Microelectronics Reliability 88–90 (2018) 360–364

Contents lists available at ScienceDirect

Microelectronics Reliability

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

Simulation-based evaluation of probing attacks to arbiter PUFs using a time-resolved emission microscope

Katsuyoshi Miura*, Atsuki Seko*, Koji Nakamae*

Graduate School of Information Science and Technology, Osaka University, Yamada-Oka 1-5, Suita, Osaka 565-0871, Japan

ARTICLE INFO

Keywords:
Arbiter PUF
Time-resolved emission microscope
Security
Authentication
Encryption

ABSTRACT

Probing attacks to arbiter PUFs (physical unclonable functions) using a time-resolved emission microscope are evaluated by simulation. It is assumed that signal delay in the arbiter PUF chip is measured directly by using a time-resolved emission microscope. Only two challenge inputs are required to do that. A simple procedure can predict the response of the arbiter PUF. The relationship between the rate of successful response estimation and the accuracy of signal timing measurement is evaluated by simulation. The simulated results show the rate of successful response estimation is 70% when the accuracy is around 30 ps. A time resolution of 12.5 ps has been achieved by the commercial time-resolved emission microscope, so that this result shows the feasibility of the probing attacks to arbiter PUFs using a time-resolved emission microscope.

1. Introduction

In the advanced information society, security technology such as authentication and encryption is getting more and more important. The secret key is indispensable in authentication and decryption of ciphertext. Once an attacker obtains a secret key, the attacker can easily pass through the authentication or decrypt ciphertext. In many systems, the secret key is recorded in a nonvolatile memory or embedded in a decryption processor chip and cannot be read out directly. It is reported there are various attack methods that steal the secret key from such a system [1]. Side channel attack is one of such attack methods [2]. This method observes secondary signals from devices such as fluctuations in power supply current and electromagnetic radiation.

PUF (Physical Unclonable Function) technology that performs encryption/decryption and authentication without directly holding a secret key itself in the system has attracted attention [3]. The PUF is a technology for generating cryptographic keys and authenticating by utilizing physical characteristics, such as electronic delays, built in the devices when they were manufactured. Because the PUF performs encryption and authentication without directly holding the key, it is tolerant to various eavesdropping attacks.

Various types of PUF such as ring oscillator PUF [4], arbiter PUF [5], and so on have been proposed. They are divided into two types: weak PUF with a small number of combinations of challenge input and response, and strong PUF with a large number of combinations. The importance of arbiter PUF, which is a strong PUF with a relatively simple structure and wide application range, is increasing.

Failure analysis tools such as the time-resolved emission microscope are used to analyze the faulty IC chip. These tools can observe the internal behavior of the IC chip. Therefore, it can be used to attack the security chip [6]. S. Tajik and colleagues showed the possibility of attack to arbiter PUFs using a time-resolved emission microscope [7]. However, the relationship between the rate of successful attack to arbiter PUFs and the accuracy of timing measurement has not been clarified.

In this study, we evaluate probing attacks to arbiter PUFs using an emission microscope. The relationship between the rate of successful response estimation and the accuracy of timing measurement is evaluated by simulation.

The rest of this paper is organized as follows. Section 2 provides a brief overview of the arbiter PUF. Section 3 explains how attackers estimate the output of arbiter PUF by using an emission microscope. Section 4 shows conditions and results of simulations that were carried out in order to evaluate the relationship between the rate of successful response estimation and the accuracy of timing measurement. Finally, Section 5 concludes this paper.

2. An overview of the arbiter PUF

Fig. 1 shows the circuit configuration of the arbiter PUF (APUF) that outputs single bit response $r \in \{0,1\}$. It consists of n stages connected in series and a timing comparator at the end of them. A D flip-flop (DFF) is

* Corresponding authors.
E-mail address: miura@ist.osaka-u.ac.jp (K. Miura).

https://doi.org/10.1016/j.microrel.2018.06.103
Received 31 May 2018; Received in revised form 26 June 2018; Accepted 28 June 2018

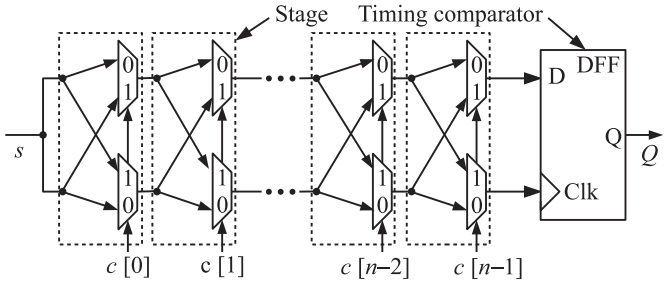

Fig. 1. Circuit configuration of the arbiter PUF.

used as the timing comparator. Each stage consisting of two multiplexers has two outputs and three inputs. One of the inputs is a single bit of challenge $c[i] \in \{0,1\}$ ($i \in \{0,\cdots,n-1\}$), and the other inputs are connected to the outputs of the previous stage. The inputs of the first stage are connected to a primary input s. A rising or falling signal is applied to the input s, and this signal reaches the timing comparator through n stages. At each stage, the signal passes through either the upper or lower multiplexer depending on the value of the challenge bit c[i]. It is difficult to predict the response because the response varies depending on the combination of challenge bits and the circuit delay along the signal propagation path.

The arbiter PUF is utilized as follows when it is applied to authentication. In advance, multiple challenges are applied to the device and corresponding responses are obtained. The challenge and response pairs are stored in the authentication server. When the authentication is carried out, a challenge transmitted from the server is applied to the device, and an observed response is returned to the server. If this observed response matches that stored in the server, the authentication succeeds. Since the challenge-response pair is disposable and not reused, eavesdropping during communication of challenge and response does not become a security risk.

3. Output estimation of arbiter PUFs using a time-resolved emission microscope

In this study, we assume an attacker estimate the response of arbiter PUFs by using the following procedure.

1. Two challenge inputs, all-0 ($c[i] = 0, \forall i$) and all-1 ($c[i] = 1, \forall i$), are applied and the light emission from driver transistors are observed at each stage with a time-resolved emission microscope. The driver transistors are indicated in Fig. 2. Three kinds of multiplexer implementations, (a) AOI, (b) NAND, and (c) transmission-gate based implementations, are shown in the figure. Gate-level and transistor-level schematics are shown in the left and the right side, respectively. The driver transistors are shaded. Here, it is assumed that a rising signal is applied to the PUF. In the case where a falling signal is applied, NMOS transistors in the pull-down network become driver transistors. Time-slice images around the driver transistors or emission intensity waveforms at the driver transistors are obtained.
2. Switching timings $T_{Px}[i]$ of multiplexers are obtained by detecting the peak of emission intensity from the time-slice images or the waveforms. Here, $P \in \{U,L\}$ denotes the upper or lower side multiplexer, $x \in \{0,1\}$ shows all-0 or all-1 challenge input, and $i \in \{0,\cdots,n-1\}$ is the stage number, as shown in Fig. 3. It is not necessary to acquire $T_{U0}[-1]$, $T_{L0}[-1]$, $T_{U1}[-1]$, and $T_{L1}[-1]$ (these are shown in dashed arrows in Fig. 3). An arbitrary value such as 0 is substituted to these variables. This value will be canceled out when two signal timings are compared in the next step.
3. The output Q of the APUF is estimated with the procedure shown in Fig. 4. In this procedure, signal transmission delay is accumulated depending on the challenge input $c[i]$. T_U and T_L are signal arrival timing at the "D" and "Clk" input terminals of the DFF (timing comparator), respectively. These signal arrival timings are compared at line 13 in Fig. 4. Here, τ is the timing offset between the two inputs.

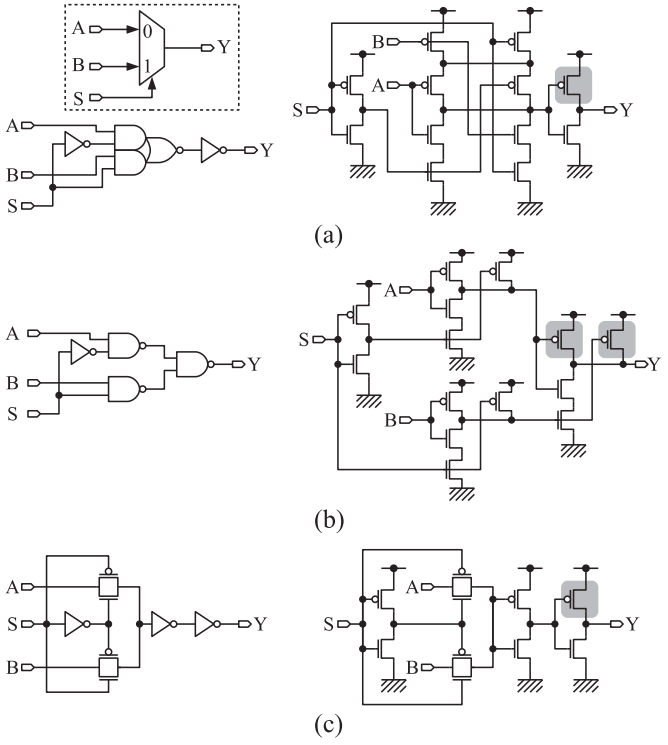

Fig. 2. Implementations of the multiplexer and driver transistor locations: (a) AOI, (b) NAND, and (c) transmission-gate based implementation.

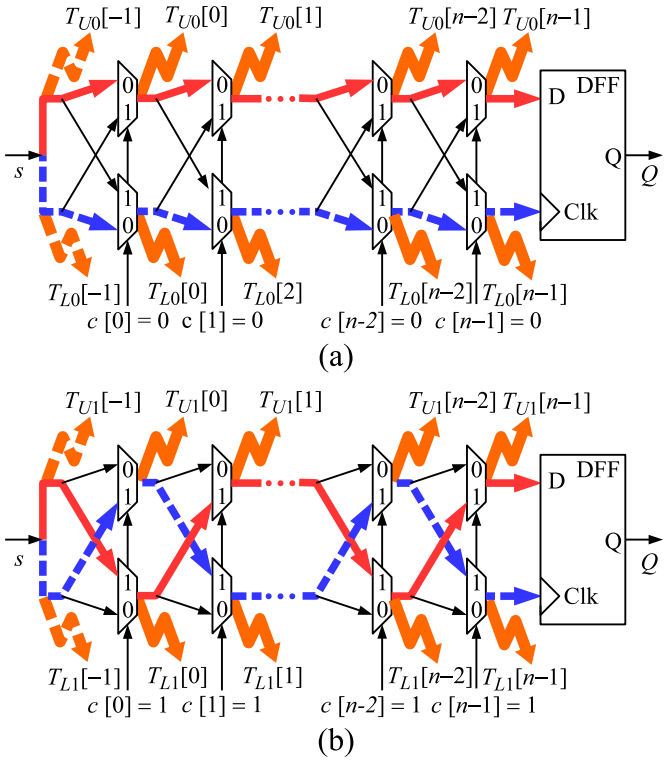

Fig. 3. Applied challenge bits and the multiplexers measured by an emission microscope: (a) all-0 and (b) all-1.