Intrinsic Random Optical Features of the Electronic Packages as Physical Unclonable Functions for Internet of Things Security

Qian Li,* Feiliang Chen,* Jianbin Kang, Pidong Wang, Juan Su, Feng Huang, Mo Li, and Jian Zhang

1. Introduction

The internet of things (IoT) is playing an increasingly important role in our daily life as billions of new devices are linked by the internet and interacting through online services every year.[1] IoT can make the remote access and control of various devices, which has virtually penetrated various fields in everyday life such as smart home, industrial control, automated vehicles, logistics monitoring, public safety, and so on.[2] The booming IoT brings people a lot of conveniences, at the same time comes about a series of problems. One of the most serious challenges is the increasing security risk.[2,3] In practice, plenty of IoT devices are physically unprotected and easily accessible to attackers, so the IoT could also become the internet of new things to be hacked. A vast number of IoT devices are suffering from security threats and malicious attacks every year.[4] Counterfeited or tampered devices such as the sensors or cameras will cause privacy leaks, property losses, and even life-threatening. For example, automated vehicles connected in the IoT might be hijacked by hackers and cause traffic accidents. As a result, trusted security policies are urgently needed, such as unique identifiers for devices, credible mutual authentication and data encryption transmission between devices and the cloud.[5–7] Different from the internet, there are a large number of sensing devices and physical nodes in IoT, so it is far from enough with only the software encryption.[8–10] Hardware-based security primitive is another essential and powerful way to protect IoT devices from various attacks. Radio frequency identification (RFID), QR codes, biometric identification, application-specific integrated circuits (ASICs) and so on are the common used hardware security strategies for tracking, authentication, and encryption in IoT.[11–14]

“The increasing security threat is a serious challenge to the internet of things (IoT). Hardware-based security primitive is an essential and powerful way to protect IoT devices from various attacks. But most of the current security hardwares are based on macrophysical features, which are usually produced by reproducible deterministic processes and can be copied by counterfeiters. Herein, a physical unclonable function (PUF) with high robustness based on the intrinsic random micro-/nanostructures of the electronic packages is proposed thereby demonstrating a low-cost and label-free hardware security solution for IoT. Using the unique surface micropattern and the spatially coded laser scattering, the proposed PUFs can be used as anticounterfeiting labels, authentication tokens and cryptographic key generators. With the help of the proposed PUFs, the safety protection is still effective even when the attacker is able to get access to the database because the secret keys are inherently hidden in the complex microscopic stochastic physical features of the PUFs but not the database. The proposed package-enabled PUFs provide a promising and practical physical protection solution for IoT security.”
based on macrophysical features, which are usually produced using reproducible deterministic processes and can be copied by counterfeiters. Especially, for the situation that terminal devices are exposed and can be physically accessed by the attackers, the clonable security hardwares remain the security vulnerabilities.

Physically unclonable functions (PUFs) exploit the inherently stochastic physical features at the microscopic level as one-way physical functions, which are easy to fabricate but practically impossible to replicate even by the original manufacturers. PUFs possess a lot of attractive properties such as uniqueness, unclonability, unpredictability, tamper evidence, and so on, making them the perfect candidates for unbreakable security hardwares. Private keys of the PUFs are inherently hidden in the complex microscopic stochastic physical features, which can be generated only at the time of the right physical stimuli or challenges. In other words, there is no need to digitally store the secret key in nonvolatile memory and the secret keys can be obtained from the PUFs in real time only when needed.

Therefore, PUFs are innate immune from cyber attacks such as cloning and tampering, and have recently aroused widespread concern and sparked intense research interest for IoT security applications including authentication, key exchange, secure communication. So far, most of the PUFs used in IoT are electronic PUFs (static random access memory (SRAM) PUFs, Arbiter PUF, Ring Oscillator PUF, field-programmable gate array (FPGA) PUFs, etc.), which are compatible with the IoT electronic devices very well. However, additional circuit chips are usually needed to construct the electronic PUFs. In addition, most of the electronic PUFs are compromised when facing machine learning-based modeling attacks. Optical and photonic PUFs are proved to be hardened against machine learning attacks and reverse engineering due to the inherently stochastic nature and the unpredictability of extremely complex input-output of their architectures. Microparticles, nanoparticles, porous microstructure, and chaotic microcavity have been used to construct optical and photonic PUFs, which can be further stimulated by quantum light to improve security. But all these PUFs still need additional labels when used in IoT and the compatibility with IoT devices should be considered.

Here, intrinsic random micro-/nanostructures of the electronic packages are exploited as optical and photonic PUFs, providing a low-cost and label-free hardware security solution for IoT. The PUFs are automatic generated during the production process of the electronic packages without intentional and additional circuit chips or optical chips. The proposed PUFs are proved to be multifunctional security primitives for IoT, including unique anti-counterfeiting labels, authentication token, as well as random number generator for encryption. Using the unique surface micropatterns, the package-enabled PUFs can be read out by a smartphone with a portable microscope handily and used as anticounterfeiting labels, authentication token. Further, when stimulated by spatially coded laser, the package-enabled PUFs can work as strong photonic PUFs and show comparable coding capacity with nanoparticles PUFs, which can be used as one-time pad authentication tokens and cryptographic key generators.

2. Results and Discussion

2.1. Intrinsic Random Surface of the Electronic Packages as Optical PUFs

Electronic package is an indispensable component for all kinds of electronic devices. Ceramic, metal, and plastic are the most used electronic package materials. It is common that most of the electronic packages have rough surfaces, which is derived from the intrinsic stochastic manufacturing processes. For example, the ceramic packages are usually made by pressing and sintering finely powdered materials such as aluminum oxide and aluminum nitride, thus random micro-/nanostructures are formed naturally. As for the metal and plastic packages, random micro-/nanostructures can also form naturally during the machine shaping process. Figure 1a–c shows a typical ceramic packaged system on chip (SOC) and the corresponding light-field and dark-field microscopy images of the package surface. The micrographs show complex irregular patterns, indicating that the packages can work as PUFs well. The morphology of the ceramic package was observed by scanning electron microscope (SEM), as shown in Figure 1g. The ceramic grains show different sizes from hundreds of nanometers to several micrometers and the average grain diameter is about 1.5 μm as shown in the statistical distribution in Figure 1i. A typical metal packaged chip and the corresponding light-field and dark-field microscopy images are also shown in Figure 1d–f. The surface of the metal package shows intricate and fine structures, as shown in Figure 1h, resulting in a gorgeous irregular pattern with various colors in the dark field of the optical microscope, which comes from the plasmonic scattering of the nanosized sharp metal protruberance. Many tiny feature points with the size of the diffraction limit can be found in the micrographs of the metal package. Both the ceramic and metal packages possess high stability and reliability, proving a practical solution to construct high robustness PUFs.

To read out the surface micropatterns of the package-enabled PUFs rapidly and handily, a table microscope equipped with a conveyor as well as a smartphone equipped with a portable microscope are proposed to register and authenticate the PUFs. The workflow for registering and authenticating a PUF is shown in Figure 2. Mass produced electron devices are transferred to the table microscope via the conveyor one by one to implement the batch intelligent registration and establish a traceable unique identity. Micrographs at several fixed positions of the package surface are recorded by the microscope and stored in the database. Then, when these registered electron devices are integrated into IoT devices such as floor mopping robot, intelligent refrigerator, web cameras, and so on, the IoT devices will possess the PUFs automatically. As for the IoT users, smartphone equipped with a portable microscope can be used to read out the PUFs and compared with the registered micrographs in the database to verify the identity of an IoT device.

To describe the identification capability of the PUFs quantitatively, the similarity and normalized Hamming distance of the ceramic and metal package-enabled PUFs were statistically estimated by comparing the microscopy images through feature matching algorithm and Gabor transform, respectively. Each microscopy images is about 3.0 Mbit and the corresponding
Figure 1. Micrographs and morphology of the package-enabled PUFs. a–c) Photograph, light-field and dark-field microscopy images of the ceramic package-enabled PUFs. d–f) Photograph, light-field, and dark-field microscopy images of the metal package-enabled PUFs. g,h) SEM image of the ceramic and metal packages surfaces. i) Statistical distribution of the diameter of the particles on ceramic package surface.

Figure 2. The batch intelligent registration workflow by a table microscope and handy authentication scheme based on smartphone equipped with a portable microscope.
The binary string after Gobar transformation is 1.5 Mbit. The normalized Hamming distance of two images is calculated by comparing the difference between their corresponding binary strings. We defined the statistical results of 100 different PUFs as intersimilarity and inter-Hamming distance while 100 times repeat measurements of the same PUF as intrasimilarity and intra-Hamming distance. The PUFs were read out by a table microscope at high magnifications and a smartphone equipped with a portable microscope at low magnifications, respectively. The corresponding statistical similarity are shown in Figure 3a–d, separately. All of the intersimilarity show lognormal distributions, whereas the intrasimilarity show normal distributions except for the intrasimilarity of the metal package-enabled PUFs read out by the table microscope. This might be due to the diffraction-limited feature points on the metal package surface captured by the table microscope at high magnifications are

![Figure 3](https://www.advancedsciencenews.com/)

**Figure 3.** The similarity and Hamming distance of the package-enabled PUFs. a,b) The similarity of the ceramic package-enabled PUF read out with a table microscope and a portable microscope, respectively. c,d) The similarity of metal package-enabled PUF read out with a table microscope and a portable microscope, respectively. e,f) Hamming distance of the ceramic and metal package-enabled PUFs read out with a table microscope and a portable microscope, respectively.
easily interfered and drifted under the environment vibration. From the overlap area of the fitted intersimilarity and intrasimilarity distributions curves, the false acceptance rate (FAR) and the false rejection rate (FRR) of the PUFs can be deduced. The insets of Figure 3a,b show that the FAR of the ceramic package-enabled PUFs are \(6.2 \times 10^{-6}\) and \(8 \times 10^{-8}\) when reading out by the table microscope and portable microscope, respectively, whereas the FRR are \(1 \times 10^{-7}\) and \(9.7 \times 10^{-10}\), respectively. The results demonstrate that PUFs readout system with the smartphone equipped with a portable microscope can obtain a comparable even better recognition performance than a table microscope with regard to the ceramic package-enabled PUFs. It is known that the variances of the inter-Hamming distance distribution represent the coding capacity of the PUFs,[40] so the statistic distribution of the Hamming distances of 100 different ceramic and metal package-enabled PUFs are measured, as shown in Figure 3e,f. The results show that the variances of the inter-Hamming distances of the ceramic package-enabled PUFs are \(1.8 \times 10^{-5}\) when reading out with the table microscope, equivalent to \(0.5(1-0.5)/(1.8 \times 10^{-7}) \approx 13.889\) independent variables. It means the PUFs can provide a theoretical key space size on the order of \(2^{13.889}\) distinguishable keys. The variances are slightly larger when reading out with the portable microscope for both the ceramic package and metal package-enabled PUFs. Therefore, the PUFs readout system with the smartphone equipped with a portable microscope can also obtain a comparable coding capacity compared with the table microscope. As a result, the smartphone equipped with a portable microscope is a good and handy readout system for the package-enabled PUFs, which is a preferred choice for practical IoT applications.

### 2.2. Advanced Photonic Strong PUFs Stimulated by a Spatially Coded Laser

It works as a weak PUF when just surface pattern is used as above since the challenge-response pairs (CPRs) are limited. The random micro-/nanostructures on the electronic packages can also be used as strong PUFs to generate a tremendous amount of CPRs when stimulated by a spatially coded laser. As shown in Figure 4a, spatial phase-coded laser wavefront modulated by a silicon liquid crystal spatial light modulator (SLM) illuminates the PUFs, then the output scattering speckle was captured by a charge coupled device (CCD). In fact, the smartphone integrated with a 3D facial recognition module based on a tunable structured laser can be directly used as portable readout equipment, making it convenient to utilize the photonic PUFs for IoT, as shown in Figure 4b. A small piece of the photonic PUF with only one cubic centimeter contains more than a terabit of structural information because the response is sensitive to subwavelength structural and material fluctuation.[40] As a result, an astronomical number of mutually uncorrelated optical speckles can be obtained from a set of different SLM phase profile inputs, which can be used for random number and key. In this experiment, three types of photonic PUFs based on TiO\(_2\) nanoparticles, ceramic package and metal package were measured and compared. More than 100 different random spatial phase-coded laser wavefronts were injected on the PUFs and the output optical speckle patterns were filtered by Gabor transform to calculate the inter-Hamming distances. The PUFs were picked and placed repeatedly more than 100 times and the output optical speckle patterns were captured under the same spatial phase coded laser wavefront input to get the intra-Hamming distances. Figure 4c shows three different input spatial phase codes (challenges) and the corresponding output speckle patterns (responses). Figure 4d–f shows the measured statistic distribution of the intra- and inter-Hamming distances. The results show that the inter-Hamming distances variance of the three PUFs are similar, that means the coding capacity of the package-enabled PUFs is comparable with the nanoparticles PUFs under the same readout system. In contrast, the intra-Hamming distance of the TiO\(_2\) nanoparticles PUFs shows much broader distribution than the package-enabled PUFs, which means the package-enabled PUFs possess better robustness. This might be due to the greater sensitivity of the nanoparticles PUFs to the environmental perturbation. The broader distribution of the intra-Hamming distance of nanoparticles PUFs leads to a large overlap and therefore worse FRR and FAR compared with package-enabled PUFs. The ceramic package-enabled PUFs show the maximal coding capacity and the best FRR and FAR among the three kinds of PUFs. Figure 4e shows the variance of the Gaussian distribution is \(8.7 \times 10^{-6}\), equivalent to \(0.5(1-0.5)/8.7 \times 10^{-6} \approx 28735\) independent binomial trials. It means the ceramic package-enabled PUFs can provide a theoretical key space size on the order of \(2^{28735}\) distinguishable keys. The inset of Figure 4e shows that the crossover point between the normalized probability distribution of intra-Hamming distance and the inter-Hamming distance is \(10^{-80}\), which means that both the FAR and the FRR are less than \(10^{-80}\) when the PUFs are used for authentication and identification. The aforementioned results demonstrate that the package-enabled PUFs can provide massive distinguishable keys and almost zero FAR and FRR.

Hundreds of different speckle patterns generated from the package-enabled PUF were transformed into binary bits by Gabor transformation and then carried out random binary hashing procedure to get random number data with 100 Mbit in length.[41] The generated keys were tested the using the NIST random number evaluation test suite. Results of NIST statistical test suite are shown in Table 1. The test results show that bit sequences obtained by our method pass most of the tests of the NIST suite except the ApproximateEntropy and OverlappingTemplate. Therefore, the package-enabled PUF can be considered as an adequate random number generator.

### 2.3. IoT Security Scheme based on the Package-Enabled PUFs

Figure 5a,d shows two application scenarios of the IoT. The first scenario is IoT wide area network (WAN) in which the IoT devices are connected via the internet at long distances geographically. A service center for big data storage and management is needed to establish trust and link among IoT devices and nodes, all the communications and resources acquisition among IoT devices need to go through the service center. In this scenario, absolute safety of the service center should be guaranteed or the attackers might access to the IoT devices through the internet. The second scenario is IoT local area network (LAN) in which the IoT devices connected each other in a local and relatively
short range via wireline, local WIFI or Bluetooth but not the internet. This scenario is relatively common in smart home and intelligent factory, in which the attackers might access the IoT devices through the LAN but impossibly through the internet. Almost all of the IoT devices contain electronic components, hence package-enabled PUFs inherently exist in all kinds of IoT devices. Based on the package-enabled PUFs, we proposed three IoT security schemes for anticounterfeiting, authentication, and communication encryption. The first security scheme is mainly focused on anticounterfeiting and authentication, as shown in Figure 5b. In this scheme, the surface patterns of the PUFs are used as the unique identity (ID) for each IoT device. In the first WAN application scenario, a new IoT device should register by its package-enabled PUF at the service center to gain access to the IoT and establish traceable ID. When two IoT devices intend to establish communication, both of them should send their unique surface patterns to the service center to verified identity. As for the second LAN application scenarios, the unique ID should be stored in each IoT devices in LAN by the administrator to establish mutual authentication network. To avoid replay

Figure 4. Scheme and results of the package-enabled PUFs stimulated by spatially coded laser. a) Schematic illustrations of the readout optical pathway diagram and the work principle of strong photonic PUFs. Inset: SEM of the TiO2 nanoparticles PUFs. b) Ideal drawing of the portable readout equipment with smartphone integrated with tunable structured laser and complementary metal oxide semiconductor (CMOS). c) Typical input spatial phase codes (challenges) and the corresponding output speckle patterns (responses) recorded by CCD. d–f) The normalized Hamming distances measured from 100 output speckle patterns of TiO2 nanoparticles PUFs, ceramic package, and metal package PUFs, respectively. The inset shows the fitting curves of intra- and inter-Hamming distance.
attack, a secure channel should be established between the service center and IoT devices in WAN and among the IoT devices in LAN. The second scheme is based on the photonic strong PUFs and applicable for both authentication and communication encryption, as shown in Figure 5c. The photonic PUFs can produce a great number of keys, so one-time-pad protocol can be used for both authentication and communication encryption.\cite{42} The CPRs should be registered and stored aforesaid in the service center for WAN and each IoT devices for LAN. This scheme is immune to replay attack, so the ID or ciphertext can be sent through public channels. The third scheme is also based on the photonic strong PUFs and applicable for both mutual authentication and communication encryption, as shown in Figure 5e. Different from the second scheme, during the registration and secret sharing phase, IoT device 1 (contain package-enabled PUF 1) and device 2 (contain package-enabled PUF 2) establish a connection in a security center or through a secure channel, then both of them produce a series of responses, i.e., private keys $K_1(A_i)$ and $K_2(B_i)$, respectively. After that, a digital XOR operator between $K_1(A_i)$ and $K_2(B_i)$ is carried out to produce public key $K_1(A_i)\oplus K_2(B_i)$ ($1 \leq i \leq n$). Only the public keys database are saved

### Table 1. Results of NIST statistical test suite.

| Test                   | P-value       | Proportion (%) |
|------------------------|---------------|----------------|
| BlockFrequency         | 0.108791      | 98             |
| CumulativeSums         | 0.282482      | 98             |
| ApproximateEntropy     | 0.000000      | 86             |
| FFT                    | 0.314124      | 99             |
| Frequency              | 0.244218      | 97             |
| LinearComplexity       | 0.699313      | 97             |
| LongestRun             | 0.534146      | 98             |
| NonOverlappingTemplate | 0.657933      | 100            |
| OverlappingTemplate    | 0.000017      | 95             |
| RandomExcursions       | 0.122325      | 100            |
| RandomExcursionsVariant| 0.066882      | 100            |
| Rank                   | 0.759756      | 98             |
| Runs                   | 0.145451      | 96             |
| Serial                 | 0.113587      | 99             |
| Universal              | 0.851383      | 99             |

**Figure 5.** Schematic illustrations of the IoT security scheme based on the package-enabled PUFs. a) The IoT WAN application scenarios based on center server and internet. b) The first security scheme for IoT based on the package-enabled optical PUFs. c) The second security scheme for IoT based on the package-enabled photonic strong PUFs. d) The IoT LAN application scenarios for smart home or intelligent factory. e) The third security scheme for IoT based on the package-enabled photonic strong PUFs.
locally on the IoT device and the service center without any sacrifice to security whereas the private keys do not need to be stored digitally. Private keys are inherently hidden in the complex microscopic stochastic physical features of PUFs and can be generated only when needed. IoT device 1 sends a ciphertext encrypted by the private key $K_i(A_i)$ generated in real time through public channels. In the authentication and decoding phase, IoT device 2 also produce a private key $K_i(B_i)$ in real time to derive the private key $K_i(A_i)$ from public key $K_i(A_i) K_i(B_i)$. In this way, both mutual authentication and encryption communication between IoT device 1 and IoT device 2 can work through a public channel. The safety protection is still effective even when the attacker is able to get access to the database because there is no private key stored digitally. A node can access the channel or decode only when it holds a right PUF entity, providing a powerful physical protection solution.

3. Conclusion

Intrinsic random optical features generated by unique surface patterns and laser scattering of the electronic packages are proposed as PUFs for versatile safety protection in IoT. We demonstrate that when the unique surface patterns are used as anti-counterfeiting labels or authentication tokens, the package-enabled PUFs can be read out by a smartphone with a portable microscope handy, providing a lightweight readout way for IoT applications. When stimulated by a spatially coded laser, the package-enabled PUFs can work as strong PUFs to generate a tremendous amount of CPRs. The experimental results prove that the package-enabled PUFs can provide massive distinguishable keys and almost zero FAR and FRR. Three IoT security schemes for anti-counterfeiting, authentication, and communication encryption are proposed based on the package-enabled PUFs, which are suitable for both LAN and WAN IoT applications. It demonstrates that the safety protection is still effective even when the attacker is able to get access to the database because the secret keys are inherently hidden in the complex microscopic stochastic physical features of PUFs and can be generated from the PUFs only when needed. As a result, the proposed package-enabled PUFs provide a low-cost, ubiquitous, practical, and powerful hardware security solution for IoT.

4. Experimental Section

**Sample Fabrication**: The package chips used as PUFs were the commercial ceramic-metal packages. Photonic PUFs based on TiO$_2$ nanoparticles were fabricated as a control group. TiO$_2$ nanoparticles with diameter of 200 ± 100 nm were spray-painted on a glass slide with thickness of 0.2 mm.

**Measurements Setup**: The morphology of the PUFs was characterized by the Nova Nano SEM 450 system. The micrographs of the PUFs were measured by either table optical microscope (Olympus MX51) with a CCD (2448 × 1920 pixels) and a 100× objective or a smartphone equipped with a 20× portable microscope (Tipscope). The scattering images of the PUFs were measured by a semiconductor laser (Lambda mini EVO 640 nm), an SLM (Hamamatsu X15223-01), and a CCD (Imavision, 2592 × 1944 pixels).

Acknowledgements

Q.L. and F.C. contributed equally to this work. The authors acknowledge the financial support from Science Challenging Project (no. T20218003) and National Natural Science Foundation of China (nos. 61875178 and U1831019). The authors also thank Dr. Gang Dai and Kun Liu for providing the ceramic-metal package chips, Mr. Binglei Zhang for his help in SEM measurement.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

Research data are not shared.

Keywords

authentication, encryption, internet of things, physical unclonable functions, securities

Received: July 14, 2021
Revised: September 25, 2021
Published online: December 16, 2021

[1] H. F. Atlam, R. Walters, G. Wills, *Int. J. Intell. Comput. Res. (IJICR)* 2018, 9, 928.
[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, *IEEE Access* 2019, 7, 82721.
[3] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, *Comput. Networks* 2015, 76, 146.
[4] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally, *Comput. Networks* 2020, 183, 107593.
[5] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma’at, I. Ahmedy, N. A. Ghani, S. Bhattacharyya, *IEEE Access* 2019, 7, 151054.
[6] Z. Yan, P. Zhang, A. V. Vasilakos, *J. Network Comput. Appl.* 2014, 42, 120.
[7] S. Challa, M. Wasid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, K. Y. Yoo, *IEEE Access* 2017, 5, 3028.
[8] V. Hassija, V. Chamola, V. Gupta, S. Jain, N. Guizani, *IEEE Internet Things J.* 2020, 8, 6222.
[9] T. Alladi, V. Chamola, *IEEE J. Sel. Areas Commun.* 2020, 39, 361.
[10] D. Arehrouij, J. Gutierrez, S. K. Ray, *J. Network Comput. Appl.* 2016, 66, 198.
[11] J. Dofe, J. Frey, Q. Yu, *IEEE Int. Symp. on Circuits and Systems (ISCAS)*, IEEE, Piscataway, NJ 2016, p. 2050.
[12] I. Butun, A. Sari, P. Osterberg, *Sensors* 2020, 20, 5729.
[13] M. Al-Asli, M. E. S. Elrabaa, M. Abu-Amara, *IEEE Internet Things J.* 2018, 6, 446.
[14] U. Chatterjee, R. S. Chakraborty, D. A. Mukhopadhyay, *ACM Trans. Embedded Comput. Syst. (TECS)* 2017, 16, 1.
[15] R. Arppe, T. J. Sørensen, *Nat. Rev. Chem.* 2017, 1, 0031.
[16] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Science 2002*, 297, 2026.
[17] Y. Gao, S. F. A. Sarawi, D. Abbott, *Nat. Electron.* 2020, 3, 81.
[18] C. Herder, M. D. Yu, F. Koushanfar, S. Devadas, *Proc. IEEE* 2014, 102, 1126.
[19] Q. Li, F. Chen, J. Kang, J. Su, F. Huang, P. Wang, X. Yang, Y. Hou, *Adv. Funct. Mater.* 2021, 31, 2010537.
[20] A. F. Smith, P. Patton, S. E. Skrabalak, Adv. Funct. Mater. 2016, 26, 1315.
[21] W. A. G. Rojas, J. J. Mc Morrow, M. L. Geier, Q. Tang, C. H. Kim, T. J. Marks, M. C. Hersam, Nano Lett. 2017, 17, 4976.
[22] Z. Hu, J. M. M. L. Comeras, H. Park, J. Tang, A. Afzali, G. S. Tulevski, J. B. Hannon, M. Liehr, S. Han, Nat. Nanotechnol. 2016, 11, 559.
[23] R. Arppe-Tabbara, M. Tabbara, T. J. Sørensen, ACS Appl. Mater. Interfaces 2019, 11, 6475.
[24] F. Chen, Q. Li, M. Li, F. Huang, H. Zhang, J. Kang, P. Wang, Chem. Eng. J. 2021, 411, 128350.
[25] M. N. Aman, K. C. Chua, B. Sikdar, IEEE Internet Things 2017, 4, 1327.
[26] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. S. Chakraborty, D. Mahata, M. M. Prabhu, IEEE Trans. Dependable Secure Comput. 2018, 16, 424.
[27] A. Babaei, Sensors 2019, 19, 3208.
[28] B. Chatterjee, D. Das, S. Maity, IEEE Internet Things J. 2018, 6, 388.
[29] F. Farha, H. Ning, K. Ali, L. Chen, C. Nugent, IEEE Internet Things J. 2020, 8, 5904.
[30] U. Rührmair, J. Solter, Design, Automation & Test in Europe Conf. & Exhibition (DATE), Dresden, Germany, March 2014.
[31] A. Vijayakumar, V. C. Patil, C. B. Prado, K. Sandip, IEEE International Symposium On Hardware Oriented Security And Trust (HOST), IEEE, Piscataway, NJ 2016, p. 19.
[32] F. Pavanello, I. O’Connor, U. Rührmair, C. F. Amy, S. Dimitris, IEEE European Test Symposium (ETS), IEEE, Piscataway, NJ 2021, p. 1.
[33] B. T. Bosworth, I. A. Atakhodjaev, M. R. Kossey, B. C. Grubel, D. S. Vresilovic, J. R. Stroud, N. Macfarlane, J. Villalba, N. Dehak, A. B. Cooper, M. A. Foster, A. C. Foster, APL Photonics 2020, 5, 010803.
[34] A. Fratalocchi, A. Fleming, C. Conti, A. D. Falco, Nanophotonics, 2021, 10, 457.
[35] B. C. Grubel, B. T. Bosworth, M. R. Kossey, A. B. Cooper, M. A. Foster, A. C. Foster, Opt. Express 2018, 26, 4710.
[36] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, R. J. Young, Appl. Phys. Rev. 2019, 6, 011303.
[37] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, P. W. H. Pinkse, Optica 2014, 1 421.
[38] H. Bay, A. Ess, T. Tuytelaars, G. L. Van, Comput. Vision Image Understanding 2008, 110, 346.
[39] D. Gabor, J. Inst. Electr. Eng. 1946, 93, 429.
[40] Q. Li, F. Chen, M. Li, H. Long, P. Sun, P. Wang, Y. Yao, J. Zhang, Opt. Quantum Electron. 2017, 49, 122.
[41] M. Akriotou, C. Mesaritakis, E. Grivas, C. Chaintoutis, A. Fragkos, D. Syvridis, Int. ISCIS Security Workshop. Springer, Cham, 2018, p. 28–37.
[42] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, C. Yang, Sci. Rep. 2013, 3, 3543.