SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2022, Vol. 65 122405:1–122405:9
https://doi.org/10.1007/s11432-021-3270-8

# Reconfigurable physical unclonable cryptographic primitives based on current-induced nanomagnets switching

Shuai ZHANG, Jian ZHANG, Shihao LI, Yaoyuan WANG, Zhenjiang CHEN, Jeongmin HONG & Long YOU*

*Wuhan National Laboratory for Optoelectronics and School of Optical and Electronic Information, Huazhong University of Science and Technology, Wuhan* 430074, *China*

Received 6 January 2021/Revised 18 April 2021/Accepted 6 May 2021/Published online 10 December 2021

**Abstract** Hardware security primitives that preserve secrets are playing a crucial role in the Internet-of-Things (IoT) era. Existing physical unclonable function (PUF) instantiations, exploiting static randomness, generate challenge-response pairings (CRPs) to produce unique security keys that can be used to authenticate devices linked to the IoT. Reconfigurable PUFs (RPUFs) with dynamically refreshable CRPs can enhance the security and robustness of conventional PUFs. The in-plane current-driven perpendicular polarized nanomagnet switching via spin-orbit torque (SOT) possesses great potential for application to memory and logic, as the write-current path is separate from the read-current path, which naturally resolves the write-read interference. However, the stochastic switching of perpendicular magnetization, without an additional symmetry-breaking field, would significantly hinder the technological viability of commercial implementations. Here, we report an initialization-free physical RPUF implemented by SOT-induced stochastic switching of perpendicularly magnetized Ta/CoFeB/MgO nanodevices. Using a $15 \times 15$ nanomagnet array, we experimentally demonstrate a security primitive that offers a near-ideal 50% uniqueness over 100 reconfiguration cycles, as well as a low correlation coefficient between every two reconfiguration cycles. Our results show that current-induced nanomagnets switching paves the way for developing highly reliable and energy-efficient reconfigurable cryptographic primitives with a smaller footprint.

**Keywords** reconfigurable physical unclonable function, spin-orbit torque, cryptographic primitive, spintronics, nanomagnet

**Citation** Zhang S, Zhang J, Li S H, et al. Reconfigurable physical unclonable cryptographic primitives based on current-induced nanomagnets switching. Sci China Inf Sci, 2022, 65(2): 122405, https://doi.org/10.1007/s11432-021-3270-8

## 1 Introduction

The severe threat to the world economy, national security, and human health associated with the counterfeiting of products and intellectual property infringement has drawn increasing public attention in recent years. Meanwhile, with the development of the Internet-of-Things (IoT), an increasing number of electronic devices are connected to the Internet, resulting in that personal security has become a critical issue. Hardware security primitives based on physical unclonable functions (PUFs) have been recently developed for authentication/counterfeit protection and secret data-encryption keys [1–7]. PUFs exploit the static randomness resulting from non-deterministic process variations to extract instance-specific secrets. The randomness characteristic of the feature guarantees non-replicable code outputs. Specifically, by stimulating the PUF device with a challenge, a response is produced correspondingly, and this challenge-response pairing (CRP) behavior is device specific and prohibitively difficult to predict. Despite their merits in terms of integration, unclonability, and robustness, existing PUF implementations typically exhibit a static CRP behavior that cannot be refreshed. Consequently, contemporary PUF designs face many challenges, such as, reliability deteriorations under extreme conditions, exhaustive CRP access

* Corresponding author (email: lyou@hust.edu.cn)

 

attacks on PUFs that have a limited number of CRPs, and modeling attacks on PUFs that possess many mutually correlated CRPs [8, 9].

Reconfigurable PUFs (RPUFs) can modify the PUF to exhibit different CRP behaviors [10]. They show strong promise in resolving the aforementioned weaknesses in the implementation of security protocols that cannot be effectively surmounted by conventional PUFs. Moreover, RPUFs may endow a PUF with many appealing features such as scalable robustness, key renewal, and revocation ability. Intrinsically alterable physical attributes are desirable for creating an RPUF to exploit physical reconfigurability, which is more efficient since no additional hardware primitive is required. Nevertheless, finding a suitable technology with which to design a physical RPUF such that the CRPs of its physical implementation possess the ideal attributes is a challenge, and this may be the reason why the figures of merits of most, if not all, of the proposed physical RPUFs are only theoretically simulated rather than experimentally demonstrated.

For the case of emerging memory-based RPUF, phase change memory (PCM) [11], resistive random access memory (RRAM) [12, 13], and spin-transfer torque magnetic random access memory (STT-MRAM) [14, 15] have drawn a lot of attention in recent years. The switching probability during programming at the nanoscale level of PCM, RRAM, and STT-MRAM devices provides a dynamic source of randomness that could be exploited in the PUF to generate reconfigurability. However, these emerging memories share the same drawback, that is, the requirement of the precise tuning of the applied voltage or current (amplitude and pulse duration) to guarantee a 50% switching probability for each cell. The requirements become tougher with the increase of the number of memory cells, making it non-trivial for practical applications. On the other hand, in a ferromagnet (FM)/heavy metal (HM) heterostructure, the coupling of spin and orbital angular momenta can produce an effective spin-orbit torque (SOT) field perpendicular to the easy magnetization axis during programming [16–24]. The resulting effective field acting on the magnetization is unable to deterministically switch the magnet with perpendicular magnetic anisotropy (PMA), but can only orient the magnetization to the in-plane direction, a metastable point [25, 26]. Therefore, a large enough programming current through HM can lead to magnetization randomly switching, from the macrospin point of view, which overcomes the issues in the aforementioned memories for RPUF application [26]. This stochastic switching of the nanomagnet provides the possibility of constructing an RPUF with SOT devices. However, current results are mainly focused on providing proof of concept. No meaningful scale experimental demonstration has been able to show its feasibility.

Here, we propose and demonstrate experimentally a novel RPUF based on the switching of a nanomagnet using an in-plane current. The stochastic switching mechanisms provide a natural source of randomness for PUF implementation, which can be almost infinitely reconfigured by reprogramming nanomagnet arrays. As the information stored in our technology only relies on the magnetization of a nanomagnet, it is highly resistant to radiation and able to withstand harsh environmental conditions, preventing the alteration of the bit information even under extreme circumstances. In addition, a nanomagnet based upon Ta/CoFeB/MgO heterostructures is demonstrated to configure the PUF, which are commonly used in out-of-plane magnetized magnetic tunnel junctions (MTJs) for commercial MRAM [27]. The low-temperature fabrication process of our devices ($< 180^{\circ}$C) makes this technology a viable option for stand-alone on-chip PUFs, as well as for interfacing with other existing technologies to create stronger security primitives.

## 2 Materials and methods

### 2.1 Illustration of the SOT-RPUF

The essential idea of the proposed RPUF is depicted in Figure 1. We first consider a nanomagnet composed of an HM/FM/oxide layered heterostructure with PMA, for example, Ta/CoFeB/MgO. As our previous study shows [25], when an in-plane current (write current, $I_{\rm w}$) is applied to the underneath Ta layer, the nanomagnet is excited to align its magnetization along the hard axis ($y$-axis direction in Figure 1) due to SOT. After the current is removed, the magnetization orientation is relaxed to the easy axis ($z$-axis direction). Depending on the thermal fluctuations, the magnetization either orients 'upwards' (red arrows in Figure 1) or 'downwards' (blue arrows in Figure 1), creating random codes. Here we show that this SOT based hardware true random number generator (TRNG) can be utilized to implement hardware security. To form the building block for PUF, one can construct an array consisting

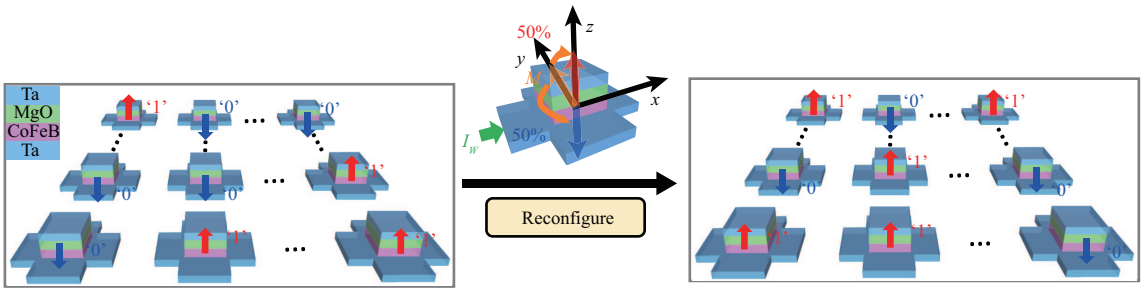


**Figure 1** (Color online) Scheme of the proposed RPUF implemented using SOT-induced stochastic magnetization switching of nanomagnets.

of $m$ number of units with each unit composed of $n$ number of SOT TRNGs. If an identical current $I_{\rm w}$ is applied to each device, a random distribution of magnetization orientations can be obtained. Then, using the digitalization method by which the upward state is encoded as logic '1' while the downward state as logic '0', $m$ groups of CRPs or PUF keys with a length of $n$ bits are generated. The CRPs gathered from a PUF are the references for the verification. Here, the PUF unit address and the magnetization orientation are the challenge and response of the PUF, respectively. If the CRPs of the PUF must be refreshed whenever necessary, one can just process one more write operation to the PUF, as illustrated in Figure 1, and the magnetizations will be reoriented randomly. In other words, the PUF is reconfigurable.

The response of a PUF is highly desired to be stable when it is stimulated by the same challenge, which is called reliability. Since the SOT based RPUF will be implemented by SOT-MRAM for practical application, the reliability and the reconfiguration times of the RPUF are limited by the retention and endurance of MRAM, respectively. The retention time (over ten years) [28] and high endurance ($> 5 \times 10^{10}$) [29] of CoFeB magnets have been widely reported in SOT-MRAM. Therefore, in theory, the proposed SOT-RPUF has dramatically high reliability and sufficient reconfiguration times.

### 2.2 Sample fabrication

A thin-film stack of Ta (10 nm)/CoFeB (1 nm)/MgO (1 nm)/Ta (2 nm) was sputter-deposited on a thermally-oxidized Si substrate at room temperature. The film was then processed into the Hall bar structure by electron beam lithography (EBL) and argon-ion milling (AIM). The Hall bars contained the entire thin film stack, with the region outside the Hall bars etched down to the insulating Si substrate. A dot pattern of 10-nm-thick titanium (Ti) with a size of 200 nm × 200 nm, which acts as an etching mask, was fabricated at the center of the Hall bars by EBL and electron beam evaporation. Argon ion milling was also used to etch the stack in the region outside the dot patterns, down to the bottom tantalum layer. The dots therefore comprised Ta (10 nm)/CoFeB (1 nm)/MgO (1 nm)/Ta (2 nm), and the regions of the Hall bar outside the dots were etched down to the bottom tantalum layer.

### 2.3 Electrical measurements

To harness the random magnetization orientations, the Hall resistance ($R_{\rm H}$) due to the anomalous Hall effect (AHE) was detected in magnetic field environment (Model EM5 & Model P7050, East Changing Technologies, Inc. Beijing) at room temperature. A constant 50-μA read current ($I_{\rm r}$) was applied using a DC current source (Keithley Model 6221), and the Hall voltage was measured using a nanovoltmeter (Keithley Model 2182A) in the usual way. The same current source was used to apply a write current ($I_{\rm w}$) with a duration of 0.2 s for the current-induced stochastic switching and reconfiguring the PUF. The external magnetic field was generated by a Helmholtz coil driven by a power supply.

## 3 Results and discussion

### 3.1 Stochastic switching of a nanomagnet induced by SOT

A scanning electron microscope image of a typical Hall bar structure with a magnetic device (200 nm × 200 nm) at the cross-section is shown in Figure 2(a). The AHE loop ($R_{\rm H}$ vs. out-of-plane field $H_z$) confirms the strong PMA of the CoFeB magnet with a coercivity field, $H_{\rm c}$, of 80 Oe (see Figure S1(a) in

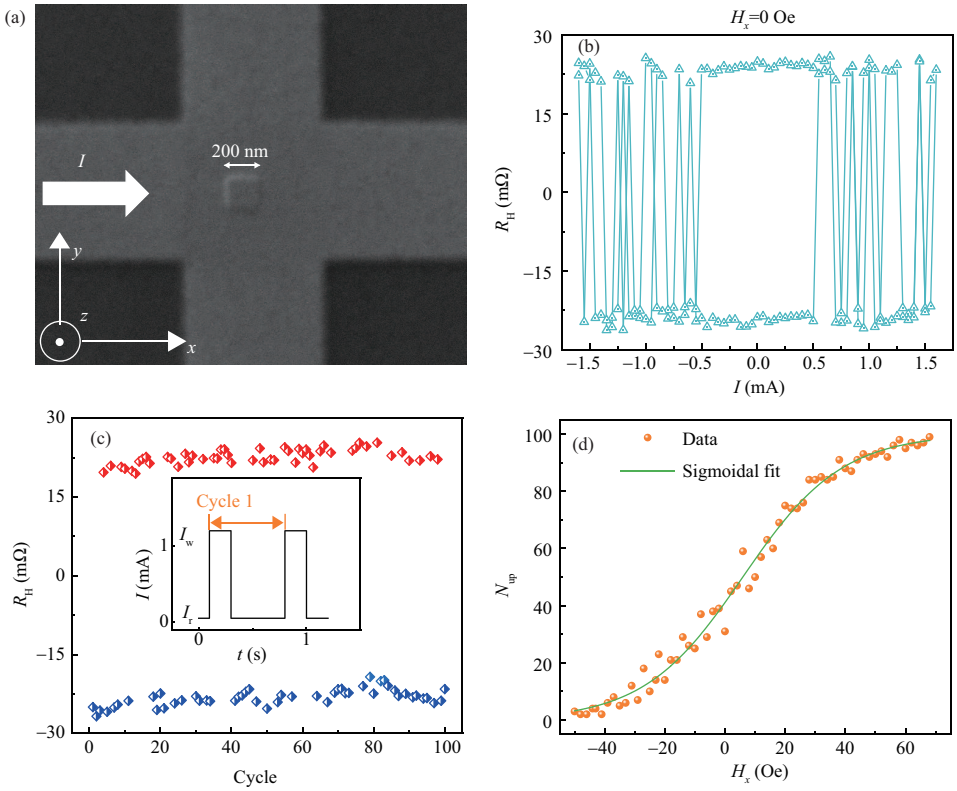


**Figure 2** (Color online) SOT-induced stochastic switching of a nanomagnet. (a) Scanning electron microscope image of a nanomagnet; (b) current-induced switching under $H_x = 0$; (c) current-induced stochastic switching of 100 repeated cycles under $I_w = 1.2$ mA and $H_x = 10$ Oe; (d) counts of upward states in 100 cycles under various $H_x$ at $I_w = 1.2$ mA (orange dots). The data is fitted by a sigmoid function (green line).

Appendix). Next, we investigated the response of $R_H$ to the in-plane current ($I$) under $H_x = -100$ Oe (Figure S1(b) in Appendix) and $H_x = 0$ (Figure 2(b)). When the applied current exceeds 0.7 mA, the SOT-induced switching is deterministic under $H_x = -100$ Oe, while the switching is stochastic without a field. Here, we choose an $I_w$ of 1.2 mA to observe the stochastic switching. An $I_r$ of 50 μA is followed by the $I_w$ to detect the magnetization orientation in every cycle, as illustrated in the inset of Figure 2(c). The obtained $R_H$ values of 100 cycles are plotted in Figure 2(c), in which the red diamonds represent the magnetization oriented upward and the bit '1', while the blue ones denote downward magnetization and represent bit '0'. The number of bits '1' ($N_{up}$), which can reveal the switching probability, was counted as 50. Of course, the switching probability is dependent on the current, with the switching probability increasing from $\sim$ 0 at 0.6 mA to $\sim$ 50% at 0.9 mA. This indicates that a current below 0.9 mA is not efficient enough to drive the nanomagnet to generate random numbers. Once the current exceeds 0.9 mA, the switching probability is always close to 50%. For detail, please see Appendix B. We define the critical current of a SOT based TRNG as the minimum write current required to reach approximately 50% probability; in this case, 0.9 mA. To reveal the time domain evolution of the magnetization, we performed micromagnetic simulations of the four possible transitions (0 to 0, 0 to 1, 1 to 0, and 1 to 1) by using a current density of $5 \times 10^{12}$ A/m$^2$ with a duration of 1 ns (Appendix C). The results confirm the assumption of SOT induced initialization-free magnetization randomly switching.

To verify the effect of the applied in-plane fields $H_x$ on $N_{up}$, we scanned the $H_x$ under a constant write current ($I_w = +1.2$ mA, here), as shown in Figure 2(d). It is interesting to note that upward switching is preferred when the current flows along the field direction, while downward switching is favored once the field direction is reversed. One can see that $N_{up} = 3$ at $H_x = -50$ Oe and $N_{up} = 93$ at $H_x = +50$ Oe. Such bipolar switching behavior also indicates that SOT, instead of Joule heating, is dominant during the current-induced magnetization switching in the Ta/CoFeB/MgO heterostructure [16, 17]. It should be noted that, here, the random switching probability ($\sim$ 50%) occurs at $H_x = 10$ Oe, instead of $H_x = 0$ which is generally expected from in-plane current switching of perpendicularly magnetized nanomagnet. This may be associated with a superfluous bias field in the structure [30, 31], which was

probably introduced via our non-optimized fabrication process. Therefore, the implementation of our TRNG, here, requires a small in-plane field. Furthermore, the switching probability could be fitted with a sigmoid function (green line in Figure 2(d)) that is an activation function of the artificial neurons or the so-called probabilistic bits [32–35], implying that our device has the potential to be used to implement neuromorphic computing.

### 3.2 Implementation of SOT based RPUF

The security hardware was implemented with a $15 \times 15$ nanomagnets (TRNG) array. We first tested the uniqueness of the PUF. After an in-plane current of 1.2 mA was applied to each device, 15 groups of original PUF keys were generated using the digitalization method, where the upward state is encoded as logic '1' while the downward state as logic '0'. The bitmap of the keys is depicted in Figure 3(a). For the statistical analysis, the parameters used to assess the quality of PUFs are statistical distances, including the intra-Hamming distance (intra-HD) and the inter-Hamming distance (inter-HD). Intra-HD reveals the variations between the responses of two tests under the same challenge for all device units. In our case, either a single device or the building block of the proposed RPUF, has a good retention property under the read current of 50 μA. The Hamming distance of two responses by two read operations for a device unit consisting of 15 devices remains zero over reconfiguration cycles (Appendix D). In other words, the testing or measurement using low current does not affect the magnetic properties (or stored information) of nanomagnets. Therefore, we can expect that there would be no difference between different tests for any one device, and estimate that the intra-HD of the proposed RPUF, which consists of 15 units, is very close to 0. On the other hand, inter-HD is the difference of two responses between different device units. The distribution of normalized HDs of the PUF is approximated with Gaussian distribution that is centered at 0.5082 with a variance of 0.1212, as shown in Figure 3(b). The mean inter-HD is close to 0.5, which means that the distributions of magnetization orientation in the PUF are completely random and the PUF has a high uniqueness with CRPs prohibitively difficult to clone and predict. Next, we refreshed the keys 99 times by repeatedly applying the current of 1.2 mA. Figure 3(c) shows the distribution of the normalized HDs of the total 100 reconfiguration cycles. In each cycle, the HDs have a Gaussian function-like distribution. Figure 3(d) depicts the mean normalized inter-HD extracted from Gaussian function fitting. The inter-HDs fluctuate near 0.5, ranging from 0.449 to 0.541, indicating that the CRPs in every reconfiguration cycle are reasonably unique.

### 3.3 Evaluation of reconfigurability

The most unique advantage of the SOT-TRNG based PUF is its reconfigurability, with which the PUF's security can be enhanced. To evaluate the reconfigurability, Figure 4(a) gives the bitmap consisting of all the keys generated in every reconfiguration cycle. In each cycle, $15 \times 15 = 225$ binary bits are produced and extracted as a row in the bitmap. Using this bitmap, we can calculate the reconfigurable Hamming distances and the correlation matrix $R$, as shown in Figures 4(b) and (c), respectively. Regarding the uniqueness of the reconfigured PUF keys, 100 continuous reconfiguration cycles for the RPUF show values close to the ideal value of the reconfigurable HD ($\mu/\sigma = 0.4862/0.0330$). The matrix element $r_{ij}$ of $R$ is defined as the correlation coefficient of the keys between reconfigure cycle $i$ and $j$. The correlation matrix demonstrates little correlation between the different reconfigured keys. Besides, we have calculated the uniformity (the proportion of "1") of the 100 reconfigure cycles of binary bits (Figure S8 in Appendix). All the mean values of uniformities are close to 0.5, indicating that the binary bits have good randomness. Furthermore, the RPUF passes almost all the listed NIST test items with average P-value $> 0.01$ (criteria value) in each item (Table 1).

Moreover, we investigated the uniqueness and reconfigurability of the RPUF under other current values, such as $I_{\mathrm{w}} = 0.8$, 1.0, 1.4, and 1.6 mA. For more details, please see Appendix E. The reconfigure-HDs and the correlation matrixes show that the RPUF has a high performance under these currents, except 0.8 mA. This is mainly because the write current of 0.8 mA is lower than the critical current (around 0.9 mA) for the random switching of an individual nanomagnet; hence, the RPUF keys between different reconfigure cycles have a relatively large correlation. Once the switching current is larger than the highest critical current among cells, the applied current would guarantee the reconfiguration of the PUF. Ideally, a nanomagnet can endure unlimited switching via current, such that unlimited reconfiguration can be achieved in the nanomagnet array. Furthermore, for practical applications, our Ta/CoFeB/MgO heterostructures can be implemented as the free-layer stack in MTJs [27], where a larger tunneling

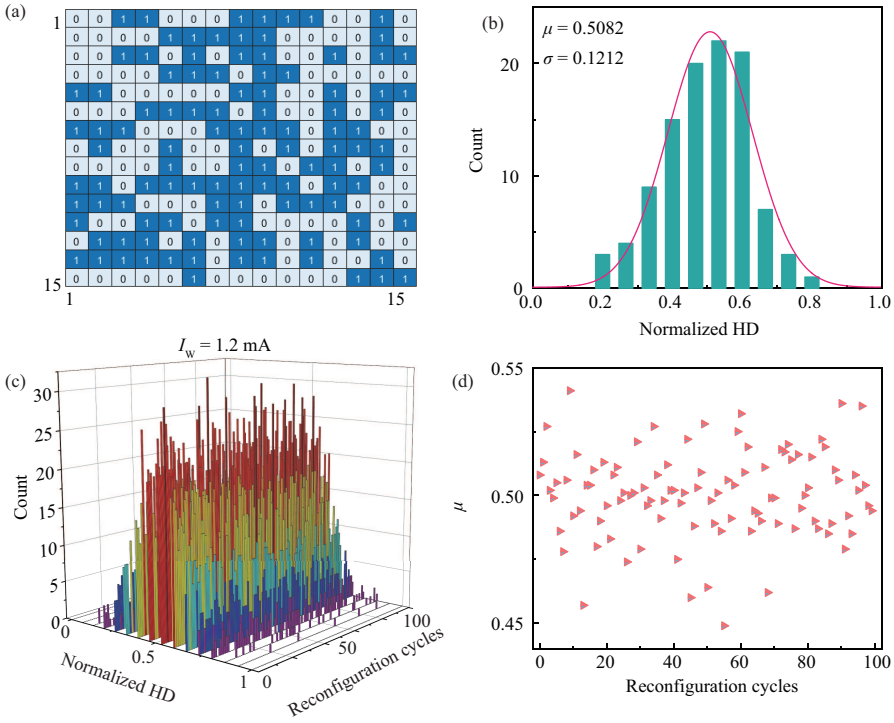


**Figure 3** (Color online) Statistical analysis of the RPUF. (a) Original 15 × 15 binary bits generated from the device array; (b) distribution of the normalized inter-HDs with Gaussian function fitting (red line); (c) distributions of the normalized inter-HDs over 100 reconfiguration cycles; (d) mean values of inter-HDs extracted from Gaussian function fittings.

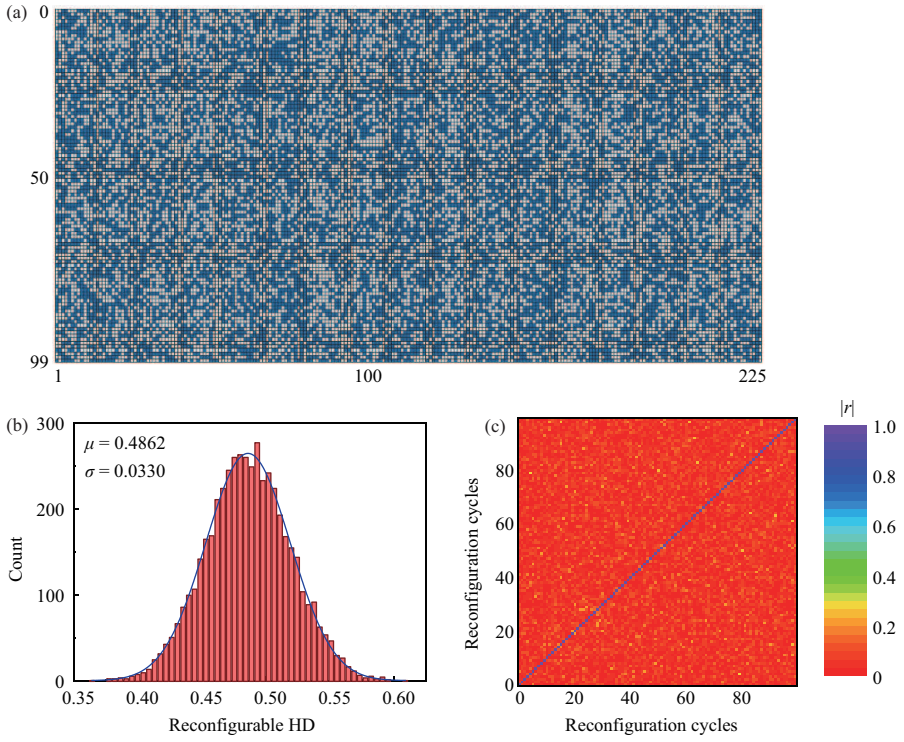


**Figure 4** (Color online) Evaluation of the reconfigurability of the RPUF. (a) Bitmap of 225 × 100 binary bits; (b) reconfigurable HD distribution between 100 reconfigured keys with Gauss fitting (blue line); (c) correlation matrix of 100 reconfigured keys.

magnetoresistance (TMR) will be obtained. Moving from the AHE measurement to magnetoresistance detection, the digitalization can be simplified by comparing with a reference resistance [36].

**Table 1** Results of 8 tests from the NIST SP800-22 statistical suite

| Statistical test | P-value (1.2 mA) | Pass rate | | | | |
|---|---|---|---|---|---|---|
| | | 0.8 mA | 1.0 mA | 1.2 mA | 1.4 mA | 1.6 mA |
| Frequency | 0.452354 | 20/20 | 20/20 | 20/20 | 17/20 | 18/20 |
| Block frequency | 0.444569 | 20/20 | 20/20 | 20/20 | 19/20 | 19/20 |
| Cumulative sums (forward) | 0.563623 | 20/20 | 20/20 | 20/20 | 17/20 | 19/20 |
| Cumulative sums (reverse) | 0.453733 | 20/20 | 19/20 | 19/20 | 17/20 | 19/20 |
| Runs | 0.451601 | 20/20 | 20/20 | 20/20 | 20/20 | 20/20 |
| Longest run | 0.446447 | 20/20 | 20/20 | 20/20 | 20/20 | 20/20 |
| FFT | 0.482718 | 20/20 | 20/20 | 20/20 | 19/20 | 20/20 |
| Approximate entropy | 0.953986 | 20/20 | 20/20 | 20/20 | 20/20 | 20/20 |
| Serial (P-value1) | 0.545685 | 20/20 | 20/20 | 20/20 | 20/20 | 20/20 |
| Serial (P-value2) | 0.547824 | 19/20 | 20/20 | 20/20 | 20/20 | 20/20 |

**Table 2** Comparison of reported RPUFs based on other emerging NVM technologies and our implementation

| | RRAM-PUF [13] | STT-PUF [14] | PCM-PUF [41] | DWM-PUF [42] | This work |
|---|---|---|---|---|---|
| Inter-HD ($\mu/\sigma$) | 0.4999/0.0435 | 0.499/– | 0.497/0.015 | 0.5036/0.0905 | 0.5082/0.1212 |
| Intra-HD | $\sim 0$ | – | $\sim 0$ | 0.005 | $\sim 0$ |
| Initialization-free | No | No | No | No | Yes |
| Reconfigurable HD ($\mu/\sigma$) | 0.4729/0.0607 | – | – | – | 0.4862/0.0330 |
| Energy/bit | 3.028 pJ | 14.31 pJ (write)/ 0.69 fJ (read) | – | – | 1.2 pJ (write)/ 9.4 fJ (read) |
| Area/bit ($\mu m^2$) | 2.86 | 0.43 | – | – | 1.39 (2T-1MTJ) |

### 3.4 Discussion

Next, we compare the demonstrated SOT based RPUF with conventional CMOS PUFs [3–5] and other state-of-the-art technologies [11–15]. The methods to implement CMOS PUFs include two major classifications: delay and memory. However, when compared to novel technology based PUFs, CMOS PUFs are suffering from large area overhead, and delay-based PUFs, including Arbiter PUFs [3], Glitch PUFs [4], and Ring Oscillator (RO) PUFs [5], cannot refresh their CRPs without additional hardware-induced entropy. On the other hand, memory-based CMOS PUFs, such as SRAM PUFs [37], Latch PUFs [38], and Flip-flop PUFs [39], can be reconfigured by means of setting memory cells in an unstable state. However, the memory cells may fail to stabilize and remain stuck in the unstable state [40]. RPUFs can also be executed using emerging devices, such as PCM [11,41], RRAM [12,13], and STT-MRAM [14,15]. However, all of these novel PUFs must be initialized to high/low resistance states at the beginning of every reconfiguration cycle, resulting in high power consumption and low speed. Moreover, the read-out/digitalization methods are complicated and inefficient for above emerging memory based RPUFs. For example, PCM based RPUF [11] counts the number of programming pulses required to make the cell resistance converge to a predetermined target value, and RRAM based RPUF requires comparing the resistance of two devices to generate one bit. On the other hand, although the RPUF based on SOT induced stochastic domain wall (DW) motion has been experimentally demonstrated in micrometer scale recently [42], it requires initialization as well. More importantly, the variation of DW motion becomes negligible when scaling down due to the DW pinned sites (the main entropy source) decreasing rapidly, causing that the RPUF cannot produce security keys anymore. Table 2 summarizes the SOT-based RPUF's features, which are further compared to other NVM based RPUFs. Energy and area consumption of the proposed RPUF consisting of $15 \times 15$ devices are evaluated at the circuit level (Appendix F), considering that the Hall-bar geometry is improved to MTJ with the same size of 200 nm $\times$ 200 nm. Using transistor models of a 0.9 V/28 nm CMOS technology and a Verilog-A based compact model, the circuit was simulated into Cadence$^{TM}$ environment. The average write/read energy per bit and the area per bit are evaluated to be 1.2 pJ ($I_w = 5 \times 10^{12}$ A/m$^2$, 1 ns)/9.4 fJ and 1.39 $\mu m^2$, respectively.

## 4 Conclusion

Nanomagnets-based crypto primitives were reconfigured through magnetization switching by applying an in-plane current via SOT. To realize SOT-induced deterministic magnetization switching in the PMA

magnet, an external in-plane magnetic field is required to break the symmetry along the current direction. Without an external field, the magnetization of such a magnet would be stochastically switched. We have experimentally demonstrated a physical RPUF based on current induced stochastically switching in nanomagnets and verified its performance by investigating key security metrics. The results show near-ideal 50% uniqueness over a hundred reconfiguration cycles in a nanomagnet array, as well as low correlation coefficients between every two reconfiguration cycles. Our proposed RPUF scheme and proof-of-concept experiment show that reconfigurable random bits generation using current induced switching of nanomagnets is a promising approach for simple, highly reliable, and energy-efficient reconfigurable physical unclonable cryptographic primitives with a small footprint. It will open a new avenue for reconfigurable hardware security primitives beyond existing RPUFs.

**Acknowledgements** This work was funded by National Natural Science Foundation of China (Grant Nos. 61674062, 61904060, 61821003), in part by Fundamental Research Funds for the Central Universities (Grant No. HUST: 2018KFYXKJC019), and in part by Research Project of Wuhan Science and Technology Bureau (Grant No. 2019010701011394).

**Supporting information** Appendixes A–F. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

**References**

1 Pappu R, Recht R, Taylor J, et al. Physical one-way functions. Science, 2002, 297: 2026–2030
2 Gassend B, Clarke D E, Dijk M V, et al. Silicon physical random functions. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, 2002. 148–160
3 Gassend B, Clarke D, van Dijk M, et al. Delay-based circuit authentication and applications. In: Proceedings of ACM Symposium on Applied Computing, Melbourne, 2003. 294–301
4 Shimizu K, Suzuki D, Kasuya T. Glitch PUF: extracting information from usually unwanted glitches. IEICE Trans Fundamentals, 2012, 95: 223–233
5 Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation. In: Proceedings of IEEE Design Automation Conference, San Diego, 2007. 9–14
6 Gao Y S, Ranasinghe D C, Al-Sarawi S F, et al. Memristive crypto primitive for building highly secure physical unclonable functions. Sci Rep, 2015, 5: 12785
7 Nili H, Adam G C, Hoskins B, et al. Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. Nat Electron, 2018, 1: 197–202
8 Rührmair U, Sehnke F, Sölter J, et al. Modeling attacks on physical unclonable functions. In: Proceedings of ACM Conference on Computer and Communications Security, Chicago, 2010. 237–249
9 Mahmoud A, Rührmair U, Majzoobi M, et al. Combined modeling and side channel attacks on strong PUFs. IACR Crypto ePrint Arch 2013, 632
10 Kursawe K, Sadeghi A R, Schellekens D, et al. Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage. In: Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust, Francisco, 2009. 22–29
11 Zhang L, Kong Z H, Chang C-H, et al. Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions. IEEE Trans Inform Forensic Secur, 2014, 9: 921–932
12 Gao Y, Ranasinghe D C. $R^3$PUF: a highly reliable memristive device based reconfigurable PUF. 2017. ArXiv:170207491
13 Pang Y, Gao B, Wu D, et al. 25.2 A reconfigurable RRAM physically unclonable function utilizing post-process randomness source with $< 6 \times 10^{-6}$ native bit error rate. In: Proceedings of IEEE International Solid-State Circuits Conference-(ISSCC), San Francisco, 2019. 402–404
14 Zhang L, Fong X Y, Chang C-H, et al. Highly reliable spin-transfer torque magnetic RAM-based physical unclonable function with multi-response-bits per cell. IEEE Trans Inform Forensic Secur, 2015, 10: 1630–1642
15 Vatajelu E I, Di Natale G, Prinetto P. Security primitives (PUF and TRNG) with STT-MRAM. In: Proceedings of IEEE 34th VLSI Test Symposium (VTS), Las Vegas, 2016. 1–4
16 Miron I M, Garello K, Gaudin G, et al. Perpendicular switching of a single ferromagnetic layer induced by in-plane current injection. Nature, 2011, 476: 189–193
17 Liu L, Pai C-F, Li Y, et al. Spin-torque switching with the giant spin hall effect of tantalum. Science, 2012, 336: 555–558
18 Qiu X, Narayanapillai K, Wu Y, et al. Spin-orbit-torque engineering via oxygen manipulation. Nat Nanotech, 2015, 10: 333–338
19 Li P, Liu T, Chang H, et al. Spin-orbit torque-assisted switching in magnetic insulator thin films with perpendicular magnetic anisotropy. Nat Commun, 2016, 7: 12688
20 Lin P H, Yang B Y, Tsai M H, et al. Manipulating exchange bias by spin-orbit torque. Nat Mater, 2019, 18: 335–341
21 Liu L, Qin Q, Lin W, et al. Current-induced magnetization switching in all-oxide heterostructures. Nat Nanotechnol, 2019, 14: 939–944
22 Zhu D, Zhao W. Threshold current density for perpendicular magnetization switching through spin-orbit torque. Phys Rev Appl, 2020, 13: 044078
23 Peng S, Zhu D, Li W, et al. Exchange bias switching in an antiferromagnet/ferromagnet bilayer driven by spin-orbit torque. Nat Electron, 2020, 3: 757–764
24 Wang M, Cai W, Zhu D, et al. Field-free switching of a perpendicular magnetic tunnel junction through the interplay of spin-orbit and spin-transfer torques. Nat Electron, 2018, 1: 582–588
25 Chen H, Zhang S, Xu N, et al. Binary and ternary true random number generators based on spin orbit torque. In: Proceedings of IEEE International Electron Devices Meeting (IEDM), San Francisco, 2018. 31–34
26 Finocchio G, Moriyama T, de Rose R, et al. Spin-orbit torque based physical unclonable function. J Appl Phys, 2020, 128: 033904

27 Ikeda S, Miura K, Yamamoto H, et al. A perpendicular-anisotropy CoFeB-MgO magnetic tunnel junction. Nat Mater, 2010, 9: 721–724

28 Honjo H, Nguyen T, Watanabe T, et al. First demonstration of field-free SOT-MRAM with 0.35 ns write speed and 70 thermal stability under 400°C thermal tolerance by canted SOT structure and its advanced patterning/SOT channel technology. In: Proceedings of IEEE International Electron Devices Meeting (IEDM), San Francisco, 2019. 21–24

29 Garello K, Yasin F, Couet S, et al. SOT-MRAM 300 mm integration for low power and ultrafast embedded memories. In: Proceedings of IEEE Symposium on VLSI Circuits, Honolulu, 2018. 81–82

30 Yu G, Upadhyaya P, Fan Y, et al. Switching of perpendicular magnetization by spin-orbit torques in the absence of external magnetic fields. Nat Nanotech, 2014, 9: 548–554

31 You L, Lee O J, Bhowmik D, et al. Switching of perpendicularly polarized nanomagnets with spin orbit torque without an external magnetic field by engineering a tilted anisotropy. Proc Natl Acad Sci USA, 2015, 112: 10310–10315

32 Sengupta A, Parsa M, Han B, et al. Probabilistic deep spiking neural systems enabled by magnetic tunnel junction. IEEE Trans Electron Dev, 2016, 63: 2963–2970

33 Zand R, Camsari K Y, Pyle S D, et al. Low-energy deep belief networks using intrinsic sigmoidal spintronic-based probabilistic neurons. In: Proceedings of the 2018 on Great Lakes Symposium on VLSI, Chicago, 2018. 15–20

34 Cai J, Fang B, Zhang L, et al. Voltage-controlled spintronic stochastic neuron based on a magnetic tunnel junction. Phys Rev Appl, 2019, 11: 034015

35 Jaiswal A, Agrawal A, Chakraborty I, et al. On robustness of spin-orbit-torque based stochastic sigmoid neurons for spiking neural networks. In: Proceedings of International Joint Conference on Neural Networks (IJCNN), Budapest, 2019. 1–6

36 Jefremow M, Kern T, Allers W, et al. Time-differential sense amplifier for sub-80 mV bitline voltage embedded STT-MRAM in 40 nm CMOS. In: Proceedings of IEEE International Solid-State Circuits Conference Digest of Technical Papers, San Francisco, 2013. 216–217

37 Holcomb D E, Burleson W P, Fu K. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In: Proceedings of the Conference on RFID Security, 2007

38 Su Y, Holleman J, Otis B. A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations. In: Proceedings of IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), San Francisco, 2007. 406–611

39 Maes R, Tuyls P, Verbauwhede I. Intrinsic PUFs from flip-flops on reconfigurable devices. In: Proceedings of the 3rd Benelux Workshop on Information and System Security (WISSec 2008), 2008

40 Adames I A B, Das J, Bhanja S. Survey of emerging technology based physical unclonable funtions. In: Proceedings of International Great Lakes Symposium on VLSI (GLSVLSI), Boston, 2016. 317–322

41 Piccinini E, Rudan M, Brunetti R. Implementing physical unclonable functions using PCM arrays. In: Proceedings of International Conference on Simulation of Semiconductor Processes and Devices (SISPAD), Kamakura, 2017. 269–272

42 Zhang J, Guo Z, Zhang S, et al. Spin-orbit torque-based reconfigurable physically unclonable functions. Appl Phys Lett, 2020, 116: 192406