On-chip ID Generation for Multi-node Implantable Devices using SA-PUF

Chang Gao*, Sara Ghoreishizadeh*†, Yan Liu*†, Timothy Constandinou*†
*Department of Electrical and Electronic Engineering, Imperial College London, SW7 2BT, UK
†Centre for Bio-Inspired Technology, Institute of Biomedical Engineering, Imperial College London, SW7 2AZ, UK
Email: gaochangw@outlook.com, {s.ghoreishizadeh14, yan.liu06, t.constandinou}@imperial.ac.uk

***Abstract*—This paper presents a 64-bit on-chip identification system featuring low power consumption and randomness compensation for multi-node bio-implantable devices. A sense amplifier based bit-cell is proposed to realize the silicon physical unclonable function, providing a unique value whose probability has a uniform distribution and minimized influence from the temperature and supply variation. The entire system is designed and implemented in a typical 0.35 μm CMOS technology, including an array of 64 bit-cells, readout circuits, and digital controllers for data interfaces. Simulated results show that the proposed bit-cell design achieved a uniformity of 50.24% and a uniqueness of 50.03% for generated IDs. The system achieved an energy consumption of 6.0 pJ per bit with parallel outputs and 17.3 pJ per bit with serial outputs.**

I. Introduction

On-chip identification (ID) provides unique embedded code to address individual devices for further authentication and communication. In multi-node biomedical implants, such as integrated electrodes for bi-directional brain machine interface, this system plays important role in processing multi-site physiological recording signal and adaptive feedback stimulation for individual implant. A master or external controller need to use the ID to establish data interface between master devices and slave implants with secured authentication. Therefore, the integrated ID system need to generate IDs with high uniqueness, stable output, low power consumption, small silicon area occupied and without any special device or post-process. Among many possible solutions, silicon physical unclonable functions (PUF) is a desirable candidate.

A PUF is a system usually implemented in conventional IC technologies that exploit physical disorder properties throughout the fabrication process for authentication purposes and is impossible to be reproduced in a replica. In recent years, as a promising identification solution, many competitive PUF architectures have been proposed. To evaluate the identifiability of individual PUF architectures, uniqueness is one important quality metric measuring the randomness of IDs generated by the PUF. The definition of the uniqueness for a given PUF design is the average normalized inter-class Hamming distances (HD) of the generated ID [1], which is given as

$$\frac{2}{m\,(m-1)}\sum_{u=1}^{m-1}\sum_{v=u-1}^{m}\frac{HD\,(R_u,R_v)}{n}\times 100\%, \qquad (1)$$

where m denotes the number of independent chips having the same PUF design implemented on. u and v denote any pair of chips out of all possible pairs. n is the length of pairwise bits R_u and R_v. For an PUF with ideal performance, the uniqueness equals to 50%, which indicates that the PUF has the highest ability to identify chips. Another important metric is called reliability [1], which measures how stable the ID generated by the same chip is. It should be measured by using real chip samples and thus is beyond the scope of this paper since the design has not been taped out.

Common PUFs architectures vary mainly with sources of randomness. By utilizing process variation such as random dopant fluctuation or device mismatch, PUF circuits such as SRAMs [2] generate random bits at power-on states. High uniqueness and process compatibility features this type of PUFs; however, the circuits suffer from ambient noise and may generate unreliable IDs. Another group of PUFs based on oscillators are composed of inverter or XOR gate rings [1], which can achieve highly random ID generation at the expense of large circuit scale and dynamic power consumption. Some other PUFs utilize the breakdown of transistor gate oxide [3] [4] to burn IDs onto the chip, which results in permanent reliability. However, post-fabrication process are required for most of these approaches, which makes them less attractive.

For the purpose of realizing on-chip ID generation on multi-node biomedical implantable devices, the target system requires not only the quality of generated IDs, but also the ability to achieve ultra-low power consumption during runtime and low hardware complexity for small chip area. This paper presents a novel PUF structure, derived from common sense amplifiers (SAs) [5]. By adding two pre-charge PMOS and multiple input NMOS devices with the gates tied to the supply voltage acting as current sources, the modified circuit can generate random bits following the procedure of **Pre-charge**, **Generation** and **Readout**. Moreover, the full-custom design of a 64-bit on-chip ID generation system is designed and implemented in 0.35 μm CMOS technology.

II. SA-PUF Bit-Cell

A. Proposed Topology

A normal SA generates binary outputs by amplifying the tiny magnitude difference of input voltages of two bit lines. Similarly the proposed bit-cell, as shown in Fig. 1, generates random bits by using the current difference caused by mismatches between two branches of current sources. Two pre-charge PMOS devices, **MP3** and **MP4**, of which gates are controlled by signal **TRIG**, are connected in parallel respectively with the two PMOS devices (**MP1**, **MP2**) of the SA. The output nodes **VL** and **VR** are connected to two access NMOS devices, of which gates are under the control of signal **EN**. Under the SA, two branches of current sources are respectively connected to the source of **MN1**, **MN2**. Each branch is composed of four NMOS devices in parallel, and all gates are directly connected to the power supply **VDD** of 3.3 V. Moreover, two NMOS devices (**MN3**, **MN4**) acting as switches are added to avoid direct connection between **VL**, **VR** and the two current sources branch in order to limit the contention current during the switching of signal **TRIG**.

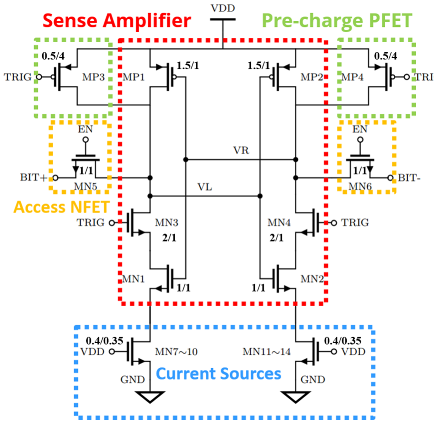


Fig. 1. Circuit of the proposed sense amplifier based PUF bit-cell with transistor size ratio W/L in μm

The principle of bit generation is to compare the difference of currents sinking into the two current source branches. Each branch contains four minimum sized transistors to maximize mismatch between current sources on each side. The other transistors in the bit-cell are all sized much larger than current source elements to reduce the effect of mismatch compared to the current source. By doing this, the polarity of the bit-cell is dominated by the mismatch of the current sources.

B. Bit Generation Scheme

The procedure of producing an ID bit follows the listed three steps:

1) **Pre-charge**: After the power-up of the cell, **TRIG** is first set to 0 to enable the two pre-charge PMOSes so that nodes **VL** and **VR** are charged and the voltage of both nodes are raised to **VDD**;
2) **Generation: TRIG** is then set to 1 to switch off the two pre-charge PMOSes. After that, nodes **VL** and **VR** start to discharge simultaneously. Any tiny difference of current between the two branches of current sources will leads to a final steady state $\{0, 1\}$ (0 for **BIT+**, 1 for **BIT-**) or $\{1, 0\}$.
3) **Readout:** After the bit-cell reach a steady state, **EN** is set to 1 to transfer the output values of the SA to bit lines.

C. Bit-Cell Uniformity

The uniformity of a bit-cell represents how random the generated bit is. For an ideal bit-cell, the polarity should be 0.5 in order to have the same possibility of generating 0 or 1. This is measured by the metric called "uniformity", which is defined as

$$\frac{1}{k}\sum_{i=1}^{k-1} R_i \times 100\%, \tag{2}$$

where R_i denotes the value of the i^{th} bit and k is the total time of execution of the bit generation scheme, which is clarified in the next section.

To achieve a bit-cell with high uniformity, the layout must be as symmetrical as possible because the polarity of the bit-cell is correlated with the total equivalent capacitance at nodes **VL** and **VR** in accordance with the following formula:

$$i = C\frac{dV}{dt}. \tag{3}$$

The equivalent circuit of the bit-cell during the **Generation** state is shown in Fig. 2.

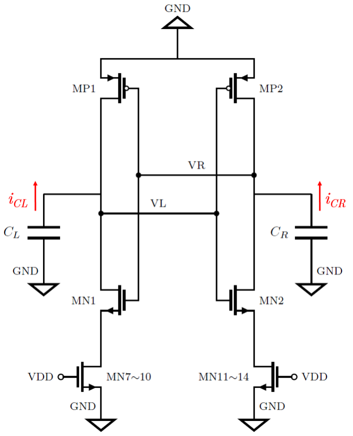


Fig. 2. Small signal equivalent circuit of the bit-cell in **Generation** state

The pre-charged PMOS and access NMOS devices are disabled during this phase. Since node **VL** and **VR** are pre-charged to **VDD**, **MP1** and **MP2** are turned off and **MN3** and **MN4** are turned on. C_L and C_R are the total equivalent parasitic capacitance at nodes **VL** and **VR**. According to Eq. 3, assuming that the rate of change of voltage across C_L and C_R are the same at the beginning of **Generation**, the two induced currents i_{CL} and i_{CR} are respectively proportional to the magnitude of capacitance of C_L and C_R. In this case, the inequality of the capacitance of C_L and C_R will result in a difference between i_{CL} and i_{CR}, which introduce a parasitic induced mismatch and interference the effect of current source.

In this case, to reduce parasitic influence, the layout of the bit-cell must be highly symmetrical for the regeneration cells. However, cross-wired interconnections **VL** and **VR** inevitably affect the symmetry of the layout. To compensate for it, excessive cross-wired interconnections can be implemented to balance parasitic capacitance at two nodes **VL** and **VR**. Moreover, guard rings are deployed for both PMOSes and NMOSes to isolate the bit-cell from the interference of adjacent circuits and noise,.

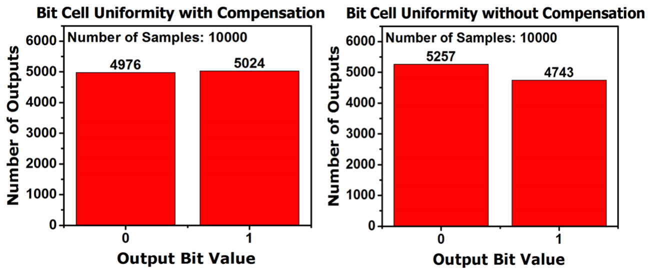


Fig. 3. Results of Monte Carlo simulation (VDD = 3.3 V, T = 28 °C) of 10000 samples on a bit-cell for the evaluation of uniformity with and without layout compensation

The Monte Carlo simulation results of uniformity with respect to compensation for a bit-cell is shown in Fig. 3. The uniformity of compensated samples is 50.24%, which is closer to 50% than that of uncompensated samples, which is 47.43%.

D. Robustness

The polarity changes against variations of temperature (T) and supply voltages (VDD) are shown in Fig. 4, and results are obtained by applying Monte Carlo sampling on 1000 times of transient simulation conducting the aforementioned bit generation procedure at each temperature or supply voltage value. Denoting R_{REF} and R_i the bit generated by single sample respectively under T_{ref}/VDD_{REF} or any other T/VDD, the number of samples with polarity shift is defined as the number of R_i that is not the same with R_{REF} at each T/VDD point. It reflects the stability of the code.

With the reference temperature (T_{ref}) set to 28 °C, in the first plot in Fig. 4, the percentage of samples with polarity shift, within the range of human body temperature (35 °C [6] $\sim$ 40 °C [7]), is from 0.45% to 0.80%. In this case, if the chip embedded with bit-cells is implanted into a human body, the polarity shift rate with respect to 37.5°, which is the midpoint of the body temperature range, is around ±0.175%.

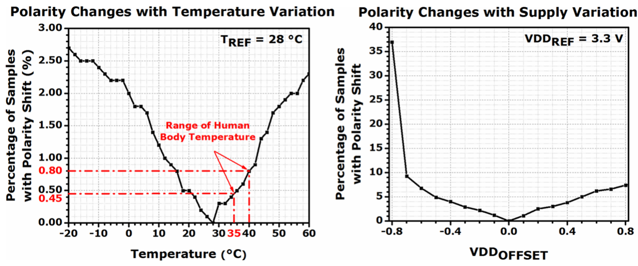


Fig. 4. Polarity changes with respect to the variation of temperature and supply voltage

The second plot in Fig. 4 depicts the polarity changes with respect to supply voltage variations and the reference supply voltage is set to be 3.3 V. According to results, the maximum polarity shift rate within a ±21% supply voltage deviation is 9.3% at VDD = 2.6 V (VDD$_{OFFSET}$ = -0.7 V). When the supply voltage is less than this magnitude, the bit-cell does not function normally.

III. ID Generation System

A. System Architecture

According to the functionality of blocks, the system is split into two parts, a **Generation** part and a **Readout** part. This is shown in the system-level block diagram in Fig. 5.

The **Generation** part is formed by a **64-Bit Array**, a buffer array called the **Trigger** and a finite-state machine as **Generation Controller**. The **64-Bit Array** contains 64 bit-cells arranged in a 8×8 matrix style, which occupies the majority of the area. Dummy cells are placed along the perimeter to protect the core array from ambient interference and to enhance the symmetry of the block. The **Trigger** is controlled by the **Generation Controller** to provide the signal **TRIG**, which is connected to gates of pre-charge PMOS devices of all bit-cells.

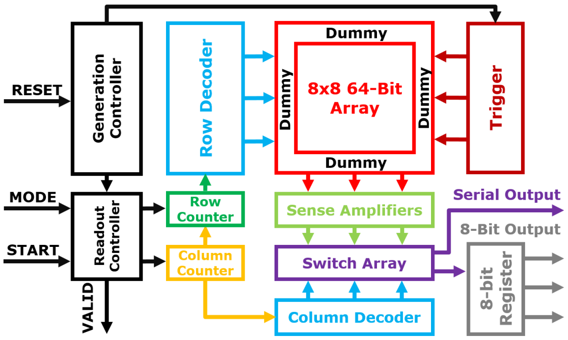


Fig. 5. Block diagram of the proposed ID generation system

All rest blocks belong to the readout part, in which the **Readout Controller** controls the collaboration between blocks and the timing of input and output signals. Two pairs of counter and decoder are respectively responsible for providing a row index and a column index for each generated bit in the array. 8 sense amplifiers formed an array for amplifying the minor voltage swing in bit lines and their complementary outputs are connected to the **Switch Array** to be divided into the **Serial Output** and the **8-Bit Output**. Each output port is finally synchronized by using a specially designed low power D-type Flip-Flop.

The layout of the final system excluding the pad ring is shown in Fig. 6. Totally 3 layers of metal (M1-M3) are used. M1 and M2 are used for connection within standard cells. M2 and M3 are used for most interconnections between cells or blocks. The dimension of the layout is 470 μm × 320 μm, which gives an approximate area of 0.15 mm^2.

B. System Performance

1) Uniqueness: By conducting Monte Carlo simulation on 1000 **Bit Array** samples at 30°C. the probability distributions

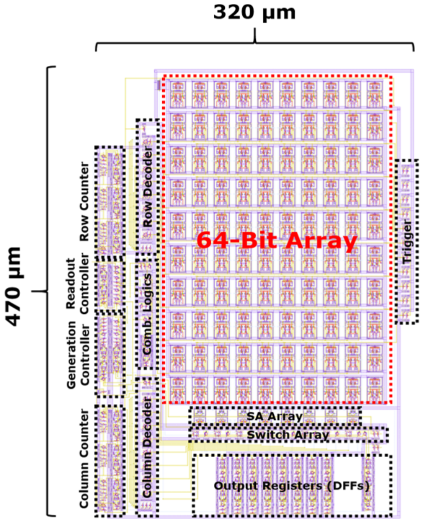
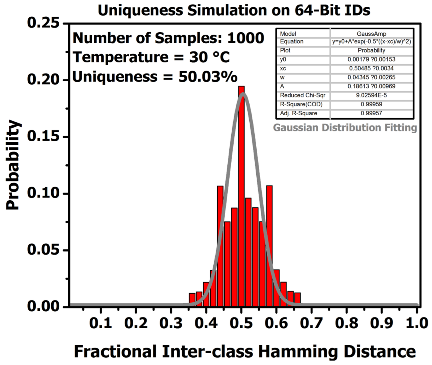


Fig. 6. Complete system layout with annotated floorplan

of fractional inter-class HD of generated IDs is shown in Fig. 7. The result shows an ID uniqueness of 50.03% and the simulation is also conducted at 20°C, 40°C and the results are 50.04% and 50.03% respectively.



Model	GaussAmp
Equation	y=y0+A*exp(-0.5*((x-xc)/w)^2)
Plot	Probability
y0	0.00179 ?0.00153
xc	0.50485 ?0.0034
w	0.04345 ?0.00265
A	0.18613 ?0.00969
Reduced Chi-Sqr	9.02594E-5
R-Square(COD)	0.99959
Adj. R-Square	0.99957

Fig. 7. Probability distribution of fractional inter-class hamming distance of generated IDs at 30°C

2) Power Consumption: The power consumption of the system is obtained from post layout simulation, and is shown in Table I. The results were measured from the power-up of the system to the moment when all bits are read out. The energy consumption in serial readout mode is distinctly higher that in the parallel readout mode, which is due to the usage of **Column Decoder** and **Column Counter** in the serial readout mode.

TABLE I
POWER CONSUMPTION OF THE SYSTEM (CLOCK FREQUENCY = 1 MHZ)

Mode	Energy/Bit	Average Power
Parallel	6.0 pJ	21.0 μW
Serial	17.3 pJ	8.0 μW

C. Comparison with Other Works

As shown in Table II, the proposed PUF system achieved the second highest uniqueness among all listed works. The energy consumption per bit for the parallel readout mode was used to be compared with other works. The work proposed by Tang et al. [4] achieved the lowest energy consumption per bit, but a more advanced technology is used.

TABLE II
PERFORMANCE COMPARISON WITH THE STATE-OF-THE-ART

	Uniqueness	Energy/Bit	Technology
This work (simulated)	50.04%	6.0 pJ	350 nm
Bhargava et al. [8]	50.00%	Not Available	65 nm
Su et al. [2]	50.13%	1.6 pJ	180 nm
Chen et al. [1]	50.90%	Not Available	Not Available
Lofstrom et al. [9]	Not Available	8330 pJ	350 nm
Tang et al. [4]	50.47%	1.2 pJ	180 nm
Liu et al. [3]	49.94%	Not Available	65 nm

IV. CONCLUSION

The proposed SA-PUF bit-cell has achieved the uniformity close to 50% and the good robustness with respect to the variation of human body temperature. Moreover, the design of an power-efficient 64-bit ID generation system with readout circuits is presented. According to evaluations through Monte Carlo simulations, IDs generated by the system has been demonstrated with high uniqueness compared to other works based on various PUF structures. With low power consumption and minimized silicon area occupied, this system is suitable for multi-node biomedical implants.

REFERENCES

[1] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rhrmair, "The bistable ring puf: A new architecture for strong physical unclonable functions," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, June 2011, pp. 134–141.

[2] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pj/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, Jan 2008.

[3] N. Liu, S. Hanson, D. Sylvester, and D. Blaauw, "Oxid: On-chip one-time random id generation using oxide breakdown," in *2010 Symposium on VLSI Circuits*, June 2010, pp. 231–232.

[4] F. Tang, D. G. Chen, B. Wang, A. Bermak, A. Amira, and S. Mohamad, "Cmos on-chip stable true-random id generation using antenna effect," *IEEE Electron Device Letters*, vol. 35, no. 1, pp. 54–56, Jan 2014.

[5] J. R. Baker, *CMOS: Circuit design, layout, and simulation - 3rd edition*, 3rd ed. United States: Wiley, John & Sons, 10 2010.

[6] J. A. Marx, R. S. Hockberger, R. M. Walls, M. H. Biros, D. F. Danzl, M. Gausche-Hill, A. Jagoda, FACEP, L. J. Ling, E. J. Newton, B. J. Zink, and A. P. of English John Marx, *Rosen's emergency medicine - concepts and clinical practice*, 8th ed. London: Elsevier, 05 2006.

[7] G. C. Cook, A. I. Zumla, J. Farrar, P. J. Hotez, and T. Junghanss, *Manson's Tropical Diseases: Expert Consult*. Saunders, 2008.

[8] M. Bhargava, C. Cakir, and K. Mai, "Attack resistant sense amplifier based pufs (sa-puf) with deterministic and controllable reliability of puf responses," in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*, June 2010, pp. 106–111.

[9] K. Lofstrom, W. R. Daasch, and D. Taylor, "Ic identification circuit using device mismatch," in *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International*, Feb 2000, pp. 372–373.