Magnetic Unclonable Functions Leveraging Remanence and Anhysteretic States

ADVANCED FUNCTIONAL MATERIALS
www.afm-journal.de

Magnetic Unclonable Functions Leveraging Remanence and Anhysteretic States

Alessandro Magni, Gabriele Barrera,* Federica Celegato, Francesco Riboli, Diederik S. Wiersma, Sara Nocentini,* and Paola Tiberto*

Physical Unclonable Functions (PUFs), derived from the unique properties of physical hardware, enable the generation of cryptographic keys with enhanced security against cloning and cyber-attacks because of their inherent randomness and on-the-fly key extraction. The scientific interest on these systems motivated the exploration of several hardware from optical, memristive to electric. Compared to optical and electric systems, magnetic PUFs offer strong robustness against environmental perturbations and easy integration into micro-devices because of their compatibility with CMOS-technology. A new magnetic platform is introduced that allows password generation with over 400 independent bits with a dual-mode operation. A deterministic mode provides a stable, repeatable response to a given interrogation, while a reconfigurable mode ensures a different response each time. This system utilizes nominally identical FeGa dot array that, given their microscopic magnetic properties, are hard to clone with current technology. This enables the extraction of highly entropic cryptographic keys via the Magneto-Optical Kerr Effect microscopy. Moreover, magnetic field-controlled key generation enables the dynamic switching between deterministic and reconfigurable key generation within the same hardware without need for multiple interrogation stimuli. This dual functionality enhances security and flexibility, opening new avenues for secure and adaptable cryptographic implementations in anti-counterfeiting and secure password generation.

1. Introduction

Nanostructured magnetic materials, even when fabricated with the utmost precision by advanced techniques, exhibit inherent randomness in their magnetic properties such as unpredictable local variations in magnetic anisotropy, magnetic domain patterns, and magnetization directions.[1–6] This randomness is exacerbated by confluent factors such as crystallographic imperfections, subtle topographical variations in surface roughness and edge shapes, impurities and defects, and stochastic thermal fluctuations.[2,3,5–7] While such randomness can pose challenges for deterministic magnetic devices,[8–10] producing noise and information loss in magnetic memory, it provides a unique foundation for developing secure hardware systems for cryptographic applications.[11–16]

Physical Unclonable Functions (PUFs) take advantage of these inherent physical variations to generate unique and unpredictable but deterministic cryptographic keys, offering a robust defense against counterfeiting, cloning, and various cyberattacks.[17–26] To practically advance their use in real-world authentication, key features such as robustness, a large number of independent key bits, and sufficient entropy are crucial. Additionally, advanced functionality beyond static hardware, such as switchability and reconfigurability can enhance the security of the physical unclonable function against attacks. A switchable PUF for which the physical properties can be varied reversibly provides a multi-level operation with a net increase on entropy and thus security,[18] while a reconfigurable PUF enables an irreversible generation of a new hardware with different properties that enhances the security and reusability in the presence of cyber attacks.[27] While PUFs can be classified by their readout mechanism—whether single[28] or multiple[29]—they typically operate in just one mode, either static or reconfigurable.[30–32] The new type of magnetic material that we present in this work allows for the realization of unclonable functions with very high entropic keys, in which static and reconfigurable hardware coexist within a single device, thereby significantly enhancing security and adaptability.

A. Magni, G. Barrera, F. Celegato, D. S. Wiersma, S. Nocentini, P. Tiberto
Istituto Nazionale di Ricerca Metrologica
Strada delle Cacce, 91, Torino 10135, Italy
E-mail: a.magni@inrim.it; g.barrera@inrim.it; s.nocentini@inrim.it
F. Riboli
Istituto Nazionale di ottica -consiglio nazionale delle ricerche
Via N. Carrara 1, Sesto Fiorentino, Firenze 50019, Italy
D. S. Wiersma
European Laboratory for Non-linear Spectroscopy LENS
Università degli studi di Firenze
Dipartimento di Fisica
Via G. Sansone 1 Sesto Fiorentino, Firenze 50019, Italy

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/adfm.202516376

DOI: 10.1002/adfm.202516376

Magnetic materials offer several advantages, making them robust and reliable in real-world scenarios and electronic authentication devices. Their unique nonlinear magnetic response and the ability to control magnetization states through magnetic field history[33] provide a rich platform for developing advanced highly secure architectures. In contrast to electrical hardware,[17,34] which can be susceptible to various attacks,[35] and optical primitives,[18,36] which may have a larger number of degrees of freedom but limited compatibility with existing CMOS fabrication and readout technologies, magnetic unclonable functions offer key advantages. They are inherently compatible with existing semiconductor fabrication processes, enabling seamless integration with existing hardware[37–39] and they are characterized by an enhanced stability to environmental perturbations such as temperature fluctuations and high electric fields,[40,41] and resilience to machine learning attacks.[42] For these reasons, in recent years much attention has been devoted to magnetic systems that offer unclonability, stable responses even to harsh environments, and compatibility with the CMOS foundry.[17,43,44] Two are the main reading mechanisms of the intrinsic disorder of the magnetic systems: resistance measurements[16,45] and magneto-optic measurements[15] that are applied to spin transfer torque magnetic random-access memory,[46] spin orbit torque[15,47–49] and magnetic tunnel junctions.[16,44] These examples show the stability and potential of magnetic hardware but still have limitations in the number of independent extracted keys (on the order of a few tens of bits and low entropy per bit) and they operate only in single mode.[48,50,51] Although some reconfigurable PUFs have been shown in electrical and optical systems,[27,30,52–54] very few exploit magnetic effects.[15,48,49] This is mainly because the proposed magnetic PUFs typically require complex, multilayer thin-film stacks that are challenging to fabricate.

In this work, we present a new type of magnetic micropatterned platform based on an ordered array of $Fe_{70}Ga_{30}$ dots, that generates physical unclonable functions characterized by very high entropy and excellent robustness. This single-layer design is a major improvement over existing similar devices,[15] as it offers lower fabrication complexity, shorter production times, and reduced costs by avoiding the need for electrical contacts.

The FeGa alloy was selected for its appealing multiphysical properties, low cost and for the possibility of depositing it on a silicon substrate,[55] characteristics that are attracting growing interest from researchers.[56] The alloy exhibits soft magnetic properties resulting from a balanced contribution of magnetocrystalline and shape anisotropies, which leads to a peculiar arrangement of magnetic domains.[57] Furthermore, its high Curie temperature (> 600 K),[58,59] similar to other Fe-based amorphous and nanocrystalline alloys[60] or Fe-doped ferromagnetic semiconductors,[61] ensures the suitability of FeGa PUFs for applications requiring higher-than-ambient operating temperature. Finally, FeGa alloy is biocompatible,[62] making it suitable for PUF devices in biomedical environments.

Magneto-optical Kerr Effect (MOKE) microscopy was chosen for extracting the cryptographic key from the magnetization distribution due to its simple, noninvasive, and fast readout mechanism. Moreover, it offers stable, robust, repeatable measurements also across different devices and laboratories.[63,64]

We demonstrate the unique dual-mode operation of the proposed magnetic PUF: it can function as both a reproducible PUF and a reconfigurable one by leveraging the influence of an external magnetic field to induce remanence and anhysteretic states, respectively. In the deterministic mode, the material is configured into a stable remanence magnetic state through the repetition of a specific dc magnetic field history. The average magnetization of each dot is associated with a single bit, resulting in a key with around 500 independent bits, with an entropy per bit of 0.88. In the reconfigurable mode, the material is configured into a stochastic anhysteretic magnetic state driven by the repetition of a related ac magnetic field history. In this case, the randomly spatially complex arrangement of magnetization within each dot was extracted by advanced multibit processing able to maximize the security and information content of the cryptographic keys resulting in over 100 independent bits.

This dual mode switching operation using a single interrogation based on the solely magnetic field history within the same device surpasses state-of-the-art systems that rely on a multilevel operation,[18,65] multi-factor authentication[66] or irreversible reconfiguration by using multiple external stimuli.[67–69]

2. Results and Discussion

2.1. Magnetic Function Fabrication and Morphological Characterization

The 2D magnetic physical unclonable function consists of an array of 27 × 20 $Fe_{70}Ga_{30}$ dots, over a total area of 81 × 60 μm^2. This results in an areal dot density of 1.1×10^5 dots/mm^2, which significantly increases (more than two orders of magnitude) the amount of information that can be stored in the PUF (see Section 2.3) with respect to previous similar work.[15]

The $Fe_{70}Ga_{30}$ composition of the alloy was verified by EDX measurements on thin films deposited using RF sputtering with the same deposition parameters as the FeGa array. The EDX spectra (shown in Figure S1, Supporting Information) and their analysis confirm an Fe/Ga ratio of 70:30 within the experimental error. Based on our previous results obtained from a thin film of a similar thickness that was fabricated using the same setup,[70] the crystalline structure of the FeGa array can be considered a mixture of the A2, B2, and $D0_3$ phases.

The array has been manufactured through a combination of direct-write laser lithography and sputtering deposition, as depicted in **Figure** 1A. This manufacturing procedure (the details are reported in the Experimental Section) results in highly ordered dots in a square configuration whose top view SEM image is shown in Figure 1B. A high-magnification SEM image of four representative dots from the array is shown in Figure 1C. Despite being fabricated during the same lithographic process, the dots are morphologically similar but not identical. Each dot displays unique nanometric features such as defects, curvatures, and deformations.

A statistical study was conducted on the morphological characteristics of the entire PUF array. In particular, elliptical fitting on the SEM image (Figure 1B) was used to determine the spatial orientation (θ, the angle between the major axis and the horizontal axis of the SEM image) and the aspect ratio (the ratio between the major a_M and minor a_m axes of the ellipse) of each FeGa dot.

The θ angles, visualized by the color of the ellipse contours in Figure 1D, show a preferential alignment near the horizontal

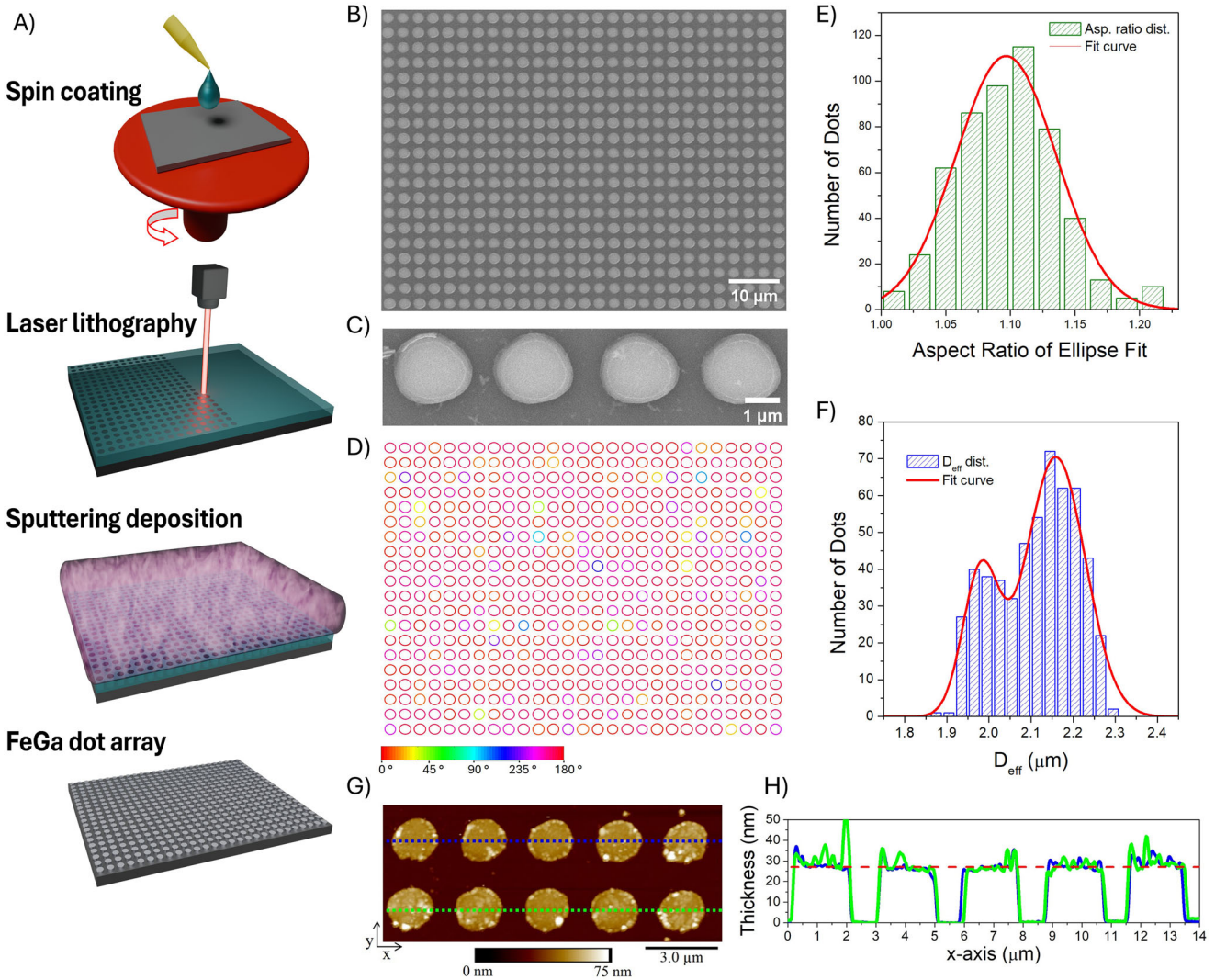

Figure 1. Fabrication and morphology analysis of the magnetic array of $Fe_{70}Ga_{30}$ dots. A) Fabrication protocols of the dot array; B) top-view SEM-image of the FeGa dot array; C) High-magnification SEM image of four representative dots; D) array of the best-fitting ellipse: the contour color displayed the orientation of the ellipse with respect to the horizontal axis of the SEM image; E) distribution of the best-fitting ellipse aspect ratio (green bars) and corresponding fitting curve (red line); F) distribution of the effective diameter (blue bars) and corresponding fitting curve (red line); G) AFM image of a representative portion of the dot array; H) height profiles extrapolated from the AFM image shown in G).

direction ($\theta \approx 0° \approx 180°$), with only a few dots exhibiting more random orientations. Furthermore, the distribution of the ellipse aspect ratio, shown in Figure 1E, extends over the range 1.00–1.21 and it is well-fitted by the Gaussian function (red curve) with a mean value ($\langle M \rangle$) of 1.10 μm and a standard deviation (SD) of 0.08 μm. This systematic distortion across all dots, from the ideal round shape to an elliptical one, could be due to minor astigmatism in the laser beam, which stretched the beam spot along the horizontal axis.

Despite this small deviation, the FeGa dots can be reasonably approximated as circles, whose effective diameter ($D_{eff} = \sqrt{a_M a_m}$) distribution (Figure 1F) is well-described by the superposition of two Gaussian functions (red curve) with a $\langle M \rangle$ of 1.98 and 2.16 μm and SD of 0.09 and 0.14 μm, respectively. As a result, the top-view morphology features of the PUF do not reveal significant dot-to-dot deviations.

The topographic features of the magnetic PUF were investigated using Atomic Force Microscopy (AFM). The AFM image of a representative PUF area (Figure 1G) reveals predominantly flat dot surfaces with a mean square root roughness of 3.21 ± 1.24 nm. Two height profiles, extracted from the AFM image (green and blue dashed lines) and shown in Figure 1H, demonstrate the sharp vertical walls of the dots and determine a dot thickness of 27 nm (see the dashed red line).

Ten (#10) nominally identical FeGa dot arrays were fabricated using the same design and process parameters. The top view SEM characterization (reported in Figure S2, Supporting Information) unequivocally demonstrates that the #10 fabricated arrays are identical in appearance, exhibiting no discernible differences in terms of morphology and size. Additionally, the ellipse-fitting analysis applied to each of the #10 arrays results in

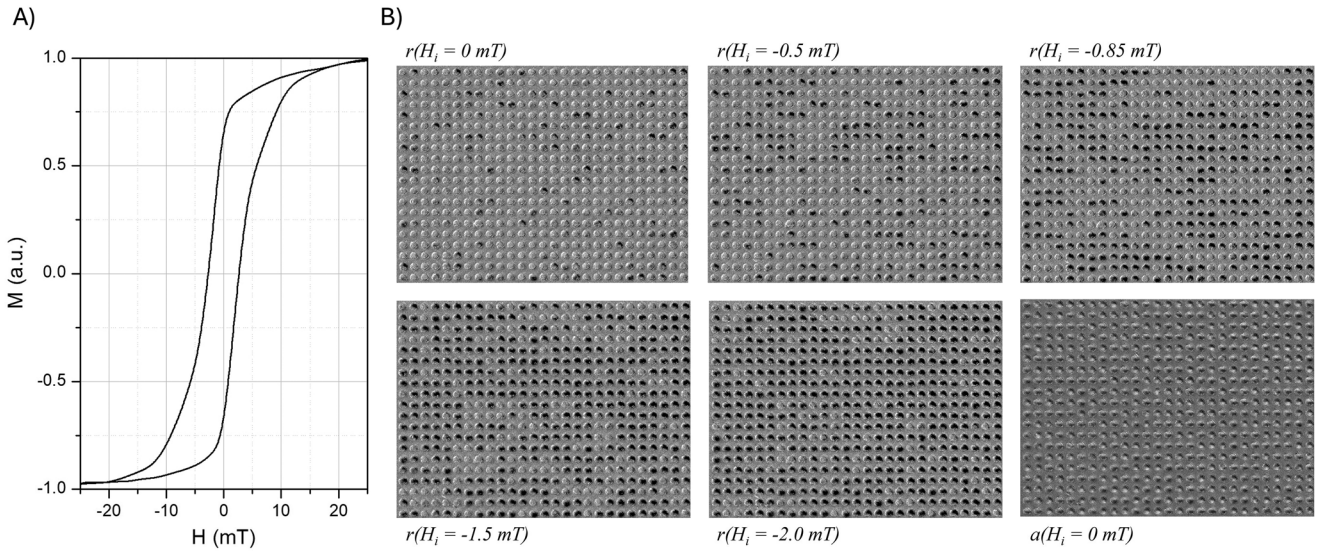

Figure 2. Magnetic characterization of PUF. A) Hysteresis loop of the FeGa dot array; B) MOKE-images of the FeGa dot array taken at selected remanence states ($r(H_i)$) and at the anhisteretic state $a(H_i = 0$ mT).

highly comparable and remarkably consistent values for aspect ratio and D_{eff}, see Figure S3 (Supporting Information).

This high degree of uniformity in the morphological characteristics among the arrays, resulting from the reliable and reproducible fabrication process, makes them suitable for authentication applications by effectively concealing the information content from visual (microscopy) inspection.

2.2. Magnetic Function Characterization and Key Generation

While morphological properties are consistent across dot arrays, inherent and uniqueness variations in magnetic properties, uncontrollable by either the manufacturer or a malicious attacker, make this hardware a suitable platform for physical unclonable functions.

The magnetic hysteresis loop of the whole FeGa dot array (**Figure** 2A) shows that the magnetization reversal occurs within a field range of ± 25 mT (the field is applied in-plane, parallel to the line of the 27 dots, called the x direction of the dot array). The monotonous and slow decrease of the $M(H)$ curve indicates that the switching process of magnetization does not occur at the same H value for each dot, but rather, a distribution of switching fields is present.

Information about the local magnetization of the FeGa array was extracted using the magneto-optical Kerr effect (MOKE) microscopy. The components parallel and antiparallel to x are displayed in white and black, while the magnetization components along the transverse direction y are displayed in an intermediate gray level. The out-of-plane magnetization component can be safely neglected in the current system.[71] Two peculiar magnetic state of the FeGa array, termed remanence state $r(H_i)$ and anhysteretic remanence state $a(H_i)$, were induced using user-defined magnetic field histories. The $r(H_i)$ state is obtained by applying a positive saturation field (here $H = +30$ mT), which is then slowly reduced to a (negative) value H_i (ranges from 0 mT to –2 mT), and finally increased to zero. The $a(H_i)$ state is obtained[72] by setting a constant DC field to H_i overimposed with an AC field (f = 17 Hz); the AC field amplitude is decreased to zero (decay time $\tau = 3$ s), and finally the DC H_i field is set to zero.

A selection of the $r(H_i)$ magnetic state, visualized by MOKE images, is shown in Figure 2B (the first five panels). At $r(H_i = 0$ mT), most of the dots are characterized by a light gray contrast, indicating that they have basically retained the saturated state induced by the previously applied positive saturation field. Only in a limited number of dots, those in dark gray, the magnetization reversed. By progressively increasing the negative amplitude of H_i, the obtained $r(H_i)$ state is characterized by an increasing number of switched dots. At $r(H_i = –0.85$ mT) state, the number of dark gray dots is comparable to the number of the light gray dots. Ultimately, at $r(H_i = –7$ mT), the dark gray dots are the most prevalent.

Figure 2B in the lower right panel shows a representative MOKE image of the $a(H_i = 0$ mT) magnetic state. Herein, each dot is no longer clearly labelled by a single gray level, but results in a mixture of light and dark grays that vary from dot to dot, indicating a complex spatial distribution of the magnetic domains.

Panels A and B of **Figure 3** present enlarged MOKE images of the same representative region of the FeGa dot array, acquired sequentially in the $r(H_i = –0.85$ mT) and $a(H_i = 0$ mT) states. Notably, the transition to $a(H_i)$ state erases any of the previous $r(H_i)$ state. Specifically, each dot switches from a predominantly light- or dark-gray contrast to a unique, randomly spatially modulated gray scale.

Furthermore, the MOKE images revealed that, in both the $r(H_i)$ and $a(H_i)$ states, nominally identical dots highlight distinct magnetic configurations under the same applied field history. This observation likely stems from small, random variations in the microstructure, such as crystallographic cell orientation, point defects, or grain boundaries, or slight variations in morphology (see Figure 1C) from one dot to another,[2,5,7] combined with the inherent characteristic of magnetic systems of

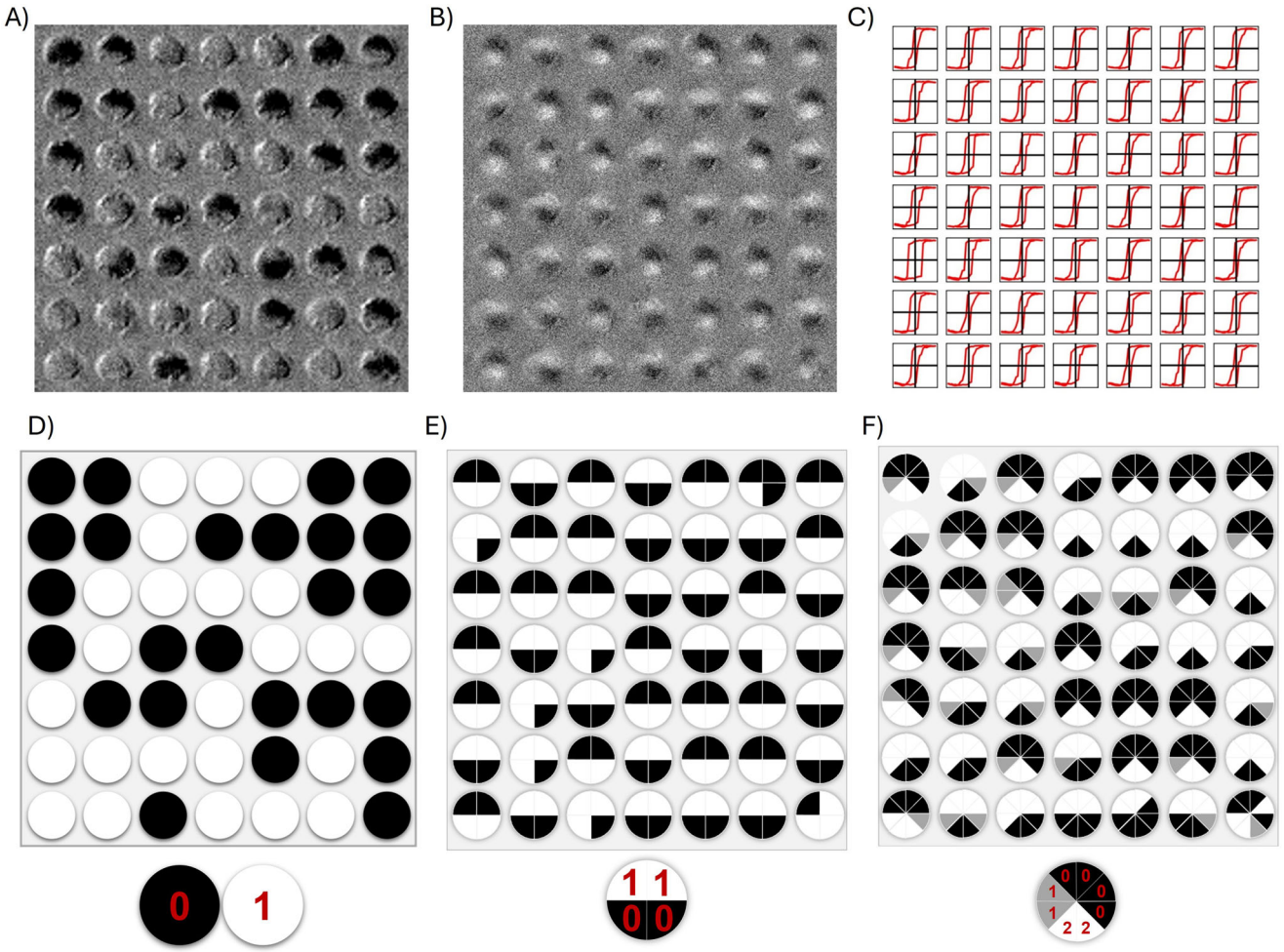

Figure 3. Cryptographic key extraction. A) MOKE image of a 7 × 7 portion of the FeGa dot array at $r(H_i$ = -0.85 mT); B) MOKE image of the same 7 × 7 portion of the FeGa dot array at $a(H_i = 0$ mT); C) individual hysteresis loops of each FeGa dot in the array portion shown in panels A and B; D) binary mask obtained from the MOKE image in panel A using a *1-bit* procedure; E) binary mask obtained from the MOKE image in panel B using a *4-bit* procedure; F) binary mask obtained from the MOKE image in panel B using an *8-trits* procedure. Legends under D–F) represent an example of the binary values extracted applying the three procedures to a single dot.

simultaneously minimizing different internal energy terms.[11] This magnetic uniqueness of each single dot is corroborated by the hysteresis loops measured for each dot individually, (Figure 3C), which exhibit significant variations in the shape, remanence and coercive field values.

The magnetic behavior of the array, and consequently the PUF functionality, are influenced by the design of the dot, including geometric parameters such as diameter, thickness, and center-to-center distance, as well as alloy composition. By changing one of these parameters, the magnetic configuration of the dot can evolve from a single domain to a more complex single or multiple vortex state, and even to a multi-domain configuration.[71,73] Examples of MOKE images taken at demagnetized state on FeGa arrays with different dot diameters (D_{eff} = 1.4 – 1.8 µm) and composition ($Fe_{80}Ga_{20}$) are shown in Figure S4 (Supporting Information). Variations in diameter within the explored range do not substantially alter the main features of the demagnetized state observed in Figure 3B. The magnetic domains consistently form a complex, randomly oriented spatial distribution. A visible variation is instead observed when the FeGa alloy composition is modified. In fact, each $Fe_{80}Ga_{20}$ dot exhibits a much more defined and oriented demagnetized state, which is constituted by two domains with opposing magnetization along the *x* direction. The correlation among magnetization distributions limits the random response of the PUF and it has not been considered within this study.

The magnetic information encoded in the $r(H_i)$ and $a(H_i)$ states of the FeGa dots array is translated into a cryptographic key (K_i) by distinct procedures based on the gray level of the MOKE images.

The first procedure (called *1-bit*) fixes a threshold equidistant between the maximum and minimum gray values of the entire corresponding MOKE image. Then, each dot is classified as 0 (black) or 1 (white), based on whether its mean gray value falls below or exceeds this threshold, respectively. As a result, each dot stores 1 bit of information. As an example, Figure 3D shows the binary image corresponding to the MOKE image of the panel A obtained following the *1-bit* procedure.

While this procedure reliably transfers magnetic information encoded in the $r(H_i)$ states to the cryptographic key, it is not suitable for analyzing the $a(H_i)$ state due to its complex spatial distribution of magnetic domains within each dot. Therefore, three different binarization procedures (called *4-bits*, *8-bits* and *8-trits*) for the $a(H_i)$ state were developed. In the *4-bits* and *8-bits* procedures, each dot in the MOKE image is divided in four 90° sectors or eight 45° sectors, respectively, then each sector is again converted to 0 (black) or 1 (white) by comparing its mean gray value with the aforementioned threshold. Each dot now encodes one of the 2^4 or 2^8 possible states. As an example, Figure 3E shows the binary image obtained by processing the image of panel B with the *4-bits* procedure. On the other hand, the *8-trits* procedure classifies the mean gray value of each of the 8 sectors into one of three levels (black, gray, or white) based on two thresholds equally spaced across the gray scale of the MOKE image. These levels are then indexed as 0, 1, and 2, respectively. Each dot now carries one of the 3^8 possible states. The processed image resulting from applying the 8-*trits* procedure to panel B is shown in Figure 3F.

2.3. Magnetic Unclonable Function

Each binary key extracted from the MOKE images is then analyzed using information theory concepts. We computed the Shannon entropy S of a single key from the 1-bit probability p_{key} and 0-bit probability $(1 - p_{key})$: $S = -p_{key}log_2(p_{key}) - (1 - p_{key})log_2((1 - p_{key}))$.[74]

On the other hand, the cross-comparison in between different keys generated from different devices (*inter* PUF) or different interrogations on the same device (*intra* PUF) is based on the Fractional Hamming Distance (FHD) metrics. This is the pairwise distance between keys normalized to bit string length. Thus ideal identical keys have a FHD equal to zero while random keys a FHD of 0.5. By comparing PUF responses generated by repeatedly interrogating the same device with same challenge (termed *like* FHD) we establish the system stability. While by applying the same challenge on different devices or different challenges on the same device (termed *inter* or *intra unlike* FHD, respectively) we access the system unclonability and ability to generate random responses.

The number of independent bits of the keys extracted from the PUF is calculated from the *inter*-FHD distribution. Under the assumption that the "0" and "1" bit are equiprobable, the FHD distribution can be associated to a binomial distribution, which, for a large number of comparisons, is also well fitted by a Gaussian distribution with an average value and a standard deviation (p, σ). The latter two parameters can be used to calculate the number of independent bits (or degrees of freedom) using the formula $N_{deg} = p(1 - p)/\sigma^2$.[75,76] In this way, the resulting number of independent bits (or entropy) is scaled down by removing eventual correlations among the keys. Considering the unpredictable nature of the configuration of the magnetic domains in each dot at the remanence states, we now highlight how such magnetic hardware behaves as a PUF by using the metric here above described.

The performance of the proposed magnetic PUF was evaluated by using 1-bit procedure key extraction.

Key randomness is a fundamental requirement for secure PUFs and it is first related to the equiprobable presence of bit 0 to bit 1 in the key, that is defined as bit uniformity. The p_{key} of the keys, interrogated with selected H_i challenges (with H_i ranging from 0 to –2 mT), was calculated and reported in **Figure 4A**. The bits uniformity is strongly correlated with H_i value. A monotonic decreases in p_{key} is observed, from $p_{key} = 0.78$ at $H_i = 0$ to $p_{key} = 0.15$ at $H_i = -2$ mT. A bit uniformity of 0.5 is obtained for $H_i \approx -0.85$ mT. Moreover, the Shannon entropy for single keys was calculated from the values of p_{key} at different H_i, see the right axis of Figure 4A. As expected, the entropy approaches the ideal entropy value of "1" in a small range around $H_i \approx -0.85$ mT, indicating that this range is where PUF shows the highest levels of unpredictability and randomness within a single key. Outside this range, a reduction in entropy is observed. This characteristic of the PUF is closely linked to the intrinsic magnetic behavior of the FeGa dot array. The magnetic field parameter H_i selects a peculiar magnetic configuration of the array from a large number of possible configurations, spanning the gradual transition between positive and negative magnetic saturation. In these extreme states, all dots in the array are in the same magnetic configuration, resulting in keys composed entirely of 1 or 0 bits, respectively. Furthermore, it is important to notice that while the entropy reported in Figure 4A analyses only the equiprobability of bits inside a cryptographic key, the number of independent bits for this type of hardware should take into account eventual correlations present in the keys extracted from different devices. Figure 4B shows the *like* distributions (colored bars) obtained from pairwise-comparisons of keys generated by repeatedly interrogating (50 times) a selected FeGa array with the same challenge H_i, where $H_i = -0.25$, –0.85, –1.75, or –2 mT. These data provide an estimate of the stability of the system that is affected by the average key noise, which corresponds to bit-flips that occur stochastically in the key generated from the same challenge applied to the PUF depending on the H_i. The H_i values were selected to investigate the magnetic reversal process of the FeGa dots array, as discussed in the Section 2.2. Each *like* distribution is then fitted by a Gaussian curve (colored lines), whose mean value and variance (ρ, σ^2) vary as a function of H_i. Notably, lower (ρ, σ^2) values indicate higher key stability,[77] resulting in greater robustness of the PUF against unwanted physical effects and intrinsic magnetic stochasticity. As a matter of fact, ρ varies as a function of H_i; therefore, the choice of H_i challenge affects not only the randomness of the key (Figure 4A), but also its stability. Despite the slightly larger fluctuations that may occur, the selection of magnetic field interrogation is dictated by the maximized entropy (see Figure 4A) that guarantees greater security of the system.

To quantitatively assess the stability of the keys within the same PUF (*like* FHD) and the uniqueness of the keys encoded in different PUFs (*inter* FHD), we characterized #10 nominally identical arrays fabricated with the same process by MOKE. The challenge has been set to $r(H_i = -0.85$ mT) and the keys have been extracted using the *1-bit* procedure. A repetition of 50 keys was generated for each array. In this way, we obtained the *inter FHD* distributions that quantify the variability of the keys generated by all possible pairs of magnetic arrays interrogated with the same challenge. Each distribution is then well approximated by a Gaussian function, whose amplitude, mean value and variance (reported

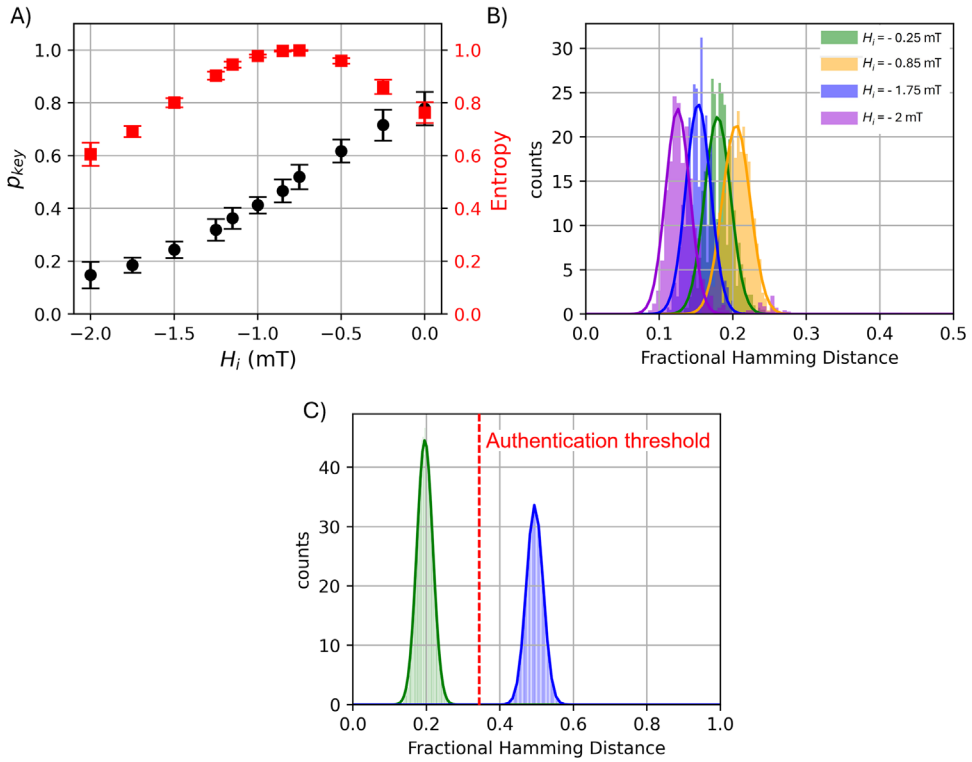

Figure 4. Analysis of the cryptographic keys from the remanence state with 1-bit encoding. A) Relative frequency p_{key} (black symbols) and entropy (red symbols) in the DC remanence states $r(H_i)$. B) Like distributions of remanence at different fields H_i. (ρ, σ^2) vary as a function of H_i. The distributions are fitted with Gaussian curves whose $\rho \pm \sigma^2$ are 0.179 ± 0.018, 0.205 ± 0.019, 0.153 ± 0.017, 0.125 ± 0.016 for $H_i = -0.25$, -0.85, -1.75, -2 mT, respectively. C) Unclonability of the system at $r(H_i = -0.85$ mT): the average cumulative like distribution of the 10 different devices (green bars and line); the average cumulative distribution of the inter FHD distributions between all the couples of devices (blue bars and line). Authentication threshold marked by red dashed line.

in Supporting Information) are comparable across different array pairs.

Their cumulative distribution is reported in Figure 4C as blue histogram. The mean Gaussian curve is drawn as blue line and summarizes all the calculated *inter FHD* distributions; its center at 0.495 and its standard deviation of 0.023 indicate a high degree of dissimilarity between keys related to the magnetic properties of the FeGa arrays. This proves that the inherent physical variations induced during the fabrication process prevent exact replication of the FeGa array in terms of identical challenge-response pairs, i.e., this magnetic PUF is unclonable and characterized by minimally correlated responses despite the identical fabrication and morphological properties at the microscale. From the *inter FHD* distribution and in particular from its mean and variance value,[78] we can estimate the number of independent bits in cryptographic keys that is around $N_{deg} = 473$ bits (over a 540 bit cryptographic key), which means an entropy per symbol (bit) of around 0.88.

The unclonability of the magnetic PUF solely based on the knowledge of the morphological properties of the FeGa dot array was also tested.[77] In particular, the Pearson coefficient (P) was used to estimate the correlation between the key generated with $H_i = -0.85$ mT challenge and the morphological parameters of the individual dots, assessed by the best-fitting ellipse procedure (described previously). The P values, obtained from testing a selected dot array, are close to zero: –0.034, –0.049, 0.064, and 0.024 for correlations with major and minor axis lengths, orientation and elliptical fit aspect ratio, respectively. This demonstrates the resistance of this PUF to cloning based on morphological parameters.

To further verify the stability of all the #10 arrays, we compared the responses to the same magnetic field history (identical challenge). From their remanence state $r(H_i = -0.85$ mT) the cryptographic keys have been extracted and pairwise-compared to calculate the *like* distributions. The ten distributions are well-fitted by a Gaussian function, whose amplitude, mean value and variance are reported in Supporting Information. The overall *like* FHD is shown as a green histogram in Figure 4C and it summarized by the Gaussian curve (green line) centered at 0.196 with standard deviation of 0.017. This result indicates that the different fabricated PUFs, despite their uniqueness, provide comparable behavior in response to the same challenge, ensuring reliable performance across multiple devices.

A relevant feature is the clear separation in between *inter* and *intra like* FHD distributions. This is an essential requirement for the efficient operation of PUFs,[79] thus minimizing the likelihood of false positive and false negative rate.[80] The authentication threshold, i.e., the FHD value for which the responses are considered *"True"* (FHD<authentication threshold) or *"False"* (FHD >authentication threshold), is typically set at the value for which the FHD distributions intersect. Since in our analysis, the experimental data are well separated, the authentication

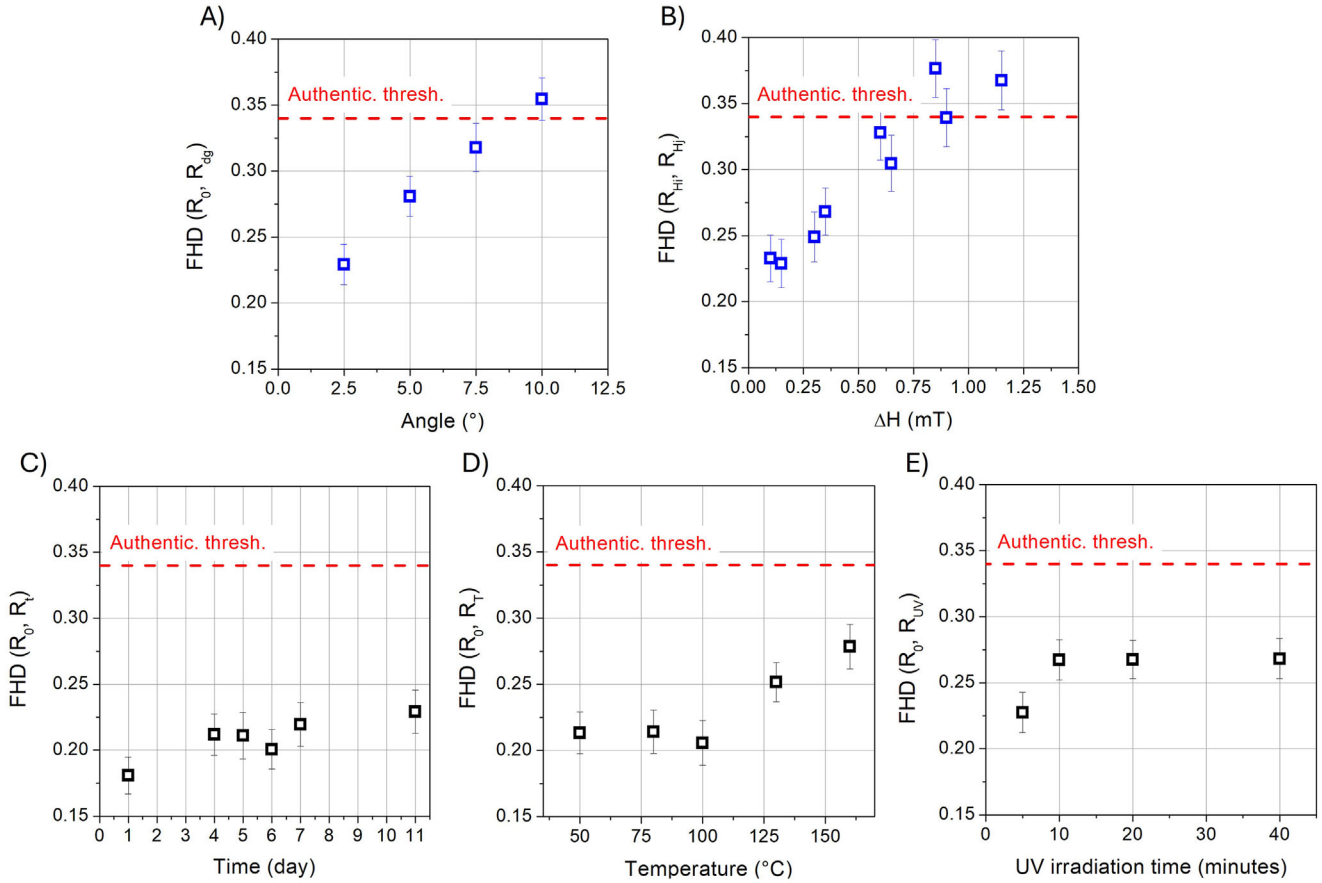

Figure 5. Stability tests of the magnetic PUF. Response sensitivity to the variation of the challenge parameters: A) alignment of the magnetic field with respect to the FeGa dot array and B) intensity of the magnetic field. C) Long-term stability over a 11-day period. Response sensitivity to environmental fluctuations: D) temperature variation and E) UV exposure time. The authentication threshold (red dashed line) is the same reported in Figure 4C.

threshold can be identified as the intersection of the two Gaussian FHD curves. For our magnetic PUF, the threshold is at 0.34 (dashed red line in Figure 4C.)

2.3.1. Stability Tests of the Magnetic Unclonable Function

The stability and robustness of the proposed magnetic PUF was tested against several factors, including unintentional variations of the challenge and environmental fluctuations that might induce aging effect, such as temperature variation and UV exposure.

Before each stability test, a reference set of 50 keys (R_0) was acquired under ideal measurement conditions with no environmental perturbations. The challenge field $r(H_i = –0.85$ mT) was used for all stability tests, unless otherwise reported. To assess the PUF's sensitivity and stability, we used the FHD metric to compare a reference response R_0 with responses R_x gathered over time or under different magnetic field and external disturbances.

First, we study the sensitivity of the responses to challenge variation[77] that can occur both as variation of the strength and alignment of direction of the magnetic field with respect to the FeGa dot array.

The effect of angular misalignment of the challenge field along the *x*-direction of the FeGa dot matrix was evaluated by acquiring four sets of 50 responses (R_{dg}) and varying the angle between 2.5° and 10°. **Figure** 5A shows the mean value and standard deviation of the resulting FHD distributions. A linear trend emerges between the mean FHD value and the angular displacement of the magnetic field that reflects the sensitivity of the magnetization of the dots with respect to the challenge as expected. For an angular variation below 7.5°, the responses obtained are below the authentication threshold making the magnetic PUF robust to small angular deviation.

When considering the stability of the PUF response to unintentional variations in the intensity of the challenge field, we observe a similar behavior. Practically, we compared Keys generated with a varying field H_j to the reference set of keys generated with the challenge field $r(H_i = –0.85$ mT) (i.e., the intensity that guarantees the bit uniformity). The resulting mean FHD and its standard deviation are reported as a function of the intensity difference $\Delta H = |H_i - H_j|$ in Figure 5B. Also in this case, a linear relationship emerges among the keys extracted from the magnetization orientation within the dots and the difference in the magnetic field intensity due to their direct proportionality. We can therefore assess that this magnetic PUF is sensitive to challenge variation in both angle and magnitude of

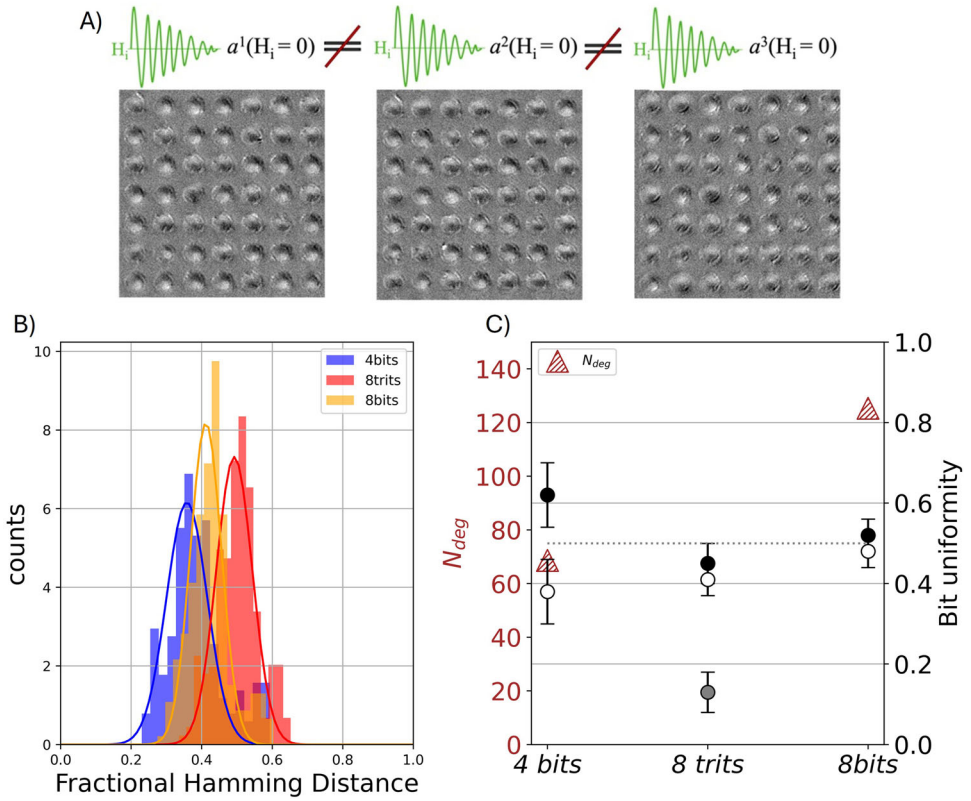

Figure 6. Multibit analysis of the keys in the anhysteretic remanence states. A) Schematics of three example $a(H_i)$ states, showing in green the demagnetization history around $H_i = 0$ mT, the MOKE images illustrates the non-repeatability of the obtained magnetis states.B) Intra unlike distributions, with *4-bits* analysis (blue), *8-trits* analysis (red), *8-bits* analysis (orange). C) For the different types of analysis *4-bits*, *8-trits*, *8-bits*: the number of degrees of freedom N_{deg} (left scale, brown triangle) and the bit uniformity (right scale, circles for the black/white bits or black/gray/white trits average values).

the magnetic field if they exceed around 10° and $\Delta H < 0.65$ mT, respectively.

The temporal stability of the magnetic PUF was evaluated over an 11-day period. Sets of 50 responses (R_t) were collected on the reported days and compared to the reference set acquired on day "0". Figure 5C reports the mean value and the standard deviation of the FHD distributions obtained over time. The PUF response shows small fluctuations along the measurement period, with all values well below the authentication threshold.

To assess the thermal stability of the magnetic PUF devices, the FeGa array was subjected to a series of high temperatures selected between 50 and 160 °C for 10 minutes. Following each thermal treatment and subsequent cooling to room temperature, a new set of 50 responses (R_T) was collected. Figure 5D shows that thermal shocks up to 100 °C do not alter the PUF response, as indicated by the constant trend of the FHD mean value. Thermal treatments at higher temperatures start to gradually compromise the information stored in the PUF, as indicated by the mean FHD value approaching the authentication threshold.

Finally, the reliability of the PUF under UV light ($\lambda = 385$ nm, $I = 12.2$ mWcm^{-2}) was also tested by irradiating the FeGa array for a time interval up to 40 minutes. After each irradiation, a new set of 50 responses (R_{UV}) was measured. A slight variation in the stored PUF information was detected within the first 10 minutes of exposure, after which the mean FHD value stabilized, see Figure 5E. It is noteworthy that all measured mean FHD values are consistently below the authentication threshold, ensuring that the device can be used in environments where UV light is present or in the case of accidental exposure.

2.4. Reconfigurable Magnetic Unclonable Function

The array of magnetic dots when subjected to an alternating field of gradually decreasing amplitude simultaneously with a steady unidirectional DC field has a more complex and unpredictable evolution of the microscopic magnetization. At the anhysteretic magnetic state $a(H_i = 0$ mT), when both fields are brought to zero, the magnetization distribution is not any more reproducible and is characterized by a more complex pattern within each dot (**Figure 6**A). This behavior leads to an unpredictable reset of the magnetization distribution within each dot, and it is herein exploited to generate new cryptographic keys from the same hardware. In other words, anhysteretic remanence states allow the use of the same hardware as reconfigurable magnetic PUFs.[67,68] Once the magnetic history is applied, the magnetization distribution is stable within each dot.

In order to grasp all the information of the magnetization distribution within the dots, we applied the *4-bits*, *8-bits*, and *8-trits* analyses. Figure 6B shows the *inter* FHD distributions of keys obtained along 21 reconfiguration cycles using the different methods for key generation. We refer as inter FHD for reconfigurable

PUFs since along the reconfiguration process we are creating different hardware. It is immediately clear that the FHD distribution for *8-bits* and *8-trits* processing allows a more faithful representation of the magnetization distribution in the keys, which results in more randomized keys (FHD ≈ 0.5) (Figure 6B). Moreover, by retrieving the number of independent bits from the FHD distributions, we found a monotonic increase relation among the extracted independent degrees of freedom and the number of bits that maps the magnetization distribution of the extracted keys (Figure 6C). Using the proposed encoding strategies with a different number of bits, the uniformity of the bit is well preserved, especially in the case of *8 trits* and *8 bits* for which we are able to extract all the magnetic information of the reconfigurable magnetic PUF. For the *8 bits* reconfigurable PUF, we obtained a larger number of independent bits close to 125 bits per key that correspond to an information spatial density of around 3300 $bits/mm^2$ (see Table 4, Supporting Information), greatly improving the reported reconfigurable magnetic PUFs.[15]

3. Conclusion

In this work, we demonstrate that arrays of Fe-Ga magnetic dots can be used to create robust and reliable physical unclonable functions. Unlike other systems, the cryptographic keys generated by our devices are based on the intrinsic magnetic properties of the material, that is not correlated to their geometrical shape. The unique magnetization states of each micrometric dot can be read thanks to the Magneto Optical Kerr Effect and converted into a cryptographic key that is extremely difficult to clone or predict, even with nanoscale inspection. Using a 27 × 20 dot array, we were able to extract a key of roughly 475 independent bits—well above the 256 bits required for a secure digital signature. With an encoding capacity of approximately 10^{144}, our magnetic system outperforms many other PUF technologies providing in a single hardware a large encoding capacity, small footprint, integrability, and reconfigurability (see Table 5, Supporting Information). Furthermore, our device is stable over time, resilient to environmental stress (thermal and UV), and tolerant to minor variations in the magnetic field used for interrogation. To enhance its functionality, we demonstrate its reconfiguration with a permanent modification of the response by using anhysteretic states. We generated single-use passwords with around 125 independent bits from the same hardware, simply by controlling the magnetic field history. This unique ability to generate both stable, reproducible keys and reconfigurable one-time passwords makes our device a versatile and promising building block for next-generation, multilevel magnetic cryptographic hardware. Two significant advantages may encourage its use in authenticating and tracking micro opto-electronic devices: first, the micro-hardware is compatible with the existing semiconductor manufacturing processes and secondly, the key readout is based on the simple and reliable MOKE technique at low field intensity, that can be adopted at low cost.

4. Experimental Section

Fabrication Process: $Fe_{70}Ga_{30}$ dot array was fabricated by combining direct-write laser lithography with the sputtering deposition technique, as sketched in Figure 1A.

The AZ1505 photoresist was spin-coated (4000 rpm, 30 s) onto a thermally oxidized silicon substrate (SiO_2: 500 nm); it was then selectively exposed in circular areas (3 µm spacing) using a Heidelberg Laser Writer with a laser power of 5 mW. The exposed photoresist was removed by immersion in 351B developer (1:5 dilution in deionized H_2O) under sonication (20 s), creating a polymer mask with circular holes 2 µm in diameter.

Subsequently, $Fe_{70}Ga_{30}$ alloy was deposited onto the polymer mask by RF-sputtering. The deposition parameters were kept constant throughout the duration of the deposition: a base pressure of 2×10^{-7} mbar, a target power density of 50 W and an Ar^+ gas pressure of 1×10^{-2} mbar.

After deposition, the polymer mask was removed by a lift-off process in acetone, revealing a FeGa dot array on the SiO_2/Si substrate constituted by 540 elements.

A series of #10 nominally identical FeGa dot arrays were fabricated using this procedure.

Sputtering and lithography techniques were selected for their parallel manufacturing capabilities to fabricate multiple devices simultaneously. Sputtering allows for the deposition of a thin layer on very large substrates in a single cycle. Likewise, the lithography process (with straightforward modifications from the proposed direct-writing such as using rigid shadow masks) can pattern an entire substrate in a single, parallel step. These fabrication approaches based on parallel processes make the device production faster and improves scalability, directly contributing to lower unit costs.

Characterization Techniques: Scanning electron microscopy (SEM - FEI InspectF) were exploited to study the morphology and shape of the FeGa dot array through top-view imaging. The micrographs were analysed by the elliptical fitting tool of the open source software Imagej. Additionally, an integrated EDX detector on the SEM was used to measure the composition of the FeGa alloy.

Atomic force microscopy (AFM - Bruker - Multimode 8), operating in intermittent contact mode, was dedicated to estimate the thickness and the surface features of the FeGa dots.

Magneto-optical Kerr effect (MOKE) microscopy (Evico magnetics) to study the magnetization reversal process of the FeGa dot array. An oil immersion objective with 100x magnification and 1.30 numerical aperture was mounted. The electromagnet, equipped with the MOKE microscope, is capable of generating a magnetic field with a magnitude of up to ±1.3 T in the plane and up to ±0.9 T out of the plane. The longitudinal sensitivity of MOKE allows for the discrimination of the orientation of magnetization components in the plane of each dot as a grayscale contrast. Non-magnetic information from MOKE image was removed subtracting each MOKE image from an reference image taken at the saturation field.

The reading time for information encoded in the magnetic PUF using MOKE is approximately 30 ms for a single raw exposition. To obtain a better signal to noise ratio, averaging mode is used both in the acquisition of the background image at saturation and in the final image. The time required for a single image at remanence $r(H_i)$ is therefore around 4 s. The acquisition of the anhysteretic remanence state $a(H_i)$ requires an additional decay time $\tau = 3$ s to reach the demagnetized state, so the total time required is around 7 s. The FeGa array was irradiated using a UV lamp (ThorLabs M385CP1-C4) operating at a wavelength (λ) of 385 nm and an intensity (I) of 12.2 mW cm^{-2}. In addition, thermal treatments of the FeGa array was performed in air by means of a heating chamber (Binder GmbH) operating in temperature range from 60 °C to 230 °C.

Fractional Hamming Distance Metric: In information theory the Hamming distance between two points is defined to be the number of bits by which they differ. Here we will define it as the normalized distance between two magnetic states. A magnetic state M (*key*) will be here defined as a set of elements $\{d_i\}$ where i is the coordinate index. Starting from an alphabet $\Sigma = \{0, 1\}$ (*1-bit*, *4-bits*, or *8-bits*) or $\Sigma = \{0, 1, 2\}$ (*8-trits*), an element $d_i \in \Sigma^n$ can be defined from the Cartesian product of the alphabet with itself Σ^n n times, with $n = 1$ (*1-bit*), $n = 4$ (*4-bits*) or $n = 8$ (*8-bits*,*8-trits*), resulting in the set of all possible n-character sequences. The FHD between two states M^1, M^2 can then be defined as $FHD = XOR(M^1, M^2))/L$ where L is the bit string length. This function applies the XOR operator to the corresponding elements d_i^1, d_i^2 in the M^1, M^2 states. In the case of $n > 1$ processing, the distance is the bit fraction that differs between d_i^1, d_i^2, with

the limit values of 0 if the state is identical $d_i^1 = d_i^2$, and 1 if it is maximally different.

Supporting Information

Supporting Information is available from the Wiley Online Library or from the author.

Acknowledgements

Part of this work was carried out at Nanofacility Piemonte, a laboratory supported by the "Compagnia di San Paolo" Foundation, and at QR Lab - Micro&Nanolaboratories, INRiM. This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union—NextGenerationEU and co-funded by the European Union—NextGenerationEU, "Integrated infrastructure initiative in Photonic and Quantum Sciences"—I-PHOQS (IR0000016, ID D2B8D520, CUP B53C22001750006). S.N. acknowledges the financial support from project "PRIN 2022 2022T3B4HS-PE11 - Multistep optical encoding in anticounterfeiting photonic tags based on liquid crystals (PHOTAG)" financed in the framework of Piano Nazionale di Ripresa e Resilienza (PNRR). G.B. acknowledges the financial support from project "PRIN 2022WY522H- PE3-10 - Fast readable label by Unique Magnetic Fingerprints on Industry 4.0: polymeric nanocomposites for a global exchange of information with a high level of security (U-MagFinger)" financed in the framework of Piano Nazionale di Ripresa e Resilienza (PNRR).

Open access publishing facilitated by Istituto Nazionale di Ricerca Metrologica, as part of the Wiley - CRUI-CARE agreement.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are openly available in Zenodo at https://zenodo.org/records/17036428, reference number 17036428.

Keywords

magnetic microstructures, physical unclonable functions, reconfigurability, robustness, unpredictable magnetic properties

Received: June 26, 2025
Revised: September 29, 2025
Published online: October 8, 2025

[1] K. Y. Camsari, P. Debashis, V. Ostwal, A. Z. Pervaiz, T. Shen, Z. Chen, S. Datta, J. Appenzeller, *Proc. IEEE* **2020**, *108*, 1322.
[2] M. Coïsson, G. Barrera, F. Celegato, A. Manzin, F. Vinai, P. Tiberto, *Sci. Rep.* **2016**, *6*, 29904.
[3] M.-Y. Im, P. Fischer, D.-H. Kim, K.-D. Lee, S.-H. Lee, S.-C. Shin, *Adv. Mater.* **2008**, *20*, 1750.
[4] F. Luo, K. Toyoki, C. Mitsumata, J. Shen, R. Nakatani, Y. Shiratsuchi, *J. Magn. Magn. Mater.* **2023**, *587*, 171228.
[5] M.-Y. Im, P. Fischer, K. Yamada, T. Sato, S. Kasai, Y. Nakatani, T. Ono, *Nat. Commun.* **2012**, *3*, 983.
[6] H. J. Ng, S. Yang, Z. Yao, H. Yang, C. Lim, *Phys. Rev. Appl.* **2023**, *19*, 034077.
[7] D. Gallina, G. Pastor, *Nanomaterials* **2021**, *11*, 1392.
[8] G. Qin, Y. Ren, N. Xiao, B. Yang, L. Zuo, K. Oikawa, *Int. Mater. Rev.* **2009**, *54*, 157.
[9] A. D. Kent, D. C. Worledge, *Nat. Nanotechnol.* **2015**, *10*, 187.
[10] C. Bran, E. Saugar, J. A. Fernandez-Roldan, R. P. Del Real, A. Asenjo, L. Aballe, M. Foerster, A. F. Rodriguez, E. M. Palmero, M. Vazquez, O. Chubykalo-Fesenko, *Nanoscale* **2021**, *13*, 12587.
[11] C. Navau, J. Sort, *APL Mater.* **2021**, *9*, 7.
[12] E. Raimondo, A. Grimaldi, A. Giordano, M. Chiappini, M. Carpentieri, G. Finocchio, in *2024 IEEE 24th International Conference on Nanotechnology (NANO)*. IEEE, **2024**, pp. 326–330.
[13] B. R. Zink, Y. Lv, J.-P. Wang, *IEEE J. Exploratory Solid-State Comput. Dev. Circuits* **2022**, *8*, 173.
[14] H. Chen, M. Song, Z. Guo, R. Li, Q. Zou, S. Luo, S. Zhang, Q. Luo, J. Hong, L. You, *Nano Lett.* **2018**, *18*, 7211.
[15] J. Lee, J. Lee, S. Yoon, M. Lee, J. Lee, Y. Jang, D. Kim, S. Choe, J. Park, Y. K. Kim, *Adv. Electron. Mater.* **2023**, *9*.
[16] Y. Shao, N. Davila, F. Ebrahimi, J. A. Katine, G. Finocchio, P. Khalili Amiri, *Adv. Electron. Mater.* **2023**, *9*, 2300195.
[17] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, R. J. Young, *Appl. Phys. Rev.* **2019**, *6*, 1.
[18] S. Nocentini, U. Rührmair, M. Barni, D. S. Wiersma, F. Riboli, *Nat. Mater.* **2024**, *23*, 369.
[19] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally, *Comput. Networks* **2020**, *183*, 107593.
[20] J.-L. Danger, S. Guilley, D. Mukhopadhyay, U. Ruhrmair, *Embedded Cryptography* **2025**, *2*, 339.
[21] H. Seo, T. Park, A. Ali, B. K. Jung, Y. K. Choi, J. Park, S. J. Oh, *Adv. Funct. Mater.* **2025**, 2507395.
[22] Y. Cho, J. Pyeon, H. Jang, G. Mun, J. Kang, B.-G. Park, G. Y. Kim, H. Kim, Y. S. Jung, *Adv. Funct. Mater.* **2025**, 2424079.
[23] A. Esidir, M. Ren, S. Pekdemir, M. Kalay, N. Kayaci, N. Gunaltay, H. Usta, X. Huang, M. S. Onses, *Adv. Funct. Mater.* **2025**, *35*, 2417673.
[24] M. Ma, S. Dong, W. Yuan, T. Ma, M. Xu, X. Jiang, J. Li, *Adv. Funct. Mater.* **2025**, *35*, 2414467.
[25] J. W. Leem, M. S. Kim, S. H. Choi, S.-R. Kim, S.-W. Kim, Y. M. Song, R. J. Young, Y. L. Kim, *Nat. Commun.* **2020**, *11*, 328.
[26] F. Jiao, C. Lin, L. Dong, Y. Wu, Y. Xiao, Z. Zhang, J. Sun, W.-B. Zhao, S. Li, X. Yang, P. Ni, L. Wang, C.-X. Shan, *ACS Appl. Mater. Interfaces* **2024**, *16*, 44328.
[27] R. Horstmeyer, S. Assawaworrarit, U. Ruhrmair, C. Yang, in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, **2015**, pp. 157–162.
[28] M. Sandomirskii, E. Petrova, P. Kustov, L. Chizhov, A. Larin, S. Bruyère, V. Yaroshenko, E. Ageev, P. Belov, D. Zuev, *Nat. Commun.* **2025**, *16*, 5097.
[29] J. Ahn, T. Park, T. Kang, S.-G. Im, H. Seo, B.-H. Kim, S. J. Kwon, S. J. Oh, *Sci. Adv.* **2025**, *11*, eadt7527.
[30] H. Kim, K. Lee, G. Zan, E. Shin, W. Kim, K. Zhao, G. Jang, J. Moon, C. Park, *ACS nano* **2025**.
[31] Y. Gao, S. F. Al-Sarawi, D. Abbott, *Nat. Electron.* **2020**, *3*, 81.
[32] R. Arppe, T. J. Sørensen, *Nat. Rev. Chem.* **2017**, *1*, 0031.
[33] B. D. Cullity, C. D. Graham, *Introduction to magnetic materials*, John Wiley & Sons, Hoboken, New Jersey, **2011**.
[34] Y. Liu, M. Jian, X. Liu, S. Peng, H. Li, L. Ding, H. Tian, T.-L. Ren, *Adv. Funct. Mater.* **2024**, *34*, 2304758.
[35] A. Vijayakumar, V. C. Patil, C. B. Prado, S. Kundu, in *2016 IEEE international symposium on hardware oriented security and trust (HOST)*. IEEE, **2016**, pp. 19–24.
[36] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Science* **2002**, *297*, 2026.
[37] D. Niarchos, *Sens. Actuators, A* **2003**, *109*, 166.

[38] C. Ó. Mathúna, N. Wang, S. Kulkarni, S. Roy, *IEEE Trans. Power Electron.* **2012**, *27*, 4799.
[39] N. P. De Leon, K. M. Itoh, D. Kim, K. K. Mehta, T. E. Northup, H. Paik, B. Palmer, N. Samarth, S. Sangtawesin, D. W. Steuerman, *Science* **2021**, *372*, eabb2823.
[40] S. Gider, B.-U. Runge, A. Marley, S. Parkin, *Science* **1998**, *281*, 797.
[41] D. L. Leslie-Pelecky, R. D. Rieke, *Chem. Mater.* **1996**, *8*, 1770.
[42] M. J. Adel, M. H. Rezayati, M. H. Moaiyeri, A. Amirany, K. Jafari, *Sci. Rep.* **2024**, *14*, 20649.
[43] R. S. Indeck, M. W. Muller, Method and apparatus for fingerprinting magnetic media, **1994**, US Patent 5,365,586.
[44] J. Kang, D. Han, K. Lee, S. Ko, D. Koh, C. Park, J. Ahn, M. Yu, M. Pakala, S. Noh, H. Lee, J. Kwon, K.-J. Kim, J. Park, S. Lee, J. Lee, B.-G. Park, *ACS Nano* **2024**, *18*, 12853.
[45] D. Koh, J. Kang, T. Kim, J. Lee, S. Noh, H. Lee, J. Kwon, S. Lee, J. Park, B.-G. Park, *Adv. Electron. Mater.* **2023**, *9*, 2201073.
[46] H. Chen, M. Song, Z. Guo, R. Li, Q. Zou, S. Luo, S. Zhang, Q. Luo, J. Hong, L. You, *Nano Lett.* **2018**, *18*, 117211.
[47] S. Lee, J. Kang, J.-M. Kim, N. Kim, D. Han, T. Lee, S. Ko, J. Yang, S. Lee, S. Lee, D. Koh, M.-G. Kang, J. Lee, S. Noh, H. Lee, J. Kwon, S.-h. C. Baek, K.-J. Kim, B.-G. Park, *Adv. Mater.* **2022**, *34*, 2203558.
[48] G. Finocchio, T. Moriyama, R. De Rose, G. Siracusano, M. Lanuzza, V. Puliafito, S. Chiappini, F. Crupi, Z. Zeng, T. Ono, M. Carpentieri, *J. Appl. Phys.* **2020**, *128*, 033904.
[49] J. Zhang, Z. Guo, S. Zhang, Z. Cao, R. Li, J. Cao, M. Song, M. Wan, J. Hong, L. You, *Appl. Phys. Lett.* **2020**, *116*, 19.
[50] J. K. Lee, Y. E. Kim, M. H. Lee, Y. K. Kim, *Small Struct.* **2025**, 2400527.
[51] C. Li, R. Xu, Y. Duan, X. Zhang, D. Zhu, A. Du, Z. Peng, S. Wang, K. Shi, W. Zhao, *Nanoscale* **2025**.
[52] T. Li, X. Guo, F. Müller, S. Abdulazhanov, X. Ma, H. Zhong, Y. Liu, V. Narayanan, H. Yang, K. Ni, T. Kämpfe, X. Li, *Nat. Commun.* **2025**, *16*, 189.
[53] R. A. John, N. Shah, S. K. Vishwanath, S. E. Ng, B. Febriansyah, M. Jagadeeswararao, C.-H. Chang, A. Basu, N. Mathews, *Nat. Commun.* **2021**, *12*, 3681.
[54] Y. Miao, X. Zhou, Z. Wang, X. Liu, Y. Yuan, Y. Jing, H. Luo, D. Zhang, J. Sun, *Adv. Funct. Mater.* **2024**, *34*, 2314883.
[55] C. Durniak, S. Foster, D. Bulla, *Sens. Actuators, A* **2025**, *383*, 116222.
[56] V. Milyutin, R. Bureš, M. Fáberová, *Condens. Matter* **2023**, *8*, 80.
[57] J. Atulasimha, A. B. Flatau, *Smart Mater. Struct.* **2011**, *20*, 043001.
[58] G. Liu, X. Dai, Z. Liu, J. Chen, G. Wu, *J. Appl. Phys.* **2006**, *99*, 9.
[59] M. Matyunina, D. Shishkin, L. Stashkova, M. Petrik, I. Razumov, M. Zagrebin, V. Sokolovskiy, V. Buchelnikov, Y. Gornostyrev, N. Ershov, *J. Magn. Magn. Mater.* **2024**, *610*, 172523.
[60] J. Zhou, J. You, K. Qiu, *J. Appl. Phys.* **2022**, *132*, 4.
[61] P. N. Hai, K. Takabayashi, K. Ejiri, M. Tanaka, *Appl. Phys. Lett.* **2025**, *126*, 16.
[62] C. Vargas-Estevez, A. Blanquer, P. Dulal, R. P. Del Real, M. Duch, E. Ibáñez, L. Barrios, G. Murillo, N. Torras, C. Nogués, B. J. H. Stadler, J. A. Plaza, J. Esteve, *Biomaterials* **2017**, *139*, 67.
[63] A. Hubert, R. Schäfer, Magnetic domains: the analysis of magnetic microstructures, Springer Science & Business Media, **1998**.
[64] A. Magni, G. Carlotti, A. Casiraghi, E. Darwin, G. Durin, L. H. Diez, B. Hickey, A. Huxtable, C. Hwang, G. Jakob, C. Kim, M. Kläui, J. Langer, C. H. Marrows, H. T. Nembach, D. Ravelosona, G. A. Riley, J. M. Shaw, V. Sokalski, S. Tacchi, M. Kuepferling, *IEEE Trans. Magn.* **2022**, *58*, 1.
[65] H. Guo, Y. Qin, Z. Wang, Y. Ma, H. Wen, Z. Li, Z. Ma, X. Li, J. Tang, J. Liu, *Adv. Funct. Mater.* **2024**, *34*, 2304648.
[66] M. D. L. Bruno, G. E. Lio, A. Ferraro, S. Nocentini, G. Papuzzo, A. Forestiero, G. Desiderio, M. P. De Santo, D. S. Wiersma, R. Caputo, G. Golemme, F. Riboli, R. C. Barberi, *ACS Appl. Mater. Interfaces* **2024**, *16*, 37063.
[67] A. Dodda, S. Subbulakshmi Radhakrishnan, T. F. Schranghamer, D. Buzzell, P. Sengupta, S. Das, *Nat. Electron.* **2021**, *4*, 364.
[68] K. Kursawe, A.-R. Sadeghi, D. Schellekens, B. Skoric, P. Tuyls, in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, **2009**, pp. 22–29.
[69] H. S. Yun, D. Wei, S. Yang, G. Park, M. S. Kim, T. J. Shin, D. M. Walba, M. J. Han, D. K. Yoon, *Adv. Mater.* **2025**, 2504288.
[70] G. Pradhan, F. Celegato, G. Barrera, E. S. Olivetti, M. Coisson, J. Hajduček, J. A. Arregi, L. Čelko, V. Uhlíř, P. Rizzi, P. Tiberto, *Sci. Rep.* **2022**, *12*, 17503.
[71] G. Pradhan, A. Magni, F. Celegato, M. Coisson, G. Barrera, L. Mikuličková, J. A. Arregi, L. Čelko, V. Uhlíř, P. Rizzi, P. Tiberto, *J. Sci. Adv. Mater. Devices* **2023**, *8*, 100608.
[72] G. Bertotti, *Hysteresis in Magnetism: For Physicists, Materials Scientists, and Engineers*, Academic Press series in electromagnetism. Elsevier Science, **1998**.
[73] R. P. Cowburn, D. Koltsov, A. Adeyeye, M. Welland, D. Tricker, *Phys. Rev. Lett.* **1999**, *83*, 1042.
[74] V. Krivokuca, S. Marcel, in *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*. **2018**, pp. 1–8.
[75] J. Daugman, *IEEE Trans. Circuits Syst. Video Technol.* **2004**, *14*, 21.
[76] J. G. Daugman, *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 400.
[77] G. E. Lio, S. Nocentini, L. Pattelli, E. Cara, D. S. Wiersma, U. Rührmair, F. Riboli, *Adv. Photonics Res.* **2022**, *4*, 2.
[78] J. Daugman, *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 400.
[79] J. Daugman, *Pattern Recognit.* **2003**, *36*, 279.
[80] J. W. Leem, M. S. Kim, S. H. Choi, S.-R. Kim, S.-W. Kim, Y. M. Song, R. J. Young, Y. L. Kim, *Nat. Commun.* **2020**, *11*, 328.