Bio-inspired electronic fingerprint PUF device with single-walled carbon nanotube network surface mediated by M13 bacteriophage template

Jae-Seung Jeong
Korea Institute of Science and Technology
Gyo Sub Lee
ASML Korea
Ki-Young Lee
Korea Institute of Science and Technology
Hyunsu Ju (hyunsuju@kist.re.kr)
Korea Institute of Science and Technology

Article

Keywords: Carbon nanotube network, Biological glue, Hydrodynamic assembly, Physical unclonable function, PUF, Hardware security

Posted Date: May 25th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1664139/v1

Bio-inspired electronic fingerprint PUF device with single-walled carbon nanotube network surface mediated by M13 bacteriophage template

Jae-Seung Jeong[a,c], Gyo Sub Lee[b], Ki-Young Lee [a,c*] and Hyunsu Ju [a,c*]

[a] Korea Institute of Science and Technology, 5, Hwarang-ro 14-gil, Seongbuk-gu, Seoul 02792, Republic of Korea
[b] ASML Korea, 25, Samsung 1-ro 5-gil, Hwaseong-si, Gyeonggi-do, Republic of Korea
[c] University of Science and Technology of Korea (UST), 217, Gajeong-ro, Yuseong-gu, Daejeon 34113, Republic of Korea
E-mails: *wotmd104@kist.re.kr; gyo-sub.lee@asml.com, kylee80@kist.re.kr* †, *hyunsuju@kist.re.kr* †

Human fingerprints are randomly created during fetal activity in the womb, resulting in unique and physically irreproducible fingerprint patterns that are applicable as a biological cryptographic primitive. Similarly, stochastically knitted single-walled carbon nanotube (SWNT) network surfaces exhibit inherently random and unique electrical characteristics that can be exploited as a physical unclonable function (PUF) in the authentication. In this study, filamentous M13 bacteriophages are used as a biological gluing template to create a random SWNT network surface with mechanical flexibility, with electrical properties determined by random variation during fabrication. The resistance profile between two adjacent electrodes was mapped for these M13-mediated SWNT network surfaces, with the results demonstrating a unique resistance profile for each M13-SWNT device, similar to that of human fingerprints. Randomness and uniqueness measures were evaluated as respectively 50.5% and 50% using generated challenge–response pairs. Min-entropy for unpredictability evaluation of the M13-WNT based PUFs resulted in 0.98. Our results showed that M13-SWNT random network exhibits cryptographic characteristics when used in a bio-inspired PUF device.

KEYWORDS: Carbon nanotube network, Biological glue, Hydrodynamic assembly, Physical unclonable function, PUF, Hardware security

Introduction

The semiconductor industry has offered various security systems, but traditional security methodologies still face tremendous threats from sophisticated attacks [1-3]. To protect against these attacks, physical unclonable functions (PUFs) employ the inherent physical characteristics of electrical devices arising from fabrication variations [4]. These characteristics vary randomly and are unduplicable, as they result from inherent structural variations. Diverse PUF implementations have been proposed based on optical devices, RFID, FPGA, integrated circuits, memory devices, organic electronics, and carbon nanotubes (CNTs) [5-14]. CNT-based PUFs have attracted significant attention for wearable applications owing to their flexibility and printable characteristic [11, 12]. Prior studies have been conducted on the implementation of CNT-based PUFs [1, 14]. These PUFs exploit an analog resistance network using a random conducting path formed by dispersed CNTs during the fabrication [10]. This analog resistance network has desirable inherent randomness for PUF fabrication. Moreover, CNT-based PUFs also have sufficient tolerance to ultraviolet light and radiation, increasing their reliability in various fields [1]. In this study, M13 phages were employed as a biological glue layer to apply single-walled carbon nanotubes (SWNTs) to a M13 nanomesh [13, 15] and implement a unique CNT-based PUF device (M13-SWNT). The SWNTs provide large effective surface areas, forming percolating structures, and provide efficient interfacing with ionic systems (electrochemical, biological, and biochemical), mechanical flexibility, and optical transparency characteristics [13]. The M13 phage, as a biological glue material, is strongly bound to the SWNTs to assemble the conductive nanomesh [15]. Consequently, the M13-SWNT surface arrangement is formed randomly from inevitable fabrication variations, and this inherent feature enables PUF device implementation in cryptographic key generation.

Materials and Methods

Device characteristics

Fabrication variation makes it physically impossible to duplicate security chips and, therefore, is essential for PUF device implementation. The M13-SWNT film was fabricated through hydrodynamic assembly process as previous published [13]. The hydrodynamic assembly method used for M13-SWNT-based PUF devices has been reported to increase fabrication variation. Briefly, SWNTs dispersed in a sodium cholate solution were mixed with a genetically engineered M13 bacteriophage. This M13 bacteriophage was used because of its filamentous nature and strong binding affinity for SWNTs, resulting from a specific peptide sequence on its body surface (p8 peptide). A mixture of SWNTs and an M13 bacteriophage solution, based on a 4:1 molar ratio of SWNT to M13 bacteriophage, was dialyzed against DI water. An M13-SWNT-conductive network film formed around the inner

wall of the dialysis membrane via a hydrodynamic assembly process because of concentration polarization. Because this phenomenon is not exactly the same in the entire area, M13-SWNT film has a locally different resistance. Theses random networks apparently formed as a result of non-reproducible variables such as wrinkles and curvature of the membrane. During the fabrication a randomly distributed surface is developed on the M13-SWNT substrate, forming resistance networks between the two electrodes (Fig. 1). M13-SWNT-based PUF devices fabricated in the same batch exhibit unique resistance networks. Similar to human fingerprints, these resistance values produce characteristic electric response patterns for the M13-SWNT-devices.

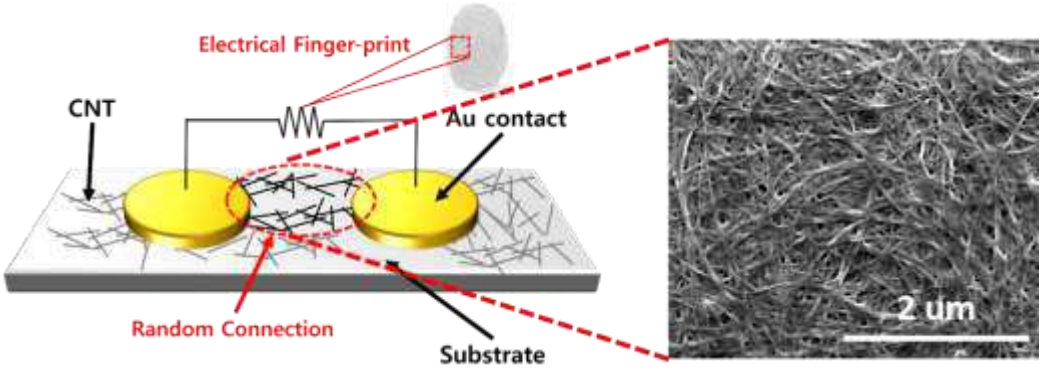

Fig. 1. Schematic of M13-SWNT-based PUF. The random resistance values are attributed to the variable M13-SWNT network surfaces, which cause the unpredictable responses.

Resistance distributions were investigated by applying a voltage pulse of 0.5 V/100 ns to measure the read current of 90 cells for three different M13-SWNT-based PUFs fabricated in the same batch. Fig. 2. represents the variations in the measured resistance. The resistance values of the M13-SWNT-based PUFs exhibit random patterns due to cell-to-cell variation, which indicates the likeliness of duplicating these PUFs. The following section (3. results and discussion) will analyze these random patterns using quantitative methods. Moreover, the significant resistance variation in the M13-SWNT material can improve authentication characteristics.

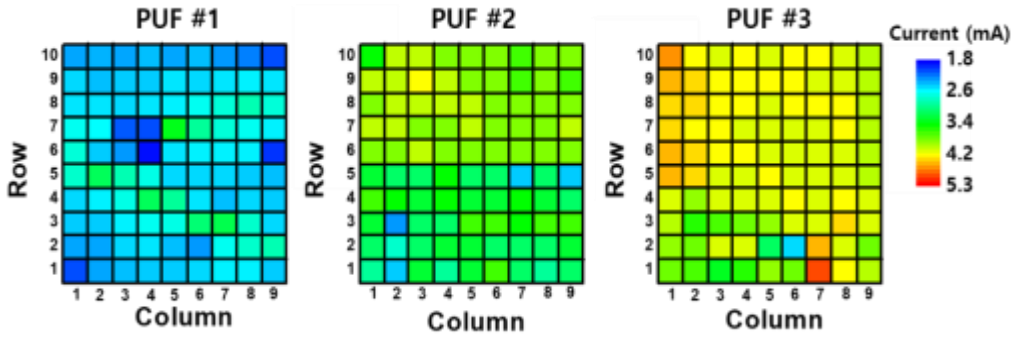

Fig. 2. Resistance variation of carbon nanotube-based conductive nanomesh. Each pixel indicates the cell current value measured for 0.5 V/10 ns. All M13-SWNT based PUFs have different resistance values at the same position, indicating that they can generate different responses to the same challenges.

Challenge–response pair (CRP) generation method

The PUF, as a cryptographic primitive, should respond to paired challenges with prearranged outputs, together referred to as challenge–response pairs (CRP). The response bit, 0 or 1, is generated by comparing the currents of the two cells selected by the challenge (Fig. 3). This CRP generation method predicts the response-bit generation mechanism more difficult than using CRP generation with a predefined reference cell because the possible cell combinations become much larger. Furthermore, it may help the response bits avoid a bias to 0 or 1, even when the current values of the cells follow a biased distribution within a specific window. Thus, the total possible combinations are $\binom{m}{2}^n$, where m is the number of cells in a PUF device, and n is the bit length of the response string.

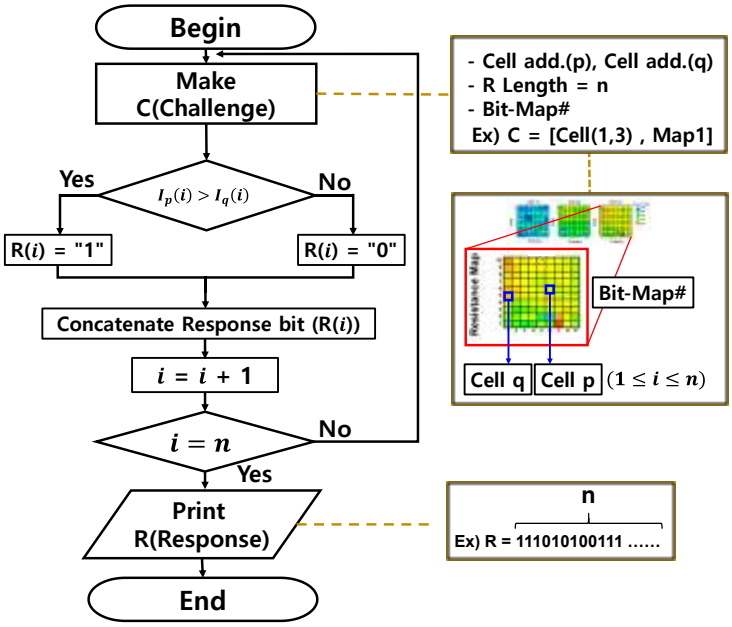

Fig. 3. Schematic of CRP generation algorithm. When a request for CRP generation arrives, a challenge (C) is generated that comprises two particular cells from a specific PUF device and a response length (R). Comparing the currents of the first and second selected cells produces a bit represented by 0 or 1. Concatenating each bit

Results and Discussion

Min-entropy

Min-entropy is the most conservative way to measure the unpredictability of a set of outcomes and is evaluated by the responses as follows [16]:

Equation 1 $H_{\min} = -\log_2(P_{\max})$,

where H_{min} denotes the min-entropy of the samples, and P_{max} maximum probability of 0 or 1 at each position of the response to the challenges.

$$\textbf{Equation 2}\quad (H_{min})_{total} = -\frac{1}{n}\sum_{i=1}^{n} log_2(P_{max})$$

If P_{max} is close to 0.5, then the min-entropy leads to an ideal value of 1. The response patterns from the PUF with a min-entropy close to 1 become almost unpredictable. All the fabricated M13-SWNT-based PUFs had a desirably high min-entropy of 0.98, regardless of the individual PUF cell distribution, demonstrating the unpredictability of their responses.

Randomness and uniqueness evaluation

Randomness evaluates the unpredictability of the responses and is obtained by measuring the number of '1s' or '0s' in the response string [17]. An ideal PUF should have randomness of 50%, which contributes to strong tolerance against brute-force attacks. Uniqueness represents how different responses are expected to be when the same challenge is applied to different PUFs [17]. It is evaluated by measuring the hamming-distance between responses of different PUFs to the same challenge, and an ideal PUF should have a uniqueness of 50%. The randomness was measured by applying 10,000 different challenges and extracting the 240-bit responses from each PUF. The uniqueness was also evaluated by applying the same challenges 10,000 times to the three PUFs and obtaining the 240-bit responses. The randomness of the M13-SWNT-based PUFs results was 50%, 50.5%, and 51%, all of which are close to the ideal value of 50%, as shown in Fig. 4(a). Moreover, the uniqueness of PUFs also tended to the ideal value of 50%, as shown in Fig. 4(b).

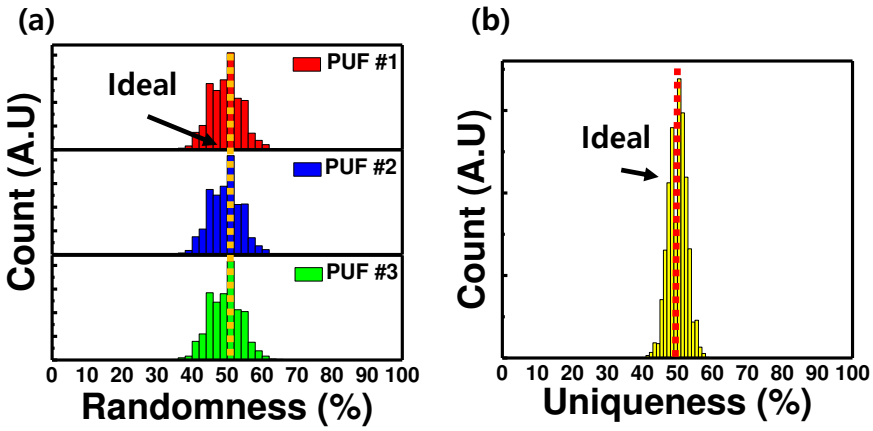

Fig. 4. Randomness and uniqueness of the M13-SWNT based PUFs. (a) The randomness of each M13-SWNT based PUFs fabricated in the same batch is close to the ideal value of 50%. (b) The uniqueness of M13-SWNT based PUFs close to the ideal value of 50%.

Environment variations

The PUF device is required to behave reliably by reproducing the same responses even under environmental variations. In particular, the M13-SWNT-based PUFs with a flexible substrate are easily exposed to physical and temperature variations, and these changes often cause a bit flip in the response electrical outputs. However, when the electrical changes can be linearly correlated with environmental variation, the corresponding relationship between resistance and environmental variation can be used to minimize the possibility of bit flips, in a process referred to as error correction [18]. Therefore, our study investigated the dependencies of resistance on bending and temperature variation. When the M13-SWNT-based PUF was subjected to bending, resistance increased, with respect to strain, (Fig. 5(a)). Moreover, a temperature increase from 25 °C to 50 °C linearly decreased the resistance, indicated by increased current flow shown (Fig. 5(b)). Based on the linear correlation of resistance with these environmental variables the bit errors induced by environmental change can be suppressed via a compensation algorithm.

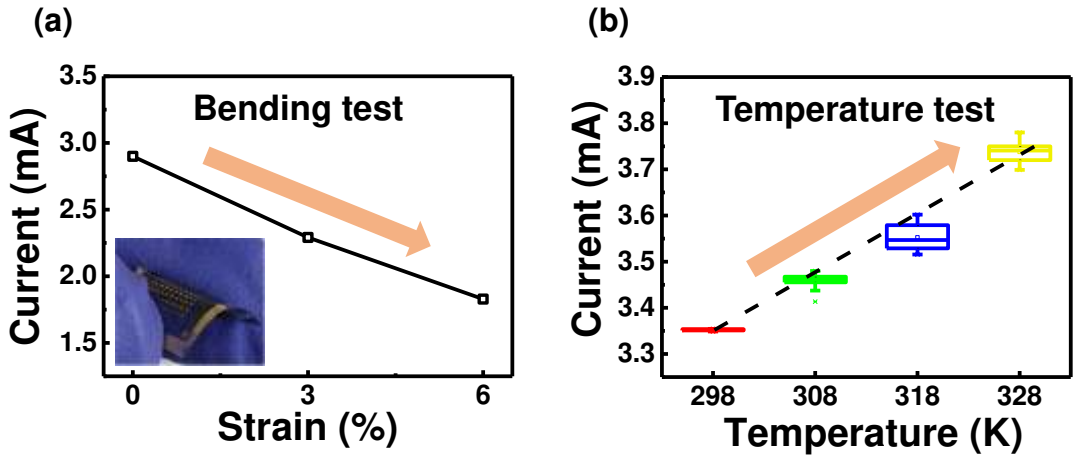

Fig. 5. Resistance variations of the M13-SWNT based PUFs caused by environmental variations. (a) Explicit negative relation between the current and the bending strain on the substrate and (b) positive tendency of the current to the temperature variation.

Conclusion

A single-walled carbon nanotube (SWNT) network surface was implemented for a PUF application using a M13 bacteriophage layer as a biological glue material through a simple hydrodynamic assembly process. This process can naturally form random SWNT connections between the two electrodes through inherent fabrication variations. The random connection variations lead to a random and unique resistance distribution for each M13-SWNT device. Individual cells in the M13-SWNT device were defined by the resistance between two adjacent electrodes. These randomly distributed and unique resistance values were then used to generate the challenge–

response pairs (CRPs) for a cryptographic primitive. To evaluate the M13-SWNT-based PUF devices, the randomness, uniqueness, and min-entropy were determined for the given CRPs. In addition, resistance was found to have a linear correlation with environmentally induced temperature and strain changes. These relationships can be used to compensate for resistance change, and thus minimize the bit errors. We successfully demonstrated the cryptographic properties of M13-SWNT and its robustness to environmental variation when used as a biomimetic PUF device.

ACKNOWLEDGMENT

J.-S. Jeong and G. S. Lee contributed equally to this work. K.-Y. Lee and H. Ju are corresponding authors. This study was supported and funded by the Korean National Police Agency (KNPA)-(PR08-04-000-21), the Ministry of Culture, Sports and Tourism (MCST) and Korea Creative Content Agency (KOCCA)-(CR202104002), the National Research and Development Program through the National Research Foundation of Korea (NRF), the Ministry of Science and ICT (2019M3F3A1A02071509 and 2020M3F3A2A01081635) and KIST institutional program (2E31551, 2E31541).

Data availability

The datasets generated and/or analyzed during the current study are not publicly available due to follows the intellectual-property protection guidelines in KIST as a national research institute, but are available from the corresponding author on reasonable request.

Reference

[1] D.-I. Moon, A. Rukhin, R.P. Gandhiraman, B. Kim, S. Kim, M.-L. Seol, K.J. Yoon, D. Lee, J. Koehne, J.-W. Han, M. Meyyappan, Physically unclonable function by an all-printed carbon nanotube network, ACS Appl. Electron. Mater. 1 (2019) 1162–1168. https://doi.org/10.1021/acsaelm.9b00166.
[2] V.v.d. Leest, R. Maes, G.-J. Schrijen, P. Tuyls, Hardware intrinsic security to protect value in the mobile market, in: ISSE, 2014, Springer, 2014 Securing Electronic Business Processes, pp. 188–198.
[3] R.H. Weber, Internet of Things–New security and privacy challenges, Comput. Law Sec. Rev. 26 (2010) 23–30. https://doi.org/10.1016/j.clsr.2009.11.008.
[4] M. Tehranipoor, C. Wang, Introduction to Hardware Security and Trust, Springer Science and Business Media, 2011.
[5] S. Dolev, Ł. Krzywiecki, N. Panwar, M. Segal, Optical PUF for non-forwardable vehicle authentication, Comput. Commun. 93 (2016) 52–67. https://doi.org/10.1016/j.comcom.2016.05.016.
[6] B. Gassend, D. Clarke, M. Van Dijk, S. Devadas, Silicon physical random functions, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 148–160.
[7] A.-R. Sadeghi, D. Naccache, Towards Hardware-Intrinsic Security, Springer, 2010.
[8] L. Bolotnyy, G. Robins, Physically unclonable function-based security and privacy in RFID systems, in: Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'07), IEEE Publications, 2007, pp. 211–220.
[9] S. Hong, S. Myung, Nanotube electronics: A flexible approach to mobility, Nat. Nanotechnol. 2 (2007) 207–208. https://doi.org/10.1038/nnano.2007.89.
[10] J.B. Wendt, M. Potkonjak, Nanotechnology-based trusted remote sensing, in: Sensors, IEEE Publications, Institute of Electrical and Electronics Engineers. 2011 (2011) 1213–1216.
[11] D. Li, W.Y. Lai, Y.Z. Zhang, W. Huang, Printable transparent conductive films for flexible electronics, Adv. Mater. 30 (2018). https://doi.org/10.1002/adma.201704738, http://www.ncbi.nlm.nih.gov/pubmed/29319214.
[12] Y. Ling, H. Zhang, G. Gu, X. Lu, V. Kayastha, C.S. Jones, W.-S. Shih, D.C. Janzen, A printable CNT-based FM passive wireless sensor tag on a flexible substrate with enhanced sensitivity, IEEE Sens. J. 14 (2013) 1193–1197. https://doi.org/10.1109/JSEN.2013.2281197.
[13] K.Y. Lee, H.H. Byeon, C. Jang, J.H. Choi, I.S. Choi, Y. Jung, W. Kim, J. Chang, H. Yi, Hydrodynamic assembly of conductive nanomesh of single-walled carbon nanotubes using biological glue, Adv. Mater. 27 (2015) 922–928. https://doi.org/10.1002/adma.201404483.
[14] Z. Hu, J.M.M.L. Comeras, H. Park, J. Tang, A. Afzali, G.S. Tulevski, J.B. Hannon, M. Liehr, S.J. Han, Physically unclonable cryptographic primitives using self-assembled carbon nanotubes, Nat. Nanotechnol. 11 (2016) 559–565. https://doi.org/10.1038/nnano.2016.1.
[15] H. Lee, B.P. Lee, P.B. Messersmith, A reversible wet/dry adhesive inspired by mussels and geckos, Nature. 448 (2007) 338–341. https://doi.org/10.1038/nature05968.

[16] M.S. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, M. Boyle, NIST, SP 800–90B: Recommendation for the entropy sources used for random bit generation, in: Tech. Rep, National Institute for Standards and Technology, 2018.
[17] R.L. Sembiring, R.R. Pahlevi, P. Sukarno, Randomness, uniqueness, and steadiness evaluation of physical Unclonable functions, in: 2021 9th International Conference on Information and Communication Technology (ICoICT), IEEE Publications, 2021, pp. 429–433.
[18] G.S. Lee, G.-H. Kim, K. Kwak, D.S. Jeong, H. Ju Ju, Enhanced reconfigurable physical Unclonable function based on stochastic nature of multilevel cell RRAM, IEEE Trans. Electron Devices. 66 (2019) 1717–1721. https://doi.org/10.1109/TED.2019.2898455.

Authorship contribution statement

J.-S. J: Data curation, Investigation, Formal analysis, Software, Writing – original draft, Writing – review & editing, Visualization, **G. S. L:** Data curation, Investigation, Writing – original draft. **K.-Y. L:** Investigation, Methodology, Visualization, Writing – review & editing, **H. J:** Project administration, Conceptualization, Supervision, Formal analysis, Visualization, Validation, Writing – original draft, Writing – review & editing.