Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm CMOS

S. Tao✉ and E. Dubrova

Physical unclonable functions (PUFs) are promising hardware security primitives suitable for resource-constrained devices requiring lightweight cryptographic methods. This Letter proposes an ultra-low-power and reliable PUF based on a customised dynamic two-stage comparator operating in the sub-threshold region. The proposed PUF is implemented in a standard 65 nm CMOS technology and validated through Monte-Carlo simulations. Evaluation results show a worst-case reliability of 98.3% over the commercial temperature range of 0°C to 85°C and 10% fluctuations in supply voltage. In addition, the 128-bit PUF array consumes only 1.33 µW at 1 Mb/s, which corresponds to 10.3 fJ/bit, being the most energy-efficient design to date.

Introduction: Physical unclonable functions (PUFs) make use of the inherent process variation in physical devices to generate unique chip IDs or secure keys. For reliable identification/authentication, PUFs should be robust against varying operating environment conditions. Moreover, silicon PUFs are usually integrated into radio-frequency identification (RFID) tags and smart card ICs [1], which are powered by battery or even harvested energy. Therefore, the circuit implementation of these PUFs must be highly energy-efficient.

Silicon PUFs developed up to now, either delay based (e.g. ring oscillator- and arbiter-PUFs) or memory based (e.g. SRAM-PUFs), mostly employ standard logic cells for circuit implementation. These conventional PUF designs have no flexibility to size the transistors for power/performance optimisation. In addition, they are generally very sensitive to environmental variations resulting in significantly increased errors in response bits. To improve the reliability, a few customised PUF implementations have been reported [2, 3], which rely on analogue/static circuit blocks. In this work, we take a step further by proposing a PUF design that does not only show sufficient uniqueness and reliability, but also achieves excellent energy-efficiency.

PUF architecture: Fig. 1 depicts the block diagram of the proposed PUF. The PUF array is composed of 128 identical PUF bit-cells that can provide 128-bit readouts at the clock rate of 1 MHz. Each PUF bit-cell is designed based on a dynamic two-stage comparator [4] and optimised to generate unique and reliable digital response. This bit-cell circuit consumes only transient current, which is proportional to the clock rate. To maximise the local mismatch and hence the reliability of the PUF, transistors are biased in the sub-threshold region. Since such a PUF architecture does not need any challenge to produce responses, it can be considered as inherently resistant to modelling attacks.

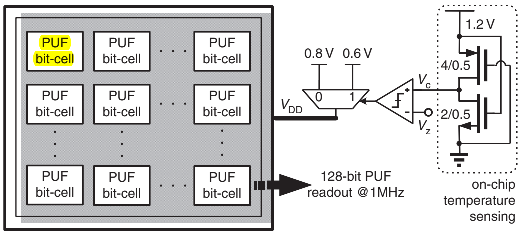

Fig. 1 *Block diagram of the temperature compensated PUF array*

To ensure the reliability of PUF responses at sub-zero temperatures, a simple temperature compensation scheme is applied. On one hand, the threshold voltage of CMOS transistors, V_{th}, decreases almost linearly with the increase in temperature. On the other hand, due to the drain-induced barrier lowering effect in sub-100 nm CMOS technology, the threshold voltage reduces approximately linearly along with the drain-to-source voltage, V_{ds}. This effect has a huge impact in the sub-threshold region due to the exponential relation between drain current and threshold voltage. If we adjust the V_{ds} of the transistors according to the temperature changes, then we can compensate for the significant variation in V_{th} at extreme temperature. The on-chip temperature sensing circuit shown in Fig. 1 generates an output voltage, V_c, which is proportional to temperature [5]. This proportional to absolute temperature voltage is then compared with a zero-temperature threshold, V_z. The comparison result, in turn, switches the V_{DD} from the nominal value of 0.6 to 0.8 V when the sensed temperature goes below zero degrees.

Circuit implementation: Fig. 2 illustrates the PUF bit-cell circuit implementation. It is composed of three stages. Stage 1 is the core of the PUF circuit, which detects the mismatch between the two input transistors M_a and M_b and converts it to a differential output at nodes 1 and 2. M_a and M_b are sized to achieve a large local mismatch in order to improve the reliability of the PUF response. By increasing the width of M_1, the delay of the PUF bit-cell can be further reduced at the expense of an increased offset. Stage 2 amplifies the sensed mismatch into a rail-to-rail output at nodes 3 and 4 using a positive feedback latched comparator. Stage 3 employs a NAND gate based SR latch to keep the final PUF output response stable over the full clock cycle.

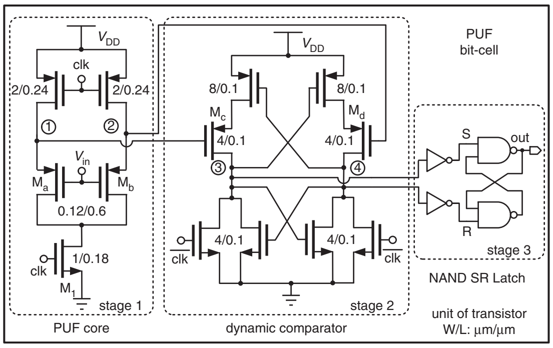

Fig. 2 *Schematic of the proposed PUF bit-cell*

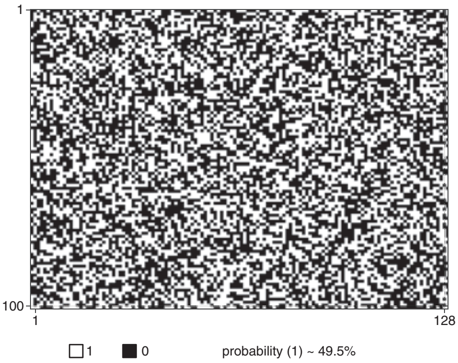

Fig. 3 *Monte Carlo simulation results: 128×100 PUF response bits*

The tail transistor M_1 is connected to the clock instead of a commonly used DC bias. M_1 is dimensioned in a way to make M_a and M_b work in the sub-threshold region, both reducing the current consumption and further maximising the device mismatch. When clk is low, nodes 1 and ② are pulled up to V_{DD} while nodes ③ and ④ are pulled down to ground. A rising edge at clk starts biasing M_1 and activating the operation of stage 1. At nodes ① and ②, the differential voltage starts increasing while the common-mode voltage starts decreasing. As long as the common-mode voltage goes down to the V_{th} of M_c and M_d, stage 2 will start latching. Since the second stage employs positive feedback, even a very small mismatch between the input transistors can be amplified into a large swing digital value. The positive feedback also minimises the static power consumption compared with the solution using an amplifier. Therefore, compared with existing PUF IC solutions based on static operation [2, 3], the proposed PUF bit-cell implementation is more energy-efficient as both stages consume no static power.

Evaluation results: The proposed PUF circuit was implemented in a standard 65 nm CMOS technology and simulated using Cadence Spectre®. To emulate the characterisation of 100 different PUF IC chips, 100 runs of Monte-Carlo simulation were performed. Both the intra-die and inter-die process variation flags were set during the simulation. The input of each PUF bit-cell, V_{in}, was tied to a 350 mV DC source. The nominal operating condition of the evaluation was at 25°C with a 0.6 V supply voltage.

We first evaluate the uniformity of the PUF responses at the nominal operating condition. Fig. 3 shows the 128-bit PUF responses from 100

PUF instances. A black pixel can be interpreted as a logic 1 and a white one as a logic 0. As the probability of generating ones is close to the ideal value of 50%, it indicates that the PUF output is not predictable and thus hard to attack. Uniqueness is another important security metrics, which measures how easily a PUF IC instance can be differentiated from others. The uniqueness of a PUF design is accessed by the Hamming distance (HD) among the responses of different IC instances. Obtained from 100 instances of the 128-bit PUF, totally $100 \times 99/2 = 4950$ comparisons are used to obtain the HD. As shown in Fig. 4, the mean HD is 64.09, corresponding to a uniqueness of 50.04%.

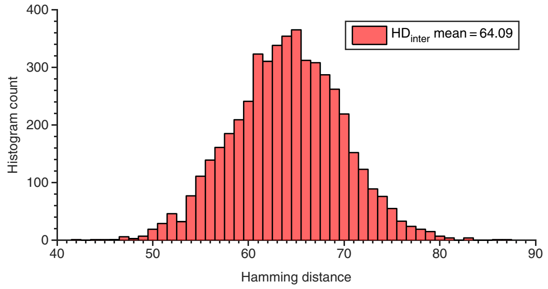

Fig. 4 *Inter-chip HD statistical distribution*

Reliability of a PUF design measures its ability to produce the same responses under varying environmental conditions, e.g. temperature and supply voltage. We first examine the reliability through measuring the bit-error-rate (BER) of the responses from the same PUF instance over a wide range of temperatures. The ground truth responses used to calculate the BER are obtained from 100 PUF instances at the nominal operating condition (25°C and 0.6 V). Then, responses from the same 100 PUF instances are extracted at a different operating condition. The BER of the PUF response versus temperature is shown in Fig. 5. Over the commercial range (0°C−85°C), the average reliability calculated from 100 PUF instances is 99.05%, and the worst-case reliability is 98.56% at 0°C. In addition, when the aforementioned temperature compensation scheme is applied, the BER is <3.2% over the entire industrial range (−40°C−100°C). It is also important to evaluate the impact of supply voltage noise on the reliability. A supply voltage variation up to $\pm 20\% V_{DD}$ is applied to the proposed PUF circuit at 25°C. As shown in Table 1, with 10 and 20% voltage changes from 0.6 V nominal supply, the worst-case BER of the PUF response is 1.7 and 3.69%, respectively.

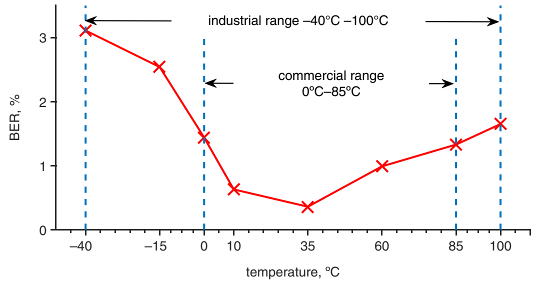

Fig. 5 *BER over the industrial and commercial temperature ranges*

Table 1: BER, P_{tot} and E_{bit} of the PUF over ±20% supply variation

V_{DD} [V]	0.48	0.51	0.54	0.57	0.60	0.63	0.66	0.69	0.72
BER [%]	3.69	3.10	1.70	0.82	–	0.48	0.92	1.08	1.27
P_{tot} [µW]	0.88	1.03	1.16	1.25	1.33	1.42	1.50	1.63	1.80
E_{bit} [fJ/b]	6.9	8.1	9.0	9.7	10.3	10.9	11.7	12.8	14.1

Energy/power consumption of a PUF design is a very important figure-of-merit for resource-constrained devices. Table 1 provides the total power consumption, P_{tot}, and the corresponding energy efficiency, E_{bit}, averaged from 100 PUF instances. The energy efficiency is calculated as: $E_{bit} = I_{avr} \times V_{DD}/f_{clk}$, where I_{avr} denotes the average current consumed to produce a response bit. The achieved E_{bit} over varying supply voltages is <14.1 fJ/bit. A comparison of energy efficiency of the presented PUF design with the state-of-the-art is shown in Fig. 6. The most representative CMOS PUF ICs published in recent 10 years have been included in this comparison. At the nominal operating condition, the proposed PUF achieves an E_{bit} of 10.3 fJ/bit, being the best compared with existing implementations.

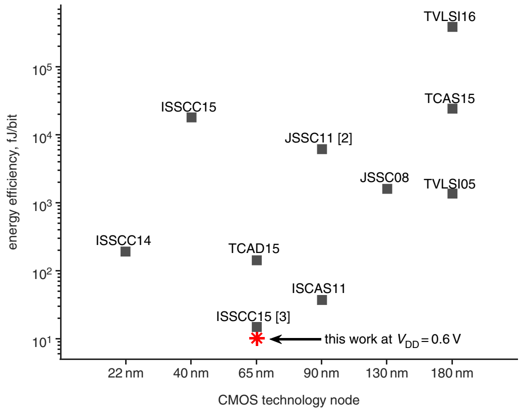

Fig. 6 *E_{bit} comparison with state-of-the-art CMOS PUF ICs*

Conclusion: A low-cost CMOS PUF that generates unique and reliable 128-bit chip IDs has been introduced and evaluated. Based on a two-stage comparator, the PUF bit-cell circuit is optimised to achieve maximum local mismatch and power efficiency. Moreover, a simple temperature compensation scheme is applied to provide improved stability for the PUF response at sub-zero temperatures. The PUF IC demonstrates close to ideal uniqueness and uniformity at the nominal condition. The reliability of the PUF is also verified under varying supply voltages of $\pm 20\% V_{DD}$ and at temperatures between −40°C and 100°C. Moreover, the PUF implementation achieves significant improvements in energy efficiency over existing PUF ICs. This demonstrates the great potential of the proposed PUF to provide affordable security for energy-constrained devices, such as wireless sensor nodes and RFID tags.

Acknowledgment: This work was supported in part by the research grant no. SM14-0016 from the Swedish Foundation for Strategic Research (SSF).

Submitted: *28 January 2016* E-first: *18 April 2016*
doi: 10.1049/el.2016.0292
One or more of the Figures in this Letter are available in colour online.

S. Tao and E. Dubrova (*School of ICT, KTH Royal Institute of Technology, Kista 16440, Stockholm, Sweden*)

✉ E-mail: stao@kth.se

References

1 Choi, B.D., Kim, T.W., and Kim, D.K.: 'Zero bit error rate ID generation circuit using via formation probability in 0.18 µm CMOS process', *Electron. Lett.*, 2014, **50**, (2), pp. 876–877

2 Stanzione, S., Puntin, D., and Iannaccone, G.: 'CMOS silicon physical unclonable functions based on intrinsic process variability', *IEEE J. Solid-State Circuits*, 2011, **46**, (6), pp. 1456–1463

3 Alvarez, A., Zhao, W., and Alioto, M.: '15 fJ/bit static physically unclonable functions for secure chip identification with <2% native bit instability and 140x inter/Intra PUF Hamming distance separation in 65 nm'. Proc. IEEE Int. Solid-State Circuits Conf., San Francisco, CA, USA, February 2015, pp. 256–258

4 Van, E.M., Van, T.E., Geraedts, P., *et al.*: 'A 10-bit charge-redistribution ADC consuming 1.9 µW at 1Ms/s', *IEEE J. Solid-State Circuits*, 2010, **45**, (5), pp. 1007–1015

5 Cortez, M., Member, S., Hamdioui, S., *et al.*: 'Intelligent voltage ramp-up time adaptation for temperature noise reduction on memory-based PUF systems', *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, 2015, **34**, (7), pp. 1162–1175