CMOS On-Chip Stable True-Random ID Generation Using Antenna Effect

Fang Tang, *Member, IEEE*, Denis G. Chen, *Member, IEEE*, Bo Wang, Amine Bermak, *Fellow, IEEE*, Abbes Amira, *Senior Member, IEEE*, and Saqib Mohamad

***Abstract*— A CMOS on-chip ID generation scheme is proposed. Using the antenna effect during the chip fabrication, one gate in a transistor pair is physically randomly broken down due to the process variation and an on-chip ID number is thus created depending on its polarity. The generated ID not only is permanently immune from environment changes such as supply voltage and temperature, but also consumes ultra-low leakage power without any dynamic transitions. The functionality of the proposed ID generation scheme has been experimentally verified by a fabricated chip in 0.18 μm CMOS process.**

***Index Terms*— CMOS on-chip ID, antenna effect, true random.**

I. Introduction

IN RECENT years, there have been continuous research efforts to innovate on-chip security mechanism in the application such as RFID monitoring and wireless sensor network, which is crucial to guarantee the origin of the deployed silicon chips [1]. On-chip stable true random ID generation circuit is one of such security mechanism. Conventionally, the chip ID is stored in ROM, which not only is unsafe but also need extra cost for the post-fabrication process. A digital chip ID circuit based on SRAM cell was proposed [2], [3]. The stored logic value in the SRAM is either one or zero depending on the process variation without consuming large power. However, the stored ID number might be changed when chip is powered on due to the noise, which makes the ID unstable to be recognized. To increase the recognition rate of the on-chip ID, an algorithm is proposed to analysis the ID series number [4], [5], however, with a significantly increased complexity and cost. A permanently stable ID generator was proposed in [6] by manually break down the transistor gate using high voltage. Although the generated ID can resist environment changes, post-fabrication process is required.

In this letter, we propose a permanent on-chip ID scheme using antenna effect during chip fabrication. The ID is immune from the environment changes while no post-fabrication process is required.

Manuscript received October 3, 2013; revised October 16, 2013; accepted October 21, 2013. Date of publication November 7, 2013; date of current version December 20, 2013. This work was supported by the Qatar National Priority Research Program under Grant 5-080-2-028. The review of this letter was arranged by Editor L. Selmi.

F. Tang is with the College of Communication Engineering, Chongqing University Chongqing 404000, China.

D. G. Chen, B. Wang, A. Bermak, and S. Mohamad are with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong (e-mail: denischn@gmail.com).

A. Amira is with the School of Computing, University of West Scotland, Paisley PA1 2BE, U.K.

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LED.2013.2287514

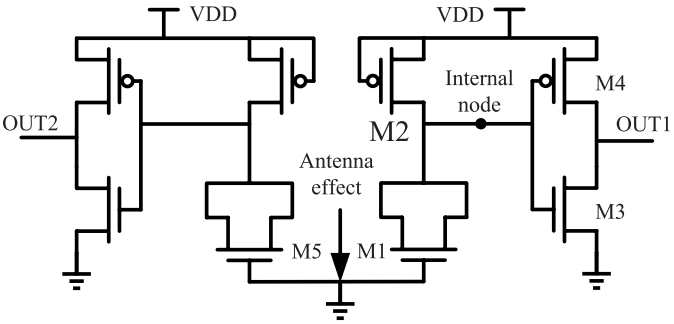

Fig. 1. Transistor level schematic of the proposed on-chip ID generation pair.

II. Proposed On-Chip ID Scheme

The schematic of the proposed ID generation pair is shown in Fig. 1. The basic ID bit consists of 2 subcells in which the NMOS transistor gates (M1 and M5) are connected together to the ground. A diode connected PMOS transistor M2 can sink a small leakage current and a digital inverter (M3 and M4) is used to buffer the digital ID number. Assuming one NMOS gate is broken down, the diffusion region of the NMOS transistor is shorted to the ground, thus the digital output OUT is '1'. If the NMOS transistor gate is not broken down, the PMOS transistor will pull up the internal node and as a result, OUT is '0'.

In order to true-randomly break down one gate in the transistor pair, we propose to use antenna effect during chip fabrication. Conventionally, if a transistor gate is connected to a large area of metal, via or contact without a leakage path, the charges during chip fabrication will be slowly accumulated and eventually break down the transistor gate which is addressed as oxide damage from gate charging during plasma processing [7], [8] or so called antenna effect in chip design stage [9]. In practice, antenna effect should be avoided to pass the design rule check. However, for ID generation, this negative effect could properly be used. In our circuit, we intentionally increase the metal, via and contact area without inserting a charge leakage path. With the charge accumulated, one of the NMOS gates is randomly broken down and the two gates will be eventually shorted to the diffusion region, thus a charge leakage path will be created through a parasitic diode illustrated as shown in the operating principle during the chip fabrication in Fig. 2. After gate broken down, no charge is further accumulated which can guarantee only one gate is broken down during chip fabrication process. In the latter fabrication stage, the two gates are grounded through the top metal which finalizes the schematic as shown in Fig. 1.

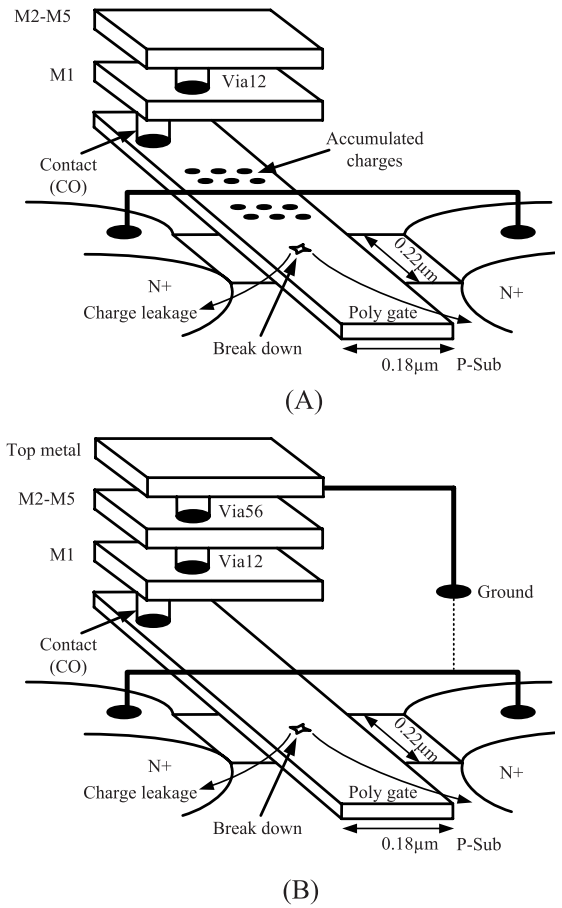

Fig. 2. Operating principle during the chip fabrication: (A) before top metal grounded (B) after top metal grounded.

III. Experimental Results

Fig. 3 shows the ID pair chip microphotograph. 64 ID pairs are fabricated in 0.18 μm CMOS process. The cell is designed with 30 μm/1.5 μm feature size and extra 40 μm is used to implement the scan D flip-flop chain. Metal 1 to Metal 5, Via 1-2 to Via 4-5 and contact (CO) layers are all fully used to maximize the gate break down chance. As a result, the via/gate area ratio is larger than 200 (<20 to pass design rule check), while the area ratio of CO/gate is larger than 250 (<10 to pass design rule check). It should be noted that, the area ratio in this letter is over-designed. After layout optimization, the cell area could be significantly reduced. If 100x antenna ratio can guarantee the gate oxide breakdown, the cell area could be reduced to 20 μm/1.5 μm. To further reduce the antenna ratio to 50x, the cell can be shrunk down to only 15 μm/1.5 μm. The optimization is not in linear scale because of the metal layer extension over the contact layer defined by the design rule and some fixed area occupied by transistors and wire connections.

The polarity of the ID series number is readout through a D flip-flop scan chain. The data in hexadecimal format of the generated ID from 20 chips are measured as shown in Table. I. The randomness of the generated ID is evaluated by analyzing the hamming distance which is defined as the amount of different bits between two chip ID binary numbers [10].

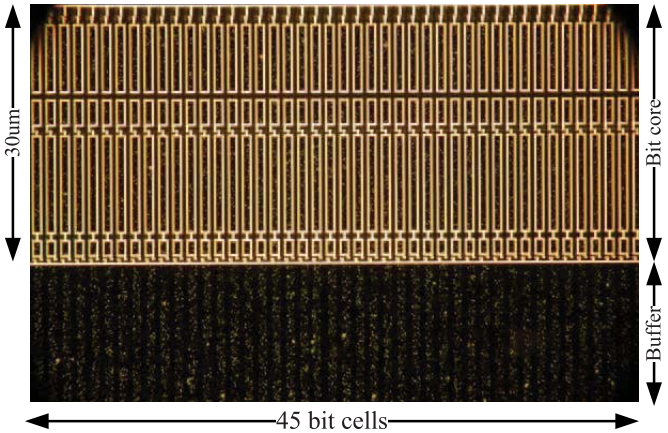

Fig. 3. Chip microphotograph.

TABLE I
Hexadecimal Format of the Measured ID

Chip 1	6BCEB81991675A51	Chip 11	9F536021CC27D9EF
Chip 2	E1E152A323E412D3	Chip 12	D17B5D47330FCA45
Chip 3	E32882F28F40C483	Chip 13	5E5C580555602148
Chip 4	3C1CF4210CFF286C	Chip 14	06B5FA84A4548463
Chip 5	DBAF0FD804F58A8E	Chip 15	B7E1CDB45D74C654
Chip 6	B76B2703E62DD6F0	Chip 16	65320E01BF1BC503
Chip 7	3074B03152CABCAA	Chip 17	331D6D0E9B8E39EB
Chip 8	2073BFEC9B13892F	Chip 18	725D5BA0BAFD0ADE
Chip 9	14A1E67DF108D4AC	Chip 19	A1668B2D68D2AA0E
Chip 10	0E8F4989747121E2	Chip 20	FC0451A0E048C28A

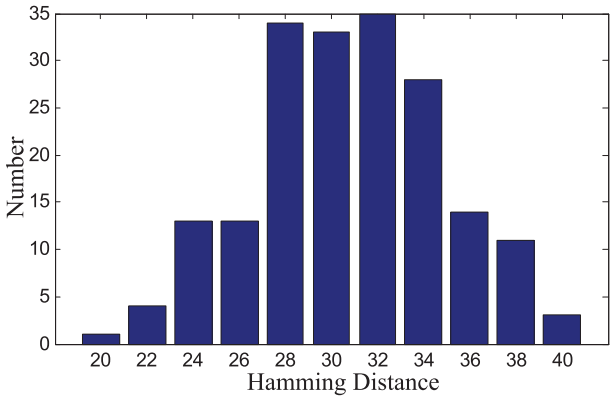

Fig. 4. Measured hamming distance from 20 dies.

Fig. 4 shows the measured hamming distance from the 20 chips, which indicates a distribution center near 32.3. The generated ID number is widely spread, unique and approximately shows an gaussian distribution as Eq. 1.

$$f(x) = \frac{1}{4.15\sqrt{2\pi}} e^{-\frac{(x-32.3)^2}{34.45}} \quad (1)$$

It should be mentioned that a shift of the ID number could be happened due to CMOS process variation during fabrication. Ideally, the mean size of the NMOS pair should be balanced in order to obtain a uniform '0' and '1' distribution across all ID bits and the peak of the hamming distance should

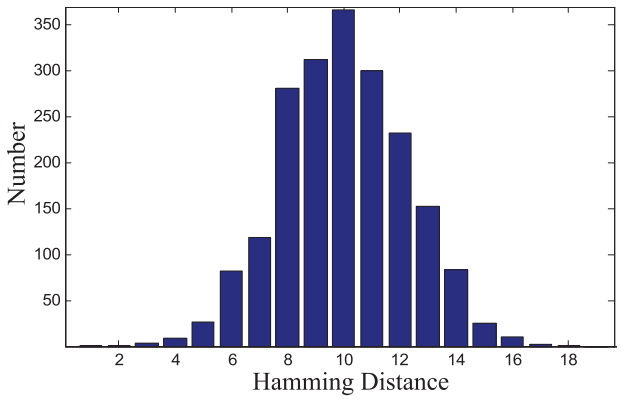

Fig. 5. Measured hamming distance from the reconstructed 64 ID strings.

TABLE II
RESULT COMPARISON

	This work	[3]	[4]	[6]
Technology	180 nm	130 nm	32 nm	65 nm
ID length	64-bit	128-bit	4K-bit	128-bit
Power	130 nW 1.2pJ/bit	162 nW 1.6pJ/bit	-	0.34pJ/bit
Aging	Ignorable	Unstable	Corrected	Ignorable
Environ. changes	Ignorable	Unstable	Corrected	Ignorable
Stabilization approach	Intrinsically stable	>3% unstable bits	Dynamic key algorithm	Post fabrication process
Principle	Antenna ID	SRAM	DRAM	Oxide ID
Cell Area	8-Transistor 45 μm^2	10-T. 71 μm^2	1-T. 0.039 μm^2	3-T. 3 μm^2

be located at 32 for 64 bit ID strings. However, due to the mask misalignment and process gradient effect on some device parameters such as the poly gate length, width and Cox, the mean value of the transistor size has some shift. This device parameter shift will directly contribute to a bias of the '0' '1' distribution. To improve the uniformity of the '0' '1' distribution, the layout of the proposed ID generation circuit should be carefully considered. Similar to a well matched analog amplifier MOS pair layout, dummy cell and symmetry are highly recommended to reduce the gradient effect. Ideally, four times larger size of the NMOS pair can enhance their matching by double. However, in order to keep the same antenna ratio, larger metal contact area should be adopted, leading to extra chip cost.

In order to verify the layout location dependency of the breakdown randomness, we reconstruct the ID number by grouping all bits with the same layout location from all 20 chips. Eventually 64 new ID strings with 20-bit width are created and 2016 hamming distance values are computed from these 64 ID strings, as shown in Fig. 5. It clearly indicates the mean value of the hamming distance near 10 and shows the generated ID is uniformly distributed in both the same chip and inter-chip, which proves the proposed ID generation circuit is insensitive to layout location.

The results compared with the prior arts summarized in Table II. The proposed work generates permanently stable ID number which is fixed during chip fabrication and can resist environment changes and aging. The generated ID is a true-random number without any post-fabricated process and on-chip algorithm. Similar to other schemes, the proposed work consumes power lower than 130 nW, which makes the proposed ID generation scheme suitable for passive RFID and sensor applications. Benefiting from smaller transistor size and thinner gate oxide, the proposed scheme could be easily scaled down to advanced technology nodes.

IV. CONCLUSION

In this letter, an on-chip ID generation scheme is proposed. By intentionally violating the design rule check against antenna effect, the proposed circuit can generate a true-random ID number during the chip fabrication process and without any post-fabrication manipulation and on-chip algorithm. The created ID is permanently stable and can resist environmental changes. The proposed chip is fabricated using 0.18 μm process. The ID number randomness is verified by the measured Hamming distance result from 20 dies. The proposed ID generation scheme consumes ignorable power providing a robust ID block for passive RFID and sensor applications.

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] J. W. Lee, D. Lim, B. Gassend, *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symp. VLSI Circuits, Dig. Tech. Papers*, Jun. 2004, pp. 176–179.
[3] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, Jan. 2008.
[4] S. Rosenblatt, D. Fainstein, A. Cestero, *et al.*, "Field tolerant dynamic intrinsic chip ID using 32 nm high-K/metal gate SOI embedded DRAM," *IEEE J. Solid-State Circuits*, vol. 48, no. 4, pp. 940–947, Apr. 2013.
[5] S. Chellappa, A. Dey, and L. T. Clark, "Improved circuits for microchip identification using SRAM mismatch," in *Proc. CICC*, Sep. 2011, pp. 1–4.
[6] N. Liu, S. Hanson, D. Sylvester, *et al.*, "OxID: On-chip one-time random ID generation using oxide breakdown," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2010, pp. 231–232.
[7] S. Fang and J. McVittie, "Thin-oxide damage from gate charging during plasma processing," *IEEE Electron Device Lett.*, vol. 13, no. 5, pp. 288–290, May 1992.
[8] H. Shin, K. Noguchi, and C. Hu, "Modeling oxide thickness dependence of charging damage by plasma processing," *IEEE Electron Device Lett.*, vol. 14, no. 11, pp. 509–511, Nov. 1993.
[9] W. Maly, C. Ouyang, S. Ghosh, *et al.*, "Detection of an antenna effect in VLSI designs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Syst.*, Nov. 1996, pp. 86–94.
[10] R. Divya and T. Thirumurugan, "A novel dynamic key management scheme based on hamming distance for wireless sensor networks," in *Proc. ICCCET*, Mar. 2011, pp. 181–185.