Millimeter-wave Chipless RFID Tag for Authentication Applications

Raymundo de Amorim, Nicolas Barbot, Romain Siragusa, Etienne Perret

Millimeter-wave Chipless RFID Tag for Authentication Applications

Raymundo de Amorim Jr, Nicolas Barbot, Romain Siragusa and Etienne Perret
Université Grenoble Alpes, Grenoble INP, LCIS, 26000 Valence, France
{raymundo.de-amorim-junior,nicolas.barbot,romain.siragusa,etienne.perret}@lcis.grenoble-inp.fr

***Abstract* — This paper presents a millimeter-wave chipless RFID tag for authentication applications. The concept is based on the idea that it is extremely difficult to identically reproduce materials that inherently have a random aspect due to manufacturing process variations. This paper introduces the paradigm of millimeter-wave authentication based on tags without any chip, including an identifier capable of communicating in the millimeter-wave range. For this purpose, millimeter-wave chipless tags without a ground plane are designed using the RF Encoding Particle (REP) technique. This approach establishes a relation between the geometrical parameters of the isolated scatter and its electromagnetic signature. An elementary particle multiplication strategy is envisaged to increase the backscattered tag level. The evaluated probability of error around 17% is reached with a fabricated tag set from the same manufacturer simultaneously. This probability is two times lower than the one obtained with a similar approach implemented in the X-band.**

***Keywords* — Authentication technology, Chipless RFID tag, Uniqueness.**

I. Introduction

The automatic identification of goods is widely used in industry, logistics, medicine, and other areas, to obtain information about a product in transit and ensure the traceability of the production chain [1]. Barcode identification is the most common technique of identification technology. In order to overcome the limitations of the barcodes, UHF RFID technology combines characteristics such as no need for line of sight toward the reader, the read range is a tenth of a meter, multiple readings are possible and a large amount of data can be stored. Chipless RFID technology is an intermediate technology between the barcodes and the UHF RFID [2]. It combines some features of the barcodes and the UHF RFID. Instead of storing the identifier in an IC, as in the case of UHF RFID, the information is directly linked to the geometry of the printed elements. In this sense, the chipless tags can be seen as a radar target designed to scatter a specific electromagnetic signature. The backscattering mechanism of the chipless tag can be divided into two quantities: the structural mode and the antenna mode. The structural mode concerns reflections due to the power part directly backscattered by the structure of the tag. The second part of the signal is the antenna mode, which contains the information about the electromagnetic (EM) chipless tag encoded information. Many applications beyond identification purposes have been reported, for instance, in [3] where an angle sensor insensitive to distance variations has been presented. In [4], a chipless tag is used as a sub-millimeter displacement sensor. Indeed, few works aim to demonstrate the potential of chipless RFID for authentication applications [5]–[7]. Concentric annular ring resonators are used in [5]. The manufacturing variations and the dielectric constant variation of the substrate provide the unique EM response. However, the authors do not give information about the probability of error in their approach. In [6], the potential for chipless RFID tags for authentication is depicted. In [7], the randomness of the fabrication process was exploited to provide a unique RF fingerprint of the chipless tag. Then some metrics were performed in the time domain and frequency domain to assess the probability of error. In this context, a probability of error of about 32% was assessed when all the tags were fabricated simultaneously by the same PCB manufacturer. It is important to note that multiple fabrications at different times produce higher randomness. The main objective of this work is to evaluate chipless authentication in V-band $(57\ \text{GHz} - 64\ \text{GHz})$ based on the tag EM response variation produced by manufacturing uncertainties. In Section II, the principle of chipless RFID authentication is detailed. Then, in Section III, a chipless tag in V-band is designed to be highly sensitive to process variations with an RCS high enough to be measured. Finally, in section IV, our approach's information richness and error probability are presented and evaluated by statistical methods.

II. Principle of chipless RFID authentification

Fig. 1 shows the basic principle of the chipless authentication process. The process can be divided into two steps:

i) Measurements of chipless RFID tags using a chipless reader for the database enrollment.
ii) The comparison of a given unknown test tag (the tag to authenticate) against the database.

In the comparison phase, no signal adjustment is made for comparison purposes. Only time-gating is performed on measurement. Then, the cosine similarity function is used as a similarity metric to compare the tag to authenticate and the database. As electromagnetic characteristics are employed, these characteristics cannot be easily spoofed. The goal is to design and implement chipless RFID tags to ensure object authenticity with a unique and unfalsifiable fingerprint. Considering passive labels at mmWave frequencies, the main drawback is low-level signals. However, techniques will be presented to overcome this constraint. Furthermore, the label

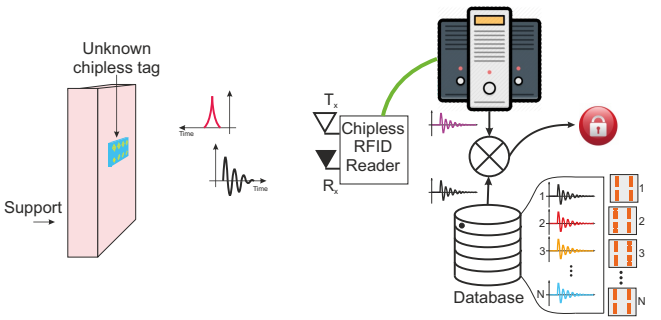

Fig. 1. Authentication procedure for a chipless RFID system.

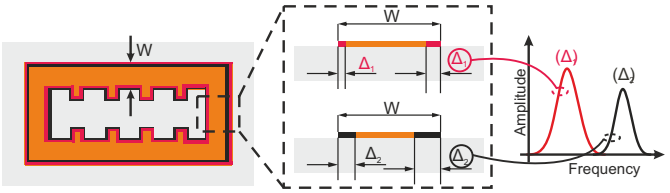

Fig. 2. The geometrical variations (Δ_1, Δ_2) imposed by the manufacturing process induce different tag EM responses.

has to provide the same signature in two authentication steps, and a counterfeit label must have a different signature from the database.

III. V-BAND CHIPLESS TAG DESIGN

The tags have been designed to obtain frequency signatures highly sensitive to physical parameter variations that naturally come from the manufacturing process. So they are challenging to duplicate because these variations are random and are difficult to mimic. These variations will be linked to in-homogeneous process variations, such as over-etching with chemical etching or printing of ink in printed electronics.

Looking at the same method and fabrications conditions, the same design is used to produce N (supposed) identical tags. However, due to the process variations during the fabrication, independent random errors affect each structure, as we can see in Fig. 2, affecting the EM response. One of the main features to be extracted in the application of V-band chipless RFID authentication is the possibility to distinguish the EM response between different realizations easily. In V-band, the size of the resonators is small compared to scatters operating in X-band. Consequently, the structures are expected to be more sensitive to the physical error process, resulting in better differentiation between the tag EM responses. In Fig. 2, each color denotes the random variations generated by the manufacturing process. Different patterns will be randomly generated within the uncertainty range as each process has uncertainty.

Fig. 3 shows the loop resonator that has been designed. The tag's electromagnetic responses were obtained by electromagnetic simulation using CST Microwave Studio. The substrate is the Rogers RT5880 with $\tan\delta = 0.005$, permittivity $\epsilon_r = 2.33$, and a thickness of 0.127 mm. In V-band, we can observe the decrease of the $Q-$factor and

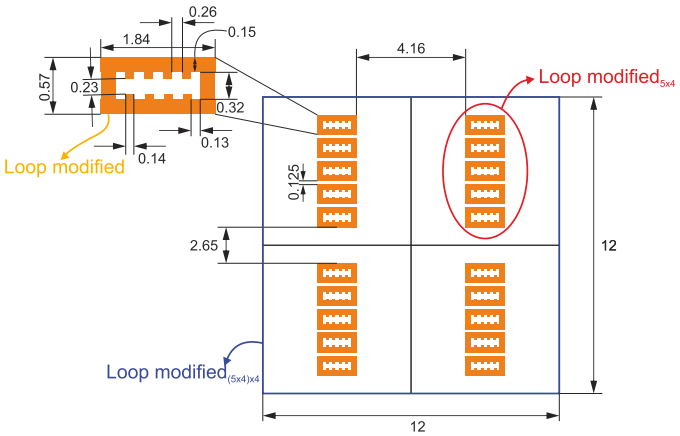

Fig. 3. V-band chipless tag for authentication applications. Multiple resonators are used to increase the RCS level of the tag. The dimensions are in millimeters.

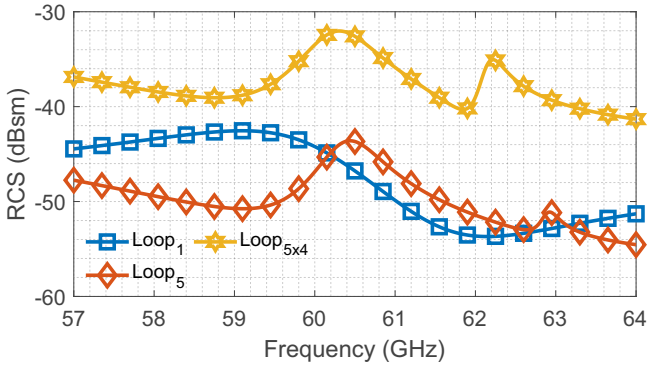

Fig. 4. Simulated RCS versus frequency of a different group of loop resonators. Loop_1 is the resonator, Loop_5 is the group of 5 loop resonators and Loop_{54} is a tag with 4 groups of 5 loops.

the mean RCS level compared to the X-band. However, the low RCS level can be challenging to measure in a real environment. Thus, an elementary particle multiplication strategy is envisaged to overcome the low-level backscattered signal. The basic principle of this method is repeating several times the same resonator on the same tag surface to increase the RCS level at a given frequency, as depicted in Fig. 4. Note that this repetition may add coupling features to the structure, then produce new randomness.

Due to coupling, the elements multiplication does not carry a proportional augmentation of the Rmethodl; hence an optimization phase was performed. Firstly, five-element (Loop_5) structures are implemented, but the RCS level remains low, as can be seen in Fig. 4. Secondly, the five-element structure is repeated, and each resonator is placed far away from the others, thus creating a tag Loop_{5x4} with a higher RCS level. The final dimensions of the structure can be seen in Fig. 3.

IV. MEASUREMENT RESULTS AND EVALUATION OF THE ERROR PROBABILITY OF THE AUTHENTICATION APPROACH

A set of 19 tags was built on the same substrate. It is important to note that all tags come from the same digital

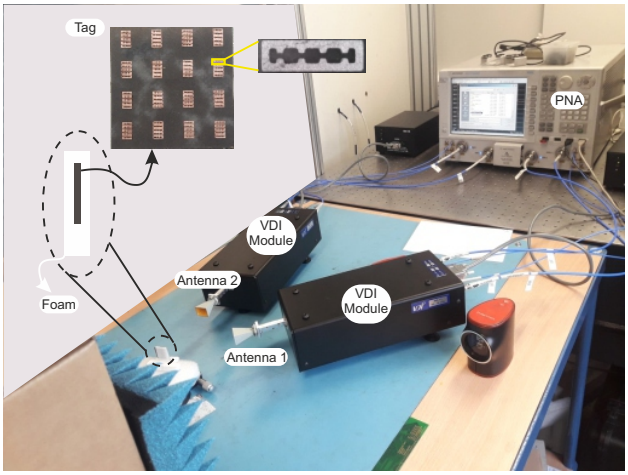

Fig. 5. Setup for V-band measurements in an office environment, the bistatic configuration is utilized, and both antennas have co-polarization orientation.

file and the same substrate, *i.e.* these tags share the same mask and fabrication process. The V-band measurements were performed with an Agilent N5222A $(0.01\ \text{GHz} - 26.5\ \text{GHz})$ PNA with Virginia Extensions (VDI modules) to operate from $57\ \text{GHz}$ to $64\ \text{GHz}$. The VDI module is a frequency multiplier combined with a mixer with a WR_{15} waveguide output. The measurement setup can be seen in Fig. 5. The tag is positioned inside a thin piece of foam. For each measurement, the tag is removed and placed in the same position to guarantee repeatability. The tags were placed $17\ \text{cm}$ far from the antennas; a bi-static configuration is used with time-gating.

The repeatability measurements are the first test. The S_{21} parameters are shown in Fig. 6 for the $\text{Loop}_{((5\times4)\times4)}$ tag, which is measured ten times. As depicted in Fig. 7, different tags have a unique electromagnetic response, highlighted by the frequency shift.

The intra-tag Probability Mass Function (PMF) is obtained by the comparison among the repetitive measurements of the same chipless tag, as depicted in Fig. 8(a), with M coefficients $(\text{M} = 19 \cdot \text{C}_2^{10} = 855)$. Eventually, the PMF inter-tag function is achieved by comparing measurements between the tags, K coefficients are obtained $\text{K} = 10 \cdot 10 \cdot \text{C}_2^{19} = 17100$, the

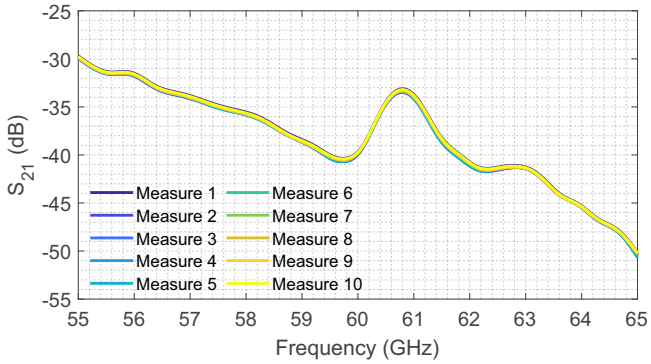

Fig. 6. The repeatability measurements of the tag n°4 $\text{Loop}_{(5\times4)\times4}$, each color corresponds to S_{21} parameter of the tag measured ten times.

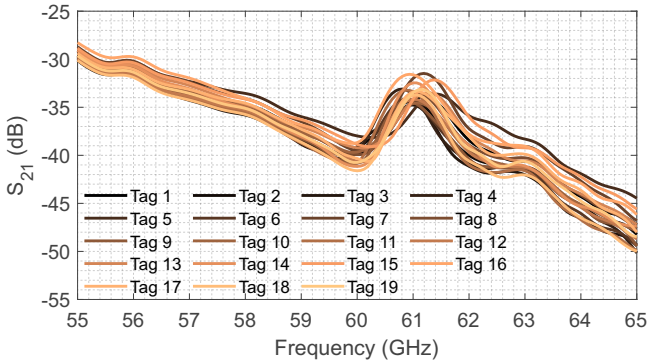

Fig. 7. EM responses of the 19 tags made with the same mask.

calculation of inter-tag coefficients values are depicted in Fig. 8(b).

The intra-tag and inter-tag probabilities are shown in Fig. 9 and Fig. 10, respectively. Both probability results are evaluated using the cosine similarity. Considering the intra-tag coefficients yield results close to 1, *i.e.*, a high similarity between the measurements is observed. The minimum value is approximately 0.97, which indicates a good agreement when evaluating the same measured tag. Analyzing the inter-tag coefficients, we can discern that the coefficients are dispersed, and most values are beneath 0.97, which indicates one differentiation between different tags.

By taking the intra-tag and inter-tag distribution coefficients, the Probability Density Functions (PDF) of each distribution are calculated. Then the Probability of False Positive (PFP) and the Probability of False Negative (PFN) are determined and depicted in Fig. 11. Finally, the probability of error is chosen to minimize the number of false positives and false negatives, which does happen precisely at the intersection point between the PDFs.

As seen in Fig. 11, the probability of error obtained is around 17%, which is relatively high compared to traditional authentication methods. However, when similar approaches

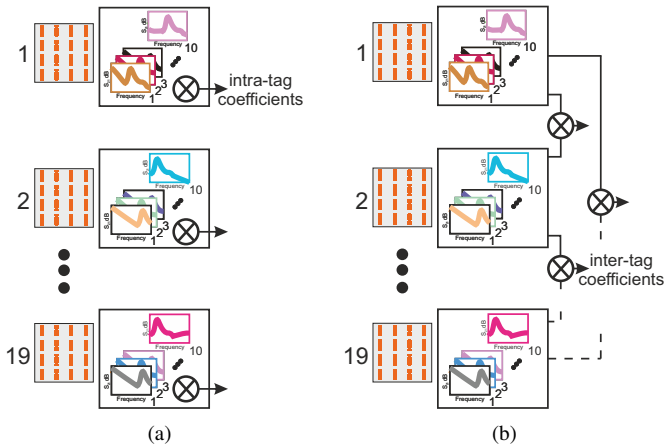

Fig. 8. (a) Intra-tag representation where $(\text{M} = 19 \cdot \text{C}_2^{10} = 855)$; (b) inter-tag coefficients $(\text{K} = 10 \cdot 10 \cdot \text{C}_2^{19} = 17100)$.

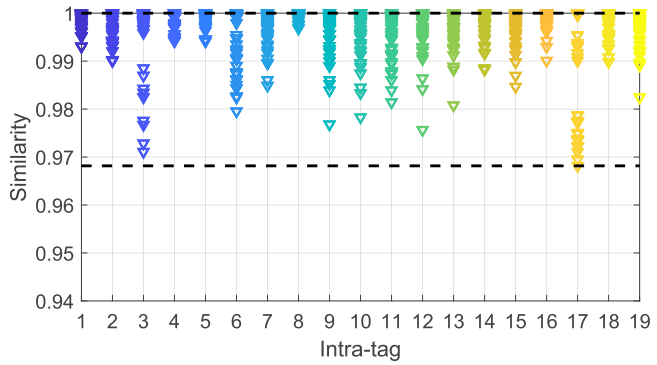

Fig. 9. Whole probabilities set considering the intra-tag case. Each point corresponds to the similarity coefficient performed by the cosine similarity metric.

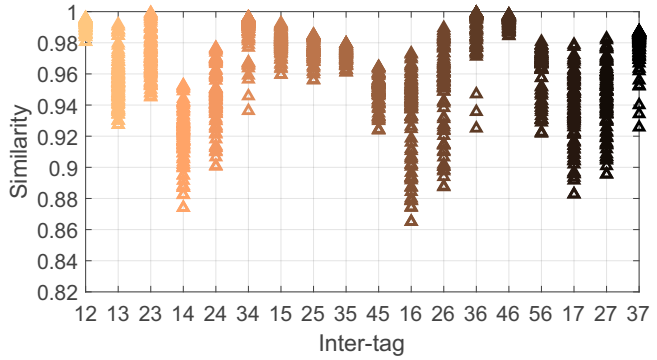

Fig. 10. Probability of error obtained when considering the inter-tag case, only some inter-tag cases are shown in the inset. Each point corresponds to the similarity coefficient extracted by cosine similarity.

using EM responses are reached, such as in [8], there is a significant reduction in the probability of error, thus resulting in an improvement given by the proposed method.

This proposed tag is efficient against cloning attacks since the adversaries cannot model the randomness variations at the same authentication time or on another manufacturing process. Furthermore, the apparatus to reproduce the EM response from the tag far exceeds the amount to manufacture the proposed tag. Moreover, the worst case was evaluated as only one realization was considered, and the tags were built simultaneously. As previously mentioned, it is expected that the comparison between inter-realizations (tags fabricated at different times) can significantly decrease the PE.

V. Conclusions

The principle of millimeter wave chipless tags for authentication applications was evaluated. This prospective study shows that the richness of information in their EM signature is potentially usable for authentication applications. To increase the RCS level, a group of five resonators was used to construct a cell. Then, the cell was repeated. A set of chipless RFID tags were developed in the V-band. These tags backscatter a unique EM response exploiting their inherent fabrication randomness. The backscattered RCS level is satisfactory for real-environment reading measurements.

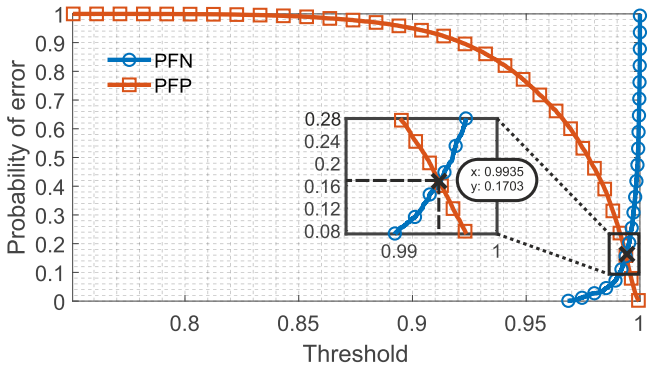

Fig. 11. Probabilities of false negative (PFN) and false positive (PFP) for intra-tag and inter-tag CMFs.

The set tags were developed, sharing the same substrate and manufacturing conditions, and one probability of error of around 17% was estimated. Whether different tag signatures are used for the authentication process, *i.e.*, independent measurements are done, the probability of error can be written as $\mathrm{PE} = 0.17^N$, where N represents the number of measured tags. The future work intends to implement a low-cost solution from the paper industry using bio-based and recyclable techniques.

Acknowledgment

The authors would like to acknowledge the UGA for financially supporting the AUSTRALE project via the ANR program funding under grant agreement ANR-18-CE39-0002 grant.

References

[1] *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3rd Edition | Wiley*, library Catalog: www.wiley.com.

[2] E. Perret, *Radio Frequency Identification and Sensors: From RFID to Chipless RFID*. John Wiley & Sons, Dec. 2014.

[3] N. Barbot, O. Rance, and E. Perret, "Angle Sensor Based on Chipless RFID Tag," *IEEE Antennas and Wireless Propagation Letters*, vol. 19, no. 2, pp. 233–237, 2020.

[4] E. Perret, "Displacement Sensor Based on Radar Cross-Polarization Measurements," *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 3, pp. 955–966, 2017.

[5] K. Yang, D. Forte, and M. M. Tehranipoor, "UCR: An unclonable chipless RFID tag," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2016, pp. 7–12.

[6] Z. Ali, F. Bonnefoy, R. Siragusa, N. Barbot, D. Hely, E. Perret, M. Bernier, and F. Garet, "Potential of chipless authentication based on randomness inherent in fabrication process for RF and THz," in *11th European Conference on Antennas and Propagation (EUCAP)*, 2017, pp. 2559–2563.

[7] Z. Ali, N. Barbot, R. Siragusa, D. Hely, M. Bernier, F. Garet, and E. Perret, "Chipless RFID Tag Discrimination and the Performance of Resemblance Metrics to be used for it," in *2018 IEEE/MTT-S International Microwave Symposium - IMS*, 2018, pp. 363–366.

[8] Z. Ali, F. Bonnefoy, R. Siragusa, N. Barbot, D. Hély, E. Perret, M. Bernier, and F. Garet, "Potential of chipless authentication based on randomness inherent in fabrication process for RF and THz," Ph.D. dissertation, Paris, France, Mar. 2017. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01800579