3D authentication approach to enhance the security level for millimeter-wave chipless tags

Raymundo Amorim, Nicolas Barbot, Romain Siragusa, Etienne Perret

3D Authentication Approach to Enhance the Security Level for Millimeter-wave Chipless Tags

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

***Abstract*—A bistatic measurement technique is implemented with an authentication approach based on tag-backscattered electric field (E-field) measurements at different orientation angles for unitary classification in the millimeter-wave (mmWave) band. The idea is based on the augmentation of information related to the aspect-independent tag-backscattered signals according to different angle measurements. Geometric uncertainties are inherent to the manufacturing process are transcribed in minor variations observed in the tag electromagnetic response and exploited from the measurement at three different angles to authenticate the tag. This information about the angle increases the authentication level. A set of sixteen E-shape chipless tags fabricated to operate at millimeter-wave frequency are fabricated, measured and analyzed. To better exploit a large amount of data collected with this approach, a Machine Learning (ML) classification is evaluated. The probability of error (PE) achieved with the method is around 0.05%. This PE is the lowest reported for chipless RFID tag authentication applications.**

***Index Terms*—Authentication, Bistatic configuration, chipless RFID tag, millimeter-wave.**

I. Introduction

Practical authentication systems attempt to optimize the trade-off between reliability and ease of implementation or even the system's complexity. In this context, new authentication propositions emerge, and chipless RFID can benefit from significant advantages in this domain due to its lower cost than other technologies. Chipless RFID tags can be seen as radar targets designed to scatter a specific electromagnetic signature [1]. Besides, the tags can be embedded directly in manufactured products. Indeed, chipless tags are composed of metallic patterns printed on a substrate, where the tag information is directly linked to the resonant frequencies of these scatterers.

Chipless RFID technology authentication provides a non-invasive method based on electromagnetic signature distinction, which does not need a line of sight and has the potential to be fully printable in bio-sourced materials by low-cost methods. The interest here is to claim a level of authentication that can be important insofar as it is linked to natural random phenomena that cannot be reproduced at accessible costs. Indeed, chipless artifacts that pretend to generate a unique backscattered response have appeared in the literature in the last 20 years [2]. In this early work, the images of two paper-based materials are compared, and the unique paper surface irregularities act as a non-replicable identifier. The application domain remains confidential, and the information is often at the concept stage. The approaches try to implement a solution that attempts to transcribe part of the randomness inherent in the material onto the RF signal using a passive chipless tag [2].

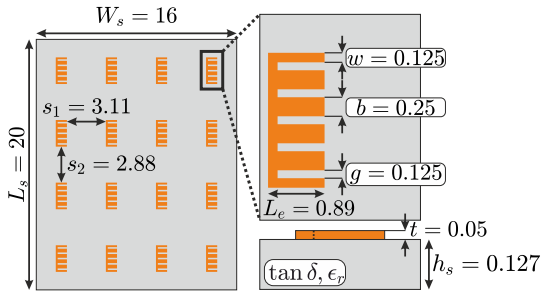
A first generation of chipless tags for authentification applications was implemented to design a tag that pretends to be hardly clonable, which means the tag exhibits a unique RF response in the UWB band. The potential of authentication using chipless RFID tags was demonstrated in [3], [4], [5]. These tags are intentionally modified to favor the inherent fabrication error introduced by the manufacturing process. Additionally, these tags are fabricated at different time lapses. Different time-lapses increase the randomness of fabricated tags, making the tags easier to distinguish. Despite these favorable conditions, the PE achieved is around $2.3\% - 4\%$.

A second generation of chipless tags focusing on the unitary authentication of manufactured products in millimeter wave band considering only one round fabrication was recently proposed [6], [7]. These chipless solutions offer an alternative by employing a lightweight commercial substrate manufactured simultaneously and without bulky designs. In [6], the authentication level achieved when two different angles are measured and considering only one round of fabrication is $\mathrm{PE} = 1\%$.

This work demonstrates that the PE associated with the mmWave chipless systems can be enhanced by adding different aspect-independent tag information using different measurement angles. However, the complexity associated with multiple-angle measurements increases the acquisition complexity. The goal is to retrieve a distinctiveness signature containing measurement angles based on a bistatic configuration that improves the tag information. Three different measurement angles are determined from the measured signals at different angles. Tag repeatability measurements are performed at each angle. An ML evaluates the tag's EM richness information, then the analysis of PE is evaluated. A significant enhancement is noted by adding a third measurement angle.

II. mmWave chipless tag fabrication

A set of 16 tags based on E-shaped resonators were fabricated to evaluate the method. The structures share the same Rogers $\mathrm{RT5880}$ substrate with $\tan\delta = 0.0027$, permittivity $\epsilon_r = 2.33$, and thickness of $0.127\ \mathrm{mm}$. The group of resonators that compose one tag are printed in only one layer, as depicted in Fig. 1. The number of resonators is chosen to achieve $-40\ \mathrm{dBsm}$, which enables a reading range around $50\ \mathrm{cm}$ considering a sensitivity level of $40\ \mathrm{dB}$ [7].



(a)

Fig. 1. Dimensions for the $E_{4\times4}$ tag, this tag do not have a ground plane. All dimensions are in millimeters.

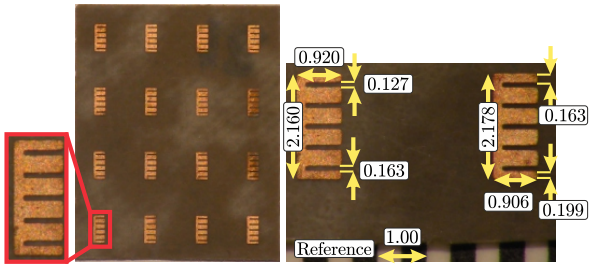
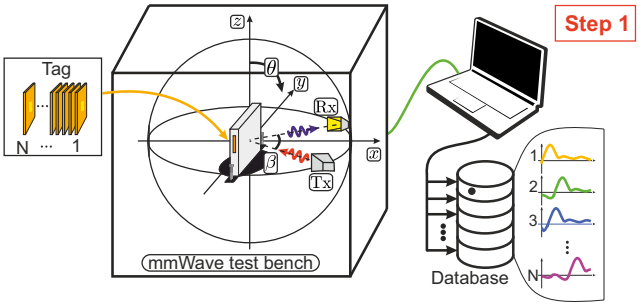


Fig. 2. Fabricated $E_{4\times4}$ tag without a ground plane. All dimensions are in millimeters.

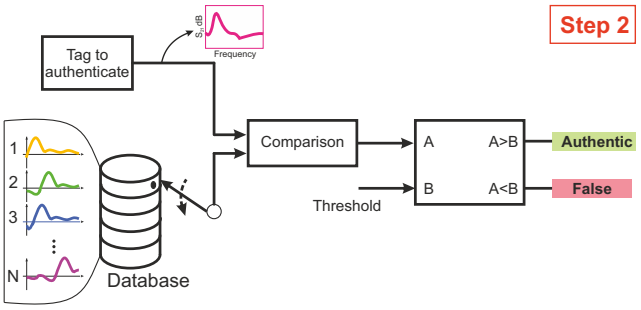
Photolithography technology is chosen to realize the tags on low-loss flexible substrates. A one-bit frequency information tag has been fabricated. Even with the same design, different lengths of the same pattern (In Fig. 1, the tag is composed of 16 identical patterns as shown in Fig. 2, which highlights the randomness evidenced during manufacturing. Indeed, the manufacturing errors depicted by the magnification in Fig. 2 occur due to under-etching and over-etching. The choice of the manufacturing method is important. In addition to being low cost, it must ensure good precision so that all the tags manufactured present a resonance around an expected frequency while allowing manufacturing errors to slightly shift this frequency (more generally, the backscattered field on a frequency band), which impacts in a unique way each tag.

III. Principle of Chipless RFID Authentication Based on Augmentation of Tag Information

A method is proposed to authenticate RFID chipless tags designed in mmWave by exploiting the process variations during tag fabrication from the measurement at different angles. In this way, differently from other approaches, this method adds aspect-independent parameters based on the tag radiation pattern. To provide a trustworthy authentication process, two steps are needed. The first is carried out after the manufacturing process, and the second is when a user needs to authenticate the tag. In the first step, the chipless RFID tags' responses are measured in bistatic configuration; each tag is measured and stored in the database as shown in Fig. 3(a). In the second step, shown in Fig. 3(b), the chipless RFID tag to authenticate is first measured in the same configuration as in step one. Then its EM signature is compared with the previously measured responses of the database. Finally,



(a)



(b)

Fig. 3. Chipless RFID system for authentication. (a) Chipless RFID measurement system on bistatic mode, each chipless tag is characterized, and the corresponding collected RF signatures compose the database, (b) authentication procedure for a chipless RF system.

the maximum similarity value resulting from comparing the database and the tag to authenticate is computed and then compared with a threshold. As illustrated in Fig. 3(b), if the comparison value (A) is greater than or equal to the threshold (B), then the RFID response is authentic or false otherwise.

The measurements are performed at three different angular positions based on optimizing the reception angles on the mmWave band, which privileges the tag resonant mode. The obtained RCS of the $E_{4\times4}$ tag is shown in Fig. 4(a). Based on the backscattering pattern of the $E_{4\times4}$ and the substrate (tag without metallic pattern), the angles that favor the useful information of the tag are implemented as shown in the Fig. 4(b). Since the conventional $\phi_1 = 0°$ was measured, the angles $\phi_2 = 40°$ and $\phi_3 = 90°$ that maximizes the tag-to-substrate signal as shown in Fig. 4(b) are chosen.

IV. Performance Evaluation

The 16 tags are fabricated on the same substrate. As aforementioned, it is important to note that all tags come from the same digital file and substrate and share the same mask and fabrication process. The measurements were performed with an Agilent N5222A (0.01 GHz – 26.5 GHz) PNA with Virginia Extensions (VDI modules) as shown in the Fig. 5 operating from 66 GHz to 71 GHz.

A. Measurements

The repeatability of the measurement (including positioning error) is the first test. The magnitude of the $|S_{21}|$ parameters are shown in Fig. 6 where the same $E_{4\times4}$ tag is measured five

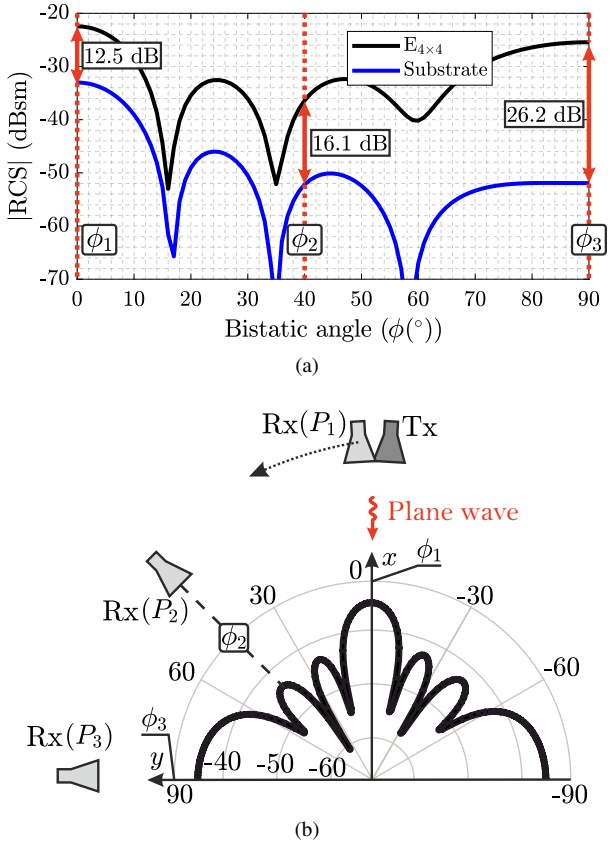


Fig. 4. (a) Simulated RCS radiation pattern for the $E_{4\times4}$ tag. (b) Simulated RCS polar diagram in dB of the $E_{4\times4}$ tag at 67.4 GHz. The measured angles $\phi_1 = 0°$, $\phi_2 = 40°$ and $\phi_3 = 90°$ are highlighted. The incident wave is normal to the tag ($\phi = 0°$); the reception probe varies from 90° to $-90°$.

times. The tag is removed from the foam for each measurement and placed in the same position. The EM responses for $\phi_1 = 0°$, $\phi_2 = 40°$ and $\phi_3 = 90°$ are shown in Fig. 6. The general shape of the signal differs between the three angles. As expected, this means that the contribution of the structure is not the same. However, the same resonance can be observed in all cases, which denotes that the backscattered fundamental mode is present in all the responses due to the resonant structure.

The 16 different tags EM response for $\phi_1 = 0°$, $\phi_2 = 40°$ and $\phi_3 = 90°$ are depicted in Fig. 7. Contrary to Fig. 6, where all the curves were very close, Fig. 7 shows curves that differ. For example, the maximum of each peak apex is no longer at the same frequency. These measurements are the first step of the authentication procedure.

B. PE evaluation

After the measurements, the first step is to assess the similarities among the signals. For that, a metric must be used, in our case, cosine similarity, which considers the differences and similarities between the measured signals. Two classes are evaluated from the tag measurements: the intra- and inter-tag classes. The intra-tag class corresponds to repeatability measurements, and the inter-tag relates to the measurement among the different tags. After the comparison, in Fig. 8,

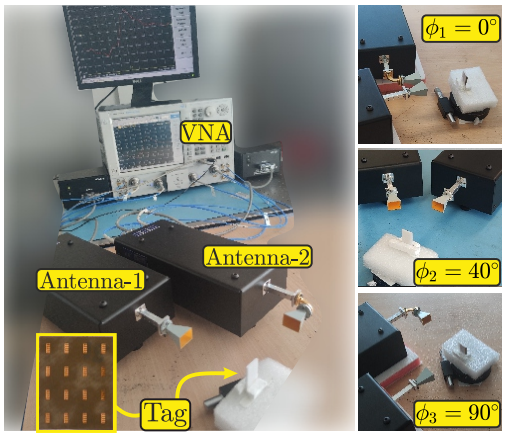


Fig. 5. Setup for V-band measurements in an office environment. Bistatic configuration is used, and both antennas are co-polarized.

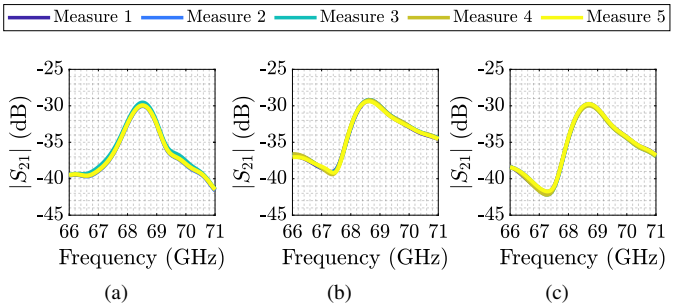


Fig. 6. Repeatability measurements of one tag from the set of designed tags for (a) $\phi = 0°$, (b) $\phi = 40°$ and (c) $\phi = 90°$. Each color corresponds to the $|S_{21}|$ tag parameter measured five times.

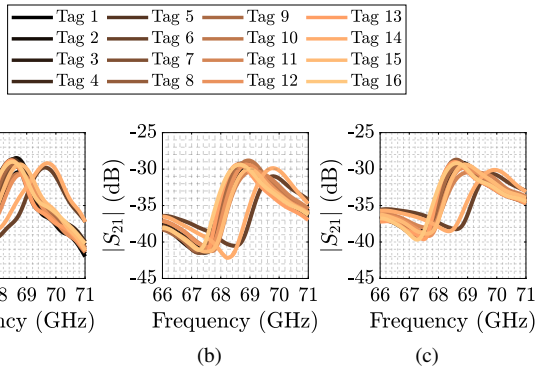


Fig. 7. EM responses of the designed tags, 16 tags were made simultaneously with the same mask. The (a) $\phi_1 = 0°$, (b) $\phi_2 = 40°$ and (c) $\phi_3 = 90°$ were measured considering the set of tags. Only one measure is shown for each tag.

the similarity values of intra-tag and inter-tag measures are mapped on a 3-D plan of coordinate $S_{intra}(\phi_1, \phi_2, \phi_3)$ or $S_{inter}(\phi_1, \phi_2, \phi_3)$, where S is the similarity function for the intra-tag class or inter-tag comparison, considering each angle. A threshold using a linear classification approach has been defined to authenticate the tags. The intra-tag coefficients yield a distribution near 1, which means a good agreement if considering measurements done at the same tag, *i.e.*, a high similarity between the measurements is obtained.

On the other hand, inter-tag coefficients are dispersed,

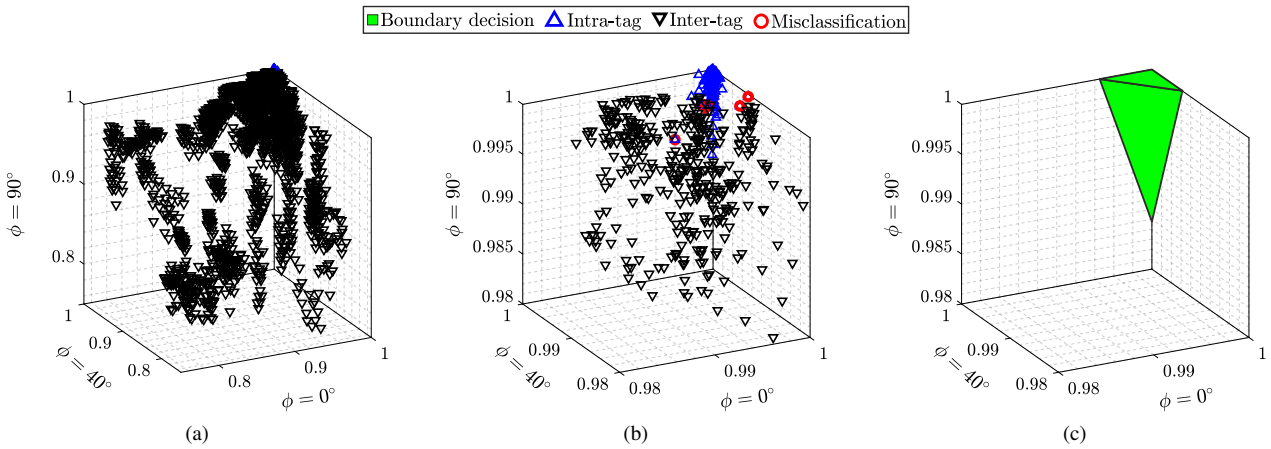


Fig. 8. (a) 3D $S_{intra}(\phi_1, \phi_2, \phi_3)$ and $S_{inter}(\phi_1, \phi_2, \phi_3)$ classes, (b) zoom in the area of interest and (c) hyperplane threshold.

TABLE I
COMPARISON BETWEEN DIFFERENT CHIPLESS RFID TAG AUTHENTICATION TECHNIQUES.

Reference	Same realization	Number of angles	Frequency GHz	PE (%)
[4]	No	1	$3-10$	3
[5]	Yes	1	$3-10$	32
[6]	Yes	1	$66-71$	5
[7]	Yes	2	$66-71$	1
This work	Yes	3	$66-71$	0.05

which indicates a good differentiation between different tag measurements. The boundary decision is established from the support vector ML classification as shown in Fig. 8(c). The misclassification cases are highlighted with the red circle in Fig. 8. It occurs when classes are assigned to a different category than the one it belongs to. The ML classification on the set of 16 tags results in a hyperplane from the linear ML approach leading to a PE of 0.05%. Note that the additional angle (ϕ_3) does not carry the same reduction experienced when only two angles are considered [7]. Therefore, this reflects the dependence among the angles when a third angle is added to the ML approach. Additionally, it increases the complexity from the point of view of measurements, and the increase in the number of angles will severely affect the complexity of the learning process.

In this context, the algorithm demonstrates good performance for authentication purposes, considering that all the tags have been fabricated simultaneously. It is important to note that the PE can significantly be decreased if tags coming from different fabrications are considered (tags manufactured at a different time). The reported methods have a PE higher than the one reported in this work, as shown in Table I.

V. CONCLUSION

A method using millimeter-wave tags for authentication applications aspiring to increase the tag aspect-independent electromagnetic parameters were evaluated. Different angles were measured to obtain a unique signature. Exploiting the backscattered field using three angles is a promising method for authentication applications. Statistical analysis was discussed, and the intra-tag and inter-tag distribution coefficients from each angle were mapped on a 3D plan for hyperplane estimation in binary classification schema. Hence, a PE around 0.05% was estimated. Chipless RFID tags can provide a unique and unfalsifiable electromagnetic signature enhancing and assuring their identification. Therefore, the contrast between low-cost applications maintaining flexible and trustworthy solutions paves the way for new high-secured authentication solutions.

ACKNOWLEDGMENT

The authors would like to acknowledge the University Grenoble Alpes for financially supporting this project AUSTRALE via the ANR program. This project has also received funding from the European Research Council (ERC) under the European Union's Horizon 2020 Research and Innovation Program (ScattererID - grant agreement N° 772539).

REFERENCES

[1] E. Perret, *Radio Frequency Identification and Sensors: From RFID to Chipless RFID*. John Wiley & Sons, Dec. 2014.
[2] J. Smith, "Imperceptible sensory channels," *Computer*, vol. 37, no. 6, pp. 84–85, Jun. 2004.
[3] 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 *2017 11th European Conference on Antennas and Propagation (EUCAP)*, Mar. 2017, pp. 2559–2563.
[4] Z. Ali, E. Perret, N. Barbot, R. Siragusa, D. Hély, M. Bernier, and F. Garet, "Authentication Using Metallic Inkjet-Printed Chipless RFID Tags," *IEEE Transactions on Antennas and Propagation*, vol. 68, no. 5, pp. 4137–4142, May 2020.
[5] 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, Université Grenoble Alpes, Paris, France, Mar. 2017. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01800579
[6] R. de Amorim, N. Barbot, R. Siragusa, and E. Perret, "Millimeter-wave Chipless RFID Tag for Authentication Applications," in *2020 50th European Microwave Conference (EuMC)*, Jan. 2021, pp. 800–803.
[7] R. de Amorim, R. Siragusa, N. Barbot, G. Fontgalland, and E. Perret, "Millimeter Wave Chipless RFID Authentication Based on Spatial Diversity and 2-D Classification Approach," *IEEE Transactions on Antennas and Propagation*, vol. 69, no. 9, pp. 5913–5923, Sep. 2021.