Journal of Engineering Technology and Applied Physics

An Enhanced Security Lock Using A Split-Ring Resonator

Loh Siu Hong[1,*], Yeap Kim Ho[1], Tan Zi Kang[1], Lee Han Kee[1] and Tan Ming Hui[2]
[1]*Faculty of Engineering and Green Technology, Universiti Tunku Abdul Rahman, 31900 Kampar, Malaysia.*
[2]*Faculty of Innovation and Technology, School of Engineering, Taylor's University, No. 1, Jalan Taylor's, 47500 Subang Jaya, Selangor, Malaysia.*
[*]*Corresponding author*: yeapkh@utar.edu.my, *ORCiD*: 0000-0001-7043-649X
https://doi.org/10.33093/jetap.2026.8.2.15
Manuscript Received: 16 January 2026, Revised: 11 March 2026, Accepted: 17 March 2026, Published: 15 September 2026

***Abstract* — In this paper, we present a novel approach to enhancing security in locking systems by incorporating microwave technology and split-ring resonators (SRRs). The locking mechanism exploits variations in the transmission coefficient and resonant frequency of a microwave resonator to enable secure authentication. The proposed lock is fabricated on an FR4 substrate, with a metallic SRR etched on the top layer and a coplanar waveguide (CPW) on the bottom side. By rotating the SRR to different orientations, it exhibits distinct frequency responses — each characterized by unique resonant frequencies and transmission coefficient magnitudes. As a proof of concept, we investigated two representative orientations (i.e., with the SRR gap positioned at 0° and 30°) to demonstrate the efficacy of the system. The user is required to store the initial configuration in a microcontroller. Once the security system is activated, the assembly can be removed. To disable the system, an assembly with an identical configuration must be reinserted. The microcontroller then evaluates the measured values against the original lock configuration. If the values align within a 5% tolerance range of the stored configuration, the security system is deactivated. The results show that even a slight angular variation of the SRR is sufficient to produce distinct electromagnetic signatures. Thus, with the integration of microwave technology and signal processing, this planar microwave-based locking concept has the potential to revolutionize traditional locking systems.**

Keywords— Split-ring resonators, Metamaterials, Resonant frequencies, Transmission coefficients, Coplanar waveguide.

I. INTRODUCTION

An effective locking system is essential for ensuring home security. In particular, strong and secure locking mechanisms protect personal belongings and, therefore, provide peace of mind. The review of multifactor door locking systems in [1] strongly suggests that the safety of a home is as important as its structural soundness, highlighting the need for enhanced security measures in modern residences. Traditional locks, such as padlocks, often fail to provide sufficient protection against increasingly sophisticated burglary methods. As evidenced in [2, 3], these traditional systems can be easily breached, thereby calling for more robust solutions.

Over the years, we have witnessed improvements in locking systems. To enhance security, many contemporary locks have integrated sophisticated technologies such as electronic keypads, radio frequency identification (RFID), and biometric recognition [3, 4]. Nevertheless, these systems are not without limitations. Some impose relatively high installation costs and are often unaffordable for households with average income levels [1, 3]. Furthermore, numerous smart locks continue to rely on physical keys or codes that remain susceptible to duplication or hacking [5–12].

Here, we propose a novel locking system based on microwave resonators to address these challenges. We demonstrate that our method leverages the distinctive characteristics of metamaterials (specifically, a split-ring resonator) to achieve a higher level of security. In our system, a signal processing unit serves as the control interface, which deactivates the lock only when the user places the correct assembly with the split-ring resonator (SRR) in the proper orientation. The system performs two levels of verification before unlocking: it first compares the intensity of the transmission dip and then the resonant frequency against the initial configuration stored in the control unit. Without prior knowledge of the geometries and

Published by MMU PRESS. URL: https://journals.mmupress.com/index.php/jetap/index

orientations of the SRR, unauthorized individuals will find it difficult to deactivate the security system.

Unlike conventional mechanical or electronic locks, our system uses the distinctive electromagnetic response of a split-ring resonator (SRR) as a physical key for authentication. Security is enforced through two independent checks: the resonant frequency and the transmission coefficient magnitude, both of which depend on the SRR's geometry and orientation. This dual-parameter verification creates a level of physical unclonability and signal-based authentication that traditional locks, keypads, or biometric systems cannot achieve, offering a new approach to secure and tamper-resistant access control.

In summary, although current locking mechanisms have advanced in terms of security technology, they still exhibit inherent weaknesses, which necessitate the development of a more secure and affordable solution, such as the proposed microwave resonator-based system. The proposed approach does not only overcome the shortcomings of existing systems but it also enhances security by leveraging advanced electromagnetic characteristics and stringent access control mechanisms.

II. OPERATION PRINCIPLE

Figure 1 presents the overall architecture of the proposed microwave locking system. The framework incorporates an SRR-based key, a microwave measurement unit for interrogating the resonator response, a signal processing stage that extracts the relevant electromagnetic signatures, and an Arduino-based controller responsible for verifying the unlocking condition. Together, these components establish the operational sequence through which the locking and authentication process is carried out.

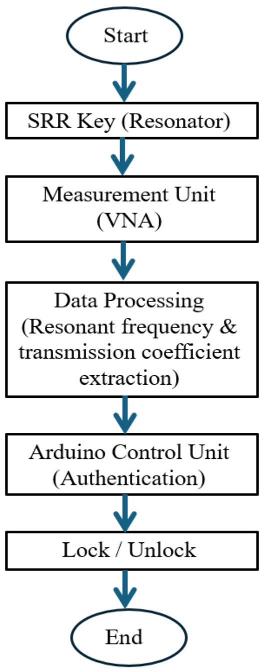


Fig. 1. System architecture of the proposed microwave SRR-based locking mechanism.

In our proposed locking system, we have developed a split-ring resonator (SRR) that is coupled with a coplanar waveguide (CPW) transmission line to produce a transmission dip and resonant frequency. When an electromagnetic wave traverses the SRR, it generates both inductive and capacitive effects, thereby forming a resonant circuit whose resonant frequency is highly sensitive to the incident electromagnetic field. The resonant frequency, denoted as f_r, can be expressed mathematically as [13 – 15]

$$f_{\mathrm{r}} = \frac{1}{2\pi\sqrt{L_{eq}C_{eq}}}, \quad (1)$$

, where L_{eq} and C_{eq} denote, respectively, the net series inductance and the total equivalent capacitance within the SRR. As discussed by Naqui *et al.* [16] and demonstrated by Ong *et al.* [17], the intensity of the magnetic field produced within the structure is dependent on the orientation of the SRR. As a result, when the SRR is orientated to different angles, the corresponding transmission coefficient dip varies accordingly as well. Changes in the SRR orientation also affect L_{eq} and C_{eq}, resulting in detuning effect in the resonant frequency.

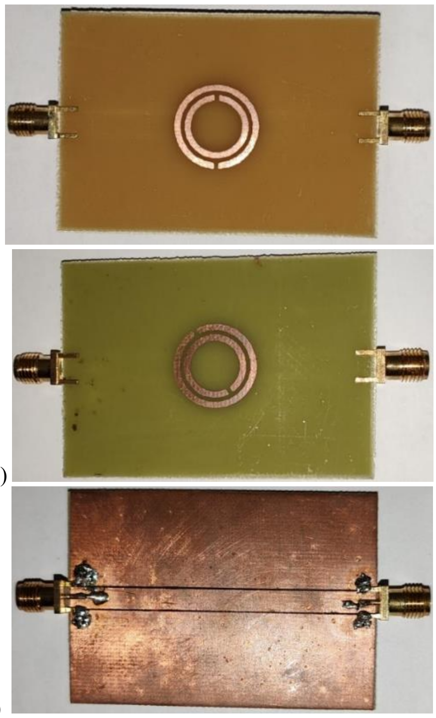
Based on this principle, our system allows a user to establish the lock by recording the initial magnitude of the transmission dip and the resonant frequency at a designated SRR orientation using a vector network analyzer (VNA) and storing these values in a control unit. In the experimental prototype, the SRR assembly includes SMA connectors that allow direct connection to the VNA. These connectors enable the microwave signal from the VNA to excite the CPW transmission line integrated with the SRR, making it possible to measure the transmission coefficient. To unlock the system, the user is required to select a substrate with the SRR positioned identically to that used in the original locking configuration and connect it to the VNA. The VNA subsequently measures the magnitude of the transmission dip and the resonant frequency and extracts this information, transmitting it to the control unit for post-processing. The role of the control unit is to compare both the resonant frequency and the magnitude of the transmission coefficient against the stored initial configuration. The system will unlock only if both measurements fall within a 5% tolerance, indicating that the user has employed a "key" with the correct geometry and SRR orientation. Any mismatch exceeding 5% in either or both the resonant frequency and the transmission coefficient will cause the system to remain locked.

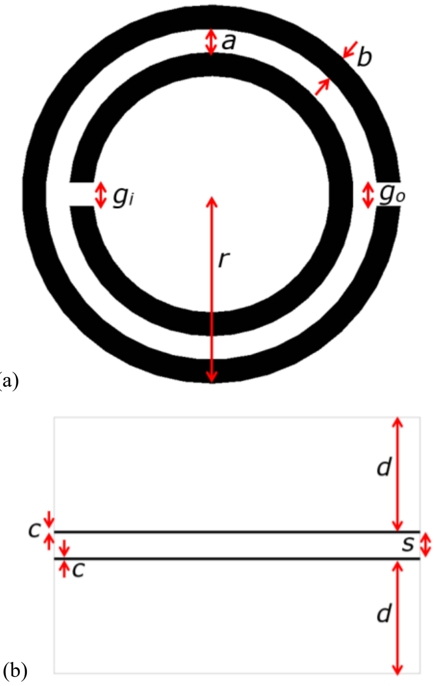
In this work, the vector network analyzer (VNA) is used mainly to experimentally characterise the resonant behaviour of the SRR structure and to verify the feasibility of the proposed locking mechanism. The scattering parameters obtained from the measurements are exported in the form of an S2P file, from which the resonant frequency and the magnitude of the transmission coefficient are extracted through post-processing. These extracted values are subsequently supplied to the control unit, where they are used as reference parameters during the locking and unlocking verification process.

It is worth noting that the use of a laboratory VNA is not essential for practical implementations. In many microwave sensing applications, resonant structures are first characterised using a VNA during the development stage, after which their responses are monitored using compact RF interrogation circuits or frequency-tracking modules integrated into dedicated electronic platforms [18–20]. In the present work, the VNA therefore serves mainly as a measurement tool for validating the proof-of-concept prototype.

III. DESIGN EXAMPLE

Since this work is intended as a proof-of-concept, only two sets of SRRs with different orientations were fabricated to demonstrate the effectiveness and usability of the proposed security lock. As shown in Fig. 2, the SRRs are oriented at 0° and 30°. These two angles were intentionally selected as representative cases to verify the fundamental operating principle, rather than to exhaustively characterise all possible orientations. These two angles were picked arbitrarily for demonstration, to show how changing the SRR orientation leads to clearly different electromagnetic responses. The system first records and stores the transmission dip and resonant frequency of the SRR positioned at 30°, followed by attempts to unlock the system using SRRs aligned at both 0° and 30°. As a reference, when the lock was initially set, the resonant frequency f_r and the transmission dip T were measured at 2.750 GHz and -4.67 dB, respectively.


(a)
(b)
(c)
Fig. 2. Top views of the lock assemblies with SRRs oriented at (a) 0° and (b) 30°, along with the (c) bottom view showing a CPW transmission line loaded onto the structure.



(a)
(b)
Fig. 3. Geometric structures of (a) the SRR and (b) the CPW used in the lock assemblies.

Table I. Parameters of the SRR and CPW used in the lock assemblies.

Parameter	**Value (mm)**
g_i	1
g_o	1
R	8
A	1
B	1
C	0.4
D	5.6
s	4

The geometric specifications of the design are given in Fig. 3 and Table I. The assembly has dimensions of 42 mm in length, 16 mm in width, and 1.6 mm in thickness, and it is constructed on a flame-retardant FR4 epoxy substrate characterized by a dielectric constant of 4.4 and a loss tangent of 0.035.

Figure 4 and Fig. 5 show the frequency responses for the initial locking configuration (SRR at 30°) and the subsequent unlocking attempts using SRRs oriented at 30° and 0°, respectively. To provide clear experimental validation, Fig. 6 and Fig. 7 illustrate the system's practical behavior through LED indicators: the green LED in Fig. 6 signals a successful unlocking attempt when the SRR orientation matches the stored configuration, while the red LED in Fig. 7 highlights an unsuccessful attempt due to mismatched orientation.

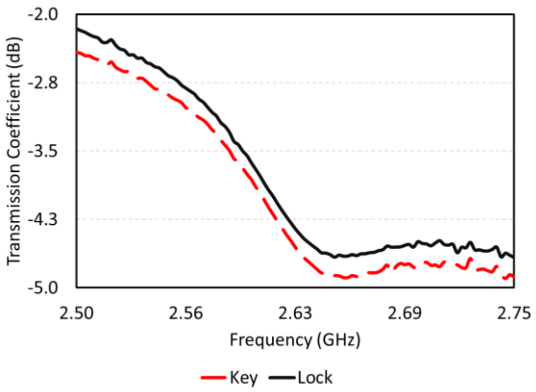


Fig. 4. Frequency response for the initial locking configuration at 30° (solid line) and the unlocking attempt with the SRR oriented at 30° (dashed line).

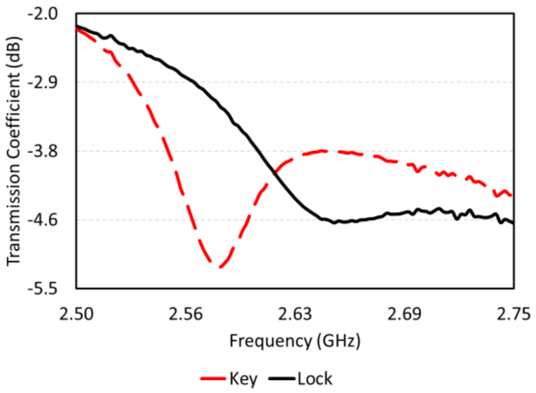


Fig. 5. Frequency response for the initial locking configuration at 30° (solid line) and the unlocking attempt with the SRR oriented at 0° (dashed line).

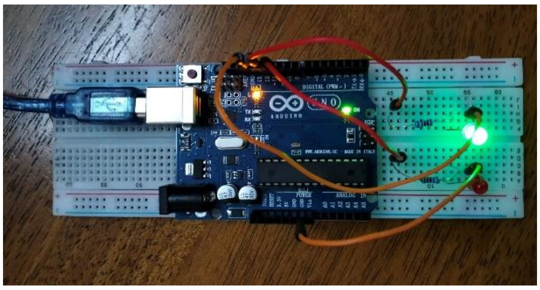


Fig. 6. Successful unlocking of the system with an SRR oriented at 30°; the green LED indicates that the measured resonant frequency and transmission dip match the stored configuration within the allowed tolerance.

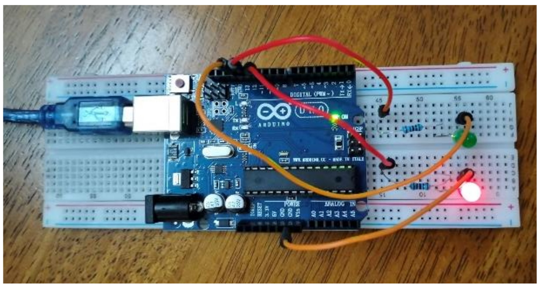


Fig. 7. Failed unlocking attempt with an SRR oriented at 0°; the red LED shows a discrepancy in the measured resonant frequency and transmission dip, keeping the system locked.

When the SRR is positioned at 30°, the measured resonant frequency f_r and transmission dip T are 2.744 GHz and -4.90 dB, both within the 5% tolerance of the initial configuration. Feeding these values into the Arduino Uno control unit confirms a valid unlocking, as indicated by the green LED. Conversely, using an SRR oriented at 0° results in f_r and T values of 2.583 GHz and -5.23 dB, exceeding the tolerance and causing the system to remain locked, as reflected by the red LED. These results demonstrate the high sensitivity of the proposed system to SRR orientation and confirm that even small angular deviations produce clearly distinguishable outcomes. Including the LED indicator figures reinforces the experimental evidence of the locking mechanism's functionality and provides a direct visual confirmation of successful and failed unlocking attempts.

IV. CONCLUSION

In summary, the microwave lock system proposed herein presents a secured and novel security solution by utilizing the distinct electromagnetic characteristics of a split-ring resonator (SRR) along with a coplanar waveguide (CPW) transmission line. This configuration offers several benefits compared to traditional locks, such as improved security through unique, geometry- and orientation-sensitive frequency responses that are challenging to duplicate or circumvent. Although only two SRR orientations were examined, the results sufficiently demonstrate the feasibility of the proposed mechanism.

Moreover, the microwave lock reduces the risks associated with password- or biometric-based smart locks, which are vulnerable to hacking, cloning, and software-related threats. By relying on both a designated resonant frequency (governed by the geometry of the SRR) and the magnitude of the transmission dip (dictated by the SRR orientation), together with a narrow tolerance to account for noise and minor fabrication mismatches, the system ensures high accuracy and can be deactivated only under precise electromagnetic conditions, thereby significantly enhancing the level of security.

ACKNOWLEDGEMENT

The support by Universiti Tunku Abdul Rahman is greatly appreciated.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Siu Hong Loh: Writing-Original Draft Preparation, Conceptualization; Kim Ho Yeap: Supervision, Formal Analysis; Zi Kang Tan: Methodology, Validation; Han Kee Lee: Visualization, Data Curation; Ming Hui Tan: Investigation, Writing–Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests was disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. https://publicationethics.org/

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article, as no datasets were generated or analyzed.

REFERENCES

[1] Y. Motwani, S. Seth, D. Dixit, A. Bagubali and R. Rajesh, "Multifactor Door Locking Systems: A Review," *Mater. Today*: *Proc.*, vol. 46, no. 17, pp. 7973 – 7979, 2021.

[2] S. Shetty, S. Shetty, V. Vishwakarma and S. Patil, "Review Paper on Door Lock Security Systems," in *Int. Conf. on Converg. to Digit. World* - *Quo Vadis,* Mumbai, India, pp. 1 – 4, 2020.

[3] V. Sharma, T. Todia and U. Vishwakarma, "Review Paper on Door Lock Security Systems", *Int. J. Res. Appl. Sci. & Eng. Technol.*, vol. 10, no. 5, pp. 3002 – 3005, 2022.

[4] K. H. Yeap, "Design of A Keyless Coded Home Lock System using Verilog Hardware Description Language," *Int. J. Electron., Comput. & Commun. Technol.*, vol. 3, no. 1, pp. 10 – 16, 2012.

[5] S. J. Kulkarni, S. N. Jadhav and M. R. Dhavale, "Remote Operated Shutter System with Fingerprint Lock," *Int. J. Trend Sci. Res. and Develop.*, vol. 3, no. 3 pp. 1554 – 1557, 2019.

[6] T. Q. Huang, "Study of Driving Force and Synchronization on A Space Docking Lock System," *Adv. Mater, Res.*, vol. 562, pp. 1137 – 1141, 2012.

[7] Q. Y. Huo and Y. Zhang, "Semi-Preemptible Range Lock in Parallel Network File System (pNFS)," *Adv. Mater. Res.*, vol. 546, pp. 1250 – 1255, 2012.

[8] S. Sharma, A. T. Pradhuman and A. Rehalia, "IOT Based Lock System," *Int. J. Res. Appl. Sci. and Eng. Technol.*, vol. 8, no. 12, pp. 400 – 403, 2020.

[9] T. Diggewadi, S. Patil, N. M. Khan and A. Gudnavar, "Customized Door Lock System," *Int. Adv. Res. J. Sci., Eng. and Technol.*, vol. 4, no. 2, pp. 37 – 42, 2017.

[10] A. A. Shankar, P. R. K. Sastry, A. L. V. Ram and A. Vamsidhar, "Finger Print Based Door Locking System," *Int. J. Eng. and Comput. Sci.*, vol. 4, pp. 10810 – 10814, 2015.

[11] B. Thiske, "Color Based Pattern Lock System," *Int. J. Res. Appl. Sci. and Eng. Technol.*, vol. 6, pp. 3366 – 3367, 2018.

[12] P. M. König, R. Roth and S. Dietrich, "Lock and Key Model System," *Europhys. Lett.*, vol. 84, no. 6, pp. 68006, 2008.

[13] Z. X. Oh, K. H. Yeap, Z. L. Chong and N. F. A. Rahman, "Square Split-Ring Resonator-Based Microwave Sensor for Dielectric Constant Measurement," *Nat. Acad. Sci. Lett.*, pp. 1-4, 2026.

[14] K. H. Yeap *et al.*, "Enhanced Sensitivity Microfluidic Microwave Sensor for Liquid Characterization," *Processes*, vol. 13, no. 7, pp. 2183, 2025.

[15] K. H. Yeap, J. L. Lam, S. H. Loh, V. Dakulagi and A. U. Mazlan, "Microwave Sensor for Sodium Chloride Density Measurement in Aqueous Solutions", *J. Eng. Technol. and Appl. Phys.*, vol. 6, pp. 52 – 56, 2024.

[16] J. Naqui, J. Coromina, A. Karami-Horestani, C. Fumeaux and F. Martín, "Angular Displacement and Velocity Sensors Based on Coplanar Waveguides (CPWs) Loaded with S-Shaped Split Ring Resonators (S-SRR)," *Sensors*, vol. 15, no.5, pp. 9628 – 9650, 2015.

[17] C. S. Ong, K. H. Yeap, Z. L. Chong and H. Nisar, "An Analysis of Split-Ring Resonators and Potential Barcode Application," *J. Eng. Technol. and Appl. Phys.*, vol. 6, pp. 76 – 81, 2024.

[18] W. J. Wu, W. S. Zhao and W. Wang, "A Novel Microwave Sensor System Based on Feedback-Type Oscillator and Modified Coplanar Waveguide Resonator for Retrieving Complex Permittivity of Liquid Samples," *IEEE Sensors J.*, vol. 24, no. 13, pp. 20571-20586, 2024.

[19] W. J. Wu and W. S. Zhao, "A Microwave Sensor Based on Frequency-Locked Loop and Multiple Complementary Split-Ring Resonators for Retrieving Complex Permittivity of Liquid Samples," *IEEE Sensors J.*, vol. 23, no. 24, pp. 30345-30359, 2023.

[20] C. H. Tseng, C. H. Pai and H. C. Chang, "A New Microwave Oscillator-Based Microfluidic Dielectric Sensor," *IEEE Trans. Microw, Theor. and Techniq.*, vol. 72, no. 1, pp. 628-637, 2023.