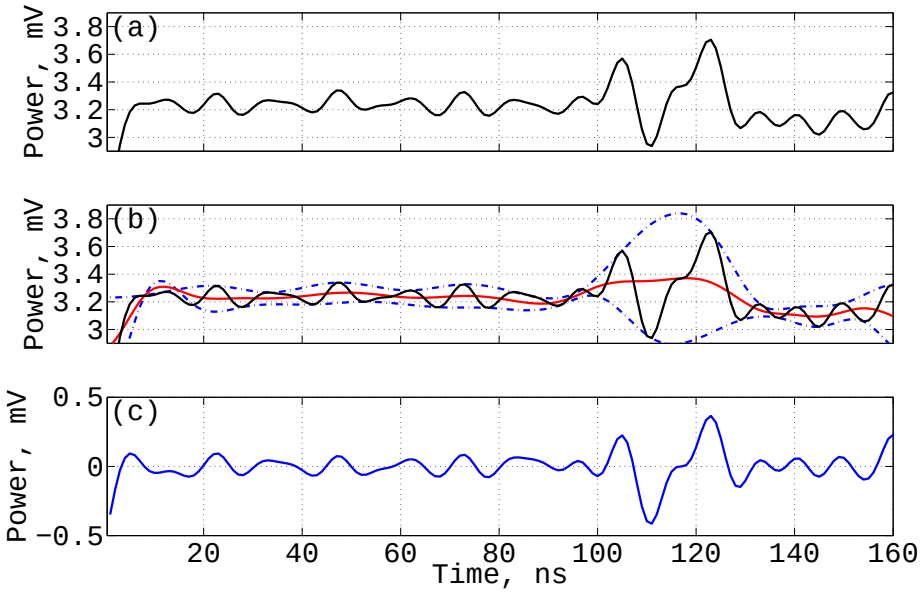


Fig. 1. Illustration of the EMD: (a) is the original signal $u(t)$; (b) $u(t)$ in thin solid black line, upper and lower envelopes are dot-dashed with their mean $m_{i,j}$ in thick solid red line; (c) shows the difference between $u(t)$ and the envelope's mean.

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.

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

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

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

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:

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

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

$a_j(t) = \sqrt{c_j^2(t) + H_{c_j}^2(t)}$ is the *instantaneous amplitude*;
$w_j(t) = \arctan\left(\frac{H_{c_j}(t+1)}{c_j(t+1)}\right) - \arctan\left(\frac{H_{c_j}(t)}{c_j(t)}\right)$ 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* [14]. In addition to the Hilbert spectrum, we define the *marginal spectrum* or *HTT power spectral density* $h(w)$, as

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

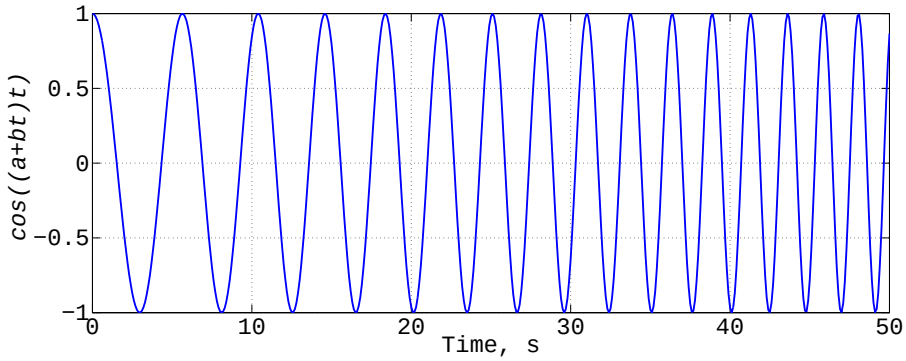
The marginal spectrum measures the total amplitude (or energy) contributed by each frequency value.

To illustrate HHT decomposition consider the function $u(t) = \cos(t\,(a + bt))$. In Fig. 2a parameters a and b were arbitrarily set to $a = 1$ and $b = 0.02$. Fig. 2a shows that the cosine's frequency increases progressively. Fig. 2b presents the Hilbert marginal spectrum of the signal $u(t) = \cos((1 + 0.02t)t)$. Fig. 2c 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. 2.1.

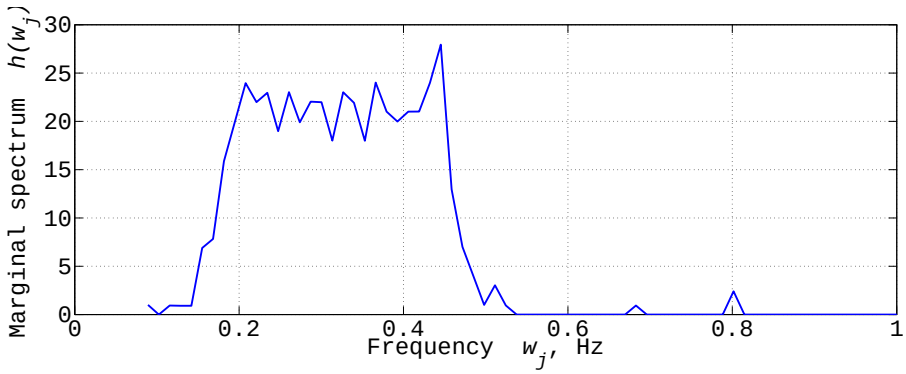
2.2 AES Hardware Implementation

The AES-128 implementation used for our experiments runs on an Altera Cyclone II FPGA development board clocked by an external 50MHz 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, used as well as a side-channel acquisition trigger. After completing the rounds the device halts and drives a `done` signal high.

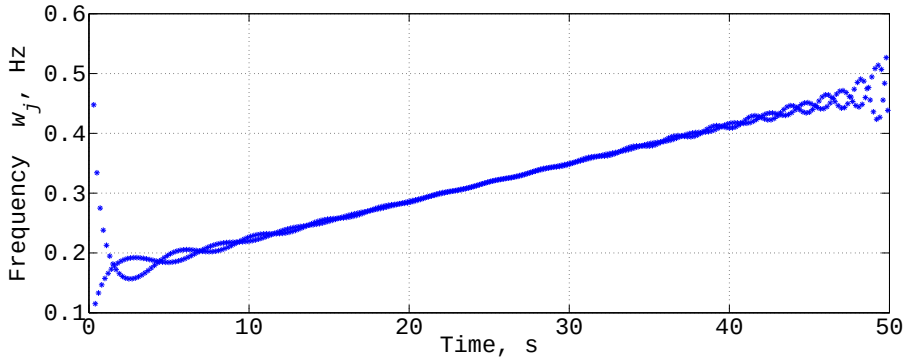
The implementation has no side-channel countermeasures. To simulate DVS, 200,000 physically acquired power consumption traces were processed by Algorithm 2. Algorithm 2 splits a time-series into segments and adds a uniformly distributed random voltage offset to each segment.



(a) The increasing frequency function $cos((a + bt)t)$



(b) Marginal Hilbert spectrum of Fig. 2a



(c) Hilbert's amplitude spectrum contour of Fig. 2a

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

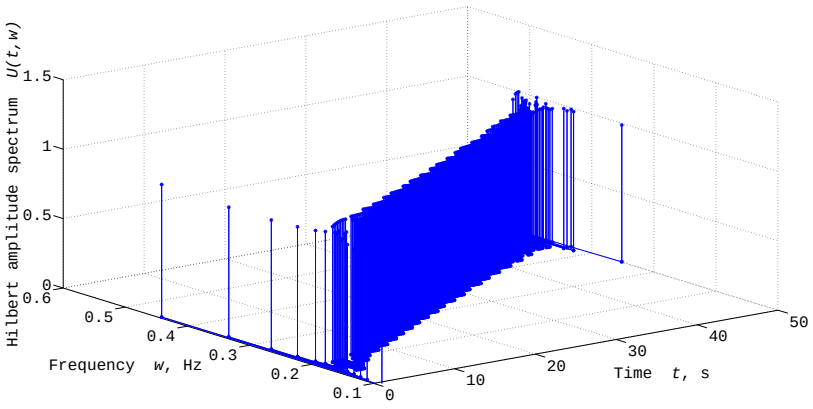


Fig. 3. Hilbert amplitude spectrum $U(t, w)$ of Fig. 2a

The rationale for simulating a DVS by processing a real signal (rather than adding to the FPGA a simple DVS module) 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's 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 period and consequently its own assortment of frequencies.

Differences in period 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. 4. Each parallel branch has a resistor r, a switch S_i and a capacitor C simulating 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.

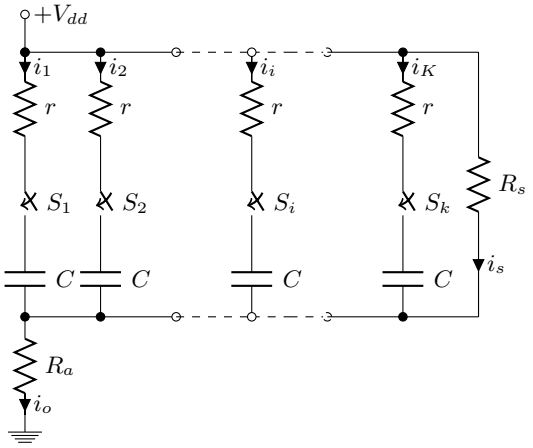


Fig. 4. Inverters switch simulation.

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:

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

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 characterizing 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 Γ% of its asymptotic value, *i.e.* $\frac{\Gamma}{100}i_s$:

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

This is equivalent to:

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

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.

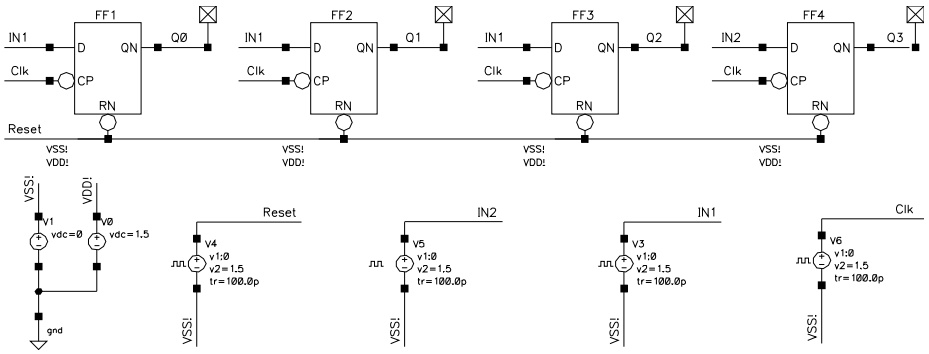


Fig. 5. Netlist of a 4-bit register.

Intuitively and dirtily, if we assimilate the curves in Fig. 6a to sines, we see that the instantaneous frequency $\frac{1}{T_k}$ reflects the number of closed switches k.

The dependency between the number of switches and spike period in equation (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 Register Simulation

The relationship between processed binary values and power amplitude is a well understood phenomenon [1,9,12,18]. However, to the best of our knowledge the dependency of instantaneous frequency on processed data has not been explored so far. This may be partially explained by the fact that Fourier Transform, previously examined 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 variations, the power consumption of a 4-bits register was simulated using the Virtuoso toolkit. Power supply was set to 1.5V and the circuit was clocked by a 50 MHz oscillator (Fig. 5).

Two scenarios were simulated under identical temperature and voltage conditions:

Single Latch: The register was reset. After a sufficiently long time a high input `IN2` was latched on flip-flop `FF4`. At the next clock rising edge the D-latch

updated its state and transmitted a 1 to `Q3`. The simulation of the register's power consumption shown in Fig. 6a (blue signal).

Triple Latch: The register was reset. After a sufficiently long time a high input `IN1` was latched on three the flip-flops `FF1`, `FF2`, `FF3`. At the next clock rising edge the three D-latches updated their state and transmitted `1`s to their outputs. Again, the power consumption's simulation is illustrated in Fig. 6a (red signal).

In classic side-channel models [9], the energies consumed for flipping 1 bit and 3 bits differ. Fig. 6a shows that such is indeed the case. As per our assumption, the *frequency signatures of these two operations are also different*.

Fig. 6a shows that the recovery time following a 3 bits change is longer than the compensation time of 1 bit. This recovery time difference results in a frequency variation. Fig. 6a shows that the 3 bits' current spike has a longer pulse period than the 1 bit spike, therefore the 3 bits signal alteration presents a lower frequency. Intuition suggests (and experiments confirm) that this difference will be detected by the HHT.

To show that HHT can detect frequency differences consider the power spectral density (PSD) of both signals during 1 bit and 3 bits switch (Fig. 6b). The maximal spectral amplitude of the 1 bit change is located at 4.99 GHz (point f_1) while the maximal spectral amplitude of the 3 bits change (point f_3) is at 4.55 GHz which is supportive of the hypothesis that HHT can distinguish frequency variations even in non-stationary signals. As expected, Fig. 6c shows that two sine functions (4.55 GHz and 4.99 GHz) correspond well to the side-channels' shapes.

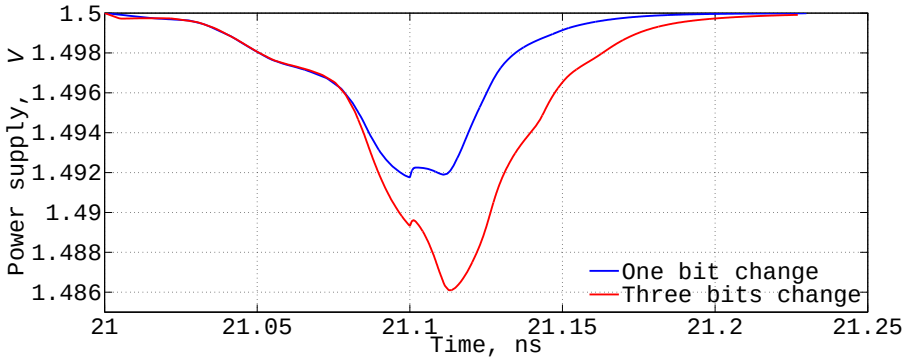
This shows that not only amplitude but also frequency varies during register switch. Logically, power consumption increases as more bits are flipped. However, simulation cannot prove that this variation is detectable in practice because frequency changes heavily depend on the Hamming weight of the data stored in the register. That is why the next section carefully examines the effect of register alteration on IF in a real AES FPGA implementation.

3.3 Hilbert Huang Transform of an AES Power Consumption Signal

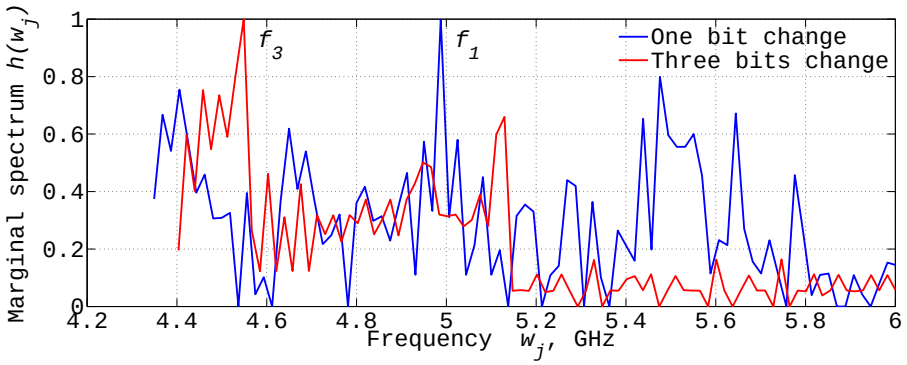
We start by performing a Hilbert Huang decomposition of a real signal. The analysis was performed on the power trace of the previously described AES-128 implementation. Signals were averaged 10 times and had 1,000 samples (Fig. 7a).

EMD decomposed the power trace to five IMFs and a residue, shown in Fig. 7b. After decomposition, each IMF was Hilbert Transformed to derive the power signal's time-frequency representation. Fig. 8 is an IF distribution of Fig. 7a.

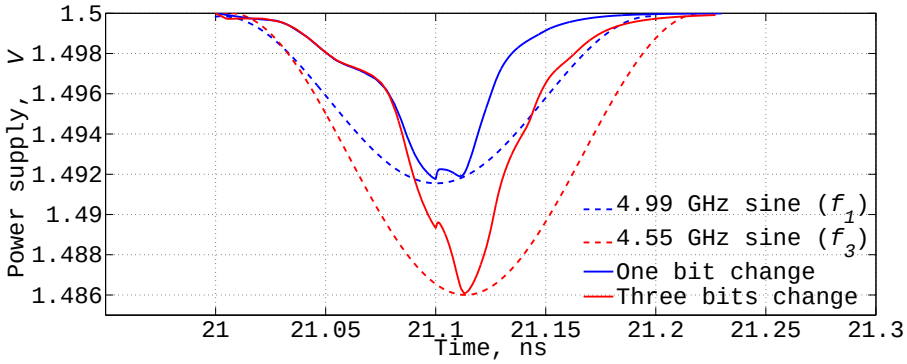
Amplitude combination over frequency gave the power spectral density plot of Fig. 9a. An important observation in Fig. 9a is that HHT spectrum shows the distribution of a periodic variable over the main peak frequencies. Notably, the



(a) Power consumption



(b) Power spectrum



(c) Power consumption and sines with the frequency of the maximum spectral amplitude

Fig. 6. Register switch of 1 and 3 bits.

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 Fig. 9b) 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. 10 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. Fig. 10 was drawn using 200,000 HHT-processed power traces. The thin solid line in Fig. 10 represents the mean IF value, obtained from the first IMF component, as a function of Hamming distance.

The principal trend is the ascending line. Fig. 10 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. 10 between Hamming distance and IF looks linear and therefore the Pearson correlation coefficient can be used as an SCA distinguisher.

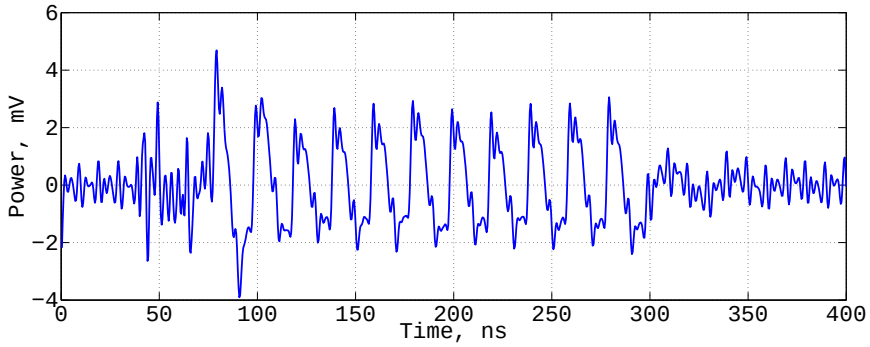
IF adoption for side-channel attacks presents some particularities. The disadvantage of the method is that data scatter is higher than in usual DPA and hence the attack requires more power traces. Another issue is that each time-series will be decomposed into a set of IMFs, hence every sample will be 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

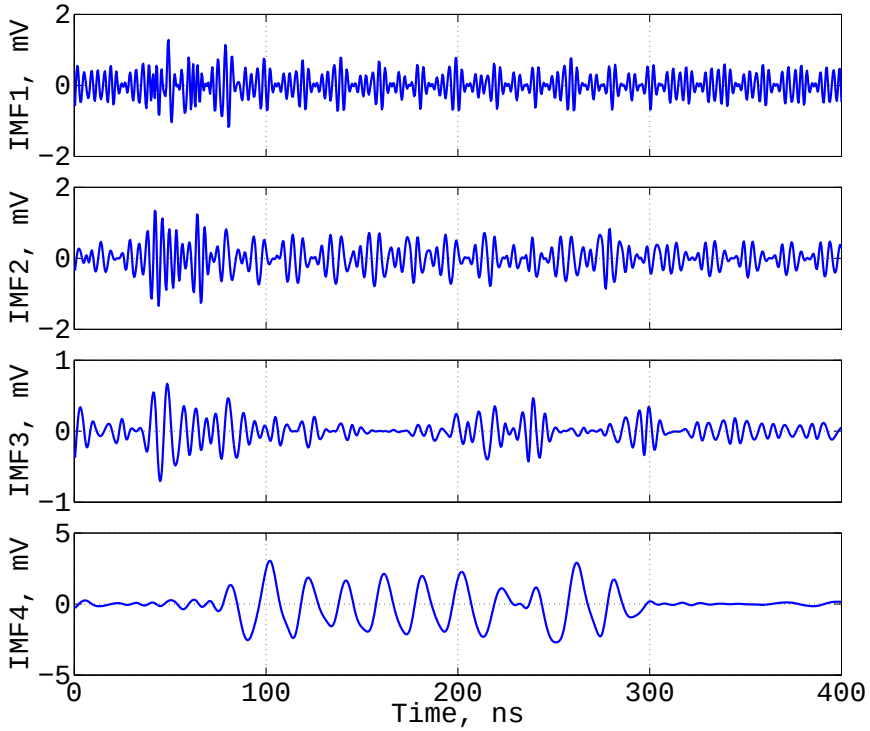
This section introduces Correlation Instantaneous Frequency Analysis (CIFA) and compares its performance with Correlation Power Analysis (CPA) and to Correlation Spectral Based Analysis (CSBA).

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



(a) Initial signal $u(t)$



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

Fig. 7. Power consumption of our experimental AES-128 implementation.

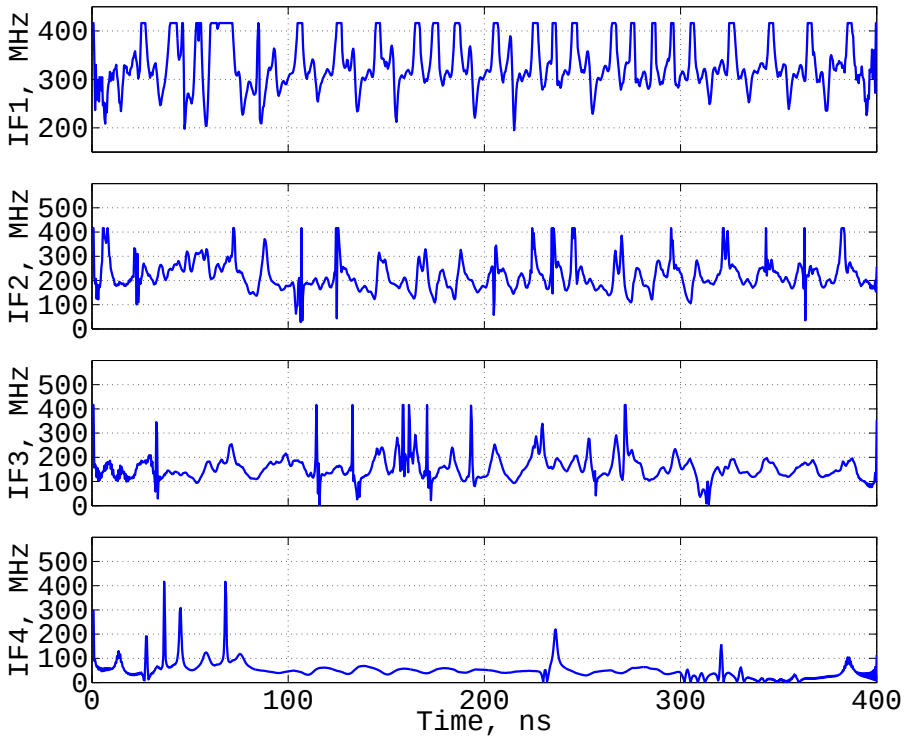


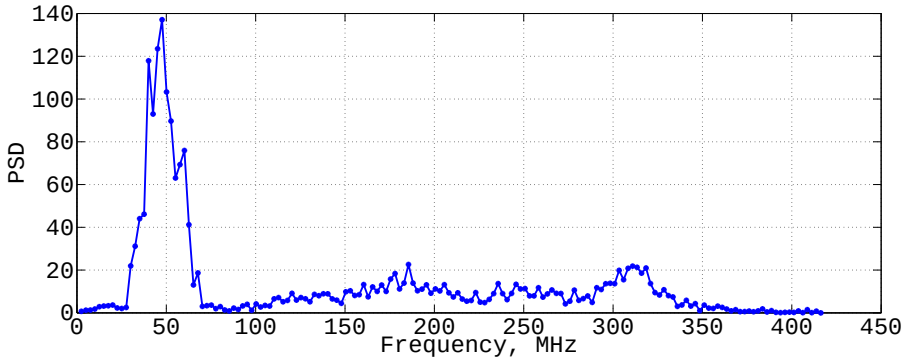
Fig. 8. IF distribution over time for the different IMFs of Fig. 7b.

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.

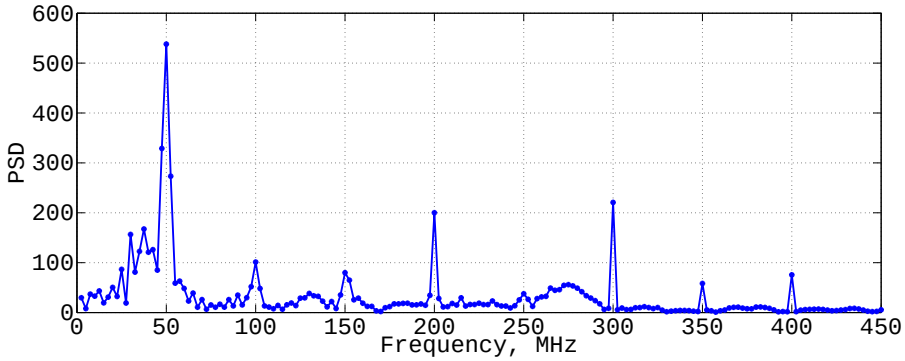
Generally, each higher rank IMF carries information present in smaller instantaneous frequencies (Fig. 8), this is why IMFs from different power traces were aligned index-wise, *i.e.* all first IMFs from every encryption were analyzed first, then all second IMFs and so on.

We chose the Hamming distance model and Pearson's correlation coefficient (see Algorithm 1) to investigate CIFA's properties and compare CIFA with other attacks.

CPA. CPA applied to power traces produces Fig. 11(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.



(a) Hilbert marginal spectrum



(b) Fourier Spectrum

Fig. 9. Power spectra of Fig. 7a

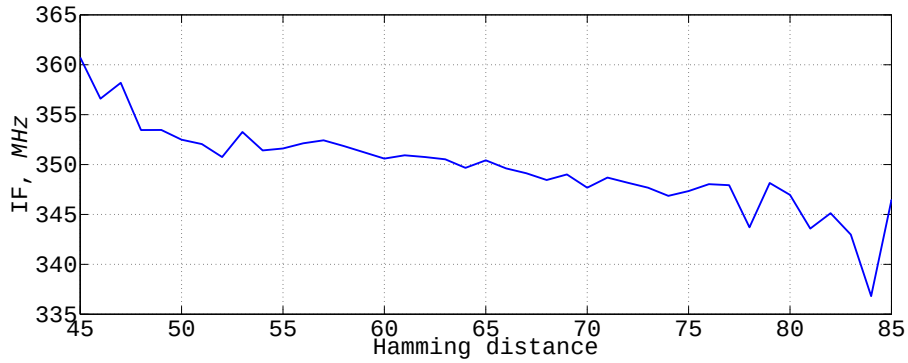


Fig. 10. Dependency between the Hamming distance of 9-th and 10-th AES round states and the IF of the first IMF component at time 276 ns (corresponding to the beginning of the last AES round).

Algorithm 1 Generic Side-Channel Analysis Algorithm

Input:

M ciphertexts $C_1, \ldots, C_M$;

u_t^j any type of side-channel information, where $j \in [1, M]$ is an encryption number, and $t \in [1, N]$ is a sample number.[1]

Output:

The maximum likelihood key byte k^*;

for $k = 0$ **to** 255 **do**

▷ *Create a power model* μ

for $j = 1$ **to** M **do**

$\mu_{k,j} \leftarrow \mathsf{HammingDistance}\left(C_j, \mathsf{InvShiftRows}\left(\mathsf{InvSbox}\left[C_j \oplus k\right]\right)\right)$

end for

▷ *Correlate the power model* μ *and the side-channel data* u

for $t = 1$ **to** N **do**

$\rho_{k,t} \leftarrow \mathrm{corr}\left(\{u_t^j\}_{j=1}^M, \{\mu_{k,j}\}_{j=1}^M\right)$

end for

▷ *For each byte value select the maximum correlation*

$\overline{\rho_k} \leftarrow \max\limits_{1 \le t \le N} \rho_{k,t}$

end for

▷ *Find the key byte maximizing correlation*

return the $k^* \in [0, 255]$ such that $\overline{\rho}_{k^*} = \max\limits_{0 \le k \le 255}(\overline{\rho_k})$

CSBA. Fig. 11(b) presents CSBA applied against Fourier power trace spectra with the same power 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. 11(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 CIFA $<$ CSBA $<$ 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 [2,19] DVS is cheap in terms of

[1] Note that t defines frequency when indexing PSD, and time when indexing power or IF.

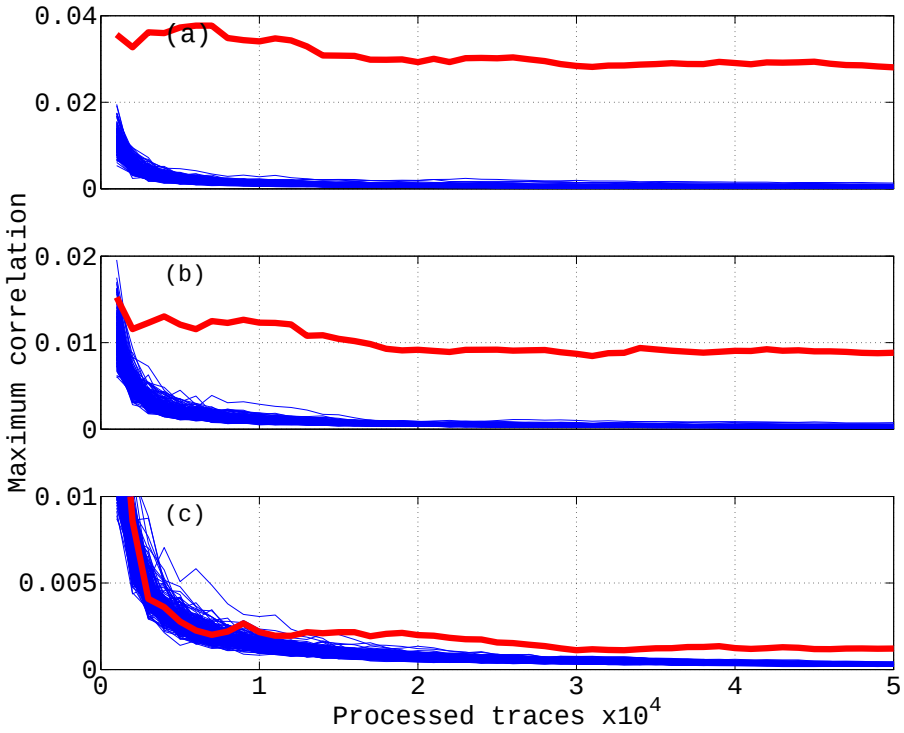


Fig. 11. Maximum correlation coefficients for a byte of the last round AES key in an unprotected implementation. Although the three attacks eventually succeed CPA>CSBA>CIFA. (a) CPA (b) CSBA (c) CIFA.

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 2. Each power trace was partitioned into γ segments of normally distributed lengths covering the whole dataset.[2]. Each segment was lifted by a uniformly distributed random offset ℓ that did not exceed a predetermined value D set to $D = 12$ mV. A trace modification example is presented in Fig. 12, in which the trace of Fig. 7a was processed by Algorithm 2.

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 (Algorithm 1).

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

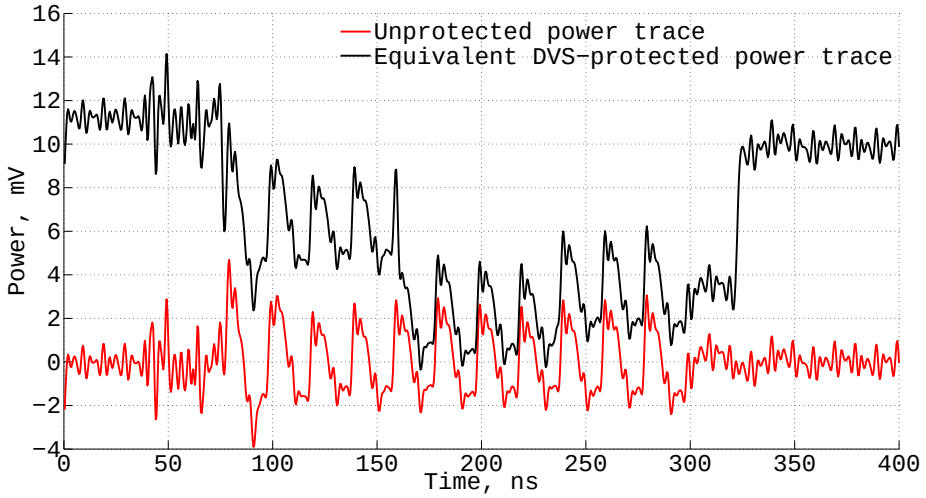


Fig. 12. Power traces of the FPGA AES implementation. The unprotected signal is shown in red. The DVS-protected signal is shown in black.

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. 13(a),13(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. 13(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.

5 Previsible Effect on other Countermeasures

In the light of the above the re-assessment of other side-channel countermeasures seems in order.

Side-channel countermeasures [21] can be categorised into 4 broad groups.

1 *Leakage reduction* diminishes the dependency between power consumption and binary data at the logic level (*e.g.* [17,27]).

  CIFA should offer no advantage when attacking a leakage reduction countermeasure because signal recovery time strongly depends on signal amplitude, which tends to be constant.

2 *Noise* consists in injecting an unpredictable component to the power trace either by scrambling amplitude or by shuffling operations in time (*e.g.* [19,21,26] or [7,8,28,29]).

Algorithm 2 Dynamic Voltage Scrambling (DVS) Simulator

Input:
A power trace $u(1), \ldots, u(N)$;
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 $u'(1), \ldots, u'(N)$;

▷ *Split the power 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 uniformilly 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

This paper showed that IF can overcome certain types of amplitude noise countermeasures. Moreover, because HHT was developed to handle non-stationary and non-linear signals, the HHT marginal spectrum can be adjusted to deal with temporal noise countermeasures.

3 *Randomization* changes the secret's representation so that sensitive data is no longer processed in clear. Randomization is typically implemented as explained in [21] or by using arithmetic and homomorphic properties of public key cryptosystems allowing to compute a result in one of many ways. Whenever the results of subroutines are independent, the defender may also execute these routines in a random order.

IF analysis is based on the Hamming weight model, hence CIFA is not expected to outperform CPA or DPA because these countermeasures prevent the attacker from creating the correct power model.

4 *Protocol-level solutions* consist in using leaky implementations in a secure way. Protocol-level countermeasures typically limit the number of encryptions per key (EEPROM counter per key), randomize encrypted or signed message or update keys continuously.

Protocol level protections limit the number of traces available to the attacker. Combination of signal amplitude, Fourier spectra and IF may bring some

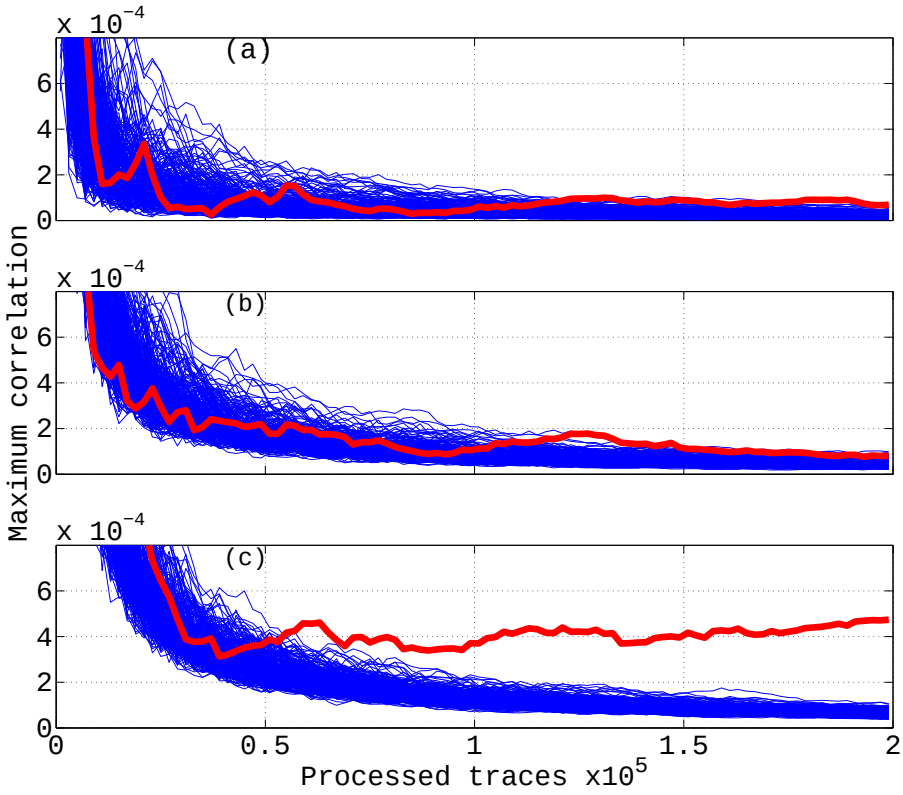


Fig. 13. Maximum correlation coefficient for a byte of the last round AES key with simulated DVS. (a) CPA (b) CSBA (c) CIFA.

advantage when discarding key values because three of these attacks rely on different noise models and may thus be applied independently. This conjecture must nonetheless be confirmed experimentally.

6 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 detecting 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.

Acknowledgement

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

References

1. Agrawal, D., Archambeault, B., Rao, J., Rohatg, P.: The EM Side-Channel(s). In: Cryptographic Hardware and Embedded Systems - CHES 2002, 4-th International Workshop. LNCS, vol. 2523, pp. 29–45. Springer (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. pp. 854–862. VLSID '07, 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. In: IBM Journal of Research and Development. vol. 17, pp. 525–532. IBM Corp. (Nov 1973)
6. Boashash, B.: Estimating and Interpreting the Instantaneous Frequency of a Signal. I. Fundamentals. In: Proceedings of the IEEE. vol. 80, pp. 520 –538 (Apr 1992)
7. Boey, K., Lu, Y., O'Neill, M., Woods, R.: Random Clock against Differential Power Analysis. In: Circuits and Systems (APCCAS) 2010. pp. 756–759 (2010)
8. Bouesse, G., Renaudin, M., Dumont, S., Germain, F.: DPA on Quasi Delay Insensitive Asynchronous Circtuits: Formalization and Improvement. In: Design, Automation and Test in Europe, 2005. vol. 1, pp. 424–429 (2005)
9. Brier, E., Clavier, C., Olivier, F.: Correlation Power Analysis with a Leakage Model. In: Cryptographic Hardware and Embedded Systems - CHES 2004: 6-th International Workshop. LNCS, vol. 3156, pp. 16–29. Springer (2004)
10. Gebotys, C., Ho, S., Tiu, C.: EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. In: Cryptographic Hardware and Embedded Systems - CHES 2005, 7-th International Workshop. LNCS, vol. 3659, pp. 250–264. Springer (2005)
11. Gebotys, C., Tiu, C., Chen, X.: A Countermeasure for EM Attack of a Wireless PDA. In: Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on. vol. 1, pp. 544 – 549 (Apr 2005)
12. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual Information Analysis - A Generic Side-Channel Distinguisher. In: Cryptographic Hardware and Embedded Systems - CHES 2008, 10-th International Workshop. LNCS, vol. 5154, pp. 426–442. Springer-Verlag (2008)

13. Huang, N., Shen, S.: The Hilbert-Huang Transform and its Applications. World Scientific Publishing Company (2005)
14. 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. In: Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences. vol. 454, pp. 903–995 (1998)
15. Kaslovsky, D., Meyer, F.: Noise Corruption of Empirical Mode Decomposition and Its Effect on Instantaneous Frequency. ArXiv e-prints (Aug 2010), http://arxiv.org/pdf/1008.4176v1
16. Keyes, R.: Physical limits in digital electronics. In: IEEE Proceedings. vol. 63, pp. 740–767 (May 1975)
17. Khatir, M., Moradi, A., Ejlali, A., Shalmani, M., Salmasizadeh, M.: A Secure and Low-Energy Logic Style using Charge Recovery Approach. In: SLPED 2008. pp. 259–264. ACM (2008)
18. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Advances in Cryptology - 19-th Annual International Cryptology Conference CRYPTO'99. LNCS, vol. 1666, pp. 388–397. Springer-Verlag (1999)
19. Krieg, A., Grinschgl, J., Steger, C., Weiss, R., Haid, J.: A Side Channel Attack Countermeasure Using System-On-Chip Power Profile Scrambling. In: On-Line Testing Symposium, IEEE International. pp. 222–227. IEEE Computer Society (2011)
20. Luo, Q.: Enhance Multi-bit Spectral Analysis on Hiding in Temporal Dimension. In: Smart Card Research and Advanced Application. LNCS, vol. 6035, pp. 13–23. Springer (2010)
21. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks - Revealing the Secrets of Smart Cards. Springer-Verlag (2007)
22. 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 (Feb 2011)
23. Mead, C., L.Conway: Introduction to VLSI systems. Addison-Wesley (1980)
24. Peng, Z., Gaoming, D., Qiang, Z., Kaiyan, C.: EM Frequency Domain Correlation Analysis on Cipher Chips. In: Information Science and Engineering (ICISE), 2009 1-st International Conference on. pp. 1729 –1732 (Dec 2009)
25. 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)
26. Standaert, F.X., Macé, F., E.Peeters, Quisquater, J.J.: Updates on the Security of FPGAs Against Power Analysis Attacks. In: ARC 2006. pp. 335–346 (2006)
27. Tiri, K., Akmal, M., Verbauwhede, I.: A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards. In: ESSCIRC 2002. pp. 403–406 (2002)
28. Yang, S., Wolf, W., Vijaykrishnan, N., Serpanos, D., Xie, Y.: Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switching Approach. In: Design, Automation and Test in Europe, 2005. pp. 64–69 (2005)
29. Zafar, Y., Park, J., Har, D.: Random Clocking Induced DPA Attack Immunity in FPGAs. In: Industrial Technology (ICIT), 2010. pp. 1068–1070 (2010)