Nanoscale

ROYAL SOCIETY OF CHEMISTRY

MINIREVIEW

View Article Online
View Journal | View Issue

Cite this: *Nanoscale*, 2025, **17**, 20865

Advances in semiconductor quantum dot-based physical unclonable functions for enhanced security applications

Partha Mishra, Aditi Manna and Nirat Ray *

Quantum dots (QDs) have garnered significant attention for their unique size-dependent optical and electronic properties, enabling their widespread use in applications ranging from high-efficiency photovoltaics and light-emitting diodes to biomedical imaging and quantum computing. Their tunable emission, high photo-stability, and ease of surface modification make them ideal candidates for precision nanotechnology applications. In this work, we explore a novel and rapidly emerging application of QDs in hardware security through the development of Quantum Dot-based Physical Unclonable Functions (QD-PUFs). Unlike conventional security paradigms, QD-PUFs leverage the intrinsic physical randomness of QD-based nanostructures to generate challenge-response pairs with superior uniqueness, reliability, and robustness. We review the integration of QDs into PUFs, beginning with their material properties and extending to entropy sources arising from synthesis and fabrication, surface and encapsulation effects. A comparative analysis of different readout mechanisms and related applications underscores the unique encoding capacity and security potential of QD-based systems. By demonstrating their feasibility for scalable, high-security applications, this study underscores the transformative impact of QDs in next-generation authentication and anti-counterfeiting technologies.

Received 7th August 2025,
Accepted 20th August 2025

DOI: 10.1039/d5nr03356j

rsc.li/nanoscale

1 Introduction

With the rapid advancement of electronic technologies, ensuring security in connected devices has become a critical challenge. Modern applications rely heavily on identifiers and secret keys to safeguard sensitive information and enable secure authentication. However, traditional cryptographic methods often rely on stored keys, which are susceptible to brute-force attacks, traffic analysis, and hardware tampering.[1] To mitigate these risks, researchers have focused on developing robust random number generators and hardware-based security solutions that enhance key protection. Among these, Physical Unclonable Functions (PUFs) have emerged as a promising approach to generating and safeguarding secret keys through intrinsic physical randomness.[2] PUFs leverage the inherent variations in physical materials or electronic components to produce unique, unpredictable outputs that could serve as cryptographic keys. Unlike traditional key storage mechanisms, PUF-based keys are not stored in memory but are generated dynamically whenever needed. This transient nature makes them resistant to invasive attacks and side-channel threats. The uniqueness and unclonability of PUFs stem from microscopic variations introduced during manufacturing. These random imperfections create a "fingerprint" that distinguishes each PUF instance.

While early PUFs were predominantly based on silicon microelectronics,[3] recent research has explored alternative materials, including organic,[4] optical,[5] and nanostructured systems.[6] Existing reviews have examined metal nanoparticles as physical tags based on their optical response,[7] the development of PUFs leveraging optical properties, circuit time-delay, and volatile/non-volatile memory characteristics,[2] as well as chemically generated PUFs for anti-counterfeiting.[8] Among these emerging approaches, quantum dots and nanocrystals have garnered significant interest due to their tunable properties, high entropy, and nanoscale fabrication potential.

Quantum dots, a class of semiconductor nanocrystals, exhibit size-dependent electronic and optical properties driven by quantum confinement.[9] Their transformative potential in science and technology was recognized with the 2023 Nobel Prize in Chemistry, awarded to Moungi Bawendi, Louis Brus, and Alexei Ekimov for their foundational contributions to the discovery and development of these materials.[10–12] This recognition highlights the versatility of quantum dots across various fields. Over the past decade, significant progress has been made in leveraging the inherent randomness and optical

Department of Materials Science and Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India. E-mail: nirat@iitd.ac.in

variability of QDs to develop secure, scalable, and reliable PUFs. Advances in fabrication techniques, readout mechanisms, and material optimization have facilitated their integration into practical security applications, including cryptographic key generation,[13] device authentication,[14] and anti-counterfeiting measures.[15] This mini-review explores recent advancements in quantum dot-based PUFs, particularly in the context of optical and multimodal PUFs that utilize the unique challenge-response pairs produced due to the properties of QDs and the potential for enhancing security applications.

2 Physical unclonable functions (PUFs): concepts and criteria

Over the past four decades, the idea of leveraging intrinsic physical variability for authentication has evolved from a conceptual sketch to a rich ecosystem. In 1983, Bauder first suggested that uncontrolled material disorder could serve as an anti-counterfeiting measure, planting the seeds of what would later become physical unclonable functions or PUFs.[16] A year later, Simmons expanded on this by proposing a physical property-based authentication scheme that relied similarly on microscopic irregularities.[17] In 1992, Naccache and Frémanteau developed one of the first protocols for smart-card memory authentication, deliberately exploiting manufacturing variability as an entropy source.[18] Shortly thereafter, in 1993, researchers demonstrated the first paper PUF by scanning unique fiber patterns in ordinary paper to generate unclonable identifiers.[19] A major turning point in the field came with the 2002 demonstration of the first optical PUF, which captured laser-speckle patterns from a random scattering medium.[20] That same year, Gassend and colleagues broadened the scope by proposing delay PUFs and RF PUFs, which harnessed the minute timing and radio frequency variations inherent in silicon fabrication.[21] Subsequent innovations rapidly expanded the PUF landscape, from coating PUFs in 2006,[22] SRAM PUFs,[23,24] metal-resistance and CD PUFs,[25] Arbiter PUFs,[26] ring oscillator PUFs,[27,28] quantum-electronic,[29,30] and quantum-optical variants.[31]

Under a specific stimulus, such as an electrical signal, optical input, the PUF generates a corresponding response. Together, the input and output form a challenge–response pair (CRP), which serves as the basis for authentication and identification due to its uniqueness, unpredictability, and reproducibility under the same conditions. Metrics exist to evaluate the performance and security of PUFs, serving as essential tools to benchmark different designs and ensure consistent operation under varying conditions. One widely used metric is the Hamming distance (HD), which quantifies the difference between two binary response strings produced by a PUF. It is particularly relevant when comparing responses to identical or slightly varied challenges. For two response strings R_1 and R_2 of length n, the Hamming distance is defined as:

$$\mathrm{HD}(R_1, R_2) = \sum_{i=1}^{n} R_1(i) \oplus R_2(i) \quad (1)$$

where $R_1(i)$ and $R_2(i)$ are the i^{th} bits of the respective responses, and $\oplus$ denotes the bitwise XOR operation. When the same challenge is applied multiple times to the same PUF, the Hamming distance between the repeated responses is referred to as the intra-HD, and it measures the stability or reproducibility of the PUF under environmental noise or temporal variation. In contrast, the inter-HD is the Hamming distance between responses from two different PUF instances to the same challenge, indicating uniqueness and device-to-device variation. The use of HD is appropriate if the output bits are independent and identically distributed (IID), but in cases where the outputs are non-IID, the fractional HD (fHD) which normalizes HD over total bits is more appropriate.[32]

Once HD and fHD have been introduced as core tools to compare PUF responses, it becomes essential to identify the specific metrics that assess whether a PUF meets the requirements of practical use. A high-quality PUF must demonstrate uniqueness, reliability, randomness, and security, which are evaluated using several standard metrics. These include:

1. *Uniqueness*: This parameter measures how different the responses are from different PUF devices when given the same challenge. In other words, for a fixed challenge, if two devices produce very different responses, the PUFs are considered unique. It is measured by calculating the inter-HD (or inter-fHD). Ideally, the average inter-chip Hamming distance should be around 50%, indicating maximum uniqueness, like a digital fingerprint which is truly distinct for each device. In other words, two different devices should differ in about half of their bits on average.

2. *Reliability*: Reliability reflects how consistently a single PUF device produces the same response when the same challenge is applied multiple times, even under varying environmental conditions such as temperature, humidity, or voltage fluctuations. In essence, it measures the stability of a PUF's output over time. To quantify this, we look at the intra-chip Hamming distance or the average number of bit differences between multiple responses generated by the same PUF to the same challenge. If the device is reliable, the responses should be nearly identical, resulting in a low intra-chip Hamming distance, ideally close to 0%. The bit-error rate (BER) is the complement of reliability, given by, reliability = 1 − BER.

3. *Bit uniformity*: The bit uniformity evaluates whether the bits in a single PUF response are evenly distributed between 0s and 1s. Mathematically,

$$\text{Bit uniformity} = \frac{1}{L}\sum_{i=1}^{L} R_i \quad (2)$$

where $R_i \in \{0,1\}$ is the i^{th} bit of the response string R, and L is the total number of bits in the response. Ideally, each bit has a 50% chance of being 1 or 0, ensuring randomness and preventing bias, therefore the bit uniformity must ideally be 0.5.

4. *Bit-aliasing*: This metric checks for repeated patterns at the same bit positions across different bit-string arrays, which should have varied randomly. Bit-aliasing is the proportion of

PUF instances in which a given bit position outputs a 1. For a bit position k, it is defined as:

$$\text{Bit-aliasing}_k = \left(\frac{1}{N}\sum_{n=1}^{N} R_{n,k}\right) \times 100\% \quad (3)$$

where N is the number of different PUF instances, and $R_{n,k}$ $\{0,1\}$ is the k^{th} bit of the response from the n^{th} PUF, to a fixed challenge. Ideally, this value should be close to 50% for every k to ensure randomness and lack of bias.

5. *Entropy*: Entropy-based metrics include Shannon entropy, Estimated Number of Independent Bits (ENIB), and min-entropy H_∞, and help evaluate how well the PUF can resist modeling attacks and predictability. The Shannon entropy for a single response bit r_i is given by:[33]

$$H(r_i) = p_i \log_2 p_i - (1 - p_i)\log_2(1 - p_i) \quad (4)$$

where p_i is the probability that the i^{th} bit is 1. ENIB is calculated by summing the Shannon entropy across all n bits in the response:

$$\text{ENIB} = \sum_{i=1}^{n} H(r_i), \quad (5)$$

and estimates the effective number of bits in the response that behave like ideal random bits. Systematic bias or correlations reduce ENIB below n. H_∞, captures the worst-case predictability of the response. For a binary string R $\{0,1\}^n$, it is defined as:

$$H_\infty(R) = -\log_2\left(\max_{r\in\{0,1\}^n} \Pr[R = r]\right) \quad (6)$$

A higher H_∞ implies better security. For an ideal PUF with uniformly random output, both ENIB and H_∞ approach n.

6. *Decidability*: Decidability is a critical metric used to assess how well a PUF can distinguish between responses arising from the same challenge (intra-chip variation) and those from different chips or instances (inter-chip variation). It quantifies the statistical separability between the intra-Hamming distance (intra-HD) and inter-Hamming distance (inter-HD) distributions. A higher decidability implies a more reliable and distinguishable response space, which is crucial for robust authentication. Mathematically, the decidability d is defined as:

$$d = \frac{|\mu_{\text{inter}} - \mu_{\text{intra}}|}{\sqrt{{\sigma_{\text{inter}}}^2 + {\sigma_{\text{intra}}}^2}} \quad (7)$$

where μ_{inter} and μ_{intra} are the means, and σ_{inter} and σ_{intra} are the standard deviations of the inter-HD and intra-HD distributions, respectively. The closer the inter-HD and intra-HD distributions are to being statistically distinct (*i.e.*, non-overlapping), the larger the value of d, and hence, the better the distinguishability of the PUF responses. False positive rate, or the chance that responses from two different PUFs are incorrectly identified as matching, is influenced by inter-HD and decidability, as poor separation between inter- and intra-HD distributions increases this likelihood.

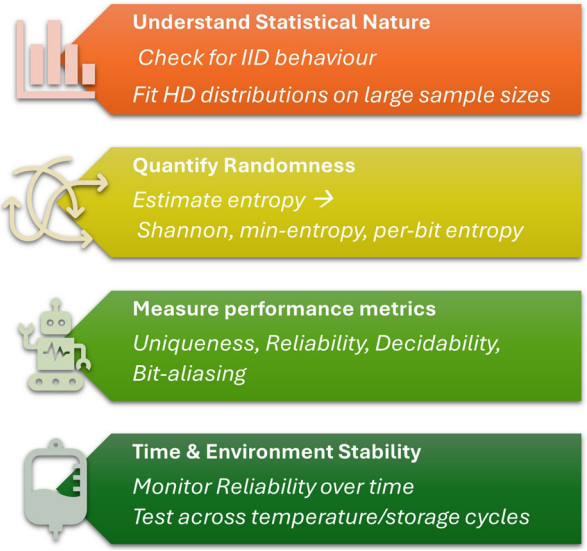

Fig. 1 Visual respresentation of guidelines for comprehensive evaluation of PUF performance.

7. *NIST SP-800-22 randomness tests*: Another important evaluation approach involves the NIST (National Institute of Standards and Technology) statistical test suite, which comprises 15 tests (such as frequency, runs, and block frequency tests) designed to assess the randomness of bit-strings, originally for cryptographic random number generators. For evaluation of 2D outputs, these tests are applied by flattening the fingerprint image into a 1D bitstring. Achieving a pass on all tests (15/15) indicates high statistical randomness and independence. While NIST-800-22 results can be informative, they should be interpreted cautiously; mathematical randomness is not a strict requirement for strong security in authentication or anti-counterfeiting use cases.

To summarize, a comprehensive evaluation of PUFs involves four key pillars: understanding the statistical nature of the output (*e.g.*, checking for IID behavior using tools like NIST SP-800-22), measuring core PUF metrics such as uniqueness, reliability, and decidability, quantifying randomness and entropy through estimators like Shannon entropy or ENIB, and evaluating stability over time and environmental conditions.[32] These interlinked steps ensure that both the security and robustness of a PUF are rigorously assessed. A visual summary of this guideline is shown in Fig. 1.

3 Integration of quantum dots in PUFs

3.1 Material properties

Recent advancements in nanomaterial-based PUFs have enabled the generation of large, diverse, and robust CRPs by exploiting the inherent stochasticity of nanoscale devices.[34]

Each unique spatial or spectral configuration of nanomaterials gives rise to a distinct response under a given challenge, enabling large-scale authentication systems. Due to their small size, QDs exhibit unique quantum properties that are not observed in bulk materials.[35–37] The quantization in energy levels becomes more observable, even at high temperatures, as the size of the dot decreases. For semiconducting quantum dots, this size-dependent effect leads to a modification in the bandgap, influencing their electronic and optical properties.[38–41] This results in tunable emission wavelengths, high photoluminescence quantum yields, and narrow spectral linewidths, making them ideal for generating diverse and distinguishable optical signatures in PUF architectures.[42,43] The size dispersion and synthetic randomness in colloidal QD ensembles naturally lend themselves to entropy generation, as even small variations in diameter (*e.g.*, ±0.5 nm) can lead to significant spectral shifts, which are easily measurable under optical excitation.[44] QDs have therefore emerged as powerful candidates for hardware security and anti-counterfeiting due to their tunable size-dependent optical,[45–47] electronic,[48,49] optoelectronic,[50–54] and thermoelectric properties.[55]

The integration of QDs into PUFs also benefits from their high surface-to-volume ratio, allowing them to be functionalized or embedded within disordered polymeric or inorganic matrices. This leads to random spatial distribution and orientation within printed or spin-coated layers, contributing to the uniqueness and unpredictability of challenge–response behavior. Their strong absorption cross-section and photostability make QDs favorable for repeated readouts with minimal signal degradation.[56] In addition, certain QDs exhibit blinking, Auger recombination, or multiexciton phenomena, all of which can introduce variability into photoluminescence intensity and lifetimes, further enriching the PUF response space.[57–59] Further, in an assembly of dots, charge transport may be dominated by the disorder in the assembly,[60–66] leading to localized variations in the electrical properties, which can form the basis for a QD based electronic PUF. Incorporating taggants with sharp optical features such as fluorescent markers or Raman-active molecules, allows for faster, more reliable CRP readouts.[8,67] Furthermore, QDs can be engineered with various core/shell structures (*e.g.*, CdSe/ZnS, InP/ZnSe), enabling enhanced stability, environmental resistance, and control over electronic energy levels.[68] Another advantage of QDs lies in their solution-based processability, enabling cost-effective, large-scale production.[69] PUFs created through chemical methods further expand the CRP space due to their high encoding capacity and fabrication-induced randomness.[70,71] The same QDs can act as covert fluorescent tags that remain invisible under ambient light yet fluoresce under UV, adding a second anti-counterfeiting layer.[71]

To ensure the consistency of QD PUFs, it is essential to carefully select the composition of dots that are sensitive to external stimuli but not prone to degradation. Tuning the composition of the shells encapsulating the QD cores can be beneficial for protecting the QDs from harsh external conditions.[72] Research has shown that epitaxial growth of inorganic materials like CdS and ZnS as shells around CdSe and CdTe cores significantly improves stability while maintaining good responsiveness to external stimuli.[73,74] Another effective approach for enhancing the stability of QDs involves adding surfactants during the growth reaction or as a post-synthesis treatment, which facilitates surface passivation and can provide additional protection without compromising the device's response and long-term reliability.[5]

3.2 Physical entropy sources in QD-PUFs

In QD-based PUFs, the security and uniqueness of each device stem from multiple layers of physical randomness embedded in the nanostructured material and its processing. These physical entropy sources encompass intrinsic variations in quantum-dot size, shape, and spatial arrangement, or morphological variability; fluctuations in optical emission properties such as spectral peak, intensity, and blinking or spectral variability; stochastic differences in charge-transport and memristive behavior when QDs form part of electronic circuits or electrical variability; chemical heterogeneities in dopant and ligand distributions or surface-chemistry disorder; and fabrication-induced structural irregularities introduced by processes like polymer encapsulation or femtosecond laser ablation classified under process-induced structural randomness. Each of these mechanisms contributes independent degrees of freedom to the challenge–response pairs, collectively generating a vast and unclonable CRP space that underpins the robustness of QD-PUF authentication. These sources are classified into four broad categories as discussed in the following sections.

3.2.1 Synthesis and fabrication induced randomness. The simplest approach to creating a QD-based PUF involves using monodisperse semiconductor QDs, which exhibit distinct photoluminescence (PL) characteristics. When these dots are deposited onto a substrate *via* drop-casting or spin-coating, slight variations in their arrangement and local environmental factors cause random fluctuations in PL intensity across different regions. This randomness can be harnessed by breaking the coated substrate into smaller fragments, each possessing a unique optical signature that can be digitized into a secure, unclonable identifier. Temperature can be used to "ripen" the dots, inducing modifications in their optical response, such as shifts in emission spectra or enhanced quantum yield and an enhanced complexity implementation utilizes this distribution of QDs with varying sizes, leveraging their size-dependent PL emission. This method generates a broader range of colours, such as RGB emissions, significantly increasing the uniqueness and entropy of the PUF. By encoding both the size distribution and corresponding PL patterns, this approach enables the creation of a higher-density and more intricate identifier system.[75] The PL maps obtained from QD-coated substrates can be digitized by applying intensity thresholds, converting the optical response into a binary or

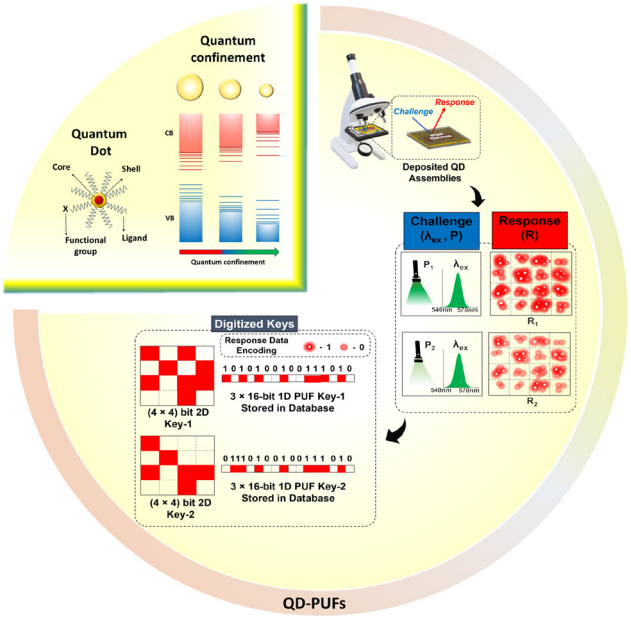

Fig. 2 Schematic highlighting the inherent properties of a QD which can be leveraged for PUF applications. The figure demonstrates how the size-dependent optical properties of quantum dots (QDs) result in varied light emissivity, with different-sized QDs emitting at distinct wavelengths. This tunable optical response serves as the foundation for a challenge-response mechanism, where an external stimulus, such as light irradiation of a specific wavelength or intensity, acts as the challenge. The QD assembly responds by emitting light at characteristic wavelengths based on the distribution of QD sizes. This emission pattern can then be processed and binarized, transforming the optical response into a distinct digitized keys.

multi-bit representation. This process effectively transforms the inherent randomness of QD arrangements into unique cryptographic keys. Fig. 2 illustrates the working principle of an optical QD-based PUF, highlighting the fundamental properties of quantum dots that make this technology feasible.

Gao *et al.*[76] employed reversible phase segregation phenomena in $CsPbBr_xI_{3-x}$ perovskite microspheres as a source of randomness. During synthesis, exposure to varying power densities induced uncontrollable variations in the Br/I composition ratio, leading to stochastic compositional heterogeneity within the microspheres. This synthesis-induced disorder served as a key entropy source for unique material configurations. Fong *et al.*[14] introduced randomness through spatial heterogeneities in colloidal InP/ZnS core/shell QD films. These originated from stochastic clustering and local density fluctuations during the self-assembly and drying processes, which inherently varied across the PUF surface. Such fabrication-induced structural randomness affected optical switching behavior and created unique configurations across regions with differing QD densities, as seen in Fig. 3(a). Kiremitler *et al.*[77] reported an electro-spraying approach that leveraged electrohydrodynamic instabilities to deposit RGB-emitting QDs. Fragmentation of ink droplets under high electric fields led to random yet well-defined dot placement on the substrate, introducing fabrication-level stochasticity into the resulting multicolour patterns (see Fig. 3(b)). Liang *et al.*[78] employed femtosecond laser ablation to introduce randomness post-deposition. Focused ultrafast laser pulses interacted nonlinearly with spin-coated QD films, generating unpredictable voids and topographical features due to nanoscale fluctuations in film morphology and laser-material interaction dynamics, as illustrated in Fig. 3(c).

3.2.2 Chemical and surface effects. Chemical and surface effects play a crucial role in shaping the entropy landscape of QD-based PUFs. Variations in local surface chemistry, molecular interactions, and responsiveness to environmental parameters govern how quantum dots assemble, adhere, and emit, resulting in structurally unique, irreproducible configurations. These effects, including pH-sensitive adhesion, surface energy variations, topography-guided deposition, and phase-responsive behavior, serve as potent entropy sources during fabrication, yielding high-dimensional, unclonable patterns as shown in several recent studies.

Torun *et al.*[79] employed electrohydrodynamic jet printing to deposit poly(2-vinylpyridine) (P2VP) templates that selectively capture QDs *via* pH-dependent electrostatic interactions. At acidic pH values (≤4), P2VP dissolves locally, creating disordered domains that promote random QD adsorption. This results in irregular fluorescence patterns driven by surface-chemical interactions and heterogeneity in adhesion, forming the basis for device-specific cryptographic keys (see Fig. 3(d)). Zhang *et al.*[13] exploited the Brownian motion of PbS nano- and microparticles in suspension to generate spatial randomness. The erratic particle trajectories, shaped by solution-phase interactions and interfacial dynamics, produced non-reproducible particle arrangements that were frozen during film formation and used as physical entropy sources in PUF encoding.

Surface morphology and energy landscape were also harnessed by Chen *et al.*,[5] who implemented a spatial-temporal encoding scheme by depositing perovskite QDs on chaotic metasurfaces (see Fig. 3(e)). These disordered topographies, formed by argon ion etching of Sapphire/Al/PMMA substrates, introduced a rugged surface featuring pits, ridges, and curves. QDs, upon deposition, preferentially adhered to high-surface-energy sites or trapped within nanoscale crevices, resulting in irregular, spatially encoded emission profiles. Torun *et al.*[83] further demonstrated entropy generation through a thermally activated dewetting mechanism of printed P2VP droplets. Thickness gradients within the droplets modulated the dewetting behavior, leading to stochastic formation of microfeatures that subsequently captured QDs *via* electrostatic affinity, adding chemical selectivity to the randomness landscape.

Huang *et al.*[80] integrated chemical selectivity and optical complexity by embedding Yb^{3+} doped perovskite nanocrystals into chiral-imprinted photonic (CIP) films (see Fig. 3(f)). The chiral polymer matrix, formed through surface templating, introduced chemical anisotropy and selective binding domains. These chemical and structural features modulated NIR emission and circularly polarized luminescence (CPL),

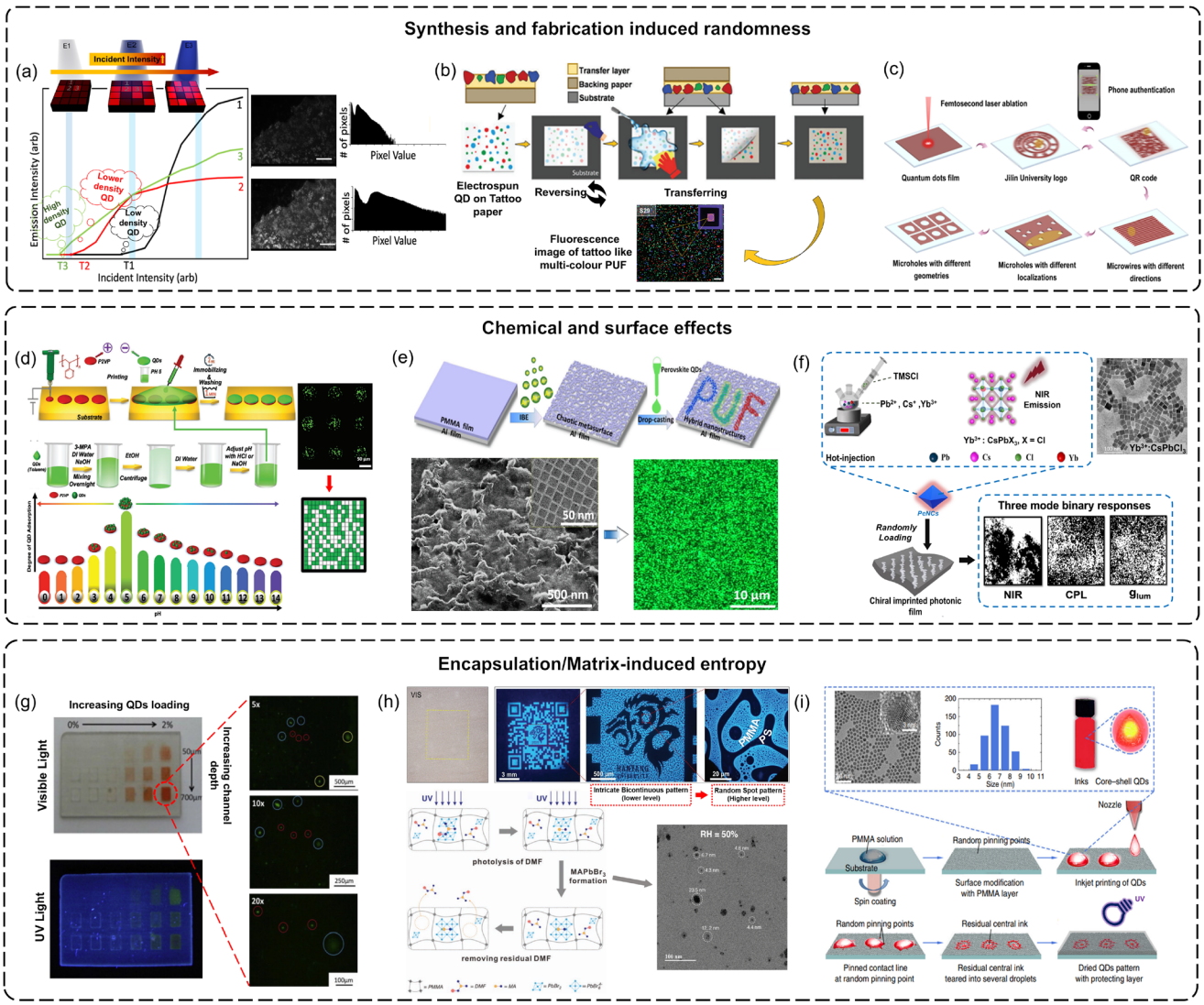

Fig. 3 Overview of the reported physical entropy sources during the fabrication of QD-PUFs. (a) Stochastic clustering and local density variations of QDs, resulting from colloidal self-assembly and drying kinetics, lead to region-specific switch-on thresholds (T1, T2, T3) under varying excitation powers (E1 → E2 → E3), as seen in the nonlinear emission response. Reproduced with permission from ref. 14. Copyright © 2022 Springer Nature. (b) A tattoo-like PUF created through stochastic deposition of multi-coloured semiconductor QDs *via* electrospraying. The electrohydrodynamic instabilities inherent to electrospraying ensure unpredictability in the position and size of features. Reproduced with permission from ref. 77. Copyright © 2023 Wiley-VCH GmbH. (c) Femtosecond laser ablation creates unpredictable topographic voids in QD films, governed by nonlinear laser-material interactions and film morphology. Reproduced with permission from ref. 78. Copyright © 2023 American Chemical Society. (d) Random microfeatures are formed *via* pH-controlled electrohydrodynamic printing of P2VP. QDs dropcast onto these surfaces adhere stochastically due to pH-sensitive interactions, enabling unique PUF encoding.[79] Reproduced with permission from ref. 79. Copyright © 2023 Wiley-VCH GmbH. (e) PUFs are created by dropcasting QDs on ion beam-etched PMMA metasurfaces. The SEM shows the resulting hybrid structure, with an inset TEM of a green-emitting $CsPbX_3$ QD. A fluorescent speckle image enables binary key extraction.[5] Reproduced with permission from ref. 5. Copyright © 2020 Elsevier. (f) Cubic perovskite nanocrystals, synthesized *via* hot-injection, are randomly deposited on chiral-imprinted photonic films, forming unclonable surfaces. Reproduced with permission from ref. 80. Copyright © 2024 American Chemical Society. (g) QD-polymer composites with varying reservoir depths (50 μm, 350 μm, 700 μm) viewed under room and UV light, incorporating QD concentrations from 0–2 wt%. QDs are manually embedded in a photopolymer and UV-cured. Right: fluorescence microscopy images of the 700 μm channel with 0.005 wt% QDs at different magnifications, showing distinctive dot shapes/sizes. Reproduced with permission from ref. 71 Copyright © 2014 Elsevier. (h) Multilevel patterns combining large-scale bicontinuous textures with fine, random-sized $MAPbBr_3$ NP spots formed by spinodal decomposition and photolysis. The resulting optical PUFs show statistically unique patterns under UV light. Reproduced with permission from ref. 81. Copyright © 2022 Wiley-VCH GmbH. (i) Inkjet-printed security labels with red-fluorescent CdSe/CdS/CdZnS QDs and a second layer of randomly distributed PMMA NPs, which create stochastic pinning at the three-phase ink contact line. Reproduced with permission from ref. 82. Copyright © 2019 Springer Nature.

resulting in spatially variant, chemically driven optical fingerprints. Wang *et al.*[84] demonstrated CMOS-compatible PUFs based on Er-doped Si QDs, fabricated using wet etching and spin-coating. The interaction of QDs with surface-coupled metastructures led to site-specific emission modulation, where local variations in surface chemistry and optical coupling introduced high entropy, without the need for foreign materials. Gan *et al.*[85] introduced a reconfigurable optical PUF using VO_2 nanocrystals, where entropy was sourced from thermally induced phase transitions. These phase changes which were sensitive to external stimuli and mediated by nanocrystal morphology and surface energy, enabled dynamic challenge–response pairs that are both unpredictable and environment-responsive.

3.2.3 Encapsulation/matrix-induced entropy. A significant source of entropy emerges when QDs are encapsulated or embedded within polymeric or functional matrices. The interaction between QDs and the surrounding medium introduces additional layers of unpredictability through phase separation, spatial confinement, or interfacial energy landscapes. These encapsulation-induced effects generate multiscale randomness that contributes to the formation of unique optical or structural fingerprints, independent of external readout tools. As a result, matrix-assisted architectures have become integral to the development of robust QD-PUF systems.

Ivanova *et al.*[71] demonstrated a foundational approach by dispersing CdSe QDs within a photopolymer composite. Stochastic clustering of QDs into agglomerates ranging from 1 to 50 μm led to spatial heterogeneity in emission patterns (see Fig. 3(g)). The randomness originated from uncontrolled inter-QD interactions and matrix confinement during polymerization, producing unique optical tags inherently resistant to duplication. Minh *et al.*[81] embedded $MAPbBr_3$ perovskite QDs within a PMMA/polystyrene polymer blend, yielding matrix-induced entropy on multiple scales. A bi-continuous, spinodal-like phase separation emerged at lower magnification, while high-resolution images revealed discrete, randomly sized emission spots, each resulting from nanoscale confinement and compositional inhomogeneity (see Fig. 3(h)). The resulting hierarchical, UV-activated optical patterns enabled high-security encoding within printed elements such as QR codes. A similar strategy was adopted by You *et al.*,[86] where spontaneous phase separation of PMMA and PS during solvent evaporation led to fingerprint-like patterns. Selective *in situ* growth of perovskite QDs in the PMMA-rich domains introduced both spatial and spectral randomness, as QD nucleation was guided by local chemical affinity and confinement effects.

Liu *et al.*[82] introduced another matrix-driven stochastic mechanism *via* inkjet printing of RGB-emitting II–VI QDs on PMMA nanoparticle-treated surfaces. The nanoparticles introduced random pinning sites that influenced the evaporation dynamics and final dot morphology at the three-phase contact line. This process generated flower-like emission features with stochastic geometries (see Fig. 3(i)), which were further enhanced by invisibility under ambient light and activation under UV. The integration of randomness at the matrix–surface level offered high entropy alongside compatibility with scalable manufacturing. Zhang *et al.*[13] incorporated PbS QDs into a thiolene polymer matrix, where ultrasonic dispersion and photoinitiated curing induced random QD positioning despite overall uniform film formation. Collectively, these works underscore how encapsulating QDs within polymers or functional matrices introduces new dimensions of entropy through uncontrolled phase behavior, surface interactions, and confinement effects. Matrix-induced randomness offers a scalable, material-intrinsic path to secure, unclonable identifiers—advancing the design of next-generation PUFs with high complexity, environmental robustness, and integration flexibility.

3.2.4 Multimodal sources. A multimodal entropy system exploits multiple intrinsic randomness sources: optical, electrical, thermal, structural, and more, triggered by different physical stimuli. Such systems enhance security and unpredictability by integrating several independently randomizable features into a single PUF framework. Wang *et al.*[84] demonstrated a CMOS-compatible multimodal platform by incorporating erbium-doped silicon QDs into inverted-pyramid metasurfaces on silicon substrates. Their architecture utilized five independent entropy sources: including geometric variations in micropatterns, shifts in PL wavelength and intensity, and differences in PL lifetimes of both Si QDs and Er^{3+} ions, to produce complex and high-density optical security keys (Fig. 4(a)).

Jung *et al.*[88] developed a QLED-based biometric system using ZnO NPs and narrow-emitting green QDs. Although not strictly a PUF, the device used scattering-induced optical randomness from skin microstructure combined with thermal entropy from rGO temperature sensors. This dual-mode approach: spatial (optical) and temporal (thermal), ensures resistance to spoofing and enhances uniqueness. Guo *et al.*[89] also presented a multimodal platform based on circularly polarized luminescence. Their hybrid material, comprising chiral dopants, QDs, and liquid crystals, exhibited color-tunable responses to external stimuli like voltage and light. Multimodal entropy emerged from both structural chirality and tunable photophysical behavior, enabling secure, real-time, and even blockchain-compatible authentication.

Most recently, Ahn *et al.*[87] introduced a nanoseed-based PUF exploiting two core physical entropy sources: optical and electrical. A hybrid film of PbS QDs and Ag NCs exhibited optical randomness *via* stochastic growth of $CsPbBr_3$ crystals on the QD surface, while electrical entropy arose from randomly formed conductive percolation paths among Ag NCs and insulating QDs (see Fig. 4(b)). The decoupled and independently measurable randomness was securely merged using a shuffling-based encryption scheme, yielding over $10^{58\,741}$ unique keys per mm^2, achieved without any external data storage. Together, these studies highlight how multiple entropy sources, when embedded within a single physical platform, can exponentially boost the complexity, security, and clone-resistance of PUFs, laying the foundation for future-proof, tamper-evident cryptographic systems.

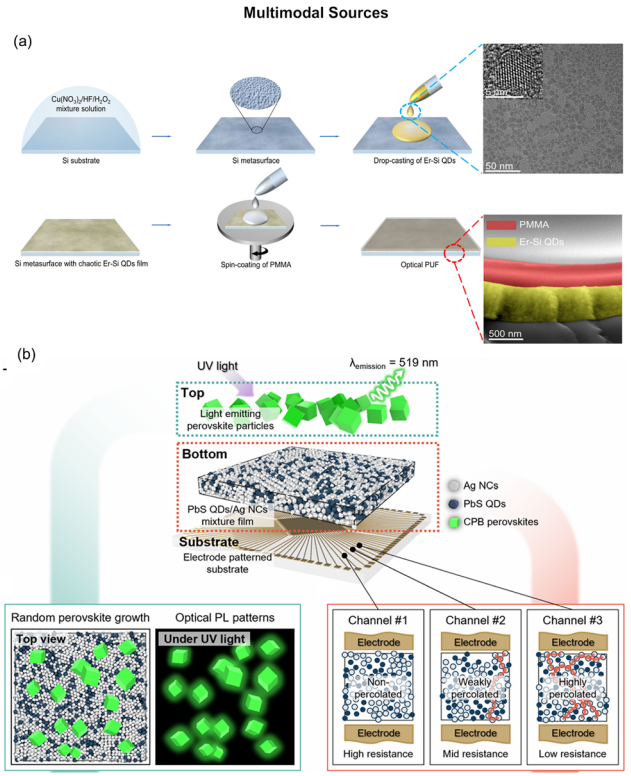

Fig. 4 Multimodal entropy sources in QD-PUFs (a). Fabrication process of an all-Si multidimensionally-encoded optical PUF. Accompanying it is a TEM image of the Er–Si QD solution and the cross-sectional SEM image of the resulting optical PUF with a PMMA encapsulation. Reproduced with permission from ref. 84. Copyright © 2024 Springer Nature. (b). A nanoseed-based PUF design layer. The zoomed-in view of these layers represents how the randomly positioned $CsPbBr_3$ particles at the top layer help generate unique PL patterns as a fundamental component of an optical PUF. It also depicts the random formation of electrical pathways in the bottom layer, which acts as a fundamental component of an electrical PUF. Reproduced with permission from ref. 87. Copyright © 2025 Science Advances.

4 Challenge-response extraction: readout mechanisms for PUFs

The effectiveness of any PUF relies not only on the entropy source but also on the readout process, which extracts the unique features embedded during encoding. Depending on the physical phenomenon probed, CRPs can take various forms—including binary images (*e.g.*, from fluorescence maps), electrical signatures (*e.g.*, resistance states), spectral outputs (*e.g.*, emission wavelengths), temporal lifetimes, or combinations thereof in multimodal systems. The choice of readout strategy—optical, electrical, spectral, physical, or multimodal—thus directly dictates the type, dimensionality, and entropy of the resulting CRP. Each readout approach offers trade-offs in speed, cost, dimensionality, and robustness, and is often selected based on the nature of the encoding material and the intended application (*e.g.*, secure ID tags, on-chip authentication, or packaging-level security). In practice, the readout mechanism shapes the final form of CRP and ultimately determines the system's applicability, repeatability, and resistance to cloning or modeling attacks.

Optical readout techniques, such as fluorescence imaging, laser scattering, and CCD/CMOS camera capture, are widely used due to their ability to enable high-dimensional and parallel interrogation in a non-contact manner. These methods offer the advantage of being relatively fast and scalable. However, they are sensitive to environmental factors such as lighting conditions, alignment, and optical noise, which can compromise the reliability of the CRPs.[77,80–82] A commonly observed response is the formation of speckle patterns, which arise from the coherent interaction of light with a random, disordered medium, producing distinct interference patterns.[5] Data collected using imaging devices, such as a spectrometer or camera for optical PUFs, is converted from analog spectral data to a digital format by extracting key features, including peak positions, intensities, and full width at half-maximum (FWHM). Fig. 5(a) schematically illustrates the three-step approach typically observed in optical PUF systems. The process begins with optical stimuli (the challenge), which generate specific optical data (the optical response) through readout using specific imaging devices. Finally, the response data is digitized into binary keys[5,90] or quaternary values.[90] Diffused reflection, transmission, and spatial scattering patterns further enable the characterization of surface roughness, particle sizes, and spatial arrangements within the QD ensemble.[91] Studies frequently combine multiple optical responses to improve functionality and increase the encoding density of QD-based PUFs.[92]

Spectral and temporal readouts leverage material-specific properties such as emission spectra, fluorescence lifetimes, or Raman scattering signals. These approaches leverage the rich photophysical phenomena of QDs to generate high-dimensional responses, often beyond static imaging or electrical measurements. Additionally, the time-dependent photoluminescence decay profiles of QDs further provide unique temporal signatures, adding another dimension to PUF responses.[82,84] An example of this is shown in Fig. 5(b). Inelastic scattering phenomena, including Stokes and anti-Stokes scattering, reveal important information about the vibrational energy levels of the QDs, serving as unique spectral fingerprints.[93] Nevertheless, they often require precise instrumentation and may be susceptible to phenomena such as blinking or photobleaching that affect repeatability.[14,76,84]

Multimodal readout strategies integrate two or more of the aforementioned approaches, combining optical, electrical, spectral, and/or temporal signals to extract richer and more secure CRPs. These methods enhance the robustness, entropy, and uniqueness of the PUF system but come at the cost of greater complexity in instrumentation and the need for advanced data fusion and interpretation techniques.[84,87] A recent study on multimodal-responsive security materials[89] with diverse stimulus-based readout, integrated six-different response modes. Under UV light, the green QDs emit and vary in luminance when viewed through opposite polarizers,

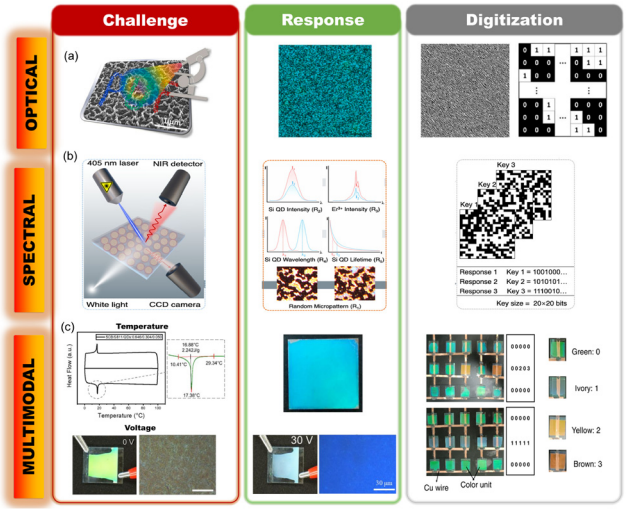

Fig. 5 Readout mechanism capturing the physical entropy sources in QD-PUFs under specific stimuli (challenge) and their encryption process. (a) A partial cyan-colored fluorescent speckle pattern of a perovskite-based QD is obtained as an optical response whose fluorescent pattern and lifetime are manipulated by chaotic metasurfaces to produce the unclonable speckle features. The speckle pattern is then converted to a Gabor-filtered bitmap and finally into the extracted binary key. Reproduced with permission from ref. 5. Copyright © 2020 Elsevier. (b) Challenge-response and authentication process of a QD-based optical PUF utilizing five different responses such as micropattern image (R_1), PL intensities of Si QDs (R_2) and Er^{3+} (R_3), wavelength shift of the PL associated with the band-to-band transition of Si QDs (R_4), and the PL lifetime of Si QDs. The final response keys are generated through a digitization route through comparisions with set threshold values. Reproduced with permission from ref. 84 Copyright © 2024 Springer Nature. (c) A digital code is generated by a voltage-dependent colour change behaviour of the MRSMs. The randomness feature for this PUF arises from stable circularly polarized luminescence materials composed of light-emitting InP/ZnSe/ZnSeS QDs. Based on the CPL structures and QDs, a multimodal responsive security tag is generated out of six different stimuli-responsive modes, including light activation, polarization, temperature, voltage, pressure, and view angle. The response of varying voltage (bottom) on emissive as well as structural properties has been shown; temperature-induced thermochromism behaviour in these MRSMs is also depicted (top). Reproduced with permission from ref. 89. Copyright © 2023 American Chemical Society.

enabling polarization-based authentication. With changes in temperature (25–100 °C), the disbanding of the helical structure turns the material colorless above the clearing point. On the other hand, voltage triggers reversible color shifts to ivory, allowing reprogrammable responses. Fig. 5(c) highlights the stimuli-response pairs based on temperature and voltage. Although pressure is considered, its readout remains unspecified. View-angle dependence causes a blue shift in reflected light. Each stimulus triggers a unique digital code, supporting a multi-layer security.

4.1 Performance evaluation of readout mechanisms for QD-based PUFs

The performance of a PUF system is influenced not only by the source of randomness or entropy but also critically by the characteristics of the readout mechanism. The chosen readout method determines how CRPs are generated, extracted, and interpreted. Among the most vital parameters for evaluating CRP-based systems are the encoding capacity, defined as the total number of unique responses or bits a system can generate, and the authentication time, *i.e.*, the time required to reliably read and validate a response. These two indicators are deeply influenced by the readout strategy. For example, spectral and imaging-based methods enable high encoding capacities due to their capability to resolve multidimensional features such as fluorescence color, intensity, spatial distribution, or lifetime. However, these often incur longer authentication times due to slower data acquisition and processing. Multimodal readout systems, which combine optical and electrical signals or multiple optical dimensions, can achieve faster authentication while maintaining a large CRP space.

The choice of readout method not only determines the hardware or instrumentation required but also significantly impacts how challenge-response pairs (CRPs) are generated and interpreted. In this context, two important considerations are encoding capacity and authentication time. Encoding capacity refers to the total amount of distinct information—typically measured in bits—that can be extracted from a single PUF instance, which in turn affects how uniquely a tag can be identified. Authentication time denotes the duration needed to reliably read and verify a CRP, shaping the speed and practicality of the system in real-world applications. These factors are strongly influenced by the readout mechanism employed; for instance, spectral and imaging-based approaches often offer high encoding densities due to their rich spatial or wavelength-resolved data but may require longer acquisition and processing times. To highlight these trade-offs, Table 1 provides a comparative summary of how various readout strategies perform across these two critical parameters.

Liu *et al.*[82] introduced a CdSe-CdS-CdZnS QD-based PUF comprising 1000 red flower-like patterns, achieving an encod-

Table 1 Comparison of readout mechanisms in QD/NC-based PUFs

Readout mechanism	Typical encoding capacity	Authentication time	Ref.
Spectral readout	Up to $10^{240\,000}$ (*e.g.*, Minh *et al.*)	High (seconds to minutes)	81, 86 and 80
Imaging (spatial patterns)	$2^{98\,888}$ to $2^{202\,000}$	Moderate (1–10 s)	77, 82 and 83
Fluorescence intensity mapping	$2^{156\,250}$ (*e.g.*, Chen *et al.*)	Moderate to fast	5
Time-resolved PL (lifetime)	Up to 10^{500} (depends on fitting resolution)	Slower (requires decay analysis)	81 and 80
Multimodal (spectral + spatial + temporal)	$>10^{58\,741}$ CRPs per mm^2	Fast (sub-second possible)	87, 86 and 84
Electro-optical hybrid	$\sim 2^{1\,000\,000}$	ms-s (*via* algorithmic shuffling)	87

ing capacity of $10^{202\,000}$ and a bit-density of 1.07×10^5 bits per mm^2. Similarly, Zhang *et al.*[13] demonstrated PbS-QD-based PUFs with exceptionally small areas (PUF-1: 14.5 nm^2, PUF-2: 54.76 nm^2) and used Auto-Correlation Function (ACF) analysis to confirm insensitivity to alignment shifts. Minh *et al.*[81] reported one of the highest encoding capacities ($10^{24\,383\,400}$) using a $MAPbBr_3$-PMMA/PS composite PUF with hierarchical structures. This resulted in a bit-density of 7.34×10^4 bits per mm^2 and DoF of 81 000 bits. Kiremitler *et al.*[77] developed a CdSe/CdS dot-in-rod QD-based multicolor PUF tattoo, achieving an encoding capacity of 4^{95} and 192-bit DoF, with sub-10 ms authentication enabled by an ORB feature matching algorithm. Torun *et al.*[83] embedded CdSe/CdS QDs in P2VP to yield an encoding capacity of 2^{370} across 30 PUF labels with NIST-compliant randomness and a reported ENIB of 97 bits.

In the case of spectral-only readouts, Gao *et al.*[76] reported $CsPbBr_xI_{3-x}$ PUFs with a DoF of 94 and low BER (5.8%), yet a modest bit density limited the scalability, achieving 2^{94} capacity and strong performance under the NIST randomness tests. Liu *et al.*[94] proposed an encoding approach using CdSe QD absorption spectra (non-PUF-specific) with a theoretical capacity above 10^{300} and decryption speed of 0.47 s per sample. Wang *et al.*[84] utilized Er-doped Si QDs in CMOS-compatible metasurfaces to create high-density optical keys from five entropy sources, achieving an encoding capacity of 5^{400} and ENIB of 400 bits, albeit with a longer readout time (1 s). Meanwhile, You *et al.*[86] replicated Minh's hierarchical PUF strategy using perovskite QDs, reaching an encoding capacity of $10^{85\,700\,000}$ and bit-density of 7.68×10^3 bits per mm^2. Although encoding capacity was comparable, the lower bit-density highlighted the critical role of readout and binarization strategies.

Ahn *et al.*[87] developed a hybrid PUF using $CsPbBr_3$/PbS QDs and Ag NCs to combine optical and electrical CRPs. Their system reached $>10^{58\,741}$ CRPs per mm^2, with total capacity of $2^{1\,000\,000}$ and ENIB values of ~499 (optical) and ~297 (electrical). Additional entropy metrics such as Lempel-Ziv, Sample Entropy, and Permutation Entropy, confirmed robust multidimensional randomness, overcoming limitations of Shannon entropy alone. These metrics underline resilience to pattern modeling attacks and reflect a highly complex and unpredictable key structure. Minh *et al.*[81] also reported excellent performance across these markers, with uniformity and uniqueness values close to ideal at both low- and high-magnification levels and long-term stability confirmed *via* 9-month delayed remeasurement. Likewise You *et al.*[86] presented strong reliability (BER < 1%) and high d' values of ~24 and 41, respectively. Wang *et al.*[84] evaluated an Er–Si QD/metasurface hybrid PUF which, despite a modest ENIB of 400, reported excellent stability with BER ~0.01 and an extremely low FPR of 2.42×10^{-22}. The decidability ($d' \approx 38.32$) and bit density of 13.5 bits per pixel reaffirm its high-performance credentials.

Some studies have proposed non-bit-based figures of merit for readout evaluation. Fong *et al.*[14] introduced authentication *via* photoluminescence power-law exponents and switch-on intensity maps, enabling spoof-resistant optical validation. Guo *et al.*[89] proposed a CPL-based figure of merit (FM = $\phi \times |g_{lum}|$), reporting one of the highest FM values (0.39) for processable QD-LC hybrids, thereby embedding security in photonic descriptors even before digitization.

Finally, environmental robustness is a key determinant for real-world PUF deployment. Systems reported by Minh *et al.*[81] and Wang *et al.*[84] showed excellent resistance to photobleaching, heat (100 °C), humidity, abrasion, and UV exposure, with signal retention above 94% and structural integrity verified *via* image correlation post-treatment.

While encoding capacity, DoF, authentication time, and NIST randomness tests are commonly cited, a more complete evaluation of QD-PUFs, especially non-IID optical systems, requires bit-level metrics such as mean (μ), variance (σ), Bit Error Rate (BER), False Positive Rate (FPR), and decidability. As illustrated in Fig. 6(b), metrics like uniformity, uniqueness, reliability, BER, and decidability provide a more grounded comparison across QD-PUF systems.

Starting with the best-performing systems, Chen *et al.*[5] reported a $CsPbBr_3$/metasurface PUF with near-ideal bit-uniformity, inter-HD of 0.499 (variance: 1.74×10^{-6}), and high reliability (0.914 ± 0.001), resulting in a BER of 0.086. Although decidability wasn't directly reported, it can be computed as 15, indicating minimal overlap between inter/intra-HD distributions. Liu *et al.*[82] developed a CdSe/CdS/CdZnS QD-PUF with AI-assisted authentication, achieving a 0% FPR at thresholds 0.5, though HD-based metrics were not discussed. Minh *et al.*[81] created $MAPbBr_3$-based hierarchical PUFs with two magnification levels, achieving excellent uniformity (0.4977 and 0.4718) and inter-HD values (0.5033 and 0.4625). The system showed only 0.0398% variation over nine months, demonstrating robust temporal stability.

Among multimodal systems, Ahn *et al.*[87] presented an electro-optic PUF combining optical and electrical CRPs with shuffled keys ($>10^{58\,741}$ per mm^2), achieving DoF values of 499 (optical) and 297 (electrical). Despite lower ENIB, metrics such as S_{LZ}, BER (0.06–1%), and decidability (~24 optical, ~21 electrical) confirm robust randomness and low overlap in key distributions. You *et al.*[86] reported (Rb,Cs)$PbBr_3$-based PUFs with

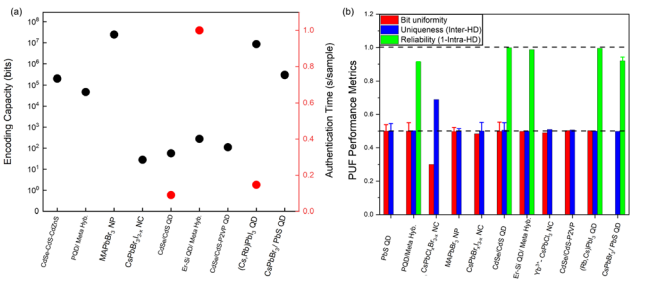

Fig. 6 Performance Evaluation of QD-PUFs. (a) A plot showing the encoding capacity and authentication time of a set of QD/NC-based optical PUFs reported in the literature. (b) A bar plot representation of the available data points containing the other performance metrics, namely Bit uniformity, uniqueness and reliability of a set of QD/NC-based optical PUFs.

DoF 431 and a BER as low as 0.00498. Uniformity, uniqueness, and reliability were all close to ideal, and a high decidability of $d \approx 41$ indicated well-separated key spaces.

Wang *et al.*[84] demonstrated an Er-doped Si QD/metasurface hybrid PUF with DoF = 400 (20 × 20 pixels, 5 responses per pixel). The system achieved low BER (~0.01), extremely low false acceptance (2.4×10^{-22}), and a high decidability ($d \approx 38.3$), confirming long-term key stability. In the lower DoF cohort, Kiremitler *et al.*[77] reported RGB tattoo-like QD-PUFs with 192 bits per tag and strong FPR (10^{-16}), though the lack of area data limits bit-density analysis. Decidability values were $d \approx 17$, 11, and 11 across color channels. Torun *et al.*[83] extracted 256 bits across 30 CdSe/CdS–P2VP tags, but only 97 of these represented independent degrees of freedom. Although NIST tests passed, the absence of BER or d data leaves robustness uncertain. Gao *et al.*[76] achieved ENIB = 94 and DoF 100 in $CsPbBr_xI_{3-x}$ QD-PUFs, but a 5.8% BER and $d \approx 10$ suggest increasing error risk at scale (TAEP 10^{-4}). Zhang *et al.*[13] focused on ultra-compact PbS QD PUFs (14.5–54.8 bits per mm^2) with strong uniformity and uniqueness, but without BER or ENIB data, limiting comparisons. Finally, Huang *et al.*[80] reported Yb^{3+}:$CsPbCl_3$ PUFs with $d \approx 14$ but high BER (0.11 in NIR, 0.28–0.29 in CPL/g_{lum} modes), suggesting poor reliability despite clear HD separation.

4.2 Role of dimensionality

Ascending the dimensionality ladder, Gao *et al.*[76] reported the fabrication of an optical Br/I perovskite-based PUF, which leveraged the reversible phase segregation phenomenon when subjected to variable irradiation densities. In this study, the $CsPbBr_xI_{3-x}$ (CPBI) microspheres with varying stoichiometric ratios are irradiated with power densities ranging from 1.82 to 3640 mW cm^{-2}. Under low irradiation intensity, characteristic PL peaks of CPBI are obtained; however, upon increasing the power density greater than the threshold limit, phase segregation of halide perovskites occurred, and the PL peaks corresponding to both $CsPbBr_3$ and $CsPbI_3$ can be witnessed. The responses corresponding to the low and high irradiation densities is termed as low and high responses, respectively, contributing to the fabrication of a low and a high PUF tag. The different quantities of iodine control the mixed halide segregation to a large extent due to inherent lattice mismatches,[95] thereby triggering more defect vacancies and resulting in a small threshold power density. Thus, PL maps of these mixed halides vary considerably due to stoichiometric differences and irradiation densities.

5 Applications and use cases

PUFs have a wide range of applications across various fields, particularly in cryptography, IoT, device authentication, and anti-counterfeiting. Their unique ability to generate unclonable identifiers based on physical characteristics makes them ideal for securing communication, verifying device identities, and ensuring product authenticity. In cryptography, PUFs are used to generate secure keys for encryption, providing an additional layer of security due to their unpredictable nature.[96]

The rapid growth of the Internet of Things (IoT) has led to the connection of various devices, from simple smart home gadgets to complex factory control systems. While IoT enables communication, security is crucial for access control, confidentiality, and protection against attacks.[97] A major challenge for IoT devices is their vulnerability to cyber-physical attacks, as secret keys and IDs are often stored in clear text. PUF-based authentication, which avoids storing secret keys in public databases, offers a secure solution for IoT devices. A use case in this aspect is the CMOS-compatible optical PUF with multidimensional encoding for secure IoT authentication.[84] According to this study, the server stores each device's identity (ID) and CRPs based on the photoluminescence wavelength of Si QDs, while the IoT device retains no information, minimizing security risks. The system supports two authentication protocols: device-server (Protocol 1) and device-device mutual authentication (Protocol 2). In Protocol 1, the IoT device sends its ID and a random number to the server, which validates the device and returns an encrypted message. The device then authenticates the message and generates new codes for mutual authentication, which the server verifies to complete the process. Protocol 2 facilitates direct authentication between two IoT devices. Device A sends its ID and a random number to device B, which forwards them to the server. The server retrieves the corresponding CRPs and sends encrypted messages back to device A. After decryption and verification, device A responds securely, triggering a challenge relay and a final handshake, ensuring successful mutual authentication.

Optical PUFs play a crucial role in anti-counterfeiting measures due to their unique optical properties, making them nearly impossible to replicate or forge. One of the significant innovations in this field is the development of secure modern currency. Traditional features of banknotes, such as holographic metal strips, are vulnerable to cloning and can be easily reproduced. Currently, the only unique identifier for banknotes is the serial number, stored in an external database. To further enhance security, new anti-counterfeiting PUF tags with dynamic authentication are being introduced, making

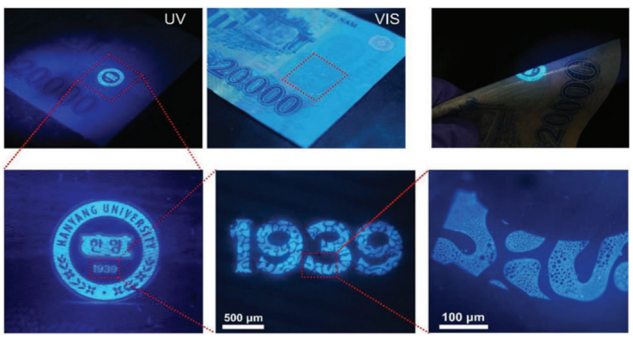

Fig. 7 Demonstration of a $MAPbBr_3$-PMMA/PS composite films as transparent anticounterfeiting label on a banknote. Reproduced with permission from ref. 81. Copyright © 2022 Wiley-VCH GmbH.

counterfeiting even more challenging. For instance, $MAPbBr_3$-PMMA/PS composite film-based PUFs reported by Minh *et al.*[81] remained highly transparent under visible light but revealed the underlying hierarchical features under UV light. These patterns were successfully transferred to banknotes with rough textures, as highlighted in Fig. 7, as well as on the curved glass surfaces of watches.

6 Challenges and future directions

While QD-based optical and electrical PUFs present significant opportunities for secure identification and authentication, they also face several technical bottlenecks that need to be addressed.

6.1 Control over fabrication

One of the primary challenges in developing PUFs based on QDs is the precise control over the fabrication process. Variations in the size, shape, and distribution of QDs can significantly affect the performance and reliability of the PUF. Achieving uniformity in the placement of QDs is critical for ensuring consistent optical responses, which can be difficult due to the stochastic nature of nanofabrication[98,99] and patterning techniques.[100] Additionally, the integration of QDs into existing electronic systems poses challenges related to compatibility and scalability.[100,101]

6.2 Cost and complexity

Optical PUFs often require sophisticated readout devices that are not integrated with the PUF itself, leading to higher costs and complexity in deployment.[98] This can limit their practical applications, especially in low-cost consumer products.[102] In contrast, electrical PUFs, while generally more cost-effective, may suffer from issues related to noise and interference, which can compromise their reliability.[102]

6.3 Environmental sensitivity

Both optical and electrical PUFs can be sensitive to environmental factors such as temperature, humidity, and electromagnetic interference. For example, the performance of electrical PUFs can degrade under varying conditions, leading to increased bit error rates.[102,103] Similarly, optical PUFs may exhibit changes in response due to fluctuations in light intensity or wavelength (*i.e.*, variation in challenges), which can affect their robustness.[104]

6.4 Security vulnerabilities

Despite their inherent security advantages, these PUFs are not immune to attacks. Machine learning techniques have been employed to model and predict the behavior of PUFs, potentially compromising their security.[84] Furthermore, invasive and semi-invasive attacks can exploit physical vulnerabilities in both optical and electrical PUFs, necessitating ongoing research into more resilient designs.[102,105] Machine learning and AI-based frameworks could significantly improve the efficiency and adaptability of PUF systems, making them more secure against replication.[82]

7 Conclusion

Quantum dot (QD)-based Physical Unclonable Functions (PUFs) represent a rapidly advancing frontier in high-security applications, leveraging the unique optical and electronic properties of QDs and nanocrystals (NCs) to generate challenge-response pairs with inherent physical randomness. This review has comprehensively examined the progress in QD- and NC-based PUFs, emphasizing their implementation in optical, electrical, and multimodal systems. The quantum confinement effects in QDs, which lead to discrete energy levels, and the combinatorial encoding achieved by integrating QDs into engineered nanostructures such as metasurfaces and polymeric matrices, have been explored as critical mechanisms for secure authentication. The integration of QDs into PUFs links fundamental material properties with entropy sources arising from synthesis, fabrication, surface effects, and encapsulation. Our comparative analysis of optical, spectral, and multimodal readout schemes, together with their emerging applications, highlights the distinctive encoding capacity and security advantages of QD-based systems. Despite these advancements, continued research is essential to refine QD-based PUFs, particularly in enhancing their stability, reproducibility, and resistance to cloning. Improvements in synthesis techniques, device integration, and multimodal authentication strategies will be key to their broader adoption. By addressing these challenges, QD-based PUFs are poised to redefine the landscape of hardware security, emerging as a transformative technology for next-generation anti-counterfeiting, cryptographic, and authentication systems.

Conflicts of interest

There are no conflicts to declare.

Data availability

No primary research results, software or code have been included and no new data were generated or analysed as part of this review.

Acknowledgements

AM acknowledges the research fellowship from the Department of Science and Technology (DST) under the Ministry of Science and Technology, Government of India under Innovation in Science Pursuit for Inspired Research (INSPIRE) fellowship for financial support.

References

1 S. Li, T. Tryfonas and H. Li, *Internet Res.*, 2016, **26**, 337–359.
2 Y. Gao, S. F. Al-Sarawi and D. Abbott, *Nat. Electron.*, 2020, **3**, 81–91.
3 B. Halak, M. Zwolinski and M. S. Mispan, 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), 2016, pp. 1–4.
4 Z. Qin, M. Shintani, K. Kuribara, Y. Ogasahara and T. Sato, *IEEE Sens. J.*, 2020, **20**, 7569–7578.
5 F. Chen, Q. Li, M. Li, F. Huang, H. Zhang, J. Kang and P. Wang, *Chem. Eng. J.*, 2021, **411**, 128350.
6 M.-K. Chung, M.-U. Kim, J.-W. Han, J.-S. Yang, B.-J. Kim, M.-S. Jo, S.-Y. Jung, S.-H. Kim and J.-B. Yoon, 2024 IEEE 37th International Conference on Micro Electro Mechanical Systems (MEMS), 2024, pp. 521–524.
7 A. F. Smith and S. E. Skrabalak, *J. Mater. Chem. C*, 2017, **5**, 3207–3215.
8 R. Arppe and T. J. Sørensen, *Nat. Rev. Chem.*, 2017, **1**, 0031.
9 K. Agarwal, H. Rai and S. Mondal, *Mater. Res. Express*, 2023, **10**, 062001.
10 A. I. Ekimov, F. Hache, M. Schanne-Klein, D. Ricard, C. Flytzanis, I. Kudryavtsev, T. Yazeva, A. Rodina and A. L. Efros, *J. Opt. Soc. Am. B*, 1993, **10**, 100–107.
11 Y. Shirasaki, G. J. Supran, M. G. Bawendi and V. Bulović, *Nat. Photonics*, 2013, **7**, 13–23.
12 L. E. Brus, *J. Chem. Phys.*, 1984, **80**, 4403–4409.
13 Y. Zhang, Z. Luan, X. Zhang, J. Shu and P. Wang, *J. Electron. Mater.*, 2019, **48**, 7603–7607.
14 M. J. Fong, C. S. Woodhead, N. M. Abdelazim, D. C. Abreu, A. Lamantia, E. M. Ball, K. Longmate, D. Howarth, B. J. Robinson, P. Speed, *et al.*, *Sci. Rep.*, 2022, **12**, 16919.
15 S. Ren, B. Liu, M. Wang, G. Han, H. Zhao and Y. Zhang, *J. Mater. Chem. C*, 2022, **10**, 11338–11346.
16 D. W. Bauder, Sandia National Labs Report SAND82-2921, 1983.
17 G. J. Simmons, Advances in Cryptology: Proceedings of CRYPTO, 1984, pp. 411–431.
18 D. Naccache and A. Frémanteau, ESORICS, 1992.
19 M. Clerc and J.-P. Wagner, Proceedings of IEEE Security and Privacy, 1993.
20 R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, *Science*, 2002, **297**, 2026–2030.
21 B. Gassend, D. Clarke, M. van Dijk and S. Devadas, Proceedings of the 9th ACM conference on Computer and communications security, 2002, pp. 148–160.
22 D. Hankerson, A. Johnson and A. J. Menezes, *IEEE Trans. Circuits Syst. I*, 2006, **53**, 1458–1465.
23 J. Guajardo, S. S. Kumar, G.-J. Schrijen and P. Tuyls, CHES 2007: Cryptographic Hardware and Embedded Systems, 2007, pp. 63–80.
24 C. Böhm, M. Hofer and W. Pribyl, 2011 5th International Conference on Network and System Security, 2011, pp. 269–273.
25 U. Rührmair, S. Devadas and F. Koushanfar, IEEE HOST, 2009.
26 S. Hemavathy and V. K. Bhaaskaran, *IEEE Access*, 2023, **11**, 33979–34004.
27 A. Maiti and P. Schaumont, *J. Cryptol.*, 2011, **24**, 375–397.
28 G. E. Suh and S. Devadas, *IEEE Trans. Inf. Forensics Secur.*, 2008, **3**, 706–717.
29 R. Xu and M. Tehranipoor, *IEEE Trans. Dependable Secure Comput.*, 2015, **12**, 248–260.
30 Y. Wang, L. Xie and C. Lin, *Nano Lett.*, 2015, **15**, 8262–8268.
31 Y. Gao, M. Yu and K. Han, *Opt. Express*, 2017, **25**, 16248–16258.
32 E. Mann-Andrews, T. McGrath, B. Halliday and R. J. Young, *Appl. Phys. Rev.*, 2025, **12**, 021314-1–021314-27.
33 C. E. Shannon, *Bell Syst. Tech. J.*, 1948, **27**, 379–423.
34 Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, *IEEE Access*, 2017, **4**, 61–80.
35 A. D. Yoffe, *Adv. Phys.*, 2001, **50**, 1–208.
36 D. Bera, L. Qian, T.-K. Tseng and P. H. Holloway, *Materials*, 2010, **3**, 2260–2345.
37 G. Markovich, C. P. Collier, S. E. Henrichs, F. Remacle, R. D. Levine and J. R. Heath, *Acc. Chem. Res.*, 1999, **32**, 415–423.
38 Y. Liu, S. Bose and W. Fan, *Optik*, 2018, **155**, 242–250.
39 R. E. Bailey and S. Nie, *J. Am. Chem. Soc.*, 2003, **125**, 7100–7106.
40 A. M. Smith and S. Nie, *Acc. Chem. Res.*, 2010, **43**, 190–200.
41 I. Moreels, K. Lambert, D. Smeets, D. De Muynck, T. Nollet, J. C. Martins, F. Vanhaecke, A. Vantomme, C. Delerue, G. Allan, *et al.*, *ACS Nano*, 2009, **3**, 3023–3030.
42 V. I. Klimov, A. A. Mikhailovsky, S. Xu, A. Malko, J. A. Hollingsworth, C. A. Leatherdale, H.-J. Eisler and M. G. Bawendi, *Science*, 2000, **290**, 314–317.
43 A. L. Efros and M. Rosen, *Annu. Rev. Mater. Sci.*, 1996, **26**, 89–116.
44 A. P. Alivisatos, *J. Phys. Chem.*, 1996, **100**, 13226–13239.
45 G. Shi, A. Kaewprajak, X. Ling, A. Hayakawa, S. Zhou, B. Song, Y. Kang, T. Hayashi, M. E. Altun, M. Nakaya, *et al.*, *ACS Energy Lett.*, 2019, **4**, 960–967.
46 N. Y. Morgan, C. Leatherdale, M. Drndić, M. V. Jarosz, M. A. Kastner and M. Bawendi, *Phys. Rev. B:Condens. Matter Mater. Phys.*, 2002, **66**, 075339.
47 S. J. Oh, Z. Wang, N. E. Berry, J.-H. Choi, T. Zhao, E. A. Gaulding, T. Paik, Y. Lai, C. B. Murray and C. R. Kagan, *Nano Lett.*, 2014, **14**, 6210–6216.
48 J.-H. Choi, A. T. Fafarman, S. J. Oh, D.-K. Ko, D. K. Kim, B. T. Diroll, S. Muramoto, J. G. Gillen, C. B. Murray and C. R. Kagan, *Nano Lett.*, 2012, **12**, 2631–2638.
49 M. S. Kang, A. Sahu, D. J. Norris and C. D. Frisbie, *Nano Lett.*, 2010, **10**, 3727–3732.
50 M. Drndić, M. Jarosz, N. Morgan, M. Kastner and M. Bawendi, *J. Appl. Phys.*, 2002, **92**, 7498–7503.
51 L. Brus, *J. Phys. Chem.*, 1986, **90**, 2555–2560.

52 Y.-S. Park, J. Roh, B. T. Diroll, R. D. Schaller and V. I. Klimov, *Nat. Rev. Mater.*, 2021, **6**, 382–401.
53 H. Weller, H. Schmidt, U. Koch, A. Fojtik, S. Baral, A. K. Henglein and W. Kunath, *Chem. Phys. Lett.*, 1986, **124**, 557–560.
54 M. A. Hines and P. Guyot-Sionnest, *J. Phys. Chem.*, 1996, **100**, 468–471.
55 D. Yang, C. Lu, H. Yin and I. P. Herman, *Nanoscale*, 2013, **5**, 7290–7296.
56 I. L. Medintz, H. M. Uyeda and E. R. Goldman, *Nat. Mater.*, 2005, **4**, 435–446.
57 M. Nirmal, B. Dabbousi, M. Bawendi, J. Macklin, J. Trautman, T. Harris and L. Brus, *Nature*, 1996, **383**, 802–804.
58 Y. Gao, C. S. Sandeep, J. M. Schins, A. J. Houtepen and L. D. Siebbeles, *Nat. Commun.*, 2013, **4**, 2329.
59 R. Osovsky, D. Cheskis, V. Kloper, A. Sashchiuk, M. Kroner and E. Lifshitz, *Phys. Rev. Lett.*, 2009, **102**, 197401-1–197401-4.
60 N. Ray, N. E. Staley, D. D. Grinolds, M. G. Bawendi and M. A. Kastner, *Nano Lett.*, 2015, **15**, 4401–4405.
61 C. R. Kagan and C. B. Murray, *Nat. Nanotechnol.*, 2015, **10**, 1013–1026.
62 R. Chandler, A. Houtepen, J. Nelson and D. Vanmaekelbergh, *Phys. Rev. B:Condens. Matter Mater. Phys.*, 2007, **75**, 085325.
63 P. Guyot-Sionnest, *J. Phys. Chem. Lett.*, 2012, **3**, 1169–1175.
64 H. Liu, A. Pourret and P. Guyot-Sionnest, *ACS Nano*, 2010, **4**, 5211–5216.
65 J. Yu, M. Luo, Z. Lv, S. Huang, H.-H. Hsu, C.-C. Kuo, S.-T. Han and Y. Zhou, *Nanoscale*, 2020, **12**, 23391–23423.
66 A. Yakimov, A. Dvurechenskii, V. Kirienko, Y. I. Yakovlev, A. Nikiforov and C. Adkins, *Phys. Rev. B:Condens. Matter Mater. Phys.*, 2000, **61**, 10868.
67 H. Cheng, Y. Lu, D. Zhu, L. Rosa, F. Han, M. Ma, W. Su, P. S. Francis and Y. Zheng, *Nanoscale*, 2020, **12**, 9471–9480.
68 X. Michalet, F. F. Pinaud, L. A. Bentolila, J. M. Tsay, S. Doose, J. J. Li, G. Sundaresan, A. M. Wu, S. S. Gambhir and S. Weiss, *Science*, 2005, **307**, 538–544.
69 R. A. John, N. Shah, S. K. Vishwanath, S. E. Ng, B. Febriansyah, M. Jagadeeswararao, C.-H. Chang, A. Basu and N. Mathews, *Nat. Commun.*, 2021, **12**, 3681-1–3681-11.
70 K. D. Longmate, N. M. Abdelazim, E. M. Ball, J. Majaniemi and R. J. Young, *Sci. Rep.*, 2021, **11**, 10999-1–10999-8.
71 O. Ivanova, A. Elliott, T. Campbell and C. Williams, *Addit. Manuf.*, 2014, **1**, 24–31.
72 H. Moon, C. Lee, W. Lee, J. Kim and H. Chae, *Adv. Mater.*, 2019, **31**, 1804294.
73 B. Xu, B. Cai, M. Liu and H. Fan, *Nanotechnology*, 2013, **24**, 205601-1–205601-13.
74 N. Órdenes-Aenishanslins, G. Anziani-Ostuni, C. P. Quezada, R. Espinoza-González, D. Bravo and J. M. Pérez-Donoso, *Front. Microbiol.*, 2019, **10**, 1587-1–1587-13.
75 N. Kayaci, R. Ozdemir, M. Kalay, N. B. Kiremitler, H. Usta and M. S. Onses, *Adv. Funct. Mater.*, 2022, **32**, 2108675.
76 X. Gao, H. Wang, H. Dong, J. Shao, Y. Shao and L. Zhang, *ACS Appl. Mater. Interfaces*, 2023, **15**, 23429–23438.
77 N. B. Kiremitler, A. Esidir, G. A. Drake, A. F. Yazici, F. Sahin, I. Torun, M. Kalay, Y. Kelestemur, H. V. Demir, M. Shim, *et al.*, *Adv. Opt. Mater.*, 2024, **12**, 2302464.
78 S.-Y. Liang, Y.-F. Liu, Z.-K. Ji and H. Xia, *ACS Appl. Mater. Interfaces*, 2023, **15**, 10986–10993.
79 I. Torun, C. Huang, M. Kalay, M. Shim and M. S. Onses, *Small*, 2024, **20**, 2305237-1–2305237-12.
80 J. Huang, X. Jin, X. Yang, T. Zhao, H. Xie and P. Duan, *ACS Nano*, 2024, 15888–15897.
81 D. N. Minh, L. A. T. Nguyen, Q. H. Nguyen, T. V. Vu, J. Choi, S. Eom, S. J. Kwon and Y. Kang, *Adv. Mater.*, 2023, **35**, 2208151.
82 Y. Liu, F. Han, F. Li, Y. Zhao, M. Chen, Z. Xu, X. Zheng, H. Hu, J. Yao, T. Guo, *et al.*, *Nat. Commun.*, 2019, **10**, 2409.
83 I. Torun, C. Huang, N. B. Kiremitler, M. Kalay, M. Shim and M. S. Onses, *Small*, 2024, **20**, 2405429.
84 K. Wang, J. Shi, W. Lai, Q. He, J. Xu, Z. Ni, X. Liu, X. Pi and D. Yang, *Nat. Commun.*, 2024, **15**, 3203.
85 Z. Gan, F. Chen, Q. Li, M. Li, J. Zhang, X. Lu, L. Tang, Z. Wang, Q. Shi, W. Zhang, *et al.*, *ACS Appl. Mater. Interfaces*, 2022, **14**, 5785–5796.
86 K. You, J. Lin, Z. Wang, Y. Jiang, J. Sun, Q. Lin, X. Hu, H. Fu, X. Guo, Y. Zhao, *et al.*, *ACS Appl. Mater. Interfaces*, 2025, 5254–5267.
87 J. Ahn, T. Park, T. Kang, S.-G. Im, H. Seo, B.-H. Kim, S. J. Kwon and S. J. Oh, *Sci. Adv.*, 2025, **11**, eadt7527.
88 H. Jung, S. Sim and H. Lee, *Sci. Rep.*, 2023, **13**, 794.
89 Q. Guo, M. Zhang, Z. Tong, S. Zhao, Y. Zhou, Y. Wang, S. Jin, J. Zhang, H.-B. Yao, M. Zhu, *et al.*, *J. Am. Chem. Soc.*, 2023, **145**, 4246–4253.
90 Y. Liu, Y. Zheng, Y. Zhu, F. Ma, X. Zheng, K. Yang, X. Zheng, Z. Xu, S. Ju, Y. Zheng, *et al.*, *ACS Appl. Mater. Interfaces*, 2020, **12**, 39649–39656.
91 K. Karrai and R. J. Warburton, *Superlattices Microstruct.*, 2003, **33**, 311–337.
92 Z. Wang, H. Wang, P. Wang and Y. Shao, *ACS Appl. Mater. Interfaces*, 2024, 27926–27935.
93 E. Fuoco, G. Cipparrone and M. P. De Santo, Ph.D. thesis, Università della Calabria, 2022.
94 S. Liu, X. Liu, X. Zhu, J. Yin and J. Bao, *ACS Nano*, 2023, **17**, 21349–21359.
95 R. Zheng, J. Ueda, K. Shinozaki and S. Tanabe, *J. Phys. Chem. Lett.*, 2022, **13**, 7809–7815.
96 T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig and R. J. Young, *Appl. Phys. Rev.*, 2019, **6**, 011303-1–011303-25.
97 H. Ning, F. Farha, A. Ullah and L. Mao, *IET Circuits Devices Syst.*, 2020, **14**, 407–424.
98 A. Wali, A. Dodda, Y. Wu, A. Pannone, L. K. Reddy Usthili, S. K. Ozdemir, I. T. Ozbolat and S. Das, *Commun. Phys.*, 2019, **2**, 39.
99 Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, *IEEE Access*, 2016, **4**, 61–80.

100 H. K. Lee, T. Park and H. Yoo, *Materials*, 2024, **17**, 5335.
101 N. M. Abdelazim, M. J. Fong, T. McGrath, C. S. Woodhead, F. Al-Saymari, I. E. Bagci, A. T. Jones, X. Wang and R. J. Young, *Sci. Rep.*, 2021, **11**, 1528-1–1528-7.
102 M. S. Mispan, B. Halak and M. Zwolinski, *J. Circuits Syst. Comput.*, 2021, **30**, 2130009-1–2130009-14.
103 R. Zhang, H. Jiang, Z. Wang, P. Lin, Y. Zhuo, D. Holcomb, D. Zhang, J. Yang and Q. Xia, *Nanoscale*, 2018, **10**, 2721–2726.
104 F. Bin Tarik, A. Famili, Y. Lao and J. D. Ryckman, *Nanophotonics*, 2020, **9**, 2817–2828.
105 Y. Gao, H. Ma, S. F. Al-Sarawi, D. Abbott and D. C. Ranasinghe, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2017, **37**, 1104–1108.