# Novel Strong PUF based on Nonlinearity of MOSFET Subthreshold Operation

Mukund Kalyanaraman and Michael Orshansky
Department of Electrical and Computer Engineering
The University of Texas at Austin
email:{*mukundkm,orshansky*}*@utexas.edu*

## I. Abstract

Many strong silicon physical unclonable functions (PUFs) are known to be vulnerable to machine-learning attacks due to linear separability of the output function. This significantly limits their potential as reliable security primitives. We introduce a novel strong silicon PUF based on the exponential current-voltage behavior in subthreshold region of FET operation which injects strong nonlinearity into the response of the PUF. The PUF, which we term subthreshold current array (SCA) PUF, is implemented as a pair of two-dimensional $n \times k$ transistor arrays with all devices subject to stochastic variability operating in subthreshold region. Our PUF is fundamentally different from earlier attempts to inject nonlinearity via digital control techniques, which could also be used with SCA-PUF. Voltages produced by nominally identical arrays are compared to produce a random binary response.

SCA-PUF shows excellent security properties. The average inter-class Hamming distance, a measure of uniqueness, is $50.2\%$. The average intra-class Hamming distance, a measure of response stability, is $4.17\%$. Crucially, we demonstrate that the introduced PUF is much less vulnerable to modeling attacks. Using machine-learning techniques of support-vector machine with radial basis function kernel and logistic regression for best nonlinear learnability, we observe that "information leakage" (rate of error reduction with learning) is much lower than for delay-based PUFs. Over a wide range of the number of observed challenge-response pairs, the error rate is $3-35$X higher than for the delay-based PUF. We also demonstrate an enhanced SCA-PUF design utilizing XOR scrambling and show that it has an up to 30X higher error rate compared to the XOR delay-based PUF.

## II. Introduction

Many electronic systems require solutions for security, unique identification, and authentication. As a low cost solution, physical unclonable functions (PUFs) have been proposed [1], [2]. PUFs are pseudo-random functions that exploit the randomness inherent in the scaled CMOS technologies to generate random output strings. In response to an input challenge a PUF generates a binary response. Because of the randomness of the input-to-output mapping, different PUFs generate a different response for the same challenge. The set of challenge-response pairs (CRPs) defines the behavior of a PUF and provides an ability to uniquely identify it.

Multiple realizations of PUFs have been proposed [1], [3]–[9]. The key distinction among different PUF constructions is between strong and weak PUFs. The distinction is based on the rate at which the number of CRPs grows with the size of the physical realization of a PUF [10]. Weak PUFs are characterized by a small number of CRPs [3], [6]. Strong PUFs are systems with a large number of CRPs, and in an ideal case, the CRP set size grows exponentially with the size of the PUF. The exponential size of the CRP set makes it impossible to record the responses for a PUF of a reasonable size.

Strong PUFs are essential for public authentication security protocols in which the number of CRPs needs to be large such that the adversary cannot record all CRPs even when in physical possession of a PUF. However, for a strong PUF to be an effective security primitive, the CRPs need to be unpredictable: given a certain set of known challenge-response pairs, it should not be possible to predict the unobserved CRPs with any reasonable probability. If that is not the case, an adversary can stage an attack based on building a model of the PUF. A number of strong PUFs have been proposed in the literature over the years. However, the unpredictability of responses in published strong PUFs has been shown to be limited. The earliest example of a strong silicon PUF is the arbiter-based PUF proposed in [1]. It exploits variation in path delays between gate stages in two parallel propagation paths to generate a binary response by using an arbiter. The arbiter-based PUF has been shown to be vulnerable to model-building attacks [11], [12]. In such attacks, machine-learning techniques, such as regression, neural networks and support vector machines, are used to construct a model of the internal parameters of a PUF based on the observed instances. Attempts to remediate this vulnerability resulted in several variants of the arbiter-based PUF [4], [5]. These approaches attempt to improve unpredictability by using digital techniques. In [8], an XOR gate is used to scramble outputs of two parallel arbiter-based PUFs. In [5], a feed-forward path is introduced within the arbiter-PUF circuit as a way to inject nonlinearity. Unfortunately, recent work [11] shows that the above-cited extensions of arbiter-based PUF are also vulnerable to model-building attacks, even though the improved versions require a larger number of observed CRPs for building a model.

This paper introduces a novel strong silicon PUF based on the essential nonlinearity of terminal current-voltage behavior of field-effect transistors (FETs) at the nanometer scale. *The*

978-1-4799-0600-0 

*fundamental principle is reliance on the subthreshold regime of the FET operation, where current is an exponential function of threshold voltage, which exhibits strong random intrinsic variability*. An additional nonlinearity is due to the exponential dependence of threshold voltage (1) on drain-to-source voltage due to drain-induced barrier (DIBL) effect, and (2) on body-to-source voltage due to body effect. Both of these are used to create coupling between FETs in the array, further improving nonlinearity and unpredictability. The new PUF shows excellent security properties.

Earlier attempts to use subthreshold operation in PUF design have focused on power minimization and did not focus on its potential to create strong nonlinearity and higher unpredictability. In [13], variable current sources are arranged in parallel combinations and selectively combined. The binary comparison is current-based and since current summation is linear this PUF also has the problem of linear separability. Single-transistor leakage current [14], [15] and saturation current in [3] are used to implement a weak PUF, thus avoiding the need to worry about unpredictability.

## III. New Source of Nonlinearity: FET Subthreshold Current

We develop a principled approach to significantly improve PUF resilience against machine-learning attacks. It has been recognized that the limitations of arbiter-based PUFs in terms of unpredictability are due to their linear additive dependence on partial delays in generating a response. Machine-learning methods are particularly effective in constructing models of such functions. Machine-learning algorithms for classification are tasked with classifying an object given a set of its attributes. In supervised learning setting, the algorithm is first given a set of training examples in which both the attributes and the label is available. If the space being learned is naturally linearly separable, it is easy for the learning algorithm to derive a classification rule with low prediction error.

Unfortunately, the known silicon realizations of PUFs have utilized output functions that are linear, or nearly linear, in the base random variables. In fact, delay-based functions are intrinsically poorly suited for this task as (1) segment delay is near-linear in threshold voltage, and (2) path delays are naturally additive, and, thus, linear, in segment delays. Most strong silicon PUFs known thus far have been derived from the original work on arbiter PUFs for which the output can be described as a linear function of the delays of individual stages, as formalized in [16]. Attempts to introduce nonlinearity in the arbiter-based PUF, such as using feed-forward paths or XORing the outputs introduce nonlinearity through digital means. Empirical results of model-building attacks show that the added nonlinearity helps but is insufficient in that low prediction errors can still be achieved. A distinct limitation of at least some digital techniques, those based on XORing outputs, is that PUF instability increases along with the improvement in unpredictability [11].

In order to aid the discussion, we introduce a formal distinction between the ways of injecting nonlinearity. For most silicon PUFs, a random bit is produced by evaluating $sgn(f(\mathbf{x})-f(\mathbf{y}))$, where $\mathbf{x}$, $\mathbf{y}$ are vectors of realizations of a random physical parameter. Function $f(\cdot)$ maps the underlying realizations of physical parameters, e.g. threshold voltages, to a measurable circuit-level quantity, e.g. delay or voltage. If function $f(\cdot)$ is expressible entirely in terms of real-valued functions we call it a fully continuous random function (FCRF), otherwise we call it a mixed continuous-discrete random function (MCDRF). With that distinction in place, we point out that the above digital techniques of achieving nonlinearity still use delay races as a building block for PUFs with the underlying mechanism of generating pseudo-random behavior remaining linear. Thus, both the XOR PUF and the feed-forward PUF start with a "native" FCRF-based PUF and ultimately use the mixed continuous-discrete random function to achieve nonlinearity. Given that the known digital techniques can be equally applied to other underlying ("native") FCRF-based PUFs, the question becomes: can strong silicon PUFs utilizing fully continuous random functions be constructed that are significantly more secure than the FCRF-based delay PUF? We provide an affirmative answer in this paper.

The key for engineering a secure silicon PUF is identifying an output function that would be nonlinear in random variables. We introduce a highly unpredictable PUF that uses the strongly nonlinear I-V terminal dependencies to generate PUF responses. Its central feature is that it moves away from the delay/digital implementation paradigm towards the current/analog one, thereby realizing the necessary degree of nonlinearity over a space of permutations. Because it doesn't rely on digital techniques for injecting the nonlinearity, it does not compromise the stability in the output response to environmental variations.

The output function should ideally have two properties: (1) be nonlinear in random parameters, and (2) introduce the coupling effect in which two or more random variables interact in producing the output. Both of these properties are enabled if the binary output is produced by comparing two voltages produced by a suitably arranged *network of FETs operating in subthreshold region*. The key to our analysis is the equation relating the subthreshold current to FET terminal voltages [17]:

$$\begin{aligned} I_{ds} &= I_S 10^{\frac{V_{gs}-V_{th}(V_{ds},V_{bs})}{S}}(1-10^{\frac{-nV_{ds}}{S}}) \\ &= I_S 10^{\frac{V_{gs}-V_{th}+\lambda V_{ds}+\gamma V_{bs}}{S}}(1-10^{\frac{-nV_{ds}}{S}}) \end{aligned} \quad (1)$$

where $I_{ds}$ is the drain-to-source subthreshold current, $I_S = 2n\mu C_{ox}\frac{W}{L}\left(\frac{KT}{q}\right)^2$ is the nominal current, $\mathrm{V}_{gs}$ is the gate-to-source voltage, $\mathrm{V}_{th}$ is the transistor threshold voltage, $\mathrm{V}_{ds}$ is the drain-to-source voltage, $\mathrm{V}_{bs}$ is the body-to-source voltage, $\lambda$, $\gamma$, and $n$ are the coefficients of drain-induced barrier lowering and body-bias, and the subthreshold coefficient respectively and $S = n\frac{kT}{q}ln(10)$ is the subthreshold slope factor. Crucially, the current is exponentially dependent on the threshold voltage $V_{th}$. This is important because $V_{th}$ exhibits large and spatially-uncorrelated variability due to random dopant fluctuation (RDF). In nanometer scale CMOS devices, RDF is very significant and grows with transistor scaling [17], [18]. Equation 1 also captures the impact of physical mechanisms of drain-induced barrier lowering and of body effect which lead to a

dependence of $V_{th}$ on $V_{ds}$ and $V_{bs}$. In the second part of the equation, we use a linear expansion of $V_{th}$ in terms of $V_{ds}$ and $V_{bs}$ to enable closed-form analysis.

## IV. Subthreshold Current Array PUF

### A. Array PUF Architecture

We now present a transistor-level realization of a subthreshold current array PUF (SCA-PUF) that exploits the above current behavior to construct a highly secure strong PUF. Figure 1 depicts the overall architecture of the SCA-PUF. The PUF is implemented as a pair of two-dimensional transistor arrays with all devices subject to stochastic variability operating in subthreshold region. The 2D organization allows to maximize the reliability and security properties of the PUF, as demonstrated by experiments.

Each PUF consists of two nominally identical arrays. The array schematic is shown in Figure 2. The array is composed of $k$ columns and $n$ rows of a unit cell. We use the term "stochastic" transistor to refer to a device with high amount of threshold voltage variability. The unit cell consists of a stochastic subthreshold nFET, which is a transistor with a highly variable threshold voltage that always operates in the subthreshold region. A non-stochastic switch transistor is arranged in parallel to the stochastic FET. The non-stochastic transistor $M0$ acts as a load device and operates in the subthreshold region (its gate terminal is tied to ground). At the bottom of each column of cells is a footer transistor $Miy$ controlled by $\overline{C_{i1}C_{i2}\ldots C_{in}}$. Its role is to ensure that there is never a low-impedance path to ground from $V_{out}$.

Both array blocks are driven with the same set of control inputs and thus in the absence of variability produce identical voltages. The randomness of transistor threshold voltages leads to the differences in two output voltages. The binary response is generated by comparing the output voltages produced by the two arrays via a comparator. The size of the CRP set is $2^{kn}$, making it a strong PUF.

We now describe in greater detail the building block of the array, the unit cell. In each cell, which we identify using a column index $i$ and a row index $j$, an NMOS transistor $Mij$ always operates in the subthreshold region: its gate terminal is tied to ground. An NMOS transistor $Mijx$, in parallel with $Mij$, acts as a switch transistor. Careful sizing of both devices is essential for correct operation. Two requirements need to be satisfied. First, only transistor $Mij$ is subject to significant variation of threshold voltage due to random dopant fluctuation. This is achieved by sizing transistors $Mij$ to their minimum size to maximize their threshold voltage variability according to Pelgrom's model [19]. Second, the subthreshold current through the switch transistor $Mijx$ needs to be negligible compared to the subthreshold current through $Mij$. At the same time, $Mijx$ needs to have small on-state resistance. These requirements can be met, for example, with $W = 10W_{min}$ and $L = 10L_{min}$. Because the nominal current $I_S$ in the subthreshold region is exponentially dependent on channel length $I_{ds}(Mijx)/I_{ds}(Mij) \approx 0$ when $C_{ij} = 0$. The body terminal of all the transistors is grounded.

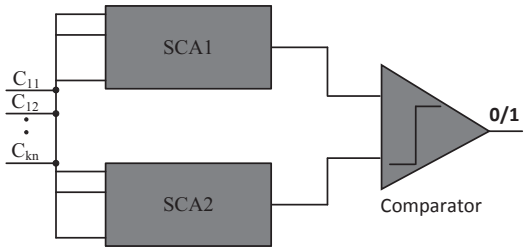



**Fig. 1:** *PUF architecture.*

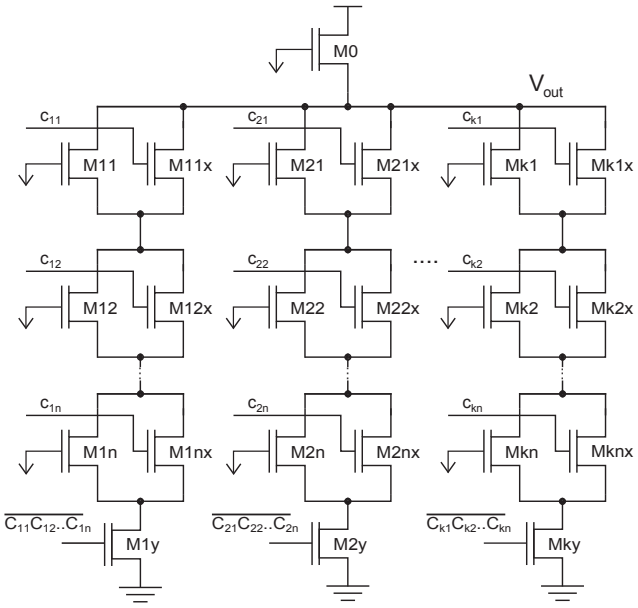



**Fig. 2:** *Circuit schematic of the 2D subthreshold current array.*

The role of the switch transistor is to set $V_{ds}$ of the stochastic transistor to zero. In this case, the impact of the stochastic transistor is effectively "removed" in that its contribution to the branch current is eliminated. At the same time, when the switch transistor is off, because its subthreshold current is negligible compared to the stochastic transistor, its contribution to the total current can be ignored. Depending on the control input, the stochastic transistor therefore is either part of the pull-down network and contributes current that depends on its threshold voltage, or does not impact total current flowing through a branch. Thus, each branch can have $2^n$ current values.

### B. Analysis of Array Nonlinearity

The principle feature of the circuit we propose is that it has a highly nonlinear boundary between the regions of PUF 1-outputs and 0-outputs in the $kn$-dimensional space of $V_{th}$. In this section, we more formally analyze the nonlinearity of the SCA-PUF. To enable analytical treatment, we derive equations for two special cases: (a) a single-column array, and (b) a single-row array. We aim to bring out the form of the nonlinearity involved in each of the two special cases (a) and (b). The two special cases of the 2D array exhibit distinct forms of nonlinearity which, when combined within a 2D array structure, form a rich nonlinear space.

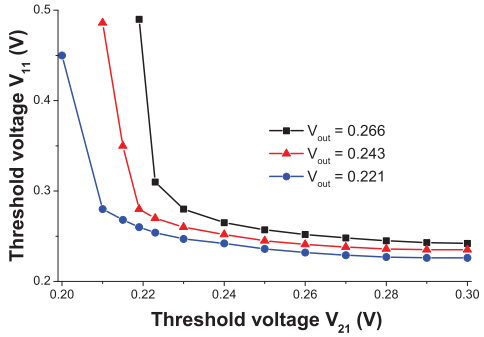



**Fig. 3:** *Response nonlinearity in the single-row array: nonlinearity of additive subthreshold current behavior.*

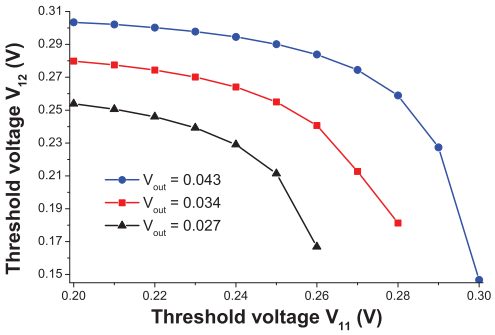



**Fig. 4:** *Response nonlinearity in the single-column array: nonlinearity of series-connected subthreshold FETs.*

First, we consider the single-row (parallel-only) array with two columns ($n = 1$, $k = 2$). To be able to derive a closed-form equation relating $V_{out}$ to threshold voltages of two "stochastic" transistors, we assume that $V_{ds}$ >100 mV. For $n = 1$ we can also ignore the impact of the body-bias effect. With that, Equation 1 can be written as:

$$\log\left(\frac{I_{ds}}{I_S}\right) = \frac{V_{gs} - V_{th} + \lambda V_{ds}}{S} \tag{2}$$

For convenience, we use a simplified notation where $V_{th,M0} = V_0$ and similar for others. Solving for $V_{out}$,

$$V_{out} = \left(\frac{S}{1+\lambda}\right)\left[\log(I_S) + \lambda V_{dd} - V_0 - \log(I_0)\right] \tag{3}$$

Applying Kirchhoff's Current Law at node $V_{out}$, $I_0 = I_{11} + I_{21}$, where $I_{11}$, $I_{21}$ are the currents through $M11$ and $M21$, and describing these currents using Equation 1, we can write an equation for the terminal voltage $V_{out}$:

$$V_{out} = \left(\frac{S}{1+\lambda}\right)\left[\frac{\lambda V_{dd}}{S} - \frac{V_0}{S} - \log\left(10^{\frac{-V_{11}+\lambda V_{out}}{S}} + 10^{\frac{-V_{21}+\lambda V_{out}}{S}}\right)\right] \tag{4}$$

Equation 4 is a transcendental equation. The key to our construction is the nonlinearity of $V_{out}$ in terms of values of threshold voltages of transistors $M11$ and $M21$. The nonlinearity of Equation 4 is explored in Figure 3.

Next we consider the single-column array ($k = 1$) with only two rows ($n = 2$). It represents a subthreshold current array with series-only "stochastic" transistors $M11$ and $M12$. Using Equation 1 for transistors $M0$, $M11$ and $M12$ respectively, and treating the source (drain) of $M11$ ($M12$) as an intermediate node $V_x$, we get:

$$\log\left(\frac{I_0}{I_S}\right) = \frac{-V_{out}(1+\lambda) - V_0 + \lambda V_{dd}}{S} + \log\left(1 - 10^{\frac{-nV_{dd}+nV_{out}}{S}}\right) \tag{5}$$

$$\log\left(\frac{I_{11}}{I_S}\right) = \frac{-V_x(1+\lambda) - V_{11} + \lambda V_{out}}{S} + \log\left(1 - 10^{\frac{-nV_{out}+nV_x}{S}}\right) \tag{6}$$

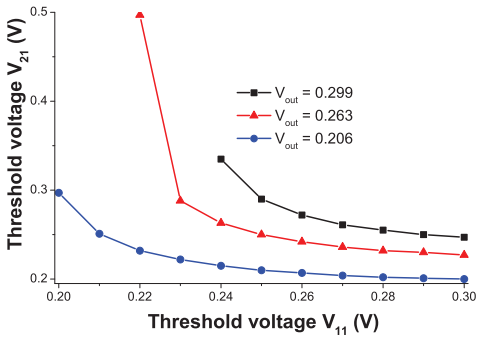



**Fig. 5:** *Response nonlinearity in the* $2 \times 2$ *SCA.*

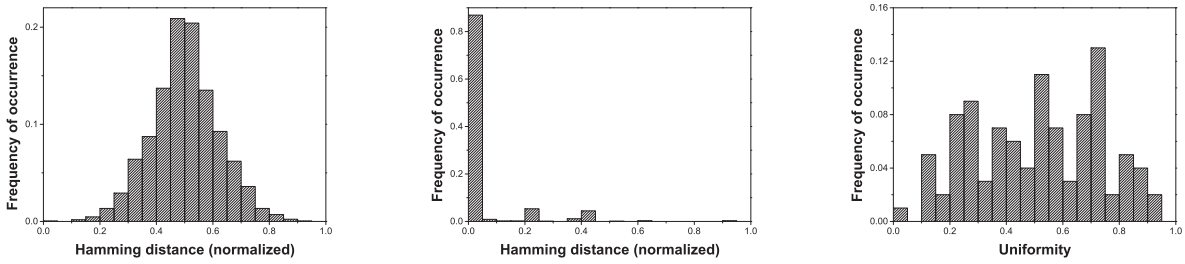
$$\log\left(\frac{I_{12}}{I_S}\right) = \frac{-V_{12} + \lambda V_x}{S} + \log\left(1 - 10^{\frac{-nV_x}{S}}\right) \tag{7}$$

We also know that $I_0 = I_{11} = I_{12}$. Unfortunately, expressing $V_{out}$ in closed form appears infeasible. By simultaneously solving the system of Equations 5, 6 and 7 numerically, we generate Figure 4 and observe the nonlinearity of the single-column (series-only) array topology. The nonlinearity is significant. Notably, while the nonlinear separating surface of the parallel-only array is convex, the surface separating 0- and 1-regions in the series-only array is concave. Interestingly, when we numerically solve the case of the $2 \times 2$ array, we find the overall non-linearity is still convex, see Figure 5.

## V. Analysis of PUF Security Properties via Transistor-Level Simulations

The performance of the proposed SCA-PUF was simulated using SPICE, the industry-standard transistor-level circuit simulator, in a 45 nm technology node using the predictive technology models [20]–[22]. The source of randomness is in $V_{th}$ variability assumed to be caused by random dopant fluctuation and therefore to be spatially uncorrelated. The threshold voltages are assumed to follow a normal distribution with a standard deviation of 40 mV, a value consistent with ITRS [23].

There are several commonly used metrics that quantify the goodness of a PUF [24]–[26]. The inter-class Hamming distance (HD) is a measure of the ability to differentiate two different PUFs under the same input. Ideally, each PUF produces an




(a) Inter-class HD (b) Intra-class HD (c) Uniformity

**Fig. 6:** *Inter-class, intra-class HD and distribution of uniformity metric for a 64-bit SCA-PUF.*

entirely unique response, and thus the ideal inter-class HD normalized to the total number of bits in the output is 0.5. Intra-class HD is the measure of the reliability of a PUF and quantifies how much response of a given PUF changes under a different set of environmental conditions and noise. Ideally, the intra-class HD is 0. Another useful measure of the goodness of a PUF is the uniformity metric defined by [24]. In an ideal PUF, the fraction of challenges that produces a response of 1 and of 0 should be equal. A useful, and closely, related metric is randomness, as defined by [26], which also quantifies uniformity but in a min-entropy sense. Reliability of the PUF responses across different environmental conditions was studied by carrying out transient noise simulations to account for thermal noise under supply voltage variation of 10% from the nominal value of 1.2V and temperature ranging from $-55\,^{\circ}\mathrm{C}$ to $125\,^{\circ}\mathrm{C}$.

Figure 6 shows the histograms of the normalized intra-class, inter-class HDs and uniformity extracted for a 64-bit ($8 \times 8$ array) SCA-PUF from 10000 randomly chosen CRPs. The mean and the standard deviation values are summarized in Table I. We observe that the mean inter-class HD is excellent and is practically indistinguishable from 0.5. The mean intra-class HD is 4.17% which is excellent given that the circuit was simulated under the "military" range of operating conditions.

**TABLE I:** *Average inter-class and intra-class Hamming distance, uniformity, and randomness for $3\sigma_{V_{os}} = 1$ mV for 64-control input SCA-PUF ($8 \times 8$ array).*

| Parameter | Mean | Standard deviation |
|---|---|---|
| Inter-class HD | 0.502 | 0.119 |
| Intra-class HD | 0.041 | 0.122 |
| Uniformity | 0.510 | 0.224 |
| Randomness | 0.556 | 0.248 |

Model-building attacks are the tool with which an adversary may attempt to overcome the authentication guarantees offered by PUFs. Therefore, the ability of a PUF to withstand model-building attacks has been suggested as the ultimate measure of their security [11]. These attacks rely on the power of machine-learning algorithms to model the inner parameters of PUFs through observation of a small set of CRPs. In this paper, the effectiveness of machine-learning attacks was investigated using a support vector machines (SVM) and logistic regression algorithm. Open-source LIBSVM and LIBLINEAR packages were used [27], [28]. A set of challenge inputs, along with their output responses, is used as a training set to estimate

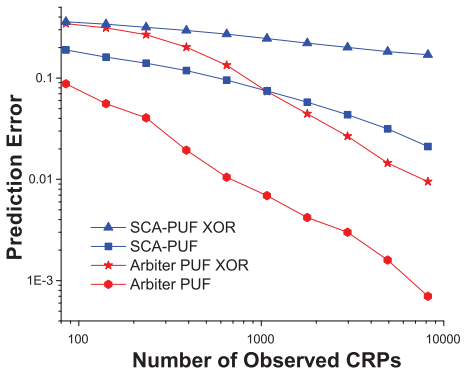



**Fig. 7:** *Classification error from modeling a 16-bit PUF via machine learning attacks.*

the PUF model parameters. The estimated model is used to compute the predicted output response for the non-training challenge inputs and the prediction error rate $\epsilon$ is measured for SVM and logistic regression and then the one with least $\epsilon$ is chosen. The arbiter PUFs is modeled using the additive linear delay model [4], [16]. The procedure is carried out for several training sample sets of different size across 100 PUF instances. Figure 7 shows the comparison of prediction error vs. training set size for the plain and 2-XOR versions of 16-bit arbiter and SCA PUFs. To maximize the learning ability of the SVM algorithm, we employed a nonlinear radial basis function (RBF) kernel. Using a nonlinear kernel makes SVM more effective in nonlinear classification problems. We further used a 5-fold cross-validation scheme to select the best kernel parameters. The results indicate that the plain SCA-PUF is significantly more secure than the delay-based PUF. The prediction error is more than an order of magnitude higher than for the arbiter PUF.

As we argued earlier, the digital techniques of injecting nonlinearity can be thought of as qualitatively distinct from the behavior of the "native" PUF. Figure 7 illustrates that the digital techniques can also be applied to SCA-PUF to further enhance its native nonlinearity and security. The 2-XOR version of the SCA-PUF shows higher prediction error compared to its delay-based counterpart especially for larger training set sizes.

Another practical aspect that we investigate is the influence of comparator characteristics on the overall PUF behavior. Offset voltage effectively determines the resolution of the comparator and it may also impact the security properties of the SCA-PUF.

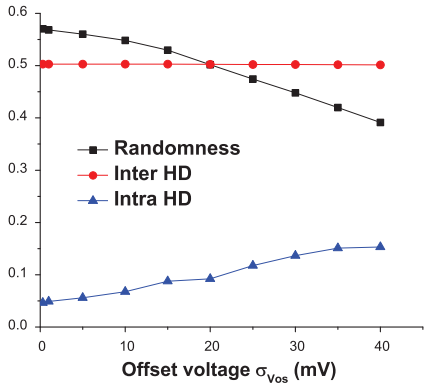



**Fig. 8:** *Dependence of randomness, inter HD, and intra HD on offset voltage spread.*

We studied the impact of offset voltage on PUFs properties by assuming it follows a normal distribution with a mean of 0 mV and a standard deviation $\sigma_{Vos}$ of several mVs. Figure 8 shows the effect of offset voltage on the mean randomness, mean inter HD and mean intra HD metrics. The inter-class Hamming distance was found to remain nearly-constant around 0.5. Based on this exploration, we find that a comparator that has an offset voltage of up to $\sigma_{Vos} = 8$ mV would be acceptable but a wider offset distribution would significantly deteriorate randomness and intra class HD. Achieving this using conventional strong-arm sense amplifier topology, e.g., [29], would require exceedingly high area. For that reason, we designed a comparator using an offset cancellation strategy [30], which allows a very small, and entirely sufficient, offset spread of $3\sigma_{Vos} = 1$ mV. At this low offset spread, the metrics of PUF security performance are not affected. The power consumption of a 64-bit SCA-PUF, estimated through simulation, is 108$\mu$W. The area is estimated to be $0.016\ mm^2$. The circuit is capable of operating at a frequency of 100 MHz.

## VI. Conclusion

We introduced a novel strong silicon PUF based on the essential nonlinearity of responses produced by the physics of field-effect transistors (FETs) at the nanometer scale. The PUF shows excellent security properties which are superior to those reported for other strong PUFs. We demonstrate that the introduced PUF is less vulnerable to modeling attacks and that its "information leakage" is significantly lower than for delay-based strong PUFs.

## References


[1] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon Physical Random functions," in *CCS*. ACM Press, 2002, pp. 148–160.

[2] J. Lee, D. Lim, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in Integrated circuits for Identification and Authentication application," in *Proc. Symp. on VLSI Circuits*. IEEE, Jun 2004, pp. 159–176.

[3] K. Lofstrom, W. Daasch, and D. Taylor, "IC Identification Circuit using Device mismatch," in *ISSCC*. IEEE, 2000, pp. 372–373.

[4] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," in *Proc. of the IEEE/ACM Int. Conf. on Computer-Aided Design*. Piscataway, NJ, USA: IEEE, 2008, pp. 670–673.

[5] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, "Identification and authentication of Integrated circuits: Research articles," *Concurrency and Computation : Practise and Experience*, vol. 16, no. 11, pp. 1077–1098, 2004.

[6] D. Holcomb, W. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proc. of the Conf. on RFID Security*, Jul. 2007.

[7] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *CHES Workshop*, ser. LNCS, vol. 4727, Sep. 2007, pp. 63–80.

[8] E. Suh and S. Devadas, "Physical Unclonable Functions for device authentication and secret key generation," in *DAC*. ACM Press, 2007, pp. 9–14.

[9] S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF protecting ip on every FPGA," in *HOST*, Jun 2008, pp. 67–70.

[10] J. Guajardo, S. Kumar, K. Kursawe, G. Schrijen, and P. Tuyls, "Intrinsic Physical Unclonable Functions in Field Programmable Gate Arrays," *ISSE/Secure: Securing Electronic Business Processes*, pp. 1–10, 2007.

[11] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *CCS*. New York, NY, USA: ACM, 2010, pp. 237–249.

[12] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing Techniques for Hardware Security," *IEEE Int. Test Conf.*, pp. 1–10, Oct 2008.

[13] M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. Nassif, "Ultra-low power current-based puf," in *IEEE Int. Symp. on Circuits and Systems (ISCAS)*. IEEE, 2011, pp. 2071–2074.

[14] D. Ganta, V. Vivekraja, K. Priya, and L. Nazhandali, "A highly stable leakage-based silicon physical unclonable functions," in *24th Int. Conf. on VLSI Design*. IEEE, 2011, pp. 135–140.

[15] M. Kassem, M. Mansour, A. Chehab, and A. Kayssi, "A sub-threshold sram based puf," in *Int. Conf. on Energy Aware Computing (ICEAC)*, dec. 2010, pp. 1 –4.

[16] L. Daihyun, "Extracting Secret Keys from Integrated Circuits," Master's thesis, MIT, Cambridge, MA, USA, 2004.

[17] T. Yuan, D. Buchanan, C. Wei, D. Frank, K. Ismail, L. Shih-Hsien, G. Sai-Halasz, R. Viswanathan, H.-J. Wann, S. Wind, and H.-S. Wong, "CMOS scaling into the nanometer regime," *Proc. of IEEE*, vol. 85, no. 4, pp. 486–504, Apr 1997.

[18] M. Orshansky, S. Nassif, and D. Boning, *Design for Manufacturability And Statistical Design: A Constructive Approach*. Springer, 2007.

[19] M. Pelgrom, A. Duinmaijer, and A. Welbers, "Matching Properties of MOS Transistors," *IEEE Journal of Solid-State Circuits*, vol. 24, no. 5, pp. 1433 – 1439, Oct 1989.

[20] W. Zhao and Y. Cao, "New Generation of Predictive Technology Model for Sub-45nm Design Exploration," *ISQED*, pp. 7–12, Mar 2006.

[21] Y. Cao, T. Sato, M. Orshansky, D. Sylvester, and C. Hu, "New Paradigm of Predictive MOSFET and Interconnect Modeling for Early Circuit Simulation," *CICC*, pp. 201–204, 2000.

[22] Y. Cao, "Predictive Technology Model," Internet: http://ptm.asu.edu/.

[23] ITRS, "International Technology Roadmap for Semiconductors," Internet: http://public.itrs.net.

[24] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of Physical Unclonable Functions," Cryptology ePrint Archive, Report 2011/657, 2011, Internet:http://eprint.iacr.org/.

[25] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*. Springer, 2010, pp. 3–37.

[26] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," *Int. Conf. on Reconfigurable Computing and FPGAs*, pp. 298–303, Dec 2010.

[27] C. Chang and C. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 27:1–27:27, 2011, software available at Internet:http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[28] R.-E. Fan, K.-W. Chang, C.-J. Hsieh, X.-R. Wang, and C.-J. Lin, "LIBLINEAR: A library for large linear classification," *Journal of Machine Learning Research*, vol. 9, pp. 1871–1874, 2008.

[29] L. Brooks, "Circuits and algorithms for pipelined adcs in scaled cmos technology." Ph.D. dissertation, MIT, Cambridge, MA, USA, 2008.

[30] F. Maloberti, *Analog design for CMOS VLSI systems*. Springer, 1st edition, 2001.