Middle-East Journal of Scientific Research
24 (Recent Innovations in Engineering, Technology, Management & Applications): 08-12, 2016
ISSN 1990-9233; © IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.RIETMA102

64 Stage Ropufs GDS2 for Device Authentication and Secret Key Generation

G. Manigandan, P. Arunkumar, T. Vignesh and R. Sivakumar

Department of ECE, Priyadarshini Engineering College, Vaniyambadi, India

Abstract: Ring Oscillator Physical Unclonable Functions (RO-PUFs) are innovative circuit primitives that extract secrets from physical characteristics of integrated circuits (ICs). We present RO-PUFs designs that exploit inherent delay characteristics of transistors that differ from chip to chip and describe RO-PUFs which can enable low-cost authentication of individual ICs and generate volatile secret keys for cryptographic operations. In this paper a 64 stage ring oscillator is implemented using the 250nm CMOS technology provided by generic with 2.5 volt power supply. The optimization design is done using Hiper- Silicon software to make the RO-PUFs as small as possible. In, addition Tanner tools 16.5v is used in the analysis and simulation to verify the predicted performance. The proposed design is suitable for DCO and Timer circuits.

Key words: Tanner EDA · Hiper Silicon · Hiper DevGen · GDS II · IC authentication · Secret keys

INTRODUCTION

It is critical for ICs to be able to perform operations such as authentication of devices, protection of confidential information and secure communication in an inexpensive yet highly secure way. A common ingredient that is required to enable the security operations is a secret on each IC, which an adversary cannot obtain or duplicate. The current best practice is to place a secret key in non-volatile memory such as fuses and EEPROM and use cryptographic primitives such as digital signature and encryption to authenticate a device and protect confidential information. But the conventional approach suffers from a couple of shortcomings.

For a high level of physical security, the IC needs to be protected using expensive tamper sensing circuitry that needs to be continually battery powered. Second, for extremely resource constrained platforms even simple cryptographic operations can be too costly.

RO-PUFs [1] are innovative primitives to derive secrets from complex physical characteristics of ICs rather than storing the secrets in digital memory. A volatile secret can be generated from the random delay characteristics of transistors used in ring oscillator. Because the RO-PUF taps into the random variation during an IC fabrication process, the secret is extremely difficult to predict or extract the needed characteristics. RO-PUFs significantly increase physical security by generating volatile *secrets* [2] that only exist in a digital form when a chip is powered on and running. This immediately requires the adversary to mount an attack while the IC is running and using the secret, a significantly harder proposition than discovering non-volatile keys; an invasive attack must accurately measure RO-PUF delays without changing the delays or discover volatile keys in registers without cutting power or tampering.

An n-bit applied challenge selects two different ROs from 2^n ROs. This paper proposes a method of how RO-PUFs can enable low-cost authentication of ICs and generate volatile secret keys for cryptographic operations. The RO-PUF design has advantages in terms of the ease of implementation and reliability over previously proposed & other designs like Hardware Metering, Secure Split Test and Antifuse-based technology for recording usage time. The RO-PUF circuits can also be used as hardware random number generators [3]. This paper only focuses on device authentication and key generation. The rest of the paper is organized as follows.

Section 2: Provides a brief overview on silicon PUFs, including the concept, a circuit design and test-chip results.

Section 3: Discuss how PUFs can be used for low-cost authentication and cryptographic key generation, respectively.

Corresponding Author: G. Manigandan, Department of ECE, Priyadarshini Engineering College, Vaniyambadi, India.

Section 4: Describes a 64 Stage ROPUF design based on ring oscillators.

Section 5: Demonstrates that the discussed applications are viable by providing experimental results on 250nm & finally concludes the paper.

Physical Unclonable Functions: In this section, we introduce the concept of Physical Unclonable Functions (PUFs).

A Physical Unclonable Function (PUF) is a function that maps a set of challenges to a set of responses based on an intractably complex physical system. The function can *only* be evaluated with the physical system and is unique for each physical instance. While PUFs can be implemented with various physical systems. This paper focuses on Ring Oscillator- PUFs (RO-PUFs) that are based on the hidden timing and delay information of IC [4]. With identical layout masks, the variations in the manufacturing process cause significant delay differences among different ICs. The PUFs provide significantly higher physical security by extracting secrets from complex physical systems rather than storing them in non volatile memory [5]. Another advantage of PUFs is that they do not require any special manufacturing process or programming and testing steps.

As the PUF circuit is rather simple, attackers can try to construct a precise timing model and learn the parameters from many input-output pairs. To prevent these model-building attacks, the PUF circuit output can be obtained by Exclusive OR, NOR ing multiple outputs.

RO-PUF Overview: Figure 1 illustrates a RO-PUF delay circuit that consists of many *identically* laid-out delay loops (ring oscillators) [6, 7]. Each ring oscillator is a simple circuit that oscillates with a particular frequency. Due to manufacturing variation, each ring oscillator oscillates with a slightly different frequency. In order to generate a fixed number of bits, a fixed sequence of oscillator pairs is selected and their frequencies are compared to generate an output bit. The output bits from the same sequence of oscillator pair comparisons will vary from chip to chip. Given that oscillators are identically laid out, the frequency differences are determined by manufacturing variation and an output bit is equally likely to be one or zero if random variations dominate.

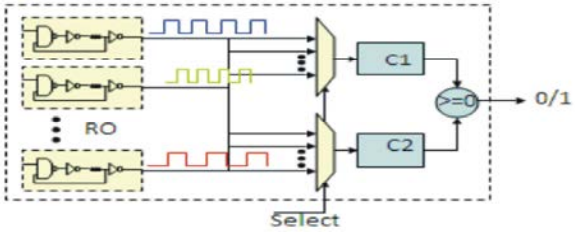


Fig. 1: Ring oscillator based PUF circuit

LOW-COST Authentication: This section discusses how PUFs can be used to authenticate individual ICs without costly cryptographic primitives. The PUF-based authentication described here can be applied even to extremely resource constrained platforms where cryptographic operations may be too ex pensive in terms of silicon area or power consumption, or off-the-shelf programmable ICs such as FPGAs where crypto graphic operations are not implemented.

As the PUF output is unique and unpredictable for each IC, provided it is long enough, it is straightforward to identify an IC with the PUF. One can simply record a PUF output and compare that with a re-generated one later. However, a single PUF output per IC is not enough for authentication; anyone who has access to an IC can obtain the PUF output and create another IC that contains the PUF output in memory.

Therefore the authentication mechanism should ensure that an adversary cannot obtain the PUF output that is used for authentication. Here, we exploit that the PUF can have exponential number of challenge response pairs where the response is unique for each IC [8]. We also assume that model-building is hard to do for a given PUF, because of non-linearities in the PUF. A trusted party, when in possession of an authentic IC, applies randomly chosen challenges to obtain unpredictable responses. The trusted party stores these challenge-response pairs in a database for future authentication operations. To check the authenticity of an IC later, the trusted party selects a challenge that has been previously recorded but has never been used for an authentication check operation and obtains the PUF response from the IC. If the response matches the previously recorded one, the IC is authentic because only the authentic IC and the trusted party should know that challenge-response-pair. To protect against man in the middle attacks, challenges are never reused. Therefore, the challenges and responses can be sent in the clear during authentication operations.

Realization: In a possible realization of our solution, silicon genetic material is" recombined" to form a PUF with challenge / response characteristics. As described in [9], silicon "genetic" material in the form of ring oscillator frequency count values are recombined, using a recombination function, so that an output response is the result of the device-specific genetic material and an input value. An implementation with a simple recombination function is shown in Figure 2 The variations of time period with voltage and temperature for all the five corner conditions (typi-typi, fast-fast, slow-slow, fast-slow, slow-fast) are observed. The variations are graphically represented in the form a 3-D plot.

The voltage was varied from ± 10% of Vdd i.e., from 2.32v to 2.58v and the temperature was varied from -40 to 150 degrees Celsius. The circuit is simulated under typical condition for different values of temperature and Vdd and the time period is noted.

The 64Stage ROPUF design based on ring oscillators. The actual implementation of the 64 stage RO-PUFS discussed in this paper is shown in the Figure 2, the schematic which is simulated in Hiper Silicon Schematic Editor v16.5 in Tanner EDA.

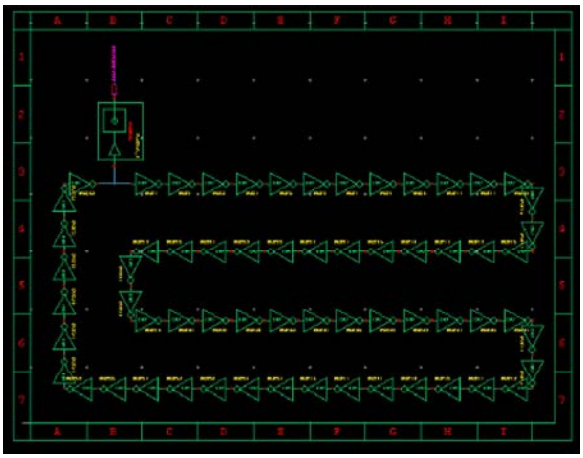


Fig. 2: 64 Stage RO-PUF

Pre-Layout Simulation: The designed 64 stage RO-PUFs works accccording to the desired functionality after the generation of netlist of Tanner SPICE. All the required input voltages such as tuning and bias voltage. The power supply is given as 2.5V.

The waveform generated for 64-stage ring oscillator *PUFs* is as shown in the Figure 2. The period of the waveform generated is ~2.98ns. Therefore the frequency generated is approximately 27MHz. During the simulation, the initial condition for the ring oscillator is set to zero in order to generate oscillations. Spikes can be seen in the waveform at the instances where output changes its state. This is because when the input voltage changes sharply, the capacitance at input of the inverter opposes sudden change in the output. By introducing a load capacitor at the output of the oscillator these glitches can be reduced.

Parameters	Average Delay	Rise Time	Fall Time
Minimum	23.6785n	54.0353n	103.0698n
Maximum	54.3786n	56.9323n	97.7180n
Mean	3.1491n	56.0870n	99.7677n
Average Delay	28.7316n	566.0872p	1.7617n
Variance	1.1587f	578.0408e	3.7826a
Standard Deviation	34.0399n	760.2900p	1.9448n

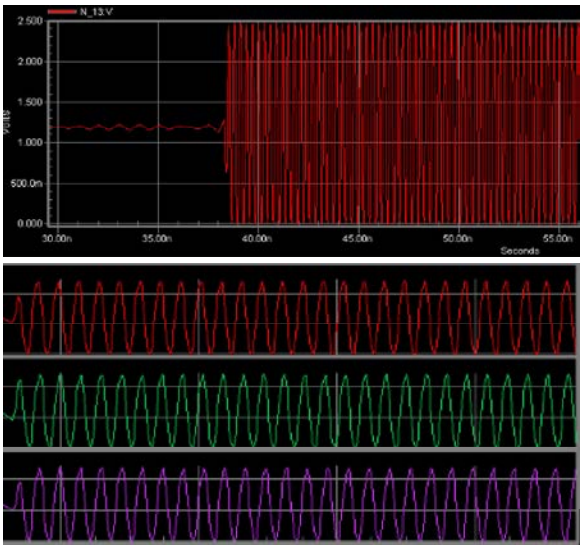


Fig. 3: Pre Layout Simulation of 64 Stage RO-PUF

The monte-carlo simulation for 2000 trials was done and the result is as shown

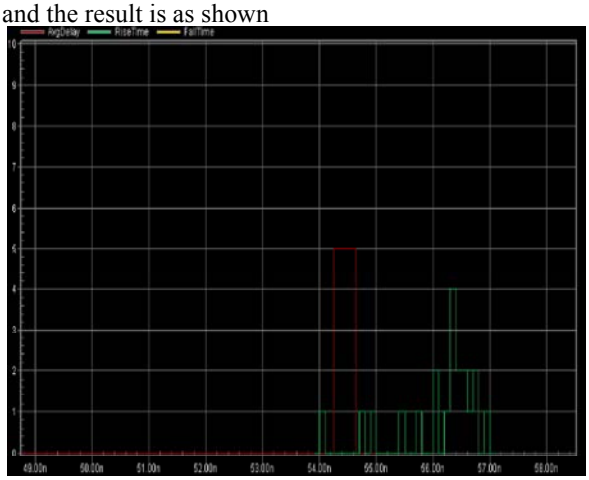
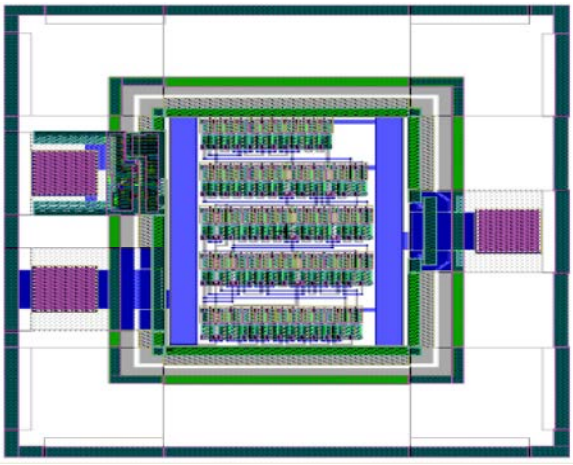
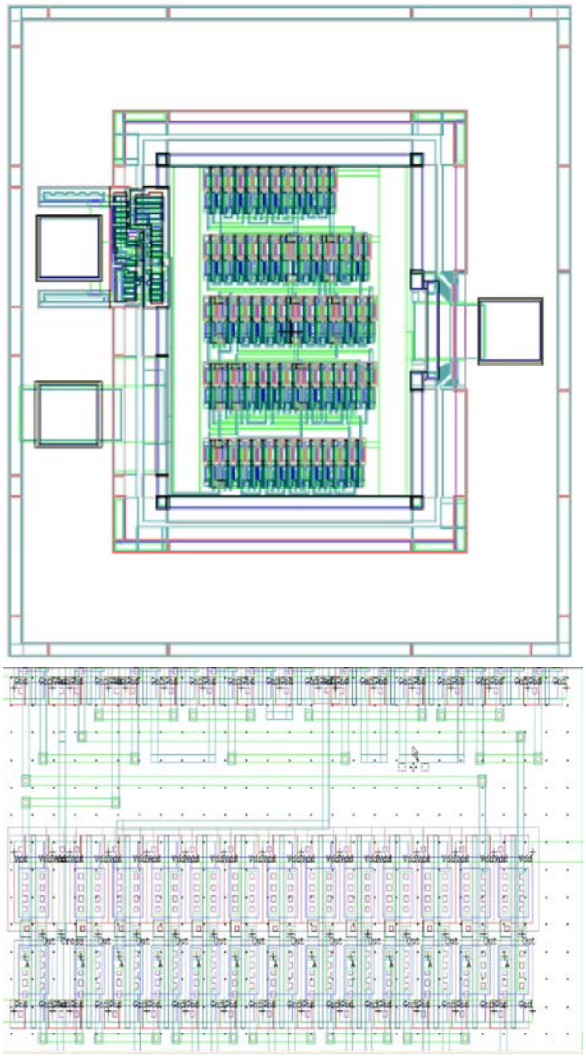


Fig. 4: Monte Carlo Simulation of RO-PUF

The layout of 64 stage RO-PUFs was obtained with Layout Editor using the Standard Tanner Cells generated using Hiper DevGen clearing the extraction warnings.



The GDSII of the above layout is as shown



CONCLUSION

A 64-stage ring oscillator puf has been designed to generate the desired frequency even in the worst conditions of process variations. The raw output (frequency) is divided using a 10-stage divider circuit (D-flip flop). A 64 stage output buffer has been designed so that it can drive a load of 1pf. The PUFs can provide low-cost authentication of ICs and generate volatile keys for both symmetric and asymmetryric cryptographic operations. Ongoing future work includes the implementation of PUF-enabled Radiofrequency IDs and the development of a secure processor that uses a PUF to generate crypto graphic keys that are only known to the processor.

REFERENCES

1. Ruhrmair, Ulrich and E. Holcomb Daniel, 2014. "PUFs at a glance," Design, Automation and Test in Europe Conference and Exhibition (DATE), pp: 1-6.
2. Katzenbeisser, Stefan and S. Kocabas ¨Unal, Ro?zi´c Vladimir, Sadeghi Ahmad-Reza, Verbauwhede, Ingrid and Wachsmann, Christian, 2012. "PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon," Cryptographic Hardware and Embedded Systems {CHES 2012, pp: 283-301.
3. Maes, Roel, Van Herrewege, Anthony and Verbauwhede, Ingrid, 2012. "Pufky: A fully functional puf-based cryptographic key generator," Cryptographic Hardware and Embedded Systems {CHES 2012, pp: 302-319.
4. Koeberl, Patrick, Li, Jiangtao, Maes, Roel, Rajan, Anand, Vishik, Claire and W´ojcik, Marcin, 2012. "Evaluation of a PUF Device Authentication Scheme on a Discrete 0.13 um SRAM," Trusted Systems, pp: 271-288.
5. Holcomb, Daniel E., and Kevin Fu. Springer Berlin Heidelberg, 2014. "Bitline PUF: Building Native Challenge-Response PUF Capability into Any SRAM," in Cryptographic Hardware and Embedded Systems CHES, pp: 510-526.
6. Gao, Mingze, Khai Lai and Gang Qu, 2014. "A Highly Flexible Ring Oscillator PUF," in Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference. ACM.

7. Rahman, Tauhidur, Forte, Domenic, Fahrny, Jim and Tehranipoor, Mohammad, 2014. "ARO-PUF: an aging-resistant ring oscillator PUF design," in Proceedings of the conference on Design, Automation & Test in Europe.
8. Cherkaoui, Abdelkarim, Viktor Fischer, Alain Aubert, and Laurent Fesquet, 2012. "Comparison of self-timed ring and inverter ring oscillators as entropy sources in FPGAs," in Design, Automation & Test in Europe Conference & Exhibition (DATE), pp: 1325-1330.