

# SECURITY ANALYSIS OF PHYSICAL UNCLONEABLE FUNCTIONS

P. Tuyls, B. Skoric, T. Akkermans, W. Ophey, S. Stallinga

Philips Research Laboratories

Prof. Holstlaan 4, AA 5656 Eindhoven, The Netherlands

{`pim.tuyls@philips.com`}

*We propose a general theoretical framework to analyze the security of Physical Uncloneable Functions (PUFs). We apply the framework to Optical PUFs. In particular we present a derivation, based on the physics governing multiple scattering processes, of the number of independent challenge-response pairs supported by a PUF. We find that the number of independent challenge-response pairs is proportional to the square of the thickness of the PUF, and inversely proportional to the wavelength of the laser and to the scattering length in the PUF. We compare our results to those of Pappu and show that they are compatible in the case where the density of scatterers becomes very high.*

## INTRODUCTION

A ‘Physical Uncloneable Function’ (PUF) is a function that is realized by a physical system, such that the function is easy to evaluate but the physical system is hard to characterize [1, 2]. PUFs were introduced by Pappu [3] as a cost-effective way of generating secure keys for cryptographic purposes. They offer an attractive alternative for the Unforgeable Subway Tokens introduced by Bennett et al. [4]. The main difference resides in the fact that PUFs are based on classical physics while Bennett’s tokens are based on the Uncloneability property of quantum bits. By storing a key in a PUF, the key becomes uncloneable. Hence, it can not be given away or copied. Therefore, PUFs are attractive in Digital Rights Management (DRM) systems.

A PUF is a physical system designed such that it interacts in a complicated way with stimuli (challenges) and leads to unique but unpredictable responses. Hence, a PUF is similar to a keyed hash function. The key is the physical system consisting of many “random” components. In order to be hard to characterise,

the system should not allow efficient extraction of the relevant properties of its interacting components by measurements.

Physical systems that are produced by an uncontrolled production process, i.e. one that contains some randomness, turn out to be good candidates for PUFs. Because of this randomness, it is hard to produce a physical copy of the PUF. Furthermore, if the physical function is based on many complex interactions, then mathematical modeling is also very hard. These two properties together are referred to as *Uncloneability*.

From a security perspective the uniqueness of the responses and uncloneability of the PUF are very useful properties. Because of these properties, PUFs can be used as unique identifiers for smart-cards and credit cards or as a ‘cheap’ source of key generation between two parties (common randomness).

At the moment there are two main candidates: optical PUFs [3, 5] and silicon PUFs [2, 6]. Silicon PUFs make use of production variation in the properties of logical gates. When these are probed at frequencies that are out of spec, a unique, unpredictable response is obtained in the form of delay times. In this paper we will only consider optical PUFs.

Optical PUFs consist of a physical structure containing some scattering material which is randomly distributed. They exploit the uniqueness of speckle patterns that result from multiple scattering of laser light in this disordered optical medium. The input (‘challenge’) can be e.g. the angle of incidence, focal distance or wavelength of the laser beam, a mask pattern blocking part of the laser light, or any other change in the wave front. The output, usually called the response, is the speckle pattern. An input-output pair is usually called a *Challenge-Response Pair* (CRP). Physical copying is difficult for two reasons: (i) The light diffusion obscures the locations of the scatterers. At this moment the best physical techniques can probe strongly diffusive materials up to a depth of  $\approx 10$  scattering lengths [7]. (ii) Even if all scatterer locations are known, precise positioning of a large number of scatterers is very hard and expensive, and requires a production process different from the original randomized process.

Modeling of optical PUFs, on the other hand, is difficult due to the inherent complexity of multiple coherent scattering [8]. Even the ‘forward’ problem turns out to be hard: given the details of all the scatterers, a computation of the speckle pattern using Feynman diagrams requires summation over a number of diagrams that grows exponentially with the number of scattering events.

## MOTIVATION

In this paper we denote the set of PUFs by  $\mathcal{K}$ , and a PUF  $K$  is modeled as a stochastic variable  $K \in \mathcal{K}$ . The amount of information about the PUF that is revealed by one response  $R$  (speckle pattern) is given by the mutual information  $\mathbf{I}(K; R)$ ,

$$\mathbf{I}(K; R) = \mathbf{H}(K) - \mathbf{H}(K|R), \quad (1)$$

where  $\mathbf{H}$  stands for the Shannon entropy. It can be easily seen that [9]

$$\mathbf{I}(K; R) = \mathbf{H}(R). \quad (2)$$

In order to be able to talk about the information content of PUFs and speckle patterns, we have to make precise what we mean by this notion. This is done in the following sections.

## Definitions

The information content of a PUF,  $\mathbf{H}(K)$ , and of its output,  $\mathbf{H}(R)$ , is determined by the measurements that can be performed on the system. This is formalized as follows. We identify a measurement with its possible outcomes.

**Definition 1** *A measurement  $\mathcal{M} = \{R_1, \dots, R_m\}$  is a partition of  $\mathcal{K}$ .*

Here  $R_j$  is the region in  $\mathcal{K}$  containing all PUFs that produce outcome  $j$  upon measurement  $\mathcal{M}$ , and  $m$  is the number of possible outcomes. Two measurements give more (refined) information than one. The composition of two measurements is denoted as  $\mathcal{M}_1 \vee \mathcal{M}_2$  and is defined as follows:

$$\mathcal{M}_1 \vee \mathcal{M}_2 = \{R_i^{(1)} \cap R_j^{(2)}\}_{i,j=1}^m. \quad (3)$$

$R_j^{(i)}$  is the set of all PUFs that produce outcome  $j$  when measurement  $\mathcal{M}_i$  is performed. By induction this definition extends to composition of more than two measurements.

**Definition 2** *Let  $\eta$  denote a probability measure on  $\mathcal{K}$ . The information obtained about a physical system  $K \in \mathcal{K}$  by performing a measurement  $\mathcal{M}$  is defined as*

$$h_{\mathcal{M}}(\mathcal{K}) = - \sum_{i=1}^m \eta(R_i) \log_2 \eta(R_i).$$

Due to the physics, one will often only have a specified set of measurements (challenges) available. We denote this set by  $\mathcal{A}$ . This set has to be specified for every situation and restricts the amount of information that can be obtained on a physical system. We introduce the following definition.

**Definition 3**<sup>1</sup> *Given the set of possible measurements  $\mathcal{A}$ , the total amount of information that can be obtained about a system  $\mathcal{K}$  is*

$$h_{\mathcal{A}}(\mathcal{K}) = \sup_q \sup_{\mathcal{M}_1, \dots, \mathcal{M}_q \in \mathcal{A}} h_{\mathcal{M}_1 \vee \dots \vee \mathcal{M}_q}(\mathcal{K}).$$

It follows from the monotonicity property  $h_{\mathcal{M}_1 \vee \mathcal{M}_2} \geq h_{\mathcal{M}_1}$  [9] that  $h_{\mathcal{A}}(\mathcal{K}) \leq H_{\eta}(K)$ , i.e. the maximum amount of information that can be obtained about a system is upper bounded by the amount of uncertainty one has in the measure  $\eta$ . If  $\eta$  is given by the uniform random measure  $\eta(K_i) = 1/|\mathcal{K}|$ , we find that  $H_{\eta}(K) = \log_2 |\mathcal{K}|$ . In the remainder of this text, we will assume that  $\eta$  is given by this measure.

Definitions 1 and 2 are very general and apply to many kinds of PUFs. In this framework, the couple  $(\mathcal{K}, \mathcal{A})$  has to be defined for a well-defined notion of PUF security. We consider two extreme cases to illustrate the definitions. A CRP measurement that distinguishes PUFs perfectly reveals all information about the PUF. If such a CRP measurement is an element of  $\mathcal{A}$ , then the PUF supports only one independent CRP. The opposite extreme case is a set of measurements  $\mathcal{A} = \{\mathcal{M}_j\}_{j=1}^n$  that can be represented as an extremely coarse partitioning of  $\mathcal{K}$ , say  $|M_1^{(j)}| = |M_2^{(j)}| = |\mathcal{K}|/2$ , where the combined measurements  $(\mathcal{M}_1 \vee \dots \vee \mathcal{M}_n)$  suffice to distinguish all elements of  $\mathcal{K}$ . In this case a minimum of  $\log_2 |\mathcal{K}|$  measurements is needed to reveal all details of the PUF.

For good PUFs, all available measurements are fuzzy, revealing little about the distribution of the optical scatterers in the PUF. It is the goal and the art to choose physical systems for which only such measurements are possible.

## OPTICAL PUFs

We illustrate Definition 2 for optical PUFs. As an optical PUF is probed with light of wavelength  $\lambda$ , it follows from the theory of electromagnetism [11] that details smaller than  $\lambda$  are very difficult to resolve. It is natural to divide the

---

<sup>1</sup>We note that this definition is in agreement with the theory of dynamical systems and dynamical entropy [12].

volume into elements (‘voxels’) of volume  $\lambda^3$ . The number of voxels is  $N_{\text{vox}} = Ad/\lambda^3$ , where  $A$  is the illuminated area of the PUF and  $d$  its thickness.

Hence, the information content of a voxel is at most 1 bit, and the PUF can be represented as a bit string of length  $N_{\text{vox}}$ :  $\mathcal{K} = \{0, 1\}^{N_{\text{vox}}}$ .  $\mathcal{A}$  is the set of atomic measurements that can be performed by means of a beam of monochromatic light. They can be varied by changing the angle of incidence, the wavefront etc. By combining all the available measurements in  $\mathcal{A}$  the details of the PUF can be probed up to size  $\lambda$ . Hence, the maximum amount of information  $\mathbf{h}_{\mathcal{A}}(\mathcal{K})$  that can be extracted from the PUF is  $\mathbf{H}_{\eta}(K) = N_{\text{vox}}$ . The couple  $(\mathcal{K}, \mathcal{A})$  as defined here is used in the remainder of the text.

## SECURITY ANALYSIS

### Definition of the Security Parameter $C$

The main goal of this paper is to estimate the number of independent CRPs. This number is denoted as  $C$ . First, we define independence of CRPs as follows.

**Definition 4** *We say that the measurements  $\mathcal{M}_1, \dots, \mathcal{M}_t$  are mutually independent if and only if*

$$\mathbf{h}_{\mathcal{M}_1 \vee \dots \vee \mathcal{M}_t} = \mathbf{h}_{\mathcal{M}_1} + \dots + \mathbf{h}_{\mathcal{M}_t}. \quad (4)$$

Note that  $\mathbf{h}_{\mathcal{M}_1 \vee \dots \vee \mathcal{M}_t} = t \cdot \mathbf{h}_{\mathcal{M}_1}$  if all measurements give the same amount of information about a PUF, i.e.  $\mathbf{h}_{\mathcal{M}_1} = \dots = \mathbf{h}_{\mathcal{M}_t}$ , which by symmetry arguments is a reasonable assumption. Independent measurements are also called *independent CRPs* since responses are implicitly incorporated in definition 0.1. In words, knowledge of independent CRPs  $\{\mathcal{M}_j\}_{j \neq i}$  does not give any information about the response to the  $i$ -th challenge. The security parameter  $C$ , the number of independent CRPs, is hence naturally defined as

$$C = \frac{\mathbf{h}_{\mathcal{A}}(\mathcal{K})}{\mathbf{h}_{\mathcal{M}}(\mathcal{K})} = \frac{\mathbf{h}_{\mathcal{A}}(\mathcal{K})}{\mathbf{H}(R)}, \quad (5)$$

where  $\mathcal{M} \in \mathcal{A}$ , and  $\mathbf{H}(R)$  denotes the information content of a response to a challenge (measurement). The second equality in Eq. (5) follows from Eq.(2). As we have already argued that  $\mathbf{h}_{\mathcal{A}}(\mathcal{K}) = N_{\text{vox}}$ , the remainder of the text focusses on the computation of  $\mathbf{H}(R)$ .

## Speckle Pattern Entropy

It has been shown in [9] that an optical PUF can be modeled as a strongly scattering waveguide of thickness  $d$ , cross-section  $A$  and scattering length  $\ell$ , satisfying  $\lambda \ll \ell \ll d$ . The waveguide allows a number of transversal modes  $N_{\text{mod}} = \pi A/\lambda^2$ .

An upper bound for the information content of a speckle pattern is obtained as follows. First, we assume that the  $N_{\text{mod}}$  outgoing modes are independent. The smallest information carriers of light are photons. The number of distinguishable ways in which the photons that create the output (speckle pattern) can be distributed over the  $N_{\text{mod}}$  outgoing modes is a natural measure for the information content of a speckle pattern. It has been shown in [9] that this upper bound is given by,

$$H_{\text{up}}(R) \approx \frac{N_{\text{mod}}}{2} \log_2 \left( \frac{\pi e}{2} \frac{N_{\varphi}}{N_{\text{mod}}} \right). \quad (6)$$

Note that the information content of a speckle pattern,  $H(R)$ , increases with the number of contributing photons  $N_{\varphi}$  in a logarithmic way. Hence, any errors that we make in estimating  $N_{\varphi}$  will only have a small effect on  $H_{\text{up}}(R)$ . We have assumed  $N_{\varphi} > N_{\text{mod}}$  in the derivation. Therefore the logarithm in (6) is positive.

In order to compute a lower bound on  $H(R)$ , we take the correlations between the scattering channels as given by [10] into account. A similar computation as the one for the upper bound is then performed but the number of independent outgoing modes is reduced by the correlations. This results in the following lower bound [9],

$$H_{\text{low}}(R) \approx \frac{3\pi}{2} \frac{A\ell}{\lambda^2 d} \log_2 \left( \frac{\pi e}{2} \frac{N_{\varphi}}{N_{\text{mod}}} \right). \quad (7)$$

## The Security Parameter for Optical PUFs

We use the results of the previous section to estimate the security parameter. Substitution of (6) and (7) in (5) leads to the following bounds for  $C$  :

$$\min \left\{ \frac{2}{\pi} \cdot \frac{1}{\log_2 \left( \frac{\pi e}{2} \frac{N_{\varphi}}{N_{\text{mod}}} \right)} \cdot \frac{d}{\lambda}, N_{\text{mod}} \right\} \leq C \leq \min \left\{ \frac{2}{3\pi} \cdot \frac{1}{\log_2 \left( \frac{\pi e}{2} \frac{N_{\varphi}}{N_{\text{mod}}} \right)} \cdot \frac{d^2}{\lambda \ell}, N_{\text{mod}} \right\}. \quad (8)$$

The  $\min\{\dots, N_{\text{mod}}\}$  function reflects the fact that the number of independent challenges cannot exceed  $N_{\text{mod}}$ , the total number of input modes. The result (8) has the following properties:

- $C$  grows with increasing  $d/\lambda$ .

- In addition, the upper bound on  $C$  grows with increasing  $d/\ell$ . This is a measure for the number of scattering events  $N_{\text{sc}}$  taking place before a photon exits the PUF. (Assuming a random walk,  $d/\ell \propto \sqrt{N_{\text{sc}}}$ ).
- Note that (8) refers to one specific area  $A$  illuminated by the laser. By shifting the laser over a distance equal to the diameter of the laser spot, one illuminates a new sub-volume of the PUF with the same number of challenges. This means that the total number of independent challenges  $C_{\text{tot}}$  is given by  $C_{\text{tot}} = C \cdot A_{\text{PUF}}/A$ .

Using some typical example numbers ( $A = 1\text{mm}^2$ ,  $\lambda = 500\text{nm}$ ,  $d = 0.5\text{mm}$ ,  $\ell = 15\mu\text{m}$ ,  $N_{\varphi} = 2.5 \cdot 10^{12}$ ), Eq. (8) gives  $32 \leq C \leq 3.6 \cdot 10^2$  independent challenges per laser spot area of  $1\text{mm}^2$ .

Finally, we compare our result (8) to the estimates in [3, 5]. Their approach is based on the memory angle  $\delta\theta \propto \lambda/d$  [10] and does not take the density of scatterers into account. Dividing the half-sphere into pieces of solid angle  $\delta\theta^2$ , they obtain a number of CRPs proportional to  $d^2/\lambda^2$ , representing the number of obtainable responses that look mutually uncorrelated. This number is larger than our upper bound for  $C$  by a factor  $\propto \ell/\lambda$ . The two approaches give comparable results only in the limit of extremely strong scattering,  $\ell \approx \lambda$ .

## REFERENCES

- [1] B. Gassend et al., *Controlled Physical Random Functions*, Proc. 18th Annual Computer Security Applications Conf., Dec. 2002.
- [2] B. Gassend et al., *Silicon Physical Unknown Functions*, Proc. 9th ACM Conf. on Computer and Communications Security, Nov. 2002.
- [3] R. Pappu, *Physical One-Way Functions*, PhD thesis, MIT 2001.
- [4] C. Bennett, G. Brassard, S. Breidbart and S. Wiesner, *Unforgeable Sub-way Tokens*, CRYPTO 82.
- [5] R. Pappu et al., *Physical One-Way Functions*, Science Vol. 297, Sept 2002, p.2026.
- [6] B.L.P. Gassend, *Physical Random Functions*, Master's Thesis, MIT 2003.

- [7] M. Magnor, P. Dorn and W. Rudolph, *Simulation of confocal microscopy through scattering media with and without time gating*, J.Opt.Soc.Am. B, Vol. 19, no. 11 (2001), pp 1695–1700.
- [8] J. F. de Boer, *Optical Fluctuations on the Transmission and Reflection of Mesoscopic Systems*, Ph D thesis, 1995, Amsterdam.
- [9] P. Tuyls, B. Skoric, S. Stallinga, T. Akkermans, W. Ophey, *Information-Theoretic Security Analysis of Physical Uncloneable Functions*, preprint available at <http://users.skynet.be/pimtuyls/pimtuyls.htm>.
- [10] S. Feng, C. Kane, P.A. Lee and A.D. Stone, *Correlations and Fluctuations of Coherent Wave Transmission through Disordered Media*, Phys.Rev.Lett. Vol.61 No.7 (1988), pp 834–837.
- [11] D. Gabor, *Light and Information*, in E. Wolf, Ed., Progress in Optics Vol. I, North-Holland, Amsterdam 1961.
- [12] K. Petersen, *Ergodic Theory*, Cambridge University Press, 2000.