Anti-Counterfeiting technique based Reflective-Physically Unclonable Functions

H. Umesh Babu*, N. Heussner**, W. Stork*

*Institute for Information Processing Technologies, Karlsruhe Institute of Technology
**FZI Forschungszentrum Informatik., Karlsruhe

mailto:harsha.umeshbabu@kit.edu

Reflective - Physically Unclonable Functions (r-PUFs) are a manifestation of a security principle where two dimensional projections of randomly distributed reflective microstructures in a three dimensional plane form the basis of an anti-counterfeiting technique. In this paper we present an overview of the system design with focus on optical aspects of the technique along with summary results.

1 Introduction

Anti-counterfeiting in a broad sense is the application of cryptological primitive or a security feature to any product or commodity with an intention of proving its authenticity, integrity or both. Physically Unclonable Functions (PUF) are physical manifestations of one way functions. We present an optical variant, reflective-Physically Unclonable Function (r-PUF), that can be used in the context of product security as an anti-counterfeiting technique. At the heart of this approach lies randomly distributed micro-structures in a three dimensional plane. The reflection pattern of such an assembly is dependent on angles of illumination (primarily) and wavelength (the size of micro-structures and their reflective properties play a role here). The projection of the reflection pattern on to a two dimensional plane (in simpler words, an image) forms the core aspect of security. Due to the random distribution of the particles, the reflection pattern too will be random in nature.

2 Background

This section can be divided into background on anti-counterfeiting techniques and PUF in general.

2.1 Overview of anti-counterfeiting techniques

There exists a host of security techniques for anti-counterfeiting that are in use today. The most common in retail product space are radio frequency identification (RFID) tags, variety of two dimensional barcodes (that have the added advantage of being useful in logistical handling), secure printing in form of watermarks and a host of optical methods such as optically variable devices, interference structures and markings with optically variable inks [1]. r-PUF fits well with these optical techniques. The state of the art, i.e., a variety of holograms and diffractive structure based secure markings has its failings, where recent advances have enabled overcoming of costly replication technology. This has increased interest in new anti-counterfeiting techniques.

2.2 PUFs

Physically unclonable functions was a term coined by Pappu et al. [2], where randomly distributed glass spheres in a Plexiglass token are used as a security tag. The speckle pattern on illumination with a coherent source serves as the core feature here. The use of coherent illumination, induces stringent requirements in terms of engineering, thus impacting practicality. Over the last ten years many other physical phenomena have been exploited to construct PUFs such as uncertainty in timing on delay line on a integrated circuit (IC), initial states of the memory elements in static random access memory units, randomly distributed dielectric parts between plates of a capacitor, random structure of the fiber in paper, imaging of the micro variations in laser markings caused by random noise in the laser source and so on. An exhaustive compilation can be found in [3].

3 System Concept

3.1 What does r-PUF entail?

r-PUF is a variant of the optical PUF, where reflective micro-structures are randomly distributed and embedded in a transparent three dimensional token. On illumination from an incoherent source, the reflection pattern can be imaged by a camera. Since the reflecting micro-structures are $5\mu m - 50\mu m$, magnification optics is required to image their reflections. Not all micro-structures contribute to the reflection pattern. The reflection pattern is dependent on angle of illumination, distribution of micro-structures and their orientation in three dimensional space. For a given token with a random distribution, one can generate many reflection patterns by varying the illumination settings. The micro-structures can be designed to be reflective to specific wavelength range. Two different varieties were explored, a UV range specific coating and another one active in visible range. However, the sensitivity to angle of illumination is of more interest and this is exploited to generate reflection patterns which serve as a security feature.

DGaO Proceedings 2014 - http://www.dgao-proceedings.de - ISSN: 1614-8436 - urn:nbn:de:0287-2014-A030-2
submitted: 25. Jul. 2014 published: 11. Aug. 2014

3.2 How does it fit into anti-counterfeiting?

An important aspect of an ideal anti-counterfeiting technique is its linkage to the product. If a technique is used extrinsically, the level of security and the incorporation into product life cycle is lowered. To this end, an intrinsic solution which is attached to the product and is a part of the manufacturing or finishing process is more attractive. r-PUF based solution uses tags of $\sim 10mm \times 10mm$, with a few hundred micrometer thickness and can be attached to a product or its packaging at the end of the assembly line. The tags themselves are transparent and the microstructures are not visible to the naked eye.

The tag is imaged with preselected illumination parameters and an unique hash code is generated and stored in a database along with product details. During the verification phase, the tag is reimaged with the same set of illumination parameters. A hash code computed and compared with the stored value in the database. In the scheme of PUF based solutions, the illumination parameters are called *challenge* and the reflection pattern that is imaged, the *response*. The security of a solution is expounded by the analysis of this relationship between the *challenge-response pairs* (CRP) for a given tag as well as the PUF family. If $iSource_{total}$ is the total number of possible illumination source positions, from which a reflection pattern can be generated, the cardinality of the CRP space is given by

$$CRP_{cardinality} = \sum_{n=1}^{iSource_{max}} \begin{pmatrix} iSource_{total} \\ n \end{pmatrix} \quad (1)$$

Some PUF analyses estimate the security of the system looking at its cardinality. The larger the cardinality, the system is considered to be more secure. For r-PUF, the value is in the order of millions [6]

3.3 Description of the end-to-end system

As a part of the study to implement r-PUFs and analyse them, an end-to-end system was built. The r-PUF tags are created, keeping the integration on assembly line manufacturing in mind. The transparent ink mixed with reflective micro-structures is applied onto the product packaging and imaged using magnification optics under given set of illumination parameters. These images are then processed to generate a unique hash code which is stored in a database. This process is called registration.

At the verification end, a cell phone with add-on optics is used to image the tag. The add-on optical module consists of a magnification lens and the illumination unit where the parameters can be tuned to fit with settings from the registration process. For this study, an android phone was used with a custom application capable of controlling the illumination parameters, computing the hash code from the image and handling the interaction with the database server.

The generation of the hash code from an image is a well researched topic. Many different approaches were explored. Hash codes generated using Gabor decomposition was found to be most suitable. Daugman [4] was the first to propose this method, where it was used for building hashes from the iris images of people for use in biometric applications. The general form of the Gabor decomposition filter [5] contains the spatial frequency component, orientation and the sub-sampling factor, which were used as design variables to tune the filter for the given application scenario, while the scale factor for Gaussian envelope was set to one octave [5]. [6] contains more detailed reporting of system requirements, analysis and design.

4 Results and conclusion

There are two specific metrics used to evaluate or compare different PUF implementations. Inter-distance is the distance between two responses to a given challenge applied to two different instantiations or tags, while intra-distance is the distance between the responses for a given challenge and a tag at two different evaluation points. Inter-distance is reflective of the uniqueness of the system while intra-distance gives a measure of robustness.

Inter-distance for r-PUF based implementation was found to be $\sim 49\%$ indicating high uniqueness, while intra-distance was found to be $< 3\%$, a representation of a robust system . This compares well with the state of the art in PUF implementations[6].

References

[1] R. L. van Renesse, “A Review of Holograms and other Microstructures as Security Features,” in *Holography, The first 50 years* (Springer series in Optical Sciences Vol.78, Springer Verlag(2003), 2003).

[2] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way functions,” Science **297**(5589), 2026 (2002).

[3] A. Sadeghi and D. Naccache, *Towards Hardware-Intrinsic Security: Foundations and Practice* (Springer-Verlag New York Inc, 2010).

[4] J. Daugman, “Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression,” Acoustics, Speech and Signal Processing, IEEE Transactions on **36**(7), 1169–1179 (1988).

[5] O. Nestares, R. Navarro, J. Portilla, and A. Tabernero, “Efficient spatial-domain implementation of a multiscale image representation based on Gabor functions,” Journal of Electronic Imaging **7**(1), 166–173 (1998).

[6] H. Umesh Babu, “Reflective-Physically Unclonable Function based System for Anti-Counterfeiting,” Ph.D. thesis (2013). Zugl.: Karlsruhe, KIT, Diss., 2013.