Research Article

ADVANCED PHOTONICS

# Authentication through residual attention-based processing of tampered optical responses

Blake Wilson,[a,b,†] Yuheng Chen,[a,b,†] Daksh Kumar Singh,[a,b] Rohan Ojha,[a] Jaxon Pottle,[c] Michael Bezick,[d] Alexandra Boltasseva,[a,b] Vladimir M. Shalaev,[a,b] and Alexander V. Kildishev[a,*]

[a]Purdue University, Elmore Family School of Electrical and Computer Engineering, West Lafayette, Indiana, United States
[b]Quantum Science Center, Oak Ridge National Laboratory, Oak Ridge, Tennessee, United States
[c]Purdue University, School of Aeronautics and Astronautics, West Lafayette, Indiana, United States
[d]Purdue University, Department of Computer Science, West Lafayette, Indiana, United States

**Abstract.** The global chip industry is grappling with dual challenges: a profound shortage of new chips and a surge of counterfeit chips valued at $75 billion, introducing substantial risks of malfunction and unwanted surveillance. To counteract this, we propose an optical anti-counterfeiting detection method for semiconductor devices that is robust under adversarial tampering features, such as malicious package abrasions, compromised thermal treatment, and adversarial tearing. Our new deep-learning approach uses a RAPTOR (residual, attention-based processing of tampered optical response) discriminator, showing the capability of identifying adversarial tampering to an optical, physical unclonable function based on randomly patterned arrays of gold nanoparticles. Using semantic segmentation and labeled clustering, we efficiently extract the positions and radii of the gold nanoparticles in the random patterns from 1000 dark-field images in just 27 ms and verify the authenticity of each pattern using RAPTOR in 80 ms with 97.6% accuracy under difficult adversarial tampering conditions. We demonstrate that RAPTOR outperforms the state-of-the-art Hausdorff, Procrustes, and average Hausdorff distance metrics, achieving a 40.6%, 37.3%, and 6.4% total accuracy increase, respectively.

Keywords: machine learning; plasmonics; physical unclonable function; anti-counterfeiting; tampering detection.

Received Apr. 1, 2024; revised manuscript received Jun. 1, 2024; accepted for publication Jun. 13, 2024; published online Jul. 17, 2024.

[DOI: 10.1117/1.AP.6.5.056002]

## 1 Introduction

The semiconductor industry has grown into a $500 billion global market over the last 60 years. However, the semiconductor fabrication pipeline has become fragmented, inadvertently giving rise to a $75 billion counterfeit chip market that jeopardizes safety and security across multiple sectors dependent on semiconductor technologies, such as aviation, communications, quantum, artificial intelligence, and personal finance.[1–5] Several techniques aimed at affirming semiconductor authenticity have been introduced to detect counterfeit chips, largely leveraging physical security tags baked into the chip functionality or packaging.[6–13] Central to many of these methods are physical unclonable functions (PUFs),[14,15] which are unique physical systems that are difficult to replicate, either because of economic constraints or inherent physical properties. Rather than being grounded in cryptographic hardness, PUFs emphasize the economic and technological challenges of duplicating a given system's physical characteristics.[16] Optical PUFs, which capitalize on the distinct optical responses of random media, are especially promising. However, achieving scalability and maintaining accurate discrimination between adversarial tampering and natural degradation, such as physical aging at higher temperatures, packaging abrasions, and humidity, poses significant challenges.[17–19]

To combat these difficulties, this study focuses on an optical PUF model utilizing the distance matrix constructed of the positions and radii of random gold nanoparticles.[20] The overview process of the PUF tamper detection method is demonstrated in Fig. 1. Due to the extreme difficulty of replicating large sets of

*Address all correspondence to Alexander V. Kildishev, kildisha@purdue.edu

†These authors contributed equally to this work.

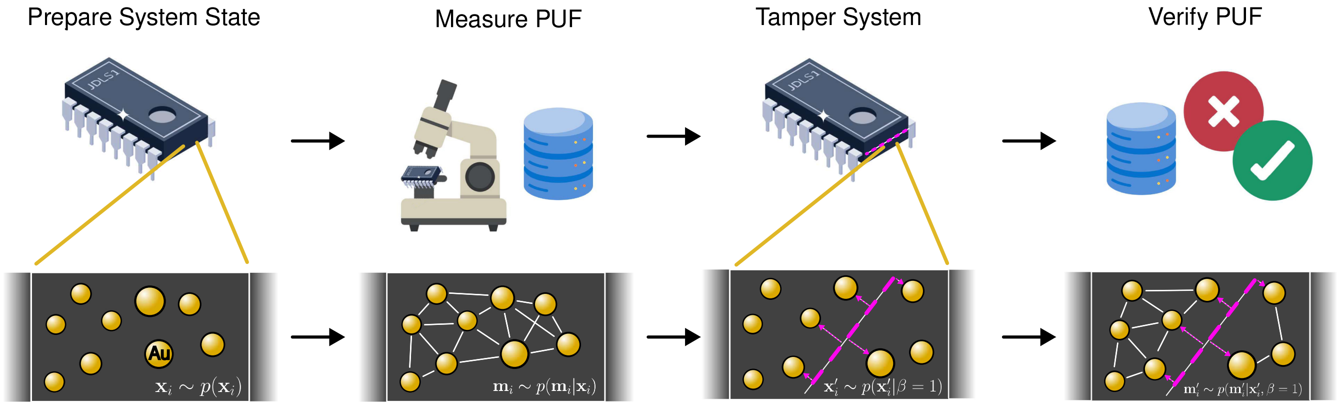
Prepare System State
Measure PUF
Tamper System
Verify PUF
JDLS1
JDLS1
Au
$\mathbf{x}_i \sim p(\mathbf{x}_i)$
$\mathbf{m}_i \sim p(\mathbf{m}_i|\mathbf{x}_i)$
$\mathbf{x}'_i \sim p(\mathbf{x}'_i|\beta = 1)$
$\mathbf{m}'_i \sim p(\mathbf{m}'_i|\mathbf{x}'_i, \beta = 1)$

**Fig. 1** PUF sampling process. An overview of the PUF tamper detection method using distance matrices of randomly positioned gold nanoparticles. The process consists of four primary stages. (i) Gold nanoparticles are randomly introduced, serving as a distinct physical system. (ii) The nanoparticles' distance matrix is recorded and archived in a reference database. (iii) The system may experience external tampering or natural degradation that can modify its initial state. (iv) The distance matrix is reassessed and cross-referenced with the initial database to identify any potential tampering or other changes.

nanoparticles with precise positions and radii, the distance matrix acts as the PUF signature. However, we demonstrate that current verification methods for distance matrix PUFs are neither sufficiently scalable nor robust enough for discriminating between natural disturbances and adversarial tampering. First, we take dark-field images of nanoparticles that are randomly distributed. The random positions and radii are extracted using semantic segmentation and labeled clustering. Then, the nanoparticles undergo treatment due to either natural degradation, e.g., minor thermal treatment and packaging abrasions, or adversarial tampering, e.g., substrate tearing, thermal tampering, and refilling. After the nanoparticles are exposed to either kind of treatment, the nanoparticle positions and radii are remeasured, and a new, posttampered distance matrix is compared against the pretampered distance matrices. Previous works use variations in the Hausdorff distance metric to classify pre- and posttampering detection. In addition to the Hausdorff metric, we also apply the Procrustes matrix distance and average-Hausdorff-distance metrics[21–30] as analytical, classical methods for discrimination.

However, under more difficult assumptions of adversarial tampering, both the Hausdorff and Procrustes metrics can be provably tampered with, as we show in Sec. 4. Addressing this gap, we present a novel deep-learning approach using residual, attention-based processing of tampered optical responses (RAPTOR),[31–33] showing marked improvements in both speed and accuracy under diverse adversarial tampering conditions.

Overall, the novelty of our approach is demonstrated as

(1) being the first method to apply an attention mechanism for PUFs authentication, using the nanoparticle radii as soft weights and the posttamper distance matrix as a value matrix;
(2) developing data set generation methods for gold nanoparticle PUFs for which there is no existing public data set;
(3) achieving high verification accuracy under difficult, real-world tampering schema using machine learning to verify the gold nanoparticle PUFs.

We begin by discussing the importance of optical PUFs for semiconductor authentication and then spotlight the challenges in current verification methods. We then introduce a statistical approach to overcoming these challenges by formalizing the problem of adversarial tampering detection. We conclude by providing accuracy and speed results for both the average distance analysis and RAPTOR.

## 2 Background

### 2.1 Physical Unclonable Functions

PUFs are distinctive physical systems characterized by a unique, irreplicable, physical fingerprint. PUFs yield a probability distribution over random measurements of a system that is practically unclonable due to current technology, economic factors, or time constraints. That is, given two random physical systems, the probability of obtaining the same distribution of measurements is extremely low. An adversary will attempt to replicate the physical system that yields the measurement distribution in order to spoof any detection schemes. The detection of adversarial tampering features introduced during the spoofing process is based on the following steps: (1) PUF system preparation, (2) pretamper measurements, (3) random tampering, and (4) posttampering adversarial detection. Previous works primarily implement this detection method using optical PUFs, which construct unique scattering and/or spectral responses of random media.[9,14] Optical PUFs are easy to fabricate and quick to measure, making them ideal for proof-of-concept experiments. Likewise, several other physical systems exhibit similar levels of randomness and measurability, including resonators,[17] laser-induced speckle patterns,[6] memristors,[10] memtransistors,[10] and intentional damaging in glass.[34] However, nanoscale metallic optical systems, otherwise known as plasmonic PUFs, have been rising in popularity due to their strong scattering response at optical wavelengths, increasing robustness during posttampering measurements. Among the early instances of plasmonic PUFs are responses from dichroic gold barcodes,[35] anisotropic gold nanoparticles grown within thin silicon dioxide films,[36] distinct surface plasmon resonance modes,[37] unique molecular configurations embedded in multilayer structures,[18,38] and 100 nm gold nanorods.[39] Nevertheless, while serving as viable PUF prototypes, these methods grapple with scalability challenges, either in fabrication or measurement robustness. To address these limitations, we reintroduce a streamlined, plasmonic PUF suitable for large-scale applications: the distance matrix verification of gold nanoparticles.[20] As we argue in Appendix A (Sec. 6.4), gold nanoparticles are sufficiently random during fabrication and can easily be measured using dark-field microscopy, a readily available technique that can integrate seamlessly into any stage of the semiconductor fabrication pipeline.

### 2.2 Distance Matrix PUFs

Figure 2 shows the distance matrix extraction process based on gold nanoparticle PUFs from dark-field images. The detailed segmentation process is found in Sec. 4.1 and Appendix A (Sec. 6.3). Distance matrix PUFs are given by the distance matrix $D$ constructed by all pairwise distances between nanoparticle positions. Let $d(\mathbf{r}_i, \mathbf{r}_j)$ be the Euclidean distance between nanoparticles $i$ and $j$, with positions $\mathbf{r}_i$ and $\mathbf{r}_j$, respectively; then the distance matrix elements $D_{ij}$ are defined as $D_{ij} \triangleq d(\mathbf{r}_i, \mathbf{r}_j)$. The merit of the distance matrix as a PUF lies in its symmetry properties: it is rotationally and translationally invariant, renormalizable, and simple enough for computer-vision measurements across varying fields of view and orientations. It is important to note that the use of distance matrix PUFs makes an implicit assumption that the probability of introducing random translations and rotations during measurement is much higher than that of fabricating two systems that are identical under a rotation and translation symmetry. This ensures that in-plane distance matrices are uniquely associated with their system state, barring unlikely rotational and translational symmetries introduced during fabrication. This motivates our use of distance matrices as reliable PUFs as we now introduce their analysis. Smith et al.[20] showed that the Hausdorff distance is robust in accounting for 5 $\mu$m translations as well as illumination discrepancies in the imaging process. In this study, we expanded the tests with a wider range of adversarial tampering through simulation by increasing the translation and rotation of the imaging lens, increasing the noise perturbations of the nanoparticle positions, and introducing adversarial tearing and refilling, as described in detail in Sec. 3.2.

## 3 Methods

Figure 3 presents our machine-learning-assisted authentication flowchart from fabrication to tampering detection. Consider a physical system state $\mathbf{x} \sim p(\mathbf{x})$ generated by a fabrication process $p(\mathbf{x})$. A PUF gives a distribution over measurements $\mathbf{m} \sim p(\mathbf{m}|\mathbf{x})$ of the system conditioned on the system state. After recording a set of measurements $\mathbf{M} = \{\mathbf{m}_0, \dots, \mathbf{m}_{|\mathbf{M}|-1}\}$, the system state $\mathbf{x}$ evolves to a new state $\mathbf{x}'$ via either an adversarial tampering process $\mathbf{x}' \sim q_a(\mathbf{x}'|\mathbf{x})$ or natural degradation process $\mathbf{x}' \sim q_n(\mathbf{x}'|\mathbf{x})$, e.g., natural thermal changes, packaging abrasions. An independent Bernoulli variable $\beta \sim \mathcal{B}$ chooses which of the two distributions produces the state evolution. The general tampering distribution $q(\mathbf{x}'|\mathbf{x}, \beta)$ is conditioned on the initial system state $\mathbf{x}$ and the tampering indicator $\beta$, i.e., $q(\mathbf{x}'|\mathbf{x}, \beta = 0) = q_n(\mathbf{x}'|\mathbf{x})$ and $q(\mathbf{x}'|\mathbf{x}, \beta = 1) = q_a(\mathbf{x}'|\mathbf{x})$. Once the system has undergone the chosen tampering, we record the posttampering measurements $\mathbf{m}' \sim p(\mathbf{m}'|\mathbf{x}')$ in a new database $\mathbf{M}' = \{\mathbf{m}'_0, \dots, \mathbf{m}'_{|\mathbf{M}'|-1}\}$. Using a discriminator function $\mathbf{Y}_\theta(\mathbf{m}, \mathbf{m}')$, with variational parameters $\theta$, we infer the tampering indicator $\beta$ to determine whether the system underwent a natural degradation process or the adversarial tampering process. Our objective function for detecting adversarial tampering is optimized by finding the optimal variational parameters $\theta$ for our discriminator function $\mathbf{Y}$, as

$$\arg\min_{\theta} \mathbb{E}_{\mathbf{x}\sim p(\mathbf{x})}[\mathbb{E}_{\substack{\beta\sim\mathcal{B} \\ \mathbf{m}\sim p(\mathbf{m}|\mathbf{x}) \\ \mathbf{m}'\sim p(\mathbf{m}'|\beta,\mathbf{x})}}[|\mathbf{Y}_\theta(\mathbf{m}, \mathbf{m}') - \beta|]], \tag{1}$$

where $p(\mathbf{m}'|\beta, \mathbf{x}) = \int p(\mathbf{m}'|\mathbf{x}')q(\mathbf{x}'|\mathbf{x}, \beta)\mathrm{d}\mathbf{x}'$ is the marginal distribution of the posttampering measurements $\mathbf{m}'$, given the initial system state $\mathbf{x}$ and tampering indicator $\beta$, which are baked into the expectation implicitly. We now apply this definition to distance matrix PUFs.

### 3.1 Nanoparticles for the PUF-D Problem

The gold nanoparticles are uniformly distributed on the substrate $\mathbf{r}_i \sim \mathcal{U}[0,1]^2$, but their radii are normally distributed $\rho_i \sim \mathcal{N}(\mu_r, \sigma_r)$, which yield a system state $\mathbf{x} = \{\mathbf{r}, \boldsymbol{\rho}\}$. Then, a database $\mathbf{M}$ of randomly positioned dark-field images is

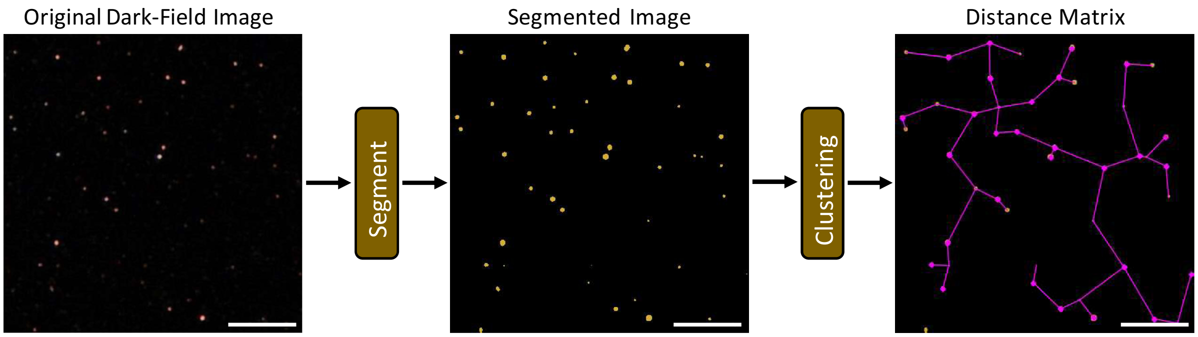

**Fig. 2** Distance matrix extraction from dark-field images. Nanoparticle dark-field images of size 448 × 448 pixels are prepared using dark-field microscopy. Then, the segmentation process classifies pixels as belonging to either a nanoparticle pattern or the dark-field background. Next, nanoparticle pattern pixel regions are clustered into local particle patterns, and their centers of mass (purple points) are extracted. Finally, the distance matrix is generated by evaluating all pairwise distances between these nanoparticle patterns. We visualize the distance matrix using its minimum spanning tree, despite the full tree being all-to-all. All scale bars represent 20 $\mu$m.

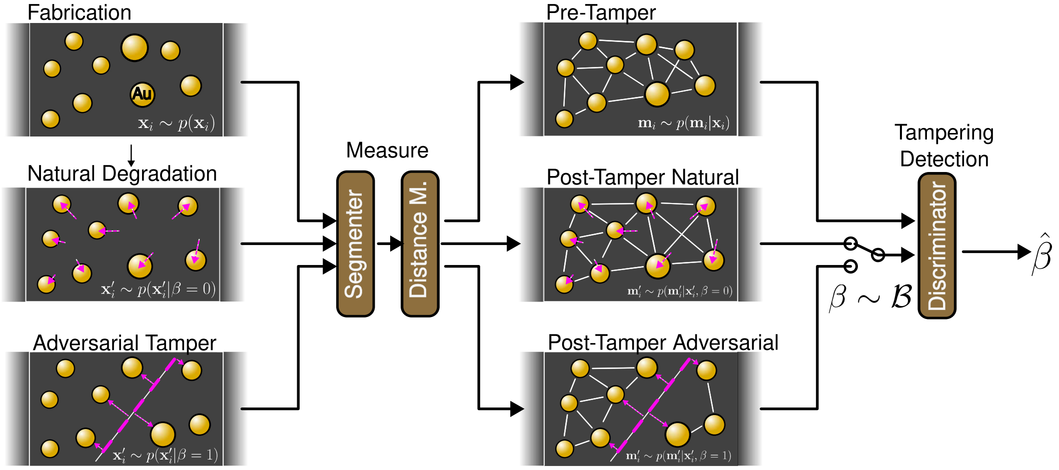
Fabrication
Au
$\mathbf{x}_i \sim p(\mathbf{x}_i)$
Natural Degradation
$\mathbf{x}'_i \sim p(\mathbf{x}'_i|\beta = 0)$
Adversarial Tamper
$\mathbf{x}'_i \sim p(\mathbf{x}'_i|\beta = 1)$
Measure
Segmenter
Distance M.
Pre-Tamper
$\mathbf{m}_i \sim p(\mathbf{m}_i|\mathbf{x}_i)$
Post-Tamper Natural
$\mathbf{m}'_i \sim p(\mathbf{m}'_i|\mathbf{x}'_i, \beta = 0)$
Post-Tamper Adversarial
$\mathbf{m}'_i \sim p(\mathbf{m}'_i|\mathbf{x}'_i, \beta = 1)$
Tampering Detection
$\beta \sim \mathcal{B}$
Discriminator
$\hat{\beta}$

**Fig. 3** Machine-learning-assisted authentication is trained by classifying synthetic posttamper measurements as being either adversarially tampered or naturally degraded, indicated by $\hat{\beta}$. We use a pretrained segmentation model, along with a labeled clustering algorithm, to compute the distance matrix and radii of the nanoparticles for both samples. Then, the discriminator network is trained by randomly choosing a synthetic tampering type according to the tampering Bernoulli distribution $\beta \sim \mathcal{B}$.

created through dark-field microscopy. Due to the extremely large number of samples taken during dark-field microscopy, the measurement density is highly correlated to the fabrication prior through a narrow Gaussian peak (Assuming dark-field microscopy is i.i.d. sampling, then the law of large numbers dictates the measurement will converge as ${\sigma_i}^2/n$ where $n$ is the number of measurements taken by the dark-field microscope on a single nanoparticle with variance ${\sigma_i}^2$.) and is approximately localized $p(\mathbf{m}|\mathbf{x}) \approx \delta(\mathbf{x} - \hat{\mathbf{x}}(\mathbf{m}))$, where $\hat{x}(\mathbf{m}) = \{\hat{\mathbf{r}}, \hat{\rho}\}$ is our approximation to the true system state $\mathbf{x} = \{\mathbf{r}, \rho\}$. Therefore, the problem objective in Eq. (1) can be approximated as

$$\mathbb{E}_{\mathbf{x}\sim p(\mathbf{x})}[\mathbb{E}_{\substack{\beta\sim\mathcal{B} \\ \mathbf{m}'\sim p(\mathbf{m}'|\beta)}}[|\mathbf{Y}_\theta(\mathbf{m}, \mathbf{m}') - \beta|]], \tag{2}$$

by marginalizing out $\mathbf{x}$ and $\mathbf{x}'$ from the inner expectations using the delta function. Taking the distance matrices of the inferred system state $\hat{\mathbf{x}}$ and the evolved system state $\mathbf{x}'$ yields a distance matrix objective function,

$$\mathbb{E}_{D(\mathbf{x})\sim p(\mathbf{x})}[\mathbb{E}_{\substack{\beta\sim\mathcal{B} \\ D(\hat{\mathbf{x}}(\mathbf{m}'))\sim p(\mathbf{m}'|\beta)}}[|\mathbf{Y}_\theta(D(\hat{\mathbf{x}}), D(\mathbf{x}')) - \beta|]], \tag{3}$$

where $\mathbf{Y}$ is now defined on the distance matrix space. (As mentioned previously, we assume here that the probability of introducing random translations and rotations during imaging is far less likely than that of producing the same distance matrix for two sets of nanoparticles.) This becomes our objective function for constructing RAPTOR. Now, we explicitly consider features of the tampering distribution $q$.

### 3.2 Adversarial Tampering

During the random tampering step, the system may undergo either natural changes given by $q_n$ or adversarial tampering given by $q_a$. Thermal fluctuations may occur for both treatments, and they introduce varying degrees of random Gaussian translations of the nanoparticles, i.e., $\mathbf{r}' = \mathbf{r} + \mathbf{r}_\Delta : \mathbf{r}_\Delta \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\sigma}_\Delta)$. However, adversarial tampering introduces Gaussian translations as well as substrate tearing and refilling, as shown in Fig. 4. Adversarial tearing introduces a random cut through the plane, displacing each nanoparticle location $\mathbf{r}_i$ by a magnitude of $\frac{w}{\sqrt{|\mathbf{r}_i - \boldsymbol{\alpha}_i|}}$, orthogonal to a cut vector $\boldsymbol{\alpha}$ weighted by a tearing coefficient $w$. As demonstrated in Fig. 4(c), introducing tears alters the average distance, thereby making adversarial tearing detectable by statistical discrimination. In the less ideal case, an adversary will attempt to refill the tear by introducing nanoparticles of a similar density as the fabrication density to recover similar features to the natural degradation. As shown in Fig. 4, filling the tear makes the average nanoparticle distance indistinguishable from natural degradation noise, with some constant distance. Therefore, a purely expected distance discrimination method between the tampering distributions $q_n$ and $q_a$ is completely unfeasible for small sample sizes under adversarial filling. Therefore, discrimination tasks necessitate conditioning on the measurements $\mathbf{M}$ and $\mathbf{M}'$.

### 3.3 Distance Matrix Authentication

Three analytical distance metrics are explored for distance matrix authentication: Hausdorff distance, Procrustes distance, and the average Hausdorff distance (AHD). For each of these metrics, the binary classification threshold is determined via logistic regression. If the distance between two matrices is above the logistic threshold, the posttamper matrix is considered too dissimilar to arise from the environment or natural degradation. Otherwise, the matrix is considered to have an acceptable level of natural changes and is therefore authentic.

#### 3.3.1 Hausdorff metric

The Hausdorff distance metric $H$ is the maximum Euclidean distance $d(\mathbf{r}_i, \mathbf{r}'_j)$ between each point $\mathbf{r}_i$ and its nearest neighbor $\mathbf{r}'_j$ as shown in Eq. (4). (Using the distance matrix elements $D$ and $D'$ instead of $\mathbf{r}$ and $\mathbf{r}'$ does not yield significant differences in results for our purposes.)

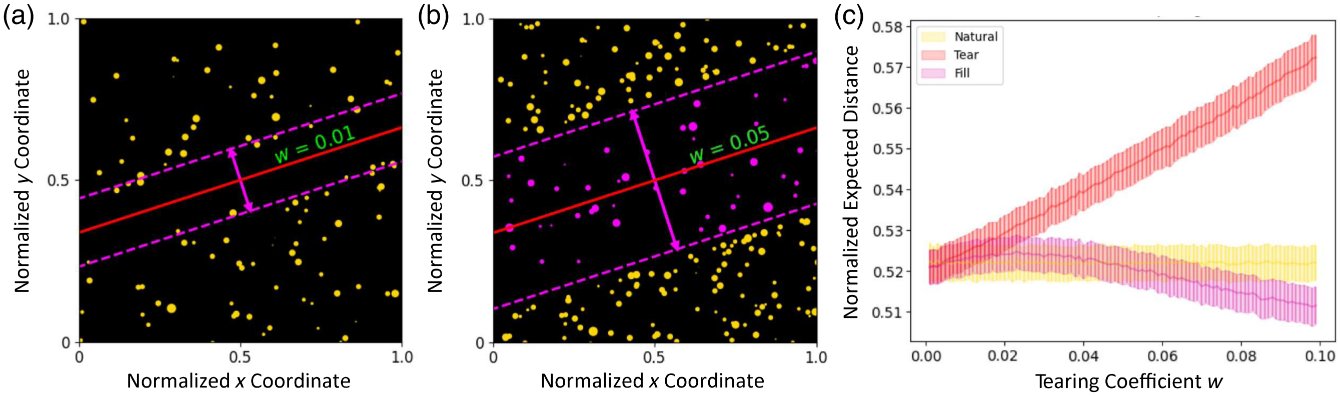

**Fig. 4** Adversarial tampering is introduced through tearing of the substrate, thereby separating the gold nanoparticles according to their distance from the tear line, and filling the tear with new nanoparticles uniformly distributed in the tear to match the original distribution. The tearing of the substrate is modeled as a random cut that shifts the nanoparticles based on the inverse square root of the perpendicular distance to the cut. (a), (b) The tearing coefficients $w = 0.01$ and $w = 0.05$ demonstrate the increased separation dependent on the tearing coefficient. (c) The normalized expected distance between nanoparticles is plotted for natural degradation, adversarial tearing without filling, and adversarial tearing with filling.

$$H(\mathbf{r},\mathbf{r}') = \max_{\forall\,\mathbf{r}_i\in\mathbf{r}}[\min_{\forall\,r'_j\in\mathbf{r}'} d(\mathbf{r}_i,\mathbf{r}'_j)]. \tag{4}$$

### 3.3.2 Procrustes metric

An alignment matrix is a matrix that aligns two sets of multivariate data by transforming one into the other. Procrustes analysis is a statistical method that finds the optimal alignment matrix $A$ that minimizes the sum of squared distances between corresponding points in $A\mathbf{r}$ and $\mathbf{r}'$, thus accounting for rotational, translational, and scaling discrepancies.[40] Procrustes distance $P$ is then given by the sum,

$$P(\mathbf{r},\mathbf{r}') = \sum_{\mathbf{r}_i\in\mathbf{r}} d(A\mathbf{r}_i,\mathbf{r}'_i)^2. \tag{5}$$

Ordering and data set size constraints make Procrustes a less reliable method for distance matrix matching. Likewise, finding the optimal alignment matrix is an iterative and time-consuming process compared to Hausdorff.

### 3.3.3 Average Hausdorff distance metric

An average-nearest-neighbor approach offers a more robust solution in practice than the Hausdorff and Procrustes metrics. Rather than simply considering the maximum nearest neighbor, it considers all nearest neighbors and is thus less sensitive to slight changes in any single nanoparticle position.[21] The AHD is defined as

$$\mathrm{AHD}(\mathbf{r},\mathbf{r}') = \frac{1}{|\mathbf{r}|}\sum_{\forall\,\mathbf{r}_i\in\mathbf{r}}[\min_{\forall\,\mathbf{r}'_j\in\mathbf{r}'} d(\mathbf{r}_i,\mathbf{r}'_j)]. \tag{6}$$

Despite the previously reported 100% accuracy of distance matrix verification schemes involving a Hausdorff-inspired metric similar to AHD,[20] we demonstrate in Sec. 4.2 that under more difficult adversarial tampering conditions, AHD eclipses both Hausdorff and Procrustes metrics, but is still beaten by RAPTOR.

## 3.4 RAPTOR

RAPTOR (Fig. 5) takes a more supervised approach to compute the authenticity of a distance matrix. For each nanoparticle $i$, we reweight the posttamper matrix $D'$ by a soft-weight matrix $A^i$ to indicate the probability that nanoparticle $i$ in the pretamper matrix $D$ is nanoparticle $j$ in the posttamper matrix $D'$ [Fig. 5(a)]. Let $\Gamma_i = [\ldots, |\rho_i - \rho'_j|, \ldots]$ be the query row tensor; then for each nanoparticle $i$, we compute the soft-weight $S^i_j = \mathrm{softmax}(\Gamma_i/\tau_i)$ where $\tau_i$ is a variational parameter. Then, we multiply each row $\mu$ of the value matrix $D'$ by the soft-weight $S^i_\mu$, thereby creating a unique attention distance matrix $A^i$ for each nanoparticle $i$, i.e.,

$$A^i_{\mu\nu} = S^i_\mu D'_{\mu\nu}. \tag{7}$$

This mechanism zeroes out rows in the posttamper matrix $D'$, whose nanoparticles are unlikely to be the same before and after tampering based on the difference in radii. Then, using the pretamper distance matrix $D$, we compute the probability that nanoparticle $i$ is the same as nanoparticle $j$, defining the matrix elements $B_{ij}$, by first encoding all pairwise rows between both matrices using a 3D ResNet encoder model $f_\theta(A^i, D)$ to compute the element $B_{ij}$ in Fig. 5(b). The feature matrix $B$ along with $\Gamma$, $D$, $D'$, and $S^i$ are concatenated along the channel dimension and fed into the residual attention-based classifier shown in Fig. 5(c). An algorithmic description of RAPTOR is included in Appendix B (Sec. 7.1).

# 4 Results and Discussion

## 4.1 Semantic Segmentation

To reliably extract the nanoparticle centers and radii, we employ semantic segmentation networks to separate the image into two classes: nanoparticle and dark-field background. First, we trained the unsupervised semantic segmentation network STEGO as ground-truth labels for a data set of 10,000 dark-field images.[41] We chose STEGO due to its prominence in

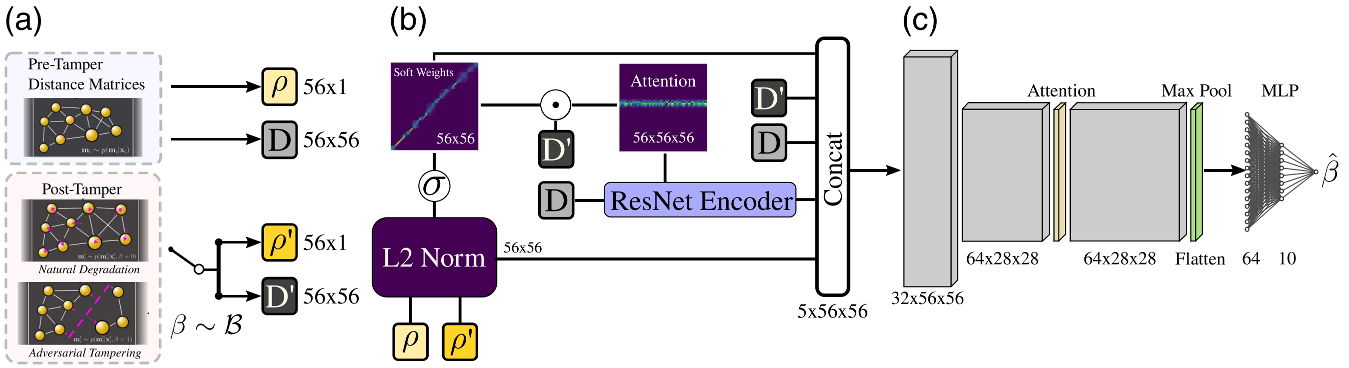

**Fig. 5** RAPTOR uses an attention mechanism for prioritizing nanoparticle correlations across pretamper and posttamper samples before passing them into a residual, attention-based deep convolutional classifier. (a) RAPTOR takes the top 56 nanoparticles in descending order of radii to construct the distance matrices $D$ and $D'$ and radii $\rho$ and $\rho'$ from the pretamper and posttamper samples. (b) The radii and distance matrices form the query and value embeddings of an attention mechanism. The attention mechanism is then used alongside the raw distance matrices $D'$ and $D$, the soft weight matrix, and $L_2$ matrix generated from the radii vectors for the classifier. (c) The classifier uses GELU activation and attention layers before applying a kernel layer and max pool layer. Then, the output is flattened into a multilayer perceptron to compute the final classification $\hat{\beta}$.

the literature in assigning meaningful and high-quality segmentation to unlabeled data. The training data set for STEGO is created by randomly selecting and positioning gold nanoparticles obtained from a data set of 2400 gold nanoparticles extracted from 40 dark-field images. Particle extraction is performed via brightness thresholding at 4% intensity, followed by regional clustering and is manually verified for each input image. A minimum pattern radius of 0.5 $\mu$m is enforced to discern the particles from noise. From this data set, samples of transformed particles are generated to match the source distributions of on average 79 particles per image ($\sigma = 20$) and source dimensions ($1280 \times 960$ pixels at 0.069 $\mu$m/pixel), thus creating an augmented data set that is visually indistinguishable from source images. We injected 4% intensity Gaussian noise to match realistic noise levels from the dark-field images data set. The particle density is uniform across samples as discussed in Appendix A (Sec. 6.4). We list detailed explanations for choosing the parameter values mentioned in Appendix A (Sec. 6.5).

STEGO is very powerful but slow for simple semantic segmentation. Hence, we train both a lightweight ResNet-based attention convolutional neural network and a Gaussian blurring filter for mimicking STEGO. Overall, as demonstrated in Table 1, our CNN model and Gaussian filters achieve binary cross-entropy losses of $10^{-3}$ and 0.56 and compute 1000 images in 27 and 33 ms on a T4 GPU, as opposed to 24 min for 1000 images using STEGO. After computing the semantic segmentation labels, all images are fed into a labeled clustering algorithm that extracts the center of mass and radii of 1000 images in 250 ms.

### 4.2 Tampering Discrimination

The tampering data set is generated synthetically at run-time offline from semantic segmentation. A substrate of size $2 \times 2$ is filled uniformly with a nanoparticle density of 100 per unit square, and the radii are normally sampled i.i.d. $\rho_i \sim \mathcal{N}(\mu_\rho = 0.006, \sigma_\rho = 0.004)$. Natural degradation is introduced through a simple displacement of nanoparticles by a factor $0.05 \cdot \mathbf{r}_\Delta$ using the r.v. $r^{x,i}_\Delta, r^{y,i}_\Delta \sim \mathcal{N}(\mu_n = 0, \sigma_n = 1)$. For adversarial tampering, a tampering configuration is chosen at

**Table 1** Overall performance comparison of each method for distance matrix extraction and discrimination tasks. For all results in the table, a 1000-sample tensor was loaded onto an NVIDIA T4 GPU (except Procrustes, which used all CPU RAM) and batched at maximum capacity for the particular model. Accuracy is measured by the number of correct pixels or authentication classifications over the total. For semantic segmentation, we include the BCE loss to show a marginal advantage in using ResNet over Gaussian blur. The computation time is measured by preloading all data onto an NVIDIA T4 GPU or CPU RAM before recording the start time.

| Task | Method | Average Accuracy (%) | Computation Time |
|---|---|---|---|
| Distance matrix extraction | STEGO | 100% (ground truth) | 24 min for 1000 images |
| | ResNet attention CNN | $10^{-3}$ (BCE) or 99% | 27 ms for 1000 images |
| | Gaussian blur | 0.56 (BCE) or 99% | 33 ms for 1000 images |
| Discrimination | RAPTOR | 97.6% | 80 ms for 1000 matrices |
| | AHD | 91.2% | 13.5 ms for 1000 matrices |
| | Hausdorff | 54.9% | 22.9 ms for 1000 matrices |
| | Procrustes | 58.2% | 3.30 s for 1000 matrices |

random using the following scheme. For adversarial displacement noise, we multiply the noise r.v. by a random coefficient, i.e., $c_a \cdot \mathbf{r}_\Delta$, where $c_a \in \{0.035, 0.04, 0.05, \ldots, 0.1\}$ is chosen uniformly. The tear coefficient $w \in \{0.01, 0.03, 0.05\}$ is also chosen uniformly. Tampering data are generated under harsher conditions than the expected imaging conditions to show robustness. Note that the tampered data are produced in the same manner as training data, with an additional tampering step. Finally, to test the imaging robustness, we randomly decide to rotate all nanoparticles about the center by a uniformly chosen angle. We also apply a constant translation in a randomly uniform direction with translation coefficients in $\{0, 0.01, \ldots, 0.12\}$. After applying the randomly chosen tampering configuration, all nanoparticles within the center unit square are sorted in descending order of radii, and their associated distance matrix and radii are extracted for authentication. RAPTOR is trained to discriminate tampering under eight different noise levels, causing random particle movements of up to 10% image width from a pessimistic 5% natural degradation level. The adversarial filling is performed under worst-scenario conditions in which filling precisely matches perforation boundaries while matching initial particle density. RAPTOR is trained in batches of 100 images, on information from the 56 largest radii particle patterns in each image, with a learning rate of 0.01. During training, RAPTOR is compared to analytical methods: Hausdorff, Procrustes, and AHD. For all analytical methods, the output distance metric is fit to a logistic regression model for determining authenticity.

Table 1 shows the average accuracy and computation times of RAPTOR alongside the analytical methods. RAPTOR has the highest average accuracy, correctly detecting tampering in 97.6% of distance matrices under worst-case-scenario tampering assumptions and exceeding the performance of the Hausdorff, Procrustes, and AHD methods by 40.6%, 37.3%, and 6.4%, respectively. The AHD has the fastest computation time in discrimination tasks and the highest accuracy among the three analytical methods.

## 5 Conclusion

In this work, we demonstrate the robustness of a new RAPTOR for the authentication of semiconductor devices, using random pattern arrays of gold nanoparticles as distance-matrix-based optical PUFs. The arrays are imaged using dark-field microscopy, and the positions and radii of individual particle patterns are extracted using semantic segmentation and labeled clustering. We introduce difficult, yet realistic, adversarial tampering features through tearing and substrate refilling, or natural deviations through thermal noise with varying levels of substrate heating. We demonstrate that RAPTOR achieves a tampering accuracy of 97.6%, greatly outperforming the Hausdorff, Procrustes, and AHD distance metrics by 40.6%, 37.3%, and 6.4%, respectively. These results indicate that RAPTOR significantly outperforms known classical distance matrix metric methods for authenticating PUFs built on the random arrays of gold nanoparticles in accuracy and speed.

The ease of fabrication of gold nanoparticles, along with rapid and robust tampering detection with RAPTOR, opens up a large opportunity for the adoption of machine-learning-based tampering detection schemes in the semiconductor industry. However, more work is required in material development to ensure that these methods are robust to unforeseen types of tampering and natural degradation. Furthermore, hyperparameter optimization and alternative deep networks may improve the speed or accuracy of RAPTOR. While our scheme greatly improves on the core bottlenecks found in these verification schemes, future work could consider the computation of the distance matrices directly without labeled clustering, or a full end-to-end network that does not use semantic segmentation as an intermediate step in the verification process.

## 6 Appendix A: PUFs and Data Set

### 6.1 Nanoparticle PUFs Fabrication

A diluted nanoparticle suspension (1 $\mu$L) of 75 nm Au (1 $\mu$L) (nanoComposix, Inc.) in deionized (DI) nanopure water (2 mL) is drop cast onto the precleaned silicon substrate, which is prepared by standard solvent cleaning [placed substrate within toluene, acetone, and iso-propyl alcohol (IPA) in three separate steps, with 5 min sonication at each step] and piranha cleaning [placed substrate in 3:1 volume ratio concentrated sulfuric acid ($H_2SO_4$) and hydrogen peroxide ($H_2O_2$) for 15 min] in a controlled cleanroom environment. Then, the sample is placed horizontally to let the liquid evaporate naturally to leave the gold nanoparticle pattern on the substrate.

### 6.2 Optical Imaging

The dark-field optical imaging system consists of a Keyence VHX-6000 digital microscope with a high-brightness LED light source, a 1/1.8-in. CMOS image sensor with virtual pixels 1600 ($H$) × 1200 ($V$) maximum, a ZS-200 RZ×200-×2000 objective lens with a fine adjustment for working distance, and a color LCD monitor with 16,770,000 colors and a 1000:1 contrast ratio. The dark-field images are taken at 1500× magnification to form the training data set for semantic segmentation and verify the uniformity of the formed PUFs prior.

### 6.3 Synthetic Dark-Field Image Dataset Generation and Segmentation

We built a data set of 10,000 images by augmenting 40 dark-field images. Over 2400 nanoparticle bounding boxes are extracted from 40 source images via connectivity-based clustering of thresholded image segments. Augmented images are generated by randomly placing nanoparticles from the set of bounding boxes in uniformly distributed positions. To ensure maximal variability in the augmented data set, we apply random rotation, shear, and additive noise transformations to each particle before placement. Due to the resolution of the dark-field microscope, we only consider nanoparticle scattering patterns with radii greater than 0.5 $\mu$m, as any smaller patterns cannot be verified to be gold nanoparticles. Gaussian noise is injected into the background to further mimic the original images, effectively reintroducing nanoparticles with average radii less than 0.5 $\mu$m to the augmented data set.

A ResNet-based convolutional neural network and a Gaussian filter are demonstrated to accurately segment 1000 dark-field images in only 27 and 33 ms, respectively. Each of these methods achieves 99% segmentation accuracy, greatly outperforming the classical methods and the ground truth unsupervised segmentation network STEGO in speed with negligible error in accuracy. (It takes 24 min for STEGO to segment 1000 images.) These segmented images are postprocessed for reliable position and radii extraction using labeled clustering.

### 6.4 Uniformity of PUFs

For a normalized uniform distribution, the expected distance between any two points is given exactly by[42] $\frac{1}{15}[2+\sqrt{2}+5\,\log(1+\sqrt{2}] \approx 0.521405$. To test the uniformity of the nanoparticle placements, we took 40 dark-field images of randomly embedded nanoparticles on the substrate and measured the expected distance between any two nanoparticles to be 0.521318, which has an error of 0.017%.

### 6.5 Parameters Choices

Our study provides a research-oriented example to demonstrate a comprehensive feasibility study. Forming an optimal or adaptive threshold for the following parameters may require additional study with auxiliary training and analysis, especially for industry-level systems.

- 2400 gold particles: The dark-field image data set must be augmented to contain maximally varied nanoparticles resembling a wide variety of real-life conditions. Also, for noninteracting scatterers, when we have a sufficiently large number of scatterers, we could apply statistical or average properties reliably in statistical mechanics and condensed matter physics.[43] To this end, we sample from 2400 nanoparticles that were extracted from an original data set of 20 dark-field images. Extracted nanoparticles were additionally transformed (rotations and shear transformations) to maximize the diversity of segmentation shapes. We found this level of variety to be sufficient to demonstrate the dexterity of tested segmentation techniques after experiments.
- 4% intensity brightness threshold: The original data set nanoparticle extraction was manually verified. A 4% brightness magnitude threshold was chosen for our specific imaging procedure. As stated above, an optimal or adaptive threshold may require additional study. For STEGO and attention CNN segmentation methods, brightness thresholding is not used. For Gaussian blur-based segmentation, a brightness threshold can be manually chosen to match imaging conditions or optimized to match the semantics of the former methods.
- Minimum pattern radius of 0.5 $\mu$m: The 0.5 $\mu$m minimal radius was enforced for the original data set creation to discern the particles from noise, since it was a typical gold nanoparticle scattering pattern radii distribution observed during the fabrication of samples and optical characterization of dark-field images. Here, we assume that particles are noninteracting. Otherwise, the scattering pattern may reach substantially larger radii. During verification, this minimal radius would be implicitly learned and optimized by the chosen segmentation method.
- 79 particles per image ($\sigma = 20$) and source dimensions ($1280 \times 960$ pixels at 0.069 $\mu$m/pixel): Particle density is a function of molecular interaction of gold nanoparticles as well as other fabrication parameters and is chosen to reflect densities seen in the original dark-field images (this density is uniform and consistent across samples, as described in Section 6.4). Image dimensions are arbitrary with respect to segmentation and are chosen simply to reflect typical imaging parameters.
- $2 \times 2$ size substrate filled with a nanoparticle density of 100 per unit square: A $2 \times 2$ frame was filled with nanoparticles so that a randomly placed $1 \times 1$ canvas of nanoparticles could be "imaged" out of a larger set. This approach simulated framing imprecision in real-world substrate imaging and allowed us to determine which methods were robust against that translational framing error. Nanoparticle density is relevant to tamper detection, since the number of nanoparticles within a unit frame determines the amount of information available to discrimination algorithms. We chose 100 to match dark-field image nanoparticle density upon sampling of a $960 \times 960$ pixels square subset from a $1280 \times 960$ pixels image.
- Natural degradation is introduced through a simple displacement of nanoparticles by a factor of 0.05: To mimic the extreme physical tampering behavior, we chose to translate particles up to 5% image width to reflect a worse-than-expected case scenario of PUF degradations. However, this number could be changed depending on the real-life packaging degradation measured for a particular packaging type.

## 7 Appendix B: Authentication Methods

### 7.1 RAPTOR Algorithmic Overview

*Inputs*:

- Pre-/posttamper nanoparticle distance matrices: $D$, $D'$ ($k \times k$ tensors)
- Pre-/posttamper nanoparticle radii: $\rho$, $\rho'$ ($k \times 1$ vectors)

*RAPTOR:*

- $L_2 \leftarrow L_2$ normalization of Euclidean distances between elements of particle radii vectors $\rho$, $\rho'$
- Soft weights ← Softmax of $L_2$ matrix divided by a trained parameter.
- Attention matrix: $A \leftarrow k \times k$ attention matrices for all nanoparticles encoding predicted particle correspondence between pre-/posttamper systems
- ResNet encoded particle correspondence: $B \leftarrow$ trained ResNet($A$, $D$)
- ResNet classifier: residual/attention blocks and a fully connected layer

*Outputs:*

- Likelihood of adversarial tampering during transit: $\hat{B}$

### 7.2 Analytical Methods

We introduce statistical authentication methods using Hausdorff, Procrustes, and AHD metrics and benchmark their performance in authenticating distance matrices extracted from dark-field images. All learning is performed in the same Jupyter environment on an NVIDIA T4 GPU with 16 GB of GPU RAM and an Intel(R) Xeon(R) CPU running at 2.30 GHz with 12.7 GB of system RAM. Each discrimination model is trained for 5000 epochs with a mini-batch of 100 random graph instances with random tampering, as discussed in Sec. 4.2. Training graphs are randomly generated at training time to prevent overfitting. Our validation step measures the average accuracy across the most recent 500 epochs. Reported accuracy is the maximum accuracy achieved by each discrimination method during the validation step.

### 7.3 Alternative Deep-Learning Networks

In an attempt to compare against other deep-learning methods, we used the same data fed into RAPTOR with different networks. We tried deep feed-forward multilayer perceptron networks, Siamese graph encoder networks, and deep residual convolutional layers. However, these were not able to consistently outperform the AHD, achieving accuracies below 70%. We also attempted to use the AHD metric as a resource for these networks, but these networks relied too heavily on the metric and converged to the same performance with minimal improvements below RAPTOR.

## Disclosures

The authors declare no competing interests.

## Code and Data Availability

The codes that support the findings of this article are not publicly available due to ongoing IP protection and licensing. The initial training data sets can be requested from the author at wilso692@purdue.edu.

### Acknowledgments

This work was supported in part by the U.S. Department of Energy (DOE) Office of Science, through the Quantum Science Center (QSC), the National Quantum Information Science Research Center (algorithm development), the National Science Foundation (NSF), and Purdue's Elmore ECE Emerging Frontiers Center "The Crossroads of Quantum and AI."

### References

1. K. S. Kumar et al., "Secure split test techniques to prevent IC piracy for IoT devices," *Integration* **58**, 390–400 (2017).
2. "Counterfeit chips a problem as global shortage increases semiconductor fraud," ASM International, 2022, https://www.asminternational.org/news/industry/-/journal_content/56/10180/49218564/NEWS/ (accessed 28 March 2024).
3. P. Karazuba, "Combating counterfeit chips," Semiconductor Engineering, 2020, https://semiengineering.com/combating-counterfeit-chips/ (accessed 28 March 2024).
4. U. Guin et al., "Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain," *Proc. IEEE* **102**(8), 1207–1228 (2014).
5. B. Wilson et al., "Empowering quantum 2.0 devices and approaches with machine learning," in *Quantum 2.0 Conf. and Exhibit.*, p. QTu2A.13 (2022).
6. K. Kim et al., "Massively parallel ultrafast random bit generation with a chip-scale laser," *Science* **371**(6532), 948–952 (2021).
7. Y. Yao et al., "Clockpuf: physical unclonable functions based on clock networks," in *Design, Autom. & Test in Eur. Conf. & Exhibit. 2013*, pp. 422–427 (2013).
8. M. Song et al., "Colors with plasmonic nanostructures: a full-spectrum review," *Appl. Phys. Rev.* **6**, 041308 (2019).
9. M. Song et al., "Enabling optical steganography, data storage, and encryption with plasmonic colors," *Laser Photonics Rev.* **15**, 2000343 (2021).
10. B. Liu et al., "Memristive true random number generator with intrinsic two-dimensional physical unclonable function," *ACS Appl. Electron. Mater.* **5**(2), 714–720 (2023).
11. A. Oberoi et al., "Secure electronics enabled by atomically thin and photosensitive two-dimensional memtransistors," *ACS Nano* **15**(12), 19815–19827 (2021).
12. P. Ebenezer, "Counterfeit mitigation with PUF-embedded readout," in *Govt. Microelectron. Appl. and Crit. Technol. Conf.* (2020).
13. U. Rührmair, S. Devadas, and F. Koushanfar, Chap. 4 in *Introduction to Hardware Security and Trust*, Springer Science Business Media (2012).
14. R. Pappu et al., "Physical one-way functions," *Science* **297**(5589), 2026–2030 (2002).
15. B. Gassend et al., "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. and Commun. Secur.*, pp. 148–160 (2002).
16. R. Maes, *Physically Unclonable Functions*, pp. 49–80, Springer Berlin, Heidelberg (2013).
17. J. Knechtel et al., "Toward physically unclonable functions from plasmonics-enhanced silicon disc resonators," *J. Lightwave Technol.* **37**(15), 3805–3814 (2019).
18. Y. Cui et al., "Multiplex plasmonic anti-counterfeiting security labels based on surface-enhanced Raman scattering," *Chem. Commun.* **51**(25), 5363–5366 (2015).
19. L. P. de Souza et al., "Influence of annealing temperature and SN doping on the optical properties of hematite thin films determined by spectroscopic ellipsometry," *J. Appl. Phys.* **119**, 245104 (2016).
20. A. F. Smith, P. Patton, and S. E. Skrabalak, "Plasmonic nanoparticles as a physically unclonable function for responsive anti-counterfeit nanofingerprints," *Adv. Funct. Mater.* **26**(9), 1315–1321 (2016).
21. O. U. Aydin et al., "On the usage of average Hausdorff distance for segmentation performance assessment: hidden error when used for ranking," *Eur. Radiol. Exp.* **5**(1), 4 (2021).
22. E. A. AlBadawy, A. Saha, and M. A. Mazurowski, "Deep learning for segmentation of brain tumors: impact of cross-institutional training and testing," *Med. Phys.* **45**(3), 1150–1158 (2018).
23. M. Livne et al., "A U-Net deep learning framework for high performance vessel segmentation in patients with cerebrovascular disease," *Front. Neurosci.* **13**, 97 (2019).
24. A. Hilbert et al., "Brave-Net: fully automated arterial brain vessel segmentation in patients with cerebrovascular disease," *Front. Artif. Intell.* **3**, 552258 (2020).
25. K. A. Powell et al., "Atlas-based segmentation of temporal bone anatomy," *Int. J. Comput. Assist. Radiol. Surg.* **12**(11), 1937–1944 (2017).
26. J. Guenette et al., "MR imaging of the extracranial facial nerve with the CISS sequence," *Am. J. Neuroradiol.* **40**(11), 1954–1959 (2019).
27. B. Peltenburg et al., "PO-0899: tumor volume delineation using non-EPI diffusion weighted MRI and FDG-pet in head-and-neck patients," *Radiother. Oncol.* **123**, S496–S497 (2017).
28. F. Rizzetto et al., "Impact of inter-reader contouring variability on textural radiomics of colorectal liver metastases," *Eur. Radiol. Exp.* **4**(1), 62 (2020).
29. M. R. Liechti et al., "Manual prostate cancer segmentation in MRI: interreader agreement and volumetric correlation with transperineal template core needle biopsy," *Eur. Radiol.* **30**(9), 4806–4815 (2020).
30. C. Chen et al., "Tracking pylorus in ultrasonic image sequences with edge-based optical flow," *IEEE Trans. Med. Imaging* **31**(3), 843–855 (2012).
31. A. Vaswani et al., "Attention is all you need," in *Adv. Neural Inf. Process. Syst. 30* (2017).
32. I. Malkiel et al., "Plasmonic nanostructure design and characterization via deep learning," *Light Sci. Appl.* **7**, 60 (2018).
33. L. Mascaretti et al., "Designing metasurfaces for efficient solar energy conversion," *ACS Photonics* **10**(12), 4079–4103 (2023).
34. A. P. Vladimirov et al., "Assessing fatigue damage in organic glass using optical methods," *Opt. Spectrosc.* **127**, 943–953 (2019).

35. L. Gonzalez-García et al., "Tuning dichroic plasmon resonance modes of gold nanoparticles in optical thin films," *Adv. Funct. Mater.* **23**, 1655–1663 (2012).
36. M. M. Hawkeye and M. J. Brett, "Glancing angle deposition: fabrication, properties, and applications of micro- and nanostructured thin films," *J. Vac. Sci. Technol. A* **25**(5), 1317–1335 (2007).
37. E. Hutter and J. H. Fendler, "Exploitation of localized surface plasmon resonance," *Adv. Mater.* **16**, 1685–1706 (2004).
38. J. Langer et al., "Present and future of surface-enhanced Raman scattering," *ACS Nano* **14**(1), 28–117 (2020).
39. C. Kuemin et al., "Oriented assembly of gold nanorods on the single-particle level," *Adv. Funct. Mater.* **22**, 702–708 (2011).
40. C. Goodall, "Procrustes methods in the statistical analysis of shape," *J. R. Stat. Soc.: Ser. B (Methodol.)* **53**, 285–321 (1991).
41. M. Hamilton et al., "Unsupervised semantic segmentation by distilling feature correspondences," in *Int. Conf. Learn. Represent.* (2022).
42. B. Burgstaller and F. Pillichshammer, "The average distance between two points," *Bull. Am. Math. Soc.* **80**(3), 353–359 (2009).
43. R. Pathria and P. D. Beale, *Statistical Mechanics*, Elsevier Ltd. (2011).

**Blake A. Wilson** earned his PhD at Purdue University in Electrical and Computer Engineering. He now works as a Research Scientist at Quantinuum, UK, working on generative AI, categorical machine learning and quantum algorithms.

**Yuheng Chen** is a third-year PhD student at the Elmore Family School of Electrical and Computer Engineering, Purdue University. His research focuses on the meeting point of AI, physics, and nanodevices, including AI-driven inverse design in photonic/quantum devices, generative machine learning model application exploration, and photonic/quantum devices electromagnetic simulation.

**Daksh Kumar Singh** is an undergraduate research assistant pursuing an integrated bachelors and masters in electrical and computer engineering at Purdue University. Currently focused on enhancing nanofabrication, characterization, and data analysis techniques through quantum algorithms and machine learning.

**Rohan Ojha** is an undergraduate electrical engineering student at Purdue University, specializing in microelectronics/semiconductors and quantum technology. At Purdue's Quantum Science and Engineering Institute, he researches machine learning applications in photonics. He interned at Sandia National Laboratories working in quantum error correction. He plans to pursue a PhD in quantum technology.

**Jaxon Pottle:** Biography is not available.

**Michael Bezick** is a rising junior undergraduate research assistant in computer science at Purdue University, with a passion for machine learning. He focuses on applications of generative models, such as variational autoencoders and diffusion models, to nanophotonic optimization problems. He plans to pursue a PhD in machine learning to contribute to the advancement of the field and further apply himself in industry post-graduation.

**Alexandra Boltasseva** received her PhD from the Technical University of Denmark and is currently the Ron and Dotty Garvin Tonjes Distinguished Professor of Electrical and Computer Engineering at Purdue University where she specializes in nanophotonics, optical metamaterials, and quantum photonics. As Purdue's Discovery Park fellow, she leads the university-wide multidisciplinary Big Idea Challenge program in quantum information science and technology/security/health. She was editor-in-chief of the Optical Society of America's *Optical Materials Express* journal.

**Vladimir M. Shalaev**, scientific director for nanophotonics at Birck Nanotechnology Center and distinguished professor of electrical and computer engineering at Purdue University, specializes in nanophotonics, plasmonics, optical metamaterials, and quantum photonics. He has received numerous awards, including APS Frank Isakson Prize, Max Born Award, etc. He is recognized as a highly cited researcher in physics by the Web of Science 2017–2023. He is a fellow of the IEEE, APS, SPIE, MRS, and Optica.

**Alexander V. Kildishev** is renowned for his groundbreaking work in optical metamaterials and transformation optics that spans theoretical concepts, advanced numerical modeling, and experimental guidance. His research has enabled superlenses, hyperlenses, and optical black holes. His recent work focuses on advanced multiphysics modeling in nonlinear optics and AI-driven inverse design in photonics. Beyond other awards, was listed as a highly cited researcher by the Web of Science in 2018, 2022, and 2023.