Faculty of Electronics and Computer Technology and Engineering

A LIGHTWEIGHT AUTHENTICATION SCHEME USING PHYSICAL UNCLONABLE FUNCTION FOR FPGA-BASED IOT APPLICATIONS

Mohammad Haziq Bin Ishak

Master of Science in Electronic Engineering

2024

A LIGHTWEIGHT AUTHENTICATION SCHEME USING PHYSICAL UNCLONABLE FUNCTION FOR FPGA-BASED IOT APPLICATIONS

MOHAMMAD HAZIQ BIN ISHAK

A thesis submitted
in fulfilment of the requirements for the degree of
Master of Science in Electronic Engineering

Faculty of Electronics and Computer Technology and Engineering

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2024

DEDICATION

I dedicate this thesis to my beloved parents, Ishak Bin Haji Ibrahim and Aini Binti Abd Hamid. Your unwavering love, encouragement, and sacrifices have been the driving force behind my academic journey. To my siblings, thank you for your constant encouragement and advice. Your presence in my life has been a source of strength and motivation. A special thank you goes to my supervisor, Ts. Dr. Mohd Syafiq Bin Mispan. Your guidance, patience, and expertise have been invaluable. You have consistently challenged me to push beyond my limits and strive for excellence. I am grateful for the countless hours you dedicated to reviewing my work, providing constructive feedback, and guiding me toward the right path. Additionally, I would like to express my gratitude to my co-supervisor, Assoc. Prof. Dr. Wong Yan Chiew, for your expertise and insights, which have enhanced the quality of my research. Your guidance and encouragement have been instrumental in my academic journey.

Finally, I thank everyone who contributed to my growth and development. Your support, encouragement, and belief in me have been instrumental in reaching this milestone. I am genuinely grateful for the opportunities I have been given and the experiences that have shaped me into the person I am today. To all those mentioned and the countless others who have played a part in my master's research, I offer my heartfelt appreciation. This thesis is dedicated to all of you as a token of my gratitude and appreciation for your unwavering support. Thank you.

ABSTRACT

The Internet of Things (IoT) describes the network of physical devices equipped with sensors and other technologies. This interconnectivity facilitates data exchange for processing and analysis, demanding a high level of trust to ensure security and authenticity for resource-constrained IoT devices. Physical Unclonable Functions (PUFs) have emerged as a promising solution to establish the root of trust for lightweight IoT devices. PUFs exploit the random intrinsic manufacturing process variations, creating unique and random mappings of challenge-response pairs (CRPs) specific to each PUF instance. This characteristic makes PUFs a promising technology for robust security applications. However, the PUF-based authentication scheme based on the CRPs database requires storing CRPs in the verifier database, which becomes a challenge as the number of devices to be authenticated grows. Additionally, while PUFs are physically unclonable, their function is susceptible to modelling attacks from machine learning (ML) techniques. Thus, developing secure PUFs for lightweight applications presents a significant challenge. Therefore, this thesis presents a lightweight authentication scheme without a CRP database by constructing a model of Arbiter-PUF with a challenge permutation technique in the verifier. This thesis presents three significant contributions. The first contribution presents the implementation of a physical Arbiter-PUF with random challenge permutation on Xilinx Artix-7 Field Programmable Gate Array (FPGA) boards. The relative placement method is used to ensure the symmetric routing for the physical Arbiter-PUF. As a result, the physical Arbiter- PUF achieves good quality in PUF metrics with 52.5% uniqueness, 96.87% steadiness, and 47.5% uniformity. In addition, the implementation of the random challenge permutation technique has successfully reduced ML-Attack vulnerability to ≈59% with 20,000 CRPs. The second contribution for this thesis is the implementation of the Arbiter-PUF model using the Artificial Neural Network (ANN) technique with random challenge permutation in the Xilinx Artix-7 FPGA board. The model is trained using MATLAB application with extracted CRPs from the physical Arbiter-PUF, achieving an accuracy of ≈98%. The successfully trained Arbiter-PUF model is subsequently designed in Xilinx System Generator and converted into an intellectual property (IP) core, which is then programmed into FPGA boards. Finally, the third contribution is the development of a lightweight PUF-based authentication scheme between the verifier (Arbiter-PUF model) and prover (physical Arbiter-PUF). The lightweight authentication scheme is implemented on two Xilinx Artix-7 FPGA boards, which serve as a verifier and a prover. Based on the validation of the authentication scheme, the verifier manages to differentiate between the genuine and the fake prover. Furthermore, the authentication scheme consumes 6.67× less area compared to the PUF-based authentication scheme based on the CRPs database for 1000 authentication processes and the power consumption for overall system's power demands consumes only 67mW, indicating a relatively low power requirement, making it well-suited for resource-constrained IoT applications.

SKIM PENGESAHAN RINGAN MENGGUNAKAN RANGKAP FIZIKAL TIDAK BOLEH KLON UNTUK APLIKASI IOT BERASASKAN FPGA

ABSTRAK

Internet Saling Berhubung (IoT) menerangkan rangkaian peranti fizikal yang dilengkapi dengan penderia dan teknologi lain. Kesalinghubungan ini memudahkan pertukaran data untuk pemprosesan dan analisis, menuntut tahap kepercayaan yang tinggi bagi memastikan keselamatan untuk peranti IoT yang dikekang oleh sumber. Physical Unclonable Functions (PUFs) telah muncul sebagai penyelesaian yang menjanjikan untuk mewujudkan akar kepercayaan bagi peranti IoT yang ringan. PUF mengeksploitasi variasi proses pembuatan intrinsik rawak, mencipta pemetaan unik dan pasangan jawapan cabaran (CRP) khusus untuk setiap PUF. Walau bagaimanapun, skim pengesahan PUF konvensional memerlukan penyimpanan CRP dalam pangkalan data pengesah, yang menjadi satu cabaran apabila bilangan peranti semakin meningkat. Walaupun PUF tidak boleh diklon secara fizikal, fungsinya terdedah kepada serangan model daripada teknik pembelajaran mesin (ML). Oleh itu, membangunkan PUF yang boleh dipercayai untuk aplikasi ringan memberikan cabaran yang ketara. Tesis ini mencadangkan skim pengesahan ringan tanpa pangkalan data CRP dengan membina model Arbiter-PUF dengan teknik pilih atur cabaran dalam pengesah. Tesis ini membentangkan tiga pencapaian. Pencapaian pertama membentangkan pelaksanaan Arbiter-PUF fizikal dengan pilih atur cabaran rawak pada papan Xilinx Artix-7 Field Programmable Gate Array (FPGA). Kaedah penempatan relatif digunakan untuk memastikan penghalaan simetri untuk Arbiter-PUF fizikal. Hasilnya, Arbiter-PUF fizikal mencapai kualiti yang baik dalam metrik PUF dengan 52.5% keunikan, 96.87% kestabilan dan 47.5% keseragaman. Selain itu, pelaksanaan teknik pilih atur cabaran rawak telah berjaya mengurangkan kerentanan ML-Attack kepada ≈59% dengan 20,000 CRP. Pencapain kedua untuk tesis ini ialah pelaksanaan model Arbiter-PUF menggunakan teknik Rangkaian Neural Buatan (ANN) dengan pilih atur cabaran rawak dalam papan FPGA Xilinx Artix-7. Model ini dilatih menggunakan aplikasi MATLAB dengan CRP yang diekstrak daripada Arbiter-PUF fizikal, mencapai ketepatan ≈98%. Model Arbiter-PUF yang berjaya dilatih kemudiannya direka bentuk dalam Penjana Sistem Xilinx dan ditukar menjadi teras harta intelek (IP) yang kemudiannya diprogramkan ke papan FPGA. Akhir sekali, pencapaian ketiga ialah pembangunan skim pengesahan berasaskan PUF yang ringan antara pengesah (model Arbiter-PUF) dan pembukti (Arbiter-PUF fizikal). Skim pengesahan ringan dilaksanakan pada dua papan Xilinx Artix-7 FPGA, yang berfungsi sebagai pengesah dan pembukti. Berdasarkan pengesahan skim pengesahan, pengesah berjaya membezakan antara pembukti tulen dan palsu. Tambahan pula, skim pengesahan menggunakan kawasan 6.67× kurang berbanding dengan skim pengesahan berasaskan PUF konvensional untuk 1000 proses pengesahan, dan penggunaan tenaga untuk permintaan tenaga keseluruhan sistem hanya menggunakan 67mW, menunjukkan keperluan tenaga yang rendah.

ACKNOWLEDGEMENT

Praise be to Allah, his majesty, for his uncountable blessings, best prayers, and peace be unto his best messenger Mohammad, his pure descendant, and his family and his noble companions.

First, I would like to thank my family. Without their support and love over the years, none of this would be possible. They have always been there for me, and I am thankful for everything they have helped me achieve.

Next, I would like to thank my supervisor Ts. Dr. Mohd Syafiq Bin Mispan, for your help and guidance over the years, which is unmeasurable, and without it, I would be where I am today. I will never forget everything that my supervisor advised and taught me for my future use.

Finally, thanks and appreciation to my parent, friend, and others for their moral support, encouragement, and constructive suggestion for the project and report completion from the beginning till the end

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

L	-	Channel length
W	-	Channel width
X_j	-	Source/drain junction depth
V_c	-	Volume of charge
Vth	-	Threshold voltage
V	-	Voltage
°C	-	Celsius
ε	-	Threshold value

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard.
ANN	-	Artificial Neural Network.
AVISPA	-	Automated Validation of Internet Security Protocols and Applications.
AID	-	Alias identities.
BST-APUF	-	Bit-self-test Arbiter-PUF.
BCH	-	Bose-Chaudhuri-Hocquenghem.
CNN	-	Convolutional Neural Networks.
CAD	-	Computer aided design.
COM	-	Communication.
CRP	-	Challenge-Response Pairs.
CRO-PUF	-	Configurable RO-PUFs.
CMA-ES	-	Covariance matrix adaptation-ES.
CMOS	-	Complementary metal oxide semiconductor.
CLB	-	Configurable Logic Blocks.
CO-PUF	-	Computational O-PUF.
DRAM	-	Dynamic Random-Access Memory.
DAPUF	-	Double-Arbiter PUF.
DL-based PUF	-	Deep Learning-based PUF.
ECC	-	Error Correction Code.
ES	-	Evolution strategies.
FPGA	-	Field Programmable Gate Array.

FIB	-	Focused Ion Beam.
FSM	-	Finite State Machine.
GPIO	-	General purpose input/output.
HD	-	Hamming Distance.
HW	-	Hamming Weight.
HMAC	-	Hash-based Message Authentication Codes.
HD UVC	-	High Definition USB-Video Class.
IR	-	Industrial Revolution.
IP	-	Intellectual property .
IC	-	Integrated Circuit.
IoT	-	Internet of Things.
I-PUF	-	Image-based PUF.
I/O	-	Input/Output.
LUT	-	Look-up Tables.
LFSR	-	Linear Feedback Shift Register.
LED	-	Light-emitting diode.
LWR	-	Linewidth roughness.
LR	-	Logistic regression.
ML	-	Machine Learning.
MUX	-	Multiplexer.
MOSFET	-	Metal oxide semiconductor field-effect transistors.
MLP	-	Multi Layer Perceptron.

NSA	-	National Security Agency.
OTV	-	Oxide thickness variation.
PMOD	-	Peripheral Module Interface.
PUF	-	Physical Unclonable Function.
PDL	-	Progammable delay logic.
PCS	-	Path-changing switches.
PKI	-	Public Key Infrastructure.
RSA	-	Rivest-Shamir-Adleman.
RPROP	-	Resilient backpropagation.
RO-PUF	-	Ring Oscillator PUF.
RAM	-	Random-Access Memory.
ReLU	-	Rectifier Linear Unit.
RDD	-	Random discrete doping.
ROM	-	Read-Only Memories.
SRAM	-	Static Random-Access Memory.
SVM	-	Support Vector Machines.
TDC	-	Time-to-Digital Converter.
TCL	-	Tool command language.
TID	-	Total ionizing dose.
TRNG	-	True random number generators.
TTP	-	Trivial Transfer Protocol.
TANH	-	Hyperbolic Tangent.

UART	-	Universal asynchronous receiver-transmitter.
XCRO-PUF	-	XOR-based CRO-PUF.
XM-PUF	-	XOR-based Multi-PUF.
2D	-	Two-dimensional.

LIST OF APPENDICES

LIST OF PUBLICATIONS

Journal

Mohammad Haziq Ishak, Mohd Syafiq Mispan, Wong Yan Chiew, Muhammad Raihaan Kamaruddin, and Mikhail Korobkov. Secure Lightweight Obfuscated Delay-Based Physical Unclonable Function Design on FPGA. Bulletin of Electrical Engineering and Informatics, 11(2):1075-1083, 2021.

Conference

Mohammad Haziq Ishak, Mohd Syafiq Mispan, Wong Yan Chiew, Muhammad Raihaan Kamaruddin, and Mikhail Korobkov. FPGA-based Obfuscated Delay PUF for Security Enhancement against ML-Attack. In 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pages 1-6, 2021.

CHAPTER 1

INTRODUCTION

Internet of Things (IoT) refers to a network of physical devices such as vehicles, home appliances, and other embedded devices. These embedded devices are integrated with processors, software, sensors, and connectivity, enabling them to establish connections and exchange data with other devices over the internet (Georgiana Dorobantu and Halunga, 2020). IoT devices can range from simple sensors and actuators to more complex devices such as smart home appliances, wearables, and industrial machinery. These devices are often designed to collect data, monitor their surroundings, and interact with other devices and systems to perform specific functions (Ammar et al., 2018). The potential benefits of IoT include increased efficiency, reduced costs, improved safety, and enhanced customer experiences. Nonetheless, the benefits of IoT also come with security challenges. A large number of devices and the complexity of the network make IoT devices vulnerable to security threats such as data breaches, cyber-attacks, and unauthorised access, ultimately compromising the security of data that is being transmitted over IoT networks. As a result, ensuring robust security for IoT devices and data privacy has become a critical concern that needs to be highlighted. These IoT devices are often limited in terms of processing power, memory, and energy resources. Therefore, providing lightweight security services such as authentication and identification presents a significant challenge.

1.1 Identification and Authentication in IoT Application

Identification and authentication in IoT applications refer to the implementation of secure and efficient mechanisms for verifying the IoT devices and users within an IoT application, as depicted in Figure 1.1. It aims to provide a balance between security, resource constraints, and computational efficiency in IoT devices, which often have limited processing power, memory, and energy resources.

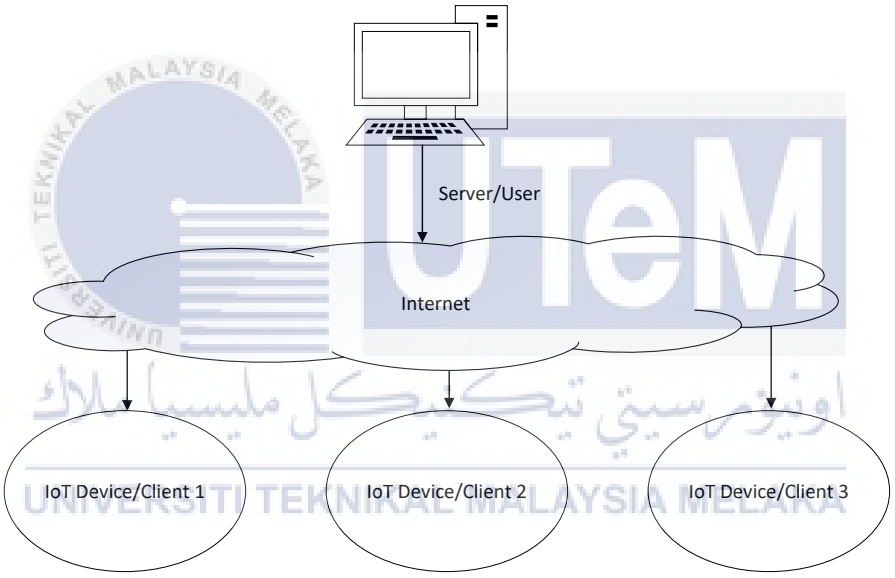

Figure 1.1: System model of IoT applications.

One commonly used technique in authentication and identification is symmetric key cryptography, which involves the use of shared secret keys for authentication and encryption. IoT devices and back-end servers securely store and exchange these keys to establish trust and authenticate each other. However, key management can become challenging as the number of IoT devices increases, requiring secure and large area overhead (Ubaidullah and Makki, 2016). Another technique in providing authentication is Hash-based Message

Authentication Codes (HMACs) which verify the integrity and authenticity of messages exchanged between IoT devices. HMAC utilises a shared secret key and a hash function to generate a message authentication code that is sent along with the message. While it provides integrity and authenticity, it does not offer confidentiality, making messages susceptible to eavesdropping (Jung and Jung, 2013).

Elliptic curve cryptography is another authentication and identification technique in IoT. It provides strong security with smaller key sizes compared to other algorithms, making it suitable for resource-constrained IoT devices. However, efficient implementation of elliptic curve cryptography may require specialised hardware support, which can increase device cost and complexity (Kumar et al., 2021). Public Key Infrastructure (PKI) is another technique that is crucial in establishing secure communication in IoT. PKI involves generating, distributing, and managing digital certificates for authentication. It provides a trusted infrastructure for identity verification and secure communication between devices and the back-end server. However, due to the associated computation and communication overhead, such certification is quite costly and not scalable for an IoT application (Chatterjee et al., 2019).

In summary, the current identification and authentication mentioned above have their limitation in terms of processing power, area overhead, and susceptibility toward adversary attack. Hence, another effective method of improving the security of resource-constrained IoT devices is necessary.

1.2 Physical Unclonable Function

Physical Unclonable Function (PUF) is a promising solution to security-related issues in resource-constrained IoT device (Di Martino et al., 2018). A PUF is defined as a function embodied in a physical material such as silicon that maps a set of challenges to a set of unique and random responses. These device-specific responses can be used as identifiers or secret keys. The key property of a PUF is the non-replicable characteristic caused by the process variations, even with a complete understanding of the design. The process variations are caused by uncontrollable deviations in the chip manufacturing process, which are unique and random from die to die and wafer to wafer. PUFs can be integrated directly into embedded systems during the manufacturing process without additional fabrication steps. In addition, a physically invasive attack to retrieve the identifier or key, which is only accessible during the power-on state through micro-probing, is likely to ruin the unique delay characteristics, thereby erasing the identification or key, which makes a PUF tamper-resistance solution. Based on the above reason, PUF is recognised as an efficient technique that provides lightweight authentication and identification for resource-constrained IoT devices.

1.3 Problem Statement

As described in Section 1.2, PUF's distinct features make it a very promising solution for providing secure, lightweight identification and authentication in IoT applications. Figure 1.2 depicts a PUF-based identification and authentication scheme that can be used

in IoT applications (Suh and Devadas, 2007; Delvaux et al., 2014). In general, the identification and authentication scheme is separated into two phases, which are enrollment and authentication. During the enrollment phase, a trusted party known as a verifier collects and securely stores the challenge-response pairs (CRPs) of genuine device A in a database. In the authentication phase, the verifier selects a random challenge from the database, sends the selected challenge to device A, and receives the corresponding PUF response from device A. If the response matches or is less than the specified Hamming Distance (HD) threshold compared to the stored value, device A passes the authentication. However, the authentication and identification scheme, as shown in Figure 1.2, opens a problem in which the verifier needs to store a huge amount of CRPs for IoT devices and poses a limitation in terms of the physical space overhead in the verifier.

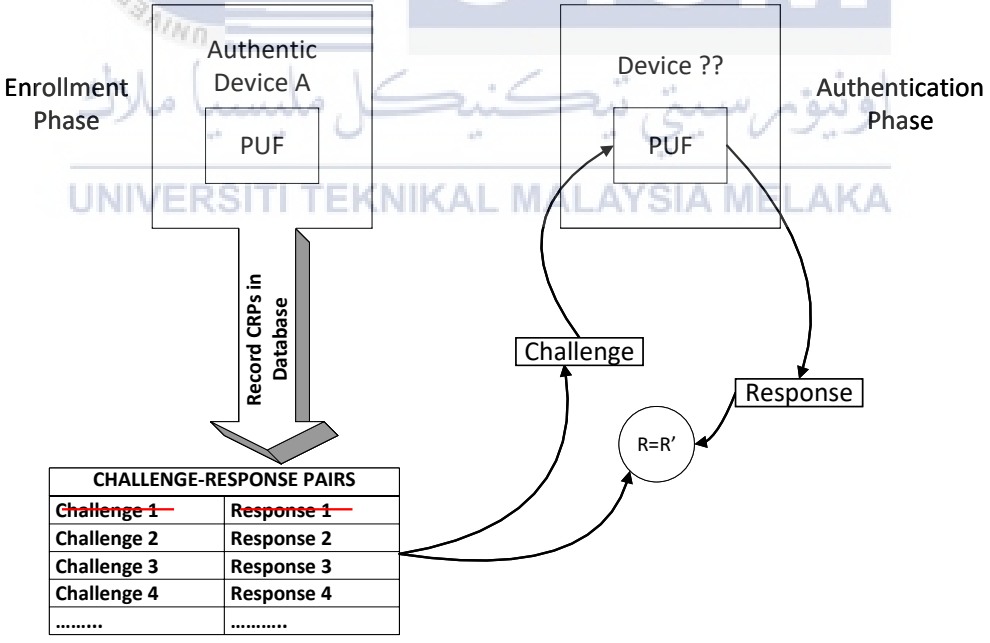

Figure 1.2: PUF-based identification and authentication.