FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Assignment of bachelor's thesis

Title:	Physical unclonable functions on ESP32
Student:	Ondřej Staníček
Supervisor:	Ing. Jiří Buček, Ph.D.
Study program:	Informatics
Branch / specialization:	Computer Security and Information technology
Department:	Department of Computer Systems
Validity:	until the end of summer semester 2022/2023

Instructions

Physical unclonable functions are an emerging cryptographic primitive that can be used for device identification, authentication, and key generation in digital devices.

* Study the topic of physical unclonable functions (PUFs). Focus primarily on SRAM PUF.
* Design and implement a simple SRAM based PUF on a suitable ESP32 microcontroller.
* Experiment with the microcontroller's internal registers to find a suitable mechanism for SRAM power state control.
* Test the function of the PUF on several devices.
* Evaluate relevant PUF parameters (especially bit stability and uniqueness).
* Evaluate the distribution of SRAM bit values depending on operating temperature and power-off time.

Electronically approved by prof. Ing. Pavel Tvrdík, CSc. on 10 January 2022 in Prague.

Bachelor's thesis

PHYSICAL UNCLONABLE FUNCTIONS ON ESP32

Ondřej Staníček

Faculty of Information Technology
Department of Computer Systems
Supervisor: Ing. Jiří Buček, Ph.D.
April 15, 2022

Contents

List of Figures

List of Tables

List of code listings

Chtěl bych poděkovat především sit amet, consectetuer adipiscing elit. Curabitur sagittis hendrerit ante. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Cras pede libero, dapibus nec, pretium sit amet, tempor quis. Sed vel lectus. Donec odio tempus molestie, porttitor ut, iaculis quis, sem. Suspendisse sagittis ultrices augue.

Declaration

I hereby declare that the presented thesis is my own work and that I have cited all sources of information in accordance with the Guideline for adhering to ethical principles when elaborating an academic final thesis. I acknowledge that my thesis is subject to the rights and obligations stipulated by the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular that the Czech Technical University in Prague has the right to conclude a license agreement on the utilization of this thesis as a school work under the provisions of Article 60 (1) of the Act.

In Prague on April 15, 2022 .....

Abstract

Fill in abstract of this thesis in English language. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Cras pede libero, dapibus nec, pretium sit amet, tempor quis. Sed vel lectus. Donec odio tempus molestie, porttitor ut, iaculis quis, sem. Suspendisse sagittis ultrices augue.

Keywords ESP32, physical unclonable functions, static random access memory, error correction codes, hardware security

Abstrakt

Fill in abstract of this thesis in Czech language. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Cras pede libero, dapibus nec, pretium sit amet, tempor quis. Sed vel lectus. Donec odio tempus molestie, porttitor ut, iaculis quis, sem. Suspendisse sagittis ultrices augue.

Klíčová slova ESP32, fyzicky neklonovatelné funkce, statická paměť, samoopravné kódy, hardwarová bezpečnost

List of Abbreviations

AES	Advanced Encryption Standard
API	application programming interface
BCH	Bose–Chaudhuri–Hocquenghem
BLE	Bluetooth Low Energy
CMOS	complementary metal–oxide–semiconductor
CTW	context-tree weighting
ECC	error correction code
FAR	false acceptance rate
FPGA	field-programmable gate array
FRR	false rejection rate
HD	Hamming distance
HW	Hamming weight
IoT	Internet of things
MAC	message authentication code
MOSFET	metal–oxide–semiconductor field-effect transistor
NBTI	negative-bias temperature instability
NIST	National Institute of Standards and Technology
POK	physically obfuscated key
POWF	physical one-way function
PRF	physical random function
PUF	physical unclonable function
ROM	read only memory
ROPUF	ring oscillator physical unclonable function
RTC	real-time clock
RTOS	real-time operating system
SoC	system on a chip
SPI	Serial Peripheral Interface
SRAM	static random access memory
TMV	temporal majority voting
TRNG	true random number generator
ULP	ultra low power

Chapter 1
Introduction

1.1 Motivation

Internet of things (IoT) is a fast growing field of the information age that we live in right now. Millions of cheap and connected devices are being used in a huge number of applications such as smart homes, self-driving cars, smart cities and wearables.

As these devices are connected to the Internet and they collect potentially sensitive data, it is crucial to make them as secure as possible. One of the key challenges of security is the generation and storage of cryptographic keys, since they play a vital role in most cryptographic algorithms used to secure the devices.

Usually, the keys are randomly generated and stored in non-volatile memory. However, the non-volatile memory needs to be secured (even from invasive physical attacks) and the generation process must be unpredictable. Satisfying both of those requirements is extremely hard and expensive.

Physical unclonable functions (PUFs) try to solve this issue. They are based on physical properties which are inherently random and unique for each device. A PUF can be compared to a device's fingerprint. The cryptographic key is not stored digitally anywhere on the device but is reconstructed from the unique physical properties. PUFs can also be used for other tasks such as identification or authentication.

One example of an especially popular IoT platform is ESP32. It consists of a family of cheap microcontrollers and software to enable easy application development. The main goal of this thesis is to analyze the possibility of implementing a particular type of PUF, the static random access memory (SRAM) PUF, on this platform.

1.2 Objectives

The objectives of this thesis are following:

- Analyze the topic of physical unclonable functions with focus on SRAM PUF.
- Find a suitable mechanism for SRAM power state control on the ESP32 microcontroller.
- Design and implement a simple SRAM based PUF on the ESP32 microcontroller.
- Evaluate relevant PUF parameters such as bit stability and uniqueness on the resulting PUF implementation.

- Evaluate the behaviour of the PUF depending on operating temperature and SRAM power-off time.
- Test the function of the resulting PUF implementation on several devices.

1.3 Thesis structure

The thesis is divided into eight chapter in the following way:

1. Introduction:
Motivation and goals of this thesis are given in this chapter.

2. Physical unclonable functions:
First, description of a PUF is given in this chapter. Then, main properties and classes of PUFs are outlined and parameters used to evaluate the performance of PUFs are defined. Lastly, concrete PUF applications and implementations are explained shortly.

3. SRAM PUF:
A thorough explanation of a SRAM PUF is given. The chapter then provides a discussion on which properties the SRAM PUF possesses and a brief introduction to silicon aging which affects this PUF implementation.

4. ESP32 platform:
An introduction into the ESP32 platform is provided in this chapter. A brief hardware and software description of the ESP32 microcontroller is given with focus on parts that are important to the PUF implementation.

5. SRAM PUF implementation on ESP32:
Two ways of SRAM power state control on ESP32 are proposed in this chapter. The raw startup memory values obtained by the two methods are then analyzed based on operating temperature and memory power-off time. Some of the evaluation parameters defined in Chapter 2 are also used during the analysis.

6. Reliable PUF response extraction:
This chapter proposes a method to extract PUF responses reliably. This enables the PUF to be used for cryptographic key generation. In order to achieve this goal, bit selection and error correction codes (ECCs) are used. At the end, the PUF is tested on 16 different devices and during different operating temperatures.

7. ESP32 SRAM PUF library:
Based on the analyses in the previous chapters a simple SRAM PUF implementation is provided in an ESP32 library. Its functionality is explained in this chapter.

8. Conclusion:
Summarization of results of this thesis is given in this chapter together with suggestion of possible future work.

Chapter 2

Physical unclonable functions

2.1 PUF description

As PUFs are the main subject of this thesis, it is important to provide a thorough explanation of what a PUF is, what types and classes exist and what are the applications of this technology.

Since more and more types of PUFs are being invented, it turns out that creating a generalizable description is not a straightforward task. A dictionary definition of a PUF could be written as: "a PUF is an expression of an inherent and unclonable instance-specific feature of a physical object". One can imagine a PUF being an object's fingerprint in a comparable way to how humans have their own unique fingerprints.[1]

The first concept of PUF was proposed by Pappu in 2001. He used the term physical one-way function (POWF), which he described as a function operating on a physical system that could be easily computed but not easily inverted.[2] The first mention of the term PUF was by Gassend et al. in 2002. He talks about physical random functions (PRFs) and a PUF implementation using field-programmable gate arrays (FPGAs).[3]

As PUF is a function, it has inputs and outputs. However, it is not a function in a true mathematical way. It could be described as a procedure performed on a particular device. Its inputs consist of a challenge and a physical state of the device. Given the input, the PUF produces an output (called a response). Together, they form challenge-response pairs.

A hugely important property of PUFs is unclonability. It is achieved by the physical state of the device which acts as the input to the function and influences the responses produced by the PUF. The concrete details of the physical state used is what distinguishes different PUF implementations. These physical properties could be for example propagation delay in the chip circuit or bias of uninitialized memory cells to 1 or 0 state. The latter is a basis for SRAM PUF, which is a topic of this thesis. These properties are fundamentally random since they are created by uncontrollable physical processes during manufacturing. This makes them physically unclonable.

Since the physical state of the device can change with time and environment (for example temperature or input voltage variations), the challenge-response pairs can change as well. The requirement is, that for the same challenge, the responses should be similar enough for us to be able to recognize that they belong to the same challenge. The PUF responses are also required to differ from device to device even with the same challenge.[4]

Because of these properties, PUFs can be used in devices to enable secure identification, authentication as well as cryptographic key generation. More of the required properties of PUFs, their classification, possible applications and implementations will be discussed in more detail in the next sections.

2.2 PUF properties

In this section, a list of PUF properties according to [5] is described. Some of them are fundamental to all PUF constructions (the first six listed). However, not all PUFs must necessarily exhibit all of the discussed properties. In Section 3.1, properties of SRAM PUFs are discussed as they are a topic of this thesis.

Constructibility

Constructibility states, that the specific PUF instance must be 'easy' to construct. This means that the laws of physics enable such PUF implementation in the first place. The construction cost of such PUF needs to also be adequate for its application.

Evaluability

The evaluability property discusses the challenge-response mechanism of PUFs. For a specific challenge, it should be 'easy' to obtain the corresponding response. Practically this requires that the response is acquired with respect to time, space, cost and power budget of the application.

Reproducibility

Reproducibility requires that for a specific PUF instance, responses produced by the same challenge must be similar enough. The metric that measures the similarity of the responses used is the intra-Hamming distance (which will be defined later in Section 2.4.2). Practically it must be possible to recognize that the responses belong to the same challenge.

Figure 2.1 reproducibility: responses to the same PUF challenge need to be similar [6].

Uniqueness

While reproducibility talks about the behaviour of a specific PUF, uniqueness is defined with respect to a set of different PUF instances. Given the same challenge, two PUFs must produce a response that is different enough in the given metric. The metric used is the inter-Hamming distance (which will be defined later in Section 2.4.3).

Identifiability

Identifiability is tied to both uniqueness and reproducibility. Given a single challenge, if the responses from the same PUF are similar and responses from different PUFs are different enough, the responses can be used as a means of identification of each PUF. More formal characterization of the words 'similar' and 'different' as well as a concrete protocol for PUF identification is explained in Sections 2.4 and 2.5.1.

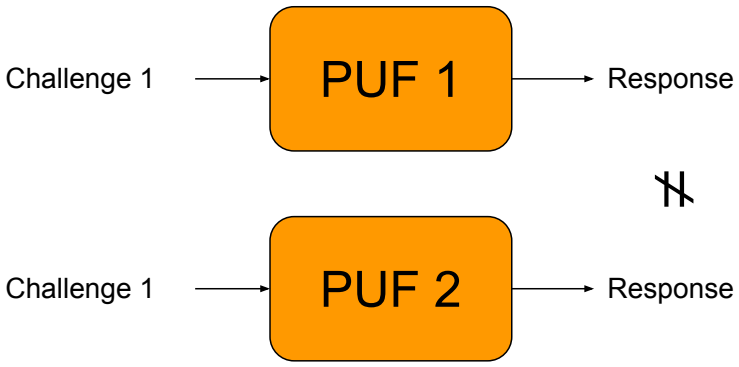


Figure 2.2 uniqueness: two PUF instances must produce different responses if given the same challenge [6].

Physical unclonability

Physical unclonability enforces that it is hard to break the uniqueness property. The 'hardness' is expressed as a technical and physical infeasibility of creating two nearly identical PUF instances. In practice, even the manufacturer is unable to break uniqueness due to the uncontrollable physical laws on which the PUF implementation relies.

Unpredictability

A PUF is said to be unpredictable, if given a limited set of challenge-response pairs, it is impossible to create an algorithm that predicts the remaining responses based on a challenge. This means that the challenge-response pair space is sufficiently random.

Mathematical unclonability

While physical unclonability talks about the impossibility of creating a real-world clone of a specific PUF, mathematical unclonability requires that no algorithm can predict the PUF behaviour.

Mathematical unclonability is a stronger model of unpredictability. It assumes unlimited physical access to a specific PUF instance. The potential adversary can learn as many challenge-response pairs as he is capable of storing and can potentially make use of other PUF observations. Even in this situation, it should be impossible for the adversary to create a prediction algorithm capable of outputting a response based on a given challenge.

Mathematical unclonability implies that the specific PUF implementation has a large number of possible challenges (more than the adversary could theoretically store). If this was not true, a simple lookup table of challenge-response pairs could be constructed, breaking mathematical unclonability.

True unclonability

PUF is considered truly unclonable if it is physically and mathematically unclonable. True unclonability thus implies mathematical and physical unclonability.

One-Wayness

The one-wayness property is similar to the requirement of cryptographic one-way functions (for example hash functions). Given a PUF instance and a response, it should be impossible to create an inversion algorithm that can find a corresponding challenge to the response.

Similar to mathematical unclonability, the PUF needs to have a sufficiently large set of possible challenges and resulting responses in order to meet this property. Otherwise, it would be possible to construct a complete lookup table and find the wanted challenge.

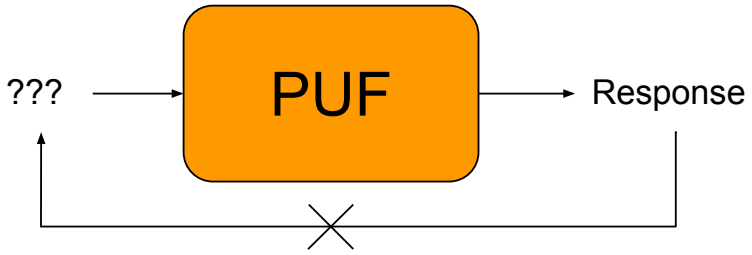


Figure 2.3 One-wayness: it is impossible to find a challenge corresponding to a given response.

Tamper Evidence

Tampering with devices in order to compromise their integrity has proven to be a successful technique. For example, invasive attacks (such as microprobing) are able to extract sensitive data from the target system.[7]

Tamper evidence helps to mitigate such attack vectors. The PUF must detect the attempt to tamper with the system and change its challenge-response pairs to a different set as if the PUF instance transforms itself to a completely different one.

To achieve this property, the PUF implementation needs to rely on physical properties that will necessarily change if the device is tampered with. This change will inherently transform the PUF.

2.3 PUF classification

A lot of different PUF implementations have been proposed. They can be classified based on fabrication, security and intrinsic evaluation[8][9]. A diagram of the discussed PUF classes is depicted in Figure 2.4.

2.3.1 Electronic, silicon and hybrid PUFs

Electronic PUFs source their randomness from electronic components. This means that they rely on properties such as capacitance, resistance or propagation delay of a circuit.

A large subclass of electronic PUFs is silicon PUFs. They can be constructed only using complementary metal–oxide–semiconductor (CMOS) technology, therefore they can be implemented on the same die together with the main chip. This prevents the need to interface with additional circuitry using external buses, lowering cost and limiting the possibility of leaking sensitive data.[1]

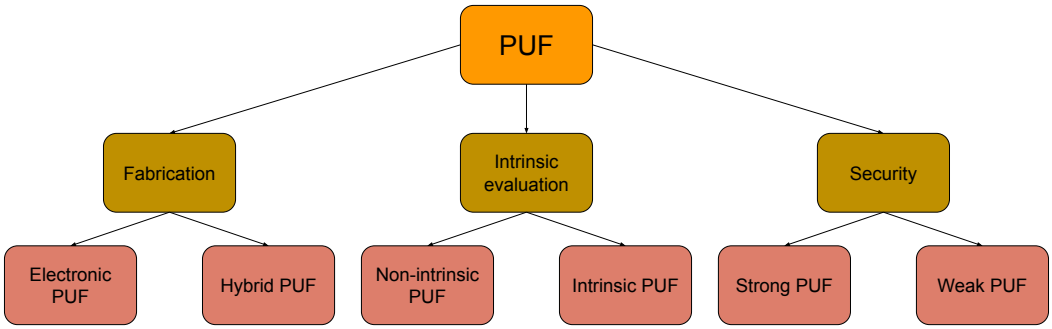


Figure 2.4 Classification of PUFs.

Examples of electronic PUFs are SRAM PUF, ring oscillator physical unclonable function (ROPUF) or arbiter PUF.

Hybrid PUFs use non-electronic phenomena to create their challenge-response pairs. While randomness introduced into the system is of non-electronic nature, the signal is usually processed and stored using electronic components. Hence the name hybrid PUFs. They can be based on optics (optical PUF), magnetism (magnetic PUF) or quantum effects (quantum PUF[10]).

2.3.2 Intrinsic and non-intrinsic PUFs

A PUF implementation is said to be intrinsic if it satisfies the following two conditions[11]:

1. responses are evaluated internally
2. instance-specific random features are introduced implicitly during the manufacturing process

Internal evaluation requires the measurement equipment of the PUF to be embedded in the device. This, similar to silicon PUFs, lowers cost and is more secure.

The second condition discusses the introduction of randomness into the system. Implicit randomness relies on process variations taking place during normal manufacturing, while explicit randomness needs to be created by special procedures which would have not been needed otherwise (such as doping with random dielectric particles for the construction of a coating PUF[12]).

SRAM and arbiter PUFs are examples of intrinsic PUFs. If the PUF construction does not satisfy the given properties, it is called non-intrinsic. For example, optical or coating PUFs are non-intrinsic.[5]

2.3.3 Strong and weak PUFs

Security based classification distinguishes PUF implementations according to the size of their challenge-response pair sets.

In order for a PUF to be classified as strong, its challenge-response pair set needs to be sufficiently large to prevent an exhaustive search by a possible attacker. The challenge-response pair size thus scales well (preferably exponentially) with some construction parameter.[13]

On the other hand, weak PUFs have only a limited set of challenge-response pairs. Some PUFs can only have one pair. They are sometimes called physically obfuscated key (POK).

As the naming implies, strong PUF constructions possess, in some sense, greater security. Weak PUFs cannot be mathematically unclonable (and consequently cannot be truly unclonable

or unpredictable). Strong PUFs can also be used in more applications, as explained in Section 2.5. However, it turns out that constructing a strong PUF is a very hard problem.[1]

2.4 PUF evaluation parameters

As PUFs rely on uncontrollable physical processes to produce their responses, it is crucial to perform an analysis of their quality. Several evaluation parameters were defined by [14], [15] and [16] and they will be discussed here.

These parameters enable us to quantify the performance of PUFs and compare them. Some of them will be used to evaluate the SRAM PUF implemented in this thesis in Sections 5.1.3 and 5.2.3.

The following evaluation parameters will be defined:

- Uniformity
- Reliability
- Uniqueness
- Bit-aliasing
- Randomness

Before the parameters can be defined, a notation used in the upcoming text is described here and in Table 2.1 to avoid possible confusion.

The Hamming weight $\mathrm{HW}(x)$ of a bit string x is defined as the number of one bits in the string.

The Hamming distance $\mathrm{HD}(x, y)$ of two bit strings x and y is defined as a number of positions where the bits of x and y differ.

The reference response $R_i^{'}(n)$ is the expected response of n bits produced by the chip i. It is usually computed as a bitwise average between m response samples taken in normal operating conditions. However, some works choose the reference response as the first measured sample.[4]

Notation	Description
k	The number of devices
m	The number of response samples
n	The number of bits in a response
$R_{i,j}(n)$	The j-th response (containing n bits) of i-th chip
$R_i^{'}(n)$	The reference response of i-th chip, containing n bits
$r_{i,j}^{'}$	The j-th bit of a reference response of chip i
$\mathrm{HW}(x)$	The Hamming weight of x
$\mathrm{HD}(x, y)$	The Hamming distance between x and y

Table 2.1 Notation used in evaluation parameters definitions.

2.4.1 Uniformity

Uniformity represents a proportion of zero and one states of the response bits. It is useful to determine if there exists a global bias towards any of these states. Since the PUF responses need to be unpredictable, there should not be any bias. Thus, the ideal value of uniformity is 50%.

The uniformity property for one response of chip i is defined by Equation 2.1:

$$U_i = \frac{1}{n}\sum_{j=1}^{n} r_{i,j}^{'} = \frac{\mathrm{HW}(R_i^{'}(n))}{n} \cdot 100\% \tag{2.1}$$

Uniformity can also be calculated as an average value between k PUF instances of the same type by Equation 2.2[16]:

$$U_{\mathrm{avg}} = \frac{1}{k}\sum_{i=1}^{k} U_i = \frac{1}{k}\sum_{i=1}^{k} \frac{\mathrm{HW}(R_i^{'}(n))}{n} \cdot 100\% \tag{2.2}$$

Since uniformity only measures a global proportion of the response bit states, it is not a perfect tool to detect a possible local bias. A trivial example could be a response defined in the following way:

$$r_{i,j}^{'} = \begin{cases} 1 & \text{if } j < \frac{m}{2} \\ 0 & \text{otherwise} \end{cases} \tag{2.3}$$

That is the first half of the response bits are ones and the second half are all zero bits. Uniformity U_i for such a response is close to the ideal value of 50% though the response is clearly not unpredictable.

2.4.2 Reliability

Reliability is a parameter that measures the consistency of PUF responses to the same challenge. It is tied to the reproducibility property from Section 2.2.

In order to calculate reliability, the intra-Hamming distance for a chip i needs to be defined first[16]:

$$\text{HD-intra}_i = \frac{1}{m}\sum_{j=1}^{m} \frac{\mathrm{HD}(R_{i,j}(n), R_i^{'}(n))}{n} \cdot 100\% \tag{2.4}$$

The reference $R_i^{'}(n)$ is obtained at nominal operating conditions (room temperature and normal voltage). The responses $R_{i,j}(n)$ are then taken at different conditions and the result is calculated. It essentially represents the percentage of bits that change compared to the reference response.

Reliability is then defined by Equation 2.5:

$$\text{Reliability} = 100\% - \text{HD-intra} \tag{2.5}$$

Since the reproducibility property requires PUFs to produce similar responses to the same challenge, the ideal HD-intra_i value is 0% and thus reliability needs to be close to 100%.

2.4.3 Uniqueness

Uniqueness measures how much responses from different PUFs vary. It is estimated by the inter-Hamming distance defined by Equation 2.6:

$$\text{HD-inter} = \frac{2}{k(k-1)}\sum_{i=i}^{k-1}\sum_{j=i+1}^{k} \frac{\mathrm{HD}(R_i^{'}(n), R_j^{'}(n))}{n} \cdot 100\% \tag{2.6}$$

The original definition of HD-inter by [17] does not specify how to choose the responses to calculate the Hamming distance from. However, [4] uses the reference responses and this definition will be used in future calculations in this thesis.

The inter-Hamming distance takes all combinations of pairs of devices and computes the average Hamming distance of their responses. The uniqueness property of PUFs in Section 2.2 requires that the responses should differ as much as possible. This is achieved when HD-inter is close to its ideal value of 50%.

2.4.4 Bit-aliasing

Uniformity in Section 2.4.1 looks at the global bias of PUF responses from a single device. On the other hand, bit-aliasing measures the proportion of zero and one state of a single bit across different devices.

Bit-aliasing is calculated as the percentage Hamming weight of the j-th bit. It is defined by Equation 2.7[16]:

$$\text{Bit-aliasing}_j = \frac{1}{k}\sum_{i=1}^{k} r'_{i,j} \cdot 100\% \tag{2.7}$$

Same as for uniformity, the ideal value for bit-aliasing is 50%. Values close to 0 or 100% would indicate bits that stay the same across different PUF instances, violating the uniqueness property.

2.4.5 Randomness

As PUF responses need to be unpredictable, they are required to contain sufficient entropy. According to [15], there are several ways to test whether the response data is sufficiently random. Two are described here, the compression test and the NIST randomness test.

NIST randomness test

The NIST randomness test uses the NIST statistical test suite to determine if the data is sufficiently random. Each test from the battery is tested for the null hypothesis that the response data is truly random on some set significance level.

Furthermore, each test is executed multiple times on different sequences of the data and a p-value for each run is calculated. These p-values are then tested for the null hypothesis that they are from a uniform distribution, as would be the case for truly random data.[18]

However, not all tests can be used as they require more input data than is practically possible to generate by the PUF. Tests for which only 170-bit string suffices are listed here[15]:

- Frequency (monobit) test
- Frequency test within a block
- Runs test
- Test for longest run of ones in block
- Serial test
- Approximate entropy test
- Cumulative sums (Cusum) test

Compression test

The idea behind compression test is simple. If a lossless compression algorithm is able to reduce the size of the tested data, it does not have full entropy[1][15].

[1] Meaning the entropy in bits is the same as the length of the data in bits.

A good example of a compression algorithm to use is the context-tree weighting (CTW) algorithm as it was shown to produce the best results out of the commonly used entropy estimators[19].

2.5 PUF applications

Thanks to the properties described in Section 2.2, PUFs are suitable for several cryptographic applications. Three main uses of PUFs according to [5] will be described here: identification, authentication and cryptographic key generation.

2.5.1 Identification

A PUF can be compared to a device's fingerprint. The PUF provides an inherent identifying feature[2] to the entity encapsulating it. Therefore, device identification is a natural application for PUFs. A simple identification protocol using the device's PUF is described.

The process of device identification consists of two phases: enrollment and identification[5].

Enrollment phase:
In this phase, the inherent identifying feature of every considered device is collected. This means saving a PUF response from each device to a database.

Identification phase:
When the device needs to be identified, it generates its PUF response. The response is then compared to other responses stored in the database.

However, the comparison of the presented PUF response is not straightforward. Since the PUF relies on a physical state of the system, errors can arise while generating responses. For this reason, the comparison is based on the Hamming distance (HD) rather than on equality.

The property of identifiability (discussed in Section 2.2) tells us that responses from a specific device will be similar (have low HD) and responses from different devices will be far apart (have high HD). Thus, a threshold value of HD needs to be chosen. Responses with lower HD than the threshold will be considered to have originated from the same device.

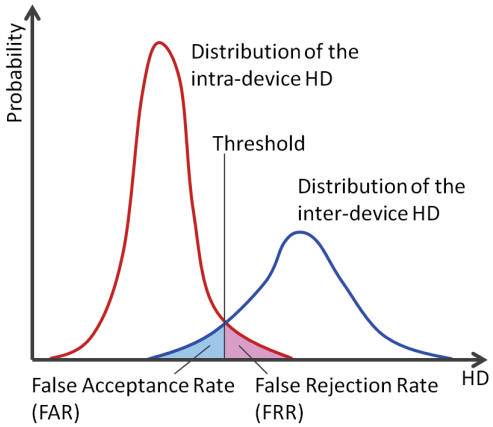


Figure 2.5 PUF identification: intra and inter HD distributions[20].

[2]Inherent identity is a unique characteristic of the device itself (a PUF response), while assigned identity is an artificially made up property (a serial number).

The threshold can be chosen based on the distributions of inter and intra HDs. While the inter-HD is a measure of how responses from different devices differ, the intra-HD indicates the similarity of responses from the same device.

If the distributions of inter and intra HDs do not overlap, the threshold value between the distributions is optimal. The false acceptance rate (FAR) (the probability of falsely identifying a device) and false rejection rate (FRR) (the probability of falsely rejecting a device) are zero.

If the distributions overlap, a compromise between FAR and FRR must be made. Reducing FAR will inevitably increase FRR and vice versa. Figure 2.5 illustrates possible intra and inter HD distributions and a chosen threshold.

2.5.2 Authentication

Authentication requires the entity, which wants to authenticate itself to a verifier, to provide proof of its identity. The entity also needs to convince the verifier that it actively participated in the creation of the proof.[5]

A simple protocol based on the challenge-response pairs of PUFs will be presented here. It is divided into two distinct phases: enrollment and authentication.[21]

Enrollment phase:

During this phase, a trusted third party (the verifier) is in possession of the device which will later be authenticated. A sufficient number of randomly generated challenges along with the corresponding responses (obtained from the device) is saved to a database.

Authentication phase:

When the device needs to be authenticated, the verifier chooses a challenge from the database and sends it to the device. The device then responds with the corresponding response. Finally, the obtained and the previously recorded responses are compared. If they are sufficiently similar, the device is authenticated successfully. This challenge-response pair is then deleted from the database and never used again.

The whole process of this PUF-based authentication protocol is illustrated in Figure 2.6.

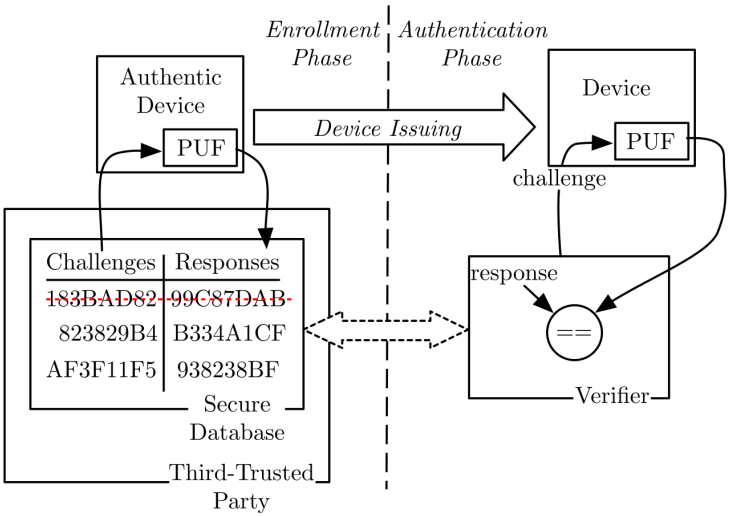


Figure 2.6 PUF-based authentication protocol[22].

The comparison of the responses is done in the same way as in PUF-based identification (Section 2.5.1). The HD is used as a distance metric and a threshold for accepting the response must be chosen appropriately.

The challenge-response pairs are deleted from the database and never reused to prevent a potential man-in-the-middle attack. Since this is not a threat, the communication between the device and the verifier does not need to be secured.

This protocol is simple and has its drawbacks. It only provides a limited number of authentications for the verifier given by the number of stored challenge-response pairs. The authentication is only one-way, the verifier is never authenticated to the device. It requires the PUF to be strong (to have a large number of available challenge-response pairs).

More advanced PUF-based authentication protocols that address some of the aforementioned drawbacks have been developed by [1], [22] and [23].

2.5.3 Key generation

Keys are required in the majority of cryptographic applications. They need to contain true randomness in order to be unpredictable and unique. The cryptographic key then needs to be stored and retrieved securely. These conditions are hard to meet and a myriad of cryptographic systems have been broken because of bad generation or handling of keys.[24]

PUF-based cryptographic key generation tries to solve those problems. The key is not stored in any memory and is generated by the PUF on demand. In some way, it is imprinted in the PUF itself. Furthermore, the uniqueness and unpredictability property of PUFs, which arise from their uncontrollable physical properties, introduce the necessary randomness.

Since the PUF responses are noisy and not 100% reliable, care needs to be taken while generating cryptographic keys. The keys need to be the same every time, otherwise the cryptographic algorithms using it would not produce the desired output. For this reason, ECCs are used to obtain the same key every time with sufficient probability.

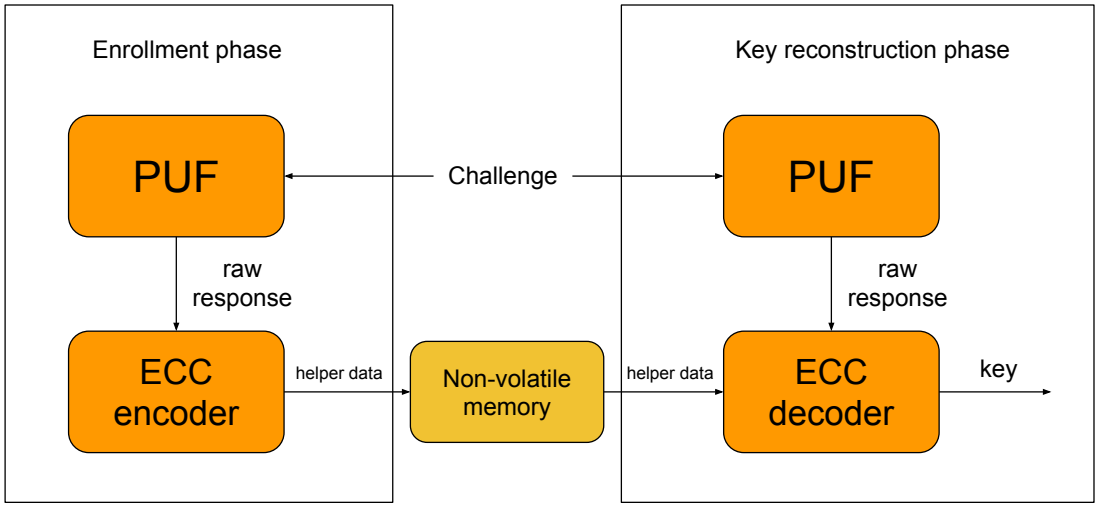


Figure 2.7 PUF-based key generation mechanism, inspired by [25].

The process of PUF-based key generation is divided into two phases: enrollment and key reconstruction[14]. It is illustrated in Figure 2.7.

Enrollment phase:

In this phase, PUF responses are generated and processed by the ECC algorithm to construct the cryptographic key. The ECC calculates helper data from the key and saves it to non-volatile memory. This data will later be used to reconstruct the key. The helper data can also contain a PUF configuration.

Key regeneration phase:
When the key is needed, the PUF produces a response and feeds it to the ECC algorithm. The key is then reconstructed by the ECC using the response and the corresponding helper data saved in the non-volatile memory.

The ECC used is usually a simple repetition code or a Bose–Chaudhuri–Hocquenghem (BCH) code. However, any ECC can be used and the codes can even be concatenated in order to increase efficiency.[26]

After key regeneration, a raw bit string key is obtained. It can be used immediately with some cryptosystems (typically symmetric ciphers such as AES). However, some systems put restrictions on the key (RSA needs two prime numbers), thus requiring further processing.

Key generation is a typical application of weak PUFs[27]. As the SRAM PUF implemented in this thesis is classified as weak, a simple key generation algorithm will be tested on top of the PUF.

It is even possible for a weak PUF to provide authentication without the need for a large number of challenge-response pairs. Once the key is generated by the weak PUF, it can be used in other cryptographic algorithms which provide authentication such as message authentication code (MAC) or digital signatures (at the cost of additional hardware/software).[27]

2.6 PUF implementations

A large number of various PUF implementations have been proposed. Four examples of these implementations have been chosen and a brief description of how they operate will be provided. This section will describe an optical PUF, an arbiter PUF, a coating PUF and a SRAM PUF. Focus will be given to the description of SRAM PUF (it will be given its own chapter), as it will be implemented in this thesis on the ESP32 microcontroller.

2.6.1 Optical PUF

A design of optical PUF was first proposed by [2] in 2001 and was called a physical one-way function.

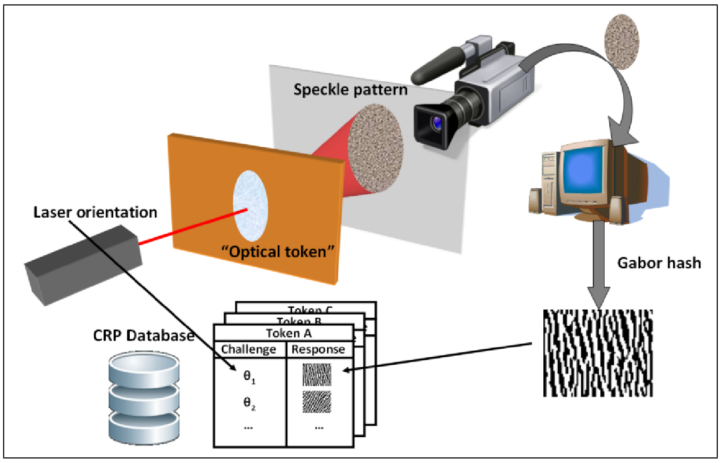


Figure 2.8 Operation of the optical PUF.

The heart of the PUF is an optical token that contains microscopic refractive particles randomly mixed in a transparent epoxy plate. This optical microstructure is then irradiated with

a laser which produces a random speckle pattern. This pattern is captured using a camera and digitally processed by an algorithm called Gabor hashing. The resulting hash works as the PUF response. Challenge is represented as a specific orientation of the laser. The operation of optical PUF is represented in Figure 2.8.

Experiments showed, that this optical PUF has the one-wayness property and the optical tokens are tamper evident.[28] Together with the fact that it is classified as strong (has a large number of challenge-response pairs) makes this PUF construction the only one with these properties. However, it is also expensive and laborious to use because of its rather large and mechanical setup.[5]

A more integrated implementation of an optical PUF was proposed by [29].

2.6.2 Arbiter PUF

The arbiter PUF was first proposed by [30]. It is a delay-based silicon PUF implementation. The idea behind this construction is to create a race condition for two digital signal paths which end in an arbiter circuit. The arbiter determines which of the two digital lines finished the race first and outputs a bit.

If the two paths have an identically designed delay in the chip, the two following cases can happen[1]:

1. The delay for one of the paths is shorter due to the manufacturing variations and the arbiter circuit will decide the race accordingly. This effect is the basis of the arbiter PUF since the variations are random for every device and stay static after fabrication of the circuit.

2. By chance, the two paths have a nearly identical delay. The arbiter circuit then enters a metastable state and its output is essentially random. This randomness is however not device-specific and is the source of unreliability of the PUF.

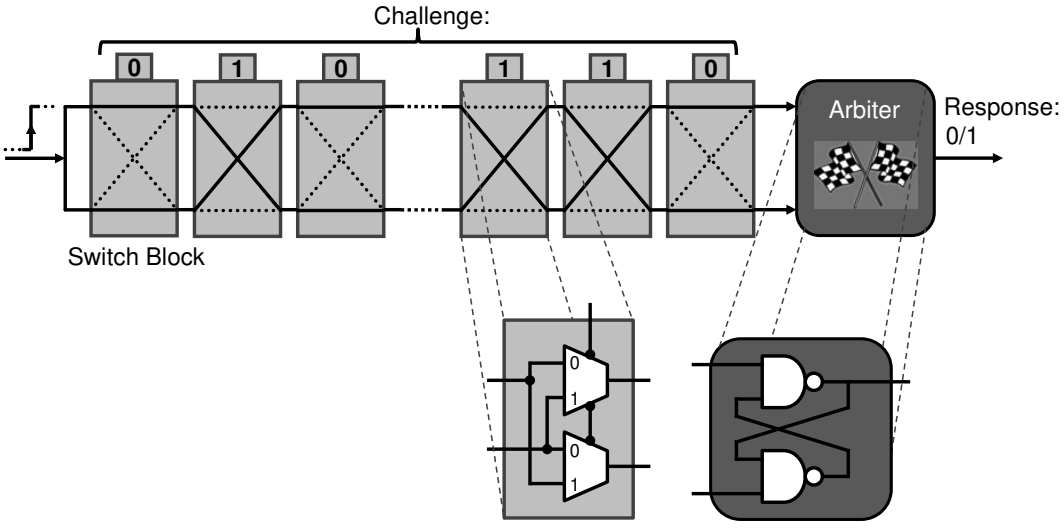


Figure 2.9 Construction of an arbiter PUF as proposed by [30], image from [5].

The initial design of the arbiter PUF by [30] used serially connected switch boxes to implement the two delay paths. A switch box connects two inputs to two output lines based on a parameter bit. The connection is either straight or switched, creating a configurable delay for the two paths.

Connecting n switch boxes results in 2^n possible delay configurations. These configuration bits are then considered to be the challenge of the PUF. The schematic of the described arbiter PUF is shown in Figure 2.9.

However, the 2^n possible challenges are not unpredictable with this design. The final delay of the path is the sum of delays on each switch box. This fact makes it possible to create a highly accurate mathematical model of the PUF while only observing a limited amount of challenge-response pairs.[30]

In order to prevent the model building attacks, extensions to the original design were proposed by introducing non-linear features. One example is a feed-forward arbiter PUF, where some of the configuration bits are set by evaluating the race at an intermediate point of the path rather than by the challenge.[31]

2.6.3 Coating PUF

The design of a coating PUF was first proposed by [32]. It gathers its randomness from measuring the capacitance by comb-shaped sensors placed in the top metal layer of an integrated circuit. The randomness is introduced into the system by spraying a passive dielectric coating on top of the sensors. The need for a special step during manufacturing to create the coating classifies this PUF construction as non-intrinsic (it breaks the second necessary condition of intrinsic PUFs as discussed in Section 2.3.2).[11]

Construction of a coating PUF is illustrated in Figure 2.10.

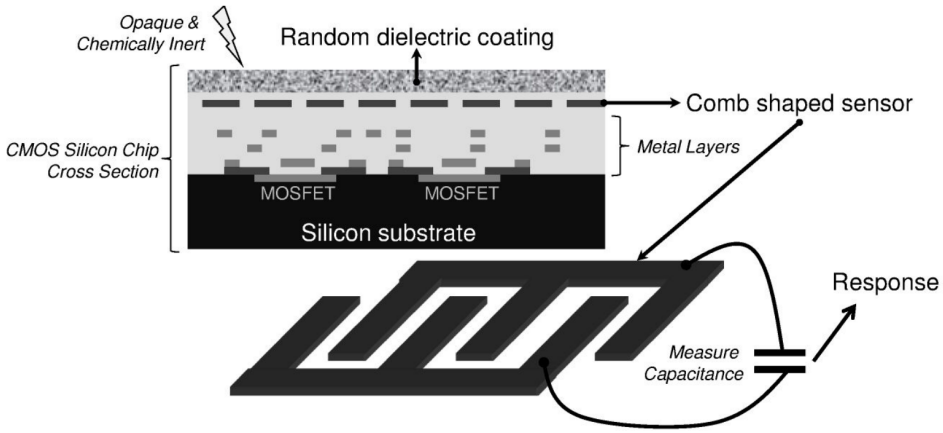


Figure 2.10 Construction of a coating PUF [5].

As the coating is inert and opaque, it provides strong protection against physical attacks. It has also been shown that the resulting PUF is tamper evident.[32]

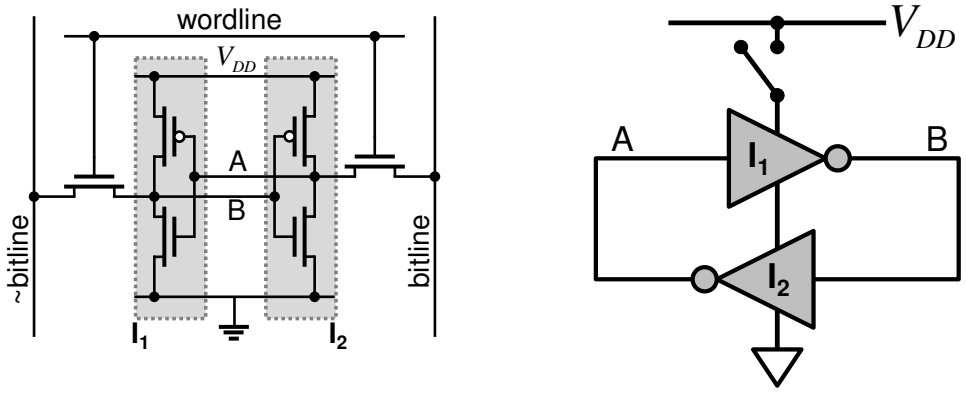
Chapter 3

SRAM PUF

SRAM PUF is based on a random startup behaviour of individual SRAM cells. It was first proposed by [13] in 2007.

In a CMOS implementation (which is used to create 99% of integrated circuits as of 2011[33]) a SRAM cell is usually made up of two cross-coupled inverters. The inverters reinforce each other of their state, thus creating a bistable circuit—a circuit with only two stable states. This enables the cell to save exactly one logical bit. Each inverter is implemented using two transistors and additional two transistors are used to enable read and write operations. This means that storage of a single bit costs six transistors in hardware.[11]

The logical diagram of a SRAM cell containing the two inverters is illustrated in Figure 3.1b and a diagram with the transistor layout of the cell is shown in Figure 3.1a.



(a) A CMOS diagram of a SRAM cell.

(b) A logic circuit diagram of a SRAM cell.

Figure 3.1 CMOS and logic circuit diagrams of a SRAM cell.[5]

The principle of a SRAM PUF is based on the power-up values of the memory cells. The memory cells are volatile—when power is lost, the data disappears from memory. After startup, each cell has to initialize to either a '1' or a '0' state. Which state the cell stabilizes on is dependent

on a relative strength[1] of the two inverters. Since the inverters are designed identically, their strength is determined by random process variations during manufacturing.[11]

For each cell independently, the two following cases can happen:

1. One of the inverters has far greater strength than the other. The cell has a significant preference for one initial state. Meaning it will either be in the '0' or the '1' state most of the time after power-up. This case is crucial for the PUF construction.
2. By chance, strengths of the two inverters are nearly identical. The resulting initial state depends on random noise in the circuit. This is the source of unreliability of the PUF.

During fabrication, each cell acquires its specific properties and thus its startup state stability according to the cases mentioned above. However, stability is not a discrete property. One cell can be less stable than some other. An illustration of this can be seen in Figure 3.2.

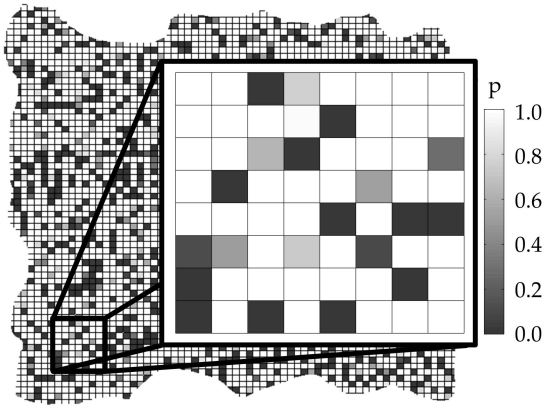


Figure 3.2 Illustration of SRAM cell stability. A small area of SRAM cells is shown. The lightness of each cell indicates the probability that the cell's startup state will be '1'. Note that most of the cells are either nearly black or nearly white. Meaning they are stable and their preferred state is '0' or '1' respectively. [34].

It turns out, that the process variations are significant enough that most SRAM cells tend to be stable. This enables the startup values of memory to be used as PUF responses. Challenge can be interpreted as a concrete address in memory. The response is then read from this address.[1]

For the construction of a SRAM PUF, stable cells are important. The unstable ones can be considered harmful as they decrease reliability. However, thanks to their unknown initial state which is determined randomly after every startup, they are useful for the construction of true random number generators (TRNGs).[34]

A huge advantage of SRAM PUFs is, that SRAM memory is usually already present in chips. If the device possesses a suitable mechanism of power state control of its memory (the ability to turn off blocks of memory, power-saving states that turn off memory), no additional hardware is needed. Therefore this type of PUF could potentially be implemented in devices that were not designed to contain a PUF at all.

3.1 SRAM PUF and its properties

PUFs constructions can be characterized by several properties. They have been discussed in Section 2.2. However, not every PUF needs to exhibit all of them. Therefore a discussion about

[1] strength here means the properties of the underlying metal–oxide–semiconductor field-effect transistor (MOSFET) transistors (such as delay)

what particular properties a SRAM PUF meets is provided according to [1]. The summary of properties of SRAM PUF can be found in Table 3.1.

Property	SRAM PUF
Constructibility	yes
Evaluability	yes
Reproducibility	yes
Uniqueness	yes
Identifiability	yes
Physical Unclonability	yes
Unpredictability	yes
Mathematical unclonability	no
True unclonability	no
One-Wayness	no
Tamper evidence	probably no

Table 3.1 Summarization of properties of SRAM PUF.

Constructibility:
Since known implementations of SRAM PUF exist (and one is provided in this thesis), it is definitely constructible. Furthermore, the effort needed to construct the PUF is low compared to the other implementations—SRAM memory is usually already present in chips and no additional hardware is needed.

Evaluability:
SRAM PUF is evaluable because it is possible to read the startup values of the SRAM cells which are interpreted as the response. However, the effort to obtain the response can be rather high since the memory needs to be read fresh after power up (before the response is overwritten by other data). Depending on the device used and its capabilities, this could potentially require procedures that take a long time (for example rebooting the device or using a power-saving state to turn off the SRAM memory). Additional hardware could mitigate this problem, increasing manufacturing costs.

Reproducibility:
The SRAM PUF possesses the reproducibility property because memory cells have a preference for some initial state. This preference is imprinted on the cell at the time of manufacturing and does not change much afterwards (however, SRAM aging effect can alter the preference of a cell over time and this is discussed later in this section).

Uniqueness:
SRAM PUFs are unique, as each memory cell creates its preference for some initial state during manufacturing independently. For this reason, the resulting PUF responses from different devices should not be similar.

Identifiability:
As identifiability is the combination of reproducibility and uniqueness, both of which are already met, the SRAM PUF is identifiable as well. This means that the intra-HD and inter-HD distributions are sufficiently separated and the responses can be used to identify devices.

Physical unclonability:
The source of randomness of SRAM PUFs is the physical variation of individual transistors that implement the memory cells. These variations take place on a micro/nano scale and are technically infeasible to control fully. Even the manufacturer is unable to create two

SRAM memory instances with similar cell startup state preferences. Thus this construction is considered physically unclonable.

Unpredictability:
Unpredictability assumes, that given a limited set of challenge-response pairs, no prediction algorithm can be designed for future challenges. Responses are interpreted as memory addresses and each cell should acquire its preference for some initial state independently. Therefore the knowledge of a challenge-response pair does not reveal any information about other pairs. For this reason, SRAM PUFs are unpredictable.

Mathematical unclonability:
Mathematical unclonability is a stronger model of unpredictability. It assumes having access to as many challenge-response pairs as can be stored. Since SRAM PUFs have only a limited number of those pairs (only one in the extreme case), a simple lookup table with all the possible pairs can be constructed easily. Thus, the property of mathematical unclonability is not met.

True unclonability:
A PUF is truly unclonable if it is physically and mathematically unclonable. Therefore, by definition, SRAM PUF is not truly unclonable since it is not mathematically unclonable.

One-wayness:
One-wayness (similar to mathematical unclonability) requires the PUF to have a sufficiently large challenge and response sets. Because SRAM PUFs are weak, they are not one-way.

Tamper evidence:
Not enough research has been conducted to declare whether SRAM PUFs are tamper evident or not[5]. However, it has been shown that it is possible to strip the device of most unrelated silicon without changing the PUF response significantly[35]. Additionally, [36] showed that it is possible to extract full PUF responses from AVR microcontrollers[2] by disabling the logic core and using a semi-invasive laser probing technique to read the startup memory values.

3.2 Stable response extraction

Since SRAM PUFs are weak, they are usually used for key generation. The resulting key must be the same every time it is reconstructed. Therefore, stability of the response needs to be guaranteed. Several methods that increase stability exist: temporal majority voting (TMV), ECC, direct bit preselection and indirect bit preselection.[37]

Temporal majority voting

TMV samples the PUF response multiple times and the resulting response is based on bitwise majority vote of the samples. This increases the time it takes to obtain the response significantly. Additionally, if a cell is very unstable, the majority vote for it could be very close and thus not stable.

Error correction codes

ECC correct the errors in the response, thus increasing stability. However, they need to store helper data in non-volatile memory to function, decrease response length and have computational

[2] the experiment was conducted on an ATMega328P and an ATXMega128A1 models

overhead. A simple repetition ECC is used in the SRAM PUF implementation in this thesis and details will be discussed in Section 6.2.

Direct bit preselection

Stable bit preselection methods try to indicate which bits are stable and they create a mask of stable bits. This mask is saved to a non-volatile memory of the device and is later used to ignore the unstable bits during response extraction.

In direct preselection, the PUF response is first measured multiple times. Stable bits are identified based on their average startup value over multiple measurements. To identify more stable bits, measurements can be made across different operating temperatures and supply voltages. However, this is a very time consuming technique. An example of average startup SRAM cells can be seen in Figure 3.3.

Figure 3.3 Average startup values of individual SRAM cells over 1000 measurements. White bits are stable '1', black are stable '0' and the rest are unstable bits with varying amounts of instability (according to the color bar on the right). Cells with average value of 0.5 are the least stable. The data was obtained from ESP32 number 12 in 20°C.

Indirect bit preselection

Indirect preselection runs a test for each bit to identify its stability. For example, stable bit can be identified by the time it takes for it to stabilize its initial state—stable bits stabilize faster than the unstable ones. The test can be performed in the following way.

First, set all the bits to the '0' state. Then, turn off the memory for a short amount of time and look at which bits flipped to the '1' state the fastest. They are the stable '1' bits. Stable '0' bits can be obtained respectively. It has been shown by [38] that up to 100% stable response can be extracted by this method.

3.3 SRAM aging

Normal operation of SRAM memory unavoidably alters its physical properties. These processes can effect the stability of SRAM PUF and are called silicon aging.

The dominant effect which directly alters the stability of memory cells is called negative-bias temperature instability (NBTI). NBTI is a data-dependent aging effect. If the cell stores a '1' bit, its startup state preference slowly starts to change towards the '0' state. This is the result of a threshold voltage increase on the transistors which are switched on in the currect state, whereas the swithed off transistors are unaffected. This means, that the SRAM PUF has a natural tendency to become less stable over time if the startup data is left unchanged in memory.[39]

Anti-aging techniques, which try to counteract NBTI and other effects, exist. A simple example is to store an inverse of the startup data after response extraction. However, this is a security risk as leakage of this data would directly reveal the startup memory values. Another solution could be to overwrite the memory with a random string after every power up. This results in less effective anti-aging, but avoids the security risk of a data leak.[40]

Chapter 4
ESP32 platform

In this chapter, a brief explanation of the ESP32 platform is presented. The main hardware and software features of the ESP32 microcontroller, which is used in this thesis, are described. The information provided is mainly based on the official ESP-IDF (the official development framework)[41] and the ESP32 Technical reference manual[42].

4.1 Hardware

ESP32 is a system on a chip (SoC) microcontroller designed by Espressif which integrates CPUs, WiFi, Bluetooth and various specialized co-processors. The main features of the ESP32 are following:

- Xtensa dual-core 32-bit LX6 microprocessor running at 160 or 260 MHz
- 520 KB SRAM, 448 KB ROM
- 8 KB FAST RTC SRAM and 8 KB SLOW RTC SRAM
- Wi-Fi: 802.11 b/g/n
- Bluetooth: v4.2 and BLE
- Cryptographic co-processors: RNG, RSA, SHA, AES
- Ultra low power (ULP) co-processor

One possible form factor of the ESP32 microcontroller can be seen in Figure 4.1. A block diagram of ESP32 functions is illustrated in Figure 4.2.

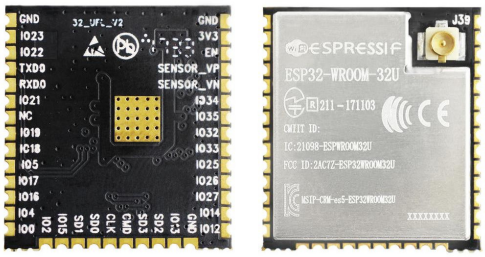


Figure 4.1 The ESP32-WROOM-32U module back and front image.[43]

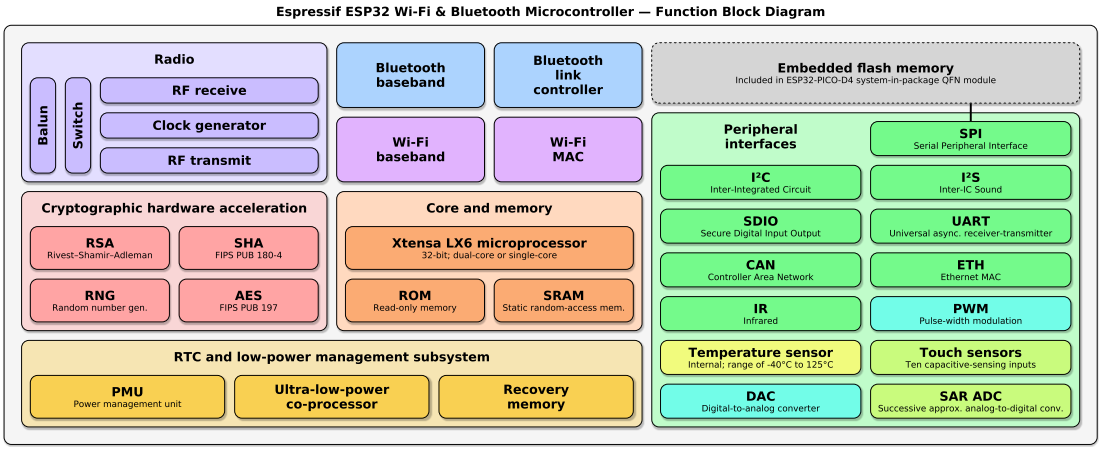


Figure 4.2 ESP32 Chip Function Block Diagram.[44]

ESP32 is a name for the original microcontroller from Espressif released in 2016. However, several other models have been developed since[41]:

ESP32-S2 A single core version of the ESP32

ESP32-S3 Version with added instructions to accelerate machine learning

ESP32-C3 Single core RISV-V CPU version instead of the Xtensa LX6 CPU

ESP32-S6 Single core RISC-V CPU with WiFi 6 support

Only the original ESP32 microcontroller was used during experiments and implementation in this thesis. However, the possibility of implementing a SRAM PUF on the other versions is discussed later in Chapter 5.

4.2 Memory layout

Memory layout of the ESP32 is important for a SRAM PUF implementation as the exact memory region used to extract the response needs to be considered. The ESP32 has several types of embedded memories and they are discussed here briefly. A detailed description of embedded memory adress mapping can be seen in Table 4.1. The ESP32 uses a Harvard memory architecture. This means, that instructions and data use separate memories with dedicated buses.[42]

ROM 0 and 1
Read only memory (ROM) is used by the hard-coded first-stage bootloader for instructions (ROM 0) and static data (ROM 1).

SRAM 0, 1 and 2
SRAM 0 is used for program instruction. SRAM 1 is mapped to both instruction and data bus simultaneously. It can also be mapped over part of ROM 0. SRAM 2 is used for program data.

FAST RTC SRAM FAST real-time clock (RTC) SRAM is mapped to both instruction and data bus and is not turned off during power-saving modes (such as deep or light sleep). It is therefore used to keep data between the power-saving modes. Only the PRO_CPU[1] can use this memory.

[1]The two CPU cores are named PRO_CPU and APP_CPU

SLOW RTC SRAM The SLOW RTC SRAM is mapped to a region shared by both the instruction and data buses. It is clocked slower compared to the other SRAM memories. It is not turned off during power-saving modes and can be used to keep data between them. The ULP co-processor also uses it as its memory.

Flash memory can either be embedded inside the SoC or connected externally using Serial Peripheral Interface (SPI). Maximum of 16 MB of flash is supported and up to 8 MB of external SRAM can also be connected using SPI.

Bus Type	Boundary Address		Size	Target	Comment
	Low Address	High Address			
Data	0x3FF8_0000	0x3FF8_1FFF	8 KB	RTC FAST Memory	PRO_CPU Only
	0x3FF8_2000	0x3FF8_FFFF	56 KB	Reserved	-
Data	0x3FF9_0000	0x3FF9_FFFF	64 KB	Internal ROM 1	-
	0x3FFA_0000	0x3FFA_DFFF	56 KB	Reserved	-
Data	0x3FFA_E000	0x3FFD_FFFF	200 KB	Internal SRAM 2	DMA
Data	0x3FFE_0000	0x3FFF_FFFF	128 KB	Internal SRAM 1	DMA
Bus Type	Boundary Address		Size	Target	Comment
	Low Address	High Address			
Instruction	0x4000_0000	0x4000_7FFF	32 KB	Internal ROM 0	Remap
Instruction	0x4000_8000	0x4005_FFFF	352 KB	Internal ROM 0	-
	0x4006_0000	0x4006_FFFF	64 KB	Reserved	-
Instruction	0x4007_0000	0x4007_FFFF	64 KB	Internal SRAM 0	Cache
Instruction	0x4008_0000	0x4009_FFFF	128 KB	Internal SRAM 0	-
Instruction	0x400A_0000	0x400A_FFFF	64 KB	Internal SRAM 1	-
Instruction	0x400B_0000	0x400B_7FFF	32 KB	Internal SRAM 1	Remap
Instruction	0x400B_8000	0x400B_FFFF	32 KB	Internal SRAM 1	-
Instruction	0x400C_0000	0x400C_1FFF	8 KB	RTC FAST Memory	PRO_CPU Only
Bus Type	Boundary Address		Size	Target	Comment
	Low Address	High Address			
Data Instruction	0x5000_0000	0x5000_1FFF	8 KB	RTC SLOW Memory	-

Table 4.1 ESP32 embedded memory address mapping.[42]

4.3 Device startup

There are several steps involved between power-up and start of the user application. It is important to understand them as some will be crucial to the implementation of the SRAM PUF. The steps are following:

1. The CPU executes the first-stage bootloader located in ROM. If the device was reset from deep sleep, a *deep sleep wake stub* is executed. The second-stage bootloader is then loaded from the flash and executed.

2. The second-stage bootloader loads the partition table from flash. The rest of the application is then loaded according to the partition table. Secure boot, over-the-air updates and flash encryption are also implemented in the second-stage bootloader.

3. C runtime and FreeRTOS are initialized. Finally, the main task of the user application is called and the booting process is complete.

The *deep sleep wake stub* is a mechanism that enables the user to run custom code early in the boot process after wake up from deep sleep. It is implemented as a function stored in the FAST RTC SRAM. This function is then called by the first-stage bootloader before it loads the second stage.[41]

4.4 ESP-IDF

ESP-IDF is an integrated development framework by Espressif. It contains libraries and source code for the ESP32 family of microcontrollers and provides a unified application programming interface (API) which is shared between the different microcontroller models. It also provides scripts for operating the toolchain, uploading applications and monitoring them.[41]

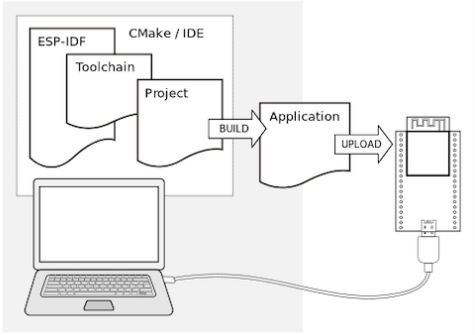


Figure 4.3 Development of applications for ESP32.[41]

4.5 FreeRTOS

A modified version of the real-time operating system (RTOS) FreeRTOS is used in ESP-IDF to create applications. Its main feature is enabling symmetric multiprocessing in order to utilize both CPU cores. Tasks play a role of threads and Wifi, Bluetooth and user tasks can be created and are managed by a real-time scheduler. The FreeRTOS also provides inter-task communication and synchronization API.[41]

Chapter 5

SRAM PUF implementation on ESP32

Chapter 6

Reliable PUF response extraction

Chapter 7

ESP32 SRAM PUF library

Chapter 8

Conclusion

Appendix A
Attachments

Sem přijde to, co nepatří do hlavní části.

Bibliography

1. MAES, Roel. Physically Unclonable Functions: Properties. In: *Physically Unclonable Functions: Constructions, Properties and Applications* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013 [visited on 2022-03-24]. ISBN 978-3-642-41395-7. Available from DOI: 10.1007/978-3-642-41395-7_3.
2. RAVIKANTH, Pappu Srinivasa. *Physical One-Way Functions* [online]. 2001 [visited on 2022-03-23]. Available from: http://alumni.media.mit.edu/~pappu/pdfs/Pappu-PhD-POWF-2001.pdf. PhD thesis. Massachusetts Institute of Technology.
3. GASSEND, Blaise; CLARKE, Dwaine; DIJK, Marten van; DEVADAS, Srinivas. Silicon Physical Random Functions. In: *Proceedings of the 9th ACM Conference on Computer and Communications Security* [online]. Washington, DC, USA: Association for Computing Machinery, 2002 [visited on 2022-03-23]. CCS '02. ISBN 1581136129. Available from DOI: 10.1145/586110.586132.
4. KODÝTEK, Filip. *PUF založený na kruhových oscilátorech pro FPGA* [online]. 2020 [visited on 2022-03-23]. Available from: https://dspace.cvut.cz/handle/10467/94208. PhD thesis. Faculty of Information Technology, Czech Technical University in Prague.
5. MAES, Roel. *Physically Unclonable Functions: Constructions, Properties and Applications (Fysisch onkloonbare functies: constructies, eigenschappen en toepassingen)* [online]. 2012 [visited on 2022-03-24]. Available from: https://lirias.kuleuven.be/retrieve/192818. PhD thesis. Katholieke Universiteit Leuven – Faculty of Engineering.
6. KODÝTEK, Filip. *HW Bezpečnost - Fyzicky neklonovatelné funkce* [online]. Faculty of Information Technology, Czech Technical University in Prague, 2017 [visited on 2022-04-04]. Available from: https://courses.fit.cvut.cz/BI-HWB/@B172/media/lectures/07/prednaska-puf-cz.pdf.
7. KÖMMERLING, Oliver; KUHN, Markus G. Design Principles for Tamper-Resistant Smartcard Processors. In: *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology* [online]. Chicago, Illinois: USENIX Association, 1999 [visited on 2022-03-27]. WOST'99. Available from: https://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf.
8. JOSHI, Shital; MOHANTY, Saraju; KOUGIANOS, Elias. Everything You Wanted to Know about PUFs. *IEEE Potentials* [online]. 2017, vol. 36 [visited on 2022-03-27]. Available from DOI: 10.1109/MPOT.2015.2490261.
9. MCGRATH, Thomas; BAGCI, Ibrahim Ethem; WANG, Zhiming M.; ROEDIG, Utz. A PUF taxonomy. *Applied Physics Reviews* [online]. 2019 [visited on 2022-03-27]. Available from DOI: 10.1063/1.5079407.

10. PHALAK, Koustubh; SAKI, Abdullah Ash-; ALAM, Mahabubul; TOPALOGLU, Rasit Onur; GHOSH, Swaroop. Quantum PUF for Security and Trust in Quantum Computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* [online]. 2021, vol. 11, no. 2, pp. 333–342 [visited on 2022-03-27]. Available from DOI: 10.1109/JETCAS.2021.3077024.

11. MAES, Roel; VERBAUWHEDE, Ingrid. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In: [online]. 2010 [visited on 2022-04-07]. ISBN 978-3-642-14451-6. Available from DOI: 10.1007/978-3-642-14452-3_1.

12. SKORIC, Boris; MAUBACH, Stefan; KEVENAAR, Tam Tom; TUYLS, Pim. Information-theoretic analysis of capacitive physical unclonable functions. *Journal of Applied Physics* [online]. 2006, vol. 100 [visited on 2022-03-27]. Available from DOI: 10.1063/1.2209532.

13. GUAJARDO, Jorge; KUMAR, Sandeep S.; SCHRIJEN, Geert-Jan; TUYLS, Pim. FPGA Intrinsic PUFs and Their Use for IP Protection. In: PAILLIER, Pascal; VERBAUWHEDE, Ingrid (eds.). *Cryptographic Hardware and Embedded Systems - CHES 2007* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 65–68 [visited on 2022-03-28]. ISBN 978-3-540-74735-2. Available from DOI: 10.1007/978-3-540-74735-2_5.

14. MISPAN, Mohd Syafiq. *Towards reliable and secure physical unclonable functions* [online]. University of Southampton, 2018 [visited on 2022-03-30]. Available from: https://eprints.soton.ac.uk/424534/. PhD thesis. University of Southampton.

15. LEEST, Vincent van der; SCHRIJEN, Geert-Jan; HANDSCHUH, Helena; TUYLS, Pim. Hardware Intrinsic Security from D Flip-Flops. In: *Proceedings of the Fifth ACM Workshop on Scalable Trusted Computing* [online]. Chicago, Illinois, USA: Association for Computing Machinery, 2010 [visited on 2022-03-30]. STC '10. ISBN 9781450300957. Available from DOI: 10.1145/1867635.1867644.

16. MAITI, Abhranil; GUNREDDY, Vikash; SCHAUMONT, Patrick. A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions. *IACR Cryptol. ePrint Arch.* [Online]. 2011 [visited on 2022-03-30]. Available from: https://eprint.iacr.org/2011/657.pdf.

17. MAITI, Abhranil; CASARONA, Jeff; MCHALE, Luke; SCHAUMONT, Patrick. A large scale characterization of RO-PUF. In: *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* [online]. 2010, pp. 94–99 [visited on 2022-04-04]. Available from DOI: 10.1109/HST.2010.5513108.

18. BASSHAM, Lawrence; RUKHIN, Andrew; SOTO, Juan; NECHVATAL, James; SMID, Miles; LEIGH, Stefan; LEVENSON, M; VANGEL, M; HECKERT, Nathanael; BANKS, D. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [online]. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2010 [visited on 2022-04-04]. Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762.

19. YUN, Gao; KONTOYIANNIS, Ioannis; ELIE, Bienenstock. Estimating the Entropy of Binary Time Series: Methodology, Some Theory and a Simulation Study. *Entropy: International and Interdisciplinary Journal of Entropy and Information Studies* [online]. 2008, vol. 10 [visited on 2022-04-04]. Available from DOI: 10.3390/entropy-e10020071.

20. HORI, Yohei; KANG, Hyunho; KATASHITA, Toshihiro; SATOH, Akashi. Pseudo-LFSR PUF: A Compact, Efficient and Reliable Physical Unclonable Function. In: *2011 International Conference on Reconfigurable Computing and FPGAs* [online]. Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, 2011 [visited on 2022-04-06]. Available from DOI: 10.1109/ReConFig.2011.72.

21. DEVADAS, Srinivas; SUH, Edward; PARAL, Sid; SOWELL, Richard; ZIOLA, Tom; KHANDELWAL, Vivek. Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications. In: *2008 IEEE International Conference on RFID* [online]. 2008 [visited on 2022-04-06]. Available from DOI: 10.1109/RFID.2008.4519377.

22. BARBARESCHI, Mario; DE BENEDICTIS, Alessandra; MAZZOCCA, Nicola. A PUF-based hardware mutual authentication protocol. *Journal of Parallel and Distributed Computing* [online]. 2018, vol. 119 [visited on 2022-04-06]. ISSN 0743-7315. Available from DOI: https://doi.org/10.1016/j.jpdc.2018.04.007.

23. ROSTAMI, Masoud; MAJZOOBI, Mehrdad; KOUSHANFAR, Farinaz; WALLACH, Dan S.; DEVADAS, Srinivas. Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching. *IEEE Transactions on Emerging Topics in Computing* [online]. 2014, vol. 2, no. 1 [visited on 2022-04-06]. Available from DOI: 10.1109/TETC.2014.2300635.

24. MAES, Roel; VAN HERREWEGE, Anthony; VERBAUWHEDE, Ingrid. PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator. In: PROUFF, Emmanuel; SCHAUMONT, Patrick (eds.). *Cryptographic Hardware and Embedded Systems – CHES 2012* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012 [visited on 2022-04-07]. ISBN 978-3-642-33027-8. Available from DOI: 10.1007/978-3-642-33027-8_18.

25. GAO, Yansong; MA, Hua; LI, Geifei; ZEITOUNI, Shaza; AL-SARAWI, Said; ABBOTT, Derek; SADEGHI, Ahmad-Reza; RANASINGHE, Damith. Exploiting PUF Models for Error Free Response Generation [online]. 2017 [visited on 2022-04-06]. Available from DOI: 10.48550/arXiv.1701.08241.

26. BÖSCH, Christoph; GUAJARDO, Jorge; SADEGHI, Ahmad-Reza; SHOKROLLAHI, Jamshid; TUYLS, Pim. Efficient helper data key extractor on FPGAs. In: [online]. 2008, vol. 5154 [visited on 2022-04-07]. ISBN 978-3-540-85052-6. Available from DOI: 10.1007/978-3-540-85053-3_12.

27. HERDER, Charles; YU, Meng-Day; KOUSHANFAR, Farinaz; DEVADAS, Srinivas. Physical Unclonable Functions and Applications: A Tutorial. *Proceedings of the IEEE* [online]. 2014, vol. 102, no. 8 [visited on 2022-04-06]. Available from DOI: 10.1109/JPROC.2014.2320516.

28. PAPPU, Ravikanth; RECHT, Ben; TAYLOR, Jason; GERSHENFELD, Neil. Physical One-Way Functions. *Science* [online]. 2002, vol. 297, no. 5589 [visited on 2022-04-07]. Available from DOI: 10.1126/science.1074376.

29. RÜHRMAIR, Ulrich; HILGERS, Christian; URBAN, Sebastian; WEIERSHÄUSER, Agnes; DINTER, Elias; FORSTER, Brigitte; JIRAUSCHEK, Christian. *Optical PUFs Reloaded* [Cryptology ePrint Archive, Report 2013/215]. 2013 [visited on 2022-04-07]. Available from: https://eprint.iacr.org/2013/215.pdf.

30. LEE, J.W.; LIM, Daihyun; GASSEND, B.; SUH, G.E.; DIJK, M. van; DEVADAS, S. A technique to build a secret key in integrated circuits for identification and authentication applications. In: *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)* [online]. 2004 [visited on 2022-04-07]. Available from DOI: 10.1109/VLSIC.2004.1346548.

31. LIM, Daihyun; LEE, J.W.; GASSEND, B.; SUH, G.E.; DIJK, M. van; DEVADAS, S. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* [online]. 2005, vol. 13, no. 10 [visited on 2022-04-07]. Available from DOI: 10.1109/TVLSI.2005.859470.

32. TUYLS, Pim; SCHRIJEN, Geert; SKORIC, Boris; GELOVEN, Jan; VERHAEGH, Nynke; WOLTERS, Rob. Read-Proof Hardware from Protective Coatings. In: [online]. 2006 [visited on 2022-04-07]. ISBN 978-3-540-46559-1. Available from DOI: 10.1007/11894063_29.

33. VOINIGESCU, Sorin. *High-Frequency Integrated Circuits* [online]. Ed. by CRIPPS, Steve C. Cambridge University Press, 2013 [visited on 2022-04-08]. ISBN 9780521873024.

34. HOLCOMB, Daniel E.; BURLESON, Wayne P.; FU, Kevin. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Transactions on Computers* [online]. 2009, vol. 58, no. 9, pp. 1198–1210 [visited on 2022-04-13]. Available from DOI: 10.1109/TC.2008.212.

35. HELFMEIER, Clemens; BOIT, Christian; NEDOSPASOV, Dmitry; SEIFERT, Jean-Pierre. Cloning Physically Unclonable Functions. In: *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* [online]. 2013, pp. 1–6 [visited on 2022-04-08]. Available from DOI: 10.1109/HST.2013.6581556.

36. NEDOSPASOV, Dmitry; SEIFERT, Jean-Pierre; HELFMEIER, Clemens; BOIT, Christian. Invasive PUF Analysis. In: *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography* [online]. 2013, pp. 30–38 [visited on 2022-04-08]. Available from DOI: 10.1109/FDTC.2013.19.

37. SHIFMAN, Yizhak; MILLER, Avi; KEREN, Osnat; WEIZMANN, Yoav; SHOR, Joseph. A Method to Improve Reliability in a 65-nm SRAM PUF Array. *IEEE Solid-State Circuits Letters* [online]. 2018, vol. 1, no. 6, pp. 138–141 [visited on 2022-04-13]. Available from DOI: 10.1109/LSSC.2018.2879216.

38. LIU, Muqing; ZHOU, Chen; TANG, Qianying; PARHI, Keshab K.; KIM, Chris H. A data remanence based approach to generate 100% stable keys from an SRAM physical unclonable function. In: *2017 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)* [online]. 2017, pp. 1–6 [visited on 2022-04-13]. Available from DOI: 10.1109/ISLPED.2017.8009192.

39. ROELKE, Alec; STAN, Mircea R. Controlling the Reliability of SRAM PUFs With Directed NBTI Aging and Recovery. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* [online]. 2018, vol. 26, no. 10, pp. 2016–2026 [visited on 2022-04-13]. Available from DOI: 10.1109/TVLSI.2018.2836154.

40. MAES, Roel; LEEST, Vincent van der. Countering the effects of silicon aging on SRAM PUFs. In: *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* [online]. 2014, pp. 148–153 [visited on 2022-04-13]. Available from DOI: 10.1109/HST.2014.6855586.

41. ESPRESSIF SYSTEMS CO., LTD. *ESP-IDF Programming Guide* [online]. 2022-01 [visited on 2022-04-14]. Available from: https://docs.espressif.com/projects/esp-idf/en/v4.4/esp32/esp-idf-en-v4.4-esp32.pdf.

42. ESPRESSIF SYSTEMS CO., LTD. *ESP32 Technical Reference Manual* [online]. 2021 [visited on 2022-04-14]. Available from: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf.

43. SOS ELECTRONIC S.R.O. *ESP32-WROOM-32U (ESP32-WROOM-32U-N16)* [online]. 2018 [visited on 2022-04-14]. Available from: https://cdn.sos.sk/productdata/6e/92/33234709/esp32-wroom-32u.jpg.

44. KRENT, Brian. *ESP32 Chip Function Block Diagram* [online]. 2018 [visited on 2022-04-14]. Available from: https://commons.wikimedia.org/w/index.php?title=File:Espressif_ESP32_Chip_Function_Block_Diagram.svg.

Contents of the enclosed CD

- `readme.txt` ..... stručný popis obsahu média
- `exe` ..... adresář se spustitelnou formou implementace
- `src`
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF