An Ultra-low Power and Lower Area Current-Mode based Physically Unclonable Function with less than 100nW Power Consumption and a Native Instability of 0.6875% for IoT Applications

Nikita Mirchandani, Nasim Shafiee, Yunsi Fei, and Aatmesh Shrivastava

Dept. of Electrical and Computer Engineering
Northeastern University, Boston, USA
{mirchandani.n, shafiee.n}@husky.neu.edu, {yfei,aatmesh}@ece.neu.edu

***Abstract*—This paper presents an ultra-low power and lower area, sequential physically unclonable function (PUF) circuit for Internet-of-Things (IoT). The proposed PUF is used to generate a 16 bit secret key array and uses a current-mode based differential bit cell architecture to exploit the inherent device mismatch. The proposed PUF design has an energy efficiency of $7.5fJ/bit$ and a native instability of 0.6875%.**

***Index Terms*—Ultra-low power, IoT, SoC, PUF, Security, AES, Cryptography.**

I. Introduction

Recent advances in Internet of Things (IoT) is leading to the deployment of a large number of sensing devices that are remotely located and widely distributed in our environment. These devices are easily accessible and vulnerable to hardware attacks. However, the existing security implementations, if any, for remotely located IoT devices are in very primitive stage. This issue is further exacerbated by the higher power and higher area of current security implementations for remote IoT devices that require ultra-low power (ULP) operation.

Physically unclonable functions (PUF) have become popular for implementing security down to the chip level. One of the functions of a PUF circuit is to generate a reliable secret key. Ideally, the key for a particular chip is repeatable but it cannot be predicted or measured. However, existing PUF implementations suffer from many non-idealities such as bit instability due to process, temperature, and voltage (PTV) variations, and instability due to device level noise in the circuits. They also suffer from poor statistical quality where the key is not purely random. Energy efficiency is another important specification for PUF particularly in the context of ULP IoT devices.

Most on-chip implementations of PUF exploit the random variation of device manufacturing to realize a purely random key. However circuit design approach, noise level, and layout considerations usually produce widely varied results. Recent research focuses on designing low power and low area PUFs to tackle IoT security challenges. PUF implementations include ring oscillator based [1]–[4], memory based [5]–[7], FPGA based [8]–[10], neural network based [11], and amplifier based circuit designs [12]–[15].

In [16], authors solve the instability produced by delay by applying differential clock signals and achieve an energy efficiency of $4fJ/bit$ and a bit error rate of 1.5%. The design is implemented in $14nm$ CMOS technology which suffers from higher cost and higher leakage power for an ULP IoT application. A DRAM based PUF circuit utilizes the randomness of the start-up of DRAM circuits to generate the key [7]. However it has more than 10% instability. The techniques discussed above mostly cater to high power mobile applications where higher performance of PUF circuits is required.

Recently, ULP circuits for implementing PUF are being discussed in literature. In [15], authors present a 2T transistor based multistage amplifier circuit to implement a key bit-cell. The circuit achieves a relative instability of 1.67% and an energy efficiency of $1.5fJ/bit$ for an isolated bit-cell. Amplifier based approach, where mismatch between devices is amplified, is also used to generate the key [12]–[14]. However, they too have higher power and higher area due to the need of a sense amplifier circuit to convert the device mismatch in to a digital logic level of one or a zero. In this paper, we present a current-mode based physically unclonable function (CM-PUF) designed with current mode based folded cascode amplifier circuit. Our simulation results show that it can achieve an energy efficiency of $7.5fJ/bit$ and a relative instability of 0.6875% which was simulated in the presence of transient noise.

II. Proposed CM-PUF Circuit Architecture

A. 1-bit PUF design

Our proposed circuit for generating 1-bit key is based on a folded cascode load based differential amplifier. It works based on the mismatch of input-pair transistors generated due to random variation in manufacturing. The mismatch in the differential pair gives rise to a current difference which is sourced to the folded cascode stage. Fig. 1 shows the detailed circuit architecture of the proposed CM-PUF circuit. To generate a n-bit key, n input pairs are used. Each input pair is selected sequentially.

In order to achieve high entropy, the amplifier needs to have a high gain. The circuit in Fig. 1 achieves high gain through the folded cascode stage. Due to a small mismatch between the input transistors, the current is not equally divided into branches with the same common mode input, V_{CM}. Therefore,

978-1-7281-8058-8/20/$31.00 ©2020 IEEE

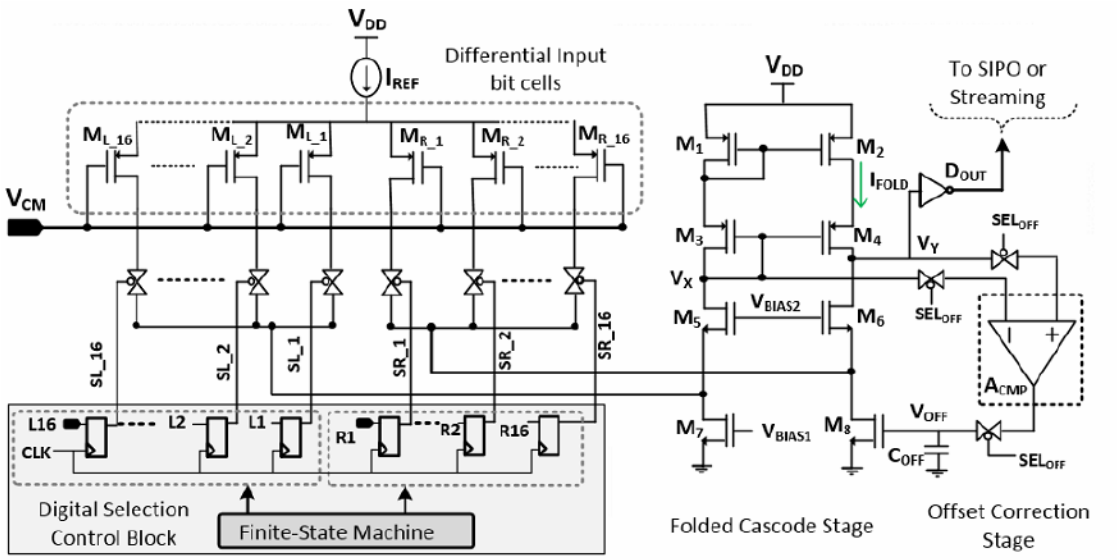


Fig. 1: Proposed architecture of CM-PUF circuit using a folded cascode differential amplifier and second-stage offset cancellation scheme.

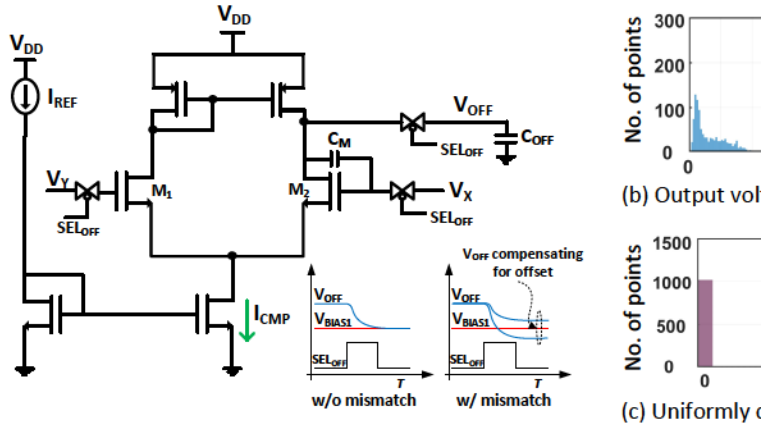
the current through one of the arms of diff-amp dominates over the other. The high gain load stage pulls up or pushes down the voltage V_Y, which results in a digitalized output at D_{OUT}. We achieve ULP operation of this circuit by utilizing sub-threshold biasing.

B. Offset corrected folded cascode 2^{nd} stage

The folded-cascode stage is used to achieve high gain of the PUF bit-cell. Higher gain helps in achieving higher entropy and better statistical quality. However, we cannot use this stage as a part of bit-cell due to higher area and power consumption. To reduce the area and power of the PUF, one instance of the folded cascode stage is shared among multiple bit cells. However this stage has its own mismatch which can result in reduced entropy.

In order to cancel the undesirable offset caused by the mismatch in the folded cascode stage, an offset compensation block as shown in Fig. 2 is utilized. The proposed circuit works in two different phases, compensation and comparison phase controlled by the signal Sel_{off}. During the compensation phase, input transistors are disconnected from the circuit. In case there is no mismatch in the folded cascode stage, both branches will have the same drain to source voltage across the transistors. Mismatch will result in voltage V_Y to go high or low.

The offset compensation scheme is shown in Fig. 2. A comparator compares the voltages V_X and V_Y and changes the bias voltage, V_{OFF}, at the gate of transistor M_8. If there is no mismatch in the load stage, then V_{OFF} equals V_{BIAS1}. If there is a mismatch between V_X and V_Y, then the V_{OFF} reaches the compensation value which balances the folded cascode stage to fully compensate the mismatch. Hence, the compensation block cancels the offset voltage and charges the capacitance C_{OFF} to work in the comparison phase. We also utilize a Miller capacitance and long channel length switches



(a) Circuit architecture of offset compensation Comparator

Fig. 2: Schematic of the offset compensation scheme used in load stage.

in the compensation block to stabilize the design and prevent further leakage currents.

In the comparison phase, the compensation block is disconnected and input transistors are connected to the load stage. The mismatch of the input pair now causes the voltage V_Y to be pulled up or down resulting in a digitized output at D_{OUT}. After the compensation phase, the input pair mismatch dominates the load stage offset. Hence, the proposed PUF works based on the mismatch between differential pairs only. Input transistors are designed to have small size to maximize the random mismatch, while higher device sizes are chosen for folded-cascode and comparator for better matching.

C. Enhancing relative stability

The PUF key is generated using the device mismatch between a differential pair. However, device noise can dominate over mismatch and result in a bit-flip leading to instability. In order to reduce the instability in the circuit, the noise component needs to be minimized while the mismatch component

needs to be maximized. The noise of the differential pair is reduced by increasing the bias current while device mismatch is increased by choosing minimum sized transistors. Small size transistors were chosen for the differential pair which is biased with $25nA$ bias current to provide very low noise voltage level.

The differential circuit was simulated with transient noise to incorporate 1000 noise seeds with cut-off frequency of $20kHz$ which is twice the amplifier bandwidth. The maximum value of input referred noise level was recorded for each seed. Fig. 3-(a) shows the distribution of the peak input-referred noise voltage. The peak input referred noise has a mean of $0.17mV$. Further, we also simulated input-referred offset voltage across 200 Monte Carlo mismatch simulations. The mismatch voltage output was converted to a probability distribution function. Fig. 3-(b) shows the probability of having input-offset below a given voltage. The probability of mismatch below the noise level of $0.17mV$ is 0.5%. This sets the lower level for the native instability of our circuit below 0.5%, which is in line with our simulated result of 0.6875%.

D. $n-$bit PUF design

To generate an $n-$bit key in a PUF design, other schemes [7], [8], [12], [14]–[16] repeat $1-$bit structure n times. However our proposed design utilizes only one folded cascode stage and offset correction stage structure with $n-$different pairs of input transistors. Each pair of input transistors participate in comparison phase followed by a compensation phase. The circuit measures the mismatch between the selected pair and generates a random digital output. For generating $n-$bit output, we only need to increase the number of differential pair as shown in Fig. 1. In order to select one pair of the transistors at a time, we have used a finite-state machine based register-bank to connect every bit of the register output to the switches corresponding to the pair. Each pair of transistors will be selected sequentially and realize one bit output. This way, the amount of power is constant despite increasing the number of PUF bits. Our power consumption is $100nW$. Another advantage of re-using the folded cascode stage is the reduced area. Since the load stage is not repeated for increasing number of bits, the area overhead is small for generating longer keys.

III. Simulation Results

The proposed PUF circuit was simulated in $130nm$ CMOS technology. The PUF structure generates a $16-$bit key array, using 16 input pairs. 8 such arrays can be used for generating

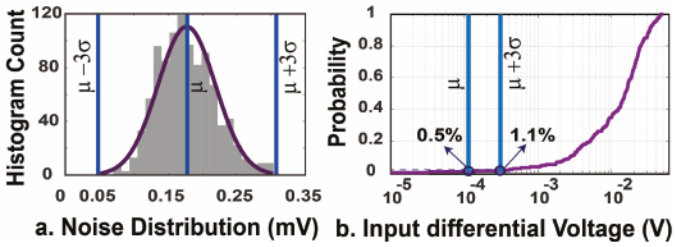


Fig. 3: (a)Histogram of input-referred noise (b) Probability distribution of input-referred offset.

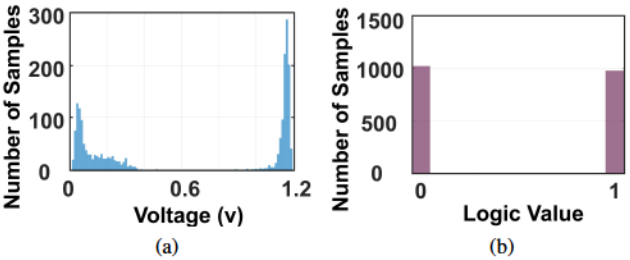
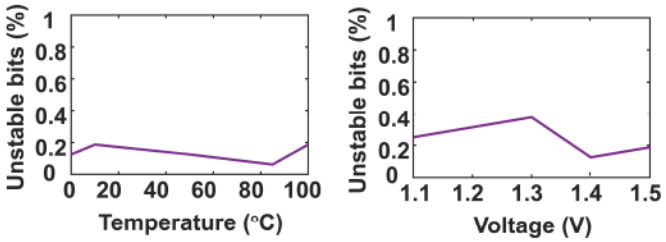


Fig. 4: Statistical distribution of output voltages before and after digitalization across 2000 mismatch simulation points. (a) Output voltage distribution at V_Y (b) Output voltage distribution at D_{OUT}



(a) Temperature instability with noise (b) voltage instability with noise

Fig. 5: Percentage of unstable bits when applying noise in different temperature and voltage values.

$128-$bit key. Fig. 4a shows the amplifier output,V_Y. The statistical distribution simulation was performed for a $1-$bit key in the presence of process and mismatch variations for 2000 points. Fig. 4b shows the output, D_{OUT}, after digitization by an inverter with almost equal distribution for ones and zeros.

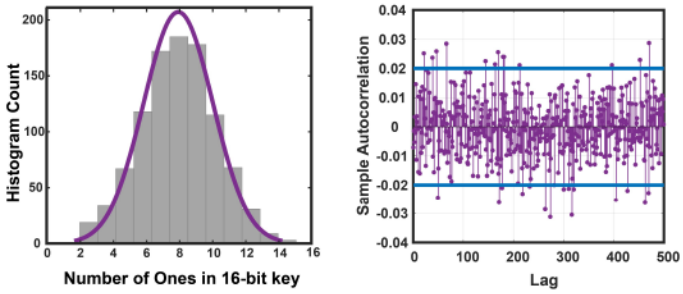
To measure stability under nominal condition ($1.2V$, 27^oC), we evaluated our design under transient noise simulation. We first obtained the key with a mismatch simulation where noise was disabled. After that we enabled transient noise simulation and compared the new key with the key without mismatch. We used this simulation set-up to obtain relative instability which came out to be 0.6875%. An important performance metric for PUFs is the Intra-PUF Hamming Distance. It measures the reliability of the PUF when subjected to different environmental conditions. It is measured by repeated observations of the same chip under different conditions. Since this paper presents preliminary simulation results for CM-PUF, we estimate Intra-chip Hamming Distance by testing our design against voltage and temperature variations in the presence of noise (Fig 5a, 5b). The uniqueness of the PUF is measured by the Inter-PUF Hamming distance by measuring the variation in responses of different PUFs under the same environmental conditions. This test is done on hardware and is simulated here using Monte Carlo process variations.

Fig. 5a and Fig. 5b show the number of unstable bits under process and voltage variation with transient noise enabled. We evaluated our proposed design under auto correlation function (ACF) to show that keys which are generated by 10000 Monte

TABLE I: Comparison Table

	Proposed *	PTAT [14]	Current Mirror [12]	2-Transistor [15]	Delay-Hardened [16]
Technology	130nm	65nm	65nm	180nm	14nm
Energy/bit (fJ/bit)	7.5	1100	15	11.3	4
Native Instability(%)	0.688	2	2.34	1.65	5.76
Entropy	0.99989	N/A	0.9967	N/A	0.99993
Bitcell area (μm^2)	3.14	3.07	25.35	17.9	1.84
Autocorrelation Function	0.0181	0.0188	0.0363	0.0173	N/A

* Simulation results



(a) (b)

Fig. 6: (a) Ones Distribution in 16-bit key for 1000 Monte Carlo simulation (b) Autocorrelation function with 0.98 confidence bound

Carlo simulations (Mismatch and Process) do not have any correlation. Fig.6b shows the result of ACF at 98% confidence level. The value of ACF is equal to 0.0181 which is close to the ideal ACF value of 0.

In order to measure the output uniformity, the normal distribution of ones was evaluated by a 1000 Monte Carlo simulation (Mismatch and Process) which has a mean of 7.957 as shown in Fig. 6a. The distribution shows that the output of the proposed PUF design has acceptable random behavior. Our PUF circuit generates a more random and stable key to make it more difficult to attack a hardware. We compare our results to the state of the art counterparts in Table I. Our proposed design has a reduced power consumption when compared to similar works. We achieve an $7.5fJ/bit$ energy efficiency which is better or comparable with other works. Our relative instability is 0.6875%. The total area of the 16 bit PUF is $50 \times 50\mu m^2$.

IV. Conclusion

In this paper, we present an ULP and low area CM-PUF design. Our design takes advantage of mismatch between differential pair with a folded cascode amplifier with a shared load stage. The offset of the load stage is compensated Our design also achieves $7.5fJ/bit$ energy efficiency and 0.6875% relative instability.

References

[1] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, Oct 2005.

[2] T. Tanamoto, S. Yasuda, S. Takaya, and S. Fujita, "Physically unclonable function using an initial waveform of ring oscillators," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 7, pp. 827–831, July 2017.

[3] M. Yoshinaga, H. Awano, M. Hiromoto, and T. Sato, "Physically unclonable function using rtn-induced delay fluctuation in ring oscillators," in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2016, pp. 2619–2622.

[4] A. Alvarez, W. Zhao, and M. Alioto, "14.3 15fj/b static physically unclonable functions for secure chip identification with x003c;2and 140 x00d7; inter/intra puf hamming distance separation in 65nm," in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, Feb 2015, pp. 1–3.

[5] Y. Pang, H. Wu, B. Gao, R. Liu, S. Wang, S. Yu, A. Chen, and H. Qian, "Design and optimization of strong physical unclonable function (puf) based on rram array," in *2017 International Symposium on VLSI Technology, Systems and Application (VLSI-TSA)*, April 2017, pp. 1–2.

[6] J. Li, T. Yang, and M. Seok, "A technique to transform 6t-sram arrays into robust analog puf with minimal overhead," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2017, pp. 1–4.

[7] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "Dram-based intrinsic physically unclonable functions for system-level security and authentication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 1085–1097, March 2017.

[8] L. Feiten, J. Oesterle, T. Martin, M. Sauer, and B. Becker, "Systemic frequency biases in ring oscillator pufs on fpgas," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 174–185, July 2016.

[9] R. S. Chakraborty, R. R. Jeldi, I. Saha, and J. Mathew, "Binary decision diagram assisted modeling of fpga-based physically unclonable function by genetic programming," *IEEE Transactions on Computers*, vol. 66, no. 6, pp. 971–981, June 2017.

[10] C. Gu and M. O'Neill, "Ultra-compact and robust fpga-based puf identification generator," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2015, pp. 934–937.

[11] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "8.7 physically unclonable function for secure key generation with a key error rate of 2e-38 in 45nm smart-card chips," in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, Jan 2016, pp. 158–160.

[12] A. B. Alvarez, W. Zhao, and M. Alioto, "Static physically unclonable functions for secure chip identification with 1.9 x2013;5.80.6 x2013;1 v and 15 fj/bit in 65 nm," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, March 2016.

[13] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant ro-puf for reliable key generation," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 335–348, July 2016.

[14] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 9, pp. 2192–2202, Sept 2016.

[15] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "8.3 a 553f2 2-transistor amplifier-based physically unclonable function (puf) with 1.67instability," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, Feb 2017, pp. 146–147.

[16] S. Satpathy, S. K. Mathew, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, R. K. Krishnamurthy, and V. K. De, "A 4-fj/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate cmos," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 4, pp. 940–949, April 2017.