Electromagnetic Transmission of Intellectual Property Data to Protect FPGA Designs

Lilian Bossuet[1], Pierre Bayon[2], Viktor Fischer[1]

1 Introduction

The microelectronics industry is faced with increased costs of production of integrated circuits (ICs). This increase is due to the costly technology refinement and the increasing complexity of systems (e.g. the transition from 32 nm to 28 nm technology has been accompanied by a 40% increase in the manufacturing costs of wafers 300 mm in diameter and by a 30% increase in the manufacturing costs of 450 mm wafers). For several years, this led to a sharp increase in the number of companies that do not have the means to produce IC (fabless companies) and to the relocation of production. ICs manufactured today are produced with a high added value in a highly competitive industry. In addition, the time-to-market is increasingly tight. This has made expensive devices the target of counterfeiting, cloning, illegal copy, theft and malicious hardware insertion (such as hardware Trojans) [1], [2].

1.1 The threat model of IC and IP

The counterfeiting of ICs has become a major problem in recent years [3]. For example, the number of counterfeit electronic circuits seized by U.S. Customs between 2001 and 2011 has been multiplied by around 700 [4]. Between 2007 and 2010, U.S. Customs confiscated 5.6 million counterfeit electronic products [5]. Overall, counterfeiting is estimated to account for about 7% of the semiconductor market [6], which represents a loss of around US$ 22 billion in 2014 for the lawful industry.

L. Bossuet, V. Fischer
Laboratoire Hubert Curien, CNRS UMR 5516
Université Jean Monnet, 42000 Saint-Etienne, France
e-mail : lilian.bossuet@univ-st-etienne.fr, fischer@univ-st-etienne.fr

P. Bayon
Brightsight, Delft, 2628, The Netherlands
bayon@brightsight.com

Fig. 1 is a simplified diagram of the life cycle of an IC from its design by a fabless designer to its recycling. This cycle includes many threats to the designer's intellectual property: netlist theft, mask theft, chip over-production (overbuilding), theft of the untested device, discarded device, reverse engineering, device counterfeiting, cloning, relabeled-repackaged-falsified "like new device", and hardware Trojan insertion.

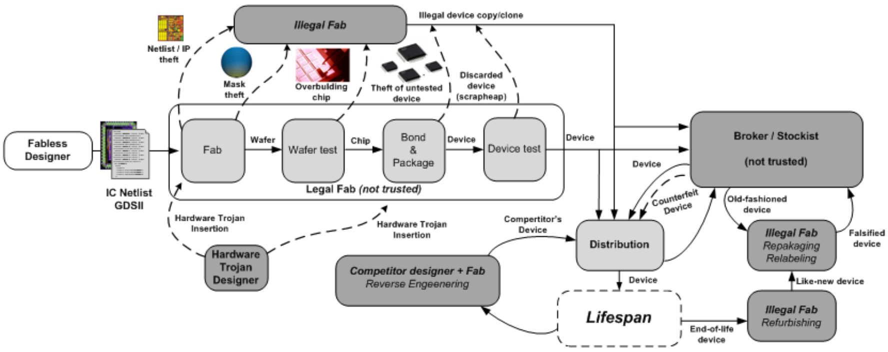


Fig. 1. Simplified life cycle of an IC from a fabless designer to device recycling and the associated threat model.

The threat model in Fig. 1 focuses on IC manufacturing and does not include the specific case of IP design and licensing. Indeed, for digital circuit design the re-use of IP is more and more important due to prohibitive cost of ASIC design, but the IP business suffers from a lack a security due to the intrinsic form of IPs sales and exchanges. Figure 2 presents a dedicated threat model focused on an IP life cycle. Many dedicated threats target the IP life cycle and result to revenues losses for the IP designers [1], [2]. The IP threat model includes illegal re-use, illegal sales, cloning (illegal copy) of the IP. The extent of threats targeting IPs is linked to the type of IP: soft IPs (typically hardware description language files), firm IPs (*synthesized* netlist), and hard IPs (FPGA bitstream or physical layout).

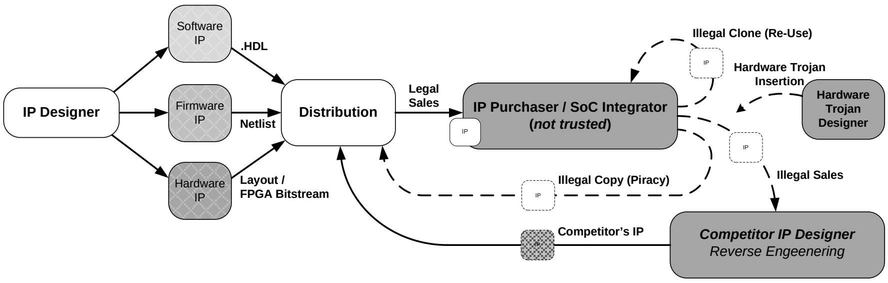


Fig. 2. Simplified life cycle of an IP with its threat model

We propose a way to counter theft, illegal copy, cloning and counterfeiting of ICs and IPs by designing a salutary hardware (*salware*) [7]. The term salware is the opposite of malware (malicious hardware). While salware can use the same techniques, strategy and means as malware [7], salware uses an embedded piece of hardware that is barely detectable, hard to circumvent, and is inserted in an IC or an IP to provide intellectual property information and/or to remotely activate the circuit or IP after its manufacture and during its use. IP watermarking, physical unclonable function (PUF) for IC authentication, remote activation, logic encryption, finite state machine (FSM) encryption, memory encryption, bus encryption, hardware metering, VHDL/Verilog obfuscation, bitstream encryption (for SRAM and Flash based FPGAs), are examples of the well-known salwares.

One of the solutions for the IP designers to protect their intellectual property is to be able to detect the presence of a copy of an IP embedded in a digital device by using IP identification. Works on IP watermarking and IP fingerprinting try to provide the IP identification service. But, most of the time the published solutions are not practical mainly because of the complexity of the watermarking/fingerprinting verification scheme [8], [9]. Efficient IP identification scheme needs to be contactless, rapid and ultra-lightweight. Up to now, these three characteristics are not available in the state-of-the-art. To meet these requirements, in this chapter we propose an ultra-lightweight binary frequency shift keying (BFSK) transmitter to forward IP identity (that could be generated for example by a feedback shift-register or a physical unclonable function [10]) discreetly using an electromagnetic channel. Such circuit is usually called "spy circuitry". Using the electromagnetic channel, it is possible to contactless check the presence of an IP inside a digital device. A preliminary version of this work was presented during the conference VLSI-SOC 2015 [11].

1.1 Salware vs. malware

In the area of security, the techniques used to attack and to defend have always been similar and the means designed for attacks can sometimes be used for protection. Our strategy in investigating the means of attack and malicious hardware is to develop new efficient salware.

Small, barely detectable hardware Trojans can disable part of a device or allow information leakage without degrading system performance [12], [13]. The same characteristics are required to design efficient salware, which is our objective. Embedding a Trojan inside an IP to protect the IP during its time-limited evaluation by the client was recently proposed in [14]. This work modifies the FSM of the IP with the aim of disrupting its normal behavior. In this way, the IP vendor can define the "expiry date" of the FSM control and disable it. In fact, this application uses a Trojan like time-based activation mechanism [12], [13]. Other activation mechanisms can be used to disrupt the IP in the case of illegal use such as an expired hardware license or an illegal copy. For example, a Trojan-like salware can use a PUF response to conditionally block an IP execution. Such a physical-condition-based activation makes it possible to link an IP to the hardware (hardware-linked license).

Another well-known threat in cryptographic engineering is side channel attacks [15], [16]. Most of the dynamic characteristics of both hardware and software implementations of cryptographic primitives can be used for side channel analysis: computation time, power consumption, electromagnetic radiation, optical radiation, even the sound produced during computation. However, the techniques used for side channel analysis can be used to implement a salware block: e.g. for reading intellectual property data from the device or for device authentication (watermark checking). Some published works propose spy circuitry using side channels to identify the embedded intellectual property. For example in [17], the thermal channel representing a contactless communication was used to transfer information from an embedded tag to a remote receiver. However the embedded thermal tag used in this commercial solution requires a relatively large area (255 Spartan-3 slices). In [18], the authors propose using two shift registers to generate a recognizable signature-dependent power consumption pattern to reveal the IP signature. Power consumption was also used in [19] to communicate the IP watermark data using classical differential power analysis (DPA [15]). To reinforce such work, the authors of [20] propose using the power supply signal of an IP as a physical hash function for fingerprinting.

As we mentioned above, hardware Trojans can be designed to change the operation of the infected device, but also to silently leak information. Hardware Trojans can use side channels to forward secret information such as a symmetric cipher key [21] from cryptographic hardware implementation [22], [23], even when secure key management is used [24]. Hardware Trojan is also used to cause or amplify side-channel leakage of cryptographic hardware [25]. Note that using side channels to detect a hardware Trojan has also been the subject of several studies [26], [27], [28].

However, designing salware with a Trojan-like hardware could present a new opportunity to protect IC and IP. In this paper, we propose a, Trojan-like, IC/IP information provider that is discreet, contactless, ultra-lightweight, and with a high bitrate. It uses an electromagnetic side channel to transmit useful information.

Except [17], all the related works use power consumption as a communication channel which is not contactless. Unlike the proposed solution, all the related works are not lightweight and rapid as the section 5 of this chapter will show.

2 EM communication of IP data

2.1 Principle

Previous works on the electromagnetic attacks targeting true random number generators (TRNGs) showed that electromagnetic radiation can be used very efficiently for both active (fault injection [29]) and passive (side channel analysis [30]) attacks. Compared to power analysis, the attacker measuring the near-field electromagnetic emissions can obtain additional partial information about the device, since, unlike measurement of power consumption, electromagnetic radiation can be measured locally. One of the main advantages of this side channel is that it is impossible to hide the leak concerning electromagnetic radiation by using a global countermeasure. Moreover the electromagnetic test bench is not expensive (less than US$ 10K without an oscilloscope, which is the most expensive component). Last but not least, a spectral analysis of the electromagnetic radiation provides information on the oscillating structure such as a ring-oscillator [30]. For all these reasons, we use the electromagnetic channel for our IC/IP identification scheme. To this end, we designed an ultra-lightweight BFSK transmitter.

As mentioned above, salware and malware can be based on similar principles. The same is true for the proposed BFSK principle, which can be used to design both salware (i.e. IP identity transmitter) and malware (i.e. stolen data transmitter driven by a hardware Trojan), as illustrated in Figure 3. There are two differences between using the BFSK as salware or malware. First, IP identification is activated outside the device by an ID checker, while the Trojan is activated internally. For example, the Trojan can be activated by a specific event (e.g. specific input sequence, internal data value, system state) or by pre-defined timing (e.g. a specific number of clock cycles) [12], [13]. Second, the enable signal of the BFSK transmitter is provided outside the salware: it is the same signal as that used to activate the IP identification. For malware, the BFSK transmitter's enable signal is driven internally by the hardware Trojan control logic. In this case, the Trojan activates the enable signal when it is ready to send the stolen data. Note that an enable signal is required in both applications to reduce the power consumed by the ring oscillator. Moreover, a permanently activated transmitter could be detected more easily by a spectral analysis of electromagnetic emanations of the device and could also cause local heating and premature aging of the chip.

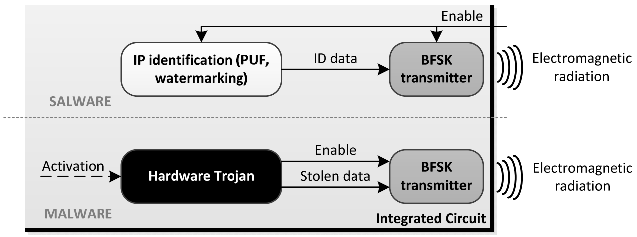


Fig. 3. Electromagnetic transmission of data (i.e. IP identification data or stolen secret data by a hardware Trojan such as the secret key for symmetric cipher).

2.2 Ultra-lightweight digital BFSK transmitter

Electromagnetic radiation is an efficient side channel since, unlike measurement of power consumption, electromagnetic radiation can be measured locally. For this reason, we use the electromagnetic channel for our IP identification scheme. To this end, we designed an ultra-lightweight BFSK transmitter which could be activated outside the device by an ID checker or internally by a specific event (e.g. specific input sequence, internal data value, system state). Note that an enable signal is required to reduce the power consumed by the ring oscillator. Moreover, a permanently activated transmitter could be detected more easily by a spectral analysis of electromagnetic emanations of the device and could also cause local heating and premature aging of the chip.

BFSK is one of the common modulation schemes used in digital communication. The binary data are sent using a sinusoidal carrier at two frequency tones f_0 and f_1, representing high ('1') and low ('0') logic levels. The binary data arriving at the transmitter input at certain bitrates determine the commutation of the tones at the transmitter output. The proposed BFSK transmitter uses a dedicated configurable ring-oscillator, as shown in Fig. 4. The configurable ring-oscillator is designed using one multiplexor, $N+K$ delay elements, and a feedback chain controlled by a NAND gate for activation of transmission to reduce power consumption. Actually, the transmitter is used only during a short time when the enable signal is high, and it consumes power only during this small piece of time. The power consumption of this transmitter is thus completely negligible.

Input data controls the multiplexor, as shown in Fig. 4. When input data is low, the ring oscillator uses N delays and its oscillation frequency is f_0. When input data is high, the ring oscillator uses $N+K$ delays and its oscillation frequency is f_1. Since the ring oscillator's oscillation frequency decreases with an increase in the number of delay elements, frequency f_0 is higher than frequency f_1. These two frequencies have to be selected according to the bandwidth of the electromagnetic analysis platform, which is used to acquire and measure the transmitted signal.

The bandwidth of our test bench, which is described in Section 3, was limited to 100 MHz and 1 GHz by the low-noise amplifier.

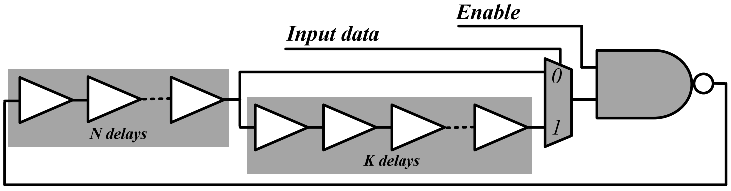


Fig. 4. Architecture of the ultra-lightweight digital BFSK transmitter based on a configurable ring oscillator.

The proposed BFSK transmitter was implemented in Microsemi FUSION flash based FPGA (130 nm CMOS technology) containing 600K logic gates (M7AFS600). The device contains 13 824 tiles, each tile can be used to implement one D-flip-flop or one configurable multiplexor-based logic block implementing any 3-input logic function.

The configurable number of delays in the ring oscillator of the proposed BFSK transmitter makes it possible to select precisely the two frequencies f_0 and f_1 using parameters N and K. Table I lists the ring oscillator frequencies and the number of Fusion tiles used by the BFSK transmitter for five values of N and K, with N ranging from 0 to 4, and K ranging from 1 to 5. According to Table I, f_0 can be chosen between 119 MHz ($N=4$) and 385 MHz ($N=0$) and f_1 can be chosen between 70 MHz ($N=4, K=5$) and 280 MHz ($N=0, K=1$). The exact value of f_0 depends on the number of delay elements, but also on the placement and routing of the transmitter. For the values N and K listed in Table I, the frequency variation was less than 1.7% (the maximum frequency deviation in Table I is 2 MHz when $N = 4$).

The number of tiles used by the BFSK transmitter is very low, i.e. from 3 tiles ($N=0, K=1$) to 11 tiles ($N=4, K=5$). These values are equivalent to less than 0.022% and less than 0.080% of the total number of tiles included in the targeted 600K-gate FUSION FPGA, respectively. This very small number of tiles is very promising for good dissimulation of the BFSK transmitter inside the sea of gates/tiles. The number of FUSION tiles required by the BFSK transmitter is given by the following equation (i).

$$Number\_FTiles = N + K + 2 \quad (i)$$

In order to estimate the number of resources needed for implementation with Xilinx SRAM FPGA or Altera SRAM FPGA, Table I gives the number of 4-input look-up-tables (LUT4) used by the BFSK transmitter with such FPGAs. The number of LUT4 required by the BFSK transmitter is given by the following equation (ii).

$$Number\_LUT4 = N + K + 1 \quad (ii)$$

To evaluate the logical resources needed by the BFSK transmitter in ASIC implementations, the right hand column in Table I gives the number of equivalent gates (EG) in the transmitter. The gate count was estimated using the Virtual Silicon standard cell library based on the UMC L180 0.18 µm 1P6M Logic process (UMCL18G212T3 [31]). The delay gates are replaced by more efficient standard NOT gates. The gate count of a standard NOT gate is 0.67 EG, and that of the standard multiplexor, 2.33 EG. The standard NAND gate uses 1 EG. So the number of gates of the whole BFSK transmitter ranges from 4.67 EG ($N = 0, K = 1$) to 10.03 EG ($N = 4, K = 5$). Note that one flip-flop requires between 5.33 EG and 12.33 EG to store a single bit [31].

TABLE I. Hardware implementation results of the BFSK transmitter

N	*K*	*f_0 (MHz)*	*f_1 (MHz)*	*Fusion Tiles*	*LUT4*	*EG*
0	*1*	*385*	*280*	*3*	*2*	*4.67*
	2	*383*	*210*	*4*	*3*	*5.34*
	3	*384*	*151*	*5*	*4*	*6.01*
	4	*385*	*130*	*6*	*5*	*6.68*
	5	*381*	*111*	*7*	*6*	*7.35*
1	*1*	*272*	*189*	*4*	*3*	*5.34*
	2	*272*	*156*	*5*	*4*	*6.01*
	3	*270*	*120*	*6*	*5*	*6.68*
	4	*271*	*106*	*7*	*6*	*7.35*
	5	*269*	*93*	*8*	*7*	*8.02*
2	*1*	*168*	*144*	*5*	*4*	*6.01*
	2	*169*	*124*	*6*	*5*	*6.68*
	3	*169*	*100*	*7*	*6*	*7.35*
	4	*168*	*91*	*8*	*7*	*8.02*
	5	*168*	*79*	*9*	*8*	*8.69*
3	*1*	*146*	*128*	*6*	*5*	*6.68*
	2	*147*	*112*	*7*	*4*	*7.35*
	3	*146*	*92*	*8*	*5*	*8.02*
	4	*145*	*84*	*9*	*6*	*8.69*
	5	*144*	*74*	*10*	*7*	*9.36*
4	*1*	*123*	*110*	*7*	*6*	*7.35*
	2	*121*	*98*	*8*	*7*	*8.02*
	3	*122*	*83*	*9*	*8*	*8.69*
	4	*121*	*77*	*10*	*9*	*9.36*
	5	*119*	*70*	*11*	*10*	*10.03*

Such a transmitter is clearly ultra-lightweight in both FPGA and ASIC implementations. The small logical resources requirement of the proposed spy circuitry makes reverse engineering it harder, although not impossible [32]. Even with recent CMOS technologies, the attacker can reverse engineer ICs using a scanning electron microscope and an automatic tool for circuitry extraction [32], [33]. Nevertheless, the smaller the piece of hardware used for BFSK transmitter the harder it is to detect during reverse engineering. Detection of the transmitter using standard Trojan detection methods [34], [35] is not feasible because the transmitter does not change the data path of the circuit and because of the ultra-low signal-to-noise ratio on the electromagnetic channel, as shown in our experimental results below (Section 4).

3. Experimental results

The electromagnetic radiation of the device was evaluated using the near-field electromagnetic analysis test bench described in [30]. The border between the far field and the near field can be considered to be about 23 mm from the device, depending on the hardware concerned. The most important part of the test bench is the acquisition chain. It determines the signal to noise ratio and measurement precision.

The chain, as presented in Fig. 5, is composed of:

- A Langer magnetic probe with a frequency range of from 30 MHz to 3 GHz and a spatial resolution of approximately 500 µm.
- A Miteq low-noise amplifier with a frequency range of from 100 MHz to 1 GHz.
- A Tektronix real time signal analyzers RSA5106B with a frequency range from 1Hz to 6.2GHz [36].

As presented in Fig. 5, the device to be tested (the board) is fixed to a XYZ table with repeatability of movement of 1 µm. The test bench, including the acquisition chain, XYZ table, FPGA configuration and power supply variations, is controlled by a computer. This test bench was first developed for electromagnetic attacks of TRNGs [29], and [30].

The targeted FPGA for the experimental work is an Altera Cyclone III EP3C25 that uses a 65nm CMOS technology. It contains 24 624 four-inputs LUT and 608 256 RAM bits.

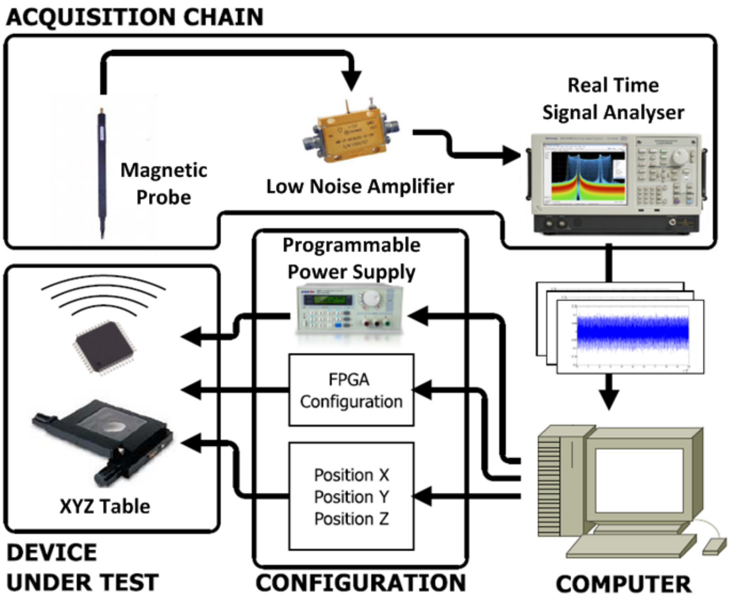


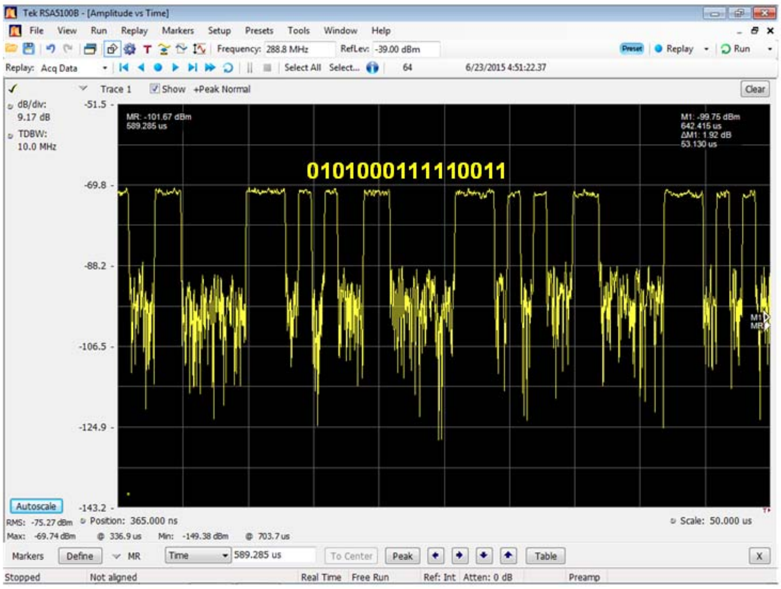
Fig. 5. Near-field electromagnetic analysis test bench

Electromagnetic analysis of IC is contactless, local, and can be spatial or/and temporal. This last point makes it possible to perform frequency analysis of the electromagnetic emanation. In the your bench the spectral range is limited to 100 MHz and 1 GHz. Standard devices aimed at direct BFSK demodulation cannot be used for these relatively high frequencies. Available integrated BFSK demodulators are limited to a few dozen megahertz. For this reason, we developed a dedicated BFSK demodulation scheme for our needs, in which a spectral analysis of the low noise amplifier output (a component of the test bench) is performed to measure the f_0 and f_1 spectral contribution. The transmitted high (low) level is detected when f_1 spectral contribution is higher (lower) than that of f_0.

For the coherent demodulation of the electromagnetic radiation, we propose a slippery window spectral analysis. Indeed, overall spectral analysis masks the effects of the no stationarity of the signal and therefore provides no information about its temporal evolution. Slippery window spectral analysis is a three-dimensional representation of the signal: amplitude, frequency, and time. It requires two quantities *Fw*, the width of the FFT window frame and the difference $\Delta\tau$ between two frames. For our experiment, we chose *Fw* equal to 16 384 points (2^{14}-point FFT) and $\Delta\tau$ equal to 100 points. For each frame, the FFT provides the software demodulator with the amplitude of signals f_0 and f_1 which enables the demodulator to distinguish between a transmitted ‘1’ or ‘0’.

To illustrate data transmission from the circuit via the EM channel, we used a shift register that stored the following 16-bit sequence: “0101000111110011”. The clock frequency of the shift register is 1 MHz. When the enable signal of the transmitter is given, the sequence is sent cyclically to the BFSK transmitter, which transmits it via the electromagnetic channel. The following gives the result of the coherent demodulation obtained at a 1 Mbps bit rate, which served as a proof of concept.

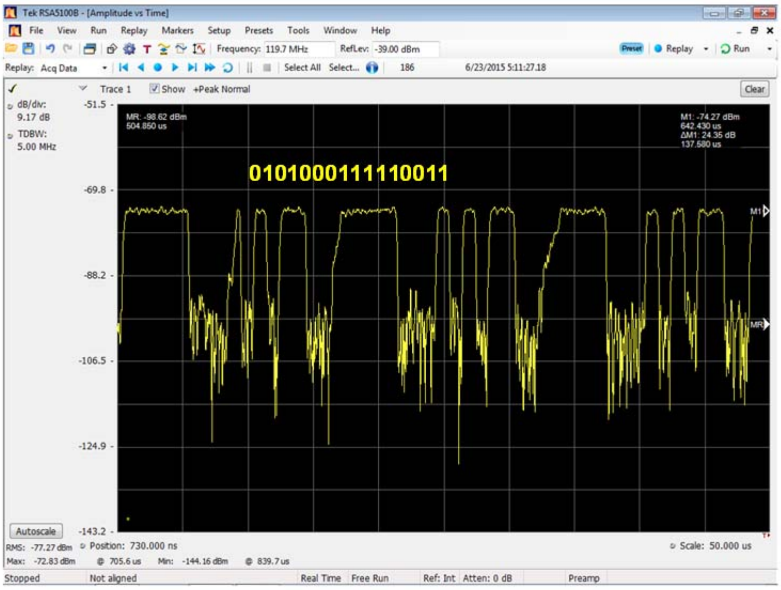
Fig. 6 and Fig. 7 present the temporal evolution of the spectral analysis (amplitude) of the BFSK transmitter's electromagnetic emission when $N = 6$ and $K = 10$, which corresponds to the following frequencies: f_0 = 289 MHz (Fig. 6) and f_1 = 119 MHz (Fig. 7). Notice also that we placed a small antenna in the close vicinity of the ring. With $N = 6$ and $K = 10$ the BFSK transmitter uses only 17 four-inputs LUT of the FPGA that represents 0.065% of the available logical resources of the used Altera FPGA for theses experimental results.


Tek RSA5100B - [Amplitude vs Time]

Frequency: 288.8 MHz
RefLev: -39.00 dBm
Replay: Acq Data
64
6/23/2015 4:51:22.37
Trace 1 ☑ Show +Peak Normal
dB/div: 9.17 dB
TDBW: 10.0 MHz
MR: -101.67 dBm
589.285 us
M1: -99.75 dBm
642.415 us
ΔM1: 1.92 dB
53.130 us
RMS: -75.27 dBm
Position: 365.000 ns
Scale: 50.000 us
Max: -69.74 dBm @ 336.9 us
Min: -149.38 dBm @ 703.7 us
Markers MR Time 589.285 us
Stopped
Not aligned
Real Time
Free Run
Ref: Int
Atten: 0 dB
Preamp

Fig. 6. Amplitude vs time evolution of the spectral analysis at f_0 = 289 MHz.

For the direct coherent demodulation of the electromagnetic radiation, we propose to use a slippery window spectral analysis in order to obtain a spectral cartography. Indeed, overall spectral analysis masks the effects of the non-stationarity of the signal and therefore provides no information about its temporal evolution. Slippery window spectral analysis provides a three-dimensional representation of the signal (spectral cartography): amplitude, frequency, and time. The used Tektronix real time signal analyzers [36] allows us to obtain directly the spectral cartography with direct reading of the patent that contains the transmitted data sequence. Fig 8 shows the spectral cartographies obtained at f_0 = 289 MHz and f_1 = 119 MHz.



Frequency: 119.7 MHz
RefLev: -39.00 dBm
Replay: Acq Data
+Peak Normal
dB/div: 9.17 dB
TDBW: 5.00 MHz
MR: -98.62 dBm
504.850 us
M1: -74.27 dBm
642.430 us
ΔM1: 24.36 dB
137.580 us
RMS: -77.27 dBm
Max: -72.83 dBm @ 705.6 us
Min: -144.16 dBm @ 839.7 us
Position: 730.000 ns
Scale: 50.000 us
Ref: Int
Atten: 0 dB

Fig. 7. Amplitude vs time evolution of the spectral analysis at f_0 = 119 MHz.

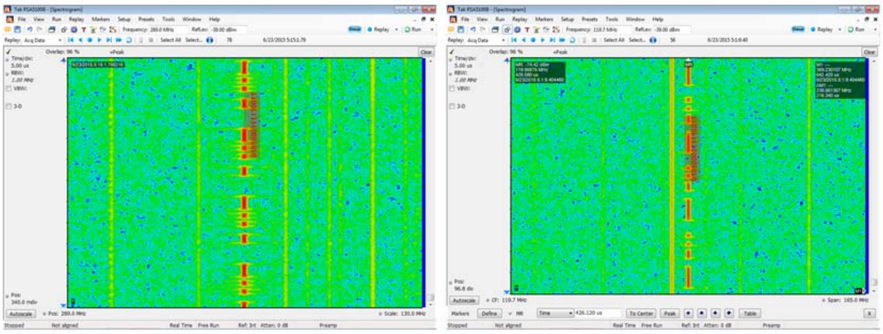


Fig. 8. Spectral cartographies center (red trace) on f_0 = 289 MHz (left) and on f_1 = 119 MHz (right) with 1Mbps data rate.

Without knowledge of the BFSK parameters, the electromagnetic transmission cannot be easily detected because it cannot be distinguished from spectral noise. The signal-to-noise ratio of the BFSK transmission is -135 dB for a 1 GHz bandwidth. Such an ultra-low SNR represents efficient protection against unwanted BFSK transmitter detection via a side channel. However, knowing the N and K parameters, the BFSK designer can calibrate the demodulation (determine the two frequencies) by electromagnetic analysis of the ring oscillators based on the differential spectral analysis as described in [30].

4 Second version of the ultra-lightweight digital EM transmitter

Now, based on the previous experimental results we propose an enhance EM transmitter. Indeed, by using the Tektronix real time signal analyzers [36], we are able to clearly distinguish the transmitter data sequence by analyzing the spectral cartography at only one frequency. Originally, we use two frequencies in order to simplify the demodulation [11].

The new version of the transmitter is based on the use of only one frequency with an on-off controllable ring-oscillator. The binary data are sent using only one sinusoidal carrier at f_0 representing high ('1') logic level. A low ('0') logic level is obtained without transmit sinusoidal carrier (i.e. the ring-oscillator is *off*). The proposed EM transmitter uses an on-off controllable configurable ring-oscillator, as shown in Fig. 9. The on-off controllable ring-oscillator is designed using one multiplexor and *K* delay elements, and a feedback chain controlled by a two NAND gate for activation of transmission. The logical resource required for this transmitter is really low because it uses only *K* 4-inputs LUT with Altera and Xilinx FPGAs.

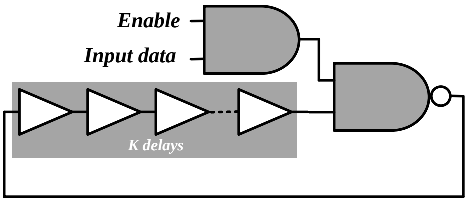
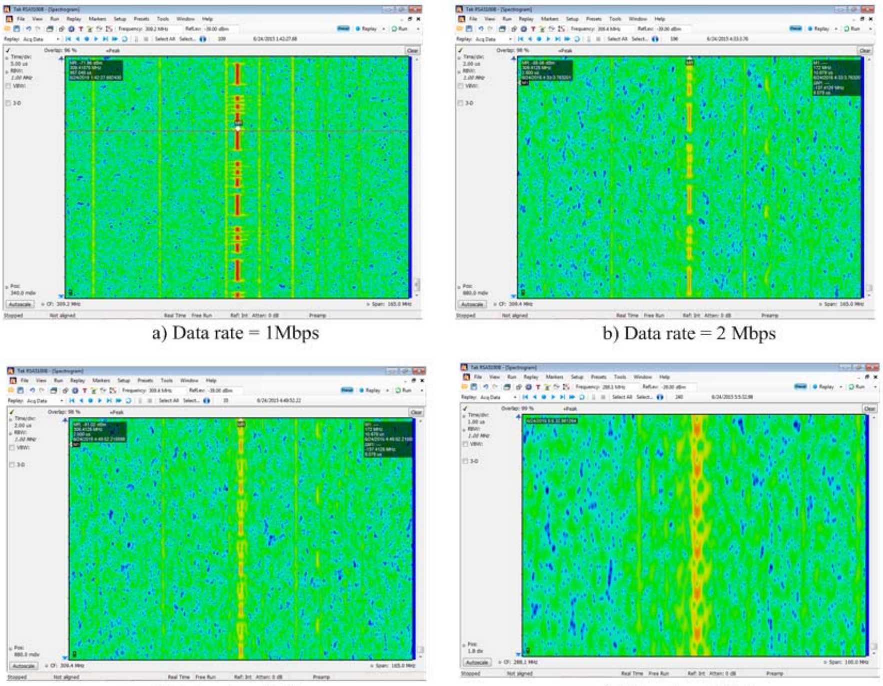


Fig. 9. Architecture of the ultra-lightweight digital EM transmitter based on an on-off controllable ring oscillator.

The previously presented (Fig. 5) experimental setup is used to test this transmitter. The parameter *K* is fixed to 6 to set the frequency f_0 to 309 MHz. The Fig. 10 presents the measured spectral cartographies center to f_0 with four data rates from 1 Mbps to 16 Mbps (we used the same data sequence that for the Fig. 8). This figure shows that it is possible to demodulate the transmitted sequence for 1 Mbps and 2 Mbps data rates without signal processing. It is harder to directly demodulate the data for 4 Mbps and 16 Mbps data rates, but they could be demodulated by using signal processing. These results clearly validate the proof of concept of the proposed EM transmitter. Nevertheless, the provided results (Fig. 10) are given when the EM transmitter works alone inside the FPGA.



a) Data rate = 1Mbps

b) Data rate = 2 Mbps

c) Data rate = 4 Mbps

d) Data rate = 16 Mbps

Fig. 10. Spectral cartographies center (red trace) on f_0 = 309 MHz with 1Mbps data rate (a), 2 Mbps (b), 4 Mpbs (c) and 16 Mbps (d).

In order to test the behavior of the EM transmitter when it is embedded in a larger system we add two large IPs in the FPGA. These two IPs are an AES cipher and a AES decipher [21]. These two IPs require 1 772 LUT4 (4.76 % of the targeted Altera FPGA) when the EM transmitter requires only 6 LUT4 (0.025 % of the targeted Altera FPGA). The transmitter ratio between the two IPs and the EM transmitter is equal to 295.3. Fig. 11 presents the floorplan of the FPGA after configuration. Notice that we have forced the placement of the EM transmitter in order to place it in the center of the full system.

In this case, it is always possible to demodulate the data sequence with 1 Mbps data rate. Nevertheless, it could be necessary to precisely place the EM probe over the device under test. Fig. 12 illustrates the modification of the spectral cartography at f_0 function of the positions of the probe. Four positions, $P_{\#0}$, $P_{\#1}$, $P_{\#2}$ and $P_{\#3}$ are tested on the same horizontal axis. The space between each position is a 3 mm gap. On Fig. 12, it appears that the data sequence is always visible, but du to other spectral contributions that come from the two other IPs inside the device, it is more difficult to directly demodulate the sequence for the positions $P_{\#0}$ and $P_{\#1}$. The position $P_{\#2}$ gives the best result. This research of the best position is really fast for the designer of the system because he knows the precise position of the EM transmitter inside the chip.

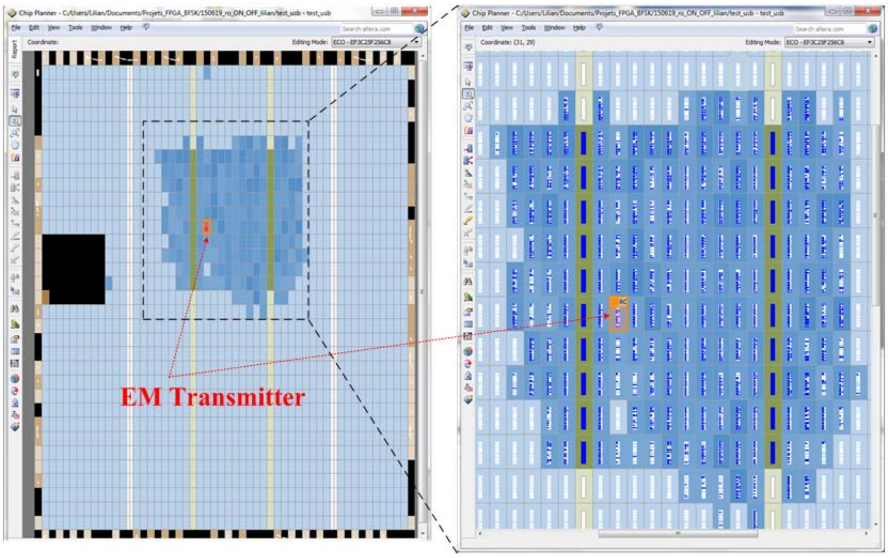

Chip Planner - C:/Users/Lilian/Documents/Projets_FPGA_BFSK/150619_ro_ON_OFF_lilian/test_usb - test_usb
File Edit View Tools Window Help
Search altera.com
Coordinate:
Editing Mode: ECO - EP3C25F256C8
Chip Planner - C:/Users/Lilian/Documents/Projets_FPGA_BFSK/150619_ro_ON_OFF_lilian/test_usb - test_usb
File Edit View Tools Window Help
Search altera.com
Coordinate: (31, 29)
Editing Mode: ECO - EP3C25F256C8
EM Transmitter

Fig. 11. Floorplan of the test system with one AES cipher, one AES decipher and the EM transmitter.

5 Comparison with state of the art spy circuitries using a side-channel

Table II compares the implementation of the proposed ultra-lightweight BFSK transmitter with other recently published state of the art methods. Table II gives the spy circuitry application (*App.*) for each reference; this may be IP protection (*IPP*) or hardware Trojan (*HT*) or both (for the presented work, *PW* [11]). In addition, Table II gives the year of publication (*YoP*), the side channel used, the hardware resources required only for the leakage generator (for example we do not take the hardware used for IP watermark generation or the Trojan's payload into account). Unfortunately, the principles compared do not use the same amount of hardware resources. For the sake of correctness, we give the implementation results as they are presented in the referenced papers. Nevertheless, the implementation bitrate of these previously published works can be roughly compared with our proposed solution. Based on published data, we computed the bitrate of all the proposals by using the number of clock cycles needed to send information via the side channel. For all the references presented in this table, the bitrate was computed using a 1 MHz frequency for data synchronization (same frequency is used during the experimental works presented previously).

As can be seen in Table II, the proposed work reaches the highest bitrate. The reason for such a good performance is first that we use a spectral analysis of the local electromagnetic leak based on a simple frequency modulation. Except for [17], all the other solutions use a global measurement of power consumption, which reduces the signal-to-noise ratio of the information leaked via the side channel. Our proposal is clearly the smallest spy circuitry ever published. Although solutions based on circular shift-registers are well adapted to last generation FPGA families, since the 16-bit shift registers can be designed using only one look-up table, they are not suitable for ASIC technologies. Currently, an ASIC implementation of a 16-bit shift register requires 16 flip-flops whereas the solution we propose occupies an area equivalent to only one D-flip-flop.

In this chapter, we present the proposed spy circuitry for IP protection, but it can also be used for hardware Trojan. Most of the other proposals could also be used for both applications. Note that in 2012, Kasper et al. proposed to use the work initiated in [22] for hardware Trojan or IP watermarking implementation [37]. However, by using electromagnetic emanation and a configurable ring oscillator, the proposed solution is the most convincing for industrial applications (e.g., those aimed at IP protection) because of its very small area and high bitrate.

TABLE II
SUMMARY OF CHARACTERISTICS OF SPY CIRCUITRIES EXPLOITING SIDE-CHANNELS

App.	*Ref.*	*YoP*	*Side channel*	*Hardware resources*	*Target*	*Bit rate @1MHz*
IPP	*[17]*	*2008*	*Thermal emanation*	*255 Spartan-3 slices*	*Xilinx Spartan-3*	*14.10^{-3} bps*
	[18]	*2008*	*Power consumption*	*16 * 16-bit circular shift-registers*	*Xilinx Spartan-3 and Virtex-II*	*400 bps*
	[19]	*2010*	*Power consumption*	*16-bit circular shift-register*	*Xilinx Virtex-II Pro*	*1 Kbps*
HT	*[22]*	*2009*	*Power consumption*	*8 parallel D-flip-flops or 16-bit circular shit register*	*Xilinx Spartan-3E and Virtex-II Pro*	*970 bps*
	[23]	*2013*	*Power consumption*	*16-bit circular shift-registers per bit*	*Xilinx Virtex-5*	*1.9 kbps*
Both	*PW*	*2015*	*Electro-magnetic emanation*	*1 configurable ring-oscillator (like a D-flip-flop in ASIC)*	*Altera Cyclone III*	*1 Mbps*

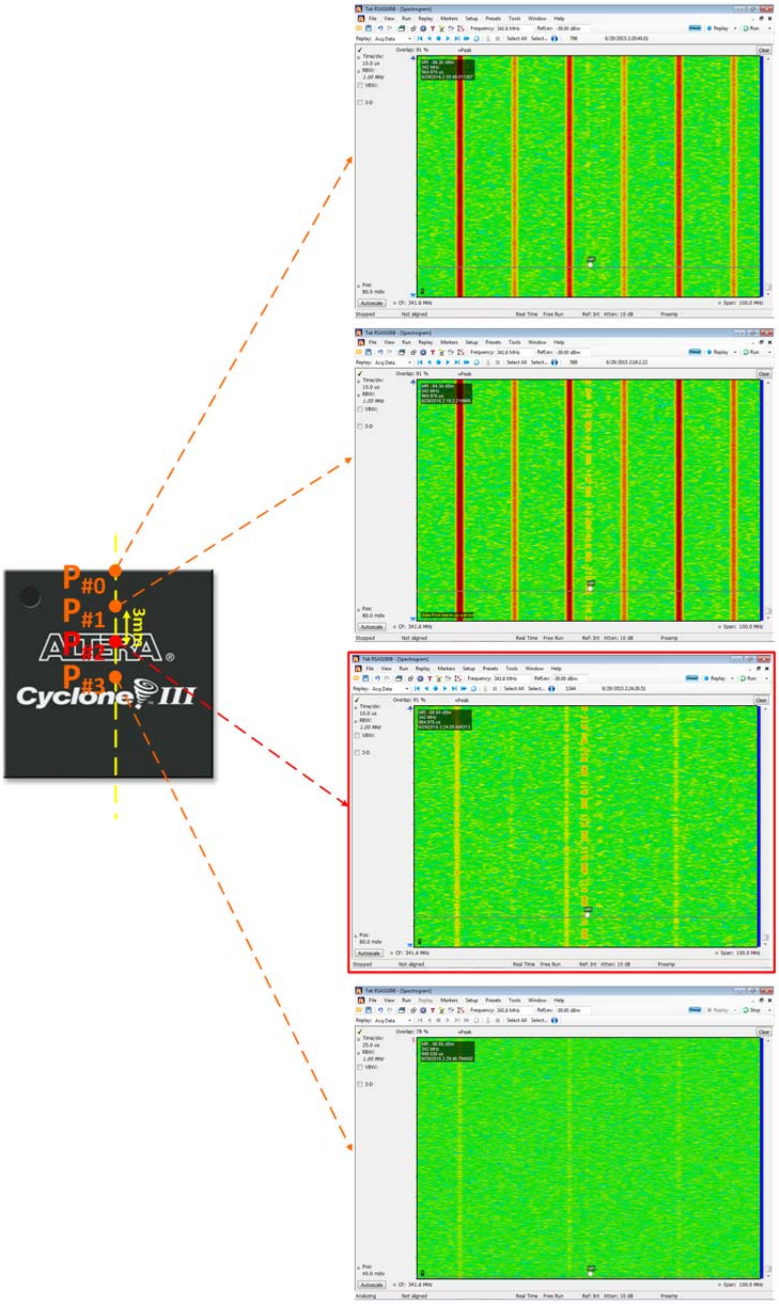


Fig. 12. Spectral cartographies center (red trace) on f_0 = 309 MHz with 1Mbps data rate for four different positions of the EM probe over the chip.

6 Industrial scenarios using the proposed IP protection

According to the previous section, in comparison with other works, our proposal goes clearly towards using a spy circuit in an industrial context for IP protection. Two industrial scenarios are presented in the following. The first scenario is the identification of embedded IP in the supply chain. This identification is used in order to be sure to don't use counterfeiting (fake) devices.

It is therefore crucial and strategic to be able to detect counterfeit IC as soon as possible in the supply chain (this is particularly crucial for military and space grad devices). Fig. 13 shows a possible framework to manage the device under test (control the enable signal) and check the IP identification by using an EM probe, an amplifier and a dedicated acquisition system including a spectral analysis and the proposed demodulation method. Due to the high bit rate of the proposition solution the identification of the ID requires less than 500 µs (with 1 Mbps bit rate). This counterfeiting detection could be completed by other physical (invasive or not) and optical inspection [38].

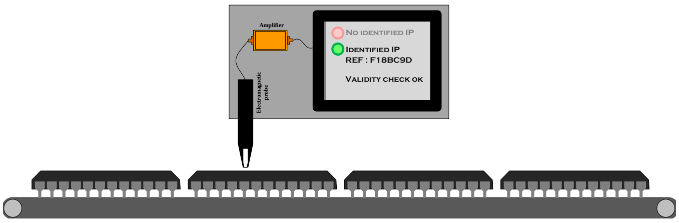


Fig. 13. Rapid and contactless IP identification in the supply chain by using EM transmission of IP' ID.

The second scenario occurs when an IP designers would like to verify the illegal presence of its IP inside a device (ASIC or FPGA). In this case the proposed transmitter provides to the identification scheme a data like a PUF [39] or a watermarking. Watermarking is a technique of steganography which provides the ownership of an IC (or an IP) by checking for the presence of hidden information called the watermark [8], [9]. Most of the watermarking methods proposed in the literature need a complex verification scheme. Nevertheless it is possible to use power consumption as proposed in [9] but it is easy and cheap to use global countermeasure in order to mask the power consumption due to the watermark [40]. Using electromagnetic emanation in this scenario is better because as electromagnetic emanation is local it is really hard to mask it by using a global countermeasure. Moreover, in this paper we have shown that due to the SNR of BFSK signal, it is unrealistic to try to detect it without the precise knowledge of the used frequencies for data transmission.

Conclusion

IP protection has become crucial topics for hardware security due to the lack of trust in IP market. In this chapter, we have presented two ultra-lightweight transmitters of IP identity using the electromagnetic side channel. Based on a configurable ring oscillator, our first solution exploits a BFSK signal to transmit information by way of the electromagnetic channel. Our second version is simpler; it is based on an on-off ring oscillator to transmit information with only one frequency. By performing a slippery window spectral analysis of the near field electromagnetic emanations captured locally over the transmitter circuitry, the proposed transmission achieves a high bitrate (experimentally at less 1 Mbps), which has not been achieved before. Moreover, the transmitter occupies very small area less than the requirement of a small D-flip-flop. Such a small requirement of logical resources makes reverse engineering of the chip very difficult and detection of the transmitter using standard Trojan detection methods is not feasible.

Acknowledgment

The work presented in this paper was realized in the frame of the SALWARE project number ANR-13-JS03-0003 supported by the French ”Agence Nationale de la Recherche”and by the French “Fondation de Recherche pour l’Aéronautique et l’Espace”.

References

[1] A. Rostami, F. Koushanfar, J. Rajendran, R. Karri, “Hardware Security: Threat Models and Metrics,” In Proceedings of the 32nd IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2013, pp. 819-823, November 2013.

[2] B. Colombier, L. Bossuet, "Survey of hardware protection of design data for integrated circuits and intellectual properties," Computers & Digital Techniques, IET, vol.8, no.6, pp.274,287, 2014.

[3] H. Ke, J.M. Carulli, Y. Makris, “Counterfeit electronics: A rising threat in the semiconductor manufacturing industry,” In Proceedings of the IEEE International Test Conference, ITC 2013, pp. 1-4, September 2013

[4] C. Gorman, “Counterfeit Chips on the Rise,” IEEE Spectrum, June 2012.

[5] AGMA, Alliance for Gray Markets and Counterfeit Adatement, http://www.agmaglobal.org

[6] M. Pecht, and S. Tiku, “Bogus! Electronic manufacturing and consumers confront a rising tide of counterfeit electronics,” IEEE Spectrum, May 2006.

[7] L. Bossuet, D. Hely, “SALWARE: Salutary Hardware to design Trusted IC,” In Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, TRUDEVICE 2013, Mai 2013.

[8] B. Legal, L. Bossuet, “Automatic low-cost IP watermarking technique based on output mark insertion,” Journal of Design Automation for Embedded System, Springer, vol. 16, no. 2, pp. 71-92, June 2012.

[9] C. Marchand, L. Bossuet, E. Jung, "IP watermark verification based on power consumption analysis," In Proceedings of the 27th IEEE International System-on-Chip Conference, SOCC 2014, pp. 330-335, 2014.

[10]

[11] Myth, Fact or Busted? A Security Evaluation of Physically Unclonalble Functions Cast in Silicon," In Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012, Spinger, Lecture Note on Computer Science, vol. 7428, pp. 283-301, September 2012.

[12] L. Bossuet, P. Bayon, V. Fischer, "Contactless transmission of intellectual property data to protect FPGAs designs", In Proceedings of the IFIP/IEEE International Conference on Very Large Scale Integration, VLSI-SOC 2015, pp. 19-24, 2015

[13] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," Computer, IEEE, vol.43, no.10, pp. 39-46, October 2010.

[14] M. Tehranipoor, and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," Design & Test of Computers, IEEE, vol.27, no.1, pp. 10-25, January-February 2010.

[15] S. Narasimhan, S. Bhunia, and R. S. Chakraborty, "Hardware IP Protection During Evaluation Using Embedded Sequential Trojan," Design & Test of Computers, IEEE , vol.29, no.3, pp.70-79, June 2012.

[16] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", in Wiener M. (Ed.), Proceedings of the 19th Annual International Cryptology Conference, CRYPTO 1999, Springer, Lecture Note on Computer Science, vol. 1666, pp. 388-397, August 1999.

[17] N. Kamoun, L. Bossuet, A. Gazel, "Experimental Implementation of 2ODPA attacks on AES design with flash-based FPGA Technology," in proceedings of the 22nd IEEE International Conference on Microelectronics, IMC 2010, pp. 407-410, 2010.

[18] C. Marsh, T. Kean, D. Mclaren, "Protecting designs with a passive thermal tag," In Proceedings of the 15th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2008, pp.218-221, September 2008.

[19] D. Ziener, J. Teich, "Power Signature Watermarking of IP Cores for FPGAs," Journal of Signal Processing Systems, Springer, vol. 51, pp. 123-136, 2008.

[20] G. T. Becker, M. Kasper, A. Moradi and C. Paar, "Side-channel based watermarks for integrated circuits," In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2010, pp. 30-35, June 2010.

[21] S. Kerckhof, F. Durvaux, F.X. Standaert, and B. Gérard, "Intellectual Property Protection for FPGA Designs with Soft Physical Hash Functions: First Experimental Results," In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, pp. 7-12, June 2013.

[22] L. Bossuet, M. Grand, L. Gaspar, V. Fischer, G. Gogniat, "Architectures of flexible symmetric key crypto engines – a survey: from hardware coprocessor to multi-crypto-processor system on chip", ACM Computing Surveys, Vol. 45, No. 4, Article 41, 32 pages, Aout 2013.

[23] L. Lin, M. Kasper, T. Güneysu, C. Paar, W. Burleson, "Trojan Side-Channels: Lightweight hardware Trojans through Side-Channel Engineering", In Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, CHES 2009, Springer, Lecture Notes in Computer Science, vol. 5747, pp. 382-395, September 2009.

[24] S. Kutzner, A. Poschmann, and M. Stöttinger, "TROJANUS: An Ultra-Lightweight Side-Channel Leakage Generator for FPGAs", In Proceedings of International Conference on Field-Programmable Technology, ICFPT 2013, pp. 160-167, December 2013.

[25] L. Gaspar, V. Fischer, F. Bernard, L. Bossuet, P. Cotret, "HCrypt: A Novel Reconfigurable Crypto-processor with Secured Key Management", In the Proceedings of the International Conference on ReConFigurable Computing and FPGAs, ReConFig 2010, pp. 280-285, 2010.

[26] J.F. Gallais, J. Großschädl, N. Hanley, M. Kasper, M. Medwed, F. Regazzoni, J.M. Schmidt, S. Tillich, and M. Wójcik, "Hardware Trojans for Inducing or Amplifying Side-Channel Leakage of Cryptographic Software," In Proceedings of the Second International Conference on Trusted Systems, INTRUST 2010, pp. 253-270, December 2010.

[27] D. Du, S. Narasimhan, R. S. Chakraborty, and S. Bhunia, "Self-referencing: A Scalable Side-Channel Approach for Hardware Trojan Detection," In Proceedings of Workshop on Crypto-

graphic Hardware and Embedded Systems, CHES 2010, Springer, Lecture Notes in Computer Science, vol. 6225, pp. 173-187, August 2010.

[28] S. Narasimhan, D. Dongdong, R.S. Chakraborty, S. Paul, F.G. Wolff, C.A. Papachristou, K. Roy, and S. Bhunia, "Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis," IEEE Transactions on Computers, vol.62, no.11, pp. 2183-2195, November 2013.

[29] R. Rad, J. Plusquellic, and M. Tehranipoor, "A Sensitivity Analysis of Power Signal Methods for Detecting Hardware Trojans Under Real Process and Environmental Conditions," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol.18, no.12, pp. 1735-1744, December 2010.

[30] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson and P. Maurine, "Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator", in Proceedings on International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012, Springer, Lecture Notes in Computer Science, vol. 7275, pp. 151-166, May 2012.

[31] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, "EM leakage analysis on True Random Number Generator: Frequency and localization retrieval method", in Proceedings of the Asia Pacific International Symposium and Exhibition on Electromagnetic Compatibility, APEMC 2013, May 2013.

[32] Virtual Silicon Inc. 0.18 µm VIP Standard Cell Library Tape Out Ready, Part Number: UMCL18G212T3, Process: UMC Logic 0.18 µm Generic II Technology: 0.18µm, 2004.

[33] R. Torrance, and D. James, "The state-of-the-art in semiconductor reverse engineering," In Proceedings of the 48th Design Automation Conference, DAC 2011, ACM/EDAC/IEEE , pp. 333-338, 2011

[34] P. Subramanyan, N. Tsiskaridze, W. Li, A. Gascon, W. Tan, A. Tiwari, N. Shankar, S. Seshia, and S. Malik, "Reverse Engineering Digital Circuits Using Structural and Functional Analyses," in IEEE Transactions on Emerging Topics in Computing, 2013.

[35] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B Sunar, "Trojan Detection using IC Fingerprinting" in Proceedings of the IEEE Symposium on Security and Privacy, pp. 296-310, 2007.

[36] Y. Jin, and Y. Makris, "Hardware Trojan Detection using Path Delay Fingerprint" in IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2008, pp. 51-57, 2008.

[37] Tektronix, RSA5000 Series, Spectrum Analyzers Datasheet, 2015.
Available online: http://www.tek.com/sites/tek.com/files/media/media/resources/RSA5000-Series-Spectrum-Analyzers-Datasheet-37W2627414_1.pdf

[38] M. Kasper, A. Moradi, G.T. Becker, O. Mischke, T. Güneysu, C. Paar and W. Burleson, "Side Channels as Building Blocks", In Journal of Cryptography Engineering, Springer, vol. 2, no. 3, pp. 143-159, 2012.

[39] M. Tehranipoor, U. Guin, D. Forte. Counterfeit Integrated Circuits - Detection and Avoidance. Springer, 2015.

[40] L. Bossuet, X. T. Ngo, Z. Cherif, V. Fischer. A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. IEEE Transactions on Emerging Topics in Computing, Vol. 2, Issue 1, pp. 30-36, 2014.

[41] N. Kamoun, L. Bossuet, and A. Ghazel, "Correlated Power Noise Generator as a Low Cost DPA Countermeasure to Secure Hardware AES Cipher," In Proceedings of the International Conference on Signals, Circuits and Systems, SCS 2009, pp. 1-6, 2009.