A Low-power Reliability Enhanced Arbiter Physical Unclonable Function Based on Current Starved Multiplexers

(Invited Paper)

Si Wang[1], Yuan Cao[2,3,*] and Chip-Hong Chang[1]
[1]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
[2]College of Internet of Things Engineering, Hohai University, Changzhou, China
[3]Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education
*Email:caoyuan0908@gmail.com

***Abstract*—Arbiter Physical Unclonable Function (APUF) is a popular lightweight strong PUF. The most criticized operational deficiency of APUF over other strong PUFs is its reliability against temperature and supply variations. In this paper, a novel low-power current starved (CS) multiplexer (MUX) based strong PUF is proposed. CS-MUX harnesses greater stochastic delay distribution from the manufacturing process variation than the CS inverter and regular MUX. Its output current can be controlled by a current mirror to minimize the energy consumption while desentizing the delay deviation against environmental variations. The proposed PUF design is simulated using 65nm CMOS technology. The results show that the power consumption of a 64-stage current starved MUX based PUF under nominal condition is only 2.1μW per challenge-response pair (CRP) at frequency of 20MHz which is equivalent to 0.105pJ per cycle. It has a reduction of 96.3% and 96.2% in energy per cycle compared with regular arbiter based and CS inverter based PUFs, respectively. Its worst-case reliability is 94.64% over a temperature range of $-5 \sim 100$ °C, which are 14.52% and 8.32% more reliable than regular arbiter based and CS inverter based PUFs, respectively. Its worst-case reliability over a supply voltage range of 1.1 $\sim$ 1.3V is 95.51%, which are 6% and 4.5% better than regular arbiter based and CS inverter based PUFs, respectively.**

I. Introduction

Since late 2000s, PUF has been a burgeoning technology in cryptography and security circles. Its tamper-sensitive physical disorder property eliminates the vulnerabilities of insecure storage and simplifies device authentication without the need for extensive computational capacity to process the keys in classical cryptographic primitives. The security of PUF resides in the irreproducibility of the intrinsic nanoscale structural disorder instead of a hard-to-solve mathematical problem. It utilizes the mismatches of electronic circuits to provide chip-unique responses to digital input words known as challenges. This challenge-response mapping mechanism cannot be Physical cloned or even duplicated by the original manufacturer [1]. Moreover, the confidential information that can be extracted from the PUF can only be produced when the device is powered on [2], [3], making it harder for invasive attacks.

PUFs can be dichotomized into weak and strong categories according to the size of their Challenge-Response Pair (CRP) space [1]. A weak PUF has a small number of CRPs, or its number of challenges increases linearly or polynomially with the number of fundamental blocks adjoined to form a PUF. It is normally used for random number and device key generation. In contrast, the number of CRPs of a strong PUF increases exponentially with the number of basic cells abutted to form a PUF [4]. It is thereby practically impossible to exhaustively collect all the CRPs within a realistic time. This attribute offers a variety of promising security applications.

Most strong PUFs are delay based because of their reduced complexity and ease of implementation. A typical representative is APUF [2]. An APUF establishes a digital race condition between two identically designed paths which include a series of switches controlled by the input challenge. The only asymmetric components are their delay mismatches that are the decisive factor to the result of the race. At the end of the delay chain, an arbiter is used to determine the winner and generate the corresponding response bit. While the entropy of PUF benefits from large stochastic device mismatches harvested from fabrication process variability, the susceptibility of path delay to dynamic environmental conditions has undesirable negative impact on uniqueness and reliability. Prodigious research activities have been attempted to improve the quality of APUFs. For example, the current starved (CS) inverter based PUF [5] enlarges the current deviation of the inverters in each stage to broaden the delay distribution induced by the fabrication process while improving its stability under environmental variations.

In this paper, we proposed a new CS multiplexer (MUX) based APUF. Current mirror is introduced into the MUX directly to more significantly broaden the delay distribution than using an extra pair of current-starved inverters without compromising the uniqueness. The optimal biasing voltage of current mirror is investigated to stabilize the PUF response against temperature and supply variations.

The rest of the paper is organized as follows. Section II

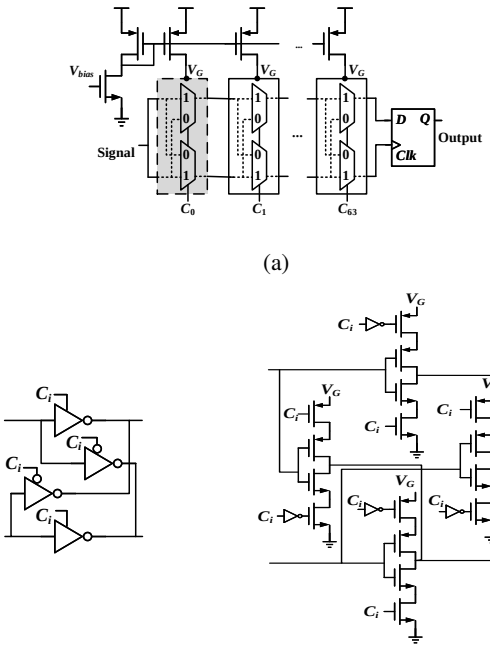

Fig. 1: (a) Basic architecture of proposed CS-MUX APUF. (b) Logic circuit of switch component. (c) Transistor-level implementation of (b).

describes the architecture of proposed PUF circuit. Section III presents and discusses the simulation results. Section IV concludes the paper.

II. Proposed PUF circuit

The architecture of our proposed PUF is shown in Fig. 1(a). By adding a current mirror to the basic architecture and replacing the conventional MUXs by CS-MUXs of a traditional APUF, the CS-MUX based APUF is formed. One extra transistor for each stage is used to control the drain current of the CS-MUX. Each switch consists of 4 tri-state inverters as shown in Fig. 1(b). The transistor-level schematic of Fig. 1(b) is detailed in Fig. 1(c). The current to each CS-MUX is supplied by the drain voltage of its corresponding mirrored transistor. C_i is the input challenge bit to the i-th CS-MUX. If C_i is 1, the two signals will travel from their respective input ports to the output ports in parallel though the i-th switch. If C_i is 0, the two signals will exchange paths. At the end of the CS-MUX chain, a positive edge-triggered D-flipflop is used to identify which signal has travelled through all the switches with a shorter delay and output a response bit accordingly. When the input signal is launched with a rising edge, the D-flipflop will output '0' if the signal in upper path arrives earlier. Otherwise, a '1' is produced.

The fundamental idea behind the proposed CS-MUX based PUF is to determine if there exists a value or range of values of V_{bias} that can reduce the output current, and at the same time, minimize the delay variation of each cell (CS-MUX) due to temperature and supply voltage variations. The delay of the CS-MUX can be approximated by the delay of the conducting tri-state inverter, which can be modelled by the regular inverter's delay expression as follows [6]:

TABLE I: Delay of different components used for construction of APUF

Metric(ps)	CS-MUX	CS Inv. [5]	Regular Inv.	Regular MUX
Mean	48.40	16.77	5.13	11.40
Standard Deviation	30.40	6.19	0.14	7.49

$$t_d = \frac{C_0 V_{dd}}{\eta I_D} \tag{1}$$

where C_0 is the total load capacitance, V_{dd} is the power supply voltage, η is a constant and I_D is the drain current of MOSFET.

From (1), reducing the thermal sensitivity of I_D will alleviate the change of propagation delay through the tri-state inverter due to temperature variation. This can be accomplished by making the temperature coefficient of current (TCC) [6] near zero. The TCC for both saturation region (TCC_{sat}) and subthreshold region (TCC_{sub}) of operation can be expressed as [6]:

$$TCC_{sat} = \frac{1}{I_D}\frac{\mathrm{d}I_D}{\mathrm{d}T} = \frac{1}{\mu}\frac{\mathrm{d}\mu}{\mathrm{d}T} - \frac{\alpha}{V_{GS}-V_t}\frac{\mathrm{d}V_t}{\mathrm{d}T} \tag{2}$$

$$TCC_{sub} = \frac{1}{\mu}\frac{\mathrm{d}\mu}{\mathrm{d}T} + \frac{2}{T} - \frac{q}{nk_BT}\left(\frac{\mathrm{d}V_t}{\mathrm{d}T} + \frac{V_{GS}-V_t}{T}\right) \tag{3}$$

where μ, α, V_{GS} and V_t are the mobility of majority charge carrier, velocity saturation index, gate-to-source voltage and threshold voltage, respectively. Among them, the two temperature dependent parameters, μ and V_t, can be expressed as [6]:

$$\mu(T) = \mu(T_0)\left(\frac{T}{T_0}\right)^{-\kappa} \tag{4}$$

$$V_t(T) = V_t(T_0) - \sigma(T - T_0) \tag{5}$$

where T_0, κ and σ are the reference temperature, the mobility temperature exponent that lies between 1.2 to 2 and mobility temperature coefficient of threshold voltage that lies between 0.5 to 3 mV/K.

TCC_{sat} and TCC_{sub} can be further simplified from (2) and (3) as follows:

$$TCC_{sat} = -\frac{\kappa}{T} + \frac{\alpha\sigma}{V_{GS}-V_t} \tag{6}$$

$$TCC_{sub} = \frac{2-\kappa}{T} - \frac{q}{nk_BT}\left(-\sigma + \frac{V_{GS}-V_t}{T}\right) \tag{7}$$

Since $V_{GS}-V_t < 0$ in the subthreshold region and $2-\kappa > 0$, TCC_{sub} is always positive and increases with decreasing V_{GS}. Furthermore, TCC_{sat} increases from negative to positive when V_{GS} decreases from a sufficiently large value. This implies that the transistors will operate in saturation region at zero TCC (ZTCC). Hence, V_{bias} should be set larger than V_t.

TABLE II: Power analysis @ nominal condition

Metric	CS-MUX	CS-Inv [5]	Regular [5]
Supply (V)	1.2	1.1	1.1
Tech. (nm)	65	45	45
Power (μW)	2.10	134	136
Freq. (MHz)	20	100	100
Energy (pJ/cycle)	0.11	1.34	1.36
Mapping to 65nm (pJ/cycle)	0.11	2.80	2.84

From [6], the effect of supply variation on delay of inverter operating in the saturation region can be analyzed by

$$t_d \propto \frac{V_{dd}}{(V_{GS} - V_t)^{\alpha}} \tag{8}$$

Since V_t decreases with increasing V_{dd} [6] due to the drain induced barrier lowering (DIBL) effect in short channel device and the value of α typically falls between 1 and 2, the nominator of (8) increases slower than the denominator. Hence, lowering V_{bias} in saturation region could lower the sensitivity of switching delay to supply voltage change. As V_t is around 0.45 V for the target technology, V_{bias} is set slightly above V_t to 0.5 V to counteract both supply voltage and temperature variations, as well as reducing the power consumption.

Table I compares the mean and standard deviation of delays under the nominal condition among CS-MUX, CS inverter [5], regular inverter and regular MUX. The results are obtained by simulating each circuit component over 100 Monte Carlo instances. From Table I, the mean of CS-MUX is $\sim$2.9$\times$ and its standard deviation is $\sim$4.9$\times$ those of the CS inverter. Its mean is $\sim$9.4$\times$ and standard deviation is $\sim$217$\times$ those of the normal inverter. Its mean and standard deviation are respectively $\sim$4.2$\times$ and $\sim$4.1$\times$ those of the regular MUX. The results show that similar or broader distribution of delay can be achieved without adding any extra inverters in the delay chain to improve the uniqueness.

III. Simulation results and discussions

A. Energy per cycle

The proposed CS-MUX based APUF is designed for TSMC 65nm CMOS process technology. It uses the same number of transistors as the 64-stage CS inverter based PUF. The power consumptions of different types of APUF are compared at nominal condition in Table II. Assuming that the energy consumption scales quadratically with the technology node due to shrinking geometries, the results show that the proposed CS-MUX APUF consumes significantly less energy per cycle than CS inverter APUF and regular APUF when they are mapped to the same 65nm CMOS technology node. It has a reduction of 96.3% in energy per cycle compared with regular APUF and a reduction of 96.2% in energy per cycle compared with CS inverter based PUF. This is attributed to the appropriate current limiting control by the current mirror.

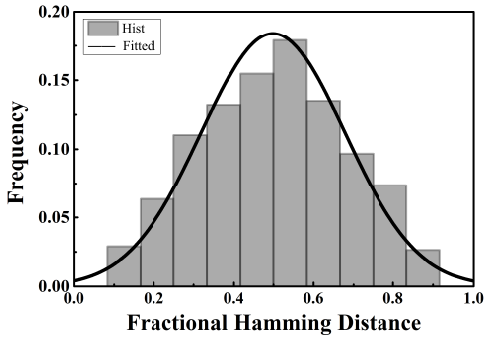

Fig. 2: Inter-die Hamming distance distribution of proposed CS-MUX based PUF (μ = 0.5013, σ = 0.1447).

B. Uniqueness

Uniqueness measures the ability to distinguish two identically designed PUF instances. The ideal uniqueness should be 50%, which means that on average half of the response bits produced by any two instances of a PUF to the same challenge are different. The uniqueness can be measured by the inter-die Hamming Distance (HD). Let R_u and R_v be the n-bit responses of two different chips, u and v, to the same challenge C, the uniqueness U for m chips is expressed as [6]:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \tag{9}$$

To evaluate the uniqueness, 128 random challenges are applied to 200 different PUF instances for the CS-MUX based APUF. The Hamming Distance distribution is shown in Fig. 2. The results show that the proposed CS-MUX PUF circuit has a mean HD closer to the ideal value than the regular APUF, which has a mean of 0.5029, and CS inverter APUF, which has a mean of 0.5086 [5].

C. Reliability

The reliability of a PUF circuit is its ability to maintain the same response for a given challenge over varying environmental conditions. It can be measured by the bit error rate (BER). Assume that R_i is an n-bit response to an input challenge C produced by a PUF instance i under the nominal operating condition. The same set of challenges are then applied k times to obtain the response $R_{i,j}$ for $j = 1, 2, \cdot, k$. The reliability S of chip i can be calculated by [6]:

$$S = 1 - BER = 1 - \frac{1}{k} \sum_{j=1}^{k} \frac{HD(R_i - R_{i,j})}{n} \times 100\% \tag{10}$$

Fig. 3 shows the reliability calculated from a set of random CRPs generated by three different types of APUF circuit under different temperatures. The results show that the CS-MUX based PUF circuit could produce more stable responses compared to the CS Inverter based PUF [5] and the regular

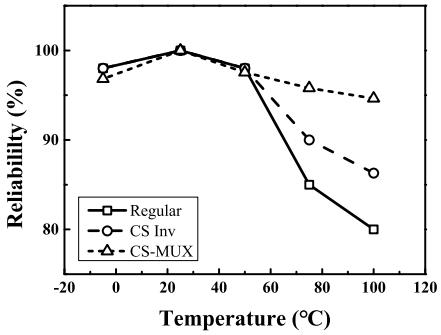

Fig. 3: Comparison of the proposed CS-MUX APUF, CS inverter APUF and regular APUF on reliability against temperature variations.

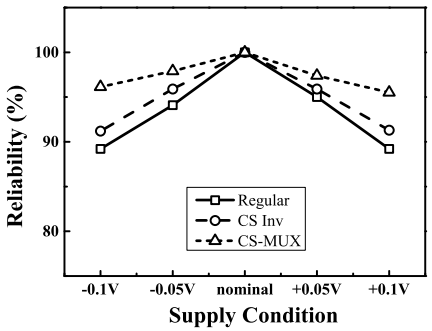

Fig. 4: Comparison of the CS-MUX APUF, CS APUF and regular APUF on reliability against supply voltage variations.

APUF [7]. It improves the worst-case reliability of regular APUF and CS Inverter based PUF by approximately 14.52% and 8.32%, respectively. This can be ascribed to the optimal biasing of CS-MUX by the current mirror to resist propagation delay variation against temperature changes.

Fig. 4 shows the influence of a $\pm$0.1V supply voltage fluctuation on the reliability of the three different types of APUF. The results imply that the responses of the proposed CS-MUX are less sensitive to the supply voltage noise than the other two types of APUF. Furthermore, the worst-case reliability has been raised from 89.2% for the regular APUF and 91.2% for the CS inverter based PUF to 95.5% for the proposed CS-MUX based PUF.

D. Randomness

Randomness refers to the ability to generate "0" and "1" bits with equal probability when random challenges are applied to a PUF circuit and the generated response bits are uncorrelated. It is often evaluated by the National Institute of Standards and Technology (NIST) test suite. Constrained by simulation time, only 10 sequences are generated, each of which consists of a 6500-bit response string. Hence, only 9 out of 15 tests are applicable. The results of the 9 statistical tests are shown in Table III. The minimum pass rate (PROP) for each statistical test is 8 for a sample size equal to 10 binary sequences. The results show that the proposed CS-MUX APUF passed all the 9 tests.

TABLE III: NIST randomness tests on responses of proposed CS-MUX APUF

Statistical	PROP	PASS?
Frequency	8/10	Y
BlockFrequency	8/10	Y
CumulativeSums(forward)	8/10	Y
CumulativeSums(backward)	8/10	Y
Runs	8/10	Y
LongestRun	9/10	Y
FFT	10/10	Y
ApproximateEntropy	9/10	Y
Serial(forward)	9/10	Y
Serial(backward)	9/10	Y
NonOverlappingTemplate	8/10	Y

TABLE IV: Comparison of the figures of merit of different APUFs

	Regular [5]	CS-Inv [5]	RG-DTM [8]	This work
Tech. (nm)	45	45	180	65
Uniqueness (%)	50.29	50.86	NA*	50.13
Worst Reliability (%)	80.12	86.32	NA	94.64
Temp Range (°C)	$-5\sim100$	$-5\sim100$	NA	$-5\sim100$
V_{dd} Range (V)	$1\sim1.2$	$1\sim1.2$	NA	$1.1\sim1.3$
Energy at 65 nm tech.(pJ/CRP)	2.838	2.796	0.548	0.105

* The mean value of uniqueness is not provided but the probability that another instance of the same type of PUF in [8] generates the same ID is provided as $3.9 \times 10^{-52}\%$.

IV. Conclusions

A novel low-power and robust CS-MUX based strong PUF is proposed in this paper. The optimal biasing voltage of current mirror is exploited to generate reliable responses under varying environmental conditions, amplify the stochastic effect of process variations and reduce energy consumption and power leakage to making accurate probing for side-channel analysis difficult. Table IV summarizes the comparison of figures of merit among the proposed work and three other types of APUFs. The proposed CS-MUX APUF consumes only 0.105pJ per CRP per cycle with higher reliability and better uniqueness compared to the state-of-the-art APUFs. These merits are attractive for the security application of resource constrained IoT devices.

Acknowledgement

This work was supported by the Singapore Ministry of Education AcRF Tier 2 Grant No. MOE 2015-T2-2-013 and the National Natural Science Foundation of China (Grant No.61601168).

References

[1] C.-H. Chang, Y. Zheng, and L. Zhang, "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," *IEEE Cir. Syst. Magazine*, vol. 17, no. 3, pp. 32–62, 2017.

[2] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. VLSI Syst.*, vol. 13, no. 10, pp. 1200–1205, 2005.

[3] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM Annual Design Automation Conf*, San Diego, CA, USA, Jun. 2007, pp. 9–14.
[4] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Proc. 2004 IEEE Symp. VLSI Circuits*, Honolulu, HI, USA, Jun. 2004, pp. 176–179.
[5] R. Kumar, V. C. Patil, and S. Kundu, "Design of unique and reliable physically unclonable functions based on current starved inverter chain," in *Proc. 2011 IEEE Int. Symp. VLSI (ISVLSI)*, Chennai, India, Jul. 2011, pp. 224–229.
[6] C. Q. Liu, Y. Cao, and C. H. Chang, "Acro-puf: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Trans. Cir. and Syst. I: Reg. Papers*, vol. 64, no. 12, pp. 3138–3149, 2017.
[7] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," in *Proc. 16th ACM/IEEE Int. Symp. Low Power Electronics Design*, Austin, TX, USA, Aug. 2010, pp. 43–48.
[8] K. Fruhashi, M. Shiozaki, A. Fukushima, T. Murayama, and T. Fujino, "The arbiter-puf with high uniqueness utilizing novel arbiter circuit with delay-time measurement," in *Proc. 2011 IEEE Int. Symp. Cir. Syst.*, Rio de Janeiro, Brazil, May 2011, pp. 2325–2328.