UNIVERSITY „POLITEHNICA” OF BUCHAREST

ETTI-B DOCTORAL SCHOOL

Decision No. 515 from 01.07.2020

EXTENDED SUMMARY

SMART MODULES FOR SECURING THE ELECTRONIC EQUIPMENT AGAINST TAMPERING

PhD student: **Eng. Daniel-Ciprian Vasile**

DOCTORAL COMMITTEE

President	**Prof. Gheorghe Brezeanu, PhD Eng.**	from	**Univ. Politehnica București**
PhD supervisor	**Prof. Paul Svasta, PhD Eng.**	from	**Univ. Politehnica București**
Reviewer	**Prof. Adriana Vlad, PhD Eng.**	from	**Univ. Politehnica București**
Reviewer	**Prof. Alexandru Șerbănescu, PhD Eng.**	from	**Academia Tehnică Militară**
Reviewer	**Sci. Res. I Liviu Coșereanu, PhD Phys.**	from	**INCD Aerospațială ”Elie Carafoli”**

BUCHAREST 2020

Contents

List of figures

List of abbreviations

ADC - analog to digital converter
AI - artificial intelligence
ARM - family of processor architectures (Arm Limited)
ASIC - application specific integrated circuit
ATDC - active tamper detection circuit
DAC - digital to analog converter
e-PTFE - expanded-polytetrafluoroethylene
ESC - electronic security circuit
FLASH - non-volatile memory
FPGA - field programmable gate array
GPIO - general purpose input/output
HASH - dispersion function
HSM - harware security module
Internet - global system of interconnected computer networks
IoT - internet of things
IT - information technology
LDS - laser direct structuring
LFSR - linear feedback shift register
NFSR - non-linear feedback shift register
NVRAM - non-volatile RAM
PC - personal computer
PCB - printed circuit board
PES - poly ether sulfone
POS - point of sale
PWM - pulse width modulation
RAM - random access memory
RF - radio-frequency
SCA - side channel attacks
TDC - tamper detection circuit
UART - universal asynchronous receiver-transmitter

Chapter 1

Introduction

1.1 Presentation of the doctoral field

The current digital age is based on communications and data processing and is characterized by changes in an accelerated rate. Electronic equipment includes electronic circuits (*hardware*) and computer applications (*software, firmware*) that implement their functions. New technologies offer countless possibilities and areas for development, but their use can expose the user to risks. For valuable resources, such as information, *hardware*, *software* and *firmware*, assessing these risks can be difficult and depends on the environment in which these resources are located.

The security of information resources is part of the evolution of any organization and is represented by protecting the profit, ensuring the security of members or the values they hold. This profile can also be defined for structures and organizations at national or international levels. The costs involved in protecting information resources depend on each computer and communications system. To be an efficient system, security costs must not outweigh the benefits of using protected resources.

Electronic security circuits (ESCs) are the modules responsible for the security of information resources in electronic equipment. They contain both logic components (such as logic gates, processors, memories, FPGA and CPLD circuits etc.) and analog components (linear power supplies, noise sources, sensors etc.).

Security data is any information processed inside electronic equipment (data, functions, protocols, routines *software* and *firmware*) that the manufacturer wishes to protect against unauthorized access. This security data is processed inside ESC using dedicated integrated circuits that implement the computer application.

Cryptography provides the mathematical means necessary for the protection of information in digital format (security data). They consist of functions, protocols and principles that ESC implements.

1.2 The purpose of the thesis

The study included in this thesis aimed to find innovative and effective solutions to protect the ESCs against the most important intrusions, in terms of the effectiveness of cryptanalytic attack, namely physical intrusions and attacks by temperature variation. The solutions proposed in the thesis consist in designing a coating with sensory characteristics to protect the ESC, made of a conductive network, and an electronic circuit to analyze the change in electrical characteristics of the conductive network.

The aim was for the physical structure, which consists of a special conductive network, to provide several detection functions, namely: short-circuit detection and interruption of conductive network paths, detection of temperature variations and shielding of protected circuits.

In the case of intrusion detection circuits, the analysis and experimental testing of several detection methods, to establish the efficiency in the cases of interest, were considered.

1.3 Content of the thesis

Chapter 1 presents the importance of electronic security circuits in the context of data communications and security of information resources. The areas of use of these circuits are highlighted in the context of modern technologies.

Chapter 2 contains a summary of attacks on electronic security circuits, such as cryptanalysis, side channel attacks and physical intrusions.

Chapter 3 describes the components of an intrusion detection circuit and the current state of the solutions available in this field.

Chapter 4 includes the contributions to the development of conductive networks and active intrusion detection circuits, which work in conjunction with them. Two types of conductive networks are studied: double layer network and triple layer network. Methods for probing conductive networks by active intrusion detection circuits are presented. They can detect physical intrusions, intrusion attempts and heat attacks (temperature variations at the conductive network level).

Chapter 5 extends the scope of intrusion detection systems, presented in Chapter 4, to the protection of electronic security circuits or copyright in computer applications.

Chapter 6 presents the original contributions and the list of original works.

The bibliography represents the last chapter of the thesis and contains the works consulted during the thesis.

Chapter 2

Attacks on electronic security circuits

An important aspect of ESC security is that it must protect the security data stored or used in the processes inside it: cryptographic keys, secret data, passwords, firmware etc. The protection must be active throughout the life of ESC, unconditioned by the presence of the power supply. In this sense, ESCs are protected by specialized circuits, equipped with sensors that constantly monitor various state parameters and detect intrusion attempts, while ensuring low power consumption. Intrusion (tampering) detection circuits are made with specialized integrated circuit (ASIC), logic gates, programmable circuits (FPGA, CPLD) or microcontrollers, to which are attached various sensors dedicated to this purpose. In the event of an intrusion being detected, the dedicated circuit takes the scheduled action so as not to disclose the security data, which generally consists of quickly deleting it. Usually, the security data is stored in a volatile RAM memory and the deletion is performed by interrupting its power supply.

Types of attacks on electronic security circuits.

Attacks on ESCs can be grouped into the following categories:

- **Cryptanalysis of cryptographic systems**;
- **Side channel attacks**;
- **Physical intrusions**.

2.1 Cryptanalysis of cryptographic systems

Cryptanalysis studies the cryptographic systems in order to find weaknesses in the functions implemented in them that could help decrypt data without knowing the encryption key [1]. In the risk analysis associated with cryptanalytic attacks it is considered that the encryption algorithm is known. Cryptanalytic attacks can be classified according to the type of information that the attacker has at his disposal [1], as follows:

- **Ciphertext-only**. In this attack scenario, only encrypted text is used and the attacker is assumed to have passive capabilities to monitor encrypted communication. Even if the attacker does not know the clear text, he still has some information about the clear text.
- **Chosen-plaintext**. In this scenario, the attacker has the option to choose the plaintext and obtain the corresponding ciphertext. In modern cryptography differential cryptanalysis is a typical example of an attack with chosen text. This attack is similar to the chosen ciphertext attack.
- **Adaptive chosen-plaintext**. It is similar to the attack with chosen text with the difference that the attacker chooses subsequent clear texts based on information learned from previous encryptions.
- **Related-keys**. As with plain text attack, the attacker gains access to encrypted text with associated keys. The keys are not known to the attacker but are in a mathematical relationship known to him.

Cryptanalytic attacks can be characterized from the point of view of the necessary resources, as follows:

- **Time**. The duration of the attack depends on the number of steps to be performed.
- **Memory**. Every attack needs memory to store working variables and vectors. Each type of attack requires a different volume of memory.
- **Required data volume**. Depending on the type of attack, the required data volume (plain text, ciphertext) must be of a certain size.

2.2 Side-channel attacks

Side-channel attacks (SCAs) use any information, unintentionally provided, from electronic devices that implement cryptographic functions. This information can be in the following forms [2] [3] [4]: processing time, sound, electromagnetic waves, dissipated power, supply currents etc. These attacks depend on how ESCs are designed and how cryptographic functions are implemented.

The FIPS 140-2 standard [5] defines four types of SCA attacks: power analysis, runtime analysis, error induction, and TEMPEST. These attacks are described as follows:

1. **Power analysis**. Attacks based on power consumption can be divided into two categories, **Simple Power Analysis** (SPA) and **Differential Power Analysis** (DPA). SPA involves a direct analysis of the waveforms of signals that characterize the consumption of power and the execution times of individual

instructions by an ESC during the execution of a cryptographic function. DPA has the same purpose as SPA but uses advanced statistical methods and specialized techniques (eg time-frequency analysis) to analyze variations in power consumption.

2. **Timing Analysis**. Duration analysis attacks are based on the accurate measurement of the execution time of mathematical operations associated with a cryptographic function. The time information collected is analyzed to determine the relationship between the ESC inputs and the cryptographic keys used by the algorithm or process in question.

3. **Fault Induction**. Fault induction attacks use external stimuli, such as microwave radio signals, extreme temperatures, and manipulation of the supply voltage to cause ESC processing errors. The analysis of these errors and the occurrence model can be used in reverse engineering of the application running in ESC, in order to reveal the implementation characteristics of cryptographic functions and, subsequently, cryptographic keys.

4. **TEMPEST**. TEMPEST analysis involves the remote detection and collection of information from unwanted electromagnetic signals emitted by a ESC.

2.3 Physical Intrusions

In addition to protection measures against cryptanalytic attacks or side channel attacks, ESCs must be protected against physical intrusions so that access to its electronic components is impossible. Physical intrusion can be defined as any action aimed at gaining access to electronic components or data buses that make up an electronic circuit. The connection to the data buses between the logic circuits of the ESC ensures the obtaining of important information from its internal processes.

Unauthorized access to the ESC's electronic circuit can cause significant damage, such as:

- Obtaining the cryptographic key. This can lead to the decryption of the communications of the device that incorporates an ESC or the decryption of the communications from the entire network to which the electronic module is connected. Thus, the confidentiality of the data can no longer be ensured.

- Intervention on the messages communicated by ESC. Message integrity can no longer be ensured.

- Assumption of ESC identity by another entity. An attacker may transmit false information to network entities as if it were transmitted by the ESC in question.

- Modify messages transferred to the network to introduce errors. The authenticity of the messages is thus compromised.

2.3.1 Measures to reduce physical intrusion attacks

Protection against physical intrusion attacks is characterized by the following types of actions:

- *Tamper detection*: is the ESC's automatic determination of an attempt to compromise physical security.
- *Tamper evidence*: is the external indication of the electronic equipment containing ESC regarding the attempt to compromise physical security.
- *Tamper response*: is the automatic action performed by ESC as soon as it detects the intrusion. The ESC shall take action against unauthorized use or disclosure of security data stored therein.

Chapter 3

Tamper detection circuits - current state

3.1 Protection of electronic security circuits against physical intrusions

ESC security is achieved through a set of multi-level protection mechanisms. The first level is the physical one: the electronic circuits are protected by a special housing, which does not allow unauthorized entry into the circuit. They are made of metallic materials and meet the following requirements: they are watertight and do not have slots or perforations that could favor the access of specialized probes (optical) at the level of electronic circuits.

The second most important level is the protection of electronic circuits and security data. An attacker should not have access to these circuits, but if it manages to pass the first level of protection, ESC has a specialized circuit that reacts in the way of protecting the security data. The response time is very short and the effect is complete, in the sense that all security data is deleted.

The solution that ensures this level of protection is the introduction, between the metal housing and the protected circuit, of a special conductive layer that is sensitive to intrusions - the conductive network. This network is periodically probed with signals by the Tamper Detection Circuit (TDC). When this circuit detects an intrusion, it performs specific security data protection functions: fast deletion of this data and execution of a special routine for deleting sensitive data inside the ESC processor.

Depending on how the probing signals of this protective layer are analyzed, intrusion detection circuits are classified into passive circuits and active circuits.

3.2 Conductive networks

To ensure a high level of protection, conductive networks (conductive meshes), made in the form of a printed circuit covering both the ESC and TDC [6], are used. The

conductive network may be flexible, made of thin printed foils, or rigid, made of printed circuit boards (PCBs), joined so as not to result in gaps that would facilitate intrusions or the introduction of probes to analyze the inside of the ESC. Any attempt to penetrate these structures determines the generation of the intrusion event.

For these conductive networks to be effective in terms of penetration attempts, both the width of the traces and the space between them must be small, generally less than $0.2mm$.

3.3 Passive Tamper Detection Circuits

Passive tamper detection circuits are based on the monitoring of electrical or logical levels, the variation of these levels outside the limits determines the triggering of the intrusion response process (*tamper response*). Depending on the consumption regime used, the parameters can be checked continuously or at a predefined period.

To ensure an increased level of security of protected data (cryptographic keys, random sequences and other secret data), intrusion detection integrated circuits can be equipped with non-volatile RAM and a real-time clock. The real-time clock provides the required time stamp in many cryptographic processes but also records the time when the intrusion event was detected. As non-volatile RAM is a part of the integrated circuit, it is intended to store a cryptographic key, necessary for the encryption of data volumes (ESC firmware, security data etc.).

3.4 Active Tamper Detection Circuits

Active tamper detection circuits (ATDC) are based on the principle of testing the conductive network by probing it with signals with appropriately chosen characteristics. The probing signals are injected into the conductive network through the input port. At its output port, the signals are sampled and analyzed, with reference to the initial signals. The principle diagram of such a circuit is presented in figure 3.6.

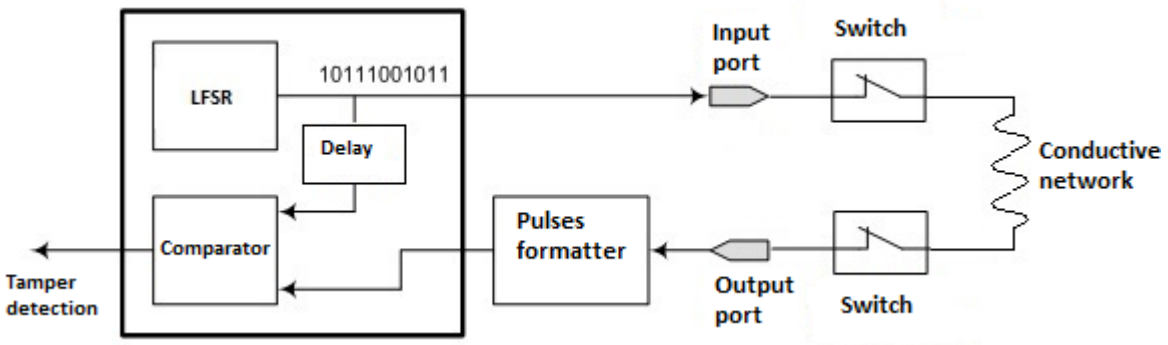


Figure 3.6: *Principle schematic of an active tamper detection circuit.*

Generally, probing signals are pulses that have variable parameters (period,

duration, shape) in order to make them impossible to reproduce in the event of a bypass attack (deactivating an area of the conductive network and injecting false pulses).

ATDC analyzes the effects that the conductive network exerts on the pulses that propagate through it. To perform this analysis, the signals resulting from the output of the conductive network are sampled and analyzed in the time and frequency domains. In this way, the dispersive characteristic of the conductive network can be exploited. This method involves using a fast analog-to-digital converter and performing a larger volume of calculations than other methods.

As with passive intrusion detection circuits, ATDC can be affected by electromagnetic interference both inside and outside the protected electronic circuit. To reduce this effect it is necessary to shield the conductive network inside and outside. In this way, the effects of external electromagnetic interference will play a useful role in detecting intrusions by affecting the probing signals due to the voluntary damage of the external shielding layer.

3.5 Structure of an intrusion protection circuit

ESCs are modules that are part of specialized electronic equipment, mainly dedicated to data and communications protection. How ESC interacts with the intrusion detection circuit and other types of attacks is shown in figure 3.7. The detection circuit constantly monitors the sensors, both during the operation of the equipment and during the period when it is not powered. During the periods when it is not powered (during transport, storage or maintenance), the detection circuit is powered by a backup battery. In case of detection of such access (intrusion, out-of-bounds change of circuit temperature, change of supply voltage etc.), the detection circuit interrupts the supply of non-volatile RAM, to provoke the loss of security data, and generates an interrupt signal to the logic circuit of ESC (microprocessor, ASIC etc.) in order to delete the data from RAM and internal registers.

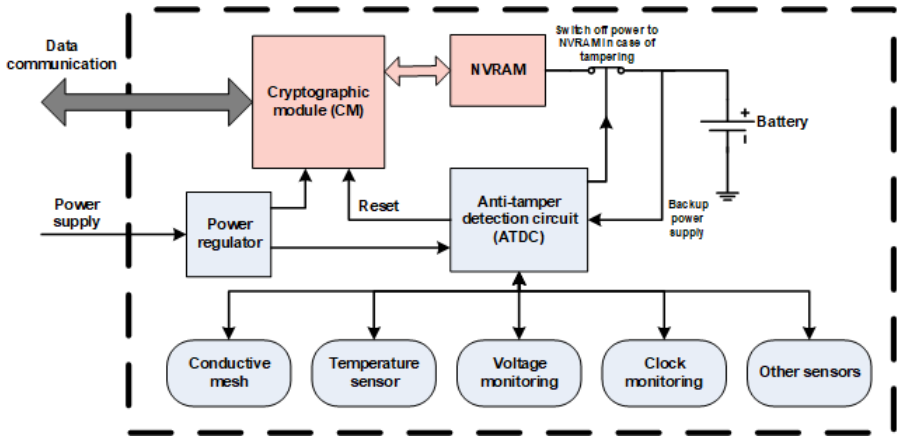


Figure 3.7: *Schematic diagram of an ESC protection circuit.*

The sensors used by TDC are: conductive network (for detecting physical intrusions), temperature sensors, sensors for monitoring supply voltages, sensors for detecting the variation of the processor clock frequency and other circuits with monitoring functions.

In order to protect the conductive network against external factors, including the electromagnetic interference, the entire ESC protection circuit is enclosed in a rigid metal case. This enclosure also protects against accidental physical intrusions. Figure 3.8 exemplifies this method of ESC protection.

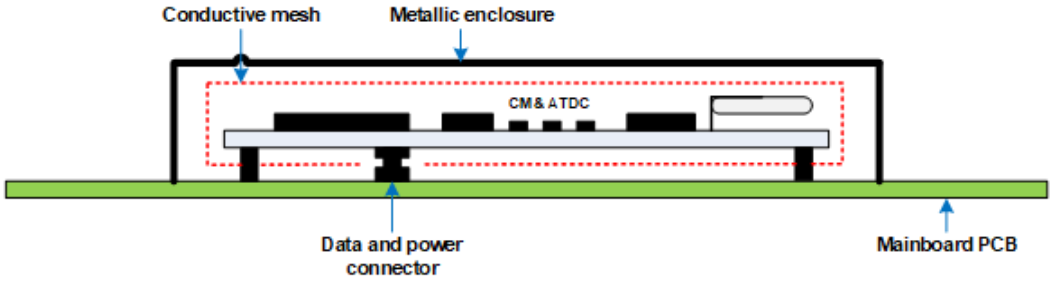


Figure 3.8: *Structure of ESC and TDC ensemble.*

The ESC is completely covered by the conductive network, except for the connector through which it is powered (during operation) and the data is transferred. The metal enclosure, which covers this structure, is connected to the ground plane of the equipment. This enclosure improves the stability over time of the intrusion detection circuit in order to reduce false triggers of intrusion events.

Chapter 4

Active tamper detection circuits

4.1 Innovative double-layer conductive network for active tamper detection circuits

In order to isolate the conductive traces from the possible electromagnetic interferences of ESC and ATDC (these being protected, as a whole, by ATDC), it is necessary to introduce a separation ground plane, connected to the ground potential of ESC and ATDC. Thus, the printed circuit will contain two conductive layers (isolated by a dielectric layer): one ground plane and one layer with a conductive network. The ground plane will be positioned between the module formed by ESC and ATDC and the conductive network.

Flexible electromagnetic screen design

To ensure increased flexibility of the conductive network, the ground plane is made in a hatched form with square perforations, with side of $0.5mm$, spaced at $1mm$. Considering that the surfaces that make up the conductive network do not exceed a square with sides of $10cm$ (100 perforations / side), the shielding efficiency is $89.5dB$.

Conductive network design

The role of the conductive network is to prevent intrusions (perforations) in order to gain access to ESC and ATDC. It is made in the form of thin traces, with a width of less than $0.2mm$, with a maximum space between paths of $0.2mm$. The traces model looks like meanders and they cover the entire surface, without leaving uncovered spaces, and is made of a single conductive circuit (it has a single input and a single output accessible at ATDC level). A sample of the conductive network is shown in figure4.1.

For conducting experimental tests, the conductive network was made of a printed circuit board (PCB) of sticlotextolite type (FR4), with two layers of copper, with a

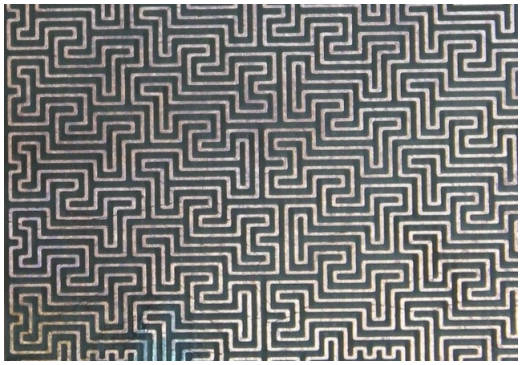


Figure 4.1: *Conductive network traces made on a PCB.*

thickness of $0.035mm$. The printed circuit board has the size of $12.5 \times 25cm$, the thickness of $0.5mm$, and the routes have the width and the distance between them of $0.2mm$. The first layer consists of conductive traces with the model shown in figure 4.1, the second consists of a complete copper foil connected to the ground plane of ESC and ATDC.

4.2 Active tamper detection circuit based on LFSR generator

The tamper detection circuit, studied in the paper [7], consists of a microcontroller, the conductive network shown in figure 4.1 and a pulse formation circuit. STM32F4-DISCOVERY development board (contains the STM32F407VG microcontroller) was used to perform the tests and measurements. The functional diagram of this circuit is presented in figure4.2.

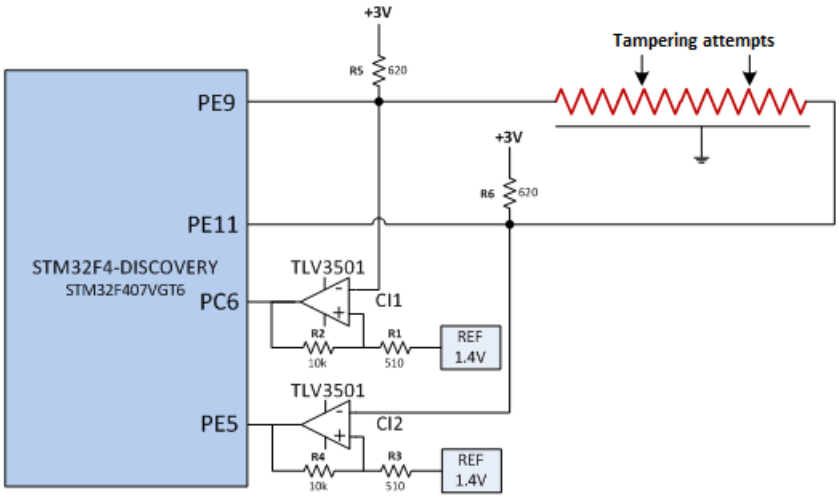


Figure 4.2: *ATDC reference diagram.*

The microcontroller generates pulses at both ends of the conductive network in order to mask the source of the probe pulses and to mislead a possible attacker who

would try to simulate these pulses. The GPIO pins PE9 and PE11 are connected to the conductive network and are configured as open drain outputs for channels 1 and 2 of the internal clock circuit *Timer 1*, in PWM mode (*Pulse Width Modulation*). These output pins are configured in open drain mode to perform the logical *AND* function required in this application. The equivalent scheme, with the concentrated parameters, is presented in figure 4.3.

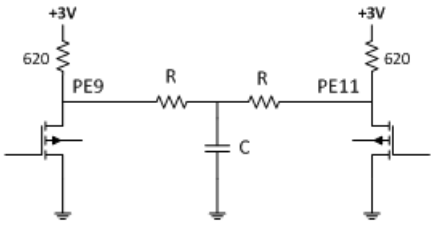


Figure 4.3: *Equivalent diagram of the conductive network connected to pins PE9 and PE11.*

The principle of generation and acquisition of probing pulses

Probing pulses are synchronized using a pseudo-random sequence generator LFSR (*Linear-Feedback Shift Register*). A modified Gollmann cascade configuration was used for the ATDC circuit, as shown in [8]. The logic diagram of this generator is presented in figure 4.4:

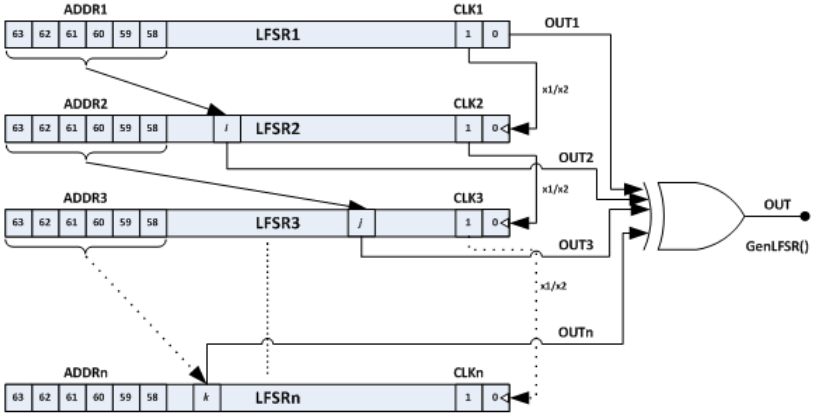


Figure 4.4: *The logic diagram of the pseudo-random generator based on the Gollmann cascade.*

This generator is used to decide which pulses are active at the output ports PE9 and PE11 (configured as alternative function 1 - TIM1_CH1, respectively, TIM1_CH2). *Timer1* is configured in PWM generation mode with the frequency of 250kHz and is synchronized by the internal clock signal of the microcontroller (with the frequency of 168MHz). At each period of $4\mu s$, *Timer1* enters the interrupt routine and, based on the output of the LFSR generator, the program determines whether

the probing pulse is generated. If the LFSR generator produces a bit 0, then the output *Timer1* is disabled, otherwise the LFSR generator provides two bits that will determine the parameters of the generated pulses.

The relationship between $D1$ and $D2$ is $D2 = D1 + d$, where d is the propagation time of the pulses through the conductive network, in this particular case $d = 162ns$.

The pulse composition mode is shown in figure 4.5 and is valid at any point of the conductive network and is due to the fact that ports PE9 and PE11 are configured in open drain mode to obtain the logic function AND (textit AND).

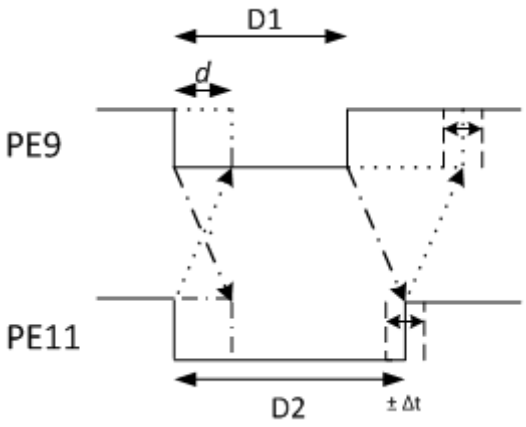


Figure 4.5: *The composition of the probing impulses of the conductive network.*

Pulses formation circuit

The pulse formation circuit is made using the TLV3501 [9] [10] comparator, used in the hysteresis comparator configuration to increase noise immunity. Noise immunity is necessary because the pulses have slow fronts and the comparator can produce oscillations at the output at times when the input signal has values near the threshold level.

Analysis of detected pulses

The pulses produced by the formation circuit, made with comparators, are analyzed by the clock circuits *Timer8*, channel 1 (TIM8_CH1), and *Timer9*, channel 1 (TIM9_CH1), connected to pins PC6 and PE5, respectively (configured as alternative function 3). These clock circuits are configured in PWM analysis mode and perform the function of detecting pulse periods and durations.

To demonstrate the operation of ATDC, the experimental circuit presented in figure 4.6 was made. This circuit contains all the modules presented above: the printed circuit board (PCB) of the conductive network (left side of the figure), the pulse formation circuit (right side of the figure) and the STM32F4-Discovery development board (central part of the figure).

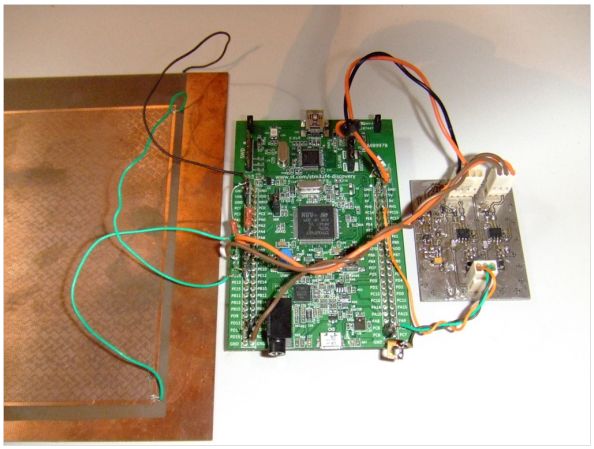


Figure 4.6: *Experimental tamper detection circuit.*

The pulses measured at the pins PE9, PE11, PC6 and PE5 are shown in figure 4.7, channels 1 to 4.

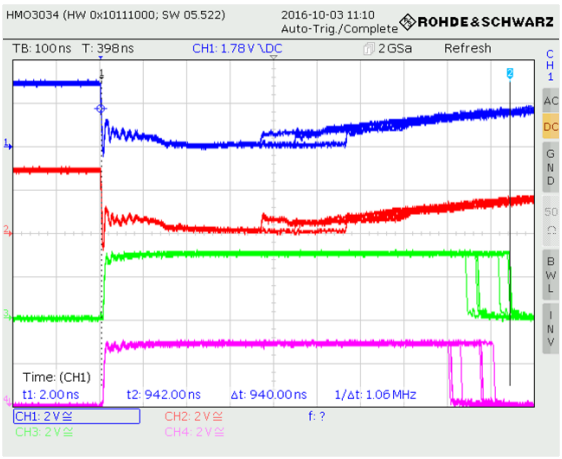


Figure 4.7: *Captures of the pulses at pins PE9, PE11, PC6 and PE5.*

The proposed method of generating probe pulses, based on a complex LFSR generator scheme, together with the principle of their composition during propagation through the conductive network do not allow determining the pulse parameters and simulating the normal operation of the detection circuit.

Following experimental tests, ATDC achieves the following performances:

- detects variations of durations between pulses greater than $5.9ns$;
- detects variations of pulse durations greater than $5.9ns$;
- detects an increase in the total capacity of the conductive network by at least $22pF$;
- detects physical intrusions made by cutting the conductive network and any intervention that can change the duration and amplitude of the signals through it.

4.3 Active tamper detection circuit based on the pulse response analysis of the conductive network

The analysis of probing pulses at the exit of the conductive network by measuring durations between fronts can be improved in the sense of increasing the sensitivity in detecting intrusion attempts. The proposed circuit analyzes the pulse delay and the total spectral power. ATDC is composed of a processing circuit, an acquisition circuit and a conductive network [11]. The principle diagram is presented in figure 4.11.

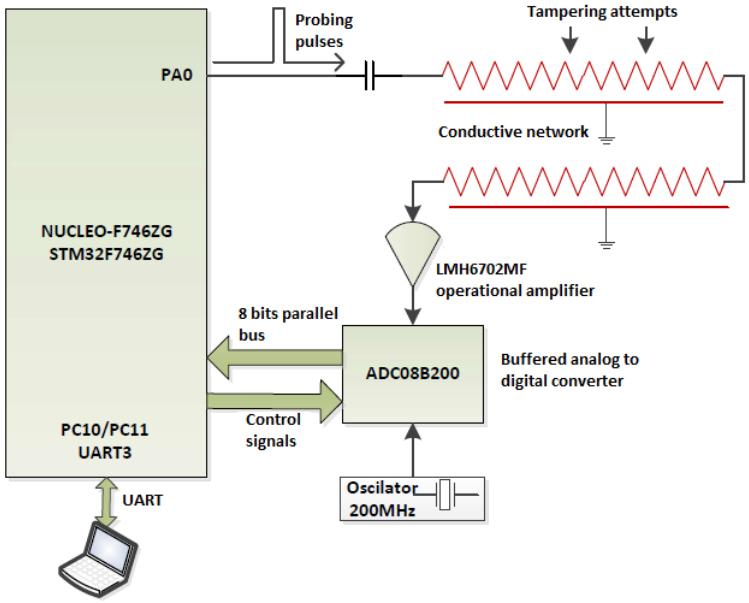


Figure 4.11: *ATDC principle schematic.*

The processing circuit generates pulses of variable duration, with a period of one second, which are applied to the conductive network on the input port, by capacitive coupling. These pulses propagate through the conductive network and the signals from the output port are amplified and adapted, using an operational amplifier, to be acquired by the analog-to-digital converter. The acquired data is analyzed to detect physical intrusions.

Processing circuit

The NUCLEO-F746ZG development board is the processing circuit, as shown in figure 4.11. It contains the STM32F746ZG microcontroller. The PA0 output port is used to generate short pulses with durations determined by a LFSR generator, implemented in software. The STM32F746ZG microcontroller controls the analog-to-digital converter, setting the times at which it starts the conversion. The acquired data is temporarily stored in the analog-to-digital converter. At the end of the acquisition, the microcontroller reads from it 256 samples of 8 bits each. The samples are analyzed in order to measure the delays and calculate the power of the spectral components.

Acquisition circuit

The acquisition circuit consists of two components: the operational amplifier LMH6702 and the analog-to-digital converter ADC08B200. The amplification and acquisition circuit is presented in figure 4.13.

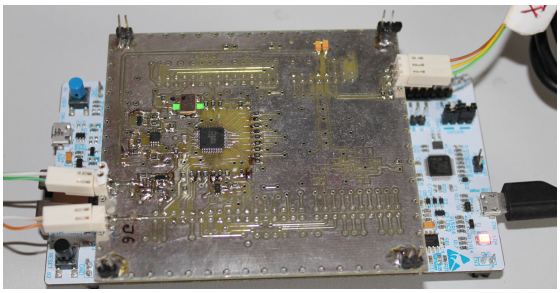


Figure 4.13: *Amplification and acquisition circuit.*

The ADC08B200 is an 8-bit analog-to-digital converter with a maximum sampling rate of 210Msps. It has a storage memory with a selectable size of 256, 512 or 1024 bytes. 256 samples were enough for this application, the converter being configured for this size.

The conductive network used is the one presented in the section 4.1.

Principle of operation

The processing circuit (NUCLEO-F746ZG) generates short pulses, with variable durations, which supply the input port of the conductive network through the capacitive coupling. The resulting signals at the output port of the conductive network are taken over by the acquisition circuit. It amplifies the signals using the LMH6702 operational amplifier and then samples them with the ADC08B200 converter. The resulting samples (256 bytes) are read by the STM32F746ZG microcontroller, within the processing circuit.

In order to detect a possible intervention on the conductive network, the samples are analyzed following two aspects: pulse delay (time domain) and power of spectral components (frequency domain).

Time domain analysis

Using the *arm_max_f32* function, the microcontroller detects the position of the peak values of the pulses in the acquired data, representing the delay of the pulses at the output port of the conductive network.

Frequency domain analysis

ATDC analyzes the response of the conductive network in the frequency domain. The change in the parameters of the probing pulses can be analyzed by the energy

spectral density of the sampled signal sequence. Pulses with durations of $13.6ns$, $22.4ns$, $35ns$ and $46.4ns$ were used to probe the conductive network. It was tested under the following conditions: no intervention, the addition of a capacitor in parallel (with capacities of $8pF$, $22pF$ and $33pF$) and the addition of a series resistor (with resistors of 1Ω, 5Ω and 10Ω). The purpose of these experiments is to analyze the ATDC response to intrusion attempts. Figures 4.22 and 4.23 show graphically the values of the spectral power for pulses of $46.4ns$.

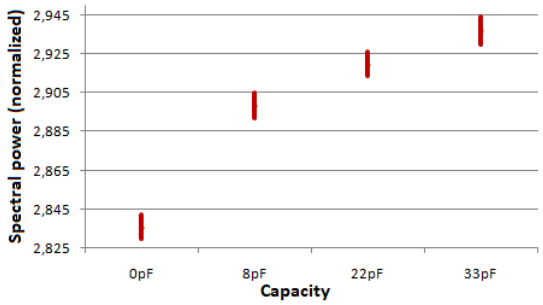


Figure 4.22: *Spectral power variation for pulses of 46.4ns in case of increasing the capacity in parallel with the conductive network (normed power, $x10^{-4}$).*

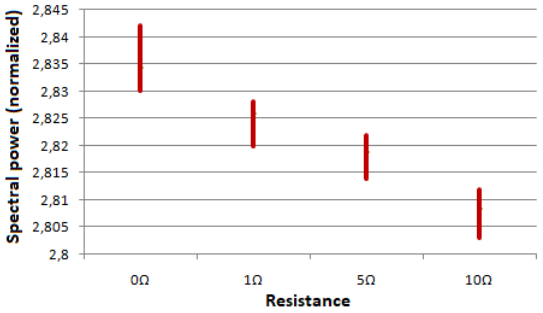


Figure 4.23: *Spectral power variation for pulses of 46.4ns in case of increasing the resistance in series with the conductive network (normed power, $x10^{-4}$).*

În time domain, ATDC can detect any pulse delay variation greater than $5ns$.

As regards the spectral analysis, the analysis of signals with a standard oscilloscope probe ($8pF/1M\Omega$) can be detected by using probing pulses with durations of $22.4ns$, $35ns$ and $46.4ns$. Also, increasing the total resistance of the conductive network path by at least 1Ω is detected for pulses of at least $22.4ns$. ATDC can detect intrusions and intrusion attempts with a high degree of certainty for probe pulses with durations of $22.4ns$, $35ns$ and $46.4ns$.

4.4 Active tamper detection circuit with dual function: temperature variation detection and statistical intrusion detection

In this section, an ATDC is proposed which, in addition to detecting physical intrusions, can detect temperature variation at the level of the protective coating formed by the conductive network. From the point of view of ESC security, it is much more efficient to detect the exceeding of the temperature limits at the level of the outer shell of the assembly consisting of ESC and ATDC than to perform this function at the level of the printed circuit board.

In addition to protection measures against collateral channel attacks based on temperature variation, the paper also offers a solution for intrusion detection by statistical analysis of the conductive network response to pulse probing.

The analysis of the ATDC behavior at the temperature variations, at the level of the conductive network, is based on the study carried out within the paper [12]. Statistical methods of intrusion detection were studied in the paper [13]. The experimental analysis was performed using the electronic circuit shown in figure 4.11.

Analysis of the response of the conductive network to temperature variations

Given the variation of the resistance and capacitance parameters, which characterize the paths of the conductive network, the probe pulses that propagate through this structure are affected differently at different temperatures. Therefore, calculating the signal strength at the output of the conductive network is an efficient method of detecting variations in the characteristics of this propagation medium depending on the temperature variation. The calculations were performed in floating point format, simple precision, using native microcontroller instructions.

Statistical analysis of the conductive network response

In order to detect the physical intrusions, a more energy efficient solution (with a small number of calculations) is the statistical approach for the analysis of sampled signals. The statistical parameters used in this paper are: arithmetic mean, root mean square (RMS), standard deviation and variance. ATDC calculates these statistical parameters and compares them with reference values to detect tampering attempts.

ATDC response to temperature variations

Temperature variation tests were performed using the ESPEC Temperature Chamber, model SH-241. The tests were performed by varying the temperature in the range of $-20^oC \div 100^oC$, with temperature stabilization at each temperature stage (10^oC steps).

The acquired values of the normed power of the signal are presented in figure 4.26. These values are used for relative comparisons in order to establish the occurrence of the physical intrusion situation. From the analyzed data, the quasi-linear variation of the power is observed having a negative slope. ATDC is able to unambiguously detect the temperature in the conductive network.

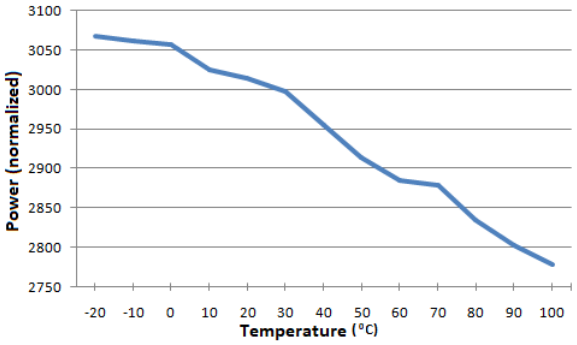
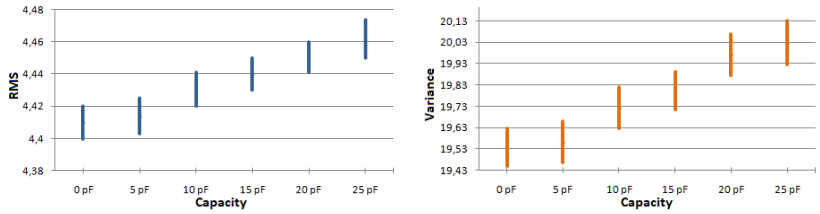


Figure 4.26: *Normalized power of the probing signal as a function of temperature.*

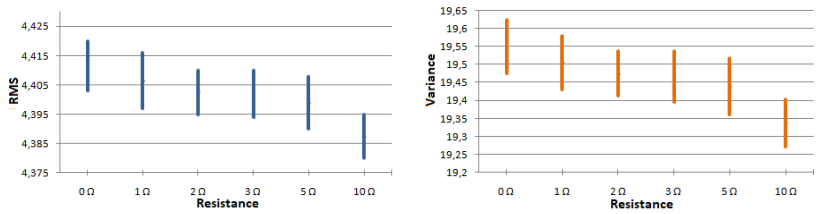
Intrusion detection based on statistical analysis

Experimental testing simulated a possible intervention on the conductive network and consisted of increasing the capacity in parallel with the conductive network (capacitors with capacities of $5pF$, $10pF$, $15pF$, $20pF$, $25pF$) and series resistance with the conductive network (resistors with resistors of 1Ω, 2Ω, 3Ω, 5Ω, 10Ω). The experimental results are represented graphically in the figures 4.27 and 4.28. Experimental results demonstrate the efficiency of ATDC for increasing series resistance by more than 10Ω and increasing total capacity by more than $10pF$.



(a) *RMS* ***(b)*** *variance*

Figure 4.27: *Variation of statistical parameters depending on the increase of capacity.*



(a) *RMS* ***(b)*** *variantă*

Figure 4.28: *Variation of statistical parameters depending on the increase of resistance.*

4.5 Innovative conductive network with triple layer structure - increasing efficiency in detecting intrusions

The main requirements for conductive networks used to protect the ESC are to ensure an increased sensitivity to tampering attempts and the impossibility of replicating the probing signal used by ATDC.

The study contained in this section is based on the article [14] and proposes an innovative type of conductive network made of three conductive layers, isolated with dielectric layers. The first layer, arranged inwards, is a compact layer connected to the ground potential and has two important roles: reference plane for probing signals and electromagnetic shield between the assembly consisting of ESC and ATDC and conductive traces probed with signals (layers 2 and 3). Layer 2 (intermediate), contains a very fine conductive network (routes with thickness $< \ 0.2mm$ and distances between them $< 0.2mm$) with meander pattern. This is the layer used by ATDC for the analysis of probing signals. The third outward layer is not directly probed by ATDC but is used to facilitate intrusion detection. The geometry of the paths on this layer copies the one on the intermediate layer, with the difference that they form closed circuits. In order to determine the behavior of the conductive network in case of physical intrusions, the structure presented in figure 4.29 was used.

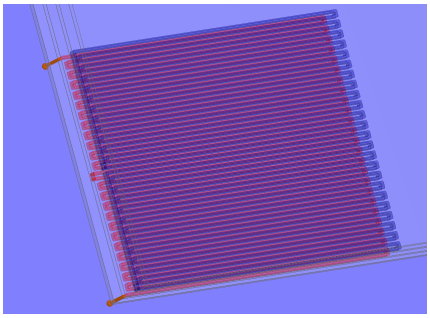


Figure 4.29: *Geometric structure of the conductive network used in simulation.*

Analyzing the signals induced in layer 3, this structure does not allow the determination of the characteristics of the probing signals used by ATDC. These signals have very small amplitudes and do not have a reference ground plane, being circuits galvanically isolated from the rest of the structure. If an attacker tries to connect to the conductive paths of layer 2, he should decommission areas of the conductive network on layer 3.

A conductive network measuring $30mm \times 30mm$ has been designed with meanders that perform inductive and capacitive couplings at different signal propagation lengths in order to produce multiple resonances at low frequencies. The ANSYS ®SIwave 2016.2.0 application was used to simulate this conductive network, shown in figure 4.35.

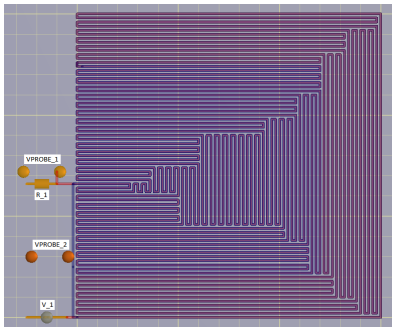


Figure 4.35: *Improved conductive network.*

The simulation was performed in the frequency range $0Hz \div 500MHz$. The simulation results for this structure are presented in figure 4.36, for the case of the detection layer is unaffected, and in figure 4.37, for the case of the physical intrusion was performed.

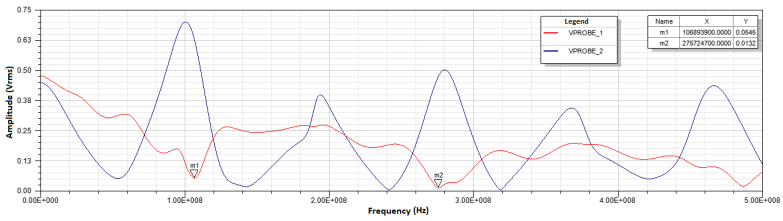


Figure 4.36: *Conductive network unaffected by intrusion: red trace - signal amplitude on resistor R_1, blue trace - signal amplitude measured at a point on the conductive trace on layer 3.*

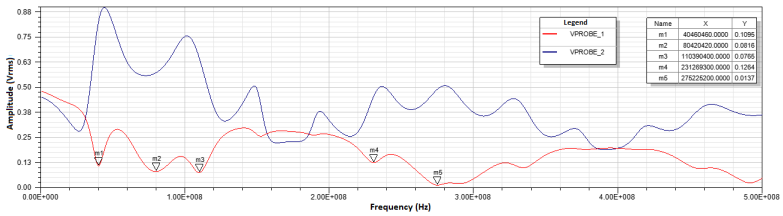


Figure 4.37: *Conductive network affected by intrusion: red trace - signal amplitude on resistor R_1, blue trace - signal amplitude measured at a point on the conductive trace on layer 3.*

When creating the intrusion, from the two graphs it is observed the increase of the resonance points and the decrease of the frequencies at which these resonances take place. Using an appropriate method for analyzing these resonances, ATDC can quickly detect an intrusion without exposing the signal path to the attacker. Structures similar to the one shown in figure 4.35 can be combined to obtain the area needed to cover the entire ESC. On layer 2 the conductive paths are connected in series, to create the signal path, and on layer 3 each zone forms a closed circuit.

Triple layer conductive network - extended structure

In the paper [15] it was evaluated the behavior in the frequency domain of a structure consisting of two square areas, with sides of $30mm$, the traces and spaces between them having a width of $0.2mm$. This structure is shown in figure 4.40. The working principle of the assembly formed by this conductive network and ATDC was proposed for publication in the patent application [16].

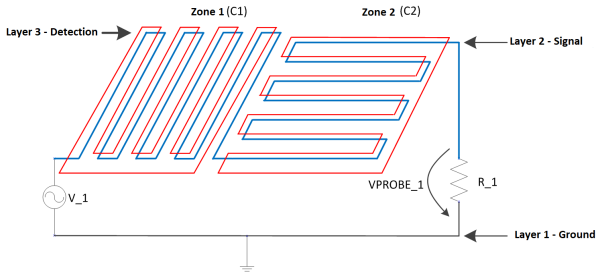


Figure 4.40: *The structure of the conductive network consisting in two active areas.*

As can be seen in figure 4.40, on layer 2, the conductive traces of the two zones are connected in series and those on layer 3 form closed circuits, corresponding to each zone. To validate the detection effect of the conductive network, it was made practically in the form of a PCB, with a dielectric thickness of $0.3mm$, with the same characteristics as the simulated model. The following cases were analyzed: no intrusions, C1 affected by intrusion and C2 affected by intrusion. The results are shown in figure 4.43.

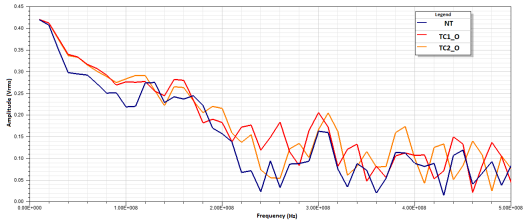


Figure 4.43: *Conductive network output characteristic (simulation): NT - no intrusion, TC1_O - C1 open circuit, TC2_O - C2 open circuit.*

The output characteristic of the conductive network is presented in figure 4.45. As can be seen from the figures 4.43 and 4.45, starting with the frequency of $30MHz$, the conductive network is efficient in detecting open circuit intrusions. The amplitude differences between the unaffected state and the one affected by the intrusion of the conductive network are easily quantifiable for wide frequency ranges.

Triple layer conductive network - short-circuit intrusion analysis

Physical intrusions on conductive networks can be performed, in addition to interrupting conductive traces, by creating short circuits between adjacent traces.

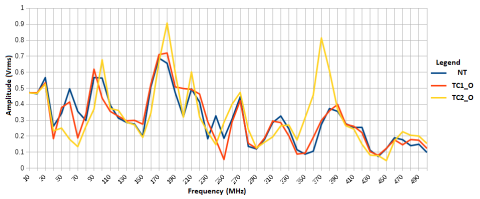


Figure 4.45: *Conductive network output characteristic (experimental test): NT - no intrusion, TC1_O - C1 open circuit, TC2_O - C2 open circuit.*

Considering the circuit presented above, the following cases were analyzed by simulation and experimental testing [17]: unaffected conductive network, short circuit between two adjacent traces and the interruption of the conductive path. A $0.1mm$ thick PES (*Poly Ether Sulfone*) conductive network, printed with SW180 conductive paste (Tatsuta Electric Wire & Cable Co. Ltd.), was tested. The result of the simulation is presented in figure 4.48.

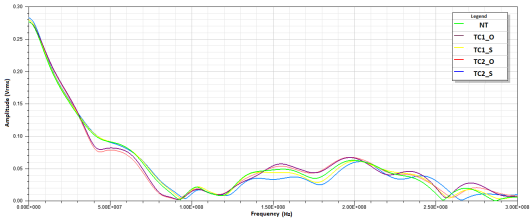


Figure 4.48: *Conductive network output characteristic (simulation): NT - no intrusion, TC1_O - C1 open circuit, TC1_S - C1 short circuit between traces, TC2_O - C2 open circuit, TC2_S - C2 short circuit between traces.*

The conductive network has wide frequency ranges useful in intrusion detection. To validate the effects of intrusions on the conductive network, it was performed practically and tested under the same conditions as the model used in the simulations. The measurements performed are shown in figure 4.52.

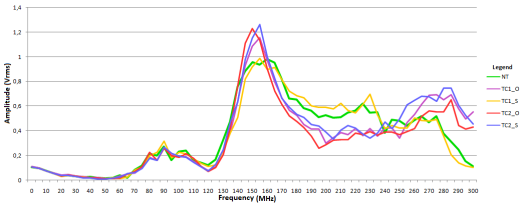


Figure 4.52: *Conductive network output characteristic (experimental test): NT - no intrusion, TC1_O - C1 open circuit, TC1_S - C1 short circuit between traces, TC2_O - C2 open circuit, TC2_S - C2 short- circuit between traces.*

Starting with the frequency of $85MHz$, this structure can be used to securely detect open-circuit and short-circuit intrusions between adjacent traces. The two modes of conductive network analysis (simulation and experimental testing) demonstrate its effectiveness in detecting interrupt or short-circuit intrusions performed on the detection layer (3).

4.6 Technological aspects of the manufacture of conductive networks on dielectric flexible foils

The conductive network printed on PES foil was made with the help of screen printing technology. For the realization of the conductive network, a graphic design was conceived, which was later transposed in a screen printing screen with metallic fabric. Printing was done with SW180 conductive paste (TATSUTA) and DEK Horizon 08 printing equipment. Figure 4.56 shows details of foils printed with SW180 conductive paste on PES foil ($0.2mm$ thick traces).

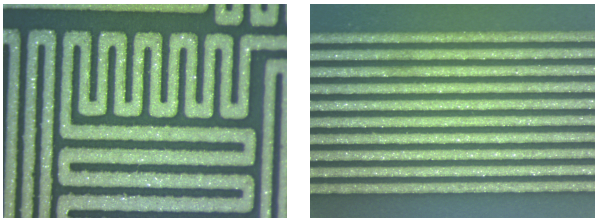
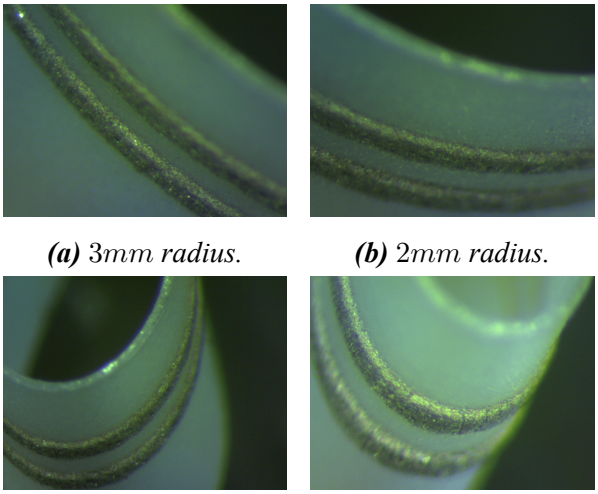


Figure 4.56: *Conductive traces printed with SW180 paste.*

An important property of the conductive network is its ability to be folded without interrupting the conductive traces. A sample of conductive network, consisting of two linear traces, was tested by bending under different radii. The tests, presented in figure 4.58, reveal that the conductive network can be bent with a minimum radius of $2mm$ without producing cracks.



(a) $3mm$ *radius.* ***(b)*** $2mm$ *radius.*

(c) $1mm$ *radius.* ***(d)*** $0.5mm$ *radius.*

Figure 4.58: *Testing of* $0.1mm$ *PES foil at bending under different radii of curvature. For radii smaller than* $2mm$*, conductive trace cracks appear.*

An important aspect of this type of conductive paste is that it has a limited mechanical strength, which is an advantage in making conductive networks for intrusion detection.

4.7 Specialized active tamper detection circuit for triple layer conductive networks

The conductive network with triple layer structure ensures the function of intrusion detection by analyzing the variation of the amplitude-frequency output characteristic. To achieve the intrusion protection of ESC, an ATDC [18] [19] using this type of conductive network was designed. The principle diagram is presented in figure 4.59.

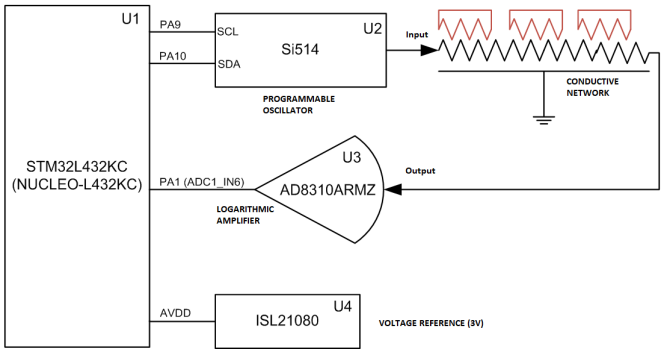


Figure 4.59: *Principle diagram of ATDC intended for probing the triple layer conductive network.*

ATDC contains, as a processing element, the STM32L432KC microcontroller (U1 in figure 4.59), part of the NUCLEO-L432KC development board. The conductive network is probed with pulses formed by sinusoidal signals, with predefined frequencies. These pulses are generated by means of the programmable oscillator Si514, connected to the microcontroller via an I2C port (pins $PA9$ and $PA10$).

The signals from the output of the conductive network (sinusoidal pulses) are detected using the AD8310 logarithmic amplifier. The output of the AD8310 amplifier is connected to the ADC1_IN6 input of the ADC1 converter (pin PA1), part of the STM32L432KC microcontroller.

The ATDC circuit is composed of two modules: the NUCLEO-L432KC development board and the interface circuit with the conductive network, as shown in figure 4.61.

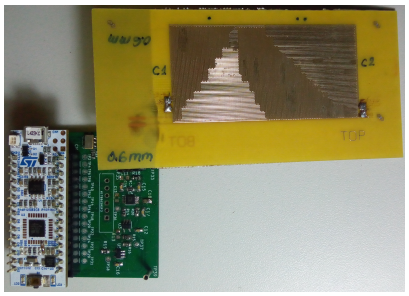


Figure 4.61: *Experimental ATDC consisting of NUCLEO-L432KC development board, interface circuit and conductive network.*

Description of the tampering detection process

The experimental implementation of this ATDC considered the testing of two important features in the protection of ESC: the detection of physical intrusions and the detection of temperature variations. To achieve optimal intrusion detection resolution, 32 frequencies were used, with a $5MHz$ gap between them. The starting frequency was chosen to be $50MHz$, resulting in a domain with a maximum frequency of $205MHz$. The program in STM32L432KC controls the Si514 oscillator so that it changes frequency every $250ms$. After a duration of $20ms$ of internal stabilization of the signal generated by Si514, its output is activated for $300\mu s$, time required for ADC1 to perform the conversion. Figure 4.62 shows a pulse generated by Si514 and the pulse at the output of AD8310.

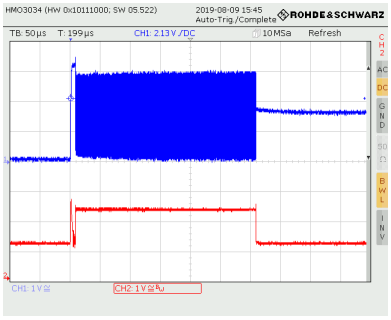


Figure 4.62: *Conductive network output signal (channel 1, blue trace) and signal detected at the output of the logarithmic amplifier (channel 2, red trace).*

Tampering detection

ATDC testing, together with the triple layer conductive network, was performed in real conditions of tampering such as interruption of the conductive trace and short circuit between adjacent traces on the detection layer (3) of the conductive network. The following cases were tested: conductive network is not tampered (NT), C1 is opened (TC1_O), C1 is short-circuited (TC1_S), C2 is opened (TC2_O), C2 is short-circuited (TC2_S) . The conductive network made of $0.1mm$ thick PES foil printed with SW180 conductive paste was analyzed. The result of the analysis is presented in figure 4.63.

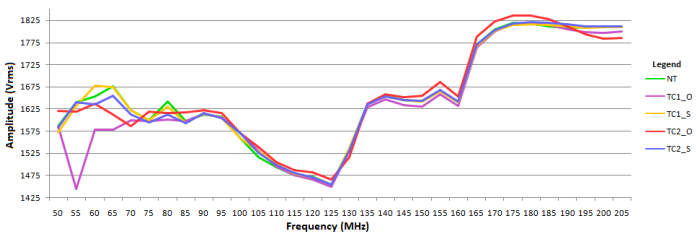


Figure 4.63: *Conductive network output characteristic: NT - not tampered, TC1_O - C1 open circuit, TC1_S - C1 short circuit, TC2_O - C2 open circuit, TC2_S - C2 short circuit.*

It can be observed that the detection of open circuit intrusions (interruption of the traces on layer 3 of the conductive network) is possible in the whole frequency range analyzed. Regarding the detection of short-circuit intrusions between adjacent traces, there are several distinct frequency ranges in which detection is efficient.

Detection of temperature variations

To counteract error-inducing attacks by temperature variations, the triple-layered conductive network together with ATDC are able to detect temperature variations and take the necessary measures to protect security data. Tests were performed for a temperature range between $-20°C$ and $80°C$, using the thermal chamber (ESPEC SH_241). The results are presented in figure 4.66.

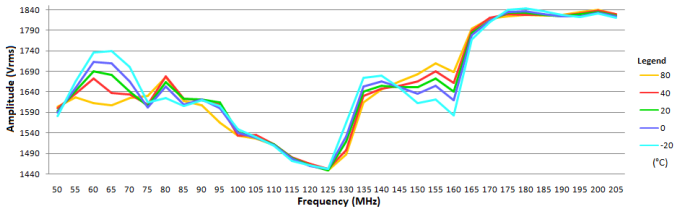


Figure 4.66: *Conductive network output characteristic: behavior at temperature variations.*

Analyzing the behavior of the conductive network at temperature variations, it is observed that the values for temperatures in the range $> -20°C$ and $< 80°C$ are framed by the traces corresponding to the limit temperatures of intrusion $-20°C$ and $80°C$. For the efficient operation of ATDC it is necessary that it allows the detection of the two types of intrusions: physical and thermal. To verify the efficiency of ATDC, the differences between the values resulting in the case of tampering and the values corresponding to the thermal intrusion limits were calculated, and the module of these differences is presented in figure 4.69. If the physical intrusion values are framed by the thermal intrusion values, the displayed value is 0.

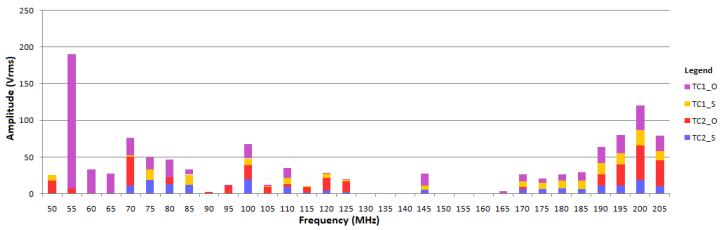


Figure 4.69: *Conductive network PES* $0.1mm$*: amplitude differences (modulus) between physical intrusions and thermal attack limits.*

Analyzing the figure 4.69, it can be observed that the system formed by ATDC and the conductive network detects both tampering and thermal attacks in approximately 80% of the spectrum. To optimize the operation of ATDC, frequencies which are not effective can be removed from the probing spectrum.

Chapter 5

Complementary security functions of the triple layer conductive network

5.1 Securing electronic security circuits

The output characteristic of the conductive network can be used in a special way to secure the ESC, as follows: the signal levels acquired at discrete frequencies are used to obtain a cryptographic key. ESC protection by ATDC covers the following cases: at startup (*boot*) and during operation.

At boot time, a cryptographic key is processed by testing the conductive network at predefined frequencies. This key is used to decrypt the ESC firmware. After the firmware is loaded correctly, it checks the state of the conductive network by probing it at predefined frequencies.

The study of this principle was performed in the paper [20], using the experimental circuit presented above. For this principle to be effective, it is necessary for each conductive network to provide an unpredictable cryptographic key. The variation of the acquired values is determined by the quantization process of the ADC, the ATDC noise and the thermal response of the conductive network.

Considering the operational thermal range between the values $-20°C$ and $80°C$, the conductive network is characterized by an operational band, bordered by the maximum and minimum traces, as shown in figure 5.2.

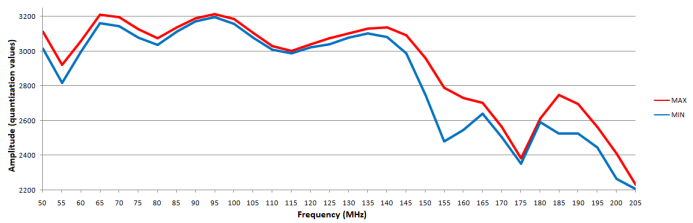
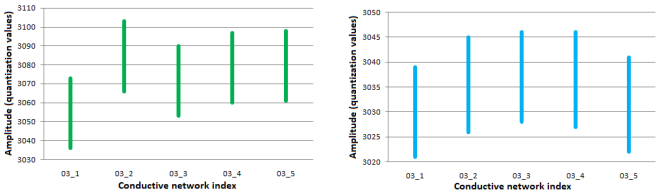


Figure 5.2: *Limits of values acquired at the output of the* $0.3mm$ *PCB conductive network, for temperature variations between* $-20°C$ *and* $80°C$.

Figure 5.4 exemplifies, for two values of the probing frequencies ($80MHz$

and $120MHz$), the response value ranges of the tested conductive networks, corresponding to the analyzed thermal range (between $-20°C$ and $80°C$).



(a) *PCB* $0,3mm$, $80MHz$.

(b) *PCB* $0,3mm$, $120MHz$.

Figure 5.4: *Examples of conductive network responses at 80MHz and 120MHz.*

Figure 5.4 shows that each tested conductive network has a unique answer, usable in setting up a cryptographic key. The cryptographic key can be obtained by dividing the amplitude space into $Q_{i,j}$ quanta, with i representing the frequency F_i and j representing the quanta number. Each quantum corresponds to a binary value, so that concatenating these values produces the cryptographic key K_D. This way of dividing the amplitude space is shown in figure 5.5.

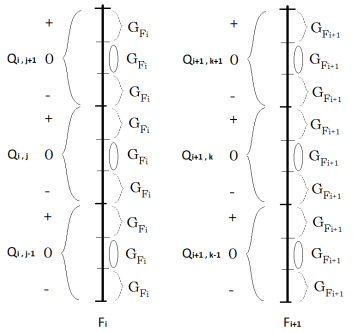


Figure 5.5: *Representation of the quantization domains corresponding to the probing frequencies of the conductive network* i *and* $i+1$.

This section proposes an innovative method of deriving cryptographic keys based on the amplitude-frequency output characteristic of the conductive network, a method that simplifies cryptographic systems by eliminating the need to store secret data, and ensures a high level of security for their internal processes. systems.

5.2 Authentication of electronic security circuits

Identification data, in the case of authentication, can be obtained from the response of the conductive network by quantizing it at discrete frequencies. The unique identification of the equipment containing a ESC, requires that the sequences obtained from the amplitude-frequency characteristic to be unique. To ensure the uniqueness, the following methods can be implemented: unique conductive networks, adding RLC elements, applying a HASH function, probing at different frequencies etc.

Chapter 6

Conclusions

This chapter summarizes the conclusions resulting from the research applied in the doctoral thesis. In the first section, the original contributions resulting from the research activity are listed. The second section contains the list of papers published by the author and the research reports from the doctoral program.

6.1 Original contributions

Chapter 2

1. I studied the types of attacks on electronic security circuits: cryptanalysis of cryptographic systems, side channel attacks and physical intrusions [11, 12, 13, 14, 15].
2. I emphasized the need to ensure the physical protection of electronic security circuits [11, 12, 13, 14, 15].

Chapter 3

1. I analyzed the characteristics of electronic security circuit protection systems against physical intrusions [11].
2. I have documented the role and types of conductive networks used in electronic security circuit protection systems [11, 12].
3. I analyzed the properties and disadvantages of passive intrusion detection circuits [11, 12, 13, 14, 15].
4. I studied the active intrusion detection circuits. We analyzed the principle of operation and the current stage of development [11, 12].
5. I have proposed a schematic diagram and a physical structure of the assembly consisting of the electronic security circuit and the intrusion detection circuit [11].

Chapter 4

Section 4.1

1. I made a conductive network consisting of a ground layer and a layer with conductive traces, intended for signal probing. The ground layer improves intrusion detection properties. It has two roles: reference plane for probing signals propagating through conductive traces and electromagnetic shield [1, 11].

Section 4.2

1. I designed an active tamper detection circuit consisting of a processing circuit, based on the STM32F407 microcontroller, and a conductive network interface circuit, consisting of hysteresis comparators [1, 11].
2. I established a method for generating probing pulses by using a LFSR pseudorandom sequence generator [1, 11].
3. I established a method for implementing probing pulses, characterized by their simultaneous generation at the two ports of the conductive network [1, 11].
4. The analysis of the probing pulses was implemented in a program executed in microcontroller [1, 11].
5. I tested the experimental intrusion detection circuit together with the double-layer conductive network and determined the intrusion detection and physical intrusion detection performances [1, 11].

Section 4.3

1. I designed an active intrusion detection circuit consisting of a processing circuit (STM32F746), an operational amplifier and an analog-to-digital converter with memory (ADC08B200) [1, 2, 11, 12].
2. I established the mode of analysis of the conductive network in order to detect intrusions, following two aspects: the delay and the power of the spectral components of the pulses [1, 2, 11, 12].
3. I have implemented tamper detection functions in the processing circuit program [1, 2, 11, 12].
4. I performed experimental tests with probing signals consisting of pulses of different durations to determine the optimal parameters for detecting intrusions and intrusion attempts (non-destructive damage to the conductive network) [1, 2, 11, 12].

5. The experimental testing of the pulse delay showed the performance of this system in the time domain [1, 2, 11, 12].

6. From the experimental testing in the frequency domain,there were determined the limits from which intrusion attempts can be detected [1, 2, 11, 12].

Section 4.4

1. For the active intrusion detection circuit, presented in section 4.3, I implemented two categories of electronic security circuit protection methods: temperature variation detection (at the level of the conductive network) and physical intrusion detection [1, 2, 3, 4, 11, 12, 13].

2. I analyzed the temperature variations by calculating the signal strength in the time domain [3, 13].

3. The detection of physical intrusions was performed by calculating the statistical parameters: mean, mean square root, standard deviation and variance [4, 13].

4. I analyzed the response of the conductive network to temperature variations in the range $-20°C \div 100°C$. The resulting graphic is quasi-linear, with a negative slope, and allows the detection of temperature variations. The detection of thermal attacks is implemented by establishing a field of operability [3, 13].

5. I extended the detection of physical intrusions to the detection of intrusion attempts by testing several values of resistors connected in series with the conductive network or of capacitors connected in parallel with it [4, 13].

6. Following the tests, values of resistances higher than 10Ω and values of capacitances higher than $10pF$ can be detected by calculating the statistical parameters root mean square, standard deviation and variance [4, 13].

Section 4.5

1. I proposed an innovative conductive network consisting of three conductive layers (ground layer, signal layer and detection layer), isolated by dielectric layers. The conductive traces that form the detection layer, exposed to the outside, are closed circuits [5, 14].

2. I established a way to probe the conductive network with signals in order to detect physical intrusions. An attacker cannot exhaustively determine the parameters of the sounding signals by analyzing the exposed conductive layer, thus making it impossible to simulate and inject false signals [5, 14].

3. I analyzed an equivalent circuit of conductive traces, which form the signal layer and the detection layer, inductively and capacitively coupled [5, 14].

4. I simulated a simple structure, formed by identical meanders, in order to obtain the output amplitude-frequency characteristic, in the following cases: unaffected network and physical intrusion (interruption of the conductive path of the detection layer) [5, 14]. The frequency range in which the simulation was performed was $0Hz \div 1GHz$.

5. The amplitude-frequency characteristics corresponding to the two cases differ substantially, by the appearance of two additional minimum points [5, 14].

6. I improved the previous conductive network by extending the surface covered by the conductive paths to a square with a side of $30mm$, formed by complex meanders [5, 14].

7. I simulated this improved structure to obtain the amplitude-frequency output characteristic, for the range $0Hz \div 500MHz$, corresponding to the cases where the detection layer is intact and the case where the trace on the detection layer forms an open circuit (intrusion) [5, 14].

8. Following the simulation, the characteristics corresponding to the two analyzed cases differ consistently at low frequencies, lower than $300MHz$ [5, 14]. This behavior is useful in designing active intrusion detection circuits because the detection and analysis of sounding signals does not require complex circuits.

9. We have exemplified a conductive network model, foil type, intended for the complete coverage of an electronic circuit (consisting of the electronic security circuit and the active intrusion detection circuit) [15].

10. I designed a conductive network consisting of two adjacent areas, with different models of conductive paths. I simulated and practically made them in the form of two circuits with a dielectric thickness of $0.3mm$ and $0.6mm$ [6, 15]. The frequency frequency range was $0Hz \div 500MHz$.

11. The simulations corresponding to the two types of circuits show measurable differences between the cases of unaffected network and the network on which an intrusion was made [6, 15].

12. Practical tests, performed under the same conditions, show a different behavior in frequency compared to simulations but the effect of intrusions is detectable to the same extent, starting with the frequency of $30MHz$ [6, 15].

13. The principle of the system formed by this conductive network and the active tamper detection circuit was proposed for publication in a patent application [16].

14. To highlight interruptions such as open circuits and short circuits between two adjacent traces (on the detection layer - 3), we simulated and tested these cases

for three types of conductive networks: PCB with a dielectric thickness of $0.3mm$, PCB with a dielectric thickness of $0.6mm$ and PES foil printed with conductive paste SW180 [7].

15. Simulations performed for the frequency range $0Hz \div 300MHz$ revealed the detection of open circuit intrusions for frequencies higher than $30MHz$ and the detection of short-circuit intrusions for higher frequencies [7].

16. The analysis of the circuits made practically showed that the conductive network of PES type, with dielectric of thickness $0.1mm$, is efficient starting with the frequency of $85MHz$, the conductive network of type PCB, with dielectric of thickness $0.3mm$, is efficient starting with the frequency of $35MHz$ and the conductive network type PCB, with dielectric of thickness $0.6mm$, is efficient starting with the frequency of $15MHz$ [7].

Section 4.6

1. I made the graphic design for the manufacture of screen printing screens necessary for printing the conductive network on PES foil with the help of DEK Horizon 08 equipment [15].

2. I performed the technological processes for printing PES foils with conductive paste SW180 [15].

3. I tested the integrity of conductive traces by bending under different radii of curvature. The conductive network, printed with SW180 paste by screen printing technology, allows bending with radii of at least $2mm$ [15].

4. This type of foil, together with the conductive paste SW180, is a suitable solution for the manufacture of conductive networks for signal characteristics and controlled friability, necessary for protection against intrusions [15].

Section 4.7

1. I designed an active tamper detection circuit specialized for probing and analyzing the previously researched triple layer conductive network [8, 9]. The structure is simple and minimal for optimizing size and consumption: a microcontroller with low power consumption, a programmable oscillator and a logarithmic amplifier.

2. I established the principle of intrusion detection and developed the application running in the microcontroller. Conductive networks were probed with radio pulses (sinusoidal signal trains) with frequencies in the range of $50MHz \div 205MHz$ [8, 9].

3. I experimentally tested the assembly consisting of the active tamper detection circuit and the conductive network. I used the three types of conductive networks investigated in section 4.5 (PES foil with a thickness of $0.1mm$ printed with conductive paste SW180, PCB with a dielectric thickness of $0.3mm$ and PCB with a dielectric thickness of $0.6mm$) . The tests performed aimed at both physical intrusions (interruption of the detector circuit, short circuit between adjacent traces of the detector circuit) and the detection of temperature variations, especially exceeding the operational thermal limits [8, 9].

4. Tests for physical intrusions revealed the detection of the four types of intrusions analyzed (open circuit, respectively, short circuit in zones 1 and 2) in most test frequencies [8, 9].

5. I performed the tests for detecting temperature variations in the thermal range $-20°C \div 80°C$. The analyzed system can detect temperature variations in the subdomains of the frequency range used. It is important that the paths corresponding to the extreme temperatures ($-20°C$ and $80°C$) fit the paths of the intermediate temperatures. Detection of attacks on thermal collateral channels can be detected in a range of frequencies [8, 9].

6. Given that the active tamper detection circuit must respond to the two types of attacks analyzed, we identified the frequencies at which the conductive network can simultaneously detect physical intrusions and exceeding operational thermal limits. Thus, in more than 80% of the analysis frequencies the system was effective in detecting the two types of attacks [8, 9].

Section 5.1

1. I identified a procedure for securing firmware programs based on the properties of the studied triple layer conductive networks. From the probing with signals of the conductive network, a cryptographic key is processed with which the firmware is encrypted [6, 10, 15].

2. This method of protecting the firmware does not require the use of a backup power source designed to ensure the uninterrupted operation of the active tamper detection circuit [6, 10, 15].

Section 5.2

1. I have identified a security circuit authentication procedure based on obtaining a unique identity from the output amplitude-frequency characteristic of the triple layer conductive network [7, 15].

2. I proposed several methods to increase the dispersion of this feature to ensure the unique identities of electronic security circuits [7, 15].

6.2 List of original works

Scientific papers published at scientific conferences and research reports presented during the doctoral program are:

1. **D. C. Vasile, A. Marghescu, P. Svasta**, *Improved tamper detection circuit based on linear-feedback shift register*, 2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Oradea, Romania, 2016, DOI: 10.1109/SIITME.2016.7777261.

2. **D. C. Vasile, P. Svasta, N. Codreanu, M. Safta**, *Active tamper detection circuit based on the analysis of pulse response in conductive mesh*, Jubilee 40th International Spring Seminar on Electronics Technology, ISSE 2017, Sofia, Bulgaria, 2017, DOI: 10.1109/ISSE.2017.8000987.

3. **D. C. Vasile, P. Svasta**, *Temperature Sensitive Active Tamper Detection Circuit*, 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, Romania, 2017, DOI: 10.1109/SIITME.2017.8259885.

4. **D. C. Vasile, P. Svasta**, *Active Tamper Detection Circuit Based on Statistical Analysis*, 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, Romania, 2017, DOI: 10.1109/SIITME.2017.8259884.

5. **D. C. Vasile, P. Svasta**, *Innovative Conductive Mesh Structure for the Protection of Security Electronic Circuits*, 2018 7th Electronic System-Integration Technology Conference (ESTC), Dresden, Germany, 2018, DOI: 10.1109/ESTC.2018.8546366.

6. **D. C. Vasile, P. Svasta**, *Antitamper Conductive Mesh Used for Securing Cryptographic Modules*, 2018 IEEE 24th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Iași, Romania, 2018, DOI: 10.1109/SIITME.2018.8599284.

7. **D. C. Vasile, P. Svasta**, *Innovative Authentication Method for IoT Devices*, 2019 22nd European Microelectronics and Packaging Conference & Exhibition (EMPC), IEEE, Pisa, Italy, 2019, DOI: 10.23919/EMPC44848.2019.8951767.

8. **D. C. Vasile, 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, Cluj-Napoca, Romania, 2019, DOI: 10.1109/SIITME47687.2019.8990877.

9. **D. C. Vasile, P. Svasta, 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, Cluj-Napoca, Romania, 2019, DOI: 10.1109/SIITME47687.2019.8990788.

10. **D. C. Vasile, S. Chițu, P. Svasta**, *Criptographic Key Derivation from an Anti-Tamper Solution*, 2020 8th Electronic System-Integration Technology Conference (ESTC), Vestfold, Norway, 2020 (work in progress).

11. **D. C. Vasile**, *Active tamper detection system for the protection of electronic security circuits*, Research Report no. 1, 2017.

12. **D. C. Vasile**, *Active tamper detection circuit based on the analysis of the impulse response of the conductive network*, Research Report no. 2, 2017.

13. **D. C. Vasile**, *Active tamper detection circuit with dual function: temperature variation detection and intrusion detection by statistical methods*, Research Report no. 3, 2018.

14. **D. C. Vasile**, *Innovative conductive network for the protection of electronic security circuits*, Research report no. 4, 2019.

15. **D. C. Vasile**, *Securing electronic security circuits: innovative conductive network for intrusion detection*, Research Report no. 5, 2019.

16. **D. C. Vasile, P. Svasta**, *Conductive network for the protection of electronic security circuits against physical intrusions*, Patent Application A / 00609, September 30, 2019.

Bibliography

[1] H. C. A. Van Tilborg. *Encyclopedia of cryptography and security*. Springer Science and Business Media, 2014.

[2] D. Gritzalis, M. Theocharidou, and G. Stergiopoulos. *Critical Infrastructure Security and Resilience - Theories, Methods, Tools and Technologies*. Springer, 2019.

[3] N. P. Smart. *Physical side-channel attacks on cryptographic systems*. Software Focus 1.2, 2000.

[4] Y. Souissi, J. L. Danger, S. Guilley, S. Bhasin, and M. Nassar. *Embedded systems security: An evaluation methodology against side channel attacks*. Proceedings of the 2011 Conference on Design & Architectures for Signal & Image Processing (DASIP) IEEE, 2011.

[5] National Institute of Standards and Technology (NIST). *Security Requirements for Cryptographic Modules, FIPS 140-2*. 2001.

[6] Enevoldsen, M. T. and West, T. T. and Wesselhoff E. and Rasmussen, J. and Mikkelsen, D. B. *Security module for protection circuit components from unauthorized access, U.S. Patent No. US 10,009,995 B2*. 2018.

[7] D. C. Vasile, A. Marghescu, and P. Svasta. *Improved tamper detection circuit based on linear-feedback shift register*. 2016 IEEE 22nd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Oradea, România, 2016.

[8] A. Marghescu, P. Svasta, and Simion E. *High Speed and Secure Variable Probability Pseudo/True Random Number Generator Using FPGA*. 2015 IEEE 21st International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Oradea, România, 2015.

[9] Texas Instruments. *TLV350x 4.5-ns, Rail-to-Rail, High-Speed Comparator in Microsize Packages*. `http://www.ti.com`, 2016.

[10] Kay, A. and Claycomb, T. *Comparator with Hysteresis Reference Design, TIDU020A, Texas Instrumens*. `http://www.ti.com`, 2014.

[11] D. C. Vasile, P. Svasta, N. Codreanu, and M. Safta. *Active tamper detection circuit based on the analysis of pulse response in conductive mesh*. Jubilee 40th International Spring Seminar on Electronics Technology, ISSE 2017, Sofia, Bulgaria, 2017.

[12] D. C. Vasile and P. Svasta. *Temperature Sensitive Active Tamper Detection Circuit*. 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, România, 2017.

[13] D. C. Vasile and P. Svasta. *Active Tamper Detection Circuit Based on Statistical Analysis*. 2017 IEEE 23rd International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, Constanța, România, 2017.

[14] 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.

[15] 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, Iași, România, 2018.

[16] D. C. Vasile and P. Svasta. *Rețea conductivă de protecție a circuitelor electronice de securitate împotriva intruziunilor fizice*. Cerere de brevet de invenție A/00609, Oficiul de Stat pentru Invenții și Mărci, 30 septembrie 2019.

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

[18] 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, Cluj-Napoca, România, 2019.

[19] 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, Cluj-Napoca, România, 2019.

[20] D. C. Vasile, S. Chițu, and P. Svasta. *Cryptographic Key Derivation from an Anti-Tamper Solution*. 8th Electronics System-Integration Technology Conference (ESTC), Vestfold, Norvegia, 2020.