Final Paper submitted for ISSCC 2000, **Technology Directions** 22.6

IC Identification Circuit Using Device Mismatch

Keith Lofstrom[1], W. Robert Daasch[2], Donald Taylor[2]

[1]SiidTech, Beaverton, OR
[2]Portland State University, Portland, OR

Contact Information:

Keith Lofstrom
SiidTech
5290 s.w. Elm Ave.
Beaverton, Oregon, USA 97005
voice: (503) 520-1993 (home office)
fax: (503) 520-1614
keithl@klic.rain.com

Robert Daasch
Department of Electrical and Computer Engineering
Portland State University
PO Box 751
Portland, OR 97207
voice: (503) 725-5409 (office)
fax: (503) 725-3807
daasch@ee.pdx.edu

Don Taylor
Department of Mathematical Sciences
Portland State University
PO Box 751
Portland, OR 97207
voice: (503) 725-3621
fax: (503) 725-3661
dont@agora.rdrop.com

ABSTRACT

IC Identification Circuit Using Device Mismatch

Keith Lofstrom, W. Robert Daasch, Donald Taylor

A repeatable binary identification is produced from random threshold mismatch in an array of addressable MOSFETs, and an auto-zeroing comparator. The analog technique is applicable to any digital or analog submicron CMOS process, without special processing or after-fabrication programming.

IC Identification Circuit Using Device Mismatch

Keith Lofstrom[1], W. Robert Daasch[2], Donald Taylor[2]
[1]SiidTech, Beaverton, OR [2]Portland State University, Portland, OR

Non-alterable, non-forgeable identification is required for tracking work in progress, detecting part rebranding, radio frequency identification (RFID), IP protection, and transaction validation. Wafer level techniques such as laser link cutting, and circuit-level EPROM techniques, require expensive machinery or special wafer processing. Integrated Circuit IDentification (ICID) extracts unique and repeatable information from the randomness inherent in silicon processing. No external programming or special process steps are needed, and the technique may be used with any standard submicron CMOS process.

MOSFET voltage thresholds depend on many process variables that are roughly uniform over a die. Thresholds are also a function of the random placement of impurity dopant atoms in the silicon channels, which vary randomly from transistor to transistor [1]. As transistors shrink, so do the number of atoms in the channel, magnifying effects of small variations. This will make future giga-scale chip designs difficult, but can be put to good use for uniquely identifying those chips. Advanced processing techniques, such as retrograde doping, will slow the increase in mismatch, but will not reverse it [2].

ICID is based on an array of addressable MOSFETs, with common gate and source and sequentially selected drains, driving a resistive load. Because of device mismatch, the drain currents will be randomly different, producing a sequence of random voltages across the load. ICID uses these sequences of random but repeatable voltages to construct unique identifications. The sequences are different for every integrated circuit die, because every transistor has a different distribution of frozen-in random dopant atoms. Figure 1 shows an array of devices producing a difference voltage sequence. The MOSFETs that form the sequence are addressed like a memory. Cell addresses for this experiment are provided externally, and about 2000 clocks read out the ID for one block. The random analog voltage sequence is converted to a binary identification sequence with an auto-zeroing comparator, by comparing successive random voltages to each other. Figure 2 is a block diagram of one ID block.

Comparisons are noisy, and mobile ion contamination and other effects may cause thresholds to shift over time. Some of the random differences will change sign, changing some of the identification bits, as shown in Figure 3. For clean sub-micron processes, the bit changes are rare, typically less than 5%. The ICID sequences are not deterministic, but with enough non-changing bits, the chance of two sequences being confused can be made as small as desired. The Hamming distance between two ID bit sequences is the number of bits that differ between them. If IDs are stored in a database during manufacturing, a single ID later compared to that database should have a small distance from its original ID (the "self" distance), and a large distance from all others (the "others" distance). Figure 4 shows the probabilities of "self" and "others" distances for a single pair of IDs, with measured data points shown against the curves expected from theory. When comparing a part to a database of IDs, a threshold bit distance can be chosen, with distances below the threshold considered a match. For this simple threshold comparison, the number of devices that can be adequately distinguished is a function of the number of ID bits and the expected worst-case drift, as shown in Figure 5.

Experimental devices were fabricated using a 0.35μm single-poly N-Well process, using two metal layers for the ICID blocks. Each ICID block has 112 identification cells, made of minimum-sized transistors. The experimental ICID blocks are not optimized for density -- static logic is used, and extra test logic is added. Array and comparator biases are brought out to external pins for sensitivity testing. 132 ICID blocks are combined onto each test chip. 55 chips were packaged and tested, for a total of 7260 ID blocks. No failures were observed, with each ICID block producing an ID differing from all others by at least 27 bits. Worst case drift was estimated by variations in frequency, temperature, and bias. Five of the parts - 660 ID blocks - were heated to 250 C for 100 hours to test drift. ID shifts of 6 or less bits were observed, with an average of 1.5 bits, corresponding to 1.3% drift. The ICID block tolerates a wide range of power supplies, biases, clock frequencies, and temperatures. Typical acceptable operating ranges are shown in Table 1. The device was tested on a Credence 312 tester, as well as a fixture powered and operated by a PC parallel port. Figure 6 shows a die photograph of a single ID block. Upper layer metal obscures most of the device.

A stable chip identification circuit, using local device mismatch and standard processing, has been fabricated and tested. The 112 bit experiment, with less than 4% drift, can reliably distinguish more than 1 million IDs with less than a 10^{-7} error rate. Mixed signal techniques are used, but all inputs and outputs are digital.

The authors gratefully acknowledge the assistance of Chi-Song Horng, Steve Sapiro, Credence Systems Corporation, and Greenforest Consulting.

References:

[1] "Intrinsic MOSFET Parameter Fluctuations Due to Random Dopant Placement", X. Tang et. al., IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 5, No. 4, December 1997, pp. 369-376.

[2] "Suppression of Random Dopant-Induced Threshold Voltage Fluctuations in Sub-0.1-μm MOSFET's with Epitaxial and σ-doped Channels", A. Asenov et. al., IEEE Transactions on Electron Devices, Vol. 46, No. 8, August 1999, pp. 1718-1724.

A note on size:

5875 characters, 919 words including title and references. Estimated 104 65 character lines, after reformatting.

Figures

Technology:	0.35 µm single poly CMOS
Block size	252x93 µm, 132 blocks/chip
Test chip size:	2060 x 1820 µm
ID bits	112

Measurements	Min.	Nom.	Max.
Vdd	1.1V	2.5V	5.0V
Idd current	50 µA	100 µA	
Temperature	TBD C	25 C	125 C
Frequency	30Hz	500KHz	>25MHz
Bit Rate	2bps	30Kbps	>1.5Mbps
Bit Drift Error	0%	1.3%	5%

Table 1: ICID block measurements

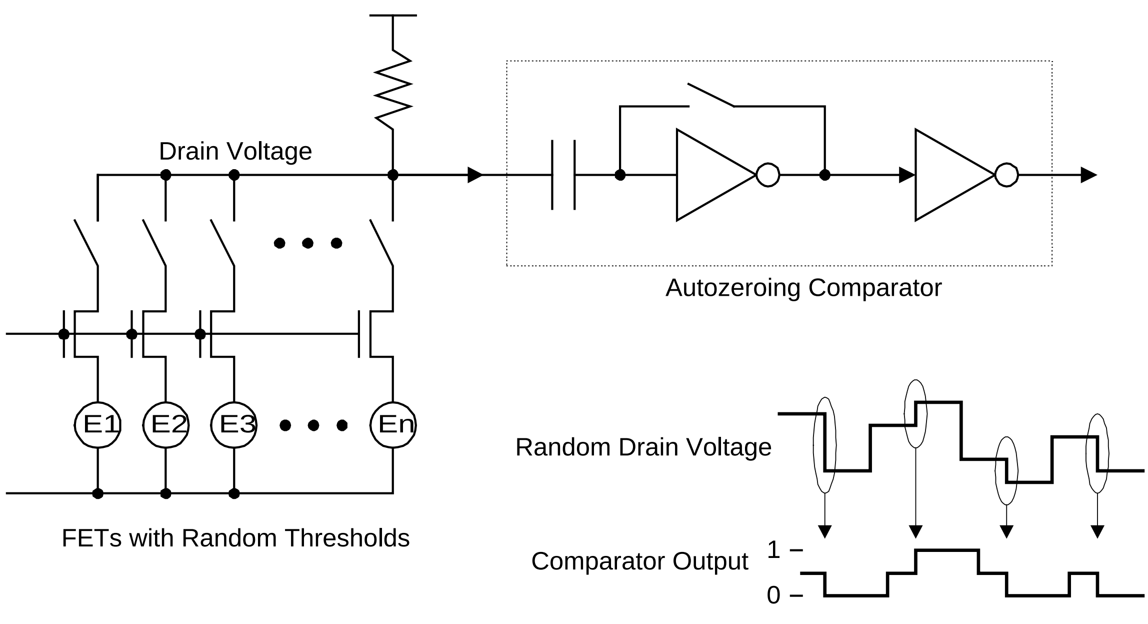

Figure 1: Array of transistors producing a sequential random voltage.

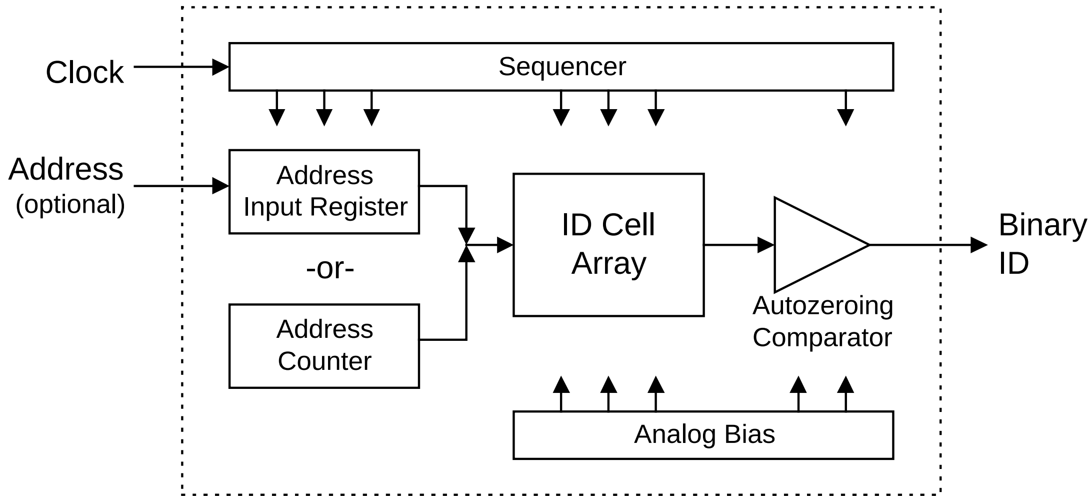

Figure 2: Block Diagram of ICID block

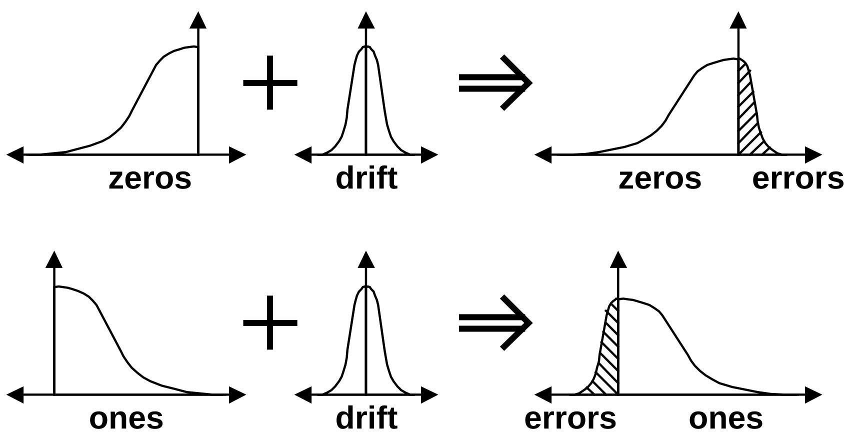

Figure 3: Random changes added to Gaussian distribution produce bit changes

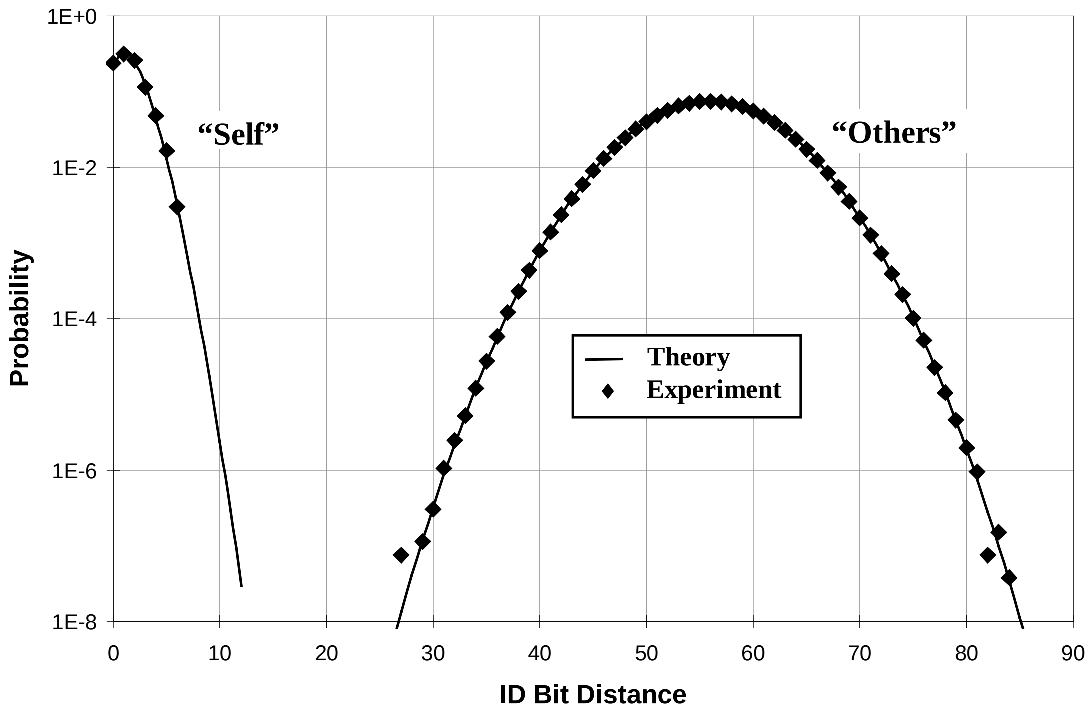

Figure 4: Probability of "self" and "others" matching versus bit distance.

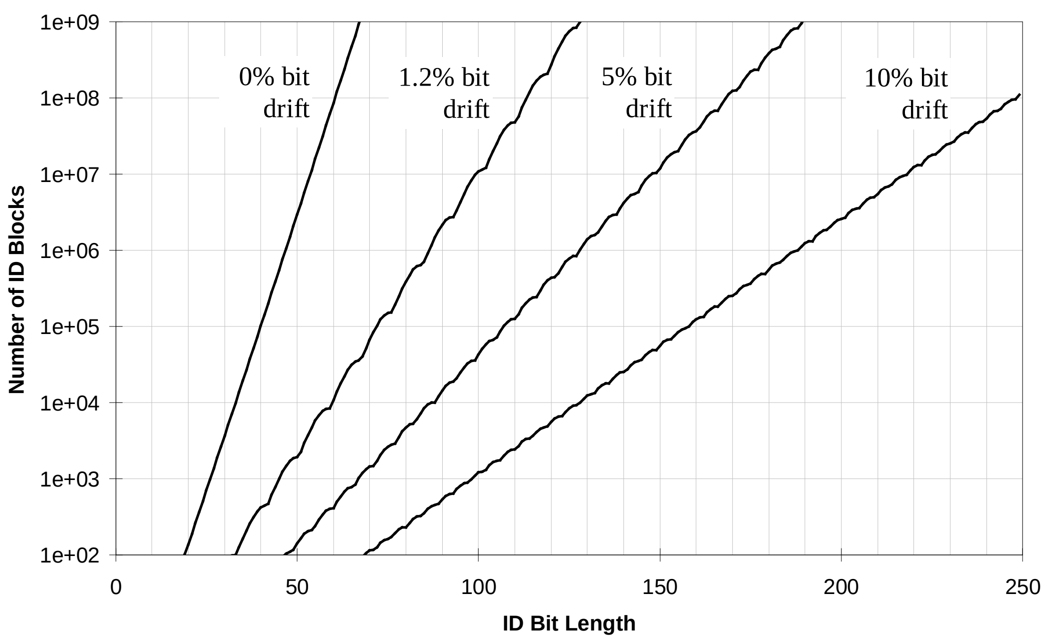

Figure 5: Number of distinguishable blocks versus drift and number of ID bits. (10% chance of false positive or negative for all devices)

Omitted for file length reasons

Figure 6: ICID single block photograph. Test die contains 132 blocks.