University of Sheffield

Reconfigurable Security for IoT Application in Handling Machine-Learning/Modelling Attacks

Cheng-Wei, Tsao

Supervisor: Dr Prosanta Gope

A report submitted in fulfilment of the requirements
for the degree of BSc in Computer Science

in the

Department of Computer Science

November 25, 2021

Declaration

All sentences or passages quoted in this report from other people's work have been specifically acknowledged by clear cross-referencing to author, work and page(s). Any illustrations that are not the work of the author of this report have been used with the explicit permission of the originator and are specifically acknowledged. I understand that failure to do this amounts to plagiarism and will be considered grounds for failure in this project and the degree examination as a whole.

Name: Cheng-Wei, Tsao

Signature: Cheng-Wei, Tsao

Date: November 15, 2021

Abstract

This report investigate and provide clear introduction on PUF(physical unclonable function), aim of the project and current progress. In introudction, there are thoroughly description on PUF, reconfigurability framework and concepts corresponding to specific machine learnings for modeling attack on PUF.

The aim for the project is to propose a novel, suitable machine learning to model PUF(physical unclonable function) and then design a reconfigurability framework to fight against such attack. The PUF structure is similar to a road network so machine learning related to ETA(estimated time arrival) problem is strongly considered.

The achievements to date are having robust understanding on PUF, reconfigurability property, and attempt to implement reinforcement learning as modeling attack. SARSALambda Q learning reinforcement learning has been tested on PUF but according to false implementation, only 50% accuracy has been achieved. The Actor-Critic reinforcement learning are considered to be useful at the moment, while further research are progressing to validate the usability.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the rapid development of the information era, many daily events are achieved by a various of electronic devices such as computer or phones. Those electronic devices highly rely on integrated circuits(ICs) to perform specific events. For example, bank transaction can be done by different devices, the process contain personal data, and including usage of sensitive information. Therefore, information security like authentication, protecting confidential data has become important in nowadays society. In order to increase security's robustness, a range of ways has been proposed. One conventional way to is by storing secret key in non-volatile memory to encrypt sensitive data with it, and use asymmetric cryptography to authenticate the device [5]. However, the implementation process of cryptography is expensive, especially on resource-constraint device, and the device is still vulnerable to invasion attack. Ideally, devices should be able to handle challenging problems corresponding to energy consumption, computational power and the ability to fight against cyber attack.

PUF(physical unclonable function) has the ability to deal with these challenges. It does not store secret in non-volatile memory, instead, the volatile secret is derived from devices' physical characteristics [5]. This is based on the inevitable random variation in ICs manufacturing process, which leads to the fact that no two IC have exact same physical characteristic. For example, each ICs has unique delay sequences in the transistors and wires. With this property, PUF does not require lots of computational power and is cost-effective because no need to implement cryptographic operation, which works particular well on resources-constraint devices such as RFID. Also, the attacker needs to perform attack when the device is on, which significantly increase the difficulty. As for invasion attack, the attacker needs to have the exact information of its unique physical characteristics to successfully derive secret. Overall, PUF provides another interesting way for reinforce security.

1.1 Aims and Objectives

The objectives split into two parts for this project. In the first stage, propose a novel machine learning to modeling different PUF(physical unclonable function) behavior, so predict the response from a given PUF when given challenge bits. For example, considered the simplest PUF which is arbiter PUF, its operation to create a response is to input a challenge bits(binary), and two signals will go thorough the multiplexers in the PUF structure depend on the value of it. Consequently response a binary bit that will indicate which signal is faster. Therefore, the machine learning for modeling will be related to ETA(estimated time arrival) problem since the structure of PUF is similar to a road network. For instance, traveling through each multiplexer is similar to traveling through each road segment, and both of them have delay to affect the time of arrival. Overall the first stage is to design a machine learning consider these concepts. In the second stage, design a reconfigurability framework to fight against such modeling. In detail, evaluate the machine learning by insert noise in PUF or experiment on OPUF(one-time-PUF) which contain reconfiguration process that can alleviate modeling attack.

1.2 Overview of the Report

The remaining of the paper will organize as follow. Chapter 2 provide literature survey of the concept of PUF, including PUF's properties, detailed circuit structure and operational process, exist modeling attack with experiment results, reconfigurability framework and application in life. Relative machine learning idea will be discuss as well. Chapter 3 describe the aim and objectives for the project , gives in-depth analyzes how the project will be evaluated, the tests and experiments that support this. Chapter 4 demonstrate the current progress on the project. Chapter 5 provide brief summary on the main achievements with a well organized future plan for the project.

Chapter 2

Literature Survey

2.1 The PUF concept

The simplest sentence to describe PUF is "A PUF is an object's fingerprint" [2]. The fingerprint can represent a specific human in the world, such as the PUF can represent an object. The fingerprint is inherently created when people was born, and the so does PUF, which is inherently exist in an object according to unique manufacturing random variation [2]. With the representation and inherent property, the fingerprint and the PUF is said to be unclonable since it is impossible to control and predict human's fingerprint. This is an important concept for PUF.

This intrinsic property can be extract from chip which has PUF circuit existed inside [1]. The way PUF works is by entering a certain length of bits(so called challenge) into the PUF, and it will generate another specific length of bits(so called response). According to the property of PUF that was discuss above, it is impossible to find two different PUF that will produce the same response when entering same challenge(See Figure 2.1).

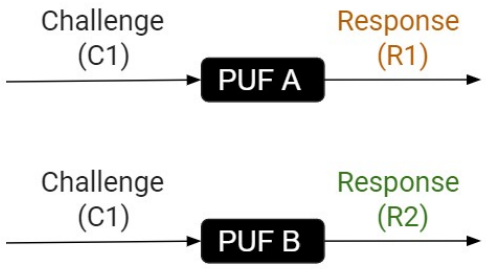

Figure 2.1: Different PUF that generate different response when input same challenge

2.2 Weak and strong PUF

PUF can be classified into two categories, weak and strong PUF according to the strength of PUF. The strength of PUF indicate the number of challenge response pairs(so called CRPs) can be generate from the PUF [3]. The higher numbers of the CRPs can a PUF generate, the better strength it has. Generally, if increasing the size of the PUF leads to a linear increase in the number of CRPs, it is consider weak PUF. On the other hand, if increasing the size of the PUF leads to a exponential increase in the number of CRPs, it is consider strong PUF.

For the weak PUF, it represent the PUF that has smaller set of CRPs. While it is impossible to create a clone of PUF, but with small set of CRPs, this will allow attacker to record all the CRPs when attacker has physical access to PUF [3]. With the knowledge of CRPs, attacker can easily provide the corresponding response to challenge as like they have a clone(See Figure 2.2). The weak PUF can be use for authentication and key storage. However, since weak PUF's CRPs can be fully access, ensure having a secure environment and whether the original PUF is being evaluating is relatively important [3].

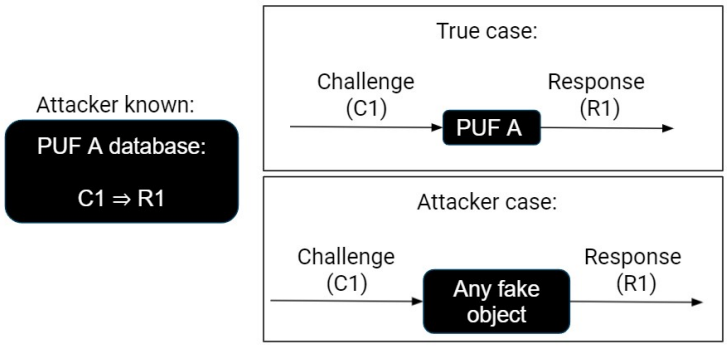

Figure 2.2: Attacker can perform same behavior as Weak PUF when have fully access to CRPs and not under secure environment

For strong PUF, means the number of CRPs is significantly large that even attacker get access, having throughout knowledge of CRPs is impossible. While the number of CRPs is so large, and the CRP are randomly selected in usage, the probability that attacker has knowledge about the CRP currently using is small. In addition, each CRPs that is used once will be discarded(See Figure 2.3) so even if attacker recorded certain CRPs, also called eavesdropped, they will not be able to put them into use. The strong PUF can also be use for authentication but do not need to protect CRPs as serious as weak PUF.

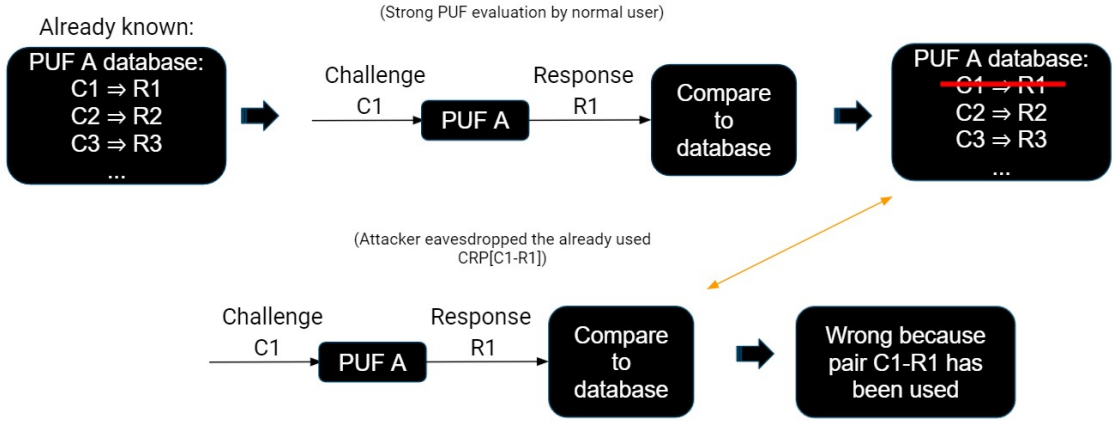

Figure 2.3: The attacker eavesdropped CRP that has been used can not successfully validate in next evaluation for strong PUF

2.3 Authentication

One of the application of PUF is authentication. As discuss in Chapter 1's introduction, PUF does not require huge computational power and are cost effective, so it is suitable for many devices, especially the resources-constraint devices. The PUF's authentication included two stages, enrollment and authentication stage. In the enrollment stage, the company possess the PUF, so company can connect server to PUF and sent lots of challenges along with recording the CRPs into the database [1] (See Figure 2.4).

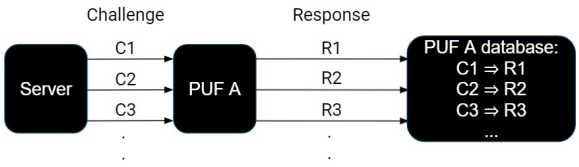

Figure 2.4: Enrollment stage in PUF authentication

After recording all the CRPs, the company can now implement PUF on electronic devices. In the authentication stage, the server sent arbitrary challenge to the devices that contain PUF while the device will return response. Afterward, the server compare the response from the device with the database, if the challenge and response pair exist in the database, the device is valid [1] (See Figure 2.5). A life example will be banking card.

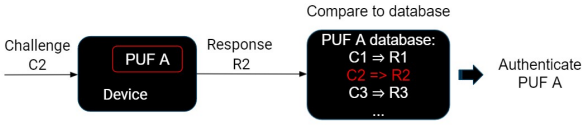

Figure 2.5: Authentication stage in PUF authentication

2.4 Arbiter PUF and XOR arbiter PUF

There are many different types of PUF such as arbiter PUF, ring oscillator PUF, lightweight PUF, etc. In this paper, arbiter PUF and its mutation will be introduced in detail. The general idea of the arbiter PUF is comparing the transition speed for two electrical signal in the PUF's structure(See Figure 2.6). The arbiter PUF's structure contains a numbers of multiplexers and a arbiter(mostly D flipflop), and two multiplexers will combined into a switching box [5]. Look at Figure 2.6, when enter a challenge bits, apply each challenge bit to a switching box, bit 1 indicate the upper and lower signal will switch while bit 0 indicate the two signals remain unchanged in each switching box. This will eventually form paths for the signals. Then the signals start transferring, the time arrived at the arbiter for two signals is different since each multiplexer and wire has unique delay. The arbiter will determine which path is faster and based on that response a binary bit, if upper path is faster, the response is 1, otherwise the response is 0.

The arbiter at the end is always fair, which will not favor any one of the path. Even there exist bias, a simple solution of adding a delay in the structure can solve the problem. For example, if the arbiter favor the lower path, by adding a delay to upper path, it can has a head start. By looking at the Figure 2.6, it is clear that the CRPs will be exponential. Assuming there are n switching boxes, two possible cases in each switching box, so the number of CRPs is 2^n, which indicate the arbiter PUF is a strong PUF. Arbiter PUF can also return longer response by input K different challenges and get a K bits response.

The normal arbiter PUF is vulnerable to modeling attack, the propose of XOR arbiter PUF is to increase the robustness of arbiter PUF. The basic concept is to integrated multiple parallel arbiter PUF, given same challenge to each arbiter PUF and XORed each response to produce final response(See Figure 2.7) [4]. According to simulation, in book [2] provides the XOR arbiter PUF will have nonlinearity property that makes it harder to model.

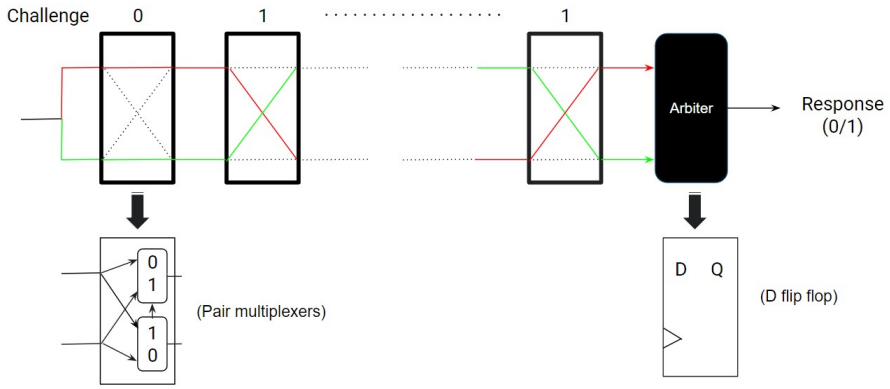

Figure 2.6: Arbiter PUF structure

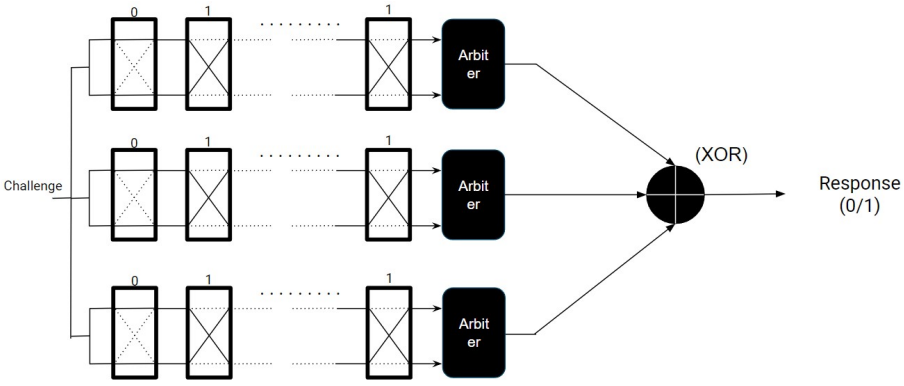

Figure 2.7: XOR arbiter PUF structure

2.5 Modeling attack on PUF

Many different threat can perform on devices, such as eavesdropped, gain access to the memory that store secret keys. For PUF, the main threat is that attacker can use technique like machine learning to simulate the behavior of CRPs(so called modeling), which means even without the devices, attacker can still response correctly when a challenge is provided. Take arbiter puf as example, assume an arbiter PUF with i switching box, and the challenge apply to each switching box is c[i]. The two signal travel through the the path determine by challenge, and arrive at the arbiter in different time because of the delay in each component. The final response depend on the sign of final delay difference:

$$r = \begin{cases} 1, & \text{if } \Delta c < 0. \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

which the delay difference is calculated by subtract the upper path with lower path's delay. The final delay difference Δc can represent as $w^T \Phi$, where w^T is a weight vector that represent delays for the components in PUF, and Φ is the applied i bits challenge [4]. It is clear that by accurately predicting the weight vector w, the pattern of the PUF can be observed. Machine learning such as logistic regression can play the role well. The modeling result for a arbiter PUF with 64 switching boxes, the logistic regression can get a good performance of 99.5% in very short time with 6800 training CRPs [4].

2.6 Reconfigurability of PUF

2.7 Summary

Chapter 3

Analysis

3.1 Project Requirements

3.2 Another Section

3.3 Ethical, Professional and Legal Issues

Chapter 4

Planning

4.1 Risk Analysis

4.2 Project Plan

4.3 Another Section if You Need It

Chapter 5

Conclusions

Bibliography

[1] Babaei, A., and Schiele, G. Physical unclonable functions in the internet of things: State of the art and open challenges. *Sensors*, 14 (2019).

[2] Maes, R. *Physically Unclonable Functions*. Springer, Berlin, Heidelberg, 2013.

[3] McGrath, T., Bagci, I. E., Wang, Z. M., Roedig, U., and Young, R. J. A puf taxonomy. *Applied Physics Reviews 6*, 12 (February 2019).

[4] Santikellur, P., Bhattacharyay, A., and Chakraborty, R. S. Deep learning based model building attacks on arbiter puf compositions. *IACR Cryptol. ePrint Arch. 2019* (2019), 566.

[5] Suh, G. E., and Devadas, S. Physical unclonable functions for device authentication and secret key generation. 9–14.

Appendices

Appendix A

An Appendix of Some Kind

Appendix B

Another Appendix