Microprocessors and Microsystems 45 (2016) 56–66

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Study on PUF based secure protection for IC design

Wei Liang[a,b,*], Bo Liao[a], Jing Long[a], Yan Jiang[a], Li Peng[a,b]

[a] College of Mathematics and Econometrics, Hunan University Changsha, Hunan, 410082, China
[b] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China

ARTICLE INFO

Article history:
Received 21 June 2015
Revised 13 February 2016
Accepted 11 March 2016
Available online 16 March 2016

Keywords:
IC
IP
Reuse
PUF
CRP

ABSTRACT

The rapid progress in integrated circuit (IC) technology makes the gates in a single chip increase by Moore's law. The complexity in design and verification grows accordingly. To address this issue, intellectual property (IP) reuse is prevalently used in system design. However, it may incur IP piracy or illegal copy, which brings big threat to IP protection. When IP dispute occurs, the ownership verifier can activate the Challenge Response Pair (CRP) of Physical Unclonable Function (PUF) to verify IP copyright. In this work, we have analyzed and summarized PUF techniques and current research status. Furthermore, several typical PUF techniques are concretely illustrated and compared. Besides, we demonstrate PUF in multiprocessor by analyzing security and overhead on previous PUF techniques. Finally, we envision the future of PUF techniques and their applications.

1. Introduction

In recent years, electronic products are widely used in people's daily life and the security issue attracts more and more attention [1]. There are many challenges to security, such as counterfeiting, cloning, reversing engineering and vicious addition of components. Although popular reuse technology has brought great convenience to Semiconductor Company, it makes Integrated Circuit (IC) copyright easy to be misused. The semiconductor companies are suffering tremendous financial loss, e.g., cable television. Illegal user may copy the circuit in the set top box and crack the secret key. They will enjoy free television service through cracking [2]. Popularly, identification system realizes ownership protection by inserting a Radio Frequency Identification (RFID) label into one of the Intellectual Property (IP) cores [3–6]. However, the insertion lacks secure protection, illegal attackers can still read the sensitive information in RFID label and clone a new card with the same functionality surreptitiously. It causes damage to benefits of Cable Television Company. Consequently, it is crucial to protect IP components in IC design by utilizing secure reliable mechanisms.

Generally, immature protection techniques bring big challenges to forensics and judicial authentication. The confidence crisis in IP ownership presses for effective protection techniques in order to deter IP infringement. Recently, researchers have proposed many IP watermarking methods [7–11]. These methods embed watermarks at various abstract levels, but cause growth of hardware resource, such as area, speed and power consumption. Furthermore, the performance of IP circuit is also affected. Therefore, there are many bottleneck issues to be solved in IP protection methods.

With the rapid advance of IC, Physical Unclonable Function (PUF) [12–15] emerges as a new technique to identify a single physical device. It is a chip-dependent unclonable challenge-response function that can uniquely identify a specific integrated circuit. The physical features of device are utilized to realize the mapping from an input signal to an unpredictable output.

The unique structure of PUF utilizes many random factors in manufacturing. So, it is hard to be forged. We utilize the notations *C, R, F*to denote the challenge of PUF, response of PUF and the mapping relationship respectively. There are four characteristics of PUF techniques, summarized as follows:

(1) Unpredictable. Given a specific PUF, it is hard to derive F from a set of challenge-responses $Q = \{C_i, R_i\}, i = 0, 1, 2, \ldots q$. To add a new challenge C_{q+i} to this structure, it is almost impossible to correctly predict R_{q+i}.
(2) Non-repeatability. Even with precise manufacturing technology and the same CRP, nobody can produce a same PUF structure B with the existing PUF A, both of which have the same mapping relationship.
(3) Uniqueness. The entities A and Bproduced by the same PUF have various mapping relationship F_A and F_B. The responses R_A and R_B are different even imposing the same challenge C to them.

* Corresponding author. Tel.: +18613981299.
E-mail addresses: idlink@163.com (W. Liang), boliao@yeah.net (B. Liao), jlong@hnu.edu.cn (J. Long), yjiang@hnu.edu.cn (Y. Jiang), lpeng@hnu.edu.cn (L. Peng).

http://dx.doi.org/10.1016/j.micpro.2016.03.012
0141-9331/

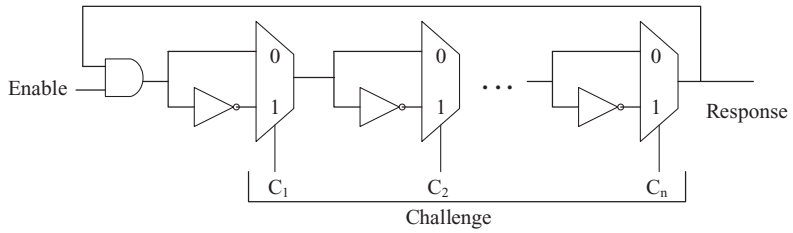

Fig. 1. The CRP structure of PUF circuit.

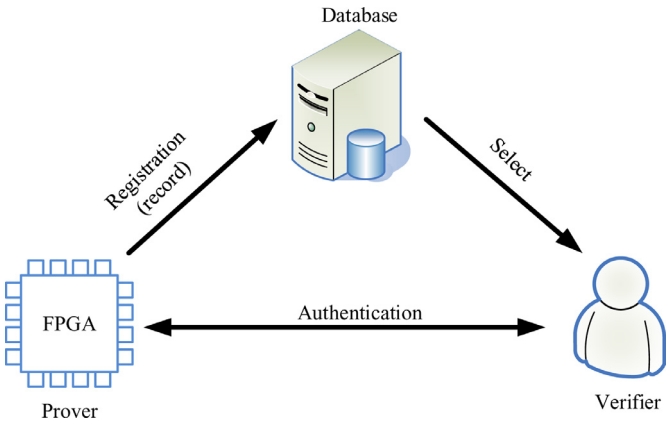

Fig. 2. The structure of PUF based identity authentication system.

(4) Robustness. With the same challenge x to PUF, the same response $y = \Gamma(x)$ is returned with a tolerance of a few errors. These errors should be within the range of distance measurement. Namely, the responses with subtle difference are close in distance measurement. The robustness of PUF is measured by intra hamming distance histogram. This feature is an essential difference between PUF and pseudo-random number generator (PRNG). Almost all of existing PUF implementations are robust.

As shown in Fig. 1, input and output signals of PUF circuit are respectively called Challenge and Response. The Challenge-Response Pair (CRP) exists when the circuit is power-on. PUF can be used to address the security issues in traditional cryptology, such as key storage. The PUF circuit of each electronic device has unique CRP, which is similar to biological identification information, such as fingerprint and voice. Consequently, one device can be distinguished from other devices according to CRP. Fig. 2 shows structure of PUF based identity authentication system. The CRPs of PUF circuit is stored in a public database. If copyright dispute occurs, the verifier can add some specific challenge information to PUF. The generated responses are then compared with the stored responses. If they are consistent, the identification is successful. Le-tus suppose that PUF is used in television business. A user carries his identification card with PUF to bank. The card is then placed in a specific terminal with the database of PUF CRPs in manufacturing. According to the ID of this card, the terminal will impose a specific challenge to PUF. By comparing the returned response and the stored one, the correctness of this card can be verified.

In this work, we summarize previous PUF based IP protection methods and analyze differences among various PUF techniques. Meanwhile, PUF techniques for real-time IP protection are studied. We predict that PUF based IP protection methods will provide good technical support for IP design and IC manufacture. Moreover, it is beneficial to sound development of future IC.

2. Concept and classification

2.1. Concept of PUF

PUF technique is a novel method to extract secret from a complex physical system. It utilizes the random variation in manufacturing, intentionally added or carried by itself, to realize the uniqueness of a chip. The challenge-response pairs of PUF exist when the product is power-on. So, the issue of key storage in IC can be addressed by PUF circuit when the product is running. The characteristic of no-cloning has greatly improved the security, making it superior in information security.

The identity authentication flow is shown in Fig. 3. The challenge and response pairs of PUF in authentic device are recorded in database. When the device is used in an untrusted environment, PUF can provide evidence in authentication. If the response is consistent with the stored one in database, authentication is successful (case 1). Otherwise, it fails (case 2). PUF utilizes manufacturing variations to authenticate device. In this way, it is unnecessary to store keys in memory. Meanwhile, the unclonable CRPs improve security of PUF circuit. It is predictable that the study on PUF-based IP protection will offer technical support to IP design and IC manufacturing. It plays an important role for healthy development of future IP circuit.

In recent years, many scholars have conducted researches on PUF based IP protection techniques. These techniques are classified into four categories based on features of PUF circuit.

2.2. Classification of PUFs

In this section, we have classified existing PUFs into four groups: Non-electronic PUF, Physical characteristic based PUF, Memory based PUF and Delay based PUF. The detailed classifications are summarized in Fig. 4. The related references are concretely illustrated in the subsections.

2.2.1. Non-electronic PUF

A typical PUF technique is proposed by Pappu et al. [16] by utilizing optical physical characteristics. It is realized by an optical device with transparent material. There are optical scattering particles in transparent material, which can be randomly added to chip manufacturing technique. When a laser beam is casted over optical scattering particles, a few random speckles are produced. These speckles can record the position, angle or other parameters (such as amplitude and wave length) of the laser. They are utilized as secret keys and added into chip manufacturing. Since the response of optical PUF always depends on physical characteristic of optical token, the circuit may have two different CRPs. In this case, it is easy to prevent IP circuit from being copied by illegal users. Moreover, Lim et al. in reference [17] proposed a structure with randomly changing characteristics based on physical attributes of the token. The structure marks the characteristic for tamper-proofing in IP circuit by altering CRP of PUF.

In addition, Bulens [18] proposed a concept of paper PUF structure that utilizes the irregular physical features in paper file to pre-