Low-Power Sub-Threshold Design of Secure Physical Unclonable Functions

Lang Lin, Dan Holcomb*, Dilip Kumar Krishnappa, Prasad Shabadi, Wayne Burleson
Department of Electrical and Computer Engineering, University of Massachusetts, Amherst
*Department of Electrical Engineering and Computer Science, University of California, Berkeley
{llin, krishnappa, shabadi, burleson}@ecs.umass.edu, *holcomb@eecs.berkeley.edu

ABSTRACT

The unique and unpredictable nature of silicon enables the use of physical unclonable functions (PUFs) for chip identification and authentication. Since the function of PUFs depends on minute uncontrollable process variations, a low supply voltage can benefit PUFs by providing high sensitivity to variations and low power consumption as well. Motivated by this, we explore the feasibility of sub-threshold arbiter PUFs in 45nm CMOS technology. By modeling process variations and interconnect imbalance effects at the post-layout design level, we optimize the PUF supply voltage for the minimum power-delay product and investigate the trade-offs on PUF uniqueness and reliability. Moreover, we demonstrate that such a design optimization does not compromise the security of PUFs regarding modeling attacks and side-channel analysis attacks. Our final 64-stage sub-threshold PUF design only needs 418 gates and consumes 0.047pJ energy per cycle, which is very promising for low-power wireless sensing and security applications.

Categories and Subject Descriptors

B.7 [**Hardware**]: Integrated Circuits; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Design, Security

Keywords

Physical unclonable function, sub-threshold circuits, RFID, embedded system security

This work was partially supported by NSF grants CNS-0627529 and CNS-0964641.

1. INTRODUCTION

A Physical Unclonable Function (PUF) is a function that maps a set of challenges to a set of responses based on complex physical variations [1]. The challenge-response pairs (CRPs) give the unique identity of each PUF instance, which is very important for chip identification and authentication in security applications. The silicon implementation of PUFs relies on the physical uncertainties during the semiconductor manufacturing process. Inter-chip and intra-chip process variations are desirable for PUFs, since they can potentially make the CRPs more distinguishable. Many different PUF designs have appeared in literature. The first PUFs did not exploit VLSI process variations but the random speckle pattern of optical materials [2]. Then many silicon PUFs are studied for integrating with circuits and systems. Some PUF circuits designed for ASIC implementation use ring oscillators or arbitrated race conditions [3]. Other PUF circuits harness the power-up states of FPGA embedded block RAMs statistically gathered by an authentication protocol [4]. PUFs utilizing power-up SRAM states in embedded systems and memory chips have also been demonstrated [5].

The most significant role of PUFs is to provide affordable security for low-power applications, such as radio frequency identification (RFID). RFID tags were originally proposed for electronic object identification purposes. Passive battery less RFID tags harvest energy through inductive coupling, which limits the power budget to 1-5μW for the tag circuits. Given the pervasiveness of RFID tags, security has become another important concern over the performance, especially in many security-critical financial, medical, and military applications [6, 7]. For example, replay and man-in-the-middle attacks can eavesdrop the open wireless communication channel between reader and tag [7]. Side-channel analysis attacks can extract secret bits stored or processed on the chip [8]. Automated reverse engineering can shatter any hope of security through obscurity [9].

Introducing cryptography into low-power devices can mitigate the security vulnerabilities, as long as the implementation budget of the cryptography does not break the low-power promise (e.g., RFID tags mandate that only 2000 gates can be used for security [10]). Although the use of lightweight cryptographic algorithms [11] can fulfill the tight budget, the low implementation complexity of lightweight algorithms can be especially vulnerable to power side-channel analysis attacks [12]. Process variations can further degrade the resistance of cryptographic implementations against side-channel attacks [13]. Instead of using cryptography, PUFs can provide equivalent security with low design overhead. PUFs have been integrated in RFID tags as a solution to low-cost authentication [14]. With the help of low-overhead post-processing algorithms [15], PUF responses can also be used for secret key generation on low-power devices.

By admitting the advantages of PUFs, we are further motivated to explore the feasibility of designing sub-threshold PUFs. Operating a circuit at a supply voltage below the threshold voltage significantly minimizes energy and power [16], which allows minimum energy operation for low-performance situations. This opens many opportunities for ultra-low design of PUFs. Moreover, sub-threshold circuits are more sensitive to process variations in deep sub-micron technologies than super-threshold

ISLPED'10, August 18–20, 2010, Austin, Texas, USA.

designs [17]. High variation sensitivity is favored by PUFs to enhance the uniqueness and security through randomness.

The contribution of this work is three-fold: (1) We investigate the optimal supply voltage to minimize power-delay product of 45nm CMOS sub-threshold PUF. (2) We compare the uniqueness and reliability of sub-threshold PUF with those of super-threshold PUF, and discuss the design trade-offs. (3) Besides power considerations, we also evaluate the security of PUFs. A recent work has demonstrated a ring oscillator-based PUF design in sub-threshold mode [18], but without analyzing the PUF uniqueness, reliability and security in detail. We demonstrate that a sub-threshold PUF has improved resistance against side-channel analysis attacks and equivalent resistance against modeling attacks.

The PUF being considered in this work consists of n stages and an arbiter (Fig. 1). A rising edge is propagated down two delay paths, and the arbiter records which input is reached first. The challenges C_1 to C_n select the paths that the edge will race down. At each stage, a challenge bit of 1 will pass the tracks straight through, and a challenge bit of 0 will cause a track switch.

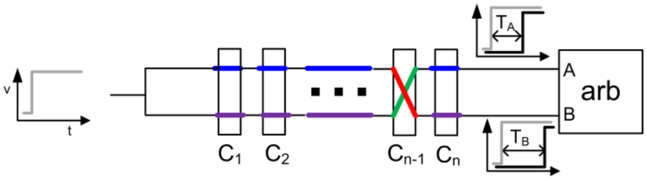


Figure 1: Arbiter PUF

1.1 Experiment Methodology

All circuit analyses use an industrial 45nm CMOS technology model. Consistent with the 2006 ITRS [19], threshold voltage (Vth) variation is assigned from a normal distribution with a standard deviation of 53mV. Channel length and width variations are assigned from a normal distribution with a standard deviation of 2nm. Since PUF circuits also rely on physical variations during IC fabrication process, interconnect parasitics through circuit layout extraction are included in the simulation netlist. The tools used in this work include Cadence schematic & layout editor, HSPICE, Calibre DRC/LVS/PEX and PERL.

The remainder of this paper is being organized as follows. Section 2 introduces the basic circuit blocks of a sub-threshold PUF. Section 3 evaluates the feasibility of a particular PUF design. Section 4 provides measurements from a placed and routed implementation of a 64-stage sub-threshold PUF in 45nm technology. Conclusions and suggestions for future work are in Section 5.

2. DESIGN STRATEGIES FOR SUB-THRESHOLD PUFS

Although moving an arbiter PUF into sub-threshold region has promise because it will reduce energy and be very sensitive to process variations, there are many design challenges. Sub-threshold operation has a weak on-current, resulting in a slow rising edge along the racing paths. Furthermore, sub-threshold circuits might be sensitive to supply voltage and temperature variations, causing unreliable responses. These design issues should be considered in reducing the supply voltage for minimal energy operation.

2.1 Stage Design

Each stage of a PUF consists of two CMOS multiplexers and a delay circuit (Fig. 2). While the CMOS design style is preferred in sub-threshold, the different inputs to each NAND gate have different timing properties. Noting that the challenge bits will always settle early, paths can be balanced by careful gate input ordering. Since *p* and *q* are always chosen together, they are assigned to the same gate input in the 2nd level NAND gates; likewise for *s* and *r*. Each stage also has RC interconnects to link the next stage and provide extra delays.

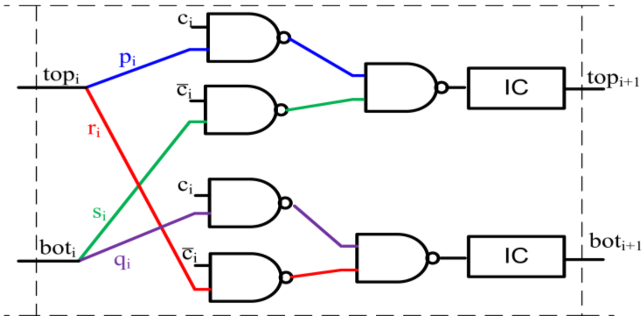


Figure 2: The *i*th stage of the CMOS PUF contains two MUXes and interconnects (denoted by IC).

As the most common element in PUF circuits, the stage should be optimized for low power and large delay variation. Since the CMOS gate delay of sub-threshold circuits is exponentially dependent on V_{th} [16], the introduction of V_{th} variation can lead to significant delay variations. We simulate the supply voltage impact on power, delay variation as well as the power-delay product (PDP) in Fig. 3. We find that the minimal PDP can be achieved at 0.43V supply voltage, which is consistent with most 45nm CMOS sub-threshold circuits [20]. Reducing the voltage further will favor the power and delay variation, but with degraded PDP. For now, we will keep using a 0.4V supply for the next sub-threshold experiments, and 1.1V for super-threshold. Later when validating the sub-threshold PUF design, we will review the optimal choice of supply voltage.

2.2 Arbiter Design

The arbiter should reliably record whether the racing edge arrives first at input A or B. The arbiter is often considered as a rising edge triggered flip-flop. A rising A / CK input causes the flip-flop to sample the B input. Thus, the sampled value depends on whether B / D rises before or after A / CK. Stated differently, the sampled value depends roughly on whether T_A is less than T_B (see Fig. 1).

Edge-triggered flip-flops are not necessarily fair arbiters. If there is a large bias in the arbiter across many PUF instances, uniqueness will be reduced [3]. If the arbiter's bias changes with temperature or supply voltage, it will hinder reliability. This section argues that an SR latch is preferred for both uniqueness and reliability to a D flip-flop. If the arbiter is a D flip-flop that uses a tri-state as in [21], the rising edge on input B / D must discharge node *rb* before the rising edge of A / CK arrives (Fig. 4(a)).

The outcome depends on an asymmetric competition between the two inputs, so the metastable condition may not coincide with simultaneously rising inputs. The outcome depends on an asymmetric competition between the two inputs, so the metastable condition may not coincide with simultaneously rising inputs. Furthermore, the relative strengths of the fighting signals can change with temperature and supply voltage.

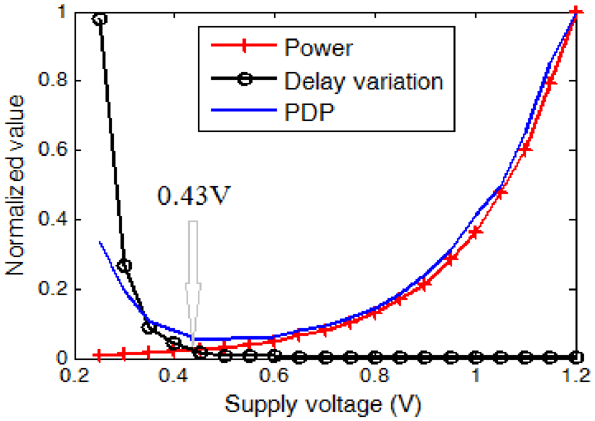


Figure 3: Supply voltage impacts on PUF stage circuit

Using an SR-latch as an arbiter should help fix the bias and variability problem. The SR latch is a symmetric circuit made of cross-coupled NAND gates (Fig. 4(b)). In the SR latch, both r and *rb* are initially pulled high. The rising edge on A will pull down r while the rising edge on B will pull down *rb*. The cross-coupling of the NANDs ensures that only one competing transition can win, and the symmetry ensures that neither input is favored in the competition. It should also resist supply and temperature variations because any change that weakens one of the competing NAND gates is likely to weaken the other similarly.

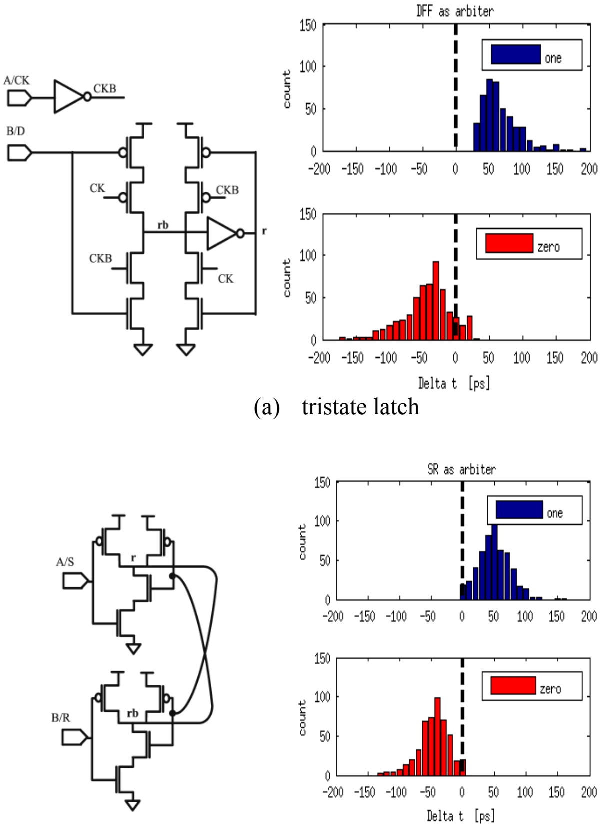
3. VALIDATION OF DESIGN FEASIBILITY

This section explores the uniqueness, reliability and security of a 16-stage sub-threshold PUF that was composed of the proposed circuits in the preceding section. High uniqueness refers to different PUF instances producing uncorrelated responses. High reliability refers to a single PUF instance producing the same responses over time. Generally, PUF design requires 50% uniqueness and 100% reliability [3]. Security refers to the vulnerabilities and information leakage of PUF with respect to a certain type of attack or threat model.

3.1 Uniqueness

Uniqueness is a measure of the independence of PUF responses to the same challenge. Any correlation across PUF instances will diminish uniqueness. While section 2.2 shows that the SR-latch arbiter does not induce correlations, some unavoidable bias in the delay stages still does. Given the PUF occupies the same area on each die, a stage bias might be caused by consistent intra-die variation. Unbalanced routing could also cause a stage bias. This section of feasibility analysis analyzes whether such a stage bias would compromise more uniqueness in sub-threshold or super-threshold region.

To add unwanted bias to the design, the interconnect of only the top path in every PUF stage is lengthened by 2μm. Any path that includes many p_i or s_i edges is statistically likely to be longer on all PUFs. This can threaten the uniqueness of the responses.



(a) tristate latch

(b) SR latch

Figure 4: Only the SR latch is an unbiased arbiter. Its bias point for choosing 0/1 is at approximately δ = 0

A set of 25 random challenges are applied to 40 sub- threshold and super-threshold PUF instances. For the two supply voltages, the Hamming Distances (HDs) of all PUF pairings are plotted in Fig. 5. A HD of 0 would indicate that two PUFs produced the same 25-bit responses to all of the challenges. In super-threshold, the mean HD is a diminished 11.84 due to the interconnect bias; in sub-threshold, the mean HD is 12.52. This indicates that operating in the sub-threshold region could overcome more systematic bias and increase uniqueness. The PUF uniqueness is the ratio of HD to the total response bit number. We further simulate the uniqueness of PUF with a supply voltage sweep as shown in Fig. 6. The uniqueness is increased by reducing supply voltage, while it significantly slows down the increase below 0.4V. This suggests that a lower supply voltage than 0.4V may not be necessary in sub-threshold PUF design.

3.2 Reliability

Reliability is a measure of the consistency of PUF CRPs with respect to operating environment changes. Since arbiter PUF circuits employ symmetric structures, the stage delay behaviors and thus the reliability should hardly be affected by supply voltage and temperature changes. Note that reliability does not refer to noise, but only to changing bias. If noise is a problem, a majority of multiple responses to the same challenge can be used.

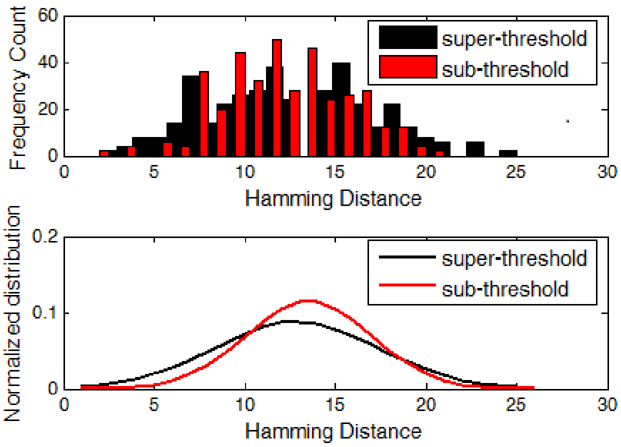


Figure 5: When the stages are biased, the mean Hamming Distance of PUF instances is improved in sub-threshold.

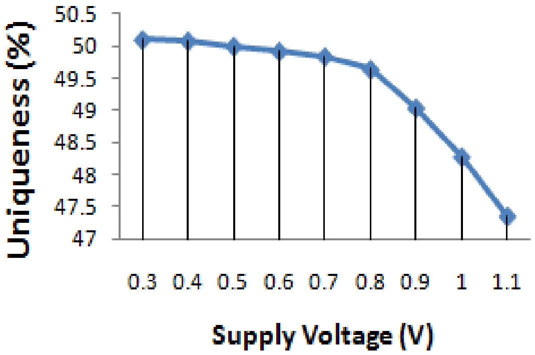


Figure 6: Supply voltage impacts on PUF uniqueness.

Figure 7 show that operating at sub-threshold supply voltage does not compromise reliability. A supply voltage bias of ±0.05V applied on the sub-threshold PUF actually results better reliability than the same bias applied on the super-threshold PUF. On the other hand, the temperature reliability of sub-threshold PUF is slightly worse than that of super-threshold PUF in general. However, at a high temperature such as 85ºC, the reliability of super-threshold PUF degrades to 83.8%. This indicates that sub-threshold PUF is less sensitive to temperature bias.

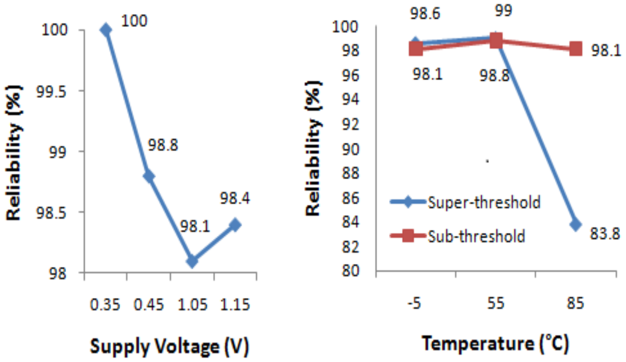


Figure 7: PUF reliability results

3.3 Security Evaluation

Since PUF is proposed for security applications, the sub-threshold PUF should at least maintain the same security level as the super-threshold design. A PUF maps challenges to responses using a physical function determined by process variation and any type of design skews. Invasive attacks such as reverse-engineering and focused ion beam attacks cannot impair the security of all PUF designs because any invasive action on the PUF circuits can alter the physical properties and thus the PUF CRPs. However, PUF-based systems may be susceptible to two threat models. If a PUF is used for authentication, the threat model will be the attacker's capability of knowing a certain number of valid CRPs to impersonate the PUF function; If a PUF is used for secret key generation, the threat model will be the attacker's capability of extracting the PUF response bits by exploiting the PUF implementation weakness. In the following sections, we evaluate the security of PUF against modeling attacks and side-channel analysis attacks regarding the two threat models.

3.3.1 Modeling Attack

Observing CRPs can allow an attacker to create a model to mimic a PUF. The proper choice of model depends on the assumptions made regarding the circuits' delay behavior. We start with a linear model. Using the same notation as in literature [22], there are 4 paths through each stage, labeled as shown in Fig. 2. A parity function $P(i)$ (Eq. 1)[1] represents the number of track switches between the ith stage and the arbiter. The parity and challenge determine exactly which n timing arcs have been traversed by the path that arrives at the top arbiter input (Eq. 2). The path to the bottom arbiter input is defined similarly.

$$P(i) = \prod_{k=i+1}^{n} C_i \quad \text{with } P(n) = 1 \qquad (1)$$

$$\mathrm{T_A} = \sum_{i=1}^{n} \begin{cases} p_i, & if\ P(i+1), C_i == +1, +1 \\ q_i, & if\ P(i+1), C_i == -1, +1 \\ s_i, & if\ P(i+1), C_i == +1, -1 \\ r_i, & if\ P(i+1), C_i == -1, -1 \end{cases} \qquad (2)$$

$$\delta = \mathrm{T_A} - \mathrm{T_B} \qquad (3)$$

Assume that m CRPs are obtained from a single n-stage PUF. Let B be an $m \times 4n$ matrix that selects the racing paths segments for each challenge, and let column vector w be the unknown weight of the $4n$ timing edges. Vector Δ contains the measured δ for each of the m challenges. Since row $\mathrm{b_j}$ Є B selects the components of w that are sensitized by the $\mathrm{j^{th}}$ challenge, the relation $\mathrm{b_j}\omega = \delta_\mathrm{j}$ holds. Therefore, the linear model of the PUF is given by Eq. 4.

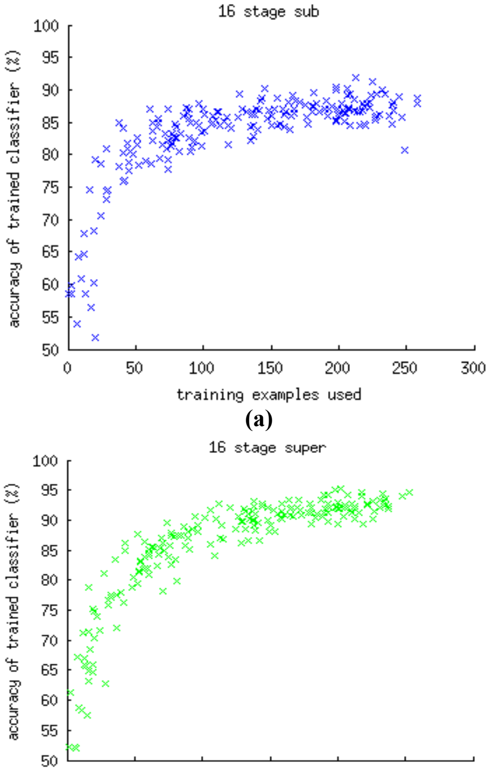
$$\mathrm{B}\omega = \Delta \qquad (4)$$

When performing a modeling attack, it is not possible to observe δ directly. However, the sign of δ can be inferred from the PUF response. As shown by Majzoobi et al. [23], each CRP of the PUF corresponds to a single linear constraint of the form $b_i w \geq 0$. With the constraints of CRPs reducing the feasible space, an optimal solution for w can be found within the feasible space by linear programming.

[1] In computing the parity vector, the challenge bits are represented using (-1, 1) instead of (0, 1).

Instead of a linear program, a Support Vector Machine (SVM) classifier can be used for a modeling attack [22]. SVM finds a maximum-margin hyperplane that separate the 0 and 1 responses. This classifier then allows future responses to be predicted. SVMs can be used with linear or non-linear kernels [24].

Using *SVM^light* [25] to perform modeling attacks, it is yet unclear whether sub-threshold operation makes a PUF easier to model. The SVM formulation used was adopted from literature [22], each data point in Fig. 8 is a cross validation of a modeling attack on 256 CRPs. The 256 CRPs are randomly split into different sized training and test sets. Whenever the training set size contains a sufficiently large number of CRPs, the prediction accuracy in is close to 90% in both sub-threshold and super-threshold (Fig. 8).



(a)

(b)

Figure 8: The difficulty of SVM modeling attack on PUF is equivalent in (a) sub-threshold and (b) super-threshold region.

3.3.2 *Side-Channel Analysis Attack*

Side-channel analysis can extract the secret information bits transferred on data buses or processed in logic elements by measuring the accompanied data-dependent physical phenomena, such as global power consumption, electromagnetic radiation and timing information. In power side-channel analysis, attackers measure the real-time power traces of the targeting device and correlate them with a power model based on brute-force hypothesis of the secret bits. The correct hypothesis of the secret bits can render the maximum correlation between the power model and the actual power traces. For a given circuit, the correlation coefficient (CC) (see Eq. 5) between a set of logic values X and a set of corresponding power values Y determines the difficulty of power attacks [26]. Attackers can hardly extract the secret bits if CC is close to 0.

$$CC(X,Y) = \frac{E[(X-\mu X)(Y-\mu Y)]}{\sigma_X \sigma_Y} \qquad (5)$$

In our sub-threshold PUF design, the SR latch actually has differential outputs to resist power attacks (the output is either a 0-1 or a 1-0 consuming a data-independent total power). However, if the loads of the two outputs (r and rb) are slightly different due to variations or skews, the latch can still leak power side-channel signals. To address this, we assign a 2µm interconnect difference on the SR latch outputs and simulate the power traces by giving random challenge bits. To extract the response bits, we calculate the CC between the response bits and the corresponding power traces. To overcome the obscuring effects of noise power from the PUF stage circuits, we keep analyzing more power traces until the CC converges. As shown in Fig. 9, the sub-threshold PUF results almost 2X smaller CC than the super-threshold design after analyzing 256 power traces.

Although the super-threshold PUF already has a very small CC to resist power attacks, we are confirmed that the sub-threshold PUF has even stronger resistance.

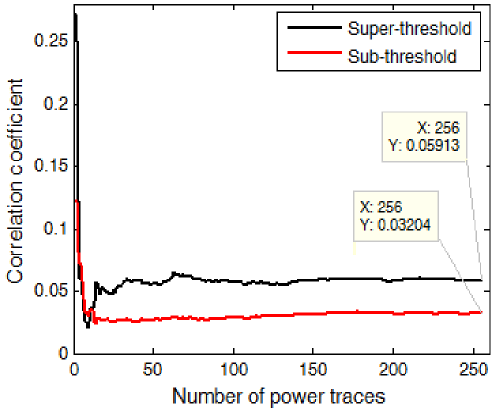


Figure 9: Correlation analysis of super-threshold and sub-threshold PUF power traces.

4. IMPLEMENTATION RESULTS

While a 16-stage sub-threshold PUF is used in the preceding feasibility analyses, a 64-stage implementation of the same sub-threshold PUF is used for power and area measurements. It is expected that this 64-stage PUF will share similar uniqueness, reliability and attack resistance properties to the 16-bit variant.

The 64-stage PUF contains 418 NAND gate equivalents. Using 45nm technology node, the stages are laid out as an 8 by 8 array within a 36µm by 50µm total die footprint. As a rough point of comparison, a previous work [27] shows an 8-bit PUF in 180nm technology that measures 1212µm by 1212µm; scaling the area by 1/8 for a 1-bit PUF, and by 1/16 to go from 180nm to 45nm, this related PUF is 5 times as large as ours. At least part of this discrepancy is explained by JTAG and input/output pins of the related work, which are absent in our work.

The power of the 64-stage PUF is measured at super- threshold and sub-threshold supply voltages. Since the sub- threshold PUF runs slower, we use the metric of energy per cycle to compare the energy-efficiency of the sub-threshold and super-threshold operation. As shown in Table 1, sub-threshold operation produces each response using only 35% as much energy as super-threshold operation.

The power consumption of our PUF is compared to the same related work [27] as above. Each arbiter PUF circuit in the related work consumes 137µW at 100MHz, or 1.37pJ per cycle. Assuming that energy scales quadratically with technology node due to shrinking geometries, this equates to 0.085 pJ per cycle in 45nm. In sub-threshold, our PUF implementation is more efficient than the technology scaled version of related work. In super-threshold, our implementation is less efficient than the technology scaled version of the related work; we hypothesize that this is due to our use of upsized gate widths, which are necessary for coping with variability in sub-threshold, but prevent us from achieving the full benefits of technology scaling.

Table 1: Comparison of sub-threshold and super-threshold operation.

	Sub-threshold	Super-threshold
Power	0.047µW @ 1MHz	136.4µW @ 1GHz
Energy/Cycle	0.047pJ	0.136pJ

5. CONCLUSION AND FUTURE WORK

We demonstrate the feasibility of a 45nm sub-threshold arbiter PUF for low-power applications, in which the system performance is not a critical design consideration. Our PUF design achieves low power, high uniqueness and acceptable levels of reliability and security. Future work includes the fabrication and post-silicon measurements of the 45nm 64-stage sub-threshold PUF presented in this paper.

6. REFERENCES

[1] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas. Silicon physical random functions. In Proceedings of the 9th ACM conference on Computer and communications security, pages 148-160, 2002.

[2] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. Science, 297(6):2026-2030, 2002.

[3] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In ACM/IEEE Design Automation Conference, pages 9-14, 2007.

[4] J. Guajardo, S. S. Kumar, G. Schrijen, and P. Tuyls. FPGA intrinsic PUFs and their use for IP protection. In Proceedings of the Workshop on Cryptographic Hardware and Embedded Security, pages 63-80, September 2007.

[5] D. E. Holcomb, W. P. Burleson, and K. Fu. Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. IEEE Transactions on Computers, 58(9):1198-1210, 2009.

[6] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In Proceedings of Symposium on Security and Privacy, pages 129-142, 2008.

[7] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. OHare. Vulnerabilities in First-Generation RFID-enabled Credit Cards. In Financial Cryptography, 2007.

[8] Y. Oren and A. Shamir. Remote password extraction from RFID tags. IEEE Transactions on Computers, 56(9):1292-1296, 2007.

[9] K. Nohl and D. Evans. Reverse-engineering a cryptographic RFID tag. In USENIX Security Symposium, pages 185-193, 2008.

[10] A. Juels and S. A. Weis. Authenticating pervasive devices with human protocols. Lecture notes in computer science, 3621:293, 2005.

[11] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel. A survey of lightweight-cryptography implementations. IEEE Design & Test of Computers, pages 522-533, 2007.

[12] T. Popp, E. Oswald, and S. Mangard. Power analysis attacks and countermeasures. IEEE Design & Test of Computers, 24(6):535-543, 2007.

[13] L. Lin and W. P. Burleson. Analysis and mitigation of process variation impacts on power-attack tolerance. In ACM/IEEE DAC, pages 238-243, 2009.

[14] Verayo PUF RFID. http://www.verayo.com/product/pufr_d.html, 2008.

[15] R. Maes, P. Tuyls, and I. Verbauwhede. Low-overhead implementation of a soft decision helper data algorithm for sram pufs. In CHES, pages 332{347. Springer-Verlag, 2009.

[16] B. H. Calhoun, A. Wang, and A. P. Chandrakasan. Modeling and sizing for minimum energy operation in sub-threshold circuits. IEEE Journal of Solid-State Circuits, volume 40, pages 1778-1786, 2005.

[17] S. Hanson, B. Zhai, D. Blaauw, D. Sylvester, A. Bryant, and X. Wang. Energy optimality and variability in subthreshold design. In ACM/IEEE ISLPED, pages 363-365, 2006.

[18] V. Vivekraja and L. Nazhandali. Circuit-Level Techniques for Reliable Physically Uncloneable Functions. In IEEE HOST, pages 30-35, 2009.

[19] International Technology Roadmap for Semiconductors. 2006 ITRS report, http://www.itrs.net/Links/2006Update/2006UpdateFinal.htm

[20] D. Bol, D. Kamel, D. Flandre, and J. D. Legat. Nanometer mosfet e_ects on the minimum-energy point of 45nm subthreshold logic. In ISLPED, pages 3-8, 2009.

[21] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal. Design and implementation of puf-based "unclonable" RFID ICs for anti-counterfeiting and security applications. In IEEE International Conference on RFID, pages 58-64, 2008.

[22] D. Lim. Extracting secret keys from integrated circuits. M.S. thesis Cambridge: Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., May 2004.

[23] M. Majzoobi, F. Koushanfar, and M. Potkonjak. Lightweight secure pufs. In ICCAD, pages 670-673, 2008.

[24] B. E. Boser, I. M. Guyon, and V. N. Vapnik. A training algorithm for optimal margin classifiers. In Proceedings of the fifth annual workshop on Computational learning theory, pages 144-152, 1992.

[25] T. Joachims. Making large scale SVM learning practical. http://svmlight.joachims.org/, 1999.

[26] S. Mangard, E. Oswald, and T. Popp. Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer-Verlag New York, Inc., 2007.

[27] 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 VLSI, 13(10):1200-1205, 2005.