Design of Side-Channel-Resistant Electromagnetic Band-Gap on IoT Microcontroller

Chung-Wei Kuo[*]*, Kuo-Yu Tsai*

Department of Information Engineering and Computer Science,
Feng Chia University,
Taiwan
cwkuo@mail.fcu.edu.tw, kytsai@fcu.edu.tw

Abstract

To ensure the security of electronic devices and to meet the requirements for data confidentiality, integrity, and accessibility, systems often utilize a combination of cryptographic techniques and communication protocols. However, devices that employ encryption mechanisms are vulnerable to side-channel attacks (SCA), which could potentially allow unauthorized access to original data. Despite advancements in encryption algorithms, the challenge of safeguarding against key theft remains significant. Our proposed solution introduces a novel approach that uses periodic structure techniques, emphasizing a shielding design with electromagnetic band-gap (EBG) characteristics. This shielding is strategically positioned on IoT device microcontrollers to defend against SCA while maintaining message transmission within the 2.4 GHz Wi-Fi frequency range. Furthermore, we have established a comprehensive SCA system to validate the security of AES-128 encrypted transmissions. In scenarios where microcontrollers lack protective mechanisms, capturing fewer than 40 traces of encrypted signals can compromise the encryption key. However, our innovative EBG structure, designed to shield specific frequency bands, ensures that encryption keys are securely protected, even when subjected to analysis involving more than 20,000 signal traces.

Keywords: Side-Channel Attack, Periodic Structure, Electromagnetic band-gap, IoT, AES

1 Introduction

Information technology analytics projects significant growth in the global market of Internet of Things (IoT) businesses to reach $525 billion from 2022 to 2027 including hardware, software, services, security, communication, and so on, which highlights the expanding range of IoT applications [1]. In recent years, significant growth has been observed in sectors such as smart cities, energy management, smart homes, healthcare, smart agriculture, and advanced retail, drawing considerable attention. The impact of IoT on people's daily routines is increasing rapidly due to a broad range of applications. For instance, smart cities utilize a range of sophisticated tools to monitor their environment, such as image surveillance, temperature and humidity sensors, gas detectors, optical sensors, pressure sensors, infrared detectors, and other similar devices.

Essential environmental data can be gathered via communication serial ports built into microcontroller chips and general-purpose input/output for sending and receiving control signals. IoT management systems consolidate and analyze collected data to provide valuable insights to system administrators, control teams, or end-users [2]. The key of achieving smart goals in IoT environment is to create appropriate responses and actions. The Universal Asynchronous Receiver/Transmitter (UART) is frequently employed for signal exchange when transmitting control signals to sensor components, control devices, or users' mobile devices. Wireless transmission technologies such as Wi-Fi, Bluetooth, LoRaWAN, etc., are utilized during transmission, with all methods incorporating control signals or essential authentication messages to establish secure communication.

Regrettably, although intended to simplify and enhance efficiency, the fundamental technical features of IoT devices have inadvertently spawned four cybersecurity risks [3].

- Collecting abundant data: In the realm of the IoT, sensors, and devices gather vast amounts of environmental and user data with great precision which is essential for IoT operations. If collected data is not correctly protected, severe consequences will occur due to cybersecurity breaches.
- Integrated physical and virtual environments: Several applications rely on environmental signals to start actions, providing convenience and exposing vulnerabilities to potential harm from online threats.
- Creating complex scenarios: The world of IoT, designed for user convenience, has paved the way for a diverse array of interconnected devices. As this network continues to grow, IoT enriches the scope of environmental data and amplifies its potential consequences on a grander scale.
- Centralized architectural approach: Centralizing all

*Corresponding Author: Chung-Wei Kuo; Email: cwkuo@mail.fcu.edu.tw
DOI: https://doi.org/10.70003/160792642025092605009

device and sensor data into a central hub improves control and response coordination. Nevertheless, information exchange in such a structure also broadens attack surface, causing IoT to become vulnerable to security breaches.

When confronted with a cybersecurity attack, critical information or control signals can be decrypted or tampered with which could lead to unusual behaviors in IoT devices at the least, and, in more severe cases, unauthorized surveillance or pilferage of sensitive internal data. To mitigate security risks, IoT device manufacturers need to consider preventive measures spanning both software and hardware realms. Ensuring the integrity of information within IoT systems to thwart forgery, theft, manipulation, invasion, and other potential risks becomes paramount.

On the software front, traditional defenses such as firewalls, antivirus tools, and access controls can be implemented within IoT systems to mitigate potential attacks. Utilizing advanced measures, such as machine learning or artificial intelligence models, can help identify the sources of attacks. defending against hardware-based attacks, illustrated by the following three instances, presents more complex challenges:

- Invasive attacks: By physically breaching chip encasements to inspect internal circuitry and gauge device connections, attackers can gather transmitted data.
- Non-invasive attacks: Employing high currents or potent electromagnetic waves to disrupt chip functions triggers errors in chip behavior, enabling attackers to scrutinize stored data content. An alternative approach involves external components measuring voltage or current fluctuations in the chip's power or ground lines. Electromagnetic probes can capture radiation generated during chip operation, permitting the analysis of transmitted data content to extract distinct features and confidential information [4].
- Semi-invasive attacks: Falling between invasive and non-invasive techniques often involves firmware attacks or fault injections compelling chips into abnormal behavior. This momentarily disables the original security mechanisms. During this encrypted timeframe, attackers intercept and scrutinize the desired information.

To tackle the aforementioned challenges, we propose an electromagnetic shielding structure to thwart side-channel attacks (SCA). The proposed structure obstructs leakage of electromagnetic radiation signals produced during microcontroller operations, thus shielding IoT device signals from interception and fortifying hardware security.

2 Background

In the realm of hardware attacks, Shwartz et al. use invasive reverse engineering techniques that include making contact with the signal pins on the device's internal chip using specialized probes. They discuss how commonly used components in IoT environments, such as a control module and a cloud camera mode, can utilize voltage or current probes to intercept UART signals, which are then subjected to analysis [5]. Unintentional exposure of image data or personal information can occur within IoT control system. However, Wang et al. take a different approach by implementing a far-field antenna positioned 15 meters away from the scrutinized device as shown in Figure 1 [6]. Wang et al.'s arrangement permits interception of encrypted signal traces and ultimately leads to successful decryption of security keys [6]. Yuan utilizes artificial intelligence (AI) technology via a training model to analyze electromagnetic signal traces emitted during the execution of each instruction within the control chip's instruction set architecture [7]. Yuan's method, depicted in Figure 2 and Figure 3, allows for the deduction of numerous instructions being executed by the control chip [7], and these findings present a significant challenge to IoT device security, with the potential for data breaches, device malfunctions, network interruptions, or unauthorized access to sensitive information. The results above represent a serious threat to the security of the relevant equipment supply chain.

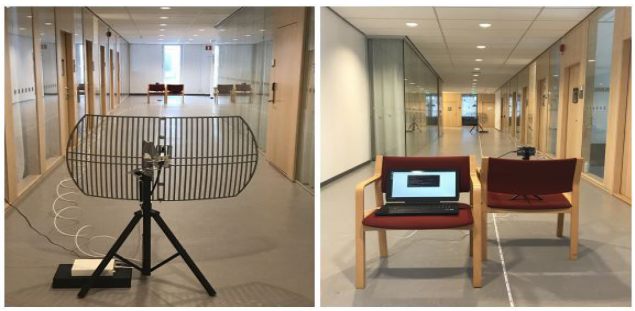

Figure 1. Experimental setup for 15m distance to target [6]

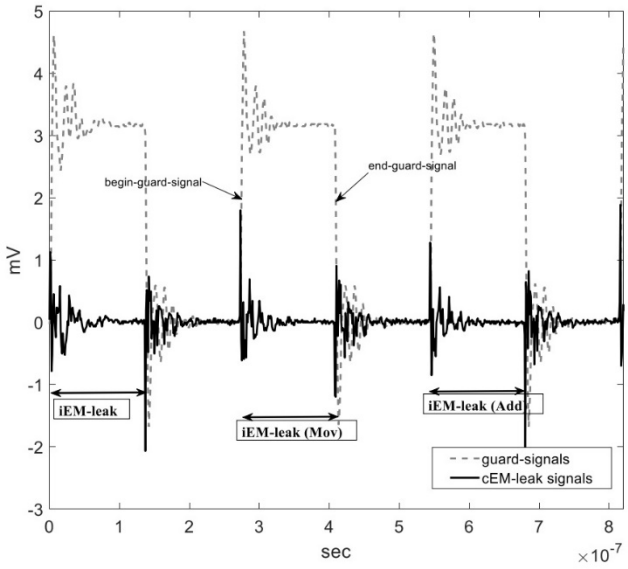

Figure 2. Program context within a testing program [7]

To tackle the discussed challenges and reduce the likelihood of manipulation or reverse engineering,

cryptographic security measures are implemented to safeguard transmitted data. Leading chip makers have already proposed viable solutions, such as hardware architecture specifically designed to provide encryption capabilities and prevent possible attacks such as theft, tampering, etc. Physically unclonable function (PUF), a security technology capitalizing on the exclusive physical characteristics or process parameters of integrated circuit components, has surfaced in recent years to produce keys resistant to replication or prediction [8-9]. While an exclusive key can be generated to resist cracking attempts, SCA may still intercept signals inadvertently leaked during the chip's operation. With further advancement of AI technology and quantum computing, even more formidable threats can be expected in the future. Bae et al.'s study [10] successfully demonstrates that attackers can still extract keys from devices employing the Masked AES encryption mechanism, using the Differential Deep Learning Analysis (DDLA) proposed in their paper. Thus, preventing recording of signal traces is an ongoing challenge.

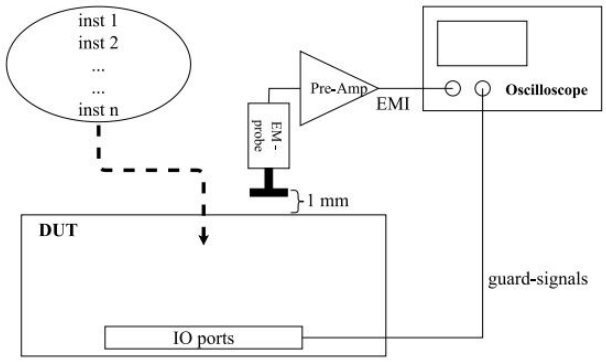

Figure 3. EM-leak measurement platform [7]

Flood sensors are integral to smart city infrastructures, facilitating critical data transmission to information platforms. These sensors are often installed in locations where connecting to traditional transmission cables is challenging, necessitating reliance on wireless communication through low-power wide-area networks (LPWAN). The requisite number of sensors for monitoring river water conditions can range from a few dozen to over a hundred, necessitating a substantial inventory of control chips. Employing a Physical Unclonable Function (PUF) circuit chip for each sensor could significantly increase costs and may not effectively address the scalability challenges posed by such deployments.

Global sales of electronic products are subject to laws and regulations. Compliance with electromagnetic compatibility (EMC) standards is required by these regulations to prevent any electromagnetic radiation emitted during operation from interfering with nearby electronic devices. Boteanu *et al*. use ANSYS' HFSS (High Frequency Structure Simulator) electromagnetic simulation software to design an aluminum alloy outer enclosure that shields sensor components in IoT devices [11]. This enclosure, with appropriate aperture sizes, satisfies EMC standards and guards against possible SCA. The method presented in this literature simulates the signal radiation mechanism of the device and the distribution of field wall energy state through software, without any empirical testing of its real-world effectiveness in an attack environment. Furthermore, Das *et al*. utilize electromagnetic simulation software to construct an internal model of IC at system level based on CMOS process technology [12]. Their proposed model aids comprehension of the radiation characteristics of the internal circuit [12]. Das *et al*. introduce STELLAR (Signature aTenuation Embedded CRYPTO with Low-Level metAI Routing) mechanism, which utilizes signatures to prevent radiation signal leakage from the higher metal layers of IC, resulting in increased resistance to SCA analysis. The article emphasizes that the outermost metal layer causes the most substantial leakage of radiation energy [12]. By suppressing radiation at metal layer, SCA can be effectively prevented. However, implementing Das *et al*.'s approach [12] may result in higher costs for chip manufacturing. To address aforementioned issues, we propose a lightweight solution that leverages the frequency characteristics of new materials utilized in RF circuits [13-14]. Proposed solution involves constructing a shielding cover with an electromagnetic band-gap (EBG) structure in a periodic layout to prevent signal characteristic leakage during microcontroller operation. Our approach also combats SCA and improves overall chip security.

3 Proposed Approach

In this section, we outline three components of our research methodology. Firstly, we will delve into the implementation of microcontroller's encryption transmission mechanism. Following this, we discuss the creation of SCA platform. The third segment focuses on the design of periodic structure. Additional, an experiment will be undertaken to validate the efficacy of the periodic structure in defending against SCA. We will transmit RFID identifiers encrypted with AES through a Wi-Fi module to the receiving system. Meanwhile, we will use the SCA platform to intercept signals leaked from the microcontroller while running. Our experiment aims to assess the level of protection against attacks provided by periodic structure in contrast with three types of other shielding materials. Detailed discussions on these topics can be found in the subsequent sections.

3.1 Implement the Encrypted Transmission Mechanism of IoT Device Control Chip

Currently, Arduino and Raspberry Pi are the most prevalent choices for control chips in IoT environments. The primary distinction between Arduino and Raspberry Pi is that Raspberry Pi has an operating system and better computing capabilities, enabling it to run a wide range of software functionalities for diverse purposes. Considering standard demands for building an extensive array of sensor units, the relatively affordable Arduino is a more suitable option for interfacing with peripheral circuits and sensor components due to Arduino's modest hardware requisites,

as Arduino only needs to regulate transmission of sensor signals for functionality. We implement transmission program for encryption mechanism using Arduino and employs SCA platform to analyze its key features. Lo et al. employs Arduino Uno control board for implementing the encryption algorithm which adopts AES-128, a widely recognized symmetric encryption technique [15-16]. AES-128 involves various functions including AddRoundKey, SubBytes, MixColumns, and ShiftRows as illustrated in Figure 4 [17]. By implementing AES-128, we acquire knowledge of power consumption signal features of internal hardware circuit when executing encryption calculations and functions. During the encryption process, we conduct real-time monitoring of voltage and current waveforms while simultaneously receiving electromagnetic radiation signals via an antenna. The measurement configuration is illustrated in Figure 5. We employ differential power analysis (DPA) to extract the encryption key of AES-128. For detailed key feature analysis, refer to [15]. The results of the real-time key analysis are presented in Figure 6. Furthermore, Wi-Fi module has been configured to transmit AES-128 encrypted data. A simulation system, including a receiver, has been assembled for data transmission via IoT modules. The objective of setup is to verify periodic construction's ability to block any potential signal leakage from microcontroller while allowing uninterrupted Wi-Fi signal transmission.

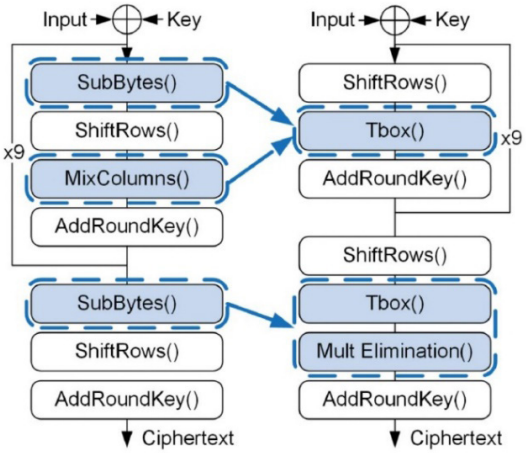

Figure 4. Schematic representation of AES-128 [17]

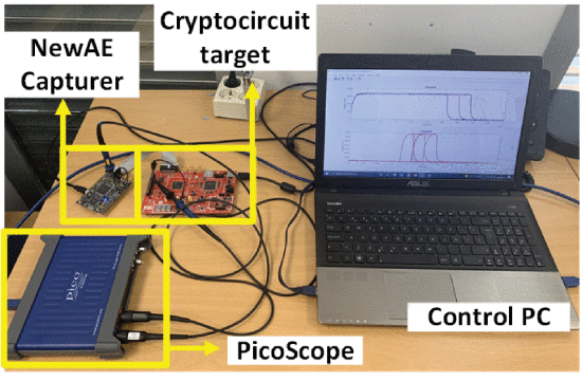

Figure 5. Attack setup with capturer, cryptocircuit target, PicoScope and control PC [17]

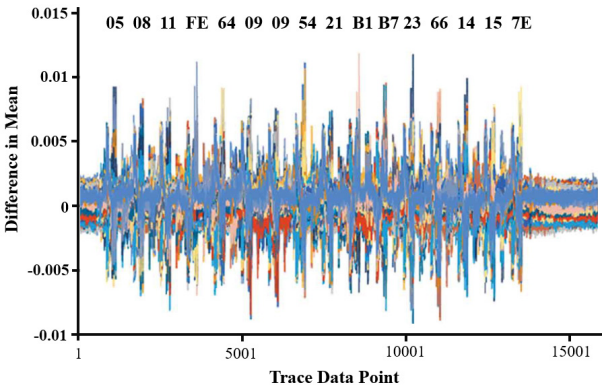

Figure 6. Hamming weight power model attack on 16-byte key [15]

3.2 Establishing A SCA Platform

SCA [18] detects and analyzes physical signals emitted by electronic devices such as voltage, current, sound, and electromagnetic radiation signals. Wired or wireless probes capture signal characteristics during device operation followed by further analysis or statistical methods to extract key information from transmitted messages within devices. As a result, this type of attack poses a significant threat to device security. In IoT environments, devices SCA targets while transmitting data will likely result in theft of confidential data. We construct a SCA platform for IoT devices with a control center (controller PC), a remote GPU computing server, and measurement equipment referencing Peng *et al.*'s study [19]. The architecture is depicted in Figure 7 and Figure 8. The control center comprises five functional blocks, as follows:

- Measure: The purpose of this step is to establish a connection with the oscilloscope and issue commands to initiate the measurement process, while concurrently monitoring the trajectory of the leaked signal emanating from the device.
- Send: It is the duty of computer in control center to convert the signal trajectory data collected by the oscilloscope into an array storage format before transmitting it to the remote computing server for a comprehensive analysis of the essential features. The real-time return value indicates the number of 16 subkeys that AES-128 could decrypt successfully. After processing, the data is saved for future reference.
- Save: The data can be used to compare and analyze the features captured by different devices and measurement methods, and to identify key information.
- Console: The console will display real-time results of key cracking and capture relevant information.
- Encrypt: This block creates a storage space to record the feature data collected during the encryption process of the device. Encryption will be activated by sending a command from the control center to initiate the encryption mechanism of the device under test.

Signal feature analysis requires significant computational correlation. The utilization of an attack

platform equipped with GPU computing power is a fundamental component of this study. To improve the accuracy of our attacks, we take samples of the signal traces captured by AES-128 to 250,000 data points for each power trace. As a result, a minimum of 40-50 traces is usually necessary to decrypt the key successfully. This involves carrying out a tremendous 10,000,000 calculations. The extent of this computational task puts significant pressure on the computer, and performing such operations typically requires several hours. Nevertheless, implementing the attack platform enables executing the aforementioned calculations in less than 10 minutes. This significantly increases the research efficiency of this paper.

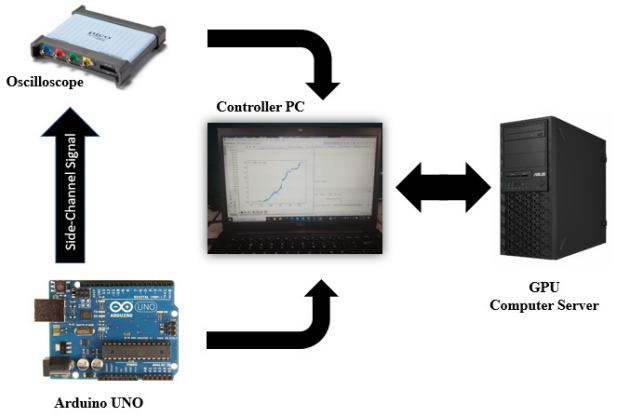

Figure 7. System architecture for SCA resistance verification

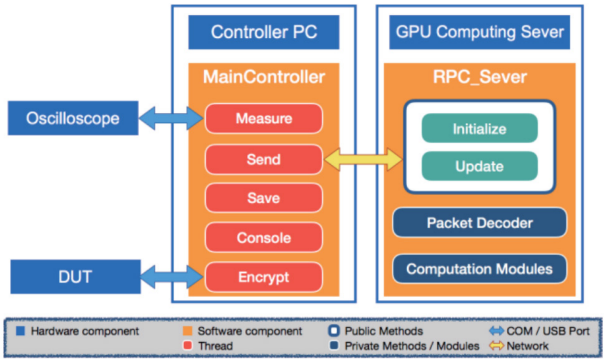

Figure 8. Software components in controller PC and GPU computing server [19]

3.3 Periodic Structures Design and Implementation

To resist SCA, this paper leverages the frequency characteristics of metamaterials to construct EBG structures [20-28] with periodic designs. These structures possess either band-pass or band-stop filter properties, effectively reducing the emission of electromagnetic radiation signals. Figure 9 shows the equivalent circuit element architecture of the EBG, while Figure 10 displays the effect on frequency-related scattering parameters. Specifically, the reflection coefficient denoted by S_{11} tends towards zero, and the energy magnitude is calculated using formula (1).

$$S_{11} = 10\log\left(P_{output} \Big/ P_{input}\right) \tag{1}$$

This indicates that all signal energy at this frequency is reflected back during transmission (p_{output} = p_{input}), preventing any signal from passing through this frequency band. In addition, S_{21} (insertion coefficient) is less than -20dB in the frequency range of 2.3GHz~13.5GHz, indicating that the energy of the signal in this frequency range is lost by more than 100 times, and the signal cannot be transmitted normally. This paper will leverage the characteristics of EBG to design band-stop and band-pass filters in the required frequency range. In the EMC definition of electromagnetic signal categories, conducted emission (CE) and radiated emission (RE) are divided into two categories. CE refers to signals below 30 MHz, while RE pertains to signals ranging from 30 MHz to 1 GHz [29]. Based on the RE definition, we will design an EBG structure that shields signals below 1GHz. Simultaneously, this structure will allow for the transmission of 2.4GHz signals through Wi-Fi, ensuring uninterrupted signal transmission for IoT devices. This paper draws inspiration from the ring-shaped periodic aperture structure designed in [30-34] as illustrated in Figure 11. We adjust the resonant frequency f_r to 2.4 GHz according to the resonance formulas (2, 3). Under free-space conditions, the speed of electromagnetic waves approximates the speed of light, denoted as c_0=3×10^{8}m/s. The dielectric constant of the printed circuit board typically falls within the range of $\in_r \approx 4.2\sim4.7$. For our simulations, we opt for the middle value of 4.5.

$$f_{LC\ Circuit} = \frac{1}{2\pi\sqrt{LC}} \tag{2}$$

$$2r_0 = \frac{c_0}{3\times f_r \times \sqrt{(\in_r +1)/2}} \tag{3}$$

$$C = \in \frac{A}{d} \tag{4}$$

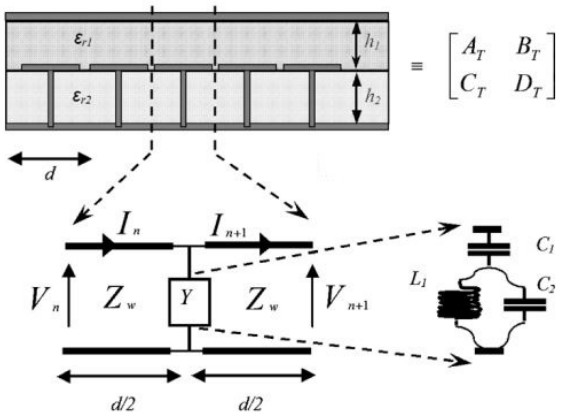

Figure 9. Each unit cell consists of a transmission line of length d with shunt admittance across midpoint of line [20]

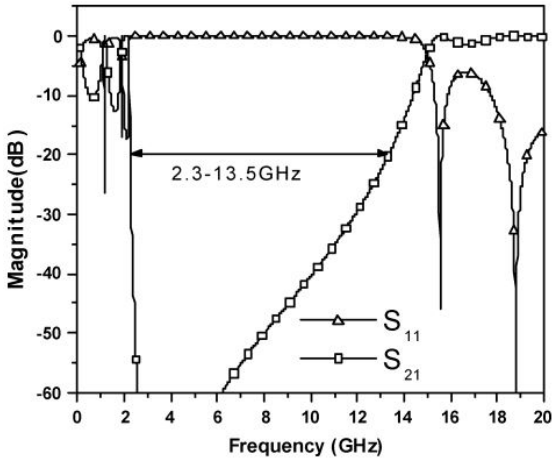

Figure 10. The magnitude of S_{21} and S_{11} [20]

The HFSS simulation results, as depicted in Figure 12, reveal that S_{11} is less than -1.79 dB below 990 MHz, signifying that approximately 65% of the signal energy at this frequency cannot pass through. At 1550 MHz and 2410 MHz, S_{11} values are -11.56 dB and -8.14 dB, respectively, indicating that only about 10% of the signal energy is reflected, while the remaining 90% can pass through the EBG.

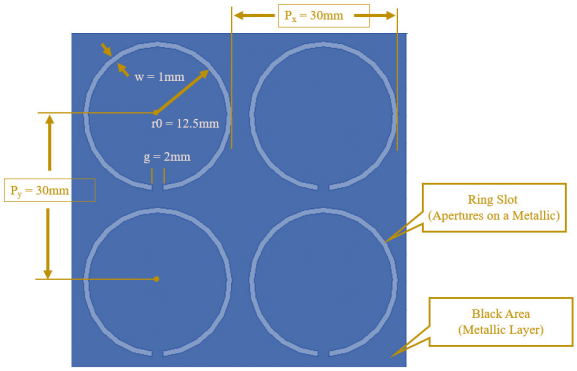

Figure 11. The unit cell of the EBG with dimensions

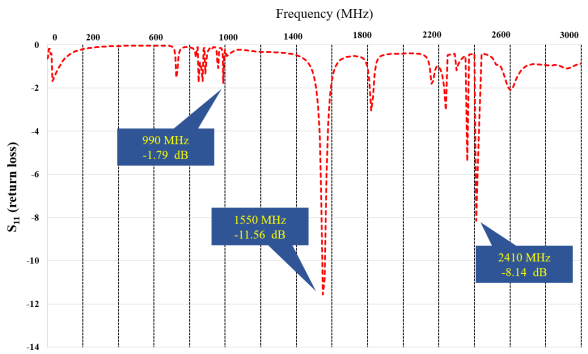

Figure 12. Reflection coefficient of the EBG

Figure 13 shows an EBG structure fabricated using FR4 material on a printed circuit board (PCB), with an $\in_r$ value of 4.5. The dimensions of w and g are controlled by formula (4), where w and g represent the distances between the dielectric plates, determining the capacitance value. Increasing w and g increases d, leading to a reduction in C and, consequently, a lower resonant frequency, as per formula (2). In this study, we conducted simulations with w and g varying from 1 to 3 mm, eventually settling on w = 1 mm and g = 2 mm as the optimal dimensions after repeated adjustments. This paper employs this structure to assess its effectiveness in defending against SCA, aiming to verify its capability to block signal interception while allowing the normal operation of 2.4 GHz wireless signals.

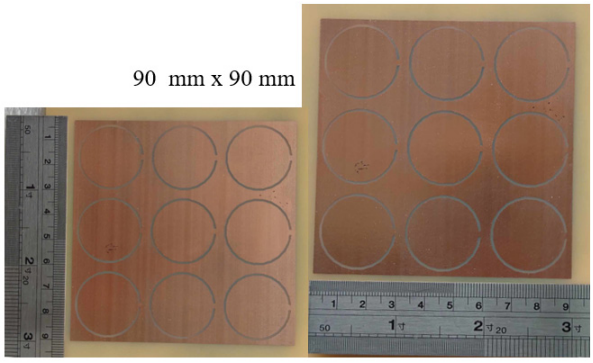

Figure 13. Entity of array of 3x3 circular rings apertures

4 Experimental Results

The experiment setup for this paper utilizes the Arduino Uno R3 board, which has ESP 8266 wireless module and the MFRC-522 RFID sensing module attached. We developed receiving software using Java to make an AES-128 decryption program for the host computer. Lastly, Wireshark 4.0 has been installed to ensure encrypted data is received correctly. These sections elaborate on the encrypted wireless device, the SCA system, and the periodic structure's shielding abilities.

4.1 Cryptographic Wireless Communication Device

This paper presents an IoT control device system that uses AES-128 encryption for transmitting data. In Figure 14, you can see the RFID reader in the lower left corner. it uses the AES-128 encryption algorithm programmed on Arduino to compose the identification code into a 16-byte package. Then, the package is transmitted via the Wi-Fi module to the host control unit, which is situated in the upper left corner of Figure 14. The program on the host computer decrypts the RFID Tag data obtained from the RFID Reader. The final output is the identification code. We also installed Wireshark packet analysis software on the host computer, as shown at the bottom of Figure 14. This software confirms whether the Arduino's encrypted data is accurately retrieved and matches the program's output. In the figure, the final data in Wireshark is shown as **47 99 2B 90 6C 8B 12 AA 51 38 CD DF C2 E3 85 78**, which matches the data received in the application we described earlier. Next, we will use the SCA platform to conduct a key feature analysis on this set of devices and introduce the EBG structure to determine its resistance to SCA.

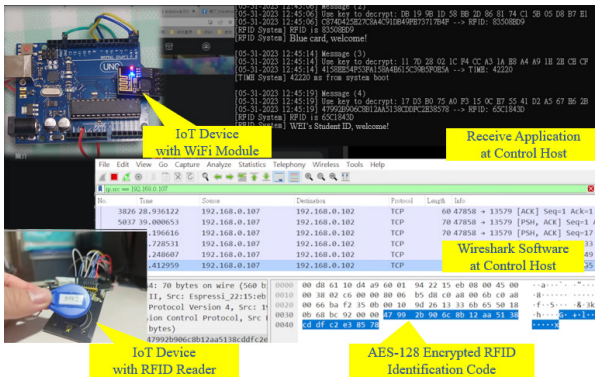

Figure 14. Wireless transmission system with AES encryption mechanism

4.2 Side Channel Attack Platform Experiment

Figure 15 and Figure 16 illustrate the procedure for measuring feature signals using a loop antenna. Subsequently, we amplify these signals with a low-noise amplifier and sample them. During this process, the microcontroller sends out one AES-128 encrypted packet, and we take 250,000 data points for each encrypted trace. The collected data is then transmitted to a remote server for DPA analysis via the host. The attack outcomes for each trace are instantly sent back to the host computer's receiver program to track the number of subkeys successfully hacked.

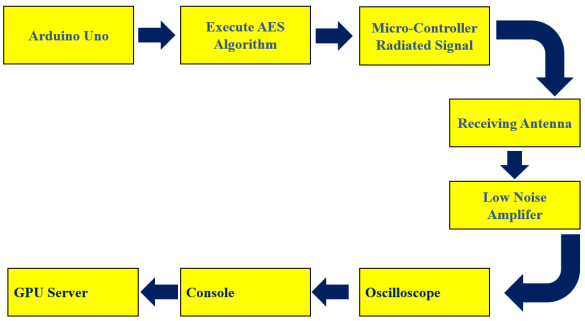

Figure 15. The measurement system setup with Arduino Uno

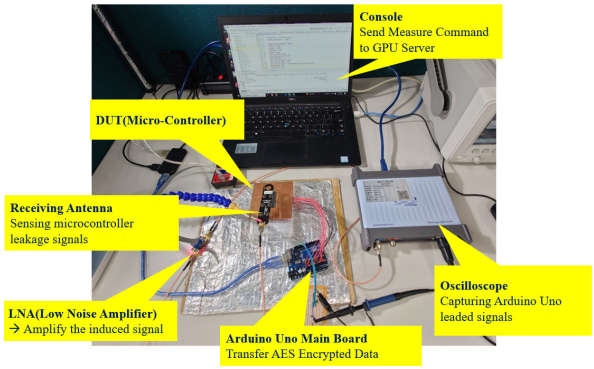

Figure 16. The Arduino Uno (cryptographic device) and the SCA measurement setup

The distance between the measurement and antenna to the microcontroller is both 300 mm, as illustrated in Figure 17. The main reason for this selection is to have enough room for the EBG design. Notably, our measuring system can break the AES-128 code from a distance of 4000 mm. During SCA testing, cracking the code can present a significant challenge.

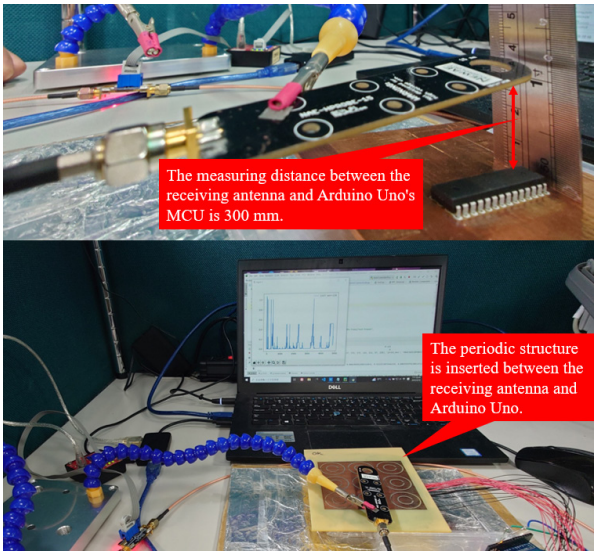

Figure 17. The distance between the measurement antenna and Arduino Uno and Insert EBG structure

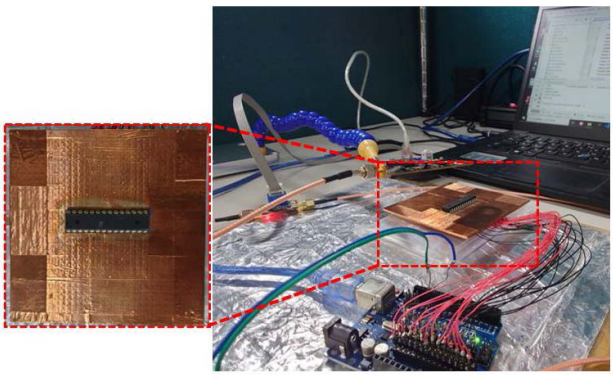

Figure 18. The Arduino Uno's MCU is mounted on a printed circuit board with signal shielding

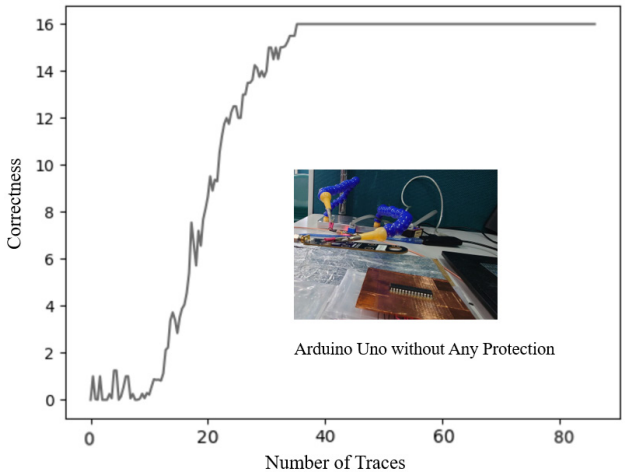

Figure 19. The correlation analyses on EM traces of Arduino Uno (no protection)

Following IEC 61967-1 standard, we place the microcontroller on a separate PCB and protect it with a metal shield, as depicted in Figure 18. During the signal acquisition process, the signal is free from interference by other components and the surrounding environment. Figure 19 illustrates the results of the key analysis. The SCA system can crack all 16 subkeys after about 40 encrypted traces when the microcontroller is unprotected. The graph's horizontal axis corresponds to the number of traces encrypted, while the vertical axis indicates the number of subkeys successfully cracked. At the bottom of Figure 17, an EBG is introduced between the receiving antenna and the microcontroller to obstruct the extraction of signal features. The results of this setup effectively thwart subkey analysis by the attack platform even after 20,000 attack analyses, thereby protecting the device's encryption key. The evaluation benchmark for the attack analysis comprised 20,000 EM traces, chosen in line with the research by Pammu *et al*. [16]. In their study, they deployed the AES-128 algorithm on the ATmega processor and observed the results of CEMA (Correlation Electromagnetic Analysis), assessing its effectiveness in resisting side-channel attacks across 16 subkeys. In the next section, we will compare the effectiveness of incorporating EBG with other shielding materials.

4.3 Comparison of Signal Blocking Effects of Different Shielding Materials

All electrical and electronic products available in the market must obtain EMC certification and meet specific regulatory requirements before being sold. Nearly all electronic products have protective casings to ensure effective control of electromagnetic interference. This measure prevents external electromagnetic energy from impacting the product's functionality. Conversely, when the product is operating, electromagnetic waves generate and become interference, which may disrupt the functioning of external electronic devices. Commonly used shielding materials available in the market include perfect electric conductor (PEC), perfect magnetic conductor (PMC), and graphene. Table 1 provides a summary of the signal shielding attributes of various materials used in our experiments, including material thickness, applicable frequency range (Freq.), and shielding effect (SE). The SE is ascertained by comparing the incident electric field with the transmitted electric field after passing through the shielding material, with the transmitted electric field serving as the denominator. A smaller denominator means that the shielding material absorbs more of the incident electric field intensity. Therefore, a higher value indicates more effective resistance to electromagnetic energy.

To crack the subkey, we use DPA to analyze the attack on each signal trace captured by the hardware device. By analyzing the 16 subkeys of AES-128, we can break the encryption by examining the statistical results of the key and private key guessing entropy (PGE) values. This process involves identifying the maximum value calculated for each subkey. Figure 20 illustrates the results of the attack, with numbers 0 to 15 representing the successfully cracked subkeys.

Table 1. Comparison of properties of various shielding materials

Material	Thickness (mm)	Freq. (Hz)	SE (dB)
PEC Copper Foil Tape	0.1	10 K ~ 20 G	60 ~ 85
PMC Flexield	0.1	10 M ~ 3 G	5 ~ 20
Graphene	0.08	1 G ~ 20 G	25 ~ 80
EBG	1.6	30 M ~ 1.57 G	22 ~ 23

Shielding materials are categorized according to the principles of electrical circuits, distinguishing between electric field shielding, magnetic field shielding, and electromagnetic field shielding. Due to the diverse circuit layouts in electronic devices, any form of energy field has the potential to escape containment. This paper presents a comparative evaluation of these three material types with EBG. PEC and EBG demonstrate the ability to maintain the security of microcontroller encryption keys despite analyzing 20,000 power tracks, which is illustrated in Figure 21 and Figure 22, the number of cracks in the 16 AES subkeys on the y-axis (Correctness) is less than 4.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE=	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	C9 0.902	72 0.932	9E 0.915	BC 0.918	ED 0.900	5E 0.920	91 0.918	8D 0.940	CC 0.907	68 0.927	9C 0.906	CE 0.915	E5 0.898	1C 0.908	AD 0.907	93 0.922
1	CA 0.325	66 0.317	A2 0.319	75 0.320	F0 0.321	AB 0.327	07 0.313	EF 0.354	50 0.318	F4 0.320	1C 0.333	C0 0.299	66 0.316	F6 0.341	AE 0.371	4C 0.349
2	C4 0.313	9D 0.311	68 0.314	49 0.311	59 0.311	A3 0.314	3A 0.312	B3 0.329	FD 0.312	6B 0.307	1F 0.317	70 0.294	02 0.306	5F 0.314	33 0.311	92 0.298
3	2F 0.306	4E 0.304	81 0.299	10 0.311	CE 0.311	F6 0.294	65 0.303	F9 0.307	A3 0.305	86 0.305	15 0.308	C6 0.292	10 0.300	5D 0.312	59 0.296	67 0.293
4	F0 0.299	E3 0.299	D1 0.290	1A 0.310	5B 0.304	9B 0.294	74 0.299	A4 0.302	8D 0.289	F1 0.302	65 0.308	90 0.292	34 0.289	29 0.311	DE 0.293	3D 0.289

Figure 20. The analysis results for the correlation coefficient of the signal trace (The sequence "C9 72 9E BC... 93" displayed at the top of the figure signifies that all 16 subkeys have been successfully cracked.)

On the other hand, PMC has completely cracked 16 subkeys when it is close to 5,000 power tracks, as depicted in Figure 23. Finally, the characteristics of graphene are that the subkey is also completely cracked when the power track is close to 400, as shown in Figure 24.

Based on the analysis of the properties of various materials, PEC material is deemed suitable for environments characterized by strong low-frequency signals. Due to its high magnetic permeability, PMC material can decrease magnetic flux density, thereby achieving an effective shielding outcome. Graphene, noted for its ultra-thin, lightweight, flexible, and corrosion-resistant qualities, is ideal for applications requiring reduced weight, such as in aviation, automotive, and sports equipment industries. According to the literature [35-36], graphene's small size and thin profile result in a less pronounced shielding effect below 1 GHz. To enhance its effectiveness, it is necessary to synthesize graphene within a composite material production process.

The modified EBG design presented in this paper utilizes PEC material. Tailored to adhere to the specific frequency band that necessitates shielding, this product features a band-stop filter effect for frequencies below 1 GHz and operates as a 2.4 GHz band-pass filter. In addition

to mitigating electromagnetic radiation leakage from electronic devices, this method also safeguards system encryption keys against SCA and ensures the uninterrupted transmission of wireless communications.

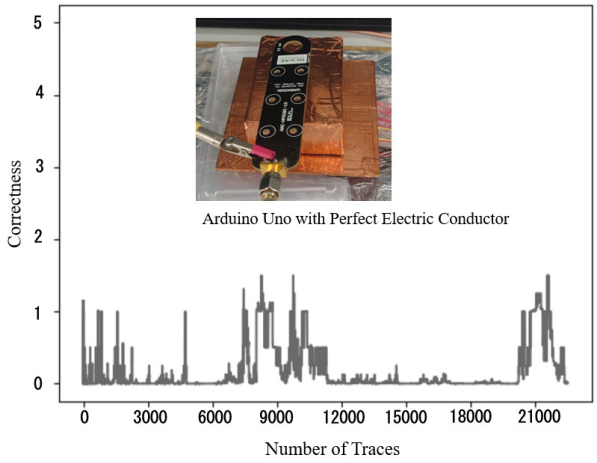

Figure 21. The correlation analyses on EM traces of Arduino Uno (with PEC)

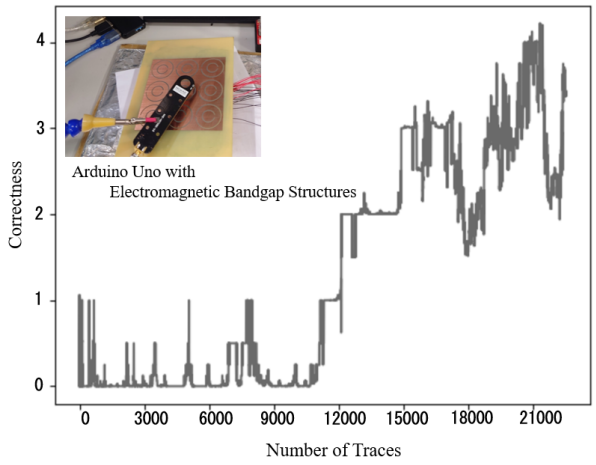

Figure 22. The correlation analyses on EM traces of Arduino Uno (with EBG)

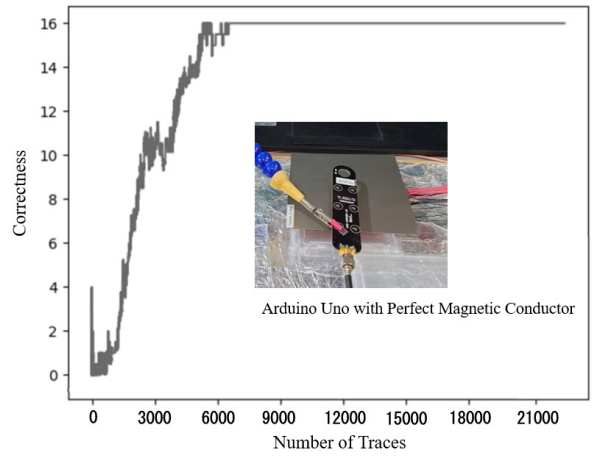

Figure 23. The correlation analyses on EM traces of Arduino Uno (with PMC)

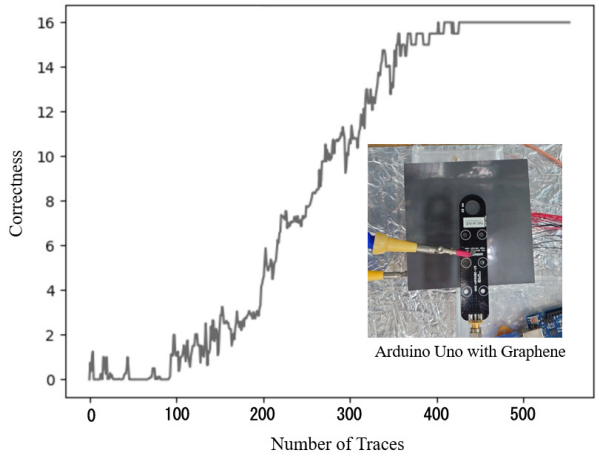

Figure 24. The correlation analyses on EM traces of Arduino Uno (with Graphene)

5 Conclusions

The periodic structure introduced in this paper exhibits EBG properties that restrict the leakage of electromagnetic wave energy from the control chip during operation within the structure. This feature makes it a suitable candidate for deployment on the exterior casing of IoT devices. Compared to the conventional approach of installing an electromagnetic shielding shell directly on electronic devices for regulatory compliance with electromagnetic compatibility requirements, the use of PEC, PMC, or graphene materials is effective in preventing both external electromagnetic interference and the electromagnetic radiation generated by the device's circuitry from interfering with surrounding devices. However, this approach may impede the wireless communication frequency bands that IoT devices require, thus failing to satisfy the wireless transmission environment's actual needs. Consequently, the EBG structure proposed in this paper effectively resists SCA while ensuring the normal operation of the Wi-Fi signal frequency band. Overall, this solution adeptly meets the practical application demands of IoT devices.

Acknowledgments

This work was supported in part by the National Science and Technology Council, Taiwan, under Grants NSTC 112-2222-E-035-002, 112-2221-E-035 -049 -, and 112-2634-F-005 -001 -MBK, and by the Longmau Technology Co., Ltd., under Grant 12B1001T.

References

[1] IoT Analytics [Online]. Available: https://iot-analytics.com/about/

[2] C. Cecchinel, M. Jimenez, S. Mosser, M. Riveill, An Architecture to Support the Collection of Big Data in the Internet of Things, *2014 IEEE World Congress on Services*, Anchorage, AK, USA, 2014, pp. 442-449. https://doi.org/10.1109/SERVICES.2014.83

[3] Trend Micro, The IoT Attack Surface: Threats and Security Solutions [Online]. Available: https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions

[4] P. Socha, V. Miškovský, M. Novotný, A Comprehensive Survey on the Non-Invasive Passive Side-Channel Analysis, *Sensors*, Vol. 22, No. 21, pp. 1-37, November, 2022.
https://doi.org/10.3390/s22218096

[5] O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici, Y. Oren, Reverse Engineering IoT Devices: Effective Techniques and Methods, *IEEE Internet of Things Journal*, Vol. 5, No. 6, pp. 4965-4976, December, 2018.
https://doi.org/10.1109/JIOT.2018.2875240

[6] R. Wang, H. Wang, E. Dubrova, Far Field EM Side-Channel Attack on AES Using Deep Learning, *The 4th ACM Workshop on Attacks and Solutions in Hardware Security*, Virtual Event, USA, 2020, pp. 35-44.
https://doi.org/10.1145/3411504.3421214

[7] S. Y. Yuan, Optimized Sequence Dataset Generation for a Two-Stage Pipelined Microcontroller Instruction-Level Electromagnetic Information Leakage Analysis, *IEEE Access*, Vol. 10, pp. 96798-96804, September, 2022.
https://doi.org/10.1109/ACCESS.2022.3204397

[8] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, Physical Unclonable Functions and Applications: A Tutorial, *Proceedings of the IEEE*, Vol. 102, No. 8, pp. 1126-1141, August, 2014.
https://doi.org/10.1109/JPROC.2014.2320516

[9] A. Al-Meer, S. Al-Kuwari, Physical Unclonable Functions (PUF) for IoT Devices, *ACM Computing Surveys*, Vol. 55, No. 14s, pp. 1-31, July, 2023.
https://doi.org/10.1145/3591464

[10] D. Bae, J. Hwang, J. Ha, Deep Learning-based Attacks on Masked AES implementation, *Journal of Internet Technology*, Vol. 23, No. 4, pp. 897-902, July, 2022.
https://doi.org/10.53106/160792642022072304024

[11] A. Boteanu, F. Răstoceanu, I. Rădoi, C. Rusea, Modeling and Simulation of Electromagnetic Shielding for IoT Sensor Nodes Case, *2019 International Conference on Speech Technology and Human-Computer Dialogue (SpeD)*, Timisoara, Romania, 2019, pp. 1-6.
https://doi.org/10.1109/SPED.2019.8906621

[12] D. Das, M. Nath, B. Chatterjee, S. Ghosh, S. Sen, STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis, *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, McLean, VA, USA, 2019, pp. 11-20.
https://doi.org/10.1109/HST.2019.8740839

[13] G. Jin, C. Zhang, T. Ye, J. Zhou, Band Gap Property Analysis of Periodic Plate Structures under General Boundary Conditions Using Spectral-Dynamic Stiffness Method, *Applied Acoustics*, Vol. 121, pp. 1-13, June, 2017.
https://doi.org/10.1016/j.apacoust.2017.01.024

[14] S. Shahparnia, O. M. Ramahi, A Simple and Effective Model for Electromagnetic Bandgap Structures Embedded in Printed Circuit Boards, *IEEE Microwave and Wireless Components Letters*, Vol. 15, No. 10, pp. 621-623, October, 2005.
https://doi.org/10.1109/LMWC.2005.856695

[15] O. Lo, W. J. Buchanan, D. Carson, Power Analysis Attacks on the AES-128 S-box Using Differential Power Analysis (DPA) and Correlation Power Analysis (CPA), *Journal of Cyber Security Technology*, Vol. 1, No. 2, pp. 88-107, 2017.
https://doi.org/10.1080/23742917.2016.1231523

[16] A. A. Pammu, K. S. Chong, W. G. Ho, B. H. Gwee, Interceptive Side Channel Attack on AES-128 Wireless Communications for IoT Applications, *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Jeju, Korea (South), 2016, pp. 650-653.
https://doi.org/10.1109/APCCAS.2016.7804081

[17] F. E. Potestad-Ordóñez, E. Tena-Sánchez, A. J. Acosta-Jiménez, C. J. Jiménez-Fernández, R. Chaves, Design and Evaluation of Countermeasures Against Fault Injection Attacks and Power Side-Channel Leakage Exploration for AES Block Cipher, *IEEE Access*, Vol. 10, pp. 65548-65561, June, 2022.
https://doi.org/10.1109/ACCESS.2022.3183764

[18] K. Mai, Side Channel Attacks and Countermeasures, in: M. Tehranipoor, C. Wang (Eds.), *Introduction to Hardware Security and Trust*, Springer, New York, NY, 2011, pp. 175-194.
https://doi.org/10.1007/978-1-4419-8080-9_8

[19] S. Y. Peng, W. C. Hong, J. T. Li, S. J. Huang, Framework for Efficient SCA Resistance Verification of IoT Devices, *2018 IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Japan, 2018, pp. 468-471.
https://doi.org/10.1109/ICASI.2018.8394287

[20] M. Zedler, C. Caloz, P. Russer, 3D Composite Right-Left Handed Metamaterials with Lorentz-type Dispersive Elements, *2007 International Symposium on Signals, Systems and Electronics*, Montreal, QC, Canada, 2007, pp. 217-221.
https://doi.org/10.1109/ISSSE.2007.4294452

[21] B. A. Munk, *Frequency Selective Surfaces: Theory and Design*, John Wiley and Sons, 2000.
https://doi.org/10.1002/0471723770

[22] D. H. Kim, J. I. Choi, Frequency Selective Surface for the Blocking of Multiple Frequency Bands, *2006 IEEE Antennas and Propagation Society International Symposium*, Albuquerque, NM, USA, 2006, pp. 4195-4198.
https://doi.org/10.1109/APS.2006.1711554

[23] Y. Rahmat-Samii, Electromagnetic Band Gap (EBG) Structures in Antenna Engineering: From Fundamentals to Recent Advances, *2008 Asia-Pacific Microwave Conference*, Hong Kong, China, 2008, pp. 1-2.
https://doi.org/10.1109/APMC.2008.4958195

[24] F. Yang, Y. Rahmat-Samii, *Electromagnetic Band Gap Structures in Antenna Engineering*, Cambridge: Cambridge University Press, 2008.
https://doi.org/10.1017/CBO9780511754531

[25] D. Sievenpiper, L. Zhang, R. F. J. Broas, N. G. Alexopolous, E. Yablonovitch, High-Impedance Electromagnetic Surfaces with a Forbidden Frequency Band, *IEEE Transactions on Microwave Theory and Techniques*, Vol. 47, No. 11, pp. 2059-2074, November, 1999.
https://doi.org/10.1109/22.798001

[26] D. Elsheakh, H. Elsheakh, E. Abdallah, *Antenna Designs with Electromagnetic Band Gap Structures*, in: C.-Y. Jiang (Ed.), *Metamaterial*, InTech, 2012, pp. 403-472.

[27] H. Kumar, M. Kumar, M. Kumar, A. Kumar, R. Kanth, Study on Band Gap Behaviour of Electromagnetic Band-Gap (EBG) Structure with Microstrip Antenna, *2012 14th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South), 2012, pp. 356-359.

[28] C. D. Wang, T. L. Wu, Model and Mechanism of Miniaturized and Stopband-Enhanced Interleaved EBG Structure for Power/Ground Noise Suppression, *IEEE Transactions on Electromagnetic Compatibility*, Vol. 55,

No. 1, pp. 159-167, February, 2013.
https://doi.org/10.1109/TEMC.2012.2210900

[29] H. Elias, N. Perez, H. Hirsch, Experimental Prediction of the Radiated Emission and Final Measurement Process Optimization based on Deep Neural Networks According to EN 55032, *2022 International Symposium on Electromagnetic Compatibility-EMC Europe*, Gothenburg, Sweden, 2022, pp. 708-713.
https://doi.org/10.1109/EMCEurope51680.2022.9901041

[30] A. Chatterjee, S. Naskar, S. Das, T. Bhowmick, A. Chatterjee, A Bandpass Frequency Selective Surface Using Ring Slots for Dual-Band Applications, *2022 Interdisciplinary Research in Technology and Management (IRTM)*, Kolkata, India, 2022, pp. 1-4.
https://doi.org/10.1109/IRTM54583.2022.9791693

[31] G. I. Kiani, L. G. Olsson, A. Karlsson, K. P. Esselle, M. Nilsson, Cross-Dipole Bandpass Frequency Selective Surface for Energy-Saving Glass Used in Buildings, *IEEE Transactions on Antennas and Propagation*, Vol. 59, No. 2, pp. 520-525, February, 2011.
https://doi.org/10.1109/TAP.2010.2096382

[32] Z. Zhao, A. Zhang, X. Chen, G. Peng, J. Li, H. Shi, A. A. Kishk, Bandpass FSS with Zeros Adjustable Quasi-Elliptic Response, *IEEE Antennas and Wireless Propagation Letters*, Vol. 18, No. 6, pp. 1184-1188, June, 2019.
https://doi.org/10.1109/LAWP.2019.2911908

[33] B. S. da Silva, A. L. P. de S. Campos, A. G. Neto, Equivalent Circuit Model for Analysis of Frequency Selective Surfaces with Ring and Double Concentric Ring Apertures, *IET Microwaves, Antennas & Propagation*, Vol. 14, No. 7, pp. 600-607, June, 2020.
https://doi.org/10.1049/iet-map.2019.0760

[34] W. Liu, Z. Yan, J. Wang, Z. Ning, Z. Min, Ultrawideband Real-Time Monitoring System Based on Electro-Optical Under-Sampling and Data Acquisition for Near-Field Measurement, *IEEE Transactions on Instrumentation and Measurement*, Vol. 69, No. 9, pp. 6603-6612, September, 2020.
https://doi.org/10.1109/TIM.2020.2968755

[35] H. N. Lin, H. C. Chen, C. W. Kuo, Y. T. Chang, Design and Application of a Mobile Miniature Current Probe for Analysing the Cause of EMI Noise in IC Circuits, *IET Science, Measurement & Technology*, Vol. 11, No. 5, pp. 655-665, August, 2017.
https://doi.org/10.1049/iet-smt.2016.0348

[36] S. Wan, Y. Li, J. Mu, A. E. Aliev, S. Fang, N. A. Kotov, L. Jiang, Q. Cheng, R. H. Baughman, Sequentially Bridged Graphene Sheets with High Strength, Toughness, and Electrical Conductivity, *Proceedings of the National Academy of Sciences (PNAS)*, Vol. 115, No. 21, pp. 5359-5364, May, 2018.
https://doi.org/10.1073/pnas.1719111115

Biographies

Chung-Wei Kuo received his B.E. degree in Department of Electronic Engineering from National Chin-Yi University of Technology, the M.E. degree in Department of Communications Engineering and the Ph.D. program of Electrical and Communications Engineering from Feng-Chia University, Taichung. His current re-search interests include information security and wireless communications.

Kuo-Yu Tsai received the M.S. and Ph.D. degrees from the Department of Information Management, National Taiwan University of Science and Technology, in 2001 and 2009, respectively. His recent research interests include Cryptography, IoT Application and Security, and m-commerce Application and Security.