UNIVERSITE CATHOLIQUE DE LOUVAIN
Ecole Polytechnique de Louvain
ICTEAM Institute
Crypto Group.

Image-based Physical Unclonable Functions for Anti-counterfeiting

Saloomeh Shariati

Thesis presented for the Ph.D. degree
in Electrical Engineering

PhD committee

François-Xavier Standaert	UCL/ICTEAM - Supervisor
Benoît Macq	UCL/ICTEAM - Supervisor
Laurent Jacques	UCL/ICTEAM
Philippe Antoine	Lambda-X SA, Belgium
Lejla Batina	Radboud University, Netherlands
Peter Schelkens	Vrije Universiteit Brussel, Belgium
Michel Verleysen	UCL/ICTEAM - Chairman

Feb 2013

To my parents, for their love, endless support and encouragement.

ACKNOWLEDGMENTS

It is my pleasure to spend few words to thank all people who have helped me throughout perusing a PhD degree.

First of all, I'm grateful to my promoters Prof. François-Xavier Standaert and Prof. Benoît Macq for the opportunities they made for me in the pursuit of a PhD degree. Prof. Benoît Macq created the opportunity for me to start working on the thesis in Image Processing group of Communications and Remote Sensing Laboratory (TELE lab). The image processing part of the thesis is achieved in this group. I would also like to thank Prof. Laurent Jacques for his consistent advises in this part of thesis.

The security part of the thesis is achieved after I joined UCL Crypto group to work with Prof. François-Xavier Standaert. I would like to thank him for his extraordinary supervision and his help in finding my way during the thesis. I am also very grateful to all my colleagues in UCL Crypto group which make it a very friendly and warm environment to work.

In addition, I thank my other jury members, Philippe Antoine, Lejla Batina and Peter Schelken for their efforts in reviewing this text and their useful remarks. I also thank Dr. François Koeune for useful discussions on security part and his help in conducting the industrial part of the thesis.

My special thanks goes to my parents and sisters for their support and encouragement during my entire life. I should specially thank my husband, Farshad Keshmiri, for his endless support during our life together, specially during this challenging period of perusing PhD. I also thank my little boy, Soren, who brought me such an enormous joy and inspiring love.

Last but not least important people whom I want to thank are my friends and colleagues which made my life enjoyable in Louvain-la-Neuve, Belgium. Among all, I name some to show my gratitude: Katayon Saeedi, Mamali Shirvani, Adel Hatami, Onur Oguz, Ilke Bayram Oguz, Maria Gonzalez, Fahime Shamsaei, Mahmood Rezaee, Sophie Mawet, Philippe Bulens, Sylvie Baudine, Mostafa Ahmadi, Shagayegh Khani, Safa Jamali, Hadi Goldansaz, Hoda Chiniforoushan, Dina Kamel, Mostafa Emam.

ABSTRACT

Physical Unclonable Functions or PUFs have gained importance since they appeared about a decade ago. PUFs are based on physical random features that can serve as primitives in designing security systems similarly to human biometrics. The basic idea of using random features for security applications seems very interesting since the randomness is there for free. However, it raises some important research questions to be studied. The first important question is that "how good are PUFs?" or in other words "what are our expectations from them and how can we experimentally validate these expectations?". The second question rising after evaluating the expected properties is that "how can we connect these physical entities to secure systems?" or "how cryptographic primitives can be used to fill the gap between physics and secure systems?".

This dissertation tries to address these two main questions for a specific category of PUFs which are called Image-based PUFs and a particular secure system i.e., anti-counterfeiting. Image-based PUFs represent a category of PUFs based on random visual features of physical objects evaluated by an imaging method.

The first part of the thesis is dedicated to build a unified model to deal with Image-based PUFs. The model includes all the procedures needed to evaluate and post-process the images taken from Image-based PUFs. We also provide practical implementations of system components. For example we introduce two new types of Image-based PUFs called Laser-written PUF and Crystal PUF. The relevance of the framework is further demonstrated by its accordance to these examples of Image-based PUFs. We also present two practical adaptive and non-adaptive image hashing methods called Gabor Binary Hashing and Random Binary Hashing.

After building the model and instantiating its components, the second part of this thesis tries to address the first question i.e., "how good are PUFs?". For that, we experimentally characterize the important properties of Image-based PUFs i.e., robustness and physical unclonability. We build datasets of some PUFs which are evaluated a number of times, and based on that, we propose a methodology to experimentally evaluate robustness and physical unclonability. We finally achieve the main interesting property of the PUF system that is the trade-off between robustness and physical unclonability.

After evaluating how good PUFs are, to address the second question, we try to connect PUFs to a secure system. For that, we focus on development of an anti-counterfeiting scheme based on Image-based PUFs and use formal cryptographic analysis to connect the security of the scheme to the evaluated properties of its underlying PUF.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

PUF	Physical Unclonable Functions
PF	Physical Function
PFS	Physical Function System
SRAM	Static Random Acess Memory
IC	Integrated Circuits
LPUF	Laser-Written PUF
CrPUF	Crystal PUF
RbEx	Random binary Extraction
GbEx	Gabor binary Extraction
WLI	White Light Interferometry
LED	Light Emitting Diode
CCD	Charge Coupled Device
CD	Compact Disk
ECC	Error Correcting Code
RFID	Radio Frequency Identification
PKI	Public Key Infrastructure
3D	Three Dimentional
2D	Two Dimentional
PP	Polypropylene
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
RSA	Rivest, Shamir, Adleman
XOR	Exclusive OR
PPT	Probabilistic Polynomial Time

PUBLICATIONS

Journal Paper

- S. Shariati, F. X. Standaert, L. Jacques, B. Macq, "Analysis and Experimental Analysis of Image-based Physical Unclonable Functions," *Volume 2, Issue 3 , Page 189-206, in Journal of Cryptographic Engineering, 2012.*

Conference Papers

- S. Shariati, F. Koeune, F. X. Standaert, "Security Analysis of Image-based PUFs for Anti Counterfeiting," *pages 27-34, in Proc. of Communications and Multimedia Security (CMS), 2012 (Best stdent paper award and best presentation award).*
- S. Shariati, L. Jacques, F. X. Standaert, B. Macq, M. A. Salhi, P. Antoine, "Randomly Driven Fuzzy Key Extraction of Uncloneable Images," *In Proc. International Conf. on Image Processing (ICIP), 2010.*
- S. Shariati, F. X. Standaert, L. Jacques, B. Macq, M. A. Salhi, P. Antoine, "Random Profiles of Laser Marks," *pages 27-34, 31th Symposium on Information Theory in the Benelux, 2010.*

Patent

- Joel De Conick, Romain Riboo, S. Shariati, F. Koeune, F. X. Standaert, "Labeling System", WO/2012/122609, Sep 2012.

CONVENTIONS

- Let A be a probabilistic procedure. Then $\mathsf{A}(x) \to y$ 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 $\mathrm{dist_H}(s, t) \triangleq \sum_{i=1}^{K} s_i \oplus t_i \in [0, K]$.

CHAPTER 1

INTRODUCTION

1.1 SCOPE AND MOTIVATION

Physical Unclonable Functions have been gaining increasing attention since they appeared about a decade ago. The basic idea relies on the fact that many physical objects contain random features that are hard to clone. These random features, if examined properly, can serve as a primitive in the design of security systems. A primary application is using random features to identify the physical object similarly to biometrics. In some cases, the random features make the physical object to behave in a complex way when a stimulus (challenge) is applied to them, generating a response. This response depends on the random features in a complex and unpredictable way. Accordingly, the challenge-response behavior of the physical objects can be interpreted as a function parameterized based on the random features with challenge being the argument. Because of this similarity to mathematical functions, the physical objects including unclonable random features are often referred to as Physical Unclonable Functions or PUFs. Many physical objects with random features have been proposed as PUF candidates. The Optical PUF, for example, consists of a transparent material containing randomly distributed light scattering particles [2]. When probed with a coherent light (e.g., Laser

beam), its response is a speckle image as a result of complex scattering of a coherent light in the structure. Some PUF candidates use the random variation inevitably existing in electronic circuits. The electronic circuit is stimulated with a challenge and provides a response according to the existing random variations. Another major category of PUF candidates, hereafter called Image-based PUFs, consists of the PUFs which their response is an image representing 2D or 3D random structure of the physical object. The challenge is usually the light used to take the images. An example is Paper PUF where the random microstructure of the paper is characterized using an imaging method [3–9].

As discussed above, the core concept put forward by PUFs is to exploit the random variations that exist in various physical objects. This primary concept of exploiting physical randomness offered by PUFs is intuitively attractive because the randomness is there for free. However, it raises some important questions. How practical can a PUF be as a security primitive? What are the important properties of a PUF? How is it connected to standard cryptographic analysis to be applied in security systems (See Fig. 1.1)?

For sure, the security of a PUF-based system relies on the properties of its underlying PUF. Although, there exist many efforts in proposing new candidates for PUFs, few attempts towards formalizing PUF properties exist. The recent work of Armknecht et al. provided the formalization of security properties of PUFs after proposing a general framework of physical functions including the procedures relevant for deploying PUFs [1]. The model focuses on physical functions in general and captures their key properties, i.e., robustness (reproducibility of output for different measurements of the same PUF), physical unclonability (the property of PUFs that cannot be achieved by purely algorithmic solutions) and unpredictability (of PUF responses for different challenges). It allows for a meaningful security analysis of PUF-based constructions. In particular, a sound quantification of the physical unclonability, that used to be pointed out as an abstract quality, motivates the use of PUFs in security systems.

In this study we focus on Image-based PUFs and their specific security application i.e., anti-counterfeiting. We investigate the required security properties that an Image-based PUF should fulfill in order to be eligible as a security primitive in the design of anti-counterfeiting systems. For that purpose, we first provide a model to deal with Image-based PUFs by adapting the general framework of physical functions [1] to Image-based PUFs. This model facilitates the design of system components for most existing and new Image-based PUFs and allows concrete evaluation of their security properties based on the formalizations provided in [1]. We instantiate the components of an Image-based PUF system by a practical implementation. In order to answer the first question of "how good are PUFs?", we provide a methodology

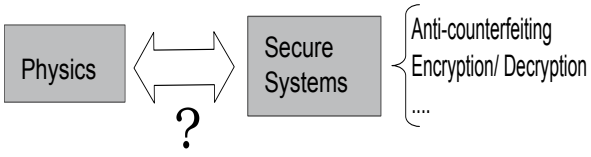


Fig. 1.1.: The connection between physics and secure systems.

to experimentally evaluate the important security properties of the system i.e., robustness and physical unclonability. To answer the second question of "how can we connect physics to secure systems?", we use cryptographic modules to fill the gap between Image-based PUFs and a secure system i.e., an anti-counterfeiting scheme. We then formally analyze the security of the anti-counterfeiting scheme which provably reduces to the physical unclonability property of the underlying PUF.

In following we elaborate more on our motivations behind designing a model dealing with Image-based PUFs, concrete experimental evaluation of their security properties and the security analysis of anti-counterfeiting systems. Then, we detail our contributions in each aspect in section 1.2. Finally, we describe the thesis outline in section 1.3.

The work in this dissertation is mainly motivated by the following three research concerns:

- Several Image-based PUF candidates have been proposed. Special attention is mostly given to introduce new PUF candidates and design dedicated techniques to deal with them. In this work we also introduce two new types of Image-based PUFs i.e., Laser-Written PUF and Crystal PUF. Diversity of the algorithms proposed to deal with this type of PUFs motivates the design of a unified model that can be applied to most existing and new Image-based PUFs. The model should be designed modularly in order to facilitate design procedure by adapting the building blocks of the model based on the specifications of a particular Image-based PUF.

- The main concern in designing a security primitive is to determine the properties required by the target security system and find efficient ways to guarantee these properties in practice. Until recently, most works on Image-based PUFs have been providing ad-hoc methods to evaluate the properties of their specific PUFs. However, some of these properties cannot be directly accredited by security systems. Moreover, non-unified definition of security properties make it difficult to fairly compare different Image-based PUFs for a specific security system. This motivates

defining the properties expected from Image-based PUFs and providing a methodology to experimentally validate these properties. The methodology should be applicable to most existing and new Image-based PUFs providing a proper asset to fairly compare their properties for the application under study.

- Another important research concern is designing a secure anti-counterfeiting system based on Image-based PUFs and formal analysis of its security. Although some anti-counterfeiting schemes have been proposed based on PUFs and Image-based PUFs in particular, there exist few attempts to formally analyze the security of the scheme according to the properties of the PUF. This motivates designing a secure anti-counterfeiting scheme and making meaningful assumptions considering the properties and constraints of Image-based PUFs and formally analyzing the security of the scheme.

1.2 CONTRIBUTIONS

In view of the above research concerns, this dissertation focuses on providing the following contributions:

1. Develop a unified model to deal with Image-based PUFs including all modules relevant for deploying Image-based PUFs. To this end, we specialize the general model of physical functions [1] to Image-based PUFs where each component of the system is adapted based on the specifications of Image-based PUFs. The model includes image-processing and cryptographic building blocks. The system, hereafter called Image-based Physical Function System, includes all the necessary components to create, evaluate and extract digital information from an Image-based PUF. Image-based Physical Function Systems include three main components i.e., Image-based PUF, evaluation process, and Image-based extraction consisting of image hashing and secure sketch procedures. A strong focus is placed on Image hashing as a specific module needed to deal with Image-based PUFs. The modular description of the system facilitates the design procedure of the system by adapting each block in accordance with the characteristics of the Image-based PUF under study.

2. Instantiate components of the Image-based Physical Function System by practical implementations. For Image based PUF component, we introduce two new Image based PUFs called Laser-Written PUF and Crystal PUF. For evaluation process, we propose to use the White Light Interferometry method to capture very high resolution images from Laser-Written PUF and use a digital microscope and a commodity digital

camera to take the images of Crystal PUF. For image hashing, after describing the concept of adaptive and non-adaptive image hashing, we provide Gabor Binary Hashing and Random Binary Hashing as examples of adaptive and non-adaptive image hashing respectively. Gabor Binary Hashing is an adaptation of the existing method [10] and Random Binary Hashing is our contribution as a fast candidate for image hashing.

3. Concretely evaluate security properties of the Image-based Physical Function System using formalizations provided by [1]. We provide a thorough experimental evaluation of security properties of an Image-based Physical Function System. We consider two minimum properties required by Image-based PUFs to be applied for anti-counterfeiting systems i.e., robustness and physical unclonability. The methodology describes how to statistically evaluate these properties from datasets of a number of PUFs evaluated a certain number of times. We also describe how to obtain the trade-off between 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.

4. Define a secure anti-counterfeiting scheme based on Image-based PUFs and formally analyze the security of the scheme. As the final step, we define a secure anti-counterfeiting protocol based on Image-based PUFs regarding their specific properties and constraints and provide a construction meeting this definition. The construction combines an Image-based Physical Function System and a Digital Signature Scheme. A strong focus is then placed on formal analysis of the security of the anti-counterfeiting protocol after investigating the attack model. We prove that the security property of the anti-counterfeiting scheme is reduced to the physical unclonability property of the underlying PUF.

1.3 THESIS OUTLINE

Chapter 2 presents some background information and tools used as foundations for this thesis. We first present Physical Unclonable Functions and some of their applications. We then emphasize on security properties that a PUF should fulfill to be eligible as a building block for security systems. We argue that the security properties of PUFs, especially physical unclonability, are not easy to evaluate as the evaluation consists of a physical phenomenon. We present a recent work of Armknecht et al. that addressed this issue by

capturing important security properties of PUFs after introducing a generic model of physical functions [1]. We bring the formalizations of two important security properties of interest for anti-counterfeiting application i.e., robustness and physical unclonability. In this chapter, an important building block of physical function model i.e., extraction procedure is highlighted. Important objectives of extraction procedure are categorized into information reconciliation and privacy amplification. Both objectives are discussed and typical constructions to meet their requirements are presented. We argue that for Image-based PUFs, it is sufficient to achieve information reconciliation purpose. We finally summarize other cryptographic and image processing tools used in this work i.e., Digital Signature Scheme, image pre-processing and Gabor hashing method.

Chapter 3 describes a unified model to deal with Image-based PUFs. We start by surveying state of the art of Image-based PUFs in literature. We further motivate building a unified framework that is applicable to most existing and new Image-based PUFs. For this purpose, we propose a unified model of Image-based physical function system by specializing the generic framework of physical functions [1]. Different components of Image-based physical function system are described and also instantiated with practical examples. An Image-based physical function system consists of Image-based PUF, evaluation process, and Image-based extraction consisting of image hashing and secure sketch procedures. In this context, we introduce two new Image-based PUFs i.e., Laser-written PUF and Crystal PUF for robust and low-cost anti-counterfeiting respectively. A strong focus is then placed on image hashing procedure as a specific module needed to deal with Image-based PUFs. We categorize image hashing procedure into adaptive and non-adaptive methods and describe these two approaches. Non-adaptive and adaptive image hashing methods are finally instantiated by presenting Random Binary Hashing and Gabor Binary Hashing respectively.

Chapter 4 presents a methodology to experimentally evaluate robustness and physical unclonability properties based on the definitions provided in chapter 2. In this view, we study datasets of images of two introduced Image-based PUFs i.e., Laser-written PUF and Crystal PUF to statistically evaluate their robustness and physical unclonability. As a preliminary analysis, we study the distribution of distances between images of both datasets. It gives an intuitive idea on the distinguishability of images according to the datasets. Next, we present the implementation settings of extraction procedures including Random and Gabor Binary Hashing methods and error correcting part of secure sketch scheme. Robustness and physical unclonability are then evaluated for both PUFs and both image hashing methods. Additionally, we investigate the binomial approach used in prior work for analysis of robustness and unclonability to check if this approach gives accurate re-

sults for Image-based PUF or not. Finally, we evaluate the key property of a physical function system for anti-counterfeiting application i.e., the trade-off between robustness and physical unclonability.

Chapter 5 studies the target application of Image-based PUFs i.e., anti-counterfeiting. Having defined the model to deal with Image-based PUF and concrete experimental evaluation of their security properties in previous chapters, this chapter presents a unified formal treatment of the use of image-based PUFs as a counterfeiting prevention tool. We start by surveying the state of the art of anti-counterfeiting schemes. Then, we define an anti-counterfeiting scheme by making appropriate assumptions according to properties and constraints of Image-based PUFs. We then investigate the security of the anti-counterfeiting scheme by formally analyzing the attack model. Finally we derive the security of the anti-counterfeiting scheme that provably reduces to the physical unclonability property of the underlying Image-based PUF.

Finally, the conclusions of this thesis are drawn in **Chapter 6.**

CHAPTER 2

BACKGROUND

In this chapter we list some background information exploited in several parts of this work. In section 2.1 we start with our main target which is Physical Unclonable Functions. We survey a number of PUF realizations and their applications. Then we describe a general model of physical functions that allows meaningful analysis of its security properties when used for PUF-based security systems. Section 2.2 highlights a building block of the physical function system called Extraction procedure by describing the requirements of the extraction procedure and studying constructions that meet these requirements. Section 2.3 presents a cryptographic tool deployed later in the anti-counterfeiting system i.e., digital signature scheme. It brings the definition of an unforgeable signature scheme against adaptive chosen-message attack. Section 2.4.1 and section 2.4.2 describe some background information on the image processing part of the work including image pre-processing and Gabor hashing.

2.1 PHYSICAL UNCLONABLE FUNCTIONS

A Physical Unclonable Function (PUF) is a function that is embodied in a physical structure and is easy to evaluate, but hard to clone. Generally, a PUF interacts with stimuli (challenges) in an intricate way, and leads to unique and unpredictable responses. In this section we first list some realizations of PUFs and their applications. Then, we study a general framework of physical functions and formalization of its important properties.

2.1.1 A short overview of PUF realizations and applications

Physical structures with random properties turn out to be good candidates to serve as a PUF. Early works that exploit the physical properties of random structures for authentication purposes date back to that in [11, 12] mainly in different attempts to design anti-counterfeiting mechanisms. A formalization of this concept was introduced as physical one-way functions by Pappu [2, 13] or physical random functions [14] and finally Physical(ly) Unclonable Functions, or PUFs. Pappu also proposed to use three-dimensional optical structures as a so-called Optical PUF. Optical PUF consists of a transparent material containing randomly distributed light scattering particles. When probed with a laser, the transmitted light is the result of multiple coherent scattering and forms a random-looking pattern of bright and dark areas known as the speckle pattern. The properties of the incoming laser beam, e.g. angle of incidence represent the challenge and the speckle pattern is the response. Since then, an increasing number of new types of PUFs has been proposed. Coating PUF is introduced by Tuyls et al. [15]. It consists of a protective coating, covering an integrated circuit. The opaque coating material is doped with dielectric particles, having random properties concerning their size, shape, and location. A comb structure of metal wire sensors below the coating layer is used to measure the local capacitance of the coating. The challenge determines the properties, e.g., frequency and amplitude of the voltage applied to the sensor array. The response includes the measured value of the local capacitance. Paper PUF is an example of non-electronic PUFs which is based on the unique and random structure of a regular or modified paper [3–9]. Phosphor PUF is another example where phosphor particles are blended with the material or with the cover of the product to form the random pattern [16, 17]. A number of PUF candidates have been proposed whose basic operation consists of a measurement of a random quantity in electronic circuits. Some examples include Arbiter PUF [18, 19], Ring Oscillator PUF [14], SRAM PUF [20], Latch PUF [21], Glitch PUF [22, 23], Butterfly PUF [24]. Fig.2.1 illustrates some instances of PUFs described above. For a

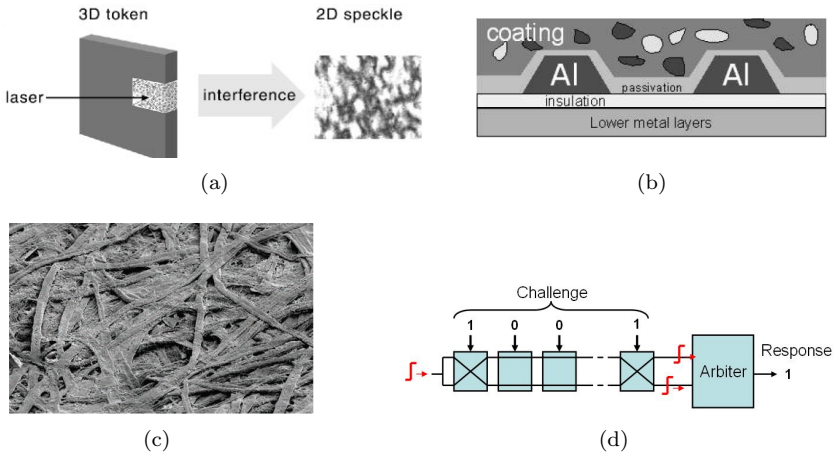


Fig. 2.1.: Schematic of some PUF realizations (a) Optical PUF (b) Coating PUF (c) Paper PUF (d) Arbiter PUF.

more complete list and description of the various proposed PUFs, we refer to [25–27].

Various application fields have also been proposed. Here we list some applications.

1. **Anti-counterfeiting**. PUFs have received much attention as a primitive in the design of secure anti-counterfeiting systems [10, 16, 17, 28]. In this application, the core concept of using PUF primitives is to rely on the unique physical unclonable properties to identify a product. In this thesis the main focus is placed on this primary application. In this chapter we only provide a short example of using PUFs for anti-counterfeiting purpose. Later, we study in detail how a PUF can contribute to secure an anti-counterfeiting protocol. First a PUF is integrated inside a product. It can be inherently part of the product (intrinsic PUF) or a distinctive object attached to the product (extrinsic PUF). In enrollment step, digital information is extracted from the PUF using an extraction algorithm and serves as its identifier. It is then stored e.g., in a database to be used in the verification phase. In verification process, the verifier validates the authenticity of the product by again extracting information from PUF and comparing it with the corresponding data in the database. If the comparison is made by matching all bits of the identifiers (which is the case in our scheme in chapter 5), the basic requirement is that the identi-

fier extracted in verification process exactly matches the one extracted in enrollment phase. To this end, an extraction algorithm is needed to map the noisy responses of the PUF in enrollment and verification phases to the same identifier. Extracting error-free outputs from noisy responses, known as "information reconciliation" procedure in literature, is usually carried out by means of a "secure sketch" scheme using an Error Correcting Code (ECC). Later, in section 2.2, we describe a secure sketch scheme aimed to achieve information reconciliation purpose [29].

2. **Authentication via challenge-response pairs**. PUFs can be integrated into a challenge-response authentication protocol [2, 30, 31]. One motivation is that they can be used for authentication of resource constrained platforms such as RFIDs where cryptographic operations may be too expensive. In this approach, a PUF is integrated inside a prover (e.g. a RFID tag). The verifier stores a number of challenges and corresponding responses in the enrollment phase. In the verification phase, the verifier sends a challenge from the database to the prover and hence to the PUF and receives the corresponding response. The verifier can then check if the response is the same as the one stored in the database. If the check is positive, the verifier accepts the authenticity and grants the requested service. From the security point of view, a PUF should possess certain advanced properties in order to be suitable for this application. For example it should be able to provide a large amount of unpredictable challenge-response pairs. First, the existence of a large amount of challenge response is necessary because each authentication round needs a new challenge-response pair. Second, the unpredictability of responses for different challenges is required to prevent an attack where the adversary replaces a PUF with a mathematical clone that upon receiving a challenge is able to generate a response similar to that of the original PUF. Because of these security requirements, few PUFs proposed until recently are applicable for these advanced types of applications.

3. **Secure key generation**. A cryptographic key can be extracted from a PUF and deployed in a more advanced protocol rather than using a challenge-response repository as described above [32–34]. To this end, an extraction algorithm is used to extract a cryptographic key from the response of the PUF to a fixed challenge. For this application, in addition to extracting error-free keys from noisy PUF responses, extraction algorithm also needs to produce keys that are uniformly random from the PUF responses which are not necessarily uniformly random. Extracting uniformly random keys, known as "privacy amplification" procedure, is usually accomplished by using a "Randomness Extractor" or "Strong

Extractor" algorithm [29]. Later in section 2.2, we describe a general example of the extraction procedure called fuzzy extraction algorithm. It consists of a secure sketch and a strong extractor to achieve information reconciliation and privacy amplification purposes respectively.

4. **Secure key storage**. The basic idea in using PUFs in secure key storage is that the key is not stored in the memory. The key is generated from the PUF whenever an application requires the key [15]. The fact that the key is not stored in a digital memory protects it against several physical attacks (e.g., invasive attacks aiming at reading the key from the memory).

5. **Intellectual Property and copy protection**. PUFs can be used to protect the Intellectual Property or IP. For example, Guajardo et al. use the PUF inside the FPGA to protect its IP [20]. The aim is to prevent the adversary from cloning an FPGA by copying its configuration file and inserting it into another FPGA. This is carried out by binding the FPGA and its IP (configuration program) via the PUF. More specifically the IP i.e., a program configured on FPGA is encrypted using the key extracted from the intrinsic PUF (e.g., SRAM PUF inside the FPGA). Upon power-up the FPGA reads the encrypted configuration file, extracts the key from the PUF, decrypts the configuration file, and configures the FPGA. The same idea can be applied for copy protection. For instance, a CD content can be bound to the CD via its intrinsic PUF i.e. the random structure of the CD [35].

The above list is not exhaustive, but gives an indication of the many potential applications that can be attributed to PUFs.

In the following, we study a general framework of physical functions in accordance with existing literature on PUFs and a formalization of the security properties of interest.

2.1.2 Framework of Physical Functions

As discussed previously, the core concept put forward by PUFs is to exploit the random variations existing in various physical objects. However, it raises an important question of how practical and secure this concept can be. Several attempts towards formalizing a PUF definition and properties exist. However, none of them captures the full spectrum of proposed PUFs and their properties. They are either too restrictive, i.e., excluding certain PUFs, or too ad-hoc, i.e., listing perceived and even assumed properties of certain PUFs instead of providing a more general model. The core issue is thus to determine the properties required by the security systems and find efficient ways to guar-

antee these properties in practice. Two key requirements for almost all security systems are robustness (reproducibility of output for different measurements of the same PUF) and uniqueness or randomness (distinguishability between outputs of different PUFs). The robustness is rather straightforward to evaluate. It suffices to statistically evaluate the probability of output match among different evaluations of the same PUF. In contrast, evaluation of uniqueness property is not straightforward because it involves assessing a physical phenomenon. The efforts made to assess uniqueness or randomness of PUFs can be categorized into two approaches. The first approach deals with the specific PUF (e.g., optical PUF) and tries to evaluate uniqueness by assessing how much information or entropy can be extracted from that PUF. For instance, the entropy of optical PUFs and coating PUFs are obtained by exploring their physical characteristics [36, 37]. In this approach, the entropy depends on the physical features and thus its evaluation requires analysis of physical interactions inside the PUF under study. The second approach, however, is more generic and can be applied for different types of PUFs. In this approach, the PUF is considered as a random number generator and its output is considered as a random variable whose entropy is estimated by means of statistical analysis of a large number of samples (different PUFs outputs) [7, 38]. In this case, the entropy can be obtained by means of well-known entropy estimators such as *Maurer*'s universal test [39] and *Context Tree Weighting* (*CTW*) entropy test [40]. The main issue is that statistical entropy estimators need a huge number of samples from a certain random variable to reliably find its entropy. That becomes more critical for big random variables (of large number of bits). Therefore, the entropy given by this approach does not turn out to be very reliable when one does not possess enough statistical samples of the random variable (PUF output). The recent work of Armknecht et al. addressed these issues by formalization of the security properties of PUFs after proposing a general framework of physical functions including the procedures relevant for deploying PUFs [1]. The model focuses on physical functions in general and captures their key properties, i.e., robustness, physical unclonability (i.e., equivalent to uniqueness) and unpredictability. It allows a meaningful security analysis of PUF-based constructions. In particular, a sound quantification of the physical unclonability, that used to be pointed out as an abstract quality, motivates the use of PUFs in security systems. In this part of the thesis, we summarize this general framework of physical functions and present the formalizations of its security properties. This framework is then specialized to Image-based PUFs in the following chapter. Because of our specific application, i.e. anti-counterfeiting, we only bring the minimum security properties required by anti-counterfeiting systems i.e. robustness and physical unclonability and we exclude unpredictability.

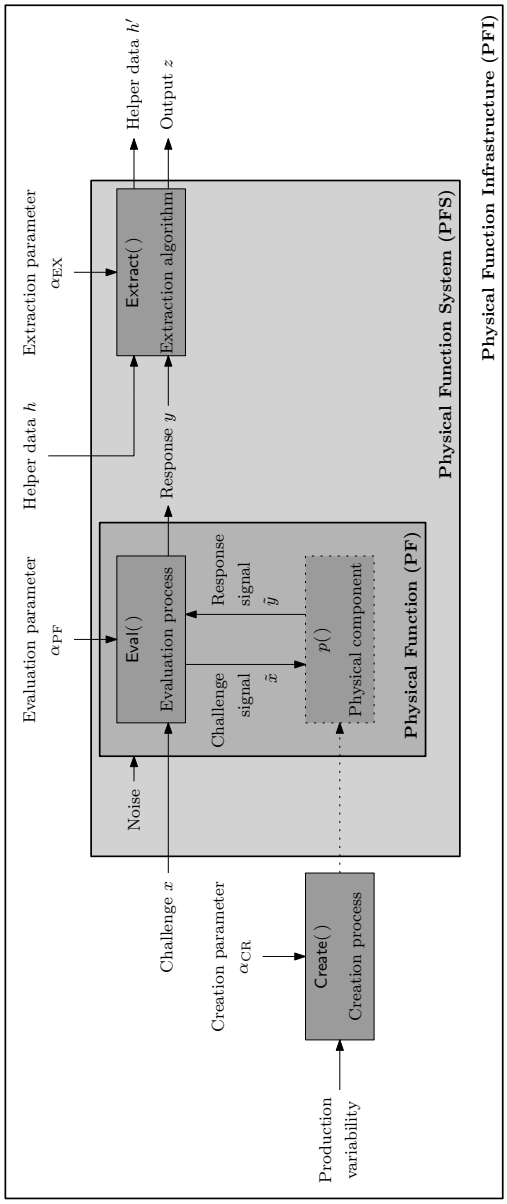


Fig. 2.2.: Generic framework for physical functions [1].

The general framework of physical functions, depicted in Fig. 2.2 shows modularly all necessary components to create, evaluate and extract digital information from a physical function.

Creation process is usually performed by the manufacturer to produce a physical component (PUF) with a creation parameter α_{CR}, and is formally defined as:

Definition 1 (Creation Process [1])**.** *A creation process* Create *is a probabilistic procedure that, on input of a creation parameter* α_{CR}*, produces a physical component* p*:*

$$\mathsf{Create}(\alpha_{\mathrm{CR}}) \rightarrow p. \tag{2.1}$$

Creation process is a probabilistic procedure because its output relates to both the creation parameter and some uncontrollable production variability (creation noise). As a practical example, consider an SRAM[1] PUF [41] which is based on the random power-up values of SRAM memory cells. The creation parameter α_{CR} of the SRAM PUF includes the different design options for an SRAM memory 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 PF *is a probabilistic procedure:*

$$\mathsf{PF}_{p,\alpha_{\mathrm{PF}}} : \mathcal{X} \rightarrow \mathcal{Y}, \tag{2.2}$$

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.,*

$$\mathsf{PF}_{p,\alpha_{\mathrm{PF}}}(x) = \mathsf{Eval}_p(\alpha_{\mathrm{PF}}, x) \rightarrow y. \tag{2.3}$$

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 an uncontrollable random noise existing in the evaluation procedure (evaluation noise). The essential assumption for all PUF examples is that the creation noise (favorable noise)

[1] Static Random Access Memory

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.

As indicated previously, a PF is usually combined with an extraction algorithm. The extraction algorithm aims at reducing undesired evaluation noise by mapping slightly different responses y corresponding to the same challenge x to a uniformly random output z according to some *extraction parameter* α_{EX} (e.g., number of corrected errors). In section 2.2, we study a general extraction algorithm named *fuzzy extraction*. The $\mathsf{Extract}$ algorithm can be executed in two different modes: *setup* and *reconstruction*. In setup mode (executed when PUF is created), output and helper data h' (helping compensate the noise) are generated and stored in a database. In reconstruction mode, the corresponding helper data h' is retrieved from the database and used as an input to the extraction algorithm (so $h = h'$), for generating the output z. In this view, if a challenge x is requested for the first time, setup mode is executed to generate an output z and *helper data* h'. Later, when challenge x is requested again together with helper data $h = h'$, the reconstruction mode is executed to recreate z.

The combination of a PF and an extraction algorithm is considered as one single building block and is defined as:

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

$$\mathsf{PFS}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}} : \mathcal{X} \times (\mathcal{H} \cup \{\epsilon\}) \to \mathcal{Z} \times \mathcal{H}, \tag{2.4}$$

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 $\mathsf{PF} = \mathsf{PF}_{p,\alpha_{\mathrm{PF}}}$ *(Definition 2) and an extraction algorithm* $\mathsf{Extract}$*, i.e.,*

$$\begin{aligned} &\mathsf{PFS}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}}(x,h) \\ &= \mathsf{Extract}_{\alpha_{\mathrm{EX}}}(\mathsf{PF}_{p,\alpha_{\mathrm{PF}}}(x),h) \to (z,h'). \end{aligned} \tag{2.5}$$

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

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

The combination of all components described above(Creation, Physical Function and Extraction) 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 $\mathcal{F}$ *refers to a fixed creation process* Create *(Definition 1) and the set of all PF systems* PFS *(Definition 3), where the physical component* p *is the result of* Create*, i.e.,*

$$\mathcal{F}_{\alpha_{\mathrm{CR}}} = (\mathsf{Create}, \{\mathsf{PFS}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}} : \mathsf{Create}(\alpha_{\mathrm{CR}}) \to p\}) \,, \tag{2.6}$$

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

The above framework allows defining security properties of the system. In the following, we present the formalizations of robustness and physical unclonability as the basic criteria expected from Image-based PUFs.

2.1.3 Robustness

As explained above, due to the evaluation noise a PF might respond to the same challenge with different responses, when queried several times. However, if these responses are "similar", it is possible to address this issue by using an appropriate extraction algorithm.

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

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

$$\begin{aligned} \rho_{\mathsf{PFS}}(x) := \Pr\,[\mathsf{PFS}(x,h) \to (z,h) : \\ \mathsf{PFS}(x,\epsilon) \to (z,h)] \,. \end{aligned} \tag{2.7}$$

This metric captures the probability that for a physical component p, the output generated by reconstruction phase matches the value generated in setup phase using its corresponding helper data h.

2.1.4 Physical Unclonability

To define the property of physical unclonability, Armknecht et al. in [1] first defined the notion of Physical Clone. They consider clones on the physical level only and exclude mathematical clones. Informally, it means that a physical function system is a clone of another physical function system if they show the same behavior provided that they deploy the same Extract algorithm. In general, protection against tampering with the Extract algorithm should be provided by mechanisms outside of the PF system and it is outside of the scope of a physical function security model. Another aspect that needs to be

considered is the following: depending on the case, only the responses of PFS to a subset of challenges might be known at all. Thus, any other PF system PFS' that coincides on this subset of challenges could be seen as a clone. Therefore, it is sufficient that the definition of a clone captures only the set of challenges $\mathcal{X}' \subseteq \mathcal{X}$ that are relevant w.r.t. the underlying use case. After above explanations, the notion of Physical Clone is formally defined by:

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

$$\Pr\left[\mathsf{PFS}'(x,h) \to (z,h) : \mathsf{PFS}(x,\epsilon) \to (z,h)\right] \geq \delta \cdot \rho_{\mathsf{PFS}}(x). \tag{2.8}$$

For simplicity, we write $\mathsf{PFS}' \overset{\delta,\mathcal{X}'}{\equiv} \mathsf{PFS}$ if Eq. 2.8 holds.

The reason to integrate the notion of robustness $\rho_{\mathsf{PFS}}()$ 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 PFS a clone PFS' is constructed.
- *Existential cloning:* means that two arbitrary PF systems PFS and PFS' are produced, where one is the clone of the other.

In this thesis we investigate the existential cloning as a worse case study because the probability of its occurrence is higher. The reason becomes more clear by comparing these two scenarios with second preimage and collision attacks on cryptographic hash functions. Selective cloning is similar to second preimage attack which refers to the event that given a specific input and its hash value, another input value is found with the same hash value. While, existential cloning is similar to collision attack which refers to finding two arbitrary inputs that hash into the same output. We know that for an n-bit hash, the second preimage attack has a time complexity of 2^n and collision attack has a time complexity of $2^{(n/2)}$ due to the effect of "Birthday Paradox" [42]. It implies that the probability of existential cloning is higher than that of selective cloning.

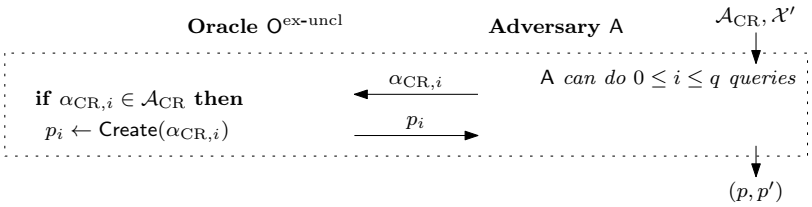


Fig. 2.3.: Existential unclonability security experiment $\mathbf{Exp}_{\mathsf{A}}^{\text{ex-uncl}}(q)$.

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. 2.3, 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 $\alpha_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}}$ and challenges $\mathcal{X}' \subseteq \mathcal{X}$. Then he outputs two arbitrary clones p, p'. This experiments is hereafter called $\mathbf{Exp}_{\mathsf{A}}^{\text{ex-uncl}}(q)$.

Definition 7 (Existential Physical Unclonability [1])**.** *Let $\mathcal{A}_{\mathrm{CR}}$ 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 $\mathcal{F}_{\mathcal{A}_{\mathrm{CR}}} := \{\mathcal{F}_{\alpha_{\mathrm{CR}}} : \alpha_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}}\}$ of PF infrastructures (Definition 4).*

A family of PF infrastructures $\mathcal{F}_{\mathcal{A}_{\mathrm{CR}}}$ is called (γ, δ, q)-cloning-resistant *w.r.t. $\mathcal{X}' \subseteq \mathcal{X}$, if*

$$\begin{aligned} \Pr\big[\mathsf{PFS}'_{p',\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}} \overset{\delta,\mathcal{X}'}{\equiv} \mathsf{PFS}_{p,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}}} : \\ (p,p') \leftarrow \mathbf{Exp}_{\mathsf{A}}^{\text{ex-uncl}}(q); \\ p \in [\mathsf{Create}(\alpha_{\mathrm{CR}})]; \alpha_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}}; \\ p' \in [\mathsf{Create}(\alpha'_{\mathrm{CR}})]; \alpha'_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}}\big] \leq \gamma. \end{aligned} \tag{2.9}$$

This means: the probability that A generates, as output of the security experiment depicted in Fig. 2.3, two physical components p and p' which (i) imply δ-clones on the PF system level and (ii) have been created using creation parameters $\alpha_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}}$, is less than γ.

Definition 7 covers two important manufacturing situations:

- *Honest manufacturer:* This case reflects the probability that an honest manufacturer creates two clones by coincidence and captures clonable PFs. In the case of $\mathcal{A}_{\mathrm{CR}} = \{\alpha_{\mathrm{CR}}\}$, i.e., where only one creation parameter is involved, the set $\mathcal{F}_{\mathcal{A}_{\mathrm{CR}}}$ "collapses" to a single PF infrastructure $\mathcal{F}_{\alpha_{\mathrm{CR}}}$. In other words, A is restricted to actions that an honest manufacturer could do within $\mathcal{F}_{\alpha_{\mathrm{CR}}}$.
- *Malicious manufacturer:* This case covers the scenario, where $\mathcal{A}_{\mathrm{CR}}$ contains more than one possible choice for the creation parameter α_{CR},

which allows the adversary A to influence the Create process in order to create a clone.

In practice, we mostly consider the case of existential physical unclonability by an honest manufacturer. It implies assuming an adversary which is limited to do what an honest manufacturer can do by confining the possible creation parameters to that of honest manufacturer ($\mathcal{A}_{\mathrm{CR}} = \{\alpha_{\mathrm{CR}}\}$). Otherwise, the assessment of uncloneability is related to the detail and cost of technical manufacturing process that is not straightforward to evaluate. We will elaborate this assumption later in chapter 5.

2.2 FUZZY EXTRACTION

As described previously an extraction algorithm is usually combined with a physical function for two main purposes. First, it aims at extracting error-free outputs from noisy responses. This so-called information reconciliation purpose is usually achieved by a secure sketch algorithm based on utilizing Error Correcting Codes. Second, in some applications such as secret key generation, extraction algorithm also aims at providing uniformly random output from not-necessarily random responses. This so-called privacy amplification purpose is usually achieved by a "randomness extractor" or "strong extractor" algorithm. In this section we describe a typical extraction algorithm widely used in PUF literature i.e., code-offset fuzzy extractor proposed by Dodis et al. [29]. It consists of a code-offset secure sketch and a strong extractor. We begin by describing a code-offset secure sketch.

Code-offset secure sketch described by Dodis et al. [29] which is equivalent to fuzzy commitment scheme proposed by Juels and Wattenberg [43] is depicted in Fig. 2.4. In this scheme the helper data h_z is constructed as a codeword from a selected error-correcting code c_{zs}, used to encode a chosen output z_s, masked with the PUF response y_s observed during setup phase. Thus $h_z = y_s \oplus c_{zs}$. The helper data h_z together with the PUF response y_r observed during reconstruction phase are mapped to a codeword c_{zr} which is decoded to the same output chosen in setup phase z_s, if the error between PUF responses y_s and y_r is less than error correction capability.

Code-offset fuzzy extractor is built from the described secure sketch and a randomness extractor Ext such as universal hash functions [44].

Fig. 2.5 illustrates how a code-offset secure sketch is adapted to build a code-offset fuzzy extractor. As described previously randomness extractor is added to the extraction procedure when the output of the physical function needs to be used as a cryptographic key. In this case, in contrast with the secure sketch, the output (that will be used as a secret key) z_s is not encoded to codeword c_{zs}, but extracted from PUF response y_s directly. In order to

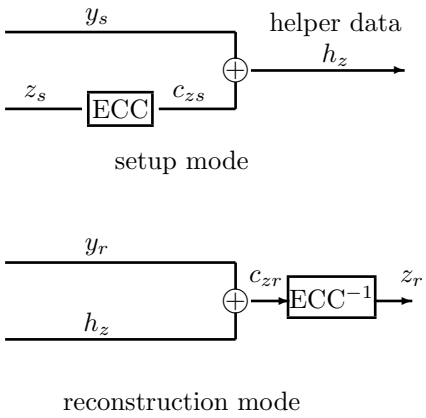


Fig. 2.4.: Code-offset secure sketch construction.

produce uniformly random output, randomness extractor needs a uniformly random "seed" r as input that can be publicly known. The code-word c_m is chosen at random by encoding a random message m and only serves for code-offset error correction. In reconstruction mode, the noisy codeword $c'_m = y_r \oplus h_m$ is corrected to c_m and then again XORed with the helper data h_m to obtain the initial PUF response y_s. Finally, a randomness extractor Ext extracts output z_s from PUF response y_s using a random seed r.

In this thesis, we have used a code-offset secure sketch described above [2]. The main task of code-offset secure sketch scheme for Image-based PUFs is to produce reproducible (error-free) outputs in setup and reconstruction phases. The reason behind choosing code-offset secure sketch 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 [45]. Producing error-free outputs in setup and reconstruction phases, brings up the opportunity to use Image-based PF system for more advanced anti-counterfeiting systems. As an example, for an anti-counterfeiting system based on digital signature scheme (described in chapter 5), the verification works properly only

[2] Code offset secure sketch is sometimes referred as a code-offset fuzzy extractor in literature. Because according to Dodis et al., for uniformly random PUF response, a secure sketch can be used as a fuzzy extractor without the need for a randomness extractor.

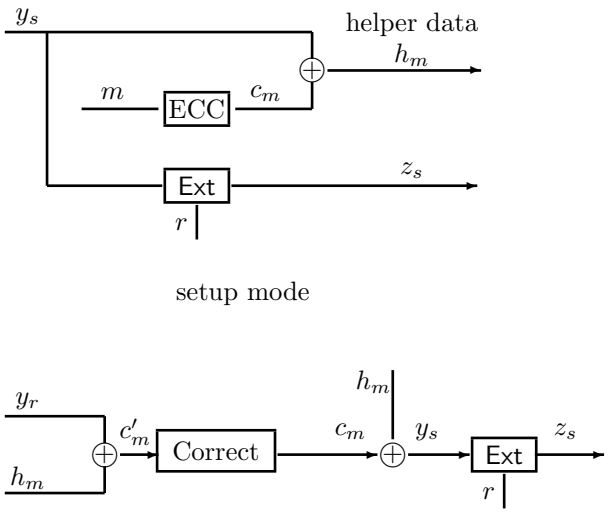


Fig. 2.5.: Code-offset fuzzy extraction.

if the output obtained in reconstruction phase perfectly matches the one produced in setup phase. Note that, for this application we do not need a secret key and the output of the physical function system acts as an identifier of the PUF that can be publicly known. That is the reason we do not need a fuzzy extractor and a secure sketch suffices. In chapter 3, we describe the pipeline of extraction procedure for Image-based PUFs consisting of image hashing and a code-offset secure sketch.

2.3 DIGITAL SIGNATURE SCHEME

The idea of combining cryptographic means such as digital signature schemes together with information extracted from the embedded PUF for authentication purpose was first applied in [7, 10, 28, 31, 32, 46]. The general idea is to digitally sign the product information (e.g. serial number or EPC code) together with the identifier extracted from the embedded PUF and use this

signature as the certificate of authenticity. This certificate can be either embedded in the product or stored in the database. The verifier checks the authenticity of the product by validating this certificate. The complete analysis of the anti-counterfeiting protocol using image-based PUF and signature scheme is given in chapter 5. Here, we bring the definition of a signature scheme. Then we define an unforgeable signature scheme against adaptive chosen-message attack which is used as a cryptographic primitive in the design of anti-counterfeiting system in chapter 5.

Definition 8 ([47]). *A signature scheme is a tuple of three probabilistic polynomial-time algorithms* $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ *satisfying the following:*

1. *The* key generation algorithm Gen *takes as input a security parameter* 1^n *and outputs a pair of keys* (pk, sk)*. These are called the public key and the private key, respectively. We assume that* pk *and* sk *each have length at least* n*, and that* n *can be determined from* pk*,* sk*.*

2. *The* signing algorithm Sign *takes as input a private key* sk *and a message* $m \in \{0,1\}^*$*. It outputs a signature* α*, denoted as* $\alpha \leftarrow \mathsf{Sign}_{sk}(m)$*.*

3. *The* deterministic verification algorithm Vrfy *takes as input a public key* pk*, a message* m*, and a signature* α*. It outputs a bit* b*, with* $b = 1$ *meaning valid and* $b = 0$ *meaning invalid. We write* $b := \mathsf{Vrfy}_{pk}(m, \alpha)$*.*

It is required that for every n*, every* (pk, sk) *output by* $\mathsf{Gen}(1^n)$*, and every* $m \in \{0,1\}^*$*, it hold that* $\mathsf{Vrfy}_{pk}(m, \mathsf{Sign}_{sk}(m)) = 1$*.*

Before defining an unforgeable signature scheme, the **signature experiment** $\mathsf{Sig} - \mathsf{forge}_{\mathcal{A}_s, \Pi_s}(n)$ is defined as follows:

Let $\Pi_s = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme, and consider the following experiment for an adversary $\mathcal{A}_s$ and parameter n.

1. $\mathsf{Gen}(1^n)$ is run to obtain keys (pk, sk).

2. Adversary $\mathcal{A}_s$ is given pk and oracle access to $\mathsf{Sign}_{sk}(m)$. The adversary then outputs (m, α). Let $\mathcal{Q}$ denote the set of messages whose signatures were requested by $\mathcal{A}_s$ during its execution.

3. The output of the experiment is defined to be 1 if and only if (1) $\mathsf{Vrfy}_{pk}(m, \alpha) = 1$, and (2) $m \notin \mathcal{Q}$

We now present the definition of an unforgeable signature scheme under an under an adaptive chosen-message attack as follows:

Definition 9. *([47]) A signature scheme* $\Pi_s = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ *is existentially unforgeable under an adaptive chosen-message attack if for all PPT* [3] *adversaries* $\mathcal{A}_s$*, there exists a negligible function negl such that*

$$Pr[\mathsf{Sig} - \mathsf{forge}_{\mathcal{A}_s,\Pi_s}(n) = 1] \leq negl(n).$$

An unforgeable signature schemes is used in the design of anti-counterfeiting system in chapter 5. Some examples of well-known unforgeable signature schemes include: RSA signature, Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) [42]. Based on performance and security requirements of the system, one of the mentioned schemes can be employed.

2.4 IMAGE PROCESSING

After presenting the background information on PUFs and some cryptographic tools, we place our focus on the signal processing and particularly image processing part of the work. Since we deal with images as the response of image-based PUFs, we need to integrate appropriate image processing techniques in the design of a practical system. In this section we point out specific image processing tools used to fulfill the above requirements in the design of image-based Physical Function System.

2.4.1 Image Pre-processing

An important role of image pre-processing is to reduce a fraction of evaluation noise between PUF responses in setup and reconstruction phases. Generally, the pre-processing algorithm is applied depending on characteristics of images of a specific image-based PUF. Some examples of typical noise reduction algorithms include median filtering [48], Non-local means denoising [49], and morphological filtering [50, 51]. For example gray scale morphological area *opening* removes from an image all the light structures that are smaller than the size parameter. Morphological area *closing* has the same effect on dark structures inside the image. In this thesis we use median and morphological filtering for noise reduction purposes, which is described more in chapter 4.

Note that noise reduction techniques reduce the noise but at the same time remove some small features on the image corresponding to the randomness existing on the physical component. It means that by reducing more noise, we lose more randomness. This compromise between noise and randomness exists in all the procedures dealing with PUF response including pre-processing,

[3] Probabilistic Polynomial Time

image hashing and extraction procedure and ultimately poses a compromise between robustness and physical unclonability.

Another important objective of image pre-processing is to adjust the images so that the images taken in setup and reconstruction phases are aligned together. This mainly enables efficient use of helper data. As an example, let us imagine a simple scheme where the helper data point out to some significant feature points (e.g., corners) inside the image . The helper data generated in setup phase is used later in reconstruction phase. It implies that to provide the same output for two images, they should be aligned together. In this thesis we perform the alignment by cropping the image to the framed region of PUF and utilize the framed region as the response of the PUF. Cropping the image to the framed region of PUF helps the responses be aligned in setup and reconstruction phases. There exist several methods to extract the boundary of an object inside the image that can be selected depending on the characteristics of images under study. In this work, we perform boundary extraction based on an appearance-based object recognition method which is described further in chapter 4 [52].

2.4.2 Gabor Hashing

As discussed earlier, a secure sketch scheme accepts a binary input. However, the response of the image-based PUF is a real-value image. Hence, we require that a specific processing (i.e., dimensionality reduction and binarization) be integrated with the extraction procedure. This step, which is called image hashing, can be carried out by means of various methods. In this part of the thesis, we summarize a method of image hashing based on utilizing Gabor transformation. This method has been proposed as an effective hashing algorithm applied to the response of optical PUFs [2, 10]. First, a Gabor basis function with the following form is applied to the response of the PUF:

$$g_\psi(b) = \frac{1}{a\sqrt{2\pi}} \sin(\nu \cdot (b-k)) \exp(-\frac{1}{4a^2}\|b-k\|^2). \tag{2.10}$$

The basis function $g_\psi(b)$ is the product of a plane wave with wave vector ν and a Gaussian with variance a centered on $k = (k_1, k_2)$. Gabor coefficients are thus obtained by projecting y on the Gabor basis functions as follows:

$$\langle g_\psi, y \rangle = \sum_{i=1}^{N} g_{\psi_i} y_i \cong G_\psi^T y, \tag{2.11}$$

where each column of G_ψ^T is a basis function g_{ψ_i}.

Next a number of the most robust Gabor coefficients (e.g., with largest absolute value) are selected and then binarized to form the binary string serving as the hash of the PUF response. The positions of most robust Gabor

coefficients constitute the first part of helper data. More details on the implementation of Gabor hashing are provided in section 3.2.4.

2.5 CONCLUSION

In this chapter we studied some background information and tools that are employed throughout this thesis. We first presented Physical Unclonable Functions and some of their applications. We then discussed that evaluating security properties of PUFs specially physical unclonability is not straightforward. Therefore, we referred to a recent work of Armknecht et al. that captures the important security properties of PUFs after introducing a general model of physical functions. The model together with the security properties of interest for our target application i.e., anti-counterfeiting have been defined. Two key security properties are robustness and physical unclonability. We then highlighted an important building block of physical function model i.e., extraction procedure. We discussed two important purposes of extraction procedure i.e., information reconciliation and privacy amplification. The primary purpose i.e., information reconciliation is usually accomplished by a secure sketch based on Error Correcting Codes. The second purpose, which is only needed for some security systems, is privacy amplification and is usually achieved by strong extractors or randomness extractors. We argued that for Image-based PUFs, using a secure sketch to achieve information reconciliation suffices because the output of the system acts as an identifier of the object and does not need to be secret as it is the case for a cryptographic key. We thus described the code-offset secure sketch scheme as a popular tool used in literature to achieve information reconciliation. Next, we brought the definition of unforgeable signature scheme as another cryptographic component used in the design of anti-counterfeiting scheme. We also listed some popular candidates of signature schemes to be used in practice. We finally summarized image processing tools employed in this work i.e., image pre-processing and Gabor hashing methods. The detailed description of the image processing tools is presented in following chapters.

CHAPTER 3

IMAGE-BASED PHYSICAL FUNCTION SYSTEM

Image-based PUFs have been receiving special attention for anti-counterfeiting applications. Image-based PUFs represent the specific category of PUFs based on random visual features of physical objects evaluated by an imaging method. By imaging we mean any method that outputs images representing a 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).

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 [3, 4]. 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 [4]. The signals from the photo detectors are coupled and then digitized to form the PUF response which serves as the PUF identifier. Clarkson et al. present a low-cost evaluation of paper random profile using commodity scanners [5]. They acquire the 3D profile of a paper using the scans taken from different orientations of the paper in the scanner. Another approach is introduced in [6] 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 [53]. In [7–9], the authors 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. Despite of an extra cost caused by an additional procedure, this method turns out to be more robust against possible paper distortions such as shrinkage. Phosphor PUF is also proposed where phosphor particles are blended with the material with the cover of the product, e.g., plastic cover to form the random pattern [16, 17]. In their approach, image processing and fuzzy extraction procedures are applied on the image of phosphor profile to produce the identifier. 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,... for identification purpose [54]. They have employed digital communication concepts along with robust perceptual hashing to design a secure identification protocol. Optical PUFs proposed by [2] can also be considered an Image-based PUF, as its response is a speckle pattern represented by an image. We also see later that the same image hashing procedures applied to optical PUFs such as Gabor Binary Hashing are also appropriate for most Image-based PUFs. However, in this thesis, as we believe that Image-based PUF 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 a large amount of unpredictable challenge response pairs allows using optical PUFs for more advanced security applications such as remote authentication [31] or secret key generation [32].

For most proposed PUFs, the properties of the system is objectively assessed by intra-distance (distance between outputs of different PUFs) and inter-distance (distance between outputs of different observations of the same PUF) characteristics [26]. The inter- and intra-distance characteristics are often summarized by 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 the uniqueness of different PUF responses while intra-distance illustrates the observation noise.

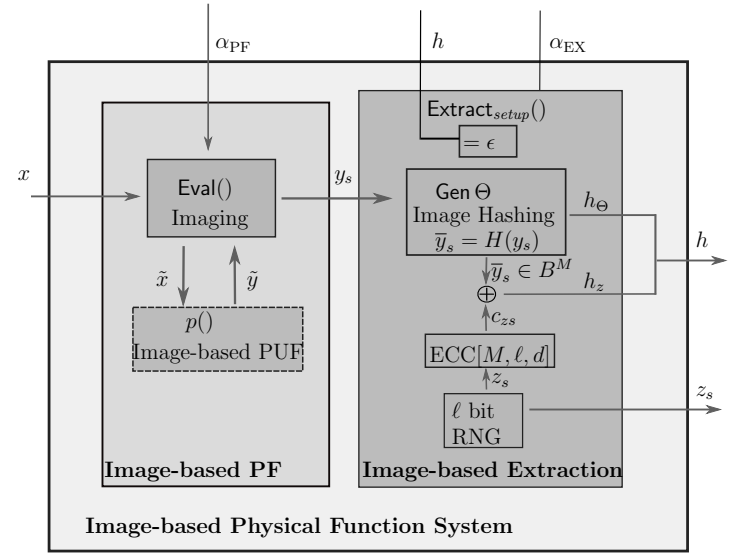
Although inter- and intra-distance characteristics are good indicators of system properties, they cannot be directly accredited by security systems.

As discussed above, the proposed methods to deal with different Image-based PUFs are very diverse. The characterizations of their security properties are also carried out using various approaches. It is therefore beneficial to put them under the same roof and design a unified framework that can be applied to most existing and new Image-based PUFs. In this thesis, in order to build a unified model dealing with Image-based PUFs, we specialize the general framework of physical functions [1] to the case of Image-based physical function. This specialization also allows us to use formalizations provided by [1] to concretely evaluate security properties of the system. Based on these formalizations, we provide a methodology to experimentally analyze the properties of Image-based physical function systems in chapter 4. The methodology serves as an asset to fairly compare different Image-based PUFs for a specific application. We also provide practical implementations of system components i.e., Image-based PUF, evaluation process, and Image-based extraction including image hashing and secure sketch. We introduce two new types of Image-based PUFs called Laser-written PUF and Crystal PUF. The relevance of the framework is further demonstrated by its accordance to these practical examples of Image-based PUFs. We also present two practical adaptive and non-adaptive image hashing methods called Gabor Binary Hashing and Random Binary Hashing. The former is an adaptation of an existing method [10] and the latter is our contribution as a fast candidate for image hashing.

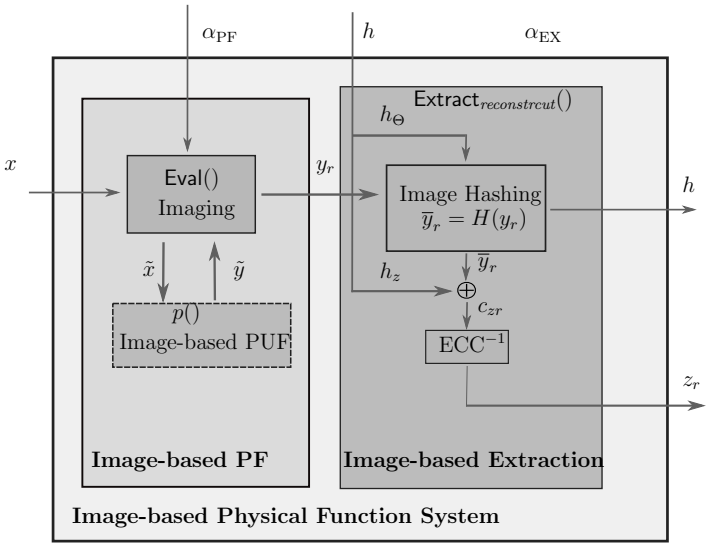
In the rest of this section, we present our specialization of the general framework of physical functions to Image-based PUFs with a particular focus on image hashing. We then provide practical instantiations of system components including Laser-written PUF, Crystal PUF, Gabor Binary Hashing and Random Binary Hashing.

3.1 IMAGE-BASED PHYSICAL FUNCTION SYSTEM

Image-based physical function systems include an Image-based Physical Function and an Image-based Extraction including an image hashing and a code-offset secure sketch [29]. Fig. 3.1 illustrates an Image-based physical function system in the setup and reconstruction mode. For the sake of simplicity, the creation process of the PUF is not included in the model. Let us describe the ingredients of the system in detail.



(a) Setup mode.



(b) Reconstruction mode.

Fig. 3.1.: Image-based physical function system.

3.1.1 Image-based Physical Function

Image-based Physical Function includes a physical component p and an evaluation procedure Eval. The physical component p (See Fig. 3.1) is a piece of a physical object containing random visual features. The challenge x is considered as the type of illumination used to take the images. 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 chapter, we assume only one fixed challenge because for our main target application, i.e., anti-counterfeiting, we do not need a function but just an output that acts as an identifier to authenticate the object (further described in chapter 5). We also assume a fixed transversal and longitudinal and resolution of the Eval procedure such that the response of the PUF 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 [1].

3.1.2 Image-based Extraction

The extraction procedure Extract of Image-based PF System, hereafter called Image-based Extraction, includes an image hashing procedure combined with a fuzzy commitment scheme or code-offset secure sketch scheme [29, 43]. As described earlier, the response of the Image-based physical function is a real-valued image with a high dimension but the secure sketch accepts a limited-size 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 later on). The code-offset secure sketch is used to decrease the error rate of PF responses by using Error Correcting Code (ECC) and code-offset construction.

3.1.2.1 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 this view, image hashing encompasses compression and quantization steps. Image hashing is

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

thus defined as:

$$h : \mathbb{R}^N \to \mathcal{B}^M,\ y \mapsto \overline{y} = H(y) = \mathrm{sign}_{\mathrm{b}}(\Theta y), \tag{3.1}$$

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 images from different observations of the same PUF give similar hash values, while images from different PUFs give different hash values with high probability [2]. 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, distinguishability of PUF 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). For a set of Image-based PUFs where inter-distance histogram of the images does not significantly overlap with the intra-distance histogram[3], image hashing 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, an image pre-processing can be performed as a first step of image hashing to enhance intra-distance distribution by reducing the evaluation noise. It reduces the evaluation noise such as ambient light change and compensates misalignment or disorientation by applying an appropriate alignment method as described in section 2.4.1.

In this part of the thesis, using the theory of sparse signal representation [55], we briefly introduce the concept of adaptive and non-adaptive compressing of the image prior to the quantization. In section 3.2.3 and 3.2.4, we present 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

[2] This contributes, together with the secure sketch to provide the same value for the same PUF and independent values for different PUFs.

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

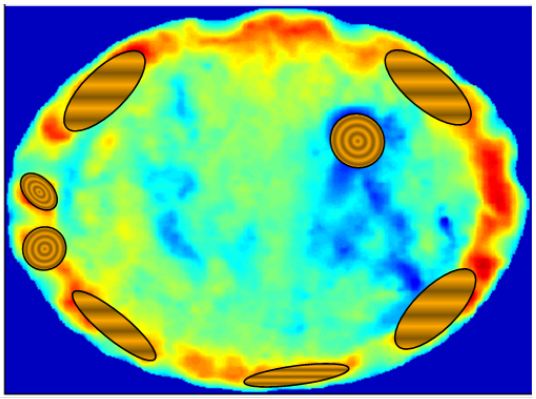


Fig. 3.2.: A view of representing an image using its sparsity basis functions.

a certain basis ψ (e.g., Fourier, Wavelet, Gabor, Curvelet), if there exists a representation of y using at most J significant (non-zero) coefficients α_i [56].

Adaptive compressing of the signal accounts for a J-term approximation. It consists of the terms of α with J largest magnitudes while setting all the other terms to zero [57]. Fig. 3.2 gives a view of how an image is represented using some representative basis functions.

Non-adaptive compressing (known as Compressed Sensing) [58], [59] is based on the fact that a signal that is sparse in one basis can be represented non-adaptively to a quality similar to that of a J-term approximation from $M = \mathcal{O}(J \log N/J)$ linear projections onto a basis Φ that is incoherent with the sparsity basis [4]. 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 are usually used to perform non-adaptive compressing. Fig. 3.3 illustrates how an image is represented by projecting it onto random matrices.

The sparsity of the signal plays a significant role in how accurate it can be characterized 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 a random value. Because, completely random images can not usually be sparsified in any known sparsity bases. In this case, both adaptive and non-

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

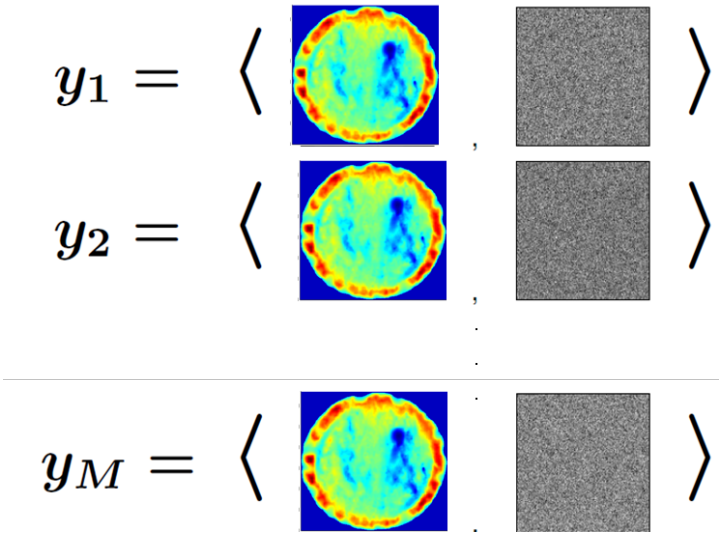


Fig. 3.3.: A view of representing an image using non-adaptive compressing.

adaptive methods seem to fail. In practice, the condition of having medium-entropy images holds for most existing Image-based PUFs. We thus believe that adaptive and non-adaptive methods are efficient tools to hash the response of Image-based PUFs in most cases.

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). In contrast, for non-adaptive hashing the sensing matrix Θ is selected independently (e.g., randomly) from the image. The implementation of non-adaptive hashing is therefore faster than the adaptive one because the sensing matrix is selected without the need to first process the image. In section 3.2.3 and 3.2.4, we describe the instantiations of non-adaptive and adaptive image hashing methods, namely Random Binary Hashing and Gabor Binary Hashing respectively. In section 4 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 thesis.

3.1.2.2 Secure Sketch Scheme

As described in section 2.2, we have used a code-offset secure sketch scheme [29] which is equivalent to a fuzzy commitment scheme [43]. By merging image hashing and the code-offset secure sketch described in section 2.2, the pipeline of Image-based Extraction in the setup and reconstruction steps is as follows:

In the **setup phase** (see Fig. 3.1), 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 $c_{zs} \in \mathcal{B}^M$. For that, a randomly chosen string $z_s \in \mathcal{B}^\ell$ with $\ell < M$ is encoded to a random code-word $c_{zs} \in \mathcal{B}^M$ using a ECC(M, ℓ, d). For ECC, ℓ is the size of input (message), M is the size of code-word and d is the minimum Hamming distance between code-words. The redundancy added to the input by transforming it into a larger code-word ($M > \ell$) enables using a suitable decoding algorithm to detect and correct up to $t = \lfloor (d-1)/2 \rfloor$ errors in the code-word [60]. The offset between $\overline{y}_s$ and c_{zs} constitutes the second part of helper data $h_z = \overline{y}_s \oplus c_{zs} \in \mathcal{B}^M$ 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 $c_{zr} = \overline{y}_r \oplus h_z$. The noisy code-word c_{zr} can then be decoded to the correct code-word c_{zs} 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_{zs}. If dist$(\overline{y}_s, \overline{y}_r) > t$, then no guarantee is provided about the output of reconstruction phase [29].

3.2 PRACTICAL IMPLEMENTATION

Having specialized the framework of physical functions to Image-based PUFs, let us show the relevance of our approach by instantiating the system com-

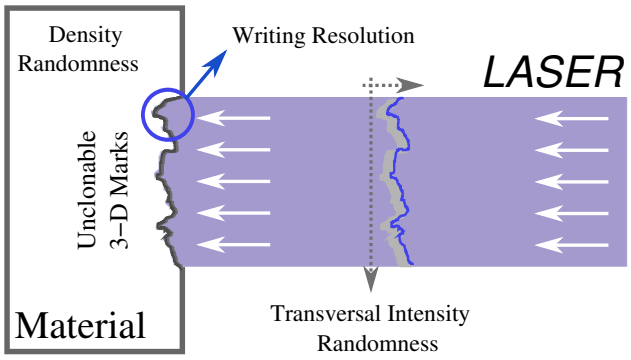


Fig. 3.4.: Creation process of a Laser-Written PUF

ponents by two practical Image-based physical functions and two practical Image-based extraction methods. We introduce two new Image-based physical functions called Laser-written PF and Crystal PF. We also instantiate image hashing part of Image-based extraction by two examples of image hashing i.e., Random Binary Hashing and Gabor Binary Hashing.

3.2.1 Laser Physical Function: Laser-Written PUF and WLI Evaluation

As a technological achievement of the TOMO3D project [61], we introduce a new Image-based PUF called Laser-Written PUF which is evaluated using a White Light Interferometry evaluation procedure. 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. Therefore, the mark profile shows a spatial variability that cannot be reproduced, at least with reasonably inexpensive technology. 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 (consider laser marks in the gemstones). It is also robust against aging especially when embedded on the bulk of the object.

The creation process $\mathsf{Create}(\alpha_{\mathrm{CR}}) \rightarrow p$ of LPUF (See Fig. 2.2) 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 such as laser beam frequency, intensity, diameter. The physical component p is the laser mark containing random features. The ran-

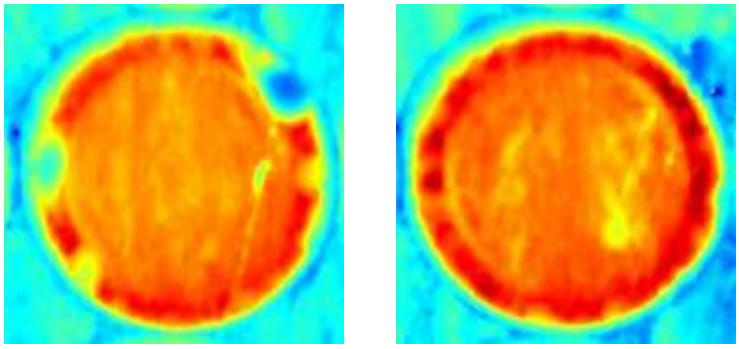


Fig. 3.5.: Two laser depth profiles.

domness relates to the creation parameter and the uncontrollable engraving variability due to both laser beam instability and random density of the object material. Fig. 3.4 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. In our case study, laser marks are engraved by focusing the beam of an excimer laser on a glass substrate. The laser wavelength is 193nm, its power is 130mW and its frequency is 200Hz. Three laser shots are used to create laser marks. The imprinted pattern is a 100×l00 matrix of 60 micron-diameter laser marks. The mean ablation depth is 350nm. The evaluation process Eval has been performed by White Light Interferometry (WLI) method implemented with a Mirau interferometer [62, 63]. For more detailed description of White Light Interferometry see Appendix-A. The challenge x is fixed to a simple white light i.e., a 4mW LED with wavelength 638nm. The response signal $\tilde{y}$ is the intensity of reflected beam from the object surface interfered with a reference beam that is captured with a CCD camera and then converted to the digital image y representing depth profile of laser marks (see Appendix-A). The evaluation parameter α_{PF} includes nanometer depth resolution and submicrometer traverse resolution which are fixed by design. The typical response (digital image) y of the WLI evaluation process for two different laser marks engraved on a glass substrate in the same condition are shown in Fig. 3.5.

3.2.2 Crystal Physical Function: Crystal PUF and digital camera evaluation

As a technological achievement of the TRACEA project [64], we introduce another type of Image-based PUF called Crystal PUF (CrPUF) to be applied for low-cost anti-counterfeiting. The cost of creating and evaluating a CrPUF can be very low, relatively to a desired level of security. It makes CrPUF particularly attractive to prevent counterfeiting of cheap products. Crystal PUF is based on a random crystal structure formed in a substrate cavity. The random crystal structure is the result of a natural but complex process of evaporation and crystallization of a polymer solution in its solvent. Creation process $\mathsf{Create}(\alpha_{\mathrm{CR}}) \rightarrow p$ consists in pouring a polymer solution in its solvent and letting it evaporate and crystallize in a substrate cavity. Fig. 3.6 illustrates the creation process of a CrPUF. For detailed description of the crystallization procedure refer to Appendix-B. The creation parameters α_{CR} include, among others, the nature of the polymer, choice of the solvent, concentration of the polymer in the solvent, temperature etc. After evaporation and formation of the crystal structure in the cavity, a transparent covering layer is added to prevent crystal distortion by time or by malicious tampering.

In our case study, the polymer i.e., polypropylene (PP) is solved in xylene with the concentration 2 $g/100ml$. The solution with the quantity 1.5 μl is poured in the substrate of size ($4mm \times 4mm\times$ 0.2 mm). The xylene evaporates in the room temperature.

We aim to capture 3D profile of CrPUF using 2D cameras (to keep the evaluation procedure low-cost). The reason to use 3D profile is to prevent the adversary to bypass the authentication process by a fake 2D copy of the image of the PUF [5]. To capture 3D profile, evaluation process can be carried out using various images taken from different angles of view (between camera and PUF) and different illumination angles (between illumination source and PUF). Imaging from different angles of view is costly. Because either more than one camera is needed to take the images with different angles of view, or one camera should be moved with respect to the PUF. Both methods force extra cost and higher overhead time. A cost-efficient method in the production line is to fix the angle of view and take the images of CrPUF when illuminated from different angles. Fig 3.7 illustrates this process using two illumination sources oriented with azimuthal angles θ_1 and θ_2 and inclination angles ϕ_1 and ϕ_2.

Because of the existence of mountains and valleys in the profile of crystals, each oriented illumination lightens some mountains constructing corre-

[5] Recall that for Laser PUF, the images already corresponds to the 3D profile of the marks.

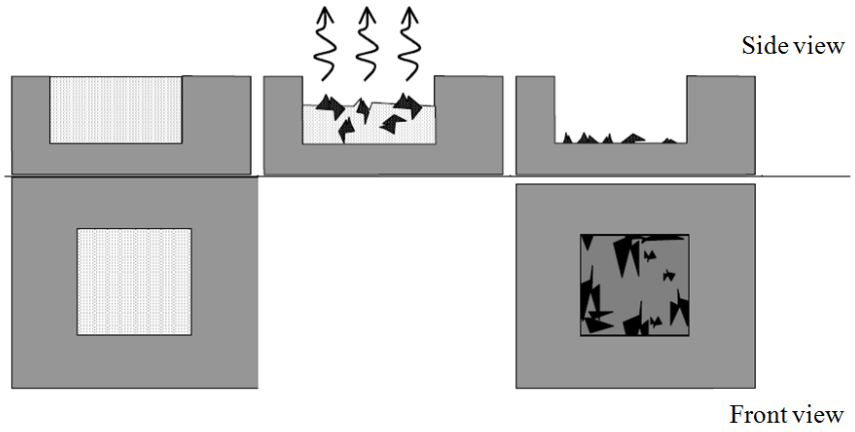


Fig. 3.6.: Creation process of a Crystal PUF

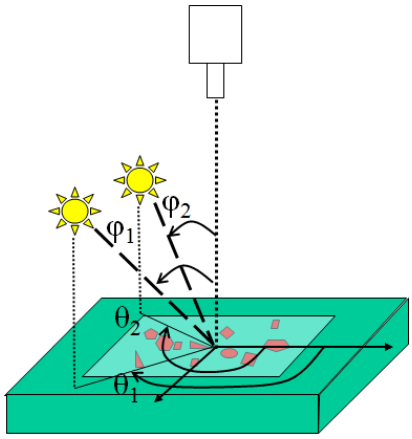


Fig. 3.7.: Using different illumination angles to capture 3D profile of a Crystal PUF.

sponding shadow regions. In this view, each image taken with an oriented illumination partly represents 3D profile of the CrPUF.

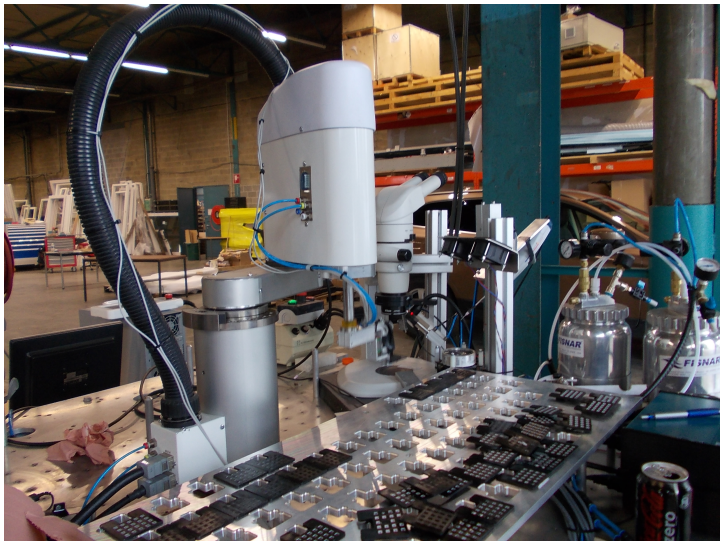


Fig. 3.8.: Crystal PUF creation and evaluation setup.

In the framework of physical functions, the challenge x represents the set of illumination angles used to take the images. A set of images taken with these illumination angles is considered as the response y. Evaluation parameter α_{PF} includes, among others, the specifications of the digital camera and the illumination source.

In our case study, the challenge consists of two illuminations with $(\theta_1, \phi_1) = 0°, 45°$ and $(\theta_2, \phi_2) = 90°, 45°$(See Fig. 3.7) [6]. A halogen lamp in an illuminator is used which brings the light through optic fibers and mini-lenses to the place to illuminate. The response y is the set of two images taken from two illumination angles by means of a digital microscope (SMZ80 Nikon) and a high resolution $B\&WCCD - IRIS$ camera. The setup used to create and evaluate CrPUFs is depicted in Fig. 3.8.

Fig. 3.9 shows two images of a CrPUF taken from two illumination angles. Although the difference between images in this figure is negligible, in order to keep the system more general we use both images. The reason is that the difference between images depends on creation parameters of CrPUF and is observed to be more significant with other creation parameters (excluded in figures because they are not evaluated in this thesis).

[6] As mentioned previously the challenge is fixed, because for our anti-counterfeiting scheme, it suffices to have a fixed challenge-response pair.

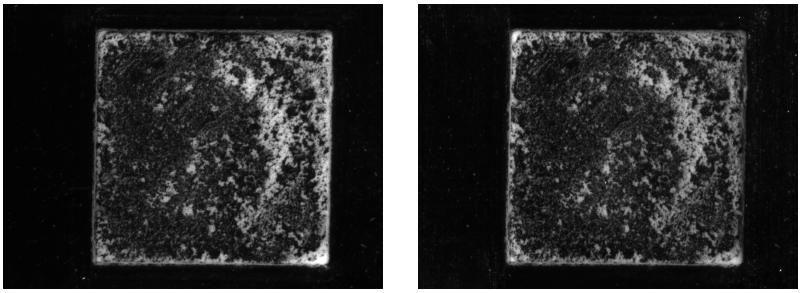


Fig. 3.9.: Image of a Crystal PUF taken with illumination angles (a) $(\theta_1, \phi_1 = 0°, 45°)$ and (b) $(\theta_2, \phi_2 = 90°, 45°)$

3.2.3 A non-adaptive image hashing: Random Binary Hashing

As discussed previously, the random matrix is incoherent with most known basis functions and can be efficiently applied for non-adaptive compressing. In this view, we instantiate non-adaptive image hashing by Random Binary Hashing as follows. 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 [7] uniformly distributed random matrix $\Phi_{ij} \sim_{\text{iid}} \pm 1/\sqrt{M}$ and many other sub-Gaussian distributions [65].

This random matrix is used as the sensing matrix Θ (See Eq. 3.1) for the image hashing. Random Binary Hashing H_R is thus defined by:

$$H_R : \mathbb{R}^N \to \mathcal{B}^M, \;\; y \mapsto \overline{y_R} = H_R(y) = \text{sign}_{\text{b}}(\Theta_R y), \tag{3.2}$$

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

$$\Pr\left[\, \left|\, \tfrac{1}{M}\text{dist}_{\text{H}}(\overline{y}, \overline{w}) - \text{dist}_\angle(y, w) \,\right| \geq \beta \,\right] \;\leq\; 2\, e^{-2\beta^2 M}. \tag{3.3}$$

This may be proved by first showing that, thanks to the isotropy of the Gaussian distribution and whatever the component $1 \leq i \leq M$, $\Pr[\overline{y_i} \oplus \overline{w_i} = 1] = \pi^{-1}\, \text{dist}_\angle yw$, as given by the probability that y and w are separated by a

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

plane normal to $\varphi_i = (\Phi_{ij})_{1\leq j\leq N}$ and containing the origin, and second, by observing therefore that $M\, d_H(\overline{y}, \overline{w})$ follows a binomial distribution $B(M, p)$ of M trials of success probability $p = \text{dist}_{\angle} yw$ that exponentially concentrates around its mean Mp when M increases [66, 67].

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 [68] 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,...) for $M = \mathcal{O}(\beta^{-2} J \log(N/J))$. They also investigate the resistance of binary random hashing in the presence of the evaluation noise. They show that for a Gaussian evaluation 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 $\text{dist}_{\angle}(\overline{y}_s, \overline{y}_r) \leq C\sigma_o$ with a constant C. This property(resistance of hashing against observation noise) is confirmed in our experiments.

Random Binary Hashing H_R reduces the dimension while preserving the distances (as measured by angle) between the images. Therefore it can be employed to hash the images when their inter-distance does not significantly overlap their intra-distance. Random Binary Hashing offers a fast and efficient hashing of the images and an effective constitution of helper data (sensing matrix) that is independent of the images. Another interesting advantage of Random Binary Hashing is that it can be integrated in the imaging hardware that makes the implementation of the algorithm quite fast and easy [69].

3.2.4 An adaptive image hashing: Gabor Binary Hashing

In Gabor Binary Hashing method, adaptive compressing relies on the use of 2-D Gabor basis functions as the sparsity basis [2, 10, 38]. Olshausen et al. 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 (See Fig. 3.10) [70] . 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.

Following the introductory description of Gabor hashing in section 2.4.2, in this part we provide the exact implementation of Gabor Binary Hashing as an example of adaptive image hashing. Gabor Binary Hashing presented in following is very similar to an existing Gabor-based hashing used to process optical PUF speckle pattern [10, 33]. 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,...) [56] when necessary.

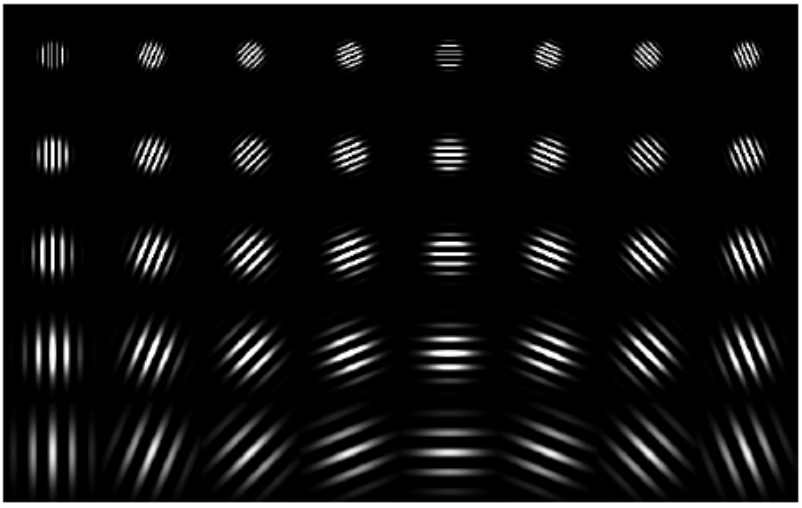


Fig. 3.10.: The schematic of Gabor basis functions.

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

$$g_\psi(b) = \frac{1}{a\sqrt{2\pi}} \sin(\nu \cdot (b-k)) \exp(-\frac{1}{4a^2}\|b-k\|^2), \tag{3.4}$$

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 $\psi = (a, \nu, k) \in \mathbb{R}_+ \times \mathbb{R}^2 \times \mathbb{R}^2$. The basis function $g_\psi(b)$ is the product of a plane wave with wave vector $\nu \in \mathbb{R}^2$ 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:

$$\langle g_\psi, y \rangle = \sum_{i=1}^{N} g_{\psi_i} y_i \cong G_\psi^T y, \tag{3.5}$$

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.

In our experiment, 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:

$$\begin{aligned}\Psi(a,\nu_0,\Delta) \;=\; \big\{&(a,\nu_f,k_m):\\ &\nu_f=\nu_0(\sin\theta_f,\cos\theta_f),\ \theta_f=2\pi f/F,\ 0\le f<F,\\ &k_m=(m_1\Delta,m_2\Delta),\ 0\le m_i<\lfloor N_i/\Delta\rfloor, i\in\{1,2\}\big\}.\end{aligned}\tag{3.6}$$

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 i^{th} strongest value[8] of $\mathcal{G}_{a,\nu_0,\Delta}$ and let $\Theta_G=[G_{\psi^{(1)}},G_{\psi^{(2)}},...,G_{\psi^{(M)}}]^T$ 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. 3.1) for the image hashing. Gabor Binary Hashing H_G is thus defined by:

$$H_G:\mathbb{R}^N\to\mathcal{B}^M,\ y\mapsto\overline{y_G}=H_G(y)=\mathrm{sign}_{\mathrm{b}}(\Theta_G y).\tag{3.7}$$

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

Let us justify why the largest Gabor coefficients are selected before being quantized.

If the dictionary $\mathcal{D}$ of all possible Gabor basis functions were an orthonormal basis , the best *M-term* approximation of $y\in\mathbb{R}^N$ would be given by $y_M\in\mathbb{R}^M$ as follows [9]:

$$y_M=\Theta_G^T\Theta_G y.\tag{3.8}$$

It means that for all w such that $w=\mathcal{D}\alpha=\sum_{i=1}^{\#\mathcal{D}}\alpha_i g_i$ where $\|\alpha\|_0\le M$,

$$\|y-y_M\|\le\|y-w\|.\tag{3.9}$$

In other words, the largest Gabor coefficients $\Theta_G y$ are the best representatives of the original image among all possible combinations of coefficients. Although, we can no longer guarantee the best approximation argument after quantizing these coefficients to build the fingerprint, we can still assume that the quantized value provides a good approximation of the image features. This is due to the fact that the quantized coefficients of a vector are living in the same orthant of the vector formed by the unquantized coefficients. Moreover, the volume of this orthant is decreasing by increasing the space dimension that is M here. In our experiments, we restrict the Gabor basis parameters to the non-overlapping lattice $k_m=(m_1\Delta,m_2\Delta)$ in the spatial domain and

[8] In absolute value sense.

[9] A set of vectors which forms a basis is an orthonormal basis if all vectors in the set are mutually orthogonal and all of unit length.

whatever the frequency and the orientation of the kernels ν_f, in cases where the tail of Gaussian envelope is roughly bounded within the grids ($4a < \Delta/2$), the kernels are not overlapping and the Gabor basis functions are close to the orthonormal basis.

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.

Finally, it is worth to remark that there exist other alternatives to perform hashing based on techniques used for perceptual image hashing. The examples include hashing based on Scale Invariant Feature Transform (SIFT) [71], Radon Soft Hash algorithm [72–74] and Block Mean Value Based Hash [75]. It remains to investigate the performance of these methods as a future study. However, it is clear that the selection of an appropriate hashing method ultimately depends on the specifications of images of the Image-based PUF under study.

3.3 CONCLUSION

In this chapter we highlighted a specific category of PUFs called Image-based PUFs and studied various examples existing in the literature. We discussed about the need to provide a unified framework dealing with most existing and new Image-based PUFs. To this end, we proposed a unified model of Image-based physical function system by specializing the generic framework of physical functions [1]. The proposed Image-based physical function system enables a systematic design of system components. It also allows concrete evaluation of its security properties, namely robustness and physical unclonability which are required by most security systems. Different components of Image-based physical function system have been described and also instantiated with practical examples. In this context, as technological outcomes of two Belgian projects, we have introduced two new Image-based PUFs. Laser-written physical function offers a benefit of being a concrete solution that is robust against aging and can be applied to protect against cloning of valuable objects such as gemstones. On the other hand, Crystal physical function has been proposed as a tool to be applied to low-cost anti-counterfeiting because of its very cheap creation and evaluation procedures.

Moreover, as an attempt to model various image hashing methods, we categorized them into adaptive and non-adaptive methods and discussed which one should be selected based the images under study. We also instantiated non-adaptive and adaptive image hashing methods by Random Binary Hashing

and Gabor Binary Hashing, respectively. To our knowledge, it is the first time that Random Binary Hashing has been applied to hash the PUF response. For Gabor Binary Hashing, we extended an existing method and presented more detailed formalizations of the method and its properties [2, 10].

CHAPTER 4

EXPERIMENTS

In this chapter we come back again to the question of determining to what extent a certain Physical Function System fulfills the requirements of a specific security application. We experimentally evaluate two key properties required by almost all security systems i.e., robustness and physical unclonability. In chapter 3, we specialized the generic framework of physical functions to the case of image-based PUFs. In chapter 2 we discussed how this generic framework allows a meaningful analysis of robustness and physical unclonability considering the fact that the PUF is barely used alone and it is usually combined with an extraction algorithm.

In this chapter we propose a methodology to experimentally evaluate robustness and physical unclonability based on the definitions provided in chapter 2. To this end, we first study datasets of responses (images) of two physical functions described in chapter 3 namely Laser physical function and Crystal physical function. The datasets are constructed to statistically evaluate robustness and physical unclonability. Next, we present the implementation settings of the extraction procedure including Random and Gabor Binary Hashing methods and error correcting part of secure sketch scheme. Robust-

ness and physical unclonability are then evaluated for both physical functions and both image hashing methods. Additionally, we investigate the accuracy of the binomial approach used in prior work for analysis of robustness and unclonability. We demonstrate that for our instantiation of physical function system, the binomial approach does not provide very reliable results especially for physical unclonability. Finally, we evaluate the key property of a physical function system i.e., the trade-off between robustness and physical unclonability. To the best of our knowledge, this evaluation has been carried out for the first time in this work. One can fairly compare the ultimate performance of different physical function systems by studying the trade-off between robustness and physical unclonability.

4.1 DATASETS AND PRE-PROCESSING

We evaluate robustness and existential physical unclonability of the examples of image-based physical function system which includes two physical functions i.e., Laser PF and Crystal PF and two extraction methods based on Random and Gabor Binary Hashing methods. Hereafter, image-based Extraction using Random Binary Hashing and Gabor Binary Hashing methods are called RbEX (Random-based-Extraction) and GbEX (Gabor-based-Extraction) respectively. For both PFs two datasets named $\mathcal{D}_1$ and $\mathcal{D}_2$ have been constructed to evaluate robustness and physical unclonability respectively. The first dataset $\mathcal{D}_1 = \{y_{pq},\ 1 \leq p \leq P,\ 1 \leq q \leq Q\} \subset \mathbb{R}^N$ contains P different PUFs evaluated Q times. The second dataset $\mathcal{D}_2 = \{y_r,\ 1 \leq r \leq R\} \subset \mathbb{R}^N$ contains R different PUFs evaluated once. For Laser PF $P = 20$, $Q = 100$, $R = 1000$ and $N = N_1 N_2 = 340 \times 340 = 115\,600$. For Crystal PF $P = 100$, $Q = 20$, $R = 600$ and $N = 2N_1 N_2 = 2 \times 860 \times 860 = 147\,9200$. Note that, as we are limited to the amount of samples in our datasets, we assume that these number of samples are sufficient to perform fair statistical analysis of the system properties.

Each image y has been first pre-processed. As described in chapter 3 image pre-processing can be considered as a first step of image hashing which is excluded in the image-based physical function model for the sake of simplicity. Let us describe the pre-processing procedure applied on the images of Laser PF and Crystal PF. For both PF images, we first apply mean normalization to compensate measurement noise due to ambient light change. Mean normalization consists of subtracting from the image the irrelevant information that is contained in the mean of the image. Then, a morphological noise removal is applied consisting of area *opening* to remove the light structures which are smaller than a certain size and area *closing* which has the same effect on dark structures [50, 76]. In our construction, the structuring element

to perform opening and closing is set to a disk with radius (Ra). The radius is then experimentally optimized according to final performance of the system. Further information on how to select this parameter is given in section. 4.7. The subsequent processing is applied differently for Laser PF and Crystal PF as follows.

For Laser PF, we extract the framed region of the PUF in the image. For that, the objects inside the image are recognized and the one with the size similar to that of laser mark is selected. The extracted region of the image is considered as the pre-processed PF response (y in the datasets).

For Crystal PF, as described in section 3.2.2, the response y is the set of two images taken with two different illumination angles i.e., $y = \{y_1, y_2\}$. After applying noise reduction methods described above, we use an intensity-based image registration by maximization of mutual information to align two images [77]. For that, one image is fixed as a reference and the other image is spatially transformed to align with a reference image by maximizing the mutual information between two images $I(y_1; y_2) = H(y_1) + H(y_2) - H(y_1, y_2)$. Where $H(y_1)$ and $H(y_2)$ are the marginal entropies of two images and $H(y_1, y_2)$ is their joint entropy.

Finally, two images are cropped to the framed region of PUF inside the images i.e., $\tilde{y}_1$ and $\tilde{y}_2$ and concatenated to construct the pre-processed response $y = (\tilde{y}_1 \| \tilde{y}_2) \in \mathbb{R}^N$ where $N = 2N_1N_2$. For the sake of consistent notation the pre-processed response is again called y. The cropping used for Laser PF did not provide reliable results for Crystal PUF due to the specific structure of Crystal images. Thus the cropping is performed by another appearance-based object recognition method described as follows [52]. A template image is built with the appearance of PUF (i.e., a square with a certain size). This template is then matched to the image and the place where they mostly match is regarded as the center of the PUF. Finally the framed region of the PUF is cropped around the center. In our construction, the main reason to perform aligning before cropping is as follows. We experimentally observed that aligning two images prior to cropping leads to more reliable cropping performance. The reason is that the alignment before cropping allows to apply the cropping algorithm on the maximal image that is the maximization between two aligned images which experimentally leads to better cropping performance. Also, after alignment, we only need to find a crop region for one image and apply it to the other.

4.2 PRELIMINARY ANALYSIS OF THE DATASETS

Before applying image extraction on the images, we analyze the distinguishability of the images to get an intuition about the amount of noise and random-

ness inside the images of the datasets. The distinguishability is characterized by exploring the Euclidean distance between images from different evaluations 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-class and inter-class Euclidean distances between PUF images are calculated by:

$$D_{intra} = \big\{\text{dist}(y_{pq}, y_{pq'}) : \\ y_{pq}, y_{pq'} \in \mathcal{D}_1, 1 \leq p \leq P,\ 1 \leq q, q' \leq Q, q \neq q'\big\}, \tag{4.1}$$

and,

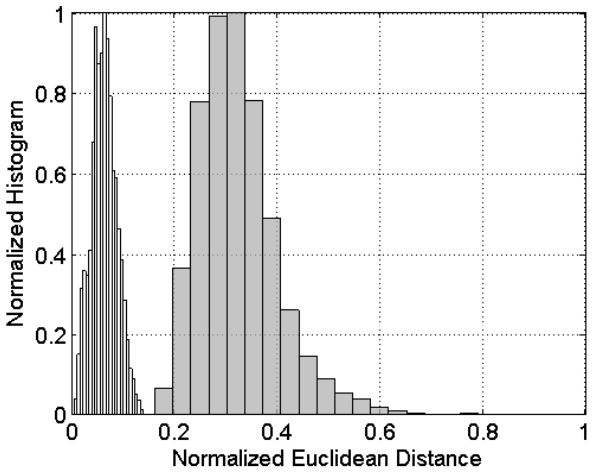
$$D_{inter} = \big\{\text{dist}(y_r, y_{r'}) : \\ y_r, y_{r'} \in \mathcal{D}_2,\ 1 \leq r, r' \leq R, , r \neq r'\}. \tag{4.2}$$

The number of comparisons made to estimate histograms is thus $P\binom{Q}{2}$ for intra-distance and $\binom{R}{2}$ for inter-distance. Fig. 4.1(a) and Fig. 4.1(b) illustrate the normalized histograms[1] of intra and inter-class normalized Euclidean distances [2] for Laser PF and Crystal PF respectively.

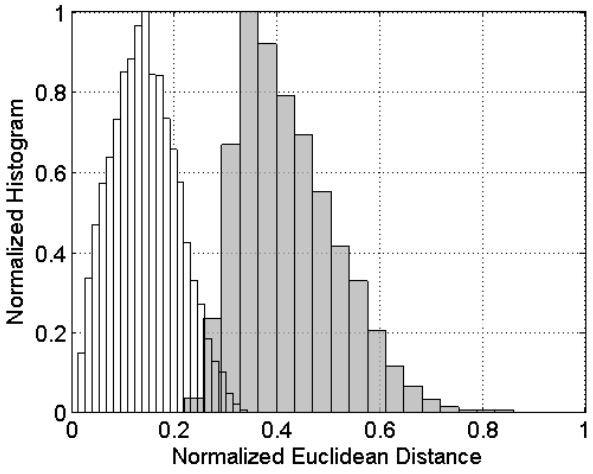
For Laser-Written PUF, the statistical mean and standard deviations of intra and inter-class normalized Euclidean distances are obtained as $(\mu_{intra}, \sigma_{intra}) = (0.06, 0.02)$ and $(\mu_{inter}, \sigma_{inter}) = (0.32, 0.08)$ respectively. For Crystal PUF, $(\mu_{intra}, \sigma_{intra}) = (0.14, 0.06)$ and $(\mu_{inter}, \sigma_{inter}) = (0.42, 0.1)$. This information already implies that CrPUF has more evaluation noise and more randomness between images.

As described before, histograms of intra- and inter-distances give the intuition about the evaluation noise and randomness (uniqueness) of PUF responses respectively. We visually observe that, for the case of Laser PF, inter-distance histogram of the images does not significantly overlap with the intra-distance histogram. Therefore, as described in section 3.1.2.1, we predict that both adaptive and non-adaptive image hashing will provide reasonable results. For Crystal PUF images, there exists more overlap and thus we predict that Random Binary image hashing might not provide good results. The reason is that as described in section 3.2.3 and Eq. 3.2, Random Binary Hashing reduces the dimension while trying to preserve the distribution of angle distances (i.e., similar to that of Euclidean distances) between the images. Therefore, we can not expect that it improves the distribution of Euclidean distances towards better discrimination between intra and inter-class distances after hashing. However, we apply both RbEX and GbEX for both physical functions and compare their results in terms of robustness and physical unclonability.

[1] Whereby the counts are replaced by the normalized counts such that the maximum frequency equals 1.
[2] Whereby the maximum Euclidean distance is normalized to 1.



(a)



(b)

Fig. 4.1.: Histogram of intra-class (white) and inter-class (gray) Euclidean distances for (a) Laser-Written PUF and (b) Crystal PUF images.

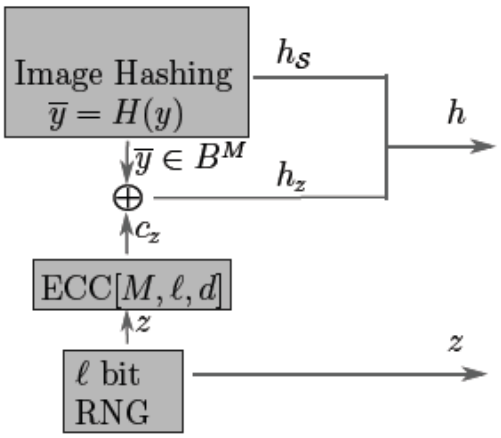


Fig. 4.2.: Image-based Extraction procedure.

4.3 IMPLEMENTATION SETTINGS OF THE EXTRACTION

In this section we analyze the experimental settings of the ingredients of image-based Extraction introduced in section 3.1.2. To recall the procedures of Image-based Extraction, see Fig. 4.2.

Random Binary Hashing $H_R(y) = \text{sign}_\text{b}(\Theta_R y)$ has been realized with another random matrix construction than Gaussian random matrix (described in section 3.2.3) in order to further accelerating the hashing process [78]. Later in 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 $U = \text{diag}\, u$ where $u \in \{-1, +1\}^N$ is a Bernoulli random vector of size N. Then the sensing matrix Θ_R of Eq. 3.2 corresponds to picking uniformly at 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 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 section 3.2.3) [79]. 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 Gaussian hashing) 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 $H_G(y) = \text{sign}_\text{b}(\Theta_G y)$ has been achieved by restricting the parameter vector ψ of the Gabor basis functions to the finite set of values $\Psi(a, \nu_0, \Delta)$ as described in Eq. 3.6. These parameters are obtained experimentally providing sub-optimal yet sufficiently good results [3]. For Laser PF, 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. For Crystal PF, the Gabor parameters are set to $\nu_0 = \pi/8$, $F = 2$, $m_1 = m_2$, $a = 5$ and $\Delta = 20$ respectively. The size of Gabor coefficients set is $\#\mathcal{G}_{a,\nu_0,\Delta} = F\lfloor N_1/\Delta \rfloor \lfloor N_2/\Delta \rfloor$. The sensing matrix of M most robust Gabor atoms Θ_G is then constructed and applied to the images using Eq. 3.7.

Error correcting code of code-offset secure sketch 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.

4.4 ROBUSTNESS

Robustness of a physical function system (defined in Definition 5) expresses the probability that an output generated by reconstruction stage matches the value generated in setup phase. We evaluate robustness using dataset $\mathcal{D}_1$ of both PFs 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 $\Delta_e = \text{dist}_\text{H}(\overline{y}_s, \overline{y}_r)$ be the Hamming distance between the fingerprints $\overline{y}_s$ and $\overline{y}_r$ of the same PUF in setup and reconstruction phase respectively. Knowing that the helper data generated in setup phase has been used in reconstruction phase, the robustness of Definition 5 is estimated by:

$$\rho_{\mathsf{PFS}} = \Pr[\Delta_e \leq t]. \tag{4.3}$$

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

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 setup phase has been used in reconstruction phase, the robustness of Definition 5 is estimated from the probability of having the same output in setup and reconstruction phases as follows:

$$\rho_{\mathsf{PFS}} = \Pr[z_r = z_s]. \tag{4.4}$$

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 and find robustness for a selection of possible pairs of ℓ, t where $t = \lfloor (d-1)/2 \rfloor$. Robustness is then plotted versus ℓ. For GbEx, the parameter M is fixed to $M = 255$ and $M = 1023$ for Laser PF and Crystal PF respectively[4].

We provide a fair statistical estimation of robustness for both approaches as follows. Given the dataset $\mathcal{D}_1$ of Q observations of P PUFs, for each PUF, one observation of the PUF is used as a target in setup 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 as target.

For the first approach, the histogram of $\Delta_e = \mathrm{dist}_{\mathrm{H}}(\overline{y}_s, \overline{y}_r)$ 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 [80]. 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.

Histograms of Δ_e for both extraction methods RbEX and GbEX have been depicted in Fig. 4.3(a) and Fig. 4.3(c) respectively for Laser PF and in Fig. 4.3(b) and Fig. 4.3(d) for Crystal PF. Fig. 4.4(a) and Fig. 4.4(c) show the robustness versus output size ℓ for Laser PF for both extraction methods RbEX and GbEX respectively. Fig. 4.4(b) and Fig. 4.4(d) show the same plots for Crystal PF. 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 capability t and thus reduces robustness. We also observe that the probability $\Pr[z_r = z_s]$ is higher than $\Pr[\Delta_e \leq t]$. This holds

[4]The reason to select this fingerprint size will be justified later in this section.

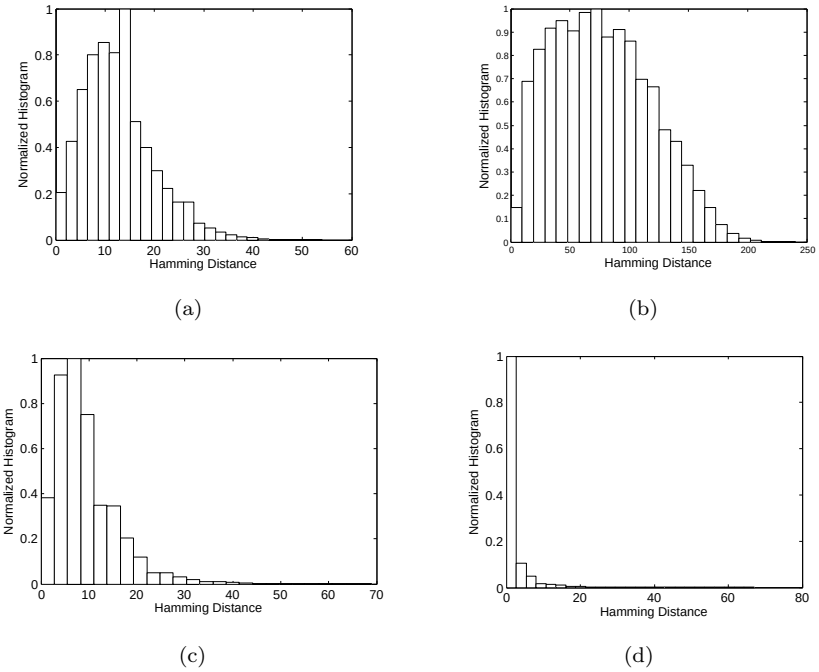


Fig. 4.3.: Histogram of intra-class Hamming distance between fingerprints of the same PUF Δ_e for (a) Laser-Written PUF, RbEX (b) Crystal PUF, RbEX, (c) Laser-Written PUF, GbEX (d) Crystal PUF, GbEX.

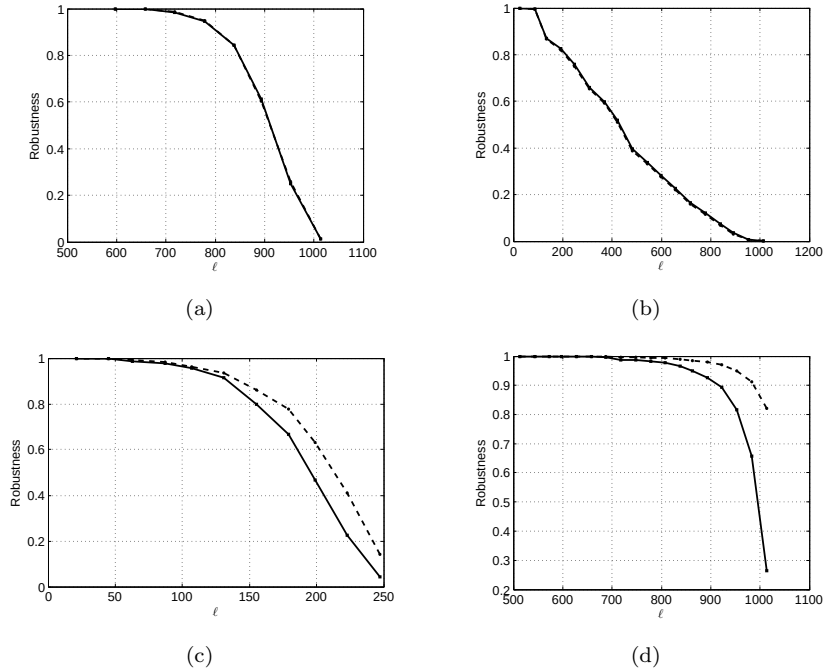


Fig. 4.4.: Robustness versus output size ℓ by (plain) $\Pr[\Delta_e \leq t]$ and (dashed) $\Pr[z_r = z_s]$ for (a) Laser-Written PUF, RbEX (b) Crystal PUF, RbEX, (c) Laser-Written PUF, GbEX (d) Crystal PUF, GbEX.

because there may exist some occurrence of $z_r = z_s$ although $\text{dist}_\text{H}(\overline{y}_s, \overline{y}_r) > t$, 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 section 3.1.2.

Because of low level of noise in PUF images of both Laser and Crystal PFs (as depicted in intra-class distance in Fig. 4.1(a) and Fig. 4.1(b)), we observe that both non-adaptive and adaptive methods provide good robustness for some values of output size ℓ. We even see that for Laser PF, non-adaptive RbEX outperforms adaptive GbEX because it exhibits better robustness for larger range of output size. However, it remains to evaluate the physical unclonability to fairly compare these two methods.

4.5 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 PF systems 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. 2.9) 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 setup and reconstruction phases. Let $\Delta_{\overline{y}} = \text{dist}_\text{H}(\overline{y}_s, \overline{y}'_r)$ be the Hamming distance between fingerprints $\overline{y}_s$ and $\overline{y}'_r$ of two different PUFs generated in setup and reconstruction phases respectively, using the same helper data. We start by considering the event $\Delta_{\overline{y}} \leq \Delta_{max}$ where Δ_{max} is an arbitrary integer value $0 \leq \Delta_{max} \leq M$. Practically $Pr[\Delta_{\overline{y}} \leq \Delta_{max}]$ can be computed using the histogram of $\Delta_{\overline{y}}$. This provides therefore a minimum value of γ according to Eq. 2.9 i.e.,

$$\gamma_{min} = Pr[\Delta_{\overline{y}} \leq \Delta_{max}] \leq \gamma. \tag{4.5}$$

Given the dataset $\mathcal{D}_2$ of R PUFs, histogram of $\Delta_{\overline{y}}$ is computed as follows. First, one PUF is chosen as a "target", the image of which is used in setup 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 $\Delta_{\overline{y}}$ 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, $\Delta_{\overline{y}}$ is computed from any possible pairs of PUFs. Fig. 4.5(a) and Fig. 4.5(c) shows the histogram of $\Delta_{\overline{y}}$ for Laser PF for both extraction methods RbEX and GbEX respectively. Fig. 4.5(b) and Fig. 4.5(d) show the same

histograms for Crystal PF. The probability $\Pr[\Delta_{\overline{y}} \leq \Delta_{max}]$ is then evaluated from the cumulative histogram of Δ_{max} as in the robustness case. It is yet to be evaluated to what extent the PF systems are considered as clones according to Definition 6. The probability that both 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 Δ_{max} bits. The probability of this event corresponds to the left-hand side of Eq. 2.8 which provides a maximum value of δ i.e.,

$$\begin{aligned}\delta_{max} &= \Pr[\Delta_{\overline{y}} \leq t : \Delta_{\overline{y}} \leq \Delta_{max}] \\ &= \sum_{i=0}^{\Delta_{max}} \Pr[\Delta_{\overline{y}} \leq t : \Delta_{\overline{y}} = i] \cdot \Pr[\Delta_{\overline{y}} = i : \Delta_{\overline{y}} \leq \Delta_{max}] \\ &= \sum_{i=0}^{\Delta_{max}} p_i \cdot \frac{pdf(i)}{cdf(\Delta_{max})} = \sum_{i=0}^{t} p_i \cdot \frac{pdf(i)}{cdf(\Delta_{max})} \geq \delta, \end{aligned} \tag{4.6}$$

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 $\Delta_{\overline{y}}$ respectively. To estimate them, the histogram of $\Delta_{\overline{y}}$ 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 $\Delta_{\overline{y}}$. It follows that the considered PF infrastructure $\mathcal{F}_{\alpha_{\mathrm{CR}}}$ 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 Δ_{max}. Smaller values for Δ_{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 $(\gamma_{min}, \delta_{max})$ are shown for a selection of Δ_{max} values using GbEX with a fixed t in Table 4.1 and in Table 4.2 for Laser PF and Crystal PF respectively.

In practice, this means that with probability γ_{min}, a manufacturer produces two PF systems that generate the same output with probability δ_{max}. So, the existential physical unclonability of a PF system can be summarized by averaging probability of cloning of Eq. 2.9 over all possible values of δ that is equivalent to $PC_{ex\mathsf{PFS}} = \mathbb{E}[\gamma_{min}\delta_{max}] = \Pr[\Delta_{\overline{y}} \leq t]$ over all the possible values of Δ_{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 (M, ℓ, d) code, we fix again the pa-

Table 4.1.: Different levels of $(\gamma, \delta, q = 2)$-cloning-resistance of LPUF using GbEx for a fixed correction capability $t = 26, \ell = 87$.

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

Table 4.2.: Different levels of $(\gamma, \delta, q = 2)$-cloning-resistance of CrPUF using GbEx for a fixed correction capability $t = 28, \ell = 748$.

Δ_{max}	γ	δ
1	$2.87 \cdot 10^{-6}$	1.00
151	0.002	0.05
301	0.06	0.02
451	0.45	$2.26 \cdot 10^{-4}$
601	0.90	$1.14 \cdot 10^{-4}$
751	0.99	10^{-4}
901	1.00	10^{-4}
1023	1.00	10^{-4}

rameter M (for GbEX to $M = 255$ and $M = 1023$ for Laser and Crystal PFs respectively and for RbEX $M = 1023$ for both Laser and Crystal PFs) and find the existential physical unclonability for a selection of possible pairs of ℓ, t where $t = \lfloor (d-1)/2 \rfloor$. For each pair of (ℓ, t), $PC_{ex\mathsf{PFS}} = \mathbb{E}[\gamma_{min}\delta_{max}]$ is estimated using the built histogram of $\Delta_{\overline{y}}$ and depicted in plain curve in Fig. 4.6(a) and Fig. 4.6(c), for Laser PF for both extraction methods RbEX and GbEX respectively. Fig. 4.6(b) and Fig. 4.6(d) show the same plots for Crystal PF.

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 $PC_{ex\mathsf{PFS}} = \Pr[z'_r = z_s : p \neq p']$ estimated from all iterations described previously. The obtained probability is depicted in dashed curve in Fig. 4.6(a) and Fig. 4.6(c) for Laser PF for both extraction

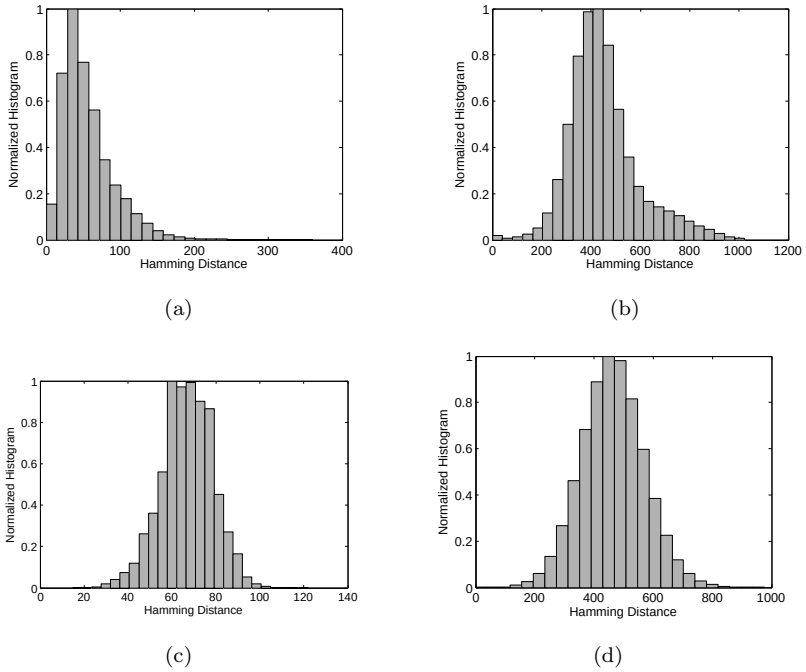


Fig. 4.5.: Histogram of inter-class Hamming distance between fingerprints of different LPUFs $\Delta_{\overline{y}}$ for (a) Laser-Written PUF, RbEX (b) Crystal PUF, RbEX, (c) Laser-Written PUF, GbEX (d) Crystal PUF, GbEX.

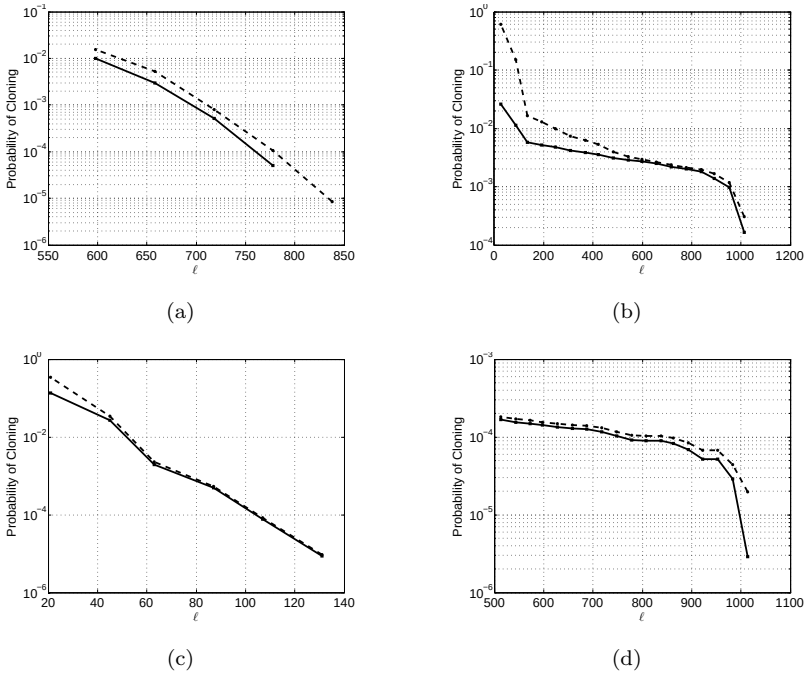


Fig. 4.6.: Probability of cloning versus output length ℓ by (plain) $\mathbb{E}[\gamma_{min}\delta_{max}]$ and (dashed) $\Pr[z'_r = z_s : p \neq p']$ for (a) Laser-Written PUF, RbEX (b) Crystal PUF, RbEX, (c) Laser-Written PUF, GbEX (d) Crystal PUF, GbEX.

methods RbEX and GbEX respectively. Fig. 4.6(b) and Fig. 4.6(d) show the same plots for Crystal PF.

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 $\Delta_{\overline{y}}$. Therefore, the obtained probability (without considering observation noise) gives us an upper-bound (worse-case) on the probability that two differently created PUFs generate the same output.

By decreasing ℓ, the error correction capability t increases meaning that more errors are corrected. Correcting more 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 $\Pr[z'_r = z_s : p \neq p']$ is higher than the one obtained from the first approach $\mathbb{E}[\gamma_{min}\delta_{max}]$. This again stems from some occurrence of $z'_r = z_s$ although $\text{dist}\,(\overline{y}_s, \overline{y}'_r) > t$.

We finally observe that for Laser PF adaptive GbEX outperforms non-adaptive RbEX because it provides the physical unclonability that decays faster with the output size ℓ. In the end of this section, we describe how to fairly compare the methods based on the trade-off between robustness and physical unclonability.

4.6 BINOMIAL APPROACH

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 setup 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, 13]. 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 this section, we compare robustness and physical unclonability based on the above assumptions with the results obtained above from experimental histograms only for Laser PF and GbEX method.

We assume that Δ_e and $\Delta_{\overline{y}}$ 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

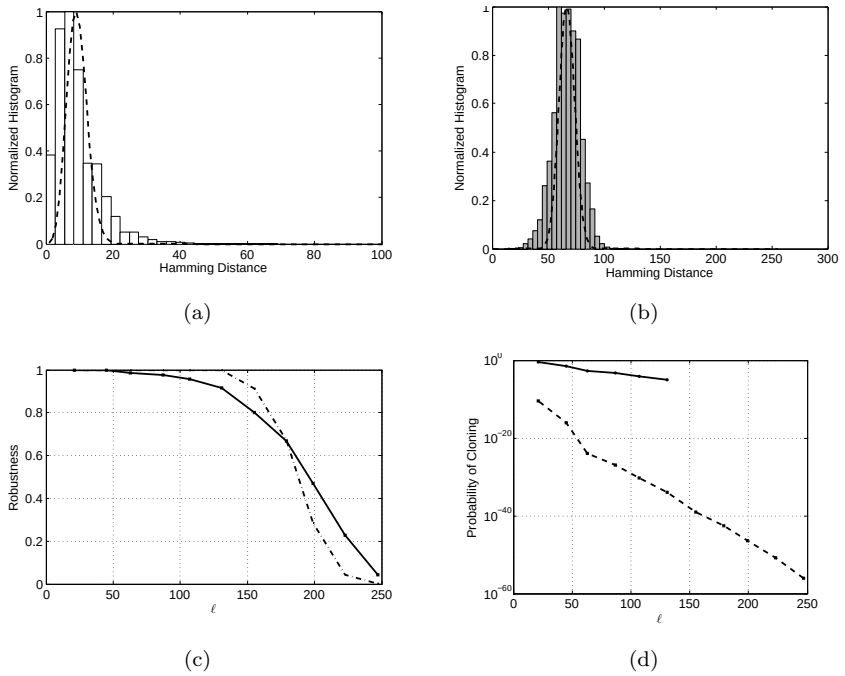


Fig. 4.7.: Approximation of probability distribution functions of intraclass (a) and interclass (b) Hamming distance between fingerprints by (plain) histogram and (dashed) binomial distribution. Robustness (c) and probability of cloning (d) versus output length ℓ using (plain) histogram approach and (dashed) binomial approach for GbEX.

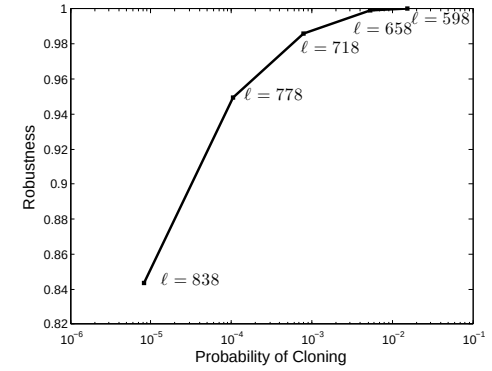
of $\Delta_{\overline{y}}$) respectively. We obtain $p_e = 0.04$ and $p_y = 0.26$ from the mean values of Δ_e and $\Delta_{\overline{y}}$ respectively from all the experimental iterations described previously. We illustrate how the experimental histogram of Δ_e and $\Delta_{\overline{y}}$ which are obtained previously match the binomial distribution in Fig. 4.7(a) and Fig. 4.7(b) respectively. We observe that especially for the inter-class distance $\Delta_{\overline{y}}$, 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 $\Delta_{\overline{y}} \sim B(M; p_y)$ instead of using the experimental histograms. Let $\mathbf{f}_{\mathsf{bino}}(t; n; p_i)$ and $\mathbf{F}_{\mathsf{bino}}(t; n; p_i)$ 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. 4.3 and physical unclonability is estimated from the probability of cloning $PC = \mathbb{E}[\gamma\delta]$ using binomial *pdf* and *cdf* in Eq. 4.5 and Eq. 4.6. Fig. 4.7(c) and Fig. 4.7(d) compare the robustness and the probability of cloning obtained from histogram approach and the 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.

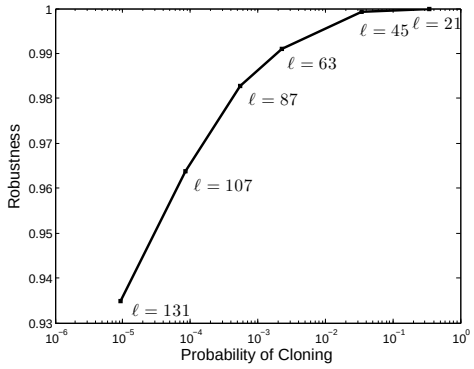
4.7 ROBUSTNESS AND PHYSICAL UNCLONABILITY TRADE-OFF

Eventually, the main property of a PF system is the trade-off between robustness and physical unclonability that provides an asset to fairly compare different PF system and select one system $\mathcal{F}$ with all its parameters (described in Definition 4) for a particular application. In this part, we compare the trade-off between robustness and physical unclonability (existential unclonability against an honest manufacturer) for two PF systems using two extraction algorithms RbEX and GbEX. Fig. 4.8 and Fig. 4.9 show this trade-off obtained from the output values, i.e., $\rho_{\mathsf{PFS}} = \Pr[z_r = z_s]$ and $PC_{ex\mathsf{PFS}} = \Pr[z'_r = z_s : p \neq p']$ for different correction capabilities t for Laser-Written PUF and Crystal PUF using both 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



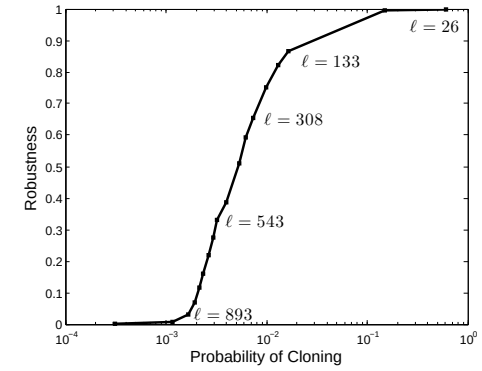
(a)



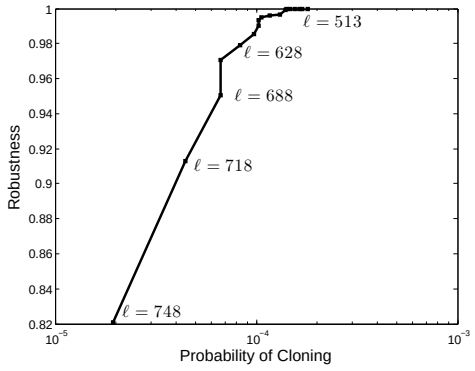
(b)

Fig. 4.8.: Robustness $\rho_{\mathsf{PFS}} = \Pr[z_r = z_s]$ versus existential physical unclonability summarized by the probability of cloning $PC_{ex\mathsf{PFS}} = \Pr[z'_r = z_s : p \neq p']$ for Laser-Written PUF using (a) RbEX (b) GbEX.

RbEX, implying better performance of the adaptive extraction method for both Laser and Crystal PF systems, because it still provides a good robustness for an acceptable value of probability of cloning. For example, for Laser PF system, the minimum of GbEX trend provides a pair of $(\rho, PC_{ext}) = (0.94, 10^{-6})$ 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



(a)



(b)

Fig. 4.9.: Robustness $\rho_{\mathsf{PFS}} = \Pr[z_r = z_s]$ versus existential physical unclonability summarized by the probability of cloning $PC_{ex\mathsf{PFS}} = \Pr[z'_r = z_s : p \neq p']$ for Crystal PUF using (a) RbEX (b) GbEX.

PUFs with a probability of 10^{-6} which is acceptable for many applications. For Crystal PF system, in the trend we can find a pair $(\rho, PC_{ext}) = (0.97, 6.10^{-4})$ that is still reasonable for some applications.

For better comparisons between two systems, we put two plots on Fig. 4.10. We can observe that with the current settings, the trend of Crystal PUF outperforms that of Laser PUF because most of the points are with higher robustness and less probability of cloning.

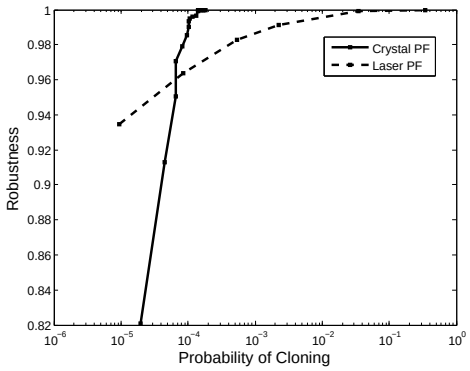


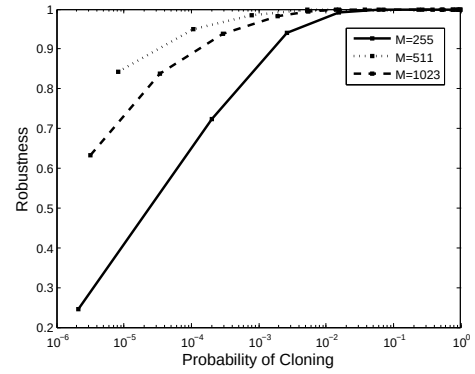
Fig. 4.10.: Robustness versus existential physical unclonability summarized by the probability of cloning for Crystal PUF (plain) and Laser PUF (dashed)

In following, we first justify the choice of parameters such as fingerprint length M and radius Ra of morphological filtering (see section. 4.1) and then bring some discussion on comparing the results with those of human biometrics and also on scalability of the results.

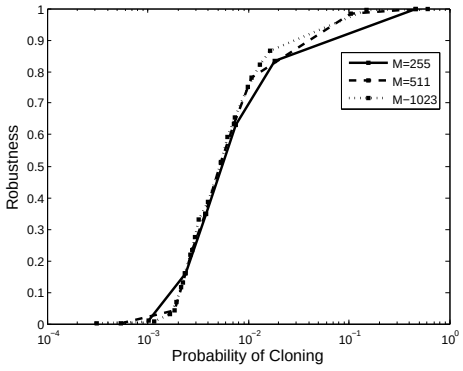
In order to find an optimum fingerprint length M, in other experiments (excluded in the figures), we find that increasing M leads to better trade-off between robustness and physical unclonability for GbEX. That is the reason why for GbEX we pick the maximum possible M with the form of $2^k - 1$ which is smaller than the size of Gabor coefficients ($\#\mathcal{G}_{a,\nu_0,\Delta}$). For RbEX, however, this limitation no longer exists and M can be arbitrarily increased till $M \neq N$. We should just keep in mind the fact that by increasing M, the size of helper data that should be stored increases accordingly. For both Laser PF and Crystal PF, we investigate the effect of increasing M that are illustrated in Fig. 4.11(a) and Fig. 4.11(b) respectively.

As we observe, the effect of increasing M on the trade-off is efficient for Laser PF and not efficient for Crystal PF. We believe that is due to the fact that there exists a big overlap between intra-distance and inter-distance of Crystal PF images (see Fig. 4.1) and as we predicted RbEX does not work efficiently for Crystal PF . Anyhow, for both Laser and Crystal PF, we pick $M = 1023$ for RbEX.

As for the radius Ra of morphological filtering, another set of experiments is performed. To give an overview, we bring results for some values of Ra for Crystal PF and GbEX in Fig. 4.12. According to these results, we select $Ra = 15$ providing the best results. It is worth to remark that optimizing all



(a)



(b)

Fig. 4.11.: Robustness versus existential physical unclonability for different M for (a) Laser-Written PUF (b) Crystal PUF.

parameters of the system based on the ultimate trade-off between robustness and unclonability is very computationally costly. So, in practice it could be more efficient to select some parameters based on other intermediate metrics, for example the overlap between intra and inter-distance histograms.

In this part, we compare the final results of our Image-based PUFs (Fig. 4.8 and Fig. 4.8) 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)

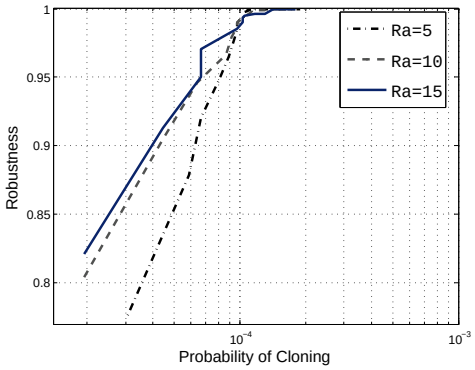


Fig. 4.12.: Robustness versus existential physical unclonability for different Ra

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 PC_{ext} respectively. The equivalent ERR for is given when $1 - \rho = PC_{ext}$ and for RbEX and GbEX are obtained as $EER_g = 0.5\%$ and $ERR_r = 0.8\%$ for Laser PF system and for $EER_g = 0.6\%$ and $ERR_r = 2\%$ Crystal PF system. These results also confirm 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 [81]. However, we should point that there exist important differences in the security constraints associated with systems based on human fingerprints and Image-based PUFs. The difference is that for verification systems based on human fingerprint, the adversary can not arbitrarily generate human fingerprints hoping to find a collision. But for Image-based PUFs, the adversary can iterate the creation process in order to find a collision. It implies that for security applications, it is required that Image-based PUFs have much lower probability of cloning comparing with biometric systems.

In order to get better results, security properties of an Image-based physical function system can be still improved as they are scalable. For example, 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 PUF on a physical object or using multiple PUFs instead of one. It is however important to remark that enlarging a PUF area can contribute more to the security comparing with using multiple PUFs. The reason is that it would be easier for an adversary to perform a divide and conquer attack when using multiple PUFs. In this case he tries to find a clone for each PUF individually and the probability of his success is higher than when he tries to find a clone for a bigger PUF.

4.8 CONCLUSION

In this chapter we experimentally characterized the security properties of practical examples of image-based physical function systems. We provided a methodology to statistically estimate robustness and existential physical unclonability from datasets of PUFs. We also described the implementation settings of the extraction procedure namely, Random and Gabor Binary Hashing and error correction part of secure sketch scheme. The experiments demonstrated the usefulness of the formalizations of the security properties made in [1] particularly to concretely assess the physical unclonability. Eventually we assessed the key outcome of the system i.e., the trade-off between robustness and physical unclonability. This trade-off makes the system adjustable for different needs. For example, for Laser-Written PUF datasets, GbEX trend provides a pair of $(\rho, PC_{ext}) = (0.94,\ 10^{-6})$ and for Crystal PUF it provides $(\rho, PC_{ext}) = (0.97,\ 6.10^{-4})$ which are sufficient for many practical systems. Moreover, these results are scalable meaning that robustness and physical unclonability can be further improved by averaging more than one response in the registration phase and by enlarging the size of Image-based PUF respectively. As an attempt to compare the performance of our system with human fingerprint verification system, we also calculated the corresponding Equal Error Rate (EER) of our systems i.e., $EER_g = 0.5\%$ for Laser PF system and $EER_g = 0.6\%$ for Crystal PF system using GbEX. Both obtained EERs are better compared with the typical EER for fingerprints verification systems.

The results also demonstrate that the image hashing methods (including the pre-processing) and parameters have a significant impact on the ultimate achievable security properties of the Image-based physical function system. This motivates more emphasis on the image hashing method in order to optimize the security properties of a particular Image-based physical function system.

As a complement to our experiments, we demonstrated that for our particular implementations of a 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 to estimate the physical unclonability of other types of PUFs should be performed with particular caution.

CHAPTER 5

ANTI-COUNTERFEITING SCHEME

Counterfeiting of trademarked products is a rapidly growing problem for the worldwide economy. Two types of threats are to be faced. On the one hand, Insider Counterfeiting (manufacturer overproduction) refers to unauthorized production by the legitimate manufacturer who realizes profits by producing extra quantities outside their license agreement [82]. On the other hand, Outsider Counterfeiting refers to unauthorized reproduction of products by other counterfeiters. 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. Despite their simplicity, overt physical identifiers normally can be easily cloned [16, 83]. *Covert identifiers*, instead, use the features that are not readily visible by naked eye. Invisible inks and *proprietary photonic inks* are examples of covert physical identifiers [83]. Another widely used covert physical identifier is a Radio Frequency Identification (RFID) Tag containing a digital identifier [16]. Uncloneability is still a big concern for covert identifiers. For example, in case of using RFID tags for anti-counterfeiting, a digital identifier together with some reference information about the product are embeded in the RFID tag. These data are read by

the verifier by means of a secure protocol in order to validate the authenticity of the product bearing this RFID tag. However, the secure protocol usually can not prevent the adversary to physically clone the tag by capturing its security related data (e.g., identification number, reference information, keys, etc.) and place them into another tag [28]. This example implies that in order to avoid cloning of the physical objects, some unclonable physical structures like PUFs should be integrated into the security protocol. In this view, the core concept of using PUF primitives for anti-counterfeiting applications is to rely on the unique physical properties that are impossible or very costly to be cloned.

As stated in section 3, Image-based PUFs have been widely used to protect counterfeiting of products. Image-based PUF can be either intrinsic in the product or extrinsic and glued to the product. Although no formal definition of an intrinsic and extrinsic PUF is provided in literature, we distinguish two conditions for an Image-based PUF to be called intrinsic:

1. The PUF is the inherent random features of the product meaning that no extra manufacturing efforts is needed to create them (e.g., Paper PUF) *or*

2. The PUF is created and concurrently inserted into the product in a way that it is inseparable from the product. By inseparable we mean that any effort aiming at removing the PUF from the product results in a considerable damage to the quality of the object (consider Laser-Written PUF engraved in gemstones).

Otherwise, the PUF is called extrinsic.

For anti-counterfeiting systems, as with any security system, it is important to embed PUFs in a sound protocol, ensuring that no unexpected weakness is present in the "mortar" binding the components together. In this chapter we present a unified formal treatment of the use of Image-based PUFs as a counterfeiting prevention tool. We first define a secure anti-counterfeiting scheme and provide a construction meeting this definition. The construction combines physical protection blocks with cryptographic protection blocks. It is worth mentioning that the basic concept i.e., to digitally sign the product information and the identifier extracted from the PUF already exists in literature. In this work we focus on the design of an anti-counterfeiting protocol based on Image-based PUFs regarding the specific properties and constraints of Image-based PUFs. We also define an attack model and derive the security property a PUF must fulfill in order to be eligible as a secure physical building block. We prove that this security property is equivalent to the physical unclonability property that was presented in chapter 2.

5.1 ANTI-COUNTERFEITING SCHEME BASED ON IMAGE-BASED PUF

In this section, we first present a general view of the components of the anti-counterfeiting scheme and the security assumptions. Then we present a formal definition of the anti-counterfeiting scheme.

5.1.1 Informal Description of Anti-counterfeiting Scheme

The anti-counterfeiting scheme is informally described as follows. Fig. 5.1 illustrates a schematic of the anti-counterfeiting system.

1. A configuration step Config is performed by the trademark owner and the PUF provider. They decide about the type of PUF, the parameters of the system, etc. A private/public key pair is also established in this step.

2. The PUF provider runs a creation process Create and delivers the created PUFs to the trademark owner.

3. A registration step Reg is performed by the trademark owner. It includes extracting digital identifier from the PUF and digitally signing this identifier plus some side information (e.g. serial number) about the product. Depending on the context, this step can take place either after the product to protect has been manufactured, or before: the PUF and registration data can for example be shipped to the manufacturer to be later physically or logically bound to the product. The PUF and data could for example be glued and printed on the product, or on a certificate of authenticity accompanying it. The product and PUF are then delivered to the market.

4. A verification process Verif is performed each time someone wants to determine whether the embedded PUF of a given product is authentic or not. Examples of entities performing the verification process includes: trademark owner, customs, wholesaler or retailer and end-user.

5.1.2 Security Assumptions

Here, we list the security assumptions for the above anti-counterfeiting scheme.

1. As a classical property of physically unclonable functions, we expect that, due to uncontrollable variations during the manufacturing pro-

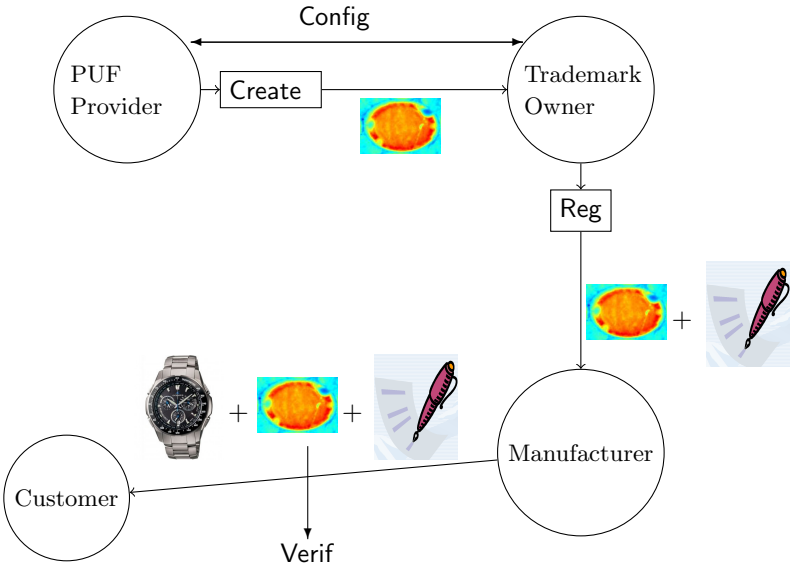


Fig. 5.1.: A schematic of the anti-counterfeiting system.

cess, PUFs cannot be physically cloned, i.e., that it is practically impossible/very costly for an adversary to generate pairs of PUFs yielding identical behavior when queried. We will provide an explicit phrasing of this expectation later in this chapter (Eq. 5.6). A PUF is usually employed to protect products whose value is less than the cost of cloning the PUF. As technology grows, we may expect that the cost of cloning a PUF does not anymore exceed the product value. As a consequence, the PUF-based system may need upgrade by time.

2. Image-based PUFs are physically unclonable and not necessarily mathematically unclonable. Mathematical unclonability means that it should be very hard to construct a mathematical procedure that yields the same challenge-response behavior as that of the PUF. Image-based PUFs in general do not have this property and a mathematical clone (e.g. a fake image) can be created by imitating the response (image) of the PUF [1]. As a consequence, we assume that any verification process involves a prior verification that a real PUF, and not a mathematical clone (e.g. a picture) is being dealt with.

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

3. The various steps of the anti-counterfeiting scheme, i.e., Config, Create, Reg and Verif are performed by trusted parties, using trusted parameters. In particular, this implies that registration is only performed on physical components originating from a trusted source.

4. We authenticate the PUF and not the product. This is equivalent to authenticating the product itself when the PUF is inherently part of the product (*intrinsic* PUF). It is not necessarily the case when the PUF is a distinct object attached to the product (*extrinsic* PUF), but is still be sufficient in most anti-counterfeiting scenarios (both insider and outsider), where the trademark owner mostly wants to control the amount of products delivered to the market[2].

The above assumptions lay down a sound framework for implementing a secure PUF-based system. Let us briefly discuss some of their consequences.

As usual, we assume (assumption 1) that the PFS system in use generates inherently unique tags. However, it is difficult to ensure that, by modifying the generation parameters, an adversary will not be able to come up with a degraded version of the PFS that will trigger collisions[3]. This could yield collision-based attacks, in a way very similar to hash-function collision attacks against signature schemes, where an adversary generates degraded tags, gets one of them registered, and can use this as a registration proof of the other ones. Checking whether a given tag was produced using the appropriate parameters is not always obvious for the registration authority or verifier. Assumption 3 allows us to get basically rid of that concern, as we assume that the only tags that will be registered are those produced by a trusted source, and thus implicitly using the correct parameters. We are thus left with the much more natural assumption that tags produced using different parameters would be sufficiently different to be sure that they cannot induce a collision with the "honest" ones. Off course, the validity of this "natural" assumption should still be asserted by the system designer when selecting a specific PUF realization.

It is worth noting that, although we assume above that the verification is performed by a trusted party, this trust is in fact only limited. An untrusted verifier is impossible to capture in a security model, in the sense that it is impossible to prevent a rogue verifier from simply providing a positive answer to any verification request. Nevertheless, the use of asymmetric cryptography

[2]For other scenarios, where an inseparable link between the PUF and the product is necessary, intrinsic PUFs, or additional measures such as using a tamper-proof seal would be necessary.

[3]As an extreme example, consider modifying an Image-based PUF so that all produced tags are uniformly black.

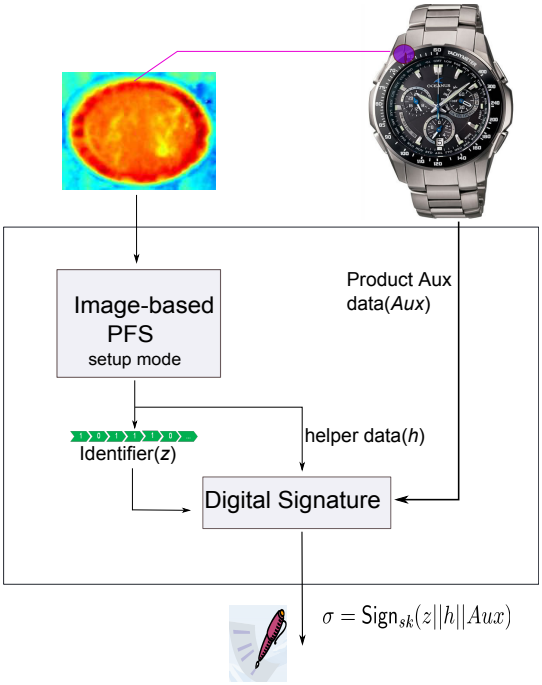


Fig. 5.2.: A schematic of the registration process Reg.

allows storing only public, non-critical keys on the verifier's side. So a compromised verifier can (inevitably) be used to provide incorrect information to its user, but it cannot be exploited to affect the system's global security.

5.1.3 Formal Description of Anti-counterfeiting Scheme

Let us now formally define our anti-counterfeiting scheme. In addition to the aforementioned Image-based Physical Function System, it relies on a signature scheme providing existential unforgeability under an adaptive chosen messages attack defined in chapter 2. Intuitively, this means that it is impossible for an adversary running in "reasonable" time to produce the signature of a new message, even if he can beforehand request the signature of many messages that he chooses.

Definition 10. *The anti-counterfeiting scheme* Π *includes tuple of four processes* (Config, Create, Reg, Verif) *satisfying the following:*

1. Config: The configuration process is performed one time and determines the type of PUF and the parameters of the system including the fixed challenge x, creation parameter α_{CR} , evaluation parameter α_{PF}, extraction parameter α_{EX} and a pair of private key sk and public key pk.

2. $\mathsf{Create}(\alpha_{\mathrm{CR}}) \rightarrow p$. The creation process takes as input the creation parameter α_{CR} and outputs the physical component p based on the creation parameter α_{CR}.

3. $\mathsf{Reg}_{x,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}},sk}(p, Aux) \rightarrow (\sigma, h, Aux)$. The registration process $\mathsf{Reg}_{x,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}},sk}$ takes as input the physical component p and optional auxiliary data. Auxiliary data Aux includes side information about the PUF such as its serial number or EPC, creation date, expiration date, distribution points, *etc.* . Since the challenge x, α_{PF} , α_{EX} and the private key sk are fixed and implicitly trusted, we usually discard them in our notation, that is we simply write Reg instead of $\mathsf{Reg}_{x,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}},sk}$. The registration process Reg is performed in two phases as illustrated in Fig. 5.2:

   1) The setup mode of the Image-based PF system (See Fig. 3.1(a)) is executed for p using x, α_{PF} and α_{EX}, yielding the output z_s and helper data h as:

   $$\mathsf{PFS}(x, \epsilon) \rightarrow (z_s, h). \tag{5.1}$$

   2) The output, helper data and auxiliary data are signed using the private key sk, yielding the signature $\sigma = \mathsf{Sign}_{sk}(z||h||Aux)$.

4. $\mathsf{Verif}_{x,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}},pk}\ (p, h, Aux, \sigma) \rightarrow b \in \{0, 1\}$. The verification process $\mathsf{Verif}_{x,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}},pk}$ takes as input a physical component p, helper data h, auxiliary data Aux and signature σ, and outputs a validity bit b. Hereafter, we simply write Verif instead of $\mathsf{Verif}_{x,\alpha_{\mathrm{PF}},\alpha_{\mathrm{EX}},pk}$. The verification process Verif is also performed in two phases as illustrated in Fig. 5.3:

   1) The reconstruction mode of Image-based PF system (See Fig. 3.1(b)) is executed for p using x, α_{PF}, α_{EX} and the helper data h. The output z_r is generated as following:

   $$\mathsf{PFS}(x, h) \rightarrow (z_r, h). \tag{5.2}$$

   2) The verification algorithm of the signature scheme is executed on $(z_r||h||Aux)$ using the public key pk to check the authenticity of the PUF. The verification algorithm of the signature scheme outputs a bit b, with $b = 1$ meaning signature valid and $b = 0$ meaning signature invalid.

   The verification process outputs the bit b.

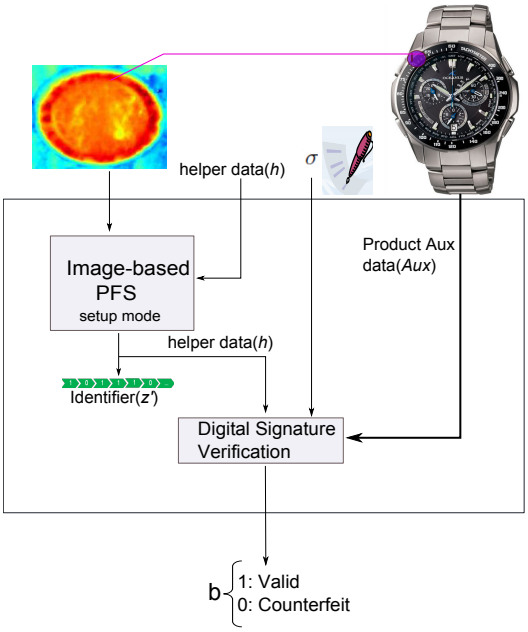


Fig. 5.3.: A schematic of the verification process Verif.

5.2 ATTACK MODEL AND SECURITY

For our security analysis, we assume that the Adversary A has access to an oracle CReg(.). When it is queried with parameter $\alpha_{\mathrm{CR,i}}$, this oracle checks whether $\alpha_{\mathrm{CR,i}} \in \mathcal{A}_{\mathrm{CR}}$ and, if it does, creates p_i, registers the created p_i and returns $(p_i, \sigma_i, h_i, Aux_i)$ (Fig. 5.4).

In practice, only adversaries with bounded time and computational effort are relevant. Thus we consider only PPT adversaries and additionally limit them to query the CReg oracle at most q times.

Definition 11 (Attack Model)**.** *Let* $\Pi = (\mathsf{Config}, \mathsf{Create}, \mathsf{Reg}, \mathsf{Verif})$ *be the anti-counterfeiting scheme. Adversary* A *is given pk and oracle access to* CReg(.) *as defined above. Let* Q *be the set of pairs* (p, Aux) *that were generated by* CReg(.)*. The adversary* A *then generates a set of* (p', h', Aux', σ')*. The output of the counterfeiting experiment* $\mathsf{Counterfeit}_{\mathsf{A},\Pi}(q)$ *is defined to be* 1 *if*

$$\mathsf{Verif}(p', h', Aux', \sigma') \to 1 \quad \text{and} \quad (p', Aux') \notin Q. \tag{5.3}$$

The security of the anti-counterfeiting scheme is then defined as follows:

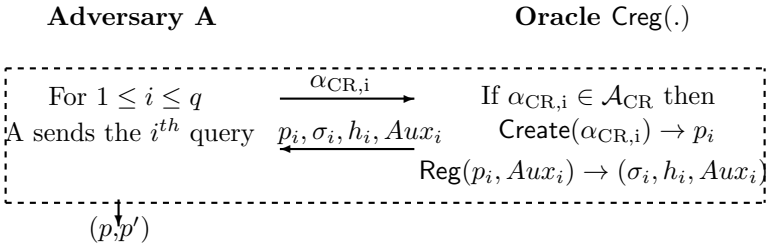


Fig. 5.4.: Counterfeiting experiment $\mathsf{Counterfeit}_{\mathsf{A},\Pi}(q)$.

Definition 12 (Security)**.** *The anti-counterfeiting scheme* Π *is* β*-secure if for all probabilistic polynomial-time (PPT) adversaries, we have:*

$$Pr\big[\mathsf{Counterfeit}_{\mathsf{A},\Pi}(q) = 1\big] \leq \beta. \tag{5.4}$$

Lemma 1. *Suppose that the signature scheme is existentially unforgeable under an adaptive chosen message attack. If the output of the adversary experiment is* 1*, then there exists at least one instance* p_i *such that there has been a registration step:*

$$\mathsf{Reg}(p_i, Aux_i) \rightarrow (\sigma_i, h_i, Aux_i), \tag{5.5}$$

and $\sigma' = \sigma_i$*,* $h' = h_i$*,* $Aux' = Aux_i$ *and* $z' = z_i$ *s.t* $\mathsf{PFS}(x, h_i) \rightarrow (z', h_i)$*.*

Proof. Suppose that there does not exist any p_i that has been registered by a trusted authority such that $\sigma' = \sigma_i$, $h' = h_i$, $Aux' = Aux_i$ and $z' = z_i$. Then, $\mathsf{Verif}(p', h', Aux', \sigma', pk) \rightarrow 1$ implies that the adversary succeed in producing a valid signature pair $((z'||h'||Aux'), \sigma')$ for a signature that has not been produced by the signature scheme. This contradicts the existential unforgeability assumption for the signature scheme. □

As a direct consequence of Lemma 1, the only way for the adversary to make a counterfeit is to produce a physical component p' that *collides* with a previously registered physical component p_i, i.e., provides the same output using its corresponding helper data h_i. Hence, the security property of the anti-counterfeiting scheme can be evaluated as follows:

Property 1. *The anti-counterfeiting scheme* Π *is* β*-secure (w.r.t.* x*) if for all PPT adversaries* A *that are limited to calling the* CReg *oracle at most* q

times, it holds that:

$$\begin{aligned} Pr\big[\mathsf{PFS}'(x,h) \rightarrow (z,h) : \mathsf{PFS}(x,\epsilon) \rightarrow (z,h) \\ \mathsf{Counterfeit}_{\mathsf{A},\Pi}(q) \rightarrow (p,p'); \\ p \in [\mathsf{Create}(\alpha_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}})]; p' \in [\mathsf{Create}(\alpha'_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}})]\big] \leq \beta, \end{aligned} \tag{5.6}$$

where ':' denotes the conditional probability and PFS' *is the PF system using* p'*. The security experiment* $\mathsf{Counterfeit}_{\mathsf{A},\Pi}(q)$ *is depicted in Fig. 5.4.*

This is equivalent to the existential physical unclonability property that was defined in section 2.1.2.

As discussed in section 5.1.2, the assumption that only tags produced by a trusted manufacturer are registered can often simplify unclonability testing. Relying on the assumption that different creation parameters will not trigger collisions with tags produced using α_{CR}, we can rewrite Eq. 5.6 as:

$$\begin{aligned} Pr\big[\mathsf{PFS}'(x,h) \rightarrow (z,h) : \mathsf{PFS}(x,\epsilon) \rightarrow (z,h) \\ (p,p') \in [\mathsf{Create}(\alpha_{\mathrm{CR}} \in \mathcal{A}_{\mathrm{CR}})] \leq \beta; \end{aligned} \tag{5.7}$$

and thus focus on the probability that an honest manufacturer creates two clones by coincidence.

As stated in section 4.5, this probability can be statistically estimated by sampling R PUFs and their corresponding images. First, one PUF is chosen as a "target", the image of which is used in setup mode to generate helper data h and output z_s. The remaining $(R-1)$ images, together with the initial helper data h, are then used in reconstruction mode, and the generated outputs are compared with z_s. This experiment is repeated R times, each PUF being selected once as target. The security property β is then estimated by:

$$Pr\big[z_r = z_s : p \neq p'\big] \leq \beta. \tag{5.8}$$

From above, it becomes clear that physical unclonability property estimated experimentally in section. 4.5 is equivalent to the security property β of the proposed anti-counterfeiting scheme. Therefore, for an anti-counterfeiting scheme, the compromise between robustness and security can be obtained by evaluating the trade-off between robustness and physical unclonability of the underlying physical function system.

5.3 CONCLUSION

In this chapter, we have proposed a secure anti-counterfeiting scheme based on Image-based PF system and a signature scheme. The security of the scheme is

then formally analyzed and provably reduced to physical unclonability of the underlying Image-based PUF. The proposed anti-counterfeiting protocol is simple and reasonably efficient. It relies on a natural property that can be expected from any Image-based Physical Function System, namely the fact that each object presents a unique, typical visual aspect. This is presumably easier to achieve in practice than more advanced properties such as the availability of a large amount of independent challenge-response pairs. From a computational point of view, product registration (resp. verification) requires one execution of an asymmetric cryptographic primitive, which is in line with the cost and computing capabilities expected from an image processing-capable device.

The protocol allows a simple key management policy, where critical, private keys can be kept under control of the trademark owner, whereas only public keys need to be distributed towards the (more difficult to control) verifiers. It also allows straightforward extensions, e.g. integrating a Public Key Infrastructure (PKI) for better scalability.

Experiments on chapter 4 confirm that some Physical Function Systems, such as Laser PF system and Crystal PF system, seem to bear the necessary properties to be integrated in our construction and provide a practical anti-counterfeiting system.

CHAPTER 6

CONCLUSION

In this thesis, we presented a comprehensive study of Image-based PUFs used for anti-counterfeiting applications. Our general goal was to address security concerns of using real-world PUFs in designing security systems. For that purpose, we selected a particular category of PUFs i.e., Image-based PUFs and considered minimum security properties that should be expected from a PUF system in general i.e., robustness and physical unclonability. We selected the work of Armknecht et al. [1] which provided concrete formalizations of these security properties and tried to validate them experimentally. Finally, we formally analyzed the security of the target security application i.e., anti-counterfeiting system based on the validated security properties of its underlying PUF. Accordingly, the following steps undertaken by this thesis can be adapted for security analysis of other PUF-based security systems.

First, we adapted the general model of physical functions [1] to build a unified model of Image-based physical function system including image processing and cryptographic modules. The modular description of the Image-based physical function system provides an asset to easily design the system for most new Image-based PUFs by adapting the components based on the spec-

ifications of the Image-based PUF under study. We further demonstrated the relevance of our model by providing practical examples. We introduced two new types of Image-based PUFs called Laser-written PUF and Crystal PUF and we showed that the system can be easily adapted for these new PUFs. We further highlighted Image hashing procedure as a particular building block needed to deal with Image-based PUFs and categorized it into adaptive and non-adaptive Image hashing methods. We further compared the relevance of these methods depending on the images under study. Finally, we provided practical examples of adaptive and non-adaptive Image hashing methods by Gabor Binary Hashing and Random Binary Hashing respectively. Gabor Binary Hashing is an extension of the existing method [10] and Random Binary Hashing is our contribution as a fast candidate for image hashing.

Second, we provided a methodology to experimentally evaluate security properties of practical Image-based physical function system based on the formalizations provided by [1]. For this purpose, we constructed datasets of PUF responses (images) for both Laser-written PUF and Crystal PUF which were then used for statistical evaluation of security properties of interest i.e., robustness and physical unclonability. As a complement to our experiments, we explored the accuracy of binomial approach (assuming binomial distribution for the Hamming distances between PUF responses) used in prior works to estimate system properties. We demonstrated that this approach does not provide accurate results especially for physical unclonability. Therefore, the binomial approach for estimating the physical unclonability of other types of PUFs should be performed with particular caution. Additionally, we obtained the trade-off between robustness and physical unclonability for both Laser-Written PUF and Crystal PUF and both image hashing methods. The trade-off trend makes the system adjustable for different needs. Our results demonstrated that the image hashing procedure has a significant impact on the trade-off that between robustness and physical unclonability can be achieved by Image-based physical function systems for both Laser-Written PUF and Crystal PUF. Although the obtained results for both robustness and physical unclonability are sufficiently acceptable for practical systems, we argued that they are still scalable meaning that robustness and physical unclonability can be further improved by averaging more than one response in the registration phase and by enlarging the size of Image-based PUF respectively.

Third, we presented a formal treatment of Image-based PUF for its target security system i.e., anti-counterfeiting system. We provided a secure anti-counterfeiting scheme, along with making appropriate assumptions based on the specifications and constraints of Image-based PUF. The anti-counterfeiting scheme is based on Image-based Physical Function system and an unforgeable digital signature scheme. We then formally analyzed the security of this anti-counterfeiting scheme by exploring the attack model. The

security of the scheme is provably reduced to the physical unclonability of its underlying Image-based PUF which has been evaluated experimentally.

Eventually, our results confirm that the security framework in [1] can be used to bridge the gap between engineering constraints and cryptographic protocols. While the work presented in chapter 4 shows that metrics such as robustness and physical unclonability can indeed be estimated for real-world PUFs, the security analysis in chapter 5 confirms that these metrics can also be connected to standard cryptographic analyses, using sound (and tight) reductions.

Perspectives

In the continuation of this thesis, several items deserve future examinations.

1. Our experiments have shown a strong effect of Image hashing procedure on the ultimate security properties that can be achieved by an Image-based PF system. This motivates further study on the image hashing methods. One interesting extension to adaptive image hashing can be using "Matching Pursuit" algorithm [84]. The working principle of this method is very close to adaptive image hashing i.e., projecting the signal on the dictionary of atoms, picking "best matching" atoms providing the biggest coefficients when applied to the image. However, the selection of best atoms in Matching Pursuit algorithm is performed in an iterative way. The algorithm finds the one atom that has the biggest scalar product with the signal, then subtracts the contribution due to that atom, and repeats the process until the signal is satisfactorily decomposed. The advantage of this iterative method over picking all best atoms at once (as in Gabor Hashing) is that by subtracting the contribution due to previously selected atom, the probability that next atom falls in the same spatial interval decreases. Hence, as the search is performed more globally on the image, the convergence of the algorithm is faster and thus using an over-complete dictionary becomes feasible. The advantage of using an over-complete dictionary is that the risk of missing some important features due to coarse discretization of the parameters of basis function will be reduced. In this view, we propose, as a future study, using Matching Pursuit algorithm to perform image hashing and compare its results with respect to robustness unclonability trade-off. It also remains to evaluate the performance of these methods to determine if they are competent with the resource constraints of a certain application. Moreover, as another future study, the model of image hashing procedure can be further generalized to cover other techniques proposed

in the literature for perceptual image hashing such as SIFT [71], RASH [72], LSH [85], etc.

2. In this study, the performance of different image hashing procedures have been compared experimentally. Another approach that deserves future work is to evaluate their performance theoretically. For that purpose, we can study the resistance of the hashing procedure against evaluation noise. The question is: how is the evaluation noise in the images transferred to their hash values? For that purpose, the evaluation noise and the coefficients before quantization step should be first modeled by assigning appropriate probability distributions to them. Then the probability of bit flips in hash values can be computed from the probability that evaluation noise, modeled for example by a Gaussian distribution, changes the sign of each coefficient. This approach has been used in [68] to model resistance of Random Binary Hashing against Gaussian evaluation noise by finding the upper bound of the probability of bit flip in the hashed value. The same approach can be applied in the future to find the hashing resistance of Gabor Binary Hashing knowing that the Gabor Coefficients usually follows Laplacian distribution. As the bits of the hashed value in Gabor Binary Hashing are constructed from ordering magnitude of the coefficients, finding a tight bound will probably require applying order statistics [86].

3. In general, the main goal in the design procedure of all the components of Image-based physical function system is to achieve better results in terms of trade-off between robustness and physical unclonability. For a fixed Image-based PUF and evaluation procedure, improvements can be made in extraction procedure i.e., either in image hashing as discussed earlier or in the secure sketch. As a possible improvement to code-offset secure sketch, a future step can be using an error correcting code with soft decision decoding as proposed for the case of SRAM PUFs [87]. The basic idea is that in addition to only the '0'- or '1'-value as input of the error correcting code, soft decision information is also provided consisting of a reliability measure for the bit values. A reliability measure for each bit is inversely related to the probability that errors occur in this bit. A soft decision decoder takes into account the reliability of the received bits and outputs the codeword that was most likely transmitted. In our case study, reliability measures can be easily provided especially for fingerprints constructed with Gabor Binary Hashing. The reason is that Gabor coefficients are ordered by their magnitude and then binarized. Therefore the largest Gabor coefficient corresponding to the first fingerprint bit has the maximum reliability measure which reduces continuously along the fingerprint bits. This information can

be used to improve the performance of error correcting decoding and eventually the final results.

4. A very important open question in terms of application is the effect of aging. What will happen if the image is partially damaged due to aging? In order to characterize the resistance of the system against aging, first step is to perform experimental characterization of images after some time intervals in range of days, months or years [1]. Then considering the change of images as the aging noise, robustness and physical unclonability of the PUF system can be evaluated against this noise. One further step can be modeling this noise and use it for the estimation of robustness and physical unclonability. The noise model may also help improving the extraction process in order to get better performance. For example, if we observe that the aging happens more on some specific parts of the image, we can exclude these parts before fingerprint extraction.

5. For study of relevance of a specific PUF for a particular security application to be complete, another important issue to be addressed is to evaluate the cost forced by protecting the system with PUFs and the cloning cost an adversary should pay including the accumulated development of a successful adversarial manufacturing process. In fact, the cloning cost dictates the value that a single PUF instance can protect. For instance, for anti-counterfeiting purpose, it only makes sense to use an Image-based PUF to protect products whose value is less than the cost of cloning the PUF [2]. This motivates a future investigation on efficient evaluation of cloning cost of a specific PUF which of course depends on the available production technology. We expect that with technology growth the cloning cost of a PUF might not exceed the product value anymore. As a consequence, the PUF-based system may need to be upgraded regularly.

6. It is also interesting to apply the same experimental strategy to evaluate the properties of other types of PUF systems such as SRAM PUF system, Arbiter PUF system, etc. As discussed throughout the thesis, a PUF is usually combined with an extraction procedure and thus it is more reasonable to validate the properties of the system rather that the PUF itself. Moreover, as we observed for a practical application e.g., anti-counterfeiting scheme, the security of the scheme is reduced to the physical unclonability of the PUF system. For sure, the properties

[1] Note that the aging can be artificially accelerated.
[2] The product value implicitly contains the cost forced by protecting the system with PUFs.

of the system reflect both properties of the PUF under study and the employed extraction algorithm. In the literature, comparisons between PUFs were typically made for the PUFs itself. We believe that more practical comparison would be possible if the properties are evaluated for the PUF system including the extraction procedure. For that, the same experimental methodology proposed in this work for estimating robustness and physical unclonability can be easily applied for other types of PUFs and their trade-off would be a good metric for comparison purposes. For more advanced application than anti-counterfeting (e.g., remote authentication), in case the PUF under study produces a lot of unpredictable challenge-response pairs, a fair evaluation of the unpredictability property would also be necessary [1].

7. This thesis formally analyzed the security of anti-counterfeiting application based on minimum security properties expected from Image-based PUFs. This opens the road toward considering more advanced applications with more challenging security requirements as a future study. For instance, consider a copy protection scenario which is very close to anti-counterfeiting application except that the output of the PUF is used as a secret key to encrypt the content of the media e.g., a CD. In this application, rather than robustness and physical unclonability that have been validated, another security concern is the secrecy of PUF output (i.e., it should be uniformly random) knowing that helper data is publicly known. One way to ensure this property can be adding a privacy amplification component in the extraction procedure to produce uniformly random output and use it as a secret key. It then remains to evaluate the secrecy of the PUF output considering the information that is leaked by the public helper data.

APPENDIX A

WHITE LIGHT INTERFEROMETRY IMAGING SYSTEM

In this appendix, we present the White Light Interferometry system used to acquire very high resolution images from Laser-Written PUFs. The schematic presentation of the system is given in Fig. A.1.

An LED is used as the light source. The beam is collimated and focused on the sample with a microscope objective . The chosen configuration utilizes a two-beam Mirau interferometer at the microscope objective. It is mounted on an piezoelectric transducer to enable fine movements. Inside the microscope objective itself, there is a beam splitter BS and a reference mirror. The beam is split into a reference beam and a probe beam. After reflections on the surface of the reference mirror and on the sample respectively, the two beams are recombined and interfere. The interference pattern is imaged on a CCD camera. The pattern recorded on a CCD camera represents the intensity of interference pattern that is further processed to give the depth profile of the sample.

With respect to the more conventional Michelson interferometer, the Mirau configuration can increase the stability between the sample and the reference path lengths. The sample is mounted on a 3-axis motorized translation stage in order to extend the field of view of the system by acquiring successive images for different positions of the samples. This is necessary to probe large areas of the sample. A computer is used to control the piezoelectric transducer, the motorized translation stage and the CCD camera to process the raw images. The intensity recorded on each pixel can be expressed as:

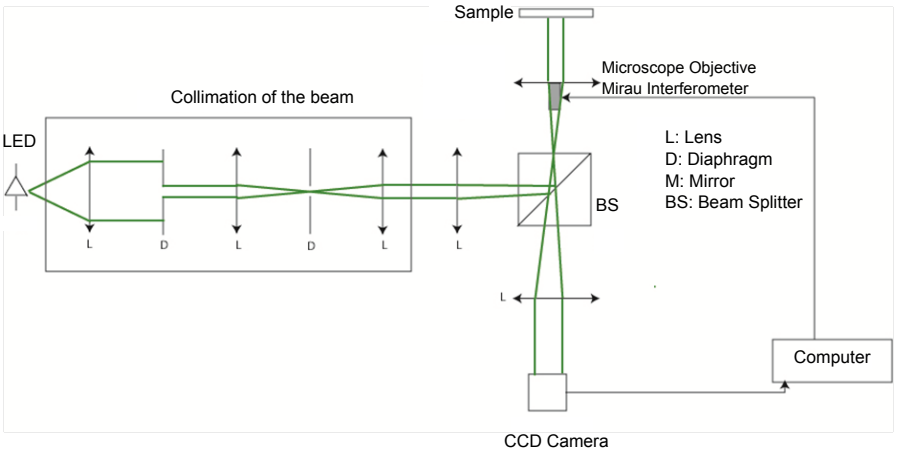


Fig. A.1.: The schematic of White Light Interferometry System

$$I(x,y) = I_0(1 + V cos(\phi)), \tag{A.1}$$

where I_0 is the sum of intensity of the two interfering beams i.e., $I_0 = I_r + I_p$, (I_r and I_p are the intensities of the reference beam and of the probe beam respectively), V is the fringe modulation of the interferences and ϕ is the phase difference between the two beams. All these parameters might be position dependent. The angle ϕ is proportional to the length difference between the two arms of the interferometer:

$$\phi = \frac{4\pi(L_r - L_p)}{\lambda}, \tag{A.2}$$

where L_r and L_p are the lengths of the reference arm and the probe arm respectively and λ is the center wavelength of the light source. The topography of the sample is then straightforwardly computed from the angle distribution $\phi(x,y)$. Since there are three unknown parameters in Eq. A.1, at least three measurements are necessary to extract the angle ϕ.

The measurements are obtained by introducing a phase shift in one of the two arms. A five-step algorithm (instead of three-step) has been chosen to make the system more robust against to the phase step error. In practice a $\pi/2$ phase step is achieved by a movement of $\lambda/8$ of the Mirau objective. The intensity of the interfering beams is recorded for each of the five positions. The phase is then calculated as:

$$\phi = \arctan(\frac{2(I_2 - I_4)}{2I_3 - I_1 - I_5}). \tag{A.3}$$

The 2D phase distribution is numerically unwrapped to calculate the absolute depth distribution. The above setup achieves a sub micron transverse resolution and a nanometer longitudinal resolution. It is worth to remark that the transverse resolution is determined by the microscope objective and CCD camera and longitudinal resolution relates to the applied phase-shifting Interferometry method.

APPENDIX B

CREATION PROCESS OF CRYSTAL PUFS

In this appendix, we provide more details on the procedure used to create Crystal PUFs. The proposed method is based on the crystallization properties of polypropylene (PP). Polypropylene is a polymer that can have different geometrical morphologies depending on the chemical structure of it. The formula

$$CH_3 - \left[-CH_2 - \underset{\displaystyle CH_3,}{\underset{|}{CH}} - \right]_n - CH_3 \tag{B.1}$$

enables various configurations. Considering the backbone of the carbon-carbon chemical bonding line, it may take various configurations as depicted in Fig. B.1.

The manufacturing process to produce the polypropylene will result in one or another type of polypropylene. The resulting crystallinity can be varied from few percentages for the "amorphous PP" (aPP) to almost 100%. Polypropylene has a high resistance to most liquids which makes it difficult to dissolve. Nevertheless one can dissolve PP in xylene solvent under reflux [88]. For the production of Crystal PUF, various types of PP and various solutions of PP in xylene have been tested. As the liquid was not hot enough, no dissolution of the cavity wall was observed. The structures can be different as a result of the random evaporation/crystallization process. The quantity

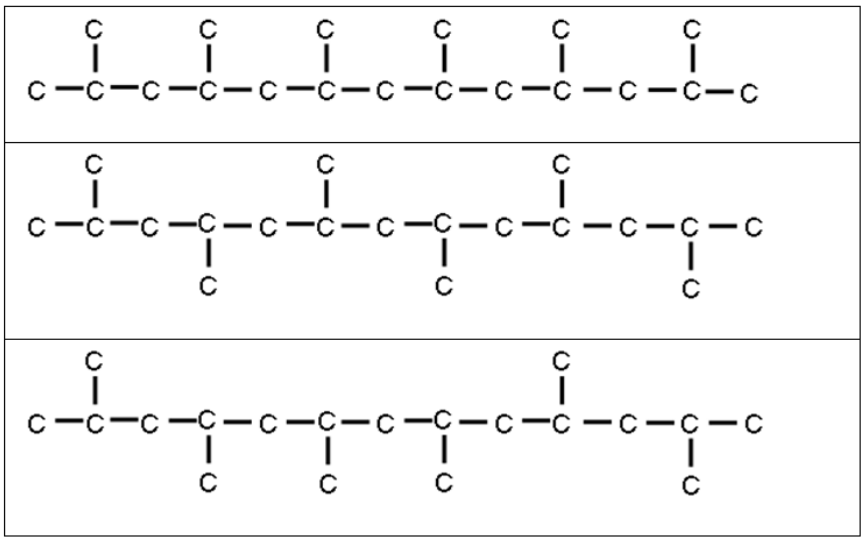


Fig. B.1.: Polypropylene possible chemical structure. From top to bottom: Isotactic; syndiotactic and amorphous.

of PP, the type of PP, the temperature and the concentration influence the structure of the material.

In practice, to produce Crystal PUFs, PP is dissolved in xylene under reflux and then let to cool down. In next step, the solutions were deposited in cavities made of a polypropylene support at room temperature and let the xylene evaporate. The resulting random 3D topography of the Crystal PUF is the result of both phenomena: evaporation of the solvent and crystallization of the PP.

Bibliography

[1] F. Armknecht, R. Maes, A. R. Sadeghi, F.-X. Standaert, and C. Wachsmann, "A formalization of the security features of physical functions," in *IEEE Symposium on Security and Privacy*, 2011, pp. 397–412.

[2] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, pp. 2026–2030, 2002.

[3] E. Metois, P. Yarin, N. Salzman, and J. R. Smit, "Fiberfingerprint identification," in *Workshop on Automatic Identification*, 2002, pp. 147–154.

[4] J. D. R. Buchanan, R. P. Cowburn, A. V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan, "Fingerprinting documents and packaging," *Nature*, p. 475, 2005.

[5] W. Clarkson, T. . Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten, "Fingerprinting blank paper using commodity scanners," in *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, 2009, pp. 301–314.

[6] A. Sharma, L. Subramanian, and E. A. Brewer, "Paperspeckle: microscopic fingerprinting of paper," in *Proceedings of the 18th ACM conference on Computer and communications security*, ser. CCS '11. ACM, 2011, pp. 99–110.

[7] P. Bulens, F.-X. Standaert, and J.-J. Quisquater, "How to Strongly Link Data and its Medium: the Paper Case," *IET Information Security*, vol. 4, no. 2, pp. 125–136, 2010.

[8] D. Kirovski, "Toward an automated verification of certificates of authenticity," in *Proceedings of the 5th ACM conference on Electronic commerce*, ser. EC '04. ACM, 2004, pp. 160–169.

[9] Y. Chen, K. Mihçak, and D. Kirovski, "Certifying authenticity via fiber-infused paper," *SIGecom Exch.*, vol. 5, pp. 29–37, April 2005.

[10] P. Tuyls, G.-J. Schrijen, F. Willems, T. Ignatenko, and B. Skoric, "Secure key storage with PUFs," *Springer*, pp. 255–268, 2008.

[11] D. Bauder, "An anti-counterfeiting concept for currency systems." Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990, 1983.

[12] C. o. E. Committee on Next-Generation Currency Design and N. R. C. Technical Systems, *Counterfeit Deterrent Features for the Next-Generation Currency Design*. The National Academies Press, 1993.

[13] R. Pappu, "Physical one-way functions," Ph.D. dissertation, MIT, March 2001.

[14] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *ACM conference on Computer and communications security*, November 2002.

[15] P. Tuyls, G. J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-proof hardware from protective coatings," in *Cryprographic Hardware and Embedded Systems Workshop*, ser. LNCS, vol. 4249. Springer, 2006, pp. 369–383.

[16] C. N. C. et al., "Anti-counterfeiting with a random pattern," in *Int. Conf. on Emerging Security Information, Systems and Tech.*, 2008, pp. 146–153.

[17] C. N. Chong and D. Jiang, "Anti-counterfeiting using phosphor PUF," in *International Conference on In Anti-counterfeiting*, 2008, pp. 59–62.

[18] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[19] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *VLSI Circuits. Digest of Technical Papers*, 2004, pp. 176–179.

[20] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Cryprographic Hardware and Embedded Systems Workshop*, vol. 4247, 2007, pp. 63–80.

[21] Y. Su, J. Holleman, and B. Otis, "A 1.6pj/bit 96 stable chip-id generating circuit using process variations," in *Solid-State Circuits Conference, 2007. ISSCC 2007. Digest of Technical Papers. IEEE International*, Feb. 2007, pp. 406–611.

[22] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," in *Cryptographic Hardware and Embedded Systems, CHES 2010*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2011, vol. 6225, pp. 366–382.

[23] K. Shimuzu, D. Suzuki, and T. Kasuya, "Glitch PUF: Extracting information from usually unwanted glitches," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E95.A, no. 1, pp. 223–233, 2012.

[24] S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting ip on every fpga," in *Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE Computer Society, 2008, pp. 67–70.

[25] P. Tuyls, B. Skoric, and T. Kevenaar, *Security with Noisy Data*. Springer, 2007.

[26] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*, ser. Information Security and Cryptography. Springer Berlin Heidelberg, 2010, pp. 3–37.

[27] R. Maes, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, KU Leuven, Auguest 2012.

[28] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in *Topics in Cryptology - CT-RSA 2006, volume 3860 of LNCS*. Springer Verlag, 2006, pp. 115–131.

[29] Y. D. et al., "Fuzzy extractors: How to generate strong secret keys from biometrics and other noisy data," in *Eurocrypt'04*, 2004, pp. 523–540.

[30] S. D. G. E. Suh, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual Design Automation Conference*. ACM, 2007, pp. 9–14.

[31] P. Tuyls and B. Škorić, "Strong authentication with physical unclonable functions," in *Security, Privacy, and Trust in Modern Data Management*, 2007, pp. 133–148.

[32] P. Tuyls and B. Skoric, "Secret key generation from classical physics," in *Philips Research Book Series*, 2005.

[33] B. Skoric, P. Tuyls, and W. Ophey, "Robust key extraction from physical uncloneable functions," in *Applied Cryptography and Network Security (ACNS)*, 2005, pp. 407–422.

[34] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on VLSI Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[35] G. Hammouri, A. Dana, and B. Sunar, "Cds have fingerprints too," in *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '09. Springer-Verlag, 2009, pp. 348–362.

[36] P. Tuyls, B. Škorić, S. Stallinga, A. H. M. Akkermans, and W. Ophey, "Information-theoretic security analysis of physical uncloneable functions," in *Proceedings of the 9th international conference on Financial Cryptography and Data Security*, ser. FC'05. Springer-Verlag, 2005, pp. 141–155.

[37] B. Škorić, S. Maubach, and T. A. M. K. andP. Tuyls, "Information-theoretic analysis of coating PUFs." *IACR Cryptology ePrint Archive*, vol. 2006, p. 101, 2006.

[38] S. Shariati, F. X. Standaert, L. Jacques, B. Macq, M. A. Salhi, and P. Antoine, "Random profiles of laser marks," in *WIC Symposium on Information Theory in the Benelux*, 2010, pp. 27–34.

[39] J.-S. Coron and D. Naccache, "An accurate evaluation of maurer's universal test," *Lecture Notes in Computer Science*, vol. 1556, pp. 57–71, 1998.

[40] F. Willems, Y. Shtarkov, and T. Tjalkens, "The context-tree weighting method: Basic properties," *IEEE Trans. on Information Theory*, vol. 41, pp. 653–664, 1995.

[41] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, ser. LNCS, vol. 4727, 2007, pp. 63–80.

[42] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc., 1996.

[43] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conference on Computer and Communications Security*, 1999, p. 28.

[44] J. Carter and M. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, pp. 143–154, 1979.

[45] T. Ignatenko, "Secret-key rates and privacy leakage in biometric systems," Ph.D. dissertation, TU Eindhoven, 2009.

[46] D. Kirovski, "Anti-counterfeiting: Mixing the physical and the digital world," in *Foundations for Forgery-Resilient Cryptographic Hardware*, ser. Dagstuhl Seminar Proceedings, J. Guajardo, B. Preneel, A.-R. Sadeghi, and P. Tuyls, Eds., no. 09282, 2010.

[47] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2008.

[48] G. Arce, *Nonlinear Signal Processing: A Statistical Approach.* John Wiley & Sons, 2005.

[49] A. Buades and B. Coll, "A non-local algorithm for image denoising," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2005, pp. 60–65.

[50] L. Vincent, "Morphological grayscale reconstruction in image analysis: Applications and efficient algorithms," *IEEE Trans. on Image Processing*, vol. 2, pp. 176–201, 1993.

[51] ——, "Grayscale area openings and closings, their efficient implementation and applications," in *First Workshop on Math. Morphology*, 1993, pp. 22–27.

[52] P. M. Roth and M. Winter, "Survey of Appearance-Based Methods for Object Recognition," Institute for Computer Graphics and Vision, Graz University of Technology, Tech. Rep., 2008.

[53] Z. Baoshi, W. Jiankang, and M. S. Kankanhalli, "Print signatures for document authentication," in *ACM Conference on Computer and Communications Security*, 2003, pp. 145–153.

[54] F. Beekhof, S. Voloshynovskiy, O. Koval, and R. Villán, "Secure surface identification codes," in *Steganography, and Watermarking of Multimedia Contents X*, ser. Proceedings of SPIE, vol. 6819, 2008.

[55] S. Mallat, *A Wavelet Tour of Signal Processing: The Sparse Way*, 3rd ed. Academic Press., Dec. 2008.

[56] L. Jacques, L. Duval, C. Chaux, and G. Peyré, "A panorama on multiscale geometric representations, intertwining spatial, directional and frequency selectivity," *CoRR*, vol. abs/1101.5320, 2011.

[57] J. N. Laska, S. Kirolos, M. F. Duarte, T.Ragheb, R. G. Baraniuk, and Y. Massoud, "Theory and implementation of an analog-to-information converter using random demodulation," in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS)*, 2007, pp. 1959–1962.

[58] E. J. Candes and J. Romberg, "Quantitative robust uncertainty principles and optimally sparse decompositions," *Found. Comput. Math.*, vol. 6, pp. 227–254, April 2006.

[59] Y. Tsaig and D. L. Donoho, "Compressed sensing," *IEEE Trans. Inform. Theory*, vol. 52, pp. 1289–1306, 2006.

[60] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge Univ. Press, 2003.

[61] W. R. B. . TOMO3D project-Tomographie optique á haute résolution, WIST2 Program contract n°616444.

[62] D. Malacara, *Optical Shop Testing*, 2nd ed. Wiley-Interscience, 1992.

[63] J. Wyant, "White light interferometry," in *Conference on Holography(SPIE)*, 2002.

[64] W. R. B. . TRACEA project-Traçabilité et anti-contrefaćon par marquage aléatoire micro structuré, Programme Mobilisateur Marshall.

[65] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A Simple Proof of the Restricted Isometry Property for Random Matrices," *Constructive Approximation*, vol. 28, pp. 253–263, 2008.

[66] M. Goemans and D. Williamson, "Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming," *ACM*, vol. 42, p. 1145, 1995.

[67] M. S. Charikar, "Similarity estimation techniques from rounding algorithms," in *In Proc. of 34th STOC*. ACM, 2002, pp. 380–388.

[68] L. Jacques, J. N. Laska, P. T. Boufounos, and R. G. Baraniuk, "Robust 1-bit compressive sensing via binary stable embeddings of sparse vectors," *ArXiv e-prints*, 2011.

[69] M. Duarte, M. Davenport, D. Takhar, J. Laska, T. Sun, K. Kelly, and R. Baraniuk, "Single-pixel imaging via compressive sampling," *IEEE Signal Proc. Mag.*, vol. 25, pp. 83–91, 2008.

[70] B. A. Olshausen and D. J. Field, "Emergence of simple-cell receptive field properties by learning a sparse code for natural images," *Nature*, vol. 381, pp. 607–609, 1996.

[71] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proceedings of the International Conference on Computer Vision-Volume 2 - Volume 2*. IEEE Computer Society, 1999, pp. 1150–.

[72] B.-J. L. F. Lefebvre, B. Macq, "Rash: Radon soft hash algorithm," in *Proceedings of the European Signal Processing Conference*, Sep. 2002.

[73] F.-X. Standaert, F. Lefebvre, G. Rouvroy, B. Macq, J.-J. Quisquater, and J. Legat, "Practical evaluation of a radial soft hash algorithm," in

Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II - Volume 02. IEEE Computer Society, 2005, pp. 89–94.

[74] C. D. Roover, C. D. Vleeschouwer, F. Lefèbvre, and B. Macq, "Robust image hashing based on radial variance of pixels," in *IEEE International Conference on Image Processing ICIP*, 2005, pp. 77–80.

[75] B. Yang, F. Gu, and X. Niu, "Block mean value based image perceptual hashing," in *Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia*. IEEE Computer Society, 2006, pp. 167–172.

[76] L. Vincent, "Grayscale area openings and closings, their efficient implementation and applications," 1993, pp. 22–27.

[77] R.Suganya, K.Priyadharsini, and S.Rajaram, "Article: Intensity based image registration by maximization of mutual information," *International Journal of Computer Applications*, vol. 1, no. 20, pp. 1–5, February 2010.

[78] F. M. Naini, R. Gribonval, L. Jacques, and P. Vandergheynst, "Compressive sampling of pulse trains: Spread the spectrum!" *Acoustics, Speech, and Signal Processing, IEEE International Conference on*, pp. 2877–2880, 2009.

[79] G. Puy, P. Vandergheynst, R. Gribonval, and Y. Wiaux, "Universal and efficient compressed sensing by spread spectrum and application to realistic fourier imaging techniques," *CoRR*, vol. abs/1110.5870, 2011.

[80] D. W. SCOTT, "On optimal and data-based histograms," *Biometrika*, vol. 66, no. 3, pp. 605–610, 1979.

[81] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, pp. 3–18, 2006.

[82] T. Staake and E. Fleisch, *Countering Counterfeit Trade: Illicit Market Insights, Best-Practice Strategies, and Management Toolbox*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[83] S. Bastia, "Next generation technologies to combat counterfeiting of electronic components," *IEEE Trans. on Components and Packaging Tech.*, vol. 25, pp. 175–176, 2002.

[84] S. Mallat and Z. Zhang, "Matching pursuit with time-frequency dictionaries," *IEEE Transactions on Signal Processing*, vol. 41, pp. 3397–3415, 1993.

[85] A. Andoni and P. Indyk, "Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions," *Commun. ACM*, vol. 51, no. 1, pp. 117–122, Jan. 2008.

[86] H. N. N. H. A. David, *Order Statistics*, 3rd ed. Wiley, 2003.

[87] R. Maes, P. Tuyls, and I. Verbauwhede, "A soft decision helper data algorithm for sram PUFs," in *IEEE International Symposium on Information Theory ISIT*, 2009.

[88] R. Rioboo, M. Voué, A. Vaillant, D. Seveno, J. Conti, A. Bondar, D. Ivanov, and J. De Coninck, "Superhydrophobic surfaces from various polypropylenes." *Langmuir*, 2008.