Disorder-Based Security Hardware: An Introduction and Overview

Ulrich Rührmair

Abstract The explicit utilization of physical disorder and of random, micro- and nanoscale phenomena is a recently emerging trend in hardware security. The associated fields of research could be termed *disorder-based security* or also *nano-security*. In this chapter, we give a high-level introduction and an overview of this arising area. We start by discussing the motivation for alternative approaches in hardware security, which mainly lies in the current uses and vulnerabilities of classical secret keys stored in non-volatile memory (NVM). This is followed by a brief description of the phenomenon of physical disorder and its useful features.
Subsequently, readers are introduced gently and inductively to the main concepts in the area via a number of concrete application examples. We show how disorder-based methods can avoid the long-term presence of key material in vulnerable systems, allow the derivation of keys in hardware without non-volatile memory, and sometimes even evade the need for any security-critical information in hardware at all. Towards the end, the chapter takes a broader perspective of the field. We illustrating its history from its first presence in patent writings in the 1960s over the privotal role of physical unclonable functions (PUFs) from the 2000s onwards to its current state. The aim of the chapter is to provide an introduction and overview of the area, and to spark and guide future research activities in the field.

1 General Context

The need to protect sensitive information is probably as old as the arts of writing or drawing themselves. Cryptography could therefore be considered with some right as one of the oldest technical disciplines. We owe several of the earliest documented examples to the Greek historian Herodotus, who describes an ancient case of a steganographic technique in the conflict between Persia and Greece around 500 BC:

Ulrich Rührmair
Technische Universität München, e-mail: ruehrmai@in.tum.de

In order to communicate sensitive information, the Greek tyrant Histiaeus shaved the head of a slave and tattoed a confidential message onto the scalp. Once the hair had re-grown, the slave could serve as a secret message carrier, passing adversarial territory unrecognizedly [23]. Herodotus also reports that around the same time, the Spartans encoded their military messages by use of a wooden stick of a well-defined diameter. A leather belt was wrapped around the stick, and the message was written across the bends. Without the stick, the symbols appeared randomly distributed over the belt; but by winding it around a stick with the same diameter, the message could be recovered [159]. Said two techniques are, to our knowledge, the first documented methods that explicitly use physical and even biological phenomena for information protection. Nothing else holds for the newly emerging fields of *"disorder-based security"* or *"nano-security"* that we discuss in this chapter — albeit the focus is now on physical phenomena at much smaller length scales, and on the explicit utilization of physical disorder and randomness at the micro- and nanoscale.

This chapter provides a first introduction and overview of these recent and fast-moving areas. It starts in Section Section 2 by motivating why alternative approaches in security are useful and on some occasions even necessary. It subsequently discusses the general phenomenon of physical disorder and its useful in a security context in Section 3, and then provides readers with three central application examples in Section 4. We thereby didactically take a inductive approach, trying to introduce readers to the central concepts in the area by virtue of the examples. The concrete advantages of disorder-based methods with hindsight to secret keys are subsumed in Section 5. The next Section 6 then takes a broader perspective of the field, explaining its (surprisingly old) history in patents and scientific writings. We conclude by a summary in Section 7.

2 Motivation, Or: Why Investigate Alternative Approaches?

Why should one investigate alternative approaches to hardware security? Why should alternatives to storing secret keys in non-volatile memory cells (NVMs) be sought? Two main reasons are discussed below.

2.1 Hardware Vulnerabilities of Secret Keys

In agreement with Kerckhoffs' principle [61], most current cryptographic and security methods rest on the concept of a secret key. This forces security hardware to permanently store a bit string that is unknown to the adversary. This requirement can be unexpectedly difficult to realize in practice: On the physical level, invasive techniques, semi-invasive methods and side channel attacks can be used to extract valuable key information [2]. On the software side, malware like Trojan horses or viruses may read out and transfer keys, even without the notice of users [2].

Three aspects play into the hands of attackers in this context. First, keys stored in non-volatile memory (NVM) are permanently present in the hardware system in a relatively easily accessible digital form [2]. What makes things worse, the permanent storage can even leave traces in the memory that allow recoverage of the key *after* it has been erased [49, 145, 160]. Second, keys are mostly strings with high entropy, allowing their identification within other, less entropic data in computer memory relatively easily [138]. Finally, the requirement that modern hardware should be lightweight, mobile, and inexpensive often leaves little room for sophisticated key protection. Functionality and cost aspects dominate security requirements in many commercial scenarios [2].

Ron Rivest accurately subsumed the situation in a keynote talk at Crypto 2011 by commenting that *"calling a bit string a secret key does not make it secret, but rather identifies it as an interesting target for the adversary"* [103]. This makes effective key protecting mechanisms — or better still: methods to entirely avoid clasiscal secret keys in vulnerable hardware — an important research topic.

2.2 Practicality and Cost Aspects

There is one second issue of classical methods. As R. Pappu et al. put it in their seminal article on Physical One-Way Functions in SCIENCE MAGAZINE [97]: *"Cryptosystems don't protect information if they're not used."* Indeed, the classic implementation of secret key schemes in hardware makes two implicit assumptions: Firstly, that the security hardware contains non-volatile memory (NVM) cells, in which the key can be stored. Secondly, that it has sufficient computational capacities to implement the cryptographic schemes which process the key.

Both assumptions are not met in certain situations. To start with, not all security-relevant hardware contains NVM cells. This includes central processing units (CPUs), several types of field programmable gate arrays (FPGAs), certain lightweight security systems, etc. If the keys are stored in a second, accompanying piece of hardware (for example the computer's hard disk), the transfer of the key to units where the key is needed (CPU, FPGA, etc.) creates an explicit attack point. This is obviously disadvantageous — a self-contained security solution would be preferrable.

Secondly, in several very low-cost scenarios, the security hardware does not possess extensive computational capacities. As an example, consider the forgery-proof tagging or "labeling" of valuable objects, such as branded products, electronic components, valuable documents, and the like. There is no computational capacity in a Rolex watch, a Nike shirt, or a paper document. Adding such capacity by RFID tags may be too expensive, apart from the obvious privacy problems it creates. Still, as pointed out by Kirovski, 7% to 10% of the world trade consists of forged products, causing an overall economic loss of the order of hundreds of billions of dollars [65].

The example illustrates the existence of highly relevant security problems that are difficult to address by standard techniques.

3 The Phenomenon of Physical Disorder and Its Usefulness

The discussion of the last section motivates the search for other methods. This chapter indeed provides an overview of an alternative approach that has emerged over the last decade(s), so-called *"disorder-based security"* or *"nano-security"*. This area explores how small-scale, random physical disorder and hadware imperfections can be exploited advantageously in security and cryptography. [1] Said physical disorder is actually omnipresent in our everyday world: Essentially all physical systems exhibit it intrinsically and "for free" on small enough length scales.

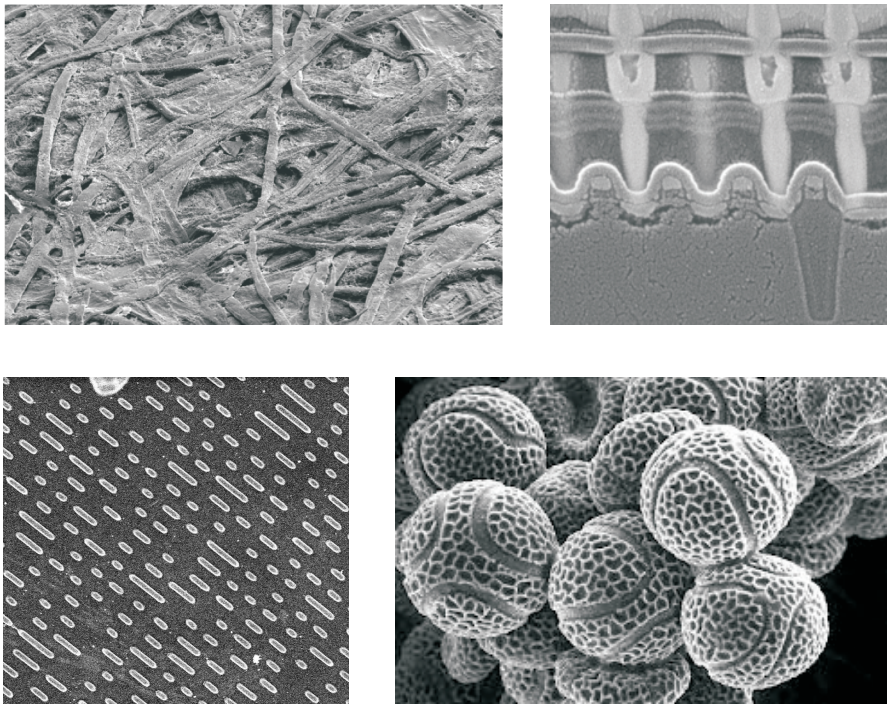

Fig. 1 Microscopic images of ordinary paper (upper left) [35], a cross section through Apple's recent A5 chip of 2011 [36], showing its transistors (upper right), the information-carrying lands and pits of an ordinary CD (bottom left) [37], and unfixed and uncoated passion flower pollens (bottom right) [38].

Four illustrating examples are given in Figure 1: Firstly, the microscopic structure of customary paper shows strong, three-dimensional irregularities in its interwoven *"paper fibers"*. Also modern integrated circuits exhibit complex manufacturing

[1] This focus distinguishes the area from other, well-known and non-standard approaches in crypto and security, such as quantum cryptography [8], noise-based crypto [24], or the bounded storage model [87, 5].

variations. These do not affect their digital functionality, but still notably influence their exact analog properties, for example the runtime delays in their individual components. Thirdly, even digital storage media such as compact discs are subject to imperfections, for example in the exact shape and length of their information-carrying indentations. The deviations are too small to affect the stored content, but still constitute a unique sub-structure of each disc. Finally, many natural structures, such as the pollens of the passion flower, show fascinating irregularities, too.

What makes physical disorder useful in cryptographic and security applications? At least four particular and distinctive features can be identified, which are discussed below.

Omnipresence.

As already emphasized, essentially all physical objects exhibit a certain amount of random disorder at sufficiently small length scales. [2] This phenomenon is not limited to the examples of Figure 1. Readers may take a short virtual tour through their offices: Any chairs, tables, walls, windows, pens, etc. exhibit small-scale disorder and imperfections, be it due to their production process, wear and tear, or both.

In fact, it is very difficult to imagine a macroscopic system or production process that is disorder-free. Usually, this is regarded as disadvantageous, for example in the context of semiconductor fabrication or nanofabrication. The approaches presented in this thesis turn the inevitability of disorder into an advantage, though, exploiting it for hardware identification, secret key derivation, and other security applications.

Hard to Clone.

A second central feature of physical disorder is that it is infeasible to perfectly clone it with current fabrication technology.[3] This is often referred to as (physical) *"unclonability"* in the literature [97, 42] and in this thesis. Interestingly, the unclonability of a system may still hold even if its entire structure is known down to every single atom to an attacker. Note that in the physical world, *knowing* the structure of a system and *rebuilding* it accurately are two different things. Consider the paper surface as of Figure 1 as an example: Even if the exact position of all paper fibers would be known, it would still remain prohibitively difficult to refabricate it

[2] The only macroscopic or mesoscopic counterexamples known to the author are highly regular crystal structures, but even they can exhibit defects or surface roughness. In addition, there are certain *microscopic* objects like photons or electrons which appear to be the same for every specimen (compare [161] for an amusing assessment of the simlarities of all electrons by two great physicists). But such *microscopic* objects or even elementary particles are not our topic in this thesis.

[3] Please note that this type of unclonability differs from another well-known type of unclonability, namely quantum unclonability. The latter is based on inherent features of quantum mechanics, the former on the technological limitations of available two- and three-dimensional fabrication techniques.

perfectly. This physical feature stands in sharp contrast to the conditions in a mathematical or Turing machine world: If you know a bitstring exactly, it is trivial to copy it with perfect accuracy. The underlying physical phenomenon could be termed *(re-) fabrication complexity*, in analogy to the well-known term computational complexity that underlies mathematical cryptography.

Hard to Fully Characterize.

Disordered systems can possess a very large entropy or random information content. As an example, consider the random information contained in the random microscopic structure of a A4-sized sheet of paper (see again Fig. 1). It is infeasible to completely measure (i.e., to "characterize" in physical parlance) this information with current technology in short time. At the same time, the generation of this disorder is very inexpensive, occuring as a natural byproduct in the fabrication process. This points to a certain *asymmetry* in the physical world between *generating* randomness and *measuring* it. Again, this asymmetry has no direct analog in the Turing world: On a Turing machine, reading a bit from the tape and generating a random bit on the tape take essentially the same effort. The associated physical phenomenon could be termed *measurement complexity* or *characterization complexity*, again analog to the well-known computational complexity.

Hard to Simulate on a Turing Machine.

Simulating the input-output behavior of complex, disordered physical structures on a Turing machine can be laborious. A straightforward example are the interference patterns created by disordered optical systems upon laser illumination (see [96, 97] and Section 4.3), but also electrical and quantum systems with similar properties exist [107, 108, 7, 25, 40, 31]. One reason for the observed simulation overheads are the inherently parallel and analog interactions in solid state systems. They are usually expensive to emulate on digital, sequential computers. This usually makes the digital simulation of a given physical system notably slower than the systems' real-time behavior, and can even render such simulation *practically infeasible* at all (compare [40]). The associated phenomenon could be called the *simulation complexity* of physical structures. Interestingly, the presence of disorder is no necessary prerequisite of simulation complexity, since also quantum systems may be hard to emulate. But in the classical physical systems that are considered in this chapter, the occurence of complex disorder usually increases the simulation overhead.

Similar to our above discussion, the phenomenon of simulation complexity has no direct counterpart in mathematical cryptography. In our sense, it can only emerge when two different worlds, like the physical and the Turing world, and their "computational speeds" are compared to each other. [4]

[4] It is interesting to comment that any physical action can in principle be interpreted as a computation and, vice versa, that computation can be understood as an inherently physical process. This

Simulation complexity can be utilized in different ways: Firstly, it may render the simulation of certain disordered structures too complex to be practically feasible at all (compare Pappu et al. [97] and Section 4.3). Secondly, simulation may be possible in practice, but notably more time consuming than the real-world behavior of the disordered structure. The latter is explicitly exploited by the recently emerging primitives of *"SIMPL systems"* [107] and *"Public PUFs"* [7].

Utilization of Physical Disorder.

Given the above discussion, it seems almost straightforward to exploit physical disorder in a security context. Just to name two examples: Why not derive unforgeable *"fingerprints"* for all everyday objects, valuable products, and security items from their individual surfaces? Why not straightforwardly derive internal secret keys from the individual disorder that is present in every piece of silicon hardware, and identify this hardware via this key? However, as common in scientific research, the problems and scientific challenges lie in the details. Certainly all everyday objects exhibit disorder on small length scales, ultimately when being scanned with an (expensive) atomic force microscope. But which features can be measured particularly inexpensively, are stable over time, and are still most difficult to forge or imitate? Which nanostructures and materials lead to particularly secure and practical fingerprints? How can honest users know the "correct" fingerprints of authentic objects, as opposed to the fingerprints of unauthentic objects? Etc.

Around these questions, a rich research landscape has emerged within the last years [84, 111]. It spans from nanophysics and electrical engineering to theoretical computer science and mathematics, and is concerned with implementational questions as well as with the theory behind disorder-based security. Some main examples are discussed throughout the rest of this book chapter.

4 Examples of Disorder-Based Security Methods and Hardware

We will now illustrate the usability of physical disorder by three concrete examples. We thereby take a inductive didactical approach, introducing readers to the main paradigms of the area by virtue of these examples. Our discussion also details the concrete security advantages of the examples over classical techniques.

---

view has been expressed by Deutsch and others [31, 32, 146], and, in a non-scientific context, even a few years before Deutsch by novelist Douglas Adams [1]. In this sense, it appears legitimate to talk about "computational speed" also when one is actually referring to physical interactions, as we do above.

4.1 Certificates of Authenticity from Paper Irregularities

According to Kirovski [65], it is estimated that 7% to 8% of world trade, 10% of the pharmaceutical market, and 36% of the software market consist of counterfeit products, causing a loss of hundreds of billions of US-Dollars every year [65]. This calls for inexpensive and effective methods that verify the authenticity of products and other objects of value. Ideally, one would like to set up a system where certain *"certification authorities"*, for example product manufacturers or state authorities, can create unforgeable *"certificates of authenticity (COAs)"* for valuable objects [65]. The COAs should be machine readable, and should be verifiable by a large number of widespread *"testing devices"* [65]. Ideally, but not necessarily, the latter might be handheld and owned by security-aware consumers themselves.

Since paper is a very widespread material, it seems suggestive to utilize the random and unclonable structure of paper in this context (compare Figure 1). Recall that the latter induces an individual fingerprint of any paper medium, including paper documents, paper packages, and paper banknotes. Approaches in this direction have indeed been suggested by a number of researchers in the past [47, 50, 144, 13, 65]. We describe their technique by the example of paper banknotes below.

Protocol 1: CERTIFICATES OF AUTHENTICITY (COAS) FOR PAPER BANKNOTES

Set-Up Assumptions:

1. The banknote manufacturer (BM) holds a secret signing key SK from some cryptographic digital signature scheme.
2. All testing devices (TDs) hold the public verification key VK that corresponds to SK.
3. The BM has implemented a physical method to measure the random structure of a given paper surface. The method produces a compact digital strong $\mathsf{UF}(\mathsf{S})$ describing the structure. [5]
4. All TDs have implemented a similar method and can reproduce the measurement results of the BM in a reliable fashion. I.e., given the same piece of paper S as the BM, each TD will derive the same description $\mathsf{UF}(\mathsf{S})$, within some error thresholds.
   This presumes that the measured paper features are sufficently stable against wear-and-tear and aging.

COA Generation:

1. The BM fabricates a paper banknote. It measures the random paper structure in a selected, marked subregion S of the banknote, producing a digital string $\mathsf{UF}(\mathsf{S})$ that describes the structure.

[5] One advantageous approach is shining a laser beam at the structure and measuring the resulting reflective interference pattern [13], but there are also other suitable techniques [101, 102, 50].

2. The BM creates a digital signature $\mathsf{DigSig}_{\mathsf{SK}}(\mathsf{UF}(\mathsf{S}), \mathsf{I})$, and prints the information
$$\mathsf{UF}(\mathsf{S}),\ \mathsf{I},\ \mathsf{DigSig}_{\mathsf{SK}}(\mathsf{UF}(\mathsf{S}), \mathsf{I})$$
onto the bank note, for example via a two-dimensional barcode.
Thereby I can be an arbitrary accompanying information, for example the banknote's value, its printing date and place, etc.

The unit consisting of an unclonable physical structure S, a digital string $\mathsf{UF}(\mathsf{S})$ that describes the unclonable features of S, and a digital signature $\mathsf{DigSig}_{\mathsf{SK}}(\mathsf{UF}(\mathsf{S}), \mathsf{I})$, is then termed a "COA" in our sense [65].

COA Verification:

1. The TD reads the information $\mathsf{UF}(\mathsf{S}),\ \mathsf{I},\ \mathsf{DigSig}_{\mathsf{SK}}(\mathsf{UF}(\mathsf{S}), \mathsf{I})$ from the banknote.
2. The TD verifies the validity of the digital signature $\mathsf{DigSig}_{\mathsf{SK}}(\mathsf{UF}(\mathsf{S}), \mathsf{I})$ by use of its verification key VK.
3. The TD measures the random paper structure of the banknote, and checks if the results match the information $\mathsf{UF}(\mathsf{S})$ printed on the banknote, again within some error thresholds.
4. If the tests in step 2 and 3 are passed, the TD regards the banknote as genuine.

4.1.1 Security Discussion

The above scheme is secure under the following assumptions:

- The adversary cannot gain access to the secret signing key stored at the manufacturer.
- The digital signature scheme is secure.
- The adversary cannot clone the paper structure, i.e., he cannot fabricate any physical system that "looks" like the original paper within the accuracy limits of the applied measurement method.

All of these assumptions are also necessary: If the adversary has access to the signing key, he can create COAs by himself. The same holds if the digital signature scheme is insecure, and if the adverary can forge signatures for any given plaintext. Thirdly, If the adversary can clone the paper in the above sense, he can fake notes by (i) copying the paper structure of a given banknote, and by (ii) using the very same digital signature from this note on the new, forged note.

4.1.2 Potential Advantages

What are the advantages and disadvantages of the above approach? One notable upside lies in the way it treats secret keys. Astonishingly, there is no secret key or other security-critical secret information on the banknotes/COAs. One could allow an adversary to inspect every atom of the banknote, and still the COAs could not

be forged: Recall that knowing the paper structure and physically reproducing it are two different things. Even the testing devices do not need to contain any security-critical information, since the adversary does not benefit from learning the public key. Both features particularly shine in applications where adversaries can easily gain long-term access the COAs (including banknotes), or whenever there are many, widespread testing devices.

The only secret key of the scheme is in the hands of the manufacturer, where it can usually be very well protected. In a scenario with many decentral fabrication sites, all of which need to generate COAs, the digital signatures could even be created centrally by one authority, and later be distributed to the sites. This keeps the number of places where a secret key needs to be protected down to one. Without going into the details, we remark that such a key distribution structure could be well applied in the context of gray-market IC overproduction, in particular whenever IC fabrication is outsourced. While the design is given to external manufacturers abroad, the certificatation process and signing key remains under the full control of the IP owner.

There is a third noteworthy security upside. Standard security features of banknotes can be mass produced by the right printing equipment. In other words, the technology to produce many identifical specimen exists already; if the adversary gains access to it, he will succeed. To the contrary, currently no fabrication technology is known that could exactly clone the complex, three-dimensional structure of paper. Even if developed some day, it would likely not immediately lend itself to cost-efficient mass fabrication. This creates an extra security margin against fraudsters.

But can digital signatures provide the long-term security required in banknotes? Recall that schemes with fixed key length may become insecure after a few decades [14]. However, there are a few counterarguments and countermeasures to this objection. Firstly, banknotes are steadily exchanged in relatively short intervals. According to information by the Deutsche Bundesbank and Giesecke&Devrient [125], for example, all German banknotes are exchanged every one to five years. The newly printed notes could use longer signature keylengths, steadily adjusting security. Similar considerations hold for archival uses of COAs where long-term security is a necessity, such as birth certificates: The digital signatures could be "refreshed" by techniques well-known in the community [151]. Finally, careful choice of keylengths and elliptic curve schemes may already in itself provide strong long-term guarantees, as detailed in [74].

While the approach offers strong security advantages as detailed above, the cost and practicality aspects are rather mixed. On the upside, it becomes unnecessary to attach dedicated labels to the banknotes, creating some cost advantages. On the other hand, extra costs in the production process are generated: The random paper structure needs to be measured, the signature must be generated, and information has to be printed on the notes. Furthermore, verification potentially requires a costly measurement device: Depending on the exact measurement technique, one may be forced to position the banknote very accuractely in order to re-generate the original measurement value.

4.1.3 Variants

The above COA-technique based on digital signatures and unclonable structures has manifold variations. Firstly, one can attach dedicated, tailor-made unclonable structures ("labels") to the valuable objects, instead of exploiting intrinsic features of the objects themselves. This partly creates extra cost. But at the same time, it can increase unforgeability, and may make the measurement process more efficient and inexpensive. Various unclonable structures have been suggested to this end (see, e.g., [13, 18, 63, 64, 28, 157, 51, 141, 20, 22], and references therein).

Secondly, COAs can be used for content protection [157, 51, 58, 47]. The key observation here is that storage media may have random, unclonable features, too. For example, the small-scale structure S of the lands and pits of a CD is subject to manufacturing variations, and thus exhibits unique features $\mathsf{UF}(\mathsf{S})$ [157, 51]. Creating a digital signature $\mathsf{DigSig}_{\mathsf{SK}}(\mathsf{UF}(\mathsf{S}), \mathsf{I})$, where I contains a hash value of the digital content stored on the CD, links this very content to its unique storage medium, thus certifying it. Copying the content onto another data carrier invalidates this certificate. Similar considerations hold for content printed on paper, such as business contracts, as discussed in [47, 20, 141].

4.2 Secret Cryptographic Keys from SRAM Power-Up States

Secret keys are at the heart of most modern cryptographic and security schemes. But as already mentioned earlier, storing them in hardware can be non-trivial: Concerning security aspect, powerful attacks have been developed, ranging from invasive to side channel techniques [2]. On the cost/practicality side, NVM is not present in every hardware system. Even if it is, sophisticated key protection measures sometimes cannot be implemented due to cost constraints.

An alternative approach, which can potentially improve both on security and practicality, is to exploit hardware-internal disorder and manufacturing variations as a secret key source. One prominent example are SRAM cells: Upon power-up of the cells, each cell contains either a zero or one, depending on the random manufacturing variations present in the cell [55, 56, 48]. The power-up states are relatively well repeatable upon multiple power-ups for each single cell, but they statistically vary from cell to cell in an SRAM array. The k cells in an SRAM array thus together create an individual power-up state "fingerprint", allowing derivation of an individual key. In the parlance of the field, an SRAM cell can act as a so-called *"physical unclonable function"* or *"PUF"*, leading to the widespread terminology "SRAM PUF" for the above phenomenon [48].

Since there must not be a single bit flip in the derived secret key, error correction is vital — the states are relatively, but not perfectly stable over repeated power-ups. Most techniques have in common that some public, non-secret "helper data" or "error-correcting data" is provided to the hardware system, allowing derivation of a stable key from the noisy power-up states [48]. It is interesting to observe that

this merely shifts the problem of storing data permanently: Instead of a binary key, now the helper data needs to be stored permanently. One difference is, though, that the helper data can be constructed not to leak any knowledge in an information-theoretic sense about the secret key. It can hence be stored publicly, and is provided to the hardware whenever key derivation is necessary. Whilst this approach creates a certain time and communication overhead, its security and practicality benefits dominate in certain settings.

One exemplary application scenario, which we describe in greater detail below, is the protection of intellectual property (IP) in the context of FPGA designs [48]. Many FPGA types do not contain non-volatile memory cells and hence cannot store application designs permanently [48]. The designs are thus stored externally and uploaded onto the FPGA when needed. Fraudsters can intercept the upload bitstream and learn the designs, which often represent a very substantial IP value. The lack of NVM prevents classical secret keys on the FPGA. At the same time, SRAM cells are present on many FPGAs. This enables IP protection schemes between the manufacturer, the FPGA, and an external memory device storing the design [48]. We give one basic example of such a scheme below [48]; other, more involved techniques are described in the same reference [48].

Protocol 2: IP PROTECTION OF FPGA DESIGNS VIA SRAM PUFS [48]

Set-Up Assumptions:

1. The scheme involves four parties: The IP provider (IPP); a system integrator or designer (SYS); the FPGA-manufacturer (HWM); and a trusted third party (TPP).
2. The communication channels between HWM and TTP, and between TTP and IPP, are authenticated and confidential.
3. The TTP and the HWM are fully trusted.
4. The HWM can disable access to the SRAM cells after reading them out in the enrollment phase (for example by blowing some fuses). No one can access the cells anymore after this operation, including adversaries.
5. For simplicity of exposition, we do not explicitly deal with error correction in this protocol. In practice, error correcting helper data does need to be used to obtain stable responses. [6]

Initialization Phase (aka "Enrollment Protocol" [48]):

1. The HWM associates an $\mathsf{ID}_{\mathsf{HW}}$ to a given FPGA. It reads out different sets of SRAM-power up states $R_1, \ldots, R_n$ of this FPGA.
2. The HWM disables external access to those SRAM-cells that have provided the above response $R_1, \ldots, R_k$. Internal access for the FPGA itself to these cells must remain intact.

[6] Following a convention stipulated in [48], readers may interpret the protocol in such a way that C_i denotes the PUF challenge *and* the corresponding helper data required to reconstruct the PUF response R_i from a noisy version R_i'.

3. The HWM sends
$$\mathsf{ID}_{\mathsf{HW}}, R_1, \ldots, R_n$$
to the TTP.

IP Authentication Protocol:

1. SYS sends
$$\mathsf{ID}_{\mathsf{SW}}, \mathsf{ID}_{\mathsf{HW}}$$
to TTP, indicating which software $\mathsf{ID}_{\mathsf{SW}}$ shall be utilized on which FPGA hardware $\mathsf{ID}_{\mathsf{HW}}$.
2. The TTP sends $\mathsf{ID}_{\mathsf{SW}}$ to the IPP, and the IPP returns the software SW to the TTP.
3. The TTP encrypts the software with the key R_i, creating a value
$$D = \mathsf{Enc}_{R_i}(\mathsf{SW}, \mathsf{ID}_{\mathsf{SW}}).$$
4. The TTP sends the message
$$C_i, C_j, D, \mathsf{MAC}_{R_j}(C_i, C_j, D)$$
to SYS.

Design Upload and Decryption on the FPGA:

1. The FPGA uploads the encrypted bitstream created by SYS, which is stored in a (non-confidential) storage medium accompanying the FPGA.
The bistream potentially contains k encrypted and authenticated software blocks of the above form
$$C_i^k, C_j^k, D^k, \mathsf{MAC}_{R_j^k}(C_i^k, C_j^k, D^k).$$
2. For each k, the FPGA internally reproduces the responses R_i^k and R_j^k by accessing and measuring the respective SRAM cells.
(Please note again that in practice, error correcting helper data must be used to this end, which must be provided from and external non-volatile, but not confidential storage medium. In the case of FPGAs, the same medium can be used that stores the encrypted upload bitstream.)
The FPGA decrypts the bitstream and verifies the authentication.
3. The FPGA is configured by the decrypted bitstream.

4.2.1 Security Discussion

We partly follow [48] in our discussion below. The protocol achieves confidentiality and integrity of the IP (i.e., software blocks) only under the following assumptions, among others: (i) The TTP and the HWM are trusted; (ii) the mutual communication channels TTP-HWM and TTP-IPP are confidential and authenticated; and (iii)

no one can externally read-out the responses R_i and R_j after access to them has been disabled by the HWM, while the FPGA itself can still access the responses internally.

These are relatively significant assumptions. In particular, hypothesis (iii) is at the least in part comparable to the standard assumption that a classical key cannot be read-out by the adversary. This observation questions the effective security gain of the above SRAM PUF approach in high-end scenarios and against well-equipped adversaries. Indeed, recent invasive attacks on SRAM PUFs [92] have been able to read-out these responses and to derive the corresponding keys. This shows that the main advantage of the above scheme lies in providing a medium level of security in an hardware enviroment without NVM, where usually no encryption could be used at all. The scheme also promises to be more secure against not well equipped adversaries than classical NVMs, since the SRAM responses are present in the system only when the cells are powered up. They can hence be read-out only during limited periods of time, and while the chip is still functional, e.g., while it has a working power supply.

In general, the scheme is structured like a classical secret key scheme, with the only exception that the key is "stored" in a different fashion. This implies that the implementation of the decryption algorithm which deciphers D and recovers SW on the FPGA must be secured against any classical hardware attacks, similar as in a classical secret key based scheme. No security gain is achieved in this particular aspect by the above SRAM PUF approach.

Finally, please note that since the TTP is trusted, it does not matter that it learns the IP during the protocol. We once more stress that the required error correcting helper data must be stored externally in a non-volatile fashion, but that this storage needs not be secret [48]. In the case of FPGAs without NVMs, this external storage poses no strong additional requirement, as the FPGA designs would need to be stored externally in any case. In other applications, however, it may constitute a substantial practical issue. Further aspects are discussed in [48, 92].

4.2.2 Potential Advantages

The main advantage of the above scheme is that it enables security (and encryption) in an environment without NVM. Without using SRAM cells as key source, no encryption would be possible at all. This could be regarded as a practicality advantage or as a security advantage, depending on personal taste.

It has also been argued that the use of SRAM PUFs brings about general security advantages in comparison with NVM cells, i.e., even in comparison with systems that do possess NVM. Such claims require further analysis, we believe. It is true that SRAM cells allow to derive a key only whenever it is needed within the hardware. This means that the key is not present permanently in the hardware, as in the case of NVMs. On the other hand, invasive or other access to the SRAM cells [92] (or similar PUFs [90]) allows derivation of the key just as in the case of NVMs. Furthermore, also cloning of SRAM PUFs has been reported recently [52]. Overall, we

recommend that the exact security gains of using SRAM PUFs over NVMs should be analyzed separately and carefully for any given practical applications.

4.2.3 Variants

One potential drawback of the scheme is that every communication runs over the TTP. As described in [48], this can be resolved as follows: The TTP forwards many pairs $(C_i, R_i), (C_j, R_j)$ to one or several IPPs, where these pairs are stored. Whenever necessary, an IPP sends C_i, C_j, D, $\mathsf{MAC}_{R_j}(C_i, C_j, D)$, where $D = \mathsf{Enc}_{R_i}(\mathsf{SW}, \mathsf{ID}_{\mathsf{SW}})$, to SYS. In this approach, no authenticated or secure channel between IPP and SYS is required. We also remark that it is possible to develop other protocols in which the TTP does not have direct access to the IP and SW; interested readers are referred to [48].

There is a second security use of the power-up states of SRAM cells that should not go unmentioned: Holcomb et al. show that those SRAM cells whose power-up states are unstable (i.e., whose power-up states flip randomly upon multiple power-ups) can be used as hardware-internal source of random numbers [55, 56].

4.3 Remote Identification by Light Scattering in Random Media

Our first example is an identification scheme suggested by Pappu et al. [96, 97] in 2001/02, which rests on optical interference phenomena. At the heart of their method is a transparent, cuboid-shaped plastic platelet of size 1 cm $\times$ 1 cm $\times$ 2.5 mm, in which a large number of micrometer-sized glass spheres have been distributed randomly during the production process. The varying sizes, shapes and positions of the spheres induce a strong disorder in the platelet, making it practically infeasible to build two specimen which are exactly the same. The platelet is *"unclonable"* by use of current technology.

When a laser beam is directed at the platelet, the laser light is scattered multiple times inside the structure. This creates a so-called *"speckle pattern"*, an interference pattern of dark and bright regions, which can be recorded conveniently by a CCD camera. Asides from the relative positioning of the platelet and the camera, which we imagine as fixed and do not consider further here, this speckle pattern sensitively depends on (i) the random positions, sizes and shapes of the spheres (i.e., on the disorder inside the token), and (ii) on the angle α and point $\mathbf{r}$ of incidence of the laser beam. The latter can be varied, with new parameters $(\mathbf{r}, \alpha)$ leading to new patterns. Leaving aside measurement noise, this allows us to regard the input-output behavior of the token as a function f that maps measurement parameters $\mathbf{r}, \alpha$ into speckle patterns $f(\mathbf{r}, \alpha)$. The situation is depicted in Figure 2.

The function f has a number of interesting properties. First, f possesses a very large number of input-output pairs $(\mathbf{r}, \alpha), f(\mathbf{r}, \alpha)$, also called *"challenge-response pairs (CRPs)"* in the parlance of the field. Pappu et al. estimate that the above

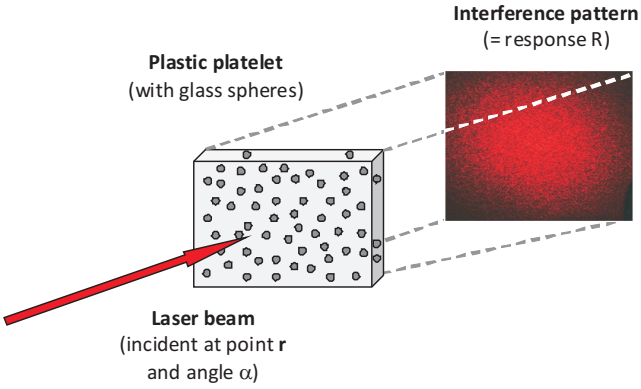

Fig. 2 Illustration of Pappu's optical, interference-based physical one-way function [96, 97].

platelet size allows around $2.37 \cdot 10^{10}$ inputs which lead to computationally independent speckle patterns as outputs. If an adversary has got access to the platelet merely for a limited time period on the order of days or weeks, he will find himself unable to measure all possible input-output pairs and to complete characterize the function f. Secondly, an adversary knowing only a subset of all input-output pairs will be unable to numerically predict the speckle pattern to a new, unknown input $\mathbf{r}, \alpha$ without making a physical measurement on the token. The main reason is that the input-output behavior of the object is too laborious to simulate on a computer. As analyzed by Pappu et al. [97], in the worst case every cubic subunit of the platelet whose side lenth is around the wavelength λ of the incoming laserlight would play a role in the scattering process. For a cube with side length 1 cm, this leads to one Terabit of relevant subunits whose interaction would need to be considered in a simulation, making the latter practically infeasible. Similar considerations, thirdly, hold for the non-invertibility of f: Given a speckle pattern, it is practically impossible to determine which challenge parameters $\mathbf{r}, \alpha$ created this speckle pattern, even if one has access to the token. This non-invertibility property of f originally inspired the name *"Physical One-Way Function"* or *"POWF"* [96, 97] for the above structure; today, it is also often refered to simply as an *"optical PUF"*.

The described optical PUF can be applied in identification protocols, for example in a bank card scenario. In the following protocol, k is the security parameter, and l is the number of envisaged executions of the identification phase.

Protocol 3: BANK CARD IDENTIFICATION WITH LIGHT SCATTERING TOKENS

Set-Up and Security Assumptions:

1. The bank can securely store secret data on a server in its headquarters.
2. Each bank terminal is connected to the bank server by a non-confidential, but authenticated channel.

3. The bank can fabricate suitable light scattering platelets itself or has access to a trusted manufacturer.

Initialization Phase:

1. The bank produces a light scattering platelet with a large number of randomly distributed scatterers, or obtains such a platelet from a trusted manufacturer. It attaches it as token to a bank card, which bears the customer identification number ID.
2. The bank chooses at random $k \cdot l$ parameters $\mathbf{r}_i, \alpha_i$, and applies a laser beam at position $\mathbf{r}_i$ and under angle α_i to the token. It measures the resulting speckle patterns, and derives from the raw data the responses R_i, for example by applying image transformation or error correction.
3. The bank stores the list $\mathcal{L}_{\mathsf{ID}} = (\mathbf{r}_1, \alpha_1, R_1), \ldots, (\mathbf{r}_{k \cdot l}, \alpha_{k \cdot l}, R_{k \cdot l})$ together with the identification number ID of the card on its server. The bank card is released to the field.

Identification Phase (can be executed maximally l times):

1. When the card is inserted into a terminal, the terminal reads the ID from the card and sends ID to the server.
2. The server looks up the list $\mathcal{L}_{\mathsf{ID}}$. It chooses the first k entries $(\mathbf{r}_1, \alpha_1, R_1), \ldots, (\mathbf{r}_k, \alpha_k, R_k)$ from the list, and sends the parameters $(\mathbf{r}_1, \alpha_1), \ldots, (\mathbf{r}_k, \alpha_k)$ to the terminal.
3. The terminal applies laser beams with the incidence coordiantes and angles given by $(\mathbf{r}_1, \alpha_1), \ldots, (\mathbf{r}_k, \alpha_k)$ to the token, and measures the corresponding speckle patterns. It derives the responses $R'_1, \ldots, R'_k$ from the raw data by applying the same image transformations or error correction as the bank in the set-up phase. The terminal returns $R'_1, \ldots, R'_k$ to the server.
4. The server compares the responses $R_1, \ldots, R_k$ and $R'_1, \ldots, R'_k$. If they match better than given error threshold, the server sends an "OK!" message to the terminal. Otherwise, it sends an abort message.
5. The first k entries are erased from the list $\mathcal{L}_{\mathsf{ID}}$.

4.3.1 Security Discussion

A meaningful discussion requires us to first fix the underlying attack model. It is reasonable to assume that an attacker will be able to access the platelet several times between different executions of the identification phase: He could set up faked terminals, or gain possession of the bank card when the customer employs it on other occasions, for example for paying in shops or restaurants. Furthermore, we should suppose that the attacker can eavesdrop the binary communication in the identification protocol and learn the used CRPs $(C_1, R_1), \ldots, (C_k, R_k)$. Under this relatively strong attack model, the security of the scheme is nevertheless upheld by the above properties of the physical one-way function f and of the token. An adversary will

be (i) unable to clone the token physically, and (ii) cannot predict the challenge-response behavior numerically, even if he knows a large number of CRPs. This renders him unable to complete the identification protocol successfully without actual possession of the real token. Interestingly, the scheme does not utilize the one-way property of f, but only the features of unclonability and unpredictability.

4.3.2 Potential Advantages

Compared to standard identification schemes, Pappu et al.'s method exhibits a few notable advantages. First and foremost, no secret digital keys need to be stored on the bank card. Assuming that the token is too complex to simulate and rebuild, there is indeed no security-critical information at all present on the card whose disclosure would break the security of the system. Even if the adversary knew all positions of the scatterers and all irregularities of the structure, he still could not rebuild or simulate it, since this would be infeasible in practice. We can allow him to possess any information in the scattering object without endangering the security of the scheme! This feature is in sharp contrast to any classical techniques, which necessitate that at least some information on the card remains secret. It is also in contrast to some PUF-based techniques, for example the SRAM PUFs presented in Section 4.2, where a disclosure of the power up states of the adversary breaks the security of the system. Secondly, no potentially laborious numerical identification schemes need to be executed on the card in Pappu et al.'s scheme. The card does not even need to carry integrated circuitry, making it extremely cost effective, at least on the card side.

4.3.3 Variants

There are a number of variants of the above scheme. Firstly, other hardware systems than the described optical PUF can be employed. Any other Strong PUFs [111] can be used, for example Arbiter PUFs and variants [42, 149], as long as they are secure against modeling [120, 122] and other attacks, for example side channels. Also secure integrated optical PUFs would be an option, preferrably with non-linear scattering materials (compare [115]). Finally, the hardware of optical PUFs can be used for a number of other, more advanced cryptographic protocols, including key exchange [33, 15, 109], bit commitment [96, 15, 94, 112, 113], or oblivious transfer [106, 15, 94].

5 Advantages of Disorder-Based Security Hardware

Let us condense and summarize the advantages of disorder-based security hardware in this section. We thereby take a pure hardware-centered perspective, ignoring some of the specific cryptographic advantages.

Security Advantage: Better Protection/Avoidance of Keys.

One of the most important upside of disorder-based techniques is their approach to cryptographic keys. All techniques of the last Section 4 avoid the presence of *"classical secret keys"* in vulnerable hardware, i.e., the presence of keys that are stored permanently in NVM, as detailed throughout the last section. Some of the presented approaches go even one step further, though. This can be seen most easily if we generalize the notion of a classical secret key. Let us call a *"security-critical information" (SCI)* any information that is present in a piece of hardware at least at one point in time, and whose disclosure to the adversary breaks the security of the system. One can then ask: Do the hardware systems of Section 4 contain any *SCI* in the above sense?

The answer differs for the three systems of Section 4. To start with, the paper structure of system 4.1 does not contain any security-critical information at all, since the adversary would be unable to refabricate the complex paper structure, even if he knew it atom by atom. Something similar holds for the optical PUF of Section 4.3: It could not be cloned, and its output could not be simulated for complexity reasons, even if the entire structure would be known to the adversary in arbitrary detail. On the other hand, the SRAM PUFs of Section 4.2 lead to systems that do contain SCI: The power-up states of the SRAM cells constitute SCI; and so does the internal key obtained from the power-up states after error correction. In this sense, the SRAM PUFs differ from optical PUFs, or from the paper based COAs of Section 4.1.

We would like to stress that this distinction is not just academic, but has a direct practical relevance. For example, it eventually enables the invasive attacks on SRAM PUFs that recently have attracted considerable interest [92]. Furthermore, the delays in Arbiter PUFs also represent a form of SCI, a fact that eventually allows modeling attacks on this type of structure [120]. In essence, the presence of SCI in a hardware system necessarily creates unwanted attack points,and well-versed adversaries will in the end exploit these. Overall, it appears preferrable to construct disorder-based systems without SCI wherever possible. We would like to encourage readers to pay increasing attention to this distinction, and to categorize disorder-based security approaches with respect to this feature wherever possible in the future.

Practicality Advantage: Hardware without NVM or ICs.

From a practicality perspective, the most important upside of the techniques of Section 4 is that they enable security features in hardware without NVM, and partly even in hardware without integrated circuits (ICs). The use of SRAM cells on FPGAs without NVM (Section 4.2) is one known example for the former, while the exploitation of surface irregularities or optical PUFs (Sections 4.1 and 4.3) are examples for the latter. Both can be decisive practicality and cost factors, as they bring security to systems where otherwise elaborate and dedicated security measures would be impossible. Recall in this context that adding non-volatile keys to hardware systems without NVM requires significant additional production steps and extra costs.

6 Historic Perspective and General Overview

This chapter would not be complete without a general overview and historic perspective of the area. As patent writings and commercial activities are not in the direct focus of this chapter, we concentrate on academic writings wherever possible. Our discussion reveals that the field has older and broader roots than usually acknowledged. It also shows the different branches of research in disorder-based security: While physical unclonable functions are clearly the central and dominant subfield, there are also other noteworthy subareas, which need to be distinguished for historic or scientific reasons. Providing a basic distinction between these subareas will also be helpful in inspiring and guiding future research in the area.

Origins of the Field.

It is non-trivial to trace back the field to its exact origins. To the knowledge of the author, the first publicly available source utilizing random, uncontrollable manufacturing variations in a security context is a US-patent with priority date 1968 by Lindstrom and Schullstrom of Saab AB, Sweden [77]. It suggests that randomly, non-uniformly distributed magnetic materials could be employed for individualizing and securing *"identification documents like driver's licences and credit cards"*. It further proposes that concealed, internal layers of such materials might protect sensitive regions of identification documents, for example the picture of the card holder, against alteration, and could detect manipulation of these regions. The latter foreshadows a security feature that today is called tamper-sensitivity. The inventors also suggest that electrical or optical materials could be used to the same end.

It has also been reported that in the 1970s, Bauder and Simmons of Sandia National Laboratories, USA, exploited the optical behavior of physically disorder media for security purposes [18, 91, 66, 65]. Their goal was to conduct secure weapons inspection during the cold war era. To this end, they reportedly spray-painted epoxy

onto nuclear warheads, shed light at it from a certain angle, and recorded pictures of the resulting optical patterns [18, 91, 66, 65]. These images could later be used to re-identify each single warhead in a forgery-proof manner [18, 91, 66, 65]. It seems very likely that this work was conducted independently of Lindstrom's and Schullstrom's approach.

Perhaps the first to combine modern cryptographic methods with physical disorder was Goldman of Light Signatures Inc., USA. In a patent writing with priority date 1980, he details the use of paper irregularities in connection with digital signatures for certifying documents [47]. Light Signatures commercialized this technique in order to authenticate stock certificates in the mid 1980s, but their activities were apparently not profitable and abandoned in 1988 [127]. Presumably independently of Goldman, Bauder (reportedly together with Simmons [18, 66]) suggested a similar concept at Sandia National Laboratories, also combing unique paper structures with digital signatures [65]. A Sandia-internal source that is multiply quoted in this context is by Bauder [6], dating from 1983. [7]

With some right, the three above, independent research groups could be seen as early forefathers of disorder-based security and also of physical unclonable functions. This would imply that the field has older roots than sometimes acknowledged.

First Presence at Scientific Conferences.

The groundbreaking ideas of Lindstrom and Schullstrom, Goldman, and Bauder and Simmons, seemingly were not discussed much in public scientific conferences or journals until the 1990s. Perhaps the earliest scientific paper that points in the relevant direction is by Simmons, dating from 1991 [143]. Independently and a few years later, a number of publications by van Renesse treat similar ideas, focusing on optical product protection systems [101, 102]. Suggestions based on magnetic materials, which are in principle related to the early patent of Lindstrom and Schullstrom, have been made independently by Chu et al. [19] and Vaidya [156] at scientific venues in 1995.

In 1998, Haist et al. [50] also discuss paper and optical probing for product protection, making explicit use of digital signatures in a similar fashion as Goldman. A closely related scientific publication is by Smith et al. [144] from 1999. It uses paper irregularities with digital signatures in order to create unforgeable postal stamps.

In 2000, Lofstrom et al. [78] for the first time suggest the variations in standard integrated circuit components for security purposes, exploiting the random threshold mismatches in transistors to identify individual circuits (compare Section 4.2). Their paper could be seen as a direct precursor of the modern PUF era, foreshadowing socallled intrinsic PUFs like SRAM PUFs and Butterfly PUFs (without explicit use of the term "PUF", though).

[7] However, copies of this paper seem unavailable to a broad public. The author of this chapter has been unsuccessful in gaining access despite considerable efforts, including multiple e-mail requests to the Sandia National Laboratories. Other researchers made partly similar experiences [66].

DNA-based Steganography.

Before we eventually turn to PUFs, let us quickly mention another independent research avenue. In 1999, the randomness in complex mixtures of DNA strands was suggested for use in security and steganography by Clelland et al. in Nature magazine [22]. If a secret message or other critical information is encoded in DNA strands, and if these strands are mixed with a huge number of other, random strands, an adversary would find it practically impossible to identify and isolate the "secret" strands. He would be faced with the proverbial search for the needle in the haystack. The fact that complex DNA mixtures can be generated by simple means plays into the hands of this method [22]. In follow-up work, DNA-based public and private key cryptography has been discussed, for example, in [73, 46]. The approach of Clelland et al. has even led to commercially available products [129].

DNA-based security might appear off topic and seems generally less known within the PUF community. Still, it has established its own research strand, with hundreds of citations, some presence at DNA-related venues, and a certain level of commercial activities. Furthermore, it likely is the first approach that explicitly exploits nanoscale phenomena for security. This foreshadows a recently emerging trend towards nano-security in the PUF area [117, 57, 105].

Physical Unclonable Functions (PUFs).

Despite all above contributions, it seems fair to say that the interest of the broader security community was not sparked until 2001/02, when a few seminal works were published at major scientific venues: Firstly, Pappu [96] in 2001, and Pappu et al. [97] in Science magazine in 2002, presented the idea of so-called *"physical one-way functions"* or *"POWFs"*. Their optical implementation of POWFs (compare Section 4.3) has a number of novel features compared to earlier optical security works [47, 101, 102, 50]; for example, it explicitly uses random 3D media and (coherent) laser light as probing signal to facilitate maximally complex response behavior. The second seminal strand of work was by Gassend et al., who published the concept of silicon, circuit-based *"physical random functions"* at ACM CCS 2002 [42], and of *"controlled physical random functions"* at ACSAC 2002 [43]. The latter papers also use the term *"physical unclonable function"* or *"PUF"* for the first time, which today is frequently employed as a synonym for the entire research area.

Compared to earlier works, one central innovation of Pappu et al. and Gassend et al. was to link disordered, unclonable media to more established cryptographic concepts like one-way functions or pseudo-random functions. Secondly, they used disordered media with a very large number of different input signals, whose behavior could be regarded as some sort of complex, disorder-based *"physical function"*. The mathematical properties of this function, such as unpredictability or one-wayness, could then be formally expressed and exploited in cryptographic protocols. Both

aspects helped attracting the interest of the cryptographic and security community and spreading the new concepts quickly.

Other seminal PUF works in the early period from 2002 to 2007 include (but are not limited to): The AEGIS security architecture by Suh et al. [148] from 2003; first information-theoretic analyses of PUFs by Tuyls et al. in 2004/05 [154, 155]; the security use of laser illuminated paper surfaces by Buchanan et al. in Nature in 2005 [13] (compare Section 4.1); and the usage of disordered electrical structures as tamper sensitive coatings by Tuyls et al. [152] in 2006. A further groundbreaking idea was the use of the individual, but repeatable power-up states of SRAM cells as secret key source. This concept is particularly useful in hardware that does not carry non-volatile memory cells. It was independently put forward by Holcomb et al. [55] and Guajardo et al. [48] in 2007.

Certificates of Authenticity (COAs).

Starting a few years later than PUFs, a parallel and independent strand of works helped popularizing the idea of disorder-based security. It roots quite directly in the original ideas of Lindstrom and Schullstrom, Goldman, and Bauder and Simmons, using very similar techniques: It combines the unique and unclonable features of disordered media with digital signatures to form so-called *"certificates of authenticity"* or *"COAs"* for objects of value. Example works of this strand include COA-specific error correction [63, 64] in 2004, optical COAs [18] (which pick up the early ideas of Bauder and Simmons [6]) in 2005, and radiowave based COAs [28] in 2007. Also work on unique optical fingerprints of compact discs, which was independently published by DeJean et al. [157] and Hammouri et al. [51] in 2009, could be associated with this research strand. A good summary of the subarea is given by Kirovski in [65]. Most COA papers are somewhat demarked from PUFs in terms of nomenclature and scientific content. Furthermore, the COA-idea arguably dates back earlier than PUFs, being present in its full-fledged form in combination with digital signatures already in the 1980s [47, 6]. We thus found it appropriate to devote a separate paragraph to it. At the same time, we remark that the current focus of the community appears to be on PUFs, both regarding research activities, quotation numbers, and nomenclature.

Status Quo and Current Research.

From 2008 onwards, a rapidly growing activity on disorder based security takes place. It is mostly, but not exlusively focused on PUFs, and often regards the two works by Pappu et al. [97] and Gassend et al. [42] as root publications of the field. Listing all published works of the last six years is beyond the intention and scope of this section; we refer the interested reader to recent survey articles [84, 111] or PUF biobliographies [126].

Rather, we find it convenient to collect several facts that exemplarily testify the rapid establishment of the area. To start with, according to Google scholar, the two root articles of Pappu et al. [97] and Gassend et al. [42] have been quoted many hundred times to date, with increasing citation figures almost every year. Since 2008, papers on PUFs and related topics have been published at CHES [12, 83, 51, 150, 166, 59, 165, 67, 112, 72, 60, 82, 81, 10, 81], EUROCRYPT [94], ASIACRYPT [3, 27], CRYPTO [15], ACM CCS [120, 141], IEEE S&P [4, 114], IEEE T-IFS [26, 79, 122], ACM TISSEC [44], and the Journal of Cryptology [80], i.e., in all top publication channels of the general cryptography and security community. Since 2010, the two large hardware security conferences CHES and HOST continously had one or even two dedicated PUF session each year (see [123, 124]). DATE, one of the two largest international design automation conferences, in 2014 offered both a standard technical session on PUFs [130], a hot topic session on PUFs [131], and a related tutorial on counterfeiting ICs [132], illustrating how PUFs have long spread from their original field of security into neighbouring areas like circuit design. Also the first coursebooks on PUFs have appeared recently [11]. Even on the commercial side, PUFs achieved some recent breakthroughs, appearing in the product lines of major companies like NXP [134, 135] and Microsemi [136, 137]. It therefore seems justified to say that almost 15 years after its popularization in scientific circles [78, 96, 97, 42, 43], and around 45 years since its very first presence in patent writings [77], the field has developed into a central subarea of hardware security, and currently shows no signs of slowing down in its rapid progress.

7 Summary and Outlook

In this chapter, we surveyed a recently emerging subfield of hardware security that could be called *"disorder-based security"* or also *"nano-security"*. It exploits the small-scale, random physical disorder that is present in essentially all solid state systems for security purposes. The roots of the field reach back surprisingly far, with first appearances in patent writings in the late 1960s. Today, its most active subfield are by far physical unclonable functions (PUFs); other, but smaller subareas are DNA-based cryptography or so-called *"certificates of authenticity"* (COAs).

The two main motivations for disorder-based hardware are practicality/cost and security aspects. Both are intimately related to the way we currently treat secret keys in secure hardware: Usually, the keys are stored in and read from non-volatile memory cells (NVM) or comparable structures, and are subsequently postprocessed by some cryptographic algorithm. Disorder-based security, for example PUFs and COAs, offer three potential improvements in this situation. Firstly, it allows keys in hardware without NVMs. Recall that not all hardware systems possess NVMs since they cause extra costs, one prime example being certain types of FPGAs. As an alternative, the keys can potentially be derived from the omnipresent physical disorder in the hardware. One concrete example are SRAM cells: They show individual and characteristic power-up states due to small manufacturing variations,

and can hence be used as key source. Secondly, it avoids the long-term presence of keys in NVM cells in vulnerable hardware. The keys derived from SRAM cells, for example, are present in the hardware system only when needed. This shorter time of presence makes attacks more difficult. As long as the system is powered off, it can be much more difficult for adversaries to obtain the keys. Thirdly, identification schemes based on so-called *"Strong PUFs"* [111], including the optical PUFs discussed in this paper, use the PUF-responses directly, meaning that no post-processing via classical cryptographic algorithms is necessary. This can potentially increase security levels, too, since these algorithms are one potential target for attacks, for example side channel techniques. For the same reason, optical PUFs can even create means for remote identification without electrical circuitry being present in the hardware, which can be a substantial cost and practicality asset in certain appliances.

We believe that the field will still rapidly expand and flourish in the foreseeable future. Current publication activity is extraordinarily high and shows no signs of slowing down. Besides a large number of scientific innovations, also some first commercial breakthroughs could be achieved recently [134, 135, 136, 137]. Regarding future activities, three promising subareas lie in the formal foundations of the field, including classification, formal definitions, and security proofs, secondly in discovering yet new primitives and uses of physical disorder beyond the currently existing approaches, and thirdly in the improved physical implementation of currenty existing concepts. The fact that these subareas span from from theoretical computer science to nanophysics and nanotechnologies arguably gives the field a unusually broad focus and attractivity.

References

1. D. Adams: *The hitchhiker's guide to the galaxy*. Pan Books, 1979.
2. R.J. Anderson: *Security Engineering: A Guide to Building Dependable Distributed Systems*. Second Edition. Wiley, 2008.
3. F. Armknecht, R. Maes, A.-R. Sadeghi, B. Sunar, P. Tuyls: *Memory Leakage-Resilient Encryption Based on Physically Unclonable Functions*. ASIACRYPT 2009, pp. 685-702, 2009.
4. F. Armknecht, R. Maes, Ahmad-Reza Sadeghi, F.-X. Standaert, C. Wachsmann: *A Formal Foundation for the Security Features of Physical Functions*. IEEE Symposium on Security and Privacy 2011, pp. 397-412, 2011.
5. Y. Aumann, Y. Z. Ding, M. O. Rabin: *Everlasting security in the bounded storage model*. IEEE Transactions on Information Theory, Vol. 48(6), pp. 1668-1680, 2002.
6. D.W. Bauder: *An anti-counterfeiting concept for currency systems.* Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990, 1983.
7. N. Beckmann, M. Potkonjak: *Hardware-based public-key cryptography with public physically unclonable functions*. Information Hiding 2009, pp. 206-220, 2009.
8. C.H. Bennett, G. Brassard: *Quantum cryptography: Public key distribution and coin tossing.* IEEE International Conference on Computers, Systems and Signal Processing, Vol. 175(150), p. 8, 1984.
9. D. J. Bernstein, J. Buchmann, E. Dahmen (Ed.): *Post-Quantum Cryptography*. Springer, 2009. ISBN 978-3-540-88701-0.

10. M. Bhargava, K. Mai: *A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement*. CHES 2013, pp. 90-106, 2013.
11. C. Böhm, M. Hofer: *Physical Unclonable Functions in Theory and Practice*. ISBN 978-1-4614-5040-5. Springer, 2013.
12. C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, P. Tuyls: *Efficient Helper Data Key Extractor on FPGAs*. CHES 2008, pp. 181-197, 2008.
13. J.D.R. Buchanan, R. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. Allwood, M. Bryan: *Fingerprinting documents and packaging*. Nature, Vol. 436(7050), p. 475, 2005.
14. J. Buchmann, A. May, U. Vollmer: *Perspectives for cryptographic long-term security*. Communications of the ACM, Vol. 49(9), pp. 50-55, 2006.
15. C. Bruzska, M. Fischlin, H. Schröder, S. Katzenbeisser: *Physical Unclonable Functions in the Universal Composition Framework.* CRYPTO 2011, pp. 51-70, 2011.
16. Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, U. Rührmair: *The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions*. HOST 2011, pp. 134-141, 2011.
17. Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, U. Rührmair: *Characterization of the Bistable Ring PUF.* DATE 2012, pp. 1459-1462, 2012.
18. Y. Chen, M.K. Mihcak, D. Kirovski: *Certifying authenticity via fiber-infused paper*. SIGecom Exchanges, Vol. 5(3), pp. 29-37, 2005.
19. M.C. Chu , L.L. Cheng, L.M. Cheng: *A novel magnetic card protection system*. European Convention on Security and Detection, pp. 207-211, 1995.
20. W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J.A. Halderman, E.W. Felten: *Fingerprinting Blank Paper Using Commodity Scanners*. IEEE Symposium on Security and Privacy 2009, pp. 301-314, 2009.
21. Clay Mathematical Institure Milllenium Prize on P vs NP. Downloaded from http://www.claymath.org/millennium/P_vs_NP, August 2012.
22. C.T. Clelland, V. Risca, C. Bancroft. *Hiding messages in DNA microdots.* Nature, Vol. 399(6736), pp. 533-534, 1999.
23. I.J. Cox, M. L. Miller, J.A. Bloon, J. Fridrich, T. Kalker: *Digital Watermarking and Steganography*. Morgan Kaufmann, 2008.
24. C. Crepeau: *Efficient cryptographic protocols based on noisy channels*. EUROCRYPT 1997, pp. 306-317, 1997.
25. 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 2010, pp. 1-6, 2010.
26. W.E. Cobb, E.D. Laspe, R.O. Baldwin, M.A. Temple, Y.C. Kim: *Intrinsic Physical-Layer Authentication of Integrated Circuits*. IEEE Transactions on Information Forensics and Security, Vol. 7(1), pp. 14-24, 2012.
27. I. Damgard, A. Scafuro: *Unconditionally Secure and Universally Composable Commitments from Physical Assumptions*. ASIACRYPT 2013, pp. 100-119, 2013.
28. G. DeJean, D. Kirovski: *RF-DNA: Radio-Frequency Certificates of Authenticity*. CHES 2007, pp. 346-363, 2007.
29. J. Delvaux, I. Verbauwhede: *Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise*. HOST 2013, pp. 137-142, 2013.
30. J. Delvaux, I. Verbauwhede: *Fault Injection Modeling Attacks on 65nm Arbiter and RO Sum PUFs via Environmental Changes*. IACR Cryptology ePrint Archive, Report 2013/619, 2013.
31. D. Deutsch: *Quantum theory, the Church-Turing principle and the universal quantum computer*. Proceedings of the Royal Society of London; Series A, Mathematical and Physical Sciences. Vol. 400(1818), pp. 97-117, 1985.
32. D. Deutsch, A. Ekert, R. Luppachini: *Machines, Logic and Quantum Physics*, arXiv:math/9911150v1, 1999. Downloaded from http://arxiv.org/abs/math.LO/9911150, August 2012.
33. M. van Dijk: *System and method of reliable forward secret key sharing with physical random functions.* US Patent No. 7,653,197, October 2004.

34. Y. Z. Ding: *Provable Everlasting Security in the Bounded Storage Model*. PhD Thesis, Harvard University, Cambridge (Massachusetts), USA, 2001.
35. Downloaded from https://freedom-to-tinker.com/blog/felten/fingerprinting-blank-paper-using-commodity-scanners, August 2012.
36. Downloaded from http://www.netbooknews.com/21848/apple-a5-processor-dissection-reveals-samsungs-handywork/, August 2012.
37. Downloaded from http://volga.eng.yale.edu/index.php/CDsAndDVDs/Methods AndMaterials?action=browse, August 2012.
38. Downloaded from http://www.dailymail.co.uk/sciencetech/article-2215052/ The-complexity-intricacy-Mother-Nature-revealed-incredible-pictures-plants–seen-inside.html, April 2014.
39. Downloaded from http://www.funtasticus.com/2008/12/09/looking-through-a-microscope/, August 2012
40. R. Feynman: *Simulating Physics with Computers.* International Journal of Theoretical Physics, Vol. 21, (6&7), pp. 467-488, 1982.
41. B. Gassend, *Physical Random Functions*, MSc Thesis, MIT, 2003.
42. B. Gassend, D.E. Clarke, M. van Dijk, S. Devadas: *Silicon physical random functions*. ACM CCS 2002, pp. 148-160, 2002.
43. B. Gassend, D.E. Clarke, M. van Dijk, S. Devadas: *Controlled Physical Random Functions*. ACSAC 2002, pp. 149-160, 2002.
44. B. Gassend, M. van Dijk, D.E. Clarke, E. Torlak, S. Devadas, P. Tuyls: *Controlled physical random functions and applications*. ACM Transactions on Information and System Security, Vol. 10(4), 2008.
45. B. Gassend, D. Lim, D.E. Clarke, M. van Dijk, S. Devadas: *Identification and authentication of integrated circuits.* Concurrency and Computation: Practice & Experience, pp. 1077 - 1098, 2004.
46. A. Gehani, T. LaBean, J. Reif: *DNA-based cryptography.* Aspects of Molecular Computing, pp. 167-188, Springer, 2004.
47. R.N. Goldman: *Non-counterfeitable document system*. US-Patent 4,423,415. Publication date: 1983. Priority date: 1980.
48. J. Guajardo, S.S. Kumar, G.J. Schrijen, P. Tuyls: *FPGA Intrinsic PUFs and Their Use for IP Protection*. CHES 2007, pp. 63-80, 2007.
49. P. Gutmann, *Secure deletion of data from magnetic and solid-state memory*. USENIX Security Symposium, 1996.
50. T. Haist, H.J. Tiziani: *Optical detection of random features for high security applications.*. Optics communications, Vol. 147.1, pp. 173-179, 1998.
51. G. Hammouri, A. Dana, B. Sunar: *CDs Have Fingerprints Too*. CHES 2009, pp. 348-362, 2009.
52. C. Helfmeier, C. Boit, D. Nedospasov, J.-P. Seifert: *Cloning Physically Unclonable Functions*. HOST 2013, pp. 1-6, 2013.
53. M. Hofer, C. Böhm: *An Alternative to Error Correction for SRAM-Like PUFs*. CHES 2010, pp. 335-350, 2010.
54. D.E. Holcomb: *PUFs at a Glance*. Talk, Hot Topic Session 12.2, Design, Automation & Test in Europe (DATE) 2014, 2014.
55. D.E. Holcomb, W.P. Burleson, K. Fu: *Initial SRAM state as a fingerprint and source of true random numbers for RFID tags*. Conference on RFID Security, 2007.
56. D.E. Holcomb, W.P. Burleson, K. Fu: *Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers*. IEEE Transactions on Computers, Vol. 58(9), pp. 1198-1210, 2009.
57. C. Jaeger, M. Algasinger, U. Rührmair, G. Csaba, M. Stutzmann: *Random pn-junctions for physical cryptography*. Applied Physics Letters 96, 172103, 2010.
58. Y. Kariakin: *Authentication of articles*. Patent writing, WO/1997/024699, 1995. Available from http://www.wipo.int/pctdb/en/wo.jsp?wo=1997024699
59. S. Katzenbeisser, Ü. Kocabas, V. van der Leest, A.-R. Sadeghi, G.-J. Schrijen, H. Schröder, C. Wachsmann: *Recyclable PUFs: Logically Reconfigurable PUFs*. CHES 2011, pp. 374-389, 2011.

60. S. Katzenbeisser, Ü. Koçabas, V. Rozic, A.-R. Sadeghi, I. Verbauwhede, C. Wachsmann: *PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon*. CHES 2012, pp. 283-301, 2012.
61. A. Kerckhoffs: *La cryptographie militaire*. Journal des sciences militaires, Vol. IX, pp. 5-38, 1883.
62. J. Kilian: *Founding cryptography on oblivious transfer*. STOC 1988, pp. 20-31, 1988.
63. D. Kirovski: *Toward an automated verification of certificates of authenticity*. EC 2004, pp. 160-169, 2004.
64. D. Kirovski: *Point Compression for Certificates of Authenticity*. Data Compression Conference 2004, p. 545, 2004.
65. D. Kirovski: *Anti-counterfeiting: Mixing the Physical and the Digital World*. In: Towards Hardware-Intrinsic Security, A.-R. Sadeghi, D. Naccache (Eds.), pp. 223-233, Springer, 2010.
66. D. Kirovski, *personal communication*, Dagstuhl 2008.
67. A.R. Krishna, S. Narasimhan, X. Wang, S. Bhunia: *MECCA: A Robust Low-Overhead PUF Using Embedded Memory Array*. CHES 2011, pp. 407-420, 2011.
68. R. Kumar, W. Burleson: *Personal communication*. 2014.
69. S.S. Kumar, J. Guajardo, R. Maes, G.J. Schrijen, P. Tuyls: *The Butterfly PUF: Protecting IP on every FPGA*. HOST 2008, pp. 67-70, 2008.
70. H. Langhuth, S. Frederic, M. Kaniber, J. Finley, U. Rührmair: *Strong Photoluminescence Enhancement from Colloidal Quantum Dot Near Silver Nano-Island Films*. Journal of Fluorescence, Vol. 21(2), pp. 539-543, 2010.
71. J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas: *A technique to build a secret key in integrated circuits with identification and authentication applications.* IEEE VLSI Circuits Symposium, pp. 176-179, 2004.
72. V. van der Leest, B. Preneel, E. van der Sluis: *Soft Decision Error Correction for Compact Memory-Based PUFs Using a Single Enrollment*. CHES 2012, pp. 268-282, 2012.
73. A. Leier, C. Richter, W. Banzhaf, H. Rauhe: *Cryptography with DNA binary strands*. BioSystems, Vol. 57(1), pp. 13-22, 2000.
74. A.K. Lenstra, E.R. Verheul: *Selecting Cryptographic Key Sizes*. Journal of Cryptology, Vol. 14(4), pp. 255-293, 2001.
75. D. Lim: *Extracting Secret Keys from Integrated Circuits*. MSc Thesis, MIT, 2004.
76. D. Lim, J.W. Lee, B. Gassend, G.E. Suh, M. van Dijk, S. Devadas: *Extracting secret keys from integrated circuits*. IEEE Transactions on VLSI Systems, Vol. 13(10), pp. 1200-1205, 2005.
77. G. Lindstrom, G. Schullstrom: *Verifiable identification document*. US-Patent 3,636,318. Publication date: 1972. Priority date: 1968.
78. K. Lofstrom, W.R. Daasch, D. Taylor: *IC identification circuit using device mismatch.* ISSCC 2000, pp. 372-373, 2000.
79. A. Maiti, I. Kim, P. Schaumont: *A Robust Physical Unclonable Function With Enhanced Challenge-Response Set*. IEEE Transactions on Information Forensics and Security, Vol 7(1), pp. 333-345, 2012.
80. A. Maiti, P. Schaumont: *Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive*. Journal of Cryptology, Vol. 24(2), pp. 375-397, 2011.
81. R. Maes: *An Accurate Probabilistic Reliability Model for Silicon PUFs*. CHES 2013, pp. 73-89, 2013.
82. R. Maes, A. Van Herrewege, I. Verbauwhede: *PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator*. CHES 2012, pp. 302-319, 2012.
83. R. Maes, P. Tuyls, I. Verbauwhede: *Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs*. CHES2009, pp. 332-347, 2009.
84. R. Maes, I. Verbauwhede: *Physically unclonable functions: A study on the state of the art and future research directions*. In: Towards Hardware-Intrinsic Security, A.-R. Sadeghi, D. Naccache (Eds.), pp. 3-37. Springer, 2010.
85. M. Majzoobi, F. Koushanfar, M. Potkonjak: *Lightweight Secure PUFs.* IC-CAD 2008, pp. 607-673, 2008.
86. M. Majzoobi, F. Koushanfar, M. Potkonjak: *Testing techniques for hardware security.* ITC 2008, pp. 1-10, 2008.

87. U. Maurer: *Conditionally-perfect secrecy and a provably-secure randomized cipher*. Journal of Cryptology, Vol. 5(1), pp. 53-66, 1992.
88. U. Maurer: *Cryptography 2000±10*. In Reinhard Wilhelm (Ed.): Informatics – 10 Years Back. 10 Years Ahead. Lecture Notes in Computer Science, Vol. 2000, pp. 63-85, Springer, 2001. ISBN 3-540-41635-8.
89. D. Merli, D. Schuster, F. Stumpf, G. Sigl: *Side-Channel Analysis of PUFs and Fuzzy Extractors*. TRUST 2011, pp. 33-47, 2011.
90. D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, G. Sigl: *Localized electromagnetic analysis of RO PUFs*. HOST 2013, pp. 19-24, 2013.
91. M.K. Mihcak: *Overview of Recent Content Authentication Research at MSR Crypto, Redmond*. Available from https://www.yumpu.com/en/document/view/10835269/m-kivanc-mihcak-uvigo-tv, or from http://tv.uvigo.es/uploads/material/Video/91/Kivanc_Mihcak.pdf.
92. D. Nedospasov, J.-P. Seifert, C. Helfmeier, C. Boit: *Invasive PUF Analysis*. FDTC 2013, pp. 30-38, 2013.
93. Y. Oren, A.-R. Sadeghi, C. Wachsmann: *On the Effectiveness of the Remanence Decay Side-Channel to Clone Memory-Based PUFs*. CHES 2013, pp. 107-125, 2013.
94. R. Ostrovsky, A. Scafuro, I. Visconti, A. Wadia: *Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions*. EUROCRYPT 2013, pp. 702-718, 2013.
95. E. Öztürk, G. Hammouri, B. Sunar: *Towards robust low cost authentication for pervasive devices*. IEEE PerCom 2008, pp. 170-178, 2008.
96. R. Pappu: *Physical One-Way Functions.* PhD Thesis, MIT, 2001.
97. R. Pappu, B. Recht, J. Taylor, N. Gershenfeld: *Physical One-Way Functions*. Science, Vol. 297, pp. 2026-2030, 2002.
98. C. Pomerance: *A Tale of Two Sieves*. Notices of the AMS, Vol. 43(12), pp. 1473-1485, 1996.
99. M. Potkonjak: *Hardware based cryptography.* US-Patent 8379856 B2. Priority date: June 17, 2009.
100. M. Potkonjak: *Personal communication*, 2011.
101. R.L. van Renesse: *3DAS: a 3-dimensional-structure authentication system*. European Convention on Security and Detection, pp. 45-49, 1995.
102. R.L. van Renesse: *Optical document security.* Artech House, third edition, 2005. ISBN-10: 1580532586
103. R. Rivest: *Illegitimi non carborundum*. Invited keynote talk, CRYPTO 2011. Downloaded from http://www.rsa.com/rsalabs/presentations/Riv11b.slides.pdf, August 2012.
104. J. Rombach: *Elektrische Charakterisierung zufälliger pn-Dioden für die Kryptographie*. Bachelor thesis, TU München, 2012.
105. M. Rostami, J.B. Wendt, M. Potkonjak, F. Koushanfar: *Quo Vadis, PUF? Trends and Challenges of Emerging Physical-Disorder based Security*. Design, Automation & Test in Europe (DATE 2014), 2014.
106. U. Rührmair: *Oblivious Transfer based on Physical Unclonable Functions (Extended Abstract)*. TRUST 2010, pp. 430 - 440, 2010.
107. U. Rührmair: *SIMPL Systems: On a Public Key Variant of Physical Unclonable Functions*. IACR Cryptology ePrint Archive, Report 2009/255, 2009.
108. U. Rührmair: *SIMPL Systems, Or: Can we build cryptographic hardware without secret key information?*. SOFSEM 2011, Springer LNCS, 2011.
109. U. Rührmair: *Physical Turing Machines and the Formalization of Physical Cryptography*. IACR Cryptology ePrint Archive, Report 2011/188, 2011.
110. U. Rührmair, H. Busch, S. Katzenbeisser: *Strong PUFs: Models, Constructions and Security Proofs.* To appear in A.-R. Sadeghi, P. Tuyls (Editors): Towards Hardware Intrinsic Security: Foundation and Practice. Springer, 2010.
111. U. Rührmair, S. Devadas, F. Koushanfar: *Security based on Physical Unclonability and Disorder.* In: Introduction to Hardware Security and Trust, M. Tehranipoor, C. Wang, pp. 65-102. Springer New York, 2012.
112. U. Rührmair, M. van Dijk: *Practical Security Analysis of PUF-Based Two-Player Protocols*. CHES 20120, pp. 251-267, CHES 2012.

113. U. Rührmair, M. van Dijk: *On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols*. Journal of Cryptographic Engineering, Vol. 3(1), pp. 17-28, 2013.
114. U. Rührmair, M. van Dijk: *PUFs in Security Protocols: Attack Models and Security Evaluations*. IEEE Symposium on Security and Privacy 2013, pp. 286-300, 2013.
115. U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, C. Jirauschek: *Optical PUFs Reloaded*. IACR Cryptology ePrint Archive, Report 2013/215, 2013.
116. U. Rührmair, D. Holcomb: *PUFs at a Glance*. Design, Automation & Test in Europe (DATE 2014), 2014.
117. U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, G. Csaba: *Applications of high-capacity crossbar memories in cryptography*. IEEE Transactions on Nanotechnology, Vol. 10(3), pp. 489-498, 2011.
118. U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, M. Stutzmann: *Security Applications of Diodes with Unique Current-Voltage Characteristics*. Financial Cryptography and Data Security (FC 2010), Lecture Notes in Computer Science, Vol. 6052, pp. 328-335, Springer Verlag, 2010.
119. U. Rührmair, U. Schlichtmann, W. Burleson: *Special Session: How Secure Are PUFs Really? On the Reach and Limits of Recent PUF Attacks*. Design, Automation & Test in Europe (DATE 2014), 2014.
120. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber: *Modeling Attacks on Physical Unclonable Functions*. ACM CCS, pp. 237-249, 2010.
121. U. Rührmair, J. Sölter, F. Sehnke: *On the Foundations of Physical Unclonable Functions.* Cryptology e-Print Archive, June 2009.
122. 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*. IEEE Transactions on Information Forensics and Security, Vol. 8(11), pp. 1876-1891, 2013.
123. See http://www.informatik.uni-trier.de/ Ley/db/conf/ches/index.html
124. See http://www.informatik.uni-trier.de/ LEY/db/conf/host/index.html
125. See http://www.gi-de.com/en/trends_and_insights/banknote_circulation/life_of_a_banknote/life-of-a-banknote.jsp
126. See http://rmaes.ulyssis.be/pufbib.php
127. See http://www.answers.com/topic/certegy-inc-1
128. See http://www.design-reuse.com/articles/16975/arm-security-solutions-and-intel-authenticated-flash-how-to-integrate-intel-authenticated-flash-with-arm-trustzone-for-maximum-system-protection.html
129. See http://www.adnas.com/products/signaturedna
130. See http://www.date-conference.com/conference/session/4.3
131. See http://www.date-conference.com/conference/session/12.2
132. See http://www.date-conference.com/category/session-types/tutorial
133. See http://www.chemistryexplained.com/St-Te/Surface-Chemistry.html
134. See www.nxp.com/documents/other/75017366.pdf
135. See http://www.nxp.com/news/press-releases/2013/02/nxp-strengthens-smartmx2-security-chips-with-puf-anti-cloning-technology.html
136. See http://investor.microsemi.com/releasedetail.cfm?ReleaseID=731250
137. See http://www.microsemi.com/products/fpga-soc/soc-fpga/smartfusion2
138. A. Shamir, N. van Someren: *Playing "Hide and Seek" with Stored Keys*. Financial Cryptography 1999: 118-124.
139. C. E. Shannon: *A Mathematical Theory of Communication*. Bell System Technical Journal, Vol. 27, pp. 379-423, 623-656, 1948. ISSN 0005-8580.
140. C. E. Shannon: *Communication Theory of Secrecy Systems*. Bell System Technical Journal, Vol. 28(4), pp. 656-715, 1949.
141. A. Sharma, L. Subramanian, E.A. Brewer: *PaperSpeckle: microscopic fingerprinting of paper.* ACM CCS 2011, pp. 99-110, 2011.
142. P.W. Shor: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing, Vol. 26(5), pp. 1484-1509, 1997.

143. G.J. Simmmons: *Identification of data, devices, documents and individuals*. Annual International Carnahan Conference on Security Technology, pp. 197-218, 1991.
144. J.R. Smith, A.V. Sutherland: *Microstructure based indicia*. Second Workshop on Automatic Identification Advanced Technologies, pp. 79-83, 1999.
145. S. Skorobogatov: *Low temperature data remanence in static RAM*. Technical Report UCAM-CL-TR-536, Computer Laboratory, University of Cambridge, 2002. Available from http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-536.pdf.
146. S. Stepney: *Journeys in non-classical computation*. In: T. Hoare, R. Milner (Eds.): Grand Challenges in Computing Research, pp. 29-32. Swindon, BCS, 2004.
147. M. Stutzmann, G. Csaba, P. Lugli, J. Finley, C. Jirauschek, C. Jaeger, U. Rührmair: *Towards Electrical, Integrated Implementations of SIMPL Systems.* European Patent (EP) 2230794 A3. Priority date: March 16, 2009.
148. G.E. Suh, D.E. Clarke, B. Gassend, M. van Dijk, S. Devadas: *AEGIS: architecture for tamper-evident and tamper-resistant processing*. ICS 2003, pp. 160-171, 2003.
149. G. E. Suh, S. Devadas: *Physical Unclonable Functions for Device Authentication and Secret Key Generation.* DAC 2007: 9-14
150. D. Suzuki, K. Shimizu: *The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes*. CHES 2010, pp. 366-382, 2010.
151. C. Troncoso, D. De Cock, B. Preneel: *Improving secure long-term archival of digitally signed documents*. StorageSS 2008: 27-36
152. P. Tuyls, G.J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, R. Wolters: *Read-Proof Hardware from Protective Coatings.* CHES 2006, pp. 369-383, 2006.
153. P. Tuyls, B. Skoric: *Strong Authentication with Physical Unclonable Functions.* In: Security, Privacy and Trust in Modern Data Management, M. Petkovic, W. Jonker (Eds.), pp. 133-148, Springer, 2007.
154. P. Tuyls, B. Skoric, S. Stallinga, A.H.M. Akkermans, W. Ophey: *An information theoretic model for physical uncloneable functions*. IEEE International Symposium on Information Theory, p. 141, 2004.
155. P. Tuyls, B. Skoric, S. Stallinga, A.H.M. Akkermans, W. Ophey: *Information-Theoretic Security Analysis of Physical Uncloneable Functions*. Financial Cryptography, pp. 141-155, 2005.
156. A.W. Vaidya: *Keeping card data secure at low cost.* European Convention on Security and Detection, pp. 212-215, 1995.
157. D. Vijaywargi, D. Lewis, D. Kirovski: *Optical DNA*. Financial Cryptography 2009, pp. 222-229, 2009.
158. S. Wolf, J. Wullschleger: *Oblivious Transfer Is Symmetric*. EUROCRYPT 2006, pp. 222-232, 2006.
159. Wikipedia's article on cryptography. Downloaded from http://en.wikipedia.org/wiki/Cryptography, August 2012.
160. Wikipedia's article on data remanence. Downloaded from http://en.wikipedia.org/wiki/Data_remanence, August 2012.
161. Wikipedia's article on a one-electron universe. Downloaded from http://en.wikipedia.org/wiki/One-electron_universe, April 2014.
162. Wikipedia's article on RSA numbers. Downloaded from http://en.wikipedia.org/wiki/RSA_numbers, August 2012.
163. Wikipedia's article on "the magic words are squeamish ossifrage". Downloaded from http://en.wikipedia.org/wiki/The_Magic_Words_are_Squeamish_Ossifrage, August 2012.
164. Wikipedia's article on the VENONA project. Downloaded from http://en.wikipedia.org/wiki/Venona_project, August 2012.
165. D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, T. Ochiai, M. Takenaka, K. Itoh: *Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches*. CHES 2011, pp. 390-406, 2011.
166. M.-D. Yu, D. M'Raihi, R. Sowell, S. Devadas: *Lightweight and Secure PUF Key Storage Using Limits of Machine Learning*. CHES 2011, pp. 358-373, 2011.