UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DESIGN OF SECURE PHYSICAL UNCLONABLE FUNCTION

This report is submitted in accordance with the requirement of the Universiti Teknikal Malaysia Melaka (UTeM) for the Bachelor of Electronics Engineering Technology (Industrial Electronics) with Honours.

by

TEE KAH KEAT

B071610467

960429-08-5755

FACULTY OF ELECTRICAL AND ELECTRONIC ENGINEERING TECHNOLOGY

2019

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN PROJEK SARJANA MUDA

Tajuk: DESIGN OF SECURE PHYSICAL UNCLONABLE FUNCTION

Sesi Pengajian: 2019/2020

Saya **TEE KAH KEAT** mengaku membenarkan Laporan PSM ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka (UTeM) dengan syarat-syarat kegunaan seperti berikut:

1. Laporan PSM adalah hak milik Universiti Teknikal Malaysia Melaka dan penulis.
2. Perpustakaan Universiti Teknikal Malaysia Melaka dibenarkan membuat salinan untuk tujuan pengajian sahaja dengan izin penulis.
3. Perpustakaan dibenarkan membuat salinan laporan PSM ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (X)

☐ SULIT* — Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia sebagaimana yang termaktub dalam AKTA RAHSIA RASMI 1972.

☐ TERHAD* Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan.

☒ TIDAK TERHAD

Yang benar,

.....

TEE KAH KEAT

Alamat Tetap:

87,jalan indah7,taman indah,

45400 sekinchan,selangor

Tarikh:

Disahkan oleh penyelia:

.....

Dr.Mohd Syafiq bin Mispan

Cop Rasmi Penyelia

Tarikh:

*Jika Laporan PSM ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan PSM ini

DECLARATION

I hereby, declared this report entitled DESIGN OF SECURE PHYSICAL UNCLONABLE FUNCTION is the results of my own research except as cited in references.

Signature: ……

Author : TEE KAH KEAT

Date:

APPROVAL

This report is submitted to the Faculty of Electrical and Electronic Engineering Technology (FTKEE) of Universiti Teknikal Malaysia Melaka (UTeM) as a partial fulfilment of the requirements for the Bachelor of Electronics Engineering Technology (Industrial Electronics) with Honours. The member of the supervisor is as follow:

Signature: …….

Supervisor : Dr.Mohd Syafiq bin Mispan

ABSTRAK

Physical Unclonable Functions (PUFs) are new primitive security based on hardware. It uses the random physical disorder or process variations to deliver specific input challenges response, called the Challenge-Response Pairs (CRP). PUF can classify into two categories the Weak PUF and the Strong PUF. Strong PUFs have many potential challenges and weak PUF normally has only a few numbers of CRPs. Strong PUFs are unpredictable and cheap authentication. Arbiter PUF is one of the kinds of strong PUF. But because of its deterministic logic, the modeling techniques can break it in a short time. Therefore the objective of this project is to develop a soft model of Arbiter PUF after that proposed a technique to increase the resistance of strong PUF against modeling attacks. The effectiveness of the proposed technique is using artificial neural network machine learning algorithm to test it. The resulting outcome is measure the predictivity, uniformity, and uniqueness. The result shows that the resistance of arbiter PUF again to the modeling attack of ML is low, so the adversary is easy to exploiting model-building attacks to break it. But, if adding a strong PUF and XOR gate the statistical analysis shows a great increase in the resistance against the modeling attacks. Therefore by using this method, the strong PUF able to reduce the predictability of PUF response to below 60% as the expectable result.

ABSTRACT

Fungsi Fizikal Unclonable (PUFs) adalah keselamatan primitif baru berdasarkan perkakasan. Ia menggunakan gangguan fizikal rawak atau variasi proses untuk menyampaikan tindak balas cabaran input tertentu, yang dipanggil Cabaran-Cabaran Pasangan (CRP). PUF boleh diklasifikasikan kepada dua kategori PUF lemah dan PUF kuat. PUF yang kuat mempunyai banyak cabaran yang berpotensi dan PUF lemah biasanya hanya mempunyai beberapa nombor CRP. PUF kuat adalah pengesahan yang tidak dapat diramalkan dan murah. Pengadil PUF adalah salah satu jenis PUF yang kuat. Tetapi kerana logik deterministiknya, teknik pemodelan dapat memecahkannya dalam masa yang singkat. Oleh itu objektif projek ini adalah untuk membangunkan model PUF Arbiter yang lembut selepas itu mencadangkan teknik untuk meningkatkan daya tahan PUF yang kuat terhadap serangan pemodelan. Keberkesanan teknik yang dicadangkan menggunakan algoritma pembelajaran rangkaian neural tiruan untuk mengujinya. Hasilnya adalah mengukur ramalan, keseragaman, dan keunikan. Hasilnya menunjukkan bahawa penentangan PUF pengadil kembali ke serangan pemodelan ML adalah rendah, jadi musuh mudah untuk mengeksploitasi serangan bangunan model untuk memecahkannya. Tetapi, jika menambah PUF dan pintu XOR yang kuat, analisis statistik menunjukkan peningkatan besar dalam rintangan terhadap serangan pemodelan. Oleh itu, dengan menggunakan kaedah ini, PUF yang kuat mampu mengurangkan ramalan PUF kepada kurang daripada 60% sebagai hasil yang diharapkan

DEDICATION

This report is dedicated to my beloved parents who educated and supported me throughout the process of doing this project. I am also wanted to say thank u to my supervisor and my friends who have encouraged, guided and inspired me to complete this project.

ACKNOWLEDGEMENTS

This report is a testament to my sincere appreciation to Universiti Teknikal Malaysia Melaka (UTeM) for giving me the opportunity to study further at the Faculty of Engineering Technology (FTK) Bachelor of Electronics Engineering Technology (Industrial Technology). I would also like to thank my supervisor, Encik Dr. Mohd Syafiq Mispan, for his guidance, advice, encouragement, inspiration and attention throughout the day in the development of my final year project (Design of Secure Physical Unclonable Functions). He directed me to complete this project with total commitment and dedication with this continuous support and interest. My appreciation goes to my beloved family and friends who always give me strength and support in achieving my project's goal. They gave me up until this project was completed thanks to their moral support and care.

CHAPTER 1

INTRODUCTION

1.1 Background

The early good hardware security is the Physical Unclonable Function (PUF). It uses random physical disorder or process variations to respond to specific input challenges, called the Challenge-Response Pairs (CRP). CRPs will different even with the same design, due to the different manufactured, so it is hard to think and clone before or after manufacturing. Therefore, the PUF has extensive hardware security applications such as authentication, certification, IP protection, and ID. The majority of PUFs can be classified into two overall categories: the Weak PUF and the Strong PUF.

The Weak PUFs is actually a new form of storing secret keys in defenseless hardware, offering a different to ROM, Flash or other non-volatile memories (NVMs). It can be used for cryptographic purposes. In 2000, one of the earliest weak PUFs was a design proposed by Lofstrom et al (Lofstrom, Daasch, and Taylor 2000) to purchase beginning imbalance for identifying circuits. A weak PUF normally has only a few numbers of CRPs. The most popular weak PUFs is SRAM PUFs. The main application of weak PUFs is cryptographic key generation.

Besides weak PUF they are second primary PUF type strong PUF. Strong PUFs have many potential challenges, this will cut-off a full read-out of all CRPs. The safety models for weak and strong PUFs have differed, the output of a weak PUF must be kept a secret, while the responses of a strong PUF do not have the same limit. Besides that, strong PUFs are unpredictable and cheap authentication. The unpredictability that is even a large subset of CRPs is known by the adversary, they cannot infer or predict the other still unknown CRPs.

Next, low-cost PUF authentication will replace secure memory and crypto-hardware on an embedded device, as PUF does not require secure non-volatile memory, anti-tamper circuitry, or additional supporting crypto-acceleration hardware, thus requiring less area, power, and mask layers than traditional authentication approaches. But very little application of strong PUFs is assumed as unprotected challenge-response interface. It is freely and publicly accessible. It can use arbitrary challenges to the strong PUF and read the corresponding responses if the person holding the PUF or the hardware carrying the PUF is. In 2002, the first strong PUF is the optical PUF of Pappu et al (Pappu et al. 2002). Strong PUFs are mainly used to identify challenges and system authentication In a banking card scenario, the first idea is described. Strong PUFs were also suggested for the basic identification scheme in cryptographic applications. The first strong PUF is called Arbiter PUF.

However, there have some attack techniques that can break strong PUFs. Machine learning (ML-attacks) is the most directly appropriate attack method for strong PUFs, but the attacker can collect a large number of all possible CRPs of a given Strong PUF, depending on the exact Strong PUF design. Modeling Attacks are not applicable in weak PUF because weak PUF has only one challenge per PUF, so no prediction of unknown CRPs from a subset of known CRPs is applicable. Then, in terms of cost-effectiveness and high prediction accuracy, it offers great advantages.

1.2 Problem Statement

As technology advance, Physical Unclonable Functions (PUF) has wide application look-out in the field of hardware security, such as authentication, IP protection, certification, and identification. Arbiter PUF is the one type of strong PUF. But it is easier to break by the ML-attack. The strong PUF usually have no protection mechanisms that keep under control in freely applying challenges and reading out their responses, so the attacker can collect a large number of all possible CRPs. They are many types of machine learning can be used to attack the strong PUF.

1.3 Objective

The aim of this project is

1. To implement and characterize a soft model of Arbiter PUF

2. To proposed a technique to increase the resistance of strong PUF against modelling attacks.

3. To evaluate the effectiveness of the proposed technique by using a suitable machine learning algorithm.

1.4 Scope of Study

This project will be a focus on to apply a basic circuit structure of Physical Unclonable Function (PUF) and represented in programming form. Next, the development of an easy and understandings solution that will improve the resistance against the modeling attacks where user can apply in arbiter PUF. After that, the development of a machine learning algorithm and used to investigate the effectiveness of the method for proving that the method is suitable to be used against the modeling attacks.

1.5 Thesis Outline

This thesis report consists of five main chapters briefly described in each chapter as follows.

In chapter 1, the introduction describes the project overview, the statement of the problem, the objectives, the scope of the study and the outline of the thesis. More about the PUF and its application was discussed in the chapter.

In chapter 2, the project literature review is the most important to assist the progress of the project in this thesis report. This chapter explains, and compares, more about summarized past research related to the project.

In chapter 3, the project methodology will explain the step taken from the project's start to the project's end. More software design and programming will be discussed in this chapter.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter is one of the project's important sections and serves as the basis for gathering information to complete the project and to make the project go smoothly without lack of understanding. All relevant information comes from many sources, such as journals, conferences, papers and the Internet. Once all material has been viewed, all information is filtered to be associated with the Physical Unclonable Function (PUF) and compiled for inclusion in the report.

2.2 Types of PUF

2.2.1 Strong PUF

Optical PUF

One of the first fulfillment device terms “physical one-way function”, it function is identical to a strong PUF which manufacture by Pappu et al. in 2002 (Pappu et al. 2002). The input challenge is a polarization and laser XY location, and the response is the corresponding speckle pattern. In the implement, the scattering medium contains a large number of random position 100-μm silica spheres breaking in the hardened epoxy resin. Each sphere acts as a small lens that, as they pass through the scatter block, refracts a single ray. The scattering block's total size is 1 mm thick.

Arbiter PUF

The main electrical and integrated strong PUF is the Arbiter PUF (Gassend et al. 2002), (Suh and Devadas 2007). The idea is using the different run delays in electrical components. In the Arbiter PUF structure, the electrical signals rivalry each other to a sequence of k stages which each made up of two multiplexers. After that, to applied at the stage each path of the signal is determined by k external bits, one bit per stage. The final arbiter part is implemented by a latch. For example, in figure 2.0 if there's 128 bits of challenge and a bit of response. Naturally, multiple identical circuits are typically run in parallel with 128 response bits. In this way, it is possible to scale an almost arbitrary number of CRPs to the PUF arbiter. The safety of the arbiter PUF is based on the assumptions of the production capacity and ultimately the metrology of the individual gate delays. Manufacturers are unable to produce two identical PUF because the PUF's characteristic is defined by the fixed of production process changing. As this would needs substantial improvements in mastering of manufacture. Next, it is difficult to measure individual gate delays directly. Example, like an attacker even with physical access still difficulty to get the individual delays. The last assumption of security is that given an arbiter PUF set of CRPs, an opponent could not calculate the gates ' internal delays. Arbiter PUF also sensitive to environmental changing such as temperature, supply voltage, aging, and even random noise all this can influence each edge’s delay to the PUF arbiter. Furthermore, if gap of delays is small, the time by the system of the latch will be violated, will cause the output become unpredictable. For the outcome, the response bit turn to unstable. For solving the problem, techniques of error-correcting are used. It used to enhance PUF stability while maintaining its safety.

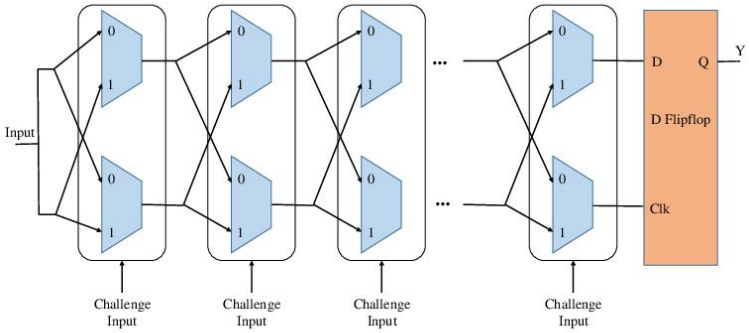

Figure2.0: Arbiter PUF

2.2.2 Weak PUF

SRAM PUF

A PUF structure with positive feedback loop in a SRAM. SRAM cell has two stable states for maintaining a1 or 0, positive feedback is one of two states that force cell selection. Once there, the cell is prevented from accidentally transitioning from the state. In theoretical, sub-stable state of the SRAM cell when the device is powered up or there is no write operation. In the absence of a metastable state, the feedback that pushes the battery to the "1" state is equal to the feedback that pushes the battery to the "0" state. Next, the final state is depends on the difference between the two feedback loops, but the measurement is differential.

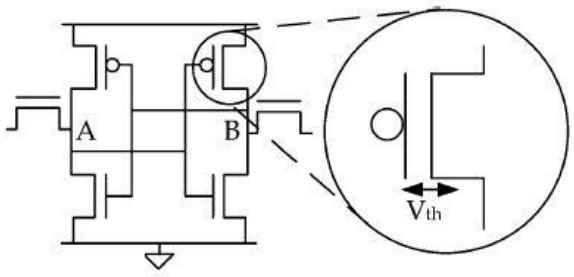

Figure2.1: SRAM cell

Ring-Oscillator PUF

The PUF structure, consisting of N ring oscillators of the same design, is synthesized into a field programmable gate array (FPGA) or an application specific integrated circuit (ASIC). The ring oscillator has slightly different frequency because of the changing in delay of the inverters. The frequencies are compared and measured to reveal one of the PUF output bits of two oscillators. However, due to the correlations the number of output bits is limited. Ring-oscillator PUF has a limited number of "challenge bits" that can configure the PUFs operation. The frequency of the ring oscillators is set during manufacture, therefore the PUF of the output bits remain constant. The error correction is important in the application of ring-oscillator PUF.

2.3 Defining PUF Parameters

2.3.1 Uniformity

PUF uniformity estimates how even the PUF response bit's ratio of ' 0 ' and ' 1 ' is uniform. The ratio must be 50 percent to obtain an accurate random PUF response. Consequently, the uniformity of the n-bit PUF identifier is the n-bit identification Hamming weight percentage (HW):

$$(Uniformity)_i = \frac{1}{n}\sum_{l=1}^{n} r_{i.l}\, x100\%$$

2.3.2 Uniqueness

Uniqueness shows the ability of a PUF to individually differentiate a particular chip in a group of chips of the same type. To evaluate uniqueness, Hamming distance (HD) is using to identifiers the between a pair of PUF. The idea value is 50%. If two chip, a and b (a $\neq$ b), have m-bit response, R_a and R_b for challenge C, the average inter-chip HD in k chips is defined as

$$Uniqueness = \frac{2}{k(k-1)}\sum_{i=0}^{n}\sum_{b=a+1}^{k}\frac{HD(R_aR_b)}{n}x100\%$$

2.4 Known ML-attack on PUFs

2.4.1 PUF with Randomized Challenge to Resist Modeling Attack

Several works have studied the susceptibility of PUFs against ML-attack. In this study, (Ye, Hu, and Li 2017), the challenge randomization module is placed before the arbiter, the function is randomize the input challenge and let the attackers cannot find which sub-challenge are the input to the arbiter PUF. The challenge randomization module has using RNG. Figure 2.3 show that the prediction accuracy is great decrease when using RPUF. The other kind PUF has highly percentage of prediction compare with the RPUF. Next, figure 2.4 show the uniformity and average uniqueness is close to the ideal value. After that, the reliability of RPUF is similar to arbiter PUF. But the RPUF confront to hardware overhead due to the n inverter and n multiplexers insides the challenge randomization module.

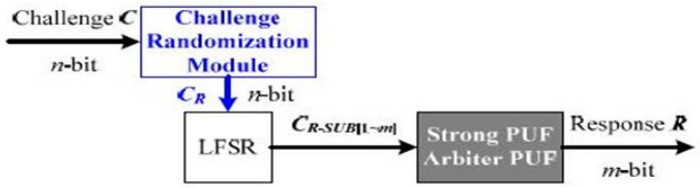

Figure 2.2: RPUF

		Number of Challenge Bits	Number of Response Bits	Number of CRPs in Training Set	Number of CRPs in Testing Set	Randomization level	P_{RNG0}	Prediction Accuracy
Current Mirror PUF	Simulation	32	1	1×10^3	2×10^4	N/A	N/A	99.9%
		64	1	1×10^4	2×10^4	N/A	N/A	99.3%
		128	1	2×10^4	2×10^4	N/A	N/A	98.0%
Voltage Transfer PUF	Simulation	32	1	1×10^3	2×10^4	N/A	N/A	99.9%
		64	1	1×10^4	2×10^4	N/A	N/A	99.3%
		128	1	2×10^4	2×10^4	N/A	N/A	98.2%
Arbiter PUF	Simulation	32	32	1×10^2	1×10^3	N/A	N/A	99.9%
		64	64	2×10^2	1×10^3	N/A	N/A	99.9%
		128	128	2×10^2	1×10^3	N/A	N/A	99.6%
	FPGA	128	128	2×10^2	1×10^3	N/A	N/A	98.7%
RPUF	Simulation	32	32	1×10^2	1×10^3	1	40%	74.1%
							50%	78.7%
							60%	73.7%
						2	40%	76.3%
							50%	74.3%
							60%	75.0%
		64	64	2×10^2	1×10^3	1	40%	79.2%
							50%	76.1%
							60%	70.4%
						2	40%	73.8%
							50%	70.8%
							60%	69.1%
		128	128	2×10^2	1×10^3	1	40%	76.3%
							50%	75.1%
							60%	79.0%
						2	40%	73.1%
							50%	66.4%
							60%	64.2%
	FPGA	128	128	2×10^2	1×10^3	1	≈50%	71.6%
						2		57.3%

Figure2.3: Result Prediction Accuracy

		Number of Challenge Bits	Number of Response Bits	Uniformity	Uniqueness	Reliability
Arbiter PUF	Simulation	32	32	50.1%	50.3%	N/A
		64	64	51.0%	51.6%	N/A
		128	128	49.6%	52.6%	N/A
	FPGA	128	128	48.6%	51.3%	94.37%
RPUF	Simulation	32	32	50.1%	50.5%	N/A
		64	64	51.1%	49.7%	N/A
		128	128	49.7%	51.6%	N/A
	FPGA	128	128	48.9%	52.2%	94.80%

Figure2.4: Result Uniformity, Uniqueness and Reliability

2.4.2 Obfuscation logic Based PUF

This PUF in this article (Ye, Hu, and Li 2015) is made out by adding the Boolean obfuscation module on the inputs challenge of the arbiter PUF. Obfuscation cell is stimulate by HSPICE, the obfuscation cell will give the value 0 and 1, if 0 the XOR gate acts like a buffer, if 1 it act like an inverter. It thus has 2^npossible logical relationships between its inputs and outputs. But the larger the challenge, the Boolean obfuscation module has more logical relations. So the chance of hardware overhead is high. The stability and randomness of Obfuscation cells is 97.27% and 49.89%. The stability and randomness of IOPUF is 93.79% and 49.95%, the value is closer to the theoretical values. Furthermore, the modeling exponents also high which can increase the computation complexities of modeling attack.

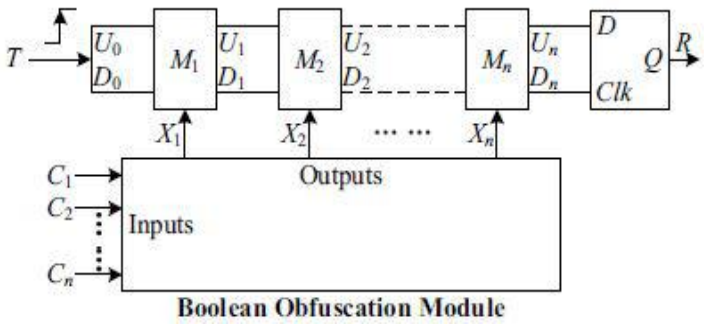

Figure2.5: OPUF Design

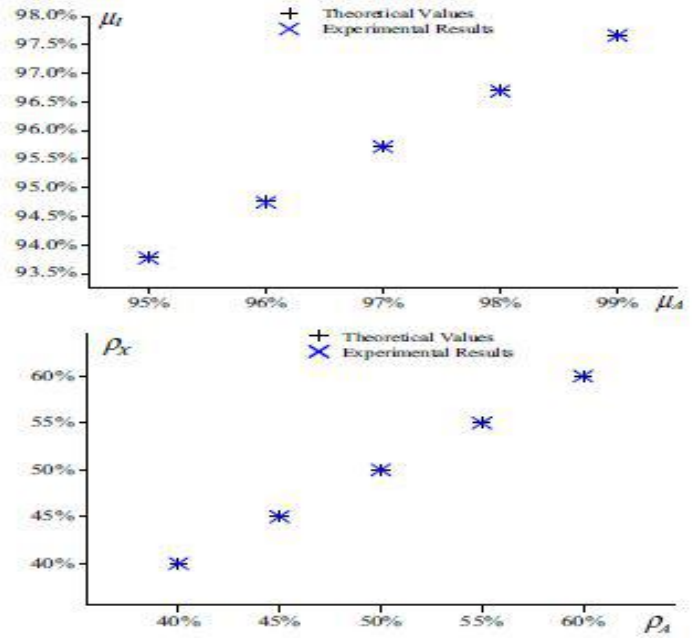

Figure2.6: Stability and Randomness of IOPUF

2.4.3 Cost-efficient modeling design for resistant PUF attacks

The method use to resist the modeling attacks is substitution and permutation technique. The arbiter PUF and the TCO-PUF has been adopted. The Challenge Replacement Technique function is to reduce the mapping correlation between challenge and response (Mispan et al. 2018). With using substitution technique, the predictability of the arbiter PUF and TCO-PUF is reduces from the zone of 90% to 66.4%and 62.5%. Next, in challenge permutation technique every time a single challenge bit is complemented the probability of output transition occurs is 0.5. If the challenge bit increase, the probability of output transition value will increase and the resilient of PUF against ML-attack also increase. But TCO-PUF does not affected by this technique. Example, for a 128-bit identifier this technique will use up less than 2000 GEs. Therefore, this technique is suitable for lightweight security devices.

2.4.4 A learning machine attacks resistant PUF design in two stages

Difference kind of PUF are combined and become a new structure, the output response from the current mirror PUF is the input of the arbiter PUF. The complexity has increase the input and output to [(16x16)] ^16 possible outcomes (Su, Zwolinski, and Halak 2018). Furthermore, the randomness of the design is boots due to the gate delay and the threshold voltage of the current mirror transistors. Next, the uniformity and uniqueness of the two stages PUF is 39.06% and 47.76% based on 32 instances and on 3200 CRPs. But, it is easily affected by external condition changes. The prediction of output is reduced which show that the resistance is much better than individual PUFs.

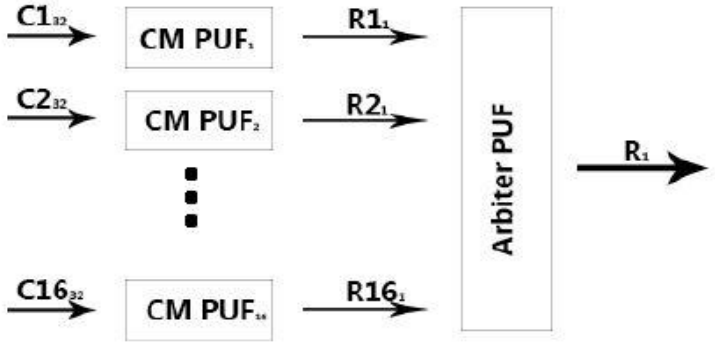

Figure2.7: two stage PUFs model

2.4.5 Machine learning attacks on 65nm Arbiter PUFs

In this paper (Hospodar, Maes, and Verbauwhede 2012), the method is 64-stage Arbiter PUFs that achieve in 65nm CMOS and using machine learning technique test on challenge response pairs (CRPs) of the PUF The aim is to analyze the effectiveness of various modeling attacks on the modern implementation of silicon. Next, Artificial Neural Networks (ANN) and Support Vector Machines (SVM) have been use to tested the ability to model physically realized Arbiter PUFs. The advantage of ANN and SVM is that they are flexible and can learn any model compared to other techniques with unknown

parameters on a previous model, which is more limited. The training set sizes on the ML-attack can range from q train= 25 to 5000 in simple Arbiter PUF and also depends heavily on the use of training CRPs, the model has been set up and severely validated on subsets consisting of random splits of a training set consisting of 70% and 30% of the training CRPs. SVM for q train <= 500yields Arbiter PUF models more accurate than ANN, but for larger training sets, ANN outperforms SVM. SVM achieves SR(50) at 70% and for q train = 500, both SVM and ANN can predict responses with nearly 90% accuracy. For q train>= 5;000, ANN is able to model an Arbiter PUF perfectly by arbitrarily achieving the success rate close to the robustness of the PUF.

2.4.6 Extract secret keys from built-in circuits

A scheme is propose named arbiter-based PUF by using a differential structure to improve the reliability of the PUFs against environmentally induced noise (Lim et al. 2005). The delay paths and generate digital information that measure the absolute delay value of PUF responses by using an arbiter and compare. Besides that, Arbiter-based PUF test-chips are manufacture using a TSMC 0.18-um process. It uses 190 different PUF pair to test Inter-chip of arbiter-based PUFs variation. The average inter-chip and minimum inter-chip variation is 23% and 17%. The result of inter-chip variation in the intermediate stage of feed-forward arbiter can caused the average and minimum inter-chip variation to increase. The environmental variation will decrease below 23% the average inter-chip variations with differential design of an arbiter-based PUF circuit. To increase noise probability, it needs seven internal arbiters in the feed-forward arbiter, and then the internal arbiter response of each noise is produces in the final response. More CRPs can extract a secret key to correct the measurement noise. This method is well fast for most applications. The performance may be facilitate by copy many delay paths and arbiters to assess parallel reaction.

2.4.7 A secure lightweight autheatication

In this paper (Gao et al. 2016), a protocol device is built on a physical unclonable function(PUF) ancient termed Obfuscated PUF (OB-PUF), it is secure, lightweight authentication and resource is hardly pervasive by modified a parameter-based authentication protocol. An OB-PUF is to receive the agreement send by obfuscated challenges by a verifier to inform the coming recovery of the obfuscated challenges is ensure. In specific, the server is to support the calculations and lower the complexity of hardware on the pervasive device as still can maintain security with high level and simulate model building attacks using known PUF exposures. Figure2.8.1 shows the structure of OB-PUF, it includes a random number generator (RNG), a controlling block and a PUF block. A PUF block consists of a number of APUFs, therefore an OB-PUF built on APUFs is analysis. As a comparison, the prediction accuracy of an XOR2-APUF is 96% when the CRPs are 50,000. The worst case of reliability of an APUF is 95.18%. Therefore, an XOR2-APUF reliability is 90.82% which under the worst case. However, the reliability of the learnt model of an OB-PUF remains well below the worst-case reliability of either an APUF or an XOR2-APUF even after training with more than 1 million obfuscated CRPs.

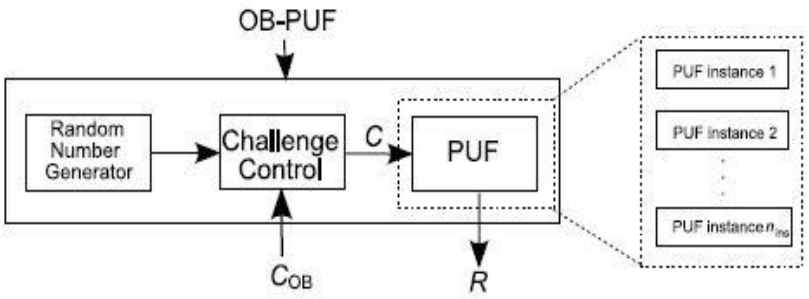

Figure2.8: Obfuscated PUF (OB-PUF) structure

2.4.8 PUF modeling of simulated and silicon data attacks

Numerical modeling attacks can damage Physical Unclonable Functions (PUFs) easily. A PUF has challenge-response pairs (CRPs), the computer algorithm will create an attack which original PUF is hard to indistinguishably on almost all CRPs. This arithmetic can afterward imitate the PUF and can be cloned and distributed arbitrarily. PUF has several subtypes like Strong PUFs, Controlled PUFs and weak PUFs. Next, the techniques of machine learning Logistic Regression and Evolution Strategies is been use in this article (Solter et al. 2013). Logistic Regression (LR) is a well-investigated supervised machine learning framework and Evolution Strategies is known as population-based heuristics which belong to an ML subfield. The experiments are carried out using a stand-alone consumer INTEL Quadcore Q9300 worth less than 1000 Euros and a 30-node cluster of AMD Opteron Quadcores worth around 30000 Euros. Successfully attacking PUFs include standard Arbiter PUFs and Ring Oscillator PUFs of arbitrary size, and other type of strong PUF of up to a given size and complexity.

2.4.9 Introduction of PUF modeling attacks

Machine learning attacks are at present most applicable and effective attack to Strong Physical Unclonable Functions (Strong PUFs). On the whole, modeling attacks on PUFs assume as an opponent Eve has, in one way or the other collected a subset of all CRPs of the PUF .Then tries to obtain a numerical model from this CRP data (Ruhrmair and Holcomb 2015). Apart from machine learning (ML) techniques, there are other methods like linear programming or algebraic techniques have been applied in the past (Oztürk, Hammouri, and Sunar 2008) (Majzoobi, Koushanfar, and Potkonjak 2008). Next, the modeling process basically has two-step procedure. First consists of setting up an internal, parametric model of the PUF and second parametric model F is used together with a suitably chosen ML algorithm for PUF learning. The main challenges of