Interconnect-Based PUF With Signature Uniqueness Enhancement

Liting Yu, Xiaoxiao Wang, *Member, IEEE*, Fahim Rahman, *Member, IEEE*, and Mark Tehranipoor, *Fellow, IEEE*

***Abstract*— Physical unclonable function (PUF) is an important security primitive, which generates unique signatures as fingerprints for each chip. This article first presents a novel interconnect-based PUF (iPUF). The proposed iPUF utilizes the manufacturing process variability of interconnect lines to introduce crosstalk variations for generating PUF signatures. By leveraging the variations of passive interconnects, iPUF minimizes the usage of active CMOS components, providing an increased resiliency against environmental variations and aging. Initiated by a linear feedback shift register (LFSR), iPUF sequentially generates 1-bit signature at each clock cycle, making it more efficient compared with ring-oscillator PUF. Second, two schemes for signature uniqueness enhancement of sequential PUFs are proposed. The self-masking scheme windows the sequential signature with an *m*-bit mask trained by the PUF's own initial sequential signature. Meanwhile, the bit-filtering scheme screens the randomness of each bit within the sequential signature by exploiting several sub-iPUFs and selects the bits with high randomness. To verify the performance of iPUF, Monte Carlo simulations of 500 samples, with variations following industrial data, are conducted in different operating corners. The uniqueness of the given sample set approaches 48.63% with a 10-bit mask. With ±10% supply voltage, 0 °*C*–100 °C temperature variations, as well as one year of unaccelerated aging, iPUF's reliability values, are as high as 96.09%, 99.06%, and 99.63%, respectively. For verification, 50 dies of iPUF chips are manufactured with a 55-nm technology node. Silicon results demonstrate that iPUF generates 1024-bit signatures with satisfied uniqueness (48.03%) while exhibiting good reliability (90.07%) under 120-mV voltage variations. Finally, iPUF's robustness against various attacks is also proven.**

***Index Terms*— Aging resistance, hardware security, interconnect, physical unclonable function (PUF), uniqueness improvement.**

I. Introduction

PHYSICAL unclonable function (PUF) is an emerging circuit module for hardware security. PUFs exploit process variations during manufacture to generate unique signatures for each chip as identifications when challenges are applied during runtime [1], [2]. Thus, PUFs store no critical information in the memory offering no possibility to be stolen, replicated, or predicted. With such characteristics, PUFs are commonly implemented for low-cost authentication and key generation [3]–[6].

Over the years, researchers have proposed various CMOS and other emerging device-based PUF architectures. Among them, the arbiter PUF [2] exploits delay differences between two symmetrical standard-cell or interconnect-based paths. Arbiter PUF has a high challenge–response pair (CRP) space, making it a strong PUF. However, its response can be predicted (e.g., training the predicting machine using a small CRP set), as the path delay is linearly dependent on challenge [7]. Ring-oscillator PUF (RO-PUF) is another common delay-based architecture, which compares the frequency differences (caused by process variations) between a group of designwise identical ring oscillators [8]. RO-PUFs can also produce numerous CRPs but generally require more area, power, and time. In addition to the above-mentioned delay-based PUFs, researchers also leverage the minute unbalances within a given cross-coupled structure, such as those in an SRAM cell (SRAM PUFs [9]), or a cross-coupled latch (butterfly PUFs [10]). However, the CRP spaces of these PUFs are very limited (in many cases, only one) making them weak PUFs. Buskeeper PUF [11], which exploits the existing buskeeper cell, could be considered as a viable alternative to D-flip-flop PUFs. Although it requires a smaller cell size, additional addressing circuits are needed. In addition, voltage-comparator-based PUF [12] employs analog sense amplifier and comparator to magnify and judge the crosstalk voltage level of two neighboring victim lines and generates signature. However, the analog components require high design cost. Moreover, once the chip is manufactured, the output signature is fixed and CRP space is inferred by knowing only one CRP.

However, all the existing PUFs suffer from reliability issues (i.e., highly sensitive to environmental variations, such as temperature, power supply noise, and aging effects), uniqueness issues, security issues (e.g., vulnerable to modeling attacks), and cost issues.

A. Previous Work

Various enhancements have been proposed to improve the reliability, uniqueness, security, and cost of the existing PUFs, which include the following.

Manuscript received April 14, 2019; revised June 25, 2019 and August 19, 2019; accepted September 2, 2019. Date of publication October 30, 2019; date of current version January 21, 2020. This work was supported by the National Natural Science Foundation of China (NSFC) under Grant 61631002, Grant 61504007, and Grant 61427803. *(Corresponding author: Xiaoxiao Wang.)*

L. Yu and X. Wang are with the School of Electronic and Information Engineering, Beihang University, Beijing 100191, China (e-mail: wangxiaoxiao@buaa.edu.cn).

F. Rahman and M. Tehranipoor are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: tehranipoor@ece.ufl.edu).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVLSI.2019.2943686

1063-8210 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

TABLE I
SUMMARY OF DIFFERENT PUF QUALITY ENHANCEMENT TECHNIQUES IN TERMS OF RELIABILITY, UNIQUENESS, SECURITY, AND COST

	Bit Selection [13] [14]	**Aging Injection [15]**	**Aging Resistant RO-PUF [16]**	**TERO PUF [17]**	**Non-Linear VTC [18]**	**Buskeeper PUF [11]**
Reliability	$\surd$	$\surd$	$\surd$	$\times$	$\times$	$\circ$
Uniqueness	$\surd$	$\surd$	$\circ$	$\surd$	$\surd$	$\circ$
Security	Not Mentioned	Not Mentioned	Not Mentioned	Resistant to Electromagnetic Attack	Resistant to Modeling Attack	Resistant to Reverse Engineering
Cost	$\times$	$\times$	$\surd$	$\times$	$\circ$	$\surd$

(1) $\surd$ indicates that the enhancement can increase the specific metric of PUFs' performance;
(2) $\circ$ indicates that the enhancement may improve the specific metric of PUFs' performance;
(3) $\times$ indicates that the enhancement may deteriorate the specific metric of PUFs' performance.

1) *Reliability Enhancement:* Enhanced bit selection takes spatial correlation of SRAM cells for SRAM-PUFs to rank the reliability of the bits [13], [14]. However, it is not applicable to common delay-based PUFs. Besides, aging injection [15] is performed to SRAM-PUFs in two phases to first achieve a targeted uniformity and then to improve the reliability. Hence, the PUF enrollment is a very slow process as one needs to consider the total aging time and profile for every PUF implementation. Furthermore, the aging injection is invisible to fab and should be completed by the IP owner, making it prohibitively expensive to the IP owner. Besides, aging-resistant RO-PUF is proposed in [16] and [19], which decreases the negative-bias temperature instability (NBTI) aging degradation of pMOS by offsetting the pMOS gate voltage to VDD when the PUF is in the standby mode. Although it shows high reliability, the design is limited to custom layout implementations.
2) *Uniqueness Enhancement:* Postprocessing is implemented for transient effect ring-oscillator (TERO) PUF [17]. The mean value of transient fluctuations for each TERO loop is derived from a large number of measurements, and the neighboring mean TERO values are subtracted to obtain a relatively unique and reliable signature. Although this mean value is related to the characteristic of the chip, it can be significantly affected by aging, which is universal for all loops. Moreover, the repeating measurements of many elementary TEROs cause serious power and area overheads. In [20], enhanced challenge–response set is generated by measuring the exact differences between every possible pair of ROs with Euclidean distances as weighting factors. However, the required arithmetic units, such as the square root and the multiplier, are vulnerable to side-channel attack and require additional area and power.
3) *Security Enhancement:* In [18], a nonlinear voltage transfer function is instantiated to create a complex mapping between the input and output of each circuit block, which is hard to attack. However, the nonlinear voltage transfer function varies with aging, and the error is accumulated at each stage, leading to low PUF reliability.
4) *Cost Enhancement:* Buskeeper PUF [11] utilizes buskeeper cell, which is smaller than DFF cells. However, the enhancement is regarding DFF PUFs and requires additional addressing circuit.

From Table I, the enhancement techniques listed earlier help to increase the reliability, uniqueness, safety, and impacts the cost of PUFs. However, the operation phase requires long test time or area overhead. What is more, the arithmetic units of some enhancements are vulnerable to side-channel attack. Thus, new PUF designs with the following features are needed: 1) exhibit high reliability to temperature, voltage variations, and aging; 2) able to generate signatures with satisfied uniqueness; 3) offer high security and resistance to attacks; and 4) require low fabrication and test cost.

B. Contributions and Article Organization

In this article, an all-digital interconnect-based PUF (iPUF) that exploits the variation in the inherent crosstalk between the interconnects to produce signature is proposed. Then, two general schemes for improving the uniqueness of iPUF signature are introduced. The proposed iPUF with the uniqueness enhancement scheme has the following advantages.

1) iPUF has improved reliability comparing with active component-based PUFs (Arbiter, RO-PUF, and so on) by utilizing passive components (interconnects that can be modeled as resistors and capacitors). Hence, iPUF is resistant to the dominant aging phenomena in active components, such as bias temperature instability (BTI), hot carrier injection (HCI), and time-dependent dielectric breakdown (TDDB) [21]. Although the interconnects can suffer from electromigration (EM), the activation duration of the iPUF with respect to the system lifetime is very small, making the EM effect practically negligible [22].
2) The uniqueness of the sequential signatures generated by iPUF is satisfying with the proposed uniqueness enhancement circuit. The novel uniqueness enhancements, including self-masking and bit-filtering schemes, efficiently improve the uniqueness and can be applied to other sequential PUFs as well without loss of generality.
3) iPUF is resilient to modeling attacks. As the coupling variance is nondeterministic, and there are multiple parameters affecting crosstalk, the crosstalk scenario is

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

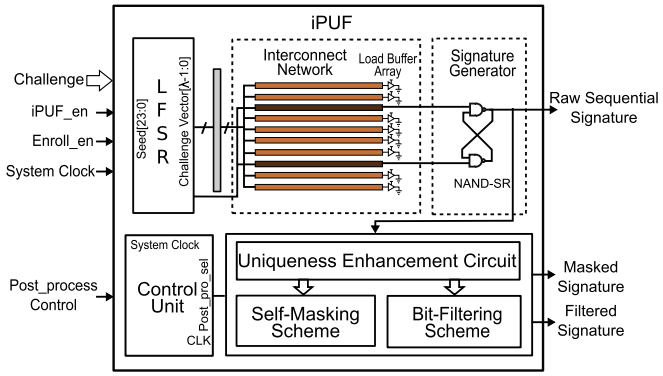


Fig. 1. Architecture of the proposed interconnect-based PUF structure.

practically infeasible to predict or clone. Besides, iPUF is proven to be resistant to several existing attacks.

4) The area and power overheads of iPUF are low with an extremely high signature generation rate (1-bit ID per clock cycle). Implemented with a K-stage linear feedback shift register (LFSR), it can generate signatures of an arbitrary length smaller than $2^K - 1$ for a given challenge, and also, the interconnects of iPUF can be routed in any uncongested metal layers without occupying the active Si layer.
5) Fifty dies of iPUF are fabricated with a 55-nm technology node. The reliability and uniqueness of iPUF with uniqueness enhancement circuit are verified by silicon data.

The rest of this article is organized as follows. Section II demonstrates the architecture of the proposed iPUF in detail. Section III illustrates two general uniqueness enhancements, including self-masking and bit-filtering schemes. Then, the implementation flow is demonstrated in Section IV. Simulation results and silicon data are exhibited in Section V, including cost, uniqueness, and reliability. In Section VI, the potential attack models are demonstrated and how the iPUF is resistant to these models are explained. Finally, the concluding remarks are given in Section VII.

II. Architecture of iPUF

As shown in Fig. 1, the proposed PUF structure is composed of three major units: iPUF, uniqueness enhancement circuit, and control unit. The high-level operation of iPUF is as follows. A challenge is supplied as the seed of an LFSR, which generates a sequence of internal challenge vectors (C_v). C_v is transmitted along the parallelly routed aggressors consisting of $\lambda - 2$ interconnects. The crosstalk on the two victim interconnects depends on C_v, as well as the process variations of interconnect network. With a proper setup, the signature generator can extract the variation of the crosstalk on victims to a digital signature of "0"/"1." The uniqueness enhancement circuit further improves the uniqueness of the iPUF signature.

The detailed working principle of iPUF is described as follows. As shown in Fig. 2(a), it is composed of LFSR, interconnect network, and signature generator.

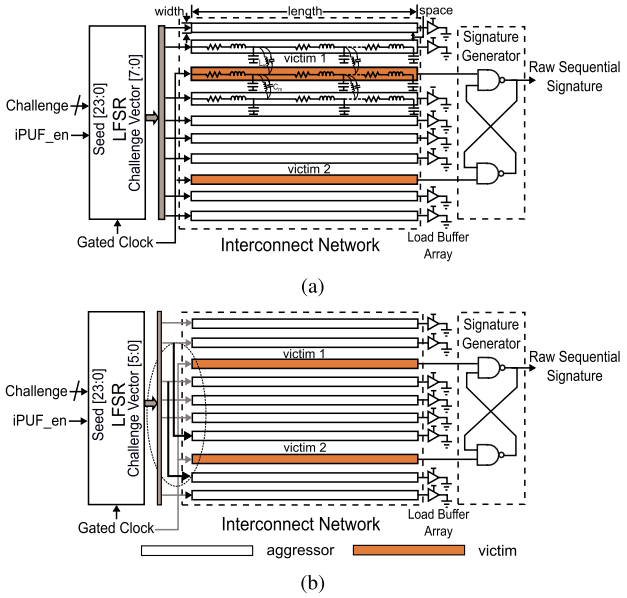


Fig. 2. iPUF unit. (a) Architecture of the primary iPUF. (b) Architecture of the improved iPUF making the interconnect variation a decidive factor of signature generation by connection the neighboring aggressors of the two victims.

A. Linear Feedback Shift Register

The LFSR in iPUF takes an external challenge as a seed. When enabled, it generates a $(\lambda - 2)$-bit width internal challenge vector (C_v) at every clock cycle, where λ is the number of interconnects within the interconnect network. For simulation purpose, an LFSR with 23-bit seed and characteristic polynomial of $F(x) = x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^7$ is considered. It should be noted that any LFSR capable of producing a $(\lambda - 2)$-bit pseudorandom number can be utilized for this purpose. Hence, the designer has a full control over the required challenge size and LFSR characteristic as opposed to arbiter/RO-PUF, of which the challenge length is determined by the delay stages or RO pairs. For modern IC, it is very common to have LFSR being already a part of it. Reusing the existing LFSR can significantly reduce area and power overheads, given that it is secure and protected from any physical or side-channel vulnerabilities.

B. Interconnect Network

The coupling variance between the interconnects is the foundation of iPUF. The interconnect network is designed to magnify the coupling variance, which is composed of λ identical interconnects routed in parallel as shown in Fig. 2(a). Among these λ interconnects, there are two victims (marked as darker lines), each of which has $(\lambda - 2)/2$ aggressors on both lateral sides. The two victims are driven by the clock. At the same time, C_vs generated by LFSR are applied and transmitted through to the aggressors. To eliminate the capacitive load-induced bias in the generated crosstalk, the end nodes of the two victims are connected to the symmetrically designed signature generator, and the end nodes of the aggressors are connected to a buffer array with equal loads. As a result, the crosstalk only depends on C_v and the interconnect

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

process variations. A particular seed (i.e., external challenge) should produce unique crosstalk in the victim lines from chip to chip. As the coupling variance is nondeterministic, and there are parameters affecting crosstalk (such as bit flipping, rise/fall delay, charging/discharging leakage path, and so on), the crosstalk scenario is practically infeasible to predict or clone, making it extremely suitable for PUF application and resilient to modeling attacks. It should be noted that due to the shielding effect and attenuation of electromagnetic fields, the crosstalk on the victims caused by neighboring aggressors tends to be much larger than that caused by the further ones. As shown in Fig. 2(a), the closest two aggressors have a greater influence on the victim lines and, therefore, have higher probability to be the decisive factor for signature generation. To ensure that the interconnect physical variation is the prominent decisive factor, the iPUF is improved as shown in Fig. 2(b), where the neighboring aggressors of the two victims are connected for leveraging nondeterministic driving impacts.

In general, the construction of interconnect network follows two rules. First, the two victims within interconnect network are symmetrically neighbored by the same number of aggressor interconnects. Second, the two neighboring aggressor interconnects of the two victims should be fed with the same input challenge vectors. In this case, the process variations of interconnects have the major effects on the delay difference of the transitions along two victims. Then, a preliminary iPUF can be constructed with two victims and eight aggressors, as shown in Fig. 2(b).

C. Signature Generator

As stated previously, the crosstalk is unique from chip to chip under the given condition and, therefore, can be exploited to generate a digital PUF signature. As shown in Fig. 2, the signature generator based on NAND-based S/R-latch works as a fast–slow arbiter. If the rising edge of victim 1 in Fig. 2(a) arrives earlier, the obtained signature bit is "0" and vice versa. Furthermore, at every falling edge of the system clock cycle, the output is reset to "1" as per the S/R latching behavior. It ensures that there is no correlation between two successive output bits. As a result, the signature generator can generate 1 bit of nondeterministic digital signature at every clock cycle. With the K-stage LFSR, it can generate signatures of an arbitrary length smaller than $2^K - 1$ for a given challenge. Hence, iPUF gives the designer full control on the runtime based on the required key length.

D. Control Unit

The control unit shown in Fig. 1 is designed to control the activation of iPUF and enable uniqueness enhancement circuit. It does not have any qualitative effect on the iPUF output, rather initiating generation and capturing of the signature. The detailed design of this unit is not provided due to space limitation.

III. Uniqueness Enhancement Circuits

As the switching probability of any deterministic aggressors is always lower than 50%; therefore, crosstalk cannot be initiated within the unswitched clock cycles, reflecting the uniqueness loss in the corresponding bits. Therefore, two uniqueness enhancement methods are proposed to improve the uniqueness of iPUF. The self-masking scheme windows the sequential signature with an m-bit mask, which is trained by the iPUF's own initial sequential signature, as shown in Fig. 3. The bit-filtering scheme screens the randomness of each bit within the sequential signature by exploiting several sub-iPUFs and selects the bits with high randomness, as shown in Fig. 5. Both the aforementioned uniqueness enhancement circuits are applicable to sequential PUFs for uniqueness improvement without loss of generality.

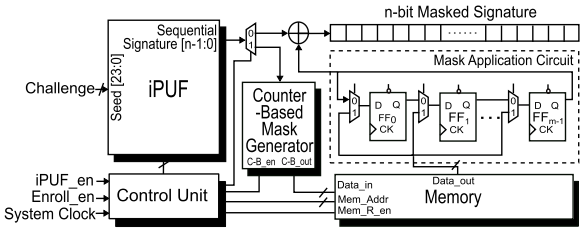


Fig. 3. Architecture of self-masking circuit.

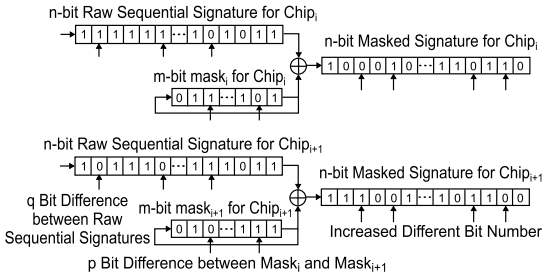


Fig. 4. Diagram for signature uniqueness improvement based on the self-masking circuit.

A. Uniqueness Enhancement Based on Self-Masking

The Self-Masking Circuit is composed of the counter-based mask generator and the mask application circuit.

1) Counter-Based Mask Generator: During the enrollment phase, the control unit initiates the mask generation scheme. To generate the mask for each iPUF, an arbitrary seed (apart from the external challenge) is applied to the LFSR and a $2^m - 1$ bit long raw sequential signature is obtained. The total occurrences of "1/0" or "rising/falling edge" within the signature can be counted by a counter and is used as the m-bit mask.

2) Mask Application Circuit: It is comprised of m number of consecutively connected DFFs so that every m-bits of the raw sequential signature could be masked by the previously obtained m-bit mask. When iPUF is operating in-field, the control unit first loads the m-bit mask value from memory into the mask application circuit. Then, during the signature generation, the n-bit raw signature is stream XORed with the m-bit mask, as shown in Fig. 4. The n-bit masked signature serves as the final output with improved uniqueness. It should be noted that, as the masking is concurrent with signature

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

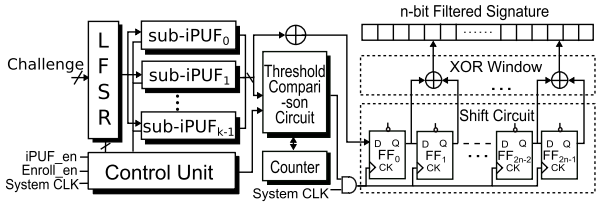


Fig. 5. Architecture of the bit-filtering circuit.

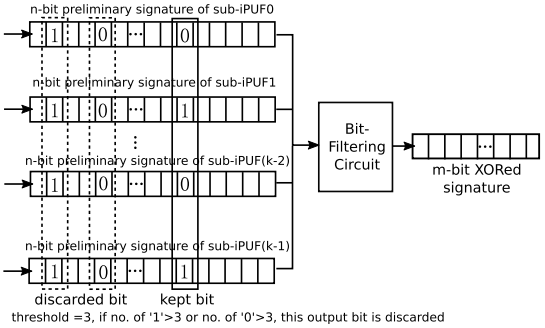


Fig. 6. Diagram for signature uniqueness improvement based on the bit-filtering circuit.

generation, only one extra memory accessing clock cycle is required for mask application.

3) Principle of Self-Masking Scheme: For one case of self-masking scheme which counts the occurrence of "1," the self-masking scheme improves the uniqueness of iPUF as follows. Let there be p-bits of differences between two m-bit masks for two iPUFs, and there are q-bits of differences between two n-bit raw signatures. Then, there would be $n-q$ number of the same bits between these two signatures. By adopting the stream rotating masking process, as shown in Fig. 4, $p/m \times 100\%$ of raw signature bits would be affected. Among these affected bits, $(n-q)/n \times 100\%$ would be flipped compared to the raw signatures, which increases the uniqueness. On the other hand, there would be $q/n \times 100\%$ bits flipped to the same values; however, they were actually different in raw signatures (reducing the uniqueness). Thus, the overall uniqueness enhancement can be given by

$$\Delta u = \frac{p}{m} \times \frac{n-q}{n} - \frac{p}{m} \times \frac{q}{n} = \frac{pn-2pq}{mn} = \frac{p}{m}\left(1-\frac{2q}{n}\right). \tag{1}$$

Therefore, the overall uniqueness is improved for cases with $q/n < 0.5$. This condition is satisfied by iPUF, of which the uniqueness of initial raw signature is lower than 50% (see Fig. 11, and the details are discussed in Section V-B). In addition, the lower the initial uniqueness (q/n) is, the more significant the improvement (Δu) would be. Also, it should be noted that an instable bit within m-bit mask can cause $(n/m)/n = 1/m$ final signature bit error rate (BER) due to the repeated mask application scheme. Therefore, it is suggested to store the mask value in nonvolatile memory or off-chip authentication server, instead of generating it at each iPUF activation. If stored off-chip, the mask value can be integrated into a hybrid/combined challenge, in a similar fashion to [23], where a portion of the hybrid challenge is used as the mask value. Note that storing the masked values does not exhibit any security vulnerability, as discussed in Section VI.

B. Uniqueness Enhancement Based on Bit Filtering

According to the crosstalk principle mentioned in Section II, the proposed iPUF is sensitive to challenge vectors, namely, the crosstalk difference caused by interconnect variation is drawn for some challenge vectors. This is clearly shown in Fig. 14(b). For some cases, the proportion of "1's" for a specific bit generated by 500 iPUF samples is 0% and 100%. Therefore, these patterns contribute little to the uniqueness of the output signature. To increase the uniqueness of sequential PUF signature, another enhancement named Bit-Filtering is devised as shown in Fig. 5, which consists of threshold comparison circuit, counter, shift circuit, and XOR window.

1) Threshold Comparison Circuit and Counter: Threshold comparison circuit is applied to select signature bits with high randomness. In this method, k sub-iPUFs are implemented in a single chip. The outputs of k sub-iPUFs are connected to threshold comparison circuit. The threshold comparison circuit determines if the relevant signature bits of all sub-iPUFs are with high randomness by counting the number of "1." This can be easily achieved with logical circuits. If the number of "1" is within the threshold range, the threshold comparison circuit generates shift enable signal. The Counter is applied to control the operating duration of threshold comparison circuit.

2) Shift Circuit and XOR *Window:* Shift Circuit is used to store the filtered signature. The output of k sub-iPUFs are XORed and connected to the input of shift circuit. When the threshold comparison circuit detects signature bits with high randomness, the shift circuit is activated by shift enable signal and shifts the corresponding signature by one bit. Finally, the first eligible $2n$ bits of filtered signature are stored in shift circuit. Then, to further increase the uniqueness, every two bits of the $2n$ bits signature are XORed by the XOR window, and n-bit filtered signature is generated.

3) Principle of Bit-Filtering Scheme: As shown in Fig. 6, for noneffective input patterns, it is more likely for sub-iPUFs of a single chip to generate more "1's" or "0's". Therefore, if the number of 1 is less or more than a threshold, the specific bit can be discarded as the cases in the dotted rectangle. In Fig. 6, the threshold is 3; namely, if the number of "1" is greater than or equaling to 3, this bit is discarded. Otherwise, this bit of signature is kept. This works as on-chip Bit-Filtering function. With an appropriate threshold, when a specific bit is evenly distributed with "0" or "1," this bit can be selected as the output signature as the case in the solid rectangle. The bit-filtering scheme improves the uniqueness of iPUF as follows. If the specific signature bits are all "0"/"1," it is more likely for iPUFs of other chips generating "0"/"1" at the same bit. The uniqueness of this bit is zero. If there are p bits with the same value ("0"/"1") and n bits with different values, the uniqueness before and after bit-filtering scheme can be

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

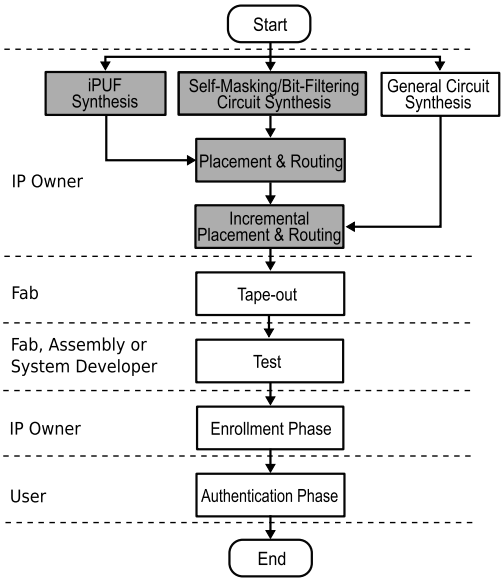


Fig. 7. Implementation flow of iPUF.

calculated respectively, by

$$u_0 = \frac{\sum_{i=1}^{n} \mathrm{HD}_{i|\mathrm{HD}_i \neq 0} + \sum_{j=1}^{p} \mathrm{HD}_{j|\mathrm{HD}_j = 0}}{n+p} \quad (2)$$

$$u_{0\_\mathrm{filtered}} = \frac{\sum_{i=1}^{n} \mathrm{HD}_{i|\mathrm{HD}_i \neq 0}}{n} \quad (3)$$

where HD_i is the average Hamming distance (HD) of bit i among all chips, and the enhanced uniqueness can be calculated by

$$\Delta u_{\_\mathrm{filtered}} = \frac{u_{0\_\mathrm{filtered}} - u_0}{u_0} = \frac{p}{n}. \quad (4)$$

If the portion of noneffective bits (p) is 0.2, the uniqueness improvement would be 0.25.

IV. Implementation Flow of iPUF and Uniqueness Enhancement Circuit

The implementation flow of iPUF with uniqueness enhancement circuit is shown in Fig. 7. We used Design Compiler [24] and Encounter [25] for the design and implementation of iPUF. Since the circuits are all-digital, the implementation and measurement flow can be easily integrated into current industrial design and test flow. The iPUF-based enrollment can be performed during functional or test phases. The details of the flow are given in the following.

- *Step 1* (iPUF, Self-Masking or Bit-Filtering Circuit, and General Circuit Synthesis): The iPUF, Self-Masking or Bit-Filtering Circuit, should be separately synthesized with circuit design. In the iPUF synthesis, the standard cells with the same load should be implemented, especially for signature generator. The synthesis of Self-Masking or Bit-Filtering Circuit is not under strict constraints, but the name of input cell should be recorded for placement and routing. There are no strict constraints for general circuit design.

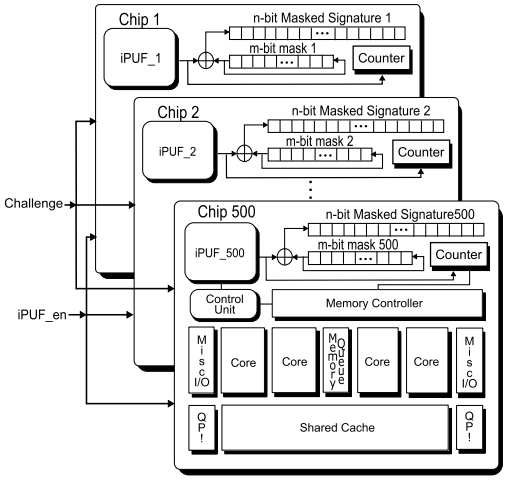


Fig. 8. Implementation of 500 iPUF samples during simulation.

- *Step 2* (iPUF, Self-Masking or Bit-Filtering Circuit Placement and Routing): The cells of iPUF architecture should be placed following a template, in which the two victim lines have nearly the same total length and the signals' arriving time of interconnect network should be the same. This is easy to achieve by manually placing the cells in a specific position with scripts. The connection between the output of signature generator and the input of Self-Masking or Bit-Filtering Circuit should be as short as possible to relieve the impact of load capacitance.
- *Step 3* (General Circuit Placement and Routing): This step is slightly different with traditional placement and routing by applying additional option *-incremental* in Encounter [25].
- *Step 4:* Tape-out and Test.
- *Step 5* (Enrollment Phase): This step is carried out in a trusted environment, which could be realized by traditional or Secure Scans [26] that may include secure split-test mechanisms (SST/CSST) [27], [28]. Then, the CRPs are securely stored in a server.
- *Step 6:* Authentication phase.

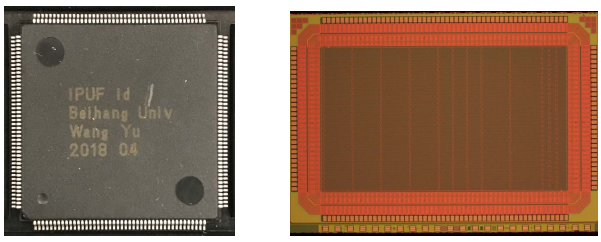
V. Experimental Results

In the experiment, Self-Masking Circuit is applied to iPUF for its smaller area overhead. To validate iPUF with Self-Masking Circuit, Monte Carlo simulations of 500 samples are performed in a 28-/32-nm technology node [29] to mimic manufacturing process variations. The design is integrated into several benchmark circuits from Gaisler [30], ITC99 [31], and OpenSPARCT2 [32], as shown in Fig. 8. The design is synthesized with a 125-MHz functional clock. Parameters used for Monte Carlo simulation are given in Table II. The signature generator is implemented with NAND2X4_LVT. During simulation, the same challenge set is applied to the LFSR of all 500 iPUF samples at 25 °C with 1.05-V supply voltage to produce a raw sequential signature of 1024-bit. Then, two uniqueness enhancements with different options are applied to the raw sequential signatures. Finally, iPUF is fabricated with a 55-nm technology. The package of taped-out

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

TABLE II
PARAMETERS USED FOR MONTE CARLO SIMULATION

Component	Nominal Value	Process Variation
Interconnect Network (passive)	$L = 900\mu m$	$3\sigma_L = 2\mu m$
	$W = 100nm$	$3\sigma_W = 10nm$
	$Sep = 10nm$	$3\sigma_{Sep} = 10nm$
NAND-based S/R Latch (Active Transistors)	$L = 30nm$	$3\sigma_L = 15\%$
	$W = 0.42\mu m(nmos)\ 0.38, 0.80\mu m(pmos)$	$3\sigma_W = 5\%$
	$T_{ox} = 2.22nm(nmos)\ 2.29nm(pmos)$	$3\sigma_{T_{ox}} = 5\%$
	$V_{Th} = 0.39V(nmos) - 0.19V(pmos)$	$3\sigma_{V_{Th}} = 20\%$



(a) (b)

Fig. 9. Image of manufactured iPUF. (a) Package of iPUF chips. (b) Schematic of iPUF with a scaling factor of 50.

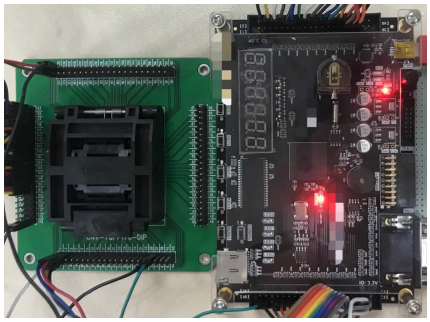


Fig. 10. Taped-out iPUF chips are tested by field-programmable gate array chips.

TABLE III
AREA OVERHEAD FOR iPUF WITH SELF-MASKING CIRCUIT

Benchmark	b19	FGU	Leon3s	s35932	VGA-LCD
Area Overhead (%)	0.19	0.08	0.15	1.86	0.16

iPUF chip is shown in Fig. 9(a). The schematic of iPUF by a microscope is shown in Fig. 9(b) under a scaling factor of 50, and the experimental setup of taped-out iPUF chips is shown in Fig. 10. Silicon data verify the reliability and uniqueness of iPUF, which is demonstrated in Section V-E.

A. Area Overhead

As shown in Fig. 1, the interconnect of iPUF can be routed in the upper metal layers that are uncongested and do not impact the active silicon area. Hence, the area overhead mainly comes from the LFSR and the Self-Masking Circuit. Table III lists the area overhead for five benchmarks with the active components, such as the 23-bit LFSR and a 10-bit mask application circuit. As seen, the area overhead is limited within 0.08%–1.86%.

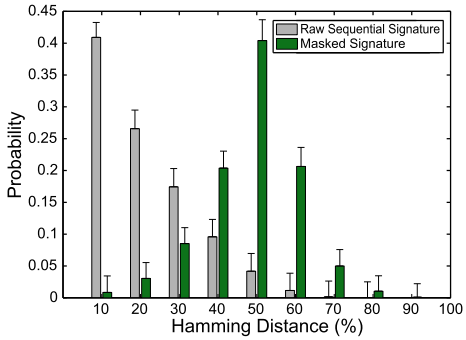


Fig. 11. HD distribution of the sequential signatures and masked signatures. The uniqueness increases to 48.63% with Self-Masking.

TABLE IV
UNIQUENESS OF MASKED SIGNATURE WITH DIFFERENT MASK LENGTHS ON iPUF'S RAW SEQUENTIAL SIGNATURE

Mask Length	No. of Masking Operation	Length of Masked Signature	Uniqueness of Mask %	Uniqueness of Masked Signature %
10-bit	103	1024	48.63	48.63
9-bit	57	512	48.67	48.53
8-bit	32	256	48.75	48.68
7-bit	19	128	48.53	48.01
6-bit	11	64	47.40	48.04
5-bit	7	32	46.25	47.82

B. Uniqueness Analysis

The uniqueness of iPUF is calculated by the average HD among responses generated from all iPUF samples when the same challenge set is applied [33]. As shown in Fig. 11, the uniqueness of the raw sequential signature (without uniqueness enhancement circuit) is only 20.62%, whereas the uniqueness of the masked signature is improved to 48.63% (ideal = 50%). Meanwhile, the average HD of mask is 49.74%, which is regarded as the source of entropy. The results demonstrate that the Self-Masking Circuit significantly increases the uniqueness of the final output of iPUFs.

To test the effectiveness of self-masking scheme when applied to sequential signatures with different lengths, the Masks are generated by sequential signatures with different lengths ranging from 31 to 1023, and correspondingly, the lengths of Masks range from 5 to 10. The uniqueness of masked signature is shown in Table IV. The third column represents the signature length used to generate a Mask and also the length of masked signature. The fifth column indicates the uniqueness of masked signatures when Masks of different lengths are applied to sequential signatures of different lengths. The results demonstrate that the self-masking scheme increases iPUFs' uniqueness to satisfied values around 50% for Masks' length ranging from 7 to 10.

The bit-filtering scheme is also applied to the sequential signatures of 500 iPUF samples, and several simulation options are listed in Table V. The bit-filtering scheme improves the overall uniqueness. However, the HD is not centrally distributed around 50% as plotted in Fig. 12, of which five sub-iPUFs are implemented in each chip with threshold equaling to

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

TABLE V
UNIQUENESS OF FILTERED SIGNATURE WITH A DIFFERENT NUMBER OF SUB-PUFS AND THRESHOLD OPTIONS

No. of sub-iPUF	Threshold	Length of Filtered Signature	Uniqueness%
2	2	128	46.96
3	3	128	50.08
4	4	128	49.65
5	4	128	48.31
5	5	128	49.42

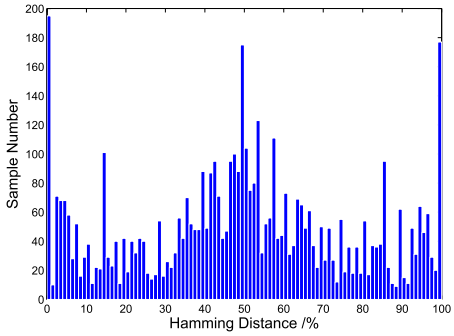


Fig. 12. HD distribution for bit-filtering scheme. Five sub-iPUFs are implemented in each chip with threshold equaling to 5.

5. Instead, there exit around 200 pairs of signatures with minimum or maximum HDs.

To further improve the uniqueness, every two bits of each filtered signature are XORed by XOR window. The HD distribution of filtered signature with and without XOR window is shown in Fig. 13 for different numbers of sub-iPUFs. As shown in Fig. 13(f), the uniqueness of XORed signature is centered around 50% with five sub-iPUFs and 2-bit XOR Window.

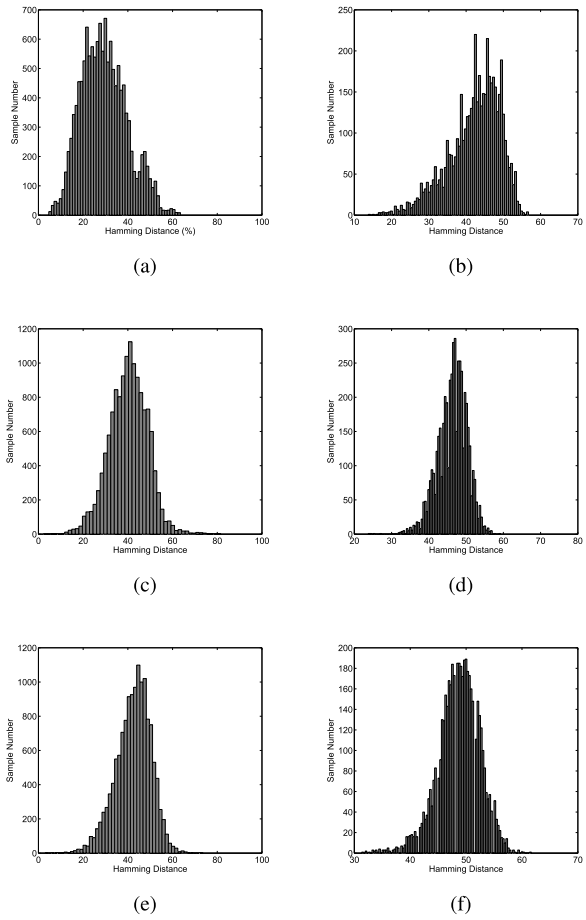


Fig. 13. HD distribution of filtered signatures without and with XOR window. (a) HD distribution for three sub-iPUFs. (b) HD distribution for three sub-iPUFs with 2-bit XOR window. (c) HD distribution for 3 sub-iPUFs. (d) HD distribution for four sub-iPUFs with 2-bit XOR window. (e) HD distribution for five sub-iPUFs. (f) HD distribution for five sub-iPUFs with 2-bit XOR window.

C. Uniformity Analysis

Uniformity represents the bias of a generated signature by calculating the proportion of "1." The ideal uniformity is 50%, indicating an equal "0/1" probability. However, any bias in the "0/1" probability reduces the uniformity and makes the PUF output vulnerable to modeling attacks. The average uniformity of the raw sequential signatures and masked signatures is 56.17% and 48.53%, as shown in Fig. 14(a) and (c), respectively. The results show that the Self-Masking Circuit improves the uniformity. Meanwhile, the bit aliasing of raw sequential signatures and masked signatures is plotted in Fig. 14(b) and (d), respectively. Note that the Self-Making Scheme reduces bit aliasing of the iPUF signature as well.

D. Reliability Analysis

The reliability of iPUF is analyzed under runtime environmental variations, such as temperature and power supply variation, as well as aging. The signatures of 500 iPUF samples are collected with temperature varying from 0 °C to 100 °C and supply voltage ranging within 1.05 V±10%, where the nominal operating condition is 1.05-V supply voltage at 25 °C. Fig. 15 shows the average reliability, measured in terms of BER. As seen, the average worst case BER caused by voltage and temperature variation is 3.91% and 0.94%, respectively. The results demonstrate that by maximizing passive components (i.e., interconnect) usage, iPUF's reliability is satisfying. Fig. 16 shows the distribution of HD between the signatures generated after one year of aging considering 24 h of unaccelerated reliability burn-in. The average intrachip HD for all 500 iPUF samples is 0.36%. The results show that with short burn-in, the aging reliability of iPUF is satisfying.

The reliability of iPUF under voltage/temperature variations and aging with variable signature sizes is compared with the related approaches in Table VI. As shown in Table VI, the reliability of iPUF is not affected by signature size, as the unreliable signature bits are randomly distributed among all the signature bits. In addition, iPUF shows better reliability than nonlinear VTC PUF [18], TERO PUF [17], and Buskeeper PUF [11].

E. Silicon Results

The taped-out 50 iPUF chips are tested under the normal condition with 1.2-V supply and 25 °C. Each chip is

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

TABLE VI

RELIABILITY OF iPUF AND THE EXISTING APPROACHES WITH VARIABLE SIGNATURE SIZES

	iPUF			Existing Literature		
Signature Size (bits)	**Vol. Variations (1.05V ± 10 %)**	**Temp. Variations (0-100°C)**	**After Aging (1-year)**	**Vol. Variations (± 10 %)**	**Temp. Variations (0-85°C)**	**After Aging**
64	96.06	99.22	99.72	96 [18]	96 (0-75°C) [18]	NA
128	95.47	98.89	99.63	96.91 [16] (± 20 %)	99.27 (0-100°C) [16]	98.42 (2.5-year) [16]
256	95.66	98.94	99.61	97.25 (252-bit, Normal Condition) [17]		NA
1024	96.09	99.06	99.64	95 [11]	80 [11]	93 (7-year) [11]

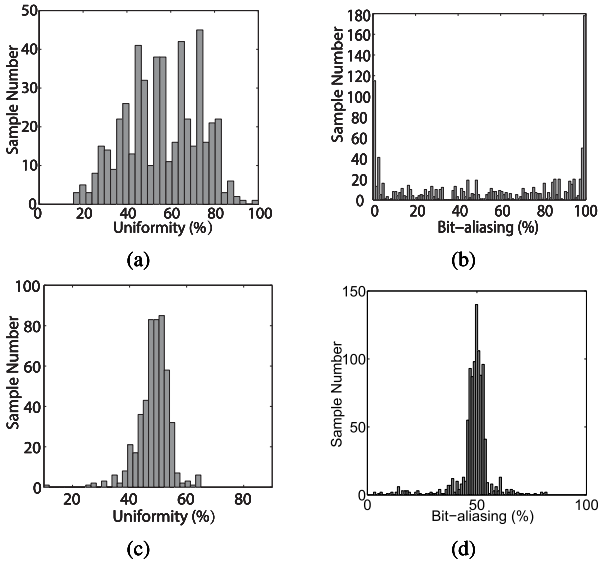


Fig. 14. Uniformity and bit aliasing for the raw sequential signatures before masking and masked signatures. (a) Uniformity of raw sequential signatures before masking, $\mu = 56.17\%$. (b) Bit aliasing of raw sequential signatures, $\mu = 56.17\%$. (c) Uniformity of masked signatures, $\mu = 48.53\%$. (d) Bit aliasing of masked signatures, $\mu = 48.53\%$.

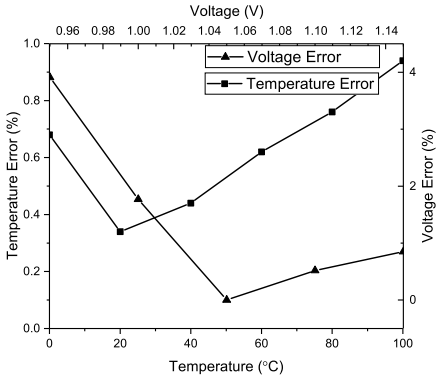


Fig. 15. Reliability of iPUF under temperature and voltage fluctuations. The average worst case reliability for all 500 iPUF samples is 96.09% and 99.06% under voltage and temperature variation, respectively.

implemented with six iPUFs, and self-masking schemes is applied to the raw sequential signatures. During each test, iPUF chips generate raw sequential signatures of 1024 bits. The uniqueness of raw sequential signatures is 39.01%. Due to process variations of NAND devices and clock skew, iPUF tends to generate signatures with more "1's" or "0's".

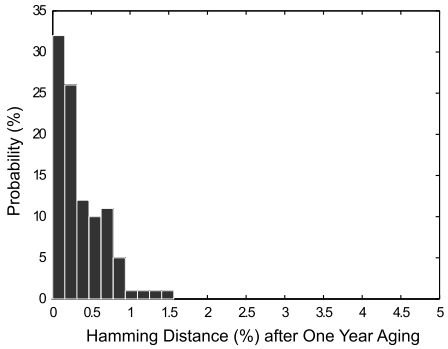


Fig. 16. HD distribution after one-year aging. The average HD is 0.36% for all 500 iPUF samples.

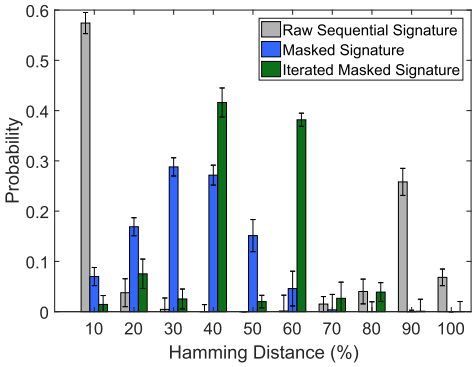


Fig. 17. HD distribution of the Raw sequential signatures, masked signatures, and Iterated masked signatures from the taped-out iPUF chips. The uniqueness increases from 39.01% to 48.03% with the iterated self-masking scheme.

Thus, the HD of raw sequential signatures distributes around 0% and 100%, as shown in Fig. 17. Then, by applying self-masking schemes, the uniqueness of masked signatures is centered around 35.33%. To further increase the uniqueness of masked signatures, the masks of each iPUF are shifted by a certain number of bits, which is decided by the sum of "1's" within each mask. Then, the masked signatures are iteratively masked with the shifted masks. The distribution of HDs for Iterated masked signatures is also shown in Fig. 17, with uniqueness increased to 48.03%.

Then, the taped-out iPUF chips are tested under environmental variations with supply voltage ranging within 1.2 V ± 60 mV. The reliability under voltage variations is within 90.07%–97.31%, as shown in Fig. 18.

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

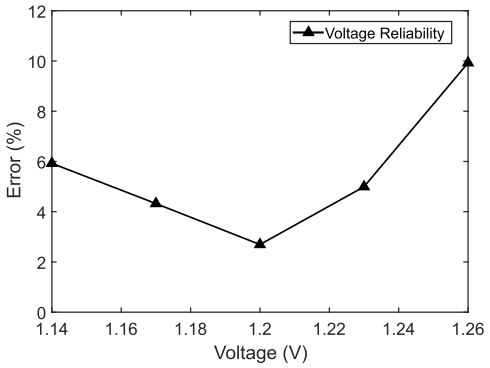


Fig. 18. Reliability of taped-out iPUF under voltage fluctuations. The average worst case reliability for 50 iPUF chips is 90.07%.

F. Scalability Analysis for New Technologies

The proposed iPUF structure is scalable for new technologies, provided that two prerequisites are satisfied (i.e., enough crosstalk between the neighboring interconnects and enough process variations of interconnect). First, assume that an interconnect network is composed of three parallel routed wires, where the wires are driven independently and simultaneously. The propagation delay of the middle wire (i.e., victim interconnect) is decided by the transitions on the neighboring two wires and can be approximated by

$$t_{p,\text{victim}} = gC_W(0.38R_W + 0.69R_D) \tag{5}$$

where C_W and R_W are the capacitance and inductance of the victim interconnect and g is the factor of crosstalk effect [34]. g is a function of the ratio $r = c_i/c_w$ and the transitions on the neighboring two aggressors, where c_i and c_w are the coupling capacitance and capacitance to ground of the wire per unit length. For different transitions, g ranges from 1 to $1+4r$. Given a scaling factor S of interconnect width, height, and substrate thickness, the ratio r with minimum coupling capacitance c_i (no fringe capacitance) can be obtained by

$$r = \frac{c_i}{c_w} \propto \frac{H}{\text{Space}} \Big/ \frac{W}{t} = \frac{1}{S \cdot \text{Space}}. \tag{6}$$

If the minimum space between two interconnects is also scaled at a factor of S, then the scaling of technology has no impact on the factor of crosstalk effect. Hence, there will still be enough crosstalk between the neighboring interconnects.

Second, for advanced technology, the process variations of interconnects remain. The process variations of interconnect dimensions come from several main processes during fabrication, including photolithography, metalization, rapid thermal process (RTP), and chemical mechanical polishing (CMP) [35]. These manufacture steps result in the variations on wire height, 10% effective linewidth, and line-edge roughness even for the advance deep UV photolithography [36]. These variations on wire dimensions can cause great differences in the coupling capacitance and inductance among the interconnect, which contributes to the uniqueness of the signatures generated by iPUF.

G. Comparison With the Existing PUFs

Nine popular PUFs, RO-PUF [8], arbiter PUF [37], SRAM-PUF [9], SRAM-PUF with bit selection [13], butterfly PUF [10], aging resistant RO-PUF [16], TERO PUF [17], nonlinear VTC [18], and buskeeper PUF [11], are selected for comparison, as shown in Table VII. According to Table VII, iPUF shows better reliability and satisfying security performance (see Section VI) compared with RO-PUF, arbiter PUF, SRAM-PUF, butterfly PUF, nonlinear VTC PUF, and buskeeper PUF. Meanwhile, iPUF requires less area overhead and shows better signature generation efficiency compared with aging-resistant RO-PUF and TERO PUF. In terms of security, the security of approaches proposed in [11], [16], and [17] is not proved in the reference. However, iPUF is proven to be resistant to several existing attacks.

VI. Security Anaylsis

IP-/IC-based mobile and embedded devices perform massive tasks in all aspects of our lives. Many of these tasks should be performed through authenticated devices to prevent malicious control, and the private information transmitted during the tasks should be securely protected with encryption. PUFs are a promising hardware primitive applicable for the above-mentioned scenarios. Hence, the security of IPs/ICs in terms of low-cost authentication and key generation is dependent on the security of PUFs.

There are several purposes for an adversary to attack on iPUF and other PUFs. For example, attackers can simply cause the PUF to fail by deteriorating the reliability of it. In addition, during devices authentication, attacker wants to be authenticated without the possession of the legal devices. Furthermore, attacker may want to steal the secure information encrypted by the keys generated by PUFs. The attack models can be even more different for varied purposes and PUFs. Several existing attacks targeting at PUF signature are analyzed as follows.

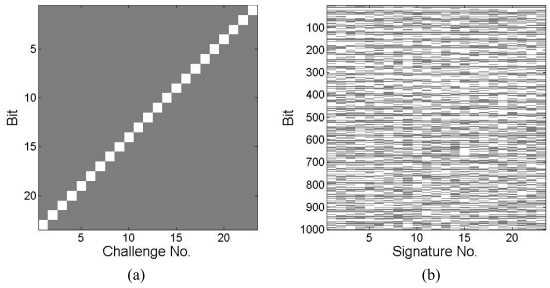
1) Modeling Attack: Machine learning (ML)-based modeling attack is currently one of the most effective attacks for strong PUFs [3], [23], [44], [45]. It is assumed that during the attack, a subset of CRPs generated by strong PUF is available to attackers through both physical access periods and simple protocol eavesdropping [44]. Modeling attack is generally carried out in three steps: 1) attacker collects a CRP set of a specific PUF; 2) attacker uses the CRP set to train the predictive model and calculate the hyperplane; and 3) attacker applies new challenges and uses the predictive model for the specific PUF to obtain the complete PUF CRPs [44]. The effectiveness of modeling attack is based on a critical fact that similar challenges tend to generate similar responses, i.e., delay variations among delay blocks are independent and the final response can be linearly model based on the input challenges. Thus, arbiter PUF, the delay of which is a linear function of the signature, is vulnerable to ML-based modeling attack. During the attack, the delay difference of two paths within an arbiter PUF can be modeled as the sum of the delay difference in each stage [41]. Then, by obtaining a certain number of CRPs, the separating hyperplane between all challenges and responses is determined. The prediction

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

TABLE VII
COMPARISON OF iPUF AND THE EXISTING PUFs

Metrics	iPUF	RO-PUF [8]	Arbiter PUF [37]	SRAM-PUF [9]	SRAM-PUF with Bit Selection [13]	Butterfly PUF [10]	Aging Resistant RO-PUF [16]	TERO PUF [17]	Non-Linear VTC [18]	Buskeeper PUF [11]
Technology Node	28/32nm	Spartan XC3S500E 90nm	180nm	NA	Xilinx Spartan-3 90nm	Xilinx Virtex-5 65nm	90nm	Altera Cyclone II 90nm	45nm	65nm
Area Overhead (transistor)	792	NA	≈4320 ($0.02mm^2$)	NA	NA	≈256	101230	relatively high	1280	4000 without addressing
Uniqueness (%)	48.63	45.9	50.0	50.0	49.8	45.0	47	48.07	49.8	49
Volt. Temp. Error (%)	0.47-3.91	3.2	3.1-15.6	3.6-12.0	0.11	6.0	3.09	1.73-2.75	4	20 (Temp.)
Aging Error (%)	0.36 (1 year)	NA	NA	4.4	0.3	NA	1.58 (2.5 year)	NA	NA	7 (4.5 year)
Signature Bit per Challenge	$\leq 2^{\lambda^*}-1$	1	$\leq 2^{k^*}$	≤ SRAM Size	≤ SRAM Size	50	128	126-252	64	1kB
Security	Robust Against Attacks Listed in Section VI	Vulnerable to Fault Injection [38] and Sinusoidal Attack [39]	Vulnerable to Modeling Attack [40] [41]	Vulnerable to Fault Injection Attack [42]	Vulnerable to Near-infrared Imaging [4]	Vulnerable to Side-channel Attack [43]	Vulnerable to Fault Injection Attack	Resistant to Electromagnetic Attack	Resistant to Modeling Attack	Resistant to Reverse Engineering

NA indicates that the data is not available.
λ is the stage of the LFSR implemented in iPUF.
k is the stage of arbiter PUF.



(a) (b)

Fig. 19. Binary images of challenges and masked signatures. Black pixels represent for "0" and white ones represent for "1." (a) Challenge. (b) Masked Signature.

rate reaches up to 95% for a 64-stage arbiter PUF given 64 CRPs [41]. However, as stated before, the iPUF depends on nonlinear components such as variations in coupling capacitors with complex dependence among associated parameters making it inherently resilient to the modeling attack. To verify the robustness of iPUF under modeling attack, 23 one-hot challenges are applied, as shown in Fig. 19(a). According to Fig. 19(b), the average HD of the 23 responses is 30.54%, indicating that iPUF is capable of yielding significantly diverged signatures for similar challenges, which introduces significant difficulty for modeling attack. In addition, the HD of the responses generated by 23 one-hot challenges is 19.34%, 25.30%, and 27.10% for 64-, 128-, and 256-bit signature sizes, respectively. The security of iPUF against ML-based modeling attack is satisfied with variable signature sizes.

2) Fault Injection Modeling Attack: During fault injection modeling attack, attacker intentionally applies environmental variations to identify reliable CRP set and shrinks the dimension of CRP space to facilitate modeling attack [38]. Hence, it is applicable to arbiter PUF and RO-PUFs, of which challenges are already reduced for reliability improvement. For RO-PUF, the frequencies of different ROs are compared to generate each signature bit. Attacker can infer the signature by sorting the ROs' frequency with a certain number of CRPs [41]. Furthermore, the fault injection attack can be applied to shrink the dimension of CRPs to accelerate the modeling attack [39]. The modeling speed is improved by 2.4 times with the largest environmental variations [39]. Based on the fact that some SRAM bits are influenced by the written data if the power-OFF time is short, fault injection can be performed by controlling the power-OFF time between the writing and querying processes of SRAM. With this method, the SRAM-PUF response of 216-bit can be recovered by using the algorithm at most 2^{64} [42]. However, for iPUF with satisfying reliability, there is no need to distinguish the reliable challenge and response bits from unstable ones. Thus, environmental variations cannot be used to shrink CRP space for iPUF. Again, the difficulty of modeling attack cannot be reduced by fault injection for iPUF.

3) Memory Attack: Although the mask is stored in memory, even if the mask is stolen [46], [47], attacker only knows how many logic one values are there in the specific raw sequential signature used during the mask training phase, and the probability of guessing another raw sequential signature using brute force is still $1/2^n$, where n is the signature length. The time effort of guessing a sequential signature with signature size larger than 64-bit is enormous. Besides, an attacker may use mask value to obtain the raw sequential signatures

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

before masking. However, for the same iPUF, as the mask is consistent, the average HD of the raw sequential signatures before masking and masked signatures is the same. Therefore, removing mask does not reduce the modeling attack difficulty.

4) Deterministic Attack: In the deterministic attack, attacker (i.e., fab) controls the process parameter to bias the output signature. For example, attacker chooses different cells for NAND1 and NAND2 in signature generator (see Fig. 2) to bias iPUF signature. A simulation is conducted, in which NAND1 and NAND2 are synthesized with NAND2X1_RVT and NAND2X2_LVT, respectively, for all 500 iPUF samples. According to the simulation results, the uniqueness of the raw sequential signatures before masking under attack is 15.95%. However, with the help of Self-Masking Circuit, the uniqueness of 1024-bit masked signatures is recovered to 46.93%. In addition, the uniqueness of iPUF is improved to 45.73%, 46.21%, and 46.58% for 64-, 128-, and 256-bit masked signatures, respectively. The results demonstrate that iPUF's signature with variable sizes is slightly biased by deterministic attack without security loss.

5) Side-Channel Attack: Side-channel attack is an effective way to gain the implementation information of a cryptosystem and can be combined with ML modeling attack to address the issue of computational complexity [43]. Side-channel attack can be performed by extracting varied power profile caused by the internal operation. Butterfly PUF, which is composed of two cross-coupled latches, is vulnerable to side-channel attack. After releasing the excite signal, two latches turn to "1" or "0." Similar to the latch-based arbiter [48], the latch-based butterfly PUF requires more power when generating signature "1" than "0". Hence, with the power side-channel attack, the current track and power consumption below each current trace can be collected [43]. Furthermore, based on the extra power consumption of each response, the portion of "1" can be deduced, which significantly improves the probability of guessing it. As for iPUF, due to the symmetrical structure of signature generator [see Fig. 2(a)], the two NAND gates generate the same switch pattern at every clock cycle. Specifically, at the rising edge of system clock, there is always one of the NAND gates switches from "1" to "0," while the other one statically holds "1." Thus, the power supply is identically impacted no matter the generated signature is "0" or "1." The correlation between 1024-bit sequential signature and 1024 power traces at one of the nearest power supply during 1024 clock cycles is 0.067, of which the sampling window is 2 ns. In addition, the correlation between sequential signature and power traces is 0.172, 0.126, and 0.097 for 64-, 128-, and 256-bit signature sizes, respectively. The results indicate a weak correlation and demonstrate that signatures of iPUF with variable sizes are resistant to side-channel attack. Although the LFSR within iPUF may be vulnerable to side-channel attacks, it leaks no information about the mapping between challenges and signatures. As the signature generated by iPUF depends on the variations of coupling capacitance and inductance with complex dependence among associated parameters, the attacker further needs the initial signatures to find out the relationship between challenge vectors and each signature bit. However, the signatures of iPUF are resistant to side-channel attack. The architecture of iPUF is proven to be capable of preventing the signatures from being attacked, and these capabilities are not weakened by reducing the signature size. However, due to the reduced cost of exhaustive method, the security of iPUF may be lowered with shorter signatures.

VII. Conclusion

In this article, a novel iPUF is proposed to overcome the drawbacks of traditional PUF design. The minimized implementation of active components makes iPUF reliable to voltage and temperature fluctuations and also resilient to aging. By introducing LFSR, the iPUF is capable of generating signatures with arbitrary length. Besides, two uniqueness enhancement schemes for sequential PUFs are proposed and applied to iPUF. Although the uniqueness enhancement schemes require extra memory, area, and power resources, it has no impact on the reliability and security of iPUF. The uniqueness of iPUF signatures is satisfying with the help of uniqueness enhancement circuit. The proposed iPUF structure has been verified on benchmarks from Gaisler, ISCAS, and OpenSPARCT2 with a 28-/32-nm technology and taped-out with a 55-nm technology. Silicon data verify the uniqueness and reliability performance of iPUF. Moreover, the proposed iPUF is resistant to potential PUF attacks.

References

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, Nov. 2002, pp. 148–160.

[3] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Automat. Conf.*, Jun. 2007, pp. 9–14.

[4] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[5] M. M. Tehranipoor, U. Guin, and D. Forte, "Counterfeit integrated circuits," in *Counterfeit Integrated Circuits: Detection and Avoidance*. Cham, Switzerland: Springer, 2015, pp. 15–36, doi: 10.1007/978-3-319-11824-6_2.

[6] K. Yang, D. Forte, and M. M. Tehranipoor, "Protecting endpoint devices in IoT supply chain," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2015, pp. 351–356.

[7] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[8] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *Proc. Int. Conf. Field Program. Logic Appl.*, Aug./Sep. 2009, pp. 703–707.

[9] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2007, pp. 63–80, doi: 10.1007/978-3-540-74735-2_5.

[10] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 67–70.

[11] P. Simons, E. van der Sluis, and V. van der Leest, "Buskeeper PUFs, a promising alternative to D flip-flop PUFs," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2012, pp. 7–12.

[12] K. Cho, K.-H. Lee, S.-Y. Kim, S.-J. Lee, and Y. You, "Implementation of a physical unclonable function (PUF) with transmission line crosstalk in a chip," in *Proc. 5th Asia Symp. Qual. Electron. Design (ASQED)*, Aug. 2013, pp. 240–244.

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

[13] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 101–106.
[14] A. Hosey, M. T. Rahman, K. Xiao, D. Forte, and M. Tehranipoor, "Advanced analysis of cell stability for reliable SRAM PUFs," in *Proc. IEEE 23rd Asian Test Symp. (ATS)*, Nov. 2014, pp. 348–353.
[15] A. Garg and T. T. Kim, "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Jun. 2014, pp. 1941–1944.
[16] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant RO-PUF for reliable key generation," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 3, pp. 335–348, Jul./Sep. 2016.
[17] L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, "A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon," *IEEE Trans. Emerg. Topics Comput.*, vol. 2, no. 1, pp. 30–36, Mar. 2014.
[18] A. Vijayakumar and S. Kundu, "A novel modeling attack resistant PUF design based on non-linear voltage transfer characteristics," in *Proc. Design, Automat. Test Eur. Conf. Exhibit. (DATE)*, Mar. 2015, pp. 653–658.
[19] M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *Proc. Design, Autom. Test Eur. Conf. Exhib.*, Mar. 2014, pp. 1–6.
[20] A. Maiti, I. Kim, and P. Schaumont, "A robust physical unclonable function with enhanced challenge-response set," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 333–345, Feb. 2012.
[21] Y. Wang, S. Cotofana, and L. Fang, "A unified aging model of NBTI and HCI degradation towards lifetime reliability management for nanoscale MOSFET circuits," in *Proc. IEEE/ACM Int. Symp. Nanoscale Archit.*, Jun. 2011, pp. 175–180.
[22] B. Li, C. Christiansen, D. Badami, and C.-C. Yang, "Electromigration challenges for advanced on-chip Cu interconnects," *Microelectron. Rel.*, vol. 54, no. 4, pp. 712–724, 2014.
[23] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2008, pp. 670–673.
[24] *Next-Generation Design Compiler*. Accessed: Sep. 24, 2019. [Online]. Available: https://www.synopsys.com/implementation-and-signoff/rtl-synthesis-test/design-compiler-nxt.html
[25] *Cadence Physical Verification System*. Accessed: Sep. 24, 2019. [Online]. Available: https://www.cadence.com/content/dam/cadence-www/global/en_US/documents/tools/digital-design-signoff/physical-verification-system-ds.pdf
[26] D. Hely, F. Bancel, M.-L. Flottes, and B. Rouzeyre, "Secure scan techniques: A comparison," in *Proc. IEEE Int. On-Line Test. Symp.*, Jul. 2006, p. 6.
[27] G. K. Contreras, M. T. Rahman, and M. Tehranipoor, "Secure split-test for preventing IC piracy by untrusted foundry and assembly," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2013, pp. 196–203.
[28] M. T. Rahman, D. Forte, Q. Shi, G. K. Contreras, and M. Tehranipoor, "CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst.*, Oct. 2014, pp. 46–51.
[29] Synopsys. *Teaching Resources*. Accessed: Apr. 5, 2017. [Online]. Available: http://www.synopsys.com/community/university-program/teaching-resources.html
[30] *Gaisler Benchmark*. Accessed: Apr. 5, 2017. [Online]. Available: http://www.gaisler.com/index.php/downloads/leongrlib
[31] *ITC99 Benchmark*. Accessed: Apr. 5, 2017. [Online]. Available: http://www.cerc.utexas.edu/itc99-benchmarks/bench.html
[32] *Opensparc T2 Benchmark*. Accessed: Apr. 5, 2017. [Online]. Available: http://www.oracle.com/technetwork/systems/opensparc/opensparc-t2-page-1446157.html#t2-to-use
[33] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design With FPGAs*, P. Athanas, D. Pnevmatikatos, and N. Sklavos, Eds. New York, NY, USA: Springer, 2013, pp. 245–267, doi: 10.1007/978-1-4614-1362-2_11.
[34] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolic, *Digital Integrated Circuits*, vol. 2. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.
[35] S. A. Campbell, *The Science and Engineering of Microelectronic Fabrication* (The Oxford Series in Electrical and Computer Engineering). Oxford, U.K.: Oxford Univ. Press, 2001.
[36] G. G. Lopez, "The impact of interconnect process variations and size effects for gigascale integration," Ph.D. dissertation, Dept. Elect. Comput. Eng., Georgia Inst. Technol., Atlanta, Georgia, 2009.
[37] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based 'Unclonable' RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 58–64.
[38] J. Delvaux and I. Verbauwhede, "Fault injection modeling attacks on 65 nm arbiter and RO sum PUFs via environmental changes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 6, pp. 1701–1713, Jun. 2014.
[39] A. T. Markettos and S. W. Moore, "The frequency injection attack on ring-oscillator-based true random number generators," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2009, pp. 317–331.
[40] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing techniques for hardware security," in *Proc. IEEE Int. Test Conf.*, Oct. 2008, pp. 1–10.
[41] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. CCS*, 2010, pp. 237–249.
[42] Y. Oren, A.-R. Sadeghi, and C. Wachsmann, "On the effectiveness of the remanence decay side-channel to clone memory-based PUFs," in *Proc. 15th Int. Conf. Cryptograph. Hardw. Embedded Syst. (CHES)*, 2013, pp. 107–125.
[43] X. Xu and W. Burleson, "Hybrid side-channel/machine-learning attacks on PUFs: A new threat?" in *Proc. Conf. Design, Autom. Test Eur. (DATE)*, Leuven, Belgium, 2014, pp. 349:1–349:6. [Online]. Available: http://dl.acm.org/citation.cfm?id=2616606.2617100
[44] U. Rührmair and J. Sölter, "PUF modeling attacks: An introduction and overview," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2014, pp. 1–6.
[45] U. Ruhrmair *et al.*, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov. 2013.
[46] G. Shi and J. Ru, "Research on classification of memory attack," in *Proc. 2nd Workshop Adv. Res. Technol. Ind. Appl. (WARTIA)*. Paris, France: Atlantis Press, May 2016, pp. 392–397, doi: 10.2991/wartia-16.2016.78.
[47] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," *Phys. Rev. Lett.*, vol. 110, no. 1, 2013, Art. no. 010503.
[48] A. Mahmoud, U. Rührmair, M. Majzoobi, and F. Koushanfar, "Combined modeling and side channel attacks on strong PUFs," Cryptol. ePrint Arch., Houston, TX, USA, Tech. Rep. 2013/632, 2013.

Liting Yu received the B.S. degree in electrical engineering from Beihang University, Beijing, China, in 2016, where she is currently working toward the Ph.D. degree at the School of Electronic and Information Engineering, along with Dr. X. Wang.

Her current research interests include on-chip monitoring sensor, high-reliable PUF, aging prediction, and reliability screening methodology.

Xiaoxiao Wang (M'04) received the B.S. and M.S. degrees in electrical engineering from Beihang University, Beijing, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Connecticut, Storrs, CT, USA.

In 2010, she joined the Defect and Fault Tolerance (DFT) Team, Microcontroller Solutions Group, Freescale Semiconductor, Austin, TX, USA. In 2014, she joined the faculty of Beihang University, where she is currently a Professor. Her current research interests include on-chip measurement architecture design, reliability, and design for testability (DFT).

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.

Fahim Rahman (S'13–M'19) received the B.S. degree in electrical and electronic engineering from the Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 2009, the M.S. degree in electrical and computer engineering from the University of Connecticut, Storrs, CT, USA, in 2015, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, in 2018.

He is currently a Research Assistant Professor with the Electrical and Computer Engineering Department, University of Florida, Gainesville. His current research interests include hardware and cybersecurity and trust, including investigation of hardware security primitives, CAD for security and automatic assessment, electronic supply-chain security, and hardware-assisted cybersecurity. His research has been sponsored by the Semiconductor Research Corporation (SRC), the Air Force Office of Scientific Research (AFOSR), the Air Force Research Laboratory (AFRL), Defense Advanced Research Projects Agency (DARPA), Cisco, Texas Instruments (TI), and the National Institute of Standards and Technology (NIST).

Prof. Rahman is a member of the Association for Computing Machinery (ACM).

Mark Tehranipoor (S'02–M'04–SM'07–F'18) received the Ph.D. degree from The University of Texas at Dallas, Richardson, TX, USA, in 2004.

He was the Founding Director of the CHASE and CSI Centers, University of Connecticut, Storrs, CT, USA. He is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in cybersecurity with the University of Florida (UF), Gainesville, FL, USA, where he is also the Founding Director of the Florida Institute for Cybersecurity Research (FICS). He has published over 400 journal articles and refereed conference articles, ten books, and more than 20 book chapters. His current research interests include hardware security and trust, supply chain security, Internet-of-Things security, and VLSI design, test, and reliability.

Dr. Tehranipoor is a Golden Core Member of the IEEE Computer Society and a member of Association for Computing Machinery (ACM) and ACM Special Interest Group on Design Automation (SIGDA). He was a recipient of a dozen best paper awards and nominations, the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 AFOSR MURI Award. He serves on the program committee of more than a dozen leading conferences and workshops. He has served as the Program Chair for a number of IEEE and ACM sponsored conferences and workshops, including HOST, DFT, D3T, DBT, and NATW. He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), where he has served as the HOST-2008 and HOST-2009 General Chair. He also serves as the Founding Editor-in-Chief for *Journal on Hardware and Systems Security* (HaSS) and an Associate Editor for the *Journal of Electronic Testing: Theory and Applications* (JETTA), the *Journal of Low Power Electronics* (JOLPE), the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, and the *ACM Transactions on Design Automation of Electronic Systems* (TODAES).

Authorized licensed use limited to: University of Florida. Downloaded on July 12,2021 at 19:38:10 UTC from IEEE Xplore. Restrictions apply.