Physically Unclonable Functions for Embeded Security based on Lithographic Variation

Aswin Sreedhar and Sandip Kundu
Email: {asreedha, kundu}@ecs.umass.edu
Department of Electrical and Computer Engineering, University of Massachusetts, Amherst MA

***Abstract*—Physically unclonable functions (PUF) are designed on integrated circuits (IC) to generate unique signatures that can be used for chip authentication. PUFs primarily rely on manufacturing process variations to create distinction between chips. In this paper, we present novel PUF circuits designed to exploit inherent fluctuations in physical layout due to photolithography process. Variations arising from proximity effects, density effects, etch effects, and non-rectangularity of transistors is leveraged to implement lithography-based physically unclonable functions (litho-PUFs). We show that the uniqueness level of these PUFs are adjustable and are typically much higher than traditional ring-oscillator or tri-state buffer based approaches.**

Keywords-PUF, IC authentication, photolithography, proximity effect, chemical mechanical polishing, hardware security

I. INTRODUCTION

Smart card technology has become highly pervasive since the beginning of this decade. The applications of smart cards range from its use for monetary transactions to its use as a replacement for keys to access buildings. Consequently, it has also become an attractive target for attackers. To prevent identity thefts and security breaches, smart cards feature security components placed in integrated circuits (IC) within smart cards.

Traditionally, cryptographic encoder circuits were embedded onto ICs to facilitate authentication that can only be decoded using a special key. Traditional attacks aim to obtain the cryptography key as a gateway for further attacks. With advanced reverse engineering techniques, such attacks have gained strength. The attacks on hardware can be classified into two groups: (i) passive attacks and (iii) active attacks [1]. Passive attacks include prying on design using its own properties. It is also known as side channel attacks. Active attacks on the other hand include additional circuits embedded into the design without the knowledge of the owner. Examples of these include Trojan circuits that aim to modify circuit operation or collect circuit information for later broadcast.

As active IC attacks could potentially render the circuit in-operable or un-recoverable, it is difficult to make ICs secure from them [2][3]. With increase in the number and ease of such attacks caused by un-trustable offshore foundries, the need for IC security and authentication has become increasingly important. A direct answer to counter these hardware-oriented breaches is to use the hardware itself to create a secret key that cannot be tampered [4][5]. Physically unclonable functions (PUF) provide such a solution. PUFs are digital circuits that generate a unique signature used for identification and authentication of an IC. These circuits have become popular in recent literature due to their ability to provide near tamper-proof solutions to hardware security [6].

PUF circuits are used to generate unique and repeatable random numbers that form the basis for crypto functions. As variations in the hardware (i.e. those between dies across the wafer) are random in nature, this can be used to provide a unique signature for each die. PUF circuits using wire and gate delays to generate the random numbers have been reported in literature [7]. As such, delays depend on both wire resistance and capacitance. PUF circuits are designed such that any active or passive tampering can change the delays□disturbing its signatures, thereby making the circuits tamper proof. PUFs are typically laid across multiple regions of the die to avoid being easily identified during reverse engineering process.

Multiple variants of PUFs have been proposed in literature using variations in wire and gate delays. More on these existing methods will be discussed in Section II. In this paper, we propose a novel PUF circuit to exploit lithographic variations. Physical design process uses a set of design rules to make layout more robust against process variations. By departing from these rules, we can engineer circuits to be highly sensitive to lithographic process variations. This is the thrust of the paper. The results are verified using lithographic simulation of designed structures. By increasing sensitivity, we increase the uniqueness of PUFs. Lithographic variations may affect multiple aspects of a physical layout. We have targeted multiple aspects of lithographic process variation to increase sensitivity of PUFs to process variations.

Rest of the paper is organized as follows. In section II we provide background information and survey of previous work. Section III describes instances of litho-PUFs used in this work with illustrations of sample circuitry. The experimental framework for our scheme, uniqueness validation and the PUF's effectiveness against well-known attacks is provided in section IV. Section V concludes out paper with ideas on future works and prospective applications.

II. PREVIOUS WORK & BACKGROUND

A. Previous work on Security PUFs

PUF architectures can be broadly classified into two categories: (a) explicitly random PUFs and (b) intrinsically random PUFs. Explicitly random PUFs are those where randomness is induced into the material to create them. They can be further sub-divided into optical and electrical PUFs. Optical PUFs consist of a layer of special transparent material which is doped with light scattering particles [8]. When the material is illuminated by a laser beam, the obtained interference pattern can be used as a response signature. The doping of light sensitive particles is a random process and cannot be controlled. Hence each interference pattern generated is highly dependent on the incident light parameters, thus providing a unique signature.

978-3-9810801-7-9/DATE11/©2011 EDAA

Electrical PUFs, otherwise termed as coating PUFs are implemented on the top layer of an IC [9]. The spacing between upper metal layers of the IC is filled randomly with dielectric material. Due to the randomness is doping, spacing width and location, the capacitance between the wires are random in nature. The capacitance variation between ICs on the wafer is measured to generate a PUF signature used to identify the IC. Any removal of the coated layer by an attacker during reverse engineering, changes the capacitance between the wires and hence the signature generated. The above two mechanisms of creating a PUF has been observed to have high manufacturing cost, area overhead and power consumption that limits their use.

PUFs that fall under the intrinsically random category can be subdivided into two types: (a) memory-based and (b) logic/delay-based. Memory-based PUFs utilize the inherent variations in the cross-coupled inverters that form the backbone of a SRAM-based memory architecture [10][11]. SRAM-PUFs also have the advantage of storing the secret key which is obtained during power-up. Upon comparison with other delay-based PUFs, SRAM-based PUFs do not have a challenge sequence and hence has only one key per chip. Even with this drawback, it has been shown to be a secure form of PUF [11].

Delay-based or silicon-PUFs exploit random variations in delays of interconnect wires and gates. They are designed to respond to an input challenge sequence with outputs of 0 or 1 based on relative delay of two different paths leading up to an arbiter or comparator [12][13]. As the fabricated circuits respond differently due to random delay variations, the response sequence can be used to uniquely identify a chip. Several variants of this circuit based on delay loop [14], multiplexor-based PUFs [15], tri-state buffer-based PUFs [13], environment aware PE-PUFs [16] and butterfly-PUFs [17] have been described in the literature. They are all based on the central idea of exploiting relative delay of two signal propagation paths that vary based on the given input challenge. The challenge sets up a race condition causing randomness of the output which is latched based on relative arrival times. The uniqueness of these circuits in terms of signature is somewhat limited. We argue that one reason for limited uniqueness is compliance with physical design rules that are specifically designed to limit lithographic process variations.

In this paper, we propose a new category of PUF circuits that are as easy to implement as delay-based PUFs, yet have uniqueness comparable to coating/electrical PUFs. We call them litho-PUFs as they are physical structures designed to respond to lithographic process variations with high sensitivity. These PUFs fall under both inherent and explicitly induced randomness based PUFs. The PUF circuits that are designed under this concept utilize the distortions existent in current sub-wavelength lithographic system to generate unique signature when given a control challenge. The following sub-section provides an insight into the existing distortions in lithography that can be utilized in the context of PUFs.

B. Lithographic Distortions

Projection photolithography has been used to create integrated circuits for the past 3 decades. With constant improvements in the ability of printing ever-smaller polygons, technology scaling has been made possible [23]. Today, the importance of lithography has risen to a level where it is now the fulcrum of the semiconductor industry. Advancements in lithography dictate the progress of the industry in terms producing smaller and faster processing units.

Photolithography prints polygons onto a silicon wafer by employing an imaging system that consists of an illumination light source, a series of lenses, an optical mask consisting of all the polygons needed to be transferred onto the wafer [18]. Photolithography, along with other processes such as oxidation, metallization, doping and etching, leads to the creation of the final IC product. In all of these manufacturing processes, statistical variations are commonplace. In lithography, distortions occur due to lens imperfections, change in focus, exposure dose, light source flare, proximity effects–caused by interference of diffraction patterns from neighboring lines, out-of-band-illumination to name a few [18][19].

Physical design process uses layout enhancements for manufacturing (LEM) techniques to mitigate process variation effects. By avoiding LEM, we can engineer litho-PUFs to be highly sensitive to process. Specifically, we take advantage of line end erosion (LEE), line-end shortening (LES), line-edge roughness (LER) and line placement near forbidden pitches to increase sensitivity. These are detailed next.

III. LITHO-PUFS

In our PUF design and analysis, we create multiple circuits that will be spread across the die utilizing the various systematic variation sources in lithography. In this section we describe in detail the type of systematic variation source being utilized and the control structures used for each case.

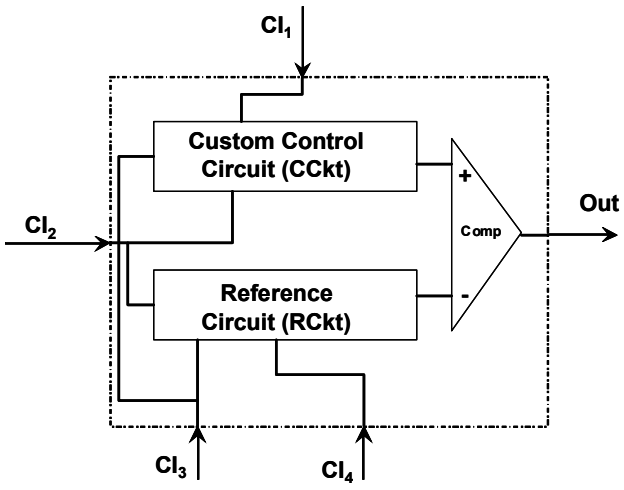

Figure 1 Description of a litho-PUF circuit used in generating the signature bits

Each of the litho-PUF circuits described in this section will incline towards creating a resistive/capacitive divider which will be compared to a reference circuitry to generate a digital value. A sample block diagram of a single PUF circuit is shown in Figure 1 . It consists of two parts namely, the control circuit (CCkt) and the reference circuit (RCkt). CIs are challenge input values going

into the PUF and *OUT* is the corresponding output bit. The resistance values obtained from the two circuits will be compared to produce the final digital output of the litho-PUF. The simplest version of the PUF would be to have circuits targeting similar kind of lithographic distortion. To decrease the possibility of having similar kind of variation on both CCkt and RCkt, they can have features that target different types of variation.

The PUFs target variations in the most basic component in lithography, i.e. polygons (interconnect, gate, diffusion etc). Each component of the circuit, i.e. polygons will undergo a different change. This change creates one unique signature per challenge sequence used. Unlike other PUF implementations where there is only type of circuit suggested, we use multiple types of circuitry targeting different variations within the die and across the wafer.

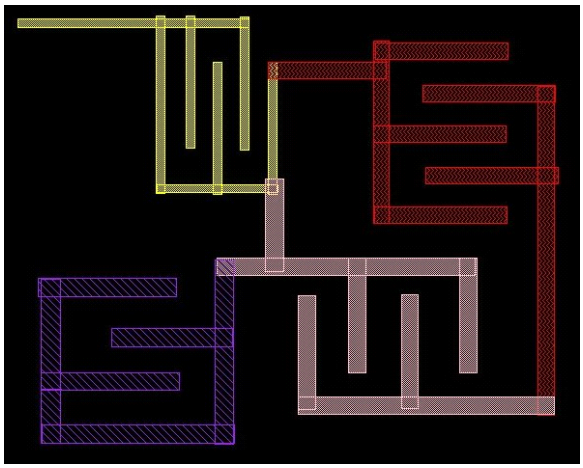

Figure 2 Illustration of a complex spiral structure

A. *Proximity-based PUFs*

Projection lithography is based on the concept of passing light through an opaque mask which is then absorbed by a light sensitive material on the wafer in order to form the required polygons. Light passing through an opaque wafer consisting of region of high and low transmittance leads to the formation of diffraction patterns. Each slit (region of high transmittance) in the mask causes a diffraction pattern of the incident light to fall on the wafer extending up to 3 times the optical source wavelength (λ) on either side of the slit. Any other slit (polygon) within this distance will cause interference between the resulting diffraction patterns. The interference pattern can lead to increase or decrease in the final polygon width on the wafer. Constructive interference occurs when the two diffraction patterns are in-phase, resulting in an increase in polygon width. Destructive interference occurs when the diffracted waves are out-of-phase with each other resulting in pinching/decrease in polygon width. Other similar types of effects have been observed at polygon corner and edges ("T" and "L" shaped features) causing corner rounding and line end shortening.

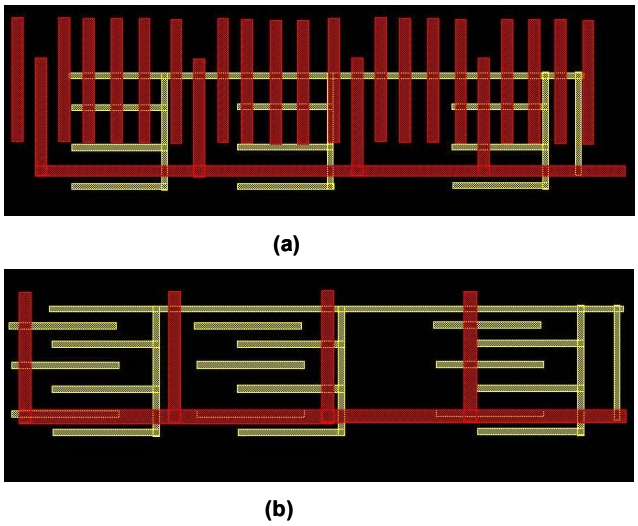

Figure 3 Dense and isolated metal lines that create CMP induced distortion (a) M4 dense, M3 isolated, (b) M4 isolated and M3 dense

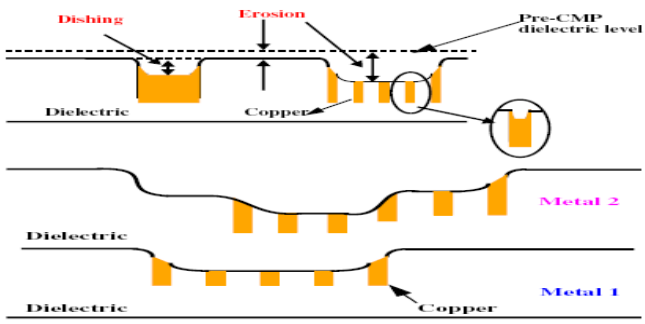

Figure 4 Illustration of change in metal height and width due to pattern density and CMP [21]

Proximity effects cause metal lines at certain pitches to increase/decrease in width. These pitches, termed as *forbidden pitches* form a range of pitches at 45nm technology producing metal width changes > 70% of drawn width. PUF circuits employ polygons placed at such pitches to trigger variations. It is also to be noted that the width of the metal line changes with any form of die-to-die change in focus. An illustration of a complex resistive feature running across multiple mask layers is shown in Figure 2

(a). The structure is vulnerable to forbidden pitches causing increase and decrease of metal line width at different region of the circuit. The distances between each metal line is carefully placed to enhance this effect.

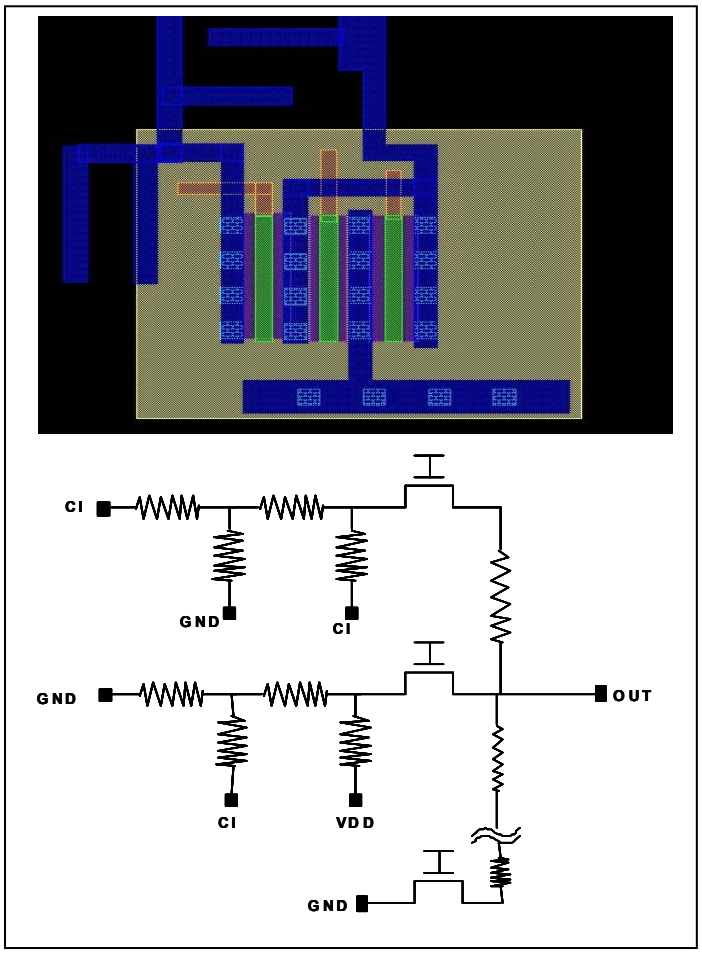

Figure 5 A snippet of pass transistor-based PUF and its circuit representation

Figure 2 (b) shows that there are certain points (marked by CI_x) in the circuit not connected to the power supply nodes. These points form a part of the challenge input nodes. By changing the value at these nodes from 0 to 1, one can change the resistances from parallel to series connections by enabling/disabling transistor switches, thereby controlling the output digital value.

B. *Density-based PUFs*

Chemical Mechanical Polishing (CMP) is a mechanical process through which metal and dielectric layers are planarized using abrasive materials to the required thickness. Stine et.al [20] showed that the post-CMP thickness is dependent on the density of current and all underlying metal layers. Isolated lines lead to decrease in final thickness (dishing) and dense features lead to erosion of the planarized material (erosion). Increase or decrease in metal layer thickness at certain areas lead to change in focus in those areas. The density effect is converted to focus variation to observe the change in metal width.

Another set of PUF structures described in this paper utilizes this change in height and width due to CMP to generate a unique set of signatures. Figure 4 illustrates this concept of dense and isolated features that vary the width and height of the features on the wafer. In Figure 3 (a) metal 4 is made dense whereas metal 3 is drawn to be isolated. In Figure 3 (b), lines drawn on mask layer 4 are isolated whereas the ones in mask layer 3 are drawn to be highly dense. These form a part existing PUF structures to increase the impact of defocus and hence increase the uniqueness factor of keys generated by the PUF circuits.

C. *NRG PUFs*

Similar to the distortions observed while printing metal interconnect lines, poly-gate masks and diffusion masks also undergo them. Proximity effects on poly masks cause fluctuations in width and length of the gate. Coupled with line end erosion (LEE), line-end shortening (LES), line-edge roughness (LER), the gate length varies along its width. Hence gates produced through the photolithography process in deep sub-wavelength lithography (DSL) are non-rectangular in nature. Non-rectangular gate (NRG) models have been proposed that closely approximate the behavior of post-silicon transistors [22], nevertheless significant variation exists among manufactured transistors.

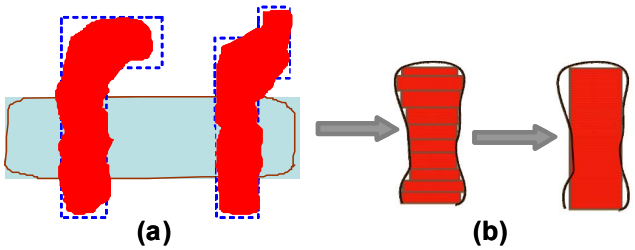

Figure 6 Illustration NRG gate (a) post-litho gate contour, (b) equivalent NRG gate model

In this PUF circuit, a series of parallel pass transistors are drawn very close to each other inducing proximity-based changes to the drawn length and width (see Figure 5). The pass-transistor type structure is drawn with their poly-gates placed at forbidden pitches without dummy lines. Figure 6 provides an illustration of the NRG gate. Like other control structure-like PUF circuits shown, the voltage generated is compared to a reference circuit to generate a final digital output. Also, control points are provided to include challenge inputs to be provided.

IV. Experimental Setup & PUF Validation

The experimentation and validation for previous works on logic-based or memory-based security PUFs involved assigning random delays or transistor mismatches respectively; and predicting the change in output signature for similar challenge inputs. Our experiments are based on lithography simulation. Lithography simulation of masks accepts certain inputs. We use a Monte Carlo process to vary these input parameters within the range of specification. The next sub-sections talk in detail regarding the experimental setup, analysis and security validation.

A. *Framework*

We use 45nm technology to perform all our experiments and validation schemes. Generic ISCAS and cryptographic circuits

such as AES and DES circuits were mapped to freely available 45nm technology library using Synopsys Design Compiler for further modification. The PUF circuits are integrated into the design by modifying the existing layouts. During the layout creation process, few cell sites within the design were marked to be unused during placement so that they can be used to fit in the PUF circuits. The rest of the PUFs were placed in multiple corners of the design. The PUFs were not allowed to have optical proximity correction or other layout enhancements for manufacturability. This is done to increase sensitivity during lithography and also anonymity from attacks. A selected set of input and outputs were connected to primary input and output ports respectively; also to camouflage the circuit within the design.

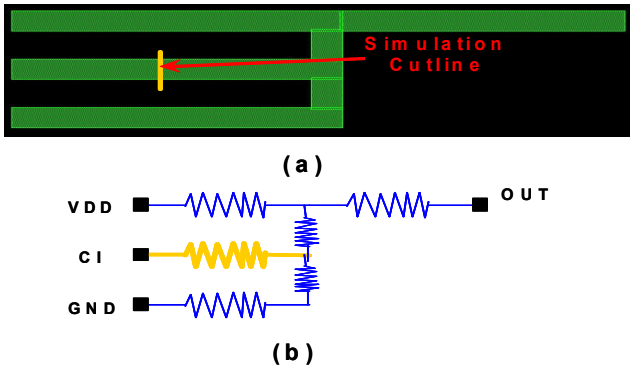

Figure 7 Sample Control circuit for illustration & analysis purpose

The simulation framework can be listed as follows

1) Inter-die Defocus: A random inter-die focus value is assigned to the entire die; showing that a set of dies located in a particular section of the wafer tend to have a different focus value compared to others in the wafer.

2) Simulation: The modified layouts are simulated using an in-house lithography simulator. This type of simulation, not only takes the inherent variation in the PUF, but also the impact of the neighborhood around the PUF circuit. As each PUF circuit runs through multiple metal layers, multiple mask simulation is performed.

3) PUF parameters: The post-simulation mask contours are scanned to obtain the width and length of each polygon forming the PUF circuit. It is important to note that the height of the polygon is obtained through lookup tables created that predicts the height of a polygon given the focus and base width obtained.

4) PUF model: The obtained parameters are fed into a pre-created PUF spice model to be simulated and observed for changes in behaviour and digital output obtained for a particular challenge input.

5) Challenge Mode: For a m-bit challenge input sequence, an n-bit signature is obtained at every defocus value. These n-bit signatures are compared against each other to estimate the level of uniqueness of signatures obtained.

B. Sample Simulation Case

To better understand the process of signature generation using litho-PUFs, consider a simple litho-PUF circuitry illustrated in Figure 7 This litho-PUF has been drawn on a single metal layer for simplicity of illustration (only CCkt shown here).

Each of the polygons drawn is of the same width (70nm) and height (~150nm). The lengths vary based on the minimum allowable spacing between the metal lines and their interconnections. Some of the metal lines are placed at near-forbidden pitch range (~160nm) to enhance linewidth fluctuation. The other part of a PUF circuit consists of a reference layout (RCkt not shown here) drawn either similar to or different from CCkt. Interconnects from RCkt and CCkt are connected as inputs to a comparator that produces a digital output value.

Both parts of the litho-PUF circuit utilize change in linewidth, length and height due to lithographic variation. To illustrate the change in these parameters of the above circuit and the resulting voltage fluctuation, we perform lithography simulation at multiple focus values. Consider a cutline at one of the polygons of the circuit as shown in Figure 7 (a) Cutlines are used to perform measurements and metrology during lithography and other manufacturing processes. At the cutline, a variation in width at multiple defocus values is observed and plotted. As 3D simulation is compute and time intensive, we perform only 2D simulation. 2D simulation does not provide any height information. We use the obtained base width information and defocus to predict the height using the focus-exposure matrix of the mask. Theory behind the focus-exposure-matrix is not within the scope of the paper, but can be found in books by Mack or Kundu et.al [18][19].

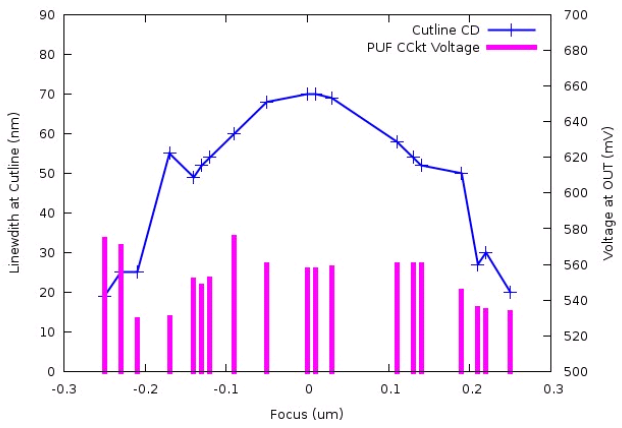

Figure 8 Linewidth & PUF voltage fluctuation with defocus at cutline

Focus variation (defocus) causes change in polygon resistance and capacitance. This leads to output voltage fluctuation. The range of this fluctuation is plotted in Figure 8 . This range varies with the type of PUF circuit used and the amount of inter-die dose fluctuation. Similarly, voltage values for the complementary circuit are obtained and compared to produce a digital output.

C. *Uniqueness Validation*

Traditional uniqueness is obtained through extensive Monte Carlo simulation of the PUF circuit in the presence of parameter variation. Since Monte Carlo lithography simulation is infeasible, we mimic the changes in width of polygons due to lithography by predicting the range of resistance change for the respective polygon in PUF circuit. This range is noted for polygons on two sample PUF circuits.

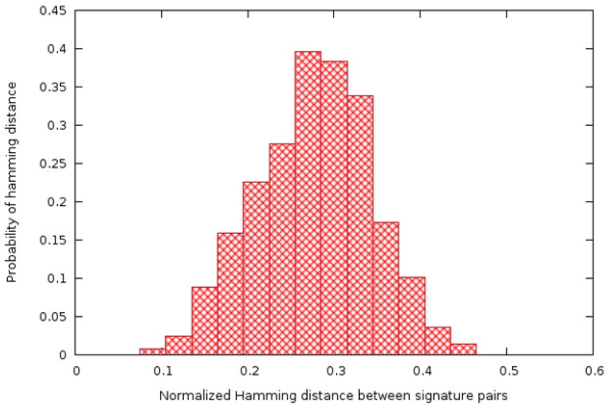

Figure 9 Hamming distance for 1000 signature pairs obtained using 250 chip signatures

Now consider 20 PUFs spread over the die, consisting of only the two selected litho-PUFs. Monte Carlo simulation is performed on the spice model of the 20 litho-PUFs. We vary the resistance of each PUF within a given range exhibiting typical behavior on the chip. To be specific, we considered a 15% fluctuation in focus between different dies on the wafer. We ran 250 simulations to estimate the uniqueness of the signatures generated. A sample set of 1000 signature pairs were compared against each other. Figure 9 shows the distribution of hamming distance between the signature pairs. A maximum of 0.45 and a minimum of 0.14 were obtained for the hamming distance (normalized) between signatures. A higher uniqueness factor can be obtained if the PUF circuits have enough variation and difference in variation from each other. We predict that, the uniqueness factor is not only tied to the challenge pattern provided, but also on the number of layout structures and the placement of the PUF circuits.

V. CONCLUSION

We presented a novel PUF architecture that utilizes inherent variations associated with lithography process. Litho-PUFs enjoy a hybrid PUF classification displaying dielectric dependence (coated-PUFs) at every metal layer and the dependence on change in resistance (delay-PUFs). The sensitivity of these PUF circuits to process variations were increased by placing them near forbidden pitches, which is normally disallowed by DRC and avoiding layout enhancements for manufacturability. Experimental results show that within published range of manufacturing process variation, the uniqueness of signatures of these PUFs are better than existing relative delay based PUF architectures. Moreover due to their simplicity and physical similarity to control structures used for metrology in a die, they are difficult to detect during reverse engineering process. Our future work involves testing the effectiveness of this approach on manufactured dies.

REFERENCES

[1] K. J. Kulikowski, M. G. Karpovsky, and A. Taubin, "Dpa on faulty cryptographic hardware and countermeasures," in FDTC, 2006, pp. 211–222.

[2] 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.

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

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

[5] J.W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication application," in Proceedings of the Symposium on VLSI Circuits, 2004, pp. 176–159.

[6] 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.

[7] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Delay-based Circuit Authentication and Applications," in Proceedings of the 2003 ACM Symposium on Applied Computing, 2003, pp. 294–301.

[8] R. Pappu, "Physical one-way functions," Phd thesis, Massachusets Institute of Tecnhology, 2001.

[9] 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.

[10] Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, Pim Tuyls, "Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection", International Conference on Field Programmable Logic and Applications (FPL), Aug 27-29, 2007, Amsterdam, The Netherlands.

[11] L. Bolotnyy and G. Robins. Physically unclonable Function-Based security and privacy in RFID systems. In 5th IEEE Int. Conf. on Pervasive Computing and Communications (PERCOM), pages 211-220, Washington, DC, USA, 2007. IEEE Computer Society.

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

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

[14] B. Gassend, D. Clarke, M. van Dijk and S. Devadas. Silicon Physical Random Functions. Proceedings of the Computer and Communications Security Conference, November 2002

[15] D. Lim, J-W. Lee, B. Gassend, M. van Dijk, E. Suh, and S. Devadas. Extracting Secret Keys from Integrated Circuits, IEEE Transactions on VLSI Systems, volume 13, Number 10, pages 1200–1205, October 2005

[16] X. Wang, M. Tehranipoor, " Novel Physical Unclonable Function with Process and Environmental Variations," in Proc. DATE 2010.

[17] 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.

[18] C. A. Mack, "Fundamentals Principles of Optical Lithography," Wiley 2008.

[19] S. Kundu, A. Sreedhar, "Nanoscale CMOS VLSI Circuits: DFM," McGrawHill 2010.

[20] B. Stine et. al., "A Closed-form Analytic Model for ILD thickness variation in CMP processes," in Proc. Chemical Mech. Polish. For VLSI/ULSI MultilevelInterconneciont Conf., 1997, pp. 266-273.

[21] T. Tugbawa, "Chip-Scale Modeling of Pattern Dependencies in Copper Chemical Mechanical Polishing Process," Ph.D. dissertation, MIT, Cambridge, MA.

[22] Ke. Cao, Sorin Dobre, Jiang Hu, "Standard Cell Characterization Considering Lithography Induced Variations," Proc. Design Automation Conference 2006.

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