Multiple-Valued Logic Physically Unclonable Function in Photonic Integrated Circuits

Duncan L. MacFarlane
Lyle School of Engineering
Southern Methodist University
Dallas, Texas U.S.A.
dmacfarlane@lyle.smu.edu

Hiva Shahoei
Lyle School of Engineering
Southern Methodist University
Dallas, Texas U.S.A.
hshahoei@smu.edu

Ifeanyi G. Achu
Lyle School of Engineering
Southern Methodist University
Dallas, Texas U.S.A.
iachu@smu.edu

Evan Stewart
Anametric, Inc.
Austin, Texas U.S.A.
evan@anametric.com

Willam V. Oxford
Anametric, Inc.
Austin, Texas U.S.A.
oxford@anametric.com

Mitchell A. Thornton
Deason Institute for Cyber Security
Southern Methodist University
Dallas, Texas U.S.A.
mitch@smu.edu

Abstract—**Physically Unclonable Function (PUF) optical circuits are described and implemented within a Photonic Integrated Circuit (PIC) to enhance certain security properties such as device authentication, anti-tamper properties, or for use as a root-of-trust value. Optical processing is advantageous for security applications such as these since they are less susceptible to eavesdropping and side channel monitoring via the difficulty of observing electromagnetic radiation emissions during PIC operation. We employ the use of State of Output Polarization (SOP) variability arising from inherent stresses, strains and manufacturing tolerances present within a fabricated PIC. A customized optical signal processing element is used in our PUF circuit that contains a very narrow "trench" structure with tiny structural variations induced during fabrication that enhances SOP variability. The tiny structural changes in fabricated PICs are fixed resulting in repeatable SOP variation of the optical signals. To avoid a need for PUF calibration, to increase robustness with respect to input power level variation, measurement device resolution and sensitivity; we show that PUF functionality can be conveniently modeled as a discrete Multiple-Valued Logic (MVL) function. The proposed MVL PUF formulation avoids the need to characterize and measure exact polarization states as well as enabling the use of PUF output measurement devices that have a wide range of resolution and sensitivity specifications. Several different PUF circuits are implemented within a single fabricated PIC and are experimentally evaluated to demonstrate its efficacy.**

Keywords— photonic integrated circuit (PIC), physically unclonable function (PUF), cyber security

I. Introduction

Physically Unclonable Functions (PUF) are implemented as hardware structures within integrated circuits (IC) that provide a unique value or "signature" that can serve as a means for device identification or other purposes that enhance cyber security. Ideally, a PUF signature is impossible to duplicate and can thus be used to authenticate individual ICs. Security applications include use as a hardware root-of-trust, anti-counterfeiting and anti-tampering support, code signing for firmware updates, device authentication signatures and others. Early work introducing the concept of a PUF include [1-5].

Ideally, a PUF instance should be representative of a "physical one-way function" indicating that it is very easy and efficient to evaluate while also being computationally difficult to invert. Conceptually, a PUF is analogous to a biometric measure of a human in that all humans are of the same species; however, each human has unique characteristics that can be used for their identification. Analogously, a collection of PICs can all implement the same internal functionality with their identical PUF circuits providing repeatable, yet different signature values arising from tiny variations occurring during their fabrication. For security purposes, it is desirable that all possible PUF signatures are equally likely to occur among a collection of PICs and that the probability of identical PUF signatures resulting from any two PICs is very small. If the PUFs adhere to these ideal features, they are described as providing the property of "collision avoidance." The precision with which a PUF response is measured and the dynamic range of among a collection of different PUF measured responses among a collection of different fabricated PUF circuits becomes an important design goal to achieve collision avoidance from a practical point of view.

It is generally the consensus among hardware security experts that a PUF implemented in conventional electronic circuitry should be based upon non-linear characteristics to prevent the use of linear error-correction codes to defeat the PUF. The chosen non-linear characteristics supporting a PUF implementation should also be repeatable and unchanging over a variety of internal and external environmental conditions for a given instance of an IC. Most prior PUF implementations have relied upon permissible tolerance variations present in the IC foundry fabrication processes such as variations among gate oxide thickness, transistor threshold voltages and other parameters that affect subthreshold currents, leakage, power and switching times [6].

PUF circuitry is included within ICs to support receiving an external input query or "challenge" signal that interacts with the internal physical PUF circuit structure, and then correspondingly generates a numerical value that serves as the as PUF "response" or output signature. To avoid masquerading attacks, PUF circuitry is typically configured to employ a

2378-2226/23/$31.00 ©2023 IEEE
DOI 10.1109/ISMVL57333.2023.00043

"challenge/response" mechanism wherein an external device provides the "challenge" value c_j to the IC that causes the internal PUF circuitry to provide a corresponding and repeatable response value r_j.

Some past examples of electronic PUF circuitry are timing-based and include the implementation of asynchronous ring oscillators whose specific oscillation frequencies are dependent upon process variations, single-bit SRAM cell switching speed [7], arbiter circuit switching speed [8] and others. As a specific example, a simple challenge/response scheme can be implemented by using an array of ring oscillators, SRAM cells, or other structures that are selected based upon the challenge value and wherein the response can also possibly be permuted in accordance with the challenge value or some other shared secret. Another commonly used class of PUFs are state-based and are typically based upon voltage values arising from differences in transistor threshold voltages or similar phenomena within CMOS circuitry.

Electronic PUF circuitry can be susceptible to eavesdropping attacks due to radiated electromagnetic energy during PUF circuit operations that can allow an adversary to accumulate a partial table of challenge/response pairs. In particular, timing based PUFs are susceptible to "modeling attacks" wherein digital clones are constructed based on tables of challenge/response pairs acquired during an eavesdropping attack [9]. Informatic-theoretic approaches can be applied to characterize the strength of state-based PUFs allowing exploitable information to be acquired by an adversary to facilitate the characterization of a particular instance of an internal PUF function [10]. More recently, PUF attacks based upon Machine Learning (ML) approaches such as "Generative Adversarial Networks" (GAN) have emerged and are of concern [11]. An important vulnerability that can be exploited to defeat PUF-based security is the ability to characterize the supporting circuitry through eavesdropping or through invasive physical attacks [12].

The consideration of these PUF vulnerabilities and attack strategies motivate us to consider the use of newly emerging "photonic integrated circuit" (PIC) technology for PUF implementations due to the inherent increase in resistance to eavesdropping and other characterizations. Furthermore, invasive attacks that use IC destructive methods, such as the so-called "scraping attack" would necessarily affect the internal stresses and strains present in the fabricated photonic components that comprise the PUF circuitry and would thus render the characterization of how a PUF could affect, for example, the "State of Polarization" (SOP) as very difficult to achieve. Therefore, we hypothesize that a PIC-based PUF circuit also provides an enhanced degree of security against scraping and similar reverse-engineering approaches that may be employed by an adversary. The ability to implement a PUF with increased resistance to this class of attacks, referred to as "anti-tamper" capabilities, is of considerable interest since appropriate means to include anti-tamper characteristics is an open problem and is an active area of research in the hardware cyber security community.

In choosing an appropriate characteristic to serve as the basis for a PIC-based PUF circuit, we observe that the SOP of an optical signal has a relatively large degree of variation when it is transmitted through an internal PIC component due to tiny perturbations in the geometry of the component. Thus, using SOP observations as a PUF response has the desirable property of variation among a collection of manufactured PICs. Likewise, there are a small but unique set of stresses and strains imparted onto the structure of an optical component during the fabrication of a PIC that also significantly contribute to SOP variability. This latter observation additionally indicates that the use of optical signal SOP is desirable from the perspective of tampering or resistance to destructive reverse engineering approaches. This resistance occurs because any attempt to tamper with a manufactured PIC, such as engaging in a scraping attack, would also necessarily change the very small stresses and strains that were originally present in the manufactured PUF circuit components. For at least these reasons, we choose to use the SOP of an optical signal as the characteristic to be observed or processed by the PUF circuit when it is generating the response to a challenge value. However, this large degree of variation also requires the external challenge signal to adhere to strict specifications in terms of power and noise levels with similarly tight constraints on the device used to measure the PUF response signal. Requiring this precise level of control of input challenge signal characteristics and corresponding PUF response measuring apparatuses is a serious challenge that we demonstrate can be overcome through the use abstracting the PUF circuit transfer function as a discrete Multiple-Valued function.

Optical signals are in the form of mathematical wave structures that obey Maxwell's equations wherein the wave functions are represented in the form of a vector with time-varying and complex-valued components [13]. Since an optical signal, or light, is inherently vectorial, its SOP can likewise be represented in the form of a vector. Because a photon is the smallest indivisible unit of energy within an optical signal, it can likewise be characterized by its SOP although a single photon's SOP is a quantum observable since SOP is a form of angular momentum and the uncertainty principle applies to momentum [14]. Since the repeatability of the PUF is an important property, the PIC-based PUF must necessarily operate in a classical manner with optical signals rather than in the single photon or quantum realm.

At a particular instance of time and geometrical location within a PIC-based circuit, an optical signal's SOP can be described in terms of its Jones vector representation [15]. A Jones vector is a two-dimensional vector comprising the relative amplitude and relative phase among two orthogonal electric field vector components. Therefore, the transformation of the signal's SOP as it propagates through a component can be modelled as the interaction of the signal's Jones vector with a 2×2 Jones matrix that describes the birefringence of that component. A succession or cascade of these 2×2 Jones matrices may be directly multiplied together to describe how the overall signal SOP changes as it propagates through a circuit or system comprised of multiple optical components.

As the frequency of an electromagnetic wave increases, the wave enters the region of the spectrum we consider as light or, an optical wave. This increase in frequency causes the optical wave to increase its sensitivity to phase disruptions. Because the geometric dimensions of PIC components are on the order of a wavelength, these phase disruptions translate into the SOP sensitivities that are desirable for the PIC-based PUF. An example of this sensitivity to phase is manifested as a change in the optical wave SOP as it propagates through such a waveguide that is manufactured with local imperfections in the boundary conditions that define the waveguide mode. In such optical components and systems, including fiber optic communication systems, this sensitivity to impairments can be characterized as "polarization mode dispersion" (PMD) and "polarization dependent loss" (PDL) [16]. These changes in the SOP can be understood and modeled as a long cascade of known and random birefringent elements that model the localized imperfections, and thus the aforementioned multiplication of a large number of 2×2 Jones matrices to determine SOP changes is justified.

For these reasons, we leverage the shift in SOP through an optical circuit to realize PUF circuitry within PICs. Path-specific impairments caused by stresses and strains, and component fabrication variability cause an output SOP to vary in response to an associated input SOP in a random but consistent manner. Multiple successively launched input wave SOPs result in corresponding multiple output SOPs with a highly repeatable SOP-to-SOP variation among a collection of undisturbed and manufactured PICs.

Our use of one or more polarizing beam splitters within the optical PUF circuit yields output power components on two ports whose ratio provides the PUF signature in an equipped PIC. In our application, the unique polarization transfer function of a photonic circuit is a ratio of powers that can be measured and are strongly dependent on a particular circuit instance. The measured PUF response signals are highly repeatable since the same birefringent perturbations are encountered by the optical challenge signal. Furthermore, we employ a new beam splitter cell that adds even more variation in SOP than other common splitter cells such as those based upon Y-splitters [17]. As will be further discussed, our new beam splitter comprises a relatively narrow "trench" and the fact that the trench is very narrow causes the ratio of the very small geometric imperfections with respect to the narrowness of the trench to have more mode variation than would be present if the larger geometries present in a beam splitter comprising Y-splitters were to be used. This larger ratio manifests as larger variations in the optical response signal SOP resulting in a higher-quality PUF response since SOP variation among different PICs is increased.

II. MVL Formulation of PUF

As previously described in detail, the SOP describes the orientation of the electric and magnetic field components over time, relative to their direction of propagation, and with respect to a static reference coordinate frame. An alternative vectorial representation of the SOP with respect to the two-dimensional Jones vector is the four-dimensional Stokes vector wherein the components are referred to as the Stokes parameters [18]. One of the Stokes parameters, S_0, is the magnitude of the instantaneous real-valued power comprising the optical signal. A convenient geometrical description of the polarization state is to consider it as a point on the surface of a Poincaré sphere[1] in three dimensions wherein the radius of the Poincaré sphere is proportional to S_0. The point of reviewing the Jones and Stokes vector characterizations of SOP here is that the PUF response could naïvely be measured using these conventional parameters; however, this could pose limitations in the accuracy of the measurement due to a variety of factors such as the resolution of the measuring device, the relative levels of interfering external light, and other factors. Therefore, we are motivated to devise an alternative characterization of the SOP that can easily permit the SOP of the PUF response to be measured without requiring detailed and narrow specifications regarding the resolution and sensitivity of the measuring device or the permissible power and noise levels of the incident challenge signal. This motivates us to formulate the mathematical description of the PUF in a manner that can inherently account for variations in these parameters and to avoid detailed calibration of each fabricated PUF circuit.

If we limit the set of permissible SOP comprising the PUF response signals to a finite and repeatable collection, then we can map a set of p distinct SOPs to a digit set defining a radix-p number system. Likewise, if the discrete set of polarization states are used as challenge values c_j for a PUF implemented within a PIC, then the response of the PIC r_j can likewise be modeled as a value within the radix-p number system. In this way, the PUF circuit can be represented by a mathematical abstraction comprising a physical one-way function. In modeling the PUF as implementing a one-way function, the set of all challenge values $\{c_j\}$ comprise the one-way function domain and the corresponding set of response values, $\{r_j\}$, comprise the co-domain. This formulation allows our PUF to be described as a physical one-way function that takes the form of a discrete Multiple-Valued Logic (MVL) function. More specifically, the PUF circuitry and the physical source of the PUF response are collectively modeled as a discrete MVL function, $f_{PUF}(c_j, r_j): \mathbb{Z}_p^n \longrightarrow \mathbb{Z}_p^m$, where the set $\mathbb{Z}_p = \{0,1,2,\cdots,p-2,p-1\}$. In this general formulation, the challenge set $\{c_j\}$ consists of a distinct set of n SOPs and the function f_{PUF} generates a corresponding set of distinct response values $\{r_j\}$ that, in our implementation, comprise a set of m distinct polarization states represented by power ratios of the the optical signals at the two output ports. The total number of challenge/response pairs embodied within a PUF, N, provides enhanced security as N grows larger in value. To summarize, the proposed one-way function models the PUF by defining a specific set of challenge/response pairs, $\{(c_j, r_j) | j = 1, \cdots, N\}$.

A significant advantage of using the MVL formulation of the one-way function that models the PUF circuitry, f_{PUF}, is that the specific polarization state as described by the Stokes parameters or Jones vectors need not be specified. All that is required is that the mapping of the discrete set of N SOPs to (c_j, r_j) pairs is unique. This formulation is particularly convenient for the PUF implementation described here since we do not measure or

[1] The normalized Poincaré sphere is equivalent to the Bloch sphere in quantum informatics when the observable is the polarization state of a photon, although the Poincaré sphere is visualized as being rotated 90° about the y-axis relative to the conventional visualization orientation of the Bloch sphere.

define actual numerical states of polarization as would be needed for the more conventional SOP characterizations in terms of Stokes parameters or Jones vectors. Furthermore, the use of a finite and discrete MVL one-way function, f_{PUF}, is consistent with typical representations of a conventional electronic PUF as a mathematical model. Additionally, the radix can be varied to correspond to measurement instrument resolutions, external noise levels, and incident PUF challenge signal power levels. Using a higher-valued radix, p, reduces the number of digits to be measured in the PUF response signal, or likewise, a smaller-valued radix could be used and fewer significant digits of the response signal measured. This degree of freedom enables a PIC PUF to be used in a variety of different environments and with a variety of different challenge signal power levels without re-calibrating and re-characterizing the PUF challenge/response tables in a PUF-based device authentication system. The use of the MVL f_{PUF} function effectively removes dependencies due to these different external parameters that would otherwise be necessary if conventional SOP characterizing metrics were used such as the Stokes or Jones vector.

III. Optical PUF Circuit

Fig.1 shows the layout of an optical circuit that we designed to provide the SOP-based PUF. This figure is extracted from a `GDSII` file that specifies the layout of a PIC containing the PUF circuit. 1550nm infrared light is coupled into and out of the PIC using edge couplers that collect and focus light into internal silicon (Si) waveguides, shown in blue, with cross-sectional dimensions of 480nm by 220nm. One superfluous branch of the photonic circuit at the top left of the figure is internally terminated within the PIC. The waveguides connect a cascade of three of our previously mentioned 2×2 trench-based couplers [17] shown as small red-lined boxes in Fig. 1.

Fig. 2 shows a "scanning electron microscopy" SEM microphotograph of the new and recently fabricated trench-based beam splitter, or coupler, in a 65nm Si process that serves as a key component in our PUF circuit. At the intersection of two waveguides, a narrow trench with a width of 100nm is etched at a 45° angle that provides, for each input port, a reflection and a transmission of the incident optical wave to the coupler. The thin, but relatively deep trench, causes "frustrated total internal reflection" (FTIR) and transmission to occur within the coupler. This nanoscale coupler structure replicates the action of a macroscopic beam splitting cube, although it requires much less area than typical splitter cells.

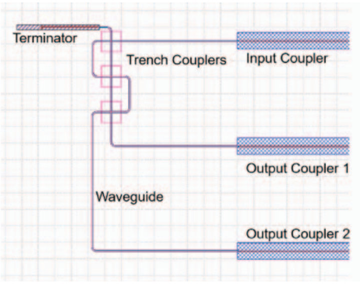

Fig. 1: Exemplary optical circuit that realizes a PUF

During operation, an input signal is coupled into the chip via the "input coupler" in Fig. 1. The wave propagates to the first 2×2 trench splitter (indicated by the topmost small red box) where it is split into reflected and transmitted components. These two signal components propagate into the second 2×2 trench splitter in the middle of Fig. 1 where recombining, reflection and transmission occurs. This process is repeated in the third and bottommost 2×2 trench splitter and the two outputs of that component propagate to two separate "output couplers." Throughout this circuit the propagating waves interact with fixed and repeatable perturbations caused by local stresses, strains and geometry variations in the waveguide and splitter dimensions that are implemented within a random range of values before fabrication, but that become fixed during fabrication. The recombination of the waves at the 2×2 trench splitters are interferometric and thus produce new SOPs resultant from the perturbations. The relative power directed to each of the two output edge couplers differs due to the polarizing fabrication variations within the 2×2 trench splitters in the circuit and the particular challenge signal SOP selected as input to PUF circuit. Importantly, different input SOP challenge signals will yield different relative powers on the two output edge couplers thus producing the desired action of a PUF.

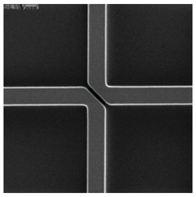

Fig. 2: SEM of a 2x2 FTIR Trench Coupler such as those used in Fig. 1

The 2×2 trench splitter was developed by the authors [17] on a previously designed PIC also fabricated by the AIM foundry [19]. It is noted that while the 2×2 trench splitter of Fig. 2 does provide significant variation in SOP due to PIC manufacturing variations, its performance in terms of signal power splitting is very consistent and flat across incident signal wavelength in the C-band (*i.e.*, 1525–1565nm). Thus, it performs very well as a power coupler for an optical wave. When this cell is used at the quantum photonic level, it also performs well as a Hadamard gate when the quantum observable is the position or location of the state-carrying photon. Fig. 3 depicts the normalized power as a function of trench width from each exiting port of the coupler (blue and red dashed lines are FDTD simulations and error bars are actual measurements for two different dies).

IV. PIC Layout, Fabrication and Packaging

The layout editor software package L-Edit [20] is used for chip layout and to generate the `GDSII` file submitted to the AIM Photonics fabrication facility. Input and output access to the trench couplers is accomplished using edge couplers that are standard and included within the AIM Process Development Kit (AIM PDK 3.5a). The edge couplers are spaced at a 127μm pitch to match the fiber array used to connect to the PIC. PICs containing several different PUF test structures were fabricated on 300 mm Si wafers using the 65 nm process in place for the AIM Photonics Multi-Project Wafer (MPW) service [19].

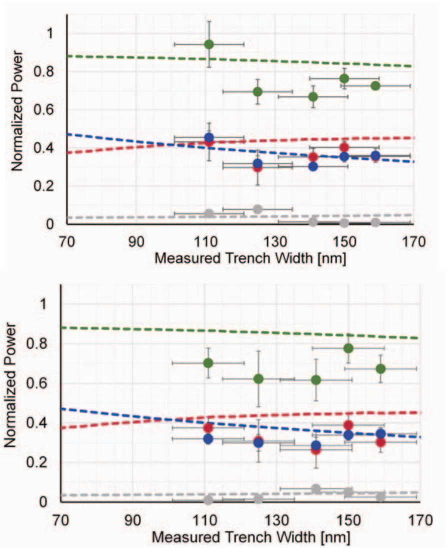

Fig. 3: Normalized Power for 2×2 Coupler vs. Trench Width for two different dies

After fabrication, the chips were packaged for reliable test and characterization. The PIC die was mounted on a ceramic carrier that, in turn, was epoxied to a "printed circuit board" (PCB). Two 32-fiber V-groove arrays were aligned to the edge couplers and also epoxied into place.

V. PIC/PUF Experimental Results

Fig. 4 depicts a block diagram of our PUF characterization set-up. A 1550nm diode laser is fiber coupled, routed to a manual polarization controller, and launched into the PIC under test. The output power from the two output edge couplers is measured by a power meter.

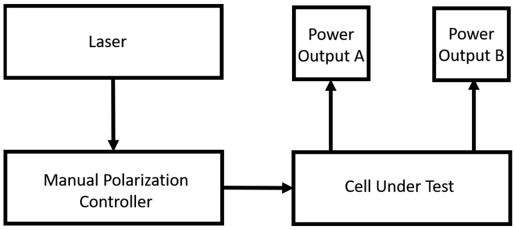

Fig. 4: Schematic of the experimental setup

The strength of the principle of operation of the PUF circuit explored here is the strong sensitivity of the polarization transfer function to perturbations of the optical path. This strong sensitivity also places demands on the laboratory set-up or instrumentation used to measure the polarization transfer function. Varying mechanical perturbations on the fibers from the laser to the polarization controller, from the polarization controller to the device-under-test and from the device-under-test to the power meters can influence the measurements. In our laboratory set-up, care was taken to maintain the mechanical environment of the optical fibers.

In Fig. 5, a photograph of the experimental apparatus is shown. The diode laser is situated at the righthand side of the photograph, the power meter is next to the laser source. The PCB and the fiber-coupled PIC are visible in the left part of the photograph. The manual polarization controller comprises three paddles whose tilt determines the input, or challenge signal SOP. In the photograph the paddles horizontal to the light table that we designate as the "0 position." Likewise, a vertical paddle orientation is in the "1 position." In the experiments reported here, we used eight different input SOPs denoted by a 3-bit code representing the paddle positions. Thus, the collection of $N = 8$ different (c_j, r_j) pairs can be mathematically modeled as $(c_j, r_j) \in \mathbb{Z}_2^3$, or alternatively, they could be modeled as $(c_j, r_j) \in \mathbb{Z}_8^1$.

VI. Results

Four 2×2 different trench coupler-based PUFs (denoted as PIC subcircuits A12, A19, A28 and B12) are characterized with eight different input signal SOPs. For each SOP, the two output signal power values measured and their ratio calculated. This data is presented in Table I. The average ratio of output polarization component powers is 0.589 and the standard deviation is 0.379. For the PUF application, it is desirable to have a standard deviation on the order of the average. In Table II, the same data is presented in digital, or radix-2, format, with power ratios expressed as corresponding 10-bit codes since it is reasonable to measure powers to one part in one thousand. If the system had a varying amount of incident PUF challenge power or a reduced resolution measurement device, fewer digits could be measured with a p=8 radix as shown in Table III. It is noted that any radix value can be chosen and it need not be a power of two.

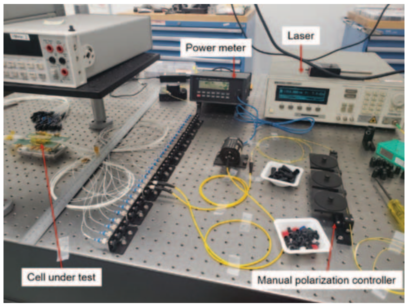

Fig. 5: Photograph of the experimental set-up.

Table I: Polarization Challenge versus Response (radix-10)

Input Polarization State Challenge	Four Different PUF Circuit Responses (Single PIC)			
	PUF A12	**PUF A19**	**PUF A28**	**PUF B12**
0	0.05897	0.45778	0.08919	0.46667
1	1.04514	0.42045	0.84861	1.37658
2	0.61097	0.78221	0.37562	1.07407
3	0.37828	0.65079	0.66124	0.63991
4	1.24345	0.74622	1.21951	1.40203
5	0.13656	0.26748	0.12695	0.48333
6	0.41358	0.22807	0.54829	0.77273
7	0.13154	0.65768	0.21042	0.31833

TABLE II: POLARIZATION CHALLENGE VERSUS RESPONSE (RADIX-2)

INPUT POLARIZATION STATE CHALLENGE	**FOUR DIFFERENT PUF CIRCUIT RESPONSES (SINGLE PIC)**			
	PUF A12	**PUF A19**	**PUF A28**	**PUF B12**
000	0000011110	0011101010	0000101101	0011101110
001	1000010111	0011010111	0110110010	1011000000
010	0100111000	0110010000	0011000000	1000100101
011	0011000001	0101001101	0101010010	0101000111
100	1001111100	0101111110	1001110000	1011001101
101	0001000101	0010001000	0001000001	0011110111
110	0011010011	0001110100	0100011000	0110001011
111	0001000011	0101010000	0001101011	0010100010

TABLE III: POLARIZATION CHALLENGE VERSUS RESPONSE (RADIX-8)

INPUT POLARIZATION STATE CHALLENGE	**FOUR DIFFERENT PUF CIRCUIT RESPONSES (SINGLE PIC)**			
	PUF A12	**PUF A19**	**PUF A28**	**PUF B12**
0	000	165	026	167
1	413	153	331	540
2	234	310	140	422
3	140	246	251	243
4	476	277	470	546
5	042	104	040	173
6	151	072	214	305
7	041	250	065	121

VII. CONCLUSIONS

A PIC-based PUF is described and modeled as a discrete MVL function. The PUF is motivated to counteract recently emerging attacks to electronic PUF circuitry-based eavesdropping through EMI and other methods since optical signals are less susceptible to extraneous leakage. The PUF model is generalized to an MVL formulation that avoids the need to specifically characterize the exact SOP. Preliminary results indicate that this approach is a viable and more secure approach for future PUF implementations as compared to conventional electronic PUF circuitry. The PUF circuitry is further enhanced due to the use of a new 2×2 power coupler devised by the authors [17].

Modeling the PUF physical one-way function as a discrete radix-p MVL function is introduced and the advantages of using this model include compatibility with past electronic PUF models while also allowing the PUF to function without requiring exact SOP state measurements.

Determining the authenticity of the PUF signature will include the repeated measurement of the PUF signature. Two approaches may be envisioned. The first is the PUF signature measurement in a trusted laboratory or with optimized peripheral instrumentation. This approach demands that the PIC be returned from the field for the validation. This undesirable step enables a more precise determination of the PUF signature and, in this case, more SOP inputs. The second approach is to embed the polarization transfer function measurement capability in the fielded unit so that independent, remote measurements of the PUF signatures may be made. Programmable polarization control on a miniaturized scale is possible and advances in this capability would benefit the PUF described herein.

Periodic resetting of the PUF signature is also a desirable property. There are, in the proposed polarization transfer function based PUF, post-fabrication techniques such as localized thermal cycling that can be deployed to enable the encoding of a new PUF signature.

REFERENCES

[1] K. Lofstrom, W.R. Daasch and D. Taylor, “IC Identification using Device Mismatch,” in proc., *IEEE Int. Solid-State Circ. Conf.*, February 2000, pp. 372-373.

[2] R.S. Pappu, “Physical One-way Functions,” *Ph.D. dissertation*, Massachusetts Institute of Technology (MIT), AAI0803255, 2001.

[3] B. Gassend, M. Dijk, D. Clarker and S. Devadas, “Controlled Random Functions,” in proc., *Ann. Comp. Sec. App. Conf.*, December 2002, pp. 149-160.

[4] B. Gassend, M. Dijk, D. Clarker and S. Devadas, “Silicon Physical Random Functions,” in proc., *ACM Conf. Comp. and Comm. Security*, November 2002, pp. 148-160.

[5] J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. Dijk and S. Devadas, “A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications,” in proc., *Symp. on VLSI Circ.*, June 2004, pp. 176-179.

[6] K.A. Bowman, S.G. Duvall and J.D. Meindl, “Impact of Die-to-die and Within-die Parameter Fluctuations on Maximum Clock Frequency Distribution for Gigascale Integration,” *IEEE Jour. of Solid-State Circ.*, **37**(2):183-190, February 2002.

[7] A.R. Korenda, F. Afghah, B. Cambou and C. Philabaum, “A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices,” in proc., *Workshop on Sec., Trust and Priv. in Emerging Cyber-physical Sys.*, 2019.

[8] M. Majzoobi, F. Koushanfar and M. Potkonjak, “Lightweight Secure PUF,” in proc., *IEEE/ACM Int. Conf. Comp.-Aided Design*, November 2008, pp. 670-673.

[9] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas and J. Schmidhuber, “Modeling Attacks on Physical Unclonable Functions,” in proc., *ACM Conf. Comp. and Comm. Sec.* (CCS), October 2010, pp. 237-249.

[10] R. van den Berg, B. Škorić and V. van der Leest, “Bias-based Modeling and Entropy Analysis of PUFs,” in proc., *Int. Workshop on Trustworthy Emb. Dev.*, November 2013, pp. 13-20.

[11] J. Yoon and H. Lee, “PUFGAN: Embracing a Self-adversarial Agent for Building a Defensible Edge Security Architecture,” in proc. *IEEE Conf. on Comp. Comm.*, July 2020, pp. 904-913.

[12] C. Helfmeier, C. Boit, D. Nedospasov, S. Tajik and J.-P. Seifert, “Physical Vulnerabilities of Physically Unclonable Functions,” in proc. *Des., Aut. & Test in Eur. Conf.*, March 2014, pp. 1-4.

[13] M. Fox, Quantum Optics An Introduction, Oxford University Press, New York, 2006.

[14] P. Lambropoulos and D. Petrosyan, Fundametals of Quantum Optics and Quantum Information, Springer, Berlin Heidelberg New York, 2007.

[15] R.C. Jones, “A New Calculus for the Treatment of Optical Systems,” *Jour. of Optical Soc. Of America*, **31**(7):488-493, 1941.

[16] C.D. Poole and J. Nagel, “Polarization Effects in Lightwave Systems,” in Opical Fiber Telecommunications Volume IIIA, I.P. Kaminow and T.L. Koch, *eds*., pp. 114-161, 1997.

[17] H. Shahoei, I.G. Achu, E.J. Stewart, U. Tariq, W.V. Oxford, M.A. Thornton, and D.L. MacFarlane, “Silicon Photonics 2×2 Trench Coupler Design and Foundry Fabrication,” *App. Optics*, **61**(16):4927-4931, 2022.

[18] G.G. Stokes, “On the Composition and Resolution of Streams of Polarized Light from Different Sources,” *Trans. Of the Cambridge Philosophical Society*, 9(399), 1852.

[19] American Institute for Manufacturing (AIM) Photonics, “Multi-Project Wafers (MPW),” https://www.aimphotonics.com/mpw, (*last accessed November 12, 2022*).

[20] Siemens Corp., “L-Edit Photonics,” https://eda.sw.siemens.com/en-US/ic/ic-custom/photonic/l-edit-photonics, (*last accessed November 12, 2022*).