Basel Halak *Editor*

Authentication of Embedded Devices

Technologies, Protocols and Emerging Applications

Springer

Authentication of Embedded Devices

Basel Halak
Editor

Authentication of Embedded Devices

Technologies, Protocols and Emerging Applications

Springer

Editor
Basel Halak
University of Southampton
Southampton, UK

ISBN 978-3-030-60768-5 ISBN 978-3-030-60769-2 (eBook)
https://doi.org/10.1007/978-3-030-60769-2

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To
Suzanne, Hanin and Sophia
with Love.

Preface

Authentication is the process of verifying the identity of a person or a physical object. One of the earliest techniques for authentication dates back to the Babylonian time in 200 BC, wherein fingerprints were used to sign contracts, which are subsequently verified by visual inspection.

Nowadays, authentication has become an integral part of electronic engineering and computer science fields. A trend driven by the proliferation of computing devices in all corners of modern life and the increased reliance on these to access services and resources online. Additionally, there are a rising number of applications that require the verification of the identity of an electronic device, such as tracking goods in manufacturing processes; secure products transfer in the consumer services industry, gaining access to subscribed TV channels, cash withdrawal in banking systems, and boarder control using e-passports.

Each of these applications has a diverse set of security requirements and a different amount of resources, which means existing solutions are no longer sufficient, either because they are too weak or because they are too expensive. This has led to a number of successful large scale cyber-attacks on vulnerable devices such as those extensively used for the internet-of things applications.

Another factor that is driving the development of new authentication schemes the significant levels of outsourcing in the hardware supply chain, which has increased the risk of integrated circuits (IC) counterfeit and intellectual property (IP) piracy. This means that there is an increase in the need to verify the authenticity of the electronic circuity in order to ensure that computing device is not forged or compromised.

The development of secure and efficient authentication schemes is therefore crucial to ensure the continued safe use of digital technology.

The prime objective of this book is to provide a timely and coherent account of the latest advances in the key research areas of authentication technology for semiconductor products. It has been developed as a collaborative effort among two international research groups, each providing an-up-to date summary of their latest findings and highlighting remaining challenges and research opportunities. To facilitate the understanding of the material, each chapter includes background

information explaining related terminologies and principles, in addition to a comprehensive list of relevant references. The book is divided into three parts to enhance its readability, namely; fingerprinting technologies, protocols and emerging applications of authentication schemes.

The Contents at Glance

This book explains principles of fingerprinting techniques with a special focus on hardware-based technologies, including physically unclonable functions and IC fingerprinting methods.

Afterword's, the book presents a number of state-of-the-art authentication protocols tailored for internet-of-things devices and energy-constrained systems. The development process of each protocol is discussed in details to allow reproducibility of the work. More specifically, the book explains how the design specifications of each protocol are derived from the system requirement, how to validate security assumptions using Scyther, and how to develop a hardware proof of concept for cost estimation and comparative analysis with existing solutions.

The book also discusses emerging applications for hardware-based authentication schemes, these include counterfeit mitigation techniques for the IC supply chain and anti-spoofing methods for the global positioning (GPS) system. More details on each chapter are provided below.

Part I: Fingerprinting Technologies.

Chapter 1 provides a comprehensive review of the fingerprinting technologies, with special, focus on circuit-based techniques.

Chapter 2 discusses in details the principles of physically unclonable functions (PUF), including design metrics, constructions and main applications.

Part II: Authentication Protocols.

Chapter 3 presents an authentication protocol and a key agreement scheme for the internet of things devices, which is based on the use of PUF technology to provide better physical security and more energy efficiency.

Chapter 4 present a two flight authentication protocol for energy constrained systems, which is based on combining elliptic curve cryptography with the use of a lightweight symmetric cipher.

Part III: Emerging Applications of Hardware-based Authentication.

Chapter 5 presents a hardware-based approach for products' authentication and tracking to mitigate the risk of counterfeiting in the IC supply chain. The technique is based on consortium blockchain and smart contract technologies, wherein each device incorporate a PUF that generates its unique digital identity.

Chapter 6 discusses hardware-oriented security applications for the authentication of users, devices, and data, and illustrates how physical properties of computing hardware (e.g. memory, computing units, and clocks) can be used for authentication applications in low power devices and the global positioning system (GPS).

Book Audience

The book is intended to provide a comprehensive coverage of the latest research advances in the key research areas of authentication technologies and protocols; this makes it a valuable resource for graduate students researchers, and engineers working in these areas. I hope this book will complement the ongoing research and teaching activities in this field.

Southampton, UK Basel Halak
June, 2020

Acknowledgments

I would like to thank all of those who contributed to the emergence, creation and correction of this book.

Firstly, I gratefully acknowledge the valuable contributions from all the authors, for taking the time to share his knowledge and for being very accommodating throughout the publication process. Special thanks go to the graduate students at the University of Southampton, University of Maryland and Morgan State University for the many hours they have spent working in their labs to generate the experimental results. Of course, the book would not be successful without the contributions of many researches and expert in hardware security and authentication protocols.

Finally, I would like to thank the great team at Springer for their help and support throughout the publication process.

Contents

Part I Fingerprinting Technologies

1 Integrated Circuit Digital Fingerprinting–Based Authentication 3
Xi Chen and Gang Qu

2 Physical Unclonable Function: A Hardware Fingerprinting Solution 29
Mohd Syafiq Mispan and Basel Halak

Part II Authentication Protocols

3 ASSURE: A Hardware-Based Security Protocol for Internet of Things Devices 55
Yildiran Yilmaz, Leonardo Aniello, and Basel Halak

4 TIGHTEN: A Two-Flight Mutual Authentication Protocol for Energy-Constrained Devices 89
Yildiran Yilmaz and Basel Halak

Part III Emerging Applications of Hardware-based Authentication

5 Securing Hardware Supply Chain Using PUF 115
Leonardo Aniello, Basel Halak, Peter Chai, Riddhi Dhall, Mircea Mihalea, and Adrian Wilczynski

6 Hardware-Based Authentication Applications 145
Md Tanvir Arafin and Gang Qu

Index 183

About the Editor

Basel Halak is the director of the embedded systems and IoT program at the University of Southampton, a visiting scholar at the Technical University of Kaiserslautern, a visiting professor at the Kazakh-British Technical University, an industrial fellow of the royal academy of engineering and a senior fellow of the higher education academy. He has written over 70-refereed conference and journal papers, and authored four books, including the first textbook on Physically Unclonable Functions. His research expertise include evaluation of security of hardware devices, development of appropriate countermeasures, the development of mathematical formalisms of reliability issues in CMOS circuits (e.g. crosstalk, radiation, ageing), and the use of fault tolerance techniques to improve the robustness of electronics systems against such issues.. Dr. Halak lectures on digital design, Secure Hardware and Cryptography, supervises a number of MSc and PhD students, and is the ECS Exchange Coordinators. He is also leading European Masters in Embedded Computing Systems (EMECS), a 2 year course run in collaboration with Kaiserslautern University in Germany and the Norwegian University of Science and Technology in Trondheim (electronics and communication). Dr. Halak serves on several technical program committees such as HOST, IEEE DATE, IVSW, ICCCA, ICCCS, MTV and EWME. He is an associate editor of IEEE access and an editor of the IET circuit devices and system journal. He is also a member of the hardware security-working group of the World Wide Web Consortium (W3C).

Part I
Fingerprinting Technologies

Chapter 1
Integrated Circuit Digital Fingerprinting–Based Authentication

Xi Chen and Gang Qu

Abstract As we move to the era of the Internet of Things (IoT), the embedded devices in IoT applications may contain a lot of sensitive information and many of them are attached to humans. This makes security and trust of these devices a new and challenging design objective. Device authentication is critical for any security-related features, but current cryptography-based authentication protocols are computational expensive. In this chapter, after a brief introduction of hardware-based lightweight authentication for embedded devices, we will focus on integrated circuit (IC) fingerprinting. Like human fingerprints, which have been used for thousands of years for identification, the key idea behind IC fingerprinting is to extract certain unique physical characteristics from the IC such that they can be used to identify and authenticate the chip (or device).

Digital fingerprinting was first proposed in 1999 for the protection of very large scale integration (VLSI) design intellectual properties (IP). Various techniques have been developed to make each copy of the IP unique in order to track the usage of the IP and trace any traitors who have misused the IP. We will review the general requirements and the available schemes to create digital fingerprints for IP protection. We will then discuss the challenges of applying these methods for device authentication in IoT applications and how to overcome these difficulties. As an example, we consider the fact that embedded devices are designed by reusing IP cores with reconfigurable scan network (RSN) as the standard testing facility and elaborate how to generate unique IC identifications (IDs) based on different configurations for the RSN. These circuit IDs can be used as IC fingerprints to solve the device identification and authentication problems. This IC fingerprinting method complies with the IEEE standards and thus has a high practical value.

Keywords IC Fingerprinting · Intellectual Properties (IP) · VLSI · Device authentication · IoT · Reconfigurable Scan Network (RSN)

X. Chen · G. Qu (✉)
University of Maryland, College Park, MD, USA
e-mail: xichen128@umd.edu; gangqu@umd.edu

B. Halak (ed.), *Authentication of Embedded Devices*,
https://doi.org/10.1007/978-3-030-60769-2_1

1.1 Introduction

An embedded system is a combination of (dedicated) software running on (customized) hardware and memory with application-specific input/output peripheral devices within another larger electrical or mechanical system. Although it is generally believed that the first embedded system is MIT's Apollo Guidance Computer designed to collect data at real time and to perform mission- and time-critical calculations for the Apollo Program, this concept was quickly picked up by the automobile industry and military applications for real-time computation, command control, and communications. In the late 1990s, with the advances in the Internet, wireless communications, and semiconductor fabrication technologies, the networked miniature embedded systems became ubiquitous and found all sorts of applications. Popular embedded systems can be found in multimedia applications (digital cameras, camcorders, TV set-top boxes, DVD players) and people's daily life (cell phones, answering machines, toasters, personal digital assistants). The key challenges for the design of these embedded systems were cost, power, size, safety, and time-to-market.

Then we entered the era of the Internet of Things (IoT). IoT is a group of devices or embedded systems that are connected by the Internet infrastructure to accomplish one or more specific applications without human interaction. Examples of the IoT include medical and healthcare systems, smart homes and buildings, and large nation-wide infrastructures such as power grid, transportation systems, and environmental monitoring systems. The embedded devices or the *THINGS* in the IoT normally have the capabilities of sensing (to collect data), computing (to process data and obtain knowledge), communication (to exchange data and knowledge), and execution (to carry out actions based on the knowledge). These *THINGS* can be sensors deployed for wild fire, earthquake, or landslide monitoring; they can be a Wi-Fi-enabled pacemaker, a smart meter in the power grid, or tire pressure sensors for an automobile. These IoT applications have brought, in addition to the design challenges for the traditional embedded systems, a set of new design objectives including: trust, security, privacy, ultra-low power, safety, and reliability [1]. The focus of this book is one important aspect of these challenges – the authentication of embedded devices, where we will review the current technologies and protocols for authentication with illustrations on emerging applications.

Embedded devices play a vital role in IoT applications; therefore, the authentication of these devices is equally important. The authenticity of a device not only identifies the device for system safety and maintenance, it also helps in cross-validating the integrity of the collected data, identifying the larger system that the device is embedded in and the user of the system, and enhancing system overall security. On the other hand, a compromised device could forge data, maliciously produce faulty results to mislead the decision-making process, or leak sensitive information of the user of the device. As we have pointed out in [1], utilizing hardware characteristics in the embedded devices for authentication has several advantages over traditional cryptographic solutions. In this chapter, we will discuss

digital fingerprinting-based approaches for device authentication with the focus on integrated circuit fingerprinting. Chapter 2 is dedicated to authentication based on physical unclonable function (PUF).

1.2 Chapter Overview

We aim to provide a comprehensive picture of the research and development of hardware digital fingerprint in the field of electronic design automation (EDA) community and the more general embedded systems design society. As we have introduced in the previous section, we will emphasize our discussion in digital fingerprinting–based device authentication.

First, in Sect. 1.3, we discuss the importance of authentication in embedded devices and IoT in general. We then briefly review some popular cryptographic solutions for authentication, which are computational expensive and thus are not applicable to the resource-constrained IoT devices. This motivates us to use hardware for lightweight authentication, which has some intrinsic advantages and is promising for IoT applications.

Then, in Sect. 1.4, we provide the foundations for integrated circuit (IC) fingerprinting-based authentication. We start with a review of the history of digital fingerprinting for VLSI design intellectual property protection. We then present the requirements and the general principles of using IC fingerprint for device authentication.

Next, in Sect. 1.5, we survey the representative approaches of IC fingerprinting techniques. These include both pre-silicon and post-silicon methods that cover all phases of IC design, fabrication, and testing.

We elaborate the details of a recently proposed circuit fingerprinting scheme based on reconfigurable scan chain network in Sect. 1.6. Because of the facts that scan chain and scan network are implemented in modern designs and the proposed scheme complies with IEEE standards, it has high practical value. Section 1.7 summarizes this chapter.

1.3 Hardware-Based Lightweight Authentication

1.3.1 The Need of Authentication in Embedded Devices

In 2013, the telecommunication giant Cisco Systems, Inc. introduced the term Internet of Everything (IoE), which brings "*together people, process, data, and things to make networked connections more relevant and valuable than ever before-turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and coun-*

tries". While IoE emphasizes the connection among the four pillars: people, process, data, and things, the things or embedded devices serve as its root. Data need to be collected and processed by devices such as sensors, people rely on devices such as smart phones to stay connected, and computer hardware does the process.

The goal of process in IoE is to "*deliver the right information to the right person (or machine) at the right time*". Authentication is the nature answer to these *rights* for all the four pillars of IoE. Although the *right* device is not explicitly mentioned in this statement, device authentication is the foundation for the authentication of others. The right information has to be collected by the right and trusted devices to ensure that the raw data is right to start with. The data integrity check is needed to verify that the data has not been modified during data transmission. On top of integrity check, devices at the senders, receivers, and all the nodes in between must be authenticated for data security. The right person can be authenticated with the person's biometric information or a password, as we will elaborate in the next section. Dedicated devices are required for such authentication and it is obvious that such devices must be authenticated and trusted. The right time can be an absolute time, which normally uses GPS as a reference, or a time instant depending on the occurrence of other events. In Chap. 6, we detail one novel approach that utilizes the system clock in the local embedded device to cross-validate the GPS signals in order to detect GPS spoofing attacks. As a conclusion, one can see that device authentication is the key for IoE security.

In 2014, when the EDA perspectives of embedded device design for IoT were presented [1], the authors listed the following design challenges for security and privacy:

- Which *THINGS* are collecting data/information?
- What data/information is collected by the *THINGS*?
- How data/information is collected and stored?
- Whom will the *THINGS* share the data/information with?
- How data/information is communicated among the *THINGS* and others?

These questions coincide precisely with the specific tasks to verify for the process we discussed above. Similarly, the answer to all of these questions is authentication. One needs to authenticate the device to know which *THINGS* are collecting data, to authenticate the data and the process of data collection and storage to ensure data integrity, to authenticate users and other devices that the *THINGS* are interacting with, and to authenticate the communication channel.

1.3.2 Classical Authentication Protocols

We briefly discuss digital signature and challenge-response protocol for authentication. More details can be found in Part II of this book. The goal of this introduction to authentication protocols is to show their high computation and run time complexities and to give the motivation for hardware-based lightweight authentication.

In the context of digital data authentication, digital signature and challenge-response protocol are two of the most popular methods. Digital signature can authenticate both the source of the message and its integrity (which means that the message has not be altered). A digital signature scheme normally has three components: key generation, which selects the cryptographic keys; signature signing, which creates the signature for a given message using the private key; and signature verifying, which validates the authenticity of the signature and the message using the public key. Current digital signature schemes in use include digital signature algorithm (DSA), elliptic curve DSA, RSA-based signatures, and so on. These schemes are all based on intractable mathematical problems and involve expensive computations such as modular exponentiation where the exponents are cryptographic keys. As it is recommended to use 1024-bit or at least 512-bit keys, most of the embedded devices cannot afford to implement traditional digital signature–based authentication.

In the challenge-response authentication protocol, one party (the verifier) asks a question (i.e., challenge) and the other party (the proofer) must provide an answer (i.e., response), which the verifier will check and then decide to accept or reject the proofer's authenticity claim. One of the simplest examples of challenge-response protocol is the password authentication method, which many systems are using. In such a method, a user (the proofer) will provide a pair of user name and password and the system will then verify the password based on the user name to authenticate the user (actually the pair of user name and password). Validation of the response typically relies on some cryptographic operation. The responses need to be stored in the system securely. Both will be a challenge for the resource-constrained embedded devices.

Recently, there is the trend of using multifactor authentications, which requires two or more of the following factors: knowledge factors (such as password, challenge-response pair, or answers to security questions that the user knows), ownership factors (such as a smart phone or an ID card that the user has), inherence factors (such as the fingerprint, iris, voice, or movement that are unique and can be used to identify the user), and other factors (such as the location where the user is). Note that most of the multifactor authentication protocols are a combination of cryptographic based methods and other noncrypto mechanisms. Although enhancing security is the goal of such combination, we see that the computation complexity is reduced at the same time.

1.3.3 Hardware-Based Lightweight Authentication

In the above multifactor authentication protocols, the noncrypto mechanisms take advantages of certain physical objects that belong to the user for authentication. For example, a code sent to the user's smart phone can be used to verify that the claimed user does possess the phone. The fingerprint or iris information of the user can be matched to that stored in the database to authenticate the user.

These operations normally do not necessarily require cryptographic computation. However, they lack a sound mathematical foundation to prove the security level of the authentication they can provide. So in multifactor authentication, these are considered as the enhancement of the crypto-based knowledge factors.

Security and privacy are among the key concerns for the development of IoT applications and the design of the IoT devices. A January 2014 article in Forbes listed many Internet-connected appliances that can already "spy on people in their own homes," including televisions, kitchen appliances, cameras, and thermostats [2]. Embedded devices in automobiles such as brakes, engine, locks, hood and truck releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network. The vehicle-to-vehicle and vehicle-to-infrastructure communication makes everyone's driving habit and daily commute route public [3].

Mathematically strong and well-developed cryptographic techniques exist for all kinds of security-related applications such as data encryption/decryption, user and devices authentication, secure computation and communication. Most of these crypto security primitives or protocols are (extremely) computationally expensive (for example, performing the modular exponentiation operation for large numbers of hundreds of bits). Unfortunately, in the IoT domain, the devices are extremely resource constrained and do not have the required computational power, memory, or (battery) power for such operations. As a result, in many IoT applications, both data and control communications, such as those between wearable/implantable medical devices and doctor or patient, are in plain text, which creates serious security vulnerabilities.

Authentication based on physical features (such as bioinformatics and hardware manufacture variations) is built on the following two important observations in IoT applications and embedded devices:

Constrained resources. The computation power, memory size, CPU speed, battery capacity, communication bandwidth, transmission range, and other resources on many embedded devices are limited and hard or impossible to renew. Thus, the mathematical sound cryptographic solutions are not applicable.

Imperfect match. Cryptographic algorithms work in the digital domain, where even one bit of error is considered as a mismatch and an erroneous bit in the key could alter many bits. However, the IoT applications normally deal with analog world where a perfect match, for example, in human fingerprint or voice, is hard to find and not necessary for authentication purpose.

Embedded device authentication demands resource efficiency but not the highest level of security. This gives us the opportunity to develop noncryptographic solutions. One promising direction is using the hardware (i.e., the chips or ICs) in the embedded devices. In this chapter, we will focus on how to generate IC fingerprints for such purpose.

1.4 Principles of Digital Fingerprinting–Based Device Authentication

1.4.1 IC Digital Fingerprints

Fingerprints are the characteristic of an object that is completely unique and incontrovertible so they can be used to identify a particular object from its peers. They have been used for human identification for ages and have been adopted in multimedia for copyright protection of widely distributed digital data. In the semiconductor and IC industry, the concept of digital fingerprinting was proposed in the late 1990s with the goal of protecting design IP from being misused [4–8]. In this context, digital fingerprints refer to *additional features that are embedded during the design and fabrication process to make each copy of the design unique*. These features can be extracted from the IP to establish the fingerprint for the purposes of identification and protection.

In [9], a new semiconductor capacitive sensor structure is proposed and the fabrication process for a single-chip fingerprint sensor stacked on a 0.5−/spl mu/m CMOS LSI is presented. This technology has been successfully commercialized, and it currently used in IoT devices for identification purpose. In [10, 11], the concept of IP metering was proposed to allow design houses to achieve postfabrication control over their ICs. The enabling technology behind metering is the creation of unique identifiers (also called tags or fingerprints) for each copy of the IP. A comprehensive survey on hardware metering can be found in [12], and we will not elaborate here. Several practical IP fingerprinting techniques were studied in [13–15], which we will discuss in the next section.

In the context of IP protection by fingerprinting, the goal is to give each user a copy of the IP containing a unique fingerprint, which can be used to identify that user in order to prove that he/she is innocent should an illegally copied IP being found. It is one instance of the so-called *statistical fingerprinting* that can be characterized as: given sufficiently many misused objects to examine, the distributor can gain any desired degree of confidence that he/she has correctly identified the compromised [16]. The identification of the fingerprint is, however, never certain. When hardware-based fingerprint is used for device authentication, this principle also applies. It is because of this fact that there is no theoretical guarantee on the strength of authentication, we refer to this approach as *lightweight authentication*.

1.4.2 Requirements for Hardware-Based Device Authentication

Based on the requirements for a fingerprinting scheme to be effective [15] and considering the specialties in embedded device authentication, we propose the following requirements for fingerprinting-based device authentication:

High credibility. The fingerprint or other hardware identifiers should be readily detectable in proving the claimed identity for authentication. The probability of coincidence (i.e., the fingerprint is caused by accident, not by design) should be low.

Low cost. The hardware-based authentication process should incur minimal resource of all kinds, including memory, energy consumption, and communication bandwidth. If the fingerprints are added only for authentication, ideally it should not introduce any design overhead.

Fast processing. The verification process of the fingerprint should be sufficiently fast in order to satisfy the requirement of real-time device authentication for many of the application scenarios.

High resilience. The fingerprint and other hardware features used for authentication purpose should be difficult or impossible to remove even with partial or complete knowledge of the authentication protocol.

No information leak. The fingerprint and other hardware features are designed to verify device identity. They should not leak any other sensitive information about the device and the data it collects or stores during the authentication process.

Large volume. Because each device must have a unique fingerprint or other hardware feature, there should be abundant of them to accommodate the large amount of embedded devices deployed in various applications. The run-time for creating these fingerprints in bulk must be low as it is impractical to generate them one by one.

High reliability. The fingerprint or other hardware feature should be ready to be extracted and processed for device authentication under the working environment of the devices. Due to the variety of the devices and the harsh environment they might be deployed to, these hardware identifiers must be reliable at the variation of factors such as temperature, humidity, altitude, air pressure, radiation, device aging, etc., which will be highly application dependent.

Collusion free. Identical devices, although they are identical, should receive different hardware identifiers or fingerprints to distinguish them from each other. These identifiers or fingerprints should be designed in such a way that it is difficult to forge a new identifier or fingerprint from the existing ones.

Most of the above requirements are not restricted to fingerprint, they are applicable to device authentication methods based on other hardware features as well. For example, silicon physical unclonable function (PUF) is considered as a unique intrinsic hardware characteristic and Chap. 2 of this book is dedicated to the authentication with PUF. As we will see in that chapter, the design and implementation of PUF based device fingerprint also consider such requirements.