Research Article | Vol. 25, No. 11 | 29 May 2017 | OPTICS EXPRESS 12710
Optics EXPRESS

Silicon photonic physical unclonable function

BRIAN C. GRUBEL, BRYAN T. BOSWORTH, MICHAEL R. KOSSEY, HONGCHENG SUN, A. BRINTON COOPER, MARK A. FOSTER, AND AMY C. FOSTER*

Department of Electrical and Computer Engineering, Johns Hopkins University, Baltimore, Maryland 21218, USA
**amy.foster@jhu.edu*

Abstract: Physical unclonable functions (PUFs) serve as a hardware source of private information that cannot be duplicated and have applications in hardware integrity and information security. Here we demonstrate a photonic PUF based on ultrafast nonlinear optical interactions in a chaotic silicon micro-cavity. The device is probed with a spectrally-encoded ultrashort optical pulse, which nonlinearly interacts with the micro-cavity. This interaction produces a highly complex and unpredictable, yet deterministic, ultrafast response that can serve as a unique "fingerprint" of the cavity and as a source of private information for the device's holder. Experimentally, we extract 17.1-kbit binary keys from six different photonic PUF designs and demonstrate the uniqueness and reproducibility of these keys. Furthermore, we experimentally test exact copies of the six photonic PUFs and demonstrate their unclonability due to unavoidable fabrication variations.

OCIS codes: (060.4785) Optical security and encryption; (320.0320) Ultrafast optics; (230.3990) Micro-optical devices.

References and links

1. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Netw. **76**, 146–164 (2014).
2. R. Anderson, *Security Engineering*, 2nd ed. (Wiley Publishing, Inc., 2008).
3. H. Busch, M. Sotáková, S. Katzenbeisser, and R. Sion, "The PUF promise," in *Proc. 3rd Int. Conf. Trust Trust. Comput.* (2010), pp. 290–297.
4. R. Maes, *Physically Unclonable Functions : Constructions, Properties and Applications* (2012).
5. R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, and C. Yang, "Physical key-protected one-time pad," Sci. Rep. **3**(1), 3543 (2013).
6. U. Ruhrmair and J. Solter, "PUF modeling attacks: An introduction and overview," Des. Autom. Test Eur. Conf. Exhib. (2014), pp. 1–6.
7. R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," Science **297**(5589), 2026–2030 (2002).
8. R. Pappu, "Physical One-Way Functions," Massachusetts Institute of Technology (2001).
9. U. Rührmair, C. Hilgers, and S. Urban, "Optical PUFs reloaded," (Eprint.Iacr.Org, 2013).
10. S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, "Quantum-secure authentication of a physical unclonable key," Optica **1**(6), 421–424 (2014).
11. S. H. Strogatz, *Nonlinear Dynamics and Chaos* (Perseus Books Publishing, LLC, 1994).
12. O. Legrand and F. Mortessagne, "Wave chaos for the Helmholtz equation," New Dir. Linear Acoust. Vib., 1–45 (2010).
13. V. Doya, O. Legrand, F. Mortessagne, and C. Miniatura, "Speckle statistics in a chaotic multimode fiber," Phys. Rev. E - Stat. Nonlinear. Soft Matter Phys. **65**, 1–15 (2002).
14. B. C. Grubel, D. S. Vresilovic, B. T. Bosworth, M. Kossey, A. C. Foster, M. A. Foster, and A. B. Cooper, "Light transport through ultrafast chaotic micro-cavities for photonic physical unclonable functions," in *Conf. Inf. Sci. Syst.* (CISS, 2017).
15. R. Osgood, "Nonlinear silicon photonics," SPIE Newsroom **4**, 535–544 (2010).
16 Photon Design, "OmniSim," (2015).
17. A. Taflove and S. Hagness, *Computational Electodynamics The Finite-Difference Time-Domain Method* (Artech House, Inc., 2005).
18. X. Sanga, E. K. Tienb, and O. Boyraz, "Applications of two-photon absorption in silicon," J. Optoelectron. Adv. Mater. **11**, 15–25 (2009).
19. A. C. Turner-Foster, M. A. Foster, J. S. Levy, C. B. Poitras, R. Salem, A. L. Gaeta, and M. Lipson, "Ultrashort free-carrier lifetime in low-loss silicon nanowaveguides," Opt. Express **18**(4), 3582–3591 (2010).

#292631 https://doi.org/10.1364/OE.25.012710
Journal © 2017 Received 11 Apr 2017; revised 12 May 2017; accepted 13 May 2017; published 22 May 2017

Optics EXPRESS

20. B. C. Grubel, B. T. Bosworth, M. Kossey, A. B. Cooper, M. A. Foster, and A. C. Foster, "Secure authentication using the ultrafast response of chaotic silicon photonic microcavities," in *Conf. Lasers Electro-Optics* (CLEO 2016), pp. 2–3.
21. B. T. Bosworth, J. R. Stroud, D. N. Tran, T. D. Tran, S. Chin, and M. A. Foster, "High-speed flow microscopy using compressed sensing with ultrafast laser pulses," Opt. Express **23**(8), 10521–10532 (2015).
22. L. Kocarev and S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications* (Springer, 2011).
23. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**(12), 728–732 (2008).
24. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**(1), 58–61 (2010).
25. C. M. Sorace-Agaskar, P. T. Callahan, K. Shtyrkova, A. Baldycheva, M. Moresco, J. Bradley, M. Y. Peng, N. Li, E. S. Magden, P. Purnawirman, M. Y. Sander, G. Leake, D. D. Coolbaugh, M. R. Watts, and F. X. Kaertner, "Integrated mode-locked lasers in a CMOS-compatible silicon photonic platform," in *CLEO 2015* (2015), paper SM2I.5.
26. P. D. Fisher and R. Nesbitt, "The test of time. Clock-cycle estimation and test challenges for future microprocessors," IEEE Circuits Devices Mag. **14**(2), 37–44 (1998).
27. M. D. Stenner, D. J. Gauthier, and M. A. Neifeld, "The speed of information in a 'fast-light' optical medium," Nature **425**(6959), 695–698 (2003).
28. M. Gu, X. Li, and Y. Cao, "Optical storage arrays: a perspective for future big data storage," Light Sci. Appl. **3**(5), e177 (2014).
29 U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. ürgen Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. 17th ACM Conf. Comput. Commun. Secur. - CCS* (2010), pp. 237.
30. A. Vijayakumar and S. Kundu, "A novel modeling attack resistant PUF design based on non-linear voltage transfer characteristics," in *Des. Autom. Test Eur. Conf. Exhib.* (2015), pp. 653–658.
31. C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," Proc. IEEE 102(8), 1126–1141 (2014).</jrn>

1. Introduction

The continual evolution of modern authentication methods reflects a persistent escalation in the battle for information security. Centuries of security innovation have created reliable tools that we use, for example, to access personal electronics and online accounts, and to purchase goods securely. Moreover, the growth of the Internet of Things is escalating the importance of information security as connected devices can, for example, administer medication, control transportation, and operate key infrastructure [1]. However, all modern authentication approaches are vulnerable to counterfeiting and fraud [2] because they rely on digital information that is presumed to be secret.

Physical keys store secret information in their physical structure and have evolved over thousands of years to securely authenticate their holder. Impressively, some modern realizations of physical keys, known as physical unclonable functions (PUFs) are sufficiently complex in their behavior to prevent their duplication. PUFs are ideally suited for applications in low-cost device authentication, key-agreement, private key storage, anti-counterfeiting, secure communication, and hardware-entangled cryptography [3–5]. Optical PUFs are generally considered more strongly unclonable than electronic PUFs due to the greater complexity of their behavior [6]. However, existing optical PUFs harness linear spatial scattering using narrow linewidth laser sources, bulk materials, and camera-based detection [5,7–10] resulting in sensitive systems that are not easily integrated into electronic circuits. Here we demonstrate and validate a PUF realized using guided-wave nonlinear silicon photonic devices, which is directly compatible with both planar semiconductor fabrication and optical communications hardware.

2. Device Design

PUFs are interrogated using a challenge-response authentication protocol and an ideal PUF should exhibit behavior that is reproducible (only by itself), unique, unclonable, one-way, unpredictable, and tamper evident [Fig. 1] [4]. Specifically, PUFs should have a highly reproducible response to the same input challenge indicating determinism and low system

Optics EXPRESS

noise [Fig. 1(a)]. Different PUF designs should be unique, such that the same challenge given to two different devices produces vastly different responses [Fig. 1(b)]. The PUF should be unclonable such that it is infeasible for an adversary with complete knowledge of a legitimate device's design to produce a copy that behaves identically to an authentic device [Fig. 1(c)]. Furthermore, the underlying PUF operation itself should be sufficiently complex that it is unreasonable to invert its behavior or predict a response to some arbitrary input [Figs. 1(d) and 1(e)]. Lastly, should an adversary tamper with a legitimate PUF, it should be evident through inspection or interrogation [Fig. 1(f)]. Notably, these desired properties form parallels to the behavior of chaotic systems [11] in that the behavior should be highly sensitive to initial conditions (i.e. both precise device structure and input challenge waveform), be of high complexity, yet be deterministic. For this reason, here we focus on a PUF design based on reverberant silicon photonic micro-cavities that exhibit ray chaotic behavior.

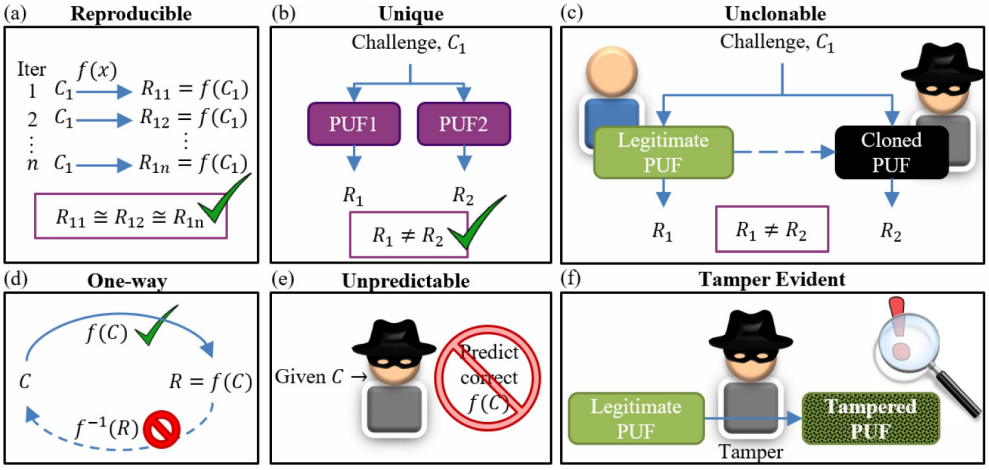

Fig. 1. Desired properties for the performance of an ideal PUF.

We design the photonic micro-cavity as a disk with a chamfer [Fig. 2(a)], which, in dynamic billiards, is known to exhibit chaotic behavior [12–14]. We leverage this ray-chaotic design to make the device's behavior highly sensitive to structural idiosyncrasies (e.g. sidewall roughness, resist granularity, precise film thickness, material impurities) and therefore thwart cloning. In any real fabrication process, these device idiosyncrasies are inevitable and are precisely the information carrying structures that make each device unique. Beyond chaos, the property of nonlinearity can also increase the complexity of the relationship between system input and output, thus enhancing its unpredictability, one-wayness, and unclonability. In addition to the ray-chaotic design, we operate the device at sufficiently high optical power levels to exploit the natural nonlinearities of silicon (e.g. Kerr, two-photon absorption, free carrier) [15]. Finally, while extreme sensitivity to precise conditions is desired we also must ensure reproducibility of the device behavior. To this end, we employ single-mode silicon waveguides for robust optical coupling to and from the micro-cavity devices as seen in Fig. 2(a).

To optimize a general baseline cavity design, we first carry out a rapid evaluation of many potential cavity geometries by performing two-dimensional finite difference time-domain (FDTD) simulations over diameter, chamfer size, and chamfer location using the OptiFDTD solver from Optiwave Systems Inc. [Fig. 2(b)]. We operate the solver at a range of mesh resolutions (10-50 nm) that inversely scales with model size, which allows a rough evaluation of total power and photon lifetime. On the input bus waveguide, a mode excitor calculates supported modes using the effective index solver for both the transverse electric (TE) and transverse magnetic (TM) modes. Sensors are placed after the mode excitor on the input and

Optics EXPRESS

output waveguides. Drude material models for silicon and silicon dioxide are used to generate the material properties and their associated response [16]. A perfectly matched layer (PML) is used to impose a first-order absorbing Silver-Mueller boundary condition on all faces of the device [17].

Notably, there is a general tradeoff between interaction complexity and optical loss. Specifically, while larger cavity geometries produce longer photon-lifetimes and thus more potential complexity of behavior, they also exhibit increased loss from the input to the output waveguide [Fig. 2(b)]. Likewise, smaller cavity geometries will exhibit decreased input-output loss but possess shorter cavity lifetimes and therefore less potential complexity of behavior. Ultimately, we selected a 30-µm diameter baseline given the tradeoff between lifetime and loss.

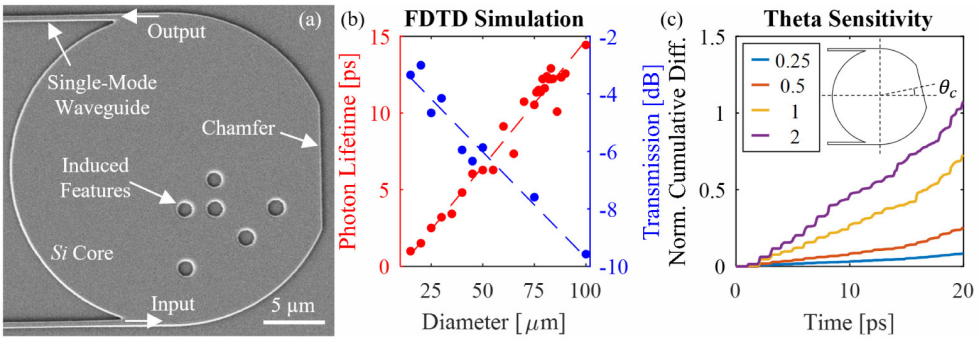

Fig. 2. Photonic PUF design and simulation. (a) Scanning electron microscope (SEM) image of an example cavity. (b) Photon lifetime and transmission for a range of cavity diameters simulated with FDTD averaged over different chamfer positions and sizes. (c) A baseline geometry was simulated via FETD with an input Gaussian envelope pulse of 100-fs FWHM at 1550 nm. Simulations of designs varying only by chamfer angle were performed with output intensity envelopes compared to the baseline geometry via a cumulative difference first normalized to the total summation of the baseline power samples after removal of exponential decay. The increased slope of each curve shows separation as a function of geometrical deviation, which agrees with chaotic behavior. The inset image shows the cavity geometry and coordinate system.

To further investigate the baseline device design, we use high-accuracy two-dimensional finite element time-domain (FETD) simulations to model the ultrafast optical interaction within the micro-cavity using the Photon Design® OmniSim FETD solver. Through a convergence study on key metrics such as total power, photon lifetime, and peak-to-average power ratio (PAPR) of the output waveform, we find that third-order elements with a nominal resolution of 300 nm are sufficient. This two-dimensional simulation of triangular elements is one finite element thick in the device *y*-direction (plane of calculation). A typical model was constructed with a mean physical element size of 34 nm and a minimum physical element size of 13 nm for a total of ~163,000 elements. We apply similar mode excitors, sensor placement, material models, and PMLs as in the FDTD simulations. We then examine the sensitivity of the time-domain response on the output port to changes in geometry to confirm the chaotic cavity behavior [Fig. 2(c)]. Four different chamfer positions are simulated and the divergence over time of the response waveforms produced by a 100-fs full-width half-maximum (FWHM) Gaussian input pulse is computed. To characterize this divergence, we calculate a normalized cumulative difference between the response waveforms of the modified cavities to the reference cavity. This is calculated by first removing the exponential decay from the response waveforms and then summing the absolute value of the difference between the waveforms over time. This is then normalized to the maximum difference observed for the cavity with the largest perturbation. The significant deviation of the waveforms, even for changes in position of the chamfer of less than a degree, demonstrates

Optics EXPRESS

our designed device's sensitivity to small changes in cavity shape. Additionally, the increasing rate of divergence of the waveforms as a function of geometrical deviation is indicative of chaotic behavior [11]. In our previous work we carried out an analysis of the chaotic behavior of these devices using a ray-based analysis and conventional metrics such as the Lyapunov exponent [14]. In this previous work, we also examine the effect of the various design parameters on these metrics and confirmed that fabrication variance increases the divergence of temporal responses, that the photon lifetime increases with radius, and that the transmission gain decreases with radius [14]. Further, we found that photon lifetime and transmission gain are inversely dependent on chamfer size and are minimally dependent on chamfer position.

3. Device Fabrication

We fabricated six device designs [Fig. 3] from single-crystal silicon-on-insulator (SOI) wafers with a 500-nm thick top silicon layer, a 3-μm buried oxide layer, and a 500-μm silicon substrate. The top silicon layer is thinned to a thickness of 220-nm in two steps of thermal oxidation, followed by removal of oxide via hydrofluoric acid etch. The second acid etch was terminated early in order to leave a 100-nm thick layer of thermal oxide to serve as a hard mask during the subsequent etching process. MaN-2405 negative tone electron-beam resist is then used to pattern the devices with electron beam lithography (EBL). The EBL tool (Joel JBX-6300FS) writes patterns of 8 nm or less, leveraging a 2.1 nm beam at a 100-kV accelerating voltage. The EBL tool has a high-precision stage that employs beam-positioning digital-to-analog conversion (DAC) of 19 bits with 0.125 nm resolution and laser interferometer with 0.6 nm resolution, which achieves a writing positional accuracy of 9 nm or less for small fields to large-area fields. After development, we transfer the device patterns to the silicon dioxide layer through reactive-ion etching (RIE), which then serves as a hard mask for the following inductively-coupled plasma RIE step that transfers the device pattern into the silicon layer. We clad the devices with a 1-μm layer of silicon dioxide with plasma-enhanced chemical vapor deposition. Finally, the wafers are diced to separate individual dies, and the edge facets are polished using fine grit diamond film in preparation for edge coupling via tapered single-mode fibers (SMF).

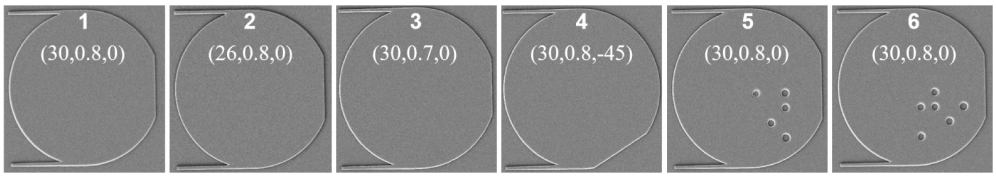

Fig. 3. SEM images of 6 prototype PUF designs with design parameters in parenthesis (diameter in microns, chamfer size as a factor of radius, and chamfer angle with respect to the unit circle).

All of the fabricated devices are perturbations on a 30-μm diameter disk cavity with a chamfer. Each design differs from at least one other design in exactly one parameter including size and position of the chamfer, as well as the presence or absence of arbitrarily positioned holes within the cavity [Fig. 3]. This makes it possible to isolate the effects on device behavior to a single parameter. Two copies of every cavity are fabricated on the same SOI die, located as close together as possible, and created in the same fabrication run, to minimize variations and permit analysis of PUF clonability. The copy of each cavity will hereafter be termed its "clone."

Optics EXPRESS

4. Device Characterization

Time-Domain and Frequency-Domain Impulse Response

We first measure the spectral and temporal impulse response of each fabricated cavity to an ultrashort input pulse using an optical spectrum analyzer (OSA) and an ultrafast optical cross-correlator [Figs. 4(a) and 4(b)]. The 175-fs input optical pulse is generated by spectrally broadening a 90-MHz repetition rate mode-locked laser (MLL) source via a normal dispersion fiber followed by a spectral filter. Finally, it is temporally compressed by a programmable spectral filter to create nearly transform-limited sinc-shaped pulses with 5 THz of bandwidth (175-fs) traveling into the cavity. A fiber splitter diverts 80% of the optical power to the photonic device and 20% to the reference arm. A polarization controller and tapered fiber are used to couple into the silicon bus waveguide that then feeds the photonic cavity; the response from the cavity is coupled out of the chip through the output silicon bus waveguide, collimated with a high-numerical aperture aspheric singlet and passed through a linear film polarizer to select the desired polarization state. While the system can operate in the TE, TM, or cross-polarized (XP) state, we focus here on the TE polarization, which provides the maximum output power and signal-to-noise ratio (SNR). This response is then amplified by an erbium-doped fiber amplifier (EDFA) before reaching the cross-correlator. Chromatic dispersion due to the single-mode fiber (SMF) in the two arms of the system (the device under test and the reference arm), is compensated up to the free-space inputs to the cross-correlator for optimal temporal resolution. As anticipated, each cavity exhibits unique spectral and temporal impulse response behavior, and small changes in cavity geometry induce distinct behaviors as shown in Fig. 4.

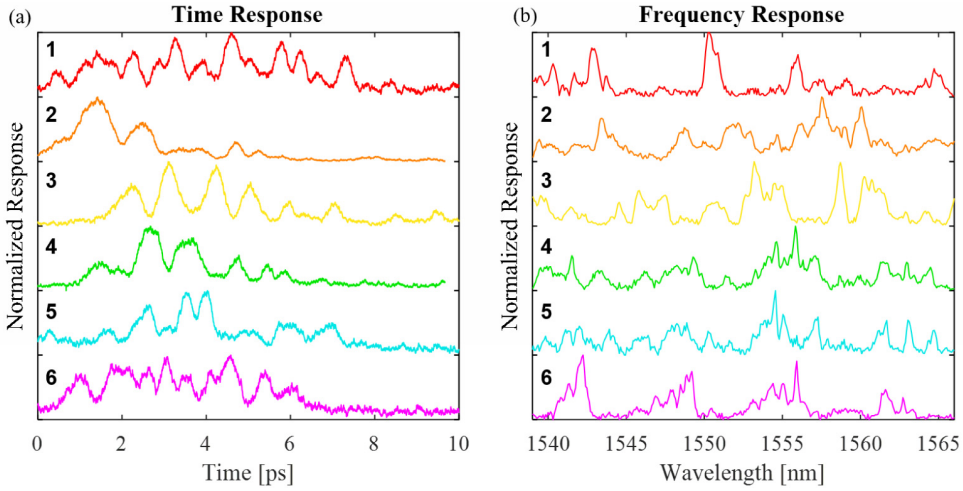

Fig. 4. (a) Normalized time-domain impulse response measured using cross-correlation with a sinc pulse (175 fs FWHM) for cavities 1-6 shown in order top to bottom. (b) Normalized spectral transfer-function magnitude for the same experiment.

Nonlinear Characterization

The existence of nonlinearity, such as a nonlinear optical response as demonstrated here, can increase the complexity of the interaction thereby enhancing its unpredictability, one-wayness, and unclonability [8]. To characterize the presence of optical nonlinearity, we first observe the change in the output spectrum as a function of input pulse energy. For this measurement, we amplify a ~175 fs FWHM input pulse from the 90-MHz MLL and associated compression stages and a variable attenuator to evaluate the different power levels. We ensure that the input spectrum does not change by observing it on an optical spectrum

Optics EXPRESS

analyzer (OSA) prior to the chip input. As shown in Fig. 5(a), we observe distinct variations in the normalized power spectral density of the temporal output waveform as a function of pulse energy, thereby verifying that the photonic PUF is operating in a nonlinear regime. There are several origins of this nonlinear behavior. In silicon devices, nonlinear effects are known to include self-phase modulation (SPM), two-photon absorption (TPA), four-wave mixing (FWM), stimulated Raman scattering (SRS), and free-carrier induced absorption and dispersion [15], and these spectral changes are a result of a combination of these mechanisms. For example, we show the presence of FWM in one of our PUF devices by inputting two 6.7-ps pulses at different wavelengths and observing the generation of FWM sidebands [Fig. 5(b)]. Further, TPA in silicon is well known to generate free carriers which introduce loss and change the refractive index [18].

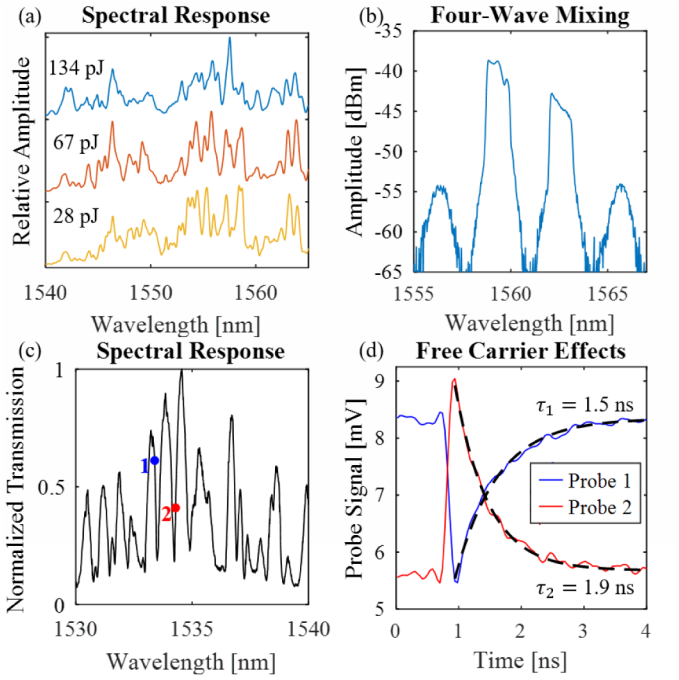

Fig. 5. Observed nonlinear effects in the photonic PUF. (a) Nonlinear power dependence of the output power spectral density of a prototype cavity in response to change in excitation pulse energies (28 pJ (yellow), 67 pJ (red), and 134 pJ (blue)) without changing input waveform or spectral content. (b) An input signal consisting of two 6.7-ps 50-pJ pulses centered at υ_1 = 191.94 THz and υ_2 = 192.43 THz are sent through the silicon cavity. Two new lightwaves at frequencies, υ_3 = 191.57 THz and υ_4 = 192.80 THz, as expected for a FWM process. (c) Spectral location of two probe measurements on sample device spectral transfer function. (d) Temporal responses of the two probes showing free carrier dispersion effects.

We show the presence of TPA generated free-carriers and the resulting free-carrier absorption (FCA) and free-carrier dispersion (FCD) in this device via a pump-probe measurement [19]. In this case, our pump is a 3.5-ps 300-pJ pulse from the 90-MHz MLL sent through a 100-GHz bandpass filter and the probe is a tunable continuous-wave source. By exciting the cavity with the pulse, free carriers are generated in the cavity which induce absorption and shift the cavity's resonance through FCD. We place the probe at two spectral locations on the cavity's spectral response that provide the greatest sensitivity to such a resonance shift and observe the temporal responses [Figs. 5(c) and 5(d)]. The positive and negative slopes of the spectral response at these probe wavelengths yield inverted temporal responses as expected. From this measurement, we also determine the free-carrier lifetime of a typical cavity to be approximately 1.9 ns. These nonlinear optical effects demonstrate the

Optics EXPRESS

system's intricate spectro-temporal interaction that is critical for the PUF's unpredictability, one-wayness, and unclonability.

5. Challenge-Response Authentication System

Experimental Setup

To demonstrate the potential of this photonic PUF for applications in information security we investigate its use as an authentication token (a hardware device that is used to prove an identity and authorize access to a protected resource) in a challenge-response authentication system [20]. As depicted in Fig. 6(a), we design a challenge-response authentication protocol that interrogates the micro-cavity token with a sequence of spectrally-encoded ultrashort optical pulses [21], termed "challenge pulses". The optical response from the cavity is then passed through a programmable spectral filter and the total transmitted pulse energy is measured using a photodetector. The binary sequence encoded on each challenge pulse and the binary sequence derived from the optical response pulse constitute a challenge-response pair (CRP) and a sequence of binary responses is extracted to determine the cavity authenticity.

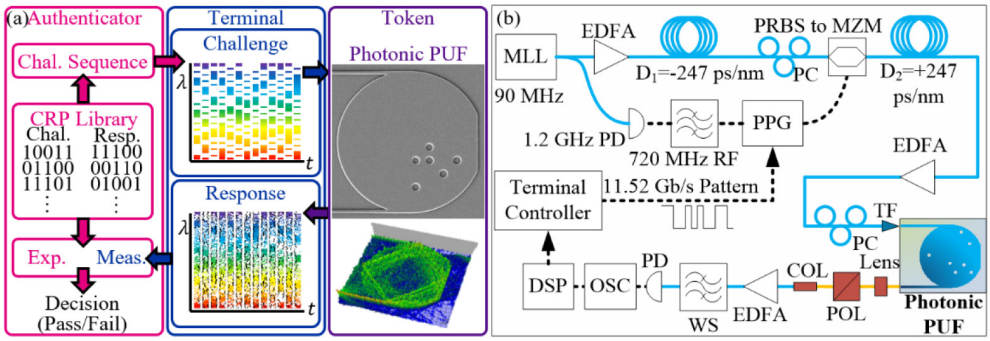

Fig. 6. Authentication system and experimental setup. (a) An authentication system is constructed from an authenticator, a terminal, and a token. A token is authenticated through interrogation by issuing a challenge and comparing its measured response to a (previously measured) expected response. (b) Experimental setup of authentication system demonstration. Pulses from a MLL are amplified, temporally stretched, and encoded with a binary sequence from a pulse pattern generator (PPG). The pulses are compressed, amplified, and sent through the cavity. The responses are amplified, sent through a programmable spectral filter (WS) to extract a subset of information from each spectral response, and detected via photo-diode (PD). The outputs are converted into binary sequences through a post-processing algorithm.

To generate the challenge pulse sequence, we implement a novel ultrafast pulse encoder as follows [21] [Fig. 6(b)]: dispersion compensating fiber (DCF) stretches each 300-fs MLL pulse (90-MHz repetition rate) to greater than 11 ns. The temporally dispersed spectrum is amplitude encoded by a length 128 pseudorandom binary sequence (PRBS), i.e. binary challenge, at 11.52 Gbit/s that is synchronized to the MLL. There is some overlap between time stretched pulses at this stage and thus neighboring pulses share some temporal features. However, they are mapped to different wavelengths and thus involve different parts of the pattern. This allows the patterns on each pulse to remain incoherent while providing more features on each pulse. We achieve 94 features within the 3-dB bandwidth of each pulse. After spectral patterning, the pulses are compressed to 6 ps using standard single-mode fiber. Using this approach, we generate a challenge pulse sequence of 8550 uniquely encoded pulses chosen to balance the total number of unique pulses and the ability to characterize the repeatability of the set within the memory buffer of the pulse pattern generator (PPG). This sequence is amplified with an EDFA to an average power of 64 mW and coupled into the token (our photonic PUF device) where the complex nonlinear optical interaction occurs.

Optics EXPRESS

To record the response sequence, the output response pulses are amplified using a second EDFA and a spectral measurement is performed by passing the response pulses through a pseudorandom spectral amplitude mask and detecting the transmitted pulse energy. The spectral mask is implemented using a programmable spectral filter with 296 random features within the optical bandwidth and the response pulse energies are recorded at the 90-MHz pulse rate. The input pulse bandwidth (1535-1575 nm) is not perfectly aligned with the spectral filter used in the experiment (1527.4-1567.5 nm), thus some of the spectrally-encoded information is lost. The pulse energies are recorded with an analog-to-digital converter (ADC) that can store over four million samples and is synchronized to the MLL. Notably, this high-throughput approach results in a key generation rate of up to 180 Mbps, which is a two order of magnitude improvement over previous work on optical scattering PUFs [5].

A post-processing algorithm extracts a binary sequence from the analog response pulse energies to enhance system robustness and maximize entropy per bit. [Fig. 7]. A probability density function (PDF) is estimated for the response energies and used in a histogram equalization algorithm to calculate non-uniform levels that will make any subsequently collected responses equiprobable when converted to binary. These non-uniform detection levels corresponding to each device are stored as helper data and are used in future challenge-response exchanges to aid in binary conversion. Using a reflected binary code (Gray code) in which adjacent levels differ by only a single bit, the power samples are then discretized and converted to binary for a specified number of resampled bits. An exclusive-or (XOR) operation is performed on adjacent sequences [22,23] to enhance complexity. A number of least significant bits (LSBs) are kept from each sample [24] and appended together to create a single bit sequence ranging from 8,550 to 51,300 bits. The resampling bits and the number of kept LSBs are optimized to minimize authentication error.

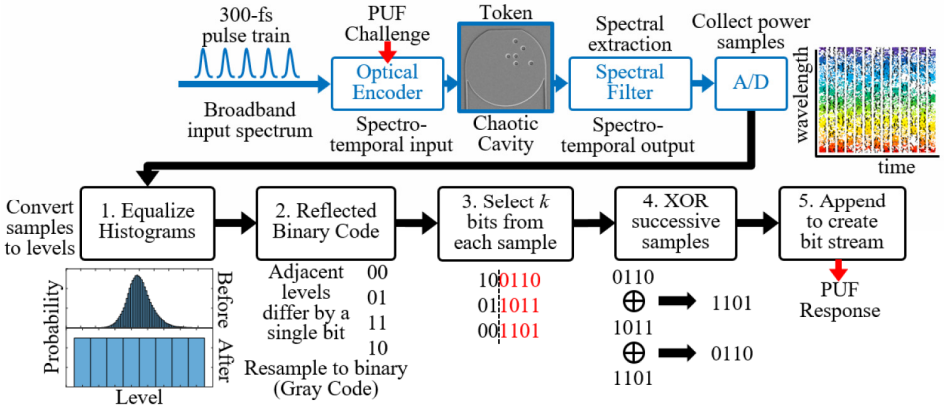

Fig. 7. Optical system elements (blue) and digital post-processing steps (black) to convert spectro-temporal responses into binary sequences.

To enroll a device, a challenge-response library (CRL) is built by averaging 460 analog response sequences from a specific token to the challenge pulse sequence (encoded with a PRBS) and calculating the resulting binary response sequence of this average response using the previously calculated non-uniform detection levels (helper data). In order to authenticate a key, the authenticator selects at random a set of CRPs from the CRL, encodes this binary sequence via spectral patterning onto a sequence of challenge pulses, sends this challenge pulse sequence to the token, measures the analog response sequence in a single shot without averaging, and converts it to a binary sequence in post-processing. This rapidly acquired binary sequence is compared to the CRL and the fraction of positions in which the sequences differ (the "fractional Hamming distance," or FHD) is employed as a metric to determine

Optics EXPRESS

authenticity. The authenticator compares the FHD to a predetermined threshold to decide whether to accept or reject the key.

Experimental Results

A set of histograms of the 460 FHDs between each individual binary response sequence of a given device and the CRL for every device are calculated and forms each row in Fig. 8(b). For each distribution, the mean and standard deviation are calculated and are presented for 6 prototype cavities. Binomial distributions are fit to each of the histograms. The histogram of FHDs from the repetitions of given device compared with the expected CRL for that device is referred to as the "same" distribution whereas the histograms of FHDs between each of those responses and the CRL of a cavity of different design forms a set of "different" distributions. The distance between the "same" distribution and the "different" distributions indicates the system's ability to discriminate between legitimate and illegitimate tokens.

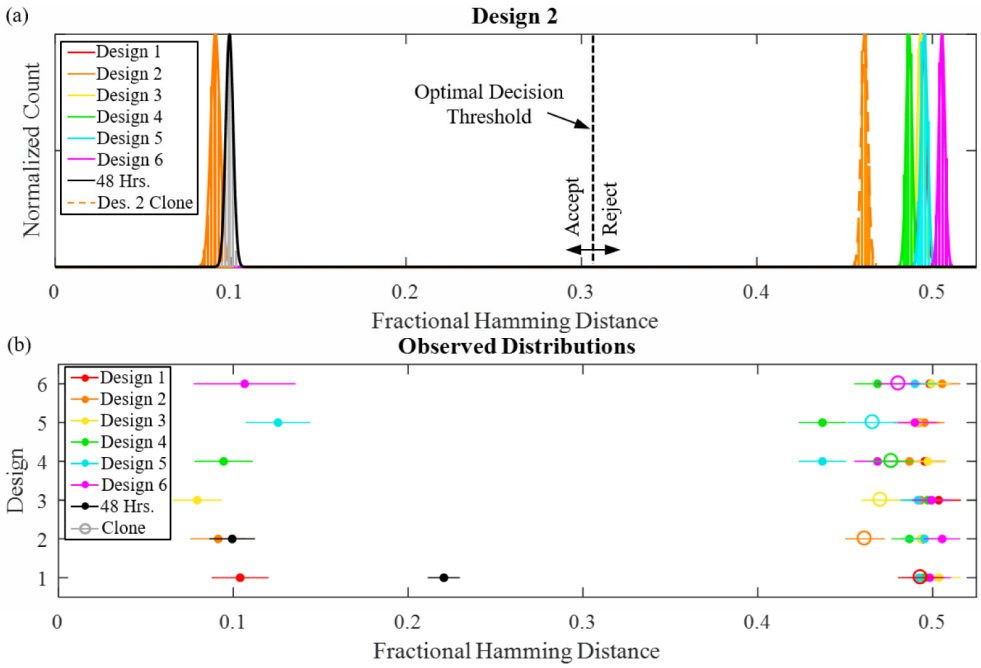

Fig. 8. Experimental authentication results. (a) The normalized FHD distributions and histograms for each design computed against the CRL for design 2 for a two LSB operating condition at a resampling of three bits post-ADC collection. The distribution representing an authentication attempt after 48 hours is also shown. (Design 1 results hidden by other distributions on the rejected side). (b) Normalized FHD distributions computed for each design against the CRL of every other design at the same operating conditions as Fig. 8(a). Design clone distribution shown in same color with circle marker. Authentication results after 48 hours shown for design 1 and 2. Error bars represent ± 6 standard deviations.

We compute system-level "same" and "different" distributions from the aggregated statistics of the individual distributions from each device, and compute an optimum decision threshold to minimize the total authentication error probability, which is the sum of the false acceptance rate (FAR) and the false rejection rate (FRR). We find that the probability of error generally increases with a decrease in the number of least significant bits (LSB) retained from each response in our post-processing algorithm. Retaining two LSBs with three-bit resampling gives a total error probability of roughly 10^{-21} of incorrectly accepting or rejecting a key for the experimentally investigated key length of 17.1 kb across distributions generated from all experimentally evaluated prototypes. Notably, the small FHD of the "same"

Optics EXPRESS

distributions indicate the reproducibility of the different designs' responses to identical challenges. The mean and standard deviation of these distributions are adversely affected by unavoidable system noise sources (shot noise, thermal noise, amplifier noise, mechanical vibration, etc.) Further, the closeness of the "different" distributions to a FHD of 0.5 indicates the uniqueness of the different designs' responses to identical challenges. The "clone" distribution [Fig. 8(a)] is generated by computing the FHD between the responses of a given cavity and the CRLs generated by the other cavities of identical design and fabrication conditions (As discussed earlier, these "clones" were fabricated on the same chip, at the same time and are located very close to one another to ensure their similarity in fabrication conditions.) Notably, this distribution closely aligns with the "different" distribution and the FAR for the cloned cavity is roughly 10^{-18} for a 17.1-kb key length across distributions generated from all interrogated prototype cavities, clearly demonstrating the devices' unclonability resulting from the sensitivity of their response to fabrication variations. We find that the unclonability of the various devices is similar. However, the addition of induced features into designs 5 and 6 adds loss and results in "same" distributions for these devices that are further from zero and having larger standard deviation indicating poorer SNR resulting from this greater loss.

Finally, we perform a repeatability over time experiment to determine the overall stability of the system. Designs 1 and 2 were investigated for this repeatability experiment. First, we enroll a typical authentication token to generate a reference CRL for the first day. We then perform a key verification process to determine the intra-distance or "same" distribution for that day to quantify its repeatability. We perform the same key verification process 48 hours later against the CRL generated on the first day to determine the shift in the mean of the FHD distribution. We did not attempt to account for or adjust the temperature and humidity conditions between the measurements within the laboratory and the power levels were generally kept within 0.3 dB between days. On the first day, the temperature was 20.8° C with a humidity of 63%. During the second measurement, the temperature was 20.6° C with a humidity of 71%. Further, the entire laboratory setup was fully deconstructed and reconstructed in between measurements. As shown in Fig. 8, the results indicate a clear repeatability of the system over time. In this proof-of-concept setup, it is challenging to isolate the stability of the cavity from the stability of the laboratory setup and thus we expect these results to be very conservative. We expect that a practical production-ready system or a system with interrogation components built directly into an integrated circuit [25] will have improved stability resulting in repeatability statistics similar to the single session repeatability that we observe here.

Security Evaluation

The security of this PUF is a result of the interaction complexity, nonlinearity, and ultrafast response speed. An adversary wishing to spoof the device has three options: direct cavity replication, or emulation using optoelectronic or computational means. As clearly shown here, the achievable precision of nanofabrication technology combined with the extreme sensitivity of the device's behavior to cavity structure prevents direct cavity replication.

Beyond direct duplication, the device's nonlinearity and ultrafast (sub-20-ps) response time prevent optoelectronic cloning using, for example, a programmable spectral filter (e.g. 4-f pulse shaper), due to the shaper's increased latency, and its inability to accurately recreate the nonlinearity of the cavity. Finally, even with complete knowledge of the CRL, to successfully emulate the device an adversary would need to measure an incident challenge, perform the necessary computations (through a lookup table or transform), and generate the appropriate response in a time interval faster than the device response time of 20 ps. Not only is this significantly shorter than a modern computer clock cycle [26], but given that information cannot travel faster than the speed of light [27], any such computational system (processor, memory, etc.) would need to be physically as small as the device (~30 μm x 30

Optics EXPRESS

μm). These stringent constraints prevent such an emulation approach with current or any foreseeable computational resources and, as one example, would require memory densities that are many orders of magnitude higher than the current state-of-the-art [28].

6. Summary, Discussion, and Future Work

Here we present a new type of PUF created from silicon photonic micro-cavities. We directly demonstrate the reproducibility, uniqueness, and unclonability properties of our photonic PUFs [Fig. 1]. We have shown that the probability of incorrectly accepting or rejecting a token based upon a 17.1-kb key is roughly 10^{-21} and the probability of falsely accepting a cloned token is roughly 10^{-18}. Notably, the system showed high repeatability after a 48-hour period by yielding similar error rates (FHD of 0.1) when compared to the same cavity authenticated at the time of CRL generation.

Future work will focus on evaluating the device's one-wayness and unpredictability properties through measuring resistance to machine learning attacks [6,9,29,30], assessing the impact of device's nonlinearity on output bit sequences, and estimating total information content [5]. As maximally identical fabricated devices ("clones") form unique responses to identical challenges, it is likely that any tampering would result in structural changes that impact the device's behavior and thus rendering the device tamper-evident via normal interrogation. This tamper evidence will also be the subject of future work as well as the analysis of the unclonability of devices fabricated using standard lithography which we expect can result in similarly unclonable devices. We will also investigate additional cavity designs, sizes, and materials to further improve on performance and the integration of various components of the interrogator onto a single CMOS platform.

Information security is of paramount importance to our information-centric society and demands continual innovation to address the evolving threats. Here we demonstrate a silicon photonic PUF, which is the first optical PUF that is directly compatible with electronic fabrication processes and telecommunications infrastructure. This photonic PUF can bring the security benefits of optical PUFs to practical applications in electronic circuits. Due to their speed, simplicity, compactness, low-cost, and technological compatibility, these photonic PUFs can find application in a range of authentication technologies including mobile devices, computers, smart tokens, credit cards, and secure data storage devices along with ensuring supply chain integrity. Furthermore, the scalability of silicon photonic integration indicates that a large number of these devices can form an interconnected system to further increase the optical interaction complexity and thus security. Additionally, due to the key extraction speed and compatibility with both electronics and optical communications, the security afforded by these devices can be readily extended beyond authentication to, for example, circuits for tamper awareness, encrypted information storage, and encrypted high-speed communications [5,31].

Funding

National Science Foundation (NSF) (EFMA-1641094; ECCS-1521415); Johns Hopkins University Catalyst Fund

Acknowledgments

The silicon devices were fabricated in part at the Center for Nanoscale Science and Technology's NanoFab at the National Institute of Standards and Technology. Portions of this work were presented at the Conference on Lasers and Electro-Optics in 2016 (paper SF1F.2).