Hardware RFID security for preventing far-field attacks

Dmitry Dobrykh*, *Member, IEEE,* Dmitry Filonov, *Member, IEEE*, Alexey Slobozhanyuk, *Member, IEEE* and Pavel Ginzburg, *Member, IEEE*.

Abstract — Radio-frequency identification (RFID) is a widely used approach for a short-range contactless data exchange, i.e., employed in billing systems. During the last years, unauthorized access has become an issue, as it has been proven on numerous unpleasant occasions. A typical theft scheme is based on approaching a victim with a card reader. However, a straightforward adaptation of the reader's antenna elements allows performing the attack from a distance, opening a severe security loophole. Here, we propose and demonstrate hardware-based protection capable of preventing a far-field attack of this kind. Our solution is based on an RFID chip shielding with an opaque metal. The Faraday-type of the enclosure has a small aperture, which suppresses electromagnetic field leakage from the device. This property affects both up and down interrogation links, virtually making the far-field attack impossible. Activation of the card is done by holding it in hand – this way, it is made accessible to an authorized readout, which still remains wireless. The physical principle of the operation is placing a high-index dielectric structure next to a subwavelength aperture, making it electromagnetically larger and, as a result, supporting the field leakage. Our experimental prototype, validated by several different users, shows the capability to diminish far-field attacks on UHF RFID tags. This hardware security solution can find usage in numerous applications, such as biometric passports, credit cards, and many others, where unauthorized access to sensitive data is highly undesirable.

Index Terms — RFID, electromagnetic shielding, wireless security.

I. INTRODUCTION

Wireless communication security has become an important topic over the past years owing to numerous thefts of different kinds. Data, being transmitted in a classical public channel, can be collected by a third party, causing a big privacy issue. Numerous security protocols have been developed to address those issues and allowed using cellular communications and other wireless applications rather safely [1]. However, several fundamental loopholes remain and seem to be unsolvable with software encryption approaches. A celebrated example is radio frequency identification (RFID), where data is encoded on a chip connected to an antenna [2]. This passive device is interrogated by an active reader. In this communication protocol, data is encoded on time-modulated back reflection from a tag. Being standardized, this wireless channel is subject to theft since any card obeying the standard should be accessible by any reader. A typical example here is data theft from contactless credit cards [3],[4]. One of the theft schemes is based on approaching a victim with a billing terminal and charging a small amount, which does not require a PIN-code authorization. While nowadays this theft scheme is applied in crowded places, where physical proximity with a victim is less alarming, RFID theft from a range is also possible [5], [6]. It is worth noting that credit cards operate at 13.6 MHz, though our investigations will concentrate on ultra-high frequency (UHF) RFID, operating around 900 MHz, depending on a licensing country [7].

The typical reading distance of RFID tags with standard readers is usually less than a meter. This performance is partially related to the need for a reliable accessibility without a demand for an accurate alignment between the tag and the reader. As a result, the directivity of interrogating antennas is quite low (close to 0 dBi). However, a straightforward adaptation of a reader antenna can significantly improve the reading range, which can prevail 10 m. Long-range passive RFID tags can show an additional improvement if state-of-the-art equipment and customized designs are used [8], [9]. In addition, the reader's radiated power can be increased. However, the effective isotropic radiated power (EIRP) is limited up to 36 dBm, depending on the licensing country. Consequently, commercially available readers obey these regulations.

Relying on the beforehand discussion, the RFID reading range increase can improve the reader's antenna gain or increase the radiated power. We found the latter approach less straightforward, as adding an external amplifier significantly degrades the noise figure, making the readout process fail. For example, cascading circulators do not solve the problem since the reader's dynamic range is optimized to receive relatively low-power signals, and any direct leakage from the transmit antenna virtually blocks the capability to interrogate. Notably, complying with the EIRP regulation is not considered a limiting

* The main numerical model and experimental part of the work was supported by the Russian Science Foundation (Project 19-79-10232). The numerical calculations and optimization of the structure parameters were partially supported by the Russian Foundation for Basic Research (Grant No. 20-37-51011). P.G. acknowledges partial support of the ERC StG "In Motion" (802279), PAZY Foundation, and Israeli Ministry of Science and Technology (Project "Integrated 2D & 3D Functional Printing of Batteries with Metamaterials and Antennas").

Alexey Slobozhanyuk is with the School of Physics and Engineering, ITMO University, Saint Petersburg 197101, Russia (email: a.slobozhanyuk@metalab.ifmo.ru).

Dmitry Dobrykh, Pavel Ginzburg are with the School of Electrical Engineering, Tel Aviv University, Tel Aviv 69978, Israel. (email: dmitryd@mail.tau.ac.il, pginzburg@post.tau.ac.il)

Dmitry Filonov is with the Center for Photonics and 2D Materials, Moscow Institute of Physics and Technology, Dolgoprudny 141700, Russia. (email: filonov.ds@mipt.ru)

Alexey Slobozhanyuk, Dmitry Filonov are with the Sirius University of Science and Technology, Sochi 354340, Russia.

factor in the case of RFID theft. Finally, based on our previous considerations, it becomes evident that a long-range RFID attack is performed from the far-field, created by a high-gain antenna. Our focus hereafter is to find a hardware solution to prevent theft of this kind.

A layout of the proposed solution appears in Fig. 1. The architecture of our device is based on metal shielding with a small aperture. The size of the aperture is well-below the operational wavelength, which prevents an efficient passage of electromagnetic radiation through it. A similar effect has been demonstrated in an RFID sensor for metal corrosion monitoring [10]. The RFID communication is performed in two steps – the first one is the activation of the tag by a reader (downlink). The second stage is the backscattering of a time-modulated signal (uplink). It means that a wave should pass through a subwavelength aperture twice. The efficiency of this process is virtually 0, making far-field interrogation of the shielded tag impossible. However, we intend to use the tag after a certain user-approved authorization. In our case, the activation is made by hand – only a card placed in the proximity of a hand can be interrogated. The physical explanation of the operation is as follows – a human hand is about 50-60% water, which is a high permittivity dielectric with a real part around 30-40 [11] at 900 MHz. Placing a contrast dielectric close to an aperture makes the later electromagnetically larger (times the refractive index of the dielectric) and, as a result, allows the wave transmission. Consequently, the tag can be interrogated by a reader. This approach is a solution to the issue of an unauthorized far-field attack.

The manuscript is organized as follows: design of the shield is discussed in detail and then followed by a set of experimental verificaitons.

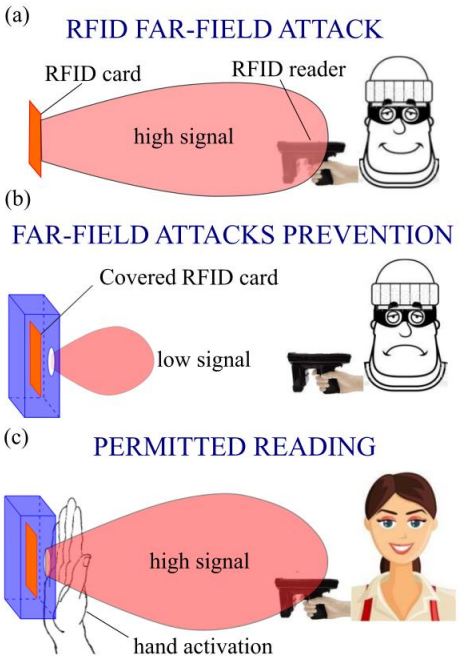

Figure 1. Concept of an RFID tag protected against a far-field attack. (a) A far-field attack performed with a standard reader with a directive antenna. (b) Far-field attacks prevention. Small aperture in the tag shielding prevents the interrogation. (c) The card authorization – a user's hand increases the aperture's electromagnetic size, allowing the readout process.

II. THE SHIELD DESIGN AND ANALYSIS

Shielding is typically used to reduce emission levels of electromagnetic sources and protect people or electronics apparatuses and systems against possible harmful effects due to external fields. The main mechanisms of electromagnetic attenuation are reflection and absorption [12]. Reflection is a typically used one, and it is based on shielding with highly conducting metals. Electromagnetic shielding effectiveness is determined by a set of parameters, such as shield thickness, operational frequency, distance to the EM source and its type, material parameters of the shield, and a few others [13]. A widely used RF shield type is a Faraday cage, based on a metal wires grid [14]. Our device, however, requires controllable shielding, which is depicted in Fig. 1.

While the beforehand discussed working principle of the device can be intuitively understood, a set of numerical optimizations is required before making a prototype. A set of full-wave numerical simulations with CST Microwave Studio was performed, introducing the real system's parameters. A standard UHF RFID tag (type AZ 9662, copper antenna) was placed in the center of a metal box with dimensions of L = 105 mm, W = 75 mm, and h = 40 mm. The cover had a square aperture with a size of 30 x 30 mm on the bottom side (Fig. 2a).

In the following discussion, we will consider both the uplink and downlink models [15]. For uplink calculation, a numerical port with complex impedance $Z = 20 - 205j$ Ohm was plugged within the tag's antenna gap. This impedance value at the resonance frequency f = 900 MHz corresponds to the datasheet of the chip (Alien Higgs 3). The integral power flux through the hemisphere with a center on the aperture was calculated for assessing uplink performances (Fig. 2d). The hemisphere radius was taken to be 120 mm on purpose – it included near and intermediate field zones to assess an unauthorized near-field attack's capability. Though the device was not optimized to diminish it, a significant suppression will be demonstrated.

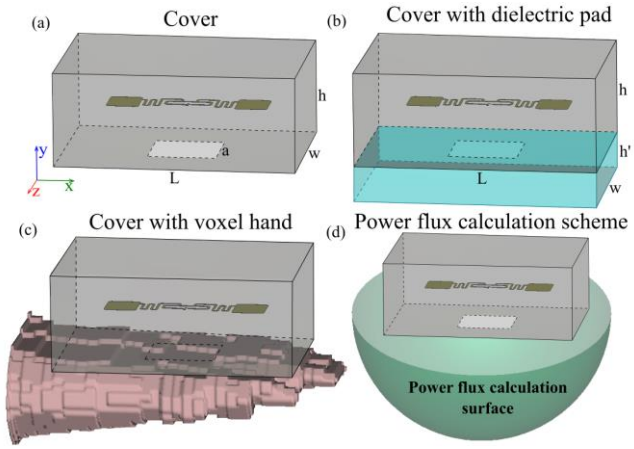

Figure 2. (a) UHF RFID tag (AZ 9662) shielded by a metallic cover with an aperture. (b) The shielded tag with a dielectric pad ($\varepsilon = 30$), placed underneath. (c) The shielded tag with a voxel model of a human arm, placed underneath. (d) The geometry with a virtual hemisphere through which the power flux is integrated.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAP.2021.3118846, IEEE Transactions on Antennas and Propagation

The relevant far-field parameter is the antenna gain, which will be investigated as well. Three scenarios were considered - (i) aperture in free space, (ii) aperture covered with a dielectric pad - height h' = 15 mm and dielectric permittivity ε = 30, and (iii) voxel model of an arm (Katja from CST voxel family, placed near the aperture).

For downlink calculations, the structure was excited by a plane wave, propagating along the z-axis and polarized along the x-axis, and a current through the chip was calculated. Figure 3a demonstrates the current in logarithmic scale as a function of frequency in the range of 800-1000 MHz. Orders of magnitude suppression owing to the smart cover can be seen. For an uplink calculation, a chip (passive lumped element) was replaced by a numerical port with the same complex impedance, and the power flux through the hemisphere along with the antenna gain was calculated (Fig. 3b). It can be seen that introducing the dielectric pad increases the integrated power flux by at least two orders of magnitude, as was expected in the preliminary discussion. However, the pad is just a mere approximation of a human hand. A hand, being around 50-60% water, has a more complex dielectric permittivity and a non-trivial shape. Nevertheless, the voxel model demonstrates a significant one-order improvement in the integrated power flux.

The performance of the system can now be assessed by considering the link budget. The link budget equations include tag antenna gain, and evaluating this parameter allows obtaining a clear understanding of the shielding impact. The black stars in Fig. 3b correspond to the realized gain values. To calculate the reading distance, we use the Friis' model [16]:

$$L = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_{TR} G_t}{P_{ch}}}, \qquad (1)$$

where the parameters are given in Table 1. The overall reading range is determined by the minimum, set by either up or down link limiting factors. Typically, chip activation is the bottleneck and, hence, Eq. 1 is provided for making the reading range assessment.

Table 1. Parameters of the RFID system for link budget calculations.

Parameter	Physical meaning	Value
P_t	Power transmitted by the reader	0.63 W (28 dBm)
G_{TR}	Gain of the reader Tx/Rx antenna	8 dBi
G_t	Realized gain of the tag	Aperture a = 20 mm: -46 dBi (cover) -31 dBi (hand) -22 dBi (dielectric pad) Aperture a = 30 mm: -36 dBi (cover) -23 dBi (hand) -15 dBi (dielectric pad)
P_{ch}	Chip sensitivity	$1 \cdot 10^{-5}$ W
λ	Wavelength	0.33 m
L	Reading distance	Aperture a = 20 mm: 8 cm (cover) 44 cm (hand) 128 cm (dielectric pad) Aperture a = 30 mm: 26 cm (cover) 115 cm (hand) 296 cm (dielectric pad)

The results, summarized in Table 1, demonstrate that the hand's activation allows increasing the reading range of the shielded tag by a factor of 4.5-5.5 depending on aperture size. In contrast, the dielectric pad can increase it by order of magnitude. Note that linear-scale gain coefficients are placed under the square root for calculating the reading range. These predictions are in good agreement with the experimental study presented in the next section. The custom-made antenna design can further improve performances, e.g., [17],[18].

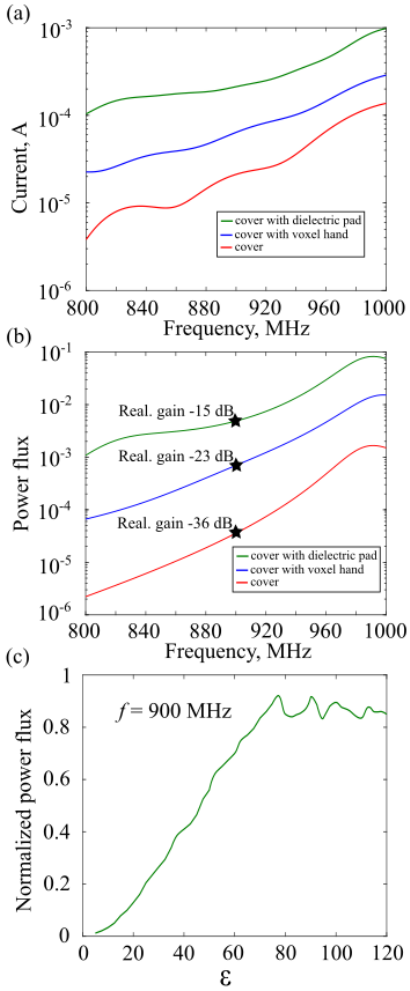

Figure 3. Current (a) and integrated power flux (b) spectra for three scenarios – (i) shielded tag in a free space (red line), (ii) shielded tag with a dielectric pad attached (green line), (iii) shielded tag with a voxel hand attached (blue line). Black stars – realized gain of corresponding systems, where the tag is connected to an active impedance matched port. (c) Integrated power flux as a function of the dielectric pad permittivity.

In terms of practical realizations, it is worth noting that hands' electromagnetic parameters can vary from user to user, making an accurate prediction to rely on statistics. Though the

last aspect will be addressed in the experimental section, the impact of permittivity can be accurately studied using an example of the nonresonant dielectric pad. Figure 3c shows the integrated power flux at 900 MHz as a function of the pad's permittivity. After a certain value permittivity (~80), the total power saturates. This results from the fact that the aperture is not resonant, and after becoming electromagnetically larger than half-a-wavelength, it starts transmitting. However, the internal arrangement of the tag has an influence. Linear sensitivity to permittivity fluctuations in the range 30-40 (expected hand permittivity dispersion) indicates that an additional optimization can further reduce device sensitivity to an end-user.

Another important parameter, which might play a role, is the aperture shape. While in the previous discussion, a square shape was used, other configurations might provide better performance. A hypothesis, which can be made, is that the effect relies on edges diffraction. If it was true, the device had to be extremely sensitive to the mutual orientation between the aperture and an activating hand. Obviously, this aspect might have a negative impact on practical aspects. However, we will show that the hypothesis is wrong, and the aperture's shape has a minor impact on the phenomenon.

Figure 4a summarizes the performances with rectangular and circular apertures. The integrated power flux was compared for those cases and showed no considerable difference. The areas of the apertures were kept the same for a fair comparison. The intermediate summary here is that the overall aperture's area is the key parameters that govern the performance.

The final step before the experimental verification is to assess the forward-to-backward ratio of the active antenna (uplink operation). From the security standpoint, this aspect is important since the card can be placed in a pocket close to a body, which poses similar electromagnetic characteristics as an activating hand. Figure 4b shows the electrical field amplitude at the X-Y plane (recall Fig. 2 for the coordinate system). It can be seen that the structure does radiate backward, but it 8 dB less intense than the main lobe towards the aperture. This parameter is satisfactory but can be further improved by shaping the metal enclosure.

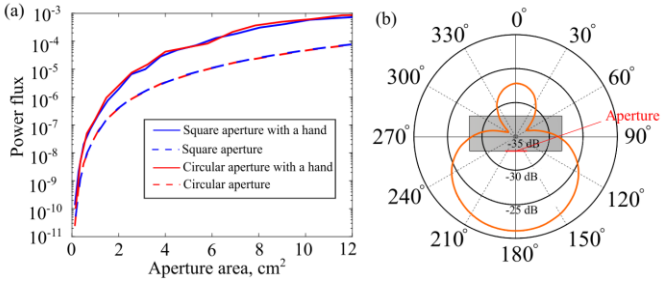

Figure 4. (a) Integrated power flux as a function of the aperture area. Square aperture – blue line, Circular – red line. Dashed lines – no activation hand, solid lines – a voxel hand attached. (b) Electric field intensity (far-field component) for the square aperture.

III. Experimental Demonstration

After discussing the design principles, an emulation of the far-field attack was made. A readout experiment was performed in an anechoic chamber. A common commercial RFID tag Alien LX-9640 was placed in the center of a polystyrene block (transparent for waves at 900 MHz) with the same dimensions as in the numerical simulations (length = 105 mm, width = 75 mm, and height = 40 mm (see Figure 2a). The block was covered with 25 μm aluminium foil (see an inset to Figure 5a). An aperture was cut in the center of one of the largest sides, exactly as it was configured in the numerical design.

The structure was evaluated in a long-range readout configuration (the photograph of the experiment layout is shown in Figure 5a). A reader device (model AS3992 LEO) was plugged into a laptop via USB port, and the maximum reading distance at the frequency of 915 MHz was monitored with the software provided by the vendor. The standard reader device comes with a low gain PCB patch antenna. This configuration is not designed to provide a long reading range. To perform the far-field attack, this antenna was replaced with a custom-made Yagi-Uda antenna that had four directors delivering an 8 dBi gain. The antenna was matched to operate at 890-930 MHz frequency band (inset to Fig. 5a).

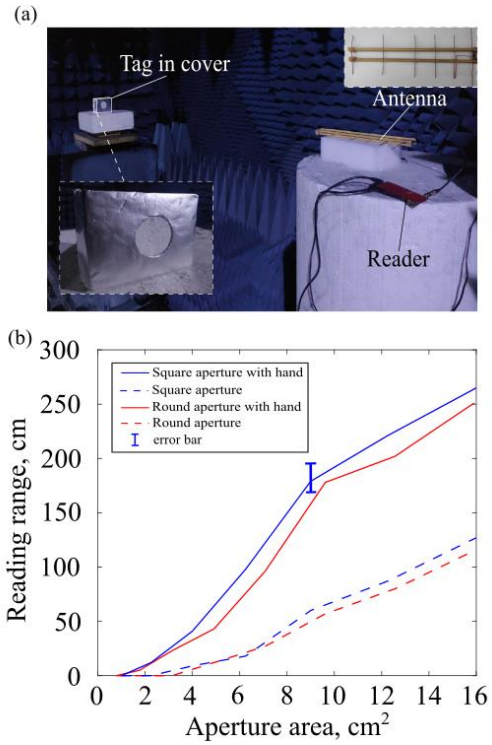

Figure 5. (a) Photo of the experimental setup in an anechoic chamber. Insets show the shielded tag and the reader antenna. (b) The maximal reading range as a function of the aperture area. The blue color lines correspond to the measurements with the square aperture; the red color lines correspond to the measurements with the circular aperture. The dashed lines indicate no activation hand; the solid lines indicate a hand attached near the aperture. The error bar corresponds to the measurements with three different hands, activating the square aperture.

The tag was placed in the antenna's E-plane and accurately moved away from the minimal distance until the received signal amplitude fell below the reader's sensitivity. This is the maximally obtainable reading distance. After that, the same measurement was made with a human arm placed near the aperture (as shown in Fig. 2c). Figure 5b demonstrates the

maximal reading range of the shielded tag as a function of the aperture's area with and without hand activation. Both circular and square apertures were tested and provided nearly the same results, as was predicted in the numerical section. To demonstrate tolerance to an end-user, measurements with three different hands were made for the fixed-size square aperture (see the error bar in Fig. 5b). The results show that the proposed realization has only a minor dependence on an end-user, making the entire concept practically relevant.

Finally, the optimal parameters of the system can be set – apertures with areas below 2 cm^2 are secure – cannot be interrogated without an authorization. Authorized access can be done from short distances, ensuring normal wireless operation of the device. The aperture size between 2 cm^2 and 12 cm^2 prevents a theft from distances, larger than 50-60 cm, and allows extending the reading rage of the authorized tag up to 2m. Further increase of the aperture size does not provide an advantage against far-field attacks.

IV. Conclusion

Introducing a hardware protection layer to communication security can significantly enhance the sustainability of a channel to various types of attack. Physical protection can rely on unpredictable, chaotic behavior, e.g., celebrated Chua circuit [19], and on more exotic modern approaches, e.g. [20],[21],[22]. This report demonstrated a hardware security layer, protecting RFID cards from the so-called far-field attack. We demonstrated that a smart cover could practically eliminate the capability of the readout without authorization. The latter is provided by holding a card in hand – the high dielectric constant of a human body virtually makes the initially opaque enclosure transparent. The set of optimizations verified with the experiment allows finding reliable designs. The proposed type of protection can be immediately introduced within the exiting regulated RFID technology without making changes in circuitry. This property is exceptionally valuable from a technological standpoint.

AKNOWLEGEMENT

The authors thank Dr. Elena Bazanova for her critical reading of the manuscript and useful suggestions.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9. Institute of Electrical and Electronics Engineers Inc., pp. 1727–1765, 01-Sep-2016, doi: 10.1109/JPROC.2016.2558521.

[2] S. B. Miles, S. E. Sarma, and J. R. Williams, *RFID Technology and Applications*. Cambridge University Press, 2011.

[3] P.-H. Thevenon, O. Savry, S. Tedjini, and R. Malherbi-Martins, "Attacks on the HF Physical Layer of Contactless and RFID Systems," in *Current Trends and Challenges in RFID*, InTech, 2011.

[4] D. Trček and P. Jäppinen, "RFID security," in *RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations*, vol. 9, no. 4, CRC Press, 2009, pp. 147–168.

[5] I. Kirschenbaum, A. W.-U. S. Symposium, and U. 2006, "How to Build a Low-Cost, Extended-Range RFID Skimmer.," *usenix.org*.

[6] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard systems," in *Proceedings - First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005*, 2005, vol. 2005, pp. 47–58, doi: 10.1109/SECURECOMM.2005.32.

[7] D. Dobkin, *The RF in RFID: Passive UHF RFID in Practice*. Oxford: Elsevier, 2007.

[8] D. Dobrykh *et al.*, "Long-range miniaturized ceramic RFID tags," *IEEE Trans. Antennas Propag.*, 2020, doi: 10.1109/TAP.2020.3037663.

[9] F. K. Byondi and Y. Chung, "Longest-Range UHF RFID Sensor Tag Antenna for IoT Applied for Metal and Non-Metal Objects," *Sensors*, vol. 19, no. 24, p. 5460, Dec. 2019, doi: 10.3390/s19245460.

[10] Y. He, "Wireless corrosion monitoring sensors based on electromagnetic interference shielding of RFID transponders," *Corrosion*, vol. 76, no. 4, pp. 411–423, Apr. 2020, doi: 10.5006/3384.

[11] S. A. Abdulrazzaq, A. Prof, and J. S. Aziz, "SAR Simulation in Human Head Exposed to RF Signals and Safety Precautions," *IJCSET*, vol. 3, no. 9, pp. 334–340, 2013.

[12] D. D. L. Chung, "Materials for Electromagnetic Interference Shielding," *J. Mater. Eng. Perform.*, vol. 9, no. 3, pp. 350–354, Jun. 2000, doi: 10.1361/105994900770346042.

[13] M. Jaroszewski, S. Thomas, and A. V. Rane, Eds., *Advanced Materials for Electromagnetic Shielding*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2018.

[14] M. Faraday, "Experimental Researches in Electricity, Volume 1," *Repr. from Philos. Trans. 1831-1838. London Richard John Edward Taylor*, vol. 1, p. 366, 1849.

[15] D. E. Brown, *RFID implementation*. McGraw-Hill, 2007.

[16] P. V. Nikitin and K. V. S. Rao, "Theory and measurement of backscattering from RFID tags," *IEEE Antennas Propag. Mag.*, vol. 48, no. 6, pp. 212–218, Dec. 2006, doi: 10.1109/MAP.2006.323323.

[17] D. Dobrykh *et al.*, "Multipole engineering for enhanced backscattering modulation," *Phys. Rev. B*, vol. 102, no. 19, p. 195129, Nov. 2020, doi: 10.1103/PhysRevB.102.195129.

[18] S. Krasikov *et al.*, "Multipolar Engineering of Subwavelength Dielectric Particles for Scattering Enhancement," *Phys. Rev. Appl.*, vol. 15, no. 2, p. 024052, Feb. 2021, doi: 10.1103/PhysRevApplied.15.024052.

[19] R. N. Madan, *Chua's Circuit: A Paradigm for Chaos*, vol. 1. WORLD SCIENTIFIC, 1993.

[20] N. Engheta, "Circuits with light at nanoscales: Optical nanocircuits inspired by metamaterials," *Science*, vol. 317, no. 5845. American

Association for the Advancement of Science, pp. 1698–1702, Sep-2007, doi: 10.1126/science.1133268.

[21] P. Ma, L. Gao, P. Ginzburg, and R. E. Noskov, "Nonlinear Nanophotonic Circuitry: Tristable and Astable Multivibrators and Chaos Generator," *Laser Photon. Rev.*, vol. 14, no. 3, p. 1900304, Mar. 2020, doi: 10.1002/lpor.201900304.

[22] P. Ma, L. Gao, P. Ginzburg, and R. E. Noskov, "Ultrafast cryptography with indefinitely switchable optical nanoantennas," *Light Sci. Appl.*, vol. 7, no. 1, pp. 2047–7538, Dec. 2018, doi: 10.1038/s41377-018-0079-9.