# CMOS Optical PUFs Using Noise-Immune Process-Sensitive Photonic Crystals Incorporating Passive Variations for Robustness

Xuyang Lu, *Student Member, IEEE*, Lingyu Hong, *Student Member, IEEE*, and Kaushik Sengupta, *Senior Member, IEEE*

***Abstract*— This paper introduces a new design methodology for incorporating process-sensitive optical nanostructures in standard CMOS processes to create robust optical physically unclonable functions (PUFs) realized through an electrical-photonic co-design approach. The passive lithographic variations of lower level metal interconnects are exploited to realize resonant photonic crystals on an array of photodetectors to include variations that are robust to noise processes. The chip is realized in a standard 65-nm CMOS process with no additional post-processing. The addition of the structures increases the coefficient of variation by a factor of 3.5× compared to only active device variations. This creates extremely robust PUF responses with a native inter-chip Hamming distance (HD) of 49.81% and intra-chip HD of 0.251% with an inter-HD/intra-HD ratio of 198× illustrating the reliability of the design. The native intra-HD can be reduced to 0.06% with 17 mV of thresholding with only 4% of the total combinations discarded. To the best our knowledge, this is also the first demonstration of photonic crystals and an optical PUF in CMOS.**

***Index Terms*— Chip identification, CMOS, CMOS imager, optical physically unclonable functions (PUFs), photodetectors, photonic crystals, process variations, PUFs.**

## I. Introduction

THE globalization of electronic supply chain is an inevitable trend that brings prosperity to consumer electronics and forthcoming danger in information security. Estimation suggests that the worldwide Internet-of-Things (IoT) revenue will skyrocket from 1927.5 billion in 2013 to 7065.3 billion in 2020, with an average compound annual growth rate of 20% [1]. The lifespan of the one-generation smartphone is typically less than 4.6 years [2]. Consequently, including third-party intellectual property is regarded as a standard practice to speed up the design process, making the products more competitive in an ever-evolving market. However, it also leads to an unavoidable concern of IP security including cloning, recycling, and reverse engineering. It has been reported that the counterfeit is happening from bottom-level transistors to end products, such as smartphones, causing increasing economic losses [3]. Prevailing information security is mostly based upon security key stored in non-volatile memories with encrypted data and logic [4]. Non-volatile memories, however, are vulnerable to invasive attacks because of the data residual problem [5]. Therefore, the physical entities must be kept in secured places, which make those methods infeasible for IoT applications in which products are accessible to end users [6].

The physically unclonable function (PUF) is a physical entity that utilizes process variations during fabrication to create a unique physical one-way function. Unlike non-volatile memories where information is stored and encrypted digitally, the information in PUFs is extracted from intrinsic lithographic variations, making the PUFs impossible to be duplicated, even with the original manufacturing process [7]. This feature makes PUFs a potential solution for massive-scale IP protection. The encryption scheme of PUF typically works as follows: given a specific set of inputs, usually called a challenge, different PUF entities exploit the differences in fabrication variations to generate unique output responses. Each response is compared with a pre-stored response to authenticate the identity of the PUF. In addition to uniqueness, PUFs should also be lightweight, low power, and low cost to be incorporated as common components in a standardized IP design protocol. When used repeatedly, the responses of PUFs for a fixed input challenge should remain unchanged. This measure of a PUF which represents its robustness is critical for its operation. This is often an issue when PUF responses are generated by exploiting active device variations due to the presence of noise in the integrated circuitry.

Typical examples of silicon PUFs in prior works include SRAM-based PUFs, where the random start-up conditions of SRAM cells are treated as digital responses [8]. Based on the mismatches between transistors, each SRAM cell is inclined to assume one of the two values. The drawback of SRAM-based PUF is that the responses are also sensitive to the history of bit writing, and therefore, has low stability. Additional processes such as aging and burn-in are then required for stability [9]. Furthermore, it may have a non-equal

Manuscript received October 31, 2017; revised February 23, 2018 and May 14, 2018; accepted June 16, 2018. Date of publication August 9, 2018; date of current version August 27, 2018. This paper was approved by Associate Editor Piero Malcovati. This work was supported by the National Science Foundation. *(Corresponding author: Kaushik Sengupta.)*

The authors are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: xuyangl@princeton.edu; lingyu@princeton.edu; kaushiks@princeton.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSSC.2018.2850941

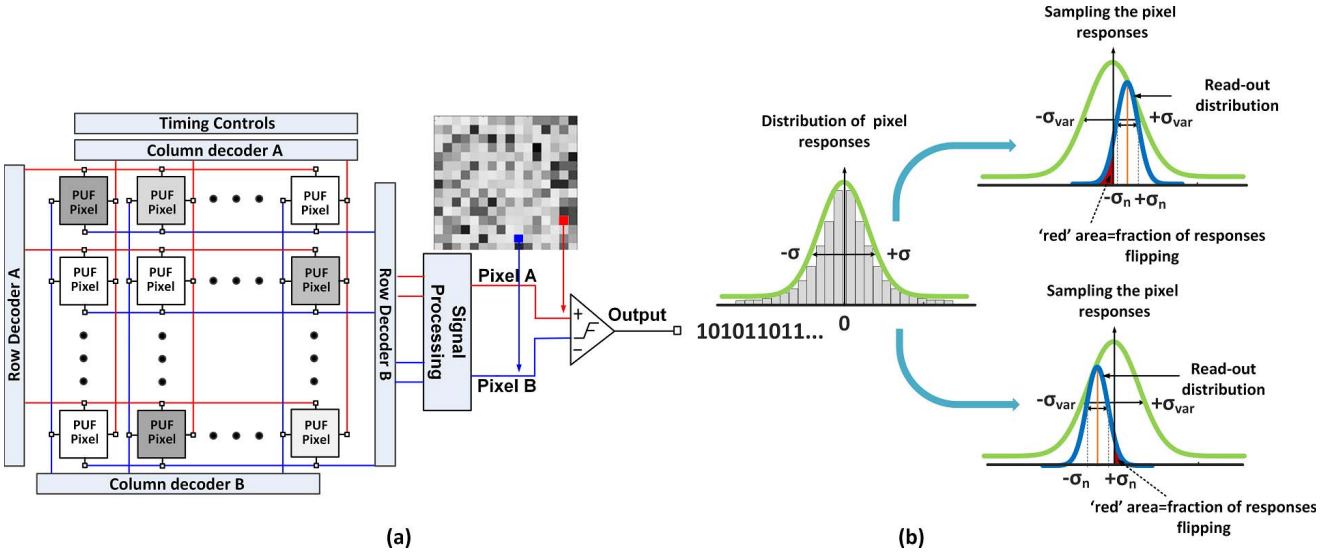


Fig. 1. (a) Architecture of a PUF that utilizes fixed-pattern noise (FPN) to create a digital response by comparing two selected pixels. (b) Given the distribution of the output responses that is sampled by a noisy readout process with a given variance, the BER of the PUF or the stability can be analytically calculated.

occurrence of zeros and ones undermining the randomness of the responses. Another category of PUFs is delay-based PUFs and examples include ring-oscillator PUFs and arbiter PUFs. The difference in the transmission time of two competing paths or the difference in oscillation frequencies of two oscillators is compared to generate a digital response. The instability of delay-based PUFs can be reduced by using a threshold on the collapsing time to reject oscillator pairs whose oscillation frequency differences are within the unstable margin. This can also be accomplished by using temporary majority voting (TMV) [10]. The difficulty of designing delay-based PUFs increases as the number of competing paths increases. This is because any asymmetry in the layout of delay paths can introduce structural bias that undermines the uniqueness of each PUF compared to others. Other PUF structures exploiting temperature-sensitive operations and subthreshold operations are also investigated in [11] and [12]. Most implementations of silicon PUFs in prior art utilize active variations during fabrication including transistor mismatches, gain, delay, and doping density variations.

In this paper, in addition to active device variations, passive lithographic variations are exploited to create responses with much reduced sensitivity to noise. As is known, the lower metal layers with the smallest feature sizes have the highest lithographic variations, but the fractional changes in these interconnect dimensions have limited effects at analog and RF frequencies. We exploit the variations of these structures in their smallest allowable lithographic dimensions (sub-200 nm) through the realization of sensitive resonant photonic crystal structures on-chip operating at optical frequencies. At these dimensions, which are comparable to the wavelengths, slight process variations can cause significant variations in light transmittance leading to extremely noise-robust PUF signatures. The magnified passive variations are combined with active device variations of photosensing pixels and digital circuits to generate stable PUF responses. While the focus of this paper is on the noise-immune properties of the passive variations and not on the security attacks, there is a past body of the work that addresses these details on strong and weak PUFs [13], [14].

The idea of using optical properties as device IDs can be traced back to the cold war time when nuclear weapons were coated with reflective powders, and the random scattering patterns are recorded as unique identifiers of the bombs [15]. The work of Pappu *et al.* [16] is the first realization of a PUF where the light transmission patterns through a scattering media under various challenges in the form of incident light patterns are recorded and processed as responses of the PUF. Compared to other forms of device IDs that rely mostly on the variation of doping and deposition, optical PUFs are not only less sensitive to noise but also utilize the complexity of light diffraction, making them both more stable and harder to be duplicated. Evidently, such complex optical structures are not compatible with solid-state integration. Recently, a CMOS imager PUF is proposed that utilizes the non-uniformity of photodiode responsivity under uniform room light excitation and dark current to generate unique responses to be used for camera authentication [17]. In this paper, the active variations of photodiode responsivity and dark current non-uniformity are combined with the passive lithographical variations of sub-wavelength metal interconnects to realize a stable PUF design. The integration of optical structures on-chip shows the first step toward more complex optical PUFs for the future. The optical PUF can be tested in the batch processing in the same way as an electrical PUF, where in addition to the electrical probe, a fixed low-cost laser interrogates the IC. The IDs can be measured during fabrication as well and can be used for later authentication to prevent chip re-use [18].

This paper is organized as follows. In Section II, quantitative estimation of the increase of PUF stability by introducing an additional source of passive variations is presented. The realization of process-sensitive photonic crystals to increase

stability and the implementation details are presented in Section III. The circuit architecture and operation principle are discussed in Section IV, followed by measurement results in Section V.

## II. PUF Stability

In general, a PUF creates a distribution of responses which is read out by a noisy readout process. Given two distributions (PUF and readout noise), the stability and bit error rate (BER) can be analytically calculated. For instance, in the case of a CMOS imager PUF with a 2-D array of photodetectors, responses can be generated by randomly selecting two pixels simultaneously, and comparing (and subsequently thresholding) the differential photocurrents of individual cells, as shown in Fig. 1(a). The signals extracted from intrinsic variations in the photodetectors to generate the responses will typically follow a normal distribution with a mean ($\mu_{\text{var}} = 0$) and a variance ($\sigma^2_{\text{var}}$), as shown by the example in Fig. 1(b). This response is read out by a noisy process with rms noise value of $\sigma_n$, as shown in Fig. 1(b). The challenge pairs that generate responses falling in the area close to the mean ($\mu_{\text{var}} = 0$) and within the noise margin are most vulnerable toward flipping, which is illustrated in Fig. 1(b).

Quantitatively, as the challenges are executed and the pixel responses are sampled with a noisy process with variance ($\sigma_n^2$), the tail end of the sampling distribution may cause bits to flip. This is shown by the red area under the curve in Fig. 1(b). The BER can be calculated by adding all these fractional areas weighted by the probability of their occurrence. Given the noise rms voltage and the distribution of the response pairs, the BER can be calculated as

$$\text{BER} = \int_{-\infty}^{\infty} \Phi_{v_n}(x) \times p(x)dx \tag{1}$$

where $p(x)$ represents the probability distribution of pixel responses and $\Phi_{v_n}(x)$ represents the probability of bit-flipping for the mean response "$x$." Denoted by the "red" area underneath the curves in Fig. 1(b), this is given as

$$\begin{aligned} \Phi_{\sigma_n}(x) &= \int_{-\infty}^{0} \frac{1}{\sqrt{2\pi}\sigma_n} e^{-\frac{(y-x)^2}{2\sigma_n^2}} dy \quad \text{for } x > 0 \\ \Phi_{\sigma_n}(x) &= \int_{0}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_n} e^{-\frac{(y-x)^2}{2\sigma_n^2}} dy \quad \text{for } x \le 0. \end{aligned} \tag{2}$$

If the authentication process is repeated multiple times, the responses generated by the pixel pairs within the noise margin will be unstable, and corresponding data processing should be implemented to ensure stability. To increase robustness and reduce BER for practical deployments of such systems, the fractional area within and close to the noise margin must be reduced substantially by stretching the distribution of output responses.

As we will see in measurements, due to circuit process variations, the differences in responses between two pixels in the implemented chip is a normal distribution with a mean of $\mu_{\text{var}} = 0$ and a variance of $\sigma_{\text{var}} = 150$ mV. During the readout process, the shot noise and the readout noise can cause the bits to flip, leading to instability. The measured output noise in the differences of two pixel outputs has an rms value of $\sigma_n = 2.96$ mV. Fig. 2 illustrates how increasing the process variations can substantially reduce BER by effectively decreasing the number of vulnerable bits within the noise margin. As we will show in measurements, the addition of these process-sensitive photonic-crystal structures can increase the variance from $\sigma_{\text{var}} = 150$ mV to $\sigma_{\text{var}} = 562$ mV. This reduces the area within the noise margin by a factor of 3.74× down to 0.42% and the resultant BER by 3.64× down to 0.17%. The measured BER of 0.25% is close to this theoretically predicted value.

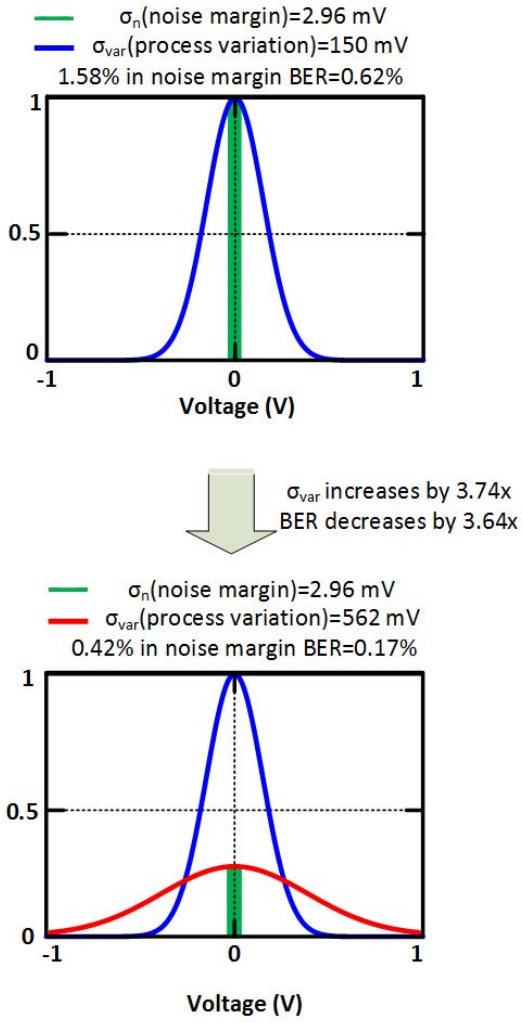


Fig. 2. Increase in stability and decrease in BER achieved by increasing the process variations through the addition of noise-immune process-sensitive resonant photonic crystal structures on the chip.

## III. Photonic Crystal as a Source of Additional Variance

Active device scaling has simultaneously enabled passive device scaling of metal interconnects with the minimum feature size down to the sub-wavelength regime at optical frequencies. While these passive lithographic variations may not show up in any considerable fashion at low frequencies, they can be amplified at optical frequencies where the feature

sizes are comparable to the wavelengths. Prior works have shown how complex nano-optical structures exploiting metal–light interaction can be integrated into a 65-nm CMOS process using the lower metal layers [19], [20], [24]–[27]. While these works aimed at creating process-invariant robust structures for sensing applications, this paper demonstrates resonant optical photonic crystal structures that are extremely sensitive to process variations, thereby enabling us to exploit them for stable PUF signatures.

### A. Photonic Crystal Operation

The photonic crystal is a periodic nano-optic structure that creates periodic interference of the electromagnetic waves to form allowed and forbidden bands. Traditionally, photonic crystals are widely used in creating highly efficient filters and for effective mode confinement in optical fibers [21]. In this paper, we place our interest at the bandedge where the light transmittance abruptly changes, and we investigate its potential of being used as a source of amplified passive variations. Based on the scale invariance nature of electromagnetic fields, we can theoretically analyze the behavior of photonic crystals using the transfer matrix method [22]. As shown in Fig. 3(a), a photonic crystal can be realized with alternate dielectric layers with different dielectric constants. If we denote $\begin{bmatrix} a_i \\ b_i \end{bmatrix}$ as the wave vector at the $i$th layer, where $a_i$ and $b_i$ represent the forward and backward propagations, respectively, [Fig. 3(a)], then the $(i-1)$th layer can be represented as

$$\begin{bmatrix} a_{i-1} \\ b_{i-1} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1+\frac{n_i}{n_{i-1}} & 1-\frac{n_i}{n_{i-1}} \\ 1-\frac{n_i}{n_{i-1}} & 1+\frac{n_i}{n_{i-1}} \end{bmatrix} \begin{bmatrix} e^{-j\frac{\omega}{c}n_i} & 0 \\ 0 & e^{j\frac{\omega}{c}n_i} \end{bmatrix} \times \begin{bmatrix} a_i \\ b_i \end{bmatrix} = T_1 \begin{bmatrix} a_i \\ b_i \end{bmatrix} \quad (3)$$

where $n_i$ is the refractive index of the $i$th layer. Therefore, the transfer matrix of photonic crystals where the unit cell consists of alternate layers of two different dielectrics has the following relationship:

$$\begin{bmatrix} a_{N-2} \\ b_{N-2} \end{bmatrix} = T_1 \times T_2 \begin{bmatrix} a_N \\ b_N \end{bmatrix} = M \begin{bmatrix} a_N \\ b_N \end{bmatrix}. \quad (4)$$

where $N$ represents the index of a unit cell with two layers, $T_1$ and $T_2$ represent the transfer matrix of each layer with different materials, respectively. If we assume the infinite number of such periodic structures, the solutions of the wave equations must satisfy Flouqet condition $E(z) = E_k(z)e^{ikz}$, where $E_k(z) = E_k(z + m(L_1 + L_2))$ is a periodic function and "$m$" is an integer [Fig. 3(a)]. In other words, the solutions must be periodic in wavevector with a constant phase shift between neighboring cells. Combining the Flouqet condition and the transfer matrix gives

$$e^{jk(L_1+L_2)} \begin{bmatrix} a_N \\ b_N \end{bmatrix} = M \begin{bmatrix} a_N \\ b_N \end{bmatrix} \quad (5)$$

where the solution can be obtained by solving the eigenvalue of the matrix [23]. With a finite number of layers, the transmission bandedge gradually forms. In Fig. 3(b), using the transfer matrix method, the complete dispersion characteristics of a photonic crystal including the location of the bandgap can be analyzed. The key idea behind using photonic crystals as a source of process variation is shown in Fig. 3(c) suggesting that the bandedge is very sensitive to the dielectric constants of either of the alternating layers. Therefore, when excited at the bandedge, slight perturbations in the effective dielectric constant of a medium due to fabrication variations can cause dramatic differences in transmission properties.

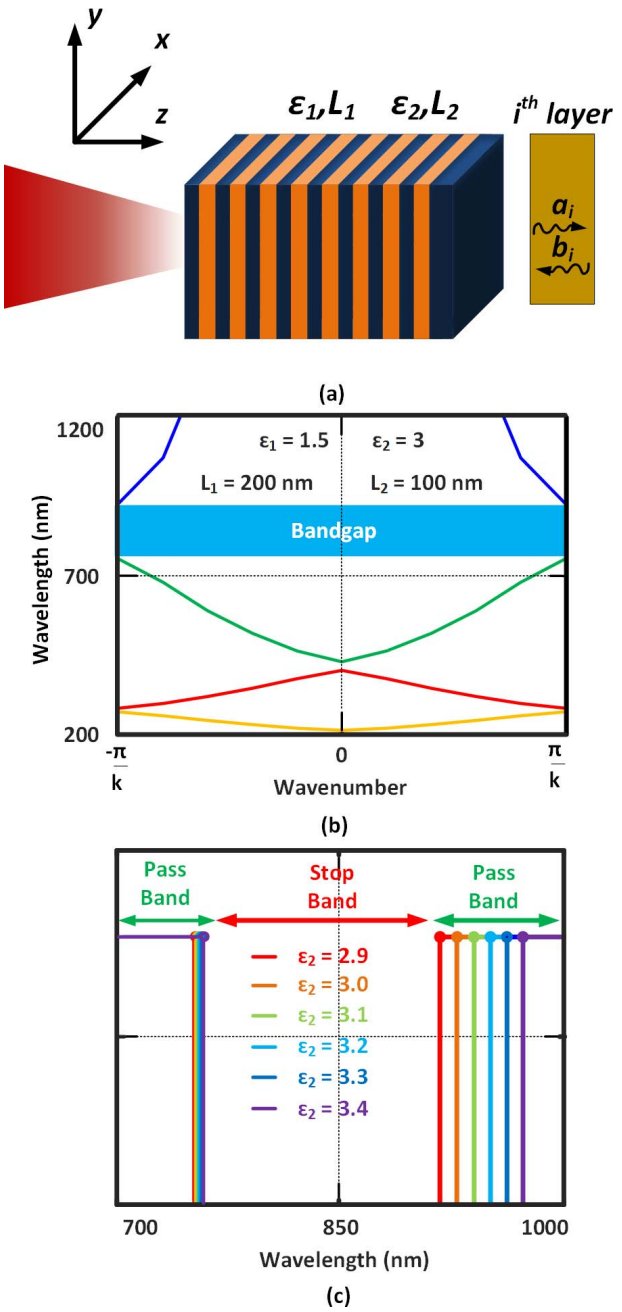


Fig. 3. (a) Example of 1-D photonic crystal formed by alternate dielectric layers. (b) Band diagram showing that there exists an optical bandgap which is a function of the properties of the periodic dielectrics and their geometry. (c) Transfer matrix model illustrates that the bandedge is very sensitive to the dielectric constants of the constituent layers.

### B. Nano-Metallic Photonic Crystals On-Chip and Optimization for Robust PUF Responses

In a CMOS process, we realize the optical PUF with the embedded lower metal layers with sub-wavelength dimension

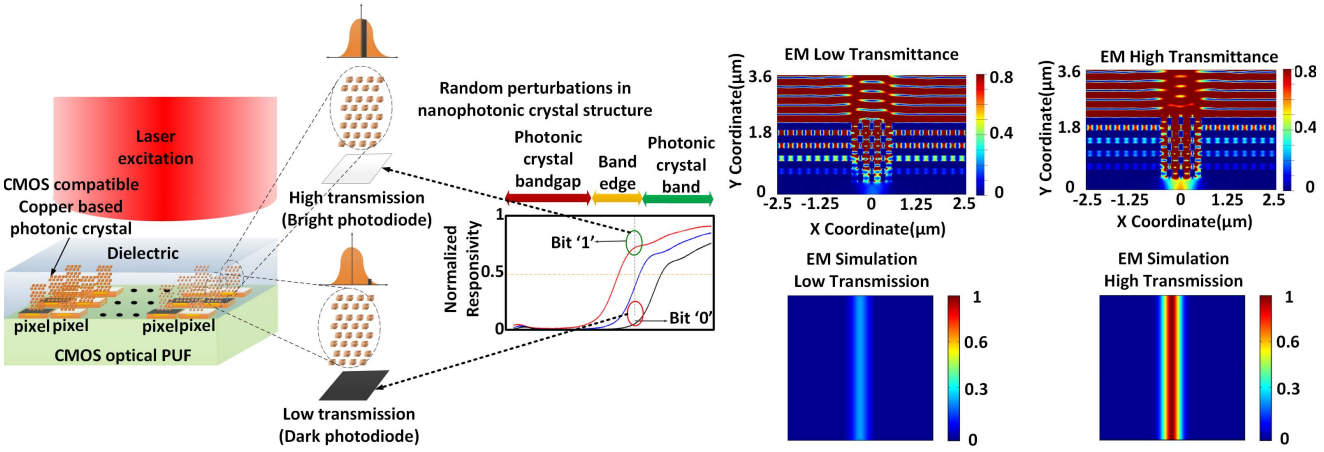


Fig. 4. Variations in light transmittance of individual pixels due to passive variations of the photonic crystals and active variations of photosensing circuitry are exploited to create PUF responses. Simulated optical transmission at 850 nm with two instances of a photonic crystal with 10-nm spacing difference illustrating large differences in optical transmission.

acting as one of the "dielectric" layers. The optical PUF consists of a 2-D array of photodetectors with individual photonic crystals placed on them. Independent small variations introduced in the geometry of the crystal create large changes of the transmittance when excited by a low-cost laser diode at the band-edge wavelength. This is illustrated in Fig. 4. Fig. 4 also displays the simulated optical field distribution in two such structures with 180 and 190 nm widths when excited at a fixed wavelength showing stark differences in transmission properties. The simulation was carried out in a finite-difference time-domain electromagnetic simulation software. Since the active variations of photodiode responsivity of each pixel and the passive variations of photonic crystals are created by different masks in fabrication, they are independent of each other. We denote the transmission of the photonic crystal as $T_{\text{ph}}$, and the responsivity of the diode and the detection circuitry collectively as $V_{\text{res}}$. Both $T_{\text{ph}}$ and $V_{\text{res}}$ are independent random variables and are subject to process variations. Therefore, neglecting the presence of offset, the responses sensed by the photodetectors ($V_{\text{op}}$) under the excitation is given as

$$V_{\text{op}} = T_{\text{ph}} V_{\text{res}}. \tag{6}$$

Let us assume that the means and variances of the passive photonic crystals ($T_{\text{ph}}$) and active device variations ($V_{\text{res}}$) are given by ($\mu_{\text{ph}}$, $\sigma^2_{\text{ph}}$) and ($\mu_{\text{res}}, \sigma^2_{\text{res}}$), respectively. Therefore, due to their independence, we have

$$\mu_{\text{op}} = \mu_{\text{ph}} \mu_{\text{res}}. \tag{7}$$

The total variance of the output is defined as

$$\begin{aligned}\sigma^2(V_{\text{op}}) &= E\left(T^2_{\text{ph}} V^2_{\text{res}}\right) - [E(T_{\text{ph}} V_{\text{res}})]^2 \\ &= \sigma^2_{\text{ph}} \times \sigma^2_{\text{res}} + \sigma^2_{\text{ph}} \times \mu^2_{\text{res}} + \mu^2_{\text{ph}} \times \sigma^2_{\text{res}}.\end{aligned}$$

Combining (6) and (7), we have

$$\frac{\sigma^2(V_{\text{op}})}{\mu^2(V_{\text{op}})} = \frac{\sigma^2_{\text{res}}}{\mu^2_{\text{res}}} + \frac{\sigma^2_{\text{ph}}}{\mu^2_{\text{ph}}} + \frac{\sigma^2_{\text{res}}}{\mu^2_{\text{res}}} \frac{\sigma^2_{\text{ph}}}{\mu^2_{\text{ph}}}. \tag{8}$$

The expression quantitatively predicts the contributions of the active and passive device variations in the optical PUF topology. The structural aspects of the photonic crystal in terms of metal width, pitch, and the number of layers in each element need to be optimized to maximize the variance of pixel responsivity $\sigma^2(V_{\text{op}})$ under the constraints of the design rules of the CMOS process. Moreover, moderately large responsivity $\mu(V_{\text{op}})$ needs to be maintained to obtain stable signal readout.

The photonic crystal structure is realized using the metal interconnects in the lower layers in a 65-nm bulk CMOS LP process. The foundry describes the nominal variation of the metal interconnects in the layers ($M_4$–$M_6$) to have a width variation of 10% for the minimum width and a thickness variation of 15%. The implemented structure of the photonic crystal is illustrated in Fig. 5(a). The unit cell consists of three metal interconnects embedded in the oxide layer forming the photonic crystal on top of a photodiode. In addition, a metal shielding is placed on the top of a reference diode for differential signal processing and for preserving the boundary condition of photonic crystals to the largest extent possible.

The number of vertical and horizontal layers and their dimensions need to be optimized to create the bandgap conditions and to ensure the sharpest bandedge for maximal variance at a wavelength where a low-cost laser is easily available. In addition, the design needs to comply with the design rule check of the CMOS fabrication. The variations of the transmittance property of the structure with the number of vertical layers are shown in Fig. 5(b). In the lossless case, a higher number of vertical layers result in sharper characteristics. However, the optical losses in the metal nanophotonic structure can significantly reduce the transmission in the passband. Three or four layers are preferred for optimal light transmittance and edge sharpness for the highest variability. Fig. 5(c) shows the red shift of the band-edge wavelength with increasing width of the individual elements from 160 to 240 nm, keeping a constant pitch of 400 nm. In this paper, we choose a metal width of 180 nm and a spacing of 220 nm

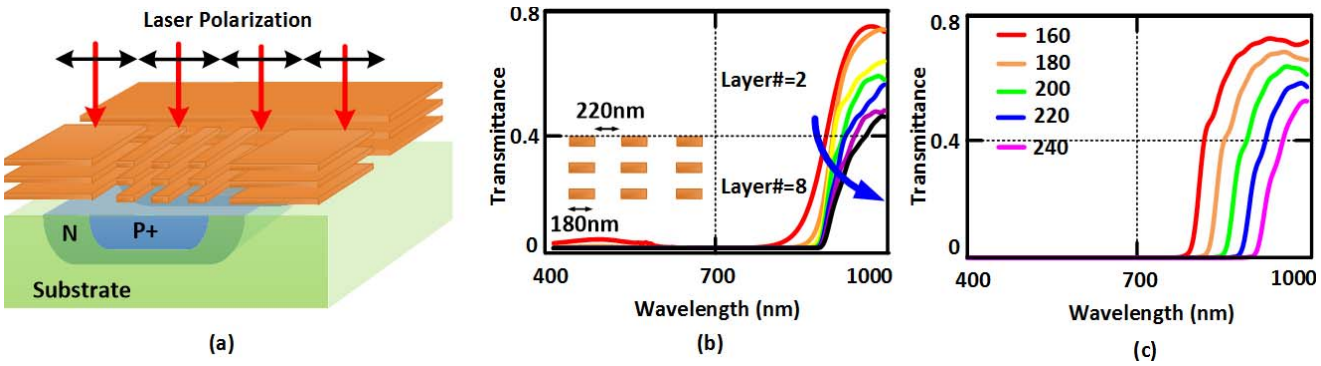


Fig. 5. (a) Structure of the PUF pixel with photonic crystals on top consisting of alternate layers of metal interconnects and the oxide layer. (b) Optimization of the number of layers of the photonic crystal design for maximal band-edge sharpness and high responsivity in the passband. (c) Optimization of the metal width with 400-nm pitch spacing to achieve best edge-sharpness, light transmittance, and band of operation combination.

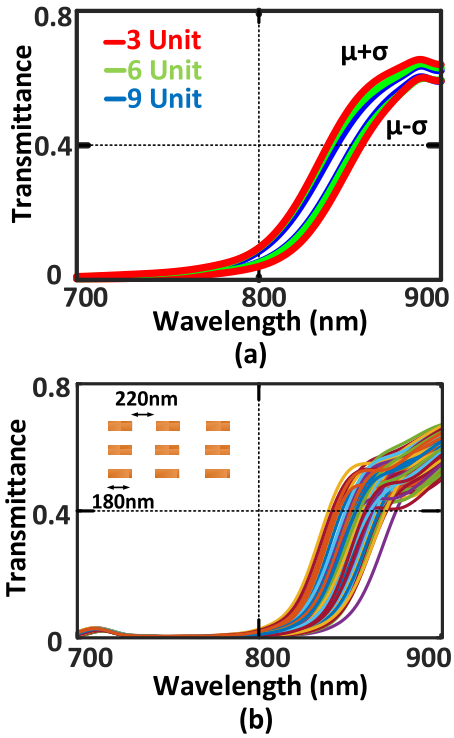


Fig. 6. (a) Plots of optical transmittance due to passive lithographic variations ($\mu \pm \sigma$) of unit photonic crystal cells with 3, 6, and 9 metal strips within each unit cell. (b) Monte Carlo simulation showing the transmission variation with variation in the width ($\sigma/\mu = 10\%$) of each unit element in the $3 \times 3$ stack cell (shown inset).

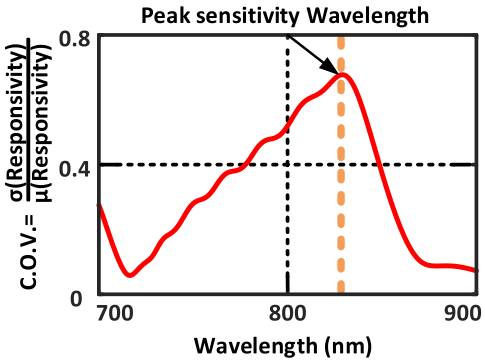


Fig. 7. Coefficient of variation ($\sigma/\mu$) of the optical transmission against wavelength showing maximum sensitivity to process variation close to the bandedge of the photonic crystal at 850 nm.

for a band-edge location near 850 nm to exploit the relative large responsivity of the photodiodes in the infrared region and the easy availability of a low-cost laser diode. It can be noted that while Fig. 3 captures the transmission and bandgap variations due to the variations in the dielectric constants of the periodic structure, the effects due to the metal width and spacing variations cannot be simply attributed to an effective dielectric change. This is essential because the individual metal structure dimensions are comparable to the wavelength, and the collective behavior cannot be represented as an averaged dielectric constant.

Another design choice is the number of horizontal elements in the crystal structure. In Fig. 6(a), Monte Carlo simulations of $3 \times 3$ (three horizontal metal bar in each of the three vertical layers), $6 \times 3$ and $9 \times 3$ metal strip stacks in each unit cell are carried out where the width of the individual metal bar varies independently with $\sigma/\mu = 10\%$. Fig. 6(a) reveals that the largest variation is observed for the three-element structure. As expected, in the collective response with a large number of independent random variations of unit elements, the transmission variations decrease with an increasing number of horizontal units due to the averaging effect. Fig. 6(b) shows the Monte Carlo simulations of the transmission properties of final photonic crystal structure ($3 \times 3$) element with independent element width variations showing the possibility of exploiting large variations at the bandedge. Fig. 7 shows the coefficient of variation (C.O.V. $= \sigma/\mu$) against wavelength illustrating that the peak sensitivity wavelength is indeed at the band-edge location near 850 nm. If a set of addresses of the pixels is used as a challenge, the differences of photoresponsivity can be compared and thresholded to generate a PUF response. This can also be extended over 2-D arrays to generate unique identifiers for each chip, shown in Fig. 8(a) with the measured data from the implemented chips. By comparing neighborhood pixels pairs (1 and 2, 3 and 4 …), a 128-bit response can be extracted from each chip. The 1792-bit result from 14 chips is concatenated to generate the autocorrelation in Fig. 8(b), showing close to zero dependence of layout geometry.

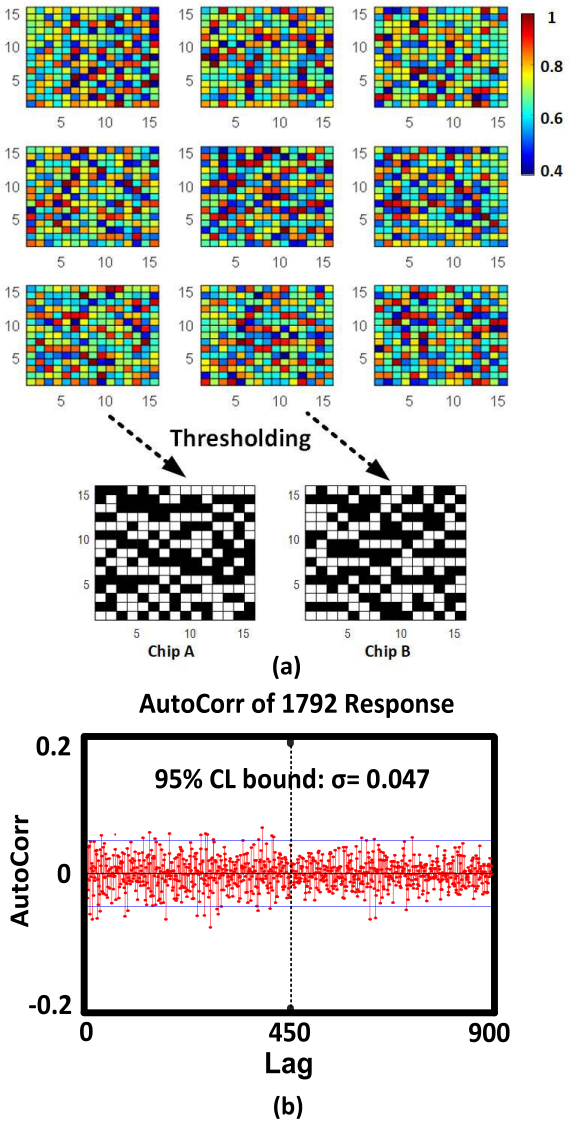


Fig. 8. (a) Measured PUF responsivity array can be used as a chip identifier when compared with the certain threshold. (b) 1-D autocorrelation of neighboring pixel pairs across 14 chips.

## IV. PUF Architecture and Constituent Circuits

The PUF architecture, the corresponding readout circuitry, and the layout of a single pixel are shown in Fig. 9. A customized 16 × 16 pixel array is designed which can be easily placed around the IP it protects. The architecture can be easily scaled to larger arrays depending on the particular application. The challenge-response pairs ($C_i$. $R_i$) can be generated in many ways. In this paper, as an example, the challenge consists of a series of pair-wise addresses of two pixels whose outputs are compared and thresholded to generate the response sequence. To accentuate the PUF responses through the optical structure variations and suppress some other sources of device variations, such as dark current differences, each PUF pixel consists of a photodiode with a photonic crystal whose output is compared against a reference shielded photodiode. The signal is then processed through a differential capacitive transimpedance amplifier (CTIA). In addition, correlated double sampling (CDS) is implemented to remove the excess variations due to offsets to capture primarily the variations enabled with the integrated optical structures. It can be noted that in a PUF implementation, the offsets between the pixels are expected to enhance the PUF stability further. The outputs of two CDS circuits corresponding to the two selected PUF pixels are converted into single-ended voltages and then compared in a clocked comparator to generate a one-bit response.

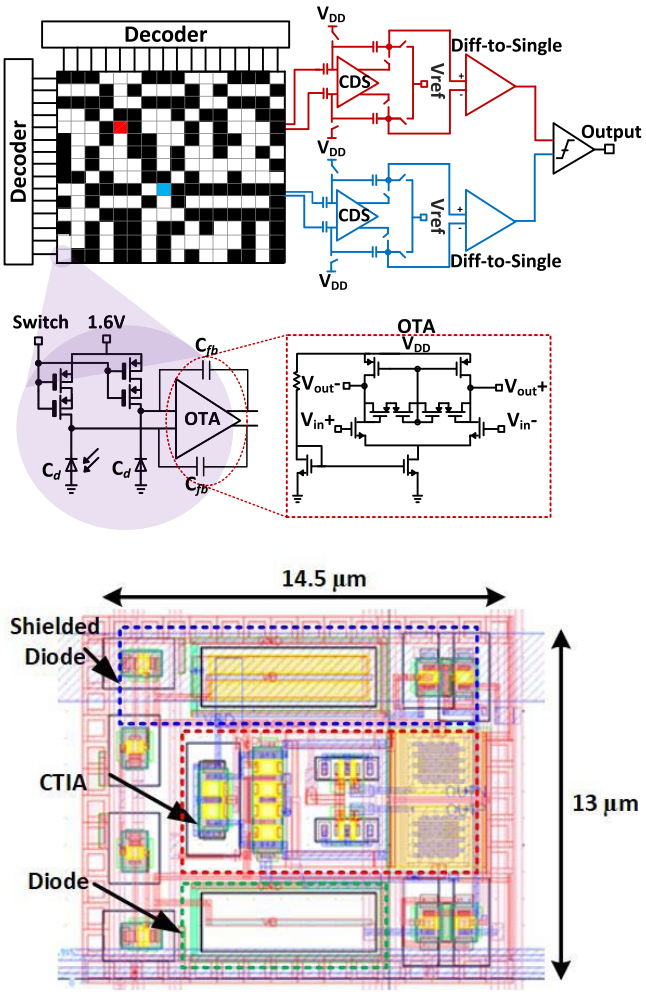


Fig. 9. Circuit architecture, readout circuitry, and the layout of a single pixel. The photonic crystal is not shown for readability.

### A. Pixel Design

The array of 256 photodetectors is realized with n-well/p-sub junctions that have been found to have the largest responsivity in the implemented CMOS process [19], [24]–[27]. Each PUF pixel occupies 14.5 $\mu$m × 13 $\mu$m as shown in Fig. 9, while each detector photodiode and the reference photodiode measures 2.2 $\mu$m × 6.5 $\mu$m. The photodiodes are controlled by double PMOS switches to reduce the leakage current by increasing the effective resistance. The dominant leakage is the p-n junction leakage due to the potential differences between the substrate and the drain

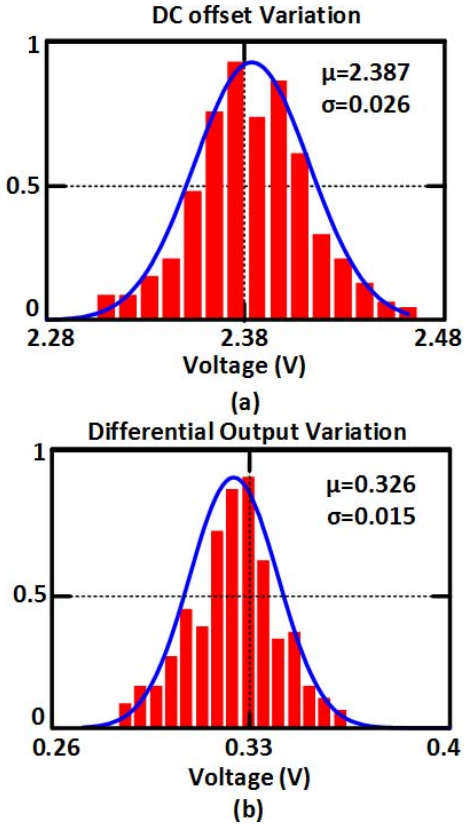


Fig. 10. Monte Carlo simulations showing active device variations including (a) DC offset variation and (b) differential output variation of the pixels' outputs. The simulations do not consider variations of the photodiode responsivity and the photonic crystals.

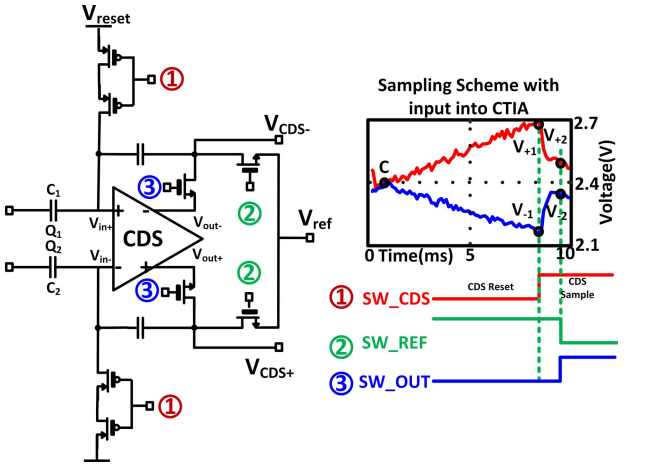


Fig. 11. CDS stage to suppress offset with sampling and timing diagram. The offset suppression is not necessary for the PUF responses and can be removed for more variations and higher stability with lower power, but is added to demonstrate the effect of the photonic crystals in increasing the variance.

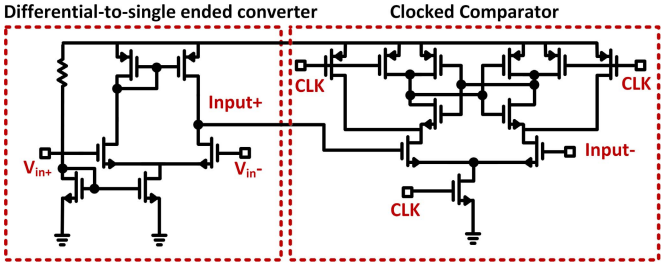


Fig. 12. Differential-to-single-ended converter and clocked comparator schematics.

nodes of the PMOS transistors. The two switches reduce the voltage across each such junction, thereby decreasing the leakage. Since the photodiodes are realized in a non-imager process with no photodiode model, the impact of the diode capacitances on the output signal is eliminated by integrating the photocurrent through a CTIA. This results in the output voltage of the CTIA to be $V_{\text{CTIA\_Output}}(t) = \int(i_{\text{photon}}(t)dt/C_{\text{fb}}(1+(1/A)) + (C_d/A)) \approx \int(i_{\text{photon}}(t)dt/C_{\text{fb}})$, where $C_{\text{fb}}$ is the feedback capacitance $\approx$ 4 fF, $C_d$ is the photodiode capacitance $\approx$ 8 fF, and $A$ is the gain of the operational amplifier ($\approx$37 dB). The high gain of the amplifier is obtained with PMOS-based pseudo-resistors biased in the cutoff region. The schematic of the operational transconductance amplifier (OTA) is also shown in Fig. 9. PMOS switch pairs are controlled by two sets of 4-bit decoder pairs to select the desired pixels pairs. The simulated Monte Carlo variations of the readout circuitry alone (without the photodiode and photonic crystal variations) are shown in Fig. 10. In real applications, the reference diodes and the CDS can be removed to save power, area, and increase PUF stability. In addition, the differential CTIA can be replaced by a simpler compact structure such as a 3-T pixel cell to include the variance contributed by the non-uniformity of dark current.

### *B. Correlated Double Sampling and Comparator*

As illustrated in Fig. 11, selected pixel outputs are further processed by CDS to suppress offsets and low frequency correlated noise. The output voltage of CDS can be expressed as $(V_{\text{out+}} - V_{\text{out-}}) = (|V_{+1} - V_{+2}| + |V_{-1} - V_{-2}|/1 + (2/A))$, where $(V_{+1}, V_{-1})$ and $(V_{+2}, V_{-2})$ represent the sampling of the differential outputs for CDS, and $A$ represents the gain of the OTA. The sampling timing diagram is illustrated in Fig. 11. As can be seen, the sample points are chosen at the end of integration and the beginning of next reset cycle to mitigate the effect of correlated noise and long-term drift. Similar to the discussion of CTIA, the CDS unit is implemented to validate the concept of passive variation and can be removed to further increase variance contributed by the offset of pixels in the real application. The differential outputs of two pixels are converted to a single-ended output and a buffer stage to shift the dc level. The signals are then compared in a dynamic latch comparator to generate a digital output, as shown in Fig. 12. The comparator draws 8.6-$\mu$A dc current.

## V. Measurement Setup, Results, and Discussion

The chip is fabricated in the 65-nm bulk LP CMOS process and the active area of the PUF occupies 217 $\mu$m $\times$ 254 $\mu$m, as shown in Fig. 13. The unmarked active area does not contain circuits belonging to the presented PUF IC.

### *A. Measurement Setup*

The measurement setup for responsivity calibration of the integrated PUF pixels is shown in Fig. 14(a). A Ø5.6 mm

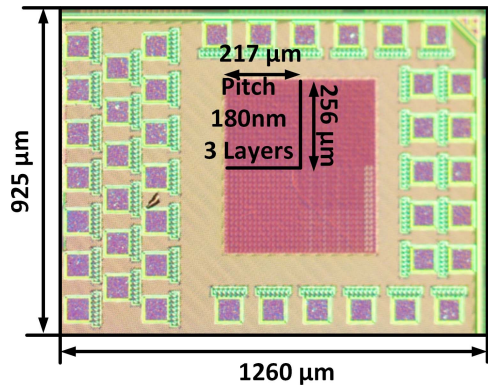


Fig. 13. Die photograph showing an active area of 217 $\mu$m $\times$ 256 $\mu$m. The unmarked regions are not part of the presented PUF IC in the work.

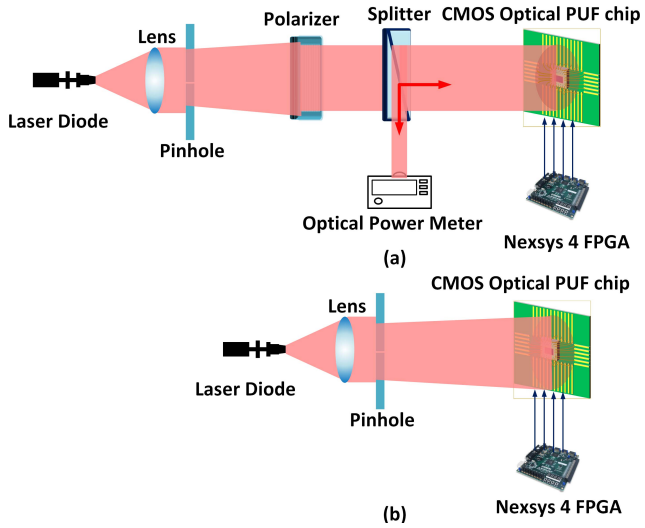


Fig. 14. (a) Measurement setup for responsivity calibration. (b) Measurement setup for generating PUF responses.

TO Cans ($\sim$20) packaged laser diode with a collimated lens shines through a polarizer, a pinhole, and a beam splitter. Half of the power goes into a commercial power meter to characterize the incident power, while the other half of the power shines uniformly on the chip active area under test to extract the transmission profiles of the photonic crystals and the photodiodes. For generating the PUF signature, only the laser is required since the photonic crystals perform like a linear polarizer that reject light from other incoming polarization, as shown in Fig. 14(b). To characterize the chip performance with temperature, a ceramic heater is placed on the backside of the PCB board with a temperature probe attached to the chip surface to monitor the chip's operating temperature.

### *B. Photoresponsivity Characterization and Contribution of the Photonic Crystals*

First, the wavelength for the maximum sensitivity which is expected to be located at the bandedge of the photonic crystals is measured. This is done by measuring the photoresponsivities of all the pixels from 405 to 980 nm to characterize the

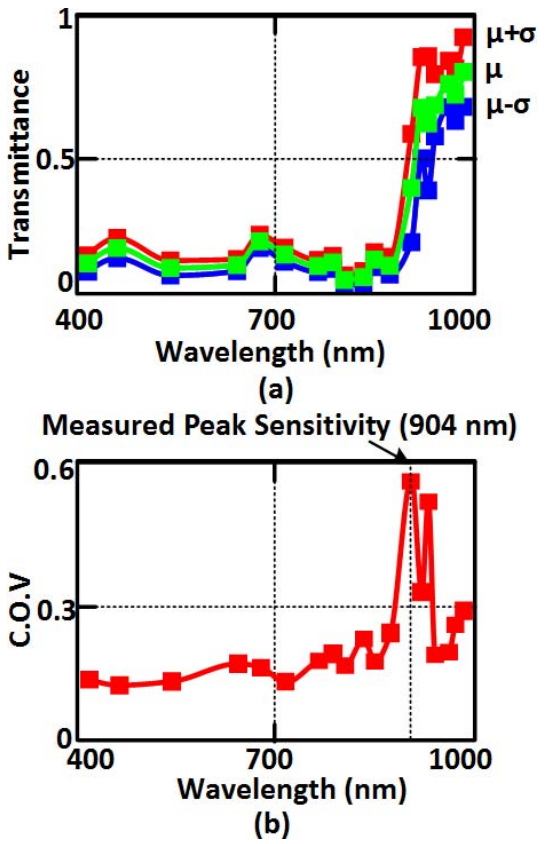


Fig. 15. (a) Measured variation of light transmission against wavelength showing the mean ($\mu$) profile and the $\mu \pm \sigma$ profiles. This figure suggests a bandedge near 904 nm for maximum sensitivity. (b) Measurement C.O.V showing peak sensitivity at 904-nm wavelength.

light transmission profiles. Fig. 15(a) illustrates the normalized mean responsivity ($\mu$) along with the $\mu \pm \sigma$ variations. As can be seen from Fig. 15(a), the bandedge for maximal variance is located near 904 nm. This is also seen in the C.O.V plot in Fig. 15(b) showing a peak value of 53% at the bandedge confirming the highest variability. The slight deviation from the simulated value of 850 nm in Fig. 7 is expected due to the slight differences of the dielectric permittivity of the oxide layers inside the chip which are typically not characterized at optical frequencies.

Revisiting expression (8) which captures the total variation as a function of the passive and active device variations, we can distinguish each variation's contribution by analyzing the C.O.V at different portions of the spectrum. As can be seen in Fig. 15(b), compared to the transmission band where the photonic crystals have relatively flat responses, the bandedge has 3.5$\times$ higher C.O.V. This justifies the addition of the photonic crystals whose extreme sensitivity to process variations increases the C.O.V from 15% to 53% at the bandedge. This is also illustrated in the pixel responsivities when excited at the incident wavelength at 904 nm. The differential photocurrent is plotted in Fig. 16(a) showing an average photocurrent of 338.4 fA and a standard deviation of 179.27 fA ($\sigma/\mu = 53\%$) with an excitation of 15 nW of optical power on the chip. Although the dark current distribution may suggest a larger C.O.V, the dark current variance is essentially arising

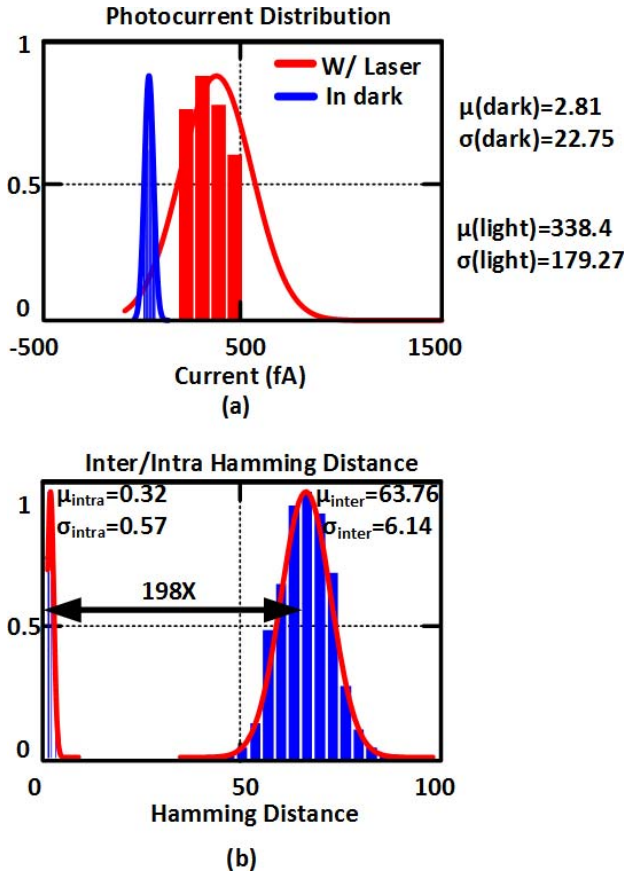


Fig. 16. (a) Photocurrent distribution with and without excitation lasers showing the increased variation because of the photonic crystals on-chip. (b) Measured native intra-chip and inter-chip HD showing a native inter/intra HD ratio of 198×, implying highly stable responses.

out of the noise in the read-out circuitry. The differential dark current has an average value of 2.81 fA with a standard deviation of 22.75 fA.

### C. Robustness and Uniqueness

Two important figures of merit of a PUF, uniqueness and robustness are characterized by measuring the inter-chip and intra-chip HD. The inter-chip Hamming distance is measured across 14 chips using 200 sets of challenges generated through an off-chip pseudo-random number generator using linear feedback shift registers (LFSR), each with a length of 128 bits (i.e., the total of 512 000 bits). During all PUF characterization, the same laser at 904 nm is used. The intra-chip HD is obtained by repeatedly applying the 200 set of challenges to each of the 14 chips for 800 measurements. The majority responses are regarded as the golden keys, and the BER is measured by calculating the HD of each measurement from the corresponding golden key. The measured native stability without any stabilizing process such as majority voting, thresholding, burn-in, error-correcting code (ECC), or masking is 99.75%. This corresponds to a mean intra-PUF HD of 0.32, while the mean inter-PUF HD for 14 chips is 63.76 with a standard deviation of 6.14. The inter/intra-chip HD are plotted in Fig. 16(b). The identifiability defined by the inter/intra PUF HD ratio is, therefore, measured to be 198× which indicates the high stability of the PUF responses. Fig. 17 shows the measured 2-D auto-correlation of the pixel responsivities averaged over 14 chips, which is calculated by shifting the pixel array by one pixel at a time. The measured results show almost no spatial bias and near-impulse response for complete alignment for the 16 × 16 pixel array. There is a slight correlation between the two vertical pixels because of the routing of the signal in the chip.

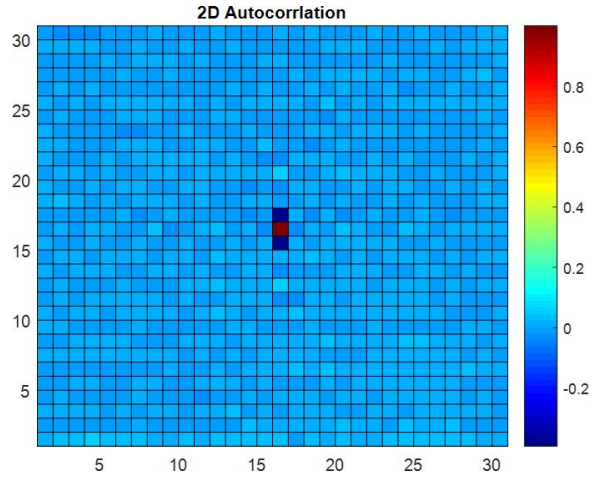


Fig. 17. Measured 2-D auto-correlation of the pixel responsivities averaged over 14 chips showing no spatial bias and near-impulse response for the 16 × 16 array.

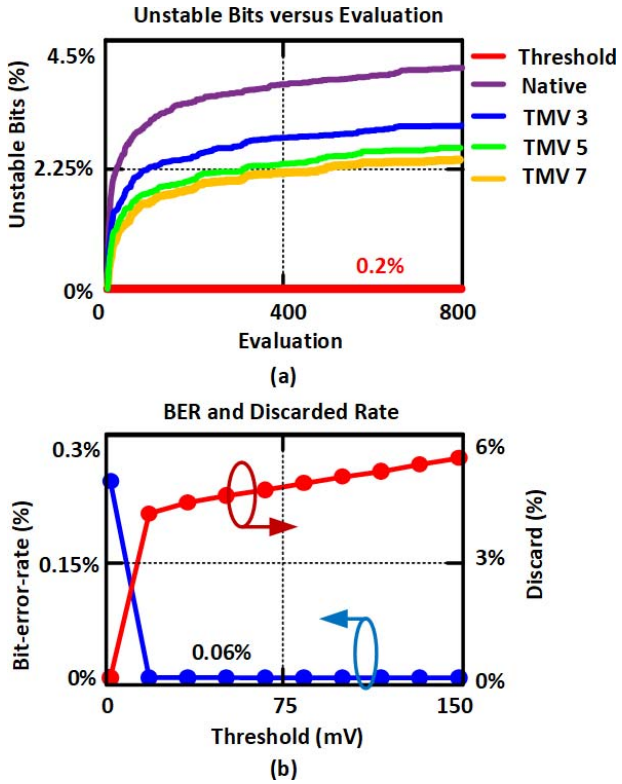


Fig. 18. (a) Percentage of unstable bits (at least one flip) against the number of evaluations shows excellent stability and robustness of responses. (b) Percentage of unstable bits can be mitigated using thresholding and/or temporal majority voting. With a 17-mV threshold, the BER can be reduced to 0.06%. (b) BER and discarded rate versus threshold.

To further characterize stability, the number of unstable bits versus the number of evaluations is plotted in Fig. 18(a). As can be seen, without any processing, less than 4% of the bits flip at least once after 800 evaluations showing the high stability of the responses. To further improve stability, error correcting including TMV with voting window 3, 5, 7, and thresholding can be applied. In Fig. 18(b), the BER defined as

$$\mathrm{BER} = \frac{1}{k}\sum_{j=1}^{k}\frac{\mathrm{HD}(R_i, R_{i,j})}{n} \times 100\% \tag{9}$$

where $R_i$ represents the golden key generated as the average of all responses under a fixed challenge and $R_{i,j}$ as the $j$th evaluation, $n$ is the number of bits, and $k$ is the number of evaluations. The BER is plotted against the threshold voltage along with the number of discarded combinations in Fig. 18(b). The measured native BER is 0.25% and can be reduced to 0.06% with 17 mV of thresholding with only 4% of the total combinations discarded.

The residual instability is caused due to the flipping of response pairs whose response is within the noise margin as described in Section III. The noise of the PUF circuit is contributed by various sources and is mainly contributed by photon shot noise and the read-out circuit noise, which includes the OTA and the reset noise. The fluctuation of the laser source is suppressed by a differential sampling of two pixels. The total output noise at each CTIA output can be summarized as

$$\sigma_n = \sqrt{(\upsilon_{\mathrm{cir}})^2 + \frac{(2qI_{\mathrm{dark}})T}{C_{fb}^2} + \frac{q(I_{\mathrm{ph}})T}{C_{fb}^2}} \tag{10}$$

where the circuit rms noise is denoted by $\upsilon_{\mathrm{cir}}$, $I_{\mathrm{ph}}$ is the average photocurrent, and $I_{\mathrm{dark}}$ is the average dark current of each photodiode. The measured rms noise at the difference of two output pixels is 2.96 mV when excited at 904 nm. The uniqueness of the PUF is given as

$$\mathrm{U} = \frac{2}{m(m-1)}\sum_{u=1}^{m-1}\sum_{\upsilon=u+1}^{m}\frac{\mathrm{HD}(R_u, R_\upsilon)}{n} \times 100\% \tag{11}$$

where $R_u$ is the response of the $u$th chip and $R_\upsilon$ is the response of the $\upsilon$th chip under the same input challenge. We characterize the uniqueness by applying 200 sets of challenges across 14 chips. The measured uniqueness is 49.81%. The autocorrelation of a 50 K response shows a 95% confidence bound of 0.0089.

The chip performance under supply voltage variation is measured against the golden key generated at nominal condition (3.3 V and 25 °C) and is plotted in Fig. 19(a) shows a worst BER less than 4%. Performance under temperature variation is characterized in Fig. 19(b). Stability across the temperature and voltage variations can be significantly enhanced by increasing the laser power incident on the chip. The randomness of the PUF is characterized by the NIST test [25], where higher $P$ values represent higher confidence of randomness. The NIST test result is shown in Table I. 896 000-bit responses are extracted from 14 chips and then divided into 70 blocks of 12 800 bits each. The intrinsic

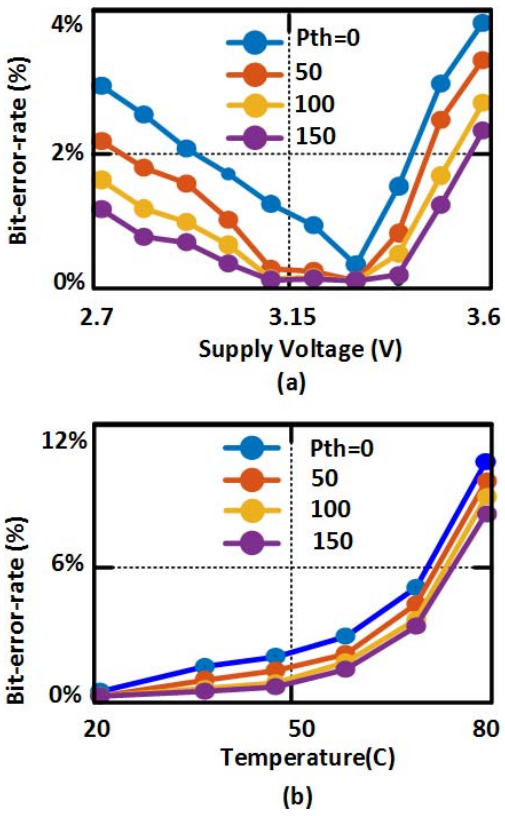


Fig. 19. (a) BER versus supply voltage. (b) Measured BER against temperature. BER can be reduced with a higher optical power.

TABLE I
NIST TEST RESULTS

| C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | Pvalue | PROP | STATISTICAL Test |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 8 | 4 | 8 | 9 | 8 | 4 | 9 | 8 | 4 | 0.7681 | 70/70 | Frequency |
| 8 | 8 | 4 | 8 | 9 | 8 | 4 | 9 | 8 | 4 | 0.7681 | 70/70 | Block Frequency |
| 11 | 4 | 9 | 3 | 8 | 6 | 5 | 6 | 7 | 11 | 0.3741 | 70/70 | CumulativeSums |
| 6 | 9 | 8 | 5 | 5 | 7 | 7 | 8 | 11 | 4 | 0.7681 | 69/70 | CumulativeSums |
| 7 | 5 | 7 | 12 | 10 | 4 | 8 | 5 | 6 | 6 | 0.5631 | 68/70 | Runs |
| 5 | 10 | 2 | 10 | 9 | 9 | 2 | 8 | 7 | 8 | 0.2299 | 70/70 | Longest Run |
| 7 | 8 | 3 | 8 | 6 | 7 | 8 | 11 | 5 | 7 | 0.7681 | 70/70 | FFT |
| 7.4 | 5.3 | 5.0 | 5.7 | 7.2 | 7.7 | 7.9 | 7.8 | 9.5 | 6.5 | 0.3801 | 68/70 | Non-Overlapping (M=4) |
| 7 | 7 | 10 | 10 | 6 | 6 | 7 | 6 | 5 | 6 | 0.9291 | 69/70 | Entropy (M=3) |
| 7 | 9 | 8 | 7 | 6 | 6 | 8 | 9 | 8 | 2 | 0.7954 | 68/70 | Serial (M=3) |
| 8 | 7 | 10 | 9 | 9 | 5 | 3 | 7 | 5 | 7 | 0.7399 | 69/70 | Serial (M=3) |
| 11 | 8 | 3 | 4 | 3 | 12 | 2 | 8 | 4 | 15 | 0.0020 | 66/70 | Linear |

maximum entropy of this PUF can be estimated based upon the total number of independent combinations as entropy $= \log_2(N!)$. The energy per bit of the design is determined by the integration time which depends on the incident power intensity. For an input light intensity of 1 $\mu$W/pixel, the energy efficiency is measured to be 12 pJ/bit excluding laser power. This can be reduced to 170 fJ/bit if a single CTIA is shared across the pixels. This energy efficiency can be significantly enhanced with a custom imager process with much higher quantum efficiency.

Table II illustrates the performance of the chip with the state of the art. The chip achieves excellent stability with one of the lowest intra-PUF HD/BER of 0.25% which results in a large inter/intra PUF HD ratio (198×) contributed by the excess variations introduced by the sub-wavelength photonic crystals. The work also achieves the lowest native auto-correlation with a 95% confidence bound showing that the read-out circuit has an extremely low bias. This additional robustness in the PUF

TABLE II
COMPARISON WITH OTHER STATE-OF-THE-ART WORK

| | [10] | [11] | [12] | [17] | [29] | [30] | [31] | This Work |
|---|---|---|---|---|---|---|---|---|
| Technology (nm) | 40 | 180 | 65 | 180 | 22 | 45 | 65 | 65 |
| Mechanism | Ring Oscillator | NAND | PTAT | FPN in CMOS Imager | Inverter Bi-stability | NAND | Current mirror | Optical (Photonic Crystal) |
| Mean Bias (%) | NA | NA | 49.3 | 50.09*1 | 48.05 | 53 | 50.16 | 49.8 |
| Uniqueness(%) | 50.07 | 49.9 | 50.01 | 49.37 | 51 | 49.8 | 50.14 | 49.81 |
| Intra-PUF (%) | 1.01 | 0.0007 | 0.57 | 2.34 | 2.684 | 0.1 | 0.3364 | 0.251 |
| Inter/Intra Ratio | 49.57 | 700 | 88 | 21.1 | 19 | 498 | 149.05 | 198 |
| Native Single Flip (%) | 12.5 | 1.67 | 6.54 | NA | 30 | NA | 2.34 | 4.27 |
| Evaluations | 1000 | 2000 | 500 | NA | 5000 | NA | 400 | 800 |
| Energy/Bit (pJ/bit) | 17.75 | 0.011*2 | 0.548 | 8900 | 0.19 | NA | 0.015 | 12*3 |
| Stabilizing Methods | Thresholding | Masking | TMV, thresholding | Thresholding | Voting, Burn-in, Mask, ECC | Masking, TMV, ECC | Masking | Thresholding |
| # chips measured | 20 | 14 | 20 | 5 | 6 | 100 | 10 | 14 |
| Temperature | -25~125 | -40~120 | 0-80 | 15~115 | 25 | -25~85 | 25~85 | 25~80 |

Table II. Comparison Table with other state-of-the-art work.
*1 Monte Carlo Simulation. *2Under 1.2V supply. *3 Assuming 1μW/per pixel of optical power, excluding laser power consumption. Can be scaled to 170fJ by sharing CTIA among pixels.

signatures is demonstrated in the incorporation of the photonic crystal structures that show a measured increase in C.O.V by a factor of 3.5× at the bandedge near 904 nm. While the presented topology belongs to a class of weak PUFs, the very nature of this topology adds considerable physical layers of security due to its dependence of wavelength and angle of incidence, which are easily controlled in a batch processing.

## VI. CONCLUSION

This paper presents a CMOS optical PUF through careful design of process-sensitive optical nanostructures in CMOS to exploit passive variations on top of active variations in order to create highly robust responses. The lower metal interconnect layers in the sub-wavelength dimensions are utilized to realize these photonic crystals on an array of photodetectors in the implemented CMOS optical PUF. Fabricated in a 65-nm CMOS process with no post-processing, the addition of the photonic crystal structures is shown to increase the C.O.V by a factor of 3.5× compared to only active device variations. These excess variations create extremely robust PUF responses. The measured inter-chip HD of 49.81% and intra-chip HD/BER of 0.25% with inter-HD/intra-HD ratio of 198× demonstrate the stability of the PUF. The chip demonstrates one of the highest stabilities in comparison to the state of the art. To the best of our knowledge, this paper is also the first demonstration of photonic crystals and optical PUF in CMOS through the designed incorporation of process-sensitive passive structures in a chip.

## ACKNOWLEDGMENT

The authors would like to acknowledge all members of the IMRL Laboratory for technical discussions.

## REFERENCES

[1] D. Lund, C. MacGillivray, V. Turner, and M. Morales, "Worldwide and regional Internet of Things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand," Int. Data Corp., Framingham, MA, USA, Tech. Rep., 2014. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS43295217
[2] C. Ely, "The life expectancy of electronics," Consumer Technol. Assoc., Arlington, VA, USA, Tech. Rep., 2014.
[3] M. Crawford *et al.*, "Defense industrial base assessment: Counterfeit electronics," U.S. Dept. Commerce Bur. Ind. Secur. Office Technol. Eval., Washington, DC, USA, Tech. Rep. 1, 2010.
[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Design Automat. Conf.*, 2007, pp. 9–14.
[5] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices," in *Proc. Int. Workshop Secur. Protocols*. Springer, 1997, pp. 125–136.
[6] K. Shamsi and Y. Jin, "Security of emerging non-volatile memories: Attacks and defenses," in *Proc. IEEE 34th VLSI Test Symp.*, Apr. 2016, pp. 1–4.
[7] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
[8] D. E. Holcomb and K. Fu, "Bitline PUF: Building native challenge-response PUF capability into any SRAM," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Springer, 2014, pp. 510–526.
[9] D. E. Holcomb, W. P. Burleson, 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.
[10] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A physically unclonable function with BER $<10^{-8}$ for robust chip authentication using oscillator collapse in 40 nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2015, pp. 1–3.
[11] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A 553F$^2$ 2-transistor amplifier-based physically unclonable function (PUF) with 1.67% native instability," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2017, pp. 146–147.
[12] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators," *IEEE J. Solid-State Circuits*, vol. 51, no. 9, pp. 2192–2202, Sep. 2016.

[13] S. Tajik *et al.*, "Photonic side-channel analysis of arbiter PUFs," *J. Cryptol.*, vol. 30, no. 2, pp. 550–571, 2017.
[14] J. Tobisch and G. T. Becker, "On the scaling of machine learning attacks on PUFs with application to noise bifurcation," in *Proc. RFIDSec*, 2015, pp. 17–31.
[15] S. N. Graybeal and P. B. McFate, "Getting out of the STARTing block," *Sci. Amer.*, vol. 261, no. 6, pp. 61–67, 1989.
[16] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.
[17] Y. Cao, L. Zhang, S. S. Zalivaka, C.-H. Chang, and S. Chen, "CMOS image sensor based physical unclonable function for coherent sensor-level authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 11, pp. 2629–2640, Nov. 2015.
[18] X. Lu, L. Hong, and K. Sengupta, "An integrated optical physically unclonable function using process-sensitive sub-wavelength photonic crystals in 65 nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2017, pp. 272–273.
[19] L. Hong, S. McManus, H. Yang, and K. Sengupta, "A fully integrated CMOS fluorescence biosensor with on-chip nanophotonic filter," in *Proc. Symp. VLSI Circuits*, Jun. 2015, pp. 206–207.
[20] L. Hong, H. Li, H. Yang, and K. Sengupta, "Fully integrated fluorescence biosensors on-chip employing multi-functional nanoplasmonic optical structures in CMOS," *IEEE J. Solid-State Circuits*, vol. 52, no. 9, pp. 2388–2406, Sep. 2017.
[21] P. Russell, "Photonic crystal fibers," *Science*, vol. 299, no. 5605, pp. 358–362, 2003.
[22] J. B. Pendry and P. M. Bell, "Transfer matrix techniques for electromagnetic waves," in *Photonic Band Gap Materials*. Dordrecht, The Netherlands: Springer, 1996, pp. 203–228.
[23] P. Yeh, *Optical Waves in Layered Media*. Hoboken, NJ, USA: Wiley, 2005.
[24] L. Hong and K. Sengupta, "Fully integrated optical spectrometer in visible and near-IR in CMOS," *IEEE Trans. Biomed. Circuits Syst.*, vol. 11, no. 6, pp. 1176–1191, Dec. 2017.
[25] L. Hong and K. Sengupta, "Fully integrated optical spectrometer with 500-to-830nm range in 65nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2017, pp. 462–463.
[26] L. Hong and K. Sengupta, "CMOS-based florescence biosensor with integrated nanoplasmonic filters," in *Proc. Conf. Lasers Electro-Opt. (CLEO)*, 2017, pp. 1–2.
[27] L. Hong, X. Lu, and K. Sengupta, "Nano-optical systems in CMOS," in *Proc. IEEE Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Boston, MA, USA, Aug. 2017, pp. 906–909.
[28] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc., McLean, VA, USA, Tech. Rep. 1, 2001. [Online]. Available: http://www.dtic.mil/docs/citations/ADA393366
[29] S. K. Mathew *et al.*, "A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2014, pp. 278–279.
[30] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45 nm smart-card chips," in *IEEE ISSCC Dig. Tech. Papers*, Jan. 2016, pp. 158–159.
[31] A. B. Alvarez, W. Zhao, and M. Alioto, "Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 V and 15 fJ/bit in 65 nm," *IEEE J. Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, Mar. 2016.

**Xuyang Lu** (S'15) received the B.S. degree in electrical engineering from Rice University, Houston, TX, USA, in 2014.

In 2015, he joined Prof. Sengupta's Lab, Princeton University, Princeton, NJ, USA. His current research interests include analysis, design, and testing of integrated circuits and antennas, with applications in high-speed wireless communication, radar, medical imaging, and bio-sensing.

Mr. Lu was a recipient of the Analog Devices Outstanding Student Designer Award in 2018. He was invited to join the Phi-Beta-Kappa National Society and the IEEE Eta-Kappa-Nu Honor Society.

**Lingyu Hong** (S'14) received the B.S. degree in physics from Peking University, Beijing, China, in 2012, with a focus on nanophotonics and plasmonics.

In 2013, he joined Prof. Sengupta's Lab, Electrical Engineering Department, Princeton University Princeton, NJ, USA. His current research interests include the implementation of interdisciplinary knowledge in photonics, electronics, and others for lab-on-chip systems, specifically for biomedical applications.

Mr. Hong was a recipient of the Analog Device Outstanding Student Designer Award in 2015, the Qualcomm Innovation Fellowship in 2015, the IEEE Solid-State Circuits Society Pre-Doctoral Achievement Award in 2017, and the Qualcomm Innovation Finalist in 2017. He received the Peking University Academic Excellence Reward and various scholarships.

**Kaushik Sengupta** (SM'17) received the B.Tech. and M.Tech. degrees in electronics and electrical communication engineering from IIT Kharagpur, Kharagpur, India, in 2007, and the M.S. and Ph.D. degrees in electrical engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 2008 and 2012, respectively.

He performed research with the University of Southern California, Los Angeles, CA, USA, and the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2005 and 2006, where he was involved in nonlinear integrated systems for high-purity signal generation and low-power RF identification tags. He joined as a Faculty Member the Department of Electrical Engineering, Princeton University, Princeton, NJ, USA, in 2013. His current research interests include high-frequency ICs, electromagnetics, and optics for various applications in sensing, imaging, and high-speed communication.

Dr. Sengupta received the DARPA Young Faculty Award in 2018, the Bell Labs Prize in 2017, and the Young Investigator Program Award from the Office of Naval Research in 2017. He received the E. Lawrence Keys, the Jr./Emerson Electric Co. Junior Faculty Award from the Princeton School of Engineering and Applied Science in 2018, and the Excellence in Teaching Award in 2018 nominated by the Undergraduate and Graduate Student Council, Princeton School of Engineering and Applied Science. He was four times selected to the Princeton Engineering Commendation List for Outstanding Teaching in 2014 and 2016–2018. He was a recipient of the Charles Wilts Prize in 2013 from Caltech Electrical Engineering for the best Ph.D. thesis, the Caltech Institute Fellowship, the Prime Minister Gold Medal Award of IIT in 2007, the IBM Ph.D. Fellowship from 2011 to 2012, the IEEE Solid State Circuits Society Predoctoral Achievement Award in 2012, the IEEE Microwave Theory and Techniques Graduate Fellowship in 2012, the Analog Devices Outstanding Student Designer Award in 2011, the Prime Minister Gold Medal Award of IIT Kharagpur in 2007, the Caltech Institute Fellowship, the Most Innovative Student Project Award of the Indian National Academy of Engineering in 2007, and the IEEE Microwave Theory and Techniques Undergraduate Fellowship in 2006. He was a co-recipient of the IEEE RFIC Symposium Best Student Paper Award in 2012 and the 2015 Microwave Prize from the IEEE Microwave Theory and Techniques Society. He serves on the Technical Program Committee of the IEEE Custom Integrated Circuits Conference, the IEEE European Solid-State Circuits Conference, and Progress in Electromagnetics Research.