Enriching the Electromagnetic Fingerprint of RFID Antennas by non-linear interrogation for Physical Unclonable Functions

Francesca M. C. Nanni[(1)], Gaetano Marrocco[(1)]

[(1)] Tor Vergata University of Rome
Via del Politecnico, 1, 00133, Italy.
francesca.nanni@uniroma2.it

Abstract

This paper investigates the information content of fingerprints of passive RFID devices by applying Shannon Information Theory to backscattered signals. The study demonstrates that interrogations with multiple input powers and frequencies can exploit the non-linear behavior of the integrated circuit (IC), so that its impedance modulation will change in a non-predictable way. Accordingly, the device will expose more information, resulting in a higher entropy value, and a richer fingerprint. This technique can be useful for the realization of Physical Unclonable Functions (PUFs) in anti-counterfeiting applications.
Index Terms *– RFID security, fingerprint, information content, entropy.*

I. Introduction

Radio-Frequency Identification (RFID) technology is widely used in logistics, bioengineering, and the Industrial and Medical Internet of Things. However, concerns have arisen about its physical security, particularly regarding RFID device vulnerability to counterfeiting and replication, which compromises system integrity and raises financial and data privacy risks [1].
RF fingerprinting has emerged as a non-destructive technology for security applications, leveraging analog imperfections in RF devices to achieve uniqueness [2]. Most approaches involve extracting features from device signals and using deep learning to classify counterfeit devices [3], while others use hardware defects to create Physical Unclonable Functions (PUF), generating unique and unpredictable keys during manufacturing [4].
In this paper, we investigate the information richness of the electromagnetic fingerprint of an RFID device using Shannon Information Theory [5] applied to backscattered RF signals. Leveraging the peculiar non-linear response of RFID Integrated Circuit (IC) transponders with respect to input power, our approach evaluates the combination of powers that maximises the information content, namely the entropy.

II. Rationale

The voltage signal $V(f, P_{in})$ returned by an RFID device in a round-trip interrogation, at frequency *f*, with a reader input power P_{in}, can be represented by its in-phase V_I and in-quadrature V_Q components, expressed as:

$$V(f, P_{in}) = |V(f, P_{in})|e^{j\phi(f,P_{in})} = V_I(f, P_{in}) + jV_Q(f, P_{in}) \quad (1)$$

where ϕ denotes the phase of the backscattered signal.
The signal is influenced by environmental factors such as path loss attenuation L_P, round-trip phase delay over a reader-tag distance *d*, cable losses L_C, reader antenna gain G_R, and input power P_{in}.
We define the *backscattering fingerprint F* of the device as the signal derived from (1) after de-embedding the aforementioned contributions:

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

where all parameters are in linear scale. By varying the frequency within a discrete set $\{f_n\}, n = 1, .., N$, the pairs $\{F_n = (F_{I,n}, F_{Q,n})\}$ form a constellation of symbols. By also varying the input power as $\{P_{in,m}\}, m = 1, .., M$, we can exploit the IC's non-linear response, as its RF impedance and sensitivity (p_{IC}) depend on the antenna's delivered power. The backscattered signal will be hence modified and new symbols will be added to the constellation, by overall enriching the fingerprint information content. Since the backscattered properties will also non-linearly depend on P_{in}, we indeed expect that if $P_{in,m} \neq P_{in,m'}$, then $F_{n,m} \neq F_{n,m'}$.
We aim of demonstrating that by expanding the set of input powers, we can increase the information content of F. The focus is, in particular, in the identification of the optimal set of powers maximizing the fingerprint information.

III. Information content

The information content associated with F, considering the interdependence of F_I and F_Q, can be quantified using Shannon's *joint entropy* $H(F_I, F_Q)$ [5].

$$H(F_I, F_Q) = -\sum_i \sum_q p(i, q) \log_2 p(i, q) \quad (3)$$

where $p(i, q)$ is the joint probability of the paired event (i, q), denoting the occurrence of the sample pair $(F_{I,i}, F_{Q,q})$ couplet across the entire antenna fingerprint. After reordering all samples on the $F_I - F_Q$ plane, *i* and *q* act as the new indexes. The typical unit of measurement of (3) is the Bit.

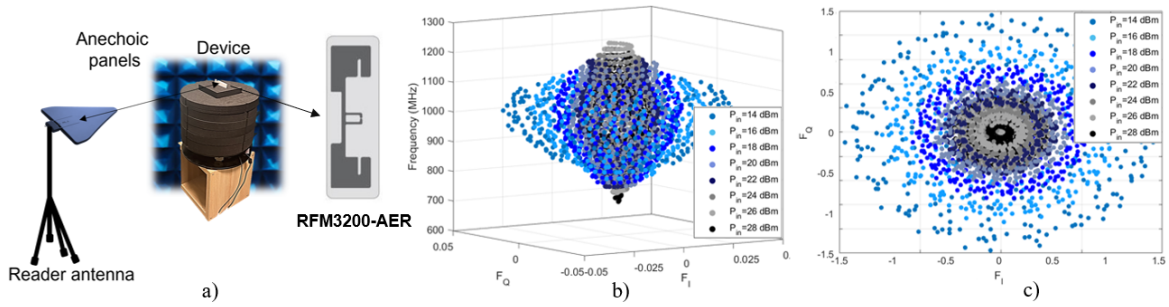

Figure 1: a) Experimental setup and multi-power fingerprint representation of the selected tag in a b) 3D and a c) top view constellation of symbols.

Table I: Best joint entropy for each combination of m powers, for m=1,...,8.

N° of powers	1	2	3	4	5	6	7	8
$\boldsymbol{H(tag)}$ [bit]	5.5	6.2	6.4	6.9	6.8	7	6.9	6.7

IV. Discussion

The above concepts are exploited by measuring the backscattering response of the RFID *RFM3200-AER* dipole tag by Axzon, with an interrogation set-up comprising the Voyantic TagFormance UHF Pro Station (Fig.1 a)), under the following conditions:

1. the reader antenna and the tag operated within each other's far field, with a query distance of 50 cm;

2. a coherent orientation of the reader antenna and the device with linear polarization for both, minimizing the impact of cross-polarization.

The $(F_{I,i}, F_{Q,q})$ couplets were collected for frequency sweeps from 600 to 1100 MHz with 1 MHz steps; and input power from 14 to 28 dBm with 2 dBm steps. Fig.1 b) shows a representation of the tag global fingerprint, which resembles an helical structure in 3D, and Fig.1 c) a flattered view of the $F_I - F_Q$ plane.
The entropies are then combined by considering the response to the 255 possible combinations of up to 8 interrogation powers. Fig. 2 shows the heatmap of all the resulting entropies that show local and absolute maximum value. The best case, as shown in Tab. I, occurs for 6 interrogation powers ($P_{in} = \{14, 16, 18, 20, 26, 28\}$ dBm), returning an entropy of 7 bits, that is nearly 2 bit higher than the one of a single power interrogation ($P_{in} = 22$ dBm).

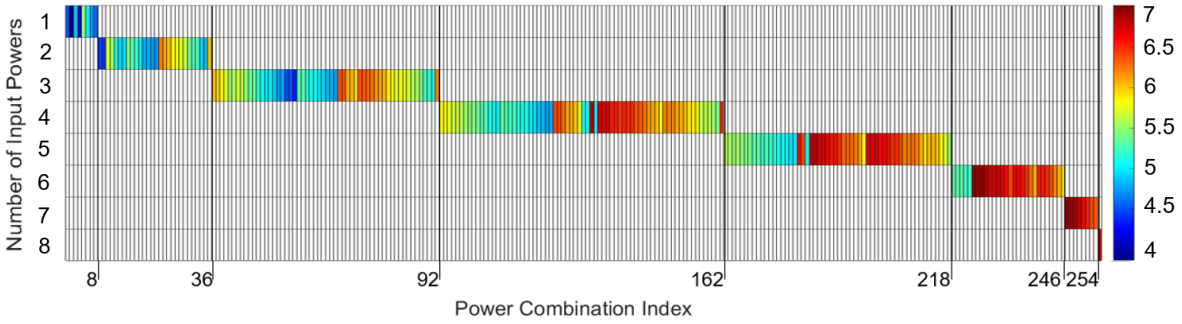

Figure 2: Entropy heatmap for all the 255 combination of input powers.

V. Conclusion

This work introduced a method to extract the information contained in the fingerprint of an RFID device, and thereby to quantify its unpredictability, through Shannon's *joint entropy*. By stimulating the non linear response of the IC, a remarkable improvement in the information content can be achieved as almost 2 bits more with additional powers for interrogation. Since higher entropy values reflect more complex signal attributes, the multi-power interrogation approach enables more robust and suitable fingerprints for authentication and physical encryption applications.

References

[1] R. Singhai and R. Sushil, "An investigation of various security and privacy issues in internet of things," *Materials Today: Proceedings*, vol. 80, pp. 3393–3397, 2023.

[2] 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.

[3] 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.

[4] 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.

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