Revisiting Optical Physical Unclonable Functions

Ulrich Rührmair
Computer Science Dept.
TU München
80333 München, Germany
ruehrmair@in.tum.de

Christian Hilgers
Computer Science Dept.
TU München
80333 München, Germany
hilgers@muc.zae-bayern.de

Sebastian Urban
Computer Science Dept.
TU München
80333 München, Germany
surban84@gmail.com

Agnes Weiershäuser
Computer Science Dept.
TU München
80333 München
agnes.weiershaeuser@gmail.com

Elias Dinter
Computer Science Dept.
TU München
80333 München
elias@dinternetz.de

Brigitte Forster
FIM
Universität Passau
94032 Passau, Germany
brigitte.forster@uni-passau.de

Christian Jirauschek
Electrical Engineering Dept.
TU München
80333 München, Germany
jirauschek@mytum.de

ABSTRACT

We revisit optical physical unclonable functions (PUFs), which were introduced by Pappu et al. [36, 37] in their seminal and historically first publication on PUFs. We start our studies with non-integrated PUFs. We discuss their resilience against machine learning attacks, and systematically study the influence of using more than one laser beam, varied laser diameters, and smaller scatterer sizes. Finally, we discuss new image transformations that maximize the PUF's output entropy while possessing similar error correction capacities [37]. The results of our study allow to enhance the security of non-integrated PUFs without causing significant additional hardware costs. Next, we discuss the novel appliation of non-integrated optical PUFs as so-called *"Certifiable PUFs"*. The latter are useful to achieve practical security in certain PUF-protocols, as recently observed by Rührmair and van Dijk at Oakland 2013 [43]. Our technique is the first mechanism for Certifiable PUFs suggested in the literature, answering an open problem posed in [43]. Finally, we turn to constructions for *integrated* optical PUFs, and build the first prototype for this kind of PUF. We investigate its security, and show that these PUFs can be attacked successfully by machine learning techniques if the employed scattering structure is linear, and if the raw interference images of the PUF are available to the adversary. Our result enforces the use of non-linear scattering structures within integrated PUFs. The quest for suitable materials is identified as an important, but open research problem. The presented work makes intensive use of two prototypes of optical PUFs that were built for this work. Our integrated optical PUF prototype is, to our knowledge, the first of its kind in the literature.

Categories and Subject Descriptors

B.0 [**Hardware**]: General; C.3 [**Special Purpose and Application-Based Systems**]: Smartcards

1. INTRODUCTION

Mobile security devices have become ubiquituous in our life. This widespread use makes them an attractive and accessible target for adversaries. The majority of known attacks are thereby not directed against the employed cryptographic primitives themselves. Rather, they often attempt to obtain the employed secret keys by physical techniques or malware. Such key-extracting strategies are not just a theoretical concern, but have been demonstrated several times in widespread, commercial systems [27, 13, 1]. The fact that the security devices shall be inexpensive aggravates the problem, leaving only little room for elaborate key protection measures.

The described situation was one motivation that led to the development of *Physical Unclonable Functions (PUFs)*. A PUF is a (partly) disordered physical system that can be challenged with so-called external stimuli or challenges C_i, upon which it reacts with corresponding responses R_i. The tuples (C_i, R_i) are thereby often called the *challenge-response pairs (CRPs)* of the PUF. The responses R_i shall be a function of the applied challenge and the micro- or nanoscale structural disorder present in the PUF. It is assumed that this disorder cannot be cloned or reproduced exactly, not even by the PUF's original manufacturer. Due to its complex internal structure, it is usually harder to read out, predict, or derive the responses of a PUF than to obtain digital keys stored in standard non-volatile memory. This can make PUF-based systems more resilient against hardware and malware attacks than classical approaches.

PUFs can be used in various cryptographic and security applications. Examples include their employment as tamper sensitive secret key storage [53, 21, 18, 52], or their use as a complex identifier for a hardware system that embeds the PUF [36, 37, 17, 52]. Recent research has also discovered their application in more complex protocols such as oblivious transfer, bit commitment, key exchange, or multi-party computation [38, 2, 32]. The practical security of the latter protocols has been discussed intensively in an attempt to keep PUF theory and PUF applications closely together [41, 42, 43].

On the implementation side, most PUF research has focused on electrical realizations. This includes SRAM PUFs [21, 24] (and variants thereof like Butterfly PUFs [28] or Buskeeper PUFs [49]), as well as the Arbiter PUF [17, 52] (and its various modifications, such as XOR Arbiter PUFs [52, 46], Lightweight PUFs [33], Feed-Forward PUFs [18, 30]). Other examples include Ring-Oscillator PUFs [52], Crossbar PUFs [40, 44], analog PUFs based on cellular non-linear networks [8], or the Bistable Ring PUF [4, 5]. Several electrical PUFs have been attacked successfully via machine learning based modeling attacks, at least up to a substantial level of size and complexity [46, 48].

Optical PUFs.

Under their initial name *"Physical One-Way Functions (POWFs)"*, the optical systems proposed by Pappu et al. [36, 37] were among the first suggested PUFs. In their original, non-integrated form, they possess several advantages:

- Low costs per piece, since a non-integrated optical PUF merely consists of an inexpensive plastic platelet with randomly distributed light scatterers inside.
- No microelectronic or silicon circuitry on the PUF-carrying object is required.
- High output complexity (each PUF-response consists of thousands of bits), which results from the complex optical interference process inside the token.
- High security against modeling or machine learning attacks [46, 48]. No successful attacks on non-integrated optical PUFs have been reported until this date (see Section 3).
- Non-integrated optical PUFs can be used as "Certifiable PUFs", i.e., it can be proven within certain limits that they have not been modified or exchanged by malicious parties (see Section 6).

On the downside, non-integrated optical PUFs a la Pappu et al. require an optical precision mechanism for read-out [36, 37]. This mechanism must establish exactly the same relative positioning of the light scattering token, the laser beam, and the CCD camera upon every single read-out. It must function in exactly the same manner at different locations worldwide and even for different read-out apparatuses. Implementing such a mechanism is both expensive and error prone. These downsides seem hard to overcome: Pappu et al.'s construction cannot be integrated or miniaturized easily, as it requires a focused laser beam to be moved across the PUF.

Related Work and Our Contributions.

Despite the obvious advantages mentioned in the last section, surprisingly little activity has been devoted to develop the conept of optical PUFs further since the appearance of Pappu et al.'s [36, 37]. The only article known to us is by Tuyls and Skoric [54]: The authors briefly discuss in theory how Pappu's PUF could be miniaturized and integrated, but present no prototypes or security analyses. Comparatively more investigations on the use of optical scattering phenomena in security have been conducted in a related, but not identical area. In this strand, the complex intereference patterns emerging from laser-illuminted surfaces are used to directly authenticate objects, products, packages, documents, and digital content. For example, the scattering behavior of paper surfaces has been suggested to secure documents or valuable goods in the Nature magazine [3], the IEEE Security and Privacy Symposium [7], ACM CCS [50], and other venues [51]. Furthermore, at CHES 2009 [22] and FC 2009 [56], it has been described how the digital content stored on compact discs can be authenticated by exploiting the individual scattering behavior of each disc.

Within this research landscape, we make the following contributions. Firstly, we deal with the optimized implementation of optical PUFs. We describe how their output complexity and security can be enhanced by simple measures such as varying the laser diameter or choosing the right size of the light scattering elements. We suggest a very simple methodology by which these parameters can be optimized in any practical implementations, and apply it to our concrete set-up. Secondly, we observe that the Gabor image transform applied by Pappu et al. [36, 37] leads to strong regularities in the derived cryptographic keys. We discuss a number of alternative transformations, showing that they can enhance the estimated response entropy by a factor of up to three. Our new transformations can be used with great benefits in *any* security application that exploits optical scattering phenomena, including the abovementioned approaches [3, 7, 50, 51].

Thirdly, we suggest that non-integrated optical PUFs could be used as so-called "Certifiable PUFs". As described recently at Oakland 2013 [43], Certifiable PUF are useful, and in a certain sense even necessary to implement secure and practical PUF protocols for advanced cryptographic tasks like oblivious transfer. We describe a method for the offline certification of non-integrated optical PUFs at low costs; it is the first construction for Certifiable PUFs in the literature. Finally, we investigate the *integrated* implementation of optical PUFs. We build a first prototype from inexpensive components and evalute its security. One surprising result is that integrated optical PUFs can be machine learning successfully if linear optical scattering structures are used, and if the adversary can access the raw scattering images before they are postprocessed. This calls for non-linear scattering media, which should ideally exhibt their non-linearities at low light intensities. We identify the construction of non-linear optical PUFs that can be easily miniaturized and integrated into microelectronic systems as an open problem in this work.

In all our analyses, real experimental data from two prototypes is used: A non-integrated optical PUF a la Pappu et al. [37, 36], and an integrated optical PUF constructed from inexpensive consumer components. To our knowledge, this is the first time that an integrated optical PUF has been built and practically investigated.

Organization of this Paper.

We start by investigating non-integrated optical PUFs: Section 2 describes our experimental set-up for this PUF-type. Section 3 discusses their security against modeling attacks. Sections 4 and 5 optimize their output complexity by tuning the laser diameter, scatterer size, and the employed image transformations, respectively. Section 6 describes their use as Certifiable PUFs. Subsequently we turn to integrated optical PUFs: Section 7 details our experimental prototype of an integrated optical PUF. Section 8 reports modeling attacks on this PUF-type. We conclude the paper in Section 9.

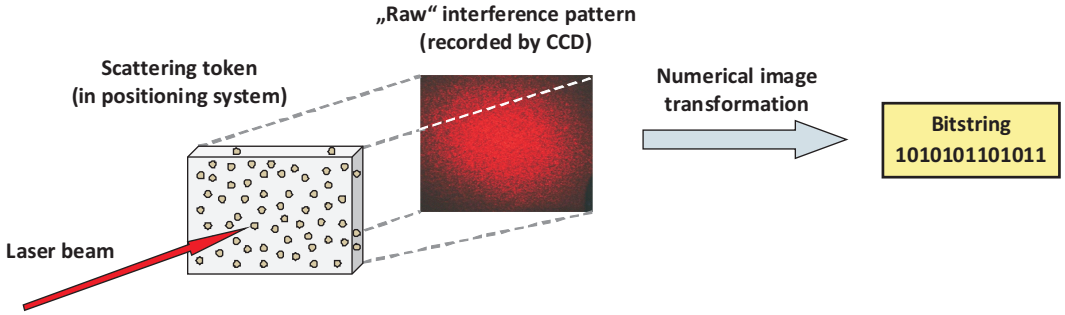

Figure 1: Schematic illustration of our implementation of a non-integrated PUF a la Pappu et al. [36, 37] (*"Pappu's PUF"*), and the necessary postprocessing for the derivation of the PUF response. As shown, we measure the speckle pattern in transmission, whereas Pappu et al. [36, 37] measure it in reflection.

2. EXPERIMENTAL SET-UP FOR PAPPU'S PUF

In the sequel, we will often refer to a non-integrated optical PUF with a linear scattering structure as described by Pappu et al. [36, 37] simply as *"Pappu's PUF"* for reasons of brevity. For our experiments, we employed a slightly modified version of Pappu et al.'s original set-up [36, 37]. Instead of measuring the reflected light as in [36], we detect the speckle pattern in transmission of the light through the optical PUF. The new set-up enabled simpler and more cost-effective realizations and thus seemed preferrable. Note that said modification does not affect the PUF's input-output complexity in any way. The schematics of our set-up are given in Figure 1. A challenge C_i to this PUF consists of a specific point and angle of incidence of the applied laser beam. The corresponding response R_i of the PUF is the result of an image transformation applied to the raw speckle pattern captured by the CCD camera. Pappu et al. apply the Gabor transformation to this end [36, 37], but several alternatives are possible (see Section 5).

As light source we used a red Lasiris SNF Laser with a wavelength of 635 nm and a power of less than 5 mW. The distance between the laser and the probe is about 980 mm. The integrated optic of the laser is adjustable, which enables the focussing of the laser beam. The optical interference pattern or "speckle pattern" of the transmitted laser light is captured with a MV-D1024E camera from Photonfocus. The distance between the PUF an the objective of camera is 26 mm. The integrated CMOS sensor of the camera prevents blooming effects, which often happens on CCD sensors. For our experiments we take 8 bit gray scale images with a resolution of 1024x1024 pixels. To apply different challenges to the PUF, analyze the robustness of the system and to allow a high number of CRPs, we used a positioning system for moving and rotating the scattering token. The positioning system is based on three stepper motors. We used two linear tables of type LM 45 for horizontal and vertical movements and also one MOGO 40 to adjust the angle of the scattering token. With this system we can move the optical PUF about 12 mm in vertical and horizontal direction. We can rotate the PUF, and thus change the angle of incidence of the laser beam, by about $\pm$ 15°.

The scattering tokens are prepared by distributing glass spheres of a certain size range randomly in a transparent matrix material. Different size ranges have been used in our various experiments (see Sections 4.2, 4.3 and 5). We used glass spheres from Mühlmeier (size ranges 400-600μm and 300-400μm) and Worf Glaskugeln (250-420μm, 105-210μm, 90-106μm, 40-80μm). From the tested matrix materials, the consumer glue UHU Plus Schnellfest was simple to handle, and led to better results than the more expensive optical adhesive NOA 61 from Norland. For the manual preparation of of the tokens, we used the following method: We applied the glue on a glass slide and scattered the glass spheres to a dense layer. After a short drying time, we apply the next layer of glue and glass spheres. Depending on the size of the spheres, we varied the number of layers between four and five.

3. SECURITY OF PAPPU'S PUF AGAINST MODELING ATTACKS

While successful modeling attacks have been reported on several electrical PUFs [46, 48], no such attacks have been published to this date on non-integrated optical PUFs. We re-investigated the hardness of this problem, collecting a substantial amount of CRPs from our set-up of the last section. We then considered in theory and/or practice the applicability of machine learning algorithms, including those techniques used in earlier attacks on electrical PUFs [46, 48]. All of our efforts remained unsuccessful, however. For example, the application of Support Vector Machines to predict single bits of the raw optical PUF output led to error rates around 50%, i.e., the prediction quality was essentially equal to random guessing [12].

From an abstract perspective, there are three main reasons for the high machine learning resilience of non-integrated optical PUFs. The first is their large information content. As argued in [37], every volume unit of size around the laser wavelength of around 600 nm in principle can have an influence on the scattering process. Given the size of our tokens, in theory up to 10^{11} volume units would have to be considered. Even though this figures represent the extreme, theoretical cases, also in practice the feature vectors of the machine learning (ML) problems associated with optical PUFs are simply too large to be handled well. In opposition, the ML problems for known electrical PUFs possess much smaller feature vectors: a 128-bit Arbiter PUF, for example, has an associated feature vector with only 129 entries [46, 48]. This can be handled quite easily by current techniques.

A second reason is the complex optical interference process inside optical PUFs. For all methods known to us, exact simulation is too laborious to be carried out in practice. Numerical approaches that strongly simplify the scattering regime are unsuited, too, since they (compare our discussion in . Note that strong simplifying assumptions cannot be made in these simulations, since the exact field distributions and resulting speckle patterns needs to be simulated. This prevents the application of ML techniques that require such simulation in the evaluation of the so-called *"fitness"* of a given feature vector. This includes evolution strategies and related meth-

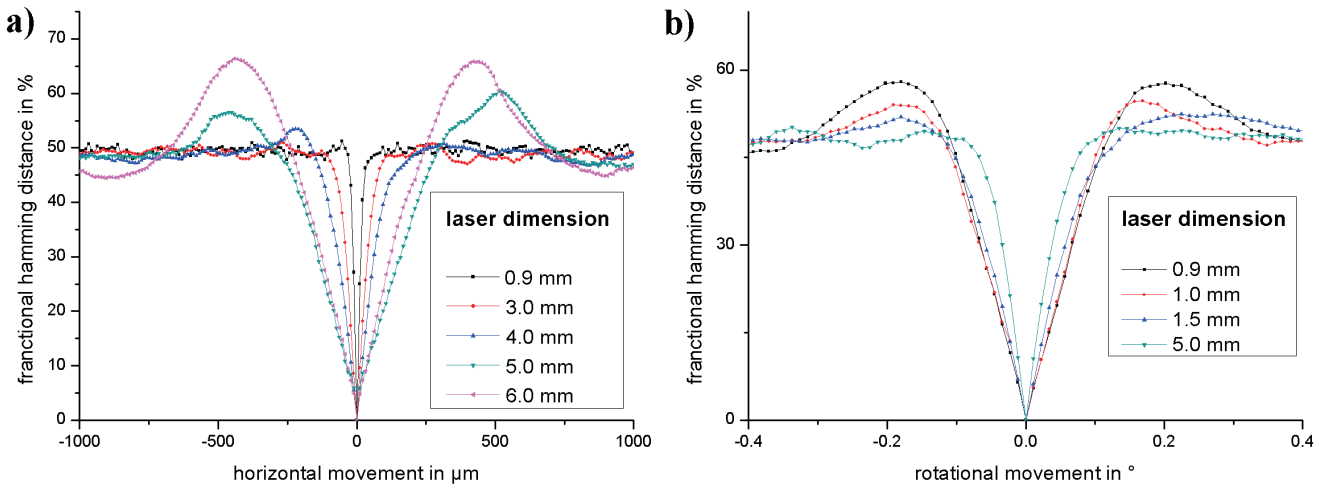

Figure 2: Decorrelation speed of the PUF output for horizontal and rotational shifts of the laser beam, as a function of different laser diameters. A fractional Hamming distance of 0.5 indicates full decorrelation between the two outputs. Smaller diameters lead to faster decorrelation for horizontal shifts, but slower decorrelation for changes in the laser angle.

ods, which had been applied successfully to electrical PUFs in the past [46, 48]. To the contrary, the internal mechanisms of current electrical PUFs can often be simulated by simplified models, such as the well-known linear additive delay model in the case of Arbiter PUFs [46, 48]. The decisive feature of optical systems here is that they have a very rich complexity while still being stable against ambient conditions and wear-and-tear. The massless photons facilitate a very complex scattering interaction, which is yet stable against varying ambient conditions, and does not alter or wear off the PUF internally. The same effect seems hard to obtain for electrical structures, since electrons do not exhibit an analog to the complex optical interference process of coherent photons at room temperature [10].

Finally, in theory each PUF-challenge should illuminate the entire scattering token. We observed that this is not the case in practice, however. The incident laser causes a light cone inside the token, meaning that for different PUF-challenges different and independent regions of the token are illuminated predominantly and cause the respective PUF-responses. This complicates or even directly prevents modeling attacks, too: Responses obtained from illuminating the upper left region of the token do not allow conclusions about the responses resulting from the lower right region, for example.

4. ENHANCING THE CHALLENGE SPACE OF PAPPU'S PUF

Pappu et al. report that their non-integrated optical PUF possesses around 2.37×10^{10} challenges for which the corresponding Gabor-tranformed responses are virtually independent and decorrelated. This comparatively low number makes an attempted complete read-out the currently most viable attack strategy on this PUF type. The relatively small challenge number is also particularly relevant in a number of recent quadratic attacks on PUF protocols published at CHES 2012 and elsewhere [41, 42]. In this section, we therefore systematically investigate methods to increase the number of decorrelated CRPs. The measures we discuss in Sections 4.2 and 4.3 are particularly inexpensive and simple to realize.

4.1 Influence of Multiple Laser Beams

One seemingly straightforward step to raise the size of the challenge space is to use several lasers beams with different frequencies, for example one red and one green laser. Due to the differing wavelengths, the interference pattern resulting from a green laser incident at point $\vec{p}$ and angle Θ *differs* from the pattern resulting from a red laser incident at exactly the same point and angle. It hence seems suggestive to use a red and a green laser, and to define one PUF challenge C_i to consist of the incidence points $\vec{p}$ and angles Θ of both lasers (i.e., $C_i := (\vec{p}_{\text{red}}, \Theta_{\text{red}}; \vec{p}_{\text{green}}, \Theta_{\text{green}})$). Such a measure promises to quadratically enhance the size of the challenge space.

There is a problem with this straightforward approach, however,as long as linear scattering structures are used. In this linear case, the pattern resulting from the challenge $C_i = (\vec{p_{\text{red}}}, \Theta_{\text{red}}; \vec{p}_{\text{green}}, \Theta_{\text{green}})$ is nothing else than the sum of the two patterns resulting from the challenges $C_i' = (\vec{p}_{\text{red}}, \Theta_{\text{red}})$ and $C_i'' = (\vec{p}_{\text{green}}, \Theta_{\text{green}})$. More precisely, the intensity in each CCD pixel for the challenge C_i is nothing else than the intensity resulting from challenge C_i' plus the intensity resulting from challenge C_i''. Besides the linearity of the scattering structure, a second reason for this simple behavior is that the red and green light are not coherent as long as two separate and standard lasers are used. No destructive interference can take place, and their resulting intensities simply add up linearly in the CCD image.

This allows a simplified adversarial full read-out of the new PUF with a red and green laser by the following method: The adversary first reads out all responses for challenges from the red laser alone, then all responses for challenges from the green laser alone. Subsequently he can derive the responses for all combined challenges $C_i = (\vec{p_{\text{red}}}, \Theta_{\text{red}}; \vec{p}_{\text{green}}, \Theta_{\text{green}})$ by adding the known response to the challenge $C_i' = (\vec{p_{\text{red}}}, \Theta_{\text{red}})$ to the known response to the challenge $C_i'' = (\vec{p}_{\text{green}}, \Theta_{\text{green}})$ in the above manner. Using two lasers hence effectively increases the challenge space only by a factor of about two. On the other hand, however, it results in a significantly increased set-up effort, as now two lasers need to be positioned independently from each other. In our and in Pappu et al.'s set-up, it is the lightweight scattering token that is moved, since the laser is much heavier and more laborious to position. With two lasers,

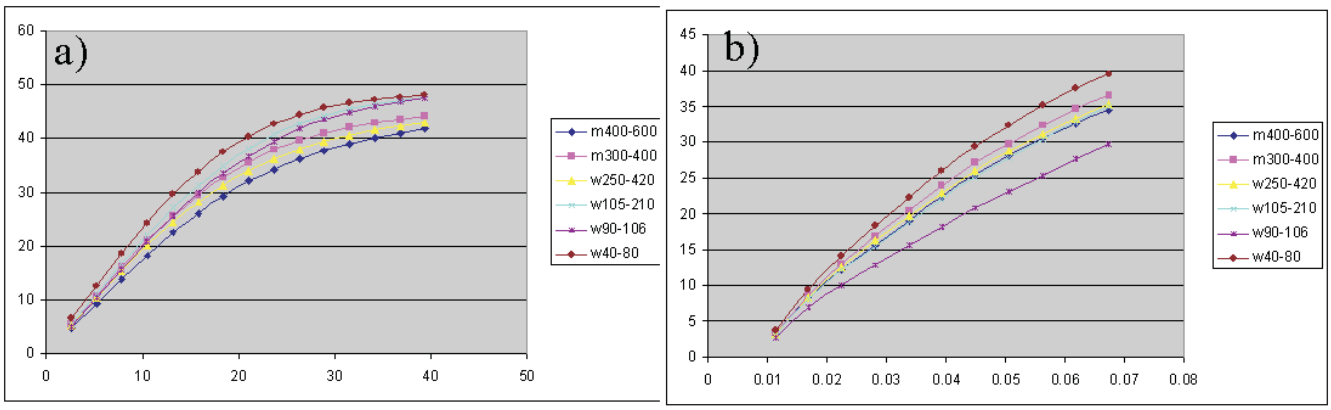

Figure 3: Decorrelation speed of the PUF output for variation of the incidence point and angle of the laser, and for different scatterer sizes. Scatterers in an overall range from 400μm to 40μm were examined. A fractional Hamming distance of 0.5 indicates full decorrelation between the two outputs. Smaller scatterers leed to faster decorrelation for both horizontal and vertical shifts.

this method is no longer applicable. Something similar holds for the case of k lasers.

In summary, using k independently positionable and spatially separated lasers (whose light is not coherent) together with a linear scattering medium will only increase the effective challenge space by at most a factor of k, while it drastically increases costs and experimental effort. It thus seems no ideal method to enhance the challenge space of a non-integrated linear optical PUF.

4.2 Influence of the Laser Diameter

We subsequently turned to the effect of the laser diameter on the effective size of their challenge space. We investigated the sensitivity of the PUF-output in dependence of the laser diameter to (i) variation of the point of incidence of the laser in the x-y-directions, and to (ii) alteration of its incidence angle. This sensitivity is a good measure for an optical PUF's security: It determines the number of virtually independent challenge-response pairs of the PUF, and thus its resilience against full read-out attacks. As modeling attacks and cloning currently are no viable strategies, the latter represents the most threatening attack method.

In our above set-up of Figure 1, the laser diameter can be adjusted by simply focusing the laser. The focal point lies beyond the entrance point of the PUF, and we measured the effective laser diameter at the entrance point. For the following experiments we used a PUF with 5 layers, 300-400μm glass spheres and UHU Plus Schnellfest. During the experiment, we move the PUF by the positioning system in equally spaced shifts and take pictures of the speckle patterns. The center position of the token was chosen as reference position. For all measured raw images, we then computed the Gabor transformed images as in [36, 37]. We determined their fractional Hamming distances [1] to the Gabor image of the reference position. A fractional Hamming distance of 0.5 signals a virtual decorrelation between the Gabor images.

Figures 2a and b depict our findings. For each of the diagrams' curves, the critical parameter is how quickly the new response decorrelates from the old one, i.e., how quickly the curve reaches the 0.5-level of the fractional Hamming distance. The faster this occurs, the more virtually independent and decorrelated challenge-response pairs of the PUF exist. The presented data illustrates that smaller diameters lead to faster decorrelation for horizontal (and also vertical) movements, but slower decorrelation in the rotational movement. This makes the choice of the optimal laser diameter an optimization problem. In practice, its solution depends on the experimental set-up and the used materials in the scattering token. It must thus be solved in each application of optical PUFs empirically by the above method to achieve optimal security. In our case, laser diameters between 1.5 mm and 2.5 mm appear optimal. Note in this context that an extreme, too small laser diameter will naturally lead to unsuited scattering images. In our case this effect could be neglected, however, since the optimal diameter was lower-bounded more closely by the negative effect of small diameters on the decorrelation for rotational movements (see Figure 2 b).

[1]The *fractional Hamming distance* of two bitstrings of the same length l is the number of all bits on which the two strings differ divided by the length l of the string(s).

4.3 Influence of the Scatterer Size

We also systematically investigated the influence of the scatterer size on the security of optical PUFs. From theoretical considerations, the optimal output complexity can be expected for a scatterer size which is similar to the wavelength of the used laser light. In this case, which is also referred to as Mie-regime [31, 10, 25], the interference pattern critically depends on the particle size. The resulting electromagnetic field distribution within the PUF can only be adequately described by exactly solving the Maxwell equations, which is numerically very demanding. The corresponding analytical solution for scattering at a spherical object is commonly referred to as Mie solution [31]. Obviously the output complexity can be further increased in this case by using spherical objects with rough surfacesor, more generally, irregularly shaped particles.

For particle sizes *significantly larger* than the optical wavelength, simplified methods such as ray tracing approaches become valid [19], which avoid the numerical complexity involved in solving the full Maxwell equations. If the propagating light undergoes many scattering events, the propagation becomes diffusion-like, i.e., the photons essentially undergo a random walk. Such a scenario can then be described by a diffusion equation approach, which has a significantly reduced complexity, since the properties of the medium are expressed by a macroscopic diffusion coefficient.

On the other hand, for particles or refractive index inhomogeneities on a length scale *much smaller* than the wavelength, the scattered light field can be described by an approximation to the Mie solution, the much simpler Rayleigh scattering solution [25]. In the extreme case of a large ensemble of far sub-wavelength objects,

the single, sub-wavelength scatterers cannot be optically resolved at all. Then the medium is suitably described by a volume-averaged effective refractive index, thus exhibiting again a low optical complexity.

The above discussion suggests that for our red laser of wavelength 632nm, particles of approximately the same sizes should be used to achieve maximally complex scattering effects. Note that this is about a factor of 1,000 smaller than the sizes used by Pappu et al. in their original experiments [36, 37]. The experimental exploration of this regime requires nanofabrication techniques, however, which we did not have available at the time of writing. Still, in order to give at least a qualitive proof that the behavior of optical PUFs becomes more complex for smaller scatterers, we carried out experiments for scatterers in the size ranges 400-600μ, 300-400μm, 250-420μm, 105-210μm, 90-106μm, and 40-80μm (compare Section 2). They proved in practive that the complexity grows for smaller scatterer sizes. The particles we used are still up to a factor of ten smaller than the scatterers employed by Pappu et al. [36, 37].

In order to quantitatively evaluate the resulting complexity of the optical PUF, we again measured how quickly the transformed images decorrelate. Our findings are depicted in Figure 3. They prove that the complexity and the number of virtually decorrelated CRPs increases steadily for smaller scatterer sizes in the length regimes examined by us, as predicted by our theoretical considerations above. In practical applications of optical PUFs, the scatterer sizes should therefore be chosen as small as possible under the given fabrication and cost constraints.

5. ENHANCING THE BIT ENTROPY OF PAPPU'S PUF

As already discussed by Pappu et al. [36, 37], the "raw" optical interference images (as recorded by a CCD camera) should not be used directly as output of an optical PUF without postprocessing. First, they are too large, making PUF protocols inefficient. Secondly, they show much regularity due to their homogeneous dark and bright sub-regions; if used directly as cryptographic keys, the keys have non-optimal bit entropy. Finally, the raw images fluctuate, for example due to small laser instabilities or air movements across the laser beam, including dust particles. Therefore a numeric transformation is usually applied to distill shorter, more stable, and more entropic bitstrings.

Pappu et al. [36, 37] utilize the well-established Gabor transformation to this end. The Gabor transform is a linear invertible transform which decomposes an image into components with respect to size and direction of the image features [34, 6, 15]. They propose that the two-dimensional Gabor-transformed images (after a threshold step for conversion into binary data) can subsequently be converted into a cryptographic key by simply reading them out line by line. There are, however, two downsides of this approach. First of all, the Gabor transformed images have very strong, zebra-stripe like regularities (see Figure 4). These regularities cause strong patterns in the cryptographic keys, i.e., regularly alternating, medium-length sequences of consecutive ones and zeros. Secondly, due to the fact that the Gabor images do not contain maximal entropy (since they exhibit said regularly striped patterns) they do not reflect the small-scale physical randomness of the optical PUF in an optimal way. This makes it in principle easier to build PUFs with the same challenge-response behavior, i.e., to clone the PUF. In order to achieve a maximal security level, these patterns should hence be avoided.

We therefore investigated various other image transformations. From theoretical considerations [9], so-called wavelet transformations seemed good candidates, since they induce less structure in the transformed image. We empirically tested a considerable number of transformations from this family for their practical performance on optical PUFs, including Daubechies wavelets [9], symlets [9], polyharmonic isotropic B-spline Wavelets [55] and quincunx wavelets based on on the McLellan transformation [14]. They all exhibit slightly worse robustness than the Gabor-transformation, however. We thus also designed a transformation in-house, which has almost the same stability as the Gabor transformation, but still causes less regularities in the transformed images (see [23] for details). Figure 4 qualitatively illustrates the difference in entropy, which is visible to the sheer eye. A more quantitative analysis will be contained in the full version of this paper.

6. PAPPU'S PUF AS CERTIFIABLE PUF

In a recent paper at Oakland 2013 [43], two new, practically relevant attack models on Strong PUF protocols have been discussed. In one of them, the so-called *"bad PUF model"*, malicious parties may replace PUFs by other, malicious hardware which looks like a PUF from the outside, but possesses hidden extra properties that allow cheating. This approach represents a practically viable attack strategy on certain advanced PUF protocols, such as oblivious transfer, bit commitment and key exchange schemes. Other, more basic PUF uses like tamper-sensitive key storage or simple identification protocols are less affected. The attack method is most relevant for integrated electrical Strong PUFs, since they communicate with external parties merely via a digital challenge-response interface; what is behind the interface remains hard to detect or verify. One example of bad PUFs are simulatable PUFs: These are hardware systems which look like a PUF from the outside, having a digital challenge-response interface etc. However, they possess a simulation code by which the manufacturer (or other malicious parties) can simulate the PUF-responses to arbitrary challenges without being in physical possession of the PUF. One example of a simulatable bad PUF are hardware systems with a pseudo-random number generator (PRNG) inside, whose secret seed is known to the manufacturer/the malicious party. This allows numerical simulation of all responses, while the hardware looks like a standard (Strong) PUF from the outside. The tacit use of such simulatable bad PUFs by a malicious party can spoil the security of several PUF protocols, for example schemes for oblivious transfer, as detailed in [43].

As a countermeasure, the authors of [43] propose the design and use of "Certifiable PUFs": These are PUFs for which it can be verified that they do possess (at least some of) the expected properties, and that they have not been manipulated or altered after their production. Currently, no strategies to "certify" PUFs in the above sense have been proposed in the literature.

Electrical integrated PUFs seem very hard to certify in said manner, since they can only be accessed via a digital challenge-response interface. What lies behind this interface remains difficult to control for users. Non-integrated optical PUFs show better potential here, since their very complex analog responses are hard to imitate for malicious PUFs, and are measured directly, i.e. not through a digital interface. We pick up this line of thought and present below a scheme for the offline certification of non-integrated optical PUFs. It uses the oblivious transfer protocol of Rührmair and van Dijk [42] as basis, employing interactive hashing as a substep (see [42] for details).

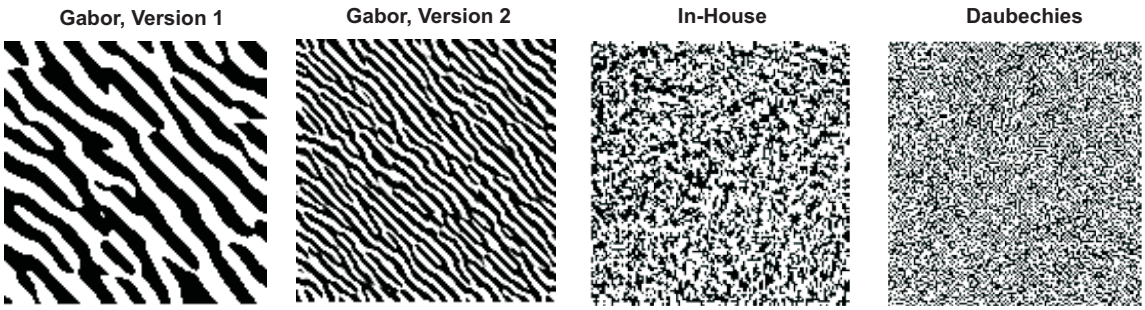

Figure 4: Images obtained from different image transformation techniques. The two leftmost images are obtained from the Gabor transformation for different parameters, and show strong regularities (zebra stripes). The other techniques applied by us – the Daubechies transformation and a transformation designed in-house – result in images with less regularity.

Protocol 1: SECURE OBLIVIOUS TRANSFER BASED ON CERTIFIABLE OPTICAL PUFS

Set-Up Assumptions:

- The used optical PUF is fabricated by a manufacturer who is trusted by both the OT-sender and the OT-receiver.
- The manufacturer uses a digital signature scheme $\mathsf{DS}_{\mathsf{Man}}$ with signing key SK and corresponding verification key VK.
- VK is known to both the OT-sender and the OT-receiver.

Pre-Protocol Steps:

- The manufacturer fabricates the optical PUF. He applies k randomly chosen challenges $C_1, \ldots, C_k$ to the PUF, for k being a small, one-digit security parameter. He obtains the responses $R_1, \ldots, R_k$.
- He generates the signature $\mathsf{Sig} := \mathsf{DS}_{\mathsf{Man}}(C_1, \ldots, C_k, R_1, \ldots, R_k)$, and defines the certificate as
$$\mathsf{Cert} := (C_1, \ldots, C_k, R_1, \ldots, R_k, \mathsf{Sig}) .$$
- The PUF is distributed together with its certificate to the OT-receiver. In practice, the certificate can be stored inexpensively via a barcode, for example, which is printed on the item in which the optical PUF is embedded.

Protocol:

Let the sender's input be two strings $s_0, s_1 \in \{0,1\}^\lambda$ and the receiver's input be a bit $b \in \{0,1\}$. The protocol then proceeds as follows:

1. The receiver verifies the certificate of the PUF. To that end, he applies the challenges $C_1, \ldots, C_k$ to the PUF, and verifies that the obtained responses are equal to $R_1, \ldots, R_k$.
2. The receiver chooses a challenge $c \in \{0,1\}^\lambda$ uniformly at random. He applies c to the PUF, obtaining the response r. He transfers the PUF together with the certificate to the sender.
3. The sender verifies the certificate of the PUF in the same manner as above.
4. The sender and receiver execute an IH protocol, where the receiver has input c. Both get outputs c_0, c_1. Let i be the value where $c_i = c$.
5. The receiver sends $b' := b \oplus i$ to the sender.
6. The sender applies the challenges c_0 and c_1 to the PUF. Denote the corresponding responses as r_0 and r_1.
7. The sender sends $S_0 := s_0 \oplus r_{b'}$ and $S_1 := s_1 \oplus r_{1-b'}$ to receiver.
8. The receiver recovers the string s_b that depends on his choice bit b as $S_b \oplus r = s_b \oplus r_{b \oplus b'} \oplus r = s_b \oplus r_i \oplus r = s_b$.

The above certification step only works due to the special features of Pappu's optical PUF: The raw, two-dimensional interference images it creates are too complex to be imitated by a malicious, bad PUF. Therefore a verification of a very small number of sample CRPs suffices to exclude that the PUF has been altered or exchanged against another PUF. The verification can be executed offline, i.e., without additional communication with the manufacturer. This is important: If an online communication with a trusted authority would be a regular step in the protocol, then the OT could be executed much simpler via this trusted authority itself.

It is interesting to consider the above protocol under the aspect of the involved computational or other assumptions. The protocol requires two assumptions: (i) an unpredictable PUF (see [39, 2] for formal definitions of the latter); (ii) a secure digital signature scheme $\mathsf{DS}_{\mathsf{Man}}$. It uses these two assumptions to implement OT. It is long known that secure digital signature schemes exist if and only if one-way functions exist [20], but currently no construction is known that implements OT merely from one-way functions. The use of PUFs hence is necessary and creates additional value in the protocol.

The technique of digitally signing a certifying, unique reflective speckle pattern seems also promising in connection with future architectures of electrical erasable PUFs [43]. The speckle pattern could be recorded directly from the surface of the electrical PUF, or an optical encapsulation could be used that enables certification of the electrical, erasable PUF inside. This eventually seems a promising technique to finally realize PUFs that are both erasable and certifiable, as suggested in [43].

Example Implementation.

We carried out an example implementation of certifiable optical PUFs by use of 2D barcodes. We chose the libdmtx library [29] for the implementation of the widely used Data Matrix Code. In order to save area requirements for the barcode, our implementation is based on the bilinear pairing based scheme by Zhang, Safavi-Naini und Susilo (ZSS) [57]. For the implementation we chose the PBC

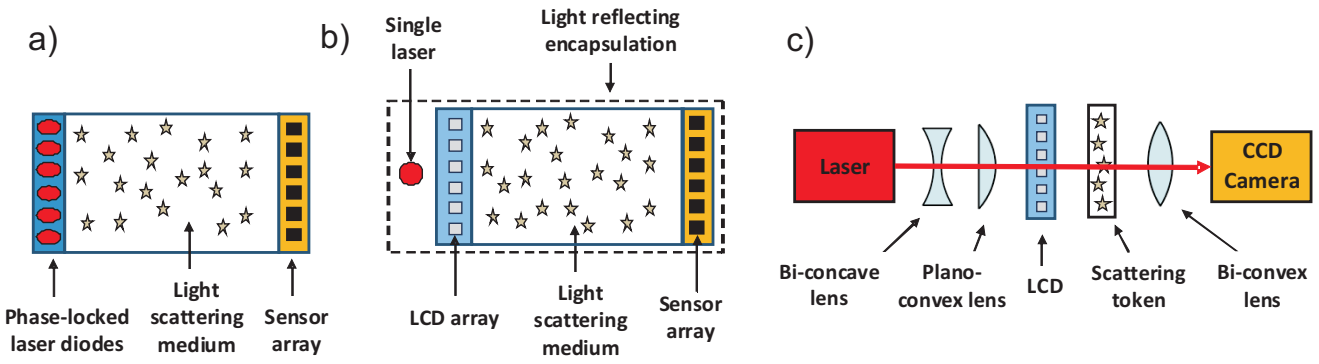

Figure 5: a) and b): Two possible theoretical types of integrated optical PUFs (compare [54, 16]). c): Schematic illustration of our prototype (not true to scale).

library [35] with the elliptic curve type F and a signature of 200 bits.

We assumed that the following information must be stored on the product: Manufacturer ID (16 bit), PUF ID (48 bit), Signature (200 bits), and image transformed speckle pattern. With a barcode module width of 0.25 mm this leads to a barcode of size on the order of 1 cm^2. An exemplary barcode generated by the above scheme is shown in Figure 6.

Figure 6: 2D Data Matrix barcode, which was generated by the above method.

7. INTEGRATED OPTICAL PUFS

One central practical research goal is to embed optical PUFs into microelectronic systems, i.e., to design secure integrated optical PUFs. Pappu's PUF is not very well suited for this purpose, since it requires movable components that must be positioned with high accuracy. Are there other constructions?

General Architecture of Integrated Optical PUFs.

Figures 5a and 5b describe two possible approaches. The goal of the constructions is to design optical PUFs without moving parts, which still allow a large number of different challenges and facilitate a complex interference process. Figure 5a shows an immobile laser diode array with k phase-locked diodes $D_1, \ldots, D_k$ [58], which is used to excite a disordered, random scattering medium. The diodes can be switched on and off independently, leading to 2^k challenges C_i. These can be written as $C_i = (b_1, \ldots, b_k)$, where each $b_i \in \{0, 1\}$ indicates whether diode D_i is switched on or off. At the right hand side of the system, an array of l light sensors $S_1, \ldots, S_l$, e.g. photodiodes, measures the resulting light intensities locally. A response R_i consist of the intensities $I_1, \ldots, I_l$ in the l sensors.

As depicted in Figure 5b, instead of phase-locked diode arrays, also a single laser source with a subsequently placed, inexpensive light modulator (LCD array) can be employed. Comparable suggestions have been made in [16, 54]. The k pixels of the LCD can be switched on and off independently, again leading to 2^k possible challenges. The whole system can be encapsulated by a reflective layer to facilitate the internal interference process. Both systems easily lend themselves to miniaturization.

In order to allow optical interference and to generate complex behavior also with linear scattering media, *all* laser light inside the scattering structure must be coherent. This necessitates the use of a phase-locked diode array (as in Figure 5a) or the employment of only one single laser source plus a subsequent light modulator/LCD (as in Figure 5b).

Our Prototype.

We built the first prototype of an integratable optical PUF from commercial components, including an LCD array from a customary beamer. The aim was not yet miniaturization, but a first proof of concept and a subsequent security analysis. Our set-up is illustrated schematically in Figure 5c. Instead of employing a mirrored encapsulation as in Figure 5b, which is mainly useful for miniaturized systems, we simply broadened the laser beam with suited optical lenses to ensure that a large area of the scattering token was illuminated.

In order to obtain a detectable influence of each single challenge bit on the optical response, we divided the LCD array symmetrically into 15×15 or 225 subareas. The k-th subarea was associated with the k-th bit of the PUF-challenge. This bit determined whether either *all* pixels of the whole k-th subarea were switched on, or whether all were switched off. This methods leads to PUF-challenges C_i of length 225 bits and a challenges space of 2^{225}. The responses were recorded by a standard CCD camera with grey scale images. As scattering objects, we used the same structures as in Section 2.

8. SECURITY OF INTEGRATED OPTICAL PUFS AGAINST MODELING ATTACKS

After our prototype was functional, we investigated the security of integrated optical PUFs. Let us start by a theoretical analysis of the situation. Under the provision that a *linear* scattering medium is used in the integrated optical PUFs of Figure 5a, the following theoretical analysis holds. Every diode D_i of the LCD-Array with $b_i = 1$ creates a lightwave, which is scattered in the medium and arrives at the sensor S_j with amplitude E_{ij} and phase shift θ_{ij}. The

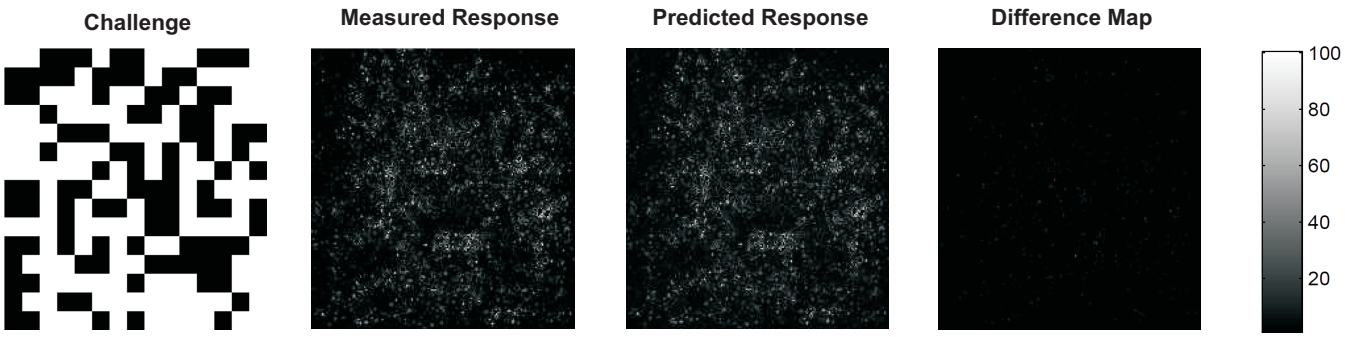

Figure 7: A randomly chosen 15 $\times$ 15 excitation pattern or challenge to the PUF; a CCD image of the response of the optical integrated PUF; the numerically predicted response; and the difference map between the latter two.

intensity I_j at the sensor S_j is then given by [10]

$$I_j = \left|E_j\right|^2 = \left|\sum_i b_i \, E_{ij} \, \cos\, \theta_{ij}\right|^2. \qquad (1)$$

For the linear scattering media, the amplitude E_{ij} and phase shift θ_{ij} are independent of whether the other diodes are switched on or off. One can hence collect many CRPs

$$(C_m, R_{C_m}) = ((b_1, \ldots, b_k), (I_1, \ldots, I_l)),$$

and derive the values E_{ij} and θ_{ij} from knowledge of these many (C_m, R_{C_m}). One suited approach are machine learning techniques, for example a standard machine learning regression. Once the parameters E_{ij} and θ_{ij} are known, the simulation of a response $R_{C_m} = (I_1, \ldots, I_l)$ to a given challenge $C_m = (b_1, \ldots, b_k)$ can be executed by simple calculation following Eqn. 1.

Analog analyses hold for the integrated PUF types shown in Figures 5b and c. In these two cases, the pixels in the LCD array themselves can be modeled as lightsources, i.e., they play analog roles as the diodes D_i in the above analysis.

In order to validate the above theoretical analysis, we applied it in practice to data that was collected from our prototype of Figure 5c. Each of the 225 LCD subareas was modeled as a single lightsource, analog to each single diode D_i of the above analysis. Standard machine learning regression was applied to 53,700 different CRPs collected from our prototype. The success is shown in Figure 7. The difference map between the actually acquired optical image and the prediction shows that only extremely small deviations that lie on the order of the usual fluctuations and measurement errors (compare [37, 36]). We stress again that our above attack assumes that linear scattering structures are used, and that the attacker has access to the raw speckle images that are produced by the set-up. The latter occurs if the attacked can invasively probe the PUF, if the postprocessing is carried out outside the optical PUF, or if the raw speckle images (or other unprocessed sensor data) are directly used as PUF-output. Note that the latter two cases are a realistic scenario for stable, integrated optical PUFs.

Our results show that non-linear optical materials must be used in integrated optical PUFs to achieve maximal practical security. For allowing easy integration in low-cost microelectronic systems, materials that exhibit optical non-linearities already at low light intensities are required. The identification of such substances and the construction of a secure integrated optical PUF constitutes an important open problem, which we pose to the community in this work. Linear integrated optical PUFs seem only secure as long as they are used within a secure perimeter and with additional postprocessing to the PUF responses (compare [16]).

9. SUMMARY

We revisited integrated and non-integrated optical PUFs, their optimal implementation, and their security in this paper, drawing on a large basis of experimental data that we obtained from two prototypical implementations. We started with non-integrated optical PUFs a la Pappu et al. [36, 37], which were often simply called *Pappu's PUF* in this publication. Using data from our prototype, we investigated the security of these PUFs, finding no vulnerabilities at all, apart from the perhaps comparatively low number of independent challenges. We then investigated simple and inexpensive measures by which the security of these PUFs can be enhanced, including optimizing the laser diameter and scatterer sizes, as well as the employment of new image transformations. These steps achieve a comparable effect than using multiple laser beams, but are much cheaper and simpler to realize. The methodology we employed in the respective sections can be applied to any practical or commercial optical PUF systems in order to optimize their security with inexpensive means. The new image transformations will be useful in other security applications of optical systems, too, such as in the use of reflective images obtained from randomly structured paper surfaces [3, 7, 50].

We then revealed an entirely new application of Pappu's PUF as so-called *"certifiable PUF"*. A few digitally signed responses (i.e., speckle patterns) of Pappu's PUF can serve as a fingerprint that certifies its input-output complexity and non-simulatability. Assuming trust in the manufacturer who issues the signature, and assuming the possession of the public verification key of the used signature scheme, this allows the offline certification of non-integrated optical PUFs for any involved parties. It enables the secure one-time use of Pappu's PUF in advanced protocols such as oblivious transfer or bit commitment. Pappu's PUF is uniquely qualified for this approach: The resulting speckle patterns are too complicated to imitate for a fraudster even if they are known to him, in opposition to the single-bit digital outputs of integrated electrical PUFs. Furthermore, the responses are measured directly from the non-integrated PUF, and are not communicated via a (potentially malicious) digital interface. Our construction of certifiable PUFs on the basis of Pappu's optical PUF addresses an open question posed at Oakland 2013 [43].

We then turned to integrated optical PUFs, and presented the – to our knowledge – first prototype of an integratable PUF in the literature. Our prototype was not yet embedded into a microelectronic system, since this was not the goal of this paper, but easily lends itself to miniaturization. We used our set-up to examine the security of this PUF type, and found that it can be successfully machine learned under two premises: (i) A linear scattering structure

is used. (ii) The adversary has direct access to the resulting raw speckle images. We gave a theoretical analysis for this case, and proved its validity in experiment by predicting entire raw speckle images with extremely high accuracy. Our findings enforce the use of non-linear scattering materials in this PUF type.

Overall, our investigations showed that there are some good reasons to put optical PUFs back on the agenda of the research community. The security and input/output complexity of their non-integrated version is unmatched by any currently known electrical architectures; they are the first PUFs for which certification or "attestation" is possible; and they allow highly interesting research in the intersection of security, embedded systems, optics, and nanotechnology.

Future Work.

Let us conclude by summarizing future research opportunities. One of the most pressing open questions of the area is how optical PUFs can be made non-linear in practice. Suited scattering materials have to be found that are inexpensive, simple to handle, stable, and non-toxic, and which exhibit strong non-linearities over a broad range of comparatively low light intensities. Once identified, they would have a manifold impact on optical PUF design: First, they could be used in Pappu's PUF in connection with k laser beams to enhance the challenge space to the power of k (while linear scattering materials only multiply the number of challenges by k, as described in Section 4.1). Furthermore, they would make integrated optical PUFs secure against the modeling attacks we presented in Section 8. Finally, they allow complex integrated PUF behavior even when they are illuminated with *non-coherent* light from different sources. This greatly simplifies integrated optical PUF design: A simple, standard diode array would then suffice. No phase-locked diodes as shown in Figure 5a would be required, which are expensive and much more complicated to handle.

A second intriguing research topic is the use of certifiable PUFs in other protocols, together with a formalization of this concept and formal security proofs. Thirdly, the ideal composition of materials and scatterer sizes, which leads to maximal input-output complexity, is an interesting research theme, both in experiment and optical simulations. Since the optimal size ranges seem to lie on the order of a few hundred nanometers (compare Section 4.3), its investigation requires nanofabrication facilities, which we did not have available at the time of writing. A final area of interest is the miniaturization of integrated optical PUFs, together with their embedding in microelectronic systems. Such a step would facilitate the widespread use of these integrated PUFs on a consumer scale, and constitutes a suggestive next research step.

Appendix

We thank Jonathan Finley, Jan Sölter and Christian Osendorfer for useful discussions, and Jonathan Finley for providing us with some of the optical equipment necessary for our experiments.

10. REFERENCES

[1] R. J. Anderson: *Security Engineering: A guide to building dependable distributed systems*. Wiley, 2010.

[2] C. Brzuska, M. Fischlin, H. Schröder, S. Katzenbeisser: *Physical Unclonable Functions in the Universal Composition Framework.* CRYPTO 2011.

[3] J. Buchanan, R. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. Allwood, and M. Bryan: *Forgery: Fingerprinting documents and packaging.* Nature, vol. 436, no. 7050, p. 475, 2005.

[4] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, U. Rührmair: *The Bistable Ring PUF: A New Architecture for Strong Physical Unclonable Functions*. HOST 2011.

[5] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, U. Rührmair: *Characterization of the Bistable Ring PUF*. DATE 2012.

[6] C. Christensen: *Frames and Bases*. Birkäuser, Boston, 2008.

[7] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. Halderman, E. Felten: *Fingerprinting blank paper using commodity scanners.* IEEE Symposium on Security and Privacy (Oakland'09), pp. 301-314, 2009.

[8] G. Csaba, X. Ju, Z. Ma, Q. Chen, W. Porod, J. Schmidhuber, U. Schlichtmann, P. Lugli, U. Rührmair: *Application of Mismatched Cellular Nonlinear Networks for Physical Cryptography*. IEEE CNNA - 12th International Workshop on Cellular Nonlinear Networks and their Applications, 2010.

[9] I. Daubechies: *Ten lectures on wavelets*. Society for industrial and applied mathematics (SIAM), 1992.

[10] W. Demtröder: *Experimentalphysik 2: Elektrizität und Optik*. Springer 2004. ISBN- 10: 3540202102.

[11] M. van Dijk, U. Rührmair: *Physical Unclonable Functions in Cryptographic Protocols: Security Proofs and Impossibility Results.* Cryptology ePrint Archive, Report 228/2012, 2012.

[12] E. Dinter: *Physikalische Einwegfunktionen.* Diplomarbeit, Technische Universität München, 2009.

[13] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, M. T. Manzuri Shalmani: *On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoqCode Hopping Scheme*. CRYPTO 2008, pp. 203-220, 2008.

[14] M. Feilner, D. Van De Ville, and M. Unser: *An orthogonal family of quincunx wavelets with continuously adjustable order*. IEEE Trans. on Image Processing, 14(4):499-510, 2005.

[15] B. Forster, P. Massopust (Eds.): *Four Short Courses in Harmonic Analysis. Wavelets, Frames, Time Frequency Methods, and Applications to Signal and Image Analysis*. Birkhäuser, 2009.

[16] B. Gassend, *Physical Random Functions*, MSc Thesis, MIT, 2003.

[17] B. Gassend, D. E. Clarke, M. van Dijk, S. Devadas: *Silicon physical random functions*. ACM Conference on Computer and Communications Security 2002, pp. 148-160, 2002

[18] B. Gassend, D. Lim, D. Clarke, M. van Dijk, S. Devadas: *Identification and authentication of integrated circuits.* Concurrency and Computation: Practice & Experience, Vol. 16(11), pp. 1077 - 1098, 2004.

[19] A. S. Glassner: *An introduction to ray tracing*. Morgan Kaufmann Pub., 1989.

[20] O. Goldreich: *The Foundations of Cryptography – Volume 2*. ISBN 0-521-83084-2, Cambridge University Press, 2004.

[21] J. Guajardo, S. S. Kumar, G. J. Schrijen, P. Tuyls: *FPGA Intrinsic PUFs and Their Use for IP Protection*. CHES 2007: 63-80

[22] G. Hammouri, A. Dana, B. Sunar: *CDs have fingerprints too.* CHES 2009, pp. 348-362, 2009.

[23] C. Hilgers: *Praktische Realisierung von Verfahren aus der Physikalischen Kryptographie*. Master Thesis, Technische Universität München, 2009.

[24] D. E. Holcomb, W. P. Burleson, K. Fu: *Power-Up SRAM State as an Identifying Fingerprint and Source of True*

Random Numbers. IEEE Trans. Computers 58(9): 1198-1210, 2009.

[25] A. Ishimaru: *Wave propagation and scattering in random media*. Vol. 1 & 2. New York: Academic press, 1978.

[26] C. Jaeger, M. Algasiner, U. Rührmair, G. Csaba, M. Stutzmann: *Random pn-junctions for physical cryptography*. Applied Physics Letter 96, 172103, 2010.

[27] T. Kasper, M. Silbermann, C. Paar: *All You Can Eat or Breaking a Real-World Contactless Payment System*. Financial Cryptography 2010, pp. 343-350, 2010.

[28] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, P. Tuyls: *The Butterfly PUF: Protecting IP on every FPGA.* HOST 2008: 67-70

[29] The libdmtx library. See http://www.libdmtx.org/

[30] 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 with identification and authentication applications.* In Proceedings of the IEEE VLSI Circuits Symposium, June 2004.

[31] G. Mie: *Beiträge zur Optik trüber Medien, speziell kolloidaler Metallösungen.*, Annalen der Physik 330(3), pp. 377-445, 1908.

[32] R. Ostrovsky, A. Scafuro, I. Visconti, A. Wadia: *Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions*. IACR Cryptology ePrint Archive 2012:143, 2012.

[33] M. Majzoobi, F. Koushanfar, M. Potkonjak: *Lightweight Secure PUFs.* IC-CAD 2008: 607-673.

[34] S. Mallat: *A wavelet tour of signal processing*. Academic Press, San Diego, 1997.

[35] The pairing based cryptography library (PBC). See http://crypto.stanford.edu/pbc/

[36] R. Pappu: *Physical One-Way Functions*. PhD Thesis, Massachusetts Institute of Technology, 2001.

[37] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld: *Physical One-Way Functions*, Science, vol. 297, pp. 2026-2030, 20 September 2002.

[38] U. Rührmair: *Oblivious Transfer based on Physical Unclonable Functions (Extended Abstract)*. TRUST Workshop on Secure Hardware, Berlin (Germany), June 22, 2010. Lecture Notes in Computer Science, Volume 6101, pp. 430 - 440. Springer, 2010.

[39] U. Rührmair, H. Busch, S. Katzenbeisser: *Strong PUFs: Models, Constructions and Security Proofs.* In A.-R. Sadeghi, P. Tuyls (Editors): Towards Hardware Intrinsic Security: Foundation and Practice. Springer, 2010.

[40] U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba: *Applications of high-capacity crossbar memories in cryptography*. IEEE Transactions on Nanotechnology, 2011.

[41] U. Rührmair, M. van Dijk: *Practical Security Analysis of PUF-based Two-Player Protocols*. CHES 2012.

[42] U. Rührmair, M. van Dijk: *On the Practical Use of Physical Unclonable Functions in Oblivious Transfer and Bit Commitment Protocols*. Journal of Cryptographic Engineering, 2013.

[43] U. Rührmair, M. van Dijk: *PUFs in Security Protocols: Attack Models and Security Evaluations*. IEEE Symposium on Security and Privacy (Oakland'13), 2013.

[44] U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, and M. Stutzmann: *Security applications of diodes with unique current-voltage characteristics.* Financial Cryptography 2010, 2010.

[45] U. Rührmair, S. Devadas, F. Koushanfar: *Security based on Physical Unclonability and Disorder.* In M. Tehranipoor and C. Wang (Editors): Introduction to Hardware Security and Trust. Springer, 2011

[46] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber: *Modeling Attacks on Physical Unclonable Functions*. ACM Conference on Computer and Communications Security, 2010.

[47] U. Rührmair, J. Sölter, F. Sehnke: *On the Foundations of Physical Unclonable Functions.* IACR Cryptology ePrint Archive 2009:277, 2009.

[48] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, S. Devadas: PUF Modeling Attacks on Simulated and Silicon Data. IACR Cryptology ePrint Archive, 2013.

[49] P. Simons, E. van der Sluis, V. van der Leest: *Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs.* HOST 2012: 7-12.

[50] A. Sharma, L. Subramanian, E. A. Brewer: *PaperSpeckle: microscopic fingerprinting of paper.* Proceedings of the 18th ACM conference on Computer and communications security (CCS'18), 2011.

[51] J. R. Smith, A. V. Sutherland: *Microstructure-Based Indicia.* Proceedings of the Second Workshop on Automatic Identification Advanced Technologies, Morristown, NJ, pp. 79-83, 1999.

[52] G. E. Suh, S. Devadas: *Physical Unclonable Functions for Device Authentication and Secret Key Generation.* DAC 2007: 9-14

[53] P. Tuyls, G. J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, R. Wolters *Read-Proof Hardware from Protective Coatings.* CHES 2006: 369-383.

[54] P. Tuyls, B. Skoric: *Strong Authentication with Physical Unclonable Functions.* In: Security, Privacy and Trust in Modern Data Management, M. Petkovic, W. Jonker (Eds.), Springer, 2007.

[55] D. Van De Ville, T. Blu, and M. Unser: *Isotropic polyharmonic B-Splines: Scaling functions and wavelets*. IEEE Transactions on Image Processing, 14(11):1798-1813, November 2005.

[56] D. Vijaywargi, D. Lewis, D. Kirovski: *Optical DNA*. Financial Cryptography 2009, pp. 222-229, 2009.

[57] F. Zhang, R. Safavi-Naini, W. Susilo: *An efficient signature scheme from bilinear pairings and its applications.* Public Key Cryptography (PKC), pp. 277-290, 2004.

[58] D. Zhou, L.J. Mawst: *Two-dimensional phase-locked antiguided vertical-cavity surfaceemitting laser arrays*. Applied Physics Letters, 77(15), pp. 2307-2309, 2000.