Bit String Analysis of Physical Unclonable Functions based on Resistance Variations in Metals and Transistors

Jing Ju, Jim Plusquellic
University of New Mexico, Albuquerque, NM
(jujing@unm.edu, jimp@ece.unm.edu)

Raj Chakraborty
Intel Corp., Santa Clara, CA
(rajkchakraborty@gmail.com)

Reza Rad
ST Microelectronics
(reza2@umbc.edu)

Abstract -- ***Security mechanisms such as encryption, authentication and feature activation depend on the integrity of embedded secret keys. The mechanism by which these 'digital secrets' are stored within Integrated Circuits (ICs) is changing from EPROMs and/or fuse technology to Physical Unclonable Functions (PUFs). PUFs leverage the naturally occurring manufacturing variations within each IC to produce repeatedly random digital identifiers. In this paper, we analyze the quality of the bit strings generated by PUFs that leverage resistance variations in 1) the power grid metal wires and transistor on-resistance in 60 copies of a 90 nm chip and 2) in the power grid metal wires of 58 copies of a 65 nm chip.***

Keywords - Physical Unclonable Function, power grid, metal resistance variations

1 Introduction

Physical unclonable functions (PUFs) leverage random manufacturing variations in ICs to produce, ideally, an exponentially long bit string from a set of embedded circuit primitives. Variations in the geometries of the wires and the physical characteristics of transistors are distinct in each copy of a chip. These physical variations manifest as analog variations in the chips' parametric properties, such as power and delay. A PUF is designed to measure and 'digitize' these analog electrical variations. The 'quality' of the bit string produced can be measured against many statistical metrics, but needs to meet three important criteria; 1) the bit string is *unique* for each chip, and thereby able to distinguish each chip in the population, 2) the bit string is *random* and therefore difficult or impossible to model and predict by an adversary, and 3) the bit string is *stable*, i.e., it remains constant for a given chip over time, and under varying environmental conditions. A PUF that is able to meet these requirements can be used in applications related to security including chip identification, authentication, as keys for encryption algorithms, for remote activation, and for protecting Intellectual Property (IP).

Nothing in the manufacturing process of a chip is exact, and therefore, all fabricated physical components, e.g., wires and transistors, on the chip vary from their nominal characteristics. Although it is possible to measure these physical variations directly, it is extremely difficult or impossible to do so without sophisticated processes and equipment. The analog electrical and parametric variations that result, on the other hand, can be measured and processed more easily, and in many cases, this can be done using on-chip instrumentation. Many proposed PUF-based systems are defined in this manner, and are differentiated by the type of electrical variation they leverage. The magnitude and stability of variations in, e.g., transient current, delay, leakage, resistance, capacitance, etc. are dependent on the technology and the environment, and therefore, some PUF systems can better meet the quality metrics described above than others.

In this paper, we investigate a PUF that measures resistance variations in metal wires that define the power grid of the chip. There are several benefits of a power grid-based PUF. Resistance of metal wires varies linearly with temperature and can easily be designed to be resistant to aging effects such as electromigration. Second, resistance can be measured using a simple DC process, which can improve signal-to-noise significantly over PUFs that leverage AC characteristics, such as delay. Third, metal components are ubiquitous on a chip, with the power grid consuming a large fraction of the metal resources, e.g., 15-25% is typical in most commercial power grid designs. Fourth, the power grid is a stacked structure, offering a **3rd dimension** in which to leverage entropy. Last, the interconnected structure of the wires in the power grid complicates the interaction among variations in resistance that occur, thereby increasing the complexity of model building attacks.

In order to fully leverage metal resistance variations, we design a PUF that can measure them in each of the metal layers of the power grid. Our experiments are carried out on a set of chips fabricated in IBM's 90 nm, 9 metal layer bulk silicon process, and on a set of 65 nm chips fabricated in IBM's silicon-on-insulator (SOI) process. The quality of the bit strings is measured using inter-chip and intra-chip Hamming Distance, as well as a suite of statistical tests available from NIST [1]. For comparison purposes, we also analyze the bit strings produced from measurements of transistor on-resistance. The results show that the bit strings derived from both metal resistance and transistor on-resistance variations score very well on the statistical tests, and can be used in both authentication and cryptography applications.

We also introduce several new techniques that have not been previously described, including a mechanism to eliminate voltage trends or 'bias' in the power grid voltage measurements, as well as a voltage threshold and majority voting scheme to identify and exclude unstable bits. The former is applicable to any type of PUF, and the latter is proposed as an alternative to error correction [5] and Helper Data schemes [24]. We demonstrate that both of these schemes provide a significant improvement to inter-chip Hamming Distance and the results obtained from NIST statistical tests.

2 Background

Random bit strings form the basis for encryption, iden-

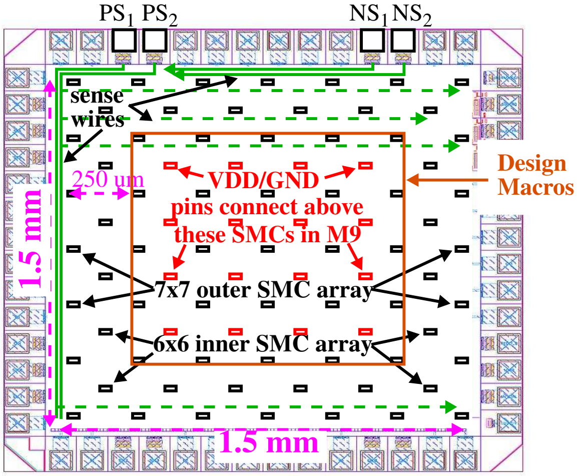

Fig. 1. a) Block diagram of 90 nm chips, with voltage sense pads along top and two arrays of SMCs, a 7x7 outer array and a 6x6 inner array.

tification, authentication and feature activation in hardware security. The introduction of the PUF as a mechanism to generate random bit strings began in [4] and [5], although their use as chip identifiers began a couple years earlier [2]. Since their introduction, there have been many proposed architectures that are promising for PUF implementations, including those that leverage variations in transistor threshold voltages [2-3], in speckle patterns [4], in delay chains and ROs [4-12+others], in thin-film transistors [13], in SRAMs [14+others], in leakage current [15+others], in metal resistance [16], in optics and phase change [17], in sensors [18], in switching variations [19], in sub-threshold design [20], in ROMs [21], using lithography effects [22], and aging [23].

We investigate the power grid (PG) PUF proposed in [16] using experimental data obtained from a much larger set of challenges, from measurements on multiple metal layers and using chips fabricated in both 65 and 90 nm technologies. We also compare the PG PUF against a second PUF that is designed to leverage transistor on-resistance variations (similar to the PUF primitive proposed in [2]).

3 Experiment Setup

3.1 Test Chip Architecture: 90 nm Chips

Fig. 1(a) gives a block diagram of the 90 nm test chip architecture. The chip padframe consists of 56 I/Os, and surrounds a chip area of approx. 1.5 mm x 1.5 mm. Four PADs labeled PS$_1$, PS$_2$, NS$_1$ and NS$_2$ along the top of the figure refer to *voltage sense* connections, the ‘P’ version for sensing voltages near V$_{DD}$ and the ‘N’ version for voltages near GND. These four terminals wire onto the chip and connect to 85 copies of a *Stimulus/Measure circuit* (SMC). The SMCs are distributed across the entire chip (see small rectangles) as two arrays, a 7x7 outer array and a 6x6 inner array. Although not shown, a scan chain connects serially to each of the SMCs to allow each of them to be controlled.

The schematic diagram of the SMC is shown in Fig. 2. A pair of large ‘shorting transistors’, capable of sinking approx. 10 mA of current through the power grid when enabled, are shown along the bottom of the figure[1]. A set of 16 ‘pseudo’ pass gates (hereafter referred to as transmissions gates or **TGs**) serve as *voltage sense* devices. Eight of the TGs connect to 8 (of the 9) metal layers that define the V$_{DD}$ stack-up of the power grid, as shown on the left side of Fig. 2, while the other 8 connect to the GND stack-up. Scan FFs and 3-to-8 decoders allow exactly one of the pass gates to be enabled in each of the stack-ups.

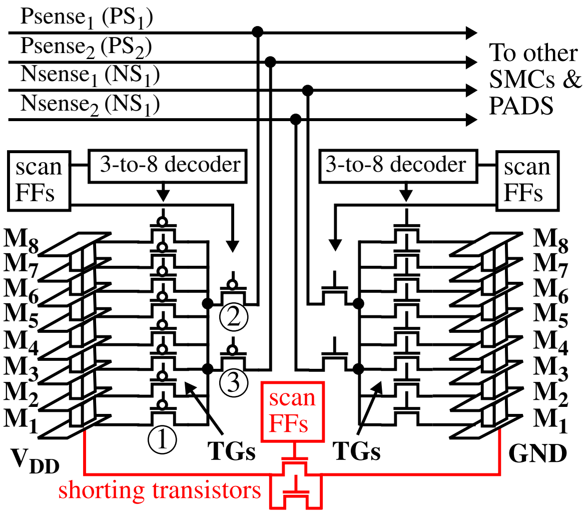

Fig. 2. SMC schematic in 90 nm chips.

Two additional TGs connect to the drains of the 8 stack-up TGs, labeled as ‘2’ and ‘3’ in Fig. 2, one pair for V$_{DD}$ and one pair for GND. Separate scan FFs control their connection to the chip-wide wires that route to the P/NS$_x$ pins of Fig. 1. This configuration and control mechanism allows any two V$_{DD}$ and any two GND voltages to be measured simultaneously using off-chip voltmeters. We refer to these experiments using **PG90**, for power grid 90 nm chips.

Although the layout of the power grid is not shown, approx. 20% of the routing resources are used to define it, as would be typical of a high-performance commercial power grid. Moreover, the metal wires defining the power grid are at least **3 times wider** than the minimum width, and **via arrays** (as opposed to single vias) are used to connect one metal layer to the next. The low resistance associated with these wires and via arrays produces voltage drops in some experiments of 500 µV or less. Although our off-chip instrumentation can measure voltage drops at high resolution (approx. 5 µV), these levels will challenge the capabilities of on-chip instrumentation. We discuss solutions to these issues and others in the following sections.

While carrying out experiments on the 90 nm chips, we realized that the regularity in the architecture of the SMC can be used to derive another type of PUF. In particular, if the voltmeters connected to the PS$_1$ and NS$_1$ pads are replaced with voltage sources, with **force** voltages set to a value below (for PS$_1$) and above (for NS$_1$) the supply voltages, then a voltage divider is created between two identical pass-gates. For example, the TGs labeled “1” and “2” in

[1] The resulting voltage drop/rise on the V$_{DD}$ and GND grid, resp. is approx. 10 mV.

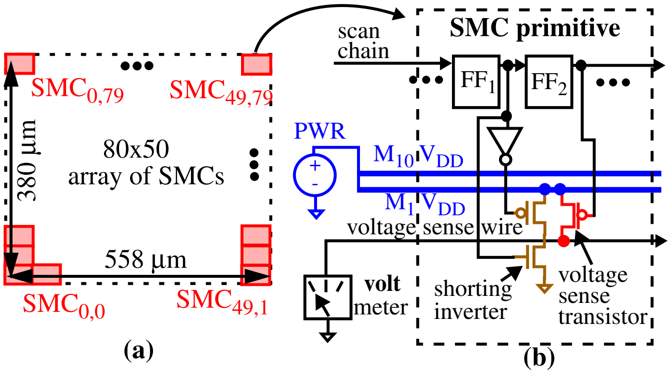

Fig. 3. a) Block diagram of 65 nm chip and (b) details of the SMC.

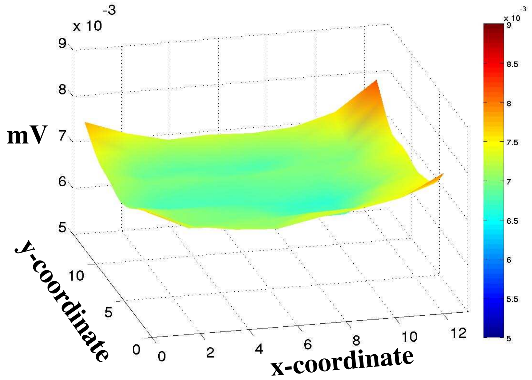

Fig. 4. V_{DD} profile using SMCs of a 90 nm chip.

Fig. 2 form a voltage divider (assuming both are enabled) when V_{DD} is set to 1.2 V and PS_1 is driven to 0.6 V. The voltage on the node between TG "1" and "2" can be sensed with TG "3". The on-resistances of the TGs determine how much of the 600 mV falls across TG "1". Random variations in the on-resistances of the TGs in the stack will change the measured voltage as different TGs are enabled. These voltages can be compared in various combinations to produce a bit string for each chip. We refer to these experiments as **TG90**.

3.2 Test Chip Architecture: 65 nm Chips

The 65 nm test chip architecture is shown as a block diagram in Fig. 3(a). A 80x50 array of SMCs are distributed, in close proximity, over a region that spans 380 µm by 560 µm. The power grid is wired in a mesh configuration over 10 metal layers using wide metal wires and via arrays. The details of the SMC are shown in Fig. 3(b). Each consists of a shorting inverter, a voltage sense transistor and two scan FFs. The shorting inverter draws approx. 1 mA and introduces a 5-10 mV drop on the V_{DD} grid. The single sense transistor allows only M1 voltages to be sensed. We refer to these experiments as **PG65**.

3.3 Challenge Scenarios

There are several 'challenge' scenarios possible in the PG90 and PG65 experiments. The basic approach we take in this paper is to enable the shorting device(s) within each SMC, as well as the corresponding pass gate(s), one at a time, and then measure the voltage drop/rise produced at each location. For the TG90 experiments, each challenge enables one of the pass-gates in the stack (see "1" in Fig. 2) and a pair of pass-gates that connect to the global force and sense wires (see "2" and "3" in Fig. 2).

Each of these voltages can be compared with other voltages in various combinations to produce a bit string. We focus our analysis on bit strings generated by using each voltage in *(n-1)* comparisons, where *n* is the total number of voltages measured from one chip. Bit strings constructed in this manner are referred to as *all combinations* or **AC**.

As is customary, we randomize the order in which the comparisons are made. On chip, this can be accomplished using an LFSR and a seed. The process is modeled in our experiments using the functions *srand(seed)* and *rand()* from the C programming library. In order to show the insensitivity of the bit strings to the value of the seed, we report statistical results using 10 different seeds.

In addition to randomizing the order of the pairings, we found that periodically inverting the output bit produced better results. In particular, inverting every group of three bits worked well for both the PG90 and PG65 experiments. For example, given a randomized set of pairings numbered 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, etc., the bits for pairings numbered 3, 4, 5, 9, 10, 11, etc. are inverted.

4 Experimental Techniques

4.1 Bias Issues

The voltages measured from the chips in our experiments consist of three basic components: bias, regional variation and noise. From the PUF perspective, only the regional variation component is important, and the other two components actually work to reduce randomness and stability, resp. Bias is a systematic voltage trend that is introduced by, e.g., a non-uniform distribution of power port connections to the power grid (the case for the PG90 chips) or a non-uniform power grid mesh (the case for the PG65 chips). Any type of systematic voltage trend will produce bits that are biased to 0 or 1 across chips, and needs to be reduced or eliminated in practice. We first discuss the biases that exist in our data sets and then methods of dealing with them.

Fig. 4 shows the *voltage drop profile* obtained from one of the 90 nm chips as each SMC is enabled, one at a time. The voltage drop profile is derived from the M1 sense transistors on the V_{DD} grid. The (x,y)-plane in the figure represents the position of the SMC in the 2-D array. From the bowl-like surface, it is clear that the voltage drops are larger along the edges of the power grid than in the center. This systematic voltage trend is caused by the non-uniform distribution of the power port connections, which from Fig. 1 are located over the 'Design Macros' in the center region of the chip, i.e., there are no power ports along the edges.

A bias also exists across the array of SMCs when the TGs are used to generate a bit string. In this case, the bias is introduced by the parasitic resistance of the 4 globally routed sense wires as shown in Fig. 1. When the P/NS_1 pins are **driven** with voltage sources, the parasitic resistance of the on-chip wires impacts the fraction of the 600 mV that falls across TG "1".

Although much less apparent, a small bias also exists in the voltage drop profile shown in Fig. 5, which is derived

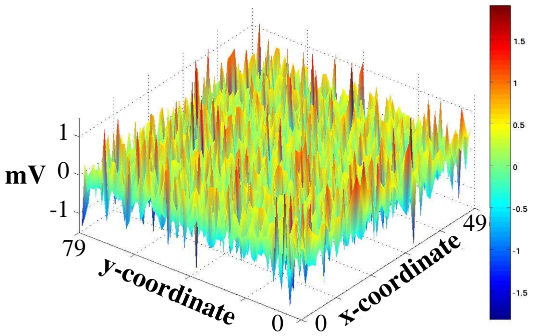

Fig. 5. Voltage drops from 4,000 SMCs on a PG65 chip.

for one of the 65 nm chips. Here, the voltage drops computed for the SMCs are plotted for each of the 4,000 elements of the array shown in Fig. 3(a). The majority of the voltage variations (approx. +/- 1 mV from Fig. 5) is introduced by regional resistance variations in the metal defining the power grid. However, a small "saw-tooth-shaped" bias exists between adjacent rows of approx. 200 uV, which is introduced by a pattern in the power grid metal mesh that is different for the even and odd rows of the array. This subtle pattern is revealed by computing an average value of the voltages measured across each row, for each of the 80 rows in the array. Averaging reduces the random variations and allows the bias effect to be more easily observed. Fig. 6 plots the average values on the y-axis for each row identified along the x-axis. It is clear the average voltages are smaller for even-numbered rows, than for odd-numbered rows. Moreover, the points labeled "edge effects" reveal a second source of bias that is introduced by the power grid architecture. In this case, the increase in the voltage drops/ rises is caused by the close proximity of these SMCs to the edges of the power grid.

4.2 Dealing with Bias

There are several ways of eliminating the bias from the voltage measurements in these chips. The multi-layered architecture of the SMCs used in the PG90 chips allow voltage drops/rises to be computed across *each of the metal layers*. These **inter-layer** voltage drops/rises can be computed by subtracting pair-wise, the voltages measured from consecutive metal layers, i.e., V_{M1} - V_{M2}, V_{M2} - V_{M3}, etc. Voltage *differences* allow the PUF to leverage the independent resistance variations that occur in each of the metal layers of the power grid, and given their differential nature, significantly reduces bias effects such as those discussed in reference to Fig. 4. A similar voltage difference approach can be used in the TG90 experiments.

In the PG65 chips, each SMC has only one voltage sense transistor connected to the V_{DD} grid, and therefore, computing inter-layer voltage drops is not possible. In this case, we *avoid* the bias by restricting voltage comparisons between SMCs positioned on every other row (to deal with the "saw-tooth" effect) and eliminate those positioned along the edges of the array (to deal with "edge effects"). In particular, we eliminate the SMCs along the left and right columns, the bottom row and the top two rows. This reduces the size of the array to 77x48, and restricts comparisons between SMCs on the 39 odd numbered rows and the 38 even numbered rows. We refer to this scheme as **bias avoidance**.

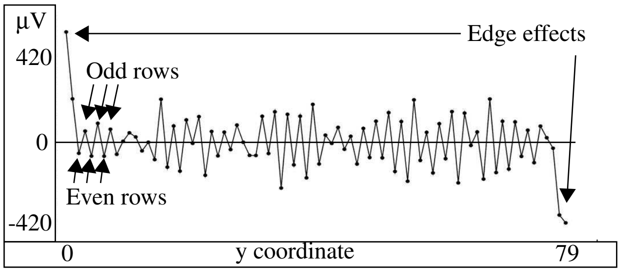

Fig. 6. Average voltage drops across 80 rows of PG65.

We also propose a more general technique to eliminate bias which is applicable to ***any type*** of PUF measurement, including, for example, RO frequencies and delays. For PUFs based on voltage measurements, the method first divides the voltage drops by a value that upper bounds the noise level. The general idea here is to eliminate the smaller noise variations, effectively reducing the range of values observed in a set of repeated samples for a given challenge to 1 or 2 distinct values. Once the voltage drops are re-digitized, the remainder from applying a modulus is used in the comparison operation to produce the bit. The modulus is chosen to preserve the regional (high frequency) variation while simultaneously 'trimming off' the bias effects. This approach is also applicable for PUFs that compare digital values, e.g., counter values in RO-based PUFs. In this case, the modulus operation eliminates systematic, across chip shifts in frequency[1].

4.3 Bit Stability

In our experiments, we found that **unstable** bits, defined as bits that are susceptible to 'flipping' because their voltages are very similar, actually reduce several quality metrics associated with the overall bit string, including inter-chip HD and NIST statistical test scores. Moreover, including unstable bits in the bit string requires the inclusion of error correction [5] and Helper Data schemes [24], that weaken security and increase overhead.

An alternative scheme that is able to identify and discard unstable bits works as follows. First, a process is applied to determine the approx. noise levels, either by using measurements carried out after manufacture or by using an on-chip noise evaluation process. In either case, noise levels can be determined empirically by applying a set of challenges repeatedly and examining the stability of the bit strings produced. In cases where bit flips occur, the magnitude of the difference between the voltages being compared is used to determine a **threshold**, that defines an upper bound on the voltage difference required to ensure bit stability. A safety margin is added to the threshold to account for environmental variations that can later occur in

[1] Trimming off high order bits is equivalent to using a modulus that is a power-of-two. If finer control is required, a modulus that is not a power-of-two can be used.

the field.

The usage scenario that enables this process to be applied in situations where exact regeneration of a bit string is required works as follows. During the initial bit string generation, the threshold method is used to identify the unstable bits. For each unstable bit, its numbered position in the sequence of challenges applied to generate the bit string (for a given seed) is recorded in non-volatile memory. Later, during regeneration, thresholding is disabled and the non-volatile memory is consulted to determine which challenges to skip during bit generation. To further enhance protection against one-time events, such as voltage spikes or scan configuration errors, repeated sampling and majority voting can be used in the regeneration process to determine the final bit string. We investigate several aspects of this process in the experimental results section below.

4.4 Statistical Characterization of the Bit Strings

Several statistical techniques are applied to evaluate the 'quality' of the bit strings produced by the PG and TG PUFs. Hamming Distance (HD) is defined as the number of bits that are different when two bit strings are compared. An **average inter-chip HD** is defined by computing the HDs across all combinations of bit strings from the chip population. The best result occurs when exactly half of the bits from any two bit strings are different, i.e., when the average HD, expressed as a percentage, is 50%. An intra-chip HD is computed using all combinations of bit strings obtained from **one** chip in the population under repeated sampling. An **average intra-chip HD** is computed by averaging all of the individual intra-chip HDs. The ideal value in this case is 0%, i.e., each chip is able to reproduce the same bit string.

The statistical tests developed at NIST are also applied at significance level of 0.01 (the default) [1]. In general, the NIST tests look for 'patterns' in the bit strings that are not likely to be found at all or above a given frequency in a 'truly random' bit string. For example, long or short strings of 0's and 1's, or specific patterns repeated in many places in the bit string work against randomness[1]. The output of the NIST statistical evaluation engine is the *number of chips* that pass the *null hypothesis* for a given test. The null hypothesis is specified as the condition in which the bit-string-under-test is random. Therefore, a good result is obtained when the number of chips that pass the null hypothesis is large.

5 Experimental Results

5.1 PG90 Experiments

We collected data from 60 copies of the 90 nm chips at room temperature and generated bit strings using the AC scenario described in Section 3.3. Although the SMC is designed to sense voltages in any of the first 8 metal layers, the voltage drops above M4 are smaller than those on the lower metal layers. This occurs because the metal wires in the upper metal layers are much wider (and thicker) than wires in the lower portion of the grids. Given the concerns we expressed in Section 3.1 regarding the capabilities of on-chip instrumentation, we restrict our analysis to voltages measured in the lower 4 metal layers.

The focus of the PG90 experiments is on inter-layer resistance variations. Inter-metal layer resistance variations can be captured by computing *voltage differences* between consecutive metal layers. The bit string is then produced by comparing these voltage *differences*, e.g., if V_{M1}-V_{M2} in the V_{DD} stack-up at SMC_1 is greater than the voltage V_{M1}-V_{M2} in the V_{DD} stack-up at SMC_2, then a '1' is generated, otherwise a '0'. Given these constraints, it is possible to produce bit strings of length 21,420 for each chip, defined with 85 SMCs as n*(n-1)/2 = 85*84/2 = 3,570 bits per inter-metal layer per grid times 3 inter-metal layers times 2 grids. These experiments are referred to as **DIFF**. For comparison purposes, we also carry out a similar analysis using the absolute voltages (referred to as **ABS**). In this case, the number of bits increases to 28,560 bits because there are 4 metal layers.

As indicated in Section 4.3, our methodology eliminates unstable bits by comparing the voltage difference of the pairing with a threshold. To increase confidence, repeated sampling is also employed during the bit stability evaluation process. For a bit to be considered stable, the voltage difference must exceed the threshold in all samples. For the DIFF experiments, a 25 uV threshold was sufficient to ensure that no bit flips occurred for voltage pairings in which the voltage difference across all samples (5 in this case) and chips was larger than this value. The threshold increased to 50 uV for the ABS analysis. Bear in mind that the threshold actually guards against voltage variations as large as the threshold ***in each voltage*** of the pairing. For example, a voltage pairing defined as (6.000 mV, 6.050 mV) in the first sample would need to vary to values larger than (6.050 mV, 6.000 mV) in all subsequent samples to violate a 50 uV threshold model.

The distribution of the HDs for the DIFF and ABS analyses are shown in Figs. 7(a) and (b), resp. HD is plotted along the x-axis against the number of instances on the y-axis. The total number of instances is given by all combinations of the chips' bit strings, i.e., 60*59/2 = 1,770. After removing unstable bits using the algorithm described above, the bit string sizes reduce by approx. 46% on average to 11,600 bits for DIFF and by approx. 12% to 25,121 bits for ABS. Bear in mind that these percentages do NOT represent the number of bit flips. The actual average intra-chip HDs are 2.63% and 0.61%, resp. The size of the bit strings used in the HD analysis is smaller still at 9,592 and 24,446 resp. This adjustment is necessary because the HD analysis must be carried out on bit strings of equal length. To accomplish this, the chip with the shortest stable bit string is used to define the length of all bit strings.

Although the number of bits discarded as unstable using the threshold method is relatively large, the benefits of constructing a stable bit string in this fashion are significant. First, the average inter-chip HD for DIFF improves from 38.2% (not shown but with unstable bits included) to 49.97% as shown in the figure. For ABS, the improvement is even more dramatic, from 8.4% to 49.79%. The superimposed Gaussian curve on the DIFF distribution of Fig. 7(a) illustrates the distribution is close to ideal, and reflects the power of differential analysis. The ABS distribution, on the

[1] See [1] for details concerning NIST tests.

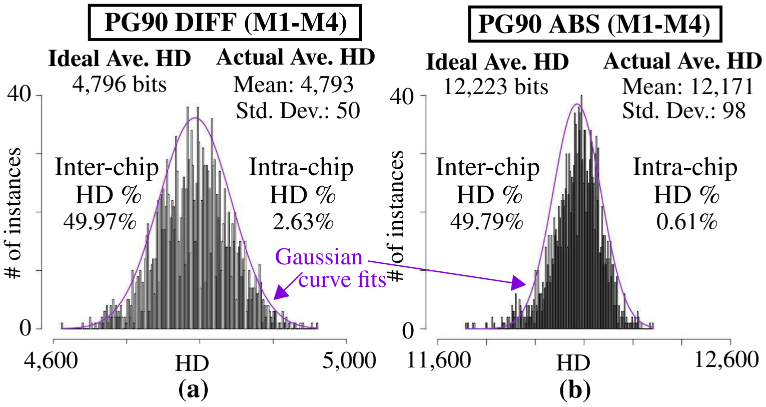

Fig. 7. Distribution of HDs using (a) stable DIFF (M1-M4) (b) stable ABS (M1-M4) bit strings from PG90 exps.

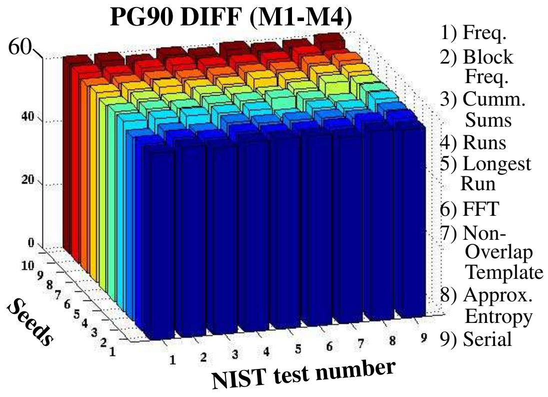

Fig. 8. NIST test suite statistics using DIFF (M1-M4) stable bit strings in PG90 exps.

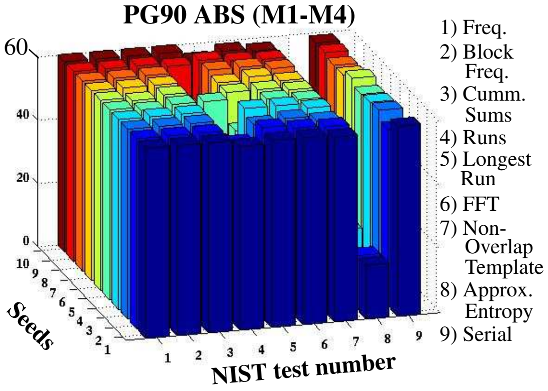

Fig. 9. NIST test suite statistics using ABS (M1-M4) stable bit strings in PG90 exps.

other hand, is skewed somewhat to the left, which indicates that a component of the bias discussed earlier in reference to Fig. 4 is still present.

Fig. 8 shows a bargraph of the number of passing chips (z-axis) for a subset of the NIST tests (x-axis) using 10 different seeds (y-axis). Only those tests applicable to bit strings of length 9,592 are applied[1]. As indicated earlier, the best result is a 'pass' for all 60 chips. Although difficult to see, an ideal score of 60 was achieved in 40 (of the 90) cases. The worst result occurs for the NonOverlapping Template test. The height of the bars for this test represent the average number of passing chips across 148 templates. Although the chips performed very well on this test overall, there are 37 cases (of a total of 1,480) where the minimum number of passing chips was not met (57 is required according to NIST). The smallest number of passing chips among these fails is 54, with the majority (20) failing by only 1 chip. In a second set of seed trials (not shown) a couple of other tests failed, e.g., Cumm. Sums test, but never by more than 2 chips. Moreover, **all of Pvalue-of-the-Pvalues tests passed**, indicating the P-values are uniformly distributed between 0.0 and 1.0. In contrast, the results for ABS data shown in Fig. 9 reveal that the bit strings fail the Runs and Approx. Entropy tests by as many as 50 chips in some instances. Overall, these results indicate the bit strings generated from the DIFF (M1-M4) version of the PG PUF are of cryptographic quality.

5.2 PG65 Experiments

As described in Section 4.2, the **bias avoidance** scheme pairs voltages from 39 odd-numbered rows + 38 even-numbered rows in all combinations to produce bit strings of length 3,413,832 in the PG65 experiments. We repeatedly applied the challenges 10 times to each of the 58 chips at 25^{o}C, and used a voltage threshold of 250 uV to eliminate all bits in the repeated samples. As indicated earlier, only V_{DD} voltages in M1 can be sensed in the 65 nm chips, so the analysis is classified as ABS.

The distribution of the inter-chip HDs is shown in Fig. 10(a). The length of the stable bit strings are 2,052,003 bits on average, which represents approx. a 40% decrease in the original length. The intra-chip hamming distance is approx. 1.2%, which indicates that a significant number of bits that are discarded as unstable do not flip in any of the 10 samples. The benefits of discarding these bits are, once again, the improvements obtained in bit string quality and the elimination of on-chip error correction hardware.

In order to illustrate the improvement in quality, Fig. 10(b) shows the distribution of the inter-chip HDs using the full length 3,413,832-bit strings. The average inter-chip HD drops from 50.0002% to 49.0851% when the unstable bits are included. Moreover, the standard deviation of the distribution is significantly larger, e.g., 624 vs. 26,353.

The bargraphs in Figs. 11 and 12 gives the NIST statistical test results for the stable and unstable bit strings, resp. The results from all 15 NIST tests are displayed along the x-axis, for 10 different seeds plotted along the y-axis. The ideal value is 58 for all tests except NIST tests 12 and 13[2]. A numerical analysis of the data indicates that 58 of the bars reach the ideal value in Fig. 11 while only 35 achieve this status in Fig. 12.

[1] For Cumm. Sums, NonOverlapp. Template and Serial, NIST software outputs 2, 148 and 2 results, resp. The bar heights for these tests represent the average values.

[2] Note: NIST tests 12 and 13 are NOT based on the number of chips, see [1] for details.

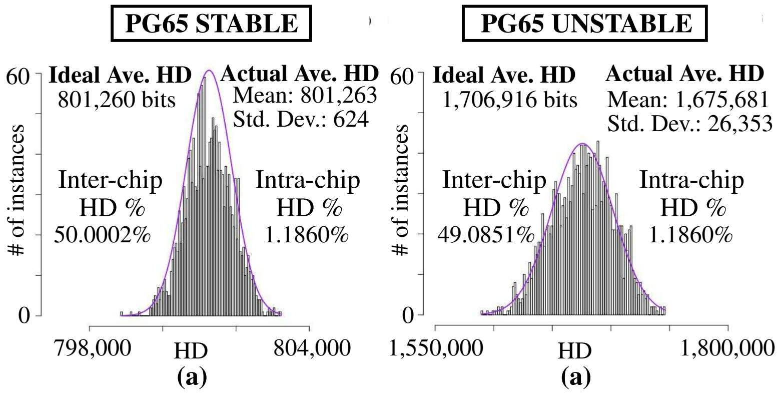

Fig. 10. Distribution of HDs using (a) stable ABS (b) unstable ABS bit strings from PG65 exps.

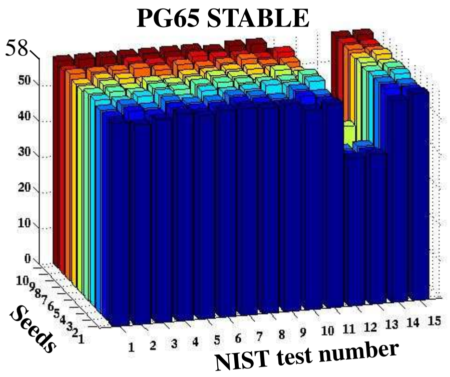

Fig. 11. NIST test suite statistics using stable bit strings for PG65 exps.

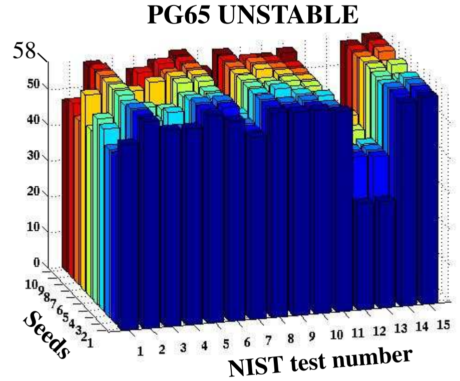

Fig. 12. NIST test suite statistics using unstable bit strings for PG65 exps.

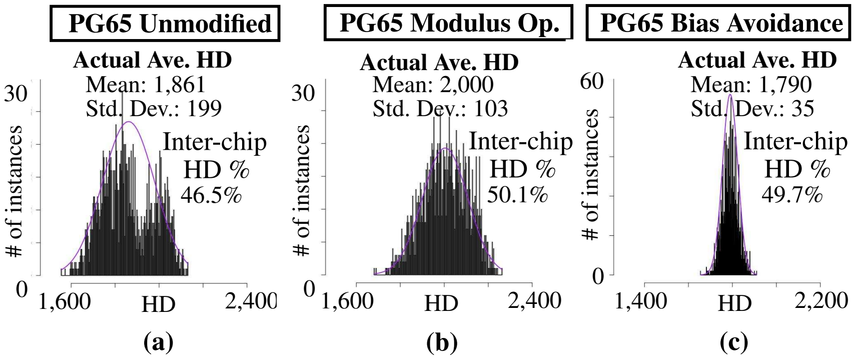

Fig. 13. HD analysis of bit strings using unmodified voltages (a) with modulus op. (b) and using bias avoidance (c) for PG65 exps.

The stable bit strings pass all tests except for 7 (of a total of 1,480) NonOverLapping Template tests. 6 of the 7 fails are by only 1 chip (54 chips passed instead of the required 55) and 1 failed by 2 chips. In addition, 3 PValue-of-the-Pvalue tests failed in this group of 1,480 tests. Moreover, three of the seeds passed every test. Overall, these results indicate that the stable bit strings are high quality and can be used in cryptographic applications.

The larger number of fails in the unstable bit string results of Fig. 12 indicate that these bit strings are lower in quality. For example, only 1 seed passed the NIST Frequency test, which measures the balance of '0's and '1's in the bit strings. Overall, 50 of the 150 (10 seeds * 15 NIST tests) fail. However, the fewest number of passing chips is 41, which is better than the worst case result obtained in the PG90 ABS M1-M4 analysis described in Section 5.1.

5.2.1 Modulus Technique for Bias

We investigate a second strategy for dealing with bias using a subset of the data from the PG65 experiments where bias is particularly evident. In these experiments, we do not use the bias avoidance scheme. The inter-chip distribution of HDs shown in Fig. 13(a) is derived from the 4,000 SMCs paired with their 'vertical' neighbor. Bias is reflected here in a lower-than-ideal average HD of 46.5% and in the bimodal shape characteristic of the distribution.

The distribution labeled 'Modulus Op." shown in Fig. 13(b) is derived using the same pairings. The voltages in this case are first manipulated (as discussed in Section 4.2) by dividing by a noise threshold of 350 uV and then using the remainder from a modulus operation (11 is used in this analysis) in the bit generation process. The removal of the bias improves the average HD to 50.1% and re-shapes the distribution to conform better to a Gaussian.

Although this technique is effective, it is no substitute for a well-designed architecture that minimizes bias. Fig. 13(c) shows the distribution obtained when the **bias avoidance** scheme is used to illustrate this concept. Note that the length of the bit strings is smaller (3,600) because of the pairing constraints. Although the average HD is slightly less than ideal at 49.7%, the shape and standard deviation of the distribution are both superior to those of Fig. 13(b).

5.3 Temperature Voltage Analysis

In a set of preliminary experiments, we collected additional data from one of the chips at 0^{o}C and 125^{o}C, and at +/- 10% of the supply voltage for each of the 3 temperatures. The data from the 125^{o}C experiments introduced 3 bit flips in the stable bits using the 250 uV threshold, and required a threshold of 300 uV to eliminate all bit flips. The primary reason for the additional bit flips at 125^{o}C is due to the increase in leakage current into the voltage sense wire, which connects to 4,000 sense transistors, 3,999 of which are in the off-state. This deficiency in the sense transistor network is addressed in the 90 nm chips by including a second sense transistor in series with the first as shown in Fig. 2. We do not expect to encounter this issue in the 90 nm

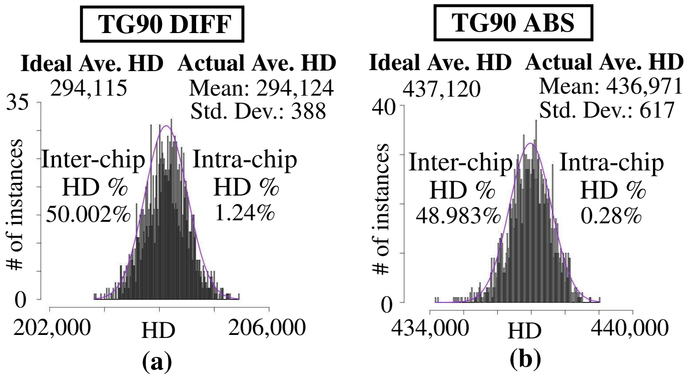

Fig. 14. Distribution of HDs using (a) stable DIFF (b) stable ABS bit strings from TG90 exps.

chips. A full temperature analysis using both sets of chips will be included in a future publication to validate this hypothesis.

5.4 TG90 Experiments

For the TG90 experiments, bit generation is expanded to include all 8 pass gates within the stacks of each SMC (the PG90 experiments restricted analysis to the lower 4 metal layers). The voltage threshold is set to 1mV to prevent bit flips in the stable bit analysis, which reduces the average bit string lengths by 15.3% and 4.3% for the DIFF and ABS analyses, resp.

The inter-chip distributions of the HDs are shown in Fig. 14(a) and (b) for DIFF and ABS, resp. The bias issue associated with the sense wire routing appears to be significantly reduced using the threshold method, as depicted by shape of the distribution and results given in Fig. 14(b). However, similar to the PG90 analysis, the shape of the DIFF distribution is a better fit to a Gaussian than the ABS distribution and the Std. Dev. is smaller, e.g., 388 vs. 617.

The length of the bit strings allows 11 of the NIST statistical tests to be performed (all except Overlapping Template, RandomExcursions, RandomExcursionsVariant and Linear Complexity). The results are summarized as follows. The ABS bit strings do poorly, producing 0 passing chips on several tests including Runs, Longest Runs, Approx. Entropy and Serial for all seeds. The poor performance is caused by the large bias that remains in the data and demonstrates that the voltage threshold technique is limited in how much bias it can remove. In contrast, the DIFF bit strings pass all tests except 2 NonOverlapping Template tests, both of which fail by only 1 chip. This result clearly demonstrates the power of differential analysis to extract randomness and eliminate the adverse effects of bias.

6 Conclusions

We analyze statistical quality metrics of bit strings produced from three PUF implementations, two that leverage resistance variations in the power grid and a second that leverages variations in transistor on-resistance. Experimental results are reported for chips fabricated in 90 nm and 65 nm technologies. A voltage threshold technique is investigated that eliminates unstable bits and is shown to significantly improve inter-chip hamming distance and the results from NIST statistical tests. All three of the PUF primitives are shown to generate cryptographic quality bit strings of length upto 1.6M bits.

7 Acknowledgements

Dhruva Acharyya and Erik Volkerink, Verigy Inc.
Kanak Agarwal, Sani Nassif, IBM ARL
Work supported by NSF grant CNS: 1018748
90 nm chips fabricated under MOSIS MEP program

References

[1] NIST: Computer Security Division, Statistical Tests, http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html

[2] K. Lofstrom, *et al.*, "IC Identification Circuits using Device Mismatch," *SSCC*, 2000, pp. 372-373.

[3] D. Puntin, *et al.*, "CMOS Unclonable System for Secure Authentication based on Device Variability", *SSCC*, 2008, pp. 130-133.

[4] R. S. Pappu, *et al.*, "Physical One-Way Functions," *Science*, 297(6), 2002, pp. 2026-2030.

[5] B. Gassend, *et al.*, "Controlled Physical Random Functions," *Conference on Computer Security Applications*, 2002.

[6] M. Majzoobi, *et al.*, "Lightweight Secure PUFs", *ICCAD*, 2008.

[7] E. Ozturk, *et al.*, "Physical Unclonable Function with Tristate Buffers," *Circuits and Systems*, 2008, pp. 3194-3197.

[8] G. Qu and C. Yin, "Temperature-Aware Cooperative Ring Oscillator PUF", *Workshop on HOST,* 2009, pp. 36-42.

[9] A. Maiti and P.Schaumont, "Improving the Quality of a Physical Unclonable Function using Configurable Ring Oscillators", *FPLA*, 2009. pp. 703-707.

[10] Y. Hori, *et al.*, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs", *Reconfig. Comp. and FPGAs*, 2010 , pp. 298-303.

[11] C. Costea, *et al.*, "Analysis and Enhancement of Ring Oscillators Based Physical Unclonable Functions in FPGAs", *Reconfig. Comp. and FPGAs,* 2010, pp. 262-267.

[12] C. Qingqing, *et al.*, "The Bistable Ring PUF: A new architecture for Strong Physical Unclonable Functions", *HOST*, 2011, pp. 134-141.

[13] S. Maeda, *et al.*, "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] J. Guajardo, *et al.*, "Physical Unclonable Functions and Public Key Crypto for FPGA IP Protection," *FPLA*, 2007, 189-195.

[15] Y. Alkabani, *et al.*, "Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach," *Information Hiding*, 2008.

[16] R. Helinski, *et al.*, "Physical Unclonable Function Defined Using Power Distribution System Equivalent Resistance Variations", *DAC*, 2009, pp. 676-681.

[17] K. Kursawe, *et al.*, "Reconfigurable Physical Unclonable Functions - Enabling Technology for Tamper-Resistant Storage", *HOST*, 2009, pp.22-29.

[18] K. Rosenfeld, *et al.*, "Sensor Physical Unclonable Functions", *HOST*, 2010, pp. 112-117.

[19] W. Xiaoxiao and M. Tehranipoor, "Novel Physical Unclonable Function with Process and Environmental Variations", *DATE*, 2010, pp. 1065-1070.

[20] L. Lin, *et al.*, "Low-Power Sub-Threshold Design of Secure Physical Unclonable Functions", *LPED*, 2010, pp. 43-48.

[21] U. Ruhrmair, *et al.*, "Applications of High-Capacity Crossbar Memories in Cryptography", *Trans. on Nanotechnology*, Volume: 10 , Issue: 3, 2011, pp. 489-498.

[22] A. Sreedhar and S. Kundu, "Physically Unclonable Functions for Embeded Security based on Lithographic Variation", *DATE*, 2011, pp. 1-6.

[23] S. Meguerdichian and M. Potkonjak, "Device Aging-Based Physically Unclonable Functions", *DAC*, 2011, pp. 288-289

[24] Y. Dodis, *et al.*, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", SIAM J. Comput., 38(1):97-139, 2008.