Intrinsic Physical Unclonable Function (PUF) Based on Laser-Induced-Graphene (LIG) UHF-RFID Antennas

Francesca M. C. Nanni, *Member, IEEE*, and Gaetano Marrocco, *Fellow, IEEE*

***Abstract*—The pursuit of eco-sustainable materials for next-generation radio-frequency and sensing devices is fostering the development of antennas and tags that are not only recyclable but also capable of ensuring physical-level authenticity. Among these, Laser-Induced Graphene (LIG) enables the direct fabrication of conductive structures on polymeric substrates. Its intrinsic fabrication variability introduces microscopic randomness that can be exploited to realize Physical Unclonable Functions (PUFs) for secure authentication. This work proposes a near-field interrogation and processing framework for LIG-based UHF-RFID antennas, enabling the extraction of digital cryptographic keys from the electromagnetic backscattered response. A dedicated signal-processing and binarization pipeline converts analog amplitude and I/Q responses into statistically balanced binary databases. An experimental campaign on 30 devices, tested with two reader antennas and two orthogonal orientations, demonstrates that the proposed method can generate up to 76 independent bits per key, with reliability exceeding 0.8 and decidability values up to 8, ensuring both repeatability and device-level distinctiveness. By varying frequency, power, and orientation, multiple uncorrelated key families can be generated.**

***Index Terms*—Laser-induced graphene (LIG), physical unclonable functions (PUFs), radio-frequency identification antennas.**

I. Introduction

IN THE rapidly expanding ecosystem of Radio-Frequency Identification (RFID), wireless sensing, and the Internet of Things (IoT), two major technological frontiers are simultaneously emerging. The first concerns environmental sustainability and the transition toward a circular economy, which are becoming increasingly critical as billions of connected objects are expected to be deployed worldwide [1], [2]. The second is related to security and anti-counterfeiting [3], especially in sectors where goods have high strategic or economic value, such as pharmaceuticals [4], [5], food logistics [6], and critical supply chains [7]. These two seemingly distinct challenges, sustainability and security, can be jointly addressed through innovative material technologies.

Received 5 November 2025; revised 18 December 2025 and 12 January 2026; accepted 22 January 2026. Date of publication 28 January 2026; date of current version 6 February 2026. This work was supported in part by the Project Ecosistema Innovazione, Digitalizzazione e Sostenibilità (ECS) 0000024 Rome Technopole [Piano Nazionale di Ripresa e Resilienza (PNRR) Mission 4 Component 2 Investment 1.5] funded by the European Union—NextGenerationEurope (EU) (Spoke: 2) under Grant CUP B83C22002820006. *(Corresponding author: Francesca M. C. Nanni.)*

The authors are with the Department of Civil Engineering and Computer Science Engineering, Tor Vergata University of Rome, 00133 Rome, Italy (e-mail: francesca.nanni@uniroma2.it; gaetano.marrocco@uniroma2.it).

Digital Object Identifier 10.1109/JRFID.2026.3658621

In this context, Laser-Induced Graphene (LIG) has recently emerged as an enabling technology for fabricating conductive patterns directly on dielectric substrates, without metallic layers or conductive inks [8]. The laser-scribing process converts carbon-rich precursors into a porous, graphene-like conductive network, enabling flexible and eco-sustainable RFID antennas and sensors [9], [10], [11], [12]. One distinctive feature of graphene technology, sometimes regarded as a limitation, is its intrinsic fabrication variability [13], [14]. The interaction between the laser beam and the precursor material induces microscopic irregularities in the carbonized surface, so that antennas fabricated with identical geometries and laser parameters will never be perfectly identical at the microscopic scale. While these random structural fluctuations have only a moderate impact on macroscopic electromagnetic performance, they introduce a unique and irreproducible physical signature that can be exploited for device authentication.

The above concept aligns with the framework of Physical Unclonable Functions (PUFs), namely hardware primitives that leverage inherent physical randomness to produce unique identifiers or cryptographic keys. In particular, *intrinsic* PUFs are those whose unclonable features arise directly from the fabrication process itself, like LIG, without requiring additional circuitry or external randomness sources [15], [16]. Focusing on a material-based approach, optical PUFs constitute one of the most mature families [17]. They rely on the random scattering of coherent light through disordered media such as polymer films, porous coatings, or colloidal nanoparticle layers. The resulting speckle patterns act as unclonable optical fingerprints with inherently high entropy and strong resistance to duplication [18], [19]. However, they require dedicated readers and are difficult to integrate into wireless systems. More recently, LIG has also been proposed for physical authentication in [20], and [21], where laser-engraved macroscopic patterns on cork substrates were electroplated with nickel to enhance conductivity. The resulting chipless markers exhibited distinct frequency responses under near-field probing, proving the feasibility of LIG for anti-counterfeiting. However, this approach lacked far-field RFID compatibility and a true quantitative cryptographic framework.

Building on this rationale, the present work investigates the cryptographic potential of LIG-based RFID tags by exploiting their intrinsic fabrication variability as a source of physical entropy, without hardware modifications. The proposed devices behave as standard RFID labels, supporting both wire-

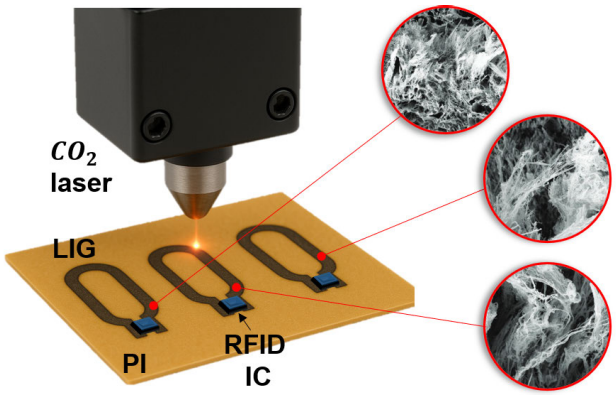

Fig. 1. Concept image of laser-induced graphene (LIG) antennas patterned on a polyimide (PI) substrate. Despite identical fabrication settings, the process yields microstructural variability, illustrated by SEM images (adapted from [9]), that serves as a source of physical entropy for device fingerprinting, retrieved through an RFID query.

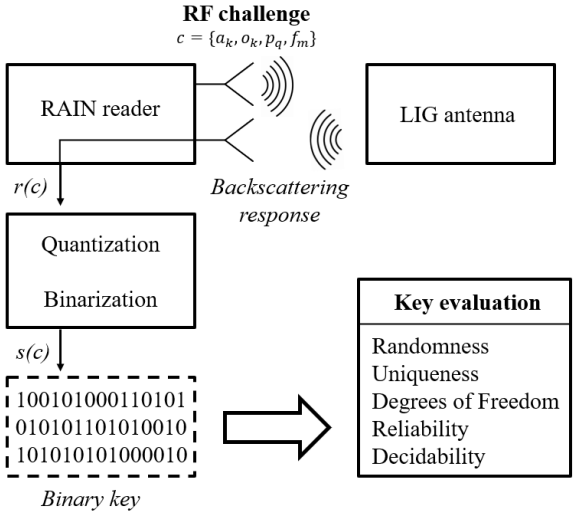

Fig. 2. General block diagram of the RF challenge–response process, to derive a binary key from the LIG antenna backscattering response.

less identification with medium-range reading and key generation through near-field interrogation. The study examines whether the microscopic irregularities inherent to LIG can serve as a basis for wireless PUFs compatible with UHF-RFID protocols, enabling statistically independent key extraction. A preliminary exploration of LIG-enabled RFID PUFs was reported in [22], where engineered variability was investigated by intentionally introducing macroscopic defects in the antenna layout, and the resulting device-to-device differences were evaluated under far-field RFID interrogation. In the present work, no intentional modification of the antenna geometry is introduced. Instead, the entropy source is the intrinsic microstructural variability that naturally arises from the laser engraving process itself.

The challenge–response mechanism is here realized in the reactive near-field, where inductive and capacitive coupling enhances sensitivity to microscopic disorder in conductivity, porosity, or edge morphology, thus increasing entropy. Antenna type or orientation can further expand the challenge space, allowing multiple uncorrelated key families to be derived from the same tag. The proposed framework therefore aims to quantify the achievable material-based digital information under each interrogation condition, ultimately identifying the maximum coding capability and the most informative configurations for entropy extraction.

The paper is organized as follows: Section II presents the formulation of the PUF–RFID reader challenge–response space and the binarization process. Section III introduces the reference metrics employed to assess the quality of the generated binary keys, with the experimental setup and protocol described in Section IV. The complete characterization of several bitstrings obtained with two antennas and different orientations are reported in Section V with particular focus on achievable degrees of freedom. Finally, Section VI concludes the work and highlights future research directions.

II. Rationale and Formulation

In the general paradigm of Physical Unclonable Functions, the device is stimulated with a *challenge*, which generates a measurable physical *response*. In the present case, the response corresponds to the electromagnetic backscattering of the LIG structure under interrogation. This analog response is then mapped on the digital domain through a binarization process, resulting in a binary key that uniquely identifies the device (Fig. 2). In cryptographic practice, such keys would typically undergo a post-processing stage (not addressed in this paper), namely a cryptographic *hashing* function [23], to generate fixed-length secrets suitable to protocols of authentication or key exchange.

During the enrollment phase, an initial key sequence, hereafter referred to as the *enrollment bitstring*, is generated and securely stored in a reference database. This bitstring acts as the device's digital fingerprint and serves as the ground truth in the authentication phase. For simplicity and to isolate the contribution of device-specific electromagnetic variability, it is assumed in this initial study that both the enrollment and verification phases are carried out using the same reader. The latter and the associated interrogation setup are therefore considered part of the challenge–response mechanism. In the following, we introduce the specific terminology adopted in this study for the definition of the challenging space, the electromagnetic response, and the stages of pre-processing, feature construction, and binarization.

A. Challenge Space

We define the challenge space as the Cartesian product of four independent dimensions:

- Reader antenna type: $a_h \in \mathcal{A}$, $h = 1..H$.
- Relative orientation between reader and tag: $o_k \in \mathcal{O} = \{o_1, o_2, ..o_K\}$.
- Transmit power: $P_q \in \mathcal{P}$, $q = 1..Q$.
- Frequency: $f_m \in \mathcal{F}$, $m = 1..M$.

A single challenge is therefore the 4-tuple:

$\mathbf{c_{hkpm}} = (a_h, o_k, P_q, f_m) \in \mathcal{C} = \mathcal{A} \times \mathcal{O} \times \mathcal{P} \times \mathcal{F}$.

For notation simplicity, we hereafter generically refer to the challenge $\mathbf{c}$ without subscript.

The challenge space is deliberately defined as a multidimensional set where each parameter provides a complementary mechanism to probe device-specific electromagnetic variability. Different reader antennas and

orientations are used to modify the near-field coupling conditions, thereby controlling the interrogation sensitivity to small perturbations in current distribution and field confinement. Frequency and transmitted power are jointly exploited to access side channels outside the optimal matching band of the tag, where the response is more strongly influenced by fabrication-induced imperfections and less constrained by the nominal antenna design. In particular, increasing the input power enables the tag to respond in weakly matched frequency regions, allowing the combined frequency–power interrogation to expand the effective challenge space and enhance the available entropy. Although transmit power can induce nonlinear variations in the IC input impedance, this study deliberately uses power as a means to probe additional spectral regions rather than to exploit chip-level nonlinearities. Overall, this multi-parameter challenge design represents a trade-off between richness of the challenge–response space and experimental complexity, while preserving manageable acquisition times and robust key extraction.

B. Raw Electromagnetic Response

For a LIG device indexed by n, the interrogation according to the $\boldsymbol{c}$ challenge produces an electromagnetic response:

$$r^{(n)}(\mathbf{c}) = \frac{1}{\sqrt{R_R P_q}} V^{(n)}(f_m, P_q) \tag{1}$$

where $V^{(n)}$ denotes the complex-valued voltage signal collected at the reader port following a standard EPC-Gen 2 interrogation at a given frequency and transmit power. $R_R = 50\,\Omega$ is the input resistance of the reader, introduced for normalization [24]. The received voltage can be decomposed into in-phase and in-quadrature (I/Q) channels as $V^{(n)} = V_I^{(n)} + jV_Q^{(n)}$. Thus the electromagnetic response hereafter considered is:

$$r^{(n)}(\mathbf{c}) = I^{(n)}(\mathbf{c}) + j\,Q^{(n)}(\mathbf{c}) \tag{2}$$

and its amplitude $A^{(n)} = \left|r^{(n)}\right|$.

C. Binary Key Construction

The physical response is transformed into a digital representation through a dedicated processing chain. The latter is carried out separately and will be independent for each challenge-response combination.

1) Preprocessing: In the first step, the signals are centralized across the device population. For each challenge $\mathbf{c}$, the mean response over all N devices is computed:

$$\bar{r}_u(\boldsymbol{c}) = \frac{1}{N}\sum_{n=1}^{N} r_u^{(n)}(\mathbf{c}). \tag{3}$$

where the $u \in \{I, Q, A\}$ denotes one of the considered output components. The residual of each response represents the *feature*:

$$\Delta_u^{(n)}(\mathbf{c}) = r_u^{(n)}(\boldsymbol{c}) - \bar{r}_u(\boldsymbol{c}). \tag{4}$$

$\Delta_u^{(n)}$ emphasizes the distinctive features of each device while suppressing most of the contributions that are common across the population. In particular, such centralization highlights the small-scale irregularities and imperfections introduced by the LIG process.

2) Quantization and Binarization: The generation of the binary key from (4) requires three processing steps: quantization followed by binarization and thinning of low informative-content bitstrings. The number of bits to perform quantization is derived from the average noise $\sigma_{noise}(\boldsymbol{c})$ and the dynamic range $D_u(\boldsymbol{c})$ inside which the features will be binarized.

The noise is estimated by interrogating a tag N_T times under the same challenge, and then calculating the average standard deviation for each challenge.

Each dynamic range is derived from the maximum and minimum values of the features over all centralized responses $\Delta_u^{(n)}$ of all the N devices, each under the specific challenge, so that:

$$D_u(\boldsymbol{c}) = max\{\Delta_u^{(n)}(\boldsymbol{c})\} - min\{\Delta_u^{(n)}(\boldsymbol{c})\},\ \forall n,\ \forall \boldsymbol{c}. \tag{5}$$

Assuming that the quantization error is uniformly distributed, the admissible range for the number $b_u(\boldsymbol{c})$ of quantization bits [25] for the specific challenge-response combination, is:

$$\log_2\left(\frac{D_u(\boldsymbol{c})}{\sqrt{12}\,\sigma_{noise,u}(\boldsymbol{c})}\right) \le b_u(\boldsymbol{c}) \le \log_2\left(\frac{D_u(\boldsymbol{c})}{2\,\sigma_{noise,u}(\boldsymbol{c})}\right), \tag{6}$$

where the lower bound ensures that the quantization noise is smaller than the measurement noise, and the upper bound guarantees that the quantization step size $s = \frac{D}{2^b}$ is at least twice the noise level ($s \ge 2\sigma_{noise}$).

The feature is then mapped into a discrete value on a scale of 2^b levels, and each quantized level is turned into its binary word by a binarization operation $\mathcal{B}$ so that the *enrollment bitstring* is obtained:

$$\boldsymbol{s_u^{(n)}}(\boldsymbol{c}) = \mathcal{B}(\boldsymbol{\Delta_u^{(n)}}(\mathbf{c})) \qquad \in \{0,1\}^{L_u(\boldsymbol{c})}. \tag{7}$$

which represents the $L_u(\boldsymbol{c})$-bits digital fingerprint of the n-th output corresponding to the specific challenge-response combination.

By stacking by rows the $\boldsymbol{s_u^{(n)}}(\boldsymbol{c})$ strings of each device generated by the responses to all the considered interrogation powers, and then stacking the so obtained bit blocks of all the N devices of the population, the *bitstring key database* $\boldsymbol{S_u}(\boldsymbol{c})$ is obtained. By exploiting multiple challenges and collecting different kinds of responses, a multiplicity of binary databases can be in principle generated from the same set of devices.

III. Cryptographic Metrics

The quality of the resulting generated keys is assessed through standard cryptographic metrics evaluated over the enrollment bitstring database, such as: *i*) uniformity, *ii*) uniqueness, *iii*) degrees of freedom, *iv*) reliability, and *v*) decidability.

A. Randomness and Thinning

The statistical quality of the enrollment bitstring database is first evaluated in terms of bit balance. Randomness (uniformity) is quantified by the Shannon entropy [26], computed along the rows and columns of the binary matrix as:

$$\begin{aligned} E_x &= -[p_x \log_2 p_x + (1-p_x)\log_2(1-p_x)], \\ E_y &= -[p_y \log_2 p_y + (1-p_y)\log_2(1-p_y)], \end{aligned} \tag{8}$$

where p_x and p_y denote the probabilities of observing ones along rows and columns, respectively. A perfectly balanced distribution yields $E_x = E_y = 1$. To retain only statistically meaningful information, a *thinning* (bit-filtering) procedure [27] discards rows and columns whose entropy falls below a threshold $E_{x,y} < t$, with $0.95 < t < 0.98$. This removes biased responses associated with specific interrogation powers and non-informative frequency challenges, retaining only near-uniform portions of the enrollment matrix. All subsequent metrics are evaluated on the resulting thinned database.

B. Uniqueness

Uniqueness is quantified through the normalized Hamming distance (HD) between pairs of binary keys generated under different devices, challenges, or components. For two bitstrings of length L, it is defined as:

$$HD(\mathbf{c}_1, \mathbf{c}_2; n_i, n_j; u_1, u_2) = \frac{1}{L} \sum_{i=1}^{L} S_{u_1}^{(n_i)}(\mathbf{c}_1)[i] \oplus S_{u_2}^{(n_j)}(\mathbf{c}_2)[i], \quad (9)$$

where n_i and n_j are device indices and $\oplus$ denotes bitwise XOR. The ideal value is 0.5, corresponding to statistically independent responses.

Uniqueness is evaluated in the following cases:

1) *Inter-device:* for a fixed challenge $\mathbf{c}$, $HD_{\text{inter}} = HD(\mathbf{c}, \mathbf{c}; n_i, n_j; u, u)$ with $n_i \neq n_j$. A distribution centered near 0.5 indicates high device distinguishability.
2) *Cross-orientation (intra-device):* for a fixed device and reader antenna, with two orthogonal orientations $o_1 \neq o_2$, $HD_{\text{orient}} = HD((a, o_1, P, f), (a, o_2, P, f); n, n; u, u)$. Values close to 0.5 indicate uncorrelated orientation challenges.
3) *Cross-channel (intra-device):* for a fixed device and challenge $\mathbf{c}$, with two output components $u_1 \neq u_2$ (e.g., I vs. Q, or vs. A), $HD_{\text{chan}} = HD(\mathbf{c}, \mathbf{c}; n, n; u_1, u_2)$.
4) *Cross-antenna (intra-device):* for a fixed device and orientation, with two reader antennas $a_1 \neq a_2$, $HD_{\text{ant}} = HD((a_1, o, P, f), (a_2, o, P, f); n, n; u, u)$. In the near-field, where the response depends on the reader, the expected average distance is 0.5, confirming uncorrelated antenna challenges.

When compared keys have different lengths, HD is computed over the common bits only.

C. Degrees of Freedom (DoF)

The Degrees of Freedom (DoF) quantify the effective number of statistically independent bits in the generated key and are computed as:

$$DoF = \frac{\mu_{inter}(1 - \mu_{inter})}{\sigma_{inter}^2}. \quad (10)$$

Here, μ_{inter} and σ_{inter} are the mean and standard deviation of the inter-device HD distribution over the device population. The corresponding encoding capacity is $c = 2^{DoF}$, which represents the maximum number of distinct keys that can theoretically be generated by the PUF prior to hashing.

D. Reliability

To assess the stability of each extracted bit, the reliability [28] is computed as:

$$\rho = 1 - \overline{HD}_{repeat}, \quad (11)$$

where $\overline{HD}_{repeat}$ is the averaged inter-HD between each bit-string and the *enrollment* one of a same tag, when measured multiple times. The tag is disassembled and reassembled before each measurement, as described in Section V:

$$HD_{repeat}^{(h)}(\boldsymbol{c}, \boldsymbol{c}; n_{enroll}, n; u, u) = \frac{1}{L} \sum_{i=1}^{L} S_u^{(n,enroll)}[i] \oplus S_u^{(n)}[i], \quad (12)$$

so that $\overline{HD}_{repeat} = \frac{1}{N_T} \sum_{h=1}^{N_T} HD_{repeat}^{(h)}$ with h being the measurement index and N_T the number of repeated measurements. The closer (11) is to 1, the more reliable the corresponding bitstring.

E. Decidability

The decidability [17] quantifies the capability of a PUF to discriminate between responses generated by different devices. Mathematically, decidability is defined as:

$$D = \frac{|\mu_{intra} - \mu_{inter}|}{\sqrt{\frac{\sigma_{intra}^2 + \sigma_{inter}^2}{2}}} \quad (13)$$

where: (μ_{intra}, σ_{intra}) are now the mean value and variance of (12). It is a statistical indicator of how well the inter-device and intra-device HD distributions are separated. High decidability values indicate clear device discrimination, whereas $D = 0$ corresponds to complete overlap of the distributions.

IV. Experimental Set-Up

The experimental evaluation of the LIG-PUF near-field architecture was carried out through the fabrication of a set of identically manufactured LIG dipoles and the acquisition of their electromagnetic fingerprints over a wide frequency and power range for two different reader antennas and two orientations.

A. LIG Devices

The reference device for this study employs Polyimide (PI) [29], [30] as the substrate material (electrical permittivity and loss tangent: $\epsilon_r = 3.2$, $tan(\delta) = 0.002$). We manufactured $N = 30$ identical LIG-based rectangular UHF dipoles ($70\,mm \times 20\,mm$) engraved onto $125\,\mu m$-thick PI films. PI layers were laminated onto a $2\,mm$-thick poly (methyl methacrylate) (PMMA) support to ensure mechanical rigidity during laser processing. The conductive traces were engraved via a *Trotec Speedy 100* CO_2 laser, using the following parameters: laser power $P = 9\ W$, scanning speed $S_S = 10$ *cm/s*, laser head defocus $h = 3\ mm$, and pulse-per-inches $PPI = 1000$. The resulting surface exhibited a sheet resistance of $R_s = 14\ \Omega/sq$, as measured through a four-point probe setup [31]. The LIG trace was then protected by a thin polyurethane layer (Tegaderm by 3M, thickness: $\sim$ 40 μm), which prevents mechanical abrasion and degradation of the graphene pattern over time. Moreover, this encapsulation hinders direct

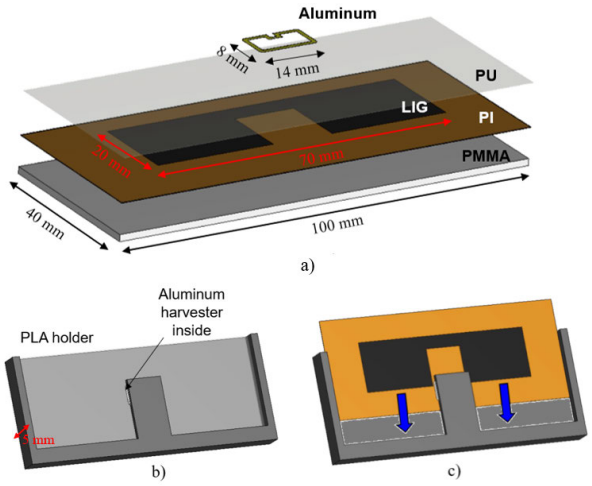

Fig. 3. a) Exploded view of the LIG reference antenna layout and the aluminum harvester with a polyurethane (PU) protection coating; b) PLA case, hosting the small loop harvester, where the LIG antenna c) is inserted properly aligned to the loop.

access to the LIG medium, as any attempt to remove the protective coating inevitably damages the conductive network, thus making impedance measurements or reverse-engineering analysis unfeasible. The LIG traces are inductively coupled to RFID ICs (*Impinj Monza R6-P*, Z_{IC} = 16.5-j139.5 Ω, power sensitivity p_{IC} = -20dBm) by means of a small aluminum loop harvester. To ensure a precise and repeatable alignment between the loop harvester and the LIG radiator, we resorted to a single IC that was embedded into a 3D printed support (Fig. 3b)) made in PLA (with 100% infill, ϵ_r = 2.55, $tan(\delta)$ = 0.007 [32]) where each of the 30 LIG cards is inserted one at a time thus precisely reproducing a stable coupling. Using a same IC for all samples permits to focus only on the cryptographic information generated by the LIG trace, dropping out the fabrication uncertainties due to the physical integration by adhesive of the loop on the graphene layer. At the same time, repeated insertion of the LIG radiators into the holder introduces small loop–antenna misalignments, whose effects are captured by the repeatability analysis and incorporated into the estimated noise floor for bit quantization, thereby accounting for residual assembly tolerances also expected in fully integrated tags. Fig. 4a) reports three representative samples selected from all 30 devices. The optical magnifications on the right highlight small but visible microstructural differences at the LIG edges, especially along internal regions where higher current density is expected. An assembled prototype is shown in Fig. 4b).

B. Querying Antennas

The UHF reader's antennas employed to perform near-field fingerprint acquisition were a loop (a_1) and a dipole (a_2) (Fig. 5). The loop (Keonn Advantenna L11 [33]) is engineered for uniform magnetic field confinement across its radiating surface (size: 137×137×0.5 mm^3). The dipole (Molex 105262 [34]) is planar and flexible, with size: 79 × 10 × 0.1 mm^3, and gain: 0.2 – 0.4 dBi @915 MHz. The loop is expected to mostly couple with the small loop harvester, while the dipole with the LIG body. This selection thus allows comparing

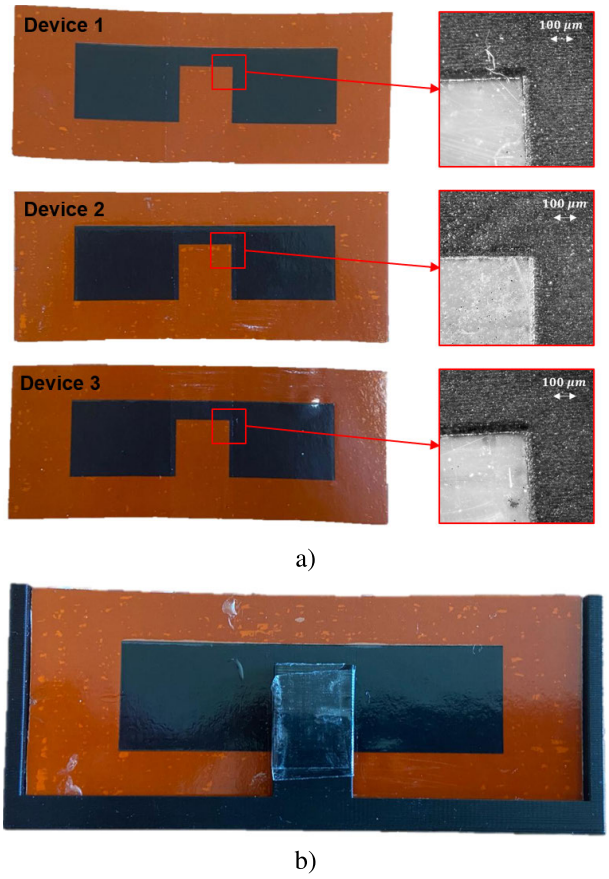

Fig. 4. Manufactured prototypes: a) three LIG antenna samples with optical microscope magnification close to one of the internal edges; b) the complete assembled device inside the PLA case hosting the loop exciter.

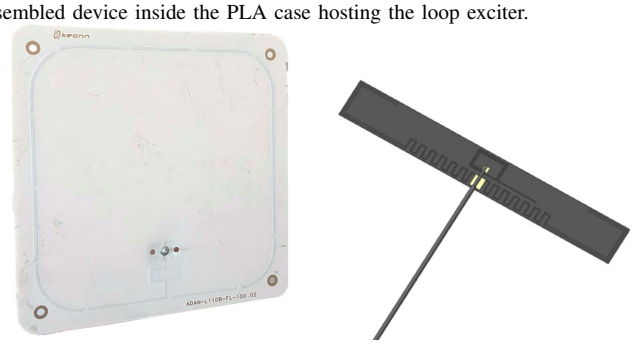

Fig. 5. a) Keonn Advantenna L11 loop reader antenna [33] and b) Molex 105262 series dipole antenna [34].

inductive and capacitive near-field coupling, and permits to evaluate the influence of each interrogating antenna on the extracted fingerprints. Both antennas were connected to a Voyantic Tagformance Pro UHF Station for multi-challenge measurements.

C. Interrogation Modes

1) Geometrical Arrangement: The LIG devices were placed on top of the reader antenna. Considering the thickness of the PLA holder, the effective spacing between the reader antenna and the LIG prototype was 0.5 *cm*.

2) Power and Frequency: The set of physical challenges included Q = 10 input power levels P_q, uniformly spaced between 21 dBm and 30 dBm with a step of 1 dBm.

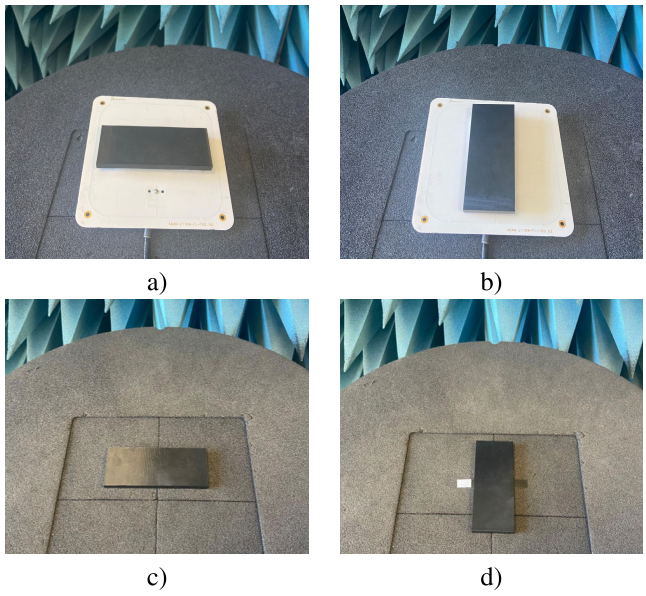

Fig. 6. Close-up example on the measurement setup for the a) ∥ and b) ⊥ orientations in the loop case, and c) ∥ and d) ⊥ orientations in the dipole case.

Interrogations were performed in the frequency range 600 MHz to 1300 MHz with 10 MHz resolution ($M = 71$).

3) Orientation: Two mutually orthogonal orientations were considered. In the first configuration (o_1), the side of the interrogating antenna hosting the input port is aligned parallel to the main axis of the LIG label (Fig. 6). The second configuration is obtained by rotating the tag by 90° with respect to o_1, resulting in an orthogonal alignment ($o_2 = o_1 + \pi/2$). Accordingly, the orientations will hereafter be denoted as $\{o_1 = \|, o_2 = \perp\}$. The acquisition protocol requires testing each reader antenna under both orientations.

Overall, a total of $M \times Q = 710$ response samples were collected for every tag, and the complete campaign produced more than $80k$ individual response samples.

V. Results

The experimental results are organized to follow the complete measurement and processing workflow, starting from the electromagnetic validation of the RFID antennas and proceeding through the acquisition noise assessment, signal preprocessing, and bitstring database construction.

Then, the statistical properties and cryptographic metrics of the generated keys are analyzed under different challenge–response configurations.

A. Antenna Performance

The devices were first tested as wireless RFID labels to assess their communication performance, specifically the maximum read distance. To this purpose, the 30 LIG dipoles were interrogated at a fixed distance of 30 cm, approximately in the far-field region by using a log-periodic antenna with a gain of approximately 4.7 dBi at 868 MHz. For each device, the turn-on power, i.e., the minimum reader power required to activate the integrated circuit, was measured. This value was then used to estimate the maximum reading range using the Friis equation, assuming a transmitted EIRP of 3.2 W (the maximum value allowed in Europe) and a conservative

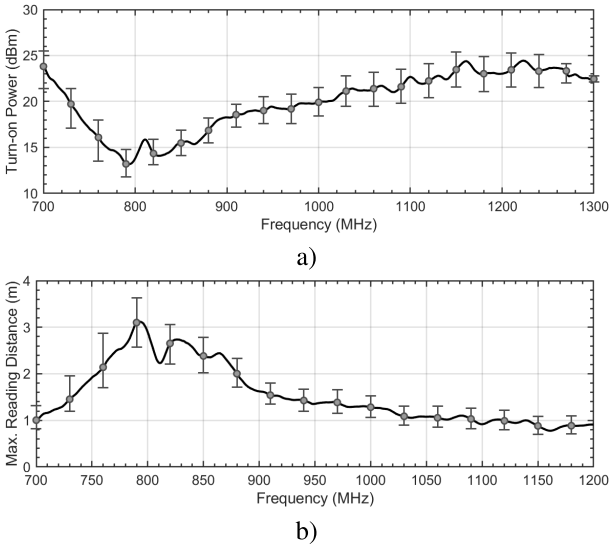

Fig. 7. a) Average turn-on power (dBm) of 30 devices measured at a distance $d = 30$ cm and b) estimated maximum reading distance (m) assuming an EIRP = 3.2 W and a circularly polarized reader antenna. The solid lines represent the mean values, while the error bars indicate the variability across the 30 specimens.

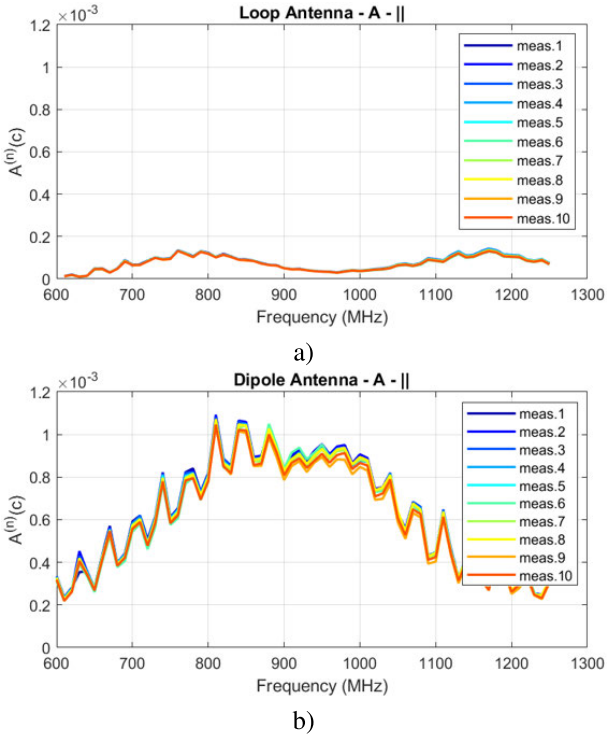

Fig. 8. Example of 10 responses of one LIG prototype, w.r.t. a) the loop and b) the dipole antenna, following a $P_{in} = 25$ dBm power challenge in the $o_1 = \|$ orientation.

polarization loss factor between labels and reader equal to $PLF = 0.5$. The communication performance is shown in Fig. 7. The tags exhibited readable distances of approximately 1.9-2.4 m within the European UHF RFID band (centered at 867.6 MHz). The slight variations among the 30 samples are probably due to intrinsic fabrication non-uniformities of the laser scribing and to measurement uncertainties.

B. Noise Variance

The noise variances are evaluated by $N_T = 10$ measurements of a same tag, varying the frequency under fixed powers and

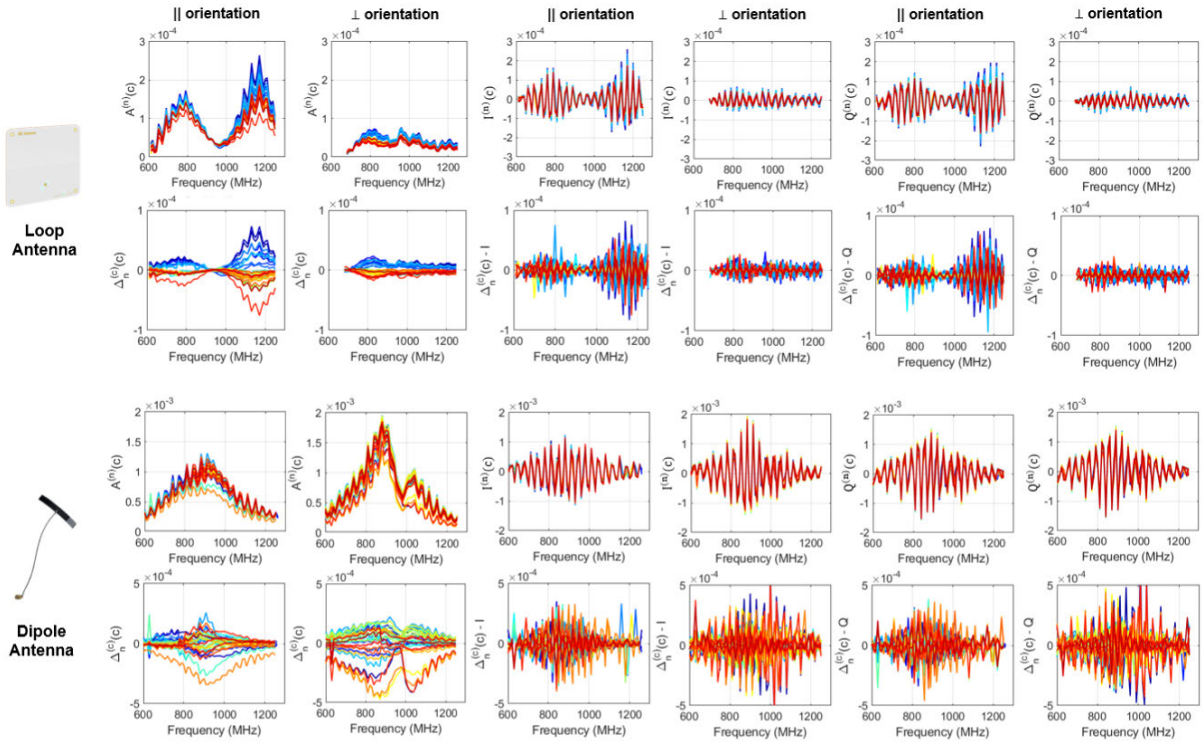

Fig. 9. Example of frequency responses of 30 tags under $P = 25\,dBm$ for two reader antennas and orientations ($\|, \perp$). Loop (top) and dipole (bottom) blocks show raw (row 1) and centralized (row 2) magnitude A, in-phase I, and in-quadrature Q components ($600 - 1300\,MHz$).

antenna/alignment challenges. The latter were repeated after removing the tag from the measurement setup, disassembling and reassembling it into its PLA case, and then repositioning it in the measurement fixture. This procedure was adopted to account for potential slight misalignments between the LIG device and the fixed loop inside the case across repeated readings.

An example set of measurements for a fixed power is reported in Fig. 8 showing almost identical behavior. The pronounced oscillations, mostly outside the UHF RFID band ($860 - 960\,MHz$), are due to the impedance mismatch of the interrogating antennas. The interrogation by dipole antenna generates an order of magnitude higher noise than in the case of loop (averaged noise across all powers for the loop antenna $\sigma_{noise,a1} = 1.1 \times 10^{-6}$ and dipole antenna $\sigma_{noise,a2} = 1.1 \times 10^{-5}$).

Additional repeated measurements performed on multiple devices under identical interrogation conditions confirmed that measurement uncertainty remains smaller than device-to-device variability. Similar repeatability levels were observed for the I/Q components, indicating comparable variability to that of the amplitude response.

C. Raw Data and Processing

Fig. 9 reports representative frequency responses of the 30 devices under a fixed power challenge (P_{in} = 25 dBm), for both reader antennas and the two orientations. For each antenna, the upper row shows the raw responses, while the lower row reports the corresponding centralized residuals. Columns are grouped by response component, namely magnitude A, in-phase I, and quadrature Q, each shown for both o_1 and o_2. By comparing the I and Q panels within the same antenna-orientation pair, it can be observed that they exhibit nearly identical spectral envelopes, differing primarily by the expected $\pi/2$ phase shift. Accordingly, although both are reported here for completeness, the subsequent cryptographic analysis focuses on the amplitude and in-phase response only.

D. Bitstring Key Database

By evaluating (5) and (6) for the resulting dynamics $D_u(c)$, the estimated number of bits is $b(loop) = 5$ for the loop for all the considered power challenges, and 4–5 for the dipole case. An example of one response processing up until the *enrollment bitstring* is extracted is shown in Fig. 10, while Fig. 11a) reports an example of the enrollment bitstring database before thinning. Extended regions with a visible bias toward '1's or '0's can be observed. As a direct consequence, the corresponding Shannon entropy diagrams Fig. 11b) exhibit values lower than unity. The thinning threshold was selected based on the trade-off between entropy, Degrees of Freedom, and key length. Low values preserve redundant samples, while high values excessively shorten the key and reduce DoF. Around t = 0.97, entropy approaches unity, and the DoF reach a maximum or plateau without excessive bit removal. This value was therefore selected as the optimal compromise.

The resulting binary databases are shown in Fig. 12, where the first row refers to the loop antenna, while the second corresponds to the dipole antenna. Within each row, the columns are organized by response component and relative orientation. The post-thinning maps are dense and differences and the bit distribution are visually different for both antenna types and orientations.

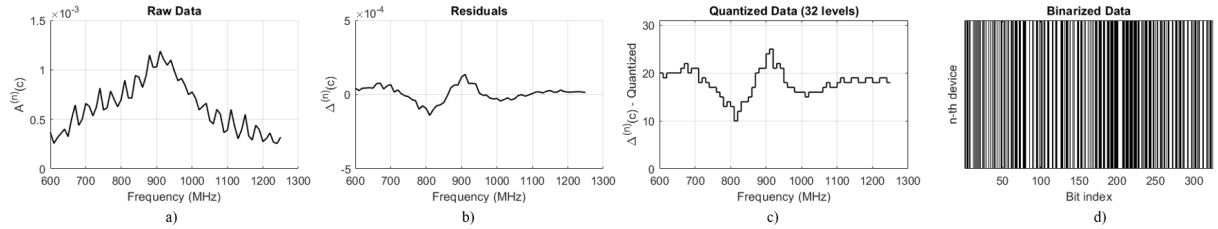

Fig. 10. Example of the processing pipeline: a) raw, b) residual, c) quantized response and d) binary key for a single device ($n = 1$) w.r.t. the dipole antenna, $P = 25$ dBm, and $\|$ orientation.

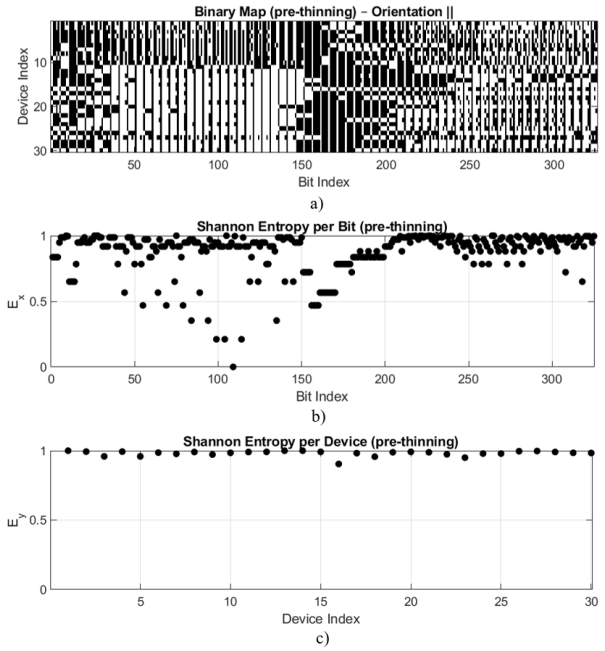

Fig. 11. a) Example of a bitstring database for the loop, before thinning, under single challenging power $P = 25$ dBm. Corresponding Shannon Entropies along b) the rows (E_x) and c) the columns (E_y).

E. Randomness Analysis After Thinning

The randomness of the generated keys was assessed through the Shannon entropy as in (8). Fig. 13 shows representative distributions for the loop and dipole antennas for both selected orientations. It is observed that for both E_x and E_y consistently remain above 0.9 in all the considered cases, indicating a balanced distribution of bits across the devices. In particular, E_x plots exhibit some gaps at specific positions along the bit index that are the direct outcome of the thinning process.

F. Uniqueness Analysis and DoF

1) Inter-Device Hamming Distance: Fig. 14 shows four heatmaps (loop and dipole, each one under both orientations) for the amplitude responses. On average, the inter-HD values converge around a mean of 0.51 ± 0.17 and 0.51 ± 0.10 for the loop and dipole respectively (amplitude case), confirming that the extracted keys preserve a sufficient level of uniqueness across the device set. However, in some cases, one of the two orientations exhibits localized clusters of pixels with Hamming distances deviating from 0.5. This indicates the presence of partial similarities among certain devices, even though the overall distribution remains consistent with a statistically diverse population. This effect may be related to the fabrication of a small subset of the tags in a different day than the majority of them, so that the environmental conditions (manual laser calibration, room humidity) could have not been exactly the same.

TABLE I

MAXIMUM DEGREES OF FREEDOM (DOF) OVER ALL THE CONSIDERED INPUT POWERS FOR EACH COMBINATION OF CHALLENGES

	Loop antenna		**Dipole antenna**	
	$\|\|$	$\perp$	$\|\|$	$\perp$
Amplitude	10	39	**42**	31
In-phase (I)	25	**76**	41	24

TABLE II

AVERAGED CROSS-ANTENNA HAMMING DISTANCE

	A		**I**	
	$\|\|$	$\perp$	$\|\|$	$\perp$
cross-antenna	0.50 ± 0.07	0.50 ± 0.05	0.50 ± 0.05	0.49 ± 0.05

2) Degrees of Freedom: Fig. 15 summarizes the Degrees of Freedom obtained from (10) as a function of the interrogation power. The most evident result is that, for both antennas, the DoF significantly differ when comparing $\|$ and $\perp$ orthogonal orientations. The orthogonal case generally tends to yield higher DoF values in the loop case, reaching a maximum of 76 independent bits. In contrast, the dipole antenna exhibits more balanced behavior across the two orientations, with a maximum of 42 independent bits.

G. Cross-Challenge Analysis

The cross-antenna Hamming distance HD_{ant} is shown in Fig. 16 where each cell corresponds to the distance between the dipole- and loop-based responses. In both orientations, the values are consistently distributed between 0.3 and 0.8, with no evidence of correlation (HD $\approx$ 0) or complementarity (HD $\approx$ 1). The average value of this metric is shown in Tab. II, indicating that the keys derived from the dipole are, to a large extent, statistically independent of those obtained from the loop. This result moreover confirms that the interrogating antenna is an integral part of the key construction process. Similar diagrams (not reported here to avoid repetitions) are obtained for the cross-orientation and cross-channel Hamming distance. The averaged results are summarized in Tab. III and Tab. IV. Data fluctuate around 0.5 with limited dispersion, thus confirming the full statistical independence even among the keys obtained by combining challenges and output channels.

H. Reliability and Decidability

Fig. 17 and Fig. 18 report the reliability and decidability values obtained for the two reader antennas under different

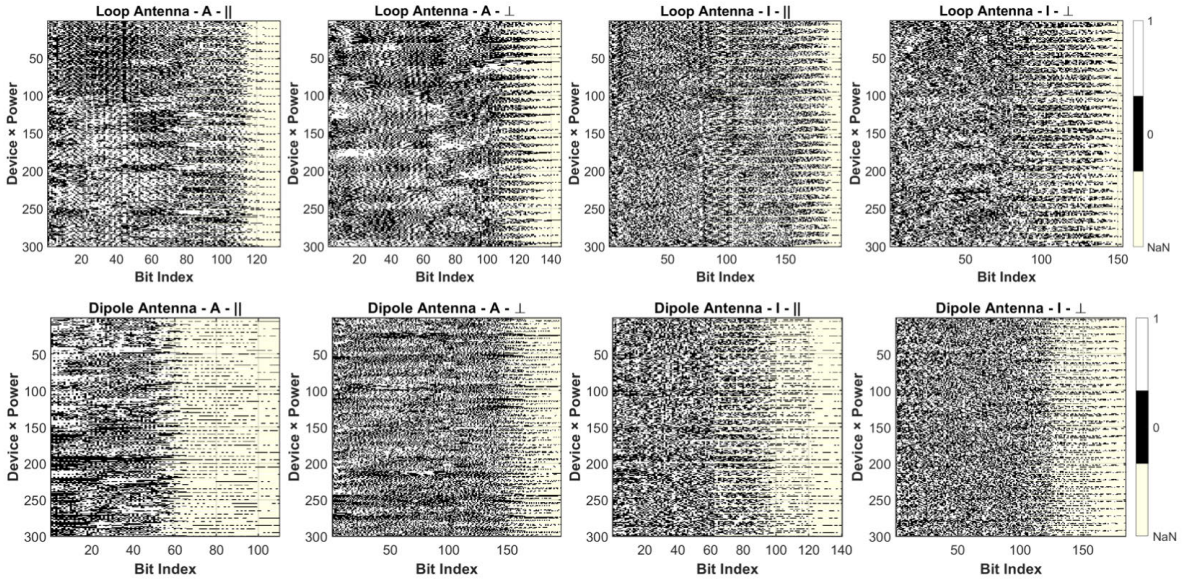

Fig. 12. Binary database after thinning of the 30 devices for all power challenges: a) Loop antenna, ∥ orientation; b) Loop antenna, ⊥ orientation; c) Dipole antenna, ∥ orientation; d) Dipole antenna, ⊥ orientation. Black and white pixels denote bit values '1' and '0', while yellow pixels indicate missing bits at frequencies where the devices did not respond.

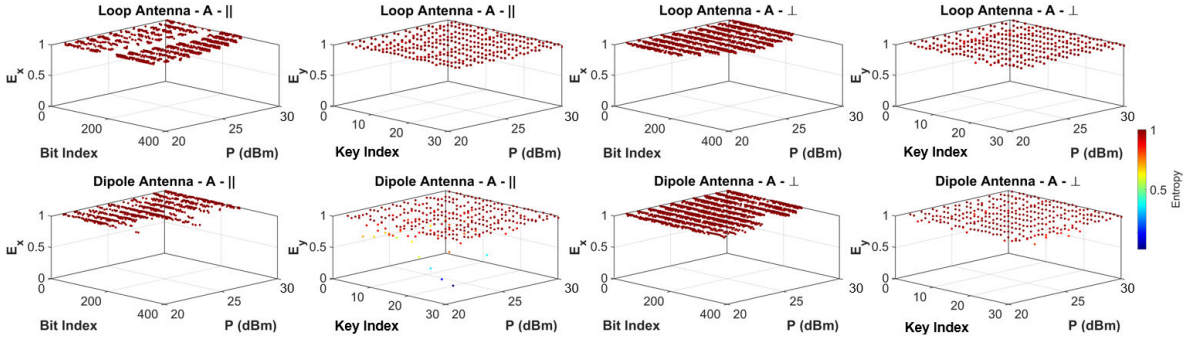

Fig. 13. Shannon entropies along the rows (E_x) and the columns (E_y) of the binary 2D databases after thinning.

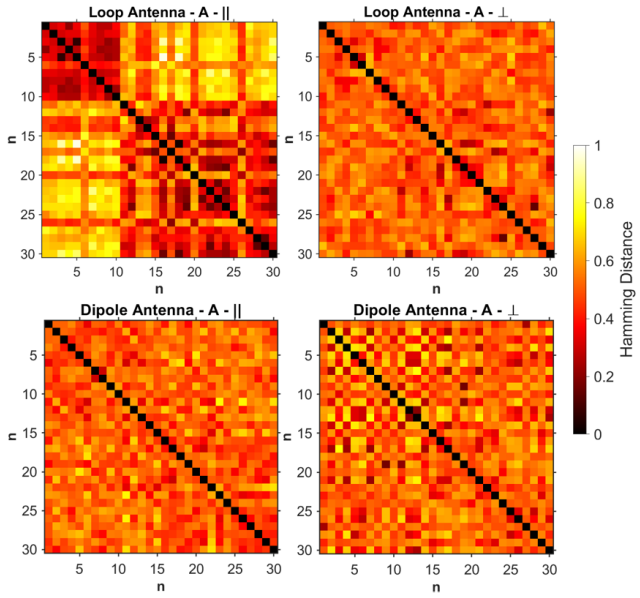

Fig. 14. Example of Inter-Hamming distance w.r.t. the amplitude responses and a P_{in} = 25 dBm power challenge.

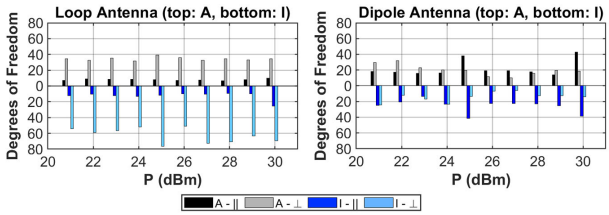

Fig. 15. Degrees of Freedom as a function of transmit power for both interrogation orientations (o_1,o_2).

TABLE III
AVERAGED CROSS-ORIENTATION HAMMING DISTANCE

	A	**I**
cross-orientation (a_1)	0.49 ± 0.05	0.50 ± 0.04
cross-orientation (a_2)	0.49 ± 0.07	0.51 ± 0.05

TABLE IV
AVERAGED CROSS-CHANNELS HAMMING DISTANCE

	∥	⊥
	A vs I	**A vs I**
cross-channels (a_1)	0.49 ± 0.04	0.49 ± 0.05
cross-channels (a_2)	0.50 ± 0.07	0.50 ± 0.05

interrogation conditions. In all configurations, the bit reliability index exceeds 0.7 and remains consistently around 0.85 on average, demonstrating that the proposed acquisition and binarization process generates stable and repeatable keys. This confirms the reproducibility of the extracted binary responses,

TABLE V
MAXIMUM OBTAINED DEGREES OF FREEDOM VERSUS THE FREQUENCY SAMPLING STEP W.R.T. THE CORRESPONDING $\{P_q, u, o_k\}$ TRIPLET

	1 MHz	5 MHz	10 MHz	15 MHz	20 MHz	25 MHz	30 MHz
Loop Antenna	66 (25, Q, ⊥)	72 (21, I, ⊥)	76 (25, I, ⊥)	38 (30, Q, ∥)	44 (27, Q, ⊥)	40 (21, I, ⊥)	44 (27, I, ⊥)
Dipole Antenna	52 (25, A, ⊥)	56 (30, A, ∥)	55 (25, Q, ∥)	54 (30, A, ∥)	39 (25, Q, ∥)	34 (25, Q, ∥)	30 (30, I, ∥)

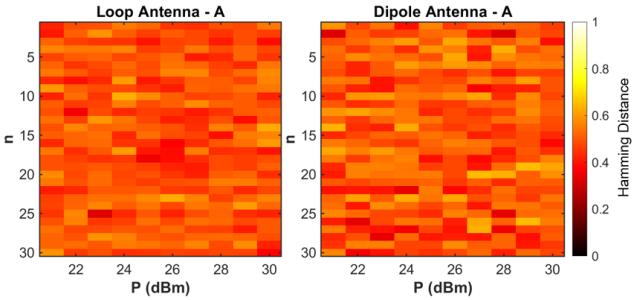

Fig. 16. Cross-antenna Hamming distance: 2D heatmaps across all 30 devices and power levels, with each cell representing the distance between loop and dipole responses for (a) ∥ orientation and (b) ⊥ orientation.

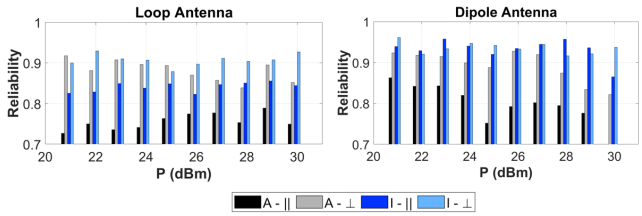

Fig. 17. Reliability w.r.t. the loop antenna and the dipole antenna for both orientations.

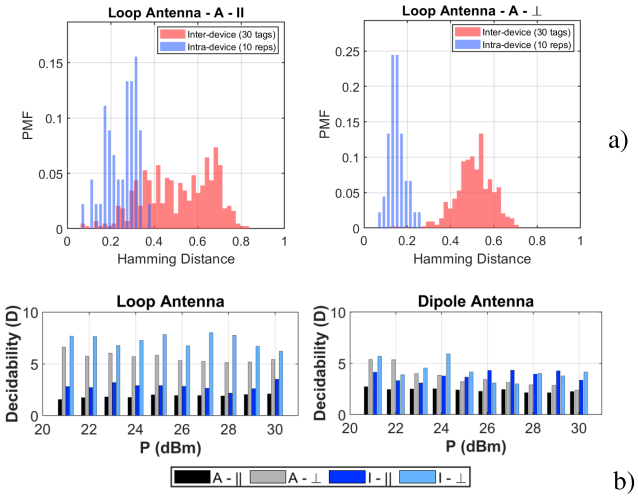

Fig. 18. Decidability. a) Example of probability mass function (PMF) distributions of the inter- and intra-Hamming distance for the loop antenna, with respect to the amplitude component and both orientations. b) Histograms versus interrogation power for all components and orientations of the loop and dipole antennas.

despite the presence of a limited residual variability that is explicitly accounted for in the estimated noise floor.

The decidability results, on the other hand, show a stronger dependence on the type of reader antenna and on the interrogation orientation. This behavior reflects the balance between inter-device variability and the finite dispersion of intra-device responses, which remains non-zero due to the limited reproducibility of the electromagnetic measurements. Fig. 18 illustrates an example of probability mass functions of the inter- and intra-Hamming distance distributions for the two orientations of the loop antenna. In case of parallel alignment, the two distributions are partially overlapped, reflecting a moderate degree of separability. In this configuration, the antenna–tag coupling is less sensitive to microscopic device-specific perturbations, resulting in a broader inter-device distribution of the HD and a partial overlap with the intra-device one. Conversely, for the orthogonal orientation, the inter- and intra-distributions are clearly distinguishable, leading to higher decidability values, up to $D \approx 8$ depending on the operating frequency. Here, the stronger and more sensitive coupling enhances the impact of device-specific electromagnetic variability, yielding a narrower inter-device distribution of HD and improved class separation. Overall, the results confirm that orthogonal configurations yield the best performance in terms of both stability and separability. More generally, these results identify the interrogation geometry as a key design parameter of the challenge–response space, enabling reliable device discrimination by maximizing sensitivity to intrinsic device-specific perturbations, even in the presence of residual measurement dispersion.

I. Impact of Sampling on the Performance

Finally, Tab. V summarizes the number of Degrees of Freedom obtained as a function of the frequency sampling density of the measurement database. The frequency step Δf was varied from 1 MHz to 30 MHz, by increments of 5 MHz, thus progressively reducing the number of spectral samples used for key generation and accordingly the measurement duration. The results indicate that the DoF values remain nearly constant up to sampling steps of 15 MHz, beyond which a gradual reduction is observed. Nevertheless, the dependence on sampling density is not dramatic: even with a coarse step of 30 MHz, corresponding to only 23 frequency samples, the system still yields up to 44 independent Degrees of Freedom, which theoretically translates to more than 10 trillion statistically independent keys.

J. Sensitivity to Small Misalignments

To further assess the robustness of the proposed PUF architecture, the sensitivity of the extracted cryptographic response to small tag–antenna misalignments was explicitly investigated. A representative and intentionally conservative configuration was considered, namely the loop antenna in ∥ orientation, which was previously shown to exhibit reduced decidability. Controlled millimetric displacements of the tag w.r.t. the nominal interrogation position were introduced along the horizontal and vertical axes of the loop antenna plane (Δx, Δy). For each displaced position, the full processing chain was

TABLE VI
COMPARISON WITH STATE OF THE ART GRAPHENE-BASED INTRINSIC PUF TECHNOLOGIES

Type	DoF [bit]	Uniqueness	Uniformity	Challenge/Response Mechanism	Wireless Compatibility	Ref.
DEP-based PUF	221	0.50 ± 0.04	0.96-0.99	RF Frequency/RF response	Yes	[35]
Graphene Quantum Capacitor	246	0.50 ± 0.01	0.99-0.98	Fixed RF source/RF response	Yes	[36]
Graphene Raman-based	118	0.51 ± 0.046	0.99	Spatial scan position/Raman spectrum	No	[37]
Graphene-Based Straintronic PUF	244	0.49 ± 0.032	0.99	Strain stimulus/GFET transfer characteristic	No	[14]
This work	76	0.51 ± 0.17	0.98-0.99	RF query/RF response	Yes	This work

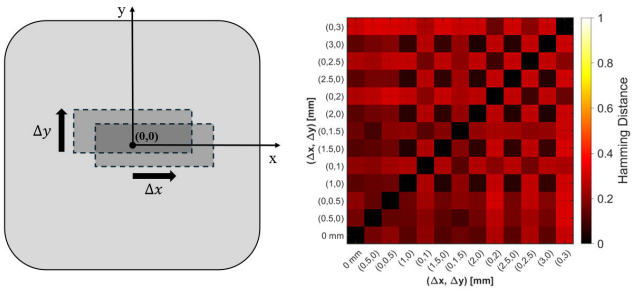

Fig. 19. (Left) Schematic representation of the relative positioning between the tag and the loop reader antenna. (Right) Pairwise intra-device HD matrix obtained by comparing the binary keys extracted from the same tag at all tested positions.

repeated, and the resulting binary keys were compared pairwise by computing the intra-device HD. The results, reported in Fig. 19, show that the average value remains around 0.2 across all tested positions, which is comparable to the variability observed in repeated measurements at a fixed position. This indicates that small positioning errors within the explored range do not significantly affect the extracted cryptographic response and do not compromise device discriminability.

VI. SUMMARY AND CONCLUSION

This work demonstrates the feasibility of extracting cryptographic information from RFID antennas fabricated through LIG for eco-sustainable authentication applications. No intentional modification of the antenna geometry is introduced: the entropy source is instead the intrinsic microstructural variability naturally induced by the laser engraving process. Through an appropriate acquisition and binarization pipeline, reproducible digital fingerprints are directly obtained from the near-field electromagnetic responses of the tags. Although the achievable number of Degrees of Freedom remains lower than that of optical or nanoscale intrinsic PUFs (Tab. VI), the proposed system generates up to 76 independent bits per key, with performance levels comparable to state-of-the-art wireless PUFs. The cryptographic analysis confirms reliability values above 0.9 and decidability exceeding 5 over a wide range of interrogation powers, indicating stable and statistically distinguishable responses. Multiple independent key families can be extracted by varying frequency, input power, and reader–tag orientation, with orthogonal configurations consistently yielding higher DoF. Although this study focuses on LIG antennas with high material-induced variability, the same framework and metrics are, in principle, applicable to commercial RFID inlays, where entropy is expected to be dominated by IC-related effects rather than by the antenna itself. Some limitations remain. The proposed PUF relies on out-of-RFID-band interrogation and on a reader configuration that must be faithfully reproduced during verification, as the employed commercial reader does not provide calibrated I/Q measurements. Accordingly, the reader and interrogation setup are considered part of the challenge-response mechanism. Future work will address reader-to-reader variability through a multi-reader experimental campaign. Moreover, further long-term experiments will nevertheless be required to confirm the robustness of the extracted cryptographic keys under prolonged environmental exposure, despite the demonstrated stability of encapsulated LIG traces [38]. Overall, the results show that LIG-based RFID antennas can act not only as identification or sensing elements, but also as intrinsic hardware cryptographic primitives. This work lays the groundwork for green, secure, and recyclable RFID technologies that combine material-level uniqueness with standard wireless interoperability.

ACKNOWLEDGMENT

The authors would like to thank Prof. Massimo Regoli for the valuable discussions.

REFERENCES

[1] M. Gallo, A. Viola, and G. Romagnoli, "The contribution of RFID to circular economy deployment: A literature review," *Int. J. RF Technol.*, vol. 15, no. 2, pp. 145–165, Aug. 2025.
[2] Y. Duroc, "RFID and the circular economy: A cross view between technical aspects and philosophical perspectives," *IEEE J. Radio Freq. Identificat.*, vol. 9, pp. 350–360, 2025.
[3] A. Kumar, A. K. Jain, and M. Dua, "A comprehensive taxonomy of security and privacy issues in RFID," *Complex Intell. Syst.*, vol. 7, no. 3, pp. 1327–1347, Jun. 2021.
[4] F. B. Jordan and M. Kutter, "Identifying counterfeit medicines with industry-suitable technologies," *Pharmaceutical Eng., Off. Mag. ISPE*, vol. 32, no. 3, 2012.
[5] Y. M. Al-Worafi, "Counterfeit medications in the developing countries," in *Handbook of Medical and Health Sciences in Developing Countries: Education, Practice, and Research*. Cham, Switzerland: Springer, 2023, pp. 1–20.
[6] B. Lecat, J. Brouard, and C. Chapuis, "Fraud and counterfeit wines in france: An overview and perspectives," *Brit. Food J.*, vol. 119, no. 1, pp. 84–104, Jan. 2017.
[7] Z. Yi, M. Yu, and K. L. Cheung, "Impacts of counterfeiting on a global supply chain," *Manuf. Service Oper. Manage.*, vol. 24, no. 1, pp. 159–178, Jan. 2022.
[8] Y. Chyan, R. Ye, Y. Li, S. P. Singh, C. J. Arnusch, and J. M. Tour, "Laser-induced graphene by multiple lasing: Toward electronics on cloth, paper, and food," *ACS Nano*, vol. 12, no. 3, pp. 2176–2183, Mar. 2018.
[9] A. Mostaccio and G. Marrocco, "Laser-induced graphene: A green technology for the IoT," *IEEE Electron Devices Mag.*, vol. 2, no. 2, pp. 11–22, Jun. 2024.
[10] A. Mostaccio, F. Naccarata, F. M. C. Nanni, J. Filippi, E. Martinelli, and G. Marrocco, "Soft and flexible wireless epidermal plaster made by laser-induced graphene," *IEEE Sensors Lett.*, vol. 8, no. 7, pp. 1–4, Jul. 2024.
[11] L. Huang, J. Su, Y. Song, and R. Ye, "Laser-induced graphene: En route to smart sensing," *Nano-Micro Lett.*, vol. 12, no. 1, p. 157, Dec. 2020.

[12] F. P. Chietera et al., "Laser-induced graphene, fused filament fabrication, and aerosol jet printing for realizing conductive elements of UHF RFID antennas," *IEEE J. Radio Freq. Identificat.*, vol. 6, pp. 601–609, 2022.
[13] A. Dodda, S. Subbulakshmi Radhakrishnan, T. F. Schranghamer, D. Buzzell, P. Sengupta, and S. Das, "Graphene-based physically unclonable functions that are reconfigurable and resilient to machine learning attacks," *Nature Electron.*, vol. 4, no. 5, pp. 364–374, May 2021.
[14] S. Ghosh, Y. Zheng, S. S. Radhakrishnan, T. F. Schranghamer, and S. Das, "A graphene-based straintronic physically unclonable function," *Nano Lett.*, vol. 23, no. 11, pp. 5171–5179, Jun. 2023.
[15] A. Al-Meer and S. Al-Kuwari, "Physical unclonable functions (PUF) for IoT devices," *ACM Comput. Surv.*, vol. 55, no. 14s, pp. 1–31, Dec. 2023.
[16] A. Yadav, S. Kumar, and J. Singh, "A review of physical unclonable functions (PUFs) and its applications in IoT environment," in *Proc. Ambient Commun. Comput. Syst. RACCCS*. Springer, 2022, pp. 1–13.
[17] E. Mann-Andrews, T. McGrath, B. Halliday, and R. J. Young, "A guide for assessing optically imaged physically unclonable functions for authentication," *Appl. Phys. Rev.*, vol. 12, no. 2, Jun. 2025.
[18] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one way functions," *Sci.*, vol. 297, no. 5589, pp. 2026–2030, 2002.
[19] U. Rührmair et al., "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov. 2013.
[20] A. Lazaro, M. R. Cujilema, R. Villarino, M. Lazaro, and D. Girbau, "A novel approach for wine anti-counterfeiting using laser-induced graphene chipless RFID tags on cork," *Sci. Rep.*, vol. 15, no. 1, p. 12750, Apr. 2025.
[21] A. Lazaro, M. R. Cujilema, R. Villarino, M. Lazaro, and D. Girbau, "Anti-counterfeiting near-field chipless RIFD tags based on laser-induced graphene on cork," *IEEE J. Radio Freq. Identificat.*, vol. 9, pp. 295–307, 2025.
[22] F. M. C. Nanni and G. Marrocco, "Defected laser-induced-graphene (LIG) antennas for physical unclonable function applications," in *Proc. 19th Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2025, pp. 1–4.
[23] G. D. Knott, "Hashing functions," *Comput. J.*, vol. 18, no. 3, pp. 265–278, Mar. 1975.
[24] F. M. C. Nanni and G. Marrocco, "Enhancing RFID antenna electromagnetic fingerprints through non-linear interrogation," *IEEE J. Radio Freq. Identificat.*, vol. 9, pp. 46–53, 2025.
[25] A. Gersho, "Principles of quantization," *IEEE Trans. Circuits Syst.*, vol. 25, no. 7, pp. 427–436, 2003.
[26] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.
[27] L. Yu, X. Wang, F. Rahman, and M. Tehranipoor, "Interconnect-based PUF with signature uniqueness enhancement," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 2, pp. 339–352, Feb. 2020.
[28] J. He et al., "A weak-PUF-assisted strong PUF with inherent security using metastability implemented on FPGAs," *Electronics*, vol. 14, no. 5, p. 1007, Mar. 2025. [Online]. Available: https://www.mdpi.com/2079-9292/14/5/1007
[29] *Dupont. Kapton HN General-Purpose Polyimide Film*. Accessed: Mar. 2004. [Online]. Available: https://www.dupont.com/electronics-industrial/
[30] *McMaster-Carr. Polyimide Sheets*. Accessed: Mar. 2004. [Online]. Available: https://www.mcmaster.com/products/polyimide-sheets
[31] Ossila. (2025). *Four-Point Probe*. Accessed: Apr. 19, 2025. [Online]. Available: https://www.ossila.com/products/four-point-probe-system
[32] L. Catarinucci, R. Colella, P. Coppola, and L. Tarricone, "Microwave characterisation of polylactic acid for 3D-printed dielectrically controlled substrates," *IET Microw., Antennas Propag.*, vol. 11, no. 14, pp. 1970–1976, Nov. 2017.
[33] Keonn Technologies S. L. (2024). *Advantenna-L11 RFID UHF Near Field Antenna*. Keonn Advantenna-L11 Datasheet, Barcelona, Spain. [Online]. Available: https://keonn.com
[34] Molex, LLC, *865/915MHz ISM Stand Alone Antenna, Series 105262*, document PS-1052620001, Product Specification, Oct. 2022. [Online]. Available: https://www.molex.com
[35] M. Yang, L. Zhu, Q. Zhong, R. El-Ganainy, and P.-Y. Chen, "Spectral sensitivity near exceptional points as a resource for hardware encryption," *Nature Commun.*, vol. 14, no. 1, p. 1145, Feb. 2023.
[36] Y. Ren, C.-H. Sun, C.-H. Liu, C.-T.-M. Wu, and P.-Y. Chen, "Wireless anti-counterfeiting labels using RF oscillators with graphene quantum capacitors," *IEEE J. Radio Freq. Identificat.*, vol. 9, pp. 38–45, 2025.
[37] S. Lee, S. Pekdemir, N. Kayaci, M. Kalay, M. S. Onses, and J. Ye, "Graphene-based physically unclonable functions with dual source of randomness," *ACS Appl. Mater. Interface*, vol. 15, no. 28, pp. 33878–33889, Jul. 2023.
[38] A. Mostaccio, G. Antonelli, M. Bragaglia, E. Martinelli, and G. Marrocco, "Comparative evaluation of laser-induced graphene (LIG) traces on polyimide under soft and hard stress for IoT applications," *IEEE J. Flexible Electron.*, vol. 2, no. 3, pp. 256–264, May 2023.

Francesca M. C. Nanni (Member, IEEE) received the M.Sc. degree (Hons.) in medical engineering from the Tor Vergata University of Rome, Italy, in 2022, where she is currently pursuing the Ph.D. degree in computer science, control, and geoinformation. She has also been a part-time Medical Engineer at RADIO6ENSE Srl. She is also part of the Cyber4Health Project, which raises international awareness about the need to apply cyber and physical security by design in medical devices. Her research interests include physical unclonable functions (PUF) made with unconventional materials, like laser-induced graphene (LIG), and how to increase the randomness of antenna structures to gain more information and unique cryptographic keys. She has been the co-author of the paper "Cyber-Tooth: Antennified Dental Implant for RFID Wireless Temperature Monitoring" being the Winner of the Best Student Paper Award at the 2021 IEEE International Conference on RFID Technology and Applications (RFID-TA). She won the Best Student Paper Award at the IEEE International Conference on RFID-TA in 2022 and 2023. She won the Gaetano Latmiral Award at Italian National Meeting on Electromagnetism (Rinem 2024).

Gaetano Marrocco (Fellow, IEEE) received the Laurea degree in electronic engineering and the Ph.D. degree in applied electromagnetics from the University of L'Aquila, Italy, in 1994 and 1998, respectively.

He was a Researcher at the University of Roma Tor Vergata from 1994 to 2014, where he was an Associate Professor of electromagnetics from 2013 to 2017, and a Guest Professor at the University of Paris-Est Marne-la-Vallée in 2015. He has been a Full Professor at the University of Rome Tor Vergata since 2018. He was the Director of the Medical Engineering School from 2018 to 2024, where he is currently the Deputy Director of the Department of Civil Engineering and Computer Science Engineering. The first part of his research career was devoted to the modelling and design of broadband and ultra-wideband antennas for satellite (ESA, ASI), avionic, and naval (Leonardo) communications. Since 2003, he has been investigating sensor-oriented miniaturized antennas for biomedical engineering and radio-frequency identification (RFID), contributing to the transition from RF object labeling to passive sensor networks in the Internet of Things era. He is the Director of the Pervasive Electromagnetics Laboratory (pervasive.ing.uniroma2.it) and the Co-Founder and the President of the University spin-off RADIO6ENSE (www.radio6ense.com), active in short-range electromagnetic sensing for the Industrial Internet of Things, smart manufacturing, automotive bioengineering, and pharma. He carried out pioneering research on body-centric and battery-less wireless sensors, including textile RFID antennas, tattoo-like sensors (flexible and stretchable epidermal electronics), and radio-sensors embedded in implantable prostheses. More recently, his research has focused on natural dielectrics and laser-based processing for a new generation of eco-friendly wireless devices.

Prof. Marrocco was a member of the IEEE Antennas and Propagation Society Awards Committee. He was the Chair of the Local Organizing Committee of the 2011 EuCAP; the TPC Chair of the IEEE RFID-TA 2012, Nice, France; the TPC Track Chair of the 2016 IEEE Antennas and Propagation International Symposium and the 2018 IEEE RFID, USA; and the General Co-Chair of the 2024 IEEE Flexible, Printable Sensors and Systems Conference (FLEPS), Tampere, Finland. He is the Chair of Italian Delegation of URSI Commission D (Electronics and Photonics). He has served as Associate Editor for IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS and IEEE JOURNAL OF RADIO FREQUENCY IDENTIFICATION. He is an Associate Editor of IEEE JOURNAL OF FLEXIBLE ELECTRONICS.