COMMUNICATIONS PHYSICS

ARTICLE

https://doi.org/10.1038/s42005-019-0139-3 OPEN

Biological physically unclonable function

Akshay Wali[1,2], Akhil Dodda[2,3], Yang Wu[3,4], Andrew Pannone[3], Likhith Kumar Reddy Usthili[3,5], Sahin Kaya Ozdemir[2,3], Ibrahim Tarik Ozbolat[2,3,4,6] & Saptarshi Das[2,3]

Information security is one of the foundational requirements for any modern society thriving on digital connectivity. At present, information security is accomplished either through software algorithms or hardware protocols. Software algorithms use pseudo random numbers generated by one-way mathematical functions that are computationally robust in the classical era, but are shown to become vulnerable in the post-quantum era. Hardware security overcomes such limitations through physically unclonable functions (PUFs) that exploit manufacturing process variations in the physical microstructures of Si integrated circuits to obtain true random numbers. However, recent upsurge in reverse engineering strategies make Si-PUFs vulnerable to various attacks. Moreover, Si-PUFs are low-entropy, power-hungry, and area-inefficient. Here we introduce a biological PUF which exploits the inherent randomness found in the colonized populations of T cells and is difficult to reverse engineer and at the same time is high-entropy, non-volatile, reconfigurable, ultra-low-power, low-cost, and environment friendly.

[1] Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802, USA. [2] Materials Research Institute, Pennsylvania State University, University Park, PA 16802, USA. [3] Department of Engineering Science and Mechanics, Pennsylvania State University, University Park, PA 16802, USA. [4] The Huck Institutes of the Life Sciences, Pennsylvania State University, University Park, PA 16802, USA. [5] Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Clappana P O, Kollam, Kerala 690525, India. [6] Department of Biomedical Engineering, Pennsylvania State University, University Park, PA 16802, USA. Correspondence and requests for materials should be addressed to S.D. (email: sud70@psu.edu or email: das.sapt@gmail.com)

Recent years have witnessed significant advancements in digital technologies augmented by the internet connectivity that has truly transformed our lives on this planet. In fact, technologies such as the Internet of Things (IoT)[1,2], big data[3], cloud computing[4], bioinformatics[5] etc. have formed a rather complex and convoluted digital network of physical objects that includes personal health monitoring devices, smart phones, smart cards, and a large number of ubiquitous electronic gadgets and appliances. As a result, a massive volume of digital information relating to our personal, professional, social, and political lives are being generated, stored, and communicated every day. Unfortunately, these digital information are susceptible to loss, manipulation, and misuse unless a rigorous and robust information security system is in place[6]. The recent cyber-attacks leading to a huge volume of data breach from government and private institutions across the globe has exposed the vulnerability of the present day state-of-the-art information security systems.

One of the most critical aspect of any information security system is the authentication of the entity or the individual seeking access to information. Such authentication protocols are commonly known as digital signatures that must be unique and unclonable. Digital signatures can be generated by software algorithms using one-way abstract mathematical functions such as prime number factorization, discrete logarithm problem, and hashing[7–9] or by hardware components using physically unclonable functions (PUFs)[10–14] derived from manufacturing process variations. Mathematical one-way functions are powerful and robust in the classical computational era since it requires nondeterministic exponential time for data decryption using brute force trials (BFTs) by the adversary. However, quantum computation[15] puts them at risk, thereby necessitating physical sources capable of generating high-entropy information. On the other hand, PUFs are associated with the inherent randomness in the physical microstructures of the hardware, mostly in integrated circuits (ICs), which can address the shortcomings of one-way mathematical functions. Since chip manufacturing processes involve multiple and intricate lithographic steps to integrate billions of devices with sub-micron dimensions, variations are unavoidable and unpredictable making it improbable for an adversary to fabricate the exact replica of any chip with reasonable resources and/or within a finite period of time. As such, PUFs that exploits the variation in ICs are becoming foundational building blocks for several cryptographic protocols and hardware security architectures[10–12,16]. It must be remembered that the concept of PUFs was first conceived by Pappu et al. as an optical PUF by exploiting the interference patterns obtained by illuminating a transparent material doped with random light scattering particles[17].

Various types of Si-PUFs[16] have been proposed: arbiter PUFs are based on random variations in interconnect and/or transistor delays, whereas, static random access memory (SRAM) and dynamic random access memory (DRAM) based PUFs exploit variation in transistor dimensions manifesting in the fluctuation in the ON state current and gate delays. Other incarnations of Si-PUFs such as butterfly PUF[18], flip-flop PUF[19], ring oscillator PUF[20], metal resistance PUF[21], digital PUF[22] etc. exploit intrinsic randomness in devices and circuits introduced by the chip fabrication processes. Si-PUFs, however, suffer from several drawbacks including low entropy (DRAM), high power consumption (SRAM), and area inefficiency due to the involvement of additional tamper detection circuitry. Further, Si-PUFs are also susceptible to environmental variations, aging, side channel attacks, and hardware trojans[23–27]. Moreover the recent decline of the Si technology owing to the slowdown of Moore's law of scaling and the emergence of dark Si have influenced and facilitated the growth in IoT technology based on novel nanomaterials and devices[28,29]. In this context, nanotech PUFs based on randomly dispersed nanoparticles[30–32], self-assembled carbon nanotubes (CNTs)[33], sub-lithographic random network of metal wires, block copolymers, and memristive crossbar arrays[34–36] are also being investigated.

In this article, we introduce a PUF which utilizes the randomness in the spatiotemporal and collective behavioral dynamics of biological species. First, we demonstrate that the spatial distribution of T cells, a class of white blood cell or lymphocyte, in a colonized population can be used as an excellent entropy source. Subsequently we use these colonized T cell populations as a biological PUF (Bio-PUF) and evaluate three important metrics namely: (a) reproducibility, (b) physical unclonability, and (c) reconfigurability to show that Bio-PUF can be regarded as a strong PUF. Although, we have used colonized T cell populations for our demonstration, the concept of Bio-PUF can be extended to any random processes associated with cellular or molecular biology. We believe that Bio-PUFs can be used in centralized locations such as servers, and data centers where an active life support system can be easily integrated. It is expected that security systems based on Bio-PUFs will be much more energy efficient and environment friendly. Furthermore, there are numerous biological species that can harvest energy to self-support. It is possible in the near future to integrate some of these benign bio-species with smart devices for on-chip information security opening opportunities for innovation.

Results

Randomness Test for Bio-PUF. Fig. 1a shows the schematic representation of how Bio-PUFs can be generated. First, the T cells are purified, stimulated, cultured, suspended, and separated. Details of cell preparation can be found in the Methods section. Next, the T cells are transferred to an imaging system with an onstage incubator and are subsequently allowed to form colonies for several hours (~20 h). Finally, the colonized T cell population is imaged and processed using a computer to generate the Bio-PUF. Figure 1b shows a representative false color optical image of an arbitrarily chosen T cell population after they have formed the colonies. The importance of colony formation will be discussed in the following section. Except for slight variation in their dimensions, the T cells are optically identical and appear to be distributed randomly within the colonies. For quantitative measure of randomness, the optical image was converted into a two dimensional (2D) binary information source by assigning digital "1" or "white" to the pixels occupied by the T cells and digital "0" or "black" to the unoccupied pixels as shown in Fig. 1c. The 2D binary image contains 64 × 64 pixels, each being a ~10 μm × 10 μm square corresponding to the average size of a T cell. This 2D binary image is used as the Bio-PUF. Figure 1d shows the entropy ($E_{x,y}$) of the Bio-PUF along both axes obtained by using the standard equation 1, where $p_{x,y}$ is defined as the probability of obtaining "1", along the respective axes.

$$\begin{aligned} E_x &= -\left[p_x \log_2 p_x + (1-p_x)\log_2(1-p_x)\right]; \\ E_y &= -\left[p_y \log_2 p_y + \left(1-p_y\right)\log_2\left(1-p_y\right)\right] \end{aligned} \quad (1)$$

Remarkably, the average entropy was found to be 0.93 ± 0.06 and 0.91 ± 0.05 along the x- and y-axis, respectively, which is close to the ideal value of 1 corresponding to a perfectly random information source. In order to perform more rigorous statistical strength tests, the Bio-PUF was divided into 64 one-dimensional (1D) keys each with 64 bits as shown in Fig. 1e. Figure 1e shows the probability mass function (PMF) of the intra-Hamming distance (H_{intra}) among ${}^{64}C_2 = 2016$ pairs of 1D keys. The Hamming distance between a pair of 1D keys is defined as

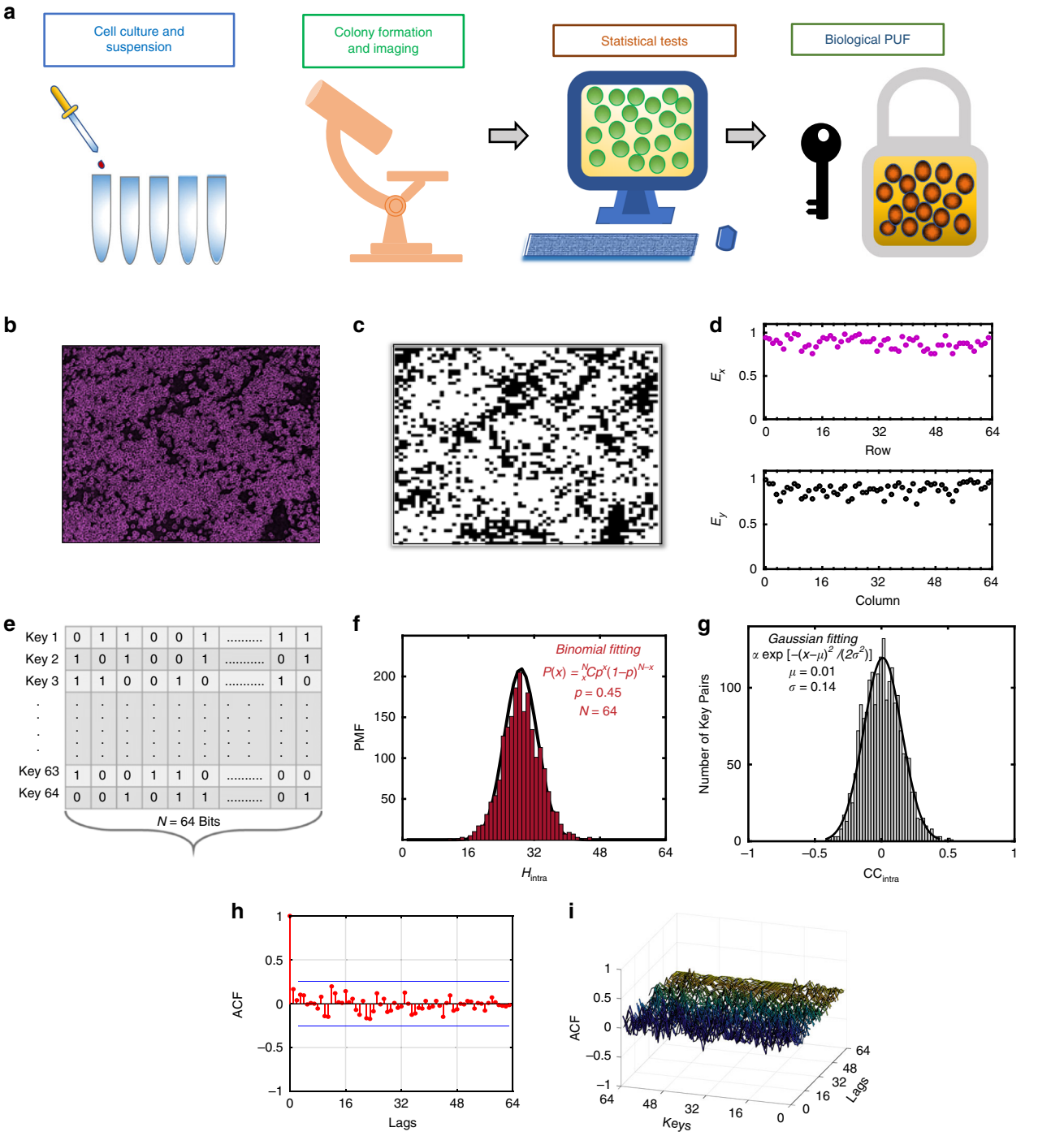


Fig. 1 Randomness of Biological Physically Unclonable Function (Bio-PUF). **a** Schematic of process flow for generating a Bio-PUF. First, the T cells are cultured and suspended in individual well(s) and then transferred to an imaging system with an onstage incubator. These T cells are subsequently allowed to form colonies for several hours (~20 h). Finally, the colonized T cell population is imaged and processed using a computer for generating the Bio-PUF. **b** False color optical image of a randomly chosen post-colonization T cell population with precise cell identification (purple). **c** Construction of Bio-PUF with 64 × 64 pixels (bits). Pixels occupied by T cells are assigned digital "1" (white), whereas, unoccupied pixels are assigned digital "0" (black). **d** Entropy ($E_{x,y}$) content of the Bio-PUF along both axes. **e** 64 1D keys each with 64 bits associated the Bio-PUF. **f** Probability mass function (PMF) of the intra-Hamming distance (H_{intra}) between the ${}^{64}C_2 = 2016$ pairs of 1D keys. The mean H_{intra} extracted using a binomial fit was found to be ≈29, which suggests close to maximum uniqueness for the 1D keys and hence the Bio-PUF. **g** Histogram of correlation coefficients (CC_{intra}) between the 1D keys. The mean CC_{intra} extracted using a Gaussian fit (inset) was found to be 0.01, which confirms lack of any correlation between the 1D keys. **h** Autocorrelation coefficient (ACF) for an arbitrarily chosen 1D key as a function of the lag. **i** 3D plot of the ACF for all 64 keys. The presence of low amplitude and narrow spikes indicate none to minimal memory effect in colonized T cell population and rationalizes the strength of Bio-PUF

the number of non-identical bits that must be flipped in order for two keys to be exactly similar. The prefix "intra" is used, when we compare the 1D keys generated from a given image, whereas the prefix "inter" is used when we compare the 1D keys generated from different sets of images in the following sections. Note that 1D keys with too short or too long of a Hamming distance are relatively easy to decipher through BFTs, whereas a Hamming distance equal to half of the key length ensures maximum uniqueness. As shown in Fig. 1f, the PMF of H_{intra} follows binomial distribution with a mean ≈29 that ensures close to maximum uniqueness of the 1D keys corresponding to a total number of BFTs of $\sim 1.38 \times 10^{18}$ required to decipher a single 1D key, and a minimum number of BFTs of $\sim 10^{1216}$ required to decipher the entire 2D image or the Bio-PUF, which is an astronomical amount. Further, Fig. 1g shows the histogram of intra-correlation coefficient (CC_{intra}) among $^{64}C_2$ pairs of 1D keys. The Correlation coefficient is a measure of the linear correlation between two statistical quantities and must be zero for independently and identically distributed random variables. Figure 1g shows that CC_{intra} follows a zero mean Gaussian distribution which confirms that the T cells are uncorrelated further adding to the strength of the Bio-PUF. The correlation coefficient of the bit sequence with itself was calculated up to a 64-bit delay (lags) for examining any periodicity and short-ranged correlations[37]. The autocorrelation coefficients (ACF) lie in the interval [−1, 1] where a value of −1 and 1 indicate anti-correlation and correlation, respectively, and a value of 0 suggests uncorrelated bits. Figure 1h shows the ACF obtained for a randomly chosen key from our Bio-PUF as a function of the lag. Figure 1i shows a 3D plot of the ACF for all 64 keys. The presence of low amplitude and narrow spikes indicate none to minimal memory effect in colonized T cell population and rationalizes the strength of Bio-PUF. Note that the total number of unique Bio-PUFs that can be generated using colonized T cells is $2^{64} \times 2^{64} = 10^{1233}$. In other words, the total number of unique images that are possible using human T cells when imaged in an area of 0.5 mm^2 is 10^{1233}. In short, the above results prove that the spatial randomness in the distribution of T cells within any colonized population can be used as an excellent entropy source with arbitrarily small statistical defects for the construction of an astronomically large number of true random numbers (TRNs) that form the foundation for Bio-PUF.

Reproducibility of Bio-PUF. PUF is usually described as a challenge-response pair (CRP) such that each challenge is associated with a unique response, which must be reproduced every time or in other words, the response must not change over time. For example, in SRAM PUF, SRAM cells produce random but reproducible bit sequences, every time the chip is turned ON. However, it is well known that ideal reproducibility is almost never achieved due to effects of temporal noise seen in any hardware based PUFs. Therefore, a revised approach is taken where a certain degree of bit-error is tolerated, known as fuzzy authentication[38]. Here, the verifying party accepts the authentication as long as the Hamming distances between the responses to an identical challenge over time fall within a predefined threshold. In order to investigate the reproducibility of the Bio-PUF, we began with freshly suspended T cell population and recorded their temporal evolution over 24 h by generating false color optical images and corresponding Bio-PUFs, every 5 min, as shown in Fig. 2a. Clearly, in the beginning, the spatial

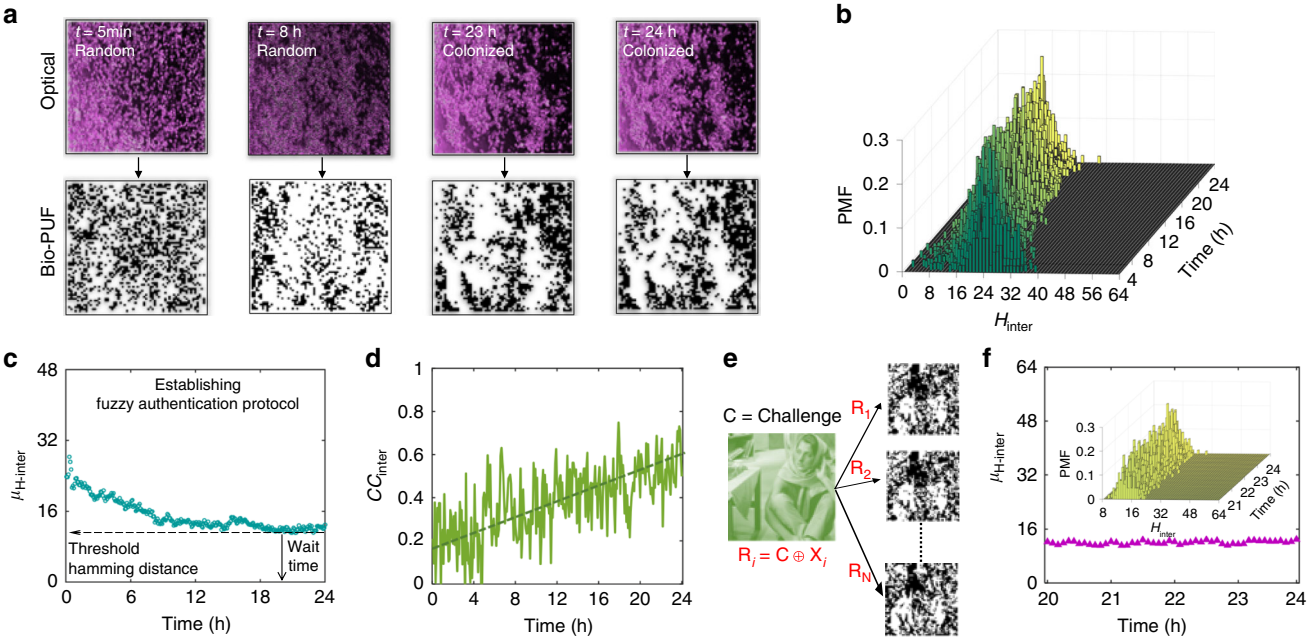


Fig. 2 Reproducibility of Biological Physically Unclonable Function (Bio-PUF). **a** False color optical images and corresponding Bio-PUFs obtained by sampling an arbitrarily chosen T cell population every 5 min for a total of 24 h. At the beginning the T cells move randomly. However, over time they renounce their temporal motion and form stable colonies, which allows the Bio-PUFs to demonstrate reproducibility. **b** Temporal evolution of probability mass function (PMF) of inter-Hamming distance (H_{inter}) between the 1D keys obtained from two successive Bio-PUFs. **c** The mean of H_{inter} drops from ~30 to ~13, as the T cell population colonizes, allowing us to determine the threshold Hamming distance (~13) and the wait time (~20 h) before the T cell population can be used as reproducible Bio-PUF. **d** Time evolution of inter-correlation coefficients (CC_{inter}) show gradual increase in correlation between the Bio-PUFs as the colony formation takes place. **e** Standard Barbara image (© 1994–2019 The MathWorks, Inc) is introduced as a challenge (*C*) to the Bio-PUFs. Responses are generated through logical XOR operation. **f** Mean H_{inter} between the responses remain below the predefined threshold ensuring the reproducibility aspect of the Bio-PUF. Inset shows the PMF of H_{inter} in post-colonization period

randomness of the T cell population is associated with their random temporal motion, which is undesirable in the context of reproducibility of PUF as discussed above. However, as time evolves, the T cell population starts to form local colonies, renouncing their temporal motion and facilitating their use as Bio-PUF. Figure 2b shows the spatiotemporal evolution of the PMF of the inter-Hamming distance (H_{inter}), i.e., the Hamming distance between the 1D keys of two successive Bio-PUFs over time. The mean of H_{inter} drops from ~30 to ~13, as the T cell population colonizes, allowing us to determine a threshold Hamming distance (~13) and the wait time (~20 h) before the T cell population can be used as Bio-PUF, as shown in Fig. 2c. A similar inference can be made from the temporal evolution of the inter-correlation coefficient (CC_{inter}) shown in Fig. 2d. The random temporal motion of the T cells ensure a lack of any correlation between the successive Bio-PUFs in pre-colonization (CC_{inter} ~ 0.2), whereas, the post-colonization Bio-PUFs are strongly correlated (CC_{inter} ~ 0.6). We further tested the reproducibility of the Bio-PUF by using the standard Barbara image as the challenge. Figure 2e shows the CRPs prepared by bitwise XOR operations between the binary version of the Barbara image, which is used as a challenge (C), and post-colonization Bio-PUFs, i.e., the binary images obtained every 5 min between 20^{th} and 24^{th} h (X_i). Figure 2f shows that the mean H_{inter} between the responses remain fairly constant at ~12 over time, which is below the threshold value of 13 for false rejection (type-I error), demonstrating the reproducibility of the Bio-PUF. Note that other logical operations such as AND, OR, etc. can also be used for generating the CRPs. The reader should also note that while the T cells are indeed a class of human white blood cell, we are not using them for biometrics. Therefore it does not matter where these cells come from. Once the cells are obtained and prepared for imaging, we harness the random distribution of their colonies as PUF. The reproducibility arises from the static nature of the colonies. Certainly if another new sample of T cell is taken even from the same person and the same procedure is repeated to image the colonies, a completely different PUF will be obtained, which proves the unclonability aspect of Bio-PUF as we will describe in the following section. This is another reason why it is so difficult to reverse engineer Bio-PUF.

Unclonability of Bio-PUF. Physical unclonability is one of the most important and basic requirement for any PUF ensuring that the response to any specific challenge generated by a cloned system is easily distinguishable from the response obtained from an authentic system and that the differences cannot be attributed to any noise or environmental variations. While all PUFs, by definition, have to be physically unclonable, recent upsurge in reverse engineering made physical cloning a possibility in some cases. In this section, we demonstrate that even with an exhaustive knowledge of the bio-PUF that includes complete information on cell preparation, cell type, cell density, cell colonization time, imaging instance, and imaging frequency; it is prohibitively difficult to clone or reverse engineer the bio-PUF by an adversary. Figure 3a shows the false color optical images and corresponding Bio-PUFs generated using post-colonization T cell population i.e., taken 24 h after cell suspension from five

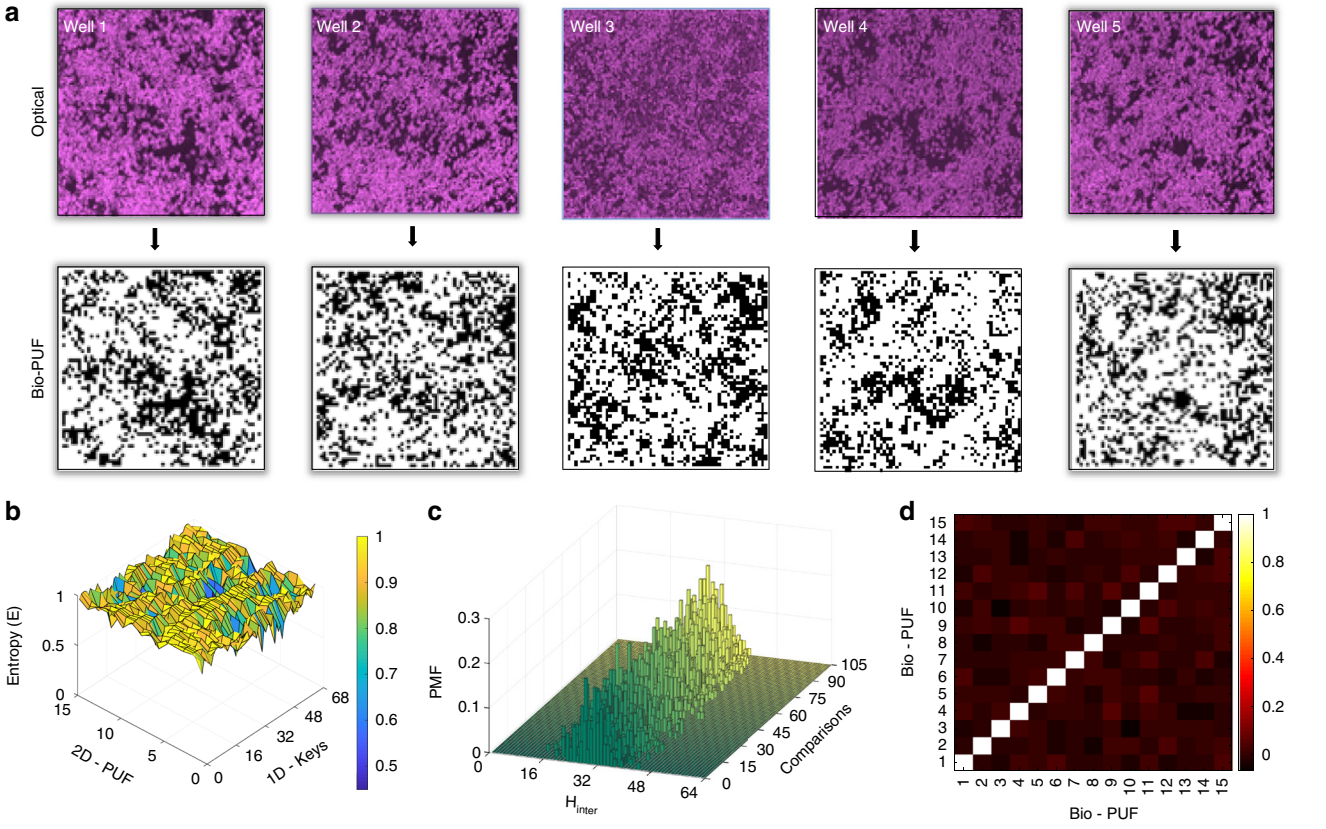


Fig. 3 Unclonability of Biological Physically Unclonable Function (Bio-PUF). **a** False color optical images and corresponding Bio-PUFs generated using post-colonization T cell population i.e. taken 24 h after cell suspension from five independently and separately prepared wells. A total of 15 Bio-PUFs, 3 from different locations of each of the 5 wells, were analyzed. **b** Entropy plot showing high-entropy values for all the 64 1D keys generated from 15 different Bio-PUFs. **c** Probability mass function (PMF) of inter-Hamming distance (H_{inter}) between the 1D keys associated with the $^{15}C_2$ pairs of Bio-PUFs. **d** Correlation coefficient colormap between the Bio-PUFs

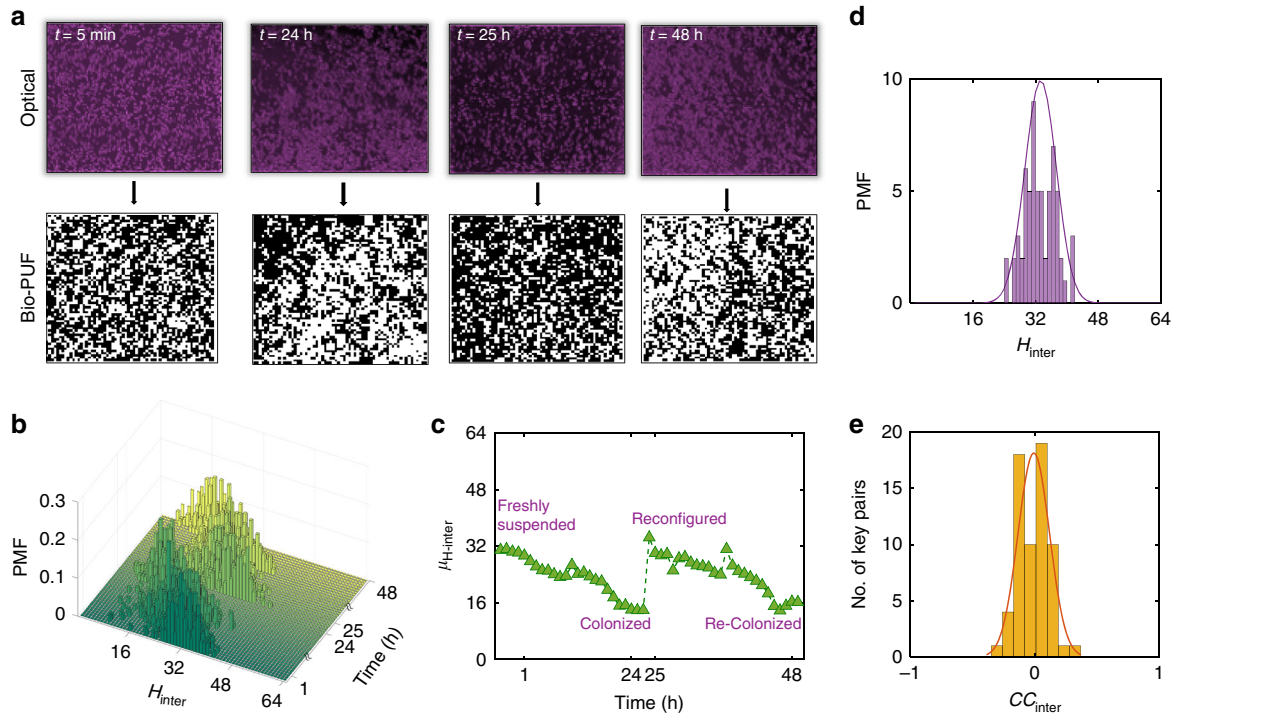


Fig. 4 Reconfigurability of Biological Physically Unclonable Function (Bio-PUF). **a** False color optical images and the associated Bio-PUFs corresponding to four different configurations of the T cell population: (1) freshly suspended (0–1 h), (2) post-colonization (23–24 h.), (3) reconfigured (24–25 h.), and (4) recolonized (47–48 h.) **b** Temporal evaluation of probability mass function (PMF) of inter-Hamming distance (H_{inter}). **c** The mean H_{inter} cycles between ~31 during the pre-colonization time to ~13 in the post-colonization time. Distribution of **d** H_{inter} and **e** inter-correlation coefficients (CC_{inter}) between the pre- and post- reconfigured Bio-PUFs. Clearly, H_{inter} follows binomial distribution with means of ~30 and CC_{inter} follows a Gaussian distribution with mean ~0 confirming that the physical unclonability aspect is uncompromised when the Bio-PUF is reconfigured

independent and separately prepared wells. A total of 15 Bio-PUFs, three from different locations of each of the five wells were analyzed. We found that irrespective of whether the colonized T cell images were obtained from the same well or from different wells, it is remarkably difficult to replicate the distribution of the T cells and their colonies. Figure 3b shows that the 64 1D keys associated with each of the 15 Bio-PUFs contain high entropy that is close to the ideal value of unity, confirming the uniqueness and true random nature of the Bio-PUF. Figure 3c shows the PMF of H_{inter} between the 1D keys associated with the $^{15}C_2$ pairs of Bio-PUFs. The mean extracted using binomial fitting was found to be fairly constant at ~30, corresponding to a total number of BFTs of $\sim 1.62 \times 10^{18}$ required to clone a single 1D key and a minimum number of BFT of 10^{1216} to clone the entire Bio-PUF. This clearly demonstrates that the T cell colonies are very difficult to reverse engineer. Further, Fig. 3d confirm that the Bio-PUFs are completely uncorrelated, reinforcing the unclonability claim for Bio-PUF.

Reconfigurability of Bio-PUF. A PUF is considered reconfigurable if there exists a mechanism that can transform the system into a new one, such that the CRPs corresponding to the reconfigured system are completely unpredictable and uncorrelated to the CRPs of the original PUF[39]. Most of the Si-PUF either completely lack reconfigurability or are resource constrained in terms of cost and complexity for reconfiguration. Optical PUF and PUFs based on novel nanodevices such as the memristive crossbar arrays do provide some reconfigurability, which is becoming a key requirement for strong PUFs due to increasing vulnerability to various model building attacks. In this section, we demonstrate that the colonized T cell population can be seamlessly reconfigured by, first, flushing new cell media into the system that breaks apart the colonies and reinstate the random temporal motion of the T cells, and then allowing them to reorganize and reform new colonies over time. Remarkably, the spatial distribution of the T cells within the new colonies is found to be completely uncorrelated from their distribution in the old colonies confirming reconfigurability without any loss of randomness or entropy. Figure 4a shows the representative false color optical images and the associated Bio-PUFs corresponding to four different configurations of the T cell population: (1) freshly suspended T cell population imaged between 0^{th} and 1^{st} hour, (2) post-colonization T cell population imaged between 23^{rd} and 24^{th} hour, (3) reconfigured T cell population imaged between 24^{th} and 25^{th} hour, and (4) recolonized T cell population imaged between 47^{th} and 48^{th} hour. The images were sampled every 5 min. As such, each set consists of 13 images. Figure 4b, c, respectively, show the temporal evaluation of PMF of H_{inter} and the corresponding mean, which cycles between ~31 during the pre-colonization time to ~13 in the post-colonization time as the system is reconfigured without any loss of reproducibility. Figure 4d, e show the normalized distribution of H_{inter} and CC_{inter} between the pre- and post- reconfigured Bio-PUFs. Clearly, H_{inter} follows binomial distribution with a mean of ~30 and CC_{inter} follows a Gaussian distribution with mean ~0 confirming that the physical unclonability aspect remains uncompromised when the Bio-PUFs is reconfigured.

Implementation of Bio-PUF. Figure 5 shows the implementation of Bio-PUF. A standard cameraman image taken from the MATLAB directory is introduced as a challenge (C) to 15 different Bio-PUFs (X_i, $i = 1, 2, 3\ldots, 15$). Figure 5a shows the

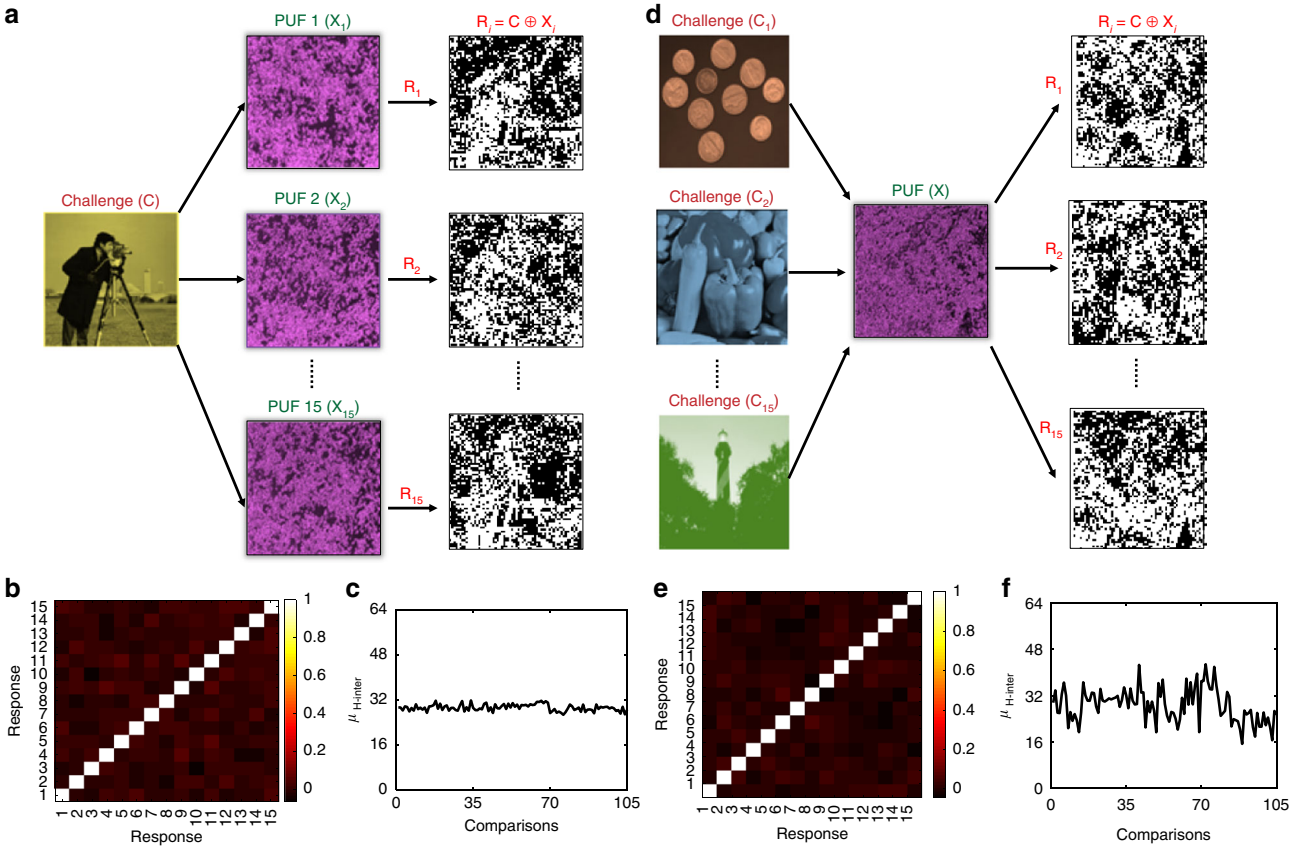
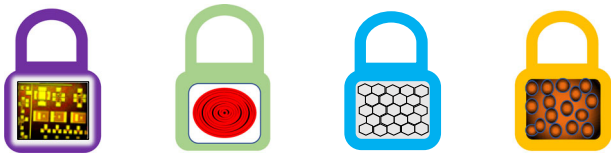


Fig. 5 Implementation of Biological Physically Unclonable Function (Bio-PUF). **a** A standard cameraman image (© 1994–2019 The MathWorks, Inc) is introduced as a challenge (*C*) to 15 different Bio-PUFs (X_i, $i = 1, 2, 3..., 15$) and the corresponding responses are generated using logical XOR operation. **b** Color map of correlation coefficient and **c** inter-Hamming distance (H_{inter}) among these 15 responses. **d** 15 unique challenges (C_i, $i = 1, 2, 3..., 15$) applied to the same Bio-PUF (*X*) to generate the corresponding responses. (© 1994–2019 The MathWorks, Inc). **e** Color map of correlation coefficient and **f** H_{inter} among these 15 responses. In both instances no correlation is observed among the responses, as well as mean H_{inter} was found to be ~32, reasserting the uniqueness and unclonability aspects of Bio-PUF

corresponding responses generated using logical XOR operation. Figure 5b, c show that the correlation coefficient and mean H_{inter} among these responses are close to their ideal values of 0 and 32 respectively, reaffirming the unclonability of Bio-PUF. Further, Fig. 5d shows 15 different challenges (C_i, $i = 1, 2, 3..., 15$) applied to the same Bio-PUF (*X*) to generate the corresponding responses. The correlation map in Fig. 5e shows near zero correlation and the H_{inter} in Fig. 5f shows near ideal mean of ~32 between the responses, reconfirming the uniqueness of the Bio-PUF. The minimum inter-hamming distance was found to be 16, which is more than the Fuzzy authentication threshold of 13, ensuring zero occurrence of false acceptance of type-II error. For practical implementation of the Bio-PUF fluorescent markers can be used to accurately capture the locations of the T cells using a high resolution digital camera in order to generate the 2D binary images. Further, the information content in each Bio-PUF can be increased either by increasing the imaging area or by using biological entities with smaller dimensions. For example, mycoplasma gallicepticum, a parasitic bacterium is 100× smaller than the diameter of the T cells, which will allow the generation of 10,000× more number of bits per unit area, making the Bio-PUF exponentially more difficult to clone. Resilience to aging and stability against environmental factors such as temperate, ambient conditions etc. are useful attributes of PUF. The typical lifespan of T cells are 60–150 days. Further, T cells are known to die when the temperature shifts from the normal human body temperature of 98 °F (37 °C). However, thermophiles that are capable of thriving at much higher temperatures ranging from 41 to 122 °C and psychrophiles, that can survive low temperatures ranging from −20 to 10 °C can be exploited for temperature invariant Bio-PUFs. Also post-colonization T cells are not completely static, instead these cells exhibit reduced motility compared to pre-colonization time that compromises on reproducibility of the Bio-PUF and requires the implementation of fuzzy authentication protocol. However, there are biological populations such as the bacteria E Coli which can be made completely static after colony formation either by storing them in an incubator or by using some rigid media.

Discussion

Figure 6 shows a thorough comparison of the Bio-PUF with other state-of-the-art PUFs that include Si-PUF, Optical-PUF, and Nanotech-PUF on the basis of various evaluation metrics. The Si chip manufacturing industry is almost flawless owing to more than six decades of investment towards making billions of identical devices. As such the device to device variation is very limited in Si ICs, which makes the Si-PUFs inherently low entropy and necessitates the use of additional pre- and/or post-processing entropy compensation units that incur more energy consumption, expensive area overhead and manufacturing cost. However, an argument can be made that while Si-PUFs are weak



Evaluation metrics	Si PUF SRAM, DRAM	Optical PUF	Nanotech PUFs CNT's, Memristors	Biological PUF
Entropy	Low	Medium	High	High
Reproducibility	Yes	Yes	Yes	Yes
Reconfigurability	No	Yes	Limited	Yes
Uniqueness	Yes	Yes	Yes	Yes
CRPs	Linear	Exponential	Linear	Exponential
Cost	High	High	High	Low
Energy consumption	High	Low	Low	Low
Reverse engineering	Possible	Very difficult	Difficult	Very difficult
Volatile/non-volatile	Volatile	Non-volatile	Non-volatile	Non-volatile
Weak/strong PUF	Weak	Strong	Strong	Strong

Fig. 6 Comparison of Biological Physically Unclonable Function (Bio-PUF). Comparison of the Bio-PUF with Si-PUF, optical-PUF, and nanotech-PUF on the basis of various evaluation metrics. Bio-PUFs can potentially supersede any other state-of-the-art PUFs and emerge as a strong PUF since they offer high entropy, low cost, low power, seamless reconfigurability, non-volatility, exponential number of CRPs and are practically impossible to reverse engineer even with an exhaustive knowledge of the biological system

from the point of view of information theory that necessitates adequate entropy, these are computationally secure since it is difficult to find a way to break them. Nevertheless, Si-PUFs have linear number of CRPs and are mostly volatile in nature. Moreover, Si-PUFs are vulnerable to reverse engineering and tampering through various side channel attacks, model building attacks, hardware Trojans, and they also lack reconfigurability, which make them weak PUF[40]. Optical PUFs offer better security solution since they are non-volatile, low power, and, to a limited extent, reconfigurable[17]. Reverse engineering is difficult for optical PUF although diffraction of light follows physical laws that can be represented by mathematical equations. Therefore, optical PUFs are regarded as strong PUF. However, the optical PUFs too have relatively poor entropy and require hashing functions for high quality randomness. Further, there exists only a limited number of light incident angles that can generate unique diffraction patterns from the same distribution of nanoparticles in the transparent scattering medium resulting in linear CRPs. Optical PUFs are also not competitive in terms of cost because the readout device is a separate apparatus and nonintegrated with the PUF. Nanotech PUFs are strong PUFs since they are mostly non-volatile, low power, high entropy, and difficult to reverse engineer owing to the inherent disorders associated with nanosystems[33]. However, nanotech PUFs encounter multiple challenges such as precise control or placement of the nanomaterial, sub-lithographic fabrication, optimization of device operating condition, which increase cost in spite of the readout circuitry being included in the PUF itself. Further, nanotech PUFs have a limited number of CRPs and offer limited reconfigurability. Bio-PUFs can potentially supersede any of the above mentioned state-of-the-art PUFs and emerge as a strong PUF since they offer high entropy, low cost, low power, seamless reconfigurability, exponential number of CRPs, and are very difficult to reverse engineer even with an exhaustive knowledge of the biological system. One of the shortcomings of the Bio-PUF based on human T cells is that it does not meet the stringent reliability and reproducibility criterion of PUF due to the slow but finite movement of colonies and thereby requiring fuzzy authentication with a certain threshold for error tolerance. However, it is possible to use other biological entities such as Escherichia Coli (E. coli), a bacterial species that remain completely static when suspended in a media without food by ceasing their growth. Therefore, it will be possible in the future to develop Bio-PUFs with potentially perfect reproducibility. Moreover, other species like extremophiles and thermophiles are known to survive large temperature variations and environmental conditions and could be a potential alternatives to T cells for more reliable security applications. Further, our Bio-PUF demonstration does not address the issue of

separate readout circuitry which can incur extra cost. However, our future work will involve seamless integration of the biological cultures in solid medium with cost-effective charge coupled devices (CCDs) or complementary metal oxide semiconductor (CMOS) imaging chips and use fluorescent nanoparticles to directly monitor and map the spatial distribution of the T cell colonies. Bio-PUFs are also non-volatile. Note that volatility is of benefit to Si-PUFs, because the response is only generated when needed. Whereas non-volatility is useful if the secure key needs to be maintained during the lifespan of the PUF integrated device.

In conclusion, we have introduced a PUF that exploits the inherent randomness found in biological species such as the T cells. We confirmed that the colonized T cell population can be used as a near ideal entropy source to create unclonable, reproducible, and unique challenge-response pairs (CRPs). We also demonstrated how Bio-PUFs can be seamlessly reconfigured without physical replacement of the system or addition of extra hardware components, which is unprecedented for any state-of-the-art PUFs.

Methods

T cells preparation and imaging. Peripheral blood mononuclear cells (PBMCs) were isolated using Ficoll-paque plus (GE Healthcare, IL). CD8+ T cells were purified using CD8-Positive Isolation Kit (Invitrogen, MA). Purity (>99%) of CD8+ T cells were confirmed by flow cytometry staining with, respective, antibodies. CD8+ T cells were stimulated using anti-CD3/anti-CD28 coated beads (Invitrogen, MA) at 1:2 (bead:cell) ratio and cultured in Roswell Park Memorial Institute medium (RPMI 1640, Corning, NY) supplemented with 10% fetal bovine serum (FBS, Atlanta Biologicals, GA), 1% penicillin/streptomycin (Corning, NY), and interleukin-2 (IL-2, Sigma-Aldrich, MO) at a 1:200 dilution for 14 days. Pellet of T cells was obtained by centrifuging the cell suspension at 1600 rpm for 5 min, followed by removable of the supernatant. T cells were then suspended in a 24-well plate (Corning, NY) using the same cell culture media to obtain cell densities of 5×10^5 cells/mL. Suspended cells were cultured in the incubator at 37 °C and 5% CO_2 for 20 min for cell precipitation. The 24-well plate was then transferred to an EVOS imaging system with onstage incubator (Invitrogen, MA), and cultured at 37 °C and 5% CO_2 during imaging. For each sample, images were taken at × 20 every 5 min for the first hour, followed by culturing the cells in the incubator at 37 °C and 5% CO_2 for 23 h, and images were taken again every 5 min for the twenty-fourth hour. Immediately after imaging, the cells in well plates were resuspended by pipetting, and the same imaging process was repeated for the resuspended cells.

Data availability

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Code availability

The codes used for data analysis are available from the corresponding authors on reasonable request.

Received: 28 November 2018 Accepted: 2 March 2019
Published online: 26 April 2019

References

1. Kruger, C. P. & Hancke, G. P. In Proc. *12th IEEE International Conference on Industrial Informatics (INDIN)*. 611–616 (IEEE, Porto Alegre, 2014).
2. Atzori, L., Iera, A. & Morabito, G. The internet of things: a survey. *Comput. Netw.* **54**, 2787–2805 (2010).
3. Mayer-Schönberger, V. & Cukier, K. *Big data: A revolution that will transform how we live, work, and think*. (Houghton Mifflin Harcourt: Boston, 2013.
4. Armbrust, M. et al. A view of cloud computing. *Commun. ACM* **53**, 50–58 (2010).
5. Swan, M. The quantified self: fundamental disruption in big data science and biological discovery. *Big Data* **1**, 85–99 (2013).
6. Bulgurcu, B., Cavusoglu, H. & Benbasat, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Q.* **34**, 523–548 (2010).
7. Naor, M. & Yung, M. In *Proc. of the twenty-first annual ACM symposium on Theory of computing*. 33–43 (ACM, Seattle, 1989).
8. McGraw, G. Software security. *IEEE Secur. Priv.* **2**, 80–83 (2004).
9. Goldwasser, S., Micali, S. & Rivest, R. L. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.* **17**, 281–308 (1988).
10. Maes, R *Physically unclonable functions*. (Springer, Berlin, 2016).
11. Suh, G. E. & Devadas, S. Design Automation Conference. DAC'07. *In Proc.4th ACM/IEEE*. 9–14 (IEEE, San Diego, 2007).
12. Maes, R. & Verbauwhede, I. *Towards Hardware-Intrinsic Security*. (Springer, Berlin, 2010).
13. Tehranipoor, M. & Wang, C. *Introduction to hardware security and trust*. (Springer Science & Business Media, Berlin, 2011).
14. Herder, C., Yu, M.-D., Koushanfar, F. & Devadas, S. Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **102**, 1126–1141 (2014).
15. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**, 303–332 (1999).
16. Gassend, B., Clarke, D., Van Dijk, M. & Devadas, S. in *Proc. of the 9th ACM conference on Computer and communications security*. 148–160 (ACM, New York, 2002).
17. Pappu, R., Recht, B., Taylor, J. & Gershenfeld, N. Physical one-way functions. *Science* **297**, 2026–2030, (2002).
18. Kumar, S. S., Guajardo, J., Maes, R., Schrijen, G.-J. & Tuyls, P. in *Proc. IEEE International Workshop on Hardware-Oriented Security and Trust*. 67–70 (IEEE, Anaheim, 2008).
19. Maes, R., Tuyls, P. & Verbauwhede, I. *3rd Benelux workshop on information and system security*. (WISSec, Eindhoven, 2008).
20. Maiti, A. & Schaumont, P. Improved ring oscillator PUF: an FPGA-friendly secure primitive. *J. Cryptol.* **24**, 375–397 (2011).
21. Chen, A. Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions. *Ieee Electr. Device L* **36**, 138–140 (2015).
22. Xu, T. & Potkonjak, M. In Proc. *24th International Conference on Field Programmable Logic and Applications (FPL)*. 1–6 (IEEE, 2014).
23. Helfmeier, C., Boit, C., Nedospasov, D. & Seifert, J.-P. In *Proc. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 1–6 (IEEE, Austin, 2013).
24. Katzenbeisser, S. et al. *International Workshop on Cryptographic Hardware and Embedded Systems*. 283–301 (Springer, Leuven, 2012).
25. Yu, M.-D. & Devadas, S. Secure and robust error correction for physical unclonable functions. *IEEE Des. Test. Comput.* **27**, 48–65 (2010).
26. Schrijen, G.-J. & Van Der Leest, V. In *Proc. of the conference on design, automation and test in Europe*. 1319–1324 (EDA Consortium, Dresden, 2012).
27. Rührmair, U. et al. PUF modeling attacks on simulated and silicon data. *IEEE Trans. Inf. Forensics Secur.* **8**, 1876–1891 (2013).
28. Frank, D. J. et al. Device scaling limits of Si MOSFETs and their application dependencies. *P Ieee* **89**, 259–288 (2001).
29. Esmaeilzadeh, H., Blem, E., Amant, R. S., Sankaralingam, K. & Burger, D. In *Proc. 38th Annual International Symposium on Computer Architecture (ISCA)*. 365–376 (IEEE, San Jose, 2011).
30. Yoon, B. et al. Recent functional material based approaches to prevent and detect counterfeiting. *J. Mater. Chem. C.* **1**, 2388–2403 (2013).
31. Demirok, U. K., Burdick, J. & Wang, J. Orthogonal multi-readout identification of alloy nanowire barcodes. *J. Am. Chem. Soc.* **131**, 22–23 (2008).
32. Kim, J. et al. Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires. *Nanotechnology* **25**, 155303 (2014).
33. Hu, Z. et al. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotechnol.* **11**, 559 (2016).
34. Rajendran, J., Rose, G. S., Karri, R. & Potkonjak, M. In *Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 84–87 (IEEE, Amherst, 2012).
35. Gao, Y., Ranasinghe, D. C., Al-Sarawi, S. F., Kavehei, O. & Abbott, D. Emerging physical unclonable functions with nanotechnology. *IEEE Access* **4**, 61–80 (2016).
36. Rose, G. S., McDonald, N., Yan, L.-K. & Wysocki, B. In *Proc. IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 830–833 (IEEE, San Jose, 2013).
37. Gunn, L. J., Chapeau-Blondeau, F., Allison, A. & Abbott, D. Towards an information-theoretic model of the Allison mixture stochastic process. *J. Stat. Mech.* **2016**, 054041 (2016).
38. De Ru, W. G. & Eloff, J. H. Enhanced password authentication through fuzzy logic. *IEEE Expert* **12**, 38–45 (1997).
39. Kursawe, K., Sadeghi, A.-R., Schellekens, D., Skoric, B. & Tuyls, P. Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage. In *Proc. IEEE International Workshop on Hardware-Oriented Security and Trust*. 22-29 (IEEE, Francisco, CA, 2009).
40. Quadir, S. E. et al. A survey on chip to system reverse engineering. *ACM J. Emerg. Technol. Comput. Syst. (JETC)* **13**, 6 (2016).

Acknowledgement
Authors would like to acknowledge Dr. Derya Unutmaz from Jackson Labs for providing T cells.

Author contributions
S.D. conceived the idea and designed the experiments. S.D., I.T.O., and S.K.O. supervised the research. A.W., A.D., Y.W., A.P., L.K.R., and S.D. performed the experiments and analyzed the data. All the authors discussed the results, agreed on their implications, and contributed to the preparation of the manuscript.

Additional information
Competing interests: The authors declare no competing interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.