Microprocessors and Microsystems 52 (2017) 325–332

Contents lists available at ScienceDirect

Microprocessors and Microsystems

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

Fast and reliable PUF response evaluation from unsettled bistable rings

Robert Hesselbarth[a,*], Johann Heyszl[a], Georg Sigl[a,b]

[a] Fraunhofer AISEC, Parkring 4, Garching 85748, Germany
[b] Institute for Security in Information Technology, Technische Universität München, Arcisstr. 21, München 80333, Germany

ARTICLE INFO

Article history:
Received 20 December 2016
Revised 8 April 2017
Accepted 4 June 2017
Available online 8 June 2017

Keywords:
Physical unclonable function
Unsettled bistable ring
Twisted bistable ring PUF
FPGA

ABSTRACT

Bistable ring (BR) based strong PUFs are promising candidates for lightweight authentication applications. It has been observed that a good '0'/'1'-balance of their responses correlates with longer settling times. This is problematic, since the state-of-the-art evaluation method requires the BR to be settled in order to generate a reliable PUF response. We show that settling times can easily extend beyond 100 ms for 70 percent of the responses in the TBR PUF, which is a BR-based PUF with good '0'/'1'-balance characteristics. Hence, it is practically impossible to wait for all BRs to settle, which results in a reliability penalty. In order to solve this problem, we present three new methods, which allow the evaluation of unsettled BRs with increased reliability compared to the state-of-the-art method. We were able to improve response reliability from 81 percent to up to 98.5 percent and achieve response reliabilities of 97 percent at an evaluation time of 320 ns. This enables the fast and reliable use of BR-based PUFs in strong PUF applications.

1. Introduction

Electrical intrinsic physical unclonable functions (PUFs) [4] are widely discussed in the literature as they can be easily and cheaply integrated into integrated circuits (ICs) and hence, into most electronic products. Their applications range from authentication and device identification [5] to cryptographic secret key generation and storage replacing secure non-volatile memory (NVM) [3,9,10]. physical unclonable functions (PUFs) can be divided into weak physical unclonable functions (PUFs) and strong physical unclonable functions (PUFs). For key generation and storage so-called weak physical unclonable functions (PUFs) are used, which provide only the number of bits needed for one or a few keys. A prominent example for a weak PUF primitive is the static randomaccess memory (SRAM) PUF [6,7]. In contrast to weak physical unclonable functions (PUFs), strong physical unclonable functions (PUFs) provide a challenge-response interface with a great number of challenge-response pairs (CRPs) making it practically impossible to read out all challenge-response pairs (CRPs). challenge-response pairs (CRPs) are device-unique and unpredictable. These properties allow authentication without the need for conventional cryptographic primitives [6,13], such as block ciphers or hash functions.

In search for electrical intrinsic PUF primitives that satisfy the strong PUF requirements, several different designs have been proposed. The arbiter PUF [9,12] was one of the first. However, its challenge-response pairs (CRPs) can be predicted with high accuracy after observing a rather small number of challenge-response pairs (CRPs) using methods of machine learning [14]. In 2011 Chen et al. proposed the bistable ring PUF (BR PUF) [1,2] in the hope that it might be more resistant against machine learning attacks because it had no obvious model who's parameters could be learned in order to predict challenge-response pairs (CRPs). A BR is an inverter ring with an even number of stages. The bistable ring PUF (BR PUF) uses the challenge to select a BR configuration, which is then used to generate a response by observing the BR's behavior. In 2014 Schuster et al. showed that an explicit model is not needed, to successfully model bistable ring PUF (BR PUF) challenge-response pairs (CRPs) [15]. They introduced an alternative BR-based PUF architecture called the twisted bistable ring PUF (TBR PUF) and showed that it has an improved modelling resistance.

Encouraged by their results, we implemented the twisted bistable ring PUF (TBR PUF) and noticed that for the majority of challenges the selected BR configurations take a very long time before they settle in a stable state, if they settle at all. In fact, in a total of 505,000 challenge-response pairs (CRPs) with 5000 challenges evaluated from our twisted bistable ring PUF (TBR PUF) implementation we observed at most 30 % settled BRs before 100 ms. This is a problem when using the response evaluation method pro-

* Corresponding author.
E-mail addresses: Robert.Hesselbarth@aisec.fraunhofer.de (R. Hesselbarth), Johann.Heyszl@aisec.fraunhofer.de (J. Heyszl), sigl@tum.de (G. Sigl).

http://dx.doi.org/10.1016/j.micpro.2017.06.001
0141-9331/

posed by Chen et al. [1]. They suggested using an evaluation time at which over 90 % of the PUF's BRs have settled. If this rarely happens within an acceptable time , as in our case with the twisted bistable ring PUF (TBR PUF), then this response evaluation method is not practical. We assume that unsettled BRs are in an oscillating state, where the output values of all stages oscillate over time [8]. If we evaluate the response before the selected BR configuration has settled, then the result depends on the phase of the oscillation at the sampling instant. Since the phase is random to a certain degree the response will also be random. This results in a low reliability of the PUF. Multiple evaluations of the same challenge could be used to increase reliability. However, this also increases the total time it takes to evaluate one CRP. As a comparison to the twisted bistable ring PUF (TBR PUF), in our bistable ring PUF (BR PUF) implementation on average for over 94 % of the challenge-response pairs (CRPs) the selected BR configurations settled within 20.48 µs. However, on average its responses were '0' for 97 % of the challenge-response pairs (CRPs), which makes it unusable for any relevant application. From our practical results, we conclude that BR-based physical unclonable functions (PUFs) with good response '0'/'1'-balance show long BR settling times. The state-of-the-art response evaluation method is not suited for unsettled BRs as it results in either impractically long evaluation times or reduced reliability.

In this paper we propose new methods for evaluating responses from unsettled, oscillating BRs, in Section 2. In Section 3, we investigate the performance of the different methods when applied to unsettled BRs. For this, we use our 64-bit twisted bistable ring PUF (TBR PUF) implementation and 20 Spartan 6 field programmable gate arrays (FPGAs). Using our methods we achieve reliabilities of up to 98.5 %, whereas the best reliability we achieved using the state-of-the-art method was 81 %. With the best performing method we achieved reliabilities of around 97 % even at the shortest evaluation time that we covered in our measurements, which was 320 ns. The hardware overhead compared to the state-of-the-art method ranged from 24 additional slice registers and 40 additional slice look-up tables (LUTs) to 329 additional slice registers and 379 additional slice look-up tables (LUTs). Note that our results are relevant for the response evaluation from any BR, as oscillating BRs can occur in any BR-based PUF. We conclude with Section 4.

2. Response evaluation methods

The task of a response evaluation method is to observe the behavior of a bistable ring (BR) in order to generate a reliable response bit. We want to stress, that all BR-based physical unclonable functions (PUFs) are compatible with the methods suggested in the following. The differences in the types of BR-based physical unclonable functions (PUFs) only concern the mechanism used to select and configure a BR for its evaluation based on the given challenge. Hence, the type of the BR-based PUF, is irrelevant to the evaluation method. Different implementations of the same type of BR-based PUF will differ in the percentage of unsettled BRs. However, unsettled BRs are oscillating, regardless of the implementation details. In this paper we propose methods that improve reliability by reducing noise caused by these oscillations. Hence, the proposed methods are able to improve the reliability of any BR based PUF implementation. Obviously, the amount of the improvement will depend on the implementation as it depends at least on the percentage of unsettled BRs.

When ignoring the circuit details of a BR-based PUF implementation concerning the selection / configuration and evaluation of a BR, then a BR is an inverter ring with an even number of stages.

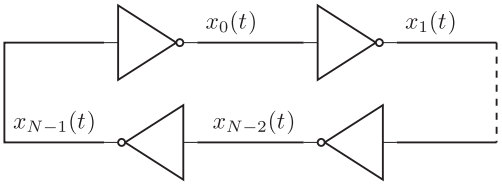

Fig. 1. N stage bistable ring and its state $x \in \mathbb{F}_2{}^N$.

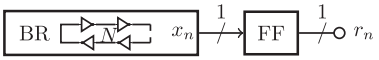

Fig. 2. Single output single sample method.

Let us consider such a BR with N stages, as shown in Fig. 1[1]. We denote the state of this BR with the state vector $x \in \mathbb{F}_2{}^N$. The nth component x_n of the state vector represents the output level, '0' or '1', of the n-th stage in the BR. The BR has the two stable states $s^+ = 10\ldots10 \in \mathbb{F}_2{}^N$ and $s^- = 01\ldots01 \in \mathbb{F}_2{}^N$. Hence, the name *bistable* ring. For the response evaluation, the BR is first forced[2] into the reset state $x^r = 0\ldots0 \in \mathbb{F}_2{}^N$. The response evaluation starts, when the BR is released from reset. We define the time at this moment as $t = 0$. After some time the BR is expected to settle in either one of the two stable states s^+ or s^-. An abstract hardware architecture for the state-of-the-art response evaluation method proposed by Chen et al. [1] is shown in Fig. 2.

One of the BR stage outputs is sampled using a single flip flop (FF). It is triggered once at the evaluation time t_e by the edge of the sampling clock, which is not shown. Hence, we call it the "single output single sample" method. Since any of the N stage outputs can be used, there are N equivalent ways to evaluate a response. Hence, we denote the response evaluated from the nth stage of the BR as:

$$r_n = x_n(t_e) \tag{1}$$

where $0 \leq n < N$. While all r_n are equally suitable as the PUF response one of them has to be selected. We use it as a state-of-the-art reference for comparing the performance of our new methods, described in the following sections. Chen et al. suggested to choose the evaluation time for this method, such that 90 % of the observed BRs settle before this time in order to ensure a high reliability of the generated responses. This is only practical if this condition is satisfied within a certain time. In our twisted bistable ring PUF (TBR PUF) implementation, less than 30 % of the 5000 different evaluated BR configurations settled before 100 ms which results in an impractical evaluation time for this method. However, if we choose a practical evaluation time, responses have to be evaluated from unsettled BRs.

We would like to explain the disadvantage of this state-of-the-art method in terms of reliability, when used to evaluate responses from unsettled BRs. We assume that an unsettled BR is in an oscillating state, where the output values of all stages oscillate over time [8]. We characterize the oscillation of the stage output value x_n with the three parameters duty cycle $\hat{\theta}_n \in [0, 1]$, phase

[1] The mechanism for forcing the reset state is not shown in Fig. 1 since it is not relevant for the considerations in this section. Also, there are many conceivable implementations. Usually, a two input NOR-gate is used instead of an inverter such that a reset signal can be applied to the second input. See also Section 3.

[2] For each PUF-use several challenge-response pairs (CRPs) must be exchanged, because BR-based physical unclonable functions (PUFs), like most strong physical unclonable functions (PUFs), return only 1-bit responses, while e.g., 128 response bits are required for a single authentication. In that case, the 128 required CRP evaluations would take at least 12.8 s.