SECURITY SYSTEM FOR DETECTING TAMPERING AND THERMAL SIDE CHANNEL ATTACKS

Daniel Ciprian VASILE[1], Paul SVASTA[2]

Security circuits are the most important elements of devices and equipment intended for secure communication and data protection. They implement cryptographic functions and protocols that are resistant to cryptanalytic attacks. Nowadays technologies allow attacking the integrated circuits used in security circuits, based on physical intrusions and thermal stress applied to the semiconductor devices.

This paper proposes a system to protect the security circuits from physical intrusions and thermal attacks. It is composed of an active tamper detection circuit and a special conductive mesh with three conductive layers. It entirely covers the security circuit and the active tamper detection circuit.

Keywords: security, tamper, mesh, detection

1. Introduction

Security circuits are protected from physical intrusions (tampering) and other kind of attacks with specialized electronic circuits that are permanently active, no matter if the equipment is powered or not from the mains supply. Security circuits (SC) use cryptographic functions and secret data in order to protect communications and data storage. Therefore, in case of tampering, the secret data must be quickly erased in order not to be revealed to the attackers.

The most efficient method to protect SC is to cover it with a special conductive mesh that is probed with signals by the tamper detection circuit. This circuit is situated near the SC, on the same PCB (Printed Circuit Board), and is also covered by the conductive mesh.

Tamper detection circuits protect SC from multiple attacks and they can be divided in two categories: passive and active. The passive tamper detection circuits use to inject small continuous currents into the conductive mesh and detect the coarse variation of them. Because there are implied high resistive values in the detection circuit, this method is sensitive to noise or high delays in taking proper actions. The active tamper detection circuits are more sensitive and respond quicker to attacks. These types of circuits probe with signals the

[1] PhD student, University POLITEHNICA of Bucharest, CETTI, Romania, e-mail: ciprian.vasile@cetti.ro
[2] Prof., University POLITEHNICA of Bucharest, CETTI, Romania, e-mail: paul.svasta@cetti.ro

conductive mesh and analyze its response in order to detect physical intrusions. The principle schematic of an active tamper detection circuit is presented in figure 1 [1].

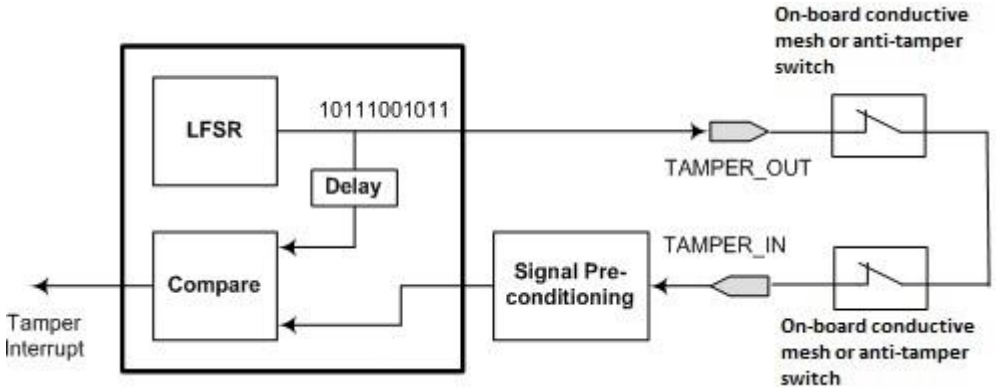

Fig. 1 Principle schematic of an active tamper detection circuit.

Generally, the probing signals are short duration pulses with variable parameters (period, duration, shape etc.) in order not to facilitate their reproduction in case of *bypass* attack (deactivation of an area of the conductive mesh and fake injection of pulses). A common method used to make pulses parameters not predictable is implementing pseudo-random generators. These generators are complex constructions based on LFSR (*Linear Feedback Shift Register*), NFSR (*Non-linear Shift Register*) or injective dispersion functions like HASH and encryption algorithms. Regarding the schematic presented in figure 1, the LFSR generator provides pulses at different periods of time. These pulses propagate through the conductive mesh (and, eventually, a few switches actuated by the equipment's access door) and, at the output port, the signals are formed (pre-conditioned) again into pulses. The delayed injected pulses and the recovered pulses are compared in a convolution function to detect any unexpected delay. If it detects an intrusion, the active tamper detection circuit can quickly erase secret data stored in non-volatile memories and notify the security processor through an interrupt (usually NMI – *non-maskable interrupt*). The notification has the role to force the security processor to erase the internal RAM (*Random Access Memory*), including all registers used in cryptographic functions, and to stop it.

This paper presents a system designed for protection of SC that innovates both aspects of it:

- the conductive mesh (CM) is formed of three conductive layers, isolated by dielectric layers;
- the active tamper detection circuit (ATDC) analyzes the probing radio pulses from the perspective of frequency response.

ATDC and CM are able to detect intrusions (interruptions of traces and short-circuit between side traces) and temperature variations at the CM level.

2. The conductive mesh

The conductive mesh is a structure formed of three layers with conductive traces separated by dielectric layers. This structure can be fabricated with a rigid PCB or with a flexible foil. They entirely wrap the CES and ATDC, with no visible gaps, in order to protect against physical intrusions.

Each layer of the CM has the following function:

- The first layer (1), the nearest one to the protected circuits (CES and ATDC), is a full conductive surface connected to the ground signal.
- The second layer (2), the one in the middle, contains thin traces with the shape like meanders. It provides an input port, where ATDC inject probing signals, and an output port where ATDC analyzes the response of the CM.
- The third layer (3), the outermost one, contains zones with conductive traces that form closed circuits. The shape of these traces is identical to the shape of the traces on layer 2 and they are exactly superposed.

In figure 2 is presented the principle of CM as was developed in the following papers [2], [3], [4], [5], [6]. This picture presents two zones of the CM, containing the three layers: layer 1 – ground plane, layer 2 (blue trace) is a continuous trace with input and output ports, layer 3 (red traces) contains two short-circuited traces corresponding to the two zones.

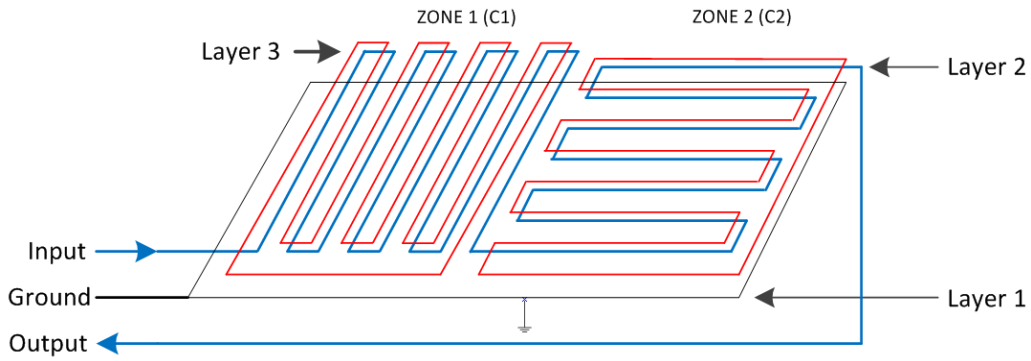

Fig. 2 Principle of the three layers conductive mesh.

The test CM used in this paper is formed of two square zones with each side of 30 mm. Traces have a transversal thickness of 0.2mm and a spacing between them of 0.2mm. In order to test different types of CM, there were used the following constructive types:

- PES (Poly Ether Sulfone) foil, with a thickness of 0.1mm, printed with conductive paste (SW180 from Tatsuta);
- PCB (FR4) with a dielectric thickness of 0.3mm;
- PCB (FR4) with a dielectric thickness of 0.6mm.

3. The structure of the active tamper detection circuit

The processing element of the ATDC is the STM32L432KC [7] microcontroller, as presented in figure 3. The NUCLEO-L432KC development board was used for this experimental study, which contains this microcontroller. STM32L432KC is a 32 bits ARM processor, running at maximum 80MHz that integrates specialized peripherals, like: GPIO (General Purposes Input Output) ports, communications ports (I2C, UART, SPI, USB etc.), ADC (Analog to Digital Converter), DAC (Digital to Analog Converter) etc. In this application, the I2C port and the ADC were used. In order to extract the data presented in this study, the UART port was used (through the virtual COM port provided by the STLINK programming interface of the NUCLEO board).

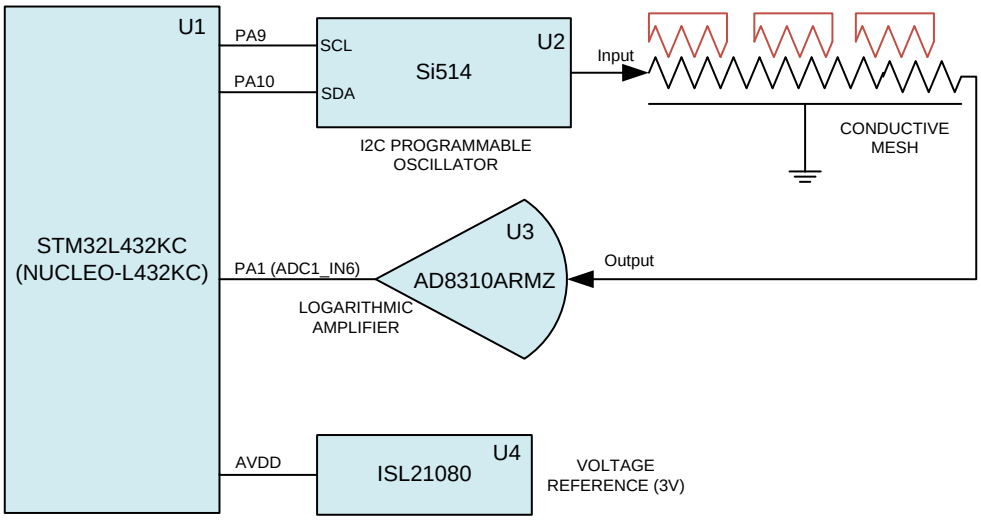

Fig. 3 Schematic of the active tamper detection circuit based on STM32L432KC microcontroller.

CM is probed with sinusoidal pulses at different frequencies. These pulses are similar to the radio pulses used in radiolocation stations. They are generated by the Si514 [8] programmable oscillator, controlled by the STM32L432KC through the I2C port (pins PA9 and PA10), which programs the frequency of every train of pulses. Si514 can provide pulses with frequencies between 100 kHz and 212,5MHz. Because of the integrative effect of the CM, the signals at the output of the CM lose some of the high frequency components, resulting in more sinusoidal like signals, as presented in Fig. 4.

Signals at the output of the CM are detected by the AD8310 [9] logarithmic amplifier. This integrated circuit meets two functions: amplifies the input signal and detects the amplified signal applying a logarithmic function.

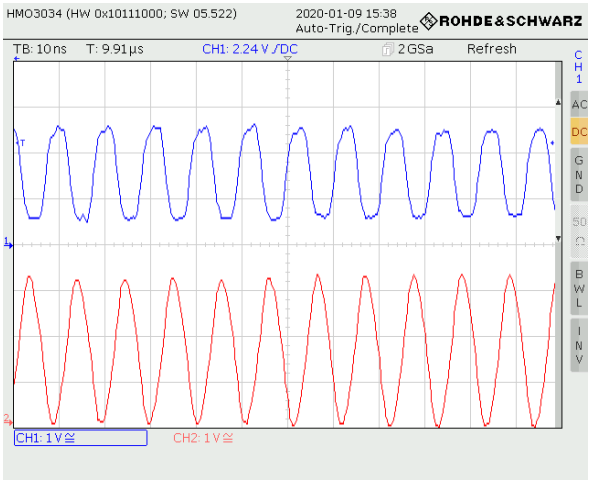

Fig. 4 100MHz signal used to probe the conductive mesh: CH1 (channel 1) – input signal, CH2 (channel 2) – output signal (acquisition made with the HMO3034 oscilloscope).

The dynamic range characteristic of AD8310 is 95 dB. This large range is very important given that the signals have a large variation of the amplitude across the analyzed spectrum. The output of the AD8310 amplifier is connected to the ADC1_IN6 input of the ADC1 converter, pin PA1. The conversion resolution of this ADC is 12 bits and can be configured to sample with a maximum frequency of 5MHz.

In order to optimize the conversion range of ADC1, it was used the ISL21080 [10] voltage reference (3V). The range of the signal at the output of the logarithmic amplifier is 0.4V÷2.6V.

The experimental ATDC used in this paper is composed of two circuits: the NUCLEO-L432KC development board and the CM interface board, containing the Si514, AD8310 and ISL21080 integrated circuits. NUCLEO-L432KC is connected to the interface board through the CN3 and CN4 connectors, as presented in Fig. 5.

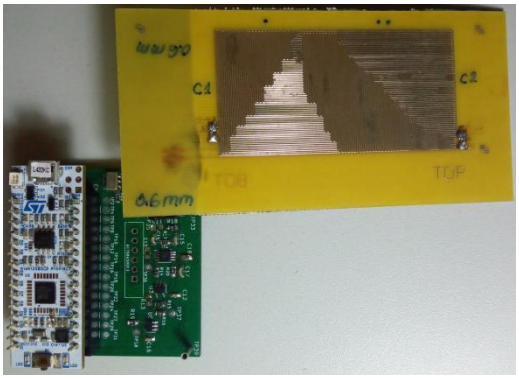

Fig. 5 The experimental ATDC connected to the 0.6mm PCB conductive mesh.

4. Tamper detection procedure

The experimental assessment of this anti-tamper system (ATDC and CM) considered two important features for SC protection: detection of physical intrusions and detection of temperature variations. CM is evaluated at discrete frequencies to detect small differences as against the reference values. These latter values are recorded in the fabrication process of the system without tampering. In order to obtain an optimal resolution of intrusions detection, 32 frequencies were used, spaced at 5MHz. The starting frequency was chosen 50MHz, so that the maximum frequency of the domain was 205MHz. The program in the STM32L432KC microcontroller sets a new frequency in the Si514 oscillator every 250ms. After a 20ms period for internal stabilization of the generated signal, Si514 activates its output for 300µs. This duration is required by the ADC1 to perform the conversion. Fig. 6 shows the generated pulse of Si514 (at the output of CM), together with the pulse resulted at the output of the AD8310 amplifier.

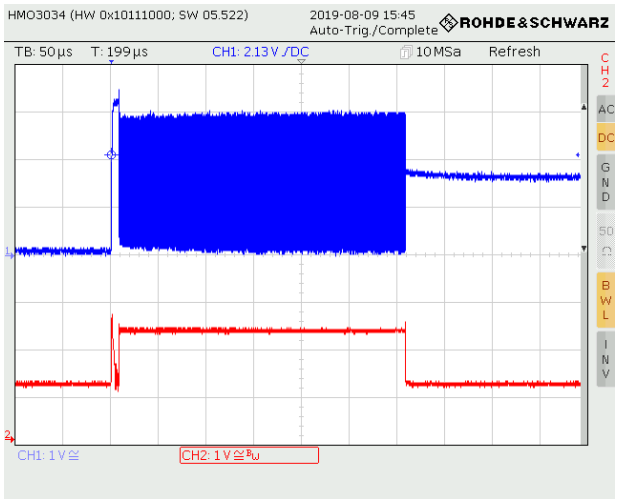

Fig. 6 Detection of probing pulses: CH1 (channel 1) - the signal at the output of the conductive mesh, CH2 (channel 2) - the detected signal at the output of the logarithmic amplifier (acquisition made with the HMO3034 oscilloscope).

After each conversion, the microcontroller compares the acquired value with the reference value in order to detect an intrusion. In case of tampering, ATDC takes proper actions to protect the security data (usually it erases the security data).

5. Experimental results

5.1. Detection of physical intrusions

ATDC assessment, along with the triple layer CM, was performed in real conditions of producing the physical intrusions: opening the conductive traces and producing a short-circuit between two adjacent traces of the layer 3. Considering the notations used in Fig. 2, the following cases were assessed:

- CM not tampered, noted as NT;
- C1 opened, noted as TC1_O;
- short-circuit between two traces on C1, noted as TC1_S;
- C2 opened, noted as TC2_O;
- Short-circuit between two traces on C2, noted as TC2_S.

The three types of CM were analyzed and the graphical results are presented in Figs. 7, 8 and 9, corresponding to the 0.1mm PES foil, 0.3mm PCB and, respectively, 0.6mm PCB. The acquired data values were analyzed by the STM32L432KC microcontroller and transmitted to the PC through the serial UART port.

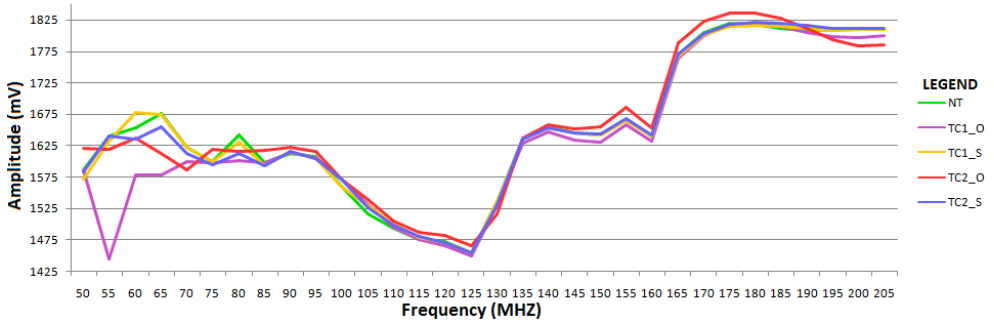

Fig. 7 The output characteristic of the 0.1mm PES conductive mesh for physical intrusions.

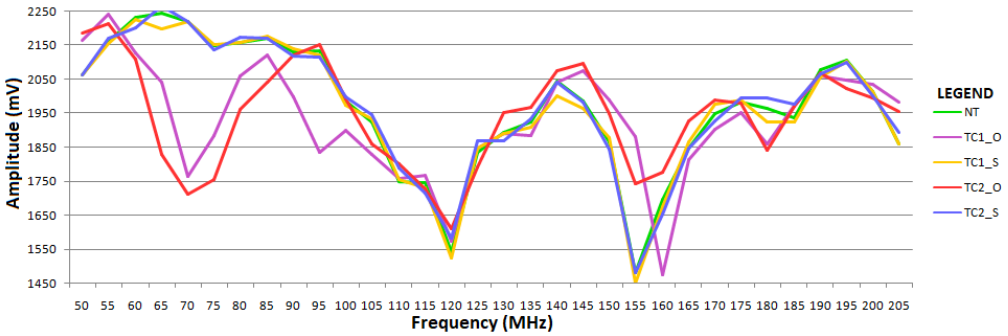

Fig. 8 The output characteristic of the 0.3mm PCB conductive mesh for physical intrusions.

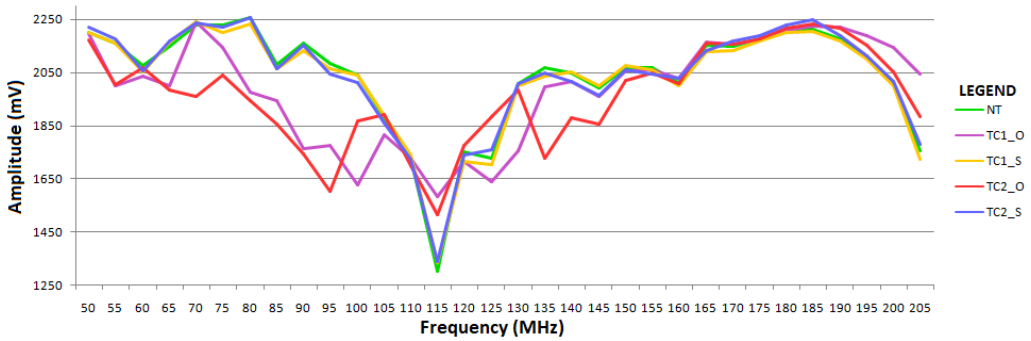

Fig. 9 The output characteristic of the 0.6mm PCB conductive mesh for physical intrusions.

As presented in Figs. 7, 8 and 9, the detection of open circuit intrusions on layer 3 is possible in the whole range of used frequencies. The PES foil shows smaller differences from reference values (green traces) than the other two CMs. Even if the differences are small, these values are easy to measure with the ADCs inside the common microcontrollers.

As regards the detection of short-circuits between traces, each CM shows many frequency sub-domains in which this function can be achieved.

In practical implementations, the frequency sub-domains are selected for analysis in order to provide the optimal results. If a specific sub-domain is proper for detection of tampering attacks, the frequency steps can be adjusted.

5.2. Detection of temperature variations

One of the most used scenarios to attack the normal functioning of logic integrated circuits is to vary of temperature outside the operational limits. This attack is part of the side channel attacks (SCA). It is known that the memory cells and the logic units can produce errors when they are subject of extreme temperatures [11]. Maintaining a high temperature for a long period of time may modify the commutation levels of the logic circuits, thus increasing the predictability of the computed data. Also, if the RAM cells are kept at low temperatures, below -40°C, then they will have a data remanence [12]. If the temperature further lowers from this value, then the data can be read with specialized equipment.

The proposed triple layer CM and ATDC together can detect temperature variations, including exceeding operational limit, and take the necessary actions to protect the security data. The system was tested for temperatures between -20°C and 80°C. All components of the system are operational in this range.

Every type of CM was tested in the ESPEC SH-241 thermal chamber. Temperature values were read from the internal sensor of the STM32L432KC microcontroller. These values, along with the acquired signal made with ADC1,

were transferred to the PC through the serial port. The results for the above-mentioned CM are presented in Figs. 10, 11 and 12.

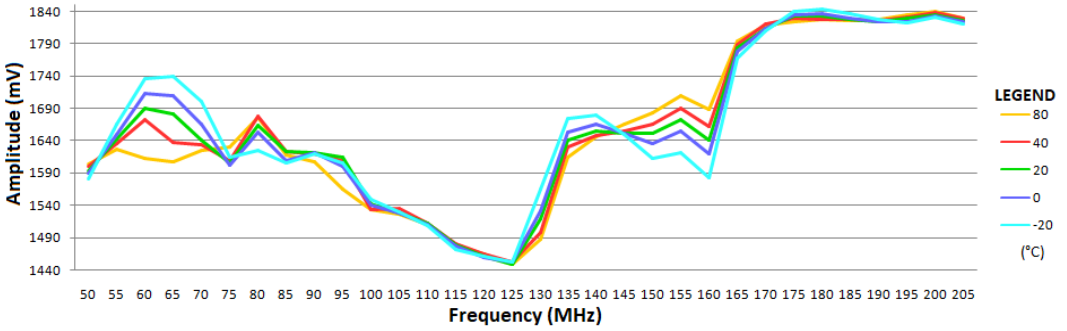

Fig. 10 The output characteristic of the 0.1mm PES conductive mesh for temperature variations.

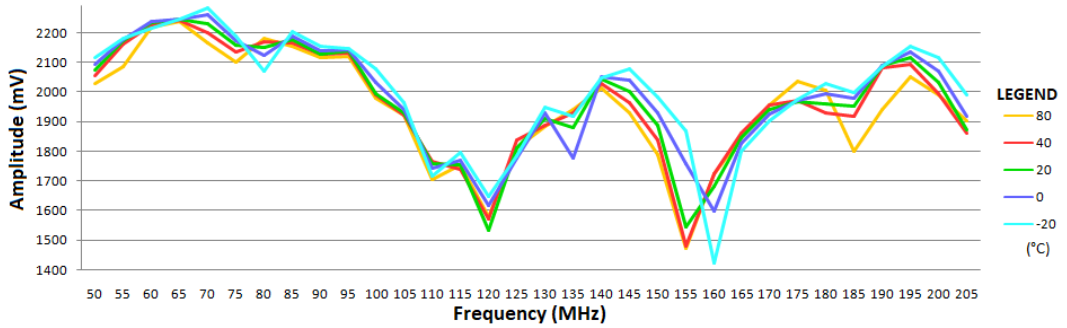

Fig. 11 The output characteristic of the 0.3mm PCB conductive mesh for temperature variations.

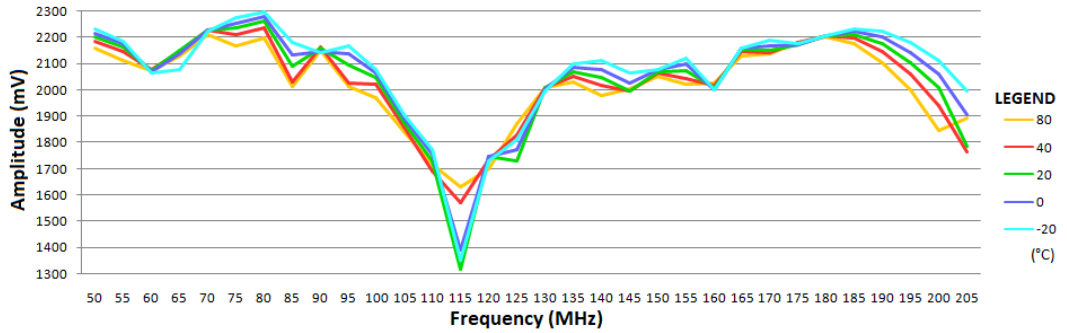

Fig. 12 The output characteristic of the 0.6mm PCB conductive mesh for temperature variations.

Figs. 10, 11 and 12 contain five traces: three traces (0°C, 20°C and 40°C) for the operational domain (most common to all electronic devices) and two traces (-20°C and 80°C) for tampering limits. These values divide the temperature in three domains of interest: operational 0°C÷40°C, tampering < -20°C and > 80°C, alert -20°C÷0°C and 40°C÷80°C. In the alert domain, ATDC may notify the

equipment, in which it is installed, that a temperature alarm is active. If the temperature exceeds the tampering limits then ATDC take proper actions to protect the security data.

Analyzing each of the Figs. 10, 11 and 12, there can be observed that operational traces are guarded by the tampering traces (-20°C and 80°C). Also, there are many frequency domains that can be used to detect thermal side channel attacks. Examples of such domains are:

- 55MHz÷70MHz, 130MHz÷145MHz and 145MHz÷165MHz for PES foil, printed with conductive paste;
- 65MHz÷80MHz, 140MHz÷165MHz and 180MHz÷200MHz for 0.3mm PCB;
- 50MHz÷60MHz, 70MHz÷100MHz, 135MHz÷145MHz and 190MHz÷205MHz for 0.6mm PCB.

For an efficient operation of ATDC, it should simultaneously detect both types of attacks: physical and thermal. ATDC must not trigger false physical intrusions while the temperature doesn't exceed the thermal tampering limits (-20°C and 80°C). On the other side, ATDC must detect physical intrusions while the temperature is inside this domain. In order to prove the ATDC efficiency, there were computed the differences between the physical intrusions' values and the values for thermal tampering. The resulted values are presented in Figs. 13, 14 and 15. If the physical intrusions values are guarded by the thermal tampering values, the printed value is 0. At these frequencies ATDC cannot detect physical intrusions because the values are positioned inside the range of thermal variations.

The differences are printed in columns, for each frequency, and the colored segments in these columns represent the differences corresponding to each type of physical intrusion, previously presented.

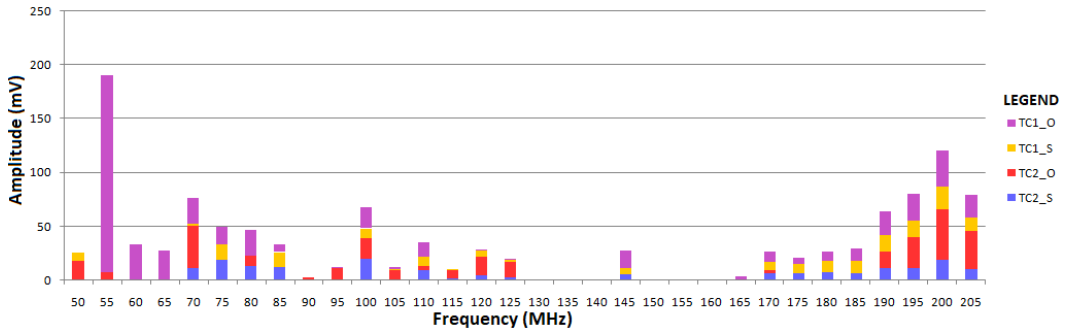

Fig. 13 Detection domains for 0.1mm PES conductive mesh.

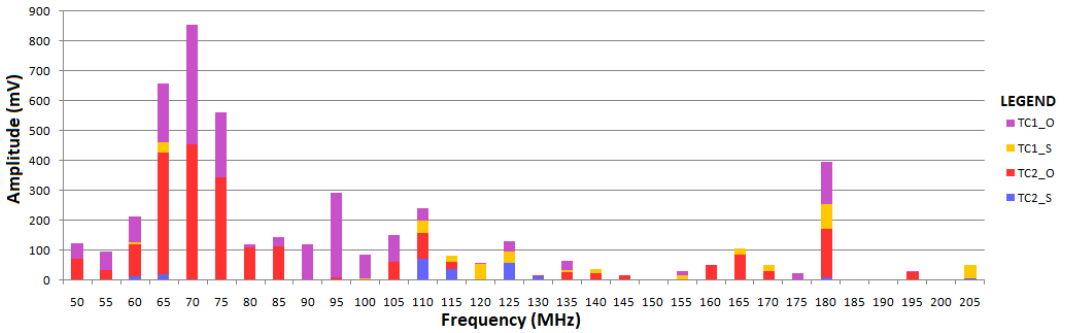

Fig. 14 Detection domains for 0.3mm PCB conductive mesh.

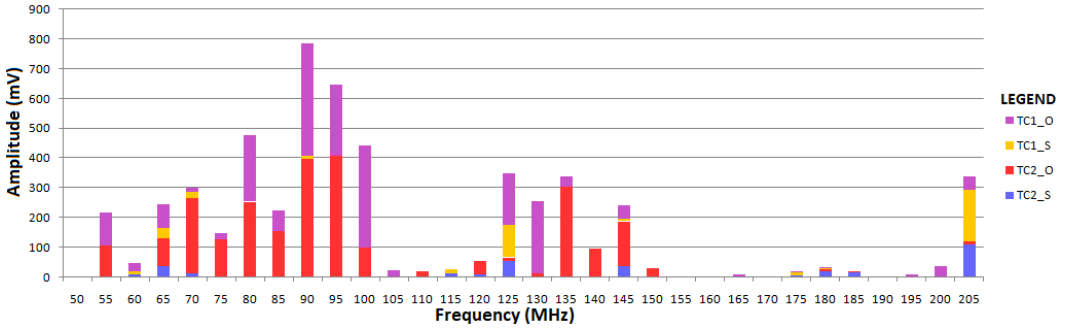

Fig. 15 Detection domains for 0.6mm PCB conductive mesh.

Analyzing Figs. 13, 14 and 15 there can be observed a few frequencies at which detection is noted with 0, meaning that ATDC, along with CM, cannot detect physical intrusions. In the rest of the frequencies, approximately 80% of all frequencies, the system can detect all types of physical intrusions. In order to optimize the operation of ATDC, all frequencies in which it cannot detect physical intrusions are eliminated from probing.

6. Conclusions

The paper presents an improved tampering detection system that mitigates the two most important attacks over security circuits: physical intrusions and thermal attacks (which is part of side channel attacks).

The system uses a conductive mesh composed of three layers with special conductive traces, isolated by dielectric layers. Its design makes the physical intrusions impossible to achieve. Any interruption or short-circuit of the exposed conductive traces trigger the tampering event and quick actions are taken to protect the secret data.

The active tamper detection circuit, which analyzes the response of the conductive mesh, has a simple structure with a few specialized components

(microcontroller, programmable oscillator, logarithmic amplifier and voltage reference) but is very efficient in detecting tampering attempts.

An important feature of this system is that it detects temperature variations at the mesh level. Thermal attacks can be detected much faster than using temperature sensors at the PCB level.

This anti-tampering system is a very good solution for protecting the security circuits or the firmware inside the electronic devices.

Acknowledgements

This research was supported by the following projects:

- *A-Succes*, SMIS: 125125, financing contract 51675/09.07.2019, POCU/380/6/13;
- *iDev4.0*, "Integrated Development 4.0", nr. 783163, call id H2020-ECSEL-2017-1-IA-two-stage;
- *Dezvoltare Integrată 4.0*, SMIS 122386, Programul Operațional Competitivitate (POC).

R E F E R E N C E S

[1]. *M. Arora, R. Pandey, P. Sareen and P. Bhargava*, "Tamper detector for secure module", U.S. Patent No. 8,689,357. 1 Apr. 2014.

[2] *D. C. Vasile and P. Svasta*, "Innovative Conductive Mesh Structure for the Protection of Security Electronic Circuits", Electronics System Integration Technology Conference (ESTC), Dresden, Germany, 2018.

[3] *D. C. Vasile and P. Svasta*, "Antitamper Conductive Mesh Used for Securing Cryptographic Modules", 2018 IEEE 24th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Iaşi, România, 2018.

[4] *D. C. Vasile and P. Svasta*, "Innovative Authentication Method for IoT Devices", 22nd Microelectronics and Packaging Conference (EMPC), IEEE, Pisa, Italia, 2019.

[5] *D. C. Vasile and P. Svasta*, "Protecting the Secrets: Advanced Technique for Active Tamper Detection Systems", 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, ClujNapoca, România, 2019.

[6] *D. C. Vasile, P. Svasta, and M. Pantazică*, "Preventing the Temperature Side Channel Attacks on Security Circuits", 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, ClujNapoca, România, 2019.

[7] *ST Microelectronics*, "Ultra-low-power Arm® Cortex®M4 32bit MCU+FPU, 100DMIPS, up to 256KB Flash, 64KB SRAM, USB FS, audio", DS11451, http://www.st.com, 2018.

[8] *SILICON LABS*, "Si514, ANY FREQUENCY I2C PROGRAMMABLE XO (100 kHz TO 250 MHZ)", https://www.silabs.com, 2018.

[9] *ANALOG DEVICES*, "AD8310, Fast, VoltageOut, DC to 440 MHz, 95 dB Logarithmic Amplifier", https://www.analog.com, 2010.

[10] *RENESAS*, "ISL21080, 300nA NanoPower Voltage References", https://www.renesas.com.

[11] *M. Hutter and J. M. Schmidt*, "The temperature side channel and heating fault attacks", International Conference on Smart Card Research and Advanced Applications, Springer International Publishing, 2013.

[12] *N. A. Anagnostopoulos*, "Low temperature data remanence attacks against intrinsic sram pufs", Report 2016/769, Cryptology ePrint Archive.