A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations

Ying Su, Jeremy Holleman, *Student Member, IEEE*, and Brian P. Otis, *Member, IEEE*

***Abstract*—A 128-bit, 1.6 pJ/bit, 96% stable chip ID generation circuit utilizing process variations is designed in a 0.13 μm CMOS process. The circuit consumes 162 nW from a 1 V supply at low readout frequencies and 1.6 μW at 1 Mb/s. Cross-coupled logic gates were employed to simultaneously generate, amplify, and digitize the random circuit offset to create a stable unique digital chip ID code. A thorough statistical analysis is presented in order to explore the ID circuit reliability and stability. Two ID generators with different layout techniques were designed and fabricated to provide a performance comparison of power consumption, ID stability, and ID statistical robustness.**

***Index Terms*—Chip identification, low-power digital electronics, mismatch, process variations, RFID, sensor networks.**

I. Introduction

MANY integrated circuit applications require a unique identification number (ID) on each die that can be read anytime during the lifetime of the chip. A robust, read-only ID is important for labeling RFID tags, addressing low power wireless sensor nodes, integrated circuit process quality control, tracking implantable electronic devices, and enabling secure documentation. Traditional methods of writing addresses into read only memories (ROM) involve post-fabrication external programming, such as laser fuses or E-fuses. These technologies incur additional expense or process modifications. Recently, Lofstrom *et al.* proposed the extraction of a unique and repeatable identification number from random variable mismatch [1], which led to new testing methodology capability, including inexpensive identification of packaged die [2]. Published results in this area suggest that it is possible to extract a unique fingerprint from each chip by comparing variations in transistor current flow or digital path delay variations that exist from die to die [1], [3]. This technique has the additional benefit that an ID number based on process variations is difficult to counterfeit, even if manufactured identically, since the physical variations creating the ID are necessarily below the resolution of the manufacturing equipment. Methods that utilize random process variables must exhibit the following characteristics to be useful in a production environment:

- The ID circuit must generate a digital output to form a binary ID code.
- The ID code must be repeatable and reliable over supply, temperature, aging and thermal noise.
- The ID code length and stability must allow high probability of correct identification of each die.
- The ID circuit must exhibit low power consumption and require no calibration.

In this work, we propose a new chip ID generating circuit that relies on cross-coupled logic gate transistor offset voltages to provide a robust 128-bit ID number. Utilizing the large gain provided by positive feedback in a digital latch, we achieve significant improvements in readout speed and power consumption over existing designs, allowing a minimum power consumption of 162 nW at low clock rates and an energy-per-bit of 1.6 pJ/bit at 1 Mb/s.

Section II of this paper describes the ID generating circuit topology and system architecture. Section III presents a statistical analysis of the ID code reliability and stability. Possible solutions to some of the potential ID reliability problems are also addressed in this section. Section IV describes circuit design and layout techniques we employed, and explores the effects of negative bias temperature instability (NBTI) and aging and provides some possible solutions. Measurement results from experimental chips are presented in Section V, followed by concluding remarks in Section VI.

II. Circuit Topology

Each bit of the identification number is extracted by comparing the uncorrelated threshold voltage $(\mathrm{V_t})$ variation of two different transistors (or sets of transistors). This offset voltage must be amplified and digitized to create a digital ID. To make the digitization circuit compact and efficient, a one bit quantization was chosen. Instead of using an explicit amplifier and comparator to process the offset voltage, we use positive feedback to simultaneously generate the offset, amplify it, and perform a one bit digitization. Each ID cell comprises a latch (comparator) composed of cross-coupled logic gates, as shown in Fig. 1. Initially, both sides of the latch (nodes A and B) are pulled low. As Reset is lowered, each latch evaluates to a state determined by the mismatch of the comparator. This mechanism directly generates logic-level output bits at ID and $\overline{ID}$ corresponding to the input-referred mismatch polarity of the latch. The offset generator and processing circuitry consists of 10 small area transistors and no passive components, allowing each ID cell to contain a processing circuit, resulting in the simultaneous evaluation of all 128-bit ID cells.

Unlike previous implementations, no offset-nulled comparator or low offset amplifier is needed to detect very small mismatch voltage variations, allowing a reduction in the circuit complexity and power dissipation. Our approach relies on the positive feedback inherent in the latch configuration,

Manuscript received April 17, 2007; revised September 5, 2007.

The authors are with the Department of Electrical Engineering, University of Washington, Seattle, WA 98195 USA (e-mail: suying@u.washington.edu).

Digital Object Identifier 10.1109/JSSC.2007.910961

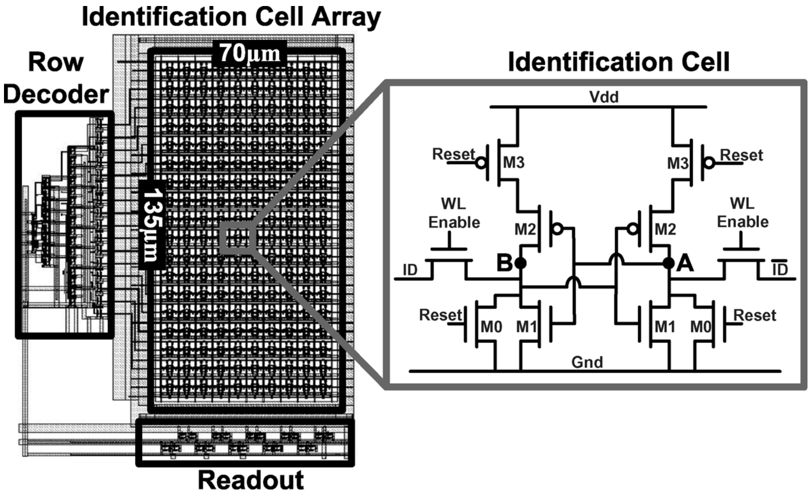

Fig. 1. Simplified ID generator schematic and layout of ID array with perimeter dummy cells.

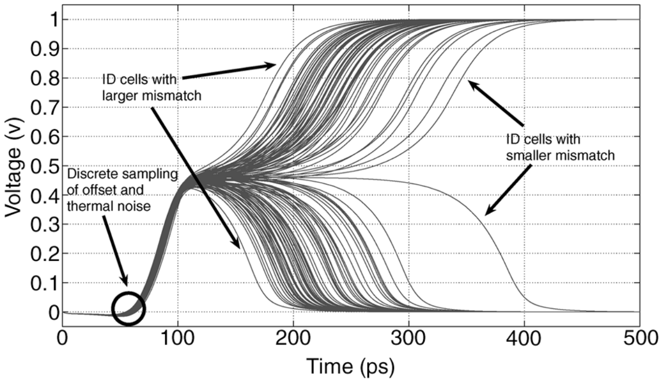

Fig. 2. Monte Carlo simulation of a 128-bit ID cell generator.

allowing large amplification of a zero-mean, high-variance random variable. Fig. 2 shows a Monte Carlo simulation of the 128-bit ID cell array, yielding a random 128-bit ID with an even distribution of logic “1”s and “0”s. As the Reset signal is lowered, pMOS device M2 is turned on and immediately begins to amplify the input to the comparator, which consists of an offset voltage and device noise. Discrete sampling of the ID cell mismatch and thermal noise thus occurs at low voltages. ID cells that have larger mismatch evaluate faster and are less susceptible to thermal noise than those with a smaller mismatch.

The ID circuit architecture is similar to a 128-bit SRAM array. The perimeter of the 8×16 ID cell array is surrounded by 52 dummy ID cells to prevent edge-effects from corrupting the ID statistics. Fig. 1 shows the complete layout of the ID generating circuit. The ID generator circuit consists of a 128-bit ID block, a row decoder and a readout circuit. All ID cells evaluate simultaneously in one clock cycle. Through a row decoder, one clock cycle is used to read out each of the 16 ID words, requiring a total of 17 clock cycles to produce a 128-bit ID.

III. Statistical Analysis

In this section, we develop the statistical analysis to investigate two concerns with this technique:

1) Since the chip ID is determined through a random process, there is a finite probability of an ID collision between chips.
2) Each ID cell must detect a small (on the order of mV) transistor offset in the presence of thermal (and other) noise sources, resulting in a finite percentage of incorrect ID bits.

A. Hamming Distance

The numerical Hamming distance is defined as the summation of the difference bits between any two identification numbers. When the number of ID bits is large, the Hamming distance between two chips should be, on average, half of the total number of bits in the ID (64 in this case). The Hamming distance between two ID numbers for the *same* chip measured on subsequent reads reflects the number of unstable bits. If the offset for a particular latch is small relative to the thermal circuit noise, it will exhibit unstable behavior. Even for a non-zero number of unstable bits, it is possible for the user to positively identify the die if a sufficient ID length is used [1].

B. ID Collision Probability

Unlike a post-fabrication programming method, the ID codes in this work are assigned randomly. Thus, there will be a finite possibility of ID code collision within a given number of chips, even if all bits in the ID code are stable [4]. Modeling the ID collision probability is important for investigating the robustness of this technique in a production environment. Consider X as the number of bits in an ID code, resulting in a total number of available ID codes of 2^X. The probability of ID collision between any two chips is then $1/2^X$. The probability that the nth fabricated chip ID would *not* collide with the existing $n-1$ chips can be shown as

$$1 - \frac{n-1}{2^X}. \tag{1}$$

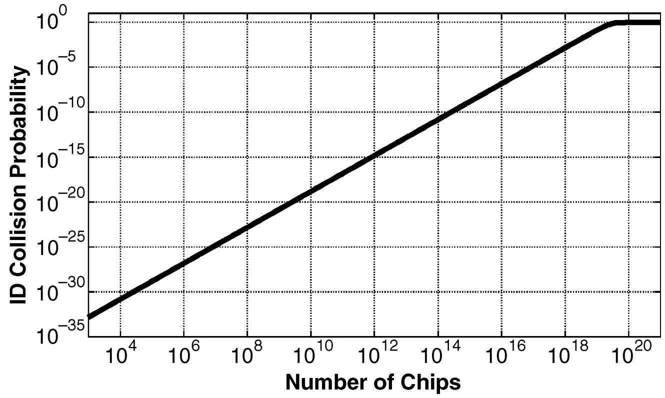

Fig. 3. Probability of ID collision versus number of chips for a randomly assigned 128-bit chip ID.

Thus, the total probability of ID collision across Y chips can be represented as

$$P_{collision} = 1 - \prod_{n=1}^{Y}\left(1 - \frac{n-1}{2^X}\right). \tag{2}$$

This probability model assumes the number of chips (Y) is smaller than the total number of available ID codes (2^X)—a reasonable assumption with a 128-bit ID length. The ID collision probability for a 128-bit ID code versus different number of chips (Y) is shown in Fig. 3. For $Y = 500$ million chips, neglecting any unstable or drifting ID cells, the probability of ID collision is 3.67 e-22. This demonstrates that the use of randomly assigned ID codes is highly reliable since the ID collision probability is vanishingly small.

C. Probability of Misidentification

The previous analysis assumed that all bits in the ID code are stable. However, in reality, a finite number of unstable bits exist in the ID codes since the process variation competes directly with thermal noise during the evaluation process. Analysis and measurements reveal that approximately 4% of the ID bits will exhibit unstable behavior. These unstable bits introduce a possibility of misidentification into the ID read and mapping process. Assume that, at fabrication time, a database is constructed of correct IDs obtained through multiple reads to average out the effects of thermal noise. Now suppose there is a chip k whose correct ID code in the database is C_k. The chip is queried at a later time and produces a code $\hat{C}_k$. The Hamming distance between C_k and $\hat{C}_k$, $HD(C_k, \hat{C}_k)$, represents the number of unstable bits for chip k. A misidentification will occur if there exists a chip l such that the Hamming distance between $(C_l, \hat{C}_k)$ is smaller than or equal to the Hamming distance between $(C_k, \hat{C}_k)$ due to the effect of the unstable bits in $\hat{C}_k$.

$$Misidentification = HD(C_l, \hat{C}_k) \leq HD(C_k, \hat{C}_k). \tag{3}$$

If we pessimistically assume that all unstable bits will always evaluate in the worst possible case (that is, $HD(C_l, \hat{C}_k) = HD(C_k, C_l) - HD(C_k, \hat{C}_k)$), the condition of misidentification can be represented as follows:

$$\begin{aligned} HD(C_k, C_l) - HD(C_k, \hat{C}_k) &\leq HD(C_k, \hat{C}_k) \\ HD(C_k, C_l) &\leq 2 \bullet HD(C_k, \hat{C}_k). \end{aligned} \tag{4}$$

In general, the misidentification condition can be re-written as a cumulative binomial distribution function, where h is a particular Hamming distance and p_{ub} is the fraction of unstable bits:

$$\sum_{h/2}^{h} \binom{h}{h/2} p_{ub}^{h/2} (1 - p_{ub})^{h-h/2}. \tag{5}$$

The total probability of misidentification is the summation of the product between the probability of each Hamming distance and the misidentification chance at that particular Hamming distance. Since the ID length in this work is 128 bits, the possible Hamming distance set would span 0 to 128.

$$\begin{aligned} p_{misid} = \sum_{h=0}^{128} \Bigg[\binom{128}{h} 0.5^h (1 - 0.5)^{128-h} \\ \bullet \sum_{h/2}^{h} \binom{h}{h/2} p_{ub}^{h/2} (1 - p_{ub})^{h-h/2} \Bigg]. \end{aligned} \tag{6}$$

Fig. 4(a) shows the probability of misidentification versus number of chips for different unstable bit percentages. When there exist more unstable bits in the ID codes, the probability of misidentification increases significantly. Three methods may be applied to reduce the influence of unstable bits on the probability of correct identification: averaging multiple reads to attenuate the effects of thermal noise, increasing the ID code length, or increasing the signal-to-noise ratio of the circuit evaluation process by increasing the mismatch variance or reducing the circuit thermal noise. Fig. 4(b) demonstrates the effects of increasing the length of the ID code to reduce the probability of misidentification (at the expense of increased chip area and power dissipation). This analysis demonstrates that moving from 128-bit ID to 256-bit ID reduces the misidentification probability from 5.89 e-13 to 2.96 e-33 for a 4% unstable bit percentage. We now discuss the circuit design techniques used in this work.

IV. Circuit Design and Layout Techniques

Based on the architecture developed in Section II and the statistical analysis in the previous section, the following goals for the design of the ID cell is targeted: minimize area and power dissipation, maximize readout speed, minimize systematic offsets, maximize random offsets, and minimize thermal noise during ID cell evaluation.

The readout stability is impacted by the ID cell's offset distribution and the thermal noise during evaluation. Theoretically, the offset voltage distribution is a zero-mean Gaussian with a variance much higher than the circuit noise. Since the ID cell mismatch is the signal of interest, its magnitude must be higher than the thermal noise of the amplifying transistors to allow a

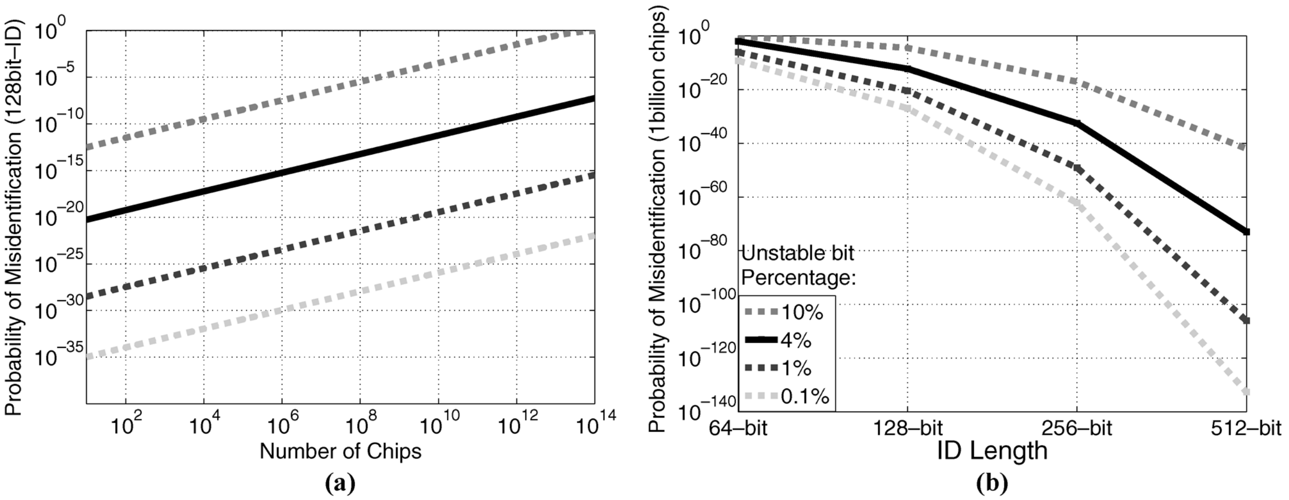

Fig. 4. (a) Probability of chip misidentification versus number of die. (b) Probability of chip misidentification as a function of ID length.

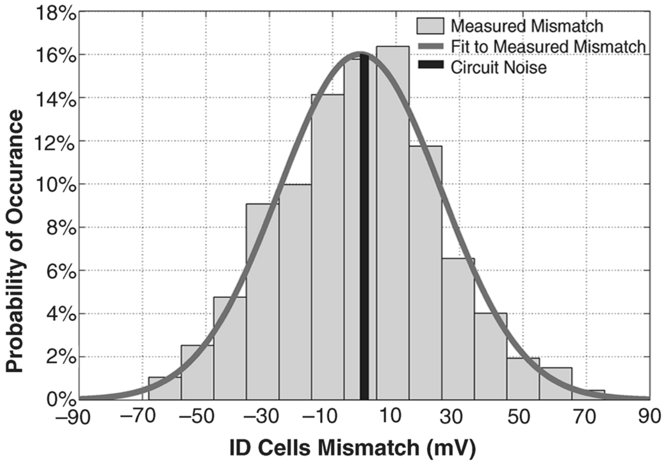

Fig. 5. Measured ID cell mismatch distribution. The calculated RMS circuit noise is annotated with the black zero-mean stripe.

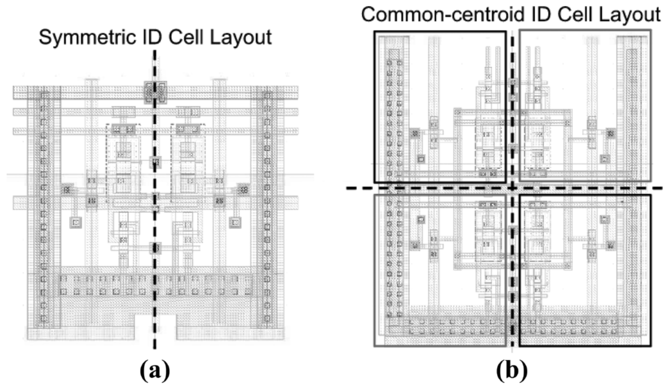

Fig. 6. Layout of a symmetric ID cell and a common-centroid ID cell.

stable ID bit. Minimum area transistor gates were used to maximize the random offset voltage [5]. A split supply on the test chip allowed individual access to both sides of the ID cell, allowing individual measurement of the voltage offset. The measured ID cells offset along with a Gaussian fit is shown in Fig. 5. The mean (μ) of the offset voltage distribution is -1.4 mV and the standard deviation (σ) is 25.6 mV. This offset is compared to the noise at the input of the ID cell during evaluation period. This noise is dominated by thermal noise of transistors M1 and M2 in Fig. 1. The noise voltage is a zero-mean random variable. Thus, those ID cells that have an offset voltage close to zero (near the peak region of the offset voltage Gaussian distribution) are likely to exhibit unstable behavior. The measured percentage of unstable bits is approximately 4%, corresponding to an input noise of about 1.5 $\mathrm{mV_{rms}}$. This noise amplitude is depicted in Fig. 5 as a black stripe region around the zero-offset region.

To achieve a large Hamming distance between the chips, the ID bits should be random and evenly distributed between ones and zeros. For an even bit distribution, systematic offsets, process gradients, and shadowing effects must be minimized, which necessitates the use of analog layout techniques. However, unlike precision analog design, this system requires a high random ID cell mismatch variation. Since this demands small area transistors, the devices can be placed within a very close proximity, allowing a large reduction in the effect of process gradients. Low-offset analog amplifiers and comparators often use a common-centroid layout technique to further minimize these effects. Two ID arrays were designed using two different layout techniques to perform a direct comparison. One uses a fully symmetric unit cell layout [Fig. 6(a)] and the other uses a common-centroid layout [Fig. 6(b)] which requires twice as many minimum-sized transistors. Dummy cells were placed around each array to prevent edge-effects. One would expect the common-centroid layout to exhibit a better bit distribution due to suppression of gradient effects at the expense of higher active area and power dissipation. The area overhead for a common-centroid layout ID block is approximately 68%.

Analysis from the previous sections reveals that the fidelity of the chip ID measurement relies on a stable offset voltage, which is dominated by the threshold voltage $(\mathrm{V_t})$ mismatch. However, due to long-term voltage stress to the circuit, the transistor $\mathrm{V_t}$ can shift over time. This $\mathrm{V_t}$ instability is known as negative bias temperature instability (NBTI). Since the rate of $\mathrm{V_t}$ degradation is not constant for every transistor, the output of the ID cell could flip from its correct logic state to the opposite, resulting in a reduction in the ID stability and reliability. To minimize the impact of NBTI on the ID cell transistors, the supply to the core ID cell circuit should be disabled between reads.

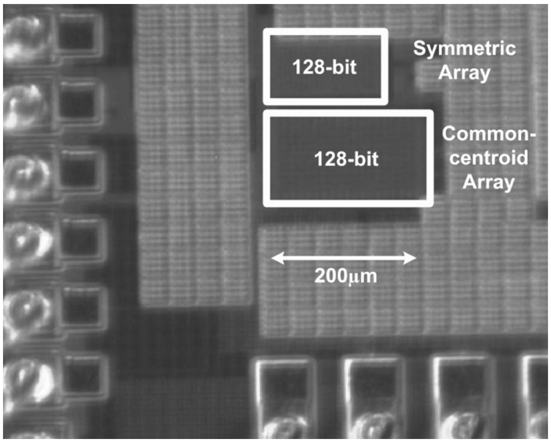

Fig. 7. 0.13 μm CMOS chip micrograph.

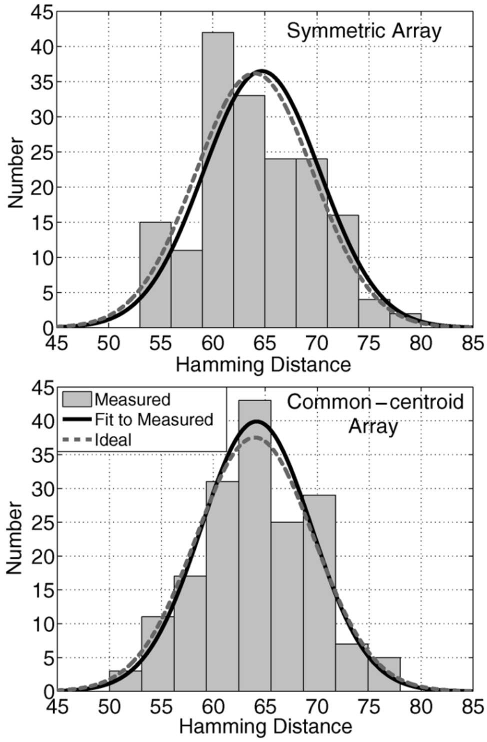

Fig. 8. Measured and ideal Hamming distance for both ID generators.

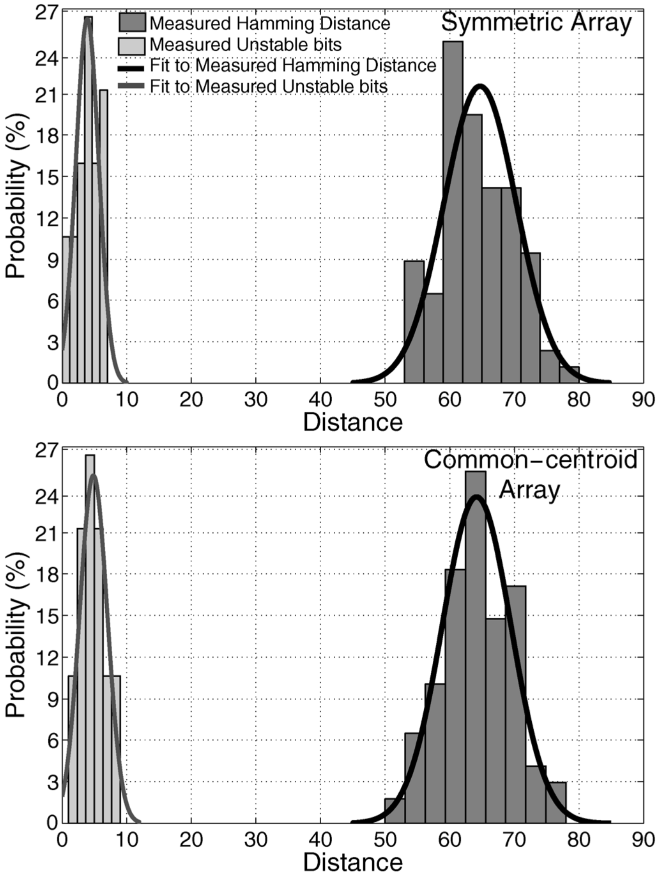

Fig. 9. Measured Hamming distance and unstable bits for both ID generators.

Another potential problem that can decrease the ID reliability is aging. Even though the power supply is enabled only during readout, which would minimize the NBTI effects on the circuit, the mechanical stress due to aging and temperature cycling can cause errors in the ID bits. Our experimental result from accelerated aging testing is presented in Section V. One possible solution to this problem is increasing the ID code length. From the probability of misidentification model in Section III and Fig. 4(b), assuming a 128-bit ID code is used, 4% unstable bits, and one billion chips, by increasing the ID code length from 128-bit to 256-bit, the ID generator circuit can tolerate an additional 4% of shifting bits due to aging while maintaining the same probability of misidentification.

V. Measured Results

Both the symmetric and common-centroid ID generators were fabricated in a 0.13 μm CMOS process. A chip micrograph is shown in Fig. 7. The decoder circuitry, readout circuit, and output pad drivers are integrated and included in all reported power consumption numbers. The active area of the 128-bit ID array, including dummies, is $(70 \times 130)\ \mu\text{m}^2$ for the symmetric layout and $(95 \times 195)\ \mu\text{m}^2$ for the larger common-centroid array. Twenty chips were packaged, but one chip failure left 19 sample die. Table I shows the ID codes in hexadecimal format for the symmetric and common-centroid arrays for all 19 chips. Table II shows the measured Hamming distance between 19 chips for both symmetric array and common-centroid array, demonstrating a unique and widely-spaced ID code for each die. Fig. 8 shows the measured histogram of the Hamming distance between all chips and a Gaussian curve fit to this histogram. In addition, the theoretical ideal Hamming distance distribution is plotted for comparison. For the 128-bit ID, the mean Hamming distance for the common-centroid ID generator is 64.16 (±0.80), while the symmetric layout shows 64.70 (±0.84) with a 95% confidence interval (CI). As anticipated, the Hamming distance for the common-centroid layout is slightly better than the symmetric layout due to the suppression of process gradients. Both layouts are relatively free of gradient effects since the spacing between the minimum-size transistors is extremely small ($< 4\,\mu$m). The number of unstable bits averaged over all 19 chips for the common-centroid layout

TABLE I
CHIP ID CODES IN HEXADECIMAL FORMAT FOR BOTH ID GENERATORS

Chip	Symmetric Array	Common-centroid Array
1	8E58485BDFA4B4232F366B17F2D19B1F	EBB3A5D74DD3D4FAF89D41192AFA7F56
2	9940ED3BA76D450E2F1B5C41BB6214A2	13F866EF80914FCA9EDF356076782315
3	24AB07A34E6AC17F2DBFF7B1417FB136	D65254D4CC278C77417B5202CD88E693
4	3F67787E4F65F14FD454B7CB9A57E685	1B654218C22E137F3932F45F457914D1
5	4C80A45E09CD2484E0463323A028E0E6	AC527345449ECF399ACD23D42B13994A
6	34B6A687E701832A1F646E648620D51A	B8B247D55E82B285600018495C4C41D1
7	F89A1AEBC15E6AECFD0018661B4AF1A0	67CF1AF935D7F215CBC3A1FD4E3F05F2
8	7F418BA924774C06AEE84DFC059EF079	8B22A75722A053021490D79A7B8CB83A
9	50A2596ED8BF3453696507077787990C3	7C6510F34DC9DBCD964DCBFFECFD12BA
10	8D76F19139169BBBCEAFD4D79B1C3F17	54A6736592801BF1DF8592384AD8B723
11	EFBA8113877057F95DC8EB4EAD8D6ABC	EBD94569BC3A63A2C183F81AAFD16B0F
12	A3AF1DFD2DEFDD535E2F09BB98E1B83F	72A88142166F17D95092FE0664BFAF53
13	3DB350453957C56D18A7B729374250F5	726BFDB10BE017C3F4CAE3B5805944E8
14	50921717F65316C79263DD925ECFE2F2	E14AFA70A761EE11DE7458B42607A856
15	0423A765A02B890A804B47128B8CA52E	E3890209134B71E5CCDF837DE976C15F
16	4E7B1F31FD9A455400C583D362BFD397	0E0AAAD2791147B2B7FA74CD483E8DAC
17	296F4A56D830EC9B362C203BDC545836	DBCD3B10866D739CA31B5A59AB772ABC
18	DB1AE6D995EFAF8D77922B12ACBF0B98	AF01FC4DC58109286D4A509606F5827E
19	72CC3D3E4033FEBD5CBF8DCE9CB6B72C	9C9F2B9E483D6795BDF46734A985C82B

TABLE II
MEASURED NUMERICAL DISTANCE (HAMMING DISTANCE) OF THE ID CODES FOR ALL COMBINATIONS OF CHIPS FOR BOTH ID GENERATORS

Chip	Symmetric Array																			
19	72	69	65	57	74	69	62	61	65	62	61	55	74	63	68	71	62	66	0	Common-centroid Array
18	54	61	75	71	60	69	62	69	73	70	53	65	74	67	66	65	68	0	73	
17	54	71	63	59	68	67	68	69	61	62	67	55	60	71	68	69	0	64	59	
16	61	74	54	64	65	74	71	64	56	65	64	64	61	56	61	0	63	63	54	
15	76	59	55	69	56	53	72	59	67	58	69	61	70	59	0	68	55	65	62	
14	73	68	64	68	65	64	61	62	58	69	62	68	61	0	66	64	59	55	64	
13	72	65	57	55	60	63	62	65	61	62	65	61	0	64	62	60	67	63	64	
12	59	64	56	60	69	72	71	62	58	61	66	0	63	61	59	65	62	70	69	
11	65	70	66	66	69	62	61	64	78	63	0	60	69	69	57	75	54	60	67	
10	62	65	65	65	80	65	72	69	75	0	64	60	61	67	63	71	70	66	69	
9	55	66	64	62	53	74	61	74	0	60	74	66	53	69	59	69	58	62	67	
8	75	60	62	72	71	66	61	0	67	55	63	59	64	62	70	58	65	61	60	
7	74	59	67	67	60	63	0	78	53	63	67	67	60	56	60	58	61	67	72	
6	63	60	60	70	67	0	63	61	66	60	64	64	65	73	65	71	70	70	73	
5	66	61	71	61	0	69	60	62	61	57	65	71	70	56	64	64	69	59	54	
4	63	62	66	0	73	60	65	65	66	66	68	54	63	77	65	65	56	64	69	
3	65	64	0	59	68	57	74	70	69	63	63	61	70	66	76	70	71	61	66	
2	61	0	69	66	63	68	69	63	66	54	62	64	67	67	63	61	70	64	71	
1	0	58	65	76	57	60	65	59	62	64	60	62	63	69	59	63	66	62	71	
Chip	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	

is 4.84 (±0.33) per chip (3.78% of the total number of ID bits). The symmetric layout demonstrated an average of 3.89 (±0.27) unstable bits per chip. Fig. 9 plots the distance between measured Hamming distance and the measured unstable bits. The distance between these distributions is a measure of the reliability of the ID code. Averaging multiple reads can easily be performed to effectively reduce the thermal noise contribution and increase the ID stability (at the expense of increased power dissipation and read-time). The environmental stability of the ID circuit block was also explored. Fig. 10 shows the ID stability over power supply, indicating the number of bits from one chip that change for one read at each voltage level from 900 mV to 1.2 V. Fig. 11 shows the ID stability over the temperature range of 0 °C to 80 °C. One hundred reads were averaged at 20 °C as a reference ID to reduce the influence of unstable bits. This temperature dependence is due to the

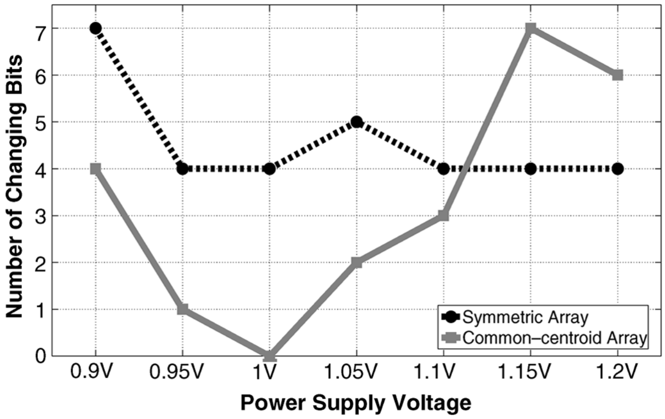

Fig. 10. Measured supply dependency of chip ID.

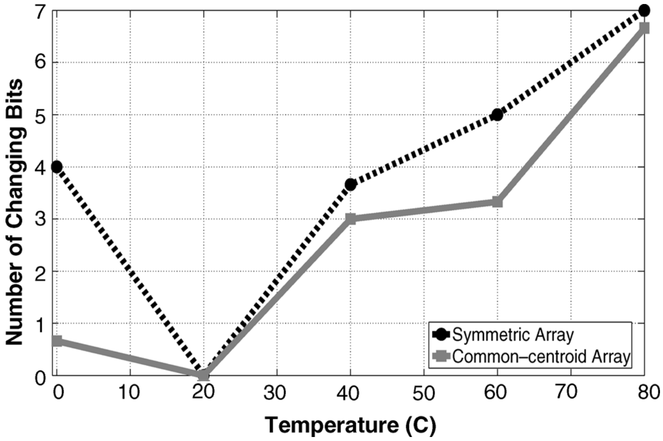

Fig. 11. Measured temperature dependency of chip ID.

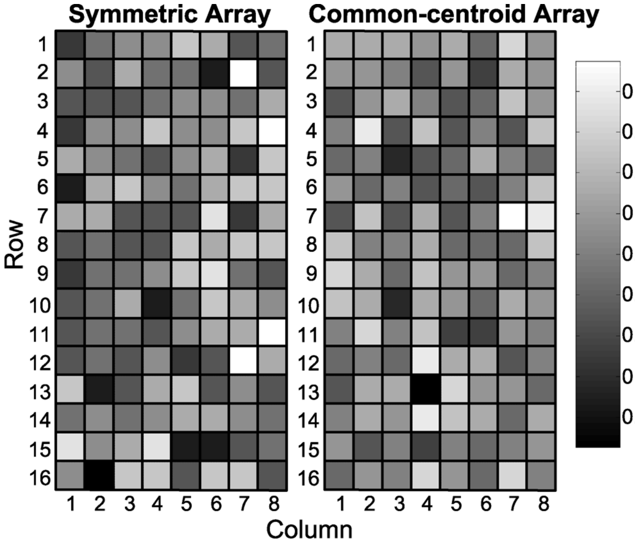

Fig. 12. Averaged ID generator output showing spatial dependency.

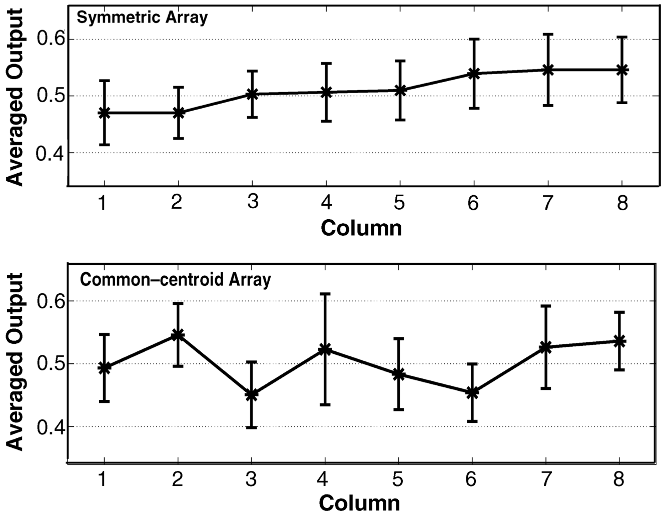

Fig. 13. Averaged output of all ID columns showing gradient effects.

TABLE III
NUMBER OF SHIFTED BITS IN EACH SAMPLE CHIP AFTER THE ACCELERATED AGING TEST FOR BOTH ID GENERATORS

	Symmetric Array	Common-centroid Array
Chip 01	3	2
Chip 02	0	1
Chip 11	1	3
Chip 12	0	1
Chip 16	0	2

variation of transistor pairs offset voltage contribution. In order to estimate the number of shifted bits due to aging, an accelerated aging test was performed through temperature cycling on five sample packaged die. The die were subjected to 100 cycles of a 0 °C to 100 °C temperature sweep. Table III shows the number of shifted bits after the accelerated aging test for each sample chip. The average shifted bit for the symmetric array is 0.8, and 1.8 for the common-centroid array. Fig. 12 shows the averaged output over 19 chips for each individual ID cell. No noticeable spatial artifacts are present in either circuit, indicating negligible systematic mismatch. Fig. 13 shows the averaged outputs for each column for both ID generators with a bounded 95% CI. The results show that averaged output of the symmetric array tends to increase from the left to right column, where the averaged output of common-centroid array shows no spatial tendency. Across 19 chips, the common-centroid array ID codes have 50.16% (±1.98% for 95% CI) logic “1” and 49.84% (±1.98%) logic “0”, while the symmetric array ID codes have 51.15% (±1.99%) logic “1” and 48.85% (±1.99%) logic “0”. We analyzed the correlation between each ID bit and its neighbor to investigate any coupling between cells. Table IV shows the probability of the adjacent bit output with the 95% CI, where the adjacent bit is defined as either the top, bottom, left or right bit. This measurement was performed on each individual cell across all 19 chips, and the measured results show no significant correlation between the bit and the adjacent bit for both ID generators.

Although the proposed cross-coupled logic gate ID generator cells require analog-inspired layout techniques, they are fundamentally digital and exhibit no static power dissipation besides subthreshold drain and gate leakage. The energy consumption of both ID generators measured at 1 V over various throughputs is shown in Fig. 14. At low clock frequencies, the power is dominated by static leakage currents (137 nW for the symmetric layout and 162 nW for the common-centroid layout). Low readout power consumption is crucial for ultra-low power

TABLE IV
PROBABILITY OF THE ADJACENT BIT OUTPUT FOR BOTH ID GENERATORS

Symmetric Array		Common-centroid Array	
Bit=0	Probability of adjacent bit=0: 50.49% ± 2.12% Probability of adjacent bit=1: 49.51% ± 2.12%	Bit=0	Probability of adjacent bit=0: 49.39% ± 2.09% Probability of adjacent bit=1: 50.61% ± 2.09%
Bit=1	Probability of adjacent bit=0: 47.82% ± 2.06% Probability of adjacent bit=1: 52.18% ± 2.06%	Bit=1	Probability of adjacent bit=0: 50.93% ± 2.09% Probability of adjacent bit=1: 49.07% ± 2.09%

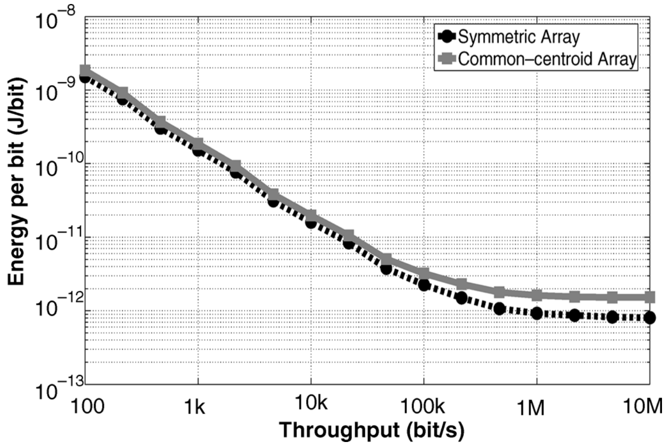

Fig. 14. Energy per bit (J/b) versus throughput (b/s). Below approximately 100 kb/s, static leakage dominates the power consumption.

TABLE V
PERFORMANCE COMPARISONS BETWEEN SYMMETRIC ARRAY AND COMMON-CENTROID ARRAY

	Symmetric Array	Common-centroid Array
V_{DD}	1 V	
Throughput (bps)	1 M	
I_{DD} Current	0.93 μA	1.6 μA
Leakage Current	137 nA	162 nA
Average Hamming Distance	64.70	64.16
Average Unstable Bits	3.04%	3.78%

TABLE VI
PERFORMANCE COMPARISONS TO TRADITIONAL TECHNOLOGY AND EXISTING WORKS

	Programming time/voltage/current	Area	ID Stability	Code Sequence
This work	0	≈ same	4% unstable bit	Random
E-fuse	≈0.6 ms/3.3 V/10 mA per fuse		0 unstable bit	Sequential/ Random

	Power (μW)	Throughput (bps)	Energy/bit (pJ/bit)	ID Length	Technology (μm)	Area (μm^2)
ISSCC '00 [1]	250 (@ 30 kbps)	1.5 M	8330 (@ 30 kbps)	112	0.35	23,436
[6]	120	5 M	24	256	0.13	4,000
Symmetric	0.93	1 M	0.93	128	0.13	15,288
Common-centroid	1.6	1 M	1.6			25,903

read applications such as RFID tags. Above a critical bitrate (approximately 100 kb/s) the dynamic power consumption begins to dominate. At a bitrate of 1 Mb/s, the symmetric latch consumes 0.93 pJ/bit and the common-centroid latch consumes 1.6 pJ/bit. The simulated brief transient peak current for the 128-bit symmetric ID generator is approximately 5 mA during evaluation of all the ID cells. To reduce this peak current, the ID cells' evaluation can be performed sequentially, significantly reducing the simultaneous switching current without incurring a power penalty. A comparison between the two layout techniques is shown in Table V. Table VI shows the comparison to a traditional technique (E-fuse in the same process) and to similar existing works. Since the proposed ID generator is loosely based on an SRAM architecture, it scales well with technology and supply voltages.

VI. CONCLUSION

We have presented a 162 nW chip ID circuit based on process variations. Each ID cell consists of a cross-coupled logic gate that simultaneously generates a random offset, amplifies the offset, and digitizes it, resulting in a stable ID bit. These cells are tiled to create a compact 128-bit ID array. Layout and circuit design techniques were discussed. Our technique allows the generation of a digital ID from a random offset distribution with small mean and high variance. Two different layout techniques were fabricated on a 0.13 μm process to demonstrate the performance comparison. Based on their unique characteristics, the symmetric array may be more suitable for low power and area limited applications, where the common-centroid array may be more appropriate for high statistical precision applications. Our ID circuit improves the power efficiency by over an order of magnitude relative to the existing state of the art. The low power operation could enable identification of energy-constrained wireless sensor nodes and RFID tags. Efficient use of power and area will be critical to enabling the next generation of wireless sensor networks.

References

[1] K. Lofstrom, W. R. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2000, pp. 372–373.

[2] A. Cabbibo *et al.*, "Feed forward test methodology utilizing device identification," in *Proc. IEEE Int. Test Conf.*, Oct. 2004, pp. 655–660.

[3] D. Lim *et al.*, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[4] J. Hirase and T. Furukawa, "Chip identification using characteristic dispersion of transistor," in *Proc. 14th Asian Test Symp.*, Dec. 2005, pp. 188–193.

[5] M. Pelgrom, A. Duinmaijer, and A. Welbers, "Matching properties of MOS transistors," *IEEE J. Solid-State Circuits*, vol. 24, no. 10, pp. 1433–1440, Oct. 1989.

[6] K. Lofstrom, "ICID–A robust, low cost integrated circuit identification method, ver. 0.9," KLIC, Mar. 2007 [Online]. Available: http://www.kl-ic.com/white9.pdf

Ying Su received the B.S. degree in electrical engineering from the University of Washington, Seattle, in 2006. She is currently pursuing the Master's degree in electrical engineering at the University of Washington. She has previously held an intern position at Emulex Corp and was awarded an SRC undergraduate research fellowship.

Her research interests include low power analog and digital circuit design techniques for mitigating and utilizing process variations in advanced CMOS technologies.

Jeremy Holleman (S'03) received the B.S. degree in electrical engineering from the Georgia Institute of Technology, Atlanta, in 1997. In 2006, he received the M.S. degree in electrical engineering from the University of Washington, where he is currently pursuing the Ph.D. degree.

From 1999 to 2001, he worked as an Embedded Systems Engineer at Data I/O. His research interests include low-power analog signal processing, biologically inspired computation, and circuits for biomedical applications.

Brian P. Otis (S'96–M'05) received the B.S. degree in electrical engineering from the University of Washington, Seattle, in 1999, and the M.S. and Ph.D. degrees from the University of California at Berkeley in 2002 and 2005, respectively.

He joined the faculty of the University of Washington as an Assistant Professor of electrical engineering in August 2005, where he directs the Wireless Sensing Laboratory. His research interests include ultra-low-power analog, digital, and RF circuits for enabling ubiquitous sensing and communication. He is the co-author of five book chapters and one book on ultra-low-power RF transceiver design. He has previously held positions at Intel Corporation and Agilent Technologies.

Dr. Otis is an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS PART II. He was the recipient of the 2003 U.C. Berkeley Seven Rosen Funds Award for innovation and co-recipient of the 2002 ISSCC Jack Raper Award for Outstanding Technology Directions Paper.