This is the accepted version of a paper published in *Electronics Letters*. This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the original published paper (version of record):

Tao, S., Dubrova, E. (2016)
An Ultra-Energy-Efficient Temperature-Stable Physical Unclonable Function in 65nm CMOS.
*Electronics Letters*

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-183776
An Ultra-Energy-Efficient Temperature-Stable Physical Unclonable Function in 65nm 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 customized dynamic two-stage comparator operating in the sub-threshold region. The proposed PUF is implemented in a standard 65nm 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 pW at 1 MHz, 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-PUF), 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 customized 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 optimized to generate unique and reliable digital response. This bit-cell circuit consumes only transient current, which is proportional to the clock frequency. 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 (DBLB) effect in sub-100nm 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 $V_{th}$ 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, $V_{out}$, which is proportional to temperature [5]. This proportional to absolute temperature (PTAT) voltage is then compared to a zero-temperature threshold, $V_{ref}$. The comparison result, in turn, switches the $V_{DD}$ from the nominal value of 0.6 V 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 $\overline{a}$ and $\overline{b}$. $M_a$ 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 $M_a$, 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 $\overline{a}$ and $\overline{b}$ 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.

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 maximizing the device mismatch. When $clk$ is low, nodes $\overline{a}$ and $\overline{b}$ are pulled up to $V_{DD}$ while nodes $a$ and $b$ are pulled down to ground. A rising edge at $clk$ starts biasing $M_1$ and activating the operation of stage 1. At nodes $\overline{a}$ and $\overline{b}$, the differential voltage starts increasing while the common-mode voltage stays decreasing. As long as the common-mode voltage goes down to $V_{th}$ of $M_a$ and $M_b$, 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 maximizes the static power consumption compared to the solution using an amplifier. Therefore, compared to 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 65nm CMOS technology and simulated using Cadence Spectre®. To emulate the characterization 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 350mV DC source. The nominal operating condition of the evaluation was at 25°C with a 0.6V 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 assessed 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. 3. Monte Carlo simulation results: 128 × 100 PUF response bits.

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 0.6V). 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 less than 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 ±20%VDD is applied to the proposed PUF circuit at 25°C. As shown in Table 1, with 10% and 20% voltage changes from 0.6V 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.

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, Ptot, and the corresponding energy efficiency, Ebit, averaged from 100 PUF instances. The energy efficiency is calculated as: \( E_{\text{bit}} = \frac{l_{\text{avr}}}{V_{\text{DD}}} \times f_{\text{clk}} \), where \( l_{\text{avr}} \) denotes the average current consumed to produce a response bit. The achieved \( E_{\text{bit}} \) over varying supply voltages is less than 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 ten years have been included in this comparison. At the nominal operating condition, the proposed PUF achieves an \( E_{\text{bit}} \) of 10.3 fJ/bit, being the best compared to existing implementations.

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 optimized 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 ±20%VDD 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).

S. Tao and E. Dubrova (School of ICT, KTH Royal Institute of Technology, Kista 16440, Stockholm, Sweden)
E-mail: stao@kth.se; dubrova@kth.se

References


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

<table>
<thead>
<tr>
<th>( V_{\text{DD}} ) [V]</th>
<th>BER [%]</th>
<th>( P_{\text{tot}} ) [μW]</th>
<th>( E_{\text{bit}} ) [fJ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.48</td>
<td>3.69</td>
<td>0.88</td>
<td>6.9</td>
</tr>
<tr>
<td>0.51</td>
<td>3.10</td>
<td>1.03</td>
<td>8.1</td>
</tr>
<tr>
<td>0.54</td>
<td>1.70</td>
<td>1.16</td>
<td>9.0</td>
</tr>
<tr>
<td>0.57</td>
<td>0.82</td>
<td>1.25</td>
<td>9.7</td>
</tr>
<tr>
<td>0.60</td>
<td>0.48</td>
<td>1.33</td>
<td>10.3</td>
</tr>
<tr>
<td>0.63</td>
<td>0.92</td>
<td>1.42</td>
<td>10.9</td>
</tr>
<tr>
<td>0.66</td>
<td>-</td>
<td>1.50</td>
<td>11.7</td>
</tr>
<tr>
<td>0.69</td>
<td>1.08</td>
<td>1.63</td>
<td>12.8</td>
</tr>
<tr>
<td>0.72</td>
<td>1.27</td>
<td>1.80</td>
<td>14.1</td>
</tr>
</tbody>
</table>

Fig. 6. \( E_{\text{bit}} \) comparison with state-of-the-art CMOS PUF ICs.