A Physical Unclonable Function Defined Using Power Distribution System Equivalent Resistance Variations

Ryan Helinski
University of New Mexico
Albuquerque, NM
helinski@unm.edu

Dhruva Acharyya
Verigy Inc.
Cupertino, CA
dhruva.acharyya@verigy.com

Jim Plusquellic
University of New Mexico
Albuquerque, NM
jimp@ece.unm.edu

ABSTRACT

For hardware security applications, the availability of secret keys is a critical component for secure activation, IC authentication and for other important applications including encryption of communication channels and IP protection in FPGAs. The vulnerabilities of conventional keys derived from digital data can be mitigated if the keys are instead derived from the inherent statistical manufacturing variations of the IC. Robust silicon-derived keys are implemented using physically unclonable functions (PUFs). A PUF consists of a specialized hardware circuit and a mechanism to retrieve a set of responses under a variety of different challenges. In this paper, we propose a PUF that is based on the measured equivalent resistance variations in the power distribution system (PDS) of an IC. The effectiveness of the PUF is evaluated on thirty-six ICs fabricated in a 65 nm technology.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection -- *Authentication.*

General Terms

Security

Keywords

Hardware security, unique identifier, process variations

1.INTRODUCTION

Many hardware security and trust mechanisms depend on the availability of a secret key or signature, i.e., a unique, unclonable identifier that can be derived from each IC. The signature of the IC defines the basis of hardware security mechanisms implemented at high levels, e.g., those that perform encryption of data communication channels, or provide IP protection in FPGAs. Conventional IC signatures are defined using digital data stored, for example, in a flash or ROM on the chip. It is critical that access to the key remains restricted to hardware circuits on the chip. Unfortunately, since the keys always remain in digital form, they are subject to an invasive attack by adversaries who may be able to extract the key, thereby defeating the security mechanisms. Also, once a digital key is stolen, it becomes possible to produce *clone* chips that have the same identifier. This is a problem for applications that use the key in authentication protocols.

The vulnerability of embedded digital keys to attacks can be mitigated if the keys are instead derived from the inherent statistical manufacturing variations of the IC. Physically unclonable functions (PUFs) are used to realize these silicon-variation-based keys [1]. A PUF consists of a specialized hardware circuit that is sensitive to process variations. A PUF also incorporates a mechanism to retrieve a unique set of responses from a variety of different challenges. Keys derived from PUFs possess important properties including *volatility* and *non-replicability*; properties which make it extremely difficult for the attacker to steal and/or duplicate the keys. Therefore, PUFs can revolutionize next generation security and trust infrastructures in ICs.

There are two general approaches to implementing PUFs, one that is based on the variability in passive and active devices [2-9] or leakage current [10] and one that is based on variability in only passive structures, e.g., metal wires [11]. Although process variations in active devices can be leveraged to create a diverse set of responses across ICs, performance variations in active devices are also subject to environmental variations such as temperature and noise. Therefore, such approaches must also incorporate a technique to calibrate for environmental variations otherwise the response of the PUF may depend on the conditions. Calibration complicates the design and use of the PUF and makes them less attractive for security applications.

On the other hand, a PUF that is based on the variations in passive components of the IC is less susceptible (and therefore more robust) to environmental variations. The challenge in this case is implementing the PUF such that the infrastructure which defines the key does not consume a large area overhead. We propose a PUF that leverages the inherent variations in the metal resistances that define the power grid [12]. Since the power grid is an existing, distributed resource in every design, the overhead of a power grid-derived PUF is limited to the added challenge/response circuitry. Moreover, the distributed nature of the power grid makes it more prone to larger random and systematic process variation effects. Distributed process variation effects introduce resistance variations whose magnitudes vary across different regions of the power grid. This characteristic improves the robustness of the PUF because it makes it less probable that the PUFs from two ICs will produce the same response.

In this paper, we investigate a PUF derived from the resistance variations in the power grids of chips fabricated in a 65 nm technology. The PUF's response is defined in two ways; 1) as set

DAC'09, July 26-31, 2009, San Francisco, California, USA

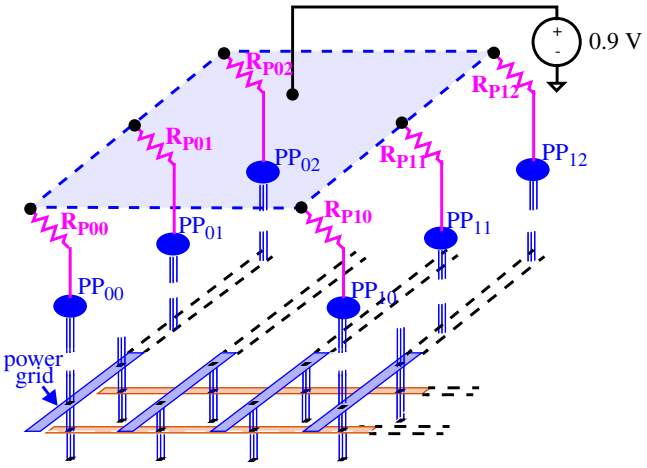

Figure 1. Power Grid Architecture

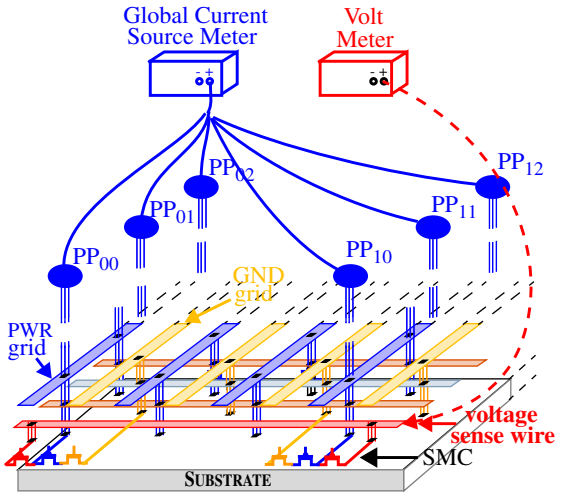

Figure 2. Instrumentation Setup

of voltage drops measured at a set of distinct locations on the power grid of the IC, and 2) as a corresponding set of equivalent resistances computed at these same locations. A distributed PUF circuit is proposed as a means of introducing a variety of stimuli (challenges) and for measuring the voltage drops (responses). A statistical analysis is carried out on the data collected from a set fabricated chips to determine the effectiveness of the PUF and to measure its susceptibility to environmental variations.

The organization of this paper is as follows. A brief background is presented in Section 2. The experimental design and test setup is described in Section 3. The PUF is described in Section 4. Section 5 describes the experiments carried out on the 65 nm chips and the experimental results. Section 6 concludes.

2.BACKGROUND

PUFs have been proposed for many applications including IC identification [13][14], addressing security in wireless sensor nodes and IC process quality control [2], hardware metering [10][15], challenge-based IC authentication [3][4][10], IP protection in FPGAs [16-18] and remote service and feature activation [19][20].

For IC authentication, a secret key is embedded that enables the IC to generate a unique response to a challenge, which is valid only for that challenge (called challenge-based IC authentication). In this manner, the key remains secret and the authentication mechanism is not vulnerable to spoofing. The authors of [7][17] propose that the same secret keys can also be used for cryptography.

The authors of [15][19] describe remote activation schemes that enable IC designers to lock each IC at start-up and then to enable it remotely, providing IP protection and hardware metering. In [19], their objectives are realized by adding states to the finite state machine (FSM) of a design and by adding control signals that are a function of the unique IDs. In effect, the hardware "locks up" waiting for a specific activation code. This offers protection against unauthorized use of Intellectual Property (IP) and hardware piracy (the illegal manufacturing of ICs).

Various PUF techniques have also been proposed that are based on mismatched delay-lines [3][6][21][22], SRAM power-on patterns [17][18], MOS device mismatch [2][13][14] and input-dependent leakage patterns [10].

3.EXPERIMENTAL DESIGN AND SETUP

A high-level representation of the power grid architecture used in the hardware experiments is shown in Figure 1. The bottom portion shows that adjacent metal layers are routed at right angles to each other in a mesh configuration with vias placed at the intersections. The GND grid (not shown) is interleaved with the power grid and routed in a similar fashion. Both grids are routed across the 10 metal layers available in the 65 nm process. The width of the wires and the granularity of the mesh vary across the metal layers. In particular, the widths of the lower metal wires are smaller and the granularity is finer than the widths and granularity of the metal wires in the upper layers. This feature of the power grid is typical of commercial designs.

The power grid is connected to a set of six C4s or power ports (**PP**s) in the top metal layer. The PPs are shown as ovals in the figure and are labeled PP_{00} through PP_{12}. The C4s enable the power grid to be connected to the power supply, either through a membrane style probe card (during wafer probe) or through the package wiring. The finite resistance of power port connections are represented as series resistances, Rp_{xy}, in the figure.

The test jig used in the experiments is shown in Figure 2. The package pins that are connected to the PPs wire onto a printed circuit board to the *global current source meter* (GCSM). The GCSM provides 0.9 V to the power grid and can measure current at a resolution of approximately 300 nA. In addition to the global currents, our technique also requires on-chip voltage measurements. The voltage is measured in our experiments using a pin that is connected internally to a globally routed *voltage sense wire*. A voltmeter is connected to this pin off-chip, as shown in Figure 2.

The last element of the proposed infrastructure is shown along the bottom of Figure 2 and in more detail in Figure 3(b). A **Stimulus/Measure Circuit** (SMC) is inserted under each of the six C4s as shown in Figure 3(a). The SMC consists of a *shorting inverter*, a *voltage sense transistor* and a set of three *scan flip-flops* (FFs). The outputs of the FFs connect to the gates of the three transistors as shown in Figure 3(b). The shorting inverter provides a controlled stimulus, i.e., a short between the power and ground grid, when the states of FF_1 and FF_2 are set to 0. The voltage on the power grid is measured using the voltage sense transistor,

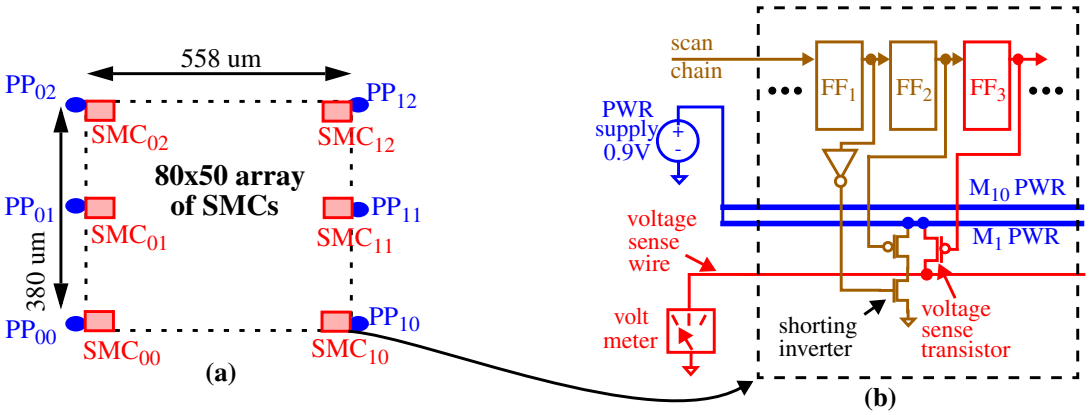

Figure 3. (a) Block diagram of the test structure and (b) details of the Stimulus/Measure Circuit (SMC).

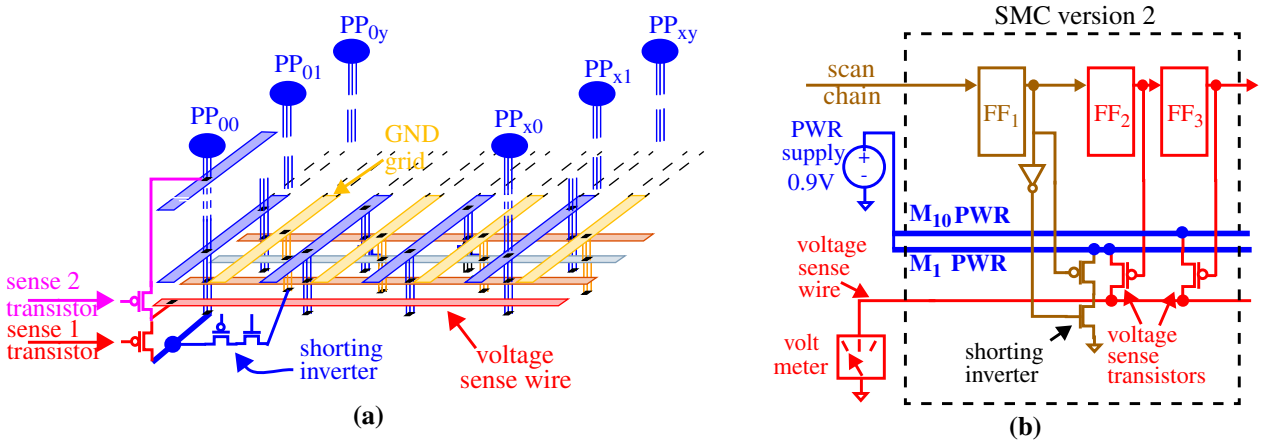

Figure 4. (a) Connections of a modified versions of SMC (b) details of the modified SMC.

enabled with a 0 in FF_3.

4.PUF SIGNATURES AND ARCHITECTURES

The PUF signature is derived using two strategies, one that is based on voltage drops and one on equivalent resistance. In either case, the signature associated with the chip is composed of six quantities, each corresponding to one of the six SMCs. The signature for a given IC under the voltage drop strategy is constructed by enabling the shorting inverters in the SMCs, one at a time, and then measuring the voltage at its source using the voltage sense transistor. A voltage drop is computed by subtracting the measured voltage from the supply voltage, 0.9 V. This process is repeated for each of the other SMCs. The resulting set of six voltages defines the signature.

The values in the voltage drop signature are affected by the magnitude of the current through the shorting inverter. The variations in the current magnitude among the shorting inverters actually adds to the 'randomness' of the PUF. However, the PUF is also more sensitive to environmental conditions, which detracts from its ability to generate the same signature (reproducibility). The equivalent resistance (ER) strategy eliminates this dependency by dividing the voltage drops by the global currents. The elimination of the current dependency makes the ER-based PUF less sensitive to environmental variations.

Bear in mind that hundreds of SMCs can be inserted into commercial power grids, which would greatly expand the complexity of the signature over that shown in these proof-of-concept experiments. Doing so is practical because the overhead of the SMC is small. For example, assuming a total of 100 SMCs, each with an area of 50 um^2 yields 5000 um^2. This is only 0.02% of the 25,000,000 um^2 area available in a 5 mm X 5 mm chip.

The PUF as described has several drawbacks. First, it is only able to produce a single signature. Second, signature generation requires the use of external instrumentation to measure the voltages and currents. Although this serves some applications, it poses problems for others that need to apply a challenge and obtain a response while operating in mission mode.

Simple modifications of the PUF architecture can address these issues. For example, the SMC shown in Figure 3(b) can be modified to incorporate more than one 'voltage sense' transistor. The left side of Figure 4 shows a modification in which a second sense transistor, 'sense 2 transistor' is added to enable the voltage to be measured in metal 10 underneath the power port. With the second sense transistor, the voltage drops between M_1 and M_{10} at different places on the power grid can be measured. This increases the number of stimulus/response pairs of the PUF from linear to quadratic because voltage drops can now be computed between any pairing of 'sense 1' and 'sense 2' transistors across the array of SMCs. The right side of the figure shows a schematic in which an additional flip-flop, FF_3, is used to control the second sense

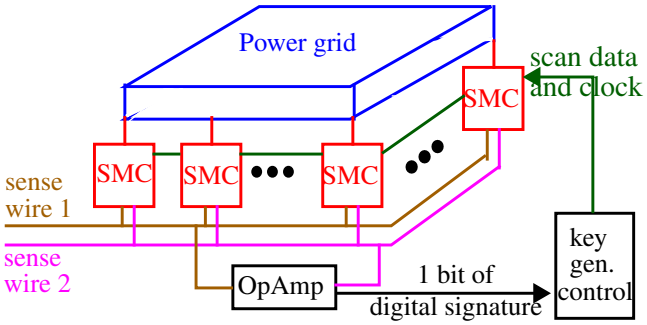

Figure 5. On-chip instrumentation for signature generation.

transistor[1].

Another strategy to increase the number of stimulus/response pairs is to allow the stimulus to be applied from more than one SMC. In these scenarios, multiple shorting inverters are enabled simultaneously at different locations and the voltage drops are measured using different combinations of sense 1 and sense 2 transistor pairs. We refer to these scenarios as multiple-on and the former as single-on. Since the power grid is a linear system, superposition applies. Therefore, to make this more resilient to attack, whereby the attacker systematically deduces the voltage drops that would occur under a multiple-on scenario by measuring the voltage drops under all single-on scenarios, this scheme can be combined with an obfuscation of the scan chain control bits. Under obfuscation, the number and position of the enabled shorting inverters are deterministically (or randomly) scrambled for a given scan chain control sequence, making it difficult or impossible to systematically apply single-on tests at known locations on the chip. We have investigated scan-chain obfuscation techniques in previous work where the objective was to prevent an adversary from using the scan chain to reverse engineer a design [23][24]. These techniques are applicable here as well. For chip-specific random scrambling, a subset of the SMCs can be used during initialization to define the state of a *selector* that controls the scan chain scrambling configuration.

The PUF as proposed requires the use of external instrumentation to measure the voltages and global currents needed to compute the IC's signature. Although this approach serves the chip authentication application well, e.g., where the objective is to periodically check the authenticity of a chip or set of chips to circumvent attempts to replace the chips with counterfeits, it is not amenable to cryptology applications that use the signature as the secret key in hardware implemented encryption/decryption algorithms. In order to serve this latter need, the signature generation process needs to occur using on-chip instrumentation.

The simplest approach to accomplishing this is shown in Figure 5. The *key generator control* unit drives the scan-in, scan-out and scan-clock signals of the SMCs with a specific pattern to enable one or more of the shorting inverters in the array of SMCs[2]. The scan pattern also enables two voltage sense transistors, one for each of the two voltage sense wires, labeled *sense wire 1* and *sense wire 2*. The two voltage sense wires are routed to the inputs of a simple differential OpAmp. The OpAmp outputs a '0' or a '1' depending on whether the voltage on 'sense wire 1' is larger or smaller than the voltage on 'sense wire 2', respectively. The 1-bit output is sent to the *key generation control* unit and the process is repeated until a sufficient number of bits are generated to realize the key. Note that this implementation is more sensitive to environmental variations because it makes use of voltages instead of equivalent resistances, as described earlier. Therefore, the response for a given chip under a given sequence of scan patterns may differ over time unless temperature and power supply noise are monitored and tightly controlled. Other more noise tolerant architectures are possible but they will increase the area overhead associated with the key generation infrastructure.

5.EXPERIMENTAL RESULTS

We carried out a set of experiments to evaluate the diversity in the voltage drops and equivalent resistances in a set of thirty-six chips. We also carried out an additional set of experiments to evaluate the stability of the PUF. The PUF stability experiments were performed on one of the chips in the set. To evaluate stability, we repeated the signature generation/measurement process seventy-two times[3]. The variation across the set of signatures from these experiments is due entirely to environmental noise and temperature variations. The stability experiments are important for determining the probability of signature aliasing, i.e., the probability that two chips from the population generate the same signature. We refer to data from the stability experiments as control data.

The experimental results for twelve of the chips from the set of thirty-six are shown in Figures 6 and 7, using the voltage drops and equivalent resistances, respectively. The left half of the figure lists the chip number along the x-axis. The right half gives twelve of the PUF stability results for one chip. The six data points defining the chip signature are displayed vertically above the chip identifier. The y axis gives the voltage drop and equivalent resistance, respectively, in each of the figures.

The diversity among the signatures in the twelve chips shown on the left side of the figures is evident in both plots. In addition to the different patterns of dispersion in the signatures, the ordering of the data points from top to bottom is also distinct across all chips. The ordering is in reference to the SMCs that each data point corresponds to. For example, SMC_{00} in Figure 3(a) is assigned 0, SMC_{01} is assigned 1, ..., SMC_{12} is assigned 5. In Figure 6, the ordering for chip 1 is 5, 1, 2, 0, 4, 3. while the ordering for chip twelve is 3, 0, 5, 1, 2, 4. Therefore, the apparent diversity among the signatures due to dispersion is actually larger because of the differences in the orderings. It is also clear from the PUF stability experiments that environmental variations have an impact on the signature and therefore, they must be taken into account.

In many cases, there are differences in the dispersion and

1. It is possible to replace the 'shorting inverter' with a single PFET. However, the stacked devices of the shorting inverter are more robust to defects and is proposed as a fault tolerant strategy to prevent yield loss that might result if a defect caused the stimulus transistor to remain in the on-state.

2. This scheme refers to the original SMC (Fig. 3) modified to include a second sense transistor connected between M1 and a new voltage 'sense wire 2' (Fig. 5).
3. No temperature control or specialized low noise test apparatus was used.

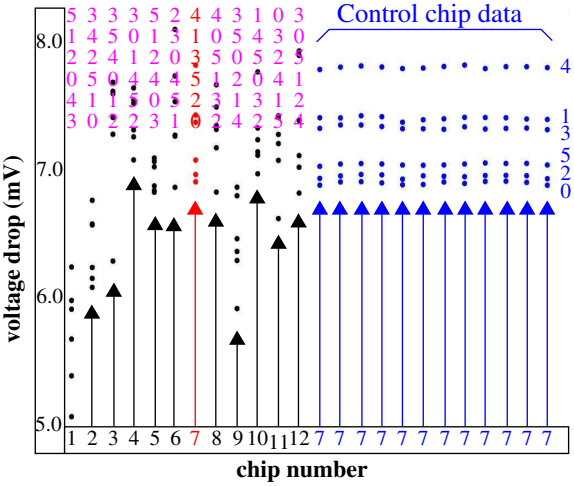

Figure 6. Voltage drop signatures for 12 chips and 12 control samples.

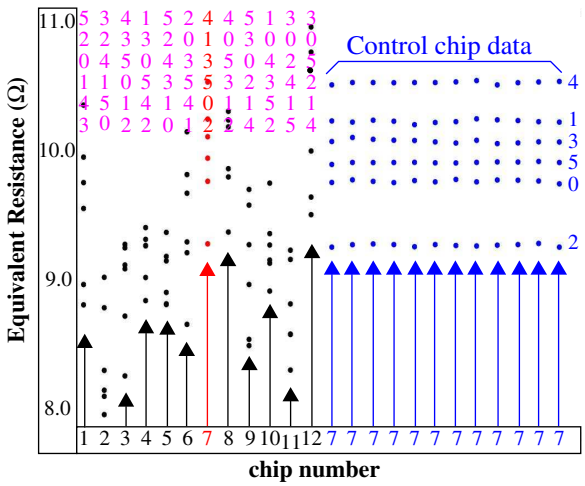

Figure 7. Equivalent resistance signatures for 12 chips and 12 control samples.

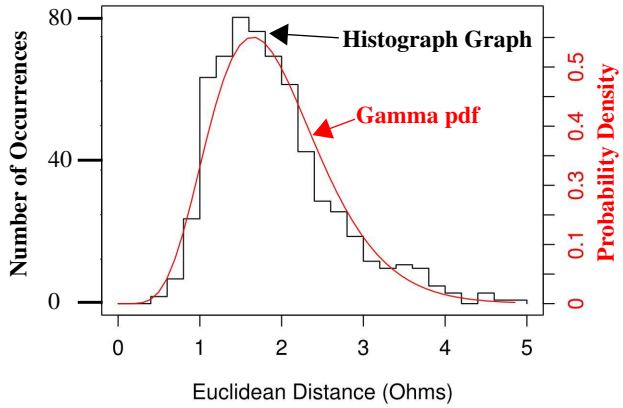

Figure 8. Gamma function fit of chip equivalent resistance histogram.

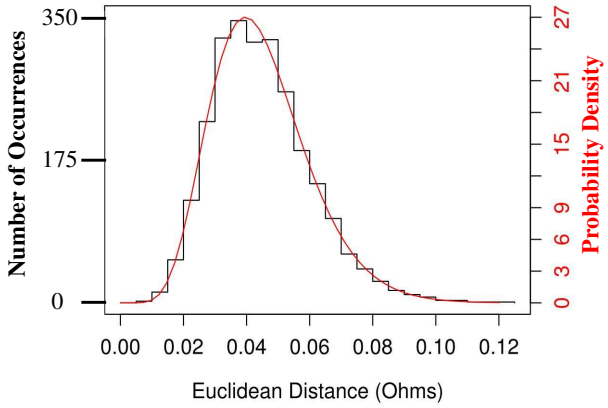

Figure 9. Gamma function fit of noise equivalent resistance histogram.

ordering of the data points for the same chip across the voltage drop and equivalent resistance analyses. This is expected because the equivalent resistance eliminates an element of the diversity introduced by variations in the magnitude of the shorting currents.

In order to quantitate the dispersion among the chip signatures, we compute the Euclidean distance between the data points and analyze their variance. The six data points in each signature can be interpreted as a single point in a six-dimensional space. The Euclidean distance between two signatures for chips x and y is given by Equation 1. The Euclidean distance is computed between

$$\text{dist} = \sqrt{(x_1 - y_1) + (x_2 - y_2) + \ldots + (x_6 - y_6)} \qquad \textbf{Eq. 1.}$$

all possible pairing of chips, i.e., (36*35)/2 = 630 combinations. The same procedure is carried out using the control data in which (72*71)/2 = 2556 combinations are analyzed.

In order to compute the probability of two chips producing the same signature given the uncertainty associated with the measurements, we first compute a histogram that tabulates the number of Euclidean distances partitioned into a set of bins for the chip and noise data sets separately. The bins in each histogram are equal in width, with each equal to 1/25th of the total span that defines the range of Euclidean distances among the 630 and 2556 combinations of chip and noise data pairings, respectively. We then fit these histograms to gamma probability density functions (pdf). The histograms and the gamma pdfs are shown superimposed in Figure 8 (chip) and Figure 9 (noise) for the equivalent resistance analysis. In both cases, the gamma functions are a good fit to the histograms. The range of values found among the 630 chip pairings is between 0.45 and 5.0, as indicated by the x-axis, while the range for the noise analysis is between 0.01 and 0.12. Therefore, the largest value in the noise data is approximately four times smaller than the smallest value in the chip data.

We compute the probability of aliasing by first determining the Euclidean distance in the noise data that bounds 99.7% (3 sigma) of the area under the pdf. This particular Euclidean distance upper bounds the worst case noise and is equal to 0.099 for the data shown in Figure 9. We then compute the cumulative distribution function (cdf) of the chip data and use this worst case noise value to determine the probability of aliasing by looking up the y value on the chip cdf associated with this x value. This gives us the

probability that the Euclidean distance between any pairing of two chips is less than or equal to the worst case Euclidean distance among the control data.

The results for the equivalent resistance and voltage analyses are given in Table 1. Using equivalent resistances, the probability of aliasing is 6.9e-8 or approximately 1 chance in 15 million. For the voltage analysis, the probability increases to approximately 1 chance in 28 billion. Given that the number of SMCs used to define the signature in these experiments is only six, we can expect, based on these results, that the probability would improve in a commercial design that included a larger number of SMCs.

Table 1: Probability of aliasing.

	Analysis Type	
	Volt.	**Eq. Res.**
Prob. Eucl. dist. of chips < 99.7% of all noise Eucl. dist.	3.5e-11	6.9e-8

6.CONCLUSIONS

Methods to provide IC security based on manufacturing variability have recently emerged for applications such as IC authentication, secure activation, encrypted communication and IP protection on FPGAs. These applications rely on intrinsic variability of the hardware to provide a signature that is probabilistically unique to each IC. Hardware circuits that leverage process variations to implement IC signatures are called physically unclonable functions (PUFs). In this paper, we propose a PUF that leverages the inherent resistance variations in the metal layers defining the power grid. Data from a set of thirty-six chips fabricated in a 65 nm technology is used to confirm the feasibility of this strategy.

7.ACKNOWLEDGEMENTS

We acknowledge Sani Nassif and Kanak Agarwal of IBM Austin Research Laboratory for their support of this research. This research was supported in part by NSF grant CNS-0716559.

8.REFERENCES

[1]R. S. Pappu, B. Recht, J. Taylor and N. Gershenfeld, "Physical One-Way Functions," *Science*, 297(6), 2002, pp. 2026-2030.

[2]Y. Su and J. Holleman and B. Otis, "A 1.6pJ/bit 96% Stable Chip ID Generating Circuit using Process Variations," *Proc. of International Solid State Circuits Conference*, 2007, pp. 406-407.

[3]B. Gassend and D. E. Clarke and M. van Dijk and S. Devadas, "Silicon Physical Unknown Functions," *Proc. of Conference on Computer and Communications Security*, 2002, 148-160.

[4]G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", *Proc. Design Automation Conference*, 2007, pp. 9-14.

[5]D. Lim, J. W. Lee, B. Gassend, G.E. Suh, M. van Dijk and S. Devadas, "Extracting Secret Keys from Integrated Circuits, " *Trans. on Very Large Scale Integration Systems*, 13(10), Oct. 2005, pp. 1200-1205.

[6]B. Gassend, D. Clarke, M. van Dijk and S. Devadas, "Controlled Physical Random Functions," *18th Annual Computer Security Applications Conference*, 2002.

[7]B. Gassend and M. Van Dijk and D. Clarke and E. Torlak and S. Devadas and P. Tuyls, "Controlled Physical Random Functions and Applications," *ACM Transactions on Information and System Security*, Volume 10, Number 4, 2008.

[8]E. Ozturk, G. Hammouri and B. Sunar, "Physical Unclonable Function with Tristate Buffers," *Proc. International Symposium on Circuits and Systems*, 2008, pp. 3194-3197.

[9]E. Ozturk, G. Hammouri and B. Sunar, "Towards Robust Low Cost Authentication for Pervasive Devices", *Proc. International Conference on Pervasive Computing and Communications*, March 2008 pp. 170-178.

[10]Y. Alkabani and F. Koushanfar and N. Kiyavash and M. Potkonjak, "Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach," *Information Hiding*, 2008.

[11]R. Helinski, "Measuring Power Distribution System Resistance Variations for Application to Design for Manufacturability and Physical Unclonable Functions," M.S. thesis, University of Maryland, Baltimore Co., July, 2008.

[12]R. Helinski, J. Plusquellic, "Measuring Power Distribution System Resistance Variations," Transactions on Semiconductor Manufacturing, Volume 21, Issue 3, pp. 444-453, Aug. 2008.

[13]S. Maeda and H. Kuriyama and T. Ipposhi and S. Maegawa and Y. Inoue and M. Inuishi and N. Kotani and T. Nishimura, "An Artificial Fingerprint Device (AFD): a Study of Identification Number Applications Utilizing Characteristics Variation of Polycrystalline Silicon TFTs," *Trans. on Electron Devices*, number 50, issue 6, June, 2003, pp.1451- 1458.

[14]K. Lofstrom, W. R. Daasch and D. Taylor, "IC Identification Circuits using Device Mismatch," *Proc. of International Solid State Circuits Conference*, 2000, pp. 372-373.

[15]J. Huang and J. Lach, "IC Activation and User Authentication for Security-Sensitive Systems," *Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, 79-83.

[16]E. Simpson and P. Schaumont, "Offline Hardware/Software Authentication for Reconfigurable Platforms," *Cryptographic Hardware and Embedded Systems*, Volume 4249, Oct., 2006, pp. 10-13.

[17]J. Guajardo, S. S. Kumar, G.-J. Schrijen and P. Tuyls, "Physical Unclonable Functions and Public Key Crypto for FPGA IP Protection," *Conference on Field Programmable Logic and Applications*, 2007, 189-195.

[18]S. S. Kumar and J. Guajardo and R. Maes and Geert-Jan Schrijen and P. Tuyls, "Extended Abstract: The Butterfly PUF Protecting IP on Every FPGA," *Proc. of IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 70-73.

[19]Y. Alkabani and F. Koushanfar and M. Potkonjak, "Remote Activation of ICs for Piracy Prevention and Digital Right Management," *Proc. of International Conference on Computer-Aided Design*, 2007, pp. 674--677.

[20]J. Guajardo, S. S. Kumar and G. Schrijen and P. Tuyls, "Brand and IP Protection with Physical Unclonable Functions," *IEEE Symposium on Circuits and Systems*, 2008, pp. 3186-3189.

[21] B. Gassend and D. Lim and D. Clarke and M. van Dijk and S. Devadas, "Identification and Authentication of Integrated Circuits, Concurrency and Computation: Practice and Experience, 2003.

[22]J. Li and J. Lach, "At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection," *Workshop on Hardware-Oriented Security and Trust*, 2008, 8-14.

[23]J. Lee, Mohammad Tehranipoor, Chintan Patel and Jim Plusquellic, "Securing Designs Against Scan-Based Side-Channel Attacks," Transactions on Dependable and Secure Computing, Volume 4, Number 4, October-December 2007, pp. 325-336.

[24]J. Lee, M. Tehranipoor, J. Plusquellic, "A Low-Cost Solution for Protecting IPs against Scan-Based Side-Channel Attacks," Proc. VLSI Test Symposium, May 2006, pp. 42-47.