22.5 A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations

Y. Su, J. Holleman, B. Otis

University of Washington, Seattle, WA

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, IC process quality control, and secure documentation. Traditional methods of writing addresses into ROMs involve external programming, incurring additional expense or process modifications. Recently, Lofstrom et al. proposed the extraction of a unique and repeatable ID from random variable mismatch [1], which led to new testing methodology capability, including inexpensive identification of packaged dice [2]. Published results in this area suggest that it is possible to extract a unique fingerprint from each chip by comparing the transistor current flow or digital path delay variations that exist from die to die [1,3]. In this work, we propose a new chip-ID generation circuit that relies on digital-latch threshold-offset voltages to provide a robust 128b ID. Using the large gain provided by cross-coupled logic gates, we achieve significant improvements in readout speed and power consumption over existing designs, allowing a minimum power consumption of 162nW at low clock rates and an energy per bit of 1.6pJ/bit at 1Mb/s.

Each ID bit is generated by a latch composed of cross-coupled NOR logic gates, as shown in Fig. 22.5.1. Both sides of the latch are initially pulled low. As the clock edge is lowered, each latch evaluates to a state determined by the threshold-voltage (V_t) mismatch of the latch transistors. This mechanism directly generates a logic-level output corresponding to the polarity of the random V_t mismatch of the latch. Unlike previous implementations, no offset-nulled comparator or low-offset amplifier is needed to detect very small V_t variations. Our approach relies on the positive feedback inherent in the latch configuration, allowing large amplification of a zero-mean, high-variance random variable. Monte-Carlo simulations indicate that all latches evaluate in less than 10ns.

The circuit architecture is similar to a 128b SRAM array. The perimeter of the 8×16 latch array is surrounded by 52 dummy latches to prevent edge effects from corrupting the ID statistics. Figure 22.5.1 shows the complete layout of the ID array. All latches evaluate 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 128b ID.

The Hamming distance is defined as the number of bits that differ between any two ID numbers. When the number of ID bits is large, the Hamming distance between two chips is, 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 V_t offset for a particular latch is small relative to the thermal 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].

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 V_t variation. Since the V_t mismatch is the signal of interest, its magnitude must be higher than the thermal noise of the amplifying transistors to allow a stable ID bit. Thus, minimum area transistor gates are used to maximize the offset voltage [4]. Two ID arrays are designed using two different layout techniques to perform a direct comparison. One array uses a fully symmetric unit cell layout and the other uses a common-centroid layout, which requires twice as many minimum-sized transistors. One expects 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.

Both the symmetric and common-centroid ID generators are fabricated in a 0.13µm CMOS process. The decoder circuitry, readout circuit, and pad drivers are integrated and included in all reported power consumption numbers. The active area of the 128b ID array, including dummies, is 70×135µm^2 for the symmetric layout and 95×195µm^2 for the common-centroid array. Twenty chips are packaged, but one chip failure left 19 sample dice. Figure 22.5.2 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 128b ID, the mean Hamming distance for the common-centroid ID generator is 64.16, while the symmetric layout shows 64.70. As anticipated, the Hamming distance for the common-centroid layout is slightly better than the symmetric layout due to the suppression of process gradients. The number of unstable bits averaged over all 19 chips for the common-centroid layout is 4.84 per chip (3.78% of the total number of ID bits). The symmetric layout demonstrates an average of 3.89 unstable bits per chip (3.04%). Averaging of multiple reads can be easily implemented to effectively reduce the thermal noise contribution and increase the ID stability. Disabling the supply to the ID generator block, except during readout can reduce the effect of long-term Vt instability due to aging and fatigue. Figure 22.5.3 shows the number of bits from one chip that change for one read at each voltage level from 900mV to 1.2V. Figure 22.5.4 shows the averaged output over 19 chips for each location in the array. No noticeable spatial artifacts are present in either circuit, indicating negligible systematic mismatch.

Although the proposed cross-coupled NOR 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 1V for various throughputs is shown in Fig. 22.5.5. At low clock frequencies, the power consumption is dominated by static leakage currents (137nW for the symmetric layout and 162nW for the common-centroid layout). The lowest achievable readout power consumption metric is crucial for ultra-low-power read applications such as RFID tags. Above 100kb/s, the dynamic power consumption begins to dominate. At a bitrate of 1Mb/s, the symmetric latch consumes 0.93pJ/bit and the common-centroid latch consumes 1.6pJ/bit. Our minimum power dissipation and energy per readout bit is significantly lower than previously published results. A comparison to existing work is shown in Fig. 22.5.6. Since the proposed ID generator is loosely based on an SRAM architecture, it scales well with technology and supply voltages and can be re-used as general random access memory. Figure 22.5.7 shows the chip micrograph.

References:

[1] K. Lofstrom, W.R. Daasch, and D. Taylor, "IC Identification Circuit using Device Mismatch," *ISSCC Dig. Tech. Papers,* pp. 372-373, Feb., 2000.

[2] A. Cabbibo, J. Conder, and M. Jacobs, "Feed Forward Test Methodology Utilizing Device Identification," *IEEE Int. Test Conf.*, pp. 655-660, Oct., 2004.

[3] D. Lim, J.W. Lee, B. Gassend, et al., "Extracting Secret Keys from Integrated Circuits," *IEEE Trans. VLSI Systems*, vol. 13, no. 10, pp. 1200-1205, Oct., 2005.

[4] 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.

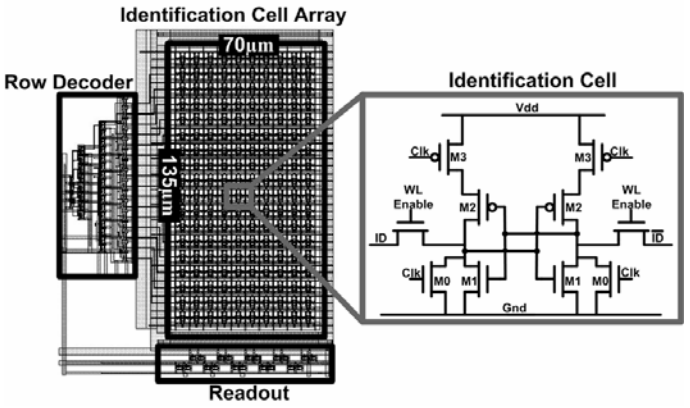

Figure 22.5.1: Layout of symmetric ID generator and schematic of one ID cell.

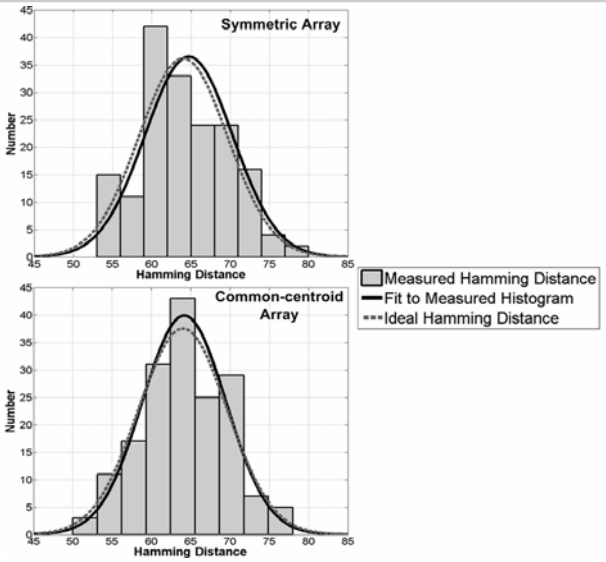

Figure 22.5.2: Measured and ideal Hamming distance for both ID generators.

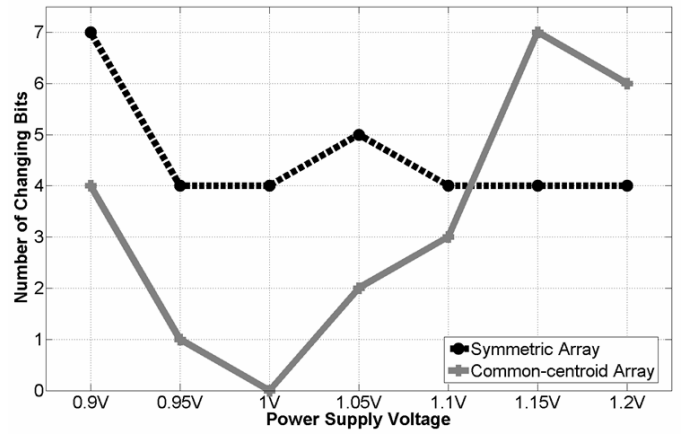

Figure 22.5.3: Measured changing bits over power supply sweep.

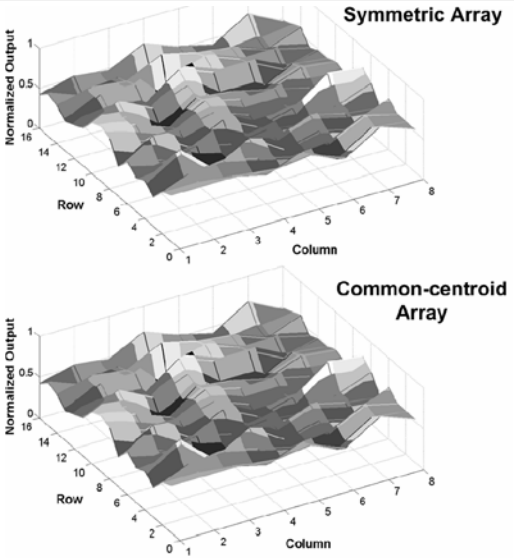

Figure 22.5.4: Normalized output showing ID generator spatial dependency.

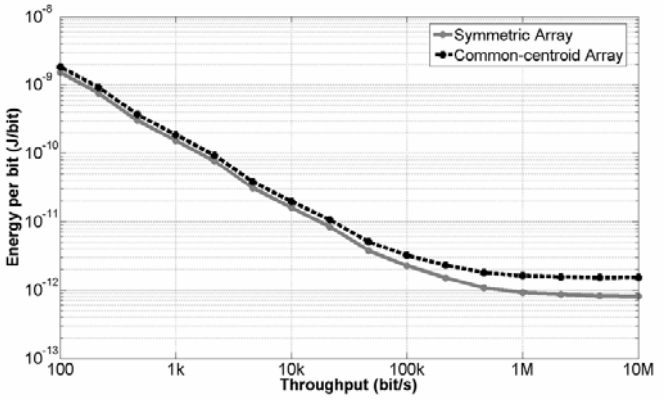

Figure 22.5.5: Energy per bit (J/b) versus throughput (b/s).

	Symmetric Layout ID Generator	Common-centroid Layout ID Generator
V_{DD}	1V	
Throughput (bps)	1M	
I_{DD} Current	0.93µA	1.6µA
Leakage Current	137nA	162nA
Average Hamming Dist. (19 die)	64.70	64.16
Average Unstable Bit (19 die)	3.04%	3.78%

	Power Consumption (µW)	Throughput (bps)	Energy/bit (pJ/bit)	ID Length	Technology (µm)	Area (µm²)
Lofstrom et. al [1]	250	30k	8330	112	0.35	23,436
This work (Symmetric)	0.93	1M	0.93	128	0.13	15,288
This work (Common-centroid)	1.6	1M	1.6	128	0.13	25,903

Figure 22.5.6: Results summary and comparison to existing work.

Continued on Page

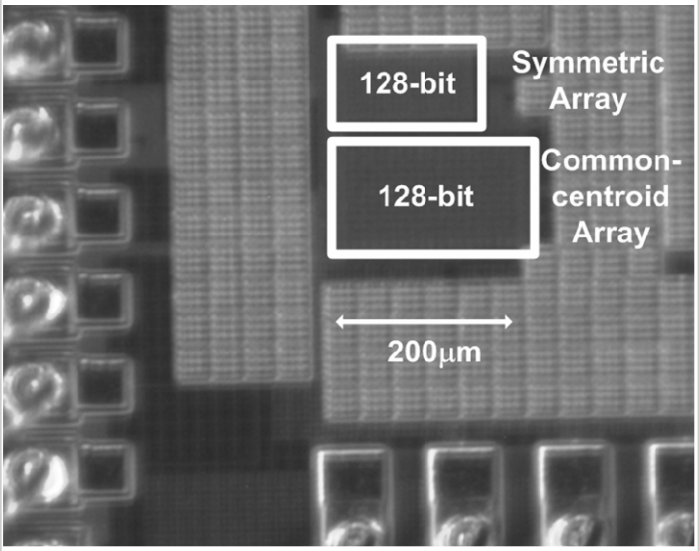

Figure 22.5.7: Chip micrograph.

