

Reconfigurable Integrated Optical Interferometer Network-Based Physically Unclonable Function

Amos Matthew Smith and H. Shelton Jacinto , Member, IEEE

Abstract—In this article we describe the characteristics of a large integrated linear optical device containing Mach–Zehnder interferometers and describe its potential use as a physically unclonable function. We propose that any tunable interferometric device of practical scale will be intrinsically unclonable and will possess an inherent randomness that can be useful for many practical applications. The device under test has the additional use-case as a general-purpose photonic manipulation tool, with various applications based on the experimental results of our prototype. Once our tunable interferometric device is set to work as a physically unclonable function, we find that there are approximately 6.85×10^{35} challenge-response pairs, where each challenge can be quickly reconfigured by tuning the interferometer array for subsequent challenges.

Index Terms—Challenge response, CMOS process, optical network, Physically Unclonable Function (PUF), Security, SOI.

I. INTRODUCTION

PHYSICALLY unclonable functions (PUFs) or physical one-way functions (POWFs) have been suggested as a method to securely authenticate a networked device or remote user. Current state-of-the-art means of authentication begins with the usage of a classical secret key, or token, stored within a read-only memory (ROM). PUFs are of particular interest since they often form the basis of hardware primitives necessary to replace shared secret keys with a non-reproducible physical object or device.

Classical CMOS-based PUFs are physical primitives that utilize process fabrication variance to create unique POWFs. Unlike non-volatile memory, where information can be stored and read digitally, information in CMOS-based PUFs is directly extracted from inherent lithographic variation, making static PUFs impossible to be duplicated; even within the original manufacturing process [1]. Other common forms of CMOS PUFs include arbiter PUFs [2] that utilize delays to measure differences in transmission times of two competing pathways in order to generate a digital response, butterfly PUFs [3], [4]

Manuscript received August 27, 2019; revised January 27, 2020 and April 22, 2020; accepted May 15, 2020. Date of publication May 20, 2020; date of current version September 1, 2020. (Amos Matthew Smith and H. Shelton Jacinto contributed equally to this work.) (Corresponding author: H. Shelton Jacinto.)

Amos Matthew Smith is with Air Force Research Lab, Rome, NY 13440 USA (e-mail: amos.smith.6@us.af.mil).

H. Shelton Jacinto is with Air Force Research Lab, Rome, NY 13440 USA, and also with Boise State University, Boise, ID 83725 USA (e-mail: sheltonjacinto@u.boisestate.edu).

Color versions of one or more of the figures in this article are available online at <https://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/JLT.2020.2996015

that examine output from a set of cross-coupled latches, and random-access memory (RAM) PUFs [5] that are based on randomly distributed mismatches between two transistors where the repeatable start-up conditions of cells are treated as digital responses.

The operating scheme for all types of PUFs remains essentially identical: Given a set of specific inputs, referred to as the challenge, a PUF will generate a unique output response. These inputs and corresponding outputs are known as the challenge-response pairs (CRPs). The manufacturer or user of the PUF enrolls the device's unique information by generating and recording all of the viable CRPs. The user can then verify the identity of the integrated (or remote) PUF, at a later time, by challenging the suspect device and comparing the response to the expected response. In this work, our challenge will be a set of randomly selected voltages applied to the device, \vec{C} . The response will be the normalized distribution of laser intensity in the output modes that results from those voltage settings, \vec{R} . The details of this scheme will be described in Section II.

PUFs based on optical measurements have been proposed with differing operating mechanisms, where either the scattering of laser-light from bulk inhomogeneous media [6], multi-mode fiber [7], or non-linear interaction in specialized integrated devices [8] are observed. One of the main reasons that electronic PUFs are commonly implemented into field programmable gate arrays (FPGAs) and other protected IPs is due to the electronic PUFs' ease of integration into the many existing CMOS-process devices, alongside their low size, weight, and power requirements. Optical PUFs often require non-trivial bulk optics and ancillary support such as micron-accurate positioning stages [6] or bulk disordered materials [7]. A more compact solution was conceived by Grubel *et al.* [8] through the utilization of photonic integrated circuits (PICs), however, these PIC PUFs require a set of completely custom-designed devices for the sole purpose of use as a PUF.

Here we propose that any large- and well-connected-enough array of linear interferometric devices can be used for both its designed purpose *and* as an optical PUF. The ongoing development of large-scale PICs, and particularly large interferometric devices [9]–[13], along with the wide range of applications from general information processing [12], quantum key distribution [11], quantum optics [9], and even the development of deep-learning and optical neural networks [14], [15], suggest that such linear PICs will become ubiquitous components in the future. Analogous to the development of RAM-based PUFs, our circuit was not specifically designed to act as a PUF. We

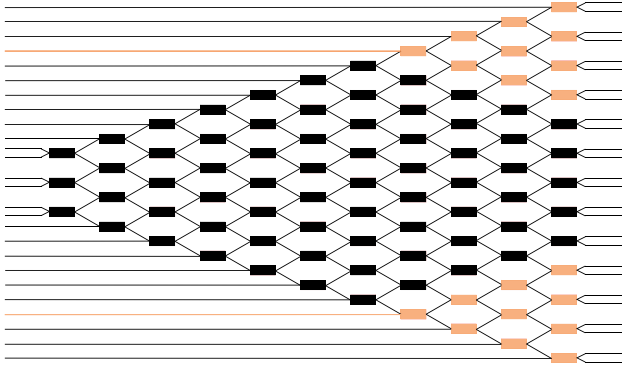


Fig. 1. Structure of Quantum Photonics Processor, where each rectangular box represents a single 2×2 MZI. The figure shows two logically separated devices (orange), consisting of 10 MZIs each, and the pumping scheme within the larger QPP. The largest PUF on the QPP is pumped down the center channel and consists of 66 MZIs.

demonstrate that the large interferometric circuits now being developed by the authors and other groups [9]–[16] have an additional application as a PUF.

In this work we describe a linear optical interferometric PIC which acts as a PUF. We demonstrate how a small sub-circuit operates as a weak PUF, but has the ability to further meet the criteria of a strong PUF. We show how the scaling of an integrated optical circuit intrinsically carries enough randomness from multi-input interference via adjustments of Mach-Zehnder interferometers (MZIs) to act as a practical PUF.

The major advantage of using such a PUF is compatibility with existing CMOS fabrication for easy adoption with existing technologies. The PIC PUF's tight integration with other PIC devices, such as those used in quantum communication, allows for improved security over add-on alternative PUF IPs. Our PUF's performance, and large number of challenges, discussed in Section IV, give it excellent characteristics as a strong PUF. Finally, the ability to use *any* large circuit of interferometers as a PUF, combined with the growing size and number of such circuits, suggest that our device could become an ubiquitous component in the near future.

II. THE QUANTUM PHOTONICS PROCESSOR

In this research we have employed the Quantum Photonics Processor (QPP)* developed in collaboration between the Air Force Research Lab (AFRL) and the photonics research group, under the direction of Dirk Englund at MIT [12], [16], as our prototype linear optical interferometric PUF. The optical PUF device is designed as a silicon-on-insulator (SOI) integrated optical chip fabricated in a CMOS foundry. The PIC device consists of 88 2×2 MZIs connected in a triangular nearest-neighbor configuration, as shown in Fig. 1.

The devices are standard Silicon on Insulator (SOI), a thermo-optic optical material, and as such each MZI can be independently, thermally, tuned by an integrated resistive heating element. The 2

$\times 2$ MZI is capable of applying an idealized 2×2 unitary transformation shown in Equation 1, expanded upon in Section III.

$$U_{MZI}(\theta, \phi) = \frac{1}{2} \begin{pmatrix} e^{j\phi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix} \begin{pmatrix} e^{j\theta} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix} \quad (1)$$

Each MZI consists of two integrated phase shifters: One phase shifter between the beam splitters and a second phase shifter on a single output-leg. The unitary transformation in Equation 1 includes two variables, θ and ϕ , which map to the internal phase setting and output phase offset, respectively, for each MZI. In this work we only employed the internal phase shifters, driven by a computer-controlled voltage driver [13], and thus have two PUF devices consisting of 10 MZIs, pumped by a Keysight laser (model 81606 A) through a single waveguide, respectively. The fiber-arrays and edge-coupling of the QPP is shown in Fig. 2. Each PUF device has 8 output ports, each connected via SMF-28 to a single standard PIN photodiode (Precision Micro Optics model DPRM-412). The subset devices used within the QPP are triangular-shaped with a light-cone-like dispersion region, visualized by the orange regions in Fig. 1.

The first source of randomness for this device is the $\approx 15.43\%$ variation between resistive heating elements, as measured, due to fabrication variances. It should be noted that the continual operation of the resistive heating elements will lead to electrode annealing, thus a change in the output of the PUF could be observed over time. A far more significant effect on randomness are the two directional couplers within each MZI. The couplers are designed to be a nominal 50:50 splitting ratio but fabrication defects stemming from variation in the etching process, sidewall roughness, and variation in minute distances between waveguides leads to unpredictable splitting ratios near 50%. An additional source of unpredictability leading to potential for randomness in the device comes from a minor design flaw: Since many of the MZIs share ground leads, positive feedback ground-loops are formed when a single MZI's voltage is set and the cascading MZI's resistive elements return a complex set of voltages, set by nearest-neighbor association. The effect of ground-loop feedback is approximately -45 dB as measured by M. Prabhu [17]. It can be expected that the positive feedback ground-loop voltage errors may be a minor factor in the device's overall behavior. To minimize unwanted global thermo-optic effects, the device was held at a steady temperature, slightly above ambient, throughout testing. The effects of operating at differing temperatures have not yet been explored, however, the device can operate at a wide range of steady temperatures, with each having an impact on output characteristics, without damage. The differing global temperature effects on the PUF are further discussed in Section IV.

The QPP is large enough to act as two distinct devices with identical structure. Two devices were programmed to be used for comparison by taking the QPP and pumping laser-light into two space-like separated regions such that the light from one device will not reach the other device, either directly or through reflections other than those coupled into the slab-mode. In addition, the two devices are electrically separated so that no positive ground-loop feedback effects exist between the devices.

*Also known as the Programable Nanophotonic Processor (PNP).

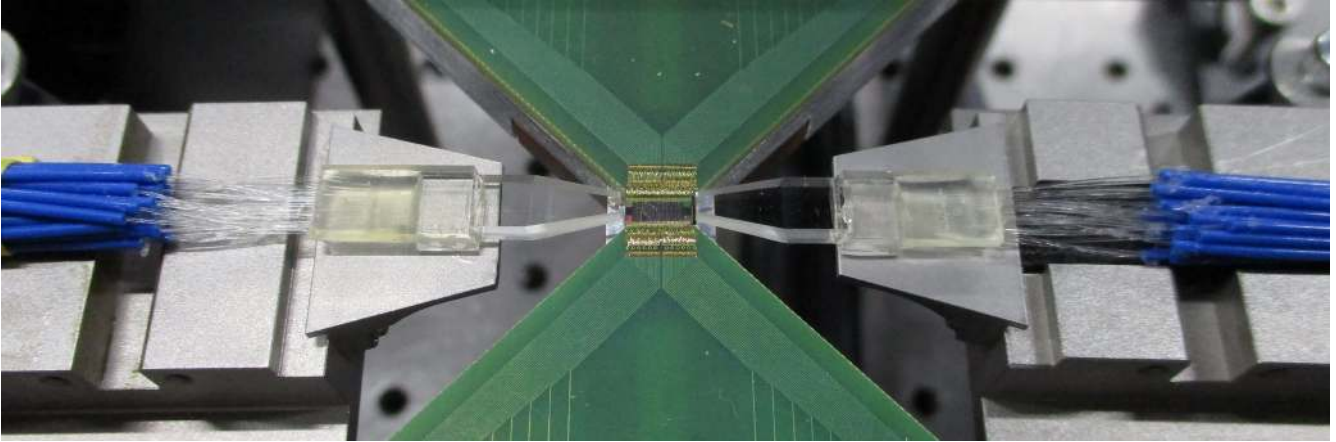


Fig. 2. Quantum Photonics Processor shown with two 26-mode fiber arrays edge-coupled to the QPP. The fiber array on the left is the input of laser-light into the QPP, connected to a printed circuit board with connections to control the integrated resistive heating elements. The fiber array on the right leads to an array of PIN photodiodes to measure intensities on the outputs.

III. PUF METRICS

We use the definitions of a weak and strong PUF given by C. Herder *et al.* [1]. A weak PUF is described as:

- a) Having a number of CRPs linearly related to the number of components,
- b) being robust against environmental effects, i.e. having stable CRPs,
- c) having unpredictable responses to any stimulus and,
- d) being extremely impractical to reproduce.

A strong PUF is characterized by all of the previous statements regarding weak PUFs with the addition of:

- e) Having enough CRPs such that the number is exponential in the number of challenge bits and
- f) that the readout will reveal only the response $\bar{R} = f(\bar{C})$ and nothing else.

One metric chosen to test the difference between CRPs is the Euclidean distance, ℓ^2 -norm, of the N outputs. To measure the Euclidean distance the analog response of each detector is divided into even-sized subsets; each of which is larger than the estimated noise of the system. For our test we chose a subset of size 0.5% of the total power detected across the m outputs, scaled by a cross-normalization factor.

To decrease and/or correct error within the testing of our PUF the size of voltage subset utilized in computation was increased to 0.1%. The increase in subset size serves to decrease the chances that any noise present on a particular channel straddles the bounds between two values. The increase in subset size also applies a reduction in resolution for the ℓ^2 distance. An alternative option to decrease and/or correct error within the testing of our PUF is to increase the collection time, thus increasing the amount of sample-averaging that forms a single CRP. The drawback to relying on increased collection times are the latency requirements, which may hamper any fast electronics requiring the output of the PUF, and the possibly of allowing an adversary additional time to perform side channel attacks.

The second set of metrics used to quantify the results and operation of the PUF are the inter- and intra-device Hamming

distances (HD_{inter}, HD_{intra}) along with the inter- and intra-device Euclidean norms ($\ell_{inter}^2, \ell_{intra}^2$). To analyze the results we modified the standard Hamming distances between a response \bar{R}_i from challenge \bar{C}_i , and response \bar{R}_j from challenge \bar{C}_j , to reduce the effects of noise. The loose Hamming distance (LHD) can be calculated between two noisy response vectors, \bar{R}_i and \bar{R}_j , for all of the corresponding laser-light intensity measurements on the output modes k as:

$$LHD = \sum_k f(\bar{R}_i, \bar{R}_j)_k = \begin{cases} 0, \forall k \text{ if } |R_{i,k} - R_{j,k}| < L \\ 1, \forall k \text{ if } |R_{i,k} - R_{j,k}| \geq L \end{cases} \quad (2)$$

Where $L \in \mathbf{N}$ defines the degree of looseness, and $L = 1$ is the normal Hamming distance. For the case of small PUFs, $L = 2$ is sufficient. The definition for LHD is used to compensate for the experimental noise and rounding errors as discussed below. In addition to the LHD , the standard ℓ^2 -norm is used following the definition given by:

$$\|\bar{x}\|_2 = \sqrt{\sum_i x_i^2}. \quad (3)$$

The major difference between these two metrics, for non-binary data, is that the Hamming distance represents the number of measurements which are different, while the Euclidean norm gives a metric of the significance of differentiation. Interestingly, we can expand upon the Hamming distances and determine the *uniqueness* of our device as described by R. Maes *et al.* [18]. Uniqueness is a calculated estimate for the amount of entropy available from a PUF and can be applied to a similar population of PUFs with an identical architecture. The uniqueness, \mathcal{U} , can be calculated for some challenge \bar{C}_i as:

$$\mathcal{U}|_{C_i} = \left(\frac{2}{n(n-1)} \sum_{i=1}^{n-1} \sum_{j=i+1}^n \frac{LHD(\bar{R}_i, \bar{R}_j)}{m} \right) \times 100\%, \quad (4)$$

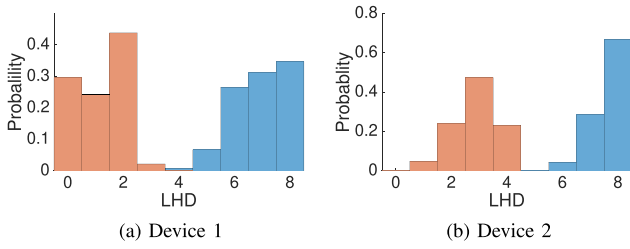


Fig. 3. Distinguishability of LHD_{intra} , for both devices. LHD_{intra} between the same repeated challenge (orange) and between a typical challenge and random challenges (blue) on the same device.

Analogous to Equation. 2, $L = 1$ gives the standard definition of uniqueness. Here, n is the number of PUFs in a population, and m represents the number of bits in the response from the PUF. An optimal uniqueness value for binary PUFs would be 50%, as this implies uncorrelated responses. Since our PUF is continuous via electronic control, we need to modify our interpretation of Equation 4. Given that $LHD = 0$, i.e. a complete collision, doesn't contribute to $\mathcal{U}|_{C_i}$ and a partial collision contributes only the fraction that didn't collide, $\mathcal{U}|_{C_i}$ is counting non-colliding responses. Regardless of the looseness this is equivalent to a target uniqueness between devices of 100%.

IV. RESULTS

For this work we created several sets of data. First, using the two small sections from Fig. 1, we created 100,000 random CRPs mirrored on each device, and an additional single CRP was repeated 5,000 times on each device. Secondly, we tested the largest PUF that would fit on the device, again with random CRPs, and a repeated CRP. All of the CRPs were randomly selected in each variable from a uniform distribution over the $v2\pi$ voltage range required for a complete switching response of a typical MZI, detailed by the sinusoidal response from Equation 1, easily modified into a sine/cosine format shown in Equation 5.

$$U_{MZI}(\theta, \phi) = \frac{1}{2} \begin{pmatrix} e^{j\phi}(e^{j\theta} - 1) & je^{j\phi}(e^{j\theta} + 1) \\ j(e^{j\theta} + 1) & -(e^{j\theta} - 1) \end{pmatrix} \\ = je^{\frac{j\theta}{2}} \begin{pmatrix} e^{j\phi} \sin\left(\frac{\theta}{2}\right) & e^{j\phi} \cos\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \end{pmatrix} \quad (5)$$

A. A Small PUF

To complete the analysis of responses of the small PUFs depicted in Fig. 1, eight output intensities were measured via a polled array of photodiodes for each device, with results below.

Fig. 3 shows the repeatability (orange, left peak) of the same challenge applied 5,000 times to each device. The two devices show a relatively low $LHD \leq 4$. The difference between Fig. 3 a and Fig. 3 b is accounted for by the differences in noise level, with a higher total noise on the second device.[†] The second

[†]This difference is likely caused by photodetector variation due to differing production batches with a result of approximately 1.5 times the noise shown on the datasheet for the PIN photodiodes previously mentioned.

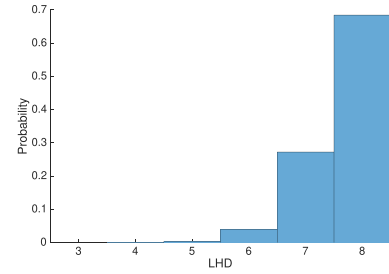


Fig. 4. LHD_{inter} . Distances between 100,000 randomly chosen challenges applied to two near-identical devices, with the comparison between the two resulting responses, showing no full collisions.

dataset in both figures (blue, right peak) shows the difference between a typical CRP and the 100,000 randomly selected CRPs. The two devices show strong repeatability through the LHD metric, by staying within a narrow variable range. The two devices additionally show strong metrics for distinguishability. The differences between a single CRP to a differing CRP set is easily identified. Ideally, $LHD_{intra} = 0$ should be true for a fixed challenge, and $LHD_{intra} = 8$ for differing challenges. The ℓ^2 -norm is necessary to provide an additional measure of the significance of differences before validating the identity of a PUF.

For applications of this PUF in authentication roles, the key importance is the inter-chip response to the same challenge. Fig. 4 depicts the LHD_{inter} metric between 100,000 randomly chosen CRPs as they apply to both devices. As discussed further, the number of challenges is too large to test all possible settings. For 100,000 challenges mirrored between the two devices, we analyze Equation 4 to find a total uniqueness of 85.28% at $L = 2$. LHD_{inter} is strongly centered around $LHD_{inter} = 8$, approximately 70% the response vectors have no corresponding measurement values in common ($R_{i,k} \neq R_{j,k}, \forall k$), and less than 10% have more than two out of eight corresponding measurements in common. We found no complete collisions[‡], which would be required for a false positive identification. This is highly encouraging as our devices are as identical as physically possible due to simultaneous fabrication (identical material, design, processing, environment, etc.) and are effectively 'clones' of one-another. Any attempt to physically recreate a device to be utilized as a PUF will inherently possess additional random variance and produce a clearly differentiated LHD_{inter} versus the original device.

The commonality of the measurements are shown in Fig. 5, where the blue (right peak) data shows the ℓ^2_{inter} distance between the two devices, for each challenge. The smallest ℓ^2_{inter} distance found was 11, with a mean of 58, median of 55, and standard deviation of 23. The orange (left peak) data shows the ℓ^2_{intra} distance between a typical response and all other responses to the same challenge on a single device. The data shown is typical with limited overlap between histograms. Some

[‡]In this context we take a collision to be complete where all output values are identical for two different given challenges, i.e. \bar{R}_i and \bar{R}_j where $R_{i,k} = R_{j,k}, \forall k$, or partial where two challenges result in some similar outputs; these are not fully distinguishable since a distinguisher can exist where a value can be differentiated from a random oracle [19].

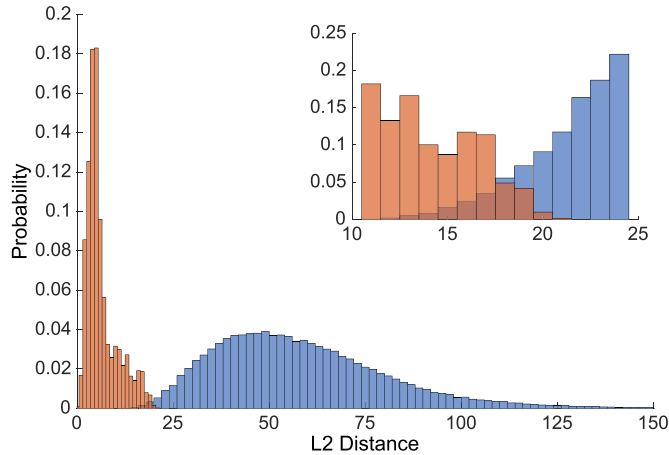


Fig. 5. Euclidean distances, showing the distance between the response to identical voltage settings on both devices (ℓ_{inter}^2 , blue) and the response of one device to the same repeated challenge (ℓ_{intra}^2 , orange, typical). The inset shows the region of overlap.

CRPs appear to have more noise than others, and multiple datasets have shown no overlap at all between histograms, the least distinguishable of which is shown as an example in Fig. 5; the ℓ_{intra}^2 data shown here has a mean of 6, median of 5, and a standard deviation of 4.

A major source of errors during measurement, unfortunately, is the instability of input- and output-coupling, leading to variability in total intensity over time. There are two significant components to the coupling errors; a high-frequency component and a slow drift caused by undamped environmental noise and sagging positioning stages holding the edge-coupled fiber arrays, respectively. The signal to noise ratio (SNR) within our system is approximately 16 dB. The laser and detector SNR is estimated to be approximately 50 dB, based on the dark-count of the photodetectors. The losses on the integrated chip are stable and do not vary with time. The PIN photodiodes used to measure the output signals have a constant background noise and gain, such that the effects of losing overall intensity represents a reduction in SNR. For our comparison, the loss of intensity can be counteracted by normalizing the total intensity and the set-sizes over each CRP to a fixed value prior to calculating the data sets. As such, the result of comparison is the difference between relative intensities for each channel and not the total intensities. The main source of the intensity error is a result of physically edge-coupled fiber arrays, on manual positioning stages, rather than permanently affixed arrays. A packaged device with permanently affixed fiber arrays are a requirement for any practical system and will nearly eliminate this source of error.

1) *Range and Number of CRPs*: The total significance of any individual setting within a CRP is not uniform across the device. Of the ten input variables in each small device, four can only affect two of the output measurements each in the current design. Physically, this can be observed as the last column of 4 MZIs or the base of the pyramid in Fig. 1 as opposed to the input or ‘tip’ of the pyramid that affects all output channels. A concern with this architecture is the possibility that a nearest-neighbor

challenge will produce a semi-predictable response and there are many fewer distinguishable responses than there are challenges.

Therefore, an important question for any proposed PUF is how many uniquely identifiable CRPs are available and how the number of CRPs scales with the size of PUF. Weak PUFs can have as few as one CRP, although this is a severe limitation on the number of applications [1]. Given the input amplitudes and detector noise on the output modes, we are able to clearly distinguish a voltage change on a single MZI of $\approx 7mV$. As each MZI in the system has a $v2\pi \approx 7$ V range, we define 10 bits of resolution in voltage as $v2\pi/1024$ for each MZI. Naïvely we could estimate that since the PUF has 10 bits of resolution, on ten independent MZIs, as shown in Fig. 1, there are $2^{10 \cdot 10} \approx 1.27 \times 10^{30}$ possible challenges on each device. However, this ignores a large number of partial collisions in the output space of the PUF and also ignores the structure of the device. When taking the largest set of MZIs in a light-cone pattern, we see that, at most, 66 MZIs exist in our architecture. Assuming a 10-bit resolution, we could again theorize a maximal upper bound of challenges for some set of 66 MZIs of $2^{10 \cdot 66} \approx 4.78 \times 10^{198}$.

However, this calculation is out of scope: Determining the number of challenges within our architecture that have *distinguishable* responses is a more difficult and productive task. For our architecture, with a light-cone diffusion, we can better approximate a maximal upper bound by following the Catalan numbers [20], C_n , from combinatorics and count the number of *distinguishable* settings by analyzing the MZI structure as a fully-rooted binary tree with $n + 1$ leaves. We can use a rooted binary tree since we pump the PUF from a single input and can calculate an upper bound given by:

$$C_n = \frac{(2n)!}{(n+1)!n!}. \quad (6)$$

Following the Catalan numbers, we calculate that for 10-bit resolution there are approximately 5.77×10^{39} combinations for an array of 66 MZIs, not necessarily our specific configuration of MZIs. This maximal upper limit is unfortunately still too large due to the number of configurations of 66 MZIs that are not possible within our architecture. The limit of the architecture where pure Catalan numbering cannot apply is due to the limited number of columns in our device. The limit in number of columns means that the Catalan numbering scheme will count combinations in a light-cone pattern that are impossible: Think of an arrangement where the first 11 MZIs are set to pass light linearly down in a straight line with an additional 55 MZIs hanging off of the end of our architecture.

To overcome the configuration limit set by the standard Catalan numbers, we must utilize a lesser-known combinatorics counting method for binary trees as described by F. Qi *et al.* [21], the method of counting by integral representation of the Catalan numbers. The method of integral counting can be directly applied to the planar tree variation of counting, similar to the work by P. Flajolet *et al.* in [22].

If, for a forest composed of a set of trees, $\mathcal{F} = \{t_0, t_1, \dots, t_k\}$, we look at a single tree, $t_i(n, h)$, this tree can represent any binary tree with or without a shared child of height h with n nodes. Simply, $\sum_h t_i(n, h) = C_n$, for the n -th Catalan number.

Algorithm 1: Algorithm to Calculate Catalan Recurrence for Planar Trees $t_i(n, h)$.

Require: $n \geq 0$ and $h > 0$
 recurs \leftarrow values of n and h into a 2 dimensional array at index $[n, h]$ with the number of combinations.
 sum \leftarrow values of operations and calculates the sum.
procedure Recurrence($[n, h]$)
 i, j , Local Variables
 n', h' , Shadow Copy of n and h
 recurs[0, 0] = 1
 if $h < n$ or $h > 2^n - 1$ **then**
 recurs[n', h'] = 0
 else if $1 \leq n \leq h \leq 2^n - 1$ **then**
 for i, j **do**
 recurs[n', h'] = recurs[n, h]
 = sum[recurs[$n - 1, h - 1 - i$]
 $\times (2 \times$ sum[recurs[j, i], ($j, 0, n - 2$)]
 + recurs[$n - 1, i$], ($i, 0, h - 1$)]
 end for
 end if
end procedure

By analysis, the Catalan recurrence for a planar tree gives the recurrence formula for $t_i(n, h)$:[§]

$$t_i(n + 1, h + 1) = 2 \sum_{m=h+1}^n t_i(m, h) \sum_{j=0}^{h-1} t_i(n - m, j) + \sum_{m=h+1}^{n-h-1} t_i(m, h) t_i(n - m, h). \quad (7)$$

The formula in Equation 7 utilizes the double summation to count the number of combinations to build a binary tree on $n + 1$ vertices whose left sub-tree has a height h_0 , and whose right sub-tree has height $h < h_0$. Doubling this value by a factor of 2 adds all trees whose right sub-tree have height h'_0 , and whose left sub-trees have height $h' < h'_0$. The final term of Equation 7 serves to count the planar trees on $n + 1$ vertices whose left and right sub-trees are of height h .

To adequately enumerate the number of distinguishably different CRPs, Algorithm 1 was used to implement Equation 7 with parameters $0 \leq n \leq 11$ and $0 \leq h \leq 66$. After running Algorithm 1, the total number of distinct CRPs that are possible with 10-bit resolution are calculated to be $\approx 6.85 \times 10^{35}$. The full trees of MZIs configured into different columns with 10-bit resolution have the number of possible configurations shown in Table I. It should not be a surprise to see that as the number of columns increases, the possible configurations increases up to a point of maximal dispersion for sub-trees. The information regarding number of configurations due to architectural change will not be discussed further in this work, but may pose as an interesting topic of research.

[§]This formula requires the following definitions $t_i(0, 0) = 1$ and $\forall t_i(0, -) = 0$.

TABLE I
 VARIATION IN NUMBER OF CONFIGURATIONS VERSUS NUMBER OF COLUMNS FOR LIGHT-CONE CONFIGURATIONS WITHIN OUR DEVICE

Number of (Columns, MZIs)	Possible 10-bit Configurations
(4, 10)	1.19×10^5
(5, 15)	2.40×10^7
(6, 21)	2.76×10^{10}
(7, 28)	1.61×10^{14}
(8, 36)	4.40×10^{18}
(9, 45)	5.43×10^{23}
(10, 55)	2.94×10^{29}
(11, 66)	6.85×10^{35}

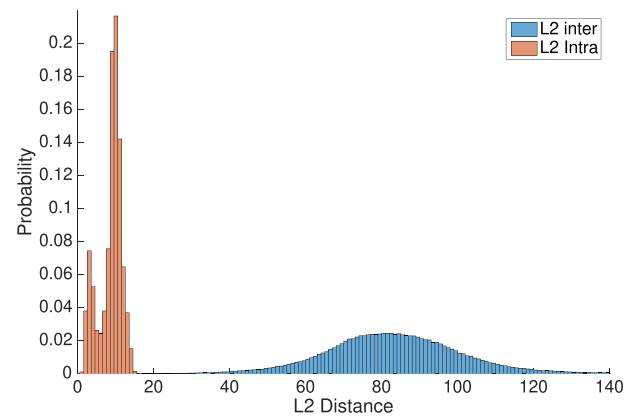


Fig. 6. Euclidean distances of the large PUFs, showing the distance between the response to identical voltage settings on the large devices (ℓ_{inter}^2 , blue) and the response of one device to the same repeated challenge (ℓ_{intra}^2 , orange, typical). The two peaks in the ℓ_{intra}^2 are most likely the result of unstable coupling combined with our normalization method, creating two distinct noise levels during data collection.

B. A Large PUF

The experiment above was repeated with the largest available PUFs on the current design of our chip. This was a ‘pyramid’ consisting of 66 MZIs, with one input mode and 22 outputs. Here the ‘top’ and ‘bottom’ individual PUFs are so large as to significantly overlap, in fact they share 45 out of 66 MZIs. Despite this overlap, we find excellent distinguishability between the two PUFs. Not surprisingly the distinguishability is improved over the small PUFs. However, there is a limit to the improvement with size. As the total intensity is distributed over an increasingly larger number of outputs, the SNR will limit the maximum size with any given laser power and sources of loss.

Fig. 6 shows the calculated ℓ^2 -norms, similar to Fig. 5. Note that the lack of an inset is the result of no overlap between the histograms. Increasing the width of the interferometer array is a route to increasing the total number of CRPs, as our current chip has three such 66 MZI subsets, giving a total number of CRPs on our device of $\approx 2.05 \times 10^{36}$. Simply adding another row of just 11 MZIs appears to add to $\approx 6.85 \times 10^{35}$ distinct CRPs.

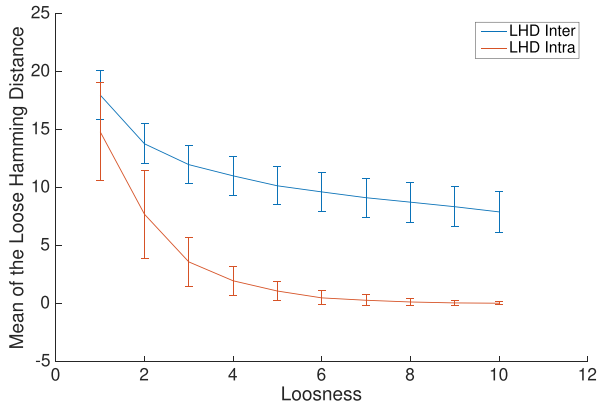


Fig. 7. Mean of the LHD with looseness, showing the difference between the mean of the LHD for different and repeated challenges at various definitions of the looseness parameter L .

One question we asked is in regard to the looseness of the Hamming Distance, LHD , and what the ideal degree of looseness would be for the system. Recall that by ‘loose’ we refer to a Hamming distance that overlooks small errors due to the noise and instability in our system. Naturally, the ideal parameter will vary based on the nature of the noise in the distributions being compared. We calculated the Hamming distance with varying degrees of looseness from the strict definition of Hamming distance ($L = 1$) to $L = 10$, and found the mean on resulting probability distribution; results shown in Fig. 7. Note that the significant overlap of the first standard deviation error bars at $L = 1$ results in the two PUFs looking all but identical under the strict Hamming distance definition. Under the ℓ^2 -norm and LHD there is no measured overlap in Fig. 6 or Fig. 7, respectively.

The mean of the LHD asymptotically approaches zero for for both test cases, however, the repeated challenge (orange, bottom curve) approaches significantly faster than the random comparisons (blue, top curve) in figure Fig. 7. The optimal parameter for the looseness was found to be between 5 and 6. At this point the two means are separated by 5.5 standard deviations of LHD_{Intra} , implying clear differentiability. This LHD -based approach is general, and as-such, this form of analysis can be used for any PUF with noisy output.

C. Attributes of an Optical CMOS-Compatible PUF

The results shown in Section IV-A1 serve to highlight the optical interferometric PUF’s ability to scale exponentially, thus meeting the first criterion for a strong PUF by C. Herder *et al.* [1]. An additional facet of the design shown is the ability to have quick reconfigurability to assess additional CRPs. Since each of the MZIs are independently tunable, we can see the response of a tuned device and change parameters for subsequent CRPs. The ability to tune our device at-will enhances application and use-cases to not only the static processing of information, but the processing of streaming information. It is thus possible to process information streamed through the device or static information where a set of CRPs is dynamically changed depending on the information received.

Unfortunately, there are several negative attributes to using a system of interferometers as a PUF. As mentioned in Section III, the nearest-neighbor challenges may give predictable results on smaller PUFs. In addition, the interferometric system is highly structured and fixed, such that a sufficient number of CRPs being calculated could lead to the device being fully characterized. Indeed the QPP was designed with such characterization in mind as the original use case was for applications and experimental testing of quantum optical networks [23]. We point out that the device was not originally intended to act as a PUF and we are merely exploiting its attributes. Since the reconfigurability of the QPP is available, it is possible to make one device clone the function of another device; for purposes as a PUF it is suggested to utilize this device in an uncalibrated mode. Custom designed interferometric circuits with more complicated interconnections, including variable feedback loops, would be more resistant to characterization and thus act as stronger PUFs. A second negative attribute of the current prototype is that the operating temperature must be stable within ± 1 °C. Allowing the temperature to vary may be a route to increasing the number of challenges and response pairs (CRPs). Whether or not two devices respond differently to temperature changes based on CRP normalization is an open research question. If temperature variation were not desired, packaging the device may lead to an easy method of stabilization. Alternatively, multiple sets of CRPs can be created for an array of temperatures prior to use. The variation with temperature observed is a direct result of using common SOI and CMOS fabrication. Silicon is a thermo-optic material and was chosen for its ease of integration into existing CMOS processes. However, the design for an interferometric optical PUF can be trivially transferred to an electro-optically controlled material such as Lithium Niobate to create a more stable standalone device, or application specific integrated circuit. It should be noted, however, that Lithium Niobate will still have a small thermo-optic effect. Conversely, each challenge \tilde{C}_i could double at as bias setting for the device. Variation in other parameters like global heating of the device, wavelength inputs, and variance in the number of pumped channels can allow each challenge to be utilized as an individual, separate, PUF. Here we have taken these parameters to be constants for simplicity but if allowed to vary, utilizing more parameters opens an enormous space of possibilities, and significantly increases the number of CRPs theoretically available.

Finally, with the software drivers used in these experiments we take approximately 3 seconds to completely set a challenge and measure a response of 1,000 physical measurements on the QPP. This has since been significantly improved with new driver optimization. The fundamental limit to the speed of the challenge and response is set by the maximum speed that the thermal switching can occur; estimated to be in the ≈ 100 kHz range [13]. This may appear slow but we stress that the experimental setup was in no way designed to optimize the speed of measurements. The system currently runs on several standard Arduino-driven Teensy boards, for ease of development. Hardware integration with an FPGA, and implementation in an electro-optical media, will result in orders of magnitude speed-ups to gigahertz speeds. If a design were optimized for usage as a PUF with the proper,

previously mentioned controls, we postulate that the existence of reconfigurable optical PUFs will greatly enhance the security of future optical communications.

V. CONCLUSION

The PIC device shown in this work meets the criteria for a weak PUF given by [1] and appears to also satisfy the definition of a strong PUF. The rapidly expanding research on large scale interferometric PICs, and the wide fields in which they are suggested for use, implies that such devices may become ubiquitous in the near future. This work shows that such large integrated devices carry with them useful amounts of unique randomness that can be used for tasks such as device identification, authentication, and other cryptographic tasks.

ACKNOWLEDGMENT

The authors would like to thank the group of D. Englund at MIT for assistance in the design and fabrication of the experimental optical chip. A. M. Smith would like to thank N. Stolten and F. H. Long of ARDEC for initial discussions prompting this line of study. H. S. Jacinto would like to thank AFRL for doctoral fellowship support. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views or endorsement of the U.S. Air Force Research Laboratory.

REFERENCES

- [1] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
- [2] T. Xu and M. Potkonjak, "Stable and secure delay-based physical unclonable functions using device aging," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2015, pp. 33–36.
- [3] S. S. Kumar, J. Guajardo, R. Maes, G. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardware-Oriented Secur. Trust*, Jun. 2008, pp. 67–70.
- [4] J. Guajardo, S. S. Kumar, G. Schrijen, and P. Tuyls, "Physical unclonable functions and public-key crypto for FPGA IP protection," in *Proc. Int. Conf. Field Programmable Logic Appl.*, Aug. 2007, pp. 189–195.
- [5] D. E. Holcomb, W. P. Bursleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.
- [6] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.
- [7] C. Mesaritakis *et al.*, "Physical unclonable function based on a multi-mode optical waveguide," *Scientific Rep.*, vol. 8, no. 1, pp. 1–12, Jun. 2018.
- [8] B. C. Grubel *et al.*, "Silicon photonic physical unclonable function," *Opt. Express*, vol. 25, no. 11, pp. 12 710–12 721, May 2017.
- [9] X. Qiang *et al.*, "Large-scale silicon quantum photonics implementing arbitrary two-qubit processing," *Nature Photon.*, vol. 12, no. 9, pp. 534–539, Sep. 2018.
- [10] J. Wang *et al.*, "Multidimensional quantum entanglement with large-scale integrated optics," *Science*, vol. 360, no. 6386, pp. 285–291, 2018.

- [11] P. Sibson *et al.*, "Chip-based quantum key distribution," *Nature Commun.*, vol. 8, no. 1, Feb. 2017, Art. no. 13984.
- [12] N. C. Harris *et al.*, "Quantum transport simulations in a programmable nanophotonic processor," *Nature Photon.*, vol. 11, no. 7, pp. 447–452, Jul. 2017.
- [13] N. C. Harris *et al.*, "Efficient, compact and low loss thermo-optic phase shifter in silicon," *Opt. Express*, vol. 22, no. 9, pp. 10 487–10 493, May 2014.
- [14] Y. Shen *et al.*, "Deep learning with coherent nanophotonic circuits," *Nature Photon.*, vol. 11, no. 7, pp. 441–446, Jul. 2017.
- [15] N. C. Harris *et al.*, "Apparatus and methods for optical neural network," U.S. Patent 10,268,232, Apr. 23 2019.
- [16] N. C. Harris *et al.*, "Linear programmable nanophotonic processors," *Optica*, vol. 5, no. 12, pp. 1623–1631, Dec. 2018.
- [17] M. Prabhu, "Towards optimal capacity-achieving transceivers with photonic integrated circuits," Master's thesis, Dept. Elect. Eng. Comput. Sci., Massachusetts Institute of Technology, Cambridge, MA, USA, 2018.
- [18] R. Maes and I. Verbauwhede, *Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions*. Berlin, Germany: Springer, 2010, pp. 3–37.
- [19] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 62–73.
- [20] T. Koshy, *Catalan Numbers With Applications*. New York, NY, USA: Oxford Univ. Press, 2008.
- [21] F. Qi and B.-N. Guo, "Integral representations of the catalan numbers and their applications," *Mathematics*, vol. 5, no. 3, pp. 1–31, 2017.
- [22] P. Flajolet and A. Odlyzko, "The average height of binary trees and other simple trees," *J. Comput. Syst. Sci.*, vol. 25, no. 2, pp. 171–213, 1982.
- [23] J. Mower, N. C. Harris, G. R. Steinbrecher, Y. Lahini, and D. Englund, "High-fidelity quantum state evolution in imperfect photonic integrated circuits," *Phys. Rev. A*, vol. 92, Sep. 2015, Art. no. 032322.

Amos Matthew Smith received the Ph.D. degree from Tulane University, New Orleans, Louisiana, USA, in 2010, where he worked on optimization of linear optics. He received a National Research Council fellowship with the Air Force Research Laboratory (AFRL) to work on cluster-state quantum computing. He completed post-doctorate research at Oak Ridge National Laboratory that focused on experimental implementations of quantum key distribution protocols. He is currently a full-time Senior Physicist at the AFRL, Information Directorate, Quantum Information Science group. His current work and research focuses on quantum frequency conversion and integrated optical devices from concept/design to fabrication and packaging.

H. Shelton Jacinto (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Boise State University, Boise, Idaho, USA, in 2020, where he worked on hardware acceleration and SoC design of secure protocols. From 2015 to 2017 he worked with Idaho National Lab and the Advanced Energy Lab researching secure communications and sensor design for nuclear reactor monitoring. From 2018 to present, he has been with the Air Force Research Laboratory, Quantum Information Science group under a fellowship researching quantum information processing systems, integrated quantum photonics, and quantum control. His research focuses on quantum network cybersecurity, quantum informatics, and secure adaptive hardware anti-tamper and encryption technologies.