nature electronics

ARTICLES

https://doi.org/10.1038/s41928-022-00788-w

Check for updates

OPEN

Nanoscale physical unclonable function labels based on block copolymer self-assembly

Jang Hwan Kim[1,2], Suwan Jeon[1], Jae Hyun In[1], Seonho Nam[3], Hyeong Min Jin[4], Kyu Hyo Han[1,2], Geon Gug Yang[1,2], Hee Jae Choi[1,2], Kyung Min Kim[1], Jonghwa Shin[1], Seung-Woo Son[3], Seok Joon Kwon[5,6] ✉, Bong Hoon Kim[7] ✉ and Sang Ouk Kim[1,2,8] ✉

Hardware-based cryptography that exploits physical unclonable functions is required for the secure identification and authentication of devices in the Internet of Things. However, physical unclonable functions are typically based on anticounterfeit identifiers created from randomized microscale patterns or non-predictable fluctuations of electrical response in semiconductor devices, and the validation of an encrypted signature relies on a single-purpose method such as microscopy or electrical measurement. Here we report nanoscale physical unclonable function labels that exploit non-deterministic molecular self-assembly. The labels are created from the multilayer superpositions of metallic nanopatterns replicated from self-assembled block copolymer nanotemplates. Due to the nanoscale dimensions and diverse material options of the system, physical unclonable functions are intrinsically difficult to replicate, robust for authentication and resistant to external disturbance. Multiple, independently operating keys—which use electrical resistance, optical dichroism or Raman signals—can be generated from a single physical unclonable function, offering millisecond-level validation speeds. We also show that our physical unclonable function labels can be used on a range of different surfaces including dollar bills, human hair and microscopic bacteria.

As the Internet of Things (IoT) develops—and the number of devices that store personal data and interconnected over wireless networks increases[1–3]—there is a growing need for secure authentication and identification methods. Software-based validation systems are currently dominant but are potentially vulnerable to external disturbance such as hacking or electromagnetic interference[4–6]. Thus, hardware-based cryptography that exploits physical unclonable functions (PUFs) has been explored for IoT systems[7–14]. PUFs typically use anticounterfeit identifiers obtainable from randomized microscale patterns[11,15–19] or non-predictable fluctuation of the electrical response in semiconductor devices[20–22], and the validation of encrypted signature typically relies on a single-purpose method, including time-consuming microscopy or electrical measurement.

In this article, we report the development of a nanoscale PUF (nanoPUF) based on block copolymer (BCP) nanopatterning. Due to thermodynamically driven microphase separation behaviour that randomly occurs under thermal fluctuation[23–26], BCP self-assembly can provide large-area parallel formation of fingerprint lamellar patterns with critical dimensions down to 3 nm. At this scale, replication of the PUF label is nearly impossible without high cost as well as time-consuming characterization/fabrication tools. The labels are created from multilayer superpositions of metallic nanopatterns replicated from the self-assembled BCP nanotemplates[27,28]. A single nanoPUF can generate multiple, independently operating keys, which use electrical resistance, optical dichroism or Raman signals. This means that a particular authentication key can be chosen for a specific system, and multiple keys can be combined for an ultrahigh security rate. To illustrate the capabilities of our approach, we show that the nanoPUF labels can be used on a range of different surfaces: dollar bills, flexible polymer substrates, human skin, human hair, an ant body and microscopic bacteria.

Multipurpose nanoPUF label generation

Biological vein networks are a complex biological medium with non-predictable connectivity and randomized length scales and are useful for high-security authentication (Fig. 1a)[29,30]. The distinctive geometric features of a vein network are hidden under human skin, yet they offer an important method of biometrics, eligible for secure authentication using a near-infrared laser. Protection and anticounterfeiting of assets that require high security, such as the banknote, can be achieved by introducing vein-like PUFs, allowing high-speed authentication by optical or electrical detection (Fig. 1b). Such a bioinspired PUF can be created via the multilayer superposition of metallic nanopatterns replicated from BCP nanotemplates[27,28], which are formed by a non-deterministic self-assembly process relying on well-established microphase separation mechanisms[23,24,31] (Fig. 1c and Methods).

Nanoscale pattern dimensions are beyond typical optical resolution limits, and thus, the straightforward morphological validation of a nanoPUF label requires tedious microscopic scanning, such as scanning electron microscopy (SEM) or atomic force microscopy[32,33]. These time-consuming validation tools limit the potential practicality of an authentication system. Thus, our nanoPUFs,

[1]Department of Materials Science and Engineering, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea. [2]National Creative Research Initiative Center for Multi-Dimensional Directed Nanoscale Assembly, KAIST, Daejeon, Republic of Korea. [3]Department of Applied Physics, Center for Bionano Intelligence Education and Research, Hanyang University, Ansan, Republic of Korea. [4]Department of Organic Materials Engineering, Chungnam National University, Daejeon, Republic of Korea. [5]School of Chemical Engineering, Sungkyunkwan Unversity, Suwon-Si, Republic of Korea. [6]SKKU Institute of Energy Science and Technology (SIEST), Sungkyunkwan University, Suwon, Republic of Korea. [7]Department of Robotics and Mechatronics Engineering, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, Republic of Korea. [8]Materials Creation, Seoul, Republic of Korea. ✉e-mail: sjoonkwon@skku.edu; bonghoonkim@dgist.ac.kr; sangouk.kim@kaist.ac.kr

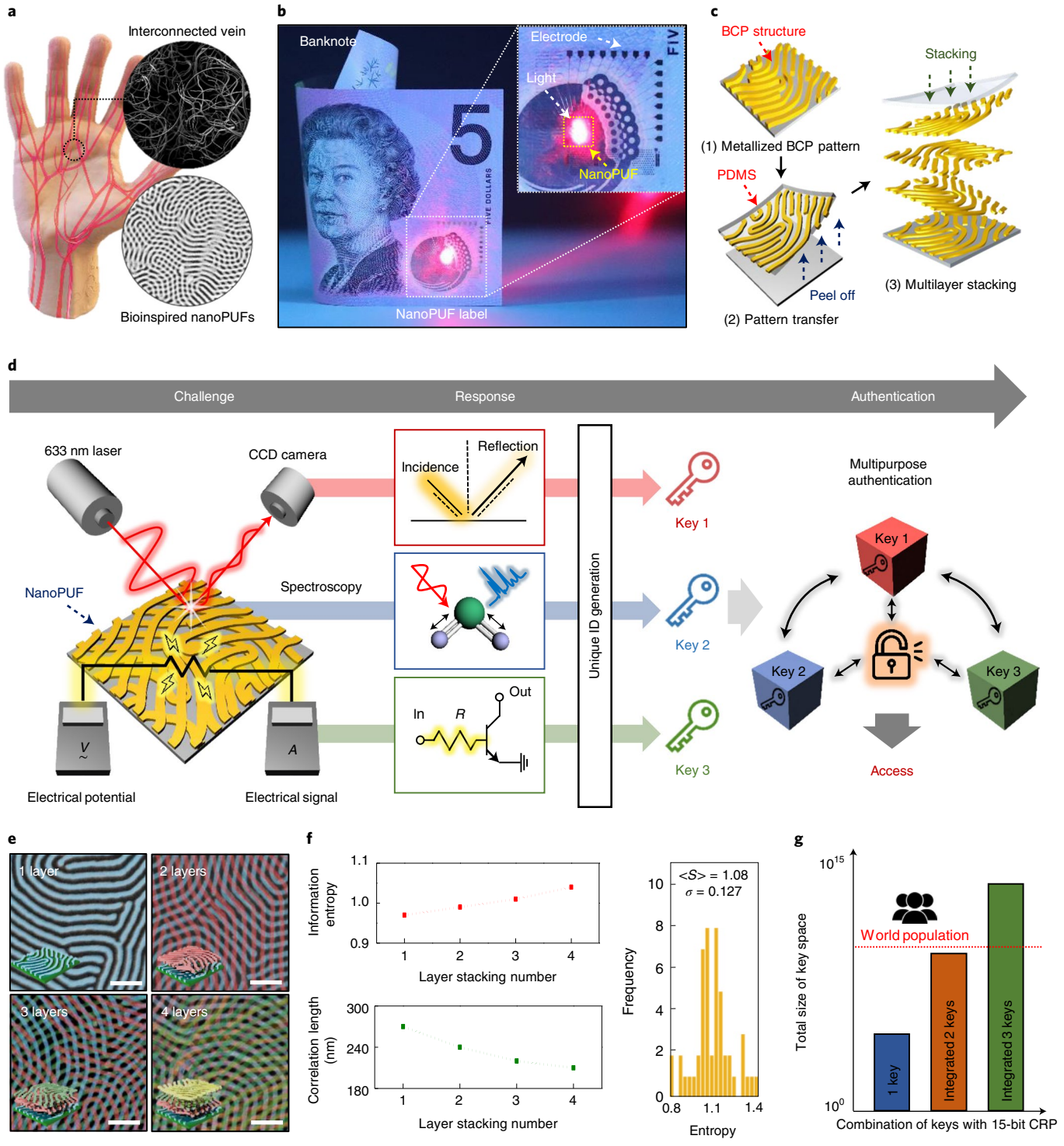


Fig. 1 | Self-organized multipurpose physical unclonable nanopatterns. a, Bioinspired motivation for nanoPUF. **b**, Real-world application of a PUF label to a banknote. **c**, Fabrication procedure for self-organized multilayer complex nanostructures. **d**, Multipurpose authentication mechanism for nanoPUF. **e**, SEM images of nanoPUFs for various layer stacking numbers. Scale bar, 200 nm. **f**, Physical properties of nanoPUFs for various layer stacking numbers. **g**, Total size of key space with the combination of authentication ways.

which are composed of nanostructured metals, respond to various physical stimuli—including electrical potential and polarized visible light—that can be used for effective validation within milliseconds and generating multiple unpredictable keys from an identical nanoPUF (Fig. 1d). These keys are encrypted through physically independent mechanisms—electrical resistance (electrical key, key 1), optical dichroism (dichroism key, key 2) and Raman scattering (Raman key, key 3)—enabling mutually independent authentication routes. Users are free to choose one of the authentication methods according to a demanded specific purpose. Furthermore, multilevel authentication with a high-security rate is possible through a combination of two or more independent authentication keys.

Multilayer stacking of BCP nanopatterns offers advantages for authentication labels. A monolayer BCP pattern provides a randomized fingerprint-like pattern with a unique length scale of lamellar period and localized orientation correlation among the neighbouring lamellae. More complex and less predictable interconnected nanopatterns can be generated via transfer printing of metallic nanopatterns, which can be overlaid several times (Fig. 1e). We theoretically calculated the two-dimensional (2D) information entropy and the orientational correlation length of the generated nanopatterns (Fig. 1f, Methods and Extended Data Fig. 1). A sample information entropy of a 2D matrix of continuous pixel values is employed, whereas the Hausdorff dimension of the 2D matrix is calculated for fractal dimension. As expected, the information entropy (pattern complexity) increases with the stacking number along with the reduction in orientational correlation length (local orientation). Multilayer stacking also allows the relatively narrow distribution of the order parameters over an arbitrarily large PUF label area. Small standard deviations for the spatial distribution of 2D information entropy (S) verify the uniform level of complexity yet fully non-predictable randomized pattern formation over the broad patterned area (Methods and Extended Data Fig. 1).

A further advantage of multilayer stacking is the reliable responsivity of the nanoPUF to physical validation methods, including electrical measurement and Raman scattering, where the formation of unpredictable conductive pathways or small nanogaps below the original lamellar period are crucial for the unpredictable signal generation. The resultant encoding capacity depends on the number of challenge–response pairs (CRPs) obtainable either from a single encryption method or a combination of several encryption methods (Methods and Fig. 1g). For example, a single key consists of a 15-bit CRP space in this work, subsequently yielding the key space of 2^{15} (Methods). Thus, the integration of only two independent validation methods can provide multibillions of key space, comparable to the worldwide population (almost 8.0×10^9). Moreover, the integration of all three methods provides an extremely large key space approaching 3.3×10^{13} (Methods). The overall encoding capacity can also be further improved by increasing the size of the CRP space for each key (inversely proportional to the pixel area for patterned measurements).

Operation of multipurpose key generation

Figure 2a illustrates the challenge–response authentication process for a nanoPUF. In the initial challenge generation step (green dashed line), arbitrary challenges are introduced into the processing unit of each method. Electrical potential, polarization angle of incident light and light exposure time are set as the typical challenges for the electrical, dichroism and Raman keys, respectively, whereas 15 strings of challenges are sequentially applied to a nanoPUF (typically, 200 μm is the distance between the electrodes for the electrical key, and $50.00\times50.00\,\mu m^2$ and $0.75\times0.75\,\mu m^2$ are the pixel sizes for the dichroism and Raman keys, respectively). In the next identification generation step (blue dashed line), the nanoPUF acts as a random number generator through unique interaction with the challenges. Subsequent digitalization is performed based on the comparison with arbitrarily set threshold values to yield 15 response bits. Final authentication (red dashed line) is carried out by comparing and evaluating the keys with preset databases.

One of the effective key generation methods from a nanoPUF relies on the generation of randomized patterns in electrical conductivity (Fig. 2b). A randomized electrical current response is expected depending on the output location even if an electrical potential is applied through an identical pair of electrodes in the nanoPUF. The electrical current is delivered through a randomized Kirchhoff resistance network composed of unpredictable combinations of conducting routes[34] (Fig. 2c). For a reliable measurement of the randomized signals without concerning the influence from measurement errors or noise, a reference electrode was fabricated on a non-patterned metal film, over which the current distribution was carefully confirmed. As shown in Fig. 2d, the reference (bare thin metal film) exhibits nearly no fluctuation in the electrical resistance level (less than the milliohm scale), whereas four randomly selected nanoPUF samples reveal considerably large fluctuations over the scale of tens of ohms. These unique output values can be transformed into binary signals (namely, barcodes or QR codes) by introducing a predetermined threshold current value (Fig. 2e, Methods and Extended Data Fig. 2).

Another method for key generation exploits the inherent optical dichroism of the nanoPUF pattern. It is well known that a subwavelength-scale metallic nanowire pattern exhibits strong optical dichroism depending on the incident wavelength and polarization[35]. This dichroism is principally determined by the local anisotropy in the in-plane orientation of nanowires, as verified by a simulation study (Fig. 2f) (Methods and Extended Data Fig. 3). Indeed, a nanoPUF formed on a quartz substrate presents a distinctive linear dichroism with polarization-selective transmission of incident light (Fig. 2g), leading to a unique intensity distribution of reflectance for a polarized incidence beam (Extended Data Fig. 4). For practical key generation, we randomly selected a 15-point set and compared the intensity distribution of the reflectance (linearly polarized light with a wavelength of 633 nm) with respect to a predetermined threshold value (Methods and Extended Data Fig. 5).

Our third method of key generation utilizes the intensity distribution of Raman scattering from a nanoPUF. Plasmonic materials with nanoscale features, including gaps, crevices or sharp geometry, induce a strong amplification of incident light, caused by the localized surface plasmon resonance, to yield signature patterns of Raman scattering intensity[36,37] (Fig. 2h). A unique plasmonic resonance is expected depending on the local angle between the stacked metal nanowires in our nanoPUF. Randomly occurring lateral gaps between the nanowires in different stacking layers are principally responsible for the enhancement in the Raman signal due to the smaller gap sizes compared with the original lamellar period (Fig. 2i, Methods and Extended Data Fig. 6). Raman keys can be readily generated by measuring the scattering intensities at the selected 15-point sets and the subsequent comparison with a threshold (Extended Data Figs. 3 and 7).

We have performed a quantitative statistical analysis of important PUF security parameters based on the experimental characterization, including uniqueness, bit aliasing and reliability[38,39] (Table 1 and Methods). Here 12 PUF cores are fabricated with 15 digital strings for each key generation. All the different key generation schemes introduced in this work exhibit nearly ideal uniqueness (that is, mean values for the measured responses of $\mu_{Electrical}=41.90\%$, $\mu_{Dichroism}=43.66\%$, $\mu_{Raman}=50.61\%$ and $\mu_{Integrated}=45.39\%$), confirming that each nanoPUF is well distinguishable from others for all the different validation mechanisms. The mean values for bit aliasing are sufficient to avoid similar responses from different PUF labels (that is, $\mu_{Electric}=28.75\%$, $\mu_{Dichroism}=32.81\%$, $\mu_{Raman}=46.11\%$ and $\mu_{Integrated}=35.89\%$). For reliability, the mean values ($\mu_{Electrical}=99.48\%$, $\mu_{Dichroism}=99.69\%$, $\mu_{Raman}=98.33\%$ and $\mu_{Integrated}=99.15\%$) are close to the ideal value (100%) to guarantee that a nanoPUF core can reproduce the same response bits under the same validation condition in a robust way. Furthermore, not only high-speed authentication is possible as a given nanoPUF generates multiple keys but high accessibility is also attainable by the unique response even with a macroscale identification resolution. Besides, it is possible to further enhance the encoding capacity by increasing the number of measurement set points for the bit generation.

Our experiment considers a simple case with six electrodes in electrical measurement or 15 points in optical and Raman measurement for the proof-of-concept realization of a nanoPUF. The size of the CRP space can be easily enlarged for our nanoPUF. For instance, in

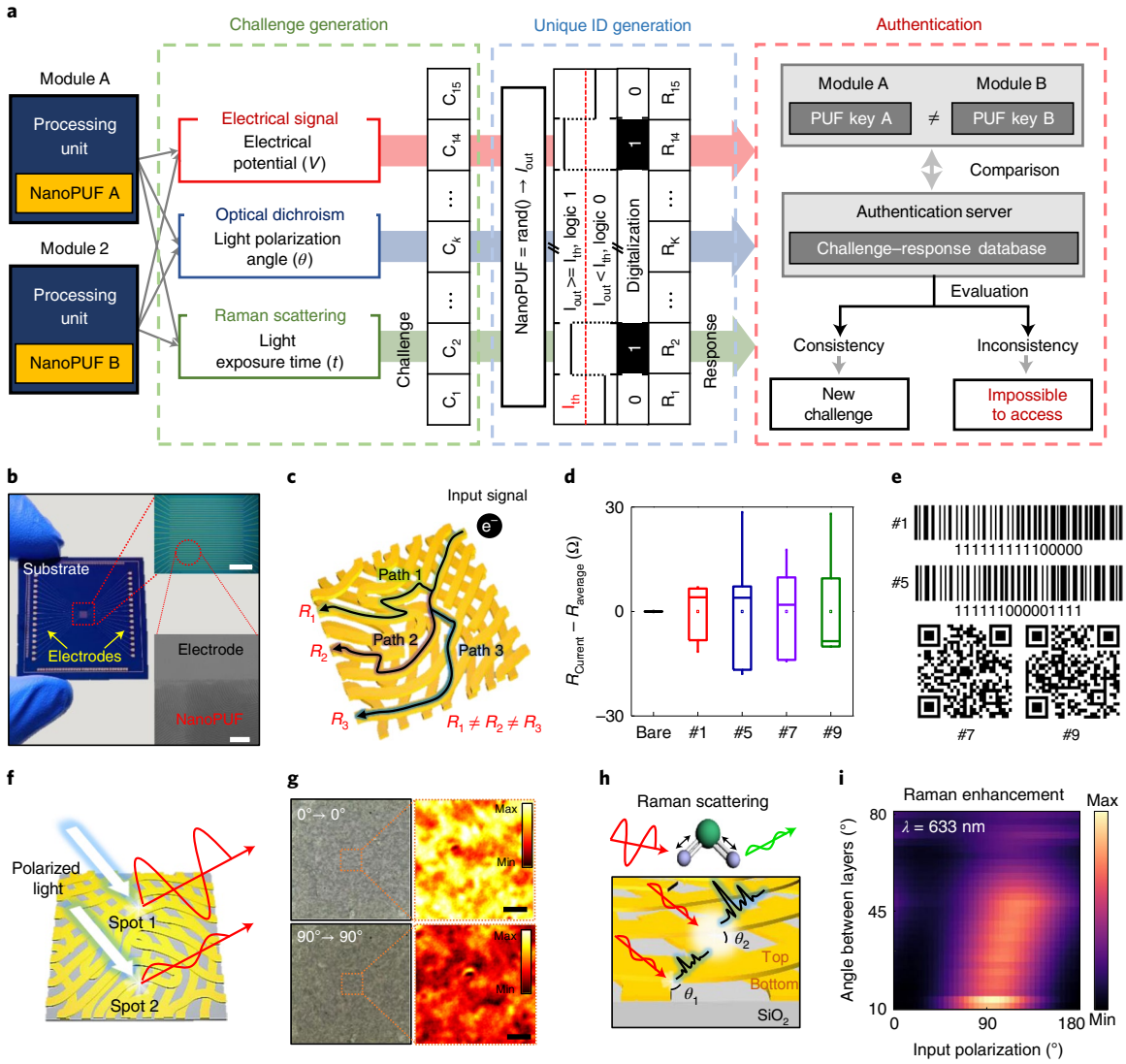


Fig. 2 | Encryption functionalities of nanoPUFs using electrical and optical properties. a, Challenge–response authentication process for a nanoPUF. **b**, Electrical measurement scheme for electrical key generation. Scale bars, 150 mm (top), 1 μm (bottom). **c**, Randomized electrical pathways in a multilayer interconnected nanoPUF. **d**, Random generation of electrical responses from a nanoPUF. **e**, Electrical key generation from various samples with different electrical thresholds. **f**, Different reflection intensities for polarized incident visible light at different spots in a nanoPUF. **g**, Polarized optical microscopy for different reflection states taken at the same sample location. Scale bars, 30.0 mm (left), 0.2 mm (right). **h**, Intensity difference in Raman scattering depending on the angle between the overlaid nanowires in stacked lamellar layers. **i**, Theoretical simulation of Raman enhancement for various input polarizations and angles between stacked nanowires.

Table 1 | PUF parameters of various authentication methods

Method	Scan speed	Resolution	Uniqueness (%)	Bit aliasing (%)	Reliability (%)	Key space (this work)
Electrical	~10 μs	~μm	41.90	28.75	99.48	2^{x} (2^{15})
Birefringence	~μs	~μm	43.66	32.81	99.69	2^{z} (2^{15})
Raman	~100 ms	~μm	50.61	46.11	98.33	2^{y} (2^{15})
Integrated	~ms	μm	45.39	35.89	99.15	2^{x+y+z} (2^{45})

the electrical method, 25 electrodes with the typical width and space down to 20 μm (centre-to-centre distance between the electrodes, 40 μm) can be readily fabricated on a single side of 1 mm × 1 mm PUF pattern by conventional photolithography, thereby incorporating a total of 100 electrodes at all the sides of a PUF pattern. For an exemplary case employing 50 μm width and space (centre-to-centre distance between the electrodes, 100 μm), ten electrodes on one side and a total of 40 electrodes can be generated over a 1 mm × 1 mm PUF. From the combination of 40–100 electrodes, 780 ($_{40}C_2$)–4,950 ($_{100}C_2$)-bit CRP space can be generated. On average, an approximately 2,000-bit CRP space can be easily generated solely for the electrical validation method.

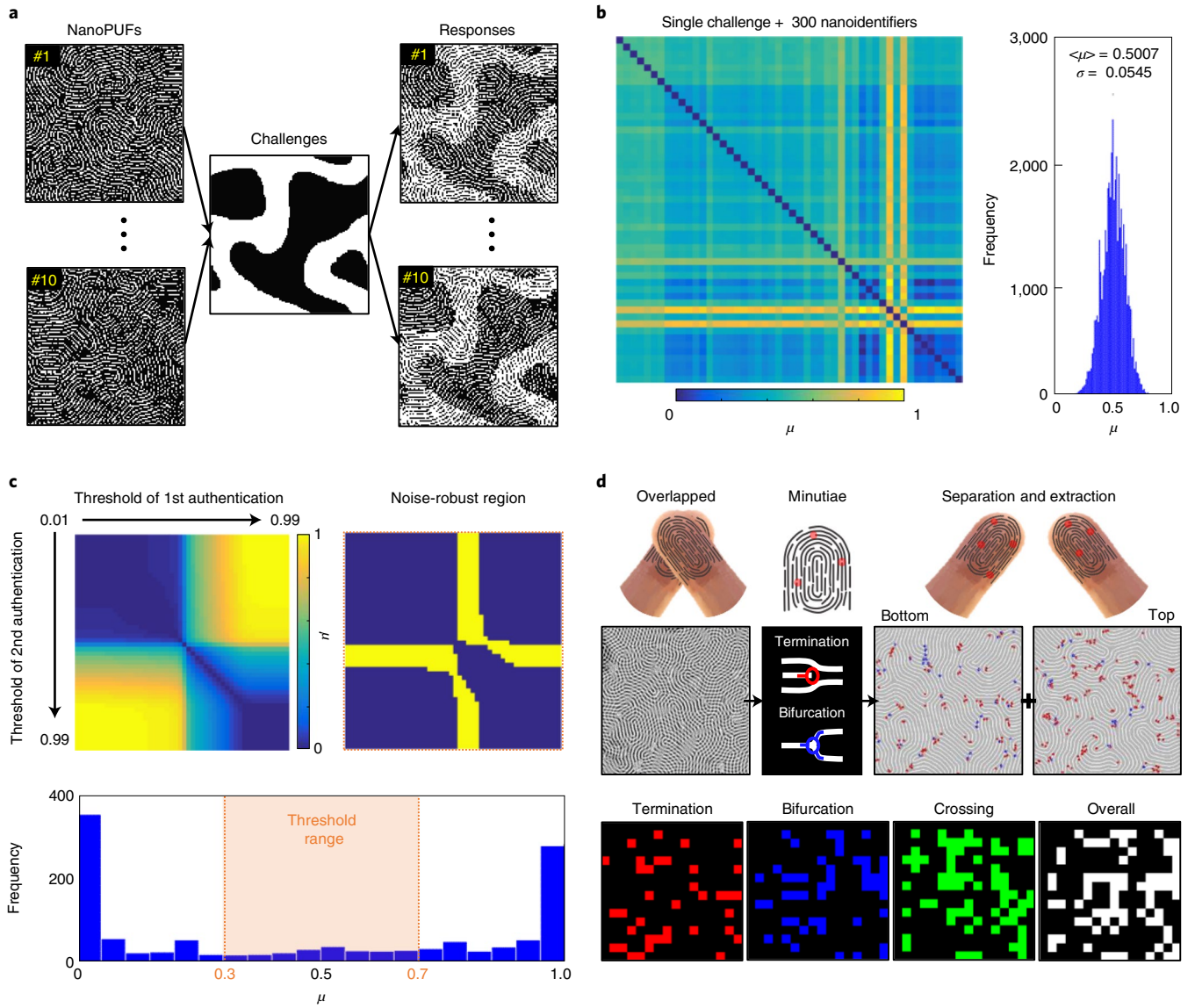


Fig. 3 | Challenge–response operation and morphological functionalities of nanoPUFs. a, XOR operation with a single challenge for multiple nanoPUF samples. **b**, Hamming distance distribution between responses from single challenge–different PUFs operation. **c**, Noise robustness test under various threshold conditions. **d**, Application of conventional fingerprint recognition principle to a nanoPUF.

Both optical dichroism and Raman-based validation methods can also provide vastly expanded CRP spaces. It is technically easy to prepare hundreds—or even thousands—of measurement pixels, as the typical spatial resolution of beam focusing is smaller than 10 μm. For the PUF area of 200 μm × 200 μm along with a spatial pixel resolution of 10 μm, we can generate a total of 400 pixels. It is possible to transform these 400 pixels into mutually independent one-dimensional (1D)-bit strings using several 2D-to-1D matrix transformation schemes, such as zigzag (that is, left or right, up or down), spiral (in or out, left or right) and space-filling curves (that is, Hilbert curve, Gosper curve, Koch curve and so on). The total number of these schemes is approximately ten. Therefore, the CRP space for optical dichroism method can be extended up to at least $400 \times 10 \approx 4{,}000$ bits. We suggest a similar manner for the Raman-based method to produce another 4,000-bit CRP space. As those three validation methods are mutually independent, it is possible to prepare an approximately $2{,}000 + 4{,}000 + 4{,}000 = 10{,}000$-bit CRP space. This scale obviously satisfies the typical criterion for a strong PUF, as the total key space is $\sim 2^{10{,}000}$ ($\sim 10^{3{,}010}$) to fulfil the requirements for a wide range of authentication purposes.

Extreme high-security nanopattern identifiers

Apart from the interesting key generation mechanisms from various physical responses, the nanoscale morphology of a nanoPUF itself can be potentially utilized as a reliable nanoidentifier for authentication. The possible number of distinguishable nanoidentifiers with a single kind of defect structure within a 1 μm × 1 μm area can be calculated as 4.8×10^{35} in our nanoPUF (Methods). Figure 3a presents that ten different nanoidentifiers exhibit sufficiently discernible responses to a single binary image challenge pattern based on a simple exclusive-OR (XOR) operation. Here 300 nanoidentifiers are identified (Supplementary Information) to yield a set of sufficiently different response patterns with the average Hamming distance ($<\mu>$) close to 0.5 (that is, $<\mu> = 0.5007 \pm 0.0545$) (Fig. 3b and Extended Data Fig. 8). This assures that a nanoPUF can serve as a unique security medium. Conversely, one nanopattern identifier can discriminate different challenges with the average Hamming

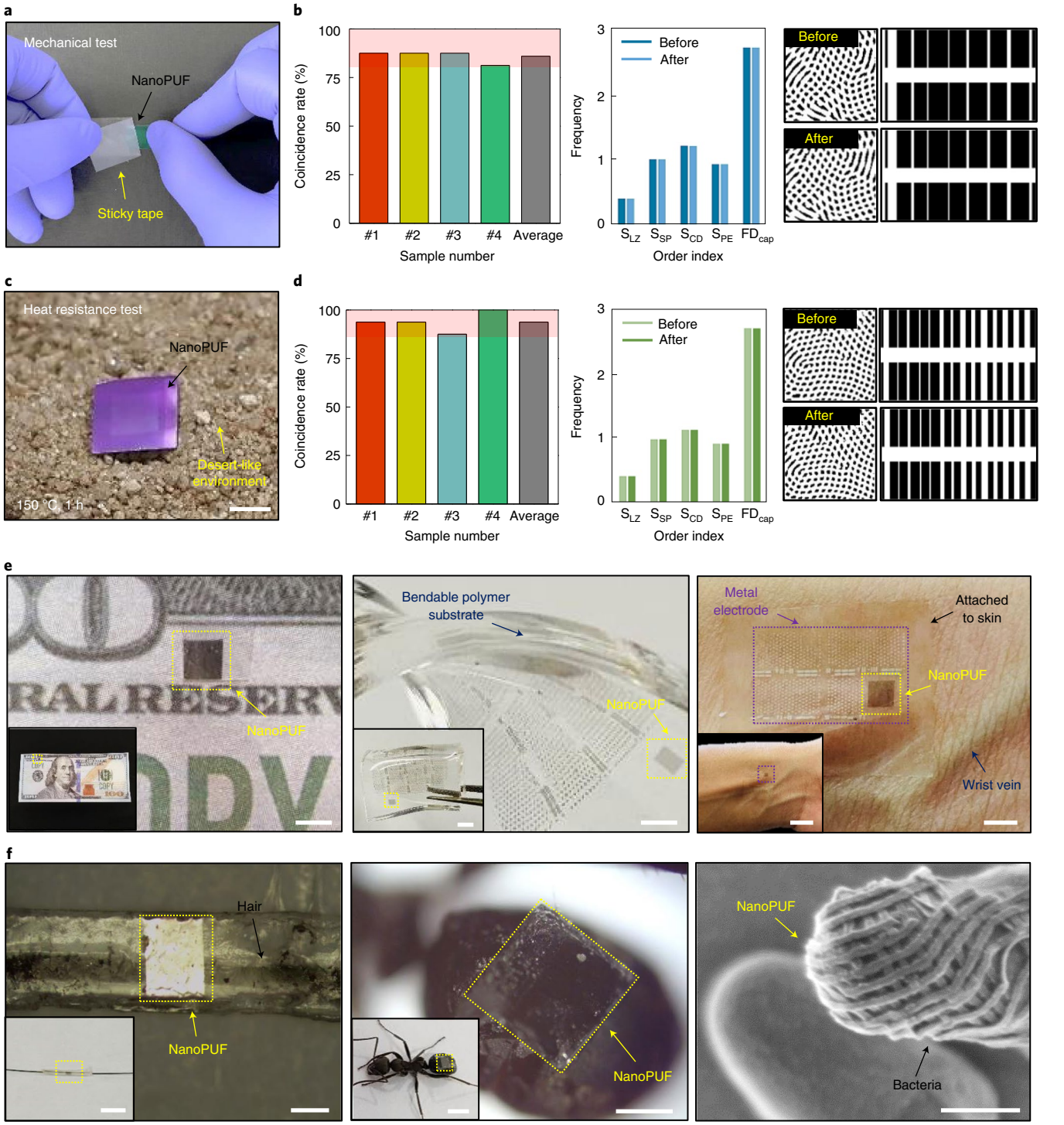


Fig. 4 | Practical application of miniaturized nanoPUFs. a, Mechanical stability test for a nanoPUF label. **b**, Variation in the physical properties and key performance after the mechanical stability test. **c**, Thermal stability test for a nanoPUF label. Scale bar, 0.5 cm. **d**, Variation in physical properties and key performance after thermal treatment. **e**, Application of nanoPUF labels to arbitrary objects, including a paper bill (left; scale bar, 0.5 cm), deformable transparent polymer substrate (middle; scale bar, 3 mm) and human wrist (right; scale bars, 4 mm and 20 mm (inset)). **f**, High-precision hidden labelling in human hair (left; scale bars, 50 μm and 1.5 mm (inset)), ant body (middle; scale bars, 50.0 mm and 3.0 mm (inset)) and microbacteria surface (right; scale bar, 300.0 nm).

distance close to 0.5 again (that is, $<\mu> = 0.4993 \pm 0.0082$) (Extended Data Fig. 8).

For an image-based nanoidentifier, noise robustness is a crucial requirement. As shown in Fig. 3c (Extended Data Fig. 8), although different threshold pixel values are set for the binarization of the greyscale image (that is, 50 different levels from 0.01 to 0.99), a nanoidentifier can provide distinguishable Hamming distance for a sufficiently wide range of thresholds, verifying safe and reliable authentication. Generally, random lamellar nanopatterns include topological defects, such as terminations and bifurcations (Fig. 3d).

The unique distribution of such defects is compatible with the identification algorithm for fingerprint pattern recognition[40,41]. From a bilayer stack of BCP patterns, spatial coordinates of topological defects can be separately extracted from the top and bottom layers (Methods and Extended Data Fig. 9). Multilayer stacking also yields additional topological defects, such as crossing points. The digitalized images for terminations, bifurcations and crossing points are constructed with a designated pixel resolution. It is noteworthy that there are other types of structural defect that can also serve as independent identifiers, such as ridge island (or short ridge), dot, bridge, spur, eye (or enclosure), double bifurcation, delta, swirl, trifurcation and so on (Extended Data Fig. 10b). Therefore, at least 12 different groups with at least ten identifiers are present, which makes 120 bits for the nanoidentifier (that is, the CRP space for the nanoidentifier is ~120 bits). The estimated maximum code capacity of a single nanopattern layer is 5.32×10^{81}. When two BCP layers are overlapped in this work, the maximum code capacity is 2.83×10^{163}, which is a sufficiently large number for high-level security applications. Consequently, a nanoidentifier can serve as a unique encryption or authentication key solely based on topological defect distribution. Notably, recent progress in high-throughput nanoscale microscopy, including multitip parallel atomic force microscopy scanning, can be employed for rapid and highly secure authentication by exploiting the inherent high encoding capacity from miniaturized nanoscale features. Nonetheless, a thorough characterization of the entire nanoscale pattern must be avoided, as it significantly threatens the security of our PUF. In this regard, optically transparent adlayer formation above the surface of the nanoPUF can be suggested, which can prevent the direct contact of scanning probe or electron beam to the nanoscale pattern, whereas electrical or optical validation can still be functional.

Stability and application of nanoPUF labels

We have tested the stability and sustainability of the nanoPUF system under various environmental conditions. Practically, PUF labels are required to work on various types of material and geometry at the target surfaces. For long-term reliable operation, PUF labels are also required to be robust against external disturbances induced by undesired physical contacts. The mechanical robustness of a nanoPUF was evaluated by the repeated attaching and detaching of commercially available sticky tapes at the PUF label surfaces (Fig. 4a) for 30 cycles. Electrically generated keys from different samples show a high sustainability and fidelity of $85.93\pm4.73\%$ (Fig. 4b). The original nanoscale geometry is also well maintained, as verified from the minimal changes in information entropy and fractal dimension. It is noteworthy that mechanical stability can be further improved by employing protective encapsulation. A thermal stability test was conducted under the harsh condition of 150 °C for 1 h (Fig. 4c). Electrically generated keys from different samples reveal the high thermal stability with a coincidence rate of $93.75\pm6.25\%$, as the nanoscale security performance is well sustained (Fig. 4d).

Figure 4e presents the versatile implementation of a nanoPUF at arbitrary target surfaces. NanoPUF labels are well integrated at the surface of a dollar bill for an anticounterfeit tag and also stabilized at the flexible polymeric surfaces and human skin for wearable or skin-attachable IoT devices. Taking advantage of the intrinsic small size and flexible thin geometry, nanoPUF labels are easily integrated onto arbitrary non-planar deformable surfaces as hidden labels. Interestingly, our high-precision miniature labels can be implemented onto unusually small objectives (Fig. 4f). A PUF label can make conformal contact at the high-curvature surface of a single strand of human hair (radius of curvature, ~80 μm). Furthermore, it can be stabilized for small living organisms, such as ants or even microscopic bacteria (~1 μm), for the unique identification of those organisms from their colonies.

Conclusions

We have shown that non-deterministic molecular self-assembly, which occurs under thermal fluctuation, can be used to create nanoscale PUF labels with secure characteristic dimensions and large encoding capacities. The approach provides reliable multipurpose authentication, including electrical and optical responses as cryptographic key generators, with fast validation speeds. Our technique downscales the critical dimensions of PUFs and could provide a generalized platform for advanced authentication systems, with potential use in, for example, hidden miniature identifiers on arbitrary surfaces or distributed multikey integrated authentication systems. The large range of material choices available with PUF labels is also potentially beneficial for ubiquitous labelling, even under harsh electromagnetic-pulse shock or invasive high-energy radiation. The seamless integration of our nanoPUF with the necessary validation tools would be a valuable next step and could lead to versatile applications including hardware-based on-demand cryptographic key generation.

Methods

Materials and characterizations. All the polymers, including BCPs (PS-*b*-PMMA) and hydroxyl-terminated P(S-*r*-MMA) random copolymers, were purchased from Polymer Source. Toluene (99.8%, anhydrous) and tetrahydrofuran (99.9%, anhydrous) were purchased from Sigma Aldrich. Hydrofluoric acid (48.0%–51.0%, ACS Reagent) was purchased from J.T.Baker. SYLGARD 184 silicone elastomer base and curing agent were purchased from Sigma Aldrich. Furthermore, 5,000 Å wet-deposited 4-inch P<100> silicon dioxide wafers were purchased from iTASCO. Sticky tape (Scotch Magic Tape) for mechanical stability test was purchased from 3M.

Electrical current measurement. All the electrical characterizations were performed using a Keithley 4200A-SCS instrument. Every cell was applied to a voltage pulse under the same conditions repetitively: voltage amplitude, 1 V; rise and fall time, 1 μs; pulse width, 10 μs, time step, 20 ns; applied voltage, five times.

Polarized optical reflectivity measurement. A polarized optical microscope was developed to obtain the polarized reflectance map in a single shot. To capture the fine reflection features by local orientation, the microscope was equipped with an objective lens (MY10X-803, Thorlabs) and a tube lens for magnification. For polarized detection, the sample was illuminated with linearly polarized light with a wavelength of 633 nm (HeNe laser, Newport), and reflected light from the sample was detected by a complementary metal–oxide–semiconductor camera (DCC3240M, Thorlabs) with a linear polarizer (LPVISE100-A, Thorlabs); the polarization angles in both sides of the source and detector were matched. In the last step, the detected image was normalized by a silver mirror to constitute a polarized reflectance map.

Raman scattering measurement. Raman scattering of the fingerprint metal patterns was observed using a dispersive Raman spectrometer (ARAMIS, Horiba Jobin Yvon). Raman scattering measurements were operated with a 633 nm wavelength laser and 100 ms exposure time.

SEM measurement. Morphology of the self-assembled BCP films and fingerprint metal patterns were observed using SEM (S-4800, Hitachi). To enhance the image contrast and identify each layer of the multilayer stacked sample, SEM measurements were operated in 3 kV in the backscattered electron mode.

Non-deterministic nanopatterning by BCP self-assembly. BCPs and hydroxyl-terminated random copolymers were used as received without any purification. Surface energy of all the silicon oxide substrates was neutrally modified with the hydroxyl-terminated random copolymer brush treatment. Briefly, a neutral brush layer was spin casted from 1 wt% toluene solution onto a silicon substrate after ultraviolet ozone treatment. The substrates were thermally treated at 160 °C in a vacuum for 12 h and then rinsed with toluene to remove unreacted brush molecules. The PS-*b*-PMMA solution was prepared by blending two PS-*b*-PMMA BCPs (M_n (the number average molecular weight) values of one set of PS and PMMA blocks, 105 and 106 kg mol^{-1}, respectively, and M_n values of the other set of PS and PMMA blocks, 5 and 5 kg mol^{-1}, respectively) with a 7:3 weight ratio with toluene (total polymer concentration, 1.5 wt%). The BCP thin films were spin casted onto brush-treated silicon oxide and annealed under tetrahydrofuran vapour atmosphere for 1–2 h at room temperature.

Metal fingerprint nanopattern formation. For pattern transfer from BCP thin films onto metal nanopatterns, PMMA lamellar nanoscale domains in the BCP thin film were selectively etched by O_2-plasma reactive ion etching, and the desired

metal layer was electron-beam evaporated onto the entire substrate surface area with a deposition thickness of 10–20 nm, followed by a lift-off process under sonication.

Transfer printing of metal nanopatterns. A polydimethylsiloxane (PDMS) stamp film was prepared by blending SYLGARD 184 silicone elastomer and curing agent at a 10:1 weight ratio, followed by a crosslinking reaction under a vacuum at 60 °C for 6 h. To peel off the metal fingerprint pattern from the silicone oxide substrate onto the PDMS stamp, the underlying silicone oxide layer was etched by hydrogen fluoride vapour. The metal pattern stabilized at the PDMS surface was stamped at the desired substrates.

Calculation of entropy of BCP self-assembled nanopatterns. *Sample entropy.* For the given data with length of N, $U=[u(1)\ u(2)\ldots u(N)]$, we can calculate the sample entropy with a sampling algorithm accompanied by embedding the dimension. For sampling, sample data $X(i)$ with length m can be extracted as follows:

$X(i)=[u(i)\ u(i+1)\ u(i+2)\ldots u(i+m-1)]$, $i=1, 2,\ldots N-m+1$.

Using $X(i)$, we can calculate the certain information measure defined as

$$C_i^m(r) = \frac{(\text{number,of } X(j) \text{ s.t. } d[X(i),X(j)]) \le r}{N-m+1},\ d[X, X^*] = \max_a |u(a) - u^*(a)|, \tag{1}$$

where $d[X, X^*]$ denotes the scalar distance between the two data vectors X and X^* and r is the threshold distance. Typically, r is set as $r=0.2\sigma$, where σ denotes the standard deviation of the overall data. Using the statistical sampling measure $C_i^m(r)$, we can calculate the variation rate of normalized information, $C_i^m(r)/(N-m)$, and translate it into the sample entropy S_{SP} as follows:

$$S_{SP} = -\log\left(\frac{\frac{C_i^{m+1}(r)}{(N-m+1)}}{\frac{C_i^m(r)}{(N-m)}}\right) = -\log\left(\frac{\#(m+1)}{\#(m)}\right). \tag{2}$$

The distribution of sample entropy of 50 bilayer PUF labels is shown in Extended Data Fig. 1.

LZ entropy. Lempel–Ziv (LZ) entropy relies on the calculation of LZ complexity[42]. For the calculation of LZ complexity, we converted the raw data into binary data with a threshold set as the overall average. With binary data, different combinations and its occurrence frequency can be translated into information complexity. When N is sufficiently large, it is known that C_{LZ} approaches the Kolmogorov complexity. A detailed calculation algorithm for LZ complexity, C_{LZ}, can be found elsewhere[42]. With this, we can calculate the LZ entropy S_{LZ} as

$$S_{LZ} = \frac{C_{LZ}}{\max(C_{LZ})} = -\frac{C_{LZ}\log_2 N\left(p\log_2 p + (1-p)\log_2(1-p)\right)}{N}. \tag{3}$$

The distribution of LZ entropy of 50 bilayer PUF labels is shown in Extended Data Fig. 1.

Permutation entropy. The entropy of information can also be calculated by considering the relative occurrence frequency of the ordinal pattern. To calculate the ordinal pattern frequency, we can apply a sampling method using order number d and delay τ such that

$$X_i^{(\tau)} = [x(i)\ x(i+\tau)\ldots x(i+d\tau)].$$

The sample data are coded with the inversion number, which denotes the possible permutation types. For example, $X_i^{(2)}$ has $3!=6$ possible permutations, which provides six different inversion numbers for the code. The code can be systematically generated with the following relationship:

$$n_d(i_1, i_2, \ldots, i_d) = \sum_{l=1}^{d} \frac{i_l\,(d+1)!}{(l+1)!}$$

With a fixed window length W, a vector containing the permutation code P with W components can be generated. For the kth window vector, we can count the occurrence frequency of certain permutation code p, $q_p(k)$. Using $q_p(k)$, we can calculate the permutation entropy S_{PE} as

$$S_{PE} = \frac{S(d,\tau,M,t)}{S_{max}} = \frac{-\sum_{j=0}^{(d+1)!-1}\frac{q_j(t)}{M}\log\frac{q_j(t)}{M}}{-\frac{(d+1)!}{M}\log\frac{1}{M}}, \tag{4}$$

The distribution of permutation entropy of 50 bilayer PUF labels is shown in Extended Data Fig. 1.

Conditional permutation entropy. To correct the noise effects on information measure, permutation entropy can be further revised into empirical conditional permutation entropy S_{CD}. This measure considers the delay effects on permutation entropy such that

$$S_{CD} = -\sum_{j=0}^{(d+1)!-1}\sum_{l=0}^{(d+1)!-1}\frac{q_j(t)}{M}\frac{p_{j,l}(t)}{q_l(t)}, \tag{5}$$

where $p_{j,l}(t)$ denotes the number of combinations with ordinal pattern code l of the sample data with delay τ, $X_{t+\tau}^{(\tau)} = [x(t+\tau)\ x(t+2\tau)\ldots x(t+d\tau+\tau)]$, given the sample data $X_t^{(\tau)} = [x(t)\ x(t+\tau)\ldots x(t+d\tau)]$, which has the ordinal pattern code j. The distribution of conditional permutation entropy of 50 bilayer PUF labels is shown in Extended Data Fig. 1.

Calculation of fractal dimensions of BCP self-assembled nanopatterns. We employed generalized entropy at order q to measure the fractal dimension of self-assembled nanopatterns. First, the dimension spectrum D_q can be defined as

$$D_q = \lim_{\mathbf{r}\to 0}\frac{1}{q-1}\frac{\log\left[\sum_{i=1}^{M(r)} p_i^q\right]}{\log(r)},\ p_i = \frac{N_i}{N},\ q = 0,\ 1,\ 2, \ldots, \tag{6}$$

where $M(r)$ denotes the number of hypercubes to cover the data or geometric patterns in the mth dimension with a unit hypercube with unit length r, N denotes the total number of signals or points in the data and N_i is the total number of data points in the ith hypercube.

Capacity fractal dimension. In the case of $q=0$, the dimension spectrum corresponds to the Kolmogorov capacity or Kolmogorov dimension, which is mathematically identical to the Hausdorff dimension and is expressed as

$$D_0 = \lim_{\mathbf{r}\to 0}\frac{\log M(r)}{\log(1/r)}. \tag{7}$$

The capacity fractal dimension is a typical fractal dimension (denoted as FD_{cap} in the paper). The distribution of capacity fractal dimension of 50 bilayer PUF labels is shown in Extended Data Fig. 1.

Information fractal dimension. In the case of $q=1$, the dimension spectrum can be expressed as

$$\begin{aligned} D_1 &= \lim_{\mathbf{r}\to 0}\lim_{\mathbf{q}\to 1}\frac{1}{q-1}\frac{\log\left[\sum_{i=1}^{M(r)} p_i^q\right]}{\log(r)} \\ &= \lim_{\mathbf{r}\to 0}\frac{1}{\sum_{i=1}^{M(r)} p_i^{q\to 1}}\frac{\sum_{i=1}^{M(r)} p_i^{q\to 1}\log p_i}{\log(r)} \\ &= \lim_{\mathbf{r}\to 0}\frac{1}{\sum_{i=1}^{M(r)} p_i}\frac{\sum_{i=1}^{M(r)} p_i\log p_i}{\log(r)} = -\lim_{\mathbf{r}\to 0}\frac{\sum_{i=1}^{M(r)} p_i\log p_i}{\log\left(\frac{1}{r}\right)}, \end{aligned} \tag{8}$$

where the numerator in equation (8), namely, $-\sum_{i=1}^{M(r)} p_i\log p_i$, is the Shannon entropy, and therefore, this fractal dimension corresponds to the information fractal dimension (denoted as FD_{inf} in the paper).

Correlation fractal dimension. In the case of $q=2$, the dimension spectrum can be expressed as

$$\begin{aligned} &D_2 = \lim_{r\to 0}\frac{\log[C(r)]}{\log(r)}, \\ &C(r) = \sum_{i=1}^{M(r)} p_i^2 \approx \frac{\sum_{i=1,\, j>i}^{N} H\left(r-\rho(\mathbf{x_i},\mathbf{x_j})\right)}{\frac{N(N-1)}{2}},\ H(x) = \begin{cases} 1 \text{ if } x \ge 0 \\ 0 \text{ if } x < 0 \end{cases}, \end{aligned} \tag{9}$$

where $H(x)$ is the Heaviside function and $\rho(x_i, x_j)$ is the Chebyshev distance between the two points x_i and x_j, which is defined as

$$\left(\mathbf{x_i},\mathbf{x_j}\right) = \sqrt{\sum_{k=1}^{m}\left(x_i(k) - x_j(k)\right)^2},\ \mathbf{x_i} = [x_i(1)\ x_i(2)\ldots x_i(m)].$$

In equation (9), $C(r)$ denotes the correlation function of the data points with distance r, and therefore, D_2 corresponds to the correlation fractal dimension (denoted as FD_{cor} in the paper).

Calculation of orientational order and correlation of self-assembled patterns. We employed a quantitative algorithm for evaluating the local orientation of self-assembled patterns in BCP thin films based on the principal components analysis algorithm. This algorithm analyses the local orientation of each pixel in the noise-processed greyscale electron microscopy images by calculating the local gradient vectors and their maximum likelihood to determine the governing orientation vector[43]. The local orientation can be represented by local orientation

angle θ', which can be rewritten as the degree of angular deviation from the average angle $\langle\theta'\rangle$ such that $\theta=\theta'-\langle\theta'\rangle$. Using θ, we calculated the pair correlation function of position-dependent local orientation[44,45] $g(r)$ such that

$$g(\mathbf{r}) = \frac{1}{N}\sum_{\mathbf{r}'}\theta(\mathbf{r})\,\theta(\mathbf{r}'), \tag{10}$$

where r and r' are the 2D position vectors of the pixels in the image and N denotes the total number of pixels in the images. From the statistical point of view, $g(r)$ provides quantitative information on the spatial variation in the orientational order over a certain distance. Therefore, it is possible to obtain a characteristic length scale for the persistence of orientational order such as an orientational-order correlation length L_{corr}, which corresponds to the smallest value of r satisfying $g(r)=0$, where $r=|r|$. A plot of the correlation function with the number of overlapped layers is depicted in Extended Data Fig. 1.

Key generation process consisting of digital bits and encoding capacity calculation. *Electrical key generation.* At least six electrodes are fabricated on the PUF label, and two electrode pairs are selected to measure the electrical current. The number of combinatorial electrode pairs is ${}_6C_2$, a total of 15. By measuring the resistance value between the electrode pairs and comparing them with an arbitrarily set threshold value (for example, the average of the resistance value), digitalization that assigns 0 or 1 proceeds to generate 15 bits (Extended Data Fig. 2). Consequently, the size of the key space that can be generated with our 15-bit CPR is 2^{15} from a single-PUF label.

Dichroism key generation. In dichroism key generation, the size of the CRP space can be assigned by dividing a reflectance map into multiple sections. As illustrated in Extended Data Fig. 4, the measured reflectance map of 200 μm × 200 μm is divided into 4 × 4 sections with each section size of 50 μm × 50 μm; 15 sections are selected among them. These patterned reflectance values can be multiplied by a normal distribution $N(\boldsymbol{\mu}=\boldsymbol{\mu}_{centre}, \sigma^2=(12\,\mu m)^2)$, where $\boldsymbol{\mu}_{centre}$ is the centre point of each section, to reduce the boundary effect, which helps consistent key generation under a minor shift variation in the image. After integrating the intensity of each section, the signal can be binarized compared with the preassigned threshold (Extended Data Fig. 5). Based on this process, one can generate unique dichroism keys, whose bits follow local polarization properties, depending on the complexity of metallic nanowires, which is extremely difficult to be replicated.

Raman key generation. Raman scattering measurements were carried out after aligning PUF labels using the preformed align keys. After laser exposure, the entire sample area is divided into 15 regions to compare the Raman scattering intensity from each region with an arbitrarily set threshold value (for example, the average of the Raman scattering intensity). Digitalization proceeds to generate 15 bits (Extended Data Fig. 7). The size of the key space that can be generated with our 15-bit CPR is 2^{15} from a single-PUF label.

Overall, the maximum size of the key space can be calculated by multiplying the number of each key space based on an independent mechanism ($2^{15}\times2^{15}\times2^{15}=2^{45}=3.3\times10^{13}$).

Polarized optical reflectivity simulation study of nanoPUF. To analyse the reflectivity difference in nanoPUFs, electrodynamic simulation (finite-difference time-domain simulation, Lumerical) was conducted for bilayer stacked metallic nanowires depending on the angle between the nanowires and the polarization of incident light. In our simulation, the width and height of the wires are set at 50 and 10 nm, respectively, and the period in the width direction is 100 nm. The simulation results (Extended Data Fig. 3a,b) indicate that the reflectance can be randomized depending on the input polarization or orientation of the nanowires.

Plasmonic resonance simulation study of nanoPUF. To analyse the plasmonic resonance effect in nanoPUFs, electrodynamic simulation (finite-difference time-domain simulation, Lumerical) was conducted for bilayer stacked metallic nanowires depending on the angle between the nanowires and the polarization of incident light, with respect to the direction of the bottom wire layer. In our simulation, the width and height of the wires are set at 50 and 10 nm, respectively, and the period in the width direction is 100 nm. The simulation result (Extended Data Fig. 6) indicates that localized surface plasmon can be coupled among the complex interlocked metallic wires to induce a strong electric-field enhancement in the nanogap. Depending on the input polarization or orientation of nanowires, electric-field enhancement can be varied to affect the Raman enhancement (proportional to $|E|^4$; Fig. 2i); the Raman enhancement was calculated by integrating $|E|^4$ of a region smaller than 500 nm in depth of the substrate.

Calculation of PUF parameters. The test code for statistical analysis was built in the Python version 3.9 environment. The Hamming distance between two data strings is the number of different bits at which the corresponding symbols are different, and the Hamming weight is the number of zeroes in an n-bit response[38,39].

Uniqueness. A PUF must be distinguishable from other PUFs obtained under the same fabrication process; however, the PUF should also be different by 50% from other PUFs. This metric is evaluated using the Hamming distance (HD) as below:

$$\text{Uniqueness} = \frac{2}{k(k-1)}\sum_{i=1}^{k-1}\sum_{j=i+1}^{k}\frac{\text{HD}\left(R_i(n),\,R_j(n)\right)}{n}\times100[\%],$$

where $R_i(n)$ and $R_j(n)$ are the n-bit responses of the ith and jth PUF, respectively, and k is the total number of PUFs.

Bit aliasing. The responses from different PUFs must be different by 50% to have identical responses. This metric is evaluated using the Hamming weight (HW) as below.

$$\text{Bit aliasing} = \frac{1}{k}\sum_{i=1}^{k}R_i(j)\times100[\%],$$

where $R_i(j)$ is the jth bit in an n-bit response from the ith PUF and k is the total number of PUFs.

Reliability. PUF must be able to generate a consistent response. This metric is evaluated using the Hamming distance as below:

$$\text{Reliability} = 100 - \frac{1}{k}\sum_{i=1}^{k}\frac{1}{T}\sum_{l=0}^{T}\frac{\text{HD}(R_i^0(n),\,R_i^l(n))}{n}\times100[\%],$$

where $R_i^l(n)$ is the n-bit response from the ith PUF at the lth trial, T is the number of trials and k is the total number of PUFs.

Calculation of number of distinguishable nanoidentifiers. By assuming that the confined area is a 1 μm × 1 μm square and the period (λ, centre-to-centre distance) of the BCP lamellar pattern is 60 nm, we were able to create a grid with a spacing of 60 nm inside the 1 μm² square[16]. Then, the effective possible positions, where minutia can exist, is the number of intersections inside the square, which is approximately 280 (17 horizontal lines and 17 vertical lines in the square). Additionally, we assume that the practical producible average minutiae density in 1 μm² is 10 (85 termination points in 8.5 μm²) for termination (ridge ending) (Extended Data Fig. 10). The estimated maximum code capacity of one layer is ${}_{280}C_{10}\cong6.937\times10^{17}$ under the assumption that there is only one type of minutiae of termination. Finally, when two fingerprint patterns are stacked, the maximum number of distinguishable nanoidentifiers can be calculated by multiplying the number of each distinguishable layer owing to the morphological independence of each layer. Therefore, the maximum number of distinguishable nanoidentifiers of the bilayer PUF label is about 4.8×10^{35}.

Designation of noise level. Here $I_{noise}=I_0(1+N_{eff}(\text{rand}-0.5))$, where I_0 is the initial greyscale pixel value, I_{noise} is the pixel value under artificial noise, N_{eff} is the factor controlling the noise effect and rand denotes a random number extracted from a uniform distribution between 0 and 1.

Layer-separation image processing for bilayer stacked BCP patterns. For the minutiae point extraction of each layer from bilayer stacked BCP nanopattern images, layer separation is required before other image processing. As shown in Extended Data Fig. 9, the pixel intensities in bilayer stacked BCP images follow a multimodal distribution, where the distinctive intensity peaks correspond to empty space (dark pixels), bottom layer (middle peak) or the cross-points of two layers (bright pixels). The pixel for only the second (top) layer is brighter in greyscale intensity than that of only the first (bottom) layer, but little darker than the cross-points. Taking the intensity of the middle peak as a threshold, the top layer image can be separated from the original image. The bottom layer is revealed after taking off the first top layer and then recovering the crossing points—the pixels have a higher intensity next to the brightest peak. After separating the two layers, the image of each layer is treated by a conventional fingerprint recognition process, consisting of image normalization, segmentation, enhancement using a Gabor filter and line thinning (skeletonization), to extract the minutiae points, such as termination, bifurcation and crossing points.

Data availability

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

Received: 14 August 2021; Accepted: 27 May 2022;
Published online: 26 July 2022

References

1. Chung, H. U. et al. Binodal, wireless epidermal electronic systems with in-sensor analytics for neonatal intensive care. *Science* **363**, eaau0780 (2019).

2. Niu, S. et al. A wireless body area sensor network based on stretchable passive tags. *Nat. Electron.* **2**, 361–368 (2019).
3. Yu, X. et al. Skin-integrated wireless haptic interfaces for virtual and augmented reality. *Nature* **575**, 473–479 (2019).
4. Neuman, B. C. & Ts'o, T. Kerberos: an authentication service for computer networks. *IEEE Commun. Mag.* **32**, 33–38 (1994).
5. Beckmann, N. & Potkonjak, M. Hardware-based public-key cryptography with public physically unclonable functions. in *Information Hiding* 206–220 (Springer, 2009).
6. Kune, D. F. et al. Ghost talk: mitigating EMI signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy* 145–159 (IEEE, 2013).
7. Pappu, R. et al. Physical one-way functions. *Science* **297**, 2026–2030 (2002).
8. Maes, R. & Verbauwhede, I. in *Towards Hardware-Intrinsic Security: Foundations and Practice* (eds Sadeghi, A.-R. & Naccache, D.) 3–37 (Springer, 2010).
9. Becker, G. T. The gap between promise and reality: on the insecurity of XOR arbiter PUFs. in *Cryptographic Hardware and Embedded Systems—CHES 2015* (eds Güneysu, T. & Handschuh, H.) 535–555 (Springer, 2015).
10. Gao, Y. et al. Memristive crypto primitive for building highly secure physical unclonable functions. *Sci. Rep.* **5**, 12785 (2015).
11. Arppe, R. & Sørensen, T. J. Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nat. Rev. Chem.* **1**, 0031 (2017).
12. Carro-Temboury, M. R. et al. An optical authentication system based on imaging of excitation-selected lanthanide luminescence. *Sci. Adv.* **4**, e1701384 (2018).
13. Gao, Y. et al. Physical unclonable functions. *Nat. Electron.* **3**, 81–91 (2020).
14. Arppe-Tabbara, R. et al. Versatile and validated optical authentication system based on physical unclonable functions. *ACS Appl. Mater. Interfaces* **11**, 6475–6482 (2019).
15. Nakayama, K. & Ohtsubo, J. Optical security device providing fingerprint and designed pattern indicator using fingerprint texture in liquid crystal. *Opt. Eng.* **51**, 040506 (2012).
16. Bae, H. J. et al. Biomimetic microfingerprints for anti-counterfeiting strategies. *Adv. Mater.* **27**, 2083–2089 (2015).
17. Wolterink, T. A. W. et al. Programmable two-photon quantum interference in 10^3 channels in opaque scattering media. *Phys. Rev. A* **93**, 053817 (2016).
18. Gu, Y. et al. Gap-enhanced Raman tags for physically unclonable anticounterfeiting labels. *Nat. Commun.* **11**, 516 (2020).
19. Martinez, P. et al. Laser generation of sub-micrometer wrinkles in a chalcogenide glass film as physical unclonable functions. *Adv. Mater.* **32**, 2003032 (2020).
20. Devadas, S. et al. Design and implementation of PUF-based 'unclonable' RFID ICs for anti-counterfeiting and security applications. In *2008 IEEE International Conference on RFID* 58–64 (IEEE, 2008).
21. Maiti, A. & Schaumont, P. Improving the quality of a physical unclonable function using configurable ring oscillators. In *2009 International Conference on Field Programmable Logic and Applications* 703–707 (IEEE, 2009).
22. Scholz, A. et al. Hybrid low-voltage physical unclonable function based on inkjet-printed metal-oxide transistors. *Nat. Commun.* **11**, 5543 (2020).
23. Bates, F. S. & Fredrickson, G. H. Block copolymer thermodynamics: theory and experiment. *Annu. Rev. Phys. Chem.* **41**, 525–557 (1990).
24. Harrison, C. et al. Mechanisms of ordering in striped patterns. *Science* **290**, 1558–1560 (2000).
25. Thurn-Albrecht, T. et al. Ultrahigh-density nanowire arrays grown in self-assembled diblock copolymer templates. *Science* **290**, 2126–2129 (2000).
26. Jeong, S.-J. et al. Universal block copolymer lithography for metals, semiconductors, ceramics, and polymers. *Adv. Mater.* **20**, 1898–1904 (2008).
27. Meitl, M. A. et al. Transfer printing by kinetic control of adhesion to an elastomeric stamp. *Nat. Mater.* **5**, 33–38 (2006).
28. Kim, J. Y. et al. Highly tunable refractive index visible-light metasurface from block copolymer self-assembly. *Nat. Commun.* **7**, 12911 (2016).
29. Yuhang, D. et al. A study of hand vein recognition method. In *IEEE International Conference Mechatronics and Automation* **4**, 2106–2110 (IEEE, 2005).
30. Kumar, A. & Prathyusha, K. V. Personal authentication using hand vein triangulation and knuckle shape. *IEEE Trans. Image Process.* **18**, 2127–2136 (2009).
31. Komiyama, H. et al. Binary nanoparticles coassembly in bioinspired block copolymer films: a stepwise synthesis approach using multifunctional catechol groups and magneto-optical properties. *ACS Appl. Nano Mater.* **1**, 1666–1674 (2018).
32. Gates, B. D. et al. New approaches to nanofabrication: molding, printing, and other techniques. *Chem. Rev.* **105**, 1171–1196 (2005).
33. Smith, B. W. & Suzuki, K. *Microlithography: Science and Technology* (CRC Press, 2020).
34. Mutiso, R. M. et al. Integrating simulations and experiments to predict sheet resistance and optical transmittance in nanowire films for transparent conductors. *ACS Nano* **7**, 7654–7663 (2013).
35. Zhao, Y. et al. Twisted optical metamaterials for planarized ultrathin broadband circular polarizers. *Nat. Commun.* **3**, 870 (2012).
36. Moskovits, M. Surface-enhanced spectroscopy. *Rev. Mod. Phys.* **57**, 783–826 (1985).
37. Stiles, P. L. et al. Surface-enhanced Raman spectroscopy. *Annu. Rev. Anal. Chem.* **1**, 601–626 (2008).
38. Maiti, A. et al. A systematic method to evaluate and compare the performance of physical unclonable functions. in *Embedded Systems Design with FPGAs* 245–267 (Springer, 2013).
39. Maiti, A. et al. A large scale characterization of RO-PUF. In *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* 94–99 (IEEE, 2010).
40. Xiao, Q. & Raafat, H. Fingerprint image postprocessing: a combined statistical and structural approach. *Pattern Recognit.* **24**, 985–992 (1991).
41. Farina, A. et al. Fingerprint minutiae extraction from skeletonized binary images. *Pattern Recognit.* **32**, 877–889 (1999).
42. Lempel, A. & Ziv, J. On the complexity of finite sequences. *IEEE Trans. Inf. Theory* **22**, 75–81 (1976).
43. XiaoGuang, F. & Milanfar, P. Multiscale principal components analysis for image local orientation estimation. In *Conference Record of the Thirty-Sixth Asilomar Conference on Signals, Systems and Computers* **1**, 478–482 (IEEE, 2002).
44. Ullner, M. & Woodward, C. E. Orientational correlation function and persistence lengths of flexible polyelectrolytes. *Macromolecules* **35**, 1437–1445 (2002).
45. Murphy, J. N. et al. Automated defect and correlation length analysis of block copolymer thin film nanopatterns. *PLoS ONE* **10**, e0133088 (2015).

Acknowledgements

Funding: This research was supported by the National Creative Research Initiative (CRI) Center for Multi-Dimensional Directed Nanoscale Assembly (2015R1A3A2033061) through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, Nano·Material Technology Development Program through the NRF funded by the Ministry of Science and ICT (2022M3H4A1A02046445) and the Development of Long-Distance Plasmonic Waveguide Materials Working for Near-IR Band (KRF2021R1F1A106405111) funded by the NRF.

Author contributions

B.H.K. proposed the initial idea for this work. J.H.K. principally performed the overall experiments and wrote the manuscript. S.J.K. analysed the physical properties of the PUF patterns and performed image processing to demonstrate the functionalities of patterns. S.N. and S.-W.S. performed the fingerprint recognition analysis of patterns. S.J. and J.S. performed the optical measurement of patterns and simulation study for plasmonic resonance. J.H.I. and K.M.K. performed the electrical measurement of patterns and calculated the PUF parameters. H.M.J., K.H.H., G.G.Y. and H.J.C. contributed to the BCP pattern formation and characterization. B.H.K. and S.O.K. supervised the entire research project and manuscript preparation.

Competing interests

The authors declare no competing interests.

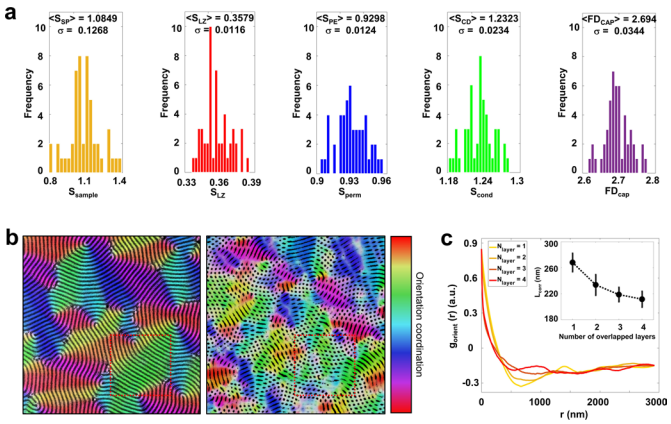
Additional information

Extended data is available for this paper at https://doi.org/10.1038/s41928-022-00788-w.

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41928-022-00788-w.

Correspondence and requests for materials should be addressed to Seok Joon Kwon, Bong Hoon Kim or Sang Ouk Kim.

Peer review information *Nature Electronics* thanks Thomas Just Sørensen and the other, anonymous, reviewer(s) for their contribution to the peer review of this work.



Extended Data Fig. 1 | Calculation of physical properties of BCP self-assembled nanopatterns. a, Distribution of sample entropy, Lempel-Ziv entropy, permutation entropy, conditional entropy and capacity fractal dimension of fifty bi-layer PUF labels. **b**, Orientation color mapping images of monolayer pattern (left) and bi-layer stacked pattern (right). Scale bar: 500 nm. **c**, Plot of correlation function with the number of overlapped layers.

Threshold value : Average electrical resistance level of each samples

Resistance < threshold = 0 , Resistance > threshold = 1, Barcode creation by code 128

PUF #1 | Threshold resistance : 62.63 Ω

Electrode #	1	2	3	4	5	6	7	8
Resistance (Ω)	66.07	66.27	66.09	65.41	65.79	68.43	68.43	68.51
Electrode #	9	10	11	12	13	14	15	Average
Resistance (Ω)	68.81	68.66	52.71	53.89	53.74	53.48	53.12	**62.63**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0

PUF #5 | Threshold resistance : 20.26 Ω

Electrode #	1	2	3	4	5	6	7	8
Resistance (Ω)	49.26	24.52	24.55	24.47	24.82	25.00	2.84	3.71
Electrode #	9	10	11	12	13	14	15	Average
Resistance (Ω)	4.00	3.98	4.00	28.59	28.59	27.80	27.70	**20.26**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1

PUF #7 | Threshold resistance : 20.33 Ω

Electrode #	1	2	3	4	5	6	7	8
Resistance (Ω)	37.71	37.63	37.27	37.40	21.99	21.94	21.93	21.93
Electrode #	9	10	11	12	13	14	15	Average
Resistance (Ω)	22.31	5.72	6.14	6.08	6.01	6.06	14.77	**20.33**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

PUF #9 | Threshold resistance : 9.47 Ω

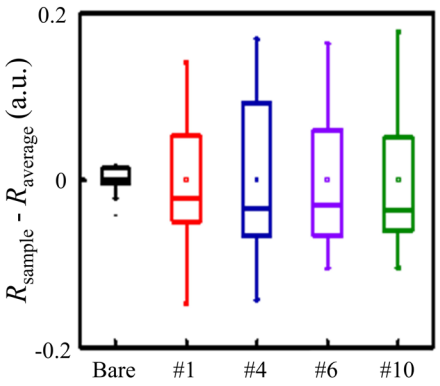
Electrode #	1	2	3	4	5	6	7	8
Resistance (Ω)	37.65	38.16	1.99	1.45	1.38	1.73	1.28	0.00
Electrode #	9	10	11	12	13	14	15	Average
Resistance (Ω)	0.01	0.02	0.03	0.04	18.96	19.62	19.74	**9.47**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1

Extended Data Fig. 2 | Electric-key generation process of PUF labels.

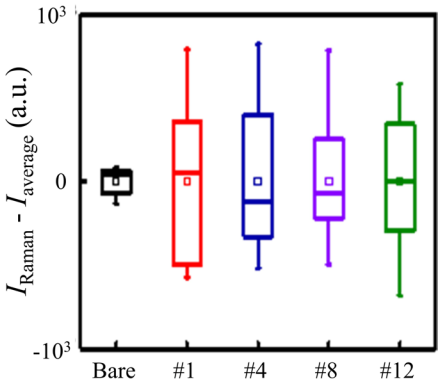
a

Reflectance distribution with randomly selected 4 samples

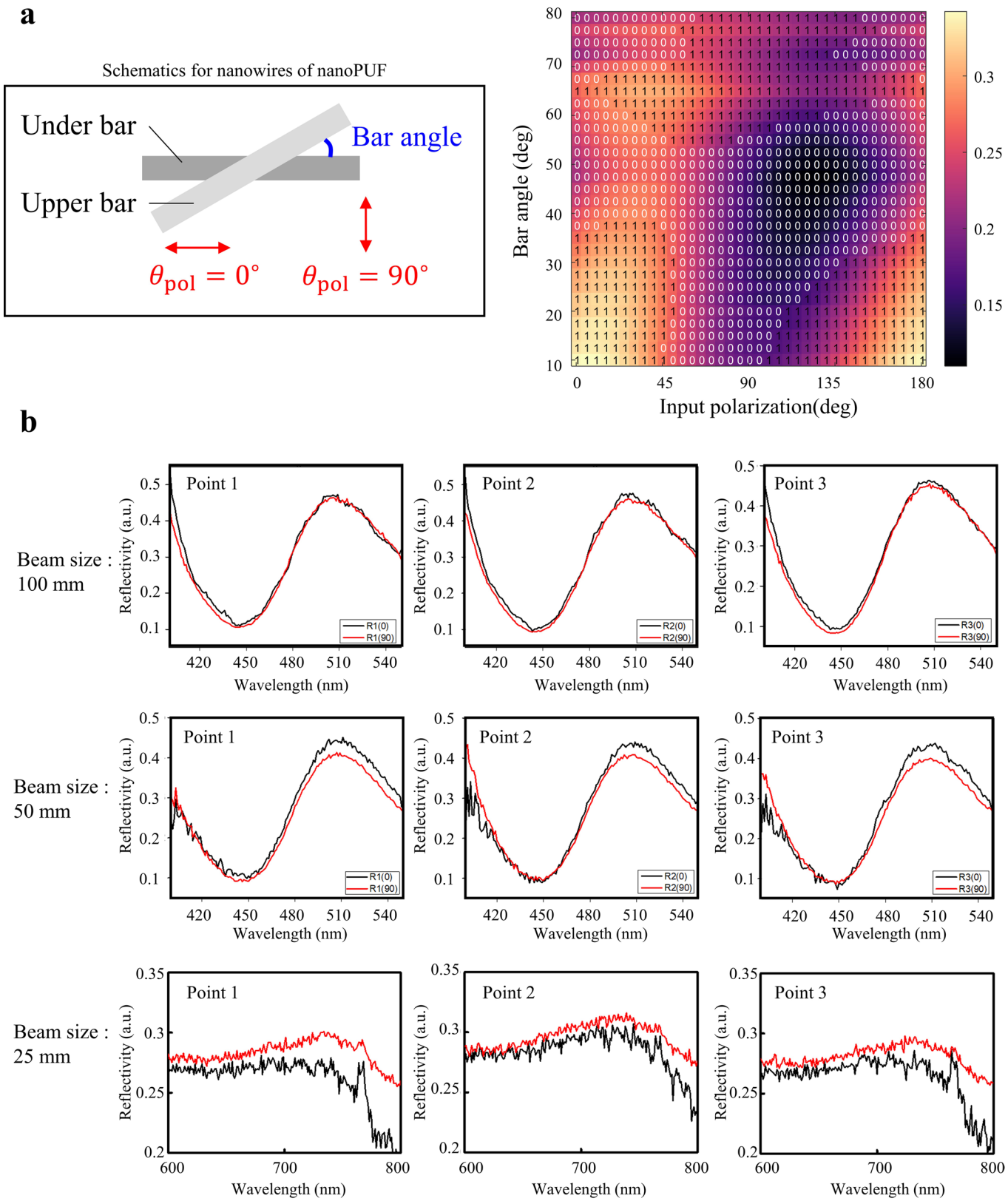


b

Raman scattering distribution with randomly selected 4 samples

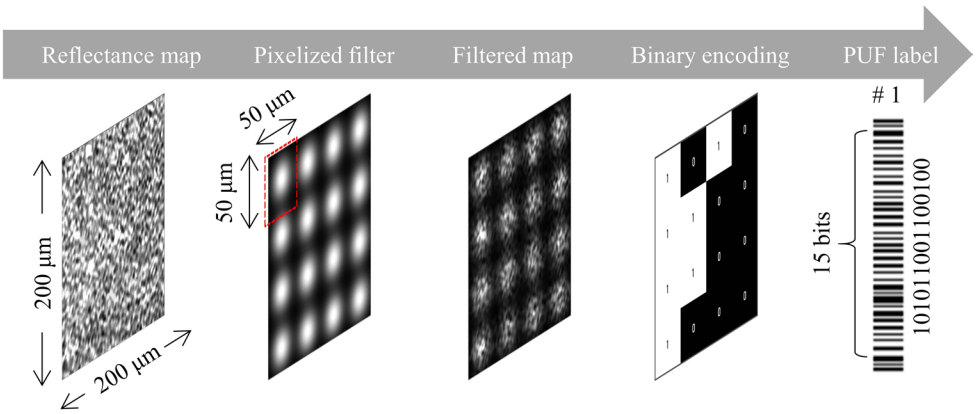


Extended Data Fig. 3 | Random distribution of a, reflectance intensity and b, Raman scattering intensity.



Extended Data Fig. 4 | Intensity distribution of reflectance for a polarized incidence beam. a, Simulation result for reflectance in nanoPUF. The input polarization and angle between wires are 180° and 10°, respectively. Give 1 when larger than threshold reflectance and 0 when less. Threshold reflectance: 0.225 (a.u.). **b**, Reflectance measurements at different selected areas of PUF labels with different beam size (from 100 mm to 25 mm) and wavelength (from 400 nm to 800 nm).

a



b

Threshold value : Average reflectivity of each samples

Reflectivity < threshold = 0 , Reflectivity ≥ threshold = 1, Barcode creation by code 128

PUF #1 | Threshold reflectivity : 1.1934

Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	1.2347	1.1563	1.2071	1.1612	1.3293	1.2812	1.1703	1.1206
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	1.3122	1.2471	1.1579	1.1618	1.2242	1.0393	1.0983	**1.1934**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	1	0	1	0	1	1	0	0	1	1	0	0	1	0	0

PUF #4 | Threshold reflectivity : 1.0273

Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	1.1123	1.1355	1.1249	1.1913	0.9228	0.9883	0.9751	0.9930
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	0.8797	0.9878	0.9536	1.1186	0.9835	0.9552	1.0881	**1.0273**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	1	1	1	1	0	0	0	0	0	0	0	1	0	0	1

PUF #6 | Threshold reflectivity : 1.0568

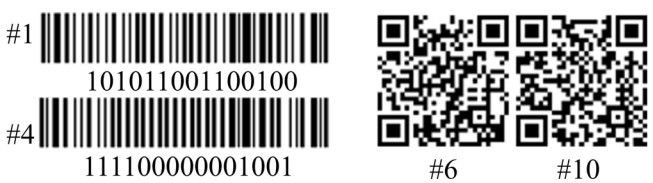
Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	1.1552	1.2134	1.1856	1.2161	1.0021	1.0426	1.0692	1.0691
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	0.9705	0.9726	0.9900	1.0472	0.9466	0.9849	0.9877	**1.0568**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	1	1	1	1	0	0	1	1	0	0	0	0	0	0	0

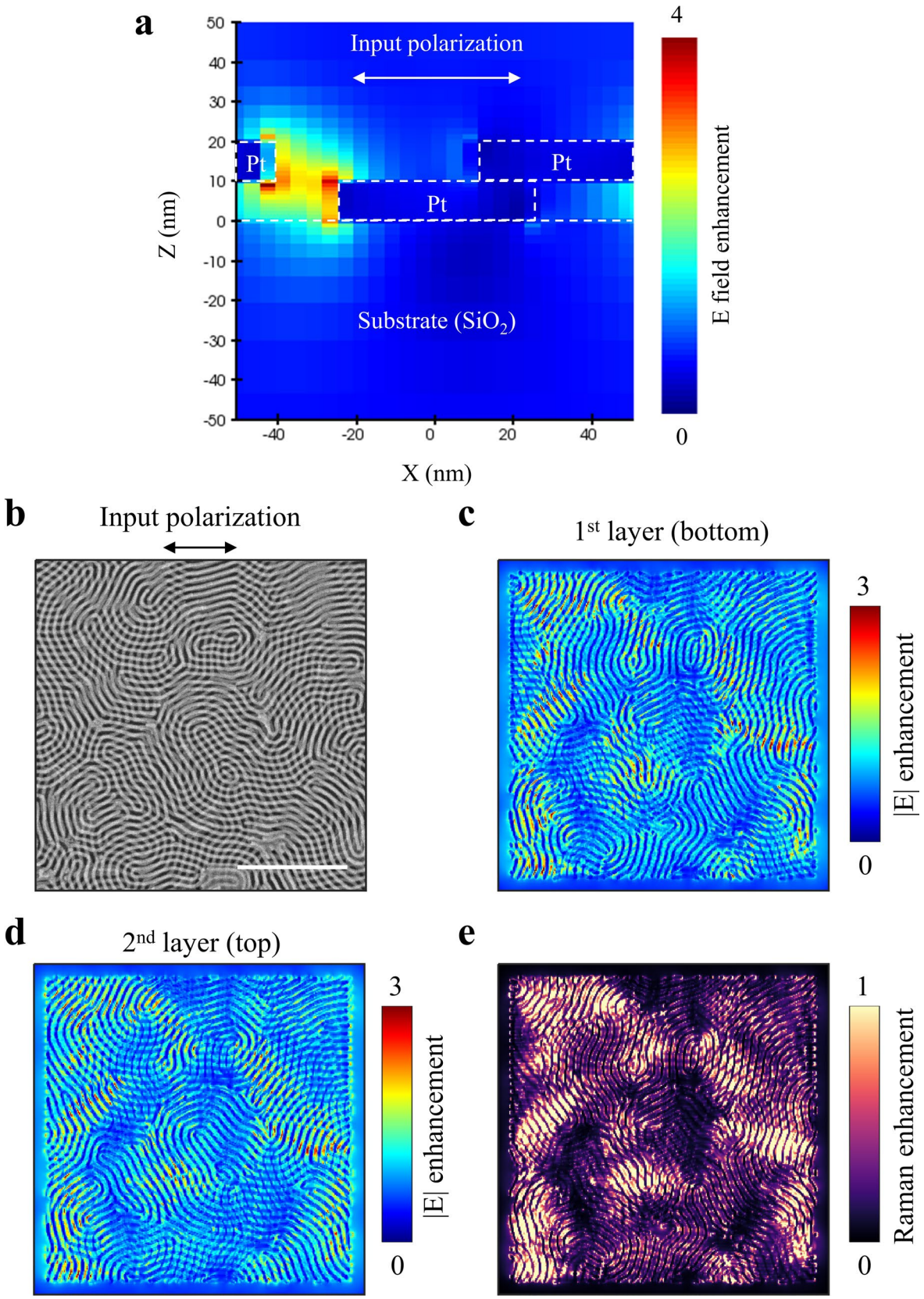
PUF #10 | Threshold reflectivity : 0.9620

Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	0.8905	0.8839	0.9229	0.8134	0.9444	0.9953	1.0650	1.0096
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	0.9077	0.9514	0.9779	0.9035	1.0844	1.1262	0.9538	**0.9620**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	0	0	0	0	0	1	1	1	0	0	1	0	1	1	0



Extended Data Fig. 5 | Birefringence-key generation process of PUF labels. a, Dividing reflectance map into multiple sections. **b**, Reflection-key generation process of PUF labels.



Extended Data Fig. 6 | Simulation result for localized surface plasmonic resonance in nanoPUF. The input polarization and angle between wires are 90° and 10°, respectively.

Threshold value : Average Raman scattering intensity of each samples

Raman scattering intensity < threshold = 0, Raman scattering intensity ≥ threshold = 1

Barcode creation by code 128

PUF #1 | Threshold Raman scattering intensity : 2401

Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	1866	3105	2319	1828	2187	1922	1905	2528
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	3192	2457	1865	2626	2763	2780	2684	**2401**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	0	1	0	0	0	0	0	1	1	1	0	1	1	1	1

PUF #4 | Threshold Raman scattering intensity : 2155

Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	1916	2030	2103	2617	1755	1634	1826	2888
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	2137	2037	2214	2977	1746	1891	2558	**2155**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1

PUF #8 | Threshold Raman scattering intensity : 2135

Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	2006	2167	2231	2485	1896	2062	2097	1637
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	1962	2921	2442	1916	2389	1991	1833	**2135**

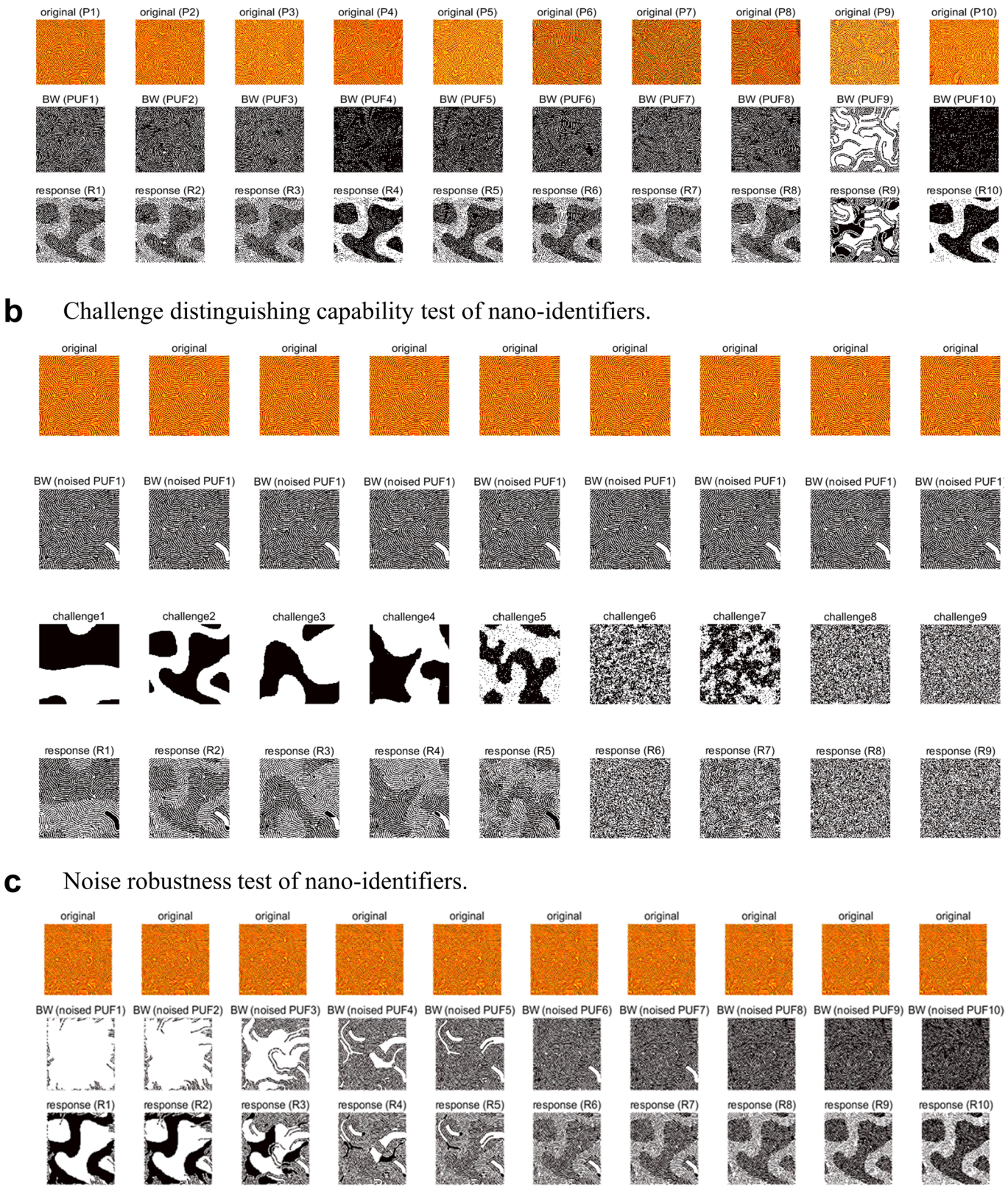
String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0

PUF #12 | Threshold Raman scattering intensity : 2473

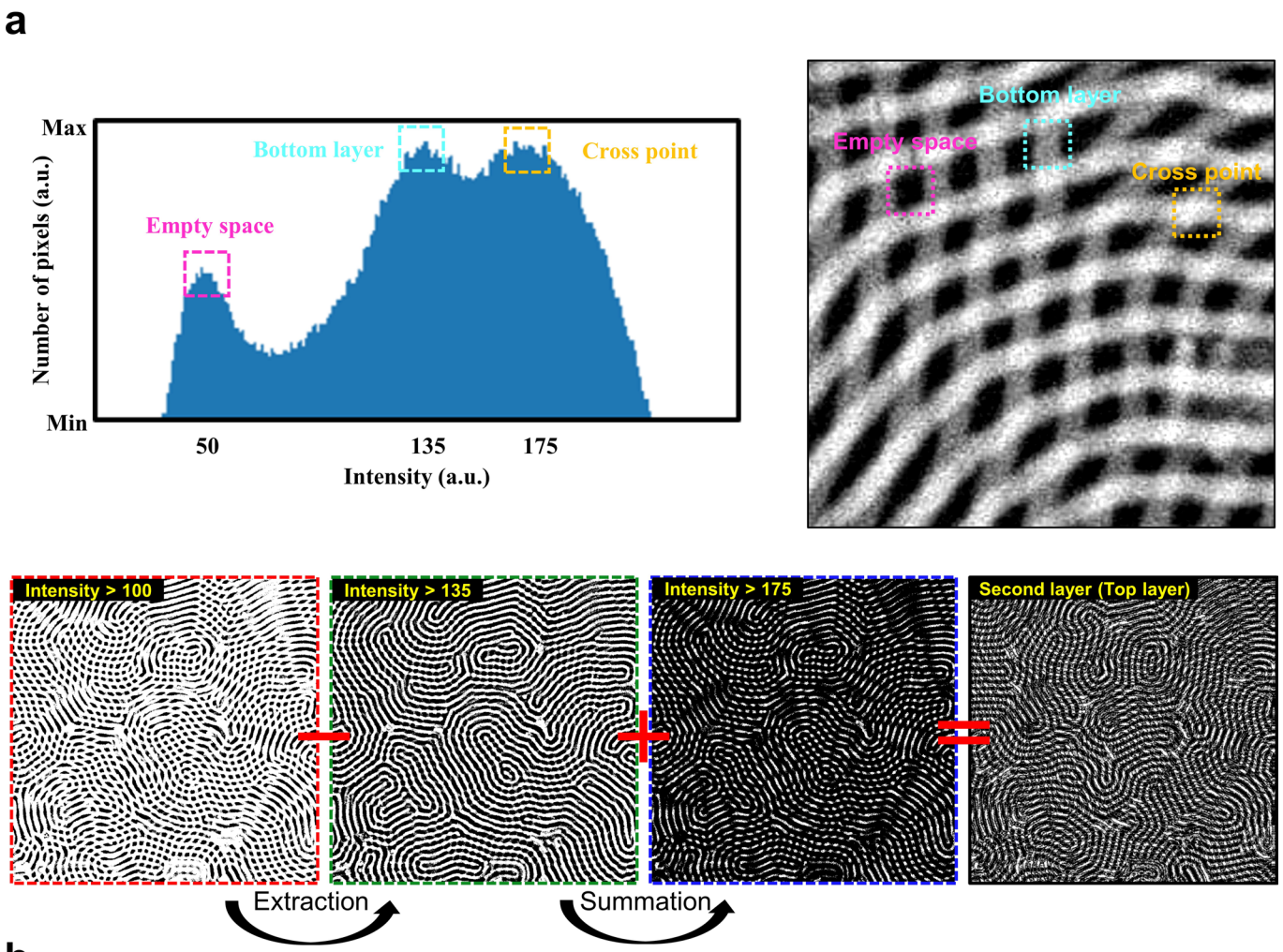
Region #	1	2	3	4	5	6	7	8
Intensity (a.u.)	2041	2180	2244	1790	2475	2698	2819	1928
Region #	9	10	11	12	13	14	15	Average
Intensity (a.u.)	2927	2925	3058	2368	2478	2699	2470	**2473**

String #	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Digit	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1

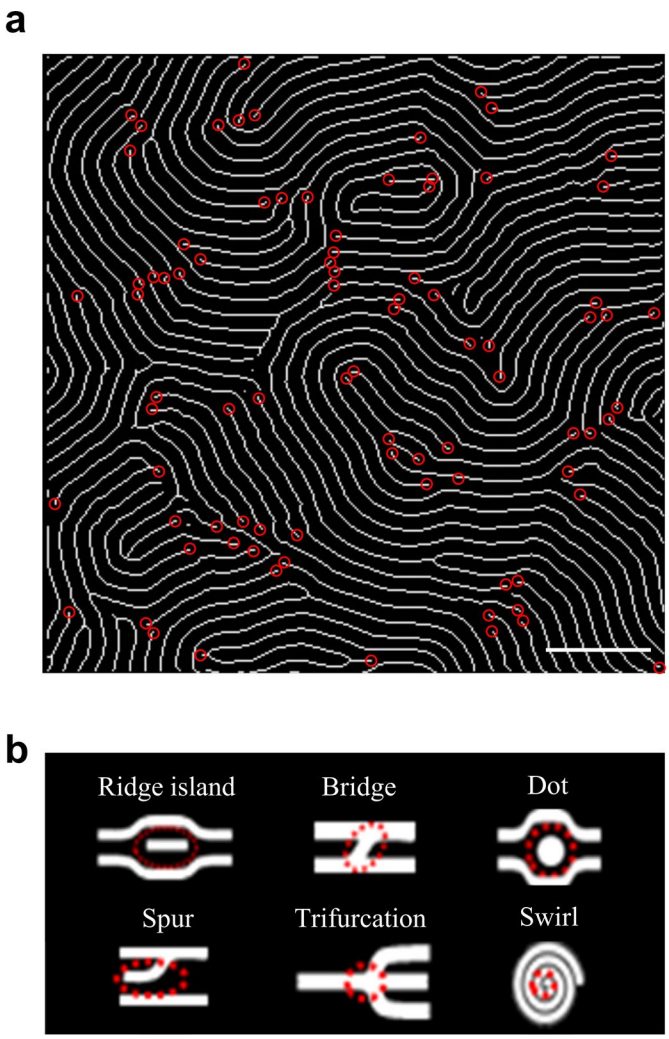
Extended Data Fig. 7 | Raman scattering-key generation process of PUF labels.



Extended Data Fig. 8 | Challenge-response operation of nanoPUF. a, Uniqueness test. **b**, Challenge distinguishing capability test. **c**, Noise robustness test of 10 nano-identifiers.



Extended Data Fig. 9 | Layer separation of overlapped patterns. a, Layer separation of overlapped patterns with various threshold levels of greyscale. **b**, Minutiae point extraction with conventional fingerprint recognition process.



Extended Data Fig. 10 | Morphological defects in BCP self-assembly patterns. a, Ridge ending point density of termination minutia in a selected nanoPUF pattern area. Scale bar: 500 nm. **b**, Schematically illustrated images for the different defects in BCP self-assembly patterns.