Enhancing RFID Antenna Electromagnetic Fingerprints through Non-Linear Interrogation

Francesca M. C. Nanni, *Graduate Student Member, IEEE,* Gaetano Marrocco, *Senior Member, IEEE*

***Abstract*—Fingerprinting stands as an effective non-intrusive and non-destructive method to ensure physical security in wireless systems and Radio-Frequency Identification (RFID) applications. Conventionally, the most common state of the art approach involves extracting signal features from the devices and employing machine learning techniques for the classification of counterfeit or cloned ones.**

This paper explores how to enhance RFID antenna electromagnetic fingerprints by proposing a multi-power interrogation approach. Unlike traditional methods, our technique emphasizes the non-linear behavior of RFID integrated circuits (ICs) by properly varying the reader input power and frequencies.

This strategy increases the unpredictability of the IC impedance modulation, thereby extracting richer and more complex information from the RFID tags. Using Shannon Information Theory, we can quantify the entropy of these enhanced fingerprints, revealing an average increase of almost 2 bits in the information content compared to single-power level interrogations. Our findings can lay the foundations to implement more robust RF physical unclonable functions (PUFs) with robust physical keys against counterfeiting and replication threats.

***Index Terms*—RFID, security, authentication, electromagnetic fingerprinting.**

I. Introduction

Radio-frequency Identification (RFID) technology is now a cornerstone in logistics and manufacturing [1], bio-engineering, and the Industrial and Medical Internet of Things. However, its extensive utilization has underscored concerns regarding physical security, particularly the susceptibility of RFID devices to counterfeiting and replication [2], [3]. After intercepting the tag during transmission, the primary goal of these attacks is to reproduce or attempt to create a near replica of the tag [4]. Cloning can compromise the integrity and reliability of RFID-enabled systems [5], leading to financial ramifications and raising serious questions about data legitimacy and confidentiality, thereby heightening the risk of security breaches [6].

Over the past few years, RFID tag authentication has emerged as a huge challenge due to the limitations of advanced cryptographic algorithms for passive tags [7], i.e., Elliptic Curve Cryptography (ECC) asymmetric algorithms [8]. Indeed, traditional authentication methods would require specialized devices, while tags only have restricted computational capabilities and resources [9], or are sensitive to environmental conditions. Recent research has focused on Physical-Layer Identification (PLI), commonly known as RF fingerprinting [10]. This is an authentication system based on distinctive features discovered during signal transmission that can be used as the device's fingerprint. Unlike cryptography-based approaches used in the upper layers of a network, these methods can provide security by exploiting signal and wireless channel unpredictability [11]. Any transmitter produces indeed device-specific distortion in its analog signal which is created by unique flaws in its hardware components. These imperfections, which are inevitably introduced during the manufacturing process, including transmitter-phase noise, digital-to-analog converters, band-pass filters, frequency mixers, and power amplifiers, contribute to the uniqueness of RF devices [12].

RF fingerprinting methods have been explored in various commercial areas, including the Automatic Dependent Surveillance broadcast (ADS-B) system used in Air Traffic Control [13], Bluetooth [14], push-to-talk transmitters [15], and RFID [16]. RFID tags in particular have been recognized as suitable candidates for fingerprinting due to inherent IC manufacturing flaws, and find applications across fields like intrusion detection, access control, cloning and counterfeit detection, and secure localization, with very low impact on the device's resources [17]. Leveraging fingerprints for anti-counterfeiting offers additional advantages. For example, fingerprints, being unique and unforgeable, provide robust security against various attacks, and they require no hardware or firmware updates on existing systems, which ensures compatibility with millions of deployed RFID tags.

Also in RFID chipless applications, where the information (i.e., the EM signal) is directly linked to the geometry of the printed elements, by leveraging the natural randomness in the tag fabrication process [18], [19], or the novel additive manufacturing technologies [20], fingeprinting allows to achieve high level of security.

Despite the fact that there is no reference protocol for RFID fingerprinting, the signal returned by the devices is commonly expoited to extract features. Experiments with RF fingerprinting have demonstrated that counterfeit devices can be identified and isolated by feature selection with machine learning (ML) [21] and deep learning techniques [22], [23], [24]. Sometimes RFID devices can also be complemented with random inexpensive physical objects, that behave as an RF certificate of authenticity (CoA), so that they become physically unique and hard to near-exactly replicate [25]. In this way, the device can provide a physically-defined fingerprint, like a Physical Unclonable Function (PUF) [26], which generates several unique and unpredictable *digital keys* by extracting variations during the microchip manufacturing process [27], [28]. In particular, the work in [29] introduced the RF-DNA for large-scale RFID identification, taking advantage of the frequency agnostic phenomenon where tags can respond within a wider band than the regulated one, to capture more features than common fingerprints. This unique RFID fingerprint is generated by the interaction between the integrated

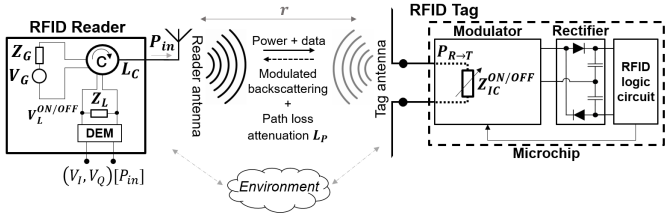

Fig. 1. Schematic of the RFID architecture including the voltage V_G and equivalent impedance Z_G of the reader generator, which is separated from the load Z_L of the reader receiving chain by a circulator *C*. The reader sends queries with a selected input power P_{in} to the tag, which has an equivalent RF modulation impedance $Z_{IC}^{ON/OFF}$, and sends back a signal which once demodulated is retrieved at the reader's load.

circuit (IC) and antenna, thereby increasing the complexity and security of the corresponding digital key. By enhancing its intrinsic information, meaning boosting its irregularity and unpredictability, the tag's response will become harder to replicate and will enable more robust authentication.

Starting from the problem formulation in [29], which defines the fingerprint of an RFID device for a fixed interrogation power, the goal of this work is to enrich the complexity of RF fingerprints by exploiting the non-linear behavior of the RFID ICs. Specifically, we leverage the distinctive non-linear response of IC impedances to the impinging RF power [30], [31], [32] to bring out more *secrets* from the device, maximize the information content and obtain a much more unpredictable response. The increase of information is quantified by Shannon's Information Theory [33], by evaluating the entropy of the RFID fingerprint.

A preliminar idea of multi-power interrogation was recently introduced in [34], proving the potential to increase the entropy of a single RFID device, although the query process had not yet been fully optimized. By extending these findings, the overall goal now is to define an optimal interrogation procedure, based on variable input power at the reader side, to maximize the achievable entropy. The method will be applied to three families of tags having different IC architectures.

The paper is organized as follows: Section II introduces the RF fingerprint of an RFID tag and the metrics for the measurement of its information content. Section III addresses the information augmentation by multiple-power interrogation and proposes a procedure for the optimal query of the tag. The outcomes of the experimental tests with three families of tags are reported in Section IV and the achievable increase of information by non-linear fingerprints is evaluated. Finally, the most valuable results and further challenges are discussed in the Conclusions.

II. Backscattering Fingerprint and Entropy

An RFID device sends back the data contained in the chip memory by switching its input impedance between two states $\{Z_{IC}^{ON}, Z_{IC}^{OFF}\}$, and thus modulating the backscattered signal so that the corresponding voltages at the reader's port (Fig. 1) load are $\{V_L^{ON}, V_L^{OFF}\}$ [35]. Under free-space conditions, the differential received voltage, after the demodulation, can be expressed in terms of both tag and reader parameters, so that:

$$V = V_L^{OFF} - V_L^{ON} = \frac{\eta_0}{k_0^2} G_R \sqrt{\frac{P_{in} R_R^{in}}{2}} g^2 \cdot \cdot \left(\frac{1}{Z_A + Z_{IC}^{OFF}} - \frac{1}{Z_A + Z_{IC}^{ON}}\right) \frac{e^{-2jk_0 r}}{r^2}, \quad (1)$$

where $\eta_0 = 120\pi\,\Omega$ is the vacuum characteristic impedance; k_0 is the propagation constant; G_R is the gain of the reader antenna; P_{in} is the power feeding the antenna of the reader; R_R^{in} is the input resistance of the reader antenna; *r* is the reader-tag distance. The term g is the normalized gain of the tag:

$$g = \sqrt{\frac{R_A^{in} G_{tag}(\hat{\boldsymbol{r}}) \chi}{\eta_0}} e^{j\phi(\hat{\boldsymbol{r}})}, \quad (2)$$

with R_A^{in} the input resistance and $G_{tag}(\hat{r})$ is the gain of the tag antenna.

The phase of the backscattered signal from the tag and retrieved by the reader is $\phi = arg(V_L^{OFF} - V_L^{ON})$ and can be expressed with respect to the antenna and IC as:

$$\phi = -2k_0 r + 2\Phi(\hat{\boldsymbol{r}}) + arg\left(\frac{1}{Z_A + Z_{IC}^{OFF}} - \frac{1}{Z_A + Z_{IC}^{ON}}\right). \quad (3)$$

The phase consists of three components: the round-trip delay $-2k_0 r$ accounts for the distance *r* between the reader and tag; the polarization term $2\Phi(\hat{\boldsymbol{r}})$ incorporates the polarization mismatch between the reader and tag; and finally, the last term includes the relationship between the phase and the input impedance of the tag antenna, as well as the impedance switch of the microchip. It is worth noticing that the term $\left(\frac{1}{Z_A + Z_{IC}^{OFF}} - \frac{1}{Z_A + Z_{IC}^{ON}}\right)$ is related to the differential radar cross section (RCS) of the tags as in [36].

A. Phase and quadrature of the fingerprint

The architecture of typical UHF RFID readers is based on a direct in-phase/quadrature (I/Q) conversion performed by the receiver [37]. After a standard interrogation at a frequency f with a reader input power P_{in} (Fig. 1), we can hence represent the voltage in (1) as a complex signal $V(f, P_{in})$, comprising an in-phase $V_I = V cos\phi$ and in-quadrature $V_Q = V sin\phi$ components:

$$V(f, P_{in}) = |V(f, P_{in})| e^{j\phi(f, P_{in})} = V_I(f, P_{in}) + jV_Q(f, P_{in}). \quad (4)$$

The measured signal also includes the contribute of the environment (path loss attenuation L_P), the round-trip phase delay along a reader-tag distance *r*, the cable losses L_C, the reader antenna gain, and the input power. We then denote *backscattering fingerprint F* of the device the following entity that is derived from (4) after de-embedding the above contributions, assumed known or dropped out by calibration, namely:

$$F(f, P_{in}) = \frac{V(f, P_{in})}{\sqrt{P_{in} G_R L_C L_P}} e^{j(\phi + 2k_0 r)} = F_I(f) + jF_Q(f) \quad (5)$$

where all parameters are in linear scale. By varying the frequency in a discrete set $\{f_n\}$, $n = 1, .., N$, the couplets $F_n = \{F_I(f_n), F_Q(f_n)\}$ form a *constellation* of symbols in the I/Q plane.

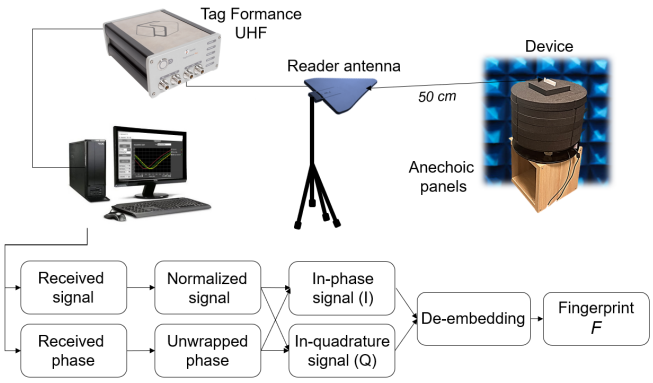

Fig. 2. Measurement setup of the experimental corroboration with the post-processing blocks, including the normalization of the signal and the coomputation of the fingerprint F.

B. Information Content

We can expect that the fingerprint will be more difficult to reproduce, and hence easily identifiable, as its variability increases, or in other words, when it contains more information. This quantity, that measures the uncertainty or unpredictability of a signal, is given by Shannon entropy. More in details, the information related to *F*, given the mutual dependence of F_I and F_Q, can be quantified specifically by the *joint entropy* $H(F_I, F_Q)$ [33], as:

$$H(F_I, F_Q) = -\sum_i \sum_q p(i,q) \log_2 p(i,q) \tag{6}$$

where $p(i,q)$ is the joint probability of the pair event, namely the occurrence of the sample $(F_{I,i}, F_{Q,q})$ couplet over the constellation corresponding to the fingerprint of the antenna, and i and q are the new indexes once we have reordered all the samples on the I/Q plane. Due to the presence of a base-two logarithm, the unit of measurement traditionally associated with (6) is the Bit.

In general, we expect higher entropy when there is more uncertainty or randomness in the data. In the context of signals, entropy will be higher when the symbols of the fingerprint constellation are rather uniformly distributed so that they are more unpredictable, as for example when the constellation tends to a very noisy or a complex non-periodic structure. On the contrary, if many symbols of the constellation are overlapped, the fingerprint will carry less information.

III. Non-linear fingerprint

In passive UHF RFID devices, the highly reactive impedance of the IC is significantly influenced by the input power, and this relationship is inherently non-linear, because of the features of the internal rectifier [31]. The RF resistance is likely to increase with respect to the power [30], and the IC sensitivity (p_{IC}, namely the minimum collected power required to activate the IC), is also dependent on the total RF power delivered to the IC by the antenna. Consequently, the backscattered properties, particularly the radar cross-section, which is inversely proportional to the IC impedance, will also non-linearly depend on the input power P_{in}. This non-linear relationship will eventually affect the fingerprint *F* as well and can be taken as an advantage, since interrogating the device with different power levels, could mean that the information returned is likely to vary. Therefore, given the non-predictable change of the impedance modulation, we expect the entropy of an augmented fingerprint corresponding to properly selected set of interrogation power levels will increase w.r.t. the one retrieved with only one interrogation power (i.e., the maximum available as in [29]).

A. Multi-power matrix

Assuming to repeat the interrogation in the same conditions, but for different input powers in the set $\{P_{in,m}\}, m = 1, .., M$, the following *fingerprint matrix* is obtained:

$$\boldsymbol{F_{NL}} = \begin{bmatrix} F_{1,1} & \cdots & F_{1,M} \\ \vdots & \ddots & \vdots \\ F_{N,1} & \cdots & F_{N,M} \end{bmatrix} \tag{7}$$

where $F_{n,m} \triangleq F(f_n, P_{in,m}) = F_{In,m} + jF_{Qn,m}$.

B. Query power optimization

As shown in the next experimental section, that entropy is expected not to increase monotonically with the number of interrogation powers since some symbols of the whole constellation could be repeated, thus lowering the amount of information. Moreover, as multiple-frequency interrogation takes time, we want to identify the smallest combination Ω_O of query powers that maximizes the entropy $H(F_{NL})$.

The total number N_C of possible combinations of *M* powers is:

$$N_C = \sum_{k=1}^{M} C(M,k);$$

where *C(M,k)* is the number of possible sets $\{\Omega_{k,l(k)}\}$ comprising k input powers, with $l(k) = 1, .., C(M,k)$, and the latter is given by the binomial coefficient:

$$C(M,k) = \frac{M!}{k!(M-k)!}.$$

Since the non-linear response of the IC is not a-priori known, and can be IC-specific, the optimal set Ω_O maximizing the entropy must be derived experimentally for the specific tag, or tag family, by the following procedure:

1) evaluate $\boldsymbol{F_{NL}}$ (namely for all the frequencies and power samples);
2) compute the entropy of the non-linear fingerprint for all the possible combinations of interrogation powers, namely $H(\boldsymbol{F_{NL}}[\Omega_{k,l(k)}])$;
3) identify the set Ω_O so that $H(\boldsymbol{F_{NL}}[\Omega_O])$ is maximum.

The set Ω_O will be then stored and used for successive authentications of the tag.

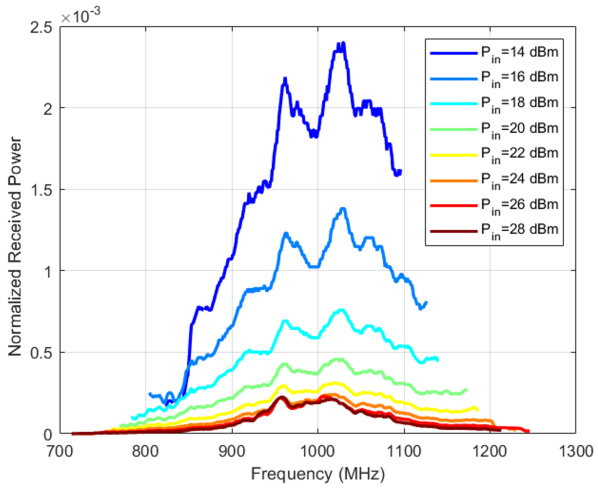

Fig. 3. Backscattered powers for the RFM3200-AER tag, normalized with respect to different P_{in} values.

IV. Experimentation

The above concepts are demonstrated by a an experimental compaign involving three reference tags having different shapes and hosting different types of IC. Namely, there is the RFM3200-AER meander line dipole ($tag\ \#1$) and a HID Omni-ID M3D patch ($tag\ \#2$), both embedding the same Magnus-S3 IC by Axzon, with a nominal sensitivity $p_{IC} = -16.6$ dBm [38]. This IC, that also provides temperature measurements, has auto-tuning capability, namely its input reactance is automatically modified through an internal varactor, to maintain a stable matching to the antenna impedance. This unique feature generally returns wide-band backscattering signals. The third tag is the UCODE A488R00 DNA dipole ($tag\ \#3$) with the Ucode IC by NXP without auto-tuning technology, with a read sensitivity $p_{IC} = -19$ dBm.

The measurement setup comprises the Voyantic TagFormance UHF Pro Station and some anechoic panels (Fig. 2). The following assumptions were consistently maintained during the tests:

- the reader antenna and the tag were placed within each other's far field, with a fixed query distance of 50 cm;
- the tags and reader antenna were oriented such to minimize the polarization mismatch.

The $(F_{I,i}, F_{Q,q})$ couplets were collected for sweeps of:

- *frequency*: from 600 to 1100 MHz with steps of 1 MHz, for a total of 701 samples. It is worth noticing that this range is much wider than the standard UHF RFID band;
- *input power*: 14 to 28 dBm with steps of 2 dBm, for a total of 8 steps.

Accordingly, the non-linear fingerprint matrix $\boldsymbol{F_{NL}}$ comprises 5608 entries.

A. Fingerprints analysis

The non-linear beavour of the response of the IC is easily visible in Fig. 3, that reports an example of backscattered power vs. frequency, normalized by the input power. The profiles are rather different and in particular the normalized backscattered powers reduce as the input power increase. This is probably due, from (1), to a possible increase of the input impedance of the IC along with the interrogation power, as documented in [30], that lower the differential RCS of the tag, and hence the backscattered power.

Fig. 4 shows all the eight fingerprints for the RFM3200-AER tag obtained for the eight interrogation powers. The profiles resemble non-cylindrical helical structures in 3D space and, as discussed above, are significantly different from one another, which confirms the advantage of a multi-power interrogation to capture a richer information from the device.

Fig. 5 shows the 3D representation of the global fingerprint $\boldsymbol{F_{NL}}(\Omega_M)$ for the all three considered RFID devices. The flattered view of the I/Q plane in Fig. 5 d), e) and f) depict diverse constellation of symbols, being those of tag #1 and #3 much richer, while that of tag #2 is restricted in a narrower frequency band. The evidence that the amount of information contained in a signal is closely related to its bandwidth is settled in the state of the art [39], [40]. We accordingly expect that tag #2 will exhibit significantly lower entropy values with respect to the two dipoles, due to its limited frequency response.

The profile referring to different input powers do not fully overlap, but contributes to a much richer structure. In all devices, the increase of the input power adds further *symbols* in the constellation, especially for low values of (F_I, F_Q). We also notice that this behavior looks independent from the type of IC technology (namely, static impedance or auto-tuning impedance). This means that under certain conditions, the device can reveal multiple secrets, uncovering details that would remain hidden with a single-power query. However, the top-view in Fig. 5 b) shows significant redundancies, which can unnecessarily increase the acquisition time without a corresponding improvement of the entropy. Indeed, Fig. 6 shows the calculated entropy referred to each considered input power, which does not grow monotonically with the input power so that, working at the highest power as in [29] is not automatically the best choice, even for a single-power interrogation.

B. Optimal input power combination

Fig. 7 shows the entropies related to all the possible $N_C = 255$ combinations $\{\Omega_{k,l(k)}\}$ of the input powers. We notice that the entropy has a large variation, in all three families, as the combinations of query powers vary. The best entropy values for each power group for the tags are given in Tab. I. In all cases, these entropies are significantly higher, almost 2 bits, than those obtained with any single power level, and the use of fewer measurements reduced redundancies. An increase of 2 bits means that the information richness is four-times larger than that for single power interrogation.

For tag $\#1$, the maximum entropy of 7 bits is achieved using six power levels, namely by six interrogations, but with four powers the entropy just reduces to 6.9 bits. For tag $\#2$, the maximum entropy of 5.5 bits was achieved with six powers. Finally, tag #3 slightly outperforms the other devices with a 7.1

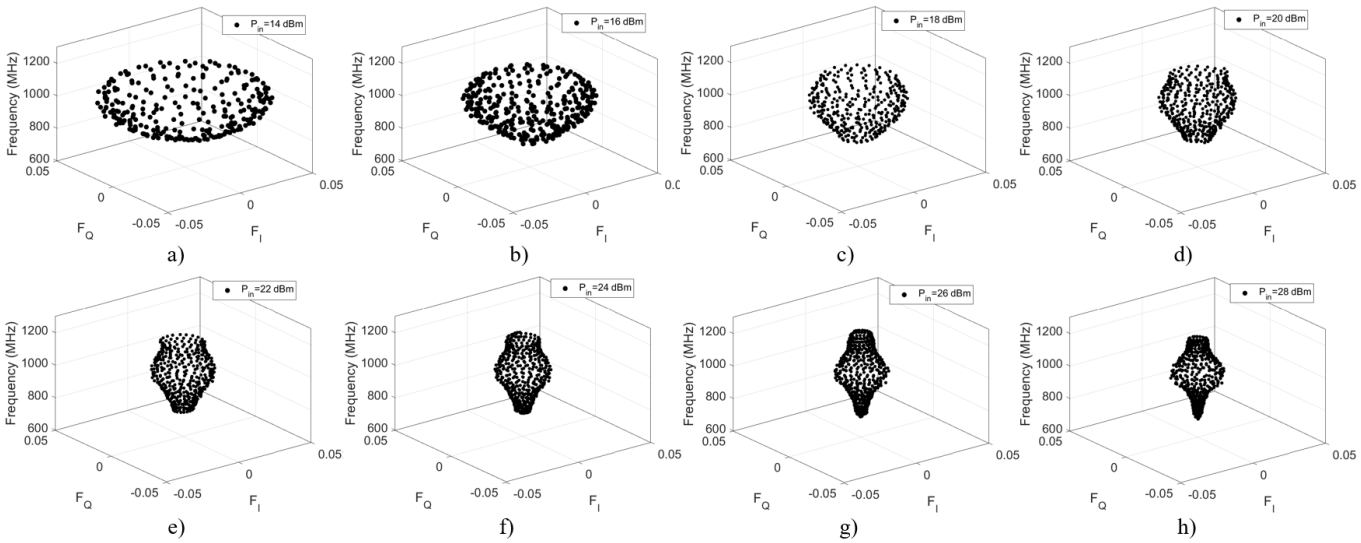

Fig. 4. Fingerprints of the the RFM3200-AER tag for different interrogation powers.

bits entropy value, as well obtained with seven interrogation power levels, but as for tag #1, five interrogation are enough if we accept a small degradation of the entropy (from 7.1 to 6.9 bits).

TABLE I
MAXIMUM JOINT ENTROPY FOR EACH COMBINATION OF POWERS, FOR M=1,..,8.

Number of powers	1	2	3	4	5	6	7	8
H tag #1 [Bit]	5.5	6.2	6.4	6.9	6.8	7	6.9	6.7
H tag #2 [Bit]	3.8	4.8	5	5.2	5.4	5.6	5.6	4.8
H tag #3 [Bit]	5.7	6.2	6.5	6.7	6.9	6.9	7.1	6.9

C. Inter-family information variability

The entropy measurement values for the three types of tags (tag #1, tag #2, and tag #3) were repeated for overall three different tags of the same model for each type. The results, as shown in Tab. II, indicate that the maximum entropy values are nearly identical, differing only in the second decimal digit. We finally found that for three tags of the same family, the optimal interrogation set and the sub-optimal one are the same (Tab. III).

TABLE II
MAXIMUM JOINT ENTROPY VALUES FOR THE THREE FAMILIES OF TAGS, EACH ONE INCLUDING THREE DIFFERENT TAGS OF THE SAME MODEL.

Family #1	H	Family #2	H	Family #3	H
1	7.02	1	5.57	1	7.09
2	7.03	2	5.59	2	7.07
3	7.01	3	5.57	3	7.08

V. CONCLUSIONS

Starting from the physical evidence that the electromagnetic response of an RFID tags is highly affected by the strength of the interrogation power, we have introduced a multi-power interrogation that is capable to enrich up to four times the information content of the RFID fingerprint with potential benefit for Physical Layer Authentication.

TABLE III
POWER SET THAT A) MAXIMIZES THE ENTROPY FOR EACH RFID DEVICE AND B) THE CORRESPONDING SUB-OPTIMAL SET .

Family	Optimal powet set [dBm]
#1	$\{14, 16, 18, 20, 26, 28\}$
#2	$\{18, 20, 22, 24, 26, 28\}$
#3	$\{14, 16, 18, 20, 22, 26, 28\}$

a)

Family	Sub-optimal powet set [dBm]
#1	$\{16, 18, 20, 26\}$
#2	$\{18, 20, 24, 26, 28\}$
#3	$\{16, 18, 20, 26, 28\}$

b)

The idea has been corroborated with tests with both static and dynamic impedance ICs. An optimal sequence of powers exists for each considered family of tags and there are also sub-optimal sets that can reduce the authentication duration at the cost of a modest degradation of the achievable information.

Further improvements could be expected by introducing more sophisticated interrogations where the input power can be optimized frequency by frequency and it will be the topic of future investigations.

ACKNOWLEDGEMENTS

Work supported by Project ECS 0000024 Rome Technopole, – CUP B83C22002820006, NRP Mission 4 Component 2 Investment 1.5, Funded by the European Union – NextGenerationEU. Spoke: 2.

The authors wish to thank Prof. Marco Donald Migliore, University of Cassino (IT), for the valuable discussions and suggestions.

REFERENCES

[1] S. Anandhi, R. Anitha, and V. Sureshkumar, "Iot enabled rfid authentication and secure object tracking system for smart logistics," *Wireless Personal Communications*, vol. 104, pp. 543–560, 2019.

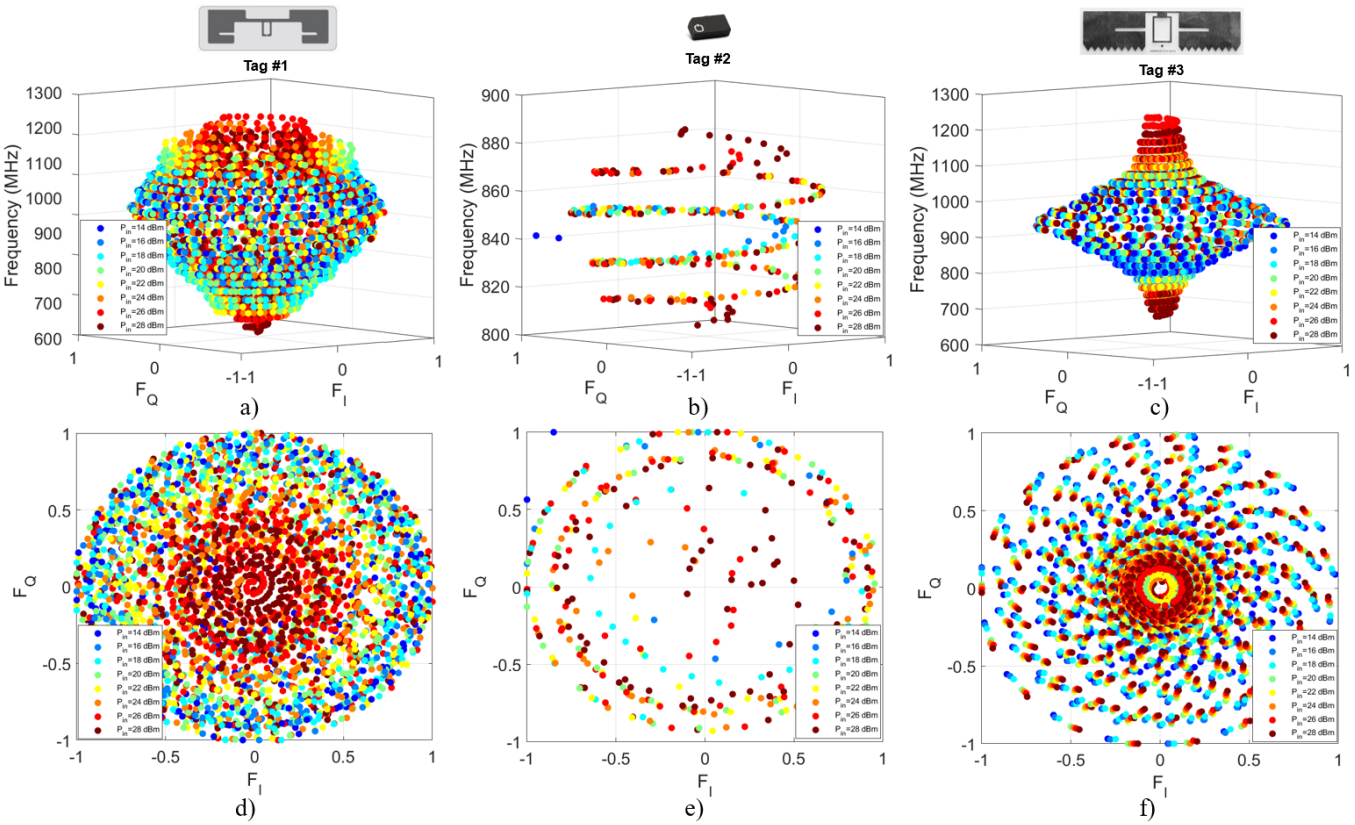

Fig. 5. Non-linear fingerprint of the RFM3200-AER tag #1 in a a) 3D visualization and a b) top view constellation of *symbols* for $P_{in} = \{14, 16, 18, 20, 22, 24, 26, 28\}$ dBm .

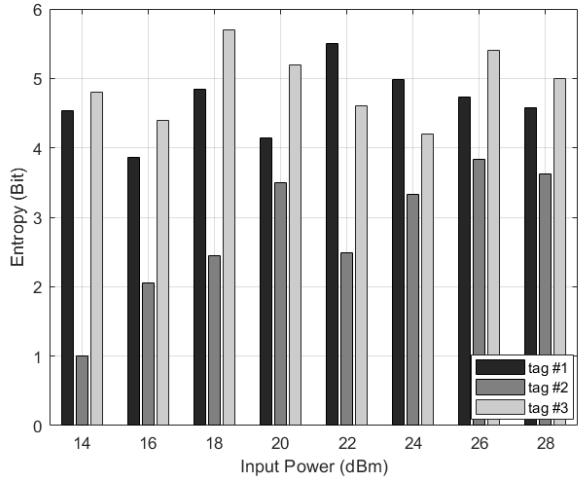

Fig. 6. Histogram of entropy values referring to each input power value, for tag #1, #2 and #3.

[2] C. Munoz-Ausecha, J. Ruiz-Rosero, and G. Ramirez-Gonzalez, "Rfid applications and security review," *Computation*, vol. 9, no. 6, p. 69, 2021.

[3] A. K. Singh and B. Patro, "Security attacks on rfid and their countermeasures," in *Computer Communication, Networking and IoT: Proceedings of ICICC 2020*. Springer, 2021, pp. 509–518.

[4] R. AL MOGBIL, M. AL ASQAH, and S. EL KHEDIRI, "Iot: Security challenges and issues of smart homes/cities," in *2020 international conference on computing and information technology (ICCIT-1441)*. IEEE, 2020, pp. 1–6.

[5] H. Kamaludin, H. Mahdin, and J. H. Abawajy, "Clone tag detection in distributed rfid systems," *PloS one*, vol. 13, no. 3, p. e0193951, 2018.

[6] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges," *Computer Networks*, vol. 219, p. 109455, 2022.

[7] A. Kumar, A. K. Jain, and M. Dua, "A comprehensive taxonomy of security and privacy issues in rfid," *Complex & Intelligent Systems*, vol. 7, no. 3, pp. 1327–1347, 2021.

[8] X. Tan, M. Dong, C. Wu, K. Ota, J. Wang, and D. W. Engels, "An energy-efficient ecc processor of uhf rfid tag for banknote anti-counterfeiting," *IEEE Access*, vol. 5, pp. 3044–3054, 2016.

[9] J. Chen, A. Miyaj, H. Sato, and C. Su, "Improved lightweight pseudo-random number generators for the low-cost rfid tags," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 17–24.

[10] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, pp. 1–29, 2012.

[11] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *Journal of Communications and Information Networks*, vol. 5, no. 3, pp. 237–264, 2020.

[12] S. U. Rehman, S. Alam, and I. T. Ardekani, "An overview of radio frequency fingerprinting for low-end devices," *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 6, no. 3, pp. 1–21, 2014.

[13] H. Ahmed, H. Khan, and M. A. Khan, "A survey on security and privacy of automatic dependent surveillance-broadcast (ads-b) protocol: Challenges, potential solutions and future directions," *Authorea Preprints*, 2023.

[14] H. Almashaqbeh, Y. Dalveren, and A. Kara, "A study on the performance evaluation of wavelet decomposition in transient-based radio frequency fingerprinting of bluetooth devices," *Microwave and Optical Technology Letters*, vol. 64, no. 4, pp. 643–649, 2022.

[15] C. Brady and S. Roy, "Analysis of mission critical push-to-talk (mcptt) services over public safety networks," *IEEE Wireless Communications Letters*, vol. 9, no. 9, pp. 1462–1466, 2020.

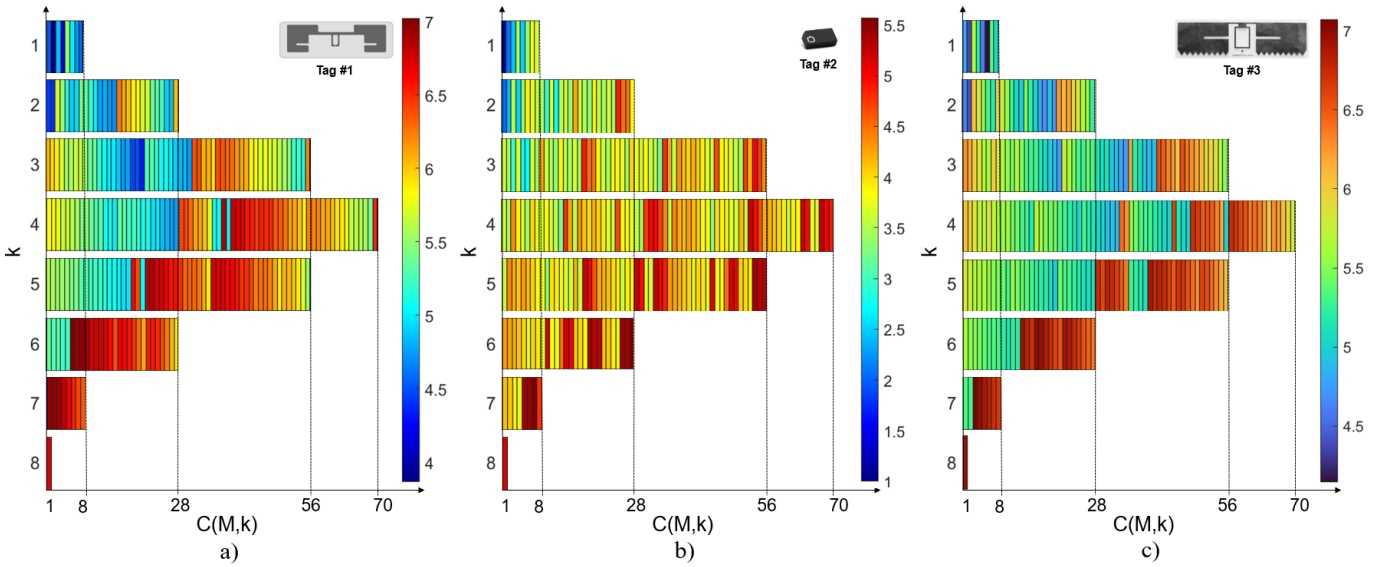

Fig. 7. Entropy heatmap for all the 255 combination of input powers for a) tag #1, b) tag #2 and c) tag #3. Each pixel represents the entropy of the global fingerprint produced by one of the possible combination of a number of interrogating power indicated in the x-axis.

[16] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 222–233, 2020.

[17] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B. C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, and T. Melodia, "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 646–655.

[18] Z. Ali, E. Perret, N. Barbot, R. Siragusa, D. Hély, M. Bernier, and F. Garet, "Detection of natural randomness by chipless rfid approach and its application to authentication," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 9, pp. 3867–3881, 2019.

[19] Z. Ali, E. Perret, N. Barbot, and R. Siragusa, *Chipless RFID Authentication: Design, Realization and Characterization*. John Wiley & Sons, 2022.

[20] S. Choudhury, F. Costa, G. Manara, and S. Genovesi, "3d chipless rfid tag for anti-counterfeiting applications," *IEEE Open Journal of Antennas and Propagation*, 2024.

[21] S. Li, M. Cheng, Y. Chen, C. Fan, L. Deng, M. Zhang, S. Fu, M. Tang, P. P. Shum, and D. Liu, "Enhancing the physical layer security of ofdm-pons with hardware fingerprint authentication: A machine learning approach," *Journal of Lightwave Technology*, vol. 38, no. 12, pp. 3238–3245, 2020.

[22] C. Peng, H. Jiang, and L. Qu, "Deep convolutional neural network for passive rfid tag localization via joint rssi and pdoa fingerprint features," *IEEE Access*, vol. 9, pp. 15 441–15 451, 2021.

[23] X. Wang, Y. Zhang, H. Zhang, X. Wei, and G. Wang, "Identification and authentication for wireless transmission security based on rf-dna fingerprint," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, 09 2019.

[24] M. Aritonang, I. D. Hutahaean, H. Sipayung, and I. H. Tambunan, "Implementation of fingerprint recognition using convolutional neural network and rfid authentication protocol on attendance machine," in *Proceedings of the 2020 10th International Conference on Biomedical Engineering and Technology*, 2020, pp. 151–156.

[25] V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. M. Tentzeris, G. R. DeJean, and D. Kirovski, "Rf fingerprinting physical objects for anti-counterfeiting applications," *IEEE Transactions on Microwave Theory and Techniques*, vol. 59, no. 2, pp. 504–514, 2011.

[26] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," *Towards Hardware-Intrinsic Security: Foundations and Practice*, pp. 3–37, 2010.

[27] B. R. Ray, M. U. Chowdhury, and J. H. Abawajy, "Secure object tracking protocol for the internet of things," *IEEE Internet of things Journal*, vol. 3, no. 4, pp. 544–553, 2016.

[28] A. Al-Meer and S. Al-Kuwari, "Physical unclonable functions (puf) for iot devices," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–31, 2023.

[29] Q. Pan, Z. An, X. Yang, X. Zhao, and L. Yang, "Rf-dna: Large-scale physical-layer identifications of rfids via dual natural attributes," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, 2022, pp. 419–431.

[30] L. W. Mayer and A. L. Scholtz, "Sensitivity and impedance measurements on uhf rfid transponder chips," in *Proc. 2nd Int. EURASIP Workshop RFID Technol*. Citeseer, 2008, pp. 1–10.

[31] T. Bauernfeind, K. Preis, G. Koczka, S. Maier, and O. Biro, "Influence of the non-linear uhf-rfid ic impedance on the backscatter abilities of a t-match tag antenna design," *IEEE transactions on magnetics*, vol. 48, no. 2, pp. 755–758, 2012.

[32] P. V. Nikitin, K. S. Rao, R. Martinez, and S. F. Lam, "Sensitivity and impedance measurements of uhf rfid chips," *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 5, pp. 1297–1302, 2009.

[33] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE mobile computing and communications review*, vol. 5, no. 1, pp. 3–55, 2001.

[34] F. M. Nanni and G. Marrocco, "Static and dynamic fingerprint of rfid devices," in *2024 9th International Conference on Smart and Sustainable Technologies (SpliTech)*. IEEE, 2024, pp. 1–3.

[35] M. C. Caccami, S. Manzari, and G. Marrocco, "Phase-oriented sensing by means of loaded uhf rfid tags," *IEEE Transactions on Antennas and Propagation*, vol. 63, no. 10, pp. 4512–4520, 2015.

[36] P. V. Nikitin, K. Rao, and R. D. Martinez, "Differential rcs of rfid tag," *Electronics letters*, vol. 43, no. 8, p. 1, 2007.

[37] D. Dobkin, *The rf in RFID: uhf RFID in practice*. Newnes, 2012.

[38] "Axzon uhf rfid tag ic: Magnus-s3 m3d passive sensor ic," Tech. Rep., available online. [Online]. Available: https://axzon-docs-public.s3.us-east-2.amazonaws.com/docs/DS003F12+Axzon+Magnus+S3+M3D+datasheet.pdf

[39] O. Bucci and G. Franceschetti, "On the spatial bandwidth of scattered fields," *IEEE transactions on antennas and propagation*, vol. 35, no. 12, pp. 1445–1455, 1987.

[40] O. M. Bucci and G. Franceschetti, "On the degrees of freedom of scattered fields," *IEEE transactions on Antennas and Propagation*, vol. 37, no. 7, pp. 918–926, 1989.