Novel Physical Unclonable Function with Process and Environmental Variations

Xiaoxiao Wang and Mohammad Tehranipoor
ECE Dept, University of Connecticut, {xwang,tehrani}@engr.uconn.edu

Abstract— **Physical Unclonable Functions (PUFs) are employed to generate unique signature to be used for integrated circuit (IC) identification and authentication. Existing PUFs exploit only process variations for generating unique signature. Due to the spatial correlation between process parameters, such PUFs will be vulnerable to be modeled or leak information under side-channel attacks. The PUF we present in this paper, called PE-PUF, takes into account both process and environmental variations which magnifies chip-to-chip signature randomness and uniqueness. PE-PUF takes into account process variations, temperature, power supply noise and crosstalk; all these effects are major sources of variations and noise in integrated circuits. Designers would be able to select PE-PUF response by applying different input patterns.? Furthermore, PE-PUF imposes no routing constraints to the design. The gates in PE-PUF are distributed across the entire chip and cannot be easily identified/modeled or leak side-channel information. Simulation results demonstrate that each IC can be uniquely characterized by PE-PUF with higher secrecy rate when compared to other PUFs that use only process variations.**

Keywords: PUF, IC Authentication, Process Variations, Environmental Variations, Hardware Security

I. Introduction

Due to the current trend in globalization, intellectual property (IP) vendors and system integrators have to deal with IC/IP counterfeiting more than ever. Many methods have already been proposed for identification and authentication of ICs [1] [2] [3]. A unique identifier in an IC can be embedded to give the IC a unique identity. Such approach can identify the IC, but may not necessarily authenticate it. A secret key must be embedded into each IC to enable authentication. Recently a major growth in the type and strength of attacks on secured devices has been observed [4] [5] [6]. Some attacks may be invasive, e.g., removal of the package and layers of the IC. However, some other attacks are non-invasive; they circumvent the data channel and instead exploit the so called side-channels. The side-channel signal analysis is proven to be effective in extracting secret keys from secure devices with much less effort and time compared to brute force attacks.

One potential solution to the above attacks is to extract the secret key from the IC itself. For the IC to work properly, this key needs to remain secret. That is, the packaged IC has to be made resistant to many different attacks that attempt to discover the key. However, making an IC tamper-resistant to all forms of attacks is a challenging problem.

Physical unclonable functions (PUFs) are receiving much attention from hardware security and cryptography community as a new approach for IC identification, authentication and key generation [1] [3] [9] [14] [22]. Silicon PUFs exploit inherent physical variations that exist in integrated circuits. PUF's inherent uncontrollable and unpredictable features make it suitable for IC identification and authentication [8]. As the variations for each IC are unique, a distinct PUF signature can be obtained for each IC. The signature can be identified by designers as a sign of genuine IC and is used to enable it. Thus, pirated ICs cannot be enabled and will become useless.

Traditionally, some secret keys are placed in non-volatile memories. However, non-volatile memories need tamper-sensing circuits or advanced manufacturing materials which require large cost overhead and power consumption. Furthermore, since key is still stored in digital format, it cannot avoid invasive attack [7]. Differently, PUFs are actually sensors which can sense the unpredictable random analog variations in an IC and convert them into secret digital keys therefore, the secrecy of key is significantly improved.

A. Prior Related Works

As mentioned above, a PUF is designed in a way to be able to sense on-chip variations and translate them into digital signatures. Generally, there are three types of PUF architectures namely cover-based PUF, memory-based PUF, and delay-based PUF. Cover-based PUF can be further divided into the categories of optical PUF and electric PUF. Optical PUF [9] is a layer of special material which has randomly distributed light scattering coefficients. If illuminated by a laser beam, random interference patterns can be obtained as response signature. However, optical PUF needs special optical material covered by additional manufacturing process, and IC authentication requires equipments such as accurate laser instruments and camera which make the application of optical PUF limited in practice. Electric PUF is implemented by protective coating. The coating layer has randomly distributed dielectric coefficients [10]. A constantly powered sensor array distributed across the whole layer is used to measure coating unit capacitance variation where generates PUF signature. The fabrication cost, sensor array power consumption, and area overhead of this PUF can be quite significant.

Memory-based PUFs exploit the vulnerable balance of SRAM cross-coupled transistors to intrinsic process variations. Uncontrollable random SRAM contents can be generated during power-up. The random contents are then used as PUF signature [11] [12] [13] [14]. The drawback of memory-based PUF is that every memory element generates a fixed one-bit signature. Hence the signature for a specific chip is fixed and non-reconfigurable, as there is no challenge mechanism involved. Furthermore, the signature in SRAM memory still has a probability of being invasively accessed.

Delay-based PUFs convert on-chip variations into random delay and use arbiter [1] [2] [15] [16] or ring oscillator [3]

* This work is supported in part by NSF grant No. CNS-0844995 and 0716535.

978-3-9810801-6-2/DATE10 © 2010 EDAA

[17] to translate random delay into PUF signature. Delay-based PUFs have the feature of being low cost (i.e., low area overhead) since most of them are composed of synthesizable digital gates and use digital signals as PUF response. However, existing delay-based PUFs exploit only IC's process variations for signature generation. Recently a new PUF was introduced in [14], called the Butterfly PUF. It is based on cross-coupling of two latches or flip-flops. The mechanism for this PUF is similar to the memory-based PUF [11] but has the advantage that it can be implemented on any SRAM FPGA.

B. Contributions and Paper Organization

Existing delay-based PUFs exploit only process variations for generating unique signatures. Due to the spatial correlation between process parameters such PUFs will be (i) vulnerable to be modeled, (ii) leak information under side-channel attacks, and (iii) provide low signature uniqueness. The PUF we present in this paper, called PE-PUF, takes into account both process and environmental variations which significantly magnifies chip-to-chip signature randomness and uniqueness. PE-PUF takes into account process variations, temperature, power supply noise and crosstalk; all these effects are major sources of variations and noise in modern integrated circuits. These noises are induced by circuit activity which is generated from applying input patterns (here, also called challenge). Designers would be able to select PE-PUF response by applying different input patterns to the IC. The gates in PE-PUF are distributed across the entire chip and cannot be easily identified/modeled or leak side-channel information. Our simulation results demonstrate that each IC can be uniquely characterized by PE-PUF with higher secrecy rate when compared to traditional ring-oscillator based PUFs that use only process variations.

The paper is organized as following. Section II decribes environmental variations' contribution to a PUF signature randomness and uniqueness. Section III presents the architecture for PE-PUF. Section IV displays experimental results to demonstrate the performance improvements of PE-PUF compared to traditional ring-oscillator PUF. Finally, concluding remarks are in Section V.

II. Environmental Variations Impact on Ring-Oscillator PUF

A. Randomness in Oscillation Frequency

A simple ring-oscillator PUF contains an odd numbers of inverters. Its oscillation frequency is determined by the sum of inverters delay. It is possible to trace the effect of process/environmental variations effect on inverter delay (t_{inv}) using first-order CMOS inverter delay equation [18] as,

$$t_{inv} = \frac{0.52 C_L V_{DD}}{\frac{W}{L_{eff}} \frac{\mu \varepsilon_{ox}}{t_{ox}} V_{DSAT}(V_{DD} - V_T - V_{DSAT}/2)} \quad (1)$$

where C_L is inverter's load capacitance, V_{DD} is supply voltage, W is gate width, L_{eff} is effective channel length, μ is the mobility of carriers, $\varepsilon_{ox} = 3.97 \times \varepsilon_0 = 3.5e-11F/m$, t_{ox} is oxide thickness, V_{DSAT} is the saturation source-drain voltage and V_T is threshold voltage. It is well known that process variations make transistor parameters C_L, W, L_{eff}, V_{DSAT}, and t_{ox} differ randomly on a manufactured IC. In addition, parameters such as V_{DD}, V_{DSAT} and V_T are susceptible to environmental variations, including temperature, supply voltage and crosstalk. Hence, inverter delay t_{inv} would be a random value due to within-die and die-to-die process and environmental variations.

The oscillation frequency f_{os} of a ring oscillator with N_{inv} inverters can vary as well due to the variations as shown in Equation 2.

$$f_{os} = \frac{1}{2 N_{inv} t_{inv}} \quad (2)$$

Therefore, individual inverter delay variations are accumulated and displayed in oscillation frequency fluctuation.

B. Analyzing the Impact of Environmental Variations on Oscillation Frequency

In modern designs, supply voltage, temperature and crosstalk variations contribute the most to on-chip environmental variations. These effects are input-pattern dependent; they differ from one pattern to another. Also, they are sequence dependent, i.e., the following patterns impact will depend on the previous pattern that was applied to the IC. The three major effects are briefly described below.

1. **Power Supply Noise**: When an input pattern is applied to a circuit, it will create a large number of switchings in the circuit. The switching will increase dynamic power and cause voltage drop on power lines and voltage increase on ground lines [24]. This effect is known as power supply noise. When the voltage reaching a gate changes, it will change the delay characteristics of the gate.
2. **Temperature**: Increase in power also increases the temperature over time depending on the type and number of patterns applied to the circuit. Temperature distribution depends on the location of switchings and distribution of power consumption in the circuit.
3. **Crosstalk**: As technology feature size scales, interconnect spacing and width are also being reduced. However, in order to keep the resistance low, the thickness of the wires is not scaled at the same rate. This produces tall sidewalls between long parallel interconnects separated by very little space, which creates a parasitic coupling capacitance between wires. Due to this fact, crosstalk has become a significant contributor to signal integrity problems in modern designs [25].

To verify environmental variations' effect on oscillator, we design a 7-inverter ring oscillator with two interconnects nearby (A1 and A2) in $90nm$ technology node [19] and simulated it by Hspice [20]. The circuit is shown in Figure 1. In Figure 2, the supply voltage of the 7 inverters on the ring oscillator are swept from 1.12V to 1.2V with 0.01V sweep range. Figure 3 shows oscillation variation when temperature changes from -35^oC to 75^oC in 5^oC step. Finally, Figure 4 displays the oscillation rising edge variation at observation point P in Figure 1 from $11.1ns$ to $11.3ns$ with interconnect

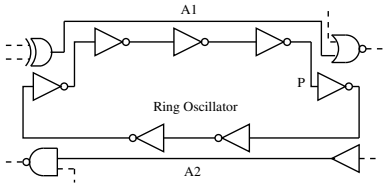


Fig. 1. A ring oscillator in a circuit with a couple of nearby interconnects.

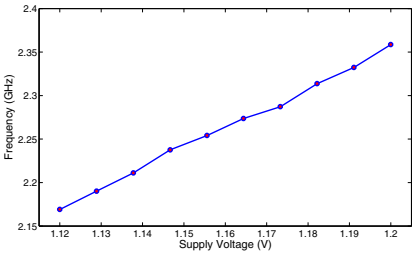


Fig. 2. The impact of supply volgate on oscillation frequency.

$A1$ rise arrival time varying in $0.2ns$ range. In this simulation $A2$ is kept quiescent. The bold line in the figure represents crosstalk-free oscillation waveform, while other lines represent crosstalk affected waveforms.

From Figures 2, 3 and 4, it can be seen that oscillation frequency changes significantly with change in temperature, supply volgate, and crosstalk. It can also be impacted "directly" by crosstalk effects between the switching on nearby nets or "indirectly" when crosstalk changes the arrival time of transitions in the circuit which impacts the distribution of voltage drop in the circuit. That will, in turn, impacts ring oscillator's frequency.

The final effect to consider in PE-PUF is **process variations**. Since traditional PUFs only take process variations into account, during IC authentication, the entire circuitry is in idle mode while ring oscillator operates. However, when the entire circuit operates at the same time as PUF, as in PE-PUF, the process variations exist in all the components

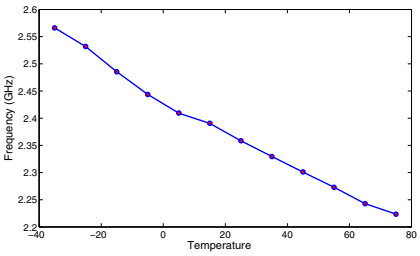


Fig. 3. The impact of temperature on oscillation frequency.

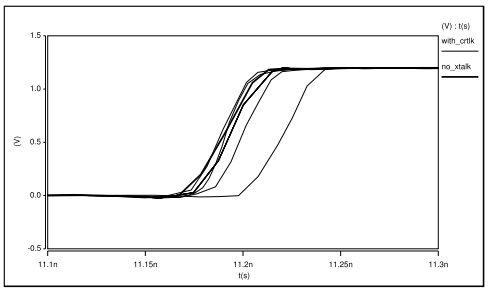


Fig. 4. Crosstalk impact on oscillation waveform.

(gates and interconnects) in the entire circuit would impact the operation of the ring oscillators. This is due to the fact that process variations would impact power supply noise distribution since it will impact the switching arrival times on circuit nets. It will impact the temperature distribution and crosstalk in a similar manner as well. Thus, environmental variations are distinct from chip to chip. With technology shrinking, manufacturing randomness on wire, gate and layer dimensions are less understood and more uncontrollable [21]. The manufacturing randomness results in unpredictable unit resistance, capacitance and inductance, which means even applying same patterns to different chips will induce different temperature, voltage drop and crosstalk.

III. PE-PUF

As mentioned earlier, the main objective in designing our PUF, called PE-PUF, is to take both process variations and environmental variations into consideration to increase randomness and uniqueness. Hence, PE-PUF signature is determined not only by process variations inherent in PUF circuitry but also by input patterns. During authentication process, PE-PUF's responses are collected as input patterns are applied to the IC. Any functional input patterns can be used as challenge to PE-PUF. In modern designs with hundreds of inputs, the challenge-response pair count could be unlimited. IC input patterns are known and chosen only by designers therefore, the adversary will not have access to PUF responses. Also, since sequence of vectors is extremely important in generating switching in the circuit to induce environmental variations, it makes it much more challenging for the adversary to model the PE-PUF and identify the right input patterns. Note that in PE-PUF, the challenges are not applied to the PUF rather they are applied to the circuit.

A. PE-PUF Architecture

When PE-PUF is impacted by the variations, the accumulated delay difference is expressed as oscillation count N_{count} in a time frame T where

$$N_{count} = \frac{T}{2N_{inv}t_{inv}} \tag{3}$$

T represents the number of input patterns applied to the circuit based on designer's chosen application frequency. Suppose process/environmental variations change one inverter's delay by Δt. Its impact on N_{count}, denoted as ΔN_{count}, will be calculated by

$$\Delta N_{count} = \frac{T}{2N_{inv}t_{inv}} - \frac{T}{2(N_{inv}t_{inv} \pm \Delta t)} \approx \pm \frac{T\Delta t}{2N_{inv}^2 t_{inv}^2} \tag{4}$$

From Equation 4, it can be seen that for certain time frame T, a smaller N_{inv} and t_{inv} means a higher sensitivity of N_{count} to delay variation Δt caused by process/environmental variations. In PE-PUF, each ring oscillator is composed of only 3 small inverters and an AND gate to enable/disable the oscillation.

Figure 5 illustrates the architecture of PE-PUF we propose. PE-PUF contains $M+1$ 3-inverter oscillators to generate M-bit signatures. One counter connects to each oscillator. The 3

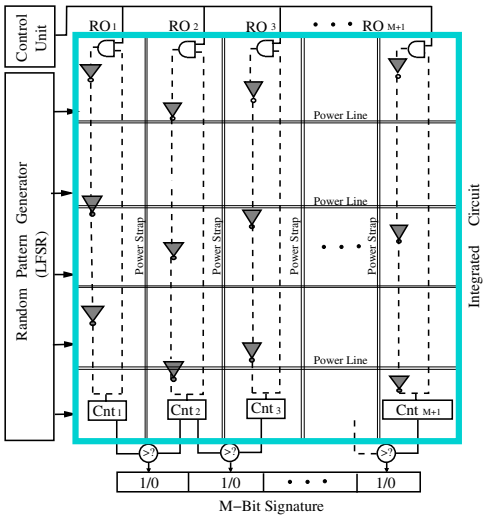


Fig. 5. PE-PUF architecture in an IC.

inverters in an oscillator are distributed across the whole die to make variations between different inverters large. The long interconnect between inverters is a good victim for crosstalk effect and interconnect variations. The linear feedback shift register (LFSR) in production test is reused to apply internal random patterns as challenges. For simplicity, ground lines are not shown in this figure. The small control unit controls the entire identification and authentication procedure. During this procedure, designers can choose random seeds known only to them. LFSR then generates input patterns according to its seeds scanned in and apply them to the circuit to induce noise.

B. PE-PUF Operation Flow

The potential challenge set for a PE-PUF is an unlimited functional pattern set generated by LFSR. The responses are collected by comparing the neighbouring oscillators after a pattern set is applied. A pattern set is defined as N number of patterns that are applied by LFSR; N=4 in this work. Comparing neighbourhing oscillators means comparing the oscillation count between RO_1 and RO_2, RO_2 and RO_3, ..., and RO_M and RO_{M+1}. If the oscillation count for RO_{i-1} is larger than that of RO_i, '1' is generated at the output line; Otherwise, a '0' will be gernerated. In our architecture, a PE-PUF with $M+1$ oscillators can generate an M-bit signature after one pattern set is applied. Finally, after applying K sets of patterns, a signature of length $K \times M$ could be generated for the IC under authentication. The PE-PUF signature generation flow is shown in Figure 6.

C. PE-PUF's Reconfigurability

Since, traditional ring-oscillator based PUFs only sense process variations, its signature is predefined during manufacturing process and cannot be changed by designers, i.e., it is input-pattern independent. However, PE-PUF has the ability of sensing both random environmental and process variations and translating them into one digital signature. The advantage of PE-PUF is that the environmental variations can be changed by the random input pattern sets chosen and applied by designers. Thus, PE-PUF's signatures can be

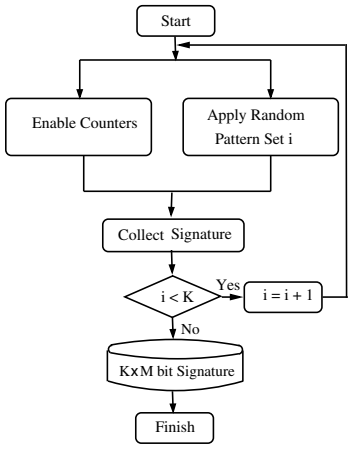


Fig. 6. PE-PUF $K \times M$-bit signature generation flow.

determined by designers. A designer can apply various random patterns generated using different seeds to the IC. Furthermore, the length of signatures can also be changed by applying different number of pattern sets. Such capability makes it extremely difficult for adversaries to obtain PE-PUF signature.

IV. Simulation Results and Analysis

A PE-PUF with M=17 ring oscillators is implemented on ISCAS'89 s9234 benchmark [26] in 90nm technology node. The challenge input patterns are 30-bit random patterns that are applied to 30 primary inputs. The patterns are applied at a frequency of 1GHz; This circuit has very short paths. Four random patterns exist in each *pattern set*, hence each pattern set application takes 4ns (i.e., T=4ns). Choosing 4 random patterns to form a patterns set is to keep counter size small and at the same time make ring oscillators sense enough environmental variations leading to sufficient counter value variations. 17 5-bit counters are enabled when the first pattern in a pattern set is applied and disabled after 4ns when the entire pattern set is applied. After a pattern set is applied, the neighbouring counters' contents are compared and a 16-bit PE-PUF signature is generated. The final signature length is determined by the number of applied pattern sets K, and it would be of length $16 \times K$ bits. The whole circuit behavior including all 17 PE-PUFs are simulated by Synopsys NanoSim tool [20].

A. Attack Analysis

Traditional ring-oscillator PUF's oscillation are usually located in pairs next to each other [17] [23]. If a PUF is used for on-chip key generation, it can be susceptible to power-based side-channel attacks. The oscillation frequency information can be easily accessed using such attacks. The dash line in Figure 7 shows the supply voltage waveform of a power pad near a traditional oscillator PUF. From the power waveform, the oscillation period can easily be analyzed by measuring the distance of valley peaks. Once adversary obtains the oscillation frequencies, obtaining the PUF signature becomes much easier. Two ring oscillators are placed in close proximity of power pad that results in large voltage drop on the power pad as seen in Figure 7.

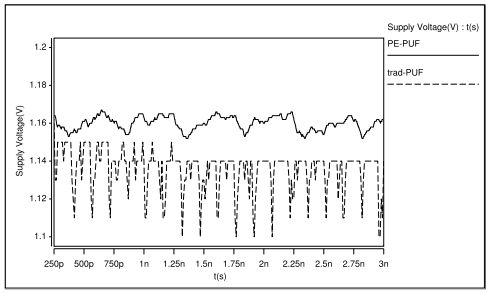


Fig. 7. Power traces of traditional oscillator PUF versus PE-PUF.

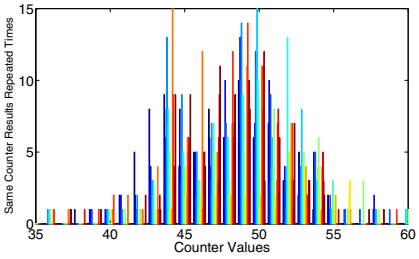


Fig. 8. Counters' values when applying random pattern sets (applying 1500 different random pattern sets to same chip and collect counter results).

PE-PUF has two main advantages in dealing with power side-channel attacks. First, each ring oscillator needs only three inverters and they are separated across the whole die as shown in Figure 5. The solid line in Figure 7 represents the power trace of the same power pad when PE-PUF is employed. Compared with the power trace of traditional oscillator PUF, the oscillation frequency information is completely submerged into the power supply noise. Secondly, the oscillation frequency highly depends on the input patterns which is known only to designer. From Figure 8, it can be seen that the counters' values of ring oscillators vary randomly when applying 1500 different random pattern sets. Hence, even if the adversary can make the oscillators oscillate and find its power pad, the signature generated by PE-PUF will be different when applying designer's pattern sets. Also, note that pattern set applied at different frequencies can result in different environmental variations in the circuit adding another layer of security to PE-PUF.

Figure 9 shows the Hamming distances of 100 16-bit PE-PUF signatures generated after applying 100 random pattern sets. Figure 9 shows that more than 65% of signatures have Hamming distance larger than 0.4 from each other. That is, on average, more than 40% of bits in each two signatures are different. Hence, by changing input pattern sets designers can change PE-PUF response, which represents PE-PUF's reconfigurability.

B. Uniqueness Analysis

Here, the signature uniqueness of traditional PUF which also has 17 ring oscillators using neighbouring counters is compared with the one generated by PE-PUF. For the traditional ring oscillator, since its signature only determined by process variations, its signature length is fixed to 16 bits. During simulation 100 signatures are collected after running traditional oscillator PUF on 100 different chips. The process variations of 100 different chips are generated in NanoSim

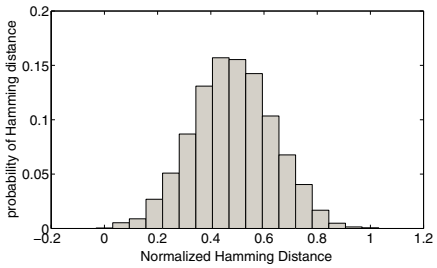


Fig. 9. Signatures from applying random pattern sets (100 16-bit signatures' Hamming distance distribution when applying 100 different random pattern sets to same chip).

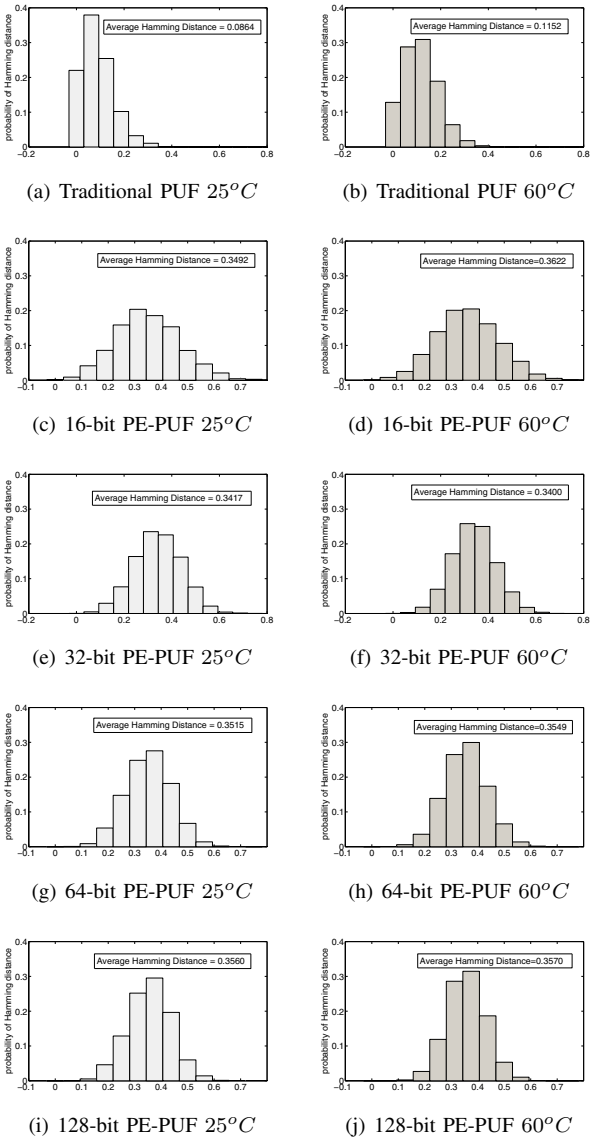
[20] Monte Carlo mode and their distrubutions as following [21]:

1. 5% intra-die, 5% inter-die, 3 sigma variation for L.
2. 15% intra-die, 15% inter-die, 3 sigma variation for V_{th}.
3. 1.5% intra-die, 1.5% inter-die, 3 sigma variation for T_{ox}.
4. 7.5% intra-die, 7.5% inter-die, 3 sigma variation for interconnect resistance R.

Same process variation distribution is used to simulate a 17 ring-oscillator PE-PUF on 100 different chips. The patterns applied to the 100 different chips are same. However, as mentioned above, PE-PUF's signature heavily depends on input patterns and its signature length is based on the number of pattern sets designers wish to apply. In this experiment 1, 2, 4 and 8 pattern sets (each pattern set include 4 patterns) are applied, and 100 16-bit, 32-bit, 64-bit and 128-bit signatures are collected, respectively. Note that since we generate 100 versions of our target design using Monte Carlo by applying various process variations, each version of the design represent one chip.

From Figure 10 and Table I, it is seen that the average Hamming distance of traditional PUF is as low as 0.0864 and 0.1152 with 1.15% and 2.20% signature pairs having Hamming distance larger than 0.3125 for 25^oC and 60^oC, respectively. That is, chips cannot be easily differentiated from each other by such signatures. In other words, the signature randomness is very low. From the 4950 signature pairs collected, 1090 signatures are identical. However, when using PE-PUF, the probability distribution of haming distance between signatures improves significantly under both temperature conditions. The increase is also seen as the pattern set count increases (see Figures 10(c)-(j)). In other words, with increasing signature length, the Hamming distances between 100 signatures (i.e. 4950 signature pairs) increases significantly as well.

As shown in Table I, by applying 8 pattern sets and generating 100 128-bit signatures, the average Hamming distance is inscreased to 0.3560/0.3570 and 82%/85.2% signature pairs have Hamming distances larger than 0.3125 for temperatures 25^oC/60^oC. To make a fair comparison with traditional PUF, compare Rows 2 and 3. Row 2 (zero pattern set) represents traditional PUF with 16-bit signature and Row 3 represents PE-PUF with one pattern set applied which generates 16-bit signatures. The comparison shows a great difference in terms of average Hamming distance. From the analysis above, it has been demonstrated that to achieve same uniqueness and randomness, the cost of PE-PUF is much lower than traditional



(a) Traditional PUF 25^oC (b) Traditional PUF 60^oC

(c) 16-bit PE-PUF 25^oC (d) 16-bit PE-PUF 60^oC

(e) 32-bit PE-PUF 25^oC (f) 32-bit PE-PUF 60^oC

(g) 64-bit PE-PUF 25^oC (h) 64-bit PE-PUF 60^oC

(i) 128-bit PE-PUF 25^oC (j) 128-bit PE-PUF 60^oC

Fig. 10. Hamming distance distribution of traditional PUF and PE-PUF under two temperature conditions (25^oC/ 60^oC) and when 1, 2, 4 and 8 pattern sets are applied.

oscillator PUFs.

V. Conclusion

In this paper, we presented a novel PUF, called PE-PUF, that takes into account all types of variations in integrated circuits. PE-PUF is able to significantly improve signature randomness and uniqueness when compared to traditional ring-oscillator PUFs that only take process variations into account. PE-PUF was implemented on ISCAS'89 s9234 benchmarks. Our analysis showed that environmental variations such as power supply noise, temperature, and crosstalk have major impact on oscillator frequency.

TABLE I

Signature Uniqueness Analysis

# of Pattern sets	Avg. Hamming Distance		Percentage> 0.3125	
	25^oC	60^oC	25^oC	60^oC
0	0.0864	0.1152	1.15%	2.20%
1	0.3492	0.3622	70.3%	75.3%
2	0.3417	0.3400	72.6%	75.6%
4	0.3515	0.3549	78.9%	81.9%
8	0.3560	0.3570	82.0%	85.2%

References

[1] R. Pappu, "Physical one-way functions," Phd thesis, *Massachusets Instutute of Tecnhology*, 2001.

[2] E. Ozturk, G. Hammouri, and B. Sunar, "Physical Unclonable Function with Tristate Buffers," in Proc. *ISCAS'08*, pp. 3194-3197, 2008.

[3] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation" in Proc. *DAC'07*, pp. 9?4, 2007.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Lecture Notes in Computer Science, vol. 1666, pp. 388.397, 1999.

[5] G. B. Ratanpal, R. D. Williams, and T. N. Blalock, "An On-Chip Signal Suppression Countermeasure to Power Analysis Attacks," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 179.188, 2004.

[6] P. C. Kocher, "Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems," Lecture Notes in Computer Science, vol. 1109, pp. 104.113, 1996.

[7] R. Anderson and M. Kuhn, "Tamper resistance - a cautionary note," in Proc. *USENIX Electronic Commerce*, pp. 1-11, 1996.

[8] Y. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security," in Proc. *USENIX Security*, pp. 291-306, 2007.

[9] K. Kursawe, A. Sadeghi, D. Schellekens, B. Skoric and P. Tuyls, "Reconfigurable Physical Unclonable Functions ?Enabling Technology for Tamper-Resistant Storage," in Proc. *IEEE International Workshop on Hardware Oriented Security and Trust*, pp. 22-29, 2009.

[10] P. Tuyls, G. Schrijen, B. Skoric, J. Geloven, N. Verhaegh and R. Wolters, "Read-Proof Hardware from Protective Coatings " in Proc. *CHES'06*, pp. 369-383, 2006.

[11] J. Guajardo, S. Kumar, G. Schrigen, P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection " in Proc. *CHES'07*, pp. 63-80, 2007.

[12] D. Holcomb, W. Burleson and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags" in Proc. *the Conference on RFID Security*, 2007.

[13] Y. Su, J. Holleman and B. Otis, "A D igital 1.6 PJ/bit Chip Identification Circuit Using Process Variations" in Proc. *ISSCC'07*, pp. 15-17, 2007.

[14] S. Kumar, J. Guajardo, R. Maes, G. Schrijen and P. Tuyls, "The butterfly PUF: Protecting IP one every PFGA" in Proc. *IEEE International Workshop on Hardware Oriented Security and Trust*, 2008.

[15] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, "Concurrency and Computation: Practice and Experience, volume 16, chapter Identification and authentication of integrated circuits" *John Wiley & Sons*, 2004.

[16] 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 International Conference on RFID 2008*, pp. 58?4, 2008.

[17] V. Vivekraja and L. Nazhandali, "Circuit Level Techniques for Reliable Physically Uncloneable Functions" in Proc. *IEEE International Workshop on Hardware Oriented Security and Trust*, pp. 30?5, 2009.

[18] J. Rabaey, A. Chandrakasan and B. Nikolic, "Digital Integrated Circuits (2nd Edition)" *Englewood Cliffs, NJ:Prentice-Hall*, pp. 199?02, 2002.

[19] http://www.synopsys.com, "Synopsys 90nm Generic Library for Teaching IC Design," Synopsys, Inc., 2009.

[20] Synopsys Inc., "User Manuals for SYNOPSYS Toolset Version 2008.03," Synopsys, Inc., 2008.

[21] http://http://www.itrs.net/, "ITRS Reports and Ordering Information 2007 Edition," ITRS, 2007.

[22] L. Bolotnyy and G. Robins, "Physically Unclonable Function -Based Security and Privacy in RFID Systems," Pervasive Computing and Communications, pp. 211-220, 2007.

[23] C.Yin and G. Qu, "Temperature-Aware Cooperative Ring Oscillator PUF," In IEEE International Workshop on Hardware Oriented Security and Trust,San Francisco,2009.

[24] S. Zhao and K. Roy, "Estimation of Switching Noise on Power Supply Lines in Deep Sub-micro CMOS circuits," in Proc. Thirteenth Int. Conf. on VLSI Design, pp. 168-173, 2000

[25] W. Chen, S. Gupta and M. Breuer, "Test Generation for Crosstalk-Induced Faults: Framework and Computational Results," in Proc. Asian Test Conf. (ATS?0), pp. 305-310, 2000.

[26] "ISCAS?9 Benchmarks," 1989. [Online]. Available: http://www.fm.vslib.cz/ kes/asic/iscas