Research Article

ADVANCED PHOTONICS NEXUS

Scalable plasmonic physical unclonable functions empowered by a multi-dimensional expanding strategy

Juntao Duan,[a,†] Guoqun Li,[b,†] Yizhe Xiong,[a] Xiangnan Zhu,[b] Yan Chen,[c] Wei Liu,[a,d] Xiaochuan Xu,[a,d] Perry Ping Shum,[e,*] Qi Hao,[b,*] and Jiawei Wang[a,d,*]

[a]Harbin Institute of Technology (Shenzhen), School of Integrated Circuits, Shenzhen, China
[b]Southeast University, Key Laboratory of Quantum Materials and Devices of Ministry of Education, School of Physics, Nanjing, China
[c]National University of Defense Technology, College of Advanced Interdisciplinary Studies, Changsha, China
[d]Harbin Institute of Technology, National Key Laboratory of Laser Spatial Information, Shenzhen, China
[e]Southern University of Science and Technology, Department of Electronic and Electrical Engineering, Shenzhen, China

Abstract. Confronting the escalating global challenge of counterfeit products, developing advanced anti-counterfeiting materials and structures with physical unclonable functions (PUFs) has become imperative. All-optical PUFs, distinguished by their high output complexity and expansive response space, offer a promising alternative to conventional electronic counterparts. For practical authentications, the expansion of optical PUF keys usually involves intricate spatial or spectral shaping of excitation light using bulky external apparatus, which largely hinders the applications of optical PUFs. Here, we report a plasmonic PUF system based on heterogeneous nanostructures. The template-assisted shadow deposition technique was employed to adjust the morphological diversity of densely packed metal nanoparticles in individual PUFs. Transmission images were processed via a hash algorithm, and the generated PUF keys with a scalable capacity from 2^{875} to 2^{43401} exhibit excellent uniqueness, randomness, and reproducibility. Furthermore, the wavelength and the polarization state of the excitation light are harnessed as two distinct expanding strategies, offering the potential for multiscenario applications via a single PUF. Overall, our reported plasmonic PUFs operated with the multidimensional expanding strategy are envisaged to serve as easy-to-integrate, easy-to-use systems and promise efficacy across a broad spectrum of applications, from anticounterfeiting to data encryption and authentication.

Keywords: physical unclonable function; plasmonic array; template-assisted deposition; scalable capacity; multidimensional expanding.

Received Jun. 27, 2024; revised manuscript received Oct. 10, 2024; accepted for publication Nov. 20, 2024; published online Dec. 6, 2024.

[DOI: 10.1117/1.APN.4.1.016003]

1 Introduction

In the rapidly evolving landscape of cybersecurity, safeguarding sensitive information and ensuring the integrity of digital systems have become paramount. Physical unclonable functions (PUFs) have emerged as a cutting-edge technology in the realm of hardware-based security, especially in combating the scourge of counterfeit medicines.[1,2] A PUF refers to a physical object with inherent and unique features that can be generated with a stochastic and nondeterministic process and therefore is impervious to replication and also resistant to physical attack.[3,4] In the realm of commercially available electronic PUFs (e.g., arbiter PUFs and static random-access memory PUFs), the inherent physical variations in semiconductor devices generate unique and unpredictable identifiers.[4] However, due to their deterministic fabrication mode and encoding mechanism, these

*Address all correspondence to Jiawei Wang, wangjw7@hit.edu.cn; Qi Hao, qihao@seu.edu.cn; Perry Ping Shum, shenp@sustech.edu.cn

†These authors contributed equally to this work.

electronic PUFs might be susceptible to modeling attacks, notably from machine-learning fronts.[2] Countermeasures, fostering randomness and unpredictability, are essential to thwart such attacks.[5,6] Optical PUFs, fueled by the inherent randomness in optics and optical materials, have been receiving increasing research interest. Such an emerging technology holds promise for addressing issues in current electronic PUFs, such as vulnerability to attack, limits in entropy sources, aging, and degradation.[4] The first demonstration of optical PUFs reported in 2002[7] employed laser speckle patterns generated by random scattering from an inhomogeneous optical medium. Over the past two decades, integrable optical materials and structures involving stochastic processes or significant structural disorders,[8,9] such as plasmonic nanostructures,[10–16] Mie resonators,[17–19] colloidal photonic crystals,[20–22] molecular self-assemblies,[23] and bionic structures,[24] have been exploited as compact optical PUFs. Despite their promise, expanding the PUF capacity with ample challenge–response pairs (CRPs) demands dedicated spatial[9,25] or spectral encoding strategies[26] of the excitation light field to generate highly flexible graphical information. The required bulky and complex equipment (e.g., a spatial light modulator) often impedes their applications.

Recently, the challenge of limited CRPs in optical PUF systems has been addressed using multimodal interrogation strategies, including both electrical and optical interrogation in the time, spatial, and spectral domains.[23,27] In terms of optical interrogations, the potential has been unfolded by leveraging various mechanisms, such as luminescence,[28] Raman scattering,[29,30] and other non-linear processes.[26] Utilizing multiple dimensions (e.g., color, intensity, and lifetime) of luminescence, plenty of integrable micro/nanoemitters[1,27,31–41] have been investigated as optical PUFs. However, the condition of complex light–matter interactions might be degraded over a long time or in extreme environments, which potentially limits PUF performance. Moreover, the practicality is significantly hindered by the system cost of the precision instruments (e.g., pump sources and spectrometers). The largely untapped potential of multidimensional expanding strategies leveraging the intrinsic properties of photons holds promise for significantly expanding capacities without the need for sophisticated external instruments.

Herein, we report a plasmonic PUF system featuring densely packed heterogeneous plasmonic nanoparticles on a transparent substrate, fabricated using a nanoporous anodized aluminum oxide (AAO) membrane as a template. Leveraging the shadow deposition assisted by centimeter-sized nanoporous templates, the two-dimensional (2D) array of PUFs reveals distinct morphologies and local disorders. The adopted hash algorithm serves as an efficient way of processing transmission images with computational efficiency and robustness to variations, enabling scalable PUF keys with good randomness, uniqueness, and also stability. In addition, we propose multidimensional expanding strategies harnessing both the wavelength and polarization of the excitation light. The proof-of-concept demonstration of responses from a single-challenge-different-keys operation suggests ultralow authentication error probability, affirming the efficiency of our approach in safeguarding against counterfeit endeavors.

2 Results and Discussion

2.1 Working Principle

Figure 1(a) illustrates the plasmonic PUF array integrated onto a quartz substrate. By partitioning the substrate into an $M \times N$ array, the boundaries of each PUF label can be clearly defined. Compared with other noble metals, gold possesses excellent chemical stability and oxidation resistance, ensuring the reliability of the PUFs over the long term. As shown in Fig. 1(b), considering both the field of view of the experimental platform and the need for efficient PUF integration, the dimensions of each PUF label were set at ~0.3 mm × 0.25 mm. This allows for the mass integration of hundreds of units onto a single chip. In contrast to conventional lithography-based approaches and bottom-up syntheses, the adopted template-assisted deposition offers an efficient route to the mass production of large-scale plasmonic nanostructures integrated on a chip (see Appendix: Experimental Section). Here, one key control knob is the deposition angle α determining the gradience in the structures and the optical responses. Compared with the deposition at a normal incidence angle, shadow deposition results in an overall decrease in the sizes of nanoparticles and clusters and hence alters the morphology-dependent localized surface plasmon resonance (LSPR).

The randomness and local defects in the nanoporous membrane template, which were often considered detrimental in applications, such as surface-enhanced Raman scattering (SERS)[42] and plasmon-enhanced fluorescence (PEF),[43] are advantages to generating unclonable anticounterfeiting labels.[36] Via deposition, the size, shape, and distributions of deposited gold nanoparticles vary significantly between each PUF label. The deposited metal structures can be mainly divided into two types [see Fig. 1(c)]: the small (sub-100 nm) particles defined by the pore size of the template and the big clusters with a size of several hundred nanometers to several micrometers due to the local defects in the template.

Owing to the LSPRs of gold nanostructures in the visible wavelength range and the resulting strong absorption and scattering, the spatial inhomogeneity in the densely packed plasmonic pattern can be easily extracted simply by transmission imaging,[44] which differs from the common readout scheme using dark-field microscopy in previously reported plasmonic PUFs.[11,12] Here, transmission images can be captured by an objective lens and recorded using a top-view image sensor (see Appendix: Experimental Section). Figure 1(d) schematically visualizes the image from a PUF label, in which the dark spots represent the effect of randomly distributed clusters, and the background signal is determined by the density and size condition of nanoparticles.

Notably, both the spatial and spectral responses are highly sensitive to the morphological disorders of each PUF label. As a result, it is, in principle, impractical to duplicate them with identical ones accurately. The images can be binarized and processed using a perceptual hash (pHash) algorithm (see Appendix: Experimental Section) and consequently form a PUF key. The output sequence generated by the pHash algorithm is generally robust against noise-related variations in the raw images. As a result, a transmission image captured at an arbitrary probe wavelength λ_p and a specific polarization state can form a PUF key, serving as a unique fingerprint for each PUF label. In addition, the PUF key becomes scalable by adjusting the frequency range used in the encoding process. In this study, the wavelength and polarization as two inherent properties of the excitation light can be employed for the reconstruction of PUF keys [see Fig. 1(e)], which can be essential in expanding the space of CRPs and also building databases with higher security.

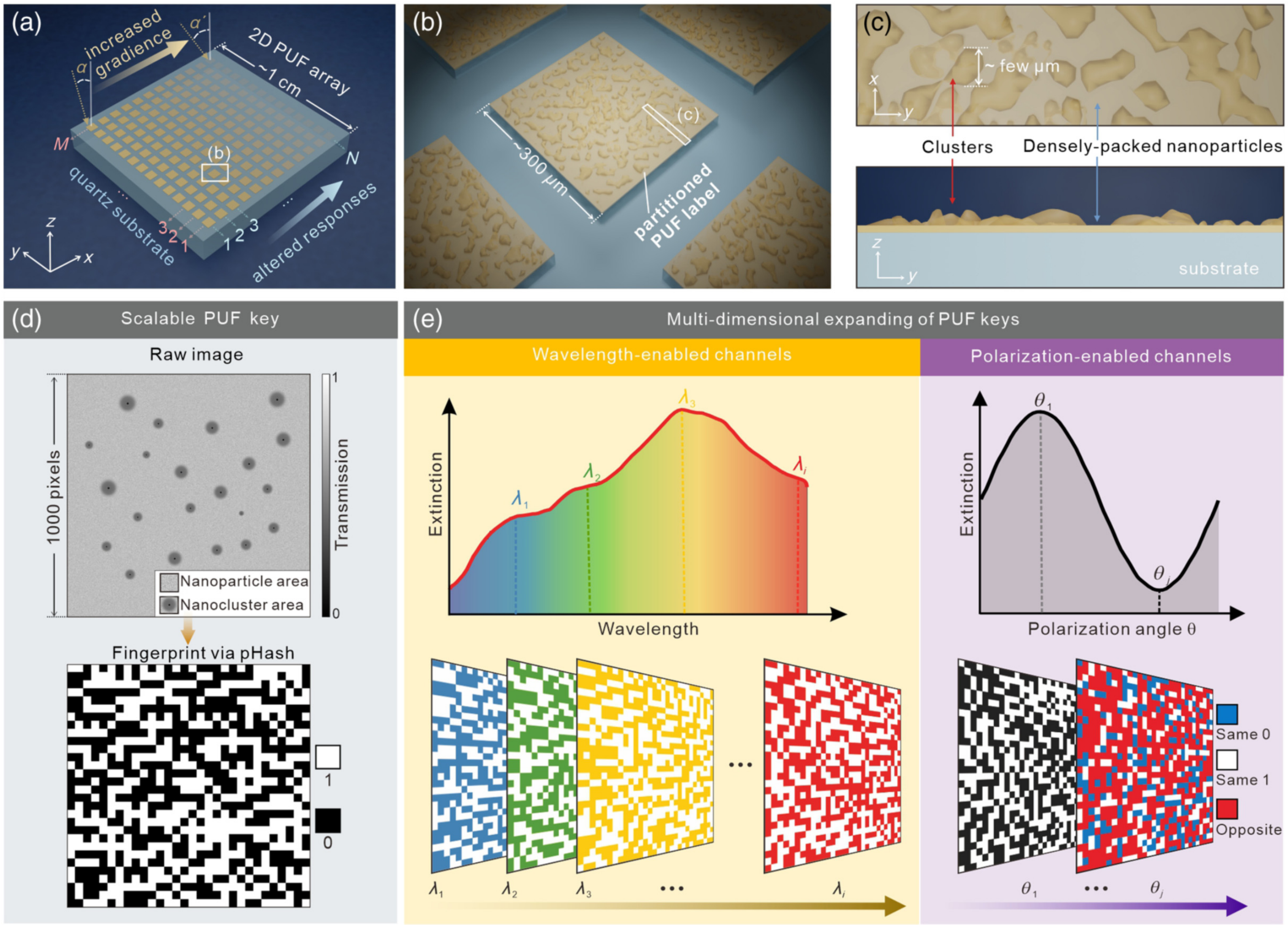

Fig. 1 Plasmonic PUF arrays empowered by a multi-dimensional expanding strategy. (a) Schematic of a plasmonic PUF system featuring gold nanostructures partitioned into 2D pixelized zones as an M-by-N array of PUF labels. The PUF labels with different N reveal a varying deposition angle α between 8 and 16 deg, corresponding to a significant variation in responses of transmission images and PUF responses. (b) Schematic of a zoomed-in view of one PUF label. (c) Schematics with the top view (top) and cross-sectional view (bottom) showing clusters and closely packed nanoparticles. (d) Schematic presenting a raw transmitted image (top) and an extracted PUF key with 30 × 30 elements (bottom). (e) Schematic of two schemes to expand the CRP space, namely, wavelength-based expansion of one PUF label with channels $1 - i$ (left) and polarization-based expansion of one PUF label with channels $1 - j$ (right).

2.2 Characterizations of Plasmonic PUFs

Figure 2(a) shows the fabricated plasmonic chip incorporating an 18-by-18 array of PUF labels (see Appendix: Experimental Section and Fig. S1 in the Supplementary Material). For PUF labels aligned along with the transverse axis (x axis, i.e., with the same N but different M), the value of the deposition angle α is almost identical. Hence, the uniqueness of PUFs can be quantified among M devices under the same fabrication configuration. Figures 2(b) and 2(c) reveal the clusters as random defects embedded in the densely packed nanoparticles that were transferred from the defect in the template induced during the template preparation.[45–47] For PUF labels aligned along with the longitudinal axis (y axis), the dimensions of clusters and nanoparticles differ significantly due to varying α between 8 and 16 deg [see Fig. 2(c)]. Figure S2 in the Supplementary Material provides the histograms of nanoparticle size with $\alpha = 8$ and 16 deg. Such a difference can also be discerned using dark-field microscopy (see Fig. S3 in the Supplementary Material), in which the relatively large particle size upon $\alpha = 8$ deg is ascertained by stronger scattering signals than those upon a larger α.

Due to the ultrahigh density of close-packed nanoparticles ($\sim 1.5 \times 10^{10}$ cm^{-2}), the PUF response can be read out by easy transmission imaging. The spectral responses have been characterized using a home-built hyperspectral imaging setup [Fig. 2(d)]. As revealed in the measured extinction spectra in Fig. 2(e), the change α results in modification of the particle sizes and subsequently alters the LSPR effect (see Figs. S4–S6 in the Supplementary Material). For a small α, an intensified LSPR with increased optical absorption and scattering strength is obtained, which is attributed to the overall large size of the packed nanoparticles and narrow interparticle spacing [see Fig. 2(f)]. In contrast, these effects are weakened upon a large

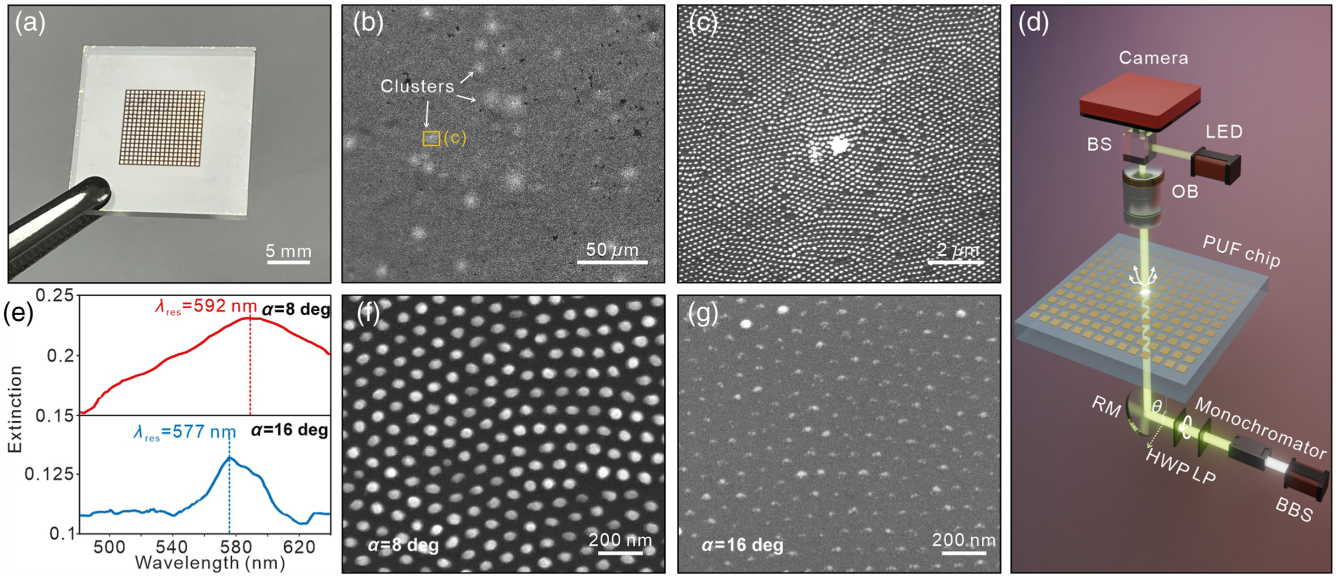

Fig. 2 Characterizations of the heterogeneous plasmonic nanostructures. (a) Picture of the PUF chip. (b) Scanning electron microscopy (SEM) image showing fine nanostructures in a PUF label on a silicon substrate. (c) Zoomed-in-view of SEM image of panel (b) showing a cluster and its vicinity. (d) Schematic of the home-built hyperspectral imaging setup. BBS, broadband source; LP, linear polarizer; HWP, half-wave plate; RM, reflection mirror; OB, objective lens; BS, beam splitter; LED, light-emitting diode. (e) Extinction spectra for PUF labels with $\alpha = 8$ deg (top) and 16 deg (bottom). The resonance wavelengths λ_{res} are denoted at the resonance peaks. SEM images of PUF labels fabricated with $\alpha = 8$ deg (f) and 16 deg (g) show the distinct sizes of nanoparticles.

α [see Fig. 2(g) and Fig. S7 in the Supplementary Material for details]. Besides, the blueshift of resonance wavelength λ_{res} from ~592 to ~577 nm in Fig. 2(e) also verifies the strong dependence between λ_{res} and the particle size, according to the LSPR theory.[48,49]

Figure 3(a) presents the raw transmission image captured by a CMOS camera at λ_p of 580 nm. One can identify local spots as well as winkle-like patterns in a nonuniform background, which are attributed to the heterogeneity of the nanostructures (see Fig. S6 in Supplementary Material for results of a PUF label with $\alpha = 16$ deg). The image was processed using the pHash algorithm (see Appendix: Experimental Section) to extract the inherent randomness, forming a 1000 × 800 matrix. One key merit here is that the encoding capacity is not dominated by the size of the raw image but becomes scalable by choosing the proper frequency range. The theoretical encoding capacity of a single PUF key becomes L^s, where L represents the bit states and s represents the size of bit sequences in the frequency domain. For proof-of-concept demonstrations, we first employ binary matrices of 30 pixel × 30 pixel for authentication, representing the key feature at the lower-frequency range [see Fig. 3(b)].

Here, we evaluate the statistical properties of 15 PUFs ($M = 1$ to 15, $N = 1$) integrated on the same chip. The bit uniformity (i.e., the number of 0 or 1 bits in a binary sequence) metric is calculated using the following equation:[1,50]

$$\text{bit uniformity} = \frac{1}{s}\sum_{i=1}^{s} K_i, \tag{1}$$

where K_i is the i'th binary bit of the key. As presented in Fig. 3(c), the bit probability for all 15 PUF keys fluctuates around an ideal value of ~0.5, thus indicating consistent bit uniformity. To examine the randomness, the 15 PUF keys are treated as one 13,500-bit cryptographic key. The National Institute of Standards and Technology (NIST) randomness test suite was adopted for evaluation (see Appendix: Experimental Section). As shown in Fig. 3(d), the successful proportions of all tests are above the acceptable threshold.

In practice, PUF labels need to be authenticated repeatedly, requiring good reproducibility between readouts of the same label and distinctiveness among different labels. Herein, we adopt normalized Hamming distance (HD) to quantify both the uniqueness (via interdevice HD) and the reproducibility (via intradevice HD). In an ideal PUF system, the interdevice HD of 0.5 means perfect uniqueness, and the intradevice HD of 0 means perfect reproducibility. Figure 3(e) presents the 2D correlation of 15 PUF labels ($M = 1$ to 15, see Fig. S8 in the Supplementary Material for details). Via a Gaussian fit $P(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$ of the probability density histogram of the interdevice HD [Fig. 3(f)], a mean value μ of 0.494 and a variance α of 0.017 are obtained, indicating the stochastic genesis of our PUF labels. The intradevice HD is examined based on 15 repeated challenge–response cycles for the same PUF (see Fig. S9 in the Supplementary Material). A Gaussian fit of the histogram returns $\mu = 0.0051$ and $\sigma = 0.0017$ [Fig. 3(f)]. As presented in Fig. 3(f), the threshold for discrimination is set as ~0.03. For practical applications, the stabilities of the anticounterfeiting keys are essential. We have therefore characterized the robustness of the PUF chip against environmental fluctuations. Through a test under the relative humidity change over 40% to 70% and a long-term test over 1 week, the PUF

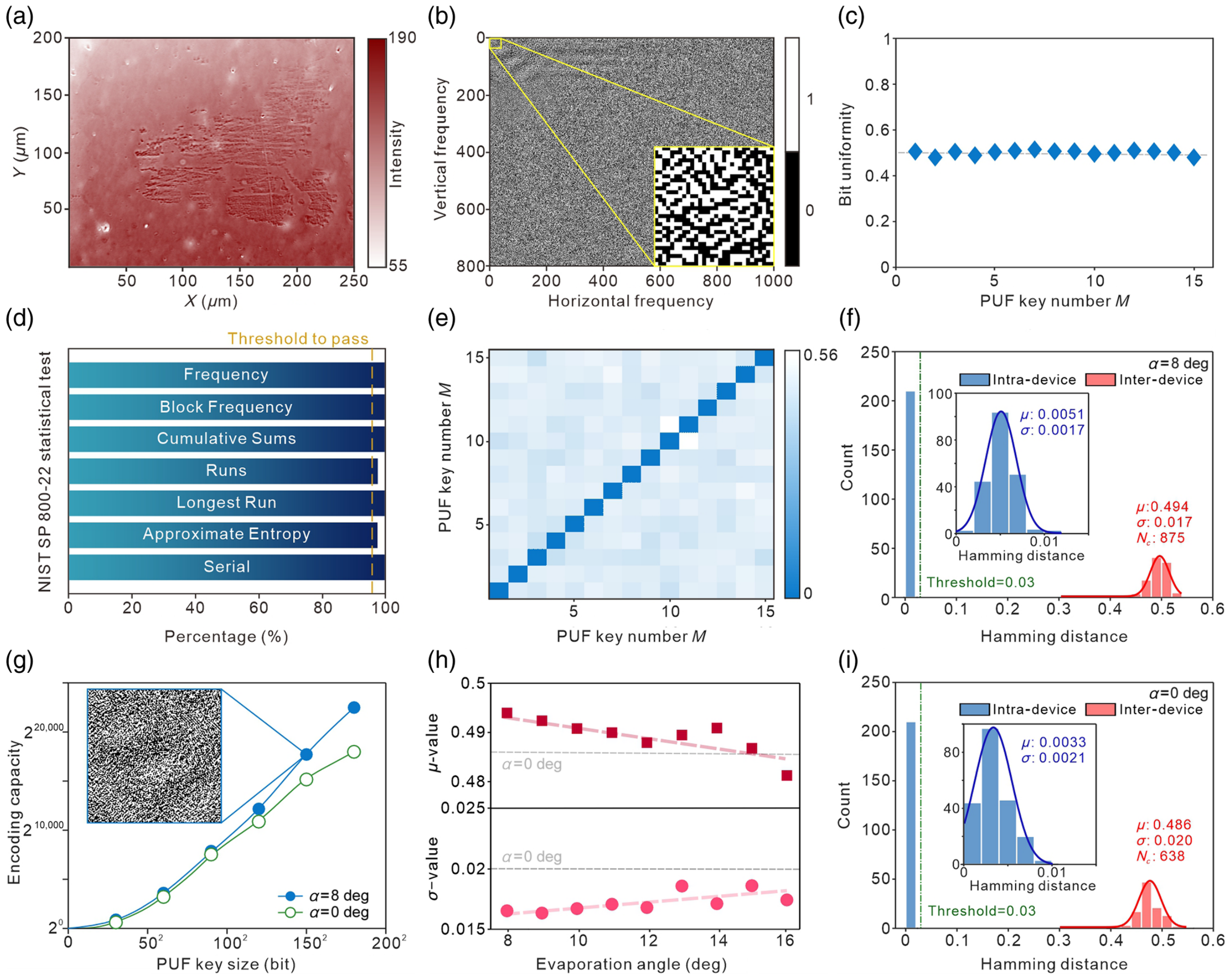

Fig. 3 Scalable PUF keys and verifications of their key performances. (a) Captured 2D image of a PUF label with $\alpha = 8$ deg. (b) A 2D code generated via the pHash algorithm. Inset: the adopted 30 × 30 PUF key with features in the lower-frequency range. (c) Bit uniformity in 15 keys generated from labels with the same N. (d) Summary of statistical NIST tests using binary sequences generated from 15 PUF keys. (e) Pairwise match of 15 PUF keys with the same N and different M to examine uniqueness. The color bar shows the extracted HD. (f) Distributions of interdevice and intradevice HDs for PUF labels prepared with $\alpha = 8$ deg. (g) The extracted relationship between the encoding capacity and the adopted size of the PUF key. Inset: a 150 × 150 PUF key. (h) Summary of μ and σ of interdevice HD as a function of α. (i) Distributions of interdevice and intradevice HDs for PUF labels prepared with $\alpha = 0$ deg.

keys suggest a fluctuation of intradevice HD of less than 0.03 (see Fig. S10 in the Supplementary Material), indicating the resilience of these plasmonic PUFs in real-world scenarios.

The distribution of interdevice HDs can be modeled with an equivalent binomial distribution $B(N, p)$ and hence can be fitted by a Gaussian function in the limit of "degree of freedom," i.e., the number of independent bits N_c. The number of mutually independent bits (i.e., degrees of freedom) is defined as $N_c = \frac{\mu(1-\mu)}{\sigma^2}$. For PUF labels with $\alpha = 8$ deg, an extracted N_c of ~875.12 results in an encoding capacity of $2^{N_c} = 2^{875}$. Notably, such a capacity can be readily scalable by expanding the frequency range (see Fig. S11 in the Supplementary Material). As presented in Fig. 3(g), the encoding capacity increases up to 2^{43401} by adopting a 210 × 210-bit PUF key with $\alpha = 8$ deg. In addition, one should also note that there is a trade-off between the PUF key size and the reproducibility (see Fig. S11 in the Supplementary Material).

Together with the morphology of the template, the deposition angle α is a key parameter shaping the heterogeneity of the plasmonic nanostructures and can be regarded as a control knob for optimizing the PUF response and the security level. Figure 3(h) summarizes the extracted values of μ and σ of the interdevice HD for PUF labels with different α. In addition, as α gets adjusted, the clear evolution of the interdevice HD can be discerned. Upon an increased α, the degraded uniqueness featuring an increased σ is attributed to the potentially reduced probability of cluster

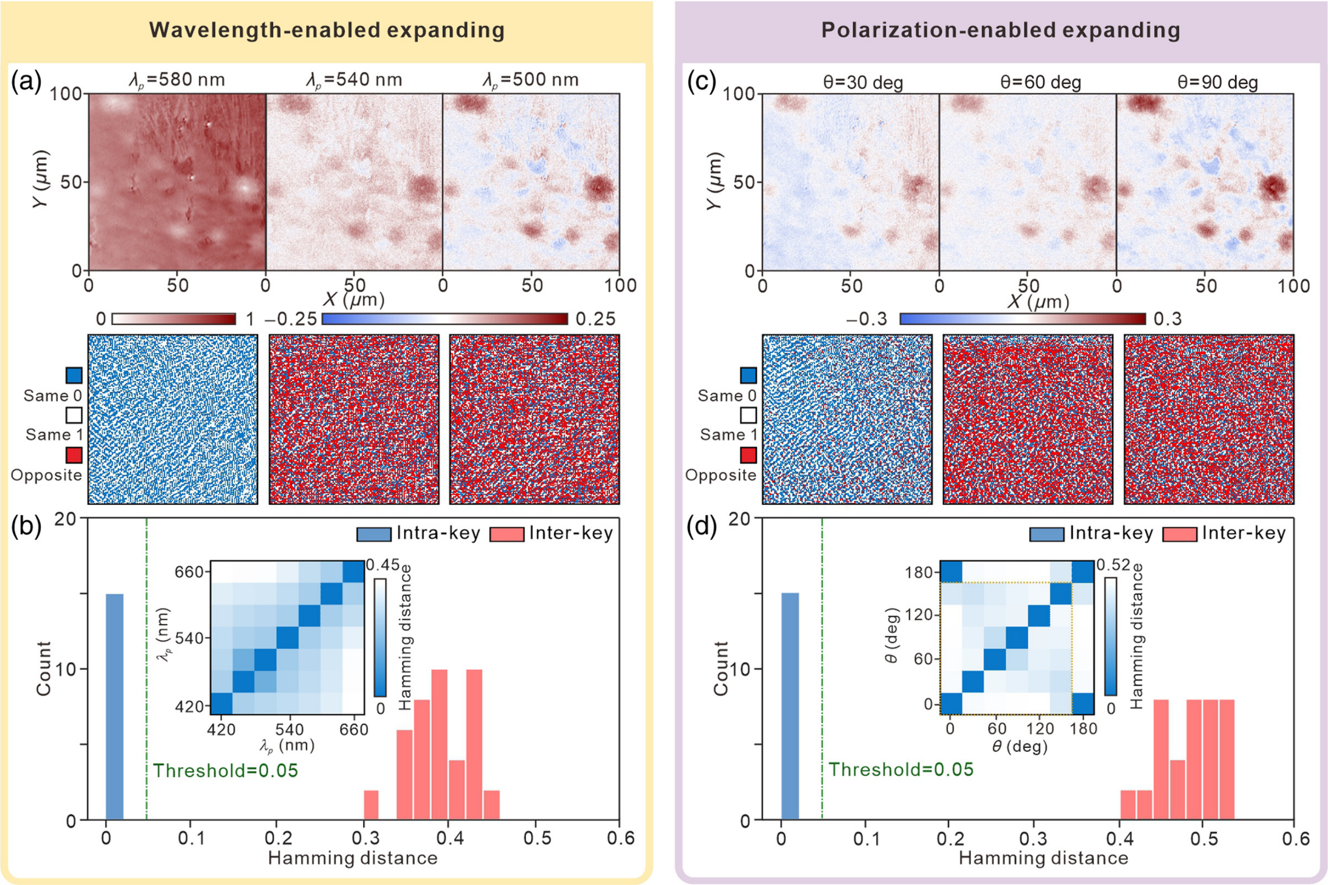

Fig. 4 Wavelength and polarization-enabled expanding strategies. (a) Top: captured raw image (left) and contrast images (middle and right) for three different λ_p. Bottom: their corresponding PUF keys. (b) Distributions of interkey and intrakey HDs using the wavelength-expanded strategy. The threshold was set to 0.05 when the PUF key size m is 150 × 150. Inset: pairwise match of seven PUF keys upon different λ_p. (c) Top: contrast images for three different θ. λ_p is fixed at 580 nm. Bottom: their corresponding PUF keys. (d) Distributions of interkey and intrakey HDs using the polarization-expanded strategy. Inset: pairwise match of seven PUF keys upon different θ. One should note that the last one ($\theta = 180$ deg) is a control test (essentially the same as $\theta = 0$ deg) examining repeatability.

formation and suppressed heterogeneity. Consequently, the estimated N_c is degraded from ~875 to ~720 upon an increased α (see Fig. S12 in the Supplementary Material). Here, control experiments on an additional PUF chip deposited at a normal angle ($\alpha = 0$ deg) were carried out. PUFs made by shadow deposition, in general, result in elevated uniqueness compared with those made at $\alpha = 0$ deg [$\mu = 0.4860$, $\sigma = 0.0200$; see Fig. 3(i)]. Meanwhile, as revealed in Fig. 3(g), the extracted encoding capacity at $\alpha = 0$ deg (e.g., $2^{N_c} = 2^{638}$ at $m = 15$) is scalable, yet in general, degraded compared with those at $\alpha = 8$ deg.

2.3 Multidimensional Expanding Strategy

Given the wavelength and polarization-sensitive response of the heterogeneous plasmonic nanostructures, these two inherent properties of light can be exploited to generate unpredictable and distinct responses. Such a multidimensional expanding strategy meets the quest for expanded space of CRPs and circumvents the precision spatial or spectral encoding processes. As presented in Fig. 4(a), three representative responses of one single PUF label upon different λ_p were studied, namely, one away from resonance (500 nm), one around the resonance (540 nm), and one aligned at the LSPR peak wavelength (580 nm). A hash function compresses an arbitrary-length input to a fixed-length output, featuring an avalanche behavior wherein at least half of the bits are flipped by a minor change in the input. Therefore, the fine changes in patterns result in distinct cryptographic keys. Considering the tolerance of PUF authentication for sufficient robustness, the channel spacing between each challenge was set as 40 nm. Hence, the single PUF would yield at least seven CRPs leveraging the flexibility of the probe wavelength in the visible range. In Fig. 4(b), the interkey HDs spanning 0.31 to 0.45 are sufficiently separated from the intrakey HD (μ of 0.015), indicating a nice uniqueness of each.

Given the anisotropic nature of the on-chip nanostructures, polarization emerges as another degree of freedom. Figure 4(c) presents three representative responses of the same PUF label upon excitation of linearly polarized light with a switched polarization angle θ. Similar to the process in the wavelength-expanding strategy, here, the channel spacing between each challenge was set as 30 deg, leading to six CRPs from one single PUF. Figure 4(d) examines the uniqueness by characterizing the interkey HDs between 0.40 and 0.52; the distribution histogram of the HDs also shows a clear separation between the intrakey and interkey HDs. As the overall expanding space is dependent on the number of CRPs, here, these two alternative channels provide a significant expansion of PUF capacity.

2.4 Practical Authentication of PUF Labels

In practical authentication, to avoid replay-based attacks, each CRP can be only used once. Therefore, authentication processes for multiple purposes require a sufficiently large CRP space.[23] Here, 12 PUF keys generated via the multidimensional expanding strategy were applied as "identifiers" to a single binary image challenge pattern using a simple exclusive-OR (XOR) operation. The identifiers and the single challenge are binary images of size 150 pixel × 150 pixel, as shown in Fig. 5(a) (see Fig. S13 in the Supplementary Material for sources). As depicted in Fig. 5(b), the different responses exhibit high discernibility. The averaged HD of $\sim 0.41 \pm 0.11$ is sufficiently far away from the preset threshold of 0.05 [see Fig. 5(c)]. Therefore, these nanoidentifiers offer sufficiently distinguishable responses in a single challenge–different PUFs and, hence, suggest a pathway to secure and reliable authentication.

Figure 5(d) illustrates the multipurpose authentication flow of products using our proposed plasmonic PUF chips. The PUF chips can be mass-produced on low-cost flexible substrates with good transparency[42] and seamlessly integrated with the packaging of cosmetics, pharmaceuticals, and other products by the manufacturers. Consequently, they can be distributed across commodity circulation networks, potentially undergoing

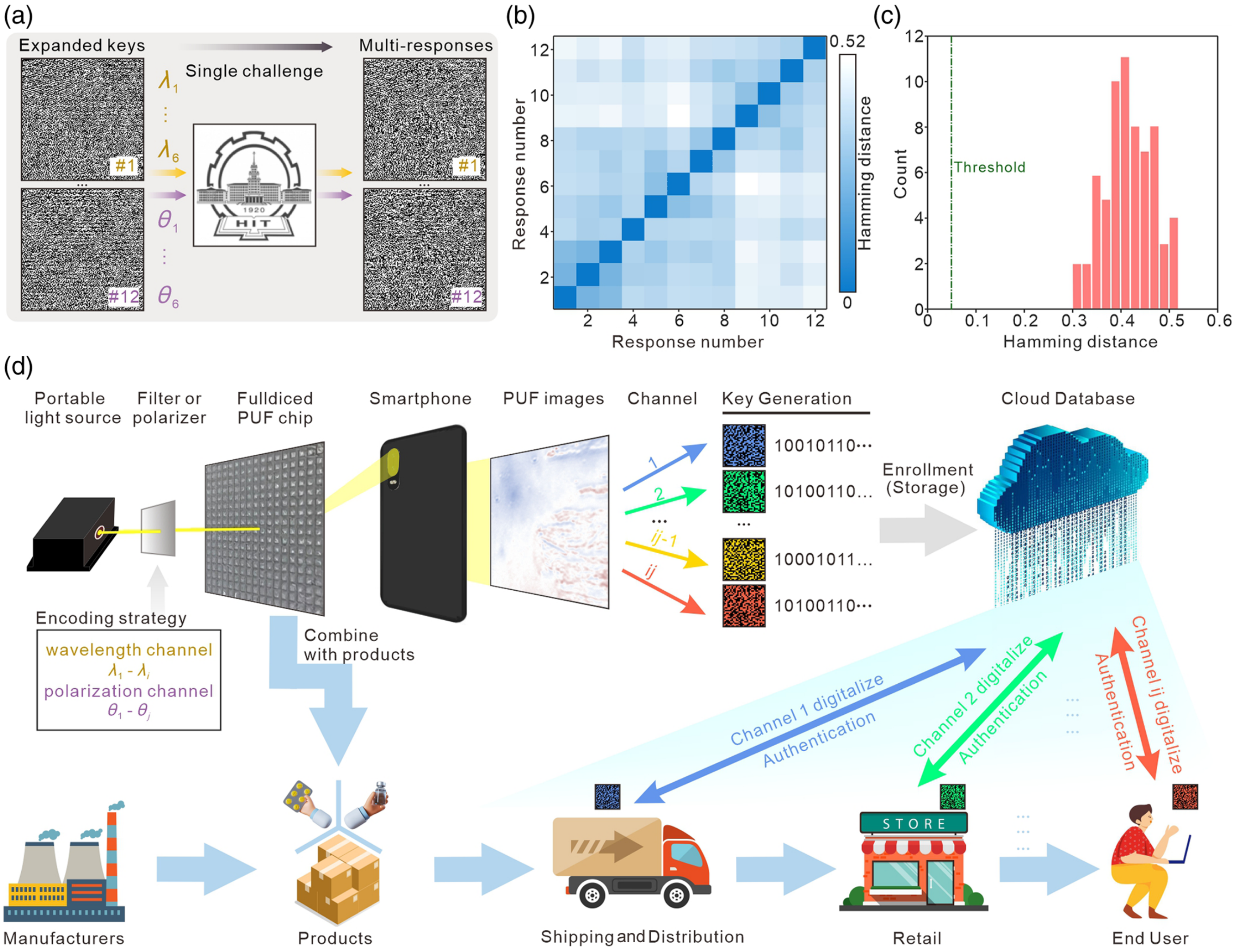

Fig. 5 Practical authentication of PUF labels using the multidimensional expanding strategy. (a) Schematic showing a series of CRPs generated with the same challenge of the logo of Harbin Institute of Technology (150 pixel × 150 pixel) using XOR operation. Each corresponding pixel is compared, resulting in a value of 0 if they are the same and 1 if they are different. (b) Pairwise match of responses from a single challenge–different PUF operation. Items 1 to 6 adopt keys obtained at varied λ_p and fixed $\theta = 0$ deg, whereas items 7 to 12 adopt keys obtained at varied θ and fixed $\lambda_p = 580$ nm. (c) Histogram of HDs for 66 CRPs. (d) Conceptual schematic of the multipurpose authentication flow of products using the plasmonic PUF chip with a multi-dimensional expanding strategy.

multiple rounds of authentication, thanks to the working principle obviating the need for spectrally resolved measurements and complex spatial encoding strategies. The multidimensional expansion can be performed by users at different phases (e.g., shipping, retail, or end-use) using compact filters and polarizers. Although the key database in the cloud can be built up by the manufacturers, users can access specific channels to read out a label and upload the key to the database for decoding and authentication.

3 Conclusion

In this paper, we proposed and demonstrated a plasmonic PUF system utilizing densely packed nanostructures with strong heterogeneity. Compared with other techniques shaping nanostructures on a chip, such as femtosecond-laser printing[51] and localized electron-beam irradiation,[52] our approach offers an efficient route for large-scale integration of densely packed plasmonic PUF arrays onto a centimeter-sized chip. Via a transmission image and pHash algorithm, the scalable cryptographic keys exhibited superior characteristics in terms of randomness, uniqueness, and reproducibility (see Table S1 in the Supplementary Material for benchmarking). Hyperspectral microscopy tests further demonstrate that the probe wavelength and polarization as inherent properties of light offer alternative avenues for expanding PUF capacity. Notably, by simplifying the system using intuitive lensless imaging, the PUF chip is compatible with low-cost and portable query systems (see Fig. S17 in the Supplementary Material).

Looking ahead, our proposed plasmonic PUF system can be readily extended into multimodal expanding and authentication schemes by leveraging the inherent plasmonic mechanisms, such as PEF[43] and SERS.[42] Ultimately, such mass-producible plasmonic PUF systems offer cryptographic keys characterized by high capacity, security, and environmental stability, paving the way for the development of customized hardware solutions for anticounterfeiting, data encryption, and authentication endeavors.

4 Appendix: Experimental Section

4.1 Fabrication of Chip-Scale Plasmonic PUFs

Laser direct writing was used to define pixelized zones on a single quartz substrate with a total area of ~10 mm × 10 mm. Each individual PUF was designed with dimensions of 0.3 mm × 0.3 mm and spaced ~200 μm apart. Nanomembranes of porous AAO were employed as a template for deposition[53] (see Section S1 in the Supplementary Material). The film thickness and averaged pore size of the AAO membranes were ~270 and ~80 nm, respectively. To engineer the heterogeneity of deposited gold nanoparticles, angle-resolved shadow evaporation was employed. The deposition angle α ranging from 8 to 16 deg was obtained by adjusting the lateral offset between the center aligned with the source and the AAO-integrated substrate. Upon a large deposition angle, some atoms are blocked by the pore walls of the nanomembrane template, resulting in a reduced amount of the atoms being deposited onto the substrate, and hence an overall gradience of particle size. As a reference study, PUF samples were also fabricated with $\alpha = 0$ deg. The electron-beam (Beijing Technol Science Co., Ltd., Beijing, China) deposition rate is 0.5 nm s^{-1} at 10^{-4} Pa. The estimated thickness at normal deposition is ~60 nm. SEM inspections (FEI Inspect F50) were performed on samples fabricated on silicon substrates with the same configuration.

4.2 Optical Characterizations

For capturing transmitted images and generation of PUF keys, optical characterizations were performed using a home-built hyperspectral microscopy setup. The wavelength of probe light was swept from 400 to 700 nm (step of 1 nm) using a monochromator (PLGL-021, PL OPTICS) coupled to a broadband source (OSL2, Thorlabs, Newton, New Jersey, United States). For polarization-dependent studies, a linear polarizer (LPVISC, Thorlabs) and a half-wave plate (AHWP10M-980, Thorlabs) were mounted onto motorized rotation stages (PRM1/MZ8, Thorlabs) to adjust the polarization state of the incident light. The ellipticity of the excitation beam was examined using a polarimeter (PAX1000, Thorlabs). The collimated linearly polarized light beam was focused onto the sample using an objective lens (PLCN20X, 20×, NA: 0.28, WD: 10.6 mm, Olympus, Tokyo, Japan). The excitation power is ~0.12 mW. The transmitted image response was recorded by a long-working-distance objective lens (MPLAN APO 378-803-3, 20×, NA: 0.25, WD: 34 mm, Mitutoyo, Kawasaki, Japan) and a monochrome CMOS Camera (MQ013MG-ON, XIMEA, 1280 pixel × 1024 pixel, frame rate: 2.8 frame/s). The exposure time for capturing all images was set to 15 ms. The extinction spectra were extracted based on the stack of hyperspectral images using MATLAB.

4.3 Algorithms for Data Processing

To avoid potential defects near the edge areas, the captured images were first cropped into a size of 1000 pixel × 800 pixel. To mitigate the effect of image jitter, a locating algorithm was implemented.[54] For each PUF label, the central region of the first image (with a size of 100 pixel × 100 pixel) is used as a reference. The optimal cross-correlation value between the processed image and the reference was evaluated. Judging from the value, the region of interest was adjusted to correct any potential spatial offsets. Such a correction ensures precise alignment between the series of images and the reference image for fair evaluations.

The extraction of PUF labels was performed through perceptual hash based on the type II discrete cosine transform.[55] The information in the frequency domain was extracted using the dct2 function in MATLAB, and the frequency domain matrix of 1000×800 was generated. Select a fixed value m, the dominant low-frequency coefficients from 1 to m^2 ($m = 30$ to 200) were included in each PUF label. The high-frequency components correlating with minor details hardly reflect the key variation of the images and therefore can be neglected. By setting a threshold of 0, the $m \times m$ low-frequency coefficients get transformed into a binary matrix (i.e., a PUF key). Therefore, the PUF key becomes scalable by adopting different values of m.

Intradevice HDs were evaluated according to the following definition:

$$\text{Intradevice HD} = \frac{1}{h}\sum_{t=1}^{h}\frac{HD(K_i, K_{i,t})}{s}, \tag{2}$$

where $K_{i,t}$ represents the s-bit keys of the i'th PUF device at the t'th time among h different acquisition numbers. Here, the size of the key s equals $m \times m$.

Interdevice HDs were evaluated according to the following definition:

$$\text{Interdevice HD} = \frac{2}{q(q-2)}\sum_{i=1}^{q-1}\sum_{j=i+1}^{q}\frac{HD(K_i,K_j)}{s}, \tag{3}$$

where K_i is the binary bit of the key in the i'th PUF device among q different PUF devices, K_j is the binary bit of the key in the j'th PUF device, and s is the size of the key. For evaluation of the reproducibility using the intradevice HD, 210 independent tests were conducted consecutively within 2 h. One should note that the interdevice HD compares PUF keys obtained from different devices, whereas the interkey HD compares keys from the same device under different excitation conditions. Despite these different contexts, the calculation method for both types of HD is identical. For evaluation of the intrakey HDs during the multidimensional expansion, the image with a fixed polarization state ($\theta = 0$ deg) and wavelength ($\lambda_p = 580$ nm) was used as a reference.

4.4 NIST tests

For evaluations of randomness in the generated cryptographic key, the NIST SP 800-22 (National Institute of Standards and Technology Special Publication 800-22) statistical test suite was adopted. A set of images was obtained from 15 PUFs on a chip and processed to form a cryptographic key sequence with a length of 13,500 bits (15 bits × 30 bits × 30 bits). The first 12,800 bits were selected and divided into 100 groups of 128 bits each. The P-values were calculated for seven tests (frequency, block frequency, cumulative sums, runs, longest run, approximate entropy, and serial). Certain tests, such as binary matrix rank, discrete Fourier transform, and nonoverlapping template matching, were omitted due to their requirement of a minimum bit length of 10^6 for a single test and 10^8 for the complete set of 100 trials.[35] The number of bits (l) in the stream being tested was set to 128, and the number of bits in a substring (block) size was set to 16. For each round of the test, the significance level (ε) was 0.01, and a pass was granted if the P-value was greater than ε. The range of acceptable proportions was determined using the confidence interval defined as $\omega \pm 3\sqrt{\frac{\omega(1-\omega)}{l}}$, where $\omega = 1 - \varepsilon$, and l is the sample size.[21] The calculated threshold to pass is 0.9602.

Disclosures

The authors declare that they have no conflicts of interest.

Code and Data Availability

The data sets that support the findings of this study are available from the corresponding authors upon reasonable request.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 62422503, 62105080, 22004016, and U22A2093), the Guangdong Basic and Applied Basic Research Foundation Regional Joint Fund (Grant Nos. 2023A1515011944, 2020B1515130006, and 2021B515120056), the Talent Recruitment Project of Guangdong (Grant No. 2021QN02X179), and the Science and Technology Innovation Commission of Shenzhen (Grant Nos. JCYJ20220531095604009 and RCYX20221008092907027).

References

1. J. W. Leem et al., “Edible unclonable functions,” *Nat. Commun.* **11**, 328 (2020).
2. C. Herder et al., “Physical unclonable functions and applications: a tutorial,” *Proc. IEEE* **102**, 1126–1141 (2014).
3. H. Ning et al., “Physical unclonable function: architectures, applications and challenges for dependable security,” *IET Circuits, Devices Syst.* **14**, 407–424 (2020).
4. Y. Gao, S. F. Al-Sarawi, and D. Abbott, “Physical unclonable functions,” *Nat. Electron.* **3**, 81–91 (2020).
5. Y. Liu et al., “A novel physical unclonable function based on silver nanowire networks,” *Adv. Funct. Mater.* **33**, 2304758 (2023).
6. A. Dodda et al., “Graphene-based physically unclonable functions that are reconfigurable and resilient to machine learning attacks,” *Nat. Electron.* **4**, 364–374 (2021).
7. R. Pappu et al., “Physical one-way functions,” *Science* **297**, 2026–2030 (2002).
8. R. Arppe and T. J. Sørensen, “Physical unclonable functions generated through chemical methods for anti-counterfeiting,” *Nat. Rev. Chem.* **1**, 0031 (2017).
9. Q. Li et al., “Intrinsic random optical features of the electronic packages as physical unclonable functions for Internet of Things security,” *Adv. Photonics Res.* **3**, 2100207 (2021).
10. N. Sun et al., “Random fractal-enabled physical unclonable functions with dynamic AI authentication,” *Nat. Commun.* **14**, 2185 (2023).
11. Y. Lu et al., “Plasmonic physical unclonable function labels based on tricolored silver nanoparticles: implications for anticounterfeiting applications,” *ACS Appl. Nano Mater.* **5**, 9298–9305 (2022).
12. J. D. Smith et al., “Plasmonic anticounterfeit tags with high encoding capacity rapidly authenticated with deep machine learning,” *ACS Nano* **15**, 2901–2910 (2021).
13. 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**, 1315–1321 (2016).
14. Q. A. Li et al., “Physical unclonable anticounterfeiting electrodes enabled by spontaneously formed plasmonic core-shell nanoparticles for traceable electronics,” *Adv. Funct. Mater.* **31**, 2010537 (2021).
15. Z. L. Tang et al., “Unclonable anti-counterfeiting labels based on plasmonic-patterned nanostructures,” *Adv. Eng. Mater.* **24**, 2101701 (2022).
16. V. Caligiuri et al., “Hybrid plasmonic/photonic nanoscale strategy for multilevel anticounterfeit labels,” *ACS Appl. Mater. Interfaces* **13**, 49172–49183 (2021).
17. P. Kustov et al., “Mie-resonant silicon nanoparticles for physically unclonable anti-counterfeiting labels,” *ACS Appl. Nano Mater.* **5**, 10548–10559 (2022).
18. S. Daqiqeh Rezaei et al., “Tri-functional metasurface enhanced with a physically unclonable function,” *Mater. Today* **62**, 51–61 (2023).
19. M. S. Kim et al., “Revisiting silk: a lens-free optical physical unclonable function,” *Nat. Commun.* **13**, 247 (2022).
20. J. Wu et al., “A high-security mutual authentication system based on structural color-based physical unclonable functions labels,” *Chem. Eng. J.* **439**, 135601 (2022).
21. A. Fratalocchi et al., “NIST-certified secure key generation via deep learning of physical unclonable functions in silica aerogels,” *Nanophotonics* **10**, 457–464 (2021).
22. H. Im et al., “Chaotic organic crystal phosphorescent patterns for physical unclonable functions,” *Adv. Mater.* **33**, 2102542 (2021).
23. J. H. Kim et al., “Nanoscale physical unclonable function labels based on block copolymer self-assembly,” *Nat. Electron.* **5**, 433–442 (2022).

24. Y. B. Wan et al., "Bionic optical physical unclonable functions for authentication and encryption," *J. Mater. Chem. C* **9**, 13200–13208 (2021).
25. K. Chen et al., "Fast random number generator based on optical physical unclonable functions," *Opt. Lett.* **46**, 4875–4878 (2021).
26. B. C. Grubel et al., "Silicon photonic physical unclonable function," *Opt. Express* **25**, 12710–12721 (2017).
27. T. Zhang et al., "Multimodal dynamic and unclonable anti-counterfeiting using robust diamond microparticles on heterogeneous substrate," *Nat. Commun.* **14**, 2507 (2023).
28. J. Zhang et al., "An all-in-one nanoprinting approach for the synthesis of a nanofilm library for unclonable anti-counterfeiting applications," *Nat. Nanotechnol.* **18**, 1027–1035 (2023).
29. Y. Gu et al., "Gap-enhanced Raman tags for physically unclonable anticounterfeiting labels," *Nat. Commun.* **11**, 516 (2020).
30. Y. W. Hu et al., "Flexible and biocompatible physical unclonable function anti-counterfeiting label," *Adv. Funct. Mater.* **31**, 2102108 (2021).
31. Y. Yamamoto et al., "Molecular and supramolecular designs of organic/polymeric micro-photoemitters for advanced optical and laser applications," *Acc. Chem. Res.* **56**, 1469–1481 (2023).
32. Y. Fan et al., "Randomly induced phase transformation in silk protein-based microlaser arrays for anticounterfeiting," *Adv. Mater.* **33**, e2102586 (2021).
33. Y. Liu et al., "Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication," *Nat. Commun.* **10**, 2409 (2019).
34. N. B. Kiremitler et al., "Tattoo-like multi-color physically unclonable functions," *Adv. Opt. Mater.* **11**, 2302464 (2023).
35. X. Gao et al., "Tunable key-size physical unclonable functions based on phase segregation in mixed halide perovskites," *ACS Appl. Mater. Interfaces* **15**, 23429–23438 (2023).
36. L. Liu et al., "Vertically aligned perovskite laser arrays for high-capacity anticounterfeiting labels," *Laser Photonics Rev.* **18**, 2301006 (2024).
37. S. L. Maurizio et al., "Covert information storage and encryption using temporal emissions from lanthanide-doped $LiYF_4$ nanoparticles," *ACS Appl. Nano Mater.* **6**, 21496–21502 (2023).
38. N. Kayaci et al., "Organic light-emitting physically unclonable functions," *Adv. Funct. Mater.* **32**, 2108675 (2022).
39. J. Feng et al., "Random organic nanolaser arrays for cryptographic primitives," *Adv. Mater.* **31**, e1807880 (2019).
40. M. R. Carro-Temboury et al., "An optical authentication system based on imaging of excitation-selected lanthanide luminescence," *Sci. Adv.* **4**, e1701384 (2018).
41. X. Y. Gao et al., "Dynamic physical unclonable function relying on lasing polarization," *ACS Photonics* **11**, 2263–2272 (2024).
42. Q. Hao et al., "Flexible surface-enhanced Raman scattering chip: a universal platform for real-time interfacial molecular analysis with femtomolar sensitivity," *ACS Appl. Mater. Interfaces* **12**, 54174–54180 (2020).
43. J. Wang et al., "Ultra-dense plasmonic nanogap arrays for reorientable molecular fluorescence enhancement and spectrum reshaping," *Nanoscale* **15**, 1128–1135 (2023).
44. S. Sun et al., "Refractometric imaging and biodetection empowered by nanophotonics," *Laser Photonics Rev.* **17**, 2200814 (2023).
45. Q. Hao et al., "Verification and analysis of single-molecule SERS events via polarization-selective Raman measurement," *Anal. Chem.* **94**, 1046–1051 (2022).
46. Q. Hao et al., "Facile design of ultra-thin anodic aluminum oxide membranes for the fabrication of plasmonic nanoarrays," *Nanotechnology* **28**, 105301 (2017).
47. Q. Hao et al., "Controlled patterning of plasmonic dimers by using an ultrathin nanoporous alumina membrane as a shadow mask," *ACS Appl. Mater. Interfaces* **9**, 36199–36205 (2017).
48. X. C. Fan et al., "Assembly of gold nanoparticles into aluminum nanobowl array," *Sci. Rep.* **7**, 2322 (2017).
49. C. L. Haynes and R. P. Van Duyne, "Nanosphere lithography: a versatile nanofabrication tool for studies of size-dependent nanoparticle optics," *J. Phys. Chem. B* **105**, 5599–5611 (2001).
50. A. Alharbi et al., "Physically unclonable cryptographic primitives by chemical vapor deposition of layered MoS," *ACS Nano* **11**, 12772–12779 (2017).
51. V. Lapidas et al., "Direct laser printing of high-resolution physically unclonable function anti-counterfeit labels," *Appl. Phys. Lett.* **120**, 261104 (2022).
52. Y. Du et al., "Nanoporous copper pattern fabricated by electron beam irradiation on Cu3N film for SERS application," *Phys. Status Solidi B* **256**, 1800378 (2018).
53. Q. Hao et al., "VO_2/TiN plasmonic thermochromic smart coatings for room-temperature applications," *Adv. Mater.* **30**, 1705421 (2018).
54. M. Xu et al., "A comprehensive survey of image augmentation techniques for deep learning," *Pattern Recognit.* **137**, 109347 (2023).
55. T. Silvério et al., "Functional mobile-based two-factor authentication by photonic physical unclonable functions," *AIP Adv.* **12**, 085316 (2022).

Perry Ping Shum is a chair professor in the Department of Electrical and Electronics Engineering at Southern University of Science and Technology, Shenzhen, China. He received his bachelor's and doctoral degrees in electronic and electrical engineering from the University of Birmingham, Birmingham, United Kingdom, in 1991 and 1995, respectively. He served at the School of Electrical and Electronic Engineering, Nanyang Technological University, from 1999 to 2020. His current research interests include fiber sensing, biophotonics, silicon photonics, and optofluidics. He is a fellow of IEEE, Optica, and SPIE.

Qi Hao is presently an associate professor in the School of Physics at Southeast University (SEU) in China. He received his PhD in physics from SEU in 2016. Following this, he undertook postdoctoral research at the Leibniz IFW Dresden in Germany from 2016 to 2019. His research focuses primarily on the development of functional nanoarrays for plasmonic applications.

Jiawei Wang is a professor in the School of Integrated Circuits at Harbin Institute of Technology, Shenzhen, China. He received his PhD in electronic and computer engineering from Hong Kong University of Science and Technology in 2016. He was a postdoctoral researcher at the Leibniz IFW Dresden and a research associate at the Chemnitz University of Technology from 2016 to 2020. His research group explores integrated all-optical and optoelectronic devices and their applications in hardware security and environmental sensing.

Biographies of the other authors are not available.