J Cryptogr Eng
DOI 10.1007/s13389-012-0041-3

REGULAR PAPER

Analysis and experimental evaluation of image-based PUFs

Saloomeh Shariati · François-Xavier Standaert · Laurent Jacques · Benoit Macq

Received: 7 May 2012 / Accepted: 19 August 2012

Abstract Physically unclonable functions (PUFs) are becoming popular tools for various applications, such as anti-counterfeiting schemes. The security of a PUF-based system relies on the properties of its underlying PUF. Usually, evaluating PUF properties is not simple as it involves assessing a physical phenomenon. A recent work (Armknecht et al. in A formalization of the security features of physical functions. In: IEEE Symposium on Security and Privacy, pp. 397–412, 2011) proposed a generic security framework of physical functions allowing a sound analysis of security properties of PUFs. In this paper, we specialize this generic framework to model a system based on a particular category of PUFs called image-based PUFs. These PUFs are based on random visual features of the physical objects. The model enables a systematic design of the system ingredients and allows for concrete evaluation of its security properties, namely robustness and physical unclonability which are required by anti-counterfeiting systems. As a practical example, the components of the model are instantiated by Laser-Written PUF, White Light Interferometry evaluation, two binary image hashing procedures namely, Random Binary Hashing and Gabor Binary Hashing, respectively, and code-offset fuzzy extraction. We experimentally evaluate security properties of this example for both image hashing methods. Our results show that, for this particular example, adaptive image hashing outperforms the non-adaptive one. The experiments also confirm the usefulness of the formalizations provided by Armknecht et al. (A formalization of the security features of physical functions. In: IEEE Symposium on Security and Privacy, pp. 397–412, 2011) to a practical example. In particular, the formalizations provide an asset for evaluating the concrete trade-off between robustness and physical unclonability. To the best of our knowledge, this experimental evaluation of explicit trade-off between robustness and physical unclonability has been performed for the first time in this paper.

Keywords Physical unclonable functions · Anti-counterfeiting · Image-based PUFs · Robustness · Physical unclonability

1 Introduction

The growing trade in counterfeit goods continues affecting the economy worldwide. Many ad-hoc methods have been proposed to avoid counterfeiting. Examples include so-called *overt* physical identifiers such as hologram and inks that visibly alter under light, or so-called *covert technology* such as invisible inks, proprietary photonic inks [2] and radio frequency identification (RFID) Tags [3]. Recently, Physically unclonable functions, or PUFs, have been introduced. Among many other applications, they are proposed as an effective tool for anti-counterfeiting systems. A physically unclonable function is a function that is embodied in a physical structure and is easy to evaluate but hard to clone. Early works that exploit the physical properties of random structures for authentication purposes date back to that in [4,5]. A formalization of this concept was introduced as physical one-way functions [6,7] or physical random functions [8] and finally physical(ly) unclonable functions, or PUFs. Examples of proposed PUFs are optical PUF [7], Coating PUF [9], Silicon PUF [8,10,11], SRAM PUF [12], Paper PUF [13–16], Laser-Written PUF [17], etc. For detailed description of various proposed PUFs, we refer to [18,19]. Generally, a

S. Shariati (✉) · F.-X. Standaert · L. Jacques · B. Macq
ICTEAM Institute, Université Catholique de Louvain,
Place du Levant 3, 1348 Louvain-la-Neuve, Belgium
e-mail: saloomeh.shariati@uclouvain.be

Published online: 23 September 2012

PUF interacts with stimuli (challenges) in an intricate way, and leads to unique and unpredictable responses. For anti-counterfeiting applications, the core concept of using PUF primitives is to rely on the unique physical properties which are hard to clone. The PUF can be either intrinsic in the product or extrinsic and glued to the object. The general idea is to digitally sign the product information (e.g., EPC code) together with the identifier extracted from the embedded PUF and use this signature as the certificate of authenticity. The verification of the authenticity is carried out by validating this certificate [20–24]. For more details on the design of anti-counterfeiting system based on image-based PUFs, we refer to [25].

Some PUFs like Coating PUFs, Silicon PUFs, SRAM PUF can be used beyond anti-counterfeiting application, e.g., key generation algorithms, or in the design of block ciphers [26–28].

The key properties of PUFs required by most security systems are *robustness* (reproducibility of responses to the same challenge), *unclonability*, and *unpredictability* (of PUF response for a new challenge). The evaluation of these properties, especially unclonability, is not trivial due to the fact that it relates to the physics and is technology dependent. Yet, for cryptographic applications, the security must be ensured through evaluation of formally defined security properties. The recent effort made by Armknecht et al. [1] provided a generic security framework that modularly captures the key properties of PUFs, i.e., robustness, unclonability and unpredictability, allowing a meaningful security analysis of PUF-based constructions.

In this paper, we investigate a particular category of PUFs hereafter called image-based PUFs. Image-based PUFs are based on random visual features of the physical objects which are assessed by imaging methods. By imaging, we mean any method that outputs images representing 2D or 3D profile of the physical object. It varies from the images taken with a simple digital camera or camera phone to those acquired with a very high resolution optical tomography device. The basic idea relies on the fact that imaging can be performed with a very high resolution such that the physical randomness is present on the outcome image. In this case, physically cloning the random profile yielding the same (or very similar) image is either impossible or requires a very high expense by a malicious party (counterfeiter). There are two reasons why we specialize in image-based PUFs. First, image-based PUFs are mainly targeted to anti-counterfeiting applications. Indeed, the input to the PUF is usually a fixed challenge and, therefore, a mathematical clone can be created by imitating the response of the PUF to this challenge.[1] Consequently, the unpredictability does not need to be studied and only minimum security properties, i.e., robustness and unclonability are considered. Second, the response of the PUF is a real-valued image and a specific processing (i.e., dimensionality reduction and binarization) needs to be designed and integrated into the cryptographic algorithms.

Several instances of image-based PUFs have been proposed. Paper PUF is an example, where the intrinsic random roughness of a paper (e.g., banknote, valuable document, prescription paper) is employed as its physical identifier [13,14]. Various methods have been proposed to evaluate paper random profile. Buchanan et al. propose to scan a focused laser beam across a sheet of white paper and continuously record the reflected intensity from different angles by means of photo detectors [14]. Clarkson et al. presented a low-cost evaluation of paper random profile using commodity scanners [15]. They acquire 3D profile of a paper using the scans taken from different orientations of the paper in the scanner. Another approach was introduced in [16] where the paper roughness is measured through its speckle pattern when illuminated with a coherent light source. Zhu et al. utilize random ink splatter occurring around any printed characters on a paper [29]. In [23,30,31], they propose adding extra randomness by pouring optical fibers on the production of papers and utilize the random distribution of fibers to construct the physical identifier of the paper. Phosphor PUF is also proposed by [3,32], where phosphor particles are blended with the material with the cover of the product, e.g., plastic cover to form the random pattern. Beekhof et al. utilize the images taken with a simple camera phone from random microstructures of various material surfaces such as metal surface (e.g., on the back of the watch), leather surface, etc. for identification purpose [33]. In [17], Laser-Written PUF has been proposed that utilizes the random profile of the laser marks embedded on the surface or bulk of the material. Optical PUF proposed by [7] can also be considered an image-based PUF, as its response is a speckle pattern represented by an image. We also see later that some image hashing procedures applied to optical PUFs such as Gabor Binary Hashing are also appropriate for most image-based PUFs. However, in this paper, as we believe that image-based PUFs are mostly suitable for anti-counterfeiting applications, we fix the challenge which is not usually the case for optical PUFs. In fact, the existence of large amount of unpredictable challenge response pairs allows for using optical PUFs for more advanced security applications such as remote authentication [20] or secret key generation [34].

The proposed procedures to deal with different image-based PUFs are very diverse. The characterizations of their security properties are also carried out using various approaches. In this paper, instead of introducing a new PUF or a new post-processing method, we establish a unified model to deal with most of existing and new image-based PUFs and describe a methodology to experimentally analyze their

[1] A mathematical procedure that yields the same challenge-response behavior as the PUF e.g., a fake image.

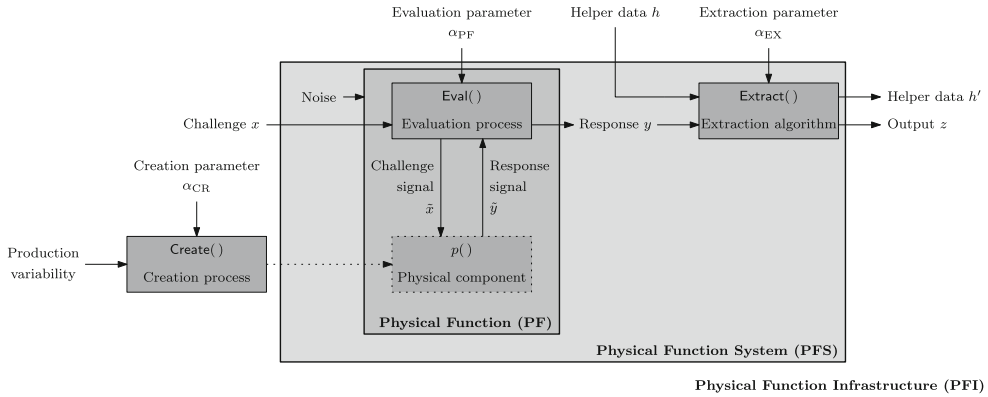


Fig. 1 Generic framework for physical functions [1]

security features. The contributions of this paper are thus threefold. First, we specialize the general framework of physical function from [1] to build the model of image-based physical function system with a particular focus on image hashing. Image-based physical function system consists of image-based PUF, evaluation procedure, image hashing and fuzzy extraction. Second, we present a practical example of image-based physical function system by instantiating its components by Laser-Written PUF, White Light Interferometry evaluation [17], two image hashing methods namely, Random Binary Hashing [35] and Gabor Binary Hashing [17,21], respectively, and code-offset fuzzy extraction [36,37]. Third, we provide a comprehensive experimental characterization of security properties of this practical example of image-based physical function system, i.e., robustness and physical unclonability. The experimental characterization of the explicit trade-off between robustness and physical unclonability is of main interest for anti-counterfeiting applications and has been carried out for the first time, to the best of our knowledge.

The paper is structured as follows. We start with summarizing the general model of physical functions [1] and the formalizations of security properties, i.e., robustness and physical unclonability in Sect. 2. In Sect. 3, we present the specialization of the general model to image-based physical function system and describe its ingredients. In Sect. 4, we instantiate the components of image-based physical function system. The security properties of this example of physical function system, i.e., robustness and physical unclonability are experimentally assessed in Sect. 5.

1.1 Conventions

Let A be a probabilistic procedure. Then, $y \leftarrow \mathsf{A}(x)$ refers to the event that on input x, procedure A outputs a value which equals y. Let A and B be some events, then $\Pr[A : B]$ denotes the conditional probability of A given B. The set $\mathcal{B}$ stands for the binary set $\{0, 1\}$. We denote with ϵ the empty string. The scalar product between two vectors $u, v \in \mathbb{R}^2$ reads $u \cdot v = u_1 v_1 + u_2 v_2$. The 1-bit quantization function $\mathrm{sign_b}$ is defined as $\mathrm{sign_b}(\lambda) = 1$ if $\lambda > 0$ and 0 else, and for $u \in \mathbb{R}^K$, $\mathrm{sign_b}(u) \in \mathcal{B}^K$ with $(\mathrm{sign_b}(u))_i = \mathrm{sign_b}(u_i)$ for $1 \leq i \leq K$. The Bernoulli random vector of size K with ± 1 entries is defined as $u \in \{-1, +1\}^K$ with $Pr[u_i = 1] = Pr[u_i = -1] = 0.5$ and $U = \mathrm{diag}\, u$ is the diagonal matrix such that $U_{ii} = u_i$. Let two vectors $u, v \in \mathbb{R}^K$, their Euclidean distance is denoted by $\mathrm{dist}(u, v) \triangleq \sqrt{\sum_{i=1}^{K} (u_i - v_i)^2}$ while their normalized angle distance reads $\mathrm{dist}_{\angle}(u, v) \triangleq \frac{1}{\pi} \arccos \sum_{i=1}^{K} \frac{u_i v_i}{\|u\| \|v\|} \in [0, 1]$ where $\|u\|$ denotes the ℓ_2-norm of vector i.e., $\|u\| = \sqrt{\sum_{i=1}^{K} |u_i|^2}$. For $s, t \in \mathcal{B}^K$, their Hamming distance is denoted by $\mathrm{dist_H}(s, t) \triangleq \sum_{i=1}^{K} s_i \oplus t_i \in [0, K]$.

2 Background

We briefly describe the generic framework of physical functions proposed by Armknecht et al. [1] which is specialized to image-based PUFs in the next section. This general framework, which is depicted in Fig. 1, shows modularly all components necessary for creating, evaluating and post-processing the output of a physical function.

In this section, we bring the formal definitions of the model components and security properties, i.e., robustness and physical unclonability.[2] They are used later to specify our image-based physical function system, and evaluate its security properties.

Creation process is usually performed by the manufacturer to produce a physical component and is defined as:

Definition 1 (*Creation Process* [1]) A creation process Create is a probabilistic procedure that, on input of a creation

[2] For detailed description of each component refer to [1].

parameter α_{CR}, produces a physical component p

$$p \leftarrow \mathsf{Create}(\alpha_{\mathrm{CR}}). \tag{1}$$

Creation process is a probabilistic procedure, because its output relates to some uncontrollable production variability (creation noise). As a practical example, consider an SRAM PUF [12]. The behavior of an SRAM PUF is based on the random power-up values of SRAM memory cells. The parameter α_{CR} of the SRAM PUF creation process includes the different design options for an SRAM cell and the controllable parameters of the CMOS production process.

A *Physical Function* (PF) consists of a *physical component* p which is evaluated by an *evaluation procedure* Eval with the evaluation parameter α_{PF}.

Definition 2 (*Physical Function* [1]) Given a physical component p and an evaluation parameter α_{PF}, a *physical function* P is a probabilistic procedure

$$\mathsf{P}_{p,\alpha_{\mathrm{PF}}} : \mathcal{X} \to \mathcal{Y}, \tag{2}$$

where $\mathcal{X}$ denotes the set of challenges (stimulating signals) and $\mathcal{Y}$ the set of responses. Internally, a PF is the combination of a physical component p and an evaluation procedure Eval, i.e.,

$$y \leftarrow \mathsf{P}_{p,\alpha_{\mathrm{PF}}}(x) = \mathsf{Eval}_p(\alpha_{\mathrm{PF}}, x). \tag{3}$$

In the case of SRAM PUF, the SRAM memory address range is considered as the challenge x to the PUF, and the power-up values of these cells are considered as the PUF response y [1]. The evaluation parameter α_{PF} describes the settings of the measurement process, e.g., typically the resolution of the analog-to-digital converter.

Physical Function is also a probabilistic procedure because on a single challenge, it may produce different outputs due to the uncontrollable random noise in the Evaluation procedure (evaluation noise). The essential assumption for all the PUF instances is that the creation noise (favorable noise) is higher than the evaluation noise (undesired noise). This stems from the fact that the evaluation process at the edge of technology is usually more accurate than the creation process.

To compensate the evaluation noise, a PF is usually combined with an extraction algorithm. The extraction algorithm maps slightly different responses y to the same challenge x to a unique output z according to some *extraction parameter* α_{EX} (e.g., number of output bits). The Extract algorithm can be executed in two different modes: *setup* and *reconstruction*. If a challenge x is requested for the first time, setup mode is used to generate an output z and some appropriate *helper data* h' (helping to compensate the noise). Later, when challenge x is requested again together with helper data $h = h'$, reconstruction mode is used to recreate z.

As explained above, a PF is usually coupled with an appropriate extraction algorithm. Their combination is considered as one single building block and is defined as:

Definition 3 (*Physical Function System* [1]) A *physical function system* S is a probabilistic procedure

$$\mathsf{S}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}} : \mathcal{X} \times (\mathcal{H} \cup \{\epsilon\}) \to \mathcal{Z} \times \mathcal{H}, \tag{4}$$

where $\mathcal{X}$ is the set of challenges, $\mathcal{H}$ the set of helper data values, ϵ the empty string, and $\mathcal{Z}$ the set of outputs.

Internally, a PF system is the combination of a physical function $\mathsf{P} = \mathsf{P}_{p,\alpha_{\mathrm{PF}}}$ (Definition 2) and an extraction algorithm Extract, i.e.,

$$\begin{aligned}(z, h') &\leftarrow \mathsf{S}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}}(x, h)\\ &= \mathsf{Extract}(\mathsf{P}_{p,\alpha_{\mathrm{PF}}}(x), h).\end{aligned} \tag{5}$$

If $h = \epsilon$, then Extract is executed in setup mode and generates a new helper data h'. In case $h \neq \epsilon$, Extract is executed in reconstruction mode and returns $h' = h$.

In the following, we omit the internal components and abbreviate $\mathsf{S} = \mathsf{S}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}}$.

The combination of all components described above is called a *Physical Function Infrastructure* (PFI) where the creation, evaluation and extraction parameters are fixed.

Definition 4 (*Physical Function Infrastructure* [1]) A *physical function infrastructure* $\mathcal{I}$ refers to a fixed creation process Create (Definition 1) and the set of all PF systems S (Definition 3), where the physical component p is the result of Create, i.e.,

$$\mathcal{I}_{\alpha_{\mathrm{CR}}} = \left(\mathsf{Create}, \left\{\mathsf{S}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}} : p \leftarrow \mathsf{Create}(\alpha_{\mathrm{CR}})\right\}\right), \tag{6}$$

where α_{CR}, α_{PF} and α_{EX} are fixed.

In the rest of this section, we bring the description and formal definitions of security properties of interest for image-based physical function system, i.e., robustness and physical unclonability.

2.1 Robustness

Robustness is evaluated by the probability to reconstruct the output of a PF system that has been produced in setup mode. Formally, it is defined as follows:

Definition 5 (*Robustness* [1]) Let S be a PF system (Definition 3) and let $x \in \mathcal{X}$ be a challenge. The *challenge robustness* of S w.r.t. x is defined as the probability

$$\begin{aligned}\rho_{\mathsf{S}}(x) := \Pr\big[&(z, h) \leftarrow \mathsf{S}(x, h) :\\ &(z, h) \leftarrow \mathsf{S}(x, \epsilon)\big].\end{aligned} \tag{7}$$

2.2 Physical unclonability

To define the property of Physical Unclonability, Arm-Knecht et al. first defined the notion of Physical Clone [1]. They consider clones on the physical level only and exclude

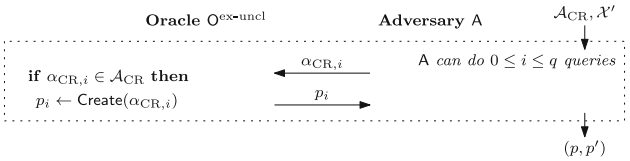


Fig. 2 Existential unclonability security experiment $\mathbf{Exper}_{\mathsf{A}}^{\text{ex-uncl}}(q)$

mathematical clones. This definition also suits for image-based PUFs which, as mentioned previously, are usually mathematically clonable.[3]

Definition 6 (*Physical Clone* [1]) Let $\mathcal{A}_{\text{CR}}$ be a set of creation parameters and let α_{PF} and α_{EX} be a fixed evaluation and extraction parameters, respectively. Moreover, let $\mathsf{S} = \mathsf{S}_{p,\alpha_{\text{PF}},\alpha_{\text{EX}}}$ and $\mathsf{S}' = \mathsf{S}_{p',\alpha_{\text{PF}},\alpha_{\text{EX}}}$ be two PF systems (Definition 3) that are identical except of their physical component, i.e., $p \neq p'$. Let $0 \le \delta \le 1$. We define that S' is a δ-*clone* of S w.r.t. $\mathcal{X}' \subseteq \mathcal{X}$ if for all $x \in \mathcal{X}'$ it holds that

$$\Pr\left[(z,h) \leftarrow \mathsf{S}'(x,h) : (z,h) \leftarrow \mathsf{S}(x,\epsilon)\right] \ge \delta \cdot \rho_{\mathsf{S}}(x). \tag{8}$$

For simplicity, we write $\mathsf{S}' \overset{\delta,\mathcal{X}'}{\equiv} \mathsf{S}$ if Eq. 8 holds.

The reason to integrate the notion of robustness $\rho_{\mathsf{S}}()$ into the definition of clones is that any PF system should be formally seen as a clone of itself. Therefore, the robustness marks a natural upper bound on "how similar a clone can become".

Cloning attacks might be of different types:

- *Selective cloning* refers to the event that for a *given* PF system S a clone S' is constructed.
- *Existential cloning* means that two arbitrary PF systems S and S' are produced, where one is the clone of the other.

For image-based PUFs, we investigate the existential physical unclonability as a worse case study.

Let us now bring the definition of existential unclonability, where the adversary A must produce two *arbitrary* clones. In this scenario, which is depicted in Fig. 2, the adversary A can make at most q queries to the Create process and ask for creation of physical components for the set of creation parameters $\alpha_{\text{CR}} \in \mathcal{A}_{\text{CR}}$ and challenges $\mathcal{X}' \subseteq \mathcal{X}$. Then, he outputs two arbitrary clones p, p'.

Definition 7 (*Existential Physical Unclonability* [1]) Let $\mathcal{A}_{\text{CR}}$ be a set of creation parameters and let α_{PF} and α_{EX} be fixed parameters for the evaluation and extraction procedures, respectively. Note that this implicitly defines a family $\mathcal{I}_{\mathcal{A}_{\text{CR}}} := \{\mathcal{I}_{\alpha_{\text{CR}}} : \alpha_{\text{CR}} \in \mathcal{A}_{\text{CR}}\}$ of PF infrastructures (Definition 4). A family of PF infrastructures $\mathcal{I}_{\mathcal{A}_{\text{CR}}}$ is called (γ, δ, q)- *cloning-resistant* w.r.t. $\mathcal{X}' \subseteq \mathcal{X}$, if

$$\begin{aligned}\Pr[\mathsf{S}'_{p',\alpha_{\text{PF}},\alpha_{\text{EX}}} &\overset{\delta,\mathcal{X}'}{\equiv} \mathsf{S}_{p,\alpha_{\text{PF}},\alpha_{\text{EX}}} : \\ &(p, p') \leftarrow \mathbf{Exper}_{\mathsf{A}}^{\text{ex-uncl}}(q); \\ &p \in [\mathsf{Create}(\alpha_{\text{CR}})]; \alpha_{\text{CR}} \in \mathcal{A}_{\text{CR}}; \\ &p' \in [\mathsf{Create}(\alpha'_{\text{CR}})]; \alpha'_{\text{CR}} \in \mathcal{A}_{\text{CR}}] \le \gamma.\end{aligned} \tag{9}$$

This means the probability that A generates, as output of the security experiment depicted in Fig. 2, two physical components p and p' which (1) imply δ-clones on the PF system level and (2) have been created using creation parameters $\alpha_{\text{CR}} \in \mathcal{A}_{\text{CR}}$ and $\alpha_{\text{CR}}{}' \in \mathcal{A}_{\text{CR}}$, is less than γ.

For practical (i.e., experimental) assessment of physical unclonability of image-based PUFs, we limit the adversary to do what an honest manufacturer can do by confining the possible creation parameters to that of the honest manufacturer ($\mathcal{A}_{\text{CR}} = \{\alpha_{\text{CR}}\}$). We argue that other scenarios are unlikely to happen. In other scenarios, the adversary tries different creation parameters which are either in the same range of accuracy as α_{CR} or more accurate (with the aid of a more powerful technology). We argue that the first case is expected not to trigger collisions with PUFs produced using α_{CR}.[4] The cost of second case is also expected to be prohibitive, as a classical property of physically unclonable functions.

3 Image-based physical function system

In this section, we specialize the generic model of physical functions (described in the above section) to image-based physical function systems.

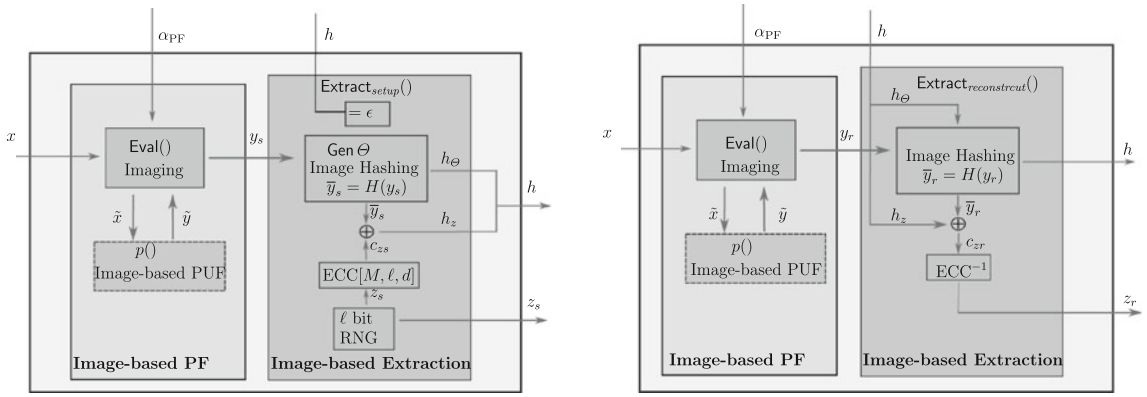
Image-based physical function systems include an Image-based physical function and an image-based Extraction including an image hashing and a typical *fuzzy extraction* [36,37]. Figure 3 illustrates an image-based physical function system in setup and reconstruction modes. For the sake of simplicity, the creation process Create is not included in the model. In the following, we describe the ingredients of the system in detail.

3.1 Image-based physical function

The physical component p (see Fig. 3) is a piece of a physical object containing random visual features. The challenge x is considered as the illumination used to take the images.

[3] Note that most PUFs are mathematically clonable when using a fixed challenge.

[4] Off course, the validity of this assumption should still be asserted by the system designer when selecting a specific PUF realization.



(a) Setup mode. **(b)** Reconstruction mode.

Fig. 3 An image-based physical function system

The illumination is characterized by the type of light, its frequency, orientation, distance from the source to the object etc. The response signal $\tilde{y}$ is the signal representing 2D or 3D profile of the physical component. The Eval procedure (e.g., typically an analog-to-digital converter or a digital camera) converts the response signal $\tilde{y}$ to a digitized response (image) y. Note that hereafter we use the notion y when referring to PUF response in general. It represents y_{s} in setup mode or y_{r} in reconstruction mode. The evaluation parameter α_{PF} describes the setting of the Eval procedure, e.g., typically the resolution of the imaging tool. In the rest of this paper, we assume only one fixed challenge because for the main target application, i.e., anti-counterfeiting, we do not need a function but just an output acting as the PUF identifier. As mentioned previously, the PUF output (identifier) together with the helper data and the product information can be digitally signed to form a signature which is further validated for authentication of the product.

We also assume a fixed transversal and longitudinal resolution of the Eval procedure such that the response of the PUF y is a vector $y \in \mathbb{R}^{N_1 \times N_2} = \mathbb{R}^N$ of $N = N_1 N_2$ samples (or pixels) each having a certain number of grayscale values.[5]

3.2 Image-based extraction

The extraction procedure Extract of an image-based PF system (hereafter called image-based extraction) includes an image hashing procedure combined with a fuzzy commitment scheme or code-offset fuzzy extraction algorithm [36,37]. However, the response of the image-based physical function is a real-valued image with a high dimension and the fuzzy extraction needs a binary string. So, we propose to integrate within the extraction scheme an image hashing procedure. It aims at reducing the dimension of the response and quantizing it into a limited length binary string while preserving the distinguishability of the image-based PUFs (further described in following). The code-offset fuzzy extraction algorithm is used to decrease the error rate of PF responses using Error Correcting Code (ECC) and code-offset construction.

3.2.1 Image hashing

Image hashing aims at reducing the dimension of the image $y \in \mathbb{R}^N$ and quantizing it into a binary string of fixed length $M \leq N$. In essence, it encompasses compression and quantization steps. Image hashing is thus defined as:

$$H : \mathbb{R}^N \to \mathcal{B}^M, \; y \mapsto \overline{y} = H(y) = \mathrm{sign}_{\mathrm{b}}(\Theta y), \tag{10}$$

where $y \in \mathbb{R}^N$ is the PF response (image), $\overline{y}$ is an M-bit hash, Θ is a $\mathbb{R}^{M \times N}$ matrix which is called sensing matrix and $\mathrm{sign}_{\mathrm{b}}$ is a 1-bit quantization function (see conventions). Hereafter, the hash $\overline{y} \in \mathcal{B}^M$ of the PF response is called the *fingerprint* of the image-based PUF because it represents the random pattern of the PUF as of biometric fingerprint.

It is required that the images from the observations of the same PUF give similar hash values, while images from different PUFs give different hash values with high probability.[6] This probability relates to both the distinguishability of PUF images and the employed image hashing. For a set of images from a specific image-based PUF, the distinguishability of the images can be determined with the distance (e.g., Euclidean norm) between images of different PUFs (inter-distance) and distance between different observations of the same PUF (intra-distance). The inter- and intra-distance characteristics are often used for an objective assessment of PUF properties in the literature [19]. They are usually summarized by

[5] Images are represented as vectors, e.g., by concatenating their rows.

[6] This contributes together with the fuzzy extraction to provide the same value for the same PUF and independent values for different PUFs.

providing histograms showing the occurrence of both distances over a number of different observations, and a number of different pairs of PUFs. The inter-distance qualitatively illustrates uniqueness of different PUF responses, while the intra-distance illustrates the observation noise. For a set of image-based PUFs where inter-distance histogram of the images does not significantly overlap with the intra-distance histogram,[7] image hashing just needs to reduce the dimension while preserving the distances between the images . Otherwise, image hashing also requires enhancing the distances towards less overlap between intra and inter-distances. For these two cases, we propose to use non-adaptive and adaptive image hashing, respectively.

Notice that based on the properties of the images provided for a specific image-based PUF, pre-processing can be performed as a first step of image hashing to reduce the observation noise such as misalignment, disorientation and ambient light change in order to enhance intra-distance distribution.

Here, using the theory of sparse signal representation [38], we briefly introduce the concept of adaptive and non-adaptive compressing of the image prior to the quantization. Next in the Sect. 4, we describe in detail the implementation of instantiations of non-adaptive and adaptive hashing methods, namely Random Binary Hashing and Gabor Binary Hashing, respectively.

In general, sparse representation of a signal means representing the signal with a linear combination of a small number of elementary signals called atoms (basis functions). The signal (image) $y = \sum_i \alpha_i \psi_i = \Psi\alpha$ is J-sparse in a certain basis (Fourier, Wavelet, Gabor, Curvelet, etc.), if there exists a representation of y using at most J significant (non-zero) coefficients [39].

Adaptive compressing of the signal accounts for a J-term approximation. It consists of the terms of α with the J largest magnitudes while setting all other terms to zero [40].

Non-adaptive compressing (known as Compressed Sensing) [41], [42] is based on the fact that a signal that is sparse in one basis can be represented non-adaptively from $M \geq \mathcal{O}(J \log N/J)$ linear projections onto a basis Φ that is incoherent with the sparsity basis Ψ.[8] Using this approach, the signal is approximated by $y_M = \Phi y$ where $\Phi = (\Phi_{ij}) \in \mathbb{R}^{M\times N}$ is incoherent with the sparsity basis Ψ. For instance, *random matrices* that are on average incoherent with most known basis functions have been used to perform non-adaptive compressing. The sparsity of the signal plays a significant role in how accurate it can be represented by both adaptive and non-adaptive approaches. In this view, we argue that both proposed methods are appropriate for image-based PUFs with so-called medium-entropy images. It means that while images contains random structures, they do not look completely random with each pixel having an *i.i.d* value. This is important since completely random images cannot usually be sparsified in any known sparsity bases. In this case, both adaptive and non-adaptive methods seem to fail. In practice, the condition of having medium-entropy images holds for most of existing image-based PUFs. Thus, we believe that adaptive and non-adaptive methods are efficient tools to hash the response of image-based PUFs.

In adaptive hashing, the sensing matrix Θ is selected adaptively based on the structure and content of the input image (by selecting the largest magnitude coefficients) while in the non-adaptive method the sensing matrix Θ is selected independently (e.g., randomly) from the image. The implementation of non-adaptive hashing is thus faster than adaptive hashing as the sensing matrix is selected without the need to first process the image. In Sect. 4.2 and 4.3, we describe the instantiations of non-adaptive and adaptive image hashing methods, namely Random Binary Hashing and Gabor Binary Hashing, respectively. In Sect. 5, we compare their results in terms of robustness and physical unclonability. The exact assessment of their computational complexity is out of the scope of this paper.

3.2.2 Fuzzy extraction

For extraction algorithm described in Sect. 2, there exist numerous methods. The general option is to use a *fuzzy extraction* algorithm. In this paper, we have used a fuzzy commitment scheme proposed by Juels and Wattenberg [36] that is equivalent to the code-offset fuzzy extraction algorithm described by Dodis et al. [37].[9] In code-offset fuzzy extraction (or fuzzy commitment scheme), the helper data are constructed as a codeword from a selected error-correcting code, used to encode a chosen output, masked with the PUF response observed during setup phase. The helper data together with the PUF response observed during reconstruction phase are mapped to a codeword which is decoded to the same output chosen in setup phase, if the error between PUF responses is less than error correction capability. The main motivation of using code-offset fuzzy extraction scheme for image-based PUFs is to produce reproducible (error-free) outputs in setup and reconstruction phases. This brings up the opportunity to use image-based PF system for more advanced security constructions (i.e., anti-counterfeiting systems). For instance, for an anti-counterfeiting system based on digital signa-

[7] The overlap between distributions can be inspected visually or by means of more precise measures e.g., Kullback-Leibler divergence between two distributions.

[8] Roughly speaking, incoherence means that no element of one basis has a sparse representation in terms of the other basis.

[9] Although, according to [37], more precise name for this scheme would be code-offset secure sketch, we prefer to be consistent with more commonly used term in literature.

ture scheme (described previously), the verification works properly only if the output obtained in reconstruction phase perfectly matches the one produced in setup phase. We believe that code offset fuzzy extraction or fuzzy commitment scheme is a good choice to extract reproducible outputs from image-based PUF. The main reason is that it is convenient and easy to implement using standard error-correcting codes. It is also a popular technique for extracting identifiers from biometrics [43]. By merging image hashing and above code-offset fuzzy extraction, the pipeline of image-based Extraction in the setup and reconstruction steps is as follows:

In the **setup phase**, PF response (image) y_s is sensed by a system modeled by a sensing matrix Θ, i.e., Θy_s is measured and then quantized into the M bit string fingerprint $\overline{y}_s \in \mathcal{B}^M$. The sensing matrix Θ is encoded to h_Θ as the first part of *helper data* that supports the recreation of the same hashed value in reconstruction phase. Note that Θ is a mathematical object and h_Θ is the minimal amount of information that is enough to represent Θ. For example for a random matrix Θ, the seed of its pseudorandom generation can serve as h_Θ. Directly correcting the noisy fingerprint is not possible since this is typically not a noisy version of a code-word but an arbitrary noisy vector.

A relatively simple but powerful construction to decode arbitrary words is the code-offset method. Using code-offset method, we transform the fingerprint $\overline{y}_s \in \mathcal{B}^M$ into a random code-word of a predefined error correcting code $c_{z_s} \in \mathcal{B}^M$. For that, a randomly chosen string $z_s \in \mathcal{B}^\ell$ with $\ell < M$ is encoded to a random code-word $c_{z_s} \in \mathcal{B}^M$ using a ECC(M, ℓ, d) which transforms $z_s \in \mathcal{B}^\ell$ to the code-words $c_{z_s} \in \mathcal{B}^M$. The redundancy added to the input by transforming it into a larger code-word enables using a suitable decoding algorithm to detect and correct up to $t = \lfloor (d-1)/2 \rfloor$ errors in the code-word [44]. The offset between $\overline{y}_s$ and c_{z_s} constitutes the second part of helper data $h_z = \overline{y}_s \oplus c_{z_s} \in \mathcal{B}^M$ where $\oplus$ denotes the bitwise exclusive or. Randomly chosen string $z_s \in \mathcal{B}^\ell$ is the output of the PF system that can be considered as the identifier of the image-based PUF. The second part of helper data supports the recreation of the same output in reconstruction phase and also allows binding the randomly chosen output (identifier) $z_s \in \mathcal{B}^\ell$ to the PUF response. The helper data $h = \{h_\Theta, h_z\}$ is stored to be further used in reconstruction phase.

In the **reconstruction phase**, the same hashing is applied to the noisy version of the PF response (image) y_r using the sensing matrix specified by the first part of helper data h_Θ to construct $\overline{y}_r$. Then, the transformation maps the noisy version of the fingerprint $\overline{y}_r$ to a noisy version of the code-word using the second part of helper data h_z such that $c_{z_r} = \overline{y}_r \oplus h_z$. The noisy code-word c_{z_r} can be decoded to the correct code-word c_{z_s} if the Hamming distance between $\overline{y}_s$ and $\overline{y}_r$ is smaller than the error correcting capability t. The output z_s can now be recovered by decoding the corrected code-word c_{z_s}. If dist$(\overline{y}_s, \overline{y}_r) > t$, then no guarantee is provided about the output of reconstruction phase [37].

In the next section, we instantiate image-based Physical Function and Image hashing procedure described in the above scheme.

4 Instantiations

4.1 Instantiation of physical function : Laser-Written PUF and WLI evaluation

We instantiate image-based physical function by Laser-Written PUF and White Light Interferometry evaluation procedure proposed in [17]. Laser-Written PUF (LPUF) is based on the 3D profile of laser mark(s) engraved on the surface or volume of a physical object. The randomness of the laser mark mainly stems from the laser beam instability and random characteristics of the object material. LPUF is a good instance of image-based PUFs to be employed for anti-counterfeiting purposes. Indeed, it can be engraved in several objects with various materials, it can be very small and it cannot be removed and copied into other objects without a considerable damage to the quality of the object (e.g., consider laser marks in the gemstones). It is also very robust against aging, especially when embedded on the bulk of the object.

The creation process Create of LPUF (see Fig. 1) includes engraving laser mark(s) on the surface or volume of a physical object. The creation parameter α_{CR} includes, among others, the controllable specifications of the laser engraving like laser beam frequency, diameter, etc. The physical component p is the laser mark containing random features. The randomness relates to the creation parameter and the uncontrollable engraving variability due to both laser beam instability and random density of the object material. Figure 4a illustrates a typical creation process of LPUF from transversal view. Assuming two dotted arrows as hypothetical transversal axes, laser beam instability is illustrated by a random-shape curve. Density randomness of the object material is also shown as the second source of randomness. The evaluation process Eval has been performed by White Light Interferometry (WLI) imaging. The challenge x is fixed to a simple white light used in WLI method and the response signal $\tilde{y}$ is the phase of reflected beam from the object surface that is then converted to the digital image y. The evaluation parameter α_{PF} includes the nanometer depth resolution and sub-micrometer traverse resolution which are lfixed by design. The typical response (digital image) y of the WLI evaluation process for two different laser marks engraved on the glass substrate is shown in Fig. 4b.

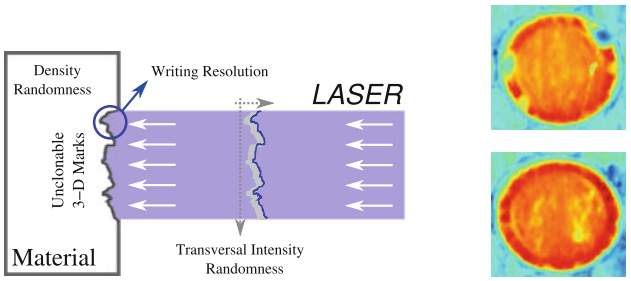


Fig. 4 **a** Laser engraving principle. **b** Two laser depth profiles [17]

4.2 Instantiation of non-adaptive image hashing: random binary hashing

Non-adaptive image hashing is instantiated by Random Binary Hashing based on [35]. Non-adaptive compressing (dimensionality reduction) in Random Binary Hashing is achieved by sensing the image with a random matrix $\Phi = (\Phi_{ij}) \in \mathbb{R}^{M\times N}$ such as Gaussian random matrix $\Phi_{ij} \sim_{\text{iid}} \mathcal{N}(0, 1/M)$ or uniformly distributed random matrix $\Phi_{ij} \sim_{\text{iid}} \pm 1/\sqrt{M}$, and many other sub-Gaussian distributions [45].[10] As discussed previously, the random matrix is incoherent with most known basis functions and can be efficiently applied for non-adaptive compressing. This random matrix is used as the sensing matrix Θ (See Eq. 10) for the image hashing. Random Binary Hashing H_{R} is thus defined by:

$$H_{\text{R}} : \mathbb{R}^N \to \mathcal{B}^M,\ y \mapsto \overline{y_R} = H_{\text{R}}(y) = \text{sign}_{\text{b}}(\Theta_R y), \quad (11)$$

where the sensing matrix Θ_R is a random matrix Φ. This nonlinear mapping (after one-bit quantization) satisfies a certain measure concentration with respect to the normalized angle distance (see conventions) between two distinct images and the normalized Hamming distance of their binary hashes. Indeed, for Gaussian random matrix Φ and for any $y, w \in \mathbb{R}^N$ and $\beta > 0$,

$$\Pr\left[\left|\frac{1}{M}\text{dist}_{\text{H}}(\overline{y}, \overline{w}) - \text{dist}_{\angle}(y, w)\right| \geq \beta\right] \leq 2\, e^{-2\beta^2 M} \quad (12)$$

The proof is given in [35,46]. So, Random Binary Hashing H_{R} reduces the dimension while preserving the distances (as measured by angle) between the images. Recently, it has been shown in [47] that $\frac{1}{M}\text{dist}_{\text{H}}(\overline{y}, \overline{w})$ is as close as desired to $\text{dist}_{\angle}(y, w)$ with high probability for all $y, w \in \mathbb{R}^N$ that are J-sparse or compressible in a certain basis (Fourier, Wavelet, etc.) for $M = \mathcal{O}(\beta^{-2} J \log(N/J))$. They also investigate the resistance of binary random hashing in the presence of the observation noise. They show that for a Gaussian observation noise $n_o \sim_{\text{iid}} \mathcal{N}(0, \sigma_o^2)$, the Hamming distance between the hash values of different observations of the same PUF is bounded by $\text{dist}_{\angle}(\overline{y}_{\text{s}}, \overline{y}_{\text{r}}) \leq C\sigma_o$ with a constant C. This property (resistance of hashing against observation noise) is confirmed in our experiments.

Random Binary Hashing offers a fast and efficient hashing of the images and an effective constitution of helper data that is independent of the images. Another interesting advantage of Random Binary Hashing is that it can be integrated in the imaging hardware [48]. It makes the implementation of the algorithm quite fast and easy.

4.3 Instantiation of adaptive image hashing: Gabor binary hashing

In Gabor Binary Hashing, adaptive compressing relies on the use of 2-D Gabor basis functions as the sparsity basis. Olshausen et al. [49] have shown that a learning algorithm that attempts to find sparse linear representation for natural scenes will develop a complete family of spatially localized, oriented, bandpass (selective to structures at different spatial scales) basis functions, similar to Gabor basis functions. So, Gabor-based representation seems to be a close to optimal choice for sparse representation of images in general and the image-based PUFs in particular.

Gabor Binary Hashing presented in following is very similar to an existing Gabor-based hashing used to process optical PUF speckle pattern [21,26]. Our contribution is to embed this method in the adaptive hashing model described previously. This facilitates extension of adaptive hashing method for other sparsity basis (Fourier, Wavelet, Curvelet, etc.) [39] when necessary.

Gabor basis functions $g_\psi(b) \in \mathbb{R}$ are defined as:

$$g_\psi(b) = \frac{1}{a\sqrt{2\pi}}\ \sin(v \cdot (b-k)) \exp(-\tfrac{1}{4a^2}\|b-k\|^2), \quad (13)$$

where '$\cdot$' denotes the scalar product between two vectors (see conventions), $b = (b_1, b_2) \in \mathbb{R}^2$ and the basis functions are parameterized by $\psi = (a, v, k) \in \mathbb{R}_+ \times \mathbb{R}^2 \times \mathbb{R}^2$. The basis function $g_\psi(b)$ is the product of a plane wave with wave vector $v \in \mathbb{R}^2$ and a Gaussian signal with variance (or *scale*) $a \in \mathbb{R}_+$ centered on $k = (k_1, k_2) \in \mathbb{R}^2$. For the PUF response $y \in \mathbb{R}^N$ (which is a discrete signal represented in one dimension), Gabor coefficients can be obtained by projecting y on the Gabor basis functions as follows:

$$\langle g_\psi, y\rangle = \sum_{i=1}^{N} g_{\psi_i} y_i \cong G_\psi^T y, \quad (14)$$

where each column of G_ψ^T is a basis function g_{ψ_i}. In this view, Gabor coefficients are calculated by the matrix multiplication of the Gabor atoms by y.

[10] i.i.d stands for Independent and Identically Distributed random variable.

In our experiments, we restrict ψ to a finite set of values $\Psi(a, \nu_0, \Delta) \subset \mathbb{R}_+ \times \mathbb{R}^2 \times \mathbb{R}^2$ defined as:

$$\begin{aligned}\Psi(a, \nu_0, \Delta) = \big\{ & (a, \nu_f, k_m) : \\ & \nu_f = \nu_0(\sin\theta_f, \cos\theta_f),\ \theta_f = 2\pi f/F,\ 0 \le f < F, \\ & k_m = (m_1\Delta, m_2\Delta),\ 0 \le m_i < \lfloor N_i/\Delta \rfloor, i \in \{1, 2\}\big\}.\end{aligned} \tag{15}$$

The size of $\Psi(a, \nu_0, \Delta)$ is $\#\Psi(a, \nu_0, \Delta) = F\lfloor N_1/\Delta \rfloor \lfloor N_2/\Delta \rfloor$, and it induces the coefficient set $\mathcal{G}_{a,\nu_0,\Delta} = \{G_\psi^T y : \psi \in \Psi(a, \nu_0, \delta)\}$ of the same size.

Let $\psi^{(i)}$ be the parameter vector pointing out the ith strongest value[11] of $\mathcal{G}_{a,\nu_0,\Delta}$ and let $\Theta_G = [G_{\psi^{(1)}}, G_{\psi^{(2)}}, \ldots, G_{\psi^{(M)}}]^T$ be the Gabor basis functions (atoms) providing the largest Gabor coefficients when applied to the image. These Gabor atoms are used as the sensing matrix Θ (See Eq. 10) for the image hashing. Gabor Binary Hashing H_G is thus defined by:

$$H_G : \mathbb{R}^N \to \mathcal{B}^M,\ y \mapsto \overline{y_G} = H_G(y) = \mathrm{sign}_b(\Theta_G y). \tag{16}$$

The parameter vector $\psi_M = \{\psi^{(1)}, \ldots, \psi^{(M)}\}$ (the positions of the most robust components) constitutes the first part of the *helper data*.

As discussed earlier, for a set of PUFs where the images inter-distance significantly overlaps their intra-distance, image hashing requires enhancing the distance distributions. Gabor Binary hashing can achieve that by reducing the effect of noise in the hashed value, by adaptively selecting a sensing matrix of robust atoms.

5 Experimental results and analysis

We evaluate robustness and existential physical unclonability of the example of image-based physical function system described in the previous section. Hereafter, image-based Extraction using Random Binary Hashing and Gabor Binary Hashing methods are called Random-based-extraction (RbEX) and Gabor-based extraction (GbEX), respectively.

5.1 Experimental settings of image-based physical function

We analyze implementation settings of the image-based physical function described in Sect. 4.1. For this purpose, we first describe the creation process of the physical component. Laser marks are engraved by focusing the beam of an excimer laser on a glass substrate. The laser wavelength is 193 nm, its power is 130 mW and its frequency is 200 Hz. Three laser shots are used to create laser marks. The imprinted pattern is a 100×100 matrix of 60 μm diameter laser marks. The mean ablation depth is 350 nm. The evaluation of the LPUF profile has been carried out by means of a White Light Interferometry method implemented with a Mirau interferometer [50,51]. The light source is a 4 mW LED with wavelength 638 nm. The interference pattern is imaged on a CCD camera which is then used to obtain the topography of the laser profile. Using this method, we achieve a sub micron traverse resolution and a nanometer longitudinal resolution.

5.2 Preliminary analysis of the datasets

For experimental analysis, the datasets of images are built using the evaluations of some randomly selected laser marks from 100×100 matrix of marks described above. Two datasets of Laser-Written PUFs named $\mathcal{D}_1$ and $\mathcal{D}_2$ are constructed to evaluate robustness and physical unclonability, respectively. The first dataset $\mathcal{D}_1 = \{y_{rq},\ 1 \le r \le R,\ 1 \le q \le Q\} \subset \mathbb{R}^N$ contains $R = 20$ different LPUFs of $N = 115{,}600$ pixels ($N = N_1 N_2 = 340 \times 340$) observed $Q = 60$ times. The second dataset $\mathcal{D}_2 = \{y_r,\ 1 \le r \le R\} \subset \mathbb{R}^N$ contains $R = 1{,}000$ different LPUFs of $N = 115{,}600$ pixels observed once. Each image has been first pre-processed to reduce the observation noise due to misalignment and ambient light change. In pre-processing, we first apply mean normalization to compensate measurement noise due to ambient light change. Then, a morphological noise removal is applied consisting of area *opening* to remove the light structures with size smaller than a certain threshold and area *closing* which has the same effect on dark structures [52,53]. Finally, the objects inside the image are recognized and the one with the size similar to that of laser mark is selected. In this way, we locate the framed region of LPUF inside the image and use this framed region as the pre-processed PF response (y in the datasets).

We begin with evaluating the distinguishability of LPUF images by exploring the Euclidean distance between images from different observations of the same PUF (intra-distance) and images of different PUFs (inter-distance) using datasets of $\mathcal{D}_1$ and $\mathcal{D}_2$, respectively. Intra and inter-class Euclidean distances between PUF images are calculated by:

$$\begin{aligned}D_{\text{intra}} = \big\{ & \mathrm{dist}(y_{rq}, y_{rq'}) : \\ & y_{rq}, y_{rq'} \in \mathcal{D}_1, 1 \le r \le R,\ 1 \le q, q' \le Q, q \ne q'\big\}\end{aligned} \tag{17}$$

and,

$$\begin{aligned}D_{\text{inter}} = \big\{ & \mathrm{dist}(y_r, y_{r'}) : \\ & y_r, y_{r'} \in \mathcal{D}_2,\ 1 \le r, r' \le R, , r \ne r'\big\}.\end{aligned} \tag{18}$$

Figure 5 illustrates the normalized histograms of intra and inter-class Euclidean distances using Eq. 17 and Eq. 18, respectively.[12] The number of comparisons made to estimate

[11] In absolute value sense.

[12] Whereby the counts are replaced by the normalized counts such that the maximum frequency equals 1.

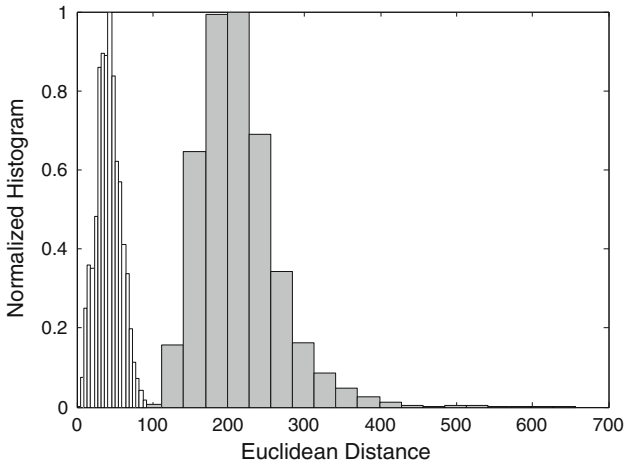


Fig. 5 Histogram of intra-class (*white*) and inter-class (*gray*) Euclidean distances between LPUF images

histograms is thus $20\binom{60}{2} = 35{,}400$ for intra-distance and $\binom{1{,}000}{2} = 499{,}500$ for inter-distance. The statistical mean and standard deviations of intra and inter-class Euclidean distances are obtained as $(\mu_{\text{intra}}, \sigma_{\text{intra}}) = (41.71, 16.02)$ and $(\mu_{\text{inter}}, \sigma_{\text{inter}}) = (212.82, 52.11)$, respectively. This preliminary analysis of the Euclidean distances between PUF images gives the intuition about the observation noise and uniqueness of original images of the datasets. We visually observe that inter-distance histogram of the images does not significantly overlap with the intra-distance histogram. Therefore, as described in Sect. 3.2.1, we predict that both adaptive and non-adaptive image hashing will provide reasonable results. So, we apply both RbEX and GbEX and compare their results in terms of robustness and physical unclonability.

5.3 Experimental settings of image-based extraction

We now describe the implementation settings of the image-based Extraction described in Sect. 4.

Random Binary Hashing is realized with another random matrix construction [54,55] than Gaussian random matrix (described in Sect. 4.2) in order to further accelerating the hashing process. Later on this section, we show that this method roughly behaves like applying Gaussian random matrix. First, the images are deliberately spread in the frequency domain. This is carried out by simply multiplying the image y by a random matrix $U = \operatorname{diag} u$ where $u \in \{-1, +1\}^N$ is a Bernoulli random vector of size N. Then, the sensing matrix Θ_R of Eq. 11 corresponds to picking uniformly random M "frequencies" in a Fourier transform of $Uy \in \mathbb{R}^N$ i.e., $\Theta_R = S\mathcal{F}U$ where S is the selection matrix, $\mathcal{F}$ is the discrete Fourier matrix and U is the random matrix described above. The effect of the spread spectrum sequence U is to spread the frequency response of $y \in \mathbb{R}^N$ so that the Fourier Transform of $Ux \in \mathbb{R}^N$ is flat on average and picking random frequencies leads to a fair random selection. In other words, all the measurements per frequency are meaningful and they do not fall in a possible gap (with no frequency content) of the spectrum of $y \in \mathbb{R}^N$. It has been shown in [55] that under the condition $M \geq \mathcal{O}(J \log N/J)$, which holds in our case, the described spread spectrum method behaves like applying a full Gaussian random matrix (described in Sect. 4.2). We have also experimentally observed that the histogram of $\Theta_R y$ components follows a Gaussian distribution. This method induces both a fast evaluation of $\overline{y} \in \mathbb{R}^M$ from $y \in \mathbb{R}^N$ in $O(N \log N)$ computations (compared to $O(MN)$ for hashing using Gaussian random matrix) and a reproducibility of Θ_R by recording in h_Θ the M selected frequencies or alternatively the seed of their pseudorandom selection.

Gabor Binary Hashing has been achieved by restricting the parameter vector ψ of the Gabor basis functions to the finite set of values as described in Eq. 15. We set Gabor parameters to $\nu_0 = \pi/3$, $F = 4$ (four orientations), $m_1 = m_2$, $a = 10$ (Gaussian scale) and $\Delta = 30$ (square grid size to apply the filter), respectively. These parameters are obtained experimentally providing sub-optimal yet sufficiently good results.[13] The size of Gabor coefficients set is, therefore, $\#\mathcal{G}_{a,\nu_0,\Delta} = F\lfloor N_1/\Delta \rfloor \lfloor N_2/\Delta \rfloor = 4\lfloor 340/30 \rfloor^2 = 484$. The sensing matrix of $M < 484$ most robust Gabor atoms Θ_G is then constructed and applied to the images using Eq. 16.

Error correcting code of code-offset Fuzzy Extraction algorithm is realized using BCH (M, ℓ, d) code which can correct up to $t = \lfloor (d-1)/2 \rfloor$ errors in the code-words (fingerprints). The code-word size, M must have the form $2^k - 1$ for some integer k.

5.4 Robustness

Robustness of a physical function system (defined in Definition 5) expresses the probability that an output generated in reconstruction stage matches the value generated in setup phase. We evaluate the robustness of the example of image-based physical function system using dataset $\mathcal{D}_1$ of LPUFs by applying both extraction methods RbEX and GbEX.
The robustness has been assessed using two approaches.

In the first approach, the robustness is evaluated by the probability that the Hamming distance between fingerprints of the same PUF in setup and reconstruction phases is less than the error correction capability, hence enabling the ECC to map them to the same output. Let $\Delta_e = \text{dist}_\text{H}(\overline{y}_\text{s}, \overline{y}_\text{r})$ be the Hamming distance between the fingerprints $\overline{y}_\text{s}$ and $\overline{y}_\text{r}$ of the same PUF in setup and reconstruction phase, respectively. Knowing that the helper data generated in setup phase is

[13] As parsing all different combinations of parameters is combinatorially complex, we adjust the parameters by experimentally tuning them to get our results.

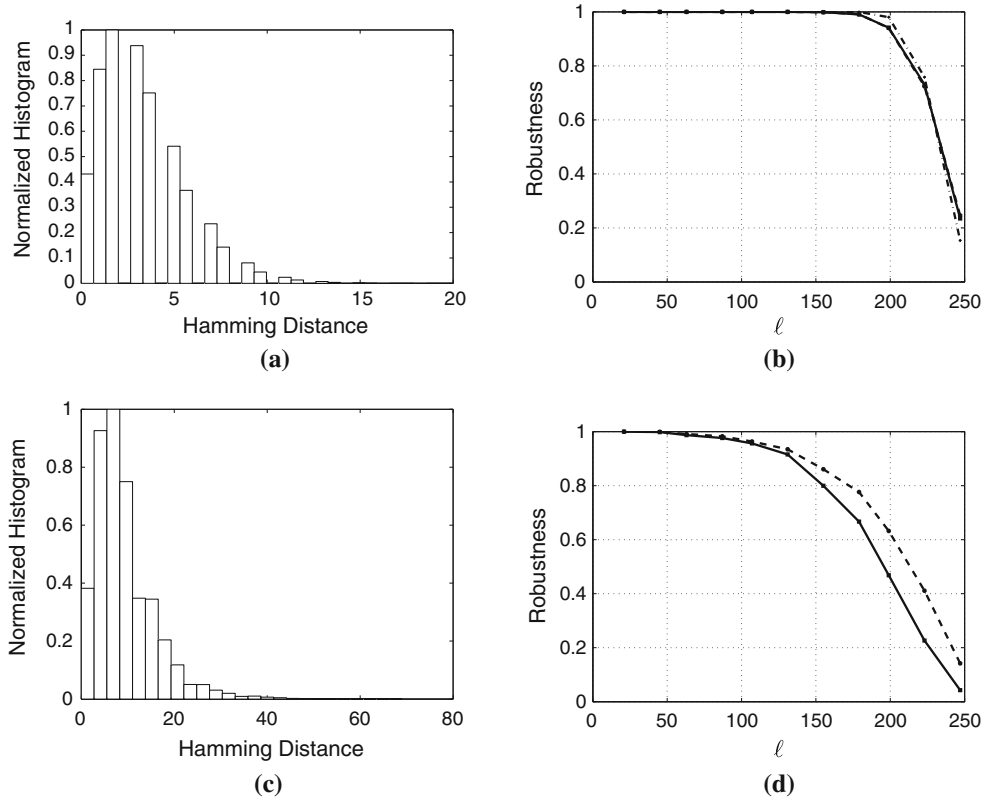


Fig. 6 Histogram of intra-class Hamming distance between fingerprints of the same PUF Δ_e and Robustness versus output length ℓ by (*plain*) $\Pr[\Delta_e \leq t]$ and (*dashed*) $\Pr[z_r = z_s]$ for RbEX (**a**, **b**) and GbEX (**c**, **d**), respectively

used in reconstruction phase, the robustness of Definition 5 is estimated by:

$$\rho_S = \Pr[\Delta_e \leq t] \tag{19}$$

In the second approach, we estimate the robustness directly on the output values z. For the same PUF, knowing that the helper data generated in set-up phase is used in reconstruction phase, the robustness of Definition 5 is estimated from the probability of having the same output in set-up and reconstruction phases as follows:

$$\rho_S = \Pr[z_r = z_s]. \tag{20}$$

For both approaches, we obtain the robustness by applying different error correction capabilities. For this purpose, we use a BCH (M, ℓ, d) code, we fix the parameter $M = 255$ and find the robustness for a selection of possible pairs of ℓ, t where $t = \lfloor (d-1)/2 \rfloor$. The robustness is then plotted versus ℓ.[14]

We provide a fair statistical estimation of robustness for both approaches as follows. Given the dataset $\mathcal{D}_1$ of Q observations of R PUFs, for each PUF, one observation of the PUF is used in set-up phase y_s to produce fingerprint $\overline{y}_s$, helper data h and output z_s. The remaining $(Q-1)$ observations together with helper data h are used in reconstruction phase that generates the new fingerprint $\overline{y}_r$ and output z_r for each observation. This is repeated Q times until each observation is used once in set-up phase.

For the first approach, the histogram of $\Delta_e = \text{dist}_H(\overline{y}_s, \overline{y}_r)$ is estimated from above iterations (between any pair of observations of the same PUF). The size of discrete intervals (bins) to estimate the histogram is selected according to the Scotts rule. It states that bin size $h = 3.5\sigma/n^{1/3}$ is optimal for random samples of normally distributed data where σ and n are the standard deviation and size of the sample data, respectively [56]. Then $\Pr[\Delta_e \leq t]$ is estimated from the cumulative distribution function using histogram of Δ_e estimated as stated above. For the second approach, the probability of $\Pr[z_r = z_s]$ is directly estimated from the same iterations as above.

The histograms of Δ_e for both extraction methods RbEX and GbEX are shown in Fig. 6a, c, respectively. Figure 6b, d shows the robustness versus output length ℓ for both extraction methods RbEX and GbEX, respectively. The plain curve corresponds to the robustness estimated with the first approach $\Pr[\Delta_e \leq t]$ and the dashed curve corresponds to the robustness estimated with the second approach $\Pr[z_r = z_s]$. We see that increasing ℓ results in decreasing robustness. The reason is that increasing ℓ means decreasing error correction

[14] The reason to select $M = 255$ will be justified later in in this section.

capability t and thus reduced robustness. We also observe that the probability $\Pr[z_r = z_s]$ is higher than $\Pr[\Delta_e \leq t]$. This holds because there may exist some occurrence of $z_r = z_s$ although $\text{dist}_H(\overline{y}_s, \overline{y}_r) > t$, since ECC may provide the same output in reconstruction phase even if there exist more than t errors between the code-words as described in Sect. 3.2. The occurrence of dashed curve going below plain curve is probably due to the distortion caused by the histogram binning in the first approach.

Because of the low level of noise in PUF images of our particular dataset (as depicted in intra-class distance in Fig. 5), we observe that both non-adaptive and adaptive methods provide good robustness for some values of output length ℓ. We even see that non-adaptive RbEX outperforms adaptive GbEX because it provides better robustness for larger range of output length ($\ell < 150$). However, it remains to evaluate the physical unclonability to fairly compare these two methods.

5.5 Physical unclonability

As discussed previously, we confine the adversary tools to those of honest manufacturer. In this view, we assess the existential cloning-resistance of LPUFs by finding the probability that an honest manufacturer produced two clones by accident. In order to calculate the probability of this event, we first evaluate the probability of a particular creation event (where the "clones" are created according to Eq. 9) and determine to what extent this creation event produces a pair of clones according to Definition 6.

We also calculate the physical unclonability using two approaches. In the first approach, we use the Hamming distances between fingerprints values in set-up and reconstruction phases. Let $\Delta_{cl} = \text{dist}_H(\overline{y}_s, \overline{y}'_r)$ be the Hamming distance between fingerprints $\overline{y}_s$ and $\overline{y}'_r$ of two different PUFs generated in set-up and reconstruction phases, respectively, using the same helper data. We start by considering the event $\Delta_{cl} \leq \Delta_{\max}$ where $\Delta_{\max}$ is an arbitrary integer value $0 \leq \Delta_{\max} \leq M$. Practically, $Pr[\Delta_{cl} \leq \Delta_{\max}]$ can be computed using the histogram of Δ_{cl}. This provides, therefore, a minimum value of γ according to Eq. 9 i.e.,

$$\gamma_{\min} = Pr[\Delta_{cl} \leq \Delta_{\max}] \leq \gamma. \tag{21}$$

Given the dataset $\mathcal{D}_2$ of R PUFs, histogram of Δ_{cl} is computed as follows. First, one PUF is chosen as a "target", the image of which is used in set-up mode to generate helper data h, fingerprint $\overline{y}_s$ and output z_s. The remaining $(R-1)$ images, together with the initial helper data h, are then used in reconstruction mode, generating fingerprints $\overline{y}_r$ and outputs z_s. This experiment is repeated R times, each PUF being selected once as target. The distance Δ_{cl} is estimated from all these $R(R-1)$ iterations by comparing the fingerprint generated in setup phase and fingerprints produced in reconstruction phase. In this way, Δ_{cl} is computed from any possible pairs of PUFs. Figure 7a, c shows the histogram of Δ_{cl} for both extraction methods RbEX and GbEX, respectively. The probability $\Pr[\Delta_{cl} \leq \Delta_{\max}]$ is then evaluated from the cumulative histogram of $\Delta_{\max}$ as in the robustness case. It is yet to be evaluated to what extent the Laser PF systems are considered as clones according to Definition 6. The probability that both Laser PF systems produce the same output is lower bounded the probability that both fingerprints $\overline{y}'_r, \overline{y}_s$ differ by no more than the error correcting capability t given that the expected difference is $\Delta_{\max}$ bits. The probability of this event corresponds to the left-hand side of Eq. 8 which provides a maximum value of δ i.e.,

$$\begin{aligned}
\delta_{\max} &= \Pr[\Delta_{cl} \leq t : \Delta_{cl} \leq \Delta_{\max}] \\
&= \sum_{i=0}^{\Delta_{\max}} \Pr[\Delta_{cl} \leq t : \Delta_{cl} = i] \cdot \Pr[\Delta_{cl} = i : \Delta_{cl} \leq \Delta_{\max}] \\
&= \sum_{i=0}^{\Delta_{\max}} p_i \cdot \frac{\text{pdf}(i)}{\text{cdf}(\Delta_{\max})} = \sum_{i=0}^{t} p_i \cdot \frac{\text{pdf}(i)}{\text{cdf}(\Delta_{\max})} \geq \delta,
\end{aligned} \tag{22}$$

where $p_i = 1$ if $i \leq t$ and 0 else. Thus, we can rewrite the sum by simply summing from $i = 0, .., t$. The functions *pdf* and *cdf* denote probability distribution function and cumulative distribution function of Δ_{cl}, respectively. To estimate them, the histogram of Δ_{cl} is divided to $i = 1, .., M$ bins. Then $pdf(i)$ is estimated from the histogram value in i^{th} bin and $cdf(\Delta_{\max})$ is estimated from cumulative histogram of Δ_{cl}. It follows that the considered PF infrastructure $\mathcal{I}_{\alpha_{CR}}$ is $(\gamma_{\min}, \delta_{\max})$-cloning resistant against an honest manufacturer. For each pair of (ℓ, t), values of $(\gamma_{\min}, \delta_{\max})$ are obtained by considering different values for $\Delta_{\max}$. Smaller values for $\Delta_{\max}$ will result in increasingly larger chances of producing the same output, but at much smaller probability to create such a PUF. At the other end of the spectrum are pairs of PF systems which are very likely to be constructed but very unlikely to produce the same output. Cloning resistance $(\gamma_{\min}, \delta_{\max})$ of the Laser PF system is shown for a selection of $\Delta_{\max}$ values in Table 1 using GbEX with a fixed t.

In practice, this means that with probability $\gamma_{\min}$, a manufacturer produces two PF systems that generate the same output with probability $\delta_{\max}$. So, the existential physical unclonability of a PF system can be summarized by averaging probability of cloning of Eq. 9 over all possible values of δ that is equivalent to $\text{PC}_{\text{exS}} = \mathbb{E}[\gamma_{\min}\delta_{\max}] = \Pr[\Delta_{cl} \leq t]$ over all the possible values of $\Delta_{\max}$. PC denotes the probability of cloning that gives us the probability that a random pair of PUFs manufactured by an honest manufacturer produces the same correct (i.e., averaged over noise) output.

To evaluate the trend of existential physical unclonability using different error correction capabilities of the BCH

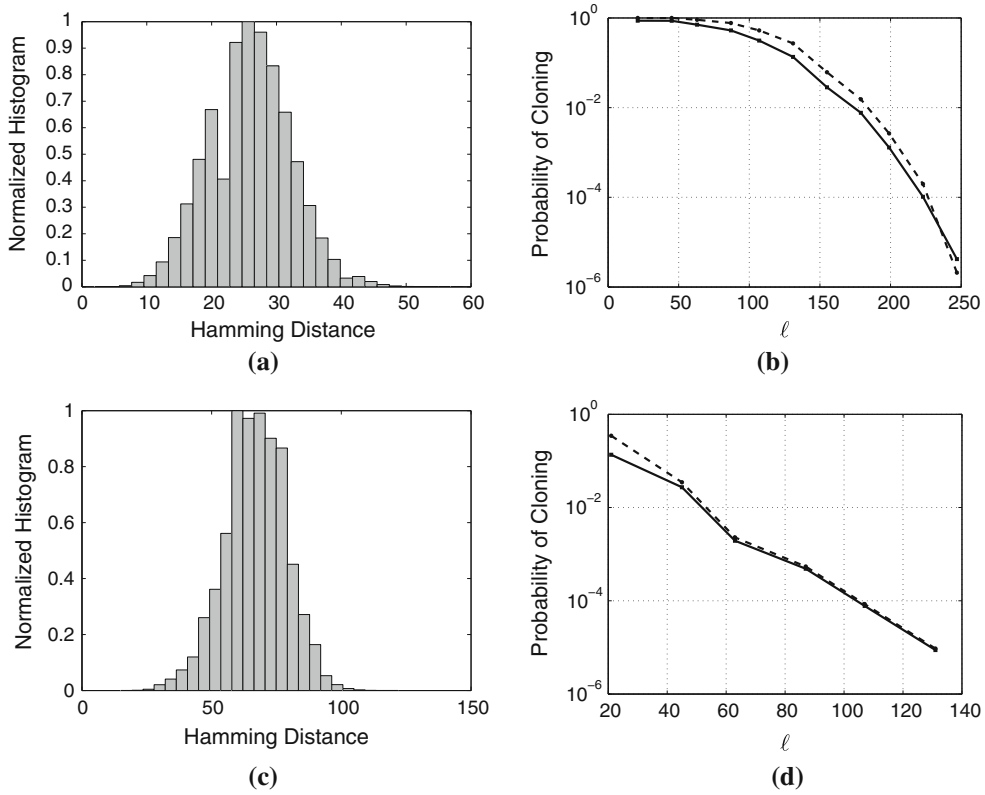


Fig. 7 Histogram of inter-class Hamming distance between fingerprints of different LPUFs Δ_{cl} and the probability of cloning versus output length ℓ by (*plain*) $\mathbb{E}[\gamma_{\min}\delta_{\max}]$ and (*dashed*) $\Pr[z'_{\mathrm{r}} = z_{\mathrm{s}} : p \neq p']$ for RbEX (**a**, **b**) and GbEX (**c**, **d**), respectively

Table 1 Different levels of $(\gamma, \delta, q = 2)$-cloning-resistance of LPUF using GbEx for a fixed correction capability $t = 26$, $\ell = 87$

$\Delta_{\max}$	γ	δ
15	1.04×10^{-6}	1.00
35	0.0076	0.06
55	0.16	0.003
75	0.77	6.82×10^{-4}
95	0.99	5.29×10^{-4}
115	1.00	5.26×10^{-4}
235	1.00	5.26×10^{-4}
255	1.00	5.26×10^{-4}

(M, ℓ, d) code, we fix again the parameter $M = 255$ and find the probability of cloning for a selection of possible pairs of ℓ, t where $t = \lfloor (d-1)/2 \rfloor$.

For each pair of (ℓ, t), $\mathrm{PC}_{\mathrm{exS}} = \mathbb{E}[\gamma_{\min}\delta_{\max}]$ is estimated using the built histogram of Δ_{cl} and depicted in plain curve in Fig. 7b, d, for both extraction methods RbEX and GbEX, respectively.

In the second approach, the existential physical unclonability of a PF system against an honest manufacturer is estimated directly from the probability of collisions between output values of different PUFs. Let z_{s} and z'_{r} be the output values of different PUFs in setup and reconstruction phase, respectively, using the same helper data. The physical unclonability is again summarized by the probability of cloning $\mathrm{PC}_{\mathrm{exS}} = \Pr[z'_{\mathrm{r}} = z_{\mathrm{s}} : p \neq p']$ estimated from all iterations described previously. The obtained probability is depicted in dashed curve in Fig. 7b, d for both extraction methods RbEX and GbEX, respectively.

Note that in the estimation of the above probability, the effect of observation noise incidence in PUF images has not been considered since we only had one observation in the dataset $\mathcal{D}_2$. However, we experimentally observe that adding simulated random observation noise decreases the above probability. This effect stems from a global increase of Hamming distance between fingerprints of different PUFs Δ_{cl}. Therefore, the obtained probability (without considering observation noise) gives us an upper-bound (worse-case) on the probability that two differently created LPUFs generate the same output.

By decreasing ℓ, the error correction capability t increases meaning that more number of errors are corrected. Correcting more number of errors results in mapping more different fingerprints to the same output and thus higher probability of cloning. We observe that the probability obtained from the second approach $\Pr[z'_{\mathrm{r}} = z_{\mathrm{s}} : p \neq p']$ is higher

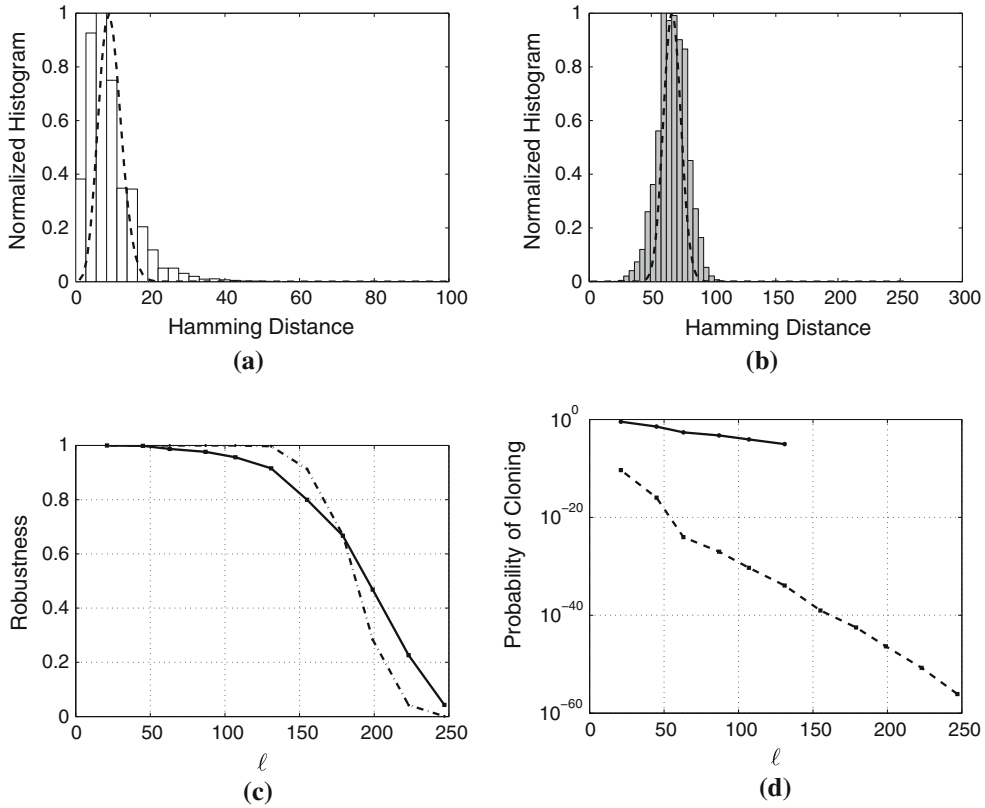


Fig. 8 Approximation of probability distribution function of intraclass (**a**) and interclass (**b**) Hamming distance between fingerprints by (*plain*) histogram and (*dashed*) binomial distribution. Robustness (**c**) and probability of cloning (**d**) versus output length ℓ using (*plain*) histogram approach and (*dashed*) binomial approach for GbEX

than the one obtained from the first approach $\mathbb{E}[\gamma_{\min}\delta_{\max}]$. This again stems from some occurrence of $z'_{\mathrm{r}} = z_{\mathrm{s}}$ although dist $(\overline{y}_{\mathrm{s}}, \overline{y}'_{\mathrm{r}}) > t$.

We finally observe that adaptive GbEX outperforms non-adaptive RbEX because it leads to a faster decay of the probability of cloning. At the end of this section, we describe how to compare the methods based on the trade-off between robustness and physical unclonability.

5.6 Binomial modeling

As a complement to our experiments, we investigate how accurately the robustness and physical unclonability can be evaluated assuming that the Hamming distance between fingerprints in set-up and reconstruction phases has the binomial distribution. This is the assumption usually made in prior works for evaluating the robustness and distinguishability of PUFs [1,6]. The Hamming distance between the fingerprints of different observations of the same PUF Δ_e relates to the observation noise and the extraction algorithm. It can be assumed to have binomial distribution if the noise is randomly distributed through the bits of the fingerprints.

In order to give an overview of the accuracy of this assumption, we compared the results based on this assumption with the results previously obtained from experimental histograms only for GbEX method. We assume that Δ_e and Δ_{cl} follow binomial distributions $B(M;\, p_e)$ and $B(M;\, p_y)$, respectively, where M is the number of bits of the fingerprints and p_e and p_y are the average number of bits that changed between two fingerprints of the same PUF (mean value of Δ_e) and two different PUFs (mean value of Δ_{cl}), respectively. We obtain $p_e = 0.04$ and $p_y = 0.26$ from the mean values of Δ_e and Δ_{cl}, respectively from all the experimental iterations described previously. We illustrate how the experimental histogram of Δ_e and Δ_{cl} which are obtained previously match the binomial distribution in Fig. 8a, b, respectively. We observe that especially for the inter-class distance Δ_{cl}, the real histogram is wider than the binomial distributions. It reflects the existing correlation between fingerprints bits. It might be the consequence of common patterns between images of different PUFs and/or the correlations caused by applied Gabor Binary Hashing. In the next step, we estimate robustness and physical unclonability assuming the binomial distributions $\Delta_e \sim B(M;\, p_e)$ and $\Delta_{cl} \sim B(M;\, p_y)$ instead of using the experimental histograms. Let $\mathbf{f}_{\mathsf{bino}}(t;\, n;\, p_i)$ and

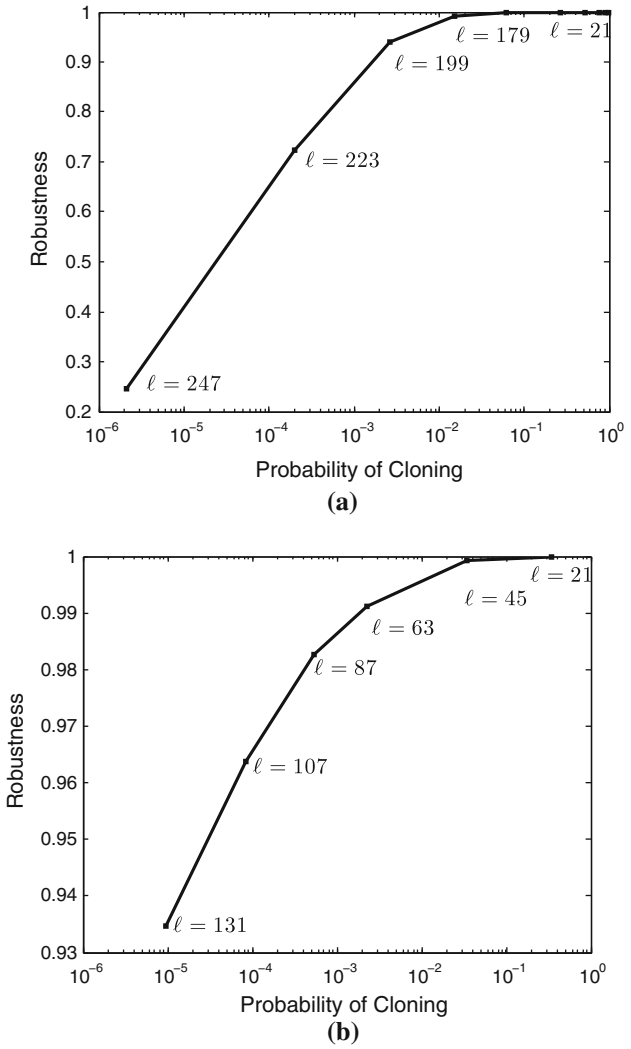


Fig. 9 Robustness $\rho_{\mathsf{S}} = \Pr[z_{\mathrm{r}} = z_{\mathrm{s}}]$ versus existential physical unclonability summarized by the probability of cloning $\mathrm{PC}_{\mathrm{exS}} = \Pr[z'_{\mathrm{r}} = z_{\mathrm{s}} : p \neq p']$ for **a** RbEX, **b** GbEX

$\mathbf{F}_{\mathsf{bino}}(t; n; p_i)$ be the probability distribution and cumulative distribution function of the binomial distribution $B(M; p_i)$. Then the robustness is estimated from $\mathbf{F}_{\mathsf{bino}}(t; n; p_e)$ using Eq. 19 and physical unclonability is estimated from the probability of cloning $\mathrm{PC} = \mathbb{E}[\gamma\delta]$ using binomial *pdf* and *cdf* in Eq. 21 and Eq. 22. Figure 8c, d compares the robustness and the probability of cloning obtained from histogram approach and binomial approach. We see that the binomial approach gives an approximate robustness trend but drastically optimistic results for the probability of cloning. Indeed, because of the existing correlation between fingerprints bits for different PUFs, the real distribution of inter-class distance is wider than the binomial distribution that causes more collisions between the outputs of different PUFs. This leads to higher probability of cloning. We conclude that the binomial assumption for the Hamming distance between the fingerprints of different PUFs is far from the reality for our particular implementation of image-based PUFs.

5.7 Robustness versus physical unclonability

Eventually, the main property of a PF Infrastructure is the trade-off between robustness and physical unclonability that provides an asset to fairly compare different PF Infrastructures and select one system $\mathcal{I}$ with all its parameters (described in Definition 4) for a particular application. Here, we compare the trade-off between robustness and physical unclonability (existential unclonability against an honest manufacturer) for two PF systems using RbEX and GbEX as the Extract procedure. Figure 9a, b shows this trade-off obtained from the output values, i.e., $\rho_{\mathsf{S}} = \Pr[z_{\mathrm{r}} = z_{\mathrm{s}}]$ and $\mathrm{PC}_{\mathrm{exS}} = \Pr[z'_{\mathrm{r}} = z_{\mathrm{s}} : p \neq p']$ for different correction capabilities t for RbEX and GbEX, respectively. They show the trade-off between robustness, probability of cloning, and length of output. We observe that the trend of GbEX outperforms that of RbEX, implying better performance of the adaptive extraction method for the Laser PF system, because it still provides a good robustness for an acceptable value of probability of cloning. For example, the minimum of GbEX trend provides a pair of $(\rho, \mathrm{PC}_{\mathrm{ext}}) = (0.94, 10^{-6})$ corresponding to $(M, \ell, d) = (255,131,36)$. It means that by correcting $t = 18$ errors, the system provides the same output of length $\ell = 131$ for the same PUF with a probability of 0.94 and provides the same output for different PUFs with a probability of 10^{-6} which is acceptable for many applications. In other experiments (excluded in the paper), we find that increasing fingerprint length M leads to better trade-off between robustness and physical unclonability for both hashing methods. That is the reason why we pick the maximum possible $M = 255$ with the form of $2^k - 1$ which is smaller than the size of Gabor coefficients ($\#\mathcal{G}_{a,\nu_0,\Delta} = 484$).

It is interesting to compare these results with the typical results given by human biometrics. In biometrics, e.g., for fingerprints verification systems, the performance of the system is often evaluated by false rejection rate (FRR), False Acceptance Rate (FAR) and equal error rate (EER). FRR is the probability of incorrectly rejected valid users and FAR is the probability of imposters incorrectly matched to a valid user's biometric. EER is the rate at which both FAR and FRR are equal. For the image-based physical function systems, FRR and FAR can be considered to be equivalent to $1 - \rho$ and $\mathrm{PC}_{\mathrm{ext}}$, respectively. The equivalent ERR is given when $1 - \rho = \mathrm{PC}_{\mathrm{ext}}$ and for RbEX and GbEX are obtained as $\mathrm{EER}_g = 0.2\ \%$ and $\mathrm{ERR}_r = 0.8\ \%$ which reconfirms the better performance of adaptive GbEX method. The typical EER for fingerprints verification systems is usually more than 2 % and thus higher (worse) than the obtained ERRs for both image-based physical function systems [57]. Note that despite fundamental differences in the security constraints

associated with systems based on human fingerprints and image-based PUFs, EER can still serve as a good measure for comparing the performance of different image-based physical function systems.

Besides, it is important to remark that security properties of an image-based physical function system are scalable. Robustness can be increased by building the response from averaging over more than one image in setup phase. Moreover, assuming a locality principle, i.e., that random variations will behave as independent events when occurring at different locations on the object, physical unclonability can be improved by increasing the size of the laser mark on a physical object.

6 Conclusion and future work

In this paper, we analyzed image-based physical function systems, which offer the benefit of being a low-cost primitive to increase the resistance of anti-counterfeiting systems against cloning. Our modular description of image-based physical function systems enables an efficient design for most image-based PUFs and a concrete evaluation of their security properties. As a practical example, we instantiated an image-based physical function system and experimentally characterized its security properties, i.e., robustness and existential physical unclonability and their trade-off. The experiments demonstrated the usefulness of the formalizations of the security properties made in [1] for assessing the accurate trade-off between robustness and physical unclonability.

We also showed that for our particular implementation of physical function system, assuming binomial distribution for the Hamming distances between fingerprints does not provide accurate results, especially for the assessment of the physical unclonability. Therefore, the binomial approach for estimating the physical unclonability of other kinds of PUFs should be performed with particular caution.

Our experiments suggest that the image hashing method and its parameters have a significant impact on the security properties achieved by an image-based physical function system. For example, adaptive GbEX provides a better trade-off between robustness and physical unclonability. It provides $(\rho, \mathrm{PC}_{\mathrm{ext}}) = (0.94, 10^{-6})$ using BCH (255,131,36).

Finally, more extensive comparison between the proposed image hashing methods performance, computational complexity, accuracy in the presence of high noise incidence and applicability based on the size of helper data is an interesting topic for future research. The study on the application of image-based PUF as a security primitive in anti-counterfeiting schemes, and analysis of possible attack scenarios is also a subject for future research.

Acknowledgments We thank François Koeune and Roel Maes for the helpful remarks. This research work was supported by the Belgian Walloon Region project TRACEA. François-Xavier Standaert and Laurent Jacques are Associate Researchers of the Belgian Fund for Scientific Research (FNRS-F.R.S.). This work has been funded in part by the ERC project 280141 (acronym CRASH).

References

1. Armknecht, F., Maes, R., Sadeghi, A.R., Standaert, F.X., Wachsmann, C.: A formalization of the security features of physical functions. In: IEEE Symposium on Security and Privacy, pp. 397–412 (2011)
2. Bastia, S.: Next generation technologies to combat counterfeiting of electronic components. IEEE Trans. Compon. Packag. Tech. **25**, 175–176 (2002)
3. Chong, C.N., et al.: Anti-counterfeiting with a random pattern. In: International Conference on Emerging Security Information, Systems and Technology, pp. 146–153 (2008)
4. Bauder, D.W.: An anti-counterfeiting concept for currency systems. Technical Report PTK-11990, Sandia National Labs, Albuquerque, NM (1983)
5. Commission on Engineering Committee on Next-Generation Currency Design and National Research Council Technical Systems. Counterfeit Deterrent Features for the Next-Generation Currency Design. The National Academies Press, Washington (1993)
6. Pappu, R.: Physical One-Way Functions. PhD thesis, MIT Press, Cambridge (2001)
7. Pappu, R.S., Recht, B., Taylor, J., Gershenfeld, N.: Physical one-way functions. Science **297**, 2026–2030 (2002)
8. Gassend, B., Clarke, D., van Dijk, M., Devadas, S.: Silicon physical random functions. In: ACM conference on Computer and Communications Security (2002)
9. Tuyls, P., Schrijen, G.J., Skoric, B., van Geloven, J., Verhaegh, N., Wolters, R: Read-proof hardware from protective coatings. In: Cryprographic Hardware and Embedded Systems Workshop. LNCS, vol. 4249, pp. 369–383. Springer, Berlin (2006)
10. Lim, D., Lee, J.W., Gassend, B., Suh, G.E., van Dijk, M., Devadas, S.: Extracting secret keys from integrated circuits. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **13**(10), 1200–1205 (2005)
11. Lee, J.W., Lim, D., Gassend, B., Suh, G.E., van Dijk, M., Devadas, S.: A technique to build a secret key in integrated circuits for identification and authentication applications. In: VLSI Circuits. Digest of Technical Papers, pp. 176–179 (2004)
12. Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: FPGA intrinsic PUFs and their use for IP protection. In: Workshop on Cryptographic Hardware and Embedded Systems (CHES). LNCS, vol. 4727, pp. 63–80 (2007)
13. Metois, E., Yarin, P., Salzman, N., Smit, J.R.: Fiberfingerprint identification. In: Workshop on Automatic Identification, pp. 147–154 (2002)
14. Buchanan, J.D.R., Cowburn, R.P., Jausovec, A.V., Petit, D., Seem, P., Xiong, G., Atkinson, D., Fenton, K., Allwood, D.A., Bryan, M.T.: Fingerprinting documents and packaging. Nature 475 (2005)
15. Clarkson, W., Weyrich, T., Finkelstein, A., Heninger, N., Halderman, J.A., Felten, E.W.: Fingerprinting blank paper using commodity scanners. In: Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, pp. 301–314 (2009)
16. Sharma, A., Subramanian, L., Brewer, E.A.: Paperspeckle: microscopic fingerprinting of paper. In: Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pp. 99–110. ACM, New York (2011)

17. Shariati, S., Standaert, F.-X., Jacques, L., Macq, B., Salhi, M.A., Antoine, P.: Random profiles of laser marks. In: WIC Symposium on Information Theory in the Benelux, pp. 27–34 (2010)
18. Tuyls, P., Skoric, B., Kevenaar, T.: Security with Noisy Data. Springer, Berlin (2007)
19. Maes, R., Verbauwhede, I.: Physically unclonable functions: a study on the state of the art and future research directions. In: Towards Hardware-Intrinsic Security, Information Security and Cryptography, pp. 3–37. Springer, Berlin (2010)
20. Tuyls, P., Škorić, B.: Strong authentication with physical unclonable functions. In: Security, Privacy, and Trust in Modern Data Management, pp. 133–148 (2007)
21. Tuyls, P., et al.: Secure Key Storage and Anti-Counterfeiting, pp. 255–268 Springer, Berlin (2008)
22. Tuyls, P., Batina, L.: RFID-tags for anti-counterfeiting. In: Topics in Cryptology—CT-RSA 2006. LNCS, vol. 3860, pp. 115–131. Springer, Berlin (2006)
23. Bulens, P., Standaert, F.-X., Quisquater, J.-J.: How to strongly link data and its medium: the paper case. IET Inf. Secur. **4**(2), 125–136 (2010)
24. Kirovski, D. Anti-counterfeiting: mixing the physical and the digital world. In: Foundations for Forgery-Resilient Cryptographic Hardware. Dagstuhl Seminar Proceedings, vol. 09282 (2010)
25. Shariati, S., Koeune, F., Standaert, F.-X.: Security analysis of image-based PUFs for anti-counterfeiting. In: Communications and Multimedia Security, pp. 27–34. Springer, Berlin (2012)
26. Skoric, B., Tuyls, P., Ophey, W.: Robust key extraction from physical uncloneable functions. In: Applied Cryptography and Network Security (ACNS), pp. 407–422 (2005)
27. Lim, D., Lee, J.W., Gassend, B., Edward Suh, G., van Dijk, M., Devadas, S.: Extracting secret keys from integrated circuits. IEEE Trans. VLSI Syst. **13**(10), 1200–1205 (2005)
28. Armknecht, F., Maes, R., Sadeghi, A.-R., Sunar, B., Tuyls, P.: Memory leakage-resilient encryption based on physically unclonable functions.In Advances in Cryptology (ASIACRYPT). LNCS, vol. 5912, pp. 685–702 (2009)
29. Baoshi, Z., Jiankang, W., Kankanhalli, M.S.: Print signatures for document authentication. In: ACM Conference on Computer and Communications Security, pp. 145–153 (2003)
30. Kirovski, D.: Toward an automated verification of certificates of authenticity. In: Proceedings of the 5th ACM conference on Electronic commerce, EC '04, pp. 160–169. ACM, New York (2004)
31. Chen, Y., Mihçak, K., Kirovski, D.: Certifying authenticity via fiber-infused paper. SIGecom Exch. **5**, 29–37 (April 2005)
32. Chong, C.N., Jiang, D.: Anti-counterfeiting using phosphor puf. In: International Conference on In Anti-Counterfeiting, pp. 59–62 (2008)
33. Beekhof, F., Voloshynovskiy, S., Koval, O., Villán, R.: Secure surface identification codes. In: Steganography, and Watermarking of Multimedia Contents X. Proceedings of SPIE, vol. 6819 (2008)
34. Tuyls, P., Skoric, B.: Secret key generation from classical physics. In: Philips Research Book Series (2005)
35. Shariati, S., Jacques, L., Standaert, F.-X., Macq, B., Salhi, M.A., Antoine, P.: Randomly driven fuzzy key extraction of uncloneable images. In: International Conference on Image Processing (ICIP) (2010)
36. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: ACM Conference on Computer and Communications Security (1999)
37. Dodis, Y., et al.: Fuzzy extractors: How to generate strong secret keys from biometrics and other noisy data. In: Eurocrypt'04, pp. 523–540 (2004)
38. Mallat, S.: A wavelet tour of signal processing: the sparse way, 3rd edn. Academic Press, New York (2008)
39. Jacques, L., Duval, L., Chaux, C., Peyré, G.: A panorama on multiscale geometric representations, intertwining spatial, directional and frequency selectivity. Signal Process. **91**, 2699–2730 (2011)
40. Laska, J.N., Kirolos, S., Duarte, M.F., Ragheb, T., Baraniuk, R.G., Massoud, Y.: Theory and implementation of an analog-to-information converter using random demodulation. In: Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1959–1962 (2007)
41. Candes, E.J., Romberg, J.: Quantitative robust uncertainty principles and optimally sparse decompositions. Found. Comput. Math. **6**, 227–254 (April 2006)
42. Tsaig, Y., Donoho, D.L.: Compressed sensing. IEEE Trans. Inf. Theory **52**, 1289–1306 (2006)
43. Ignatenko, T.: Secret-Key Rates and Privacy Leakage in Biometric Systems. PhD thesis, TU Eindhoven (2009)
44. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
45. Baraniuk, R., Davenport, M., DeVore, R., Wakin, M.: A simple proof of the restricted isometry property for random matrices. Constr. Approx. **28**, 253–263 (2008)
46. Goemans, M., Williamson, D.: Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. ACM **42**, 1145 (1995)
47. Jacques, L., Laska, J. N., Boufounos, P.T., Baraniuk, R.G.: Robust 1-bit compressive sensing via binary stable embeddings of sparse vectors. ArXiv e-prints (2011)
48. Duarte, M.F., Davenport, M.A., Takhar, D., Laska, J.N., Sun, T., Kelly, K.F., Baraniuk, R.G.: Single-pixel imaging via compressive sampling. IEEE Signal Proc. Mag **25**, 83–91 (2008)
49. Olshausen, B.A., Field, D.J.: Emergence of simple-cell receptive field properties by learning a sparse code for natural images. Nature **381**, 607–609 (1996)
50. Malacara, D.: Optical Shop Testing, 2nd edn. Wiley, New York (1992)
51. Wyant, J.C.: White light interferometry. In: Conference on Holography (SPIE) (2002)
52. Vincent, L.: Grayscale area openings and closings, their efficient implementation and applications. pp. 22–27 (1993)
53. Vincent, L.: Morphological grayscale reconstruction in image analysis: applications and efficient algorithms. IEEE Trans. Image Process. **2**, 176–201 (1993)
54. Naini, F.M., Gribonval, R., Jacques, L., Vandergheynst, P.: Compressive sampling of pulse trains: spread the spectrum! In: IEEE International Conference on Acoustics Speech Signal Processing, pp. 2877–2880 (2009)
55. Puy, G., Vandergheynst, P., Gribonval, R., Wiaux, Y.: Universal and efficient compressed sensing by spread spectrum and application to realistic fourier imaging techniques. CoRR, abs/1110.5870 (2011)
56. David, W.: SCOTT. On optimal and data-based histograms. Biometrika **66**(3), 605–610 (1979)
57. Cappelli, Raffaele, Maio, Dario, Maltoni, Davide, Wayman, James L., Jain, Anil K.: Performance evaluation of fingerprint verification systems. IEEE Trans. Pattern Anal. Mach. Intell. **28**, 3–18 (2006)