(Received 1 March 2026, Accepted 2 April 2026, Scheduled 30 April 2026)

A Proximity-Activated UHF RFID Tag with a Detachable Coupling Loop for Enhanced Physical Layer Security

Hamza Othmani[1,*], Mohamed K. Azizi[2], and Luca Catarinucci[3]

[1] *Microwave Electronics Research Laboratory, Faculty of Sciences of Tunis University of Tunis El Manar, Tunis 2092, Tunisia*
[2] *Microwave Electronics Research Laboratory, Higher Institute of Arts and Multimedia University of Manouba, Manouba 2010, Tunisia*
[3] *Department of Innovation Engineering (EM-Tech Laboratory), University of Salento, Lecce 73100, Italy*

ABSTRACT: This paper presents a proximity-activated UHF RFID tag based on a discrete-component architecture aimed at enhancing user privacy at the physical layer. The RFID chip is physically separated from the main meandered dipole antenna and mounted on a *detachable* coupling loop. Tag activation occurs only when the loop is positioned at approximately 1 mm from the antenna, enabling near-field inductive coupling and conjugate impedance matching. In the default configuration, the chip remains effectively unreadable, while selective activation is achieved by applying the external coupling loop when tag interrogation is required. Two coupling-loop geometries are investigated: a simple rectangular loop and a multi-turn spiral loop, both integrated with capacitively loaded dipole antennas optimized for the European UHF RFID band at 866 MHz. Full-wave simulations confirm the intended on/off behavior, with minimum reflection coefficients of −34.8 dB at 866.7 MHz and −31.1 dB at 867 MHz, respectively. When the loop is removed, both designs exhibit severe impedance mismatch across the operating band. Experimental results validate the proposed concept. The rectangular loop achieves a peak read range of 6.0 m, while the spiral loop reaches 0.7 m. Misalignment tests indicate that both configurations maintain functionality under practical lateral and vertical offsets. Overall, the rectangular loop provides a wider and more robust activation region, making it suitable for applications requiring controlled, on-demand RFID readability for product authentication and quality verification without continuous exposure to RFID tracking.

1. INTRODUCTION

Radio Frequency Identification (RFID) technology has become an essential component of modern wireless identification systems, providing a reliable and contactless means for object tracking [1], access control [2], and inventory management [3]. Depending on their powering mechanism, RFID tags are classified as active [4], semi-active (battery-assisted passive) [5, 6], and passive types [7]. Active tags integrate an internal battery that powers both the integrated circuit (IC) and signal transmission, whereas passive tags rely entirely on the electromagnetic energy transmitted by the reader antenna to activate the IC. Semi-active tags combine both concepts, using an internal battery only to power the chip while maintaining passive back-scatter communication.

RFID systems operate across multiple standardized frequency bands, typically Low Frequency (LF, 125–134 kHz), High Frequency (HF, 13.56 MHz), and Ultra-High Frequency (UHF, 860–960 MHz), each offering different reading ranges and coupling mechanisms [8]. Communication between the reader and the tag relies on the modulation and back-scattering of electromagnetic waves, where the tag antenna captures the incident RF field and reflects a portion of it back to the reader. Functionally, a typical RFID tag consists of an antenna and an RFID chip, which together determine the system's impedance behavior and communication performance. The chip is often connected through a coupling loop, which enhances the induced current and facilitates efficient IC activation [9]. Depending on operating frequency, RFID tags can exploit inductive coupling (dominant at LF and HF) or radiative coupling (dominant at UHF) [10, 11]. Among these, passive UHF tags have gained wide adoption due to their low cost [12], long read range [13], and suitability for item-level identification in retail [14], logistics and industrial environments [15].

The increasing integration of RFID technology into retail [16], logistics [17], and product authentication systems has raised significant concerns regarding data security and privacy protection [18]. In conventional RFID tags, the chip remains continuously active within the interrogation range of any reader operating at the same frequency, making the stored information vulnerable to unauthorized scanning or cloning. Several studies have attempted to address this issue through cryptographic protocols, lightweight encryption algorithms, and coding-based authentication schemes [19–23]. These approaches improve data confidentiality, authentication, and resistance to cloning by protecting the exchanged information or the tag identity itself. However, they do not prevent the tag from being physically interrogated by a compatible reader within range, and they often rely on additional circuitry, key-management procedures, or increased implementation

* Corresponding author: Hamza Othmani (hamza.othmani.official@gmail.com).

TABLE 1. Representative RFID security approaches.

Approach	Mechanism	Layer
Klein Algorithm	Lightweight encryption	Software/Logic
Synchronized Secret	Cloning detection	Authentication
AES Encryption	UID encryption	Cryptographic
Our Approach	Physical antenna/chip separation	Physical

complexity, which may limit their adoption in low-cost RFID applications [24–26]. To overcome this limitation, other works have investigated physical-layer security approaches using shielding structures, selective detuning, or switchable connections; yet these methods often suffer from poor reliability, permanent detuning, or sensitivity to fabrication tolerances [27, 28].

Table 1 presents a comparative analysis of representative RFID security approaches reported in the literature. As shown, most existing methods aim to protect the communication layer through cryptographic or authentication-based strategies, including lightweight encryption [21], synchronized-secret schemes [23], and AES-based protection [22]. These approaches improve data confidentiality, message integrity, and resistance to cloning or unauthorized data extraction. However, they do not suppress the electromagnetic visibility of the tag itself, which remains susceptible to wireless interrogation by any compatible reader operating within its range. In contrast, the proposed architecture addresses this limitation directly at the physical layer by physically separating the RFID chip from the radiating element. In the absence of the external coupling element, the electromagnetic link required for efficient power transfer and backscatter communication is not established, and the tag therefore remains effectively unreadable in practice. RFID functionality is restored only when intentional proximity coupling is created. This operating principle provides an additional and complementary layer of protection for applications in which privacy preservation, controlled activation, and reduction of unauthorized scanning are critical requirements.

A practical scenario illustrating the relevance of the proposed concept is related to the verification of returned consumer goods. In many product categories, manufacturers must authenticate an item and retrieve its production data, for instance, to confirm its batch number, validate warranty conditions, or detect counterfeits. Embedding a conventional UHF RFID tag directly inside the product would simplify tracking, but may raise legitimate privacy concerns for end users, who could object to the presence of a permanently readable identifier after purchase.

The proposed architecture addresses this challenge by integrating only a minimal chip module equipped with a small inductive loop inside the product, which remains electromagnetically inert under normal conditions. In this default state, the module does not include a functional antenna and is therefore practically unreadable by standard UHF RFID readers, ensuring that no inadvertent tracking or long-range identification occurs once the product is in the hands of the customer.

When verification is required — such as during a return procedure or a quality inspection — the operator applies a thin detachable adhesive antenna specifically designed to couple with the internal loop. This auxiliary antenna is positioned on a predefined area of the product surface, enabling near-field inductive coupling at the required separation distance. Once the external antenna is applied, the two elements operate together as a functional tag, and the item can be read using a standard UHF RFID reader. After the inspection is completed, the adhesive antenna is removed, and the embedded module returns to its unreadable state.

This mechanism enables controlled and on-demand activation of RFID functionality without exposing the user to continuous tag readability. It provides a practical balance between traceability and privacy, allowing manufacturers to perform authentication and warranty verification while preventing persistent or unauthorized identification during normal use. An illustrative example of this operating principle is shown in Fig. 1, where the product remains unreadable until the external detachable antenna is intentionally applied to enable inductive coupling with the embedded chip module.

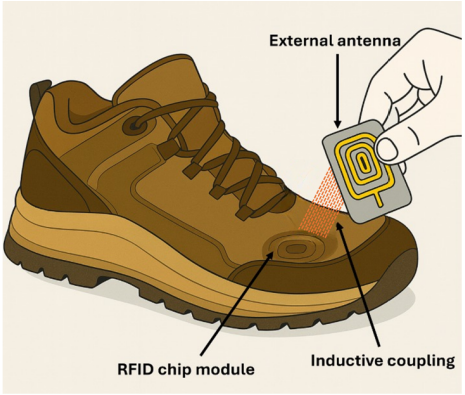

FIGURE 1. Illustrative example of a consumer product embedding an internal RFID chip module with an inductive coupling loop. The tag becomes readable only when an external detachable antenna is applied on the product surface for authentication or quality-control operations.

This paper is organized as follows. Section 2 describes the detailed design of the proposed RFID tag antennas. Design 1 employs a simple rectangular coupling loop, whereas Design 2 integrates a multi-turn spiral loop intended to investigate its influence on magnetic coupling strength and misalignment tolerance. Both tag antennas are based on meandered dipole structures optimized for operation in the European UHF RFID band centered at 866 MHz. Section 3 presents the full-wave elec-

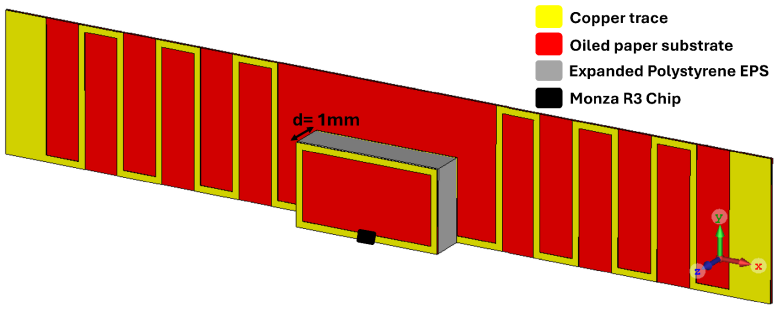

FIGURE 2. Architecture of the proposed proximity-activated RFID tag.

tromagnetic simulations carried out to analyze the activation and deactivation mechanisms and to optimize the geometrical parameters of both designs. Section 4 details the experimental validation performed using a Voyantic Tagformance system, including the measurement of the read range and an in-depth analysis of positional tolerance along the X-, Y-, and Z-axes to evaluate the practical robustness of the proposed concept. Finally, Section 5 discusses the main findings, summarizing the activation mechanism, robustness, and practical relevance of the tag.

2. ANTENNA ARCHITECTURE AND DESIGN METHODOLOGY

This work introduces a passive UHF RFID tag based on a physically segmented architecture. In this configuration, the radiating element is deliberately separated from the RFID integrated circuit (IC), forming a two-part system composed of a primary meandered dipole antenna and a detached chip module, as illustrated in Fig. 2. The operation of the tag is governed by a mechanical activation mechanism: the RFID chip is activated only when the detached module is positioned in close proximity to the antenna.

For proper activation, the chip module must be placed above the main antenna with a precisely defined vertical separation of 1 mm along the z-axis. This critical spacing is maintained by a layer of Expanded Polystyrene (EPS), chosen for its low dielectric permittivity ($\varepsilon_r \approx 1.03$) and its negligible influence on electromagnetic coupling in the near field. The mechanical rigidity of EPS also provides reliable control of the separation distance, preventing unwanted detuning during assembly or handling.

The RFID chip module hosts the Impinj Monza R3 IC [29], which is connected to a small copper loop acting as the coupling interface. When the module is in proximity of the antenna, magnetic coupling occurs between the loop and the integrated coupling region of the antenna, establishing conjugate impedance matching and enabling data back-scattering. When physically detached, the tag becomes completely deactivated, providing a user-controlled privacy mechanism at the hardware level.

This specific vertical spacing was determined through parametric simulation to be critical for meeting two essential design requirements: proper impedance matching between the antenna and the chip and efficient inductive coupling. These conditions are governed by the following fundamental relations.

Impedance Matching Condition: The maximum power transfer from the antenna to the chip occurs when their impedance is complex conjugated, as expressed by the following:

$$Z_{\text{ant}} = Z^*_{\text{chip}}, \tag{1}$$

where $Z_{\text{chip}} = 32 - j228\,\Omega$ is the input impedance of the Impinj Monza R3 integrated circuit. The degree of matching is practically assessed using the reflection coefficient Γ, which should be minimized according to:

$$\Gamma = \frac{Z_{\text{ant}} - Z^*_{\text{chip}}}{Z_{\text{ant}} + Z_{\text{chip}}}. \tag{2}$$

Inductive Coupling Mechanism: The inductive coupling between the meandered dipole antenna and the loop of the chip module can be modeled as a transformer. The input impedance observed at the chip terminals is therefore given by:

$$Z_{\text{in}} = Z_{\text{loop}} + \frac{(2\pi f M)^2}{Z_{\text{ant}}}, \tag{3}$$

where $Z_{\text{loop}} = j2\pi f L_{\text{loop}}$ is the impedance of the isolated coupling loop; L_{loop} is its self-inductance; M represents the mutual inductance; and f is the operating frequency. While the transformer model in Eq. (3) provides a useful conceptual description of the inductive coupling mechanism, its quantitative accuracy at UHF frequencies is limited by radiative effects and parasitic capacitances. Therefore, all design optimization and performance characterization results presented in this work are based on full-wave electromagnetic simulations performed in CST Studio Suite and on experimental validation. The optimized 1 mm separation along the z-axis ensures a suitable value of M, providing the transformed impedance Z_{in} that satisfies the conjugate-matching condition in Eq. (1). This configuration enables efficient energy transfer and reliable activation of the tag.

Beyond this transformer-based description, the interaction between the chip loop and the meandered dipole can also be interpreted using the classical model of two resonant elements coupled through a mutual inductance. In this framework, the coupling strength is quantified by the coupling coefficient

$$k = \frac{M}{\sqrt{L_1 L_2}}, \tag{4}$$

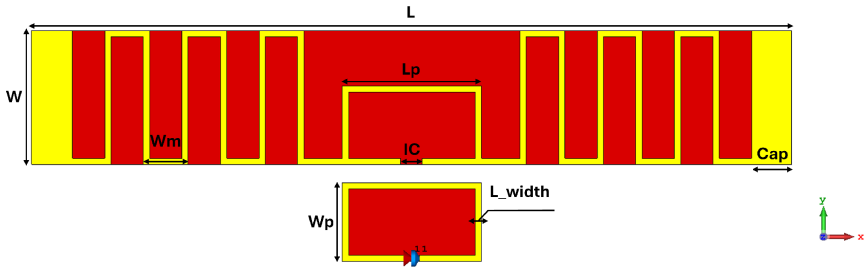

FIGURE 3. Design 1 — Simple loop configuration.

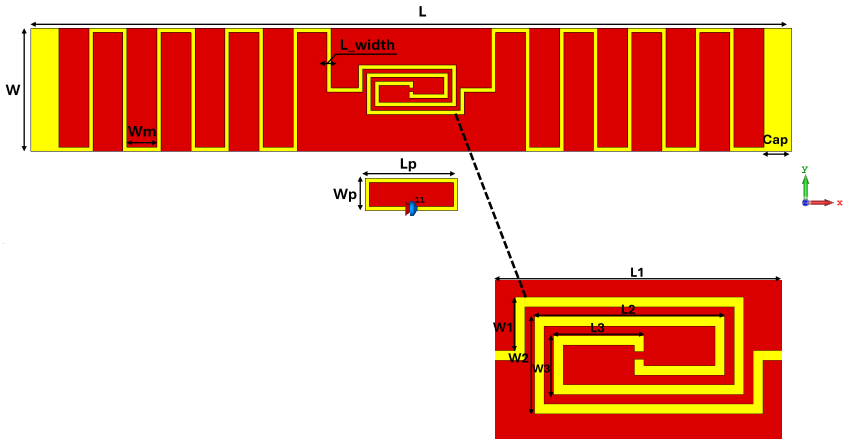

FIGURE 4. Design 2 — Spiral loop configuration.

where L_1 is the self-inductance of the chip loop, and L_2 is the effective inductive contribution of the dipole near its resonance. A sufficiently high k enhances the impedance transformation in (3), enabling the chip to reach a deep resonance of conjugate-matched. In contrast, when the distance increases or when lateral misalignment occurs, the mutual inductance M decreases rapidly; the value of k collapses; and the equivalent impedance becomes mismatched with respect to the RFID chip.

This behavior explains the presence of a well-defined activation distance in the proposed architecture. At an optimized separation of approximately 1 mm, the mutual inductance is large enough to ensure efficient power transfer and a pronounced resonance in the reflection coefficient. As soon as the distance exceeds a few millimeters, the coupling coefficient becomes too small to sustain conjugate matching, and the tag transitions into a completely detuned state. This distance-dependent evolution of k is fully consistent with the simulated and measured results and represents the physical mechanism that enables controlled activation and deactivation of the tag.

The baseline structure, hereafter referred to as *Design 1*, is illustrated in Fig. 3. The antenna was fabricated on a flexible oiled-paper substrate selected for its relative permittivity of $\varepsilon_r = 3.87$ and thickness of $h = 0.2$ mm. The conductive traces are made of copper with a uniform line width L_{width}. The dipole employs a meandered configuration optimized to achieve compact dimensions while maintaining resonance within the European UHF RFID band centered at 866 MHz. The overall geometry of the dipole is defined by its length L and width W.

To enhance impedance matching and obtain a stable resonance, capacitive loading was introduced at both ends of the dipole arms. This was implemented using widened patches of constant width *Cap*, effectively tuning the input reactance and improving power transfer efficiency.

A key feature of this configuration is the simple rectangular coupling loop located at the antenna feed point, characterized by its length L_p and width W_p. This loop establishes the inductive link with the chip module. The Impinj Monza R3 chip is mounted on a separate but identically shaped loop fabricated on the same oiled-paper substrate, forming a detachable module that completes the circuit only when in proximity.

2.1. Design 2: Spiral Loop Geometry and Coupling Mechanism

The second design, designated as *Design 2*, was developed to explore an alternative coupling strategy. This variant retains the same meandered dipole layout as in Design 1. The only modification concerns the coupling loop, which in this configuration is replaced by a compact spiral geometry integrated into the antenna structure, as illustrated in Fig. 4.

The primary objectives of adopting a spiral geometry were twofold: first, to enhance the magnetic coupling strength and localized flux density, and second, to provide a greater degree of spatial tolerance for the positioning of the chip module. The spiral structure effectively increases the loop inductance, theoretically improving the magnetic coupling between the antenna and the chip module. In addition, the larger footprint of the spi-

ral loop was deliberately designed to allow more flexibility in aligning the chip module, easing the activation process.

A closer examination of the spiral loop is provided in Fig. 4. As shown, its outer dimensions are intentionally larger than those of the simple loop used in Design 1. This design choice ensures that the chip module — retaining the same rectangular loop geometry as in the first configuration — can still achieve efficient inductive coupling even when not perfectly centered. This improvement offers a practical advantage by making the tag more tolerant to small misalignments during manual activation, thereby enhancing the user experience while maintaining the physical-layer security principle.

2.2. Monza R3 Chip Description and Integration Approach

In this work, the Impinj Monza R3 RFID chip was selected as the integrated circuit of the tag. Although this chip is not among the most recent generations of UHF RFID, it remains highly suitable for laboratory prototyping because of its practical packaging format. The Monza R3 chip features a quad-pad configuration composed of two RF input pads (RF1 and RF2) and two ground pads (GND), as illustrated in Fig. 5.

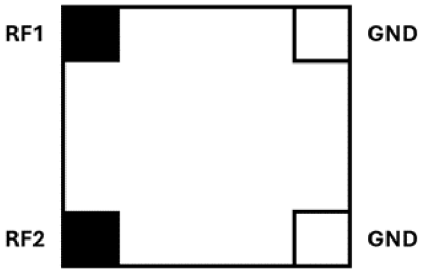

FIGURE 5. Pad layout of the Impinj Monza R3 chip showing two RF terminals and two ground pads.

This configuration greatly facilitates manual soldering and alignment during fabrication, enabling reliable electrical contact without requiring specialized assembly equipment.

It should be noted that recent generations of RFID chips, such as the Monza R6 series, offer advanced sensing capabilities, including temperature and humidity measurement. However, these modern chips are manufactured in extremely compact packages that make manual soldering virtually impossible. To address this limitation, companies such as Murata (Japan) have developed specialized packaging modules that encapsulate these miniature chips and provide external connection pads similar to those of the Monza R3. Although this approach enables easier integration, it significantly increases the overall tag cost due to the price of both the advanced chip and the proprietary Murata packaging.

Additionally, it is important to note that the Monza R3 chip exhibits a lower read sensitivity of approximately -15 dBm than -22 dBm for newer-generation chips, such as the Monza R6. This difference of around 7 dB introduces an additional challenge in achieving longer read ranges and stronger coupling efficiency [29, 30]. Nevertheless, the experimental results presented in this work remain highly acceptable given the characteristics of the chip and could be further improved by employing newer high-sensitivity RFID chips in future implementations.

2.3. Geometrical Parameters and Optimization Summary

The final geometric optimization of the proposed tag architecture required a two-step procedure. First, a parametric sweep was conducted to quantify the sensitivity of the inductive coupling to the separation distance between the dipole and the chip loop. Second, the global geometrical parameters of both antenna designs were re-optimized to restore a conjugate match with the chip impedance at the target frequency.

2.3.1. Parametric Sweep of the Coupling Distance

To justify the selection of the 1 mm activation gap used throughout this work, a dedicated parametric analysis was performed in CST Studio Suite by varying the separation distance d between the dipole and the chip loop from 0 mm to 5 mm. This sweep was executed for both configurations — Design 1 (rectangular loop) and Design 2 (spiral loop) — to verify that the distance dependence of the inductive link remains consistent across the two coupling geometries.

Figures 6(a) and 6(b) present the simulated reflection coefficient S_{11} for the different values of d. In both cases, small separation distances (0–1 mm) lead to strong inductive coupling and produce a deep, well-defined resonance. As distance increases, mutual inductance M decreases rapidly, resulting in a reduction in the coupling coefficient $k = M/\sqrt{L_1 L_2}$ and a progressive degradation of the matching condition. For d greater than a few millimeters, the link becomes too weak to sustain conjugate matching, and the tag transitions into a fully tuned state.

This monotonic deterioration of the coupling observed in both designs confirms that the 1 mm spacing corresponds to the region, where energy transfer is efficient while still enabling a clear separation between the activated and deactivated states of the tag. The similar trend across the two loop geometries further demonstrates that distance d is the dominant parameter governing the activation mechanism.

In addition to the parametric study of the separation distance, a sensitivity analysis was conducted to evaluate the effect of fabrication tolerances on the matching condition. Variations of ± 0.1 mm in the loop dimensions (L_p and W_p) resulted in resonance-frequency shifts below 3 MHz and read-range variations within ± 0.5 m, confirming the robustness of the design against typical manufacturing uncertainties. Furthermore, the use of a rigid EPS spacer with a thickness tolerance of ± 0.05 mm helps ensure consistent electromagnetic performance in scalable production environments.

2.3.2. Final Optimized Dimensions

After quantifying the influence of the coupling distance, a comprehensive optimization of the global geometry was performed to reestablish the conjugate match with the chip impedance ($Z_{\text{chip}} = 32 - j228\,\Omega$) at 866 MHz. In addition to the global parameters such as the dipole length (L), width (W), and meander

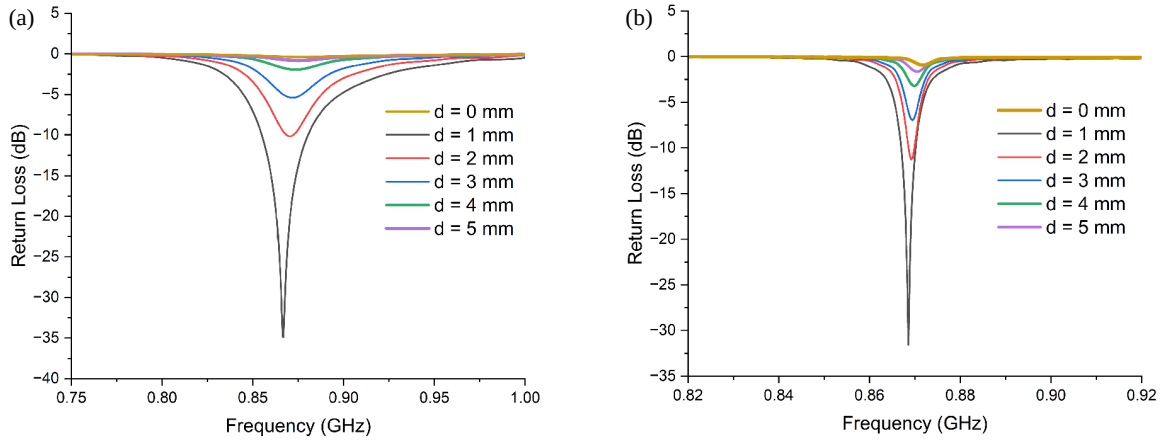

FIGURE 6. Simulated reflection coefficient S_{11} for different separation distances d (0–5 mm) for (a) Design 1 and (b) Design 2.

TABLE 2. Optimized geometrical parameters for Designs 1 and 2.

Parameter	Description	Design 1 (mm)	Design 2 (mm)
L	Antenna length	71	123.6
W	Antenna width	12.5	20
L_p	Loop length	13	15
W_p	Loop width	7.3	5.2
W_m	Meander line width	3	4.9
L_{width}	Line trace width	0.58	0.67
Cap	Capacitance width	3.8	4.5
IC	Chip location	1.6	1.6
Th_sub	Substrate thickness	0.2	0.2
L_1	Outer spiral length	-	15.9
L_2	Middle spiral length	-	13.2
L_3	Inner spiral length	-	6.27
W_1	Outer spiral width	-	3.7
W_2	Middle spiral width	-	6.7
W_3	Inner spiral width	-	4.0

width (W_m), particular attention was given to the critical tolerances of the chip loop. Variations in the loop length (L_p) and width (W_p) were found to alter its self-inductance and thus the transformed impedance presented to the dipole. Similar sensitivity was observed for the effective electrical length of the dipole, which can shift the resonance if fabrication deviations occur.

The optimized values summarized in Table 2 represent the geometry that ensures robust conjugate matching at the selected activation distance of 1 mm while remaining resilient to realistic fabrication tolerances for both loop architectures.

3. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

3.1. Validation of the Activation Mechanism via Impedance Matching

The operating principle of the secure tag is validated by analyzing its reflection coefficient, as detailed in Fig. 7. This figure shows the frequency responses of both designs in their activated and deactivated states, allowing for a direct and clear comparison.

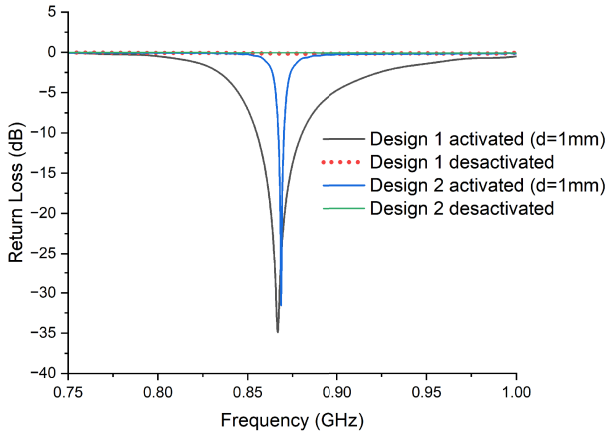

FIGURE 7. Simulated input impedance matching: comparison of activated and deactivated states for both tag designs.

To quantitatively characterize the coupling strength, the coupling coefficient k was extracted from full-wave simulations as a function of vertical separation and lateral misalignment. The results show that k decays rapidly as the separation distance increases, decreasing from 0.21 at 1 mm to 0.04 at 3 mm for Design 1. Correlation with the impedance-matching and read-range results indicates a reliable activation threshold of $k_{\text{th}} \approx 0.10$, below which $|S_{11}|$ exceeds -10 dB, and the tag becomes effectively unreadable. This threshold provides a quantitative design criterion for proximity-activated RFID systems.

Activated State: Coupling at 1 mm

When the chip module is placed at the optimized coupling distance of 1 mm, both antennas demonstrate a sharp impedance match. The Design 1 (simple loop) achieves a minimum reflection coefficient of -34.8 dB at 866.7 MHz. Design 2 (spiral loop), with its modified coupling geometry, exhibits a similarly strong but distinct resonance, with a minimum $|S_{11}|$ of -31.1 dB at 867 MHz. The specific matching depth and the slight frequency shift observed for Design 2 indicate that the increase in the inductance of the

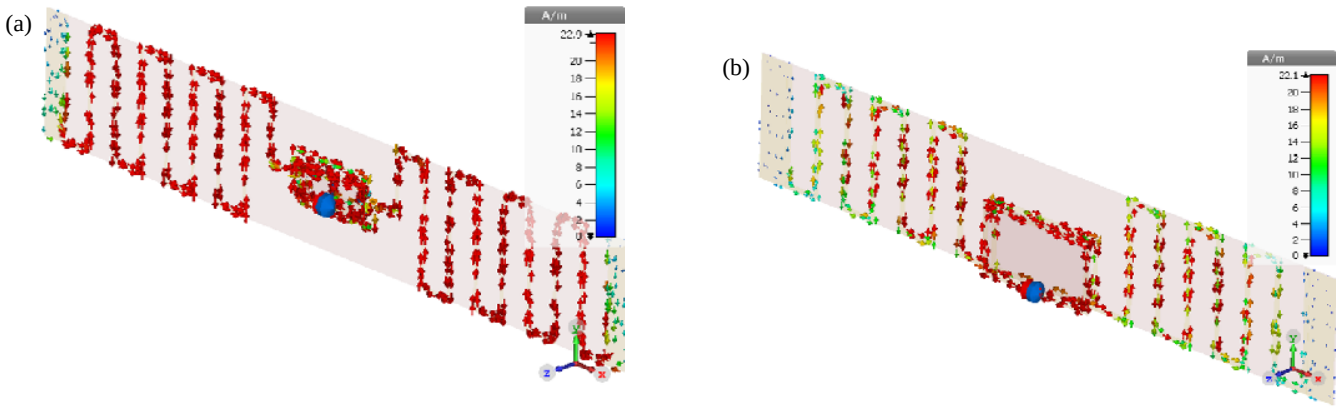

FIGURE 8. Simulated surface current distribution demonstrating uniform current concentration for both (a) Design 1 and (b) Design 2 at 866 MHz.

spiral influences the matching network, a point we will analyze further in the discussion.

Deactivated State: Decoupled

As soon as the chip module is displaced from the main antenna (separation $\gg$ 1 mm), the inductive coupling is interrupted. The result is immediate and definitive: the reflection coefficient increases to approximately 0 dB across the entire UHF RFID band for both designs. This complete disappearance of resonance confirms that the antenna is severely mismatched and radiates inefficiently, rendering the tag undetectable to the reader. The clear contrast between a perfectly matched state and a completely mismatched one forms the fundamental proof-of-concept for the proposed physical switch.

3.2. Surface Current Distribution

The surface current distribution at 866 MHz was analyzed for both designs (Fig. 8). Both the simple loop (Design 1) and the multi-turn loop (Design 2) exhibit a strong and uniform current concentration, confirming that both geometries effectively channel currents and establish a magnetic field suitable for coupling at the target frequency. The similar current distribution suggests that the performance difference observed in practical measurements, discussed in Section 4, likely stems from factors other than fundamental resonant behavior, such as sensitivity to manufacturing tolerances.

4. EXPERIMENTAL VALIDATION

4.1. Measurement Setup and Calibration

The read range performance of the fabricated tag prototypes was characterized using a Voyantic Tagformance Pro RFID measurement system. The setup, illustrated in Fig. 9, consisted of the integrated reader unit of the system connected by a coaxial cable to a circularly polarized reader antenna. This reader antenna was positioned horizontally, and to establish a known and fixed communication link, it was separated from the test zone by a 30 cm thick block of expanded polystyrene ($\varepsilon_r \approx 1.03$), which acts as a low-loss dielectric spacer.

The Voyantic Tagformance Pro system was calibrated prior to each measurement session using the manufacturer-provided

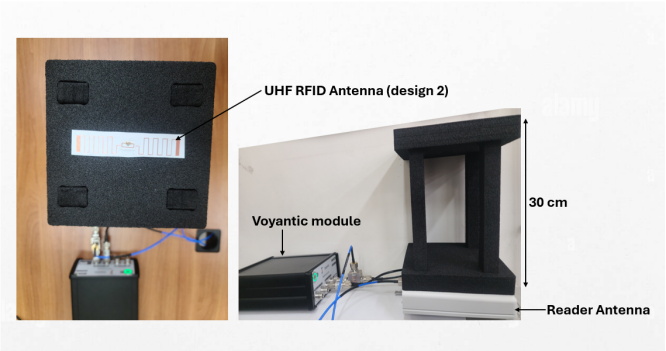

FIGURE 9. Experimental setup for read range characterization using the Voyantic Tagformance system.

reference tag. The calibration procedure compensates for cable losses and reader antenna characteristics, ensuring that the reported read range corresponds to the equivalent isotropic read range under free-space conditions.

The tag under test was placed on the opposite side of this spacer. To investigate the activation mechanism and tolerance for misalignment, the chip module was mounted on a manual 3-axis translation stage. Precise control over the separation distance (z-axis) was achieved using spacers of calibrated thickness (1 mm to 9 mm). Lateral misalignment was introduced by moving the module in 1 mm increments along the x and y axes from the optimal central position, as shown in Fig. 10. The Tagformance software was configured to sweep the European UHF RFID band (865–868 MHz) and report the calibrated read range, providing a direct and accurate measure of the operational performance.

4.2. Read-Range Measurement and Functional Validation

The measured peak read range for both tag designs in their optimally activated state (chip module at 1 mm) is presented in Fig. 11. This result serves as a direct validation of the proposed activation mechanism and provides a clear reference for performance comparison.

The Design 1 tag, with the simple coupling loop, achieved a strong peak read range of 6.0 m within the European UHF band, confirming the efficient power transfer predicted by sim-

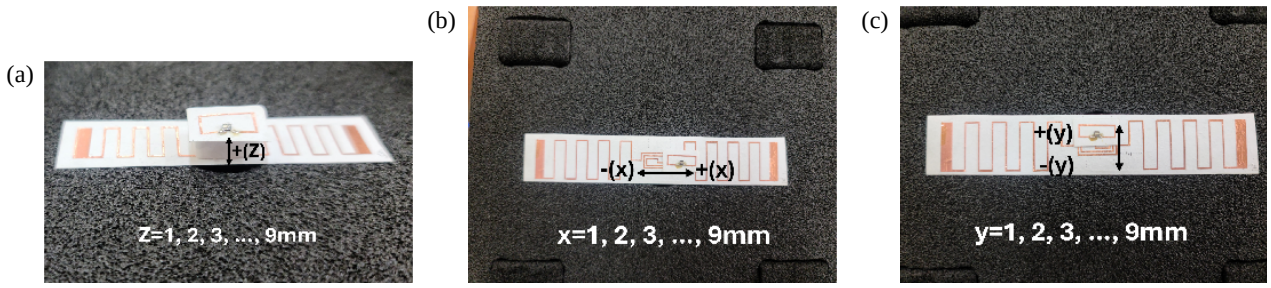

FIGURE 10. Controlled displacement of the RFID loop along the (a) Z-, (b) X-, and (c) Y-axes.

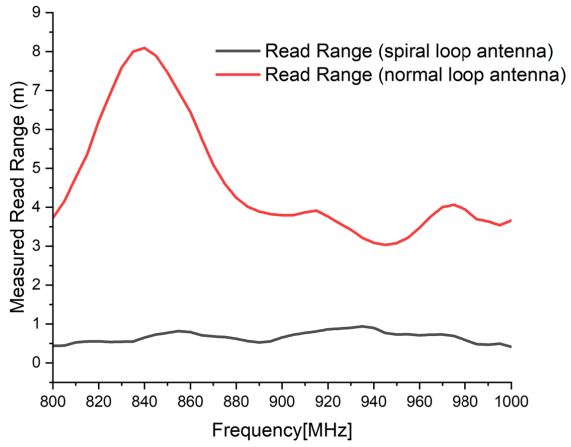

FIGURE 11. Measured read range for Designs 1 and 2 under optimal activation (loop-antenna spacing of 1 mm).

ulations. In contrast, the Design 2 tag, which incorporates the spiral loop, exhibited a significantly lower peak read range, reaching a maximum of only 0.7 m under the same ideal alignment conditions.

This substantial difference in peak read range between the two designs — despite their similar simulated impedance matching — demonstrates a critical performance gap. The following subsection investigates the robustness of this performance against positional misalignment.

4.3. Misalignment Sensitivity and Robustness Evaluation

The practical deployment of a mechanically activated tag depends on its functional stability under positional variation. The measured read-range sensitivity to misalignment along the lateral (X/Y) and vertical (Z) axes is summarized in Fig. 12. These results assess the consistency of the tag's readability, which is more critical than its peak range for this application.

Our analysis reveals a fundamental difference in how each design maintains its function when displaced. For Design 1, the read range progressively decreases from its peak of 6.0 m as displacement increases. For example, a 2 mm offset in any direction reduces the range to approximately 3.0 m, and a 3 mm offset to approximately 2.5 m. This gradual decline demonstrates a stable and wide functional zone, ensuring that the tag remains readable over a useful distance even with significant misalignment.

In contrast, Design 2 operates with a much narrower functional margin. Although it achieves a maximum read range of 0.7 m in the optimal position, this functionality is highly sensitive to positional variations. The read range shows a sharp decline with even minimal displacement, dropping to around 0.6 m. This indicates that the operational state of Design 2 is confined to a very critical point rather than a robust zone, making successful activation highly sensitive to user placement precision.

5. DISCUSSION

This study successfully demonstrates a novel, physically activated UHF RFID tag based on a discrete-component architecture. The core operational principle, which makes the tag readable only when its two parts are brought into precise proximity, has been clearly validated through both simulation and measurement. The following discussion synthesizes these results to clarify the physical origin of the activation mechanism, the performance difference between the two coupling geometries, and the practical relevance of the proposed concept.

Realization of the Security Principle. The most significant result of this work is the experimental confirmation of the tag's on/off activation mechanism. As systematically shown in Sections 3.1 and 4.2, the transition between operational states is well defined. The tag shifts from a perfectly matched radiator ($|S_{11}| < -30$ dB, read range of 6.0 m for Design 1) to a completely de-tuned structure ($|S_{11}| \approx 0$ dB, unreadable) purely due to the physical separation of the chip module. This behavior, consistent across simulation and measurement, provides a robust, user-controlled privacy switch that ensures physical-level protection against unauthorized activation. The separation distance of 1 mm was identified as the critical threshold where the inductive coupling is strong enough to facilitate conjugate impedance matching, thus activating the tag.

At the same time, the security provided by the proposed architecture should be interpreted realistically. In principle, adversarial activation could still be attempted by placing a resonant structure or a near-field probe in very close proximity to the embedded chip loop. However, such an action would require precise knowledge of the loop geometry, its location inside the tagged object, and accurate positioning. Compared with conventional RFID tags, which are continuously readable by any compatible reader within range, the proposed architecture significantly raises the barrier against unauthorized or inad-

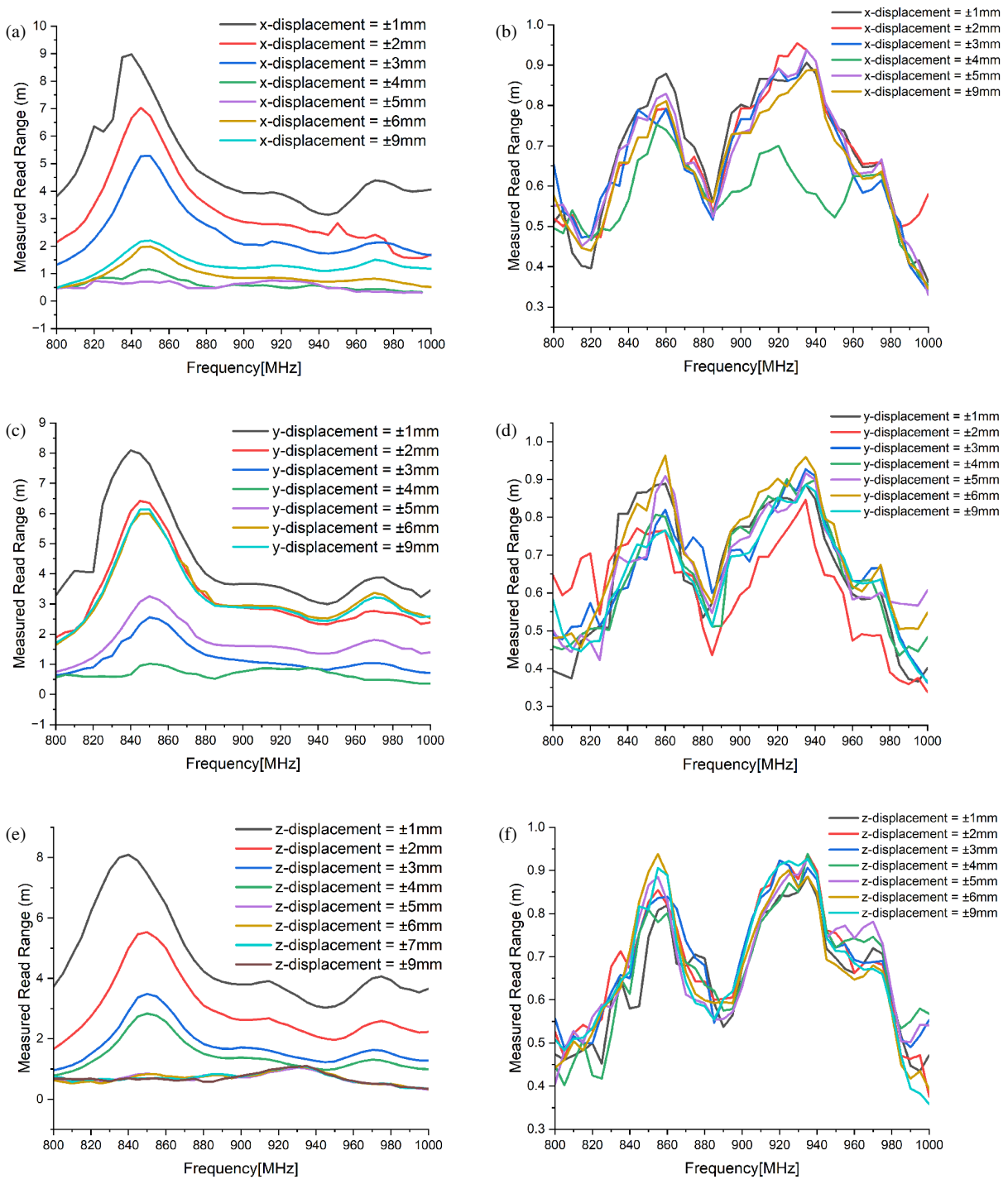

FIGURE 12. Comparative alignment tolerance: Read-range degradation versus misalignment for the simple loop (Design 1) and spiral loop (Design 2).

vertent interrogation. For applications requiring stronger protection, the present physical-layer solution can also be combined with cryptographic RFID chips or tamper-evident packaging.

Comparative Analysis of Coupling Loop Performance. A key finding of our investigation is the critical influence of the geometry of the coupling loop on the practical robustness of the tag. Although both Design 1 (simple loop) and Design 2 (spiral loop) achieved excellent simulated impedance matching and exhibited a uniform current distribution (Fig. 5), their real-world performance diverged significantly. The experimental results on alignment tolerance (Section 4.3) reveal the cause of this variation. Design 1 features a stable and robust functional zone, with the read range gradually decreasing from 6.0 m at 1 mm to approximately 0.6 m at a 9 mm offset, ensuring reliable functionality even under imperfect user alignment. In contrast, Design 2, despite its intended enhancement of magnetic coupling, operates within an extremely narrow and critical zone. Its already limited peak read range (0.7 m) drops rapidly with minimal displacement.

To further explain this difference, the electromagnetic behavior of the two coupling geometries was analyzed beyond the impedance-matching condition alone. Although both designs exhibit similarly deep resonances in the activated state, their measured read ranges remain markedly different. This indicates that good matching is a necessary condition for activation, but not a sufficient one for achieving high RFID performance.

The spiral loop of Design 2 provides a stronger inductive contribution, but it also introduces more pronounced parasitic effects and higher losses than the simple rectangular loop of Design 1. These combined effects degrade the overall power-transfer efficiency and make the response of Design 2 more sensitive to small practical variations in fabrication and alignment. By contrast, the rectangular loop offers a more favorable trade-off between coupling strength, low-loss behavior, and electromagnetic predictability.

This interpretation is also consistent with the full-wave simulation results, which suggest that Design 1 benefits from better radiation efficiency and realized gain, whereas Design 2 is more strongly penalized by the parasitic-capacitive and resistive effects associated with the spiral geometry. As a result, Design 1 converts the coupled power into useful radiation more effectively, which explains why its read range remains substantially higher despite the similar matching depth observed in simulation.

Practical Implications and Design Guidelines. Beyond peak read range, the practical usability of a mechanically activated RFID tag depends strongly on its tolerance to positional variation. In this respect, the results of Fig. 12 show that Design 1 exhibits a significantly broader activation region than Design 2. This broader operating zone means that the tag can still be activated reliably even when the loop is not positioned with perfect accuracy, which is particularly important in realistic handling conditions.

Based on these observations, the concept of an Activation Robustness Zone (ARZ) can be introduced as the spatial region in which the tag remains reliably activated. According to the measured misalignment behavior, the ARZ of Design 1 is substantially larger than that of Design 2, confirming that the rectangular-loop configuration provides a better balance between activation strength and ease of use. From a practical design perspective, this result suggests that future proximity-activated RFID systems should prioritize lateral tolerance and a sufficiently wide vertical activation range, rather than maximizing inductive coupling alone.

The measured performance also confirms that the tag becomes virtually undetectable when the two parts are separated by more than a few millimeters. This ensures strong protection against unauthorized reading in the decoupled state. Moreover, the robust misalignment tolerance of Design 1 makes it suitable for real-world applications where perfect alignment cannot be guaranteed, such as user-activated authentication or item-level privacy protection in retail and logistics.

From a manufacturing perspective, the proposed architecture is also compatible with scalable production. The tag can be fabricated using standard flexible manufacturing processes, while the required spacing can be maintained through a rigid EPS spacer with controlled thickness. Since no additional active electronics, switches, or auxiliary components are required, the structure remains simple and potentially low cost. These characteristics make the concept particularly relevant for applications such as product authentication, warranty verification, and controlled RFID activation during inspection procedures.

Although the Monza R3 chip was selected in this work because its package is convenient for manual assembly and proof-of-concept validation, the proposed architecture is not limited to this chip family. Preliminary simulations suggest that the use of more recent high-sensitivity chips, such as the Monza R6, would improve the achievable read range and moderately enlarge the activation distance while preserving the sharp transition between the activated and deactivated states. This confirms the future scalability of the concept without altering its underlying operating principle.

Based on these findings, the main guideline for future development of mechanically coupled secure RFID tags is to prioritize geometric simplicity and electromagnetic predictability over theoretical coupling enhancements that compromise robustness. The simple loop configuration thus emerges as the optimal solution, meeting the dual objectives of reliable activation and secure deactivation for next-generation privacy-aware RFID systems. More broadly, the results demonstrate that the performance of proximity-activated RFID tags is governed by a combination of coupling efficiency, parasitic effects, radiation behavior, and positional robustness. The proposed architecture therefore provides a credible foundation for future privacy-aware RFID systems and may also serve as a platform for hybrid solutions combining physical-layer activation control with higher-layer authentication mechanisms when stronger security is required.

6. CONCLUSION

This paper presents the design, simulation, and experimental validation of two proximity-activated UHF RFID tag antennas based on a split architecture for privacy-aware identification. Both designs employ a meandered dipole radiator with capacitive end-loading, while differing in the geometry of the coupling loop: a simple rectangular loop in Design 1 and a spiral loop in Design 2. The RFID chip (Monza R3) is mounted on a detachable coupling loop magnetically linked to the antenna when positioned at a 1 mm separation, allowing selective activation through near-field inductive interaction.

Full-wave simulations and experimental results confirmed the effectiveness of the proposed activation mechanism. Design 1 achieved a strong impedance match with a reflection coefficient of -34.8 dB at 866 MHz, while Design 2 exhibited a similar but slightly weaker resonance of -31.1 dB at 867 MHz. When the coupling loop was separated beyond the activation distance of 1 mm, both configurations became completely mismatched across the UHF band, validating the intended physical on/off switching behavior.

Although spiral geometry was conceived to enhance magnetic coupling, it resulted in higher losses and reduced efficiency, limiting the read range to only 0.7 m, compared to 6.0 m for the rectangular-loop configuration. Misalignment

tests demonstrated that Design 1 maintains robust functionality under moderate displacement of the coupling module along the X-, Y-, and Z-axes, confirming practical tolerance to fabrication or handling variations. Design 2, in contrast, exhibits a very narrow functional zone, highlighting the trade-off between theoretical coupling enhancement and practical robustness.

In summary, the proximity-controlled UHF RFID tag developed achieves reliable selective activation and inherent data security through physical separation of the chip and antenna. This approach establishes a solid foundation for next-generation, user-controlled, and privacy-preserving RFID systems. Future work will aim to enhance electromagnetic efficiency and integrate newer, high-sensitivity RFID chips to further extend the operational range and industrial applicability of this concept.

REFERENCES

[1] Megalou, S., K. Tsiakoumis, A. R. Chatzistefanou, S. Siachalou, T. V. Yioultsis, and A. G. Dimitriou, "Lane keeping and tracking through RFID technology," *IEEE Journal of Radio Frequency Identification*, Vol. 8, 114–124, Feb. 2024.

[2] Othmani, H., S. Beldi, and M. K. Azizi, "Design of an SHF RFID reader antenna for access control and security systems," in *2024 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET)*, 1–5, Hammamet, Tunisia, 2024.

[3] Imdaad, B. H. M., S. I. Jayalath, P. C. G. Mahiepala, M. K. T. Sampath, and S. R. Munasinghe, "RFID based fruit monitoring and orchard management system," *IEEE Transactions on Agri-food Electronics*, Vol. 2, No. 2, 413–418, Sep.–Oct. 2024.

[4] Hansen, S., C. Bredendiek, G. Briese, and N. Pohl, "A compact harmonic radar system with active tags at 61/122 GHz ISM band in SiGe BiCMOS for precise localization," *IEEE Transactions on Microwave Theory and Techniques*, Vol. 69, No. 1, 906–915, Jan. 2021.

[5] Low, J.-H., P.-S. Chee, and E.-H. Lim, "Cavity-backed double H-slot antenna with IPMC flaps for designing frequency-switchable on/in-metal semi-active tag," *IEEE Transactions on Antennas and Propagation*, Vol. 71, No. 1, 288–298, Jan. 2023.

[6] Kracek, J., M. Švanda, M. Mazanek, and J. Machac, "Implantable semi-active UHF RFID tag with inductive wireless power transfer," *IEEE Antennas and Wireless Propagation Letters*, Vol. 15, 1657–1660, Jan. 2016.

[7] Gao, S., M. Yang, H. Zhao, and X. Yin, "Independent dual-circularly polarized passive RFID tag for incident angle measurement," *IEEE Antennas and Wireless Propagation Letters*, Vol. 24, No. 4, 1013–1017, Apr. 2025.

[8] Dobkin, D., *The RF in RFID: UHF RFID in Practice*, 2nd ed., Newnes, Oxford, U.K., 2012.

[9] Görtschacher, L. J. and J. Grosinger, "UHF RFID sensor system using tag signal patterns: Prototype system," *IEEE Antennas and Wireless Propagation Letters*, Vol. 18, No. 10, 2209–2213, 2019.

[10] Erman, F., S. Koziel, E. Hanafi, R. Soboh, and S. Szczepanski, "Miniaturized metal-mountable U-shaped inductive-coupling-fed UHF RFID tag antenna with defected microstrip surface," *IEEE Access*, Vol. 10, 47 301–47 308, Apr. 2022.

[11] Andrenko, A. S., "Numerical analysis and applications of planar series feed antennas for near-field UHF RFID, sensing and radiative WPT," in *2024 International Conference on Electromagnetics in Advanced Applications (ICEAA)*, Lisbon, Portugal, 2024.

[12] Abd Alhasan, A. Q., M. F. Rohani, and M. S. Abu-Ali, "Ultra-lightweight mutual authentication protocol to prevent replay attacks for low-cost RFID tags," *IEEE Access*, Vol. 12, 50 925–50 934, Apr. 2024.

[13] Choudhary, A. and D. Sood, "Long range, compact, flippable UHF RFID tag for metallic base environments, compliant with ETSI/FCC bands," *IEEE Journal of Radio Frequency Identification*, Vol. 9, 274–285, May 2025.

[14] Škiljo, M., P. Šolić, Z. Blažević, L. D. Rodić, and T. Perković, "UHF RFID: Retail store performance," *IEEE Journal of Radio Frequency Identification*, Vol. 6, 481–489, 2021.

[15] Erman, F., S. Koziel, and L. Leifsson, "Broadband/Dual-band metal-mountable UHF RFID tag antennas: A systematic review, taxonomy analysis, standards of seamless RFID system operation, supporting IoT implementations, recommendations, and future directions," *IEEE Internet of Things Journal*, Vol. 10, No. 16, 14 780–14 797, Aug. 2023.

[16] Zhang, B., "Human behavior recognition in retail environments with graph-driven RFID signal embedding," *IEEE Sensors Journal*, Vol. 25, No. 8, 13 828–13 839, 2025.

[17] Skowron-Grabowska, B. and T. Szczepanik, "Application of RFID technologies in logistics centres to improving operations of courier firms," in *2017 IEEE International Conference on RFID Technology & Application (RFID-TA)*, 140–145, Warsaw, Poland, 2017.

[18] Nandhini, S. D., B. H. Sri, N. Abimathi, *et al.*, "Vehicular identification and authentification system using RFID," in *2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)*, 1–5, Coimbatore, India, 2017.

[19] Phan, R. C.-W., "Cryptanalysis of a new ultralightweight RFID authentication protocol — SASI," *IEEE Transactions on Dependable and Secure Computing*, Vol. 6, No. 4, 316–320, Oct.-Dec. 2009.

[20] Shi, Z., J. Chen, S. Chen, and S. Ren, "A lightweight RFID authentication protocol with confidentiality and anonymity," in *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 1631–1634, Chongqing, China, 2017.

[21] Gautam, G. R., V. Murali, and E. G. AbdAllah, "Enhancing radio frequency identification systems security using KLEIN algorithm," in *2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA)*, 103–106, Aveiro, Portugal, 2023.

[22] Ayodele, F., H. Singh, and E. G. AbdAllah, "Securing RFID-based attendance management systems: An implementation of the AES block cipher algorithm," in *2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA)*, 99–102, Aveiro, Portugal, 2023.

[23] Oluwaseun, B., A. Ogunmilua, and E. G. AbdAllah, "Enhancing security of RFID implants in the healthcare industry," in *2024 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, 177–180, Daytona Beach, FL, USA, 2024.

[24] Ahmed, I., N. Rakhaine, A.-D. Mahbub, B. Halder, M. R. Islam, and S. ul Mulk, "IoT-driven smart workplace ecosystem with RFID security and environmental monitoring featuring app integration," in *2024 IEEE International Conference on Power, Electrical, Electronics and Industrial Applications (PEEIACON)*, 664–669, Rajshahi, Bangladesh, 2024.

[25] Ramu, G., Z. Mishra, and B. Acharya, "Hardware implementation of piccolo encryption algorithm for constrained RFID application," in *2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON)*, 85–89, Jaipur, India, 2019.

[26] Pârvulescu, C., M. Aldrigo, R. Tomescu, V. Anăstăsoaie, and D. Cristea, "Multilayer anti-counterfeiting tag with holographic elements integrated into a compact RFID system," in *2023 IEEE 13th International Conference on RFID Technology and Applications (RFID-TA)*, 107–110, Aveiro, Portugal, 2023.

[27] Essam, G., H. Shehata, T. Khattab, K. Abualsaud, and M. Guizani, "Novel hybrid physical layer security technique in RFID systems," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 1299–1304, Tangier, Morocco, 2019.

[28] Gouissem, A., K. Abualsaud, E. Yaacoub, T. Khattab, and M. Guizani, "Hybrid physical layer security for passive RFID communication," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, 150–156, Las Vegas, NV, USA, 2020.

[29] Inc., I., *Impinj Monza R3 Datasheet*, Impinj Inc., product Datasheet, available: https://www.impinj.com/fr/products/tag-chips, Aug. 2025.

[30] Inc., I., *Monza R6 Tag Chip Datasheet*, version 7.0, Impinj Inc., available: https://www.impinj.com, Oct. 2021.