Flexible and Wearable Encryption Primitive Based on Optical Physically Unclonable Functions

Min Seong Kim, Min Hyung Kang, Jun Soo Kim, Young Kyu Hong, and Gil Ju Lee

(Invited Paper)

***Abstract*—According to explosive and rapid development of flexible circuit technology, massive demand for wearable devices has arisen. Furthermore, wearable devices with integrated smartphones have contributed to a potential influence on online banking, digital healthcare service, and digital personal identification. This all-in-one device enables user to experience enhanced convenience; however, it also entails the inherent risk of cyber infiltration. A single successful hack into the device could endanger the security of user. Therefore, it is imperative to implement robust encryption and authentication mechanisms within wearable devices. Herein, we suggest a flexible and wearable encryption primitive based on an optical physically unclonable function which has a high capability of being embedded into a wearable device. Stochastic and unpredictable process-driven security concept, physically unclonable function (PUF) can operate as a solid identifier against online and offline intrusion. The physically unclonable tag consists of screen-printed Ag on the polyimide. The micro-scaled morphological characteristics of Ag-paste tag (APT) diverge as the fabrication step is repeated. In terms of PUF appliance potential (i.e., uniformity, reproducibility, uniqueness, and randomness) and real-case demonstration results (i.e., sensor-attached and smartphone-integrated operation) manifest that the APT functions as a strong encryption system embedded in a wearable device.**

***Index Terms*—Ag paste tag, flexible device encryption primitive, optical PUF, screen-printing.**

Manuscript received 31 July 2023; revised 4 October 2023 and 15 December 2023; accepted 16 December 2023. Date of publication 20 December 2023; date of current version 2 January 2024. This work was supported in part by the Korea Evaluation Institute of Industrial Technology (KEIT) grant funded by the Korea Government MOTIE, under Grant RS-2022-00154781, Development of large-area wafer-level flexible/stretchable hybrid sensor platform technology for formfactor-free highly integrated convergence sensor, in part by the National Research Foundation of Korea NRF under Grant RS-2023-00217312, Development of Core Technology for Integrated W-band Photonic Radar System, and in part by the Institute of Information and Communications Technology Planning and Evaluation IITP under Grant RS-2023-00233416, Development of ultra-efficient outdoor display with zero-cooling/zero-light pollution based on AI learning. *(Min Seong Kim and Min Hyung Kang contributed equally to this work.) (Corresponding authors: Young Kyu Hong; Gil Ju Lee.)*

Min Seong Kim, Jun Soo Kim, and Gil Ju Lee are with the Department of the Electronics engineering, Pusan National University, Busan 46241, South Korea (e-mail: rlaeksrhf@pusan.ac.kr; wnstn2047@pusan.ac.kr; gjlee0414@pusan.ac.kr).

Min Hyung Kang and Young Kyu Hong are with the Smart Electronics Research Center, Korea Electronics Technology Institute, Jeonju-si 54853, South Korea (e-mail: mhkang@keti.re.kr; ykhong@keti.re.kr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSTQE.2023.3345178.

Digital Object Identifier 10.1109/JSTQE.2023.3345178

I. Introduction

WEARABLE devices are becoming increasingly popular due to their high compatibility with the human body. These devices are equipped with fitness trackers that can monitor a range of biometric signals (e.g., heart rate, blood pressure, and oxygen levels) [1], [2], [3], [4] and store personal identification data (e.g., personal information and credit card information) [5], [6], [7]. Also, wearable devices can function as a key for a digital door lock [8], [9] or serve a mobile banking platform [10], [11]. These multifunctional devices make users more convenient but also involve the risk of leaking personal information. Recently, breaches into healthcare data have incurred significant economic losses and affected device consumers [12], [13]. To address these social issues, researchers have reported various efforts to develop a reliable encryption system, such as a random number generator (RNG) [14], [15], [16], quantum key distribution (QKD) [17], [18], [19], and artificial intelligence (AI) [20], [21], [22]. Above all, the hardware-type encryption principle, physically unclonable functions (PUFs), can act as a durable and robust identifier against intrusion by preventing the copying of the unique key [23], [24], [25], [26]. All PUFs have a bijective input-output pair, which is equivalent to a challenge-response pair (CRP) [27], [28]. What sets PUFs apart from other security concepts is their uniqueness, which arises from micro or nanoscale stochastic and unpredictable manufacturing processes. Consequently, PUFs operate independently of any specific procedural logic, making the system algorithm-free. Repeating the same fabrication process leads to dissimilar micro/nano-scaled geometrical feature of the identifier (e.g., electronic device fabrication, powder dispersion, and self-assembled layers) [29], [30], [31], [32], [33], [34].

These black-box like characteristics which converted to electric/magnetic signal, or optical image itself can be utilized for the "physically unclonable" fundamental [35], [36], [37], [38]. Bulky devices like smart watch can serve sufficient electrical power to record the unique electrical signal for electrical PUF as active element form. In contrast, for skin-laminated wearable devices, a compact readout system is necessary due to the need for minimal power consumption in the overall device. Considering this limitation, one effective method to establish a PUF system is by employing optical phenomena – an optical PUF, where a light sensor detects the transmitted or reflected light from the optical tag. Light emitted from the source (probing part) reaches the

optical token and resulting pattern received on the readout part (e.g., multiple scattered, reflected, or objected speckle) becomes the random key. The optical tag and the probe-readout part can be physically separated in this system (i.e., need not be accompanied or synchronized). Therefore, this fundamental aspect of a "passive PUF" is suitable for skin-laminated device owing to its independence from power consumption. However, despite the simplicity of the probe-and-readout procedure in optical PUF and the advantage of a passive PUF, several challenges still exist, such as a complex optic system and an additional tag production step.

Herein, we suggest the encryption primitive that utilizes screen-printed Ag-paste on a flexible and wearable device. The metal embedded in the device can function as both an electrode and an optical token. The cost-friendly process of screen-printing with reasonable critical dimensions not only facilitates metallic patterning over a large area but also supports low power consumption due to its high-resolution characteristic. Additionally, no subsequent manufacturing process is required for the initially printed Ag-paste, except low-temperature curing. During the printing through the mesh-like screen mask and the hardening of the Ag ink, micro-scaled morphological divergence occurs in metallic structures. Implicit microscopic scale deviation from the same procedure induces a dissimilar response. The performance of the Ag-paste tag (APT) as a PUF tag has been successfully verified by evaluating bit uniformity, normalized Hamming distances, and NIST 800-22 test suite. We demonstrated using a real-case imitated sensor-equipped flexible circuit to highlight our encryption primitive, recording gravitational acceleration, angular velocity, and temperature. Additionally, smartphone-integrated APT tagging showcases a compact portable probe-readout integrated as part of the optical PUF.

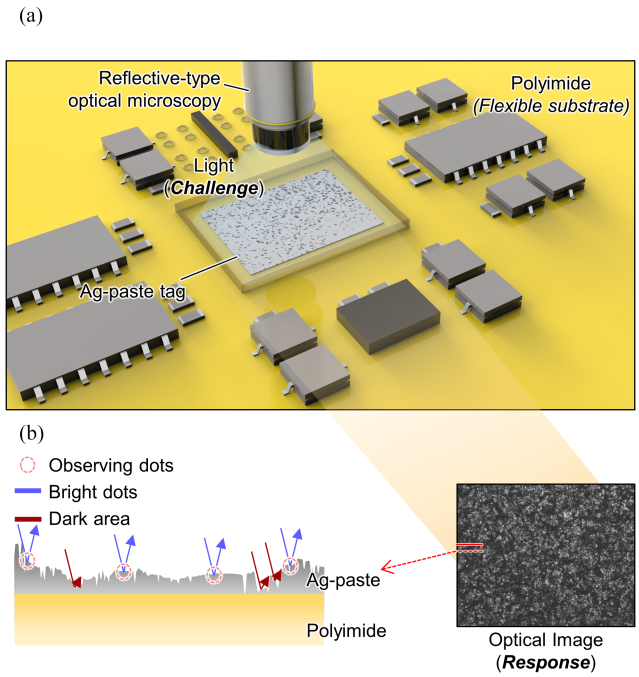

Fig. 1. Flexible and wearable encryption primitive. (a) Schematic of Ag-paste tag on flexible and wearable device. The light (challenge) reflects on Ag-paste tag becomes the optical image (response) by observing with the reflective-type microscopic image. The Ag-paste tag has high compatibility for the polyimide, which is widespread material owing to its chemical and physical robustness. (b) In a reflective-type optical microscopy, hardened Ag reflects incident light towards the observing plane appearing as white dots in the image. Conversely, polyimide transmits the incident light, resulting in black backgrounds in the image.

II. Implanting Optical PUF in a Wearable Device

Fig. 1(a) illustrates the device schematic of APT for the PUF system. Optical microscopy (OM) captures optical images corresponding to randomly distributed Ag flake on the flexible substrate. The observed images serve as raw data for the response of the optical PUF system. Light, which corresponds to a challenge, from reflective-type optical microscopy is reflected on the surface of APT. The APT has groovy surface, relatively higher region can be observed as a white dots and lower region becomes dark area in an observed image, which corresponds to a response (Fig. 1(b)). Polyimide (PI), which identified as suitable for wearable devices [39], [40], is employed as the substrate for demonstrating the flexible and wearable optical PUF. Besides, the wearable device consists of a plenty of electronic components (e.g., near-field communications chip; NFC chip, Bluetooth module, and healthcare sensors) thus high integrated metal electrode deposition and low energy usage are required. The cost-effective and high-resolution screen-printing process is suitable for the wearable device. A microstructural analysis is performed to determine the minimum linewidth of the Ag-paste screen-printing. The large-scale fabrication and mass production potential of the Ag-paste tag is illustrated as shown in Fig. 2(a).

Each discrete printed circuit integrated with sensors is demonstrated for the flexible and wearable device encryption system. Fig. 2(b) shows a suggested application of the embedded APT in the wearable device. All devices have a physical identifier using the same fabrication procedure within the internal electronic circuit. Each device has a unique optical tag, therefore APT tag can be regarded as a digital fingerprint. Thus, the implanted APT can be regarded as a fingerprint of the device. Based on the microscopic image from this tag, the instantly extracted key is compared to the stored database according to authentication criteria. The encrypted bit sequence only originates from the physical identifier, therefore online back-tracking is obviously prevented due to this physical one-way characteristic.

III. Screen-Printing Process

Cost-effective screen-printing of Ag-paste enables large area fabrication and high-resolution printing of the metal electrode and optical tag. Fig. 3(a) illustrates the screen-printing process of Ag-paste. A squeegee presses the screen mask, which consists of a mesh-like polyester structure, square-shaped holes and pattern-engraved metal foil covering the polyester mesh. The minimum printed dot size depends on the mesh wire diameter and hole size (i.e., opening), which are normally determined by mesh counts. The deposited Ag ink, during the squeegee-pressing procedure, transforms into the following carved pattern onto a screen mask.

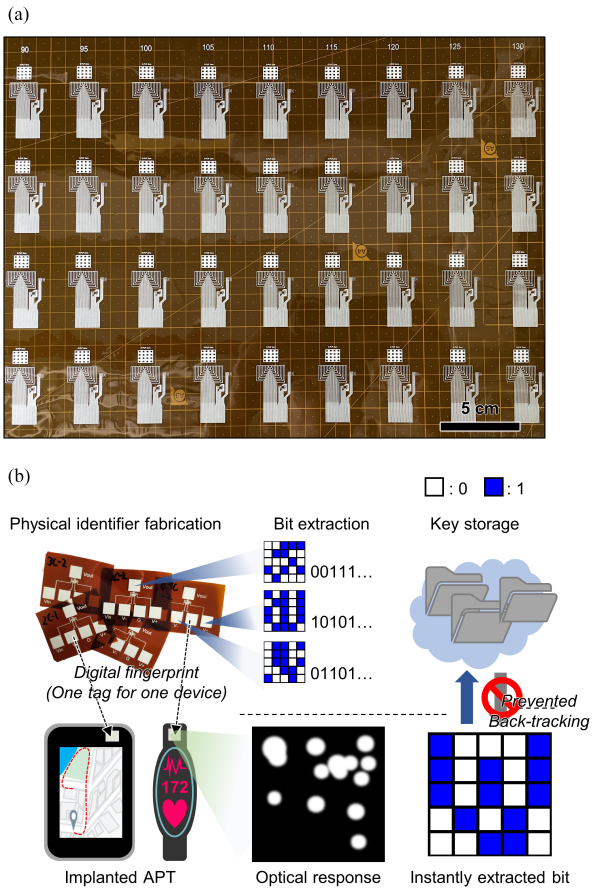

Fig. 2. Fabrication and application of Ag-paste tag. (a) Large area fabrication potential of the Ag-paste screen-printing process. (b) Application of the wearable encryption primitive. Manufactured physical identifier (*i.e.*, Ag-paste tag) is implanted into portable, and wearable devices while producing stage. Generated keys are stored in a cloud database which is prevented online back-tracking owing to physical one-way characteristic.

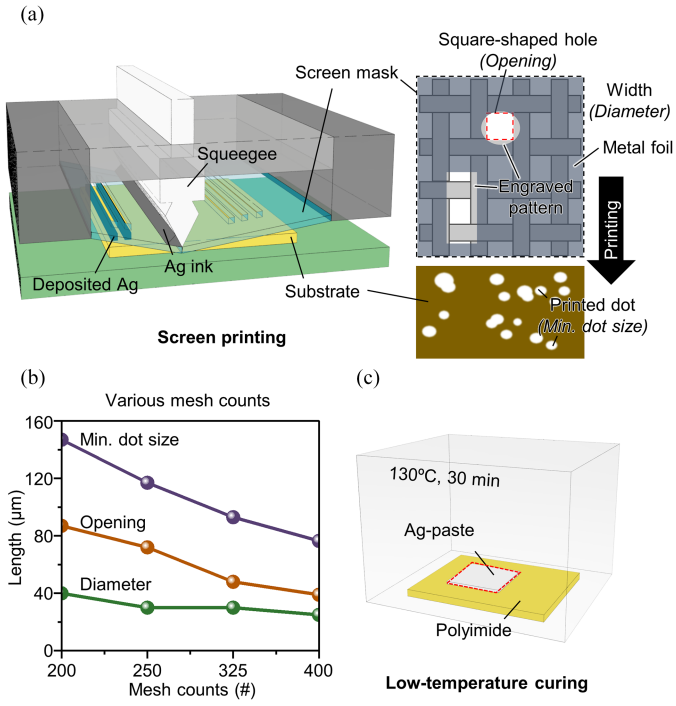

Fig. 3. Schematic of screen-printing process. (a) A squeegee presses the screen mask, liquid state Ag-ink infiltrate into the opening region of the screen mask. Included Ag flakes are dissipated and overlapped stochastically while pressed with a squeegee. (b) Variating dot size as changing mesh counts of screen mask. As mesh counts increases, minimum dot size and opening size reduces. This examination enables low-power consumption chip and smaller chip packaging. (c) Deposited Ag ink is low-temperature cured at oven, 130 °C for 30 minutes. During this process, self-coagulated Ag ink transforms to micro-sized Ag grain.

The Ag ink that passes through the opening of the mesh becomes a printed dot, and these dots overlap with each other stochastically. Additionally, the liquid state of ink contains Ag flakes with a diameter of around 5 μm; thus, these micro-scaled fragments disperse randomly throughout the printing procedure. Fig. 3(b) shows the opening, diameter, and minimum dot size for different mesh counts in screen-printing. Mesh counts over 250 are considered due to narrow linewidth (i.e., minimum dot size of 100 μm) suitable for small package chip designing. As mesh counts increases (i.e., higher resolution), dot size can reach near 100 μm. After screen-printing, the patterned Ag-paste needs thermal curing, therefore the sample is cured in an oven for 30 minutes at 130 °C (Fig. 3(c)). The uniqueness of the APT derives from three processes: 1) stochastically overlapping dots during screen-printing, 2) unpredictably dispersed Ag flake in a liquid state paste, and 3) non-deterministically solidifying under low-temperature curing. Thus, completely replicating the APT is significantly hindered by these three stages.

To consider performance of the metal electrode and optical token of the APT, the designed screen mask pattern is illustrated in Fig. 4. The designed gap between two electrodes varies

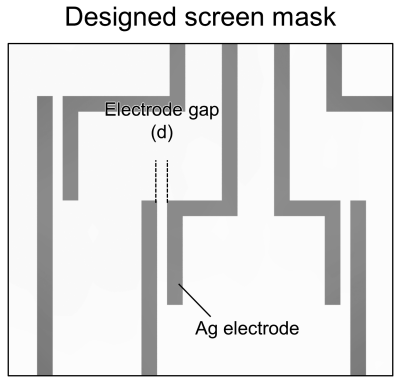

Fig. 4. Designed screen mask pattern to define critical dimension of screen-printing. Gap between two electrodes is varied for 100, 110 and 120 μm.

such as 100, 110, and 120 μm. Fig. 5 shows the 3D profiling measurement of the printed two electrodes. The electrode gap is 110 μm where the two electrodes contact each other. According to this microscopic analysis, measured critical dimension of the APT is 110 μm. Consequently, screen-printing is suitable for highly integrated electrode patterns for wearable devices and can operate as an unclonable tag. Moreover, microscopic deviations as changing mesh counts are depicted in Fig. 6(a). The mesh counts of printed APT is varied for 200, 250, 325

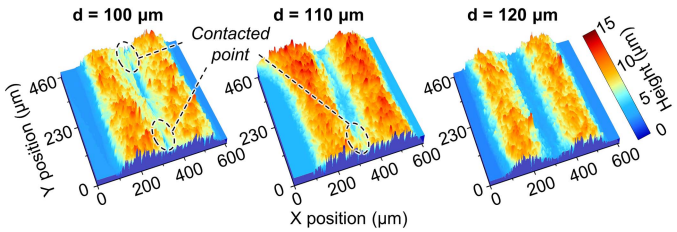

Fig. 5. 3D profiled result for each case of linewidth. Contacting region of two electrodes is observed at 110 μm, therefore the critical dimension of screen-printing is 110 μm.

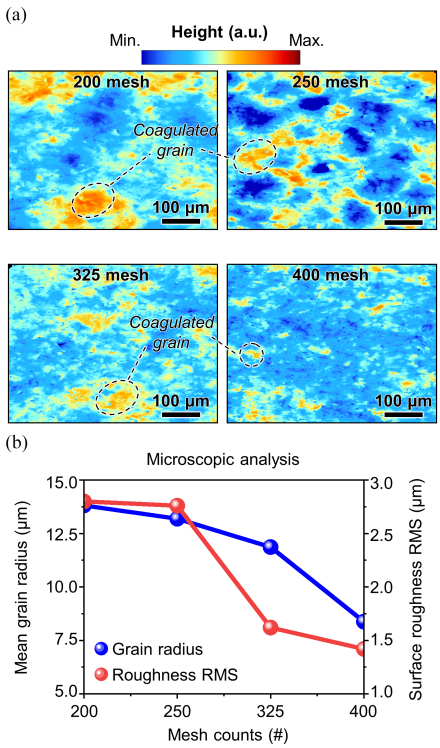

Fig. 6. 3D profiled contour map for different mesh counts. (a) Large number of the mesh in the screen mask enables high resolution printing, therefore smaller coagulated grain size is observed as adding the mesh counts. (b) Roughness rms and mean grain size analysis result for each mesh counts.

and 400. With increasing mesh counts for the screen mask, less Ag ink infiltrates onto PI substrate owing to the narrower mesh openings. A smaller grain size can enhance the resolution of the screen-printing of APT. Surface roughness and mean grain radius from the microscopic analyses are described in Fig. 6(b). More mesh counts lead to the formation of smaller grain sizes in the APT. Consequently, the surface roughness, quantified by the root mean square and average grain size, decreases with increasing mesh counts.

IV. Evaluation of APT-PUF Performance

Digitized keys from the APT exhibit biased characteristics, with varying numbers of 0s and 1s. The multipass tuple-output von Neumann extractor equalizes the number of 0s and 1s in each bit sequence [41]. Evaluating PUF performances, entire 106 generated bitstreams from 106 different tags are considered. Fig. 7 shows the representative 30 responses from 30 different APT-PUF. Bit uniformity, which is the degree of bias in the final bit sequence, is defined as the ratio of the number of '1's in a sequence (i.e., Hamming weight) to the length of the sequence. All bit sequences should ideally have the same '0's and '1's, aiming to minimize the probability of guessing valid bit sequence. This probability is defined as the reciprocal of the total number of possible bit sequence cases:

$$P = 1/{}_n\mathrm{C}_r = \frac{r! \times (n-r)!}{n!} \quad (\text{where } n\text{: length of sequence}, r\text{ : the number of '1's}) \qquad (1)$$

The captured image is resized to 256 $\times$ 256, binarized, and debiased by multipass tuple-output von Neumann extractor (Fig. 8(a)). Captured raw image shows relatively low bit uniformity, therefore the binarized images are debiased by a multipass tuple-output von Neumann extractor, instead of classic von Neumann debiasing [32]. The binary bitstream is sliced into two bits, and the same bit sequences (00 and 11), while different bit sequences (01 and 10) have only their first bit extracted. In pre-save bits, same bit slice 1111 and 0000 is discarded, resulting in a bit uniformity of 0.5 (Fig. 8(b)). The condition to minimize the value of P involves $n = 0.5r$, (i.e., ideal bit uniformity is 0.5). Fig. 9(a) illustrates the bit uniformity of the APT-PUF, indicating near-ideal value of 0.5. To determine whether two bits are same or not, normalized Hamming distance (normalized-HD) is evaluated. The number of positions at which corresponding elements in the two strings differ is defined by the Hamming distance. The normalization of this value is achieved by dividing it by the length of one sequence (i.e., 144 bits). Repeating the same bit extraction process for an identical challenge should result in the same response. Consequently, normalized-HD is evaluated for the responses generated from a single PUF; this is referred to as intra-device Hamming distance (intra-HD). 10 key extraction sequences for the same PUF are repeated for inducing intra-HD. To determine the distinctiveness of each response, normalized-HD derives from the comparing all different obtained response bits; inter-device Hamming distance (inter-HD). The intra-/inter-HD distribution of the APT-PUF is nearly ideal, indicating an intra-HD of 0 and an inter-HD of 0.5, respectively (Fig. 9(b)). From the Gaussian-fitted distribution of intra-/inter-HD, the point of intersection between the two distributions is defined as the authentication criterion (Fig. 9(c)). In the authentication stage, the instantly extracted response is compared to all database-stored responses to evaluate the normalized-HD. Smaller than the normalized-HD of 0.1589, which is a cutoff point of this criteria, is regarded as a valid response. All collected bits have successfully passed the all test suite of NIST 800-22, these test results highlight the randomness of APT-PUF (Fig. 9(d)). Each test is performed using 96 sequences of individual 159 bits from total collected 15264 (106 responses $\times$ 144 bits) bits. All sequences are found to be random surpassing the p-value of 0.0001 and proportion rate of 0.9583 (= 92/96).

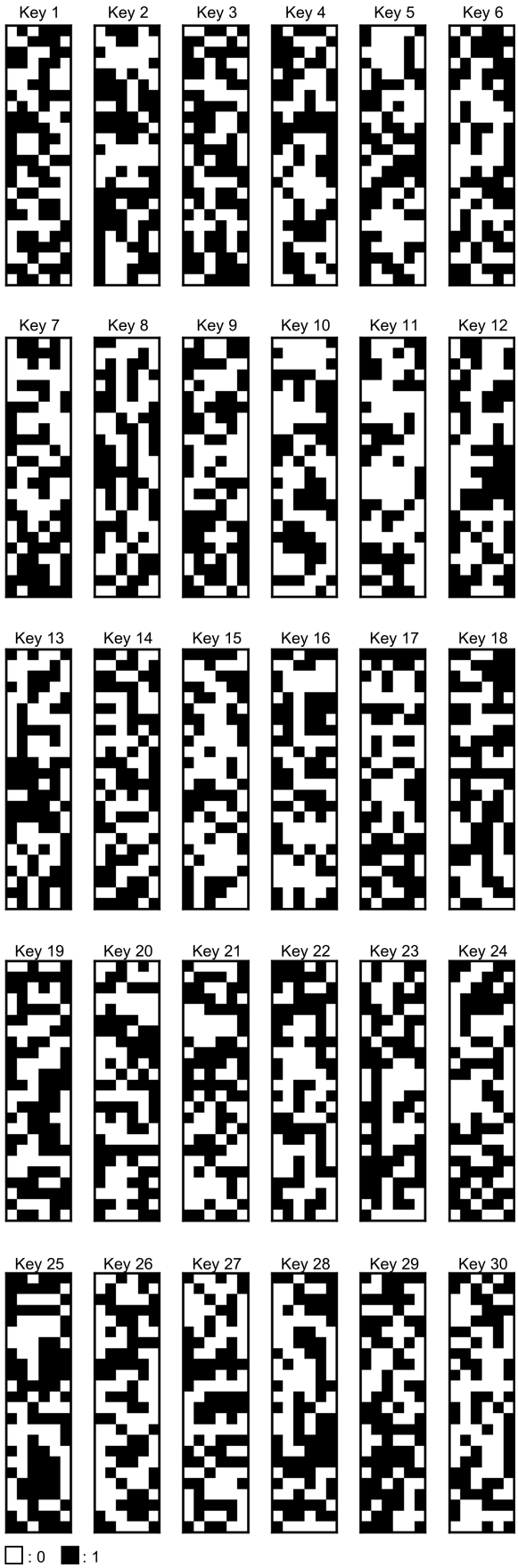

Fig. 7. Extracted 30 representative bit sequences from the 30 different APT-PUF. Each bit sequence consists of 144 bits.

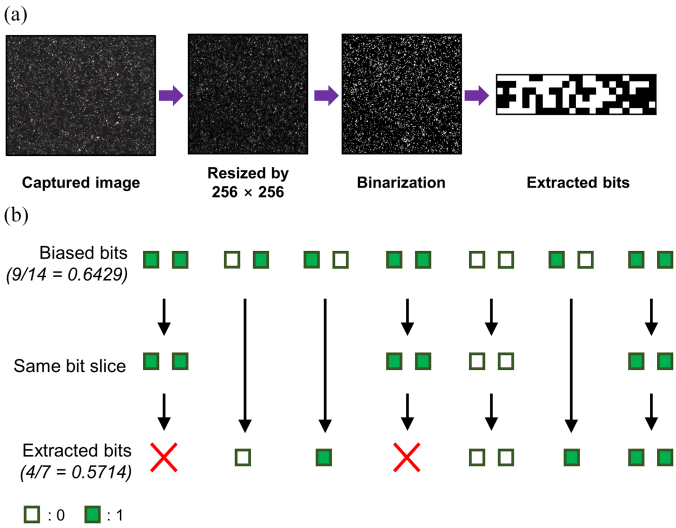

Fig. 8. Schematic of the key generation process and multipass tuple-output von Neumann extraction. (a) Captured image is resized by 256 × 256, binarized and debiased. (b) During the bit extraction process, same bit array is almost discarded, therefore the bit uniformity becomes 0.5.

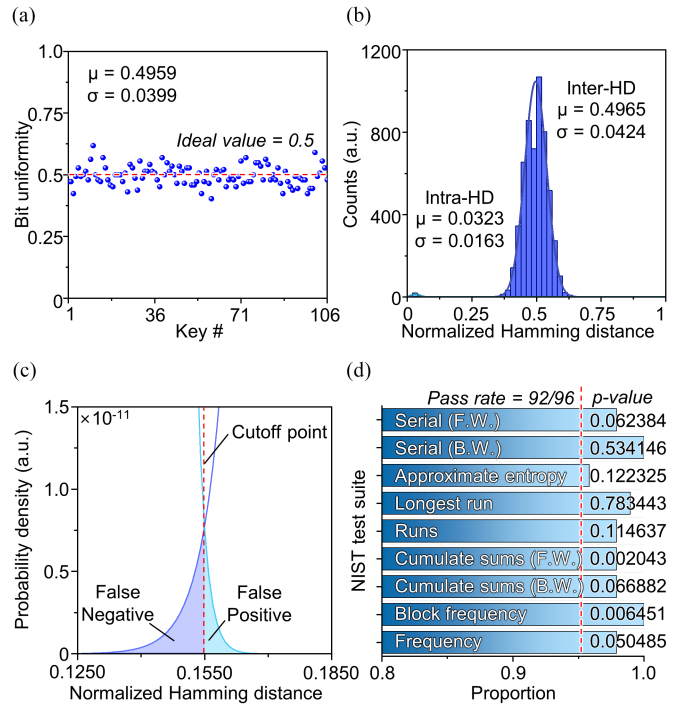

Fig. 9. Evaluated PUF performances. (a) Bit uniformity indicates near ideal value of ~0.5. (b) Normalized Hamming distances; intra-HD and inter-HD. Each criterion expresses the ideal PUF performance, intra-HD of 0.0323 and inter-HD of 0.4965. (c) Cutoff point for authentication mode for APT-PUF. Meeting point of Gaussian fitted intra-HD and inter-HD distribution is determined the cutoff Hamming distance. (d) NIST 800-22 test suite results. The minimum pass rate for each statistical test is 92 for a sample size of 96 binary sequences.

V. Demonstration of Flexible and Wearable Encryption Primitive

Due to high compatibility of the APT with the flexible substrate of PI, suggesting APT-PUF has a large potential of flexible circuit and wearable device. To demonstrate its applicability in flexible circuits and wearable devices, an APT device is

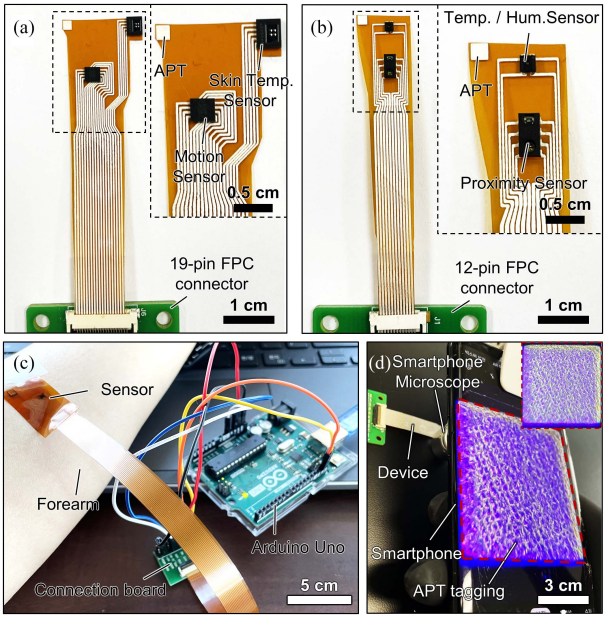

Fig. 10. Real-case demonstration for flexible and wearable encryption primitive. (a) Prepared circuit for evaluating skin temperature, gravitational acceleration, angular velocity (b) Temperature, relative humidity and proximity. Zoomed insets images highlight the configuration of each device. This sensor-equipped flexible device corresponds to the flexible and wearable device. (c) Experimental setup image to measure motion, body temperature and relative humidity attached to the forearm. (d) Image of tagging APT by a smartphone-combined with a microscopic lens.

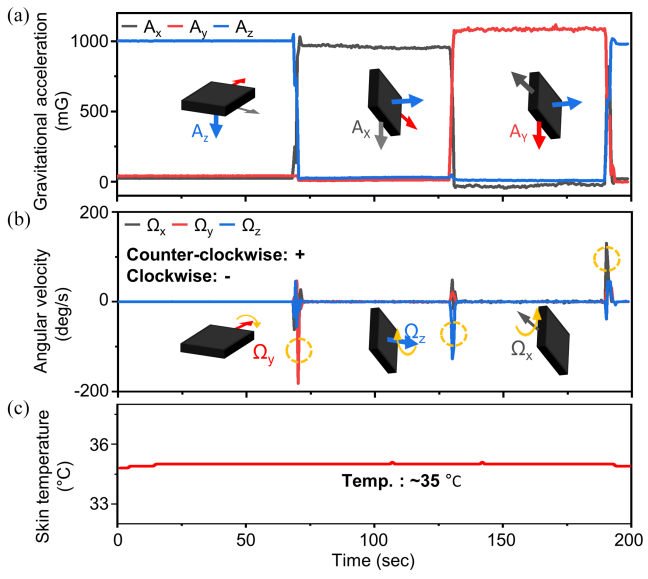

Fig. 11. Physical measurement while attached APT on circuit. (a) Gravitational acceleration data obtained from 6-axis motion sensor. (b) Angular velocity data obtained from 6-axis motion sensor. (c) Forearm skin temperature obtained from temperature sensor.

integrated with 6-axes motion sensor and a skin temperature sensor (Fig. 10(a)). Considering that wearable devices are in close proximity to the human skin most of the time, factors like proximity and humidity should also be considered (Fig. 10(b)). High-resolution printing enables a compact size for the flexible circuit. A real-case imitation of a wearable device measurement

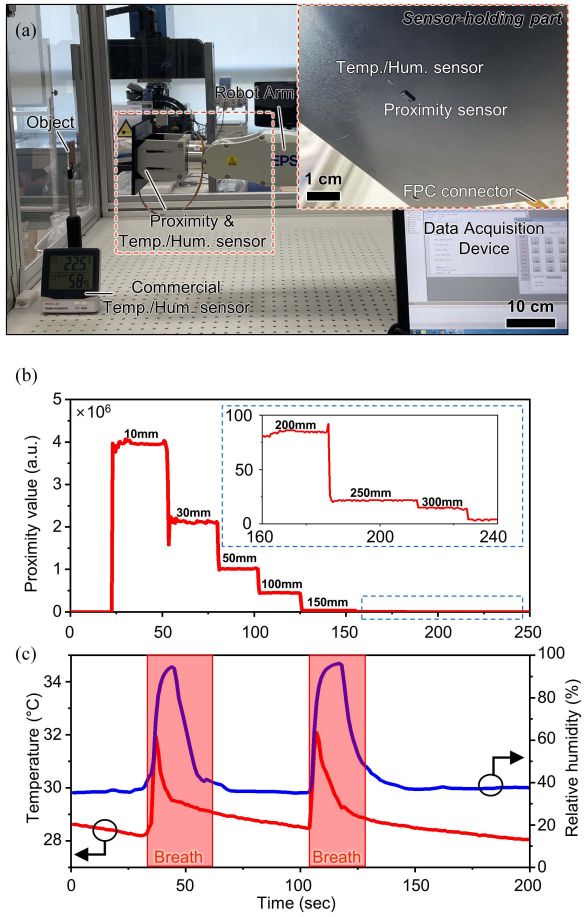

Fig. 12. Proximity and temperature data. (a) Proximity and humidity test setup with robot arm. Zoomed inset shows the sensor holding part of robot arm. (b) Obtained proximity value from proximity sensor according to the distance of 10, 30, 50, 100, 150, 200, 250 and 300 mm. (c) Changed temperature/humidity data obtained from the temperature/humidity sensor.

setup is illustrated at Fig. 10(c). Recorded data from the motion sensor and temperature sensor are logged using a 19-pin FPC (flexible printed circuit) connector and Arduino Uno. Fig. 9(d) illustrates the concept of a smartphone-integrated optical PUF system. The inset image is captured optical response from smartphone microscope. To define the active area of the APT, microscope-attached UV lamp can determine the working region. Owing to camera-attachable objective lens, a smartphone can serve the key generation process, make it applicable as a portable and compact readout component for optical PUF.

The wearable device undergoes external forces and adheres with human skin, external forces to the APT circuit are recorded with attached APT. A 6-axes motion sensor and a temperature sensor record the gravitational acceleration, angular velocity and forearm skin temperature of APT-embedded flexible circuit (Fig. 11(a)–(c)). To imitate a more accurate working condition of the skin-laminated device, a circuit equipped with proximity sensor and temperature/humidity sensor is demonstrated with robot arm (Fig. 12(a)). The distance between the sensor-holding part and fixed object is gradually reduced at 25-second intervals (Fig. 12(b)). The measured temperature and relative humidity represent the surrounding conditions of the real device, as shown

in Fig. 12(c). Based on these demonstration results, the proposed APT can function as an encryption primitive with wearable sensors in various environments.

VI. Conclusion

We propose a robust encryption primitive which can be embedded into flexible and wearable device by evaluating of PUF performance and demonstrating compatibility of human body. The optical response from APT based on the physical identifier, prevents online backtracking due to the bijective characteristic of the PUF. The screen-printing of APT offers a reasonable critical dimension, enabling large-scale production, and high entropic tag fabrication. A printing condition with a mesh count over 250 is chosen compact circuit and smaller chip packaging. Furthermore, the APT satisfies the requirements of optical PUF, estimating the bit uniformity (~ 0.4959), normalized Hamming distance (intra/inter-HD $\sim 0.0323/\sim 0.4965$) and NIST 800-22 test suite (pass rate over 92/96). Demonstrations that imitate real-case scenarios of a skin-laminated device, incorporating several sensors (i.e., temperature sensor, humidity sensor, and proximity sensor), smartphone-integrated optical PUF system, and an examination with a robot arm clearly express the potential for a lightweight optical PUF system and the robustness of APT against various external surroundings.

References

[1] Y. Guo et al., "A review of wearable and unobtrusive sensing technologies for chronic disease management," *Comput. Biol. Med.*, vol. 129, Feb. 2021, Art. no. 104163.

[2] G. Lee, Q. Wei, and Y. Zhu, "Emerging wearable sensors for plant health monitoring," *Adv. Funct. Mater.*, vol. 31, no. 52, Oct. 2021, Art. no. 2106475.

[3] M. N. Ul Hasan and I. I. Negulescu, "Wearable technology for baby monitoring: A review," *J. Textile Eng. Fashion Technol.*, vol. 6, no. 4, Jul. 2020, Art. no. 15406.

[4] A. Palumbo, P. Vizza, B. Calabrese, and N. Ielpo, "Biopotential signal monitoring systems in rehabilitation: A review," *Sensors*, vol. 21, no. 21, Oct. 2021, Art. no. 7172.

[5] J. Q. Cheng et al., "WatchID: Wearable device authentication via reprogrammable vibration," in *Proc. Int. Conf. Mobile Ubiquitous Syst.: Comput., Netw., Serv.*, 2022, pp. 813–833.

[6] L. Cilliers, "Wearable devices in healthcare: Privacy and information security issues," *Health Inf. Manage. J.*, vol. 49, no. 2/3, May 2019, Art. no. 183335831985168.

[7] W. Huifeng, S. N. Kadry, and E. D. Raj, "Continuous health monitoring of sportsperson using IoT devices based wearable technology," *Comput. Commun.*, vol. 160, pp. 588–595, Jul. 2020.

[8] M. Husni, H. T. Ciptaningtyas, R. R. Hariadi, I. A. Sabilla, and S. Arifiani, "Integrated smart door system in apartment room based on internet," *TELKOMNIKA (Telecommun. Comput. Electron. Control)*, vol. 17, no. 6, pp. 2747–2754, Dec. 2019.

[9] S. Seneviratne et al., "A survey of wearable devices and challenges," *IEEE Commun. Surveys Tut.*, vol. 19, no. 4, pp. 2573–2620, Fourthquarter 2017.

[10] S. Liu, W. Shao, T. Li, W. Xu, and L. Song, "Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey," *Digit. Signal Process.*, vol. 125, Jun. 2021, Art. no. 103120.

[11] A. Bianchi and I. Oakley, "Wearable authentication: Trends and opportunities," *Inf. Technol.*, vol. 58, no. 5, pp. 255–262, Jan. 2016.

[12] A. H. Seh et al., "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, May 2020, Art. no. 133.

[13] F. Schlackl, N. Link, and H. Hoehle, "Antecedents and consequences of data breaches: A systematic review," *Inf. Manage.*, vol. 59, no. 4, Jun. 2022, Art. no. 103638.

[14] R. Sivaraman, A. Sridevi, S. Rajagopalan, S. Janakiraman, and A. Rengarajan, "Design and analysis of ring oscillator influenced beat frequency detection for true random number generation on FPGA," in *Proc. IEEE Int. Conf. Comput. Commun. Inform.*, 2019, pp. 1–6.

[15] F. James and L. Moneta, "Review of high-quality random number generators," *Comput. Softw. Big Sci.*, vol. 4, pp. 1–12, Jan. 2020.

[16] K. Bhattacharjee and S. Das, "A search for good pseudo-random number generators: Survey and empirical studies," *Comput. Sci. Rev.*, vol. 45, Aug. 2022, Art. no. 100471.

[17] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, no. 1, Aug. 2017, Art. no. 30.

[18] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Des., Codes Cryptography*, vol. 78, no. 1, pp. 351–382, Dec. 2015.

[19] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions," *Opt. Exp.*, vol. 26, no. 18, Aug. 2018, Art. no. 24260.

[20] B. Li, Y. Feng, Z. Xiong, W. Yang, and G. Liu, "Research on AI security enhanced encryption algorithm of autonomous IoT systems," *Inf. Sci.*, vol. 575, pp. 379–398, Oct. 2021.

[21] D. Xu, G. Li, W. Xu, and C. Wei, "Design of artificial intelligence image encryption algorithm based on hyperchaos," *Ain Shams Eng. J.*, vol. 14, no. 3, Jul. 2022, Art. no. 101891.

[22] N. Garcia et al., "Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence," *J. Netw. Comput. Appl.*, vol. 173, Jan. 2021, Art. no. 102871.

[23] S. Lee, H. H. Kim, J. Seo, B. C. Jang, and H. Yoo, "Disordered mixture of self-assembled molecular functional groups on heterointerfaces with p-Si leads to multiple key generation in physical unclonable functions," *Amer. Chem. Soc. Appl. Mater. Interfaces*, vol. 15, no. 1, pp. 1693–1703, Dec. 2022.

[24] D. Zhong et al., "Twin physically unclonable functions based on aligned carbon nanotube arrays," *Nature Electron.*, vol. 5, no. 7, pp. 424–432, Jul. 2022.

[25] M. S. Kim et al., "Revisiting silk: A lens-free optical physical unclonable function," *Nature Commun.*, vol. 13, no. 1, Jan. 2022, Art. no. 247.

[26] N. Kayacı et al., "Organic light-emitting physically unclonable functions," *Adv. Funct. Mater.*, vol. 32, no. 14, pp. 2108675–2108675, Dec. 2021.

[27] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electron.*, vol. 3, no. 2, pp. 81–91, Feb. 2020, doi: 10.1038/s41928-020-0372-5.

[28] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Appl. Phys. Rev.*, vol. 6, no. 1, Mar. 2019, Art. no. 011303.

[29] Y. Hu et al., "Flexible and biocompatible physical unclonable function anti-counterfeiting label," *Adv. Funct. Mater.*, vol. 31, no. 34, Jun. 2021, Art. no. 2102108.

[30] J.-M. Yu et al., "A poly-crystalline silicon nanowire transistor with independently controlled double-gate for physically unclonable function by multi-states and self-destruction," *Adv. Electron. Mater.*, vol. 7, no. 5, pp. 2000989–2000989, Apr. 2021.

[31] J.-S. Jeong, G. S. Lee, T.-E. Park, K.-Y. Lee, and H. Ju, "Bio-inspired electronic fingerprint PUF device with single-walled carbon nanotube network surface mediated by M13 bacteriophage template," *Sci. Rep.*, vol. 12, no. 1, Nov. 2022, Art. no. 20096.

[32] M. S. Kim and G. J. Lee, "Visually hidden, self-assembled porous polymers for optical physically unclonable functions," *Amer. Chem. Soc. Appl. Mater. Interfaces*, vol. 15, no. 3, pp. 4477–4486, Jan. 2023.

[33] D.-Y. Kim et al., "Reconfigurable electronic physically unclonable functions based on organic thin-film transistors with multiscale polycrystalline entropy for highly secure cryptography primitives," *Adv. Funct. Mater.*, vol. 33, no. 11, pp. 2210367–2210367, Dec. 2022.

[34] J. H. Kim et al., "Nanoscale physical unclonable function labels based on block copolymer self-assembly," *Nature Electron.*, vol. 5, no. 7, pp. 433–442, Jul. 2022.

[35] Y. Kim et al., "Reconfigurable multilevel optical PUF by spatiotemporally programmed crystallization of supersaturated solution," *Adv. Mater.*, vol. 35, no. 22, Apr. 2023, Art. no. 2212294.

[36] R. Pappu, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[37] J. W. Leem et al., "Edible unclonable functions," *Nature Commun.*, vol. 11, no. 1, pp. 1–11, Jan. 2020.

[38] J.-W. Nam, J.-H. Ahn, and J.-P. Hong, "Compact SRAM-based PUF chip employing body voltage control technique," *IEEE Access*, vol. 10, pp. 22311–22319, 2022.

[39] W.-Y. Wu et al., "Wearable devices made of a wireless vertical-type light-emitting diode package on a flexible polyimide substrate with a conductive layer," *Amer. Chem. Soc. Appl. Electron. Mater.*, vol. 3, no. 2, pp. 979–987, Feb. 2021.
[40] M. H. Kang et al., "Outdoor-useable, wireless/battery-free patch-type tissue oximeter with radiative cooling," *Adv. Sci.*, vol. 8, no. 10, Mar. 2021, Art. no. 2004885.
[41] R. Maes et al., "Secure key generation from biased PUFs: Extended version," *J. Cryptographic Eng.*, vol. 6, no. 2, pp. 121–137, 2016.

Min Seong Kim was born in Busan, South Korea, in 1996. He received the B.S. degree in electronic engineering from Pukyoung National University, Busan, in 2021. He is currently working toward the M.S. degree in electronics engineering with Pusan National University, Busan. From 2016 to 2017, he was the Republic of Korea Marine Corps 2nd Division, Gimpo, Gyong-gi do. His research interests include the application for micro/nano-scaled photonic structure in visible light region. He has authored one research paper and coauthored another. He was the recipient of the PNU fellowship in 2022 and 2023.

Min Hyung Kang received the B.S. degree in electrical engineering from Kyungpook National University, Daegu, South Korea, in 2019, and the M.S. degree in electrical engineering and computer sciences from the Gwangju Institute of Science and Technology, Gwangju, South Korea, in 2021. From January to September 2021, he was a Senior Researcher with LG Display Company Ltd. Since 2021, he has been a Researcher with Smart Electronics Research Center, Korea Electronics Technology Institute. His research interests include the development of a sensor device and radio frequency module based on the printing process. He has an interest in optical simulation technology for illumination modules and optical lens design. He was the recipient of the Samsung Humantech Paper Award for Encouragement Award in 2021.

Jun Soo Kim was born in Busan, South Korea, in 2001. He is currently working toward the B.S. degree in electronics engineering with Pusan National University, Busan, South Korea.

Young Kyu Hong received the Ph.D. degree in physics from Jeonbuk National University, Jeonju, South Korea, in 2000. He was a Postdoctoral Fellow with the Korea Research Institute of Standards and Science, Daejeon, South Korea. Since 2009, he has been a Managerial Researcher with the Smart Electronics Research Center, Korea Electronics Technology Institute, Seongnam, South Korea. From 2018 to 2019, he was an Adjunct Professor with Jeonbuk National University, Jeonju, South Korea. His research interests include energy storage, switchable optical devices, and biosensors.

Gil Ju Lee received the B.S. degree in electronics engineering from Pusan National University, Busan, South Korea, in 2016, and the Ph.D. degree in electrical engineering and computer sciences from the Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, in 2021. From March to September 2021, he was a Postdoctoral Research Associate with the School of Electrical Engineering and Computer Science, GIST. He is currently an Assistant Professor with the Department of Electrical Engineering, Pusan National University. His research interests include multifunctional nanophotonics, energy-photonics, advanced optoelectronics, and optical security devices.