An ultra-lightweight transmitter for contactless rapid identification of embedded IP in FPGA

Lilian Bossuet, Pierre Bayon, Viktor Fischer

An ultra-lightweight transmitter for contactless rapid identification of embedded IP in FPGA

L. Bossuet, *Senior Member, IEEE*, P. Bayon, V. Fischer

***Abstract*— This letter presents the first ultra-lightweight transmitter based on electromagnetic emanation to send embedded intellectual properties (IP) identity (ID) quickly and discreetly. The proposed solution is based on a binary frequency shift keying (BFSK) transmitter that ensures an exceptionally high data rate. In addition, we present a coherent demodulation method using slippery window spectral analysis to recover data outside the device. The hardware resources occupied by the transmitter represent less than 0.022% of a 130 nm Microsemi Fusion FPGA. The experimental bitrate of the data transmission is around 500 times higher than the bitrate available for other state of the art spy circuitry using power consumption. In comparison with other works, our proposal goes clearly towards using a spy circuit in an industrial context for IP protection.**

***Index Terms*—IP protection, side channel, electromagnetic emanation analysis.**

I. Introduction

FOR digital circuit design the re-use of embedded intellectual properties (IP) is more and more important due to prohibitive cost of ASIC design. Nevertheless the IP business suffers from a lack a security due to the intrinsic form of IPs sales and exchanges. Many dedicated threats target the IP life cycle and result to revenues losses for the IP designers [1]. 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: software IPs (typically hardware description language files), firmware IPs (*synthesized* netlist), and hardware IPs (FPGA bitstream or physical layout).

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 [2]. 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 letter 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 [1]) 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.

The rest of this letter is organized as follows. In Section 2, we present related works. In Section 3, we detail the proposed electromagnetic communication of data (i.e. IC/IP information). In Section 4, we present a method to analyze the electromagnetic spectrum to BFSK signal demodulation and in Section 5 we present our conclusions.

II. Related Work

Well-known threat in cryptographic engineering is side channel attacks [3]. 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. These side channels can be used as transmission channels to send intellectual property data from a device or an embedded IP. For example in [4], 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 [5], 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 [6] to communicate the IP identity. To reinforce such work, the authors of [7] propose using the power supply signal of an IP as a physical hash function for fingerprinting.

Related works can be found also in the malicious hardware field such as hardware Trojans design. Such systems use side channels to forward secret information such as a symmetric cipher key from cryptographic hardware implementation [8], [9], but also to cause or to amplify side-channel leakage of cryptographic hardware [10].

Except [4], 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

Manuscript submitted June 3, 2015. The work presented in this biref 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".

L. Bossuet and V. Fischer are with the Laboratoire Hubert Curien, University of Lyon, Saint-Etienne, 42000, France (e-mail: lilian.bossuet@univ-st-etienne.fr, fischer@univ-st-etienne.fr).

P. Bayon is with Brightsight, Delft, 2628, The Netherlans. (e-mail: bayon@brightsight.com).

and rapid as this letter will show.

III. Proposed EM communication of deep data

Electromagnetic radiation is an efficient side channel 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 [11]. For all these reasons, 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 Figure 1. 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 Figure 1. When input data is low, the configurable ring oscillator uses N delays and its oscillation frequency is f_0. When input data is high, the configurable 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

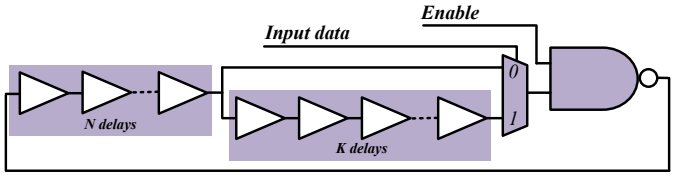

Fig. 1. Architecture of the ultra-lightweight digital BFSK transmitter based on a configurable ring oscillator.

used to acquire and measure the transmitted signal. The bandwidth of our test bench, which is presented in [11], was limited to 100 MHz and 1 GHz by the low-noise amplifier.

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 configurable 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. Fig. 2 shows the configurable ring oscillator frequencies evolution with N ranging from 0 to 4, and K ranging from 1 to 5. According to Fig. 2, 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 ($N=0$, $K=1$).

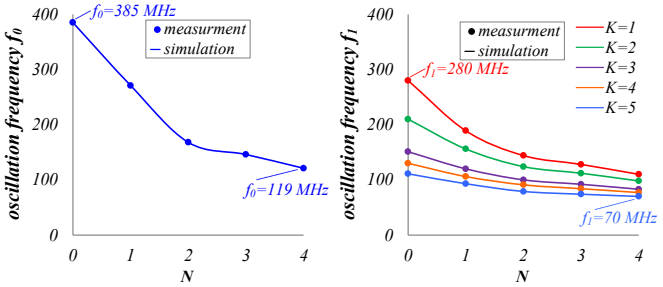

Fig. 2. Evolution of the configurable ring oscillator frequencies (f_0 and f_1) with N ranging from 0 to 4, and K ranging from 1 to 5.

The number of FUSION 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. For XILINX and ALTERA SRAM FPGAs the BFSK consumes from 2 4-input- LUT ($N=0$, $K=1$) to 10 4-input- LUT ($N=4$, $K=5$). To evaluate its size in ASIC implementations, the gate count is estimated using the Virtual Silicon standard cell library based on the UMC L180 0.18 µm 1P6M Logic process (UMCL18G212T3 [12]). The delay gate count is estimated by the gate count of a standard NOT gate, 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 [12].

The small requirement of logical resources of the proposed spy circuitry makes reverse engineering it harder, although not impossible [13]. Even with recent CMOS technologies, the attacker can reverse engineer ICs using a scanning electron

microscope and an automatic tool for circuitry extraction [13], [14]. 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 [15], [16] 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).

IV. Experimental Results

The electromagnetic radiation of the device was evaluated using the near-field electromagnetic analysis test bench described in [11] with a spectral range 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.

Fig. 3 illustrates the spectral analysis of the BFSK transmitter's electromagnetic emission when $N = 1$ and $K = 1$, which corresponds to a small transmitter with high frequencies (f_1=*189.2 MHz* and f_0=*272.2 MHz*). For the spectral analysis, a 16 384 points FFT was computed. This figure presents a zoom (X and Y axis) on the global spectrum of the local EM emanation of the circuit when the BFSK transmitter sends a '1' (*in red*) and when the BFSK transmitter sends a '0' (*in blue*).

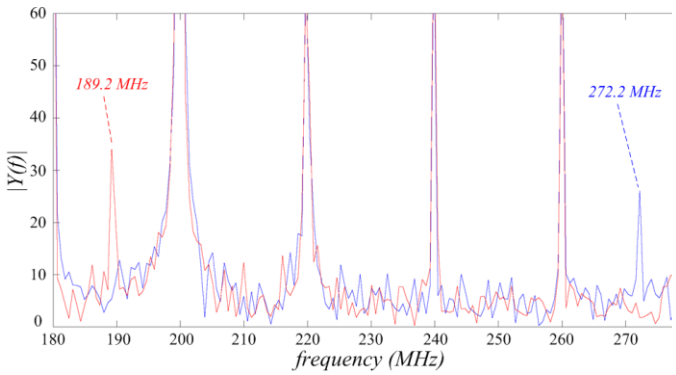

Fig. 3. Parts (zoom in x-axis and y-axis) of the electromagnetic emanation spectral analysis of the proposed BFSK transmitter when it sends a high level at f_1=189.2MHz (in red) and when it sends a low level at f_0=272.2 MHz (in blue).

Notice also that we placed a small antenna in the close vicinity of the ring. The amplitude of the spectral rays at 180, 200, 220, 240, 260, 280 MHz are very high compared to the two spectral rays at 189.2 MHz and 272.2 MHz. However, we have cut the upper part of the spectrum in order to see the two interesting rays (at 189.2 MHz and 272.2 MHz). These frequencies correspond to the spectral contribution of the BFSK frequencies f_0 and f_1.

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 in Fig. 3 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 according to [11].

The spectral contribution of the two BFSK frequencies during transmission (which is limited by the transmitter enable signal) at the low-noise amplifier output is measured to determine the transmitted bit sequence. In order to apply the demodulation technique described here, called coherent demodulation, theoretically the bitstream rate (bitrate) is limited to 0.5 times the frequency difference between f_0 and f_1. In the case shown in Fig. 3, theoretically the maximum bitrate is 41.5 Mbps (theoretically limited to 53 Mbps when $N = 0$ and $K = 1$). The bitrate of best IP identification methods using power consortium in the literature is always less than 1 Kbps even with recent device (i.e. XILINX Virtex V) [6-9].

For the coherent demodulation of the electromagnetic radiation, we propose a slippery window spectral analysis. Indeed, overall spectral analysis masks the effects of the nonstationarity 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: "1011110111011100". The clock frequency of the shift register is 500 kHz. 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. Fig. 4 gives the result of the coherent demodulation obtained at a 500 Kbps bit rate (500 times more than [6-9]), which served as a proof of concept.

V. Conclusion

In this letter, we have presented an ultra-lightweight transmitter of IP identity using the electromagnetic side channel for FPGA implantation. Based on a configurable ring oscillator, our solution exploits a BFSK signal to transmit information by way of the electromagnetic channel. By performing a slippery window spectral analysis of the near

field electromagnetic emanations captured locally over the BFSK transmitter circuitry, the proposed transmission achieves a high bitrate (theoretically limited to 53 Mbps with a Microsemi Fusion FPGA), which has not been achieved before. Moreover, the transmitter occupies very small area.

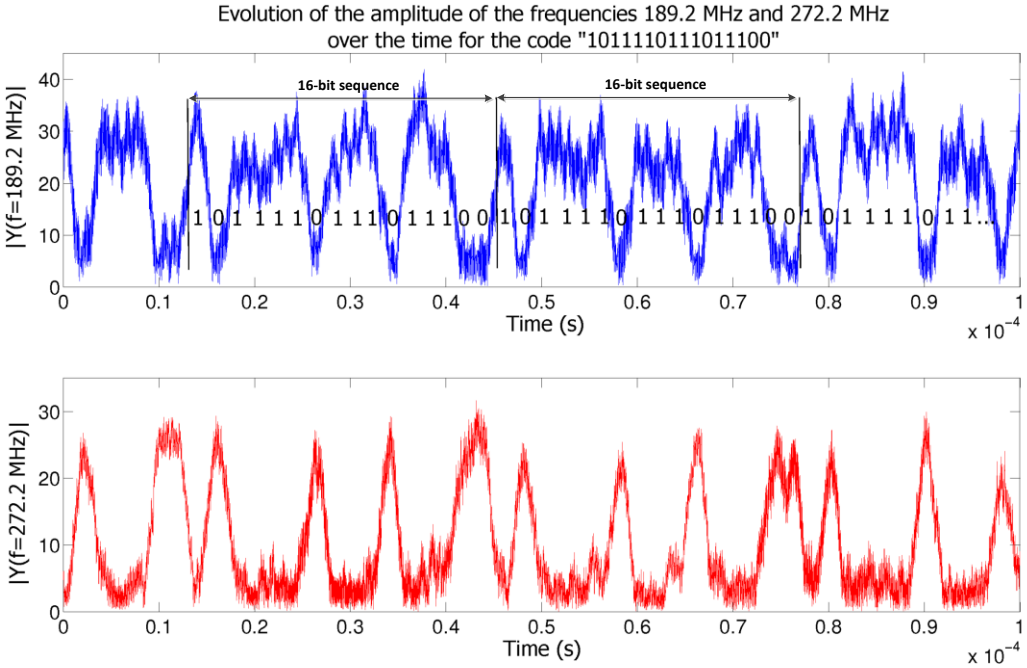

Fig. 4 Coherent demodulation of the 16-bit code word "1011110111011100" cyclically sent by the BFSK transmitter at 500 Kbps. The top (bottom) graph in blue (red) corresponds to the evolution over the time of the amplitude of the spectral contribution at f_1=189.2 MHz (at f_0=272.2 MHz).

For the highest frequency and data rate, our solution requires 4.67 equivalent gates, which it is less than the requirement of a small D-flip-flop. Such a small area makes reverse engineering of the chip very difficult and detection of the transmitter using standard Trojan detection methods is not realistic.

ACKNOWLEDGMENT

The work presented in this letter 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] 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.

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

[3] 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, 1999.

[4] 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, 2008.

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

[6] 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, 2010.

[7] 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, 2013.

[8] 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, 2009.

[9] 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, 2013.

[10] 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, 2010.

[11] 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, 2013.

[12] 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.

[13] 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

[14] 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.

[15] 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.

[16] 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.