ScanPUF: Robust Ultralow-Overhead PUF Using Scan Chain

Yu Zheng
Department of EECS
Case Western Reserve Univ.
Cleveland, OH, 44106
e-mail: yu.zheng3@case.edu

Aswin Raghav Krishna
Department of EECS
Case Western Reserve Univ.
Cleveland, OH, 44106
e-mail: ark70@case.edu

Swarup Bhunia
Department of EECS
Case Western Reserve Univ.
Cleveland, OH, 44106
e-mail: skb21@case.edu

Abstract— Physical Unclonable Functions (PUFs) have emerged as an attractive primitive to address diverse hardware security issues, such as chip authentication, intellectual property (IP) protection and cryptographic key generation. Existing PUFs, typically acquired and integrated in a design as a commodity, often incur considerable hardware overhead. Many of these PUFs also suffer from insufficient challenge-response pairs. In this paper, we propose *ScanPUF*, a novel PUF implementation using a common on-chip structure used for improving circuit testability, namely scan chain. It exploits path delay variations between the scan flip-flops in a scan chain to create high-quality (in terms of uniqueness and robustness) secret keys. Furthermore, since a scan chain provides large pool of scan paths to create a signature, we can achieve high volume of secret keys from each chip. Since it uses a prevalent on-chip structure, the overhead is extremely small (2.3% area of the RO-PUF), primarily contributed by small additional logic in the signature-generation cycle controller. Circuit-level simulation results with 1000 chips under inter- and intra-die process variations show high uniqueness of 49.9% average inter-die Hamming distance and good reproducibility of 5% intra-die Hamming distance below 85 °C. The temporal variations due to device aging effect e.g. bias temperature instability (BTI) lead to only 4% unstable bits for ten-year usage. The experimental evaluation on FPGA (Altera Cyclone-III) exhibits 47.1% average inter-Hamming distance, as well as 3.2% unstable bits at room temperature.

I. Introduction

The generation of unique keys by Integrated Circuits (ICs) has important applications in areas such as Intellectual Property (IP) counter-plagiarism and embedded security integration. Traditionally, they need the secret key to be stored in a non-volatile memory (NVM) that cannot be easily accessed or duplicated by adversaries. However, such storage is vulnerable to invasive attack while the high tampering resistance environment is expensive [1]. Furthermore, since the number of secret keys is small (usually one), attackers may steal them successfully by intercepting the communication between the user and the provider.

In order to address these issues, Physical Unclonable Functions (PUFs) [2], [4]–[9] have been explored to build tamper-resistant hardware. PUFs are realized by creating a challenge-response protocol that exploits the inherent random variations in a manufacturing process to generate unique signatures [2]. Process variations cause fluctuations in device parameters, such as threshold voltage (V_{th}), channel length (L), leading to variations in circuit level parameters (e.g. path delay), which are typically used in a PUF for signature generation. PUFs have the following advantages when applied in many hardware security applications. First, the challenge-response pairs are random and difficult to predict for an attacker. In addition, the challenge-response space can be vast enough that makes random trials ineffective. Second, unlike digital keys stored in NVM, PUFs are safer since a signature is available only when the chips are running and a specific challenge vector is applied. Finally, the cost of a PUF is expected to be lower than digital key storage accompanied by tampering resistance.

However, a majority of existing PUFs (e.g. [5]–[7]) demand dedicated circuit structures, which incur considerable area overhead and hence may not be suitable for many area-constrained embedded applications. On the other hand, PUFs realized with on-chip structures (e.g. embedded memory [9] [10] or intrinsic flip-flops (FFs) [11]) are effective to greatly lower the hardware overhead and design effort/cost. The SRAM PUF and intrinsic PUF respectively leverage on random initialization of embedded memory cells and FFs under process variation. However, they only generate one-bit signature per cell and hence suffer from insufficient challenge-response pairs. To address this issue, a memory-based PUF, referred to as *MECCA PUF* [10], which uses the write-pulse duration as challenge, creates signatures based on write failures in memory cells. However, *MECCA PUF* can only be employed to embedded memory of specific structures. Moreover, both types of memory PUF require a reasonably large size of embedded memory to generate acceptable volume of challenge-response pairs.

In this paper, we present *ScanPUF*, a novel PUF implementation using a common on-chip structure. It exploits the prevalent scan chain based design-for-test (DFT) structure to create large volume of signatures from a chip based on random delay variations in timing paths between two scan flip-flops (SFFs). Fig. 1 illustrates the overall approach of signature

978-1-4673-3030-5/13/$31.00 ©2013 IEEE

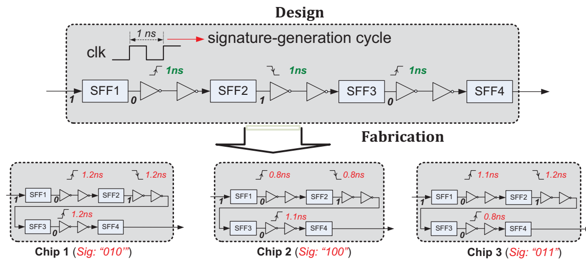

Fig. 1. Illustration of PUF realization using on-chip scan structure.

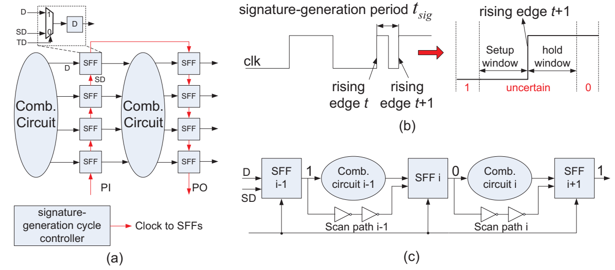

Fig. 2. (a) *ScanPUF* architecture; (b) signature-generation cycle; and (c) illustration of signature generation procedure.

generation in *ScanPUF*. We assume the scan path delays (defined as (1) in section II-B) are 1 ns in the nominal corner. Post manufacturing, the delays deviate (from chip to chip and within a chip) due to process variations. These deviations can be captured in the logic values latched in different SFFs (SFF1, SFF2, SFF3) by the signature-generation cycle controller. Then these values can be shifted out from the scan chain to obtain a signature.

We have evaluated the effectiveness of *ScanPUF* through circuit level simulations with realistic model of parameter variations as well as hardware measurements using Field Programmable Gate Array (FPGA) devices. In the nanometer regime, increasing inter/intra-die variations in device parameters such as V_{th}, L causes large shift in scan path delays. The variations on L and other device parameters can be represented as additional contribution to V_{th} variation [3]. In our simulation, we consider 15% inter- and 10% intra-die standard deviations on V_{th} to analyze the process variations effect on scan path. We observe *scanPUF* achieves high uniqueness (49.88% average inter-die Hamming distance) and reproducibility ($<$ 5% unstable bits below 85 °C). We analyze the Shannon entropy of *ScanPUF* and its robustness under temporal variations due to aging effects such as bias temperature instability (BTI). We observe that aging-induced V_{th} increase of 17 mV in PMOS with ten-year usage results in only 4% flipped bits. Finally, we compare the hardware overhead of *ScanPUF* with a RO-PUF, a common PUF structure. Since *ScanPUF* is realized with already available resources in a chip, it incurs much smaller area overhead than other PUFs (only 2.28% area of the RO-PUF).

The remainder of the paper is organized as follows: Section II presents the proposed PUF implementation. Simulation results on uniqueness, robustness and aging effect, as well as experimental evaluation on FPGA are presented in Section III. Section IV discusses some important issues. Conclusions are drawn in Section V.

II. Scan Chain Based PUF (*ScanPUF*)

A. ScanPUF *Architecture*

Fig. 2(a) shows the architecture of proposed *ScanPUF* realized in the scan chain. Scan chain is a standard DFT component introduced in a design for improving controllability and observability of internal circuit nodes. The SFF is realized by adding a two-input multiplexor to D flip-flop (DFF), and an SFF output is directly connected to the scan-in port (SD) of the next SFF. When 'TD' is zero, the scan chain works in the test mode that all the SFFs form a shift register. Hence, the test vector can be shifted into SFFs serially from primary inputs (PIs) to detect functional or timing faults during manufacturing test. In the test mode, the signature-generation cycle controller in a chip produces one cycle with period t_{sig} as shown in Fig. 2(b) to obtain the signature. Note some buffers may be inserted into the scan paths for two reasons. First, the delay of scan path need be augmented so that the corresponding t_{sig} is longer than the minimum pulse duration of passing through the clock tree. Second, the scan path delay and t_{sig} need certain characteristics under process variations for the signature uniqueness and robustness.

B. *Signature Generation Procedure*

Fig.2(c) explains the signature generation procedure of *ScanPUF*. The SFFs, $i-1$, i, $i+1$ are pre-loaded with an initial sequence of alternating '1's and '0's (i.e. '101' in this case). As 'TD' is set as zero, the input of SFF i is '1'. The output of SFF i becomes '1' after the CK-to-Q delay $t_{clk2q,i}$, after the rising edge t of system clock. Then it propagates through the scan path i, comprised of buffers and a 2:1 multiplexor, and reaches the input port of DFF in SFF $i+1$ with the latency $t_{com,i}$. The rising edge $t+1$ (interval t_{sig} after the rising edge t) latches the input value of SFF $i+1$, which may include three choices as shown in Fig. 2(b). SFF $i+1$ outputs '1', if 0→1 transition arrives before the setup window of width $t_{setup,i+1}$; or uncertain as a result of within the setup and hold window; otherwise '0'. For simplicity, we can consider the output as '0' for the latter two cases, since both of them correspond to the failure of capturing the new value '1'. If ignoring clock tree skewing on scan chain (deskew as [13]), the output value O_{i+1} of SFF $i+1$ after the rising edge t is

$$O_{i+1} = \begin{cases} 1 \;\; if \;\; t_{sig} > t_{clk2q,i} + t_{com,i} + t_{setup,i+1}, i = 0, 1... \\ 0 \;\; otherwise \end{cases} \tag{1}$$

(1) is the case for $0 \rightarrow 1$ transition to be captured by SFFs. Also, we can derive the case for $1 \rightarrow 0$ transition by simply swapping zero and one in (1). Here, $t_{clk2q,i}+t_{com,i}+t_{setup,i+1}$ is called the delay of scan path i.

In the CMOS processes, both inter-die and intra-die variations affect V_{th} [3]. The inter-die V_{th} variation is shard by the transistors on the same die and varies from die to die. Additionally, the V_{th} of each transistor also randomly shifts due to the intra-die variations. After manufacturing, the scan

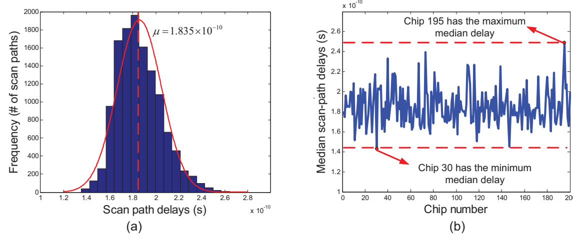

Fig. 3. (a) Scan path delays of 200 chips; and (b) median delay of scan paths for each chip.

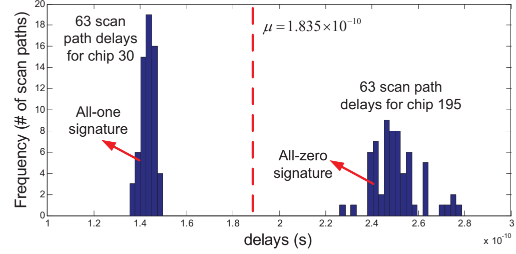

Fig. 4. Scan path delays for the chip 30 and 195.

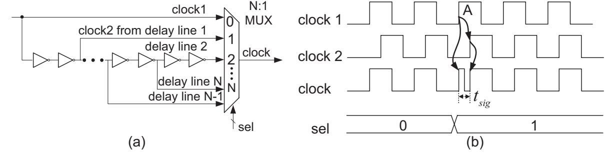

Fig. 5. (a) Signature-generation cycle controller; and (b) signal waveform.

path delays shift from the nominal corner to produce random SFF outputs as signature under application of proper t_{sig}. In summary, the major steps are as follows:

1) Choose the SFFs in a design to generate the signature. Here, the scan paths with better stability on supply voltage, temperature and aging effect described in Section III are preferred.
2) In the test mode, scan sequence of alternating '0' and '1' from PIs into the SFFs as input challenge, which ensures the SFFs store stable values initially. Moreover, $0 \rightarrow 1$ or $1 \rightarrow 0$ transition can happen on the input port of SFFs after the rising edge t of system clock.
3) Produce the rising edge $t+1$ of system clock after t_{sig}.
4) Finally, shift out the response bits (signature) stored in the SFFs through primary outputs (POs).

C. Scan Path Delay Distribution

Four inverters are cascaded on each scan path as buffers, for example, to analyze the delay distribution of a scan chain under process variations. We model both inter-die and intra-die variations using Gaussian distribution on V_{th}. For Predictive Technology Model (PTM) 45nm CMOS process [14], the Monte-Carlo simulation in Hspice with 15% inter-die and 10% intra-die standard deviations is carried out on 200 dies. Each die has 63 scan paths of equally nominal delay. From Fig. 3(a), the scan path delay for $0 \rightarrow 1$ transition approximately follows the Gaussian distribution with median delay $\mu = 1.835 \times 10^{-10}$ seconds on the nominal corner. Institutively, the fixed $t_{sig} = \mu$ can generate the signatures far from each other, since the probability of zero or one on each bit position is 0.5. Fig. 3(b) exhibits the large fluctuation of the median delay around μ for each chip, because of the different inter-die V_{th} deviations. Specifically, the scan path delays of chip 195 and 30 in Fig. 4 imply all-zero and all-one signatures when $t_{sig} = \mu$, which is the case for more than 100 chips. It is not desired, since each chip requires the unique signature for authentication or secret key. As a result, the signature-generation cycle can be inserted by a controller within die to make t_{sig} track the scan path delays for much smaller all-zero or all-one probability of signature, since the gates on it have the same amount of inter-die V_{th} shift.

D. Signature-generation cycle controller

In Fig. 5(a), a signature-generation cycle controller includes multiple clock delay lines (cascaded inverters). Each clock delay line inserts one signature-generation cycle of period t_{sig} (median value $\bar{t}_{sig}$) into the system clock 'clock1'. For example, 'clock2' is a delayed version of 'clock1' by the interval t_c (median value $\bar{t}_c$) on delay line 1. The multiplexor selects 'clock1', 'clock2' or others, as 'clock' to trigger SFFs. In Fig. 5(b), the signature generation starts at the rising edge A of 'clock1'. Since synchronized with 'clock', 'sel' becomes '1' after the rising edge A to pass the delayed edge A in 'clock2'. 'clock' may produce the two adjacent rising edges with interval t_{sig}, if the delay of signal transition at the multiplexor output is smaller than t_c satisfying the minimum pulse width requirement of passing through clock tree. Hence, several buffers may be cascaded on scan path to match $\bar{t}_c$. From the Hspice simulation, it can be observed $t_c \approx t_{sig}$. t_{sig} and the scan path delays in each chip should have nearly the same shift caused by the inter-die V_{th} variation. Fig. 6 shows a specific case for the gates on clock delay line and scan paths with L =135 nm and L =90 nm respectively. Hence, the probability of all-zero (or all-one) signature may be rather small.

In addition to tracking the inter-die V_{th} variation, the intra-die V_{th} variation also deviates t_{sig} from the expected value and therefore changes the probability of zero (or one) in signature. Hence, such deviation should be controlled as small as possible. Usually, the standard deviation $\sigma_{th,intra}$ of intra-die V_{th} for a gate with L and W is modeled as [3]

$$\sigma_{th,intra} = \sigma_{th0,intra}\sqrt{\frac{W_{min}L_{min}}{WL}} \qquad (2)$$

Where $\sigma_{th0,intra}$ is the standard deviation of intra-die V_{th} for the gate of minimum width W_{min} and length L_{min} in a specific CMOS process. As a result, we choose the gates of larger length and width on the clock delay line than those on the scan paths to limit the fluctuation of t_{sig} caused by intra-die V_{th} variation, while tracking the delay shift of inter-die V_{th} variation similar to Fig. 6.

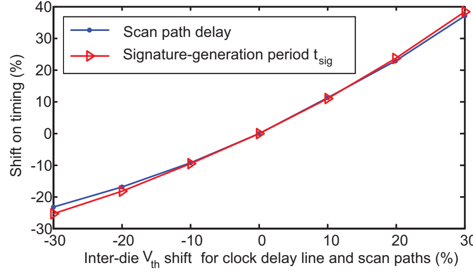

Fig. 6. Shift of scan path delay and t_{sig} under inter-die V_{th} shift.

E. Shannon Entropy Estimation

The first part of *ScanPUF* challenge is the pre-stored values in the SFFs, as it decides on which paths $0 \rightarrow 1$, $1 \rightarrow 0$ or no transition is propagated. The same scan path may show different delays for $0 \rightarrow 1$ and $1 \rightarrow 0$ transitions. Second, signatures also change with different $\bar{t}_{sig}$, since SFF outputs rely on the comparison between scan path delays and t_{sig}. To evaluate randomness, the Shannon entropy is estimated for different $\bar{t}_{sig}$ with 0→1 transition (similar for 1→0 transition).

Assume $x_{j,k}$ denotes the output of SFF k for chips when $\bar{t}_{sig} = t_j$ and d_k is the delay of scan path k for $0 \rightarrow 1$ transition, $j = 1, 2, ...$ From (1), $P(x_{j,k} = 1) = P(d_k < t_{sig}|\bar{t}_{sig} = t_j) = p_{j,k}$ and $P(x_{j,k} = 0) = 1 - p_{j,k}$. Considering statistical independence of $x_{j,k}$, $k = 1, 2, ...$, it is simplified as x_j with probability p_j and the entropy

$$H(x_j) = -p_j log_2 p_j - (1 - p_j) log_2(1 - p_j) \tag{3}$$

$H(x_j)$ is maximized when $p_j = 0.5$. Considering m signature-generation periods (t_0, t_1,...t_m), the entropy of each SFF is $H(x_1, x_2, ..., x_m) = \sum_{i=1}^{m} H(x_i|x_1, x_2, ..., x_{i-1})$. With generality, assume $t_1 = \mu$ for $p_1 = 0.5$. Since $t_j \neq t_1$, $j \geq 1$, it can be derived $H(x_j) < H(x_1)$. As $H(x_j) \leq H(x_j|x_1, x_2, ..., x_{j-1})$, $H(x_1, x_2, ..., x_j) \leq \sum_{j=1}^{m} H(x_j) < m$ is hold. The inter- and intra-die V_{th} variations impact the entropy, because both of them alter p_j associated with $\bar{t}_{sig}$. $H(x_j)$ is maximized only when completely tracking the shift on scan path delays caused by inter-die V_{th} variation and minimizing the deviation from intra-die V_{th} variation.

III. Simulation Results and Analysis

The *ScanPUF* of 128-bit signature is evaluated on uniqueness and stability for $m = 1000$ chips by the Monte-Carlo simulation in Hspice using PTM 45nm CMOS Process, with V_{th} variation of standard deviation $\sigma_{th,inter} = 15\%$ and $\sigma_{th0,intra} = 10\%$. All scan paths have the nominal delay μ. $\bar{t}_{sig} = \mu$, $\bar{t}_{sig} < \mu$ and $\bar{t}_{sig} > \mu$ are considered, since the entropy grows with the number of $\bar{t}_{sig}$. A clock delay line includes four inverters (L_{NMOS}=L_{PMOS}=135 nm, W_{NMOS}=500 nm, W_{PMOS}=700 nm); four inverters (L_{NMOS}=L_{PMOS}=90 nm, W_{NMOS}=100 nm, W_{PMOS}=140 nm) are cascaded on scan path. To further reduce the negative influence of intra- and inter-die V_{th} variation on entropy, eight clock delay lines are employed (each for a 16-bit signature).

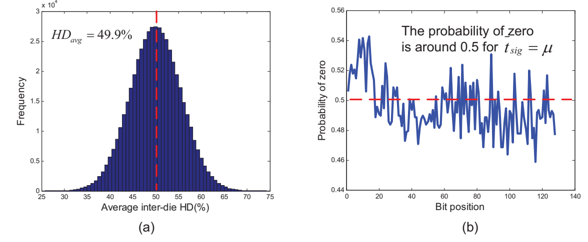

Fig. 7. Under $t_{sig} = \mu$ (a) inter-die HD distribution of 1000 chips; and (b) probability of zero for each bit.

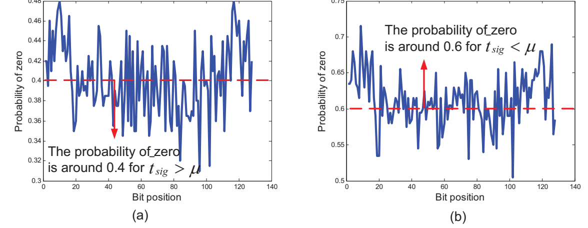

Fig. 8. Probability of zero for (a) $\bar{t}_{sig} < \mu$; and (b) $\bar{t}_{sig} > \mu$.

A. Uniqueness Analysis

For authentication, the signatures need be far away from each other. We introduce the Hamming distance (HD) to evaluate the signature distance quantitatively. The simulation results are plotted in Fig. 7 for $\bar{t}_{sig} = \mu$ and $0 \rightarrow 1$ transition on the scan paths. Fig. 7(a) shows around 50% (64 bits) inter-die HD, which means approximate one-bit entropy for each scan path. The probability of zero for each bit in Fig. 7(b) is around 0.5. Such probabilities are skewed from 0.5 to 0.4 and 0.6 respectively for $\bar{t}_{sig} > \mu$ and $\bar{t}_{sig} < \mu$ as Fig. 8. Assuming $HD_{i,j}$ is the HD between chip i and chip j, the average HD for m chips, denoted by HD_{avg}, is calculated as [12]

$$HD_{avg} = \frac{2}{m \cdot (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} HD_{i,j} \tag{4}$$

When $\bar{t}_{sig} = \mu$, HD_{avg} is 49.9% near the theoretical value 50% ($128 \times 0.5 = 64$ bits). For $\bar{t}_{sig} < \mu$ and $\bar{t}_{sig} > \mu$, their HD_{avg} are reduced to 47.44% and 48.0% respectively.

B. Robustness Analysis

The robustness measures the signature reproducibility under non-ideal environment such as high temperature and supply voltage variation. The unstable or flipped bits need be as few as possible required in security applications. In Fig. 9(a), the percentage of unstable bits is nearly 18% when supply voltage becomes 0.8 Volt from the nominal 1 Volt, which is reduced to 9% when the supply is 0.9 Volt. Fig. 9(b) shows the percentage of unstable bits with the temperature increased from 25 °C to 85 °C at the interval of 15 °C. When the temperature is no more than 85 °C, the unstable bits are nearly 5% on average. In particular, 92.1% chips have no more than 10 flipped bits.

According to (1), SFF k in certain chip outputs zero when the distance $dis_k(V_1, temp_1)$ between t_{sig} and path delay is less than zero under supply voltage V_1 and temperature $temp_1$. When they shift to V_2 and $temp_2$, if $dis_k(V_2, temp_2) < 0$ still holds, SFF k produces a stable bit; otherwise unstable.

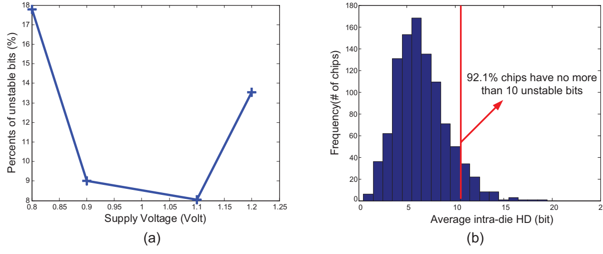

Fig. 9. Average intra-die HD from 1000 chips for *ScanPUF*s: (a) for supply voltage variation (nominal Vdd=1V); and (b) for temperature variation.

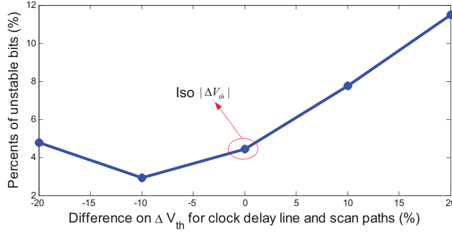

Fig. 10. Percents of unstable bits under varying NBTI effects in clock delay line and scan paths.

Hence, it can be derived that the larger $|dis_k(V_1, temp_1)|$ may yield better stability under temperature and supply voltage fluctuation. To tolerate the unstable bits (only a small fraction in our simulations), the simplest method is to discard them. Moreover, post-processing procedures such as fuzzy extractor can reconciliate them and improve the stability [17].

C. Aging Effect

For nano-scale CMOS process, the aging effect is no longer ignored during the early stage of design cycle. Negative bias temperature instability (NBTI) occurs on the stressed PMOS gates due to the generated traps at Si/SiO_2 interface by the increased electric field across the thin oxide. As the gate oxide thickness reaches 4 nm, the V_{th} degradation of PMOS has played the major role in temporal performance degradation of circuits, instead of hot-carrier injection (HCI) of NMOS transistors [15]. Under PTM 90nm CMOS process, the PMOS ΔV_{th} may achieve 17.3mV after ten years [16], which is ample for 45nm CMOS process, given the reduced electric field across gate oxide [15].

Considering the possibly non-identical aging effects between clock delay line and scan paths, their different percents (from -20% to 20%) on ΔV_{th} are accounted to simulate the results in Fig. 10. If PMOS $|\Delta V_{th}|$ is 17.3mV for both scan paths and clock delay line, nearly 4% bits become unstable after ten-year usage. When $|\Delta V_{th}|$ on clock delay line achieves 0.0204 Volt (+20% larger than that of scan paths), the percentage of unstable bits is 11% that drops to less than 5% for -20%. Hence, the different NBTI effects on the clock delay line and scan paths impact the unstable bits proportion during aging. The tolerance of unstable bits is addressed from two perspectives. First, make the number as small as possible. As a result, some modifications need be introduced on the circuit level to adjust aging for ΔV_{th} between -10% and 0%. Secondly, we can specify the proportion of unstable bits caused by NBTI in the design cycle and choose more powerful error-correcting codes to tolerate them in the fuzzy extractor.

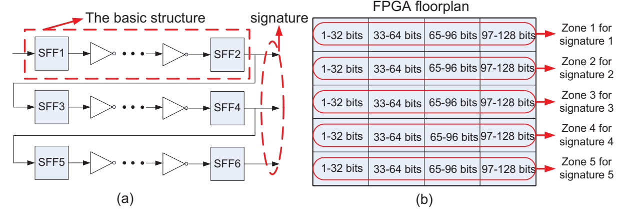

Fig. 11. (a) Mapping of scan chain into FPGA; and (b) floorplan showing mapping of signature bits.

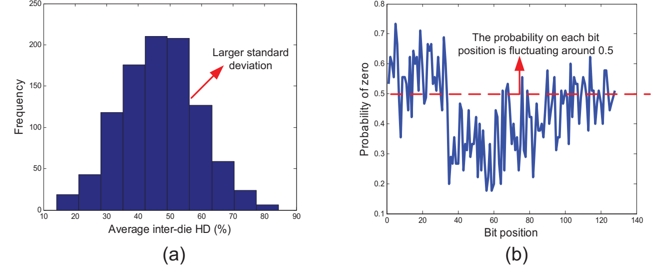

Fig. 12. Experimental results in FPGA: (a) average inter-die HD for 45 *ScanPUF*s; and (b) probability of zero for each bit.

D. Experimental Validation on FPGA

ScanPUF is evaluated on FPGA for $\bar{t}_{sig} = \mu$. A logic array block (LAB) of Altera's Cyclone III contains 16 four-input logic elements (LEs) and 16 registers. In the experiment, each basic unit in Fig. 11(a) is mapped into a single LE for one-bit signature with the post-fitting scan path delay (5.42±0.02ns) after compilation. In addition, the number of inverters on the clock delay line is adjusted for an approximate $\bar{t}_{sig}$. An FPGA is splitted into five non-overlapped zones from the top to the bottom as Fig. 11(b). A zone is horizontally partitioned into four parts. Each part includes 32 basic units and one clock delay line to produce a 32-bit signature. Totally, 45 128-bit signatures are obtained from nine FPGAs. Signature uniqueness can be improved by: (1) the approximate shift on t_{sig} and scan path delays for the same inter-die variation, (2) up-sizing the gates on the clock delay line to reduce intra-die variation influence. The two conditions are uncontrollable in FPGA, because of the impossibility to modify the basic unit (e.g. LE). Hence, the inter-die HD distribution in Fig.12(a) is expected with a larger standard deviation than Fig.7(a). The zero probability on each bit is shown in Fig.12(b) and HD_{avg} is 47.14%. For reproducibility, the signature includes 3.17% flipped bits on average at room temperature.

IV. Discussions

Because of the unbalanced wire lengths, fan-out loads and residual clock skewing, the nominal delays of different scan paths may not be identical in real IC designs. In such scenario, we can select a set of scan paths with near-identical nominal delays during post-layout timing analysis and design the clock delay line according to this nominal delay. This approach can be extended to create multiple such sets of scan paths and corresponding clock delay line, which can provide, in

aggregate, a signature of desired length. Since such grouping reduces the impact of intra-die V_{th} variations on clock delay line, uniqueness of signature improves (Section III).

A. Area Overhead

An important advantage of *ScanPUF* is the use of existing scan chain resources in a chip. In the simulation, a signature-generation cycle controller with eight clock delay lines (4 inverters each) is employed for 128-bit signature. An RO-PUF of 128-bit signature includes 35 RO rings (five inverters and AND gate for each), if all ordering of ROs are possible. It also requires additional 35 2:1 MUXs, two 32-bit counters and one 32-bit comparator. The areas of RO-PUF (from Design Compiler) and *ScanPUF* ($\bar{t}_{sig} = \mu$, stick-diagram layout) for PTM 45nm CMOS process are listed in Table I. Since buffers are likely to be inserted into the scan path during scan synthesis for avoiding the hold violation, ideally the signature-generation cycle controller can be the only it only rises to 303.96/2721.4=11.17%.

TABLE I
AREA COMPARISON BETWEEN RO-PUF AND *ScanPUF*

	RO-PUF	*ScanPUF*	
		w/ INVs	w/o INVs
Area(μm^2)	2721.40	303.96	62.04

B. Influence on Power

The scan paths for signature generation can be modified by inserting extra inverters/buffers that influence power dissipation in the normal functional mode and test mode. In the functional mode, the modified scan path can be power-gated to stop the signal propagation and therefore incurs virtually no extra power. During the manufacturing test, the extra power cannot be avoided, since the test vectors and responses are shifted on the scan paths. We observe, through Hspice simulation, that compared to the scan path comprised of only wires (i.e. no buffers), the average power is increased by 9.65% with four inverters inserted. However, the total test power is primarily contributed by the combinational circuit, which takes 78% of test power) [18]. In addition, the extra inverters are selectively inserted into a small fraction of scan paths. For example, the scan chain of 64-bit Alpha processor includes 2408 SFFs and 128/2407=5.32% scan paths need to be modified for one 128-bit signature [19]. Due to extra inverters in scan paths, the test power increases only by 5.32%×22%×9.65%=0.11%.

V. CONCLUSION

We have presented *ScanPUF*, a novel PUF implementation using a prevalent on-chip structure, scan chain. *ScanPUF* uses random delay variations in the scan paths to generate unclonable signatures. We show that use of existing resources in a chip to realize PUF can drastically reduce the hardware overhead and design effort compared to alternative PUFs. The low hardware overhead makes it attractive for many resource-constrained embedded applications. It, however, causes modest increase in scan shift power during test. We show that the impact on total test power can be minimal since test power is dominated by redundant switching in combinational logic and only a small fraction of scan paths need be modified. The area and test power overhead can be further reduced by accounting for the buffers in scan path, which are often inserted in a design to address the hold violation. Through extensive circuit-level simulations and hardware measurements using FPGA devices, we show that *ScanPUF* can achieve high uniqueness of signatures. Furthermore, since the challenge vectors in *ScanPUF* are comprised of initial patterns in the scan chain, selection of scan flip-flops and signature-generation periods, it is capable of producing vast set of signatures. We also show that it achieves high robustness under temporal variations in device parameters due to device aging effects and temperature/voltage fluctuations.

ACKNOWLEDGMENTS

This work is supported in part by fund provided by National Science Foundation (NSF) grant # CNS-1054744.

REFERENCES

[1] J. R. Anderson and G. M. Kuhn, “Low cost attacks on tamper resistant devices,” *IWSP*, 1997, pp. 125-136.
[2] R. Pappu, “Physical one-way functions,” PhD thesis, Massachusetts Institute of Technology, 2001.
[3] S. Mukhopadhyay, H. Mahmoodi and K. Roy, “Modeling of failure probability and satistical design of SRAM array for yield enhancement in nanoscale CMOS,” *IEEE Trans. Computer-Aided Design Integr. Circuit Syst.*, vol. 24, no. 12, pp. 1859-1880, 2005.
[4] P. Tuyls, G. Schrijen and B. Skoric, “Read-proof hardware from protective coatings,” *CHES*, 2006, pp. 369-381.
[5] D. Lim, J-W. Lee, B. Gassend, M. Van Dijk, E. Suh and S. Devadas, “Extracting secret keys from integrated circuits,” *IEEE Trans. VLSI Syst.*, vol. 13, no. 10, pp. 1200-1205, 2005.
[6] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” *DAC*, 2007, pp. 9-14.
[7] S. Kumar, J. Guajardo, R. Maes, G.J. Schrijen and P. Tuyls, “The butterfly PUF: protecting IP on every FPGA,” *HOST*, 2003, pp. 2809-2825.
[8] X. Wang and M. Tehranipoor “Novel physical unclonable function with process and environmental variations,” *DATE*, 2009, pp. 1344-1348.
[9] Y. Su, J. Holleman and B. Otis, “A 1.6J/bit 96% stable chip ID generating circuit using process variation,” *ISSCC*, 2007, pp. 406-611.
[10] A. R. Krishna, S. Narasimhan, X. Wang and S. Bhunia, “MECCA: a robust low-overhead PUF using embedded memory array,” *CHES*, 2011, pp. 407-420.
[11] R. Maes, P. Tuyls and I. Verbauwhede, “Instrinsic PUFs from flip-flops on reconfigurable devices,” *WISSec*, 2008.
[12] A. Maiti, J. Casarona, L. Mchale and P. Schaumont, “A large scale characterization of RO-PUF,” *HOST*, 2010, pp. 94-99.
[13] C. E. Dike, N. A. Kurd, P. Patra and J. Barkatullah, “A design for digital, dynamic clock deskew,” *IEEE Symp. on VLSI Circuits*, 2003, pp. 21-24.
[14] Predictive Technology Model, http://www.eas.asu.edu/ ptm/
[15] S. Bhardwaj, W. Wang, R. Vattikonda and Y. Cao, “Modeling and minimization of PMOS NBTI effect for robust nanometer design,” *DAC*, 2006, pp. 1047-1052.
[16] L. Hong, W. Yu, K. He, R. Long, H. Yang and Y. Xie, “Modeling of PMOS NBTI effect considering temperature variation,” *ISQED*, 2007, pp. 139-144.
[17] Y. Dodis, L. Reyzin and A. Smith, “Fuzzy extractors: how to generate strong keys from biometrics and other noisy data,” *EUROCRYPT*, 2004, pp. 523-540.
[18] S. Gerstendrfer and H. J. Wunderlich, “Minimized power consumption for scan-based BIST,” *ITS*, 1999, pp. 77-84.
[19] D. Ernst, *et al*, “Razor: a low-power pipeline based on circuit-level timing speculation,” *MICRO*, 2004, pp. 523-540.