SIDE CHANNEL ATTACK PERFORMANCE OF CORRELATION POWER ANALYSIS METHOD IN NOISE

*Fikret Garipay(1), Kemal Uzgören(2), İsmail Kaya(3) **

(1) CyberPath Training Ltd. Inc. Ankara; (2) Komtel Electronic Ltd. Inc. Trabzon;
(3) Karadeniz Technical University, Trabzon
Turkey

* Corresponding Author, or, e-mail: *ikaya@ktu.edu.tr*

Abstract: This article explores the use of artificial noise to defend against power analysis and power analysis-based side-channel attacks on AES encryption. The study covers both hardware and open-source software components for performing power analysis and provides an analysis of attack performance. It also explains how security measures against side-channel attacks can be implemented without disrupting system operation.

Key words: Side-Channel Attack, Software Security, Embedded Security, Correlation Power Analysis, Artificial Noise.

1. INTRODUCTION

Cryptography is a method for securing information by converting it into a format that is unreadable without the proper key. This process involves the use of mathematical functions for both encryption and decryption, which are based on a specific key value [1]. However, the use of semiconductor materials in hardware can cause weaknesses in these techniques. Paul Kocher [2] was one of the first to study the area of power analysis exploiting these weaknesses, followed by Thomas Messerges et al. [3] who introduced the differential power analysis (DPA) method. To counter side-channel attacks, Rambus offers protection methods such as the DPA Software Library, DPA Resistant Hardware Core, and DPA Workstation. The company provides libraries to design hardware that is resistant to side-channel attacks. NewAE Technology Inc. provides security training for embedded systems and applications to understand side-channel attacks.

A side-channel attack using a security vulnerability in a microprocessor or system that tries to uncover information by measuring and analyzing various parameters of known cryptography methods, such as AES encoding. However

attackers are able to detetct the encryption method as well. Although the detection of the encryption method is not covered in this paper.

The methods used in side-channel attacks include timing measurements [4, 5], electromagnetic emission [6], and power consumption [2]. This study focuses on power analysis-based side-channel attacks, which are one of the most aggressive forms of attack, as they monitor the system's power consumption. To avoid power analysis-based attacks, software and hardware measures must be taken, as it is impossible to prevent the system's power consumption.

The study evaluates the performance of side-channel attacks made using conventional power analysis methods with added artificial noise to the power supply. The study aims to develop a noise protection method that adds noise to the source when the AES keys are resolved by the program and analyzes its performance. The designed method allows the processor to operate with a standard power supply at all other times.

2. POWER ANALYSIS ATTACKS

Power analysis is a type of side-channel attack that assesses the power consumption of a microprocessor or system [2]. The power consumption of electronic systems fluctuates based on the data processed in the system or the operations performed. The attacker can use various power measurement techniques to find the key, and if needed, analyze the power consumption during encryption. This is done by sending known plain texts to the target system and measuring the power consumption. Subsequently, the power consumption measures are analyzed using Simple Power Analysis (SPA), Differential Power Analysis (DPA), or Correlation Power Analysis (CPA). This results in the attacker gaining information about the encryption process.

SPA, or Simple Power Analysis, looks at changes in power consumption during cryptography by comparing obtained power samples from target microcontroller unit (MCU). DPA, or Differential Power Analysis, focuses on the dynamic power consumption caused by data flow within the system, taking into account the Hamming weight and its relationship with power consumption and the number of 0s and 1s in a byte.

In this study, the resilience of the Correlation Power Analysis (CPA) side-channel attack method is evaluated. CPA is preferred over SPA and DPA because it can generate more accurate results by computing the correlation coefficient between the power samples and actual power consumption, providing a more in-depth examination of the data.

2.1. Correlation Power Analysis (CPA)

CPA is an advanced form of DPA, which involves calculating the correlation coefficient between the power samples collected and the actual power consumption for each byte. This enables the correlation between the subcode guesses and the

measured traces to be determined. The calculation requires a model of the bit changes in the system, with the simplest being the Hamming distance (W) model, which is related to the Hamming weight model. The Hamming distance is calculated by XORing the subsets of the Hamming weight, using the formula below with subsets M and R.

$$W(M,R) = HW(M \oplus R) \tag{1}$$

In the real case with N power curves for prediction, random data words M_i associated with, W_i and, N. Known data words for a given reference state, R, $H_{i,R} = H(M_i \oplus R)$ produce a set of estimated Hamming distances, N. Estimation of the ρ_{WH} correlation factor is as follows [14].

$$\rho_{WH}(R) = \frac{N \sum W_i H_{i,R} - \sum W_i H_{i,R}}{\sqrt{N(\sum W_i^2 - (\sum W_i)^2}\sqrt{N(\sum H_{i,R}^2 - (\sum H_{i,R})^2}} \tag{2}$$

Correlation power analysis allows the depreciation of the complexity of the attack. For example, a 128-bit AES key has a probability of 2^{128}. It is not possible to try this number of possible keys. Therefore, it is not possible to perform a brutal force channel attack. When we use a CPA Side Channel Attack, each subkey size is 1 byte. A byte has 2^8 possibilities Since the size of the entire password is 16 bytes, the probability is calculated as 2^{12} from $2^8 \times 2^4$. This calculated probability value creates a testable result based on a brute-channel attack.

3. AN ENHANCED CARD FOR SIDE-CHANNEL ATTACKS: CHIPWHISPERER NANO

The study utilized the ChipWhisperer-Nano[7], produced by NewAE, for side-channel power analysis. The ChipWhisperer-Nano is a low-cost, external power consumption analyzer and Voltage Glitching device, as depicted in Figure 1. It consists of two components: a measurement part and a target part featuring an STM32F030 microcontroller, connected to the measurement part via a power connection resistor series. However, since the STM32F030 microcontroller does not have an internal Digital to Analog Converter (DAC), the study employed the STM32L432KC[8] microcontroller with a 5 Ms/s DAC (shown in Figure 1) as the external target. The measurement part includes an 8-bit Analog to Digital Converter (ADC) from Texas Instruments, which can sample up to 20MS/s and perform power measurements for side-channel attacks. The ADC samples using either the external target device clock or internal synchronous/asynchronous clock, and a low-cost amplifier is used to amplify the power signals before they are sampled, since noise power is not very significant in comparison to main power supply. The device also features a positive edge-triggered flip-flop from Texas Instruments and a CMOS Clock Buffer from Skyworks for Clock Routing and selection. The Multiplexer has two clock inputs, one from the internal 12 MHz crystal oscillator in the measurement

part and the other from an external clock. The ChipWhisperer Nano employs a Microchip SAM 4S16 microcontroller for communication with the host via USB and sample storage, with firmware written by ChipWhisperer to interact with the host's Python API and perform side-channel attacks. However, due to hardware restrictions in transmitting the ADC samples over USB in real-time, the number of samples that can be taken from the target device is limited to 50,000 by the RAM capacity of the microcontroller. The device boasts a key feature of Synchronous Capture technology, allowing for loop-accurate signal measurement and outperforming a standard asynchronous oscilloscope by taking fewer samples in synchronous mode. It is designed for external target attacks, either by cutting from the indicated red column line on the PCB or by cutting the series resistors at the target device's power supply input.

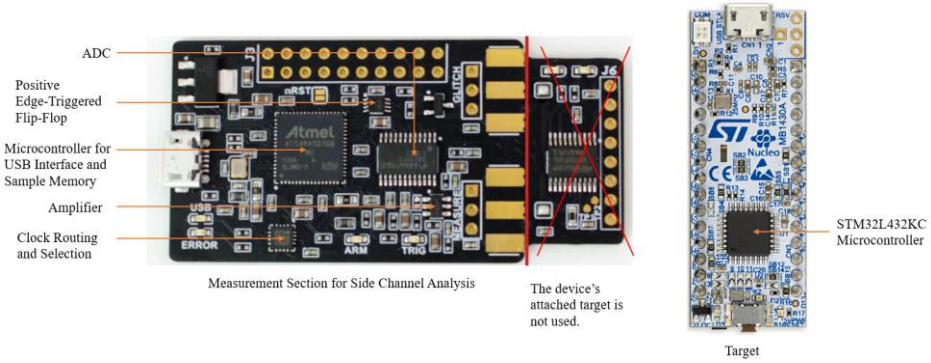

Figure 1. A picture of ChipWhisperer Nano Power Analysis Device and Target Nucleo Board

3.1. ChipWhisperer Software

The ChipWhisperer software [9] is a set of open-source tools designed for hardware security researchers. It includes hardware components (ChipWhisperer cards) to measure from target devices, firmware written in C for microcontrollers, and a Python library that enables communication between the ChipWhisperer hardware and the host [10] computer. This setup allows for various side-channel attacks to be created using the Python API on the target device.

4. IMPLEMENTATION OF SIDE-CHANNEL ATTACK

In the diagram shown in Figure 2, power measurements were made with the ChipWhisperer Nano in the system used for measurements over the serial resistance at the power input of the target microcontroller. For syntetic noise injection, the DAC output of the target microcontroller is connected to the power input of the microcontroller, and it is aimed to mask the information arising from the noise at the input of the microcontroller. DC signals at the DAC output are filtered with a DC blocking capacitor.

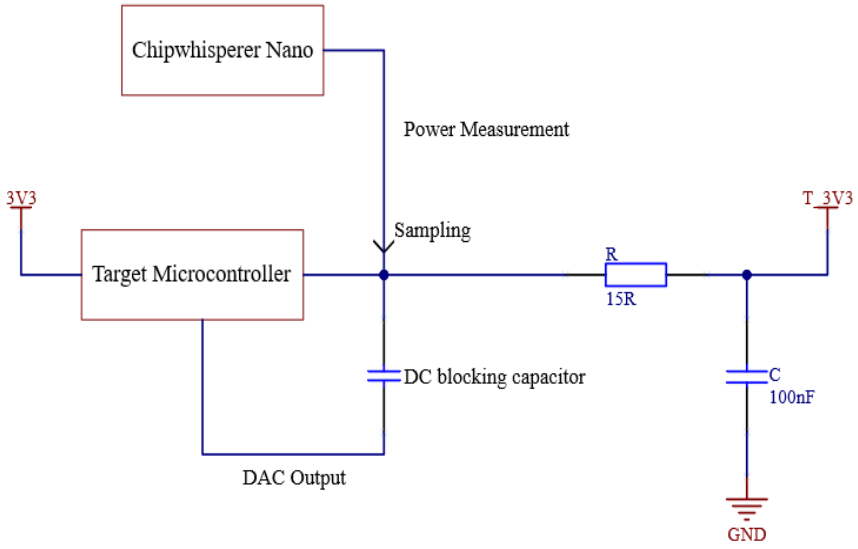

Figure 2. Connection Circuit of ChipWhisperer Nano and target Target Microcontroller for preventing CPA Side Channel Attack by syntetic noise.

4.1. Designing the Noise to be Created by Software Control

In this study, the embedded software was developed using the STM32CubeMX software and the ARM GCC compiler. The software was designed to run on the STM32L432KC microcontroller, and it utilized a C-programmed AES encoder named Tiny-AES[11] with 128-bit AES keys. A special design was created for the STM32L432KC microcontroller to implement the side-channel analysis attack. The microcontroller was equipped with a DAC component, which was used to generate white noise through the configurable White Noise Generator provided by STM[12]. This generated noise was uniformly distributed, with a flat spectral distribution, but it was not Gaussian.

The white noise produced by the White Noise Generator had an output voltage of $256mV$. However, for the tests conducted in this study, higher mV values were required, and thus the magnitude of the noise was adjusted using a gain defined in Figure 3 of the block diagram. The output voltage of the DAC was calculated using the equation:

$$v_{out} = v_{White\ Noise} * gain \quad (3)$$

The frequency of the signal generated at the DAC output of the microcontroller was controlled by the divider, which was dependent on the timer component. The frequency was determined using the following expression:

$$f_{DAC} = \frac{f_{Timer}}{Prescaler} \quad (4)$$

During the operation of the AES algorithm, the signal generated at the DAC output of the STM32L432KC microcontroller was applied to the power input of the microcontroller. The software block diagram for the microcontroller is shown in Figure 3.

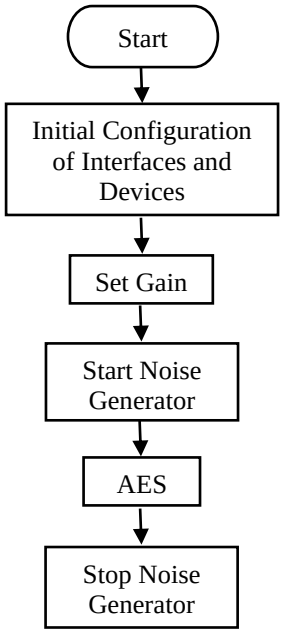

Figure 3. Block Diagram of the Developed Algorithm for for preventing CPA Side Channel Attack by syntetic noise.

5. CPA TEST RESULTS

As the AES algorithm was executed on the STM32L432KC target microcontroller, the tests began to apply white noise starting at $1mV$. The CPA Side Channel Attack recorded the first incorrect AES subkeys when a noise value of $512mV$ was introduced. As the noise level increased, the CPA Side Channel Attack's calculation errors also increased exponentially At $910mV$, the CPA Side Channel Attack miscalculated all AES subkeys. The results of the analysis performed by the ChipWhisperer-Nano system were recorded and represented in Figures 4, 5, and 6.

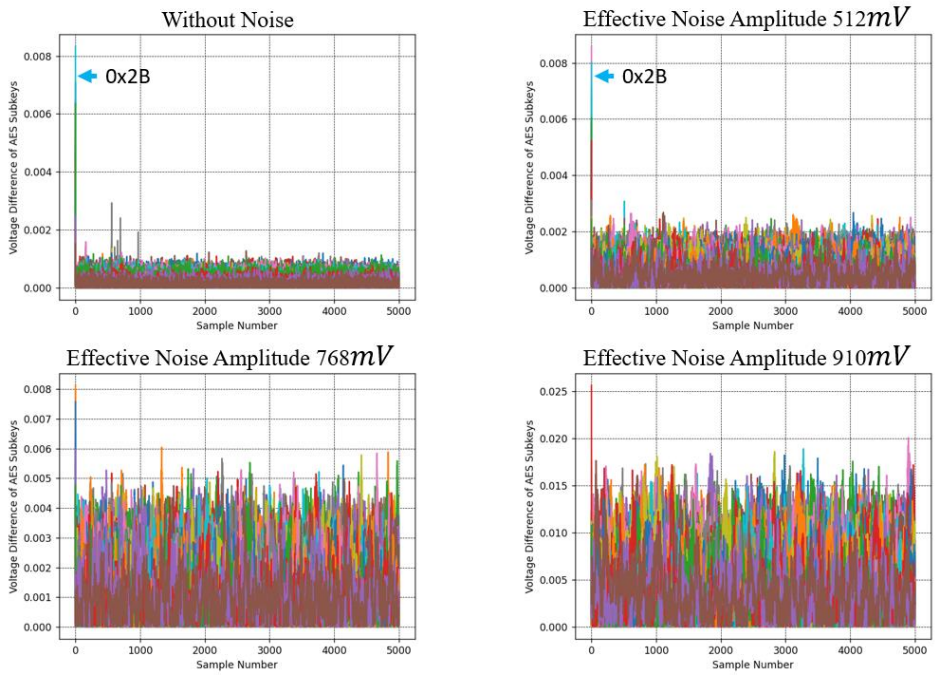

Figure 4. It displays graphs depicting the values recorded by ChipWhisperer-Nano while the AES algorithm was being executed on the STM32L432KC microcontroller, with variations in power input and noise levels. The AES subkeys, ranging from 0x00 to 0xFF, are depicted using different colors. The corret subkey AES subkey 0x2B, is represented in light blue.

Figure 4 specifically shows the results of the Side Channel Attack with noise injection. The correct AES subkey (0x2B) was depicted in light blue, while the other AES subkeys from 0x00 to 0xff were shown in different colors. When the tests were performed in a noiseless environment, it was observed that the power difference generated by the correct subkey was significantly higher compared to the other subkeys. As the noise level was increased to $512mV$, the effect of noise injection on the other subkeys was evident, with an increase in power values. However, even with the added noise, the correct AES subkey still generated a higher power value, and the first subkey was successfully obtained through the Side Channel Attack. At the highest noise levels of $768mV$ and $910mV$, the power consumption difference created by the switches was effectively masked by the noise, as the AES subkeys from 0x00 to 0xff had similar power consumption values.

The results of the Side Channel Attack with masked power input information can be seen in Figures 5 and 6. At the start of the tests, when the power input information was not masked, the success rate of the CPA Side Channel Attack was 100%. However, as the noise level was increased, starting from $512mV$, the success

rate started to decrease exponentially. At the highest noise level of $910mV$, no correct AES subkey could be obtained, and the success rate of the CPA Side Channel Attack was reduced to 0%, as shown in Figure 5 in volts. Figure 6 is the signal to noise representation of injectdet syntetic noise, while the power supply voltage of target CPU is equal to 3.3 Volts.

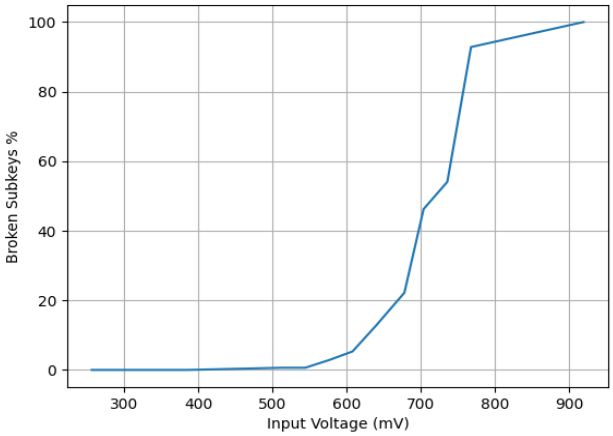

Figure 5. The number of incorrect AES subkeys obtained in CPA Side Channel Attack tested with 320 different AES subkeys between $256mV$-$910mV$ *values.*

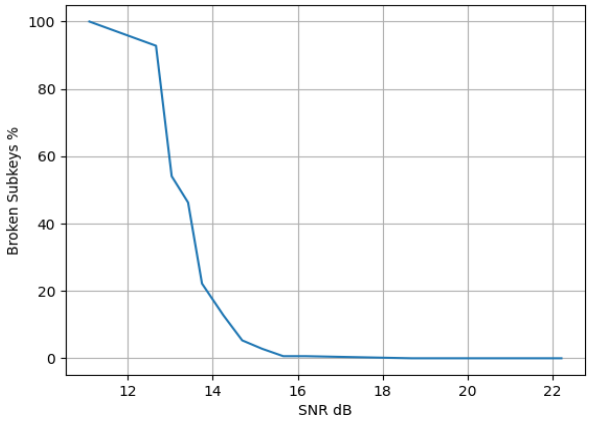

Figure 6. The noise power converted to signal to noise ratio (SNR) using the 3.3 volts of CPU power supply from Figure 5.

It has been established through the conducted experiments that the application of noise to mask the power input information of the target microcontroller effectively reduces the success rate of CPA Side Channel Attacks.

6. CONCLUSION

This paper explores the power analysis type of side-channel attack and its vulnerability when an artificial noise is added to the power supply. The results showed that injecting noise at a level of $12\,dB$, which does not impact digital operations, effectively prevented security keys from being obtained via correlation-based power analysis (CPA). This highlights the potential for systems to prevent attacks by adding noise to the power supply through a DAC unit or an external noise source. While this does not guarantee complete security, it provides an additional barrier for attackers. The authors view their noise analysis, which assesses the performance of a CPA Side Channel Attack, as a noteworthy contribution and a foundation for the development of more effective side-channel attack prevention methods.

As a future work, a software-controlled circuit that can randomly draw power can be added to microcontroller design, making it possible to develop and validate this study within an FPGA. This way, more secure designs (IPs) can be created for Side Channel Attacks in microcontroller and FPGA systems.

ACKNOWLEDGEMENT

The authors thank Zübeyir Durğut and Yeşim Er for their technical and theoretical support for this study.

REFERENCES

[1] Schneier, B, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, 1996, (758 p.)

[2] Kocher, P., Jaffe, J., & Jun, B. Differential power analysis. In *Annual international cryptology conference*. Springer, Berlin, Heidelberg, 1999, pp. 388-397. DOI: 10.1007/3-540-48405-1_25

[3] Messerges, T. S., Dabbish, E. A., & Sloan, R. H. Investigations of Power Analysis Attacks on Smartcards. In *USENIX Workshop on Smartcard Technology*. Chicago, Illinois, USA, 1999, pp. 151-161.

[4] Kocher, P. C. Kocher, P. C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference*. Springer, Berlin, Heidelberg, pp. 1996, 104-113.

[5] Dhem, J. F., Koeune, F., Leroux, P. A., Mestré, P., Quisquater, J. J., & Willems, J. L. A practical implementation of the timing attack. In *International Conference on Smart*

Card Research and Advanced Applications. Springer, Berlin, Heidelberg, 1998, pp. 167-182.

[6] Van Eck, W. Electromagnetic radiation from video display units: An eavesdropping risk?. *Computers & Security*, vol.4, no.4, 1985, pp. 269-286. DOI: 10.1016/0167-4048(85)90046-X

[7] NewAE, *Cw1101 ChipWhisperer-Nano*. URL: https://rtfm.newae.com/Capture/ChipWhisperer-Nano/#cw1101-chipwhisperer-nano (Visited on 26.12.2022).

[8] STMicroelectronics, *Stm32l432kb stm32l432kc*, 2018. URL: https://www.st.com/resource/en/datasheet/stm32l432kc.pdf, (Visited on 26.12.2022).

[9] NewAE, *Overview*. URL: https://chipwhisperer.readthedocs.io/en/latest/getting-started.html (Visited on 26.12.2022).

[10] ChipWhisperer, *ChipWhisperer Software*. URL: https://pypi.org/project/chipwhisperer/ (Visited on 26.12.2022).

[11] kokke, *tiny-aes*. 2021, URL: https://github.com/kokke/tiny-AES-c (Visited on 26.12.2022).

[12] STMicroelectronics, *An3126 application note*, 2020. URL: https://www.st.com/resource/en/application_note/an3126-audio-and-waveform-generation-using-the-dac-in-stm32-products-stmicroelectronics.pdf (Visited on 26.12.2022).

[13] Kocher, P., Jaffe, J., Jun, B. et al. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, no 1, 2011, pp. 5–27. DOI: 10.1007/s13389-011-0006-y

[14] Brier, E., Clavier, C., & Olivier, F. Correlation power analysis with a leakage model. In *International workshop on cryptographic hardware and embedded systems*. Springer, Berlin, Heidelberg, 2004, pp. 16-29. DOI: 10.1007/978-3-540-28632-5_2

[15] Duan, X., Cui, Q., Wang, S., Fang, H., & She, G. Differential power analysis attack and efficient countermeasures on PRESENT. In *2016 8th IEEE International Conference on Communication Software and Networks (ICCSN)*, Beijing, China, 2016, pp. 8-12. DOI: 10.1109/ICCSN.2016.7586627

[16] van Woudenberg, J., & O'Flynn, C. *The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks*. No Starch Press. 2021.

[17] Gamaarachchi, H., & Ganegoda, H. *Power Analysis Based Side Channel Attack*. CO411/2: Individual Project I & II – Report, 2018. URL: https://arxiv.org/abs/1801.00932, DOI: 10.48550/arXiv.1801.00932 (Visited on 26.12.2022).

[18] Hnath, W., & Pettengill, J. *Differential power analysis side-channel attacks in cryptography*. Major Qualifying Project, Worcester Polytechnic Institute. URL: https://digital.wpi.edu/show/zg64tn24r (Visited on 26.12.2022).

[19] Rambus, *Protecting Electronic Systems from Side-Channel Attacks* (Ebook). URL: https://www.rambus.com/security/dpa-countermeasures/ (Visited on 26.12.2022).

[20] Rambus, *Introduction to Side-Channel Attacks* (Ebook). URL: https://www.rambus.com/security/dpa-countermeasures/ (Visited on 26.12.2022).

[21] ChipWhisperer, *ChipWhisperer Hardware*. URL: https://pypi.org/project/chipwhisperer/ (Visited on 26.12.2022).

[22] STMicroelectronics, *An4230 application note*, 2022. URL: https://www.st.com/resource/en/application_note/dm00073853-stm32-microcontroller-random-number-generation-validation-using-the-nist-statistical-test-suite-stmicroelectronics.pdf (Visited on 26.12.2022).

Information about the authors:

Fikret Garipay – Fikret Garipay is working as Software Engineer at CyberPath Training. His areas of interest are Embedded Systems, Telecommunication Systems, and Cloud.

Kemal Uzgören – Kemal Uzgören is working as Hardware Engineer at Komtel Electronic. His areas of interest are Embedded Systems and Telecommunication Systems.

İsmail Kaya – İsmail Kaya is a Professor in The Department of Electrical and Electronics Engineering at Karadeniz Technical University. He is the head of the Telecommunication Research group in the same department.

Manuscript received on 7th January 2023
Revised paper received on 5 February 2023