(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 February 2016 (04.02.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/018503 A1

(51) International Patent Classification:
G11C 16/04 (2006.01)

(21) International Application Number:
PCT/US2015/032914

(22) International Filing Date:
28 May 2015 (28.05.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/030,914 30 July 2014 (30.07.2014) US

(71) Applicant: **UNIVERSITY OF SOUTH FLORIDA** [US/US]; 3802 Spectrum Blvd., Suite 100, Tampa, FL 33612 (US).

(72) Inventors: **DAS, Jayita**; 6923 NE Ronler Way, Apt. 2226, Hillsboro, OR 97124 (US). **SCOTT, Kevin, P.**; 4030 Sparrow Hawk Rd., Melbourne, FL 32934 (US). **BURGETT, Drew, H.**; P.O. Box 1890, High Springs, FL 32655 (US). **RAJARAM, Srinath**; 2020 S Luxury Ln, Apt D107, Meridian, ID 83642 (US). **BHANJA, Sanjukta**; 8343 Golden Prairie Dr., Tampa, FL 33647 (US).

(74) Agents: **PERILLA, Jason, M.** et al.; Thomas I Horstemeyer, LLP, 400 Interstate North Parkway, Suite 1500, Atlanta, GA 30339 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,

[Continued on next page]

(54) Title: MAGNETIC MEMORY PHYSICALLY UNCLONABLE FUNCTIONS

(57) Abstract: A magnetic random access memory (MRAM) physically unclonable function (PUF) device that uses the geometric variations in magnetic memory cells to generate a random PUF response is described herein. Within the MRAM, one or more magnetic memory cells can be used for the PUF. The PUF response is generated by destabilizing the one or more magnetic memory cells and then allowing them to relax. The MRAM PUF has also a relatively small footprint among all other silicon PUFs. Timing and control signals for the MRAM PUF are also described along with power and delay characteristics for use with with field and spin transfer torque driven destabilization operations.

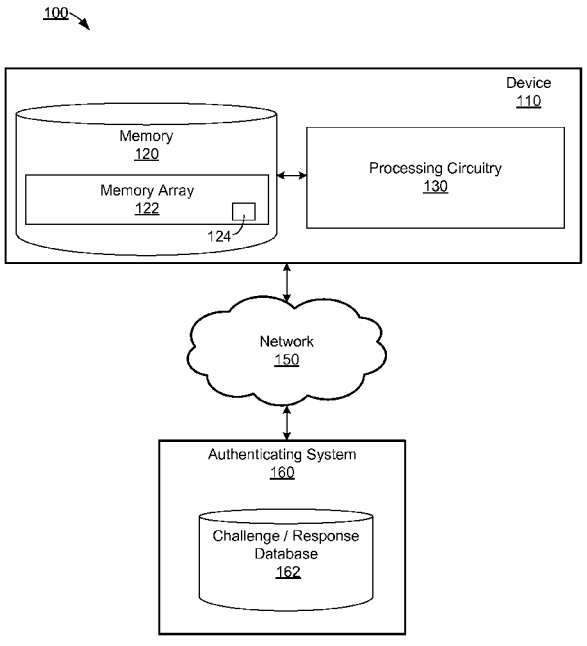

FIG. 1

WO 2016/018503 A1

TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

MAGNETIC MEMORY PHYSICALLY UNCLONABLE FUNCTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 62/030,914, filed July 30, 2014, the entire contents of which are hereby incorporated herein by reference.

GOVERNMENT LICENSE RIGHTS

[0002] This invention was made with government support under contract numbers 0639624 awarded by the National Science Foundation. The government has certain rights in the invention.

BACKGROUND

[0003] Physically unclonable functions (PUFs) rely upon a type of challenge-response authentication. A PUF may be embodied as a physical device or structure which is relatively easy to evaluate but difficult to predict. The response of a unique PUF device should be practically impossible to duplicate, even using the same process used to manufacture it. In this regard, a unique PUF device may be considered the hardware equivalent of a unique one-way function.

[0004] Rather than relying upon a single key, PUFs makes use of challenge-response authentication. When a stimulus is applied to the physical device or structure, it generates an unpredictable but repeatable response. The response may be due to the interaction of the stimulus with the physical microstructure of the device. In this context, the applied stimulus is called the challenge, and the reaction of the PUF to the stimulus is called the response. A challenge and its response together form a challenge-response pair. A

challenge-response pair, once known, can be used to verify or authenticate a device, for example, or for other purposes.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] For a more complete understanding of the embodiments described herein and the advantages thereof, reference is now made to the following description, in conjunction with the accompanying figures briefly described as follows:

[0006] FIG. 1 illustrates a system for device authentication according to various example embodiments described herein.

[0007] FIG. 2 illustrates a memory device including magnetic memory cells according to various example embodiments described herein.

[0008] FIGS. 3A-3C illustrate the structure and logic states of an example magnetic tunnel junction.

[0009] FIG. 4 illustrates the structure and logic states of an example MTJ cell in the memory device of FIG. 2 according to various example embodiments described herein.

[0010] FIG. 5 illustrates an example energy profile of a magnetic memory cell in which the cell is taken to a hard axis or maximum energy state.

[0011] FIG. 6 illustrates an example error rate for MTJ PUF cells against tilt angle in easy axis.

[0012] FIG. 7 illustrates a multilayer hysteresis plot of an MTJ cell according to various aspects of the embodiments described herein.

[0013] FIG. 8 illustrates a scanning electron microscope image of an array of MTJ PUF cells with variations in cell geometry, including a magnified 3 × 3 section of the array.

[0014] FIG. 9A illustrates a SEM image of an MTJ PUF cell from the array in FIG. 8 according to aspects of the embodiments described herein.

[0015] FIG. 9B illustrates a mask of the MTJ PUF cell in FIG. 9A.

[0016] FIG. 9C illustrates the initialization or destabilization of an MTJ PUF cell uniformly along the hard axis according to aspects of the embodiments described herein.

[0017] FIG. 9D illustrates the ground state of a settled MTJ PUF cell according to aspects of the embodiments described herein.

[0018] FIG. 10A illustrates error rate in PUF cells at different temperatures according to aspects of the embodiments described herein.

[0019] FIG. 10B illustrates error rate in PUF cells with thickness variation in the fixed layer according to aspects of the embodiments described herein.

[0020] FIG. 10C illustrates error rate in PUF cells at 300K for different thicknesses of the free layer according to aspects of the embodiments described herein.

[0021] FIG. 10D illustrates error rate in PUF cells at 300K for different cell areas with same 3:2 aspect ratio according to aspects of the embodiments described herein.

[0022] FIG. 10E illustrates error rate in PUF cells at 300K for different aspect ratios with same cell area according to aspects of the embodiments described herein.

[0023] FIG. 11 illustrates a process for generating a PUF response to an authentication challenge.

[0024] FIG. 12 illustrates timing signals which may be used in a memory device for the process of generating a PUF response to an authentication challenge.

[0025] The drawings illustrate only example embodiments and are therefore not to be considered limiting of the scope described herein, as other equally effective embodiments are within the scope and spirit of this disclosure. The elements and features shown in the drawings are not necessarily drawn to scale, emphasis instead being placed upon clearly illustrating the principles of the embodiments. Additionally, certain dimensions may be exaggerated to help visually convey certain principles. In the drawings, similar reference

numerals between figures designate like or corresponding, but not necessarily the same, elements.

DETAILED DESCRIPTION

[0026] As described above, PUFs rely upon a type of challenge-response authentication. When a stimulus is applied to a PUF device or structure, it generates an unpredictable but repeatable response. The response may be due to the interaction of the stimulus with the physical structure of the device. In this context, the applied stimulus is called the challenge, and the reaction of the PUF to the stimulus is called the response. A challenge and its response together form a challenge-response pair.

[0027] According to one definition for a PUF, (i) at the time of its creation, a PUF may be created without any user control over it; (ii) the PUF is unique and specific to every instance; and (iii) creating two PUF instances, *i.e.*, PUF_1 and PUF_2, that produce the same response to the same challenge is not feasible. As noted above, two terms are closely associated with PUF usage: i) challenge, which is an input $x_k \in X_P$ to the PUF, and ii) response, which is the PUF output y to the challenge. The challenge / response process may be called "evaluating" the PUF. There are two statistical parameters which determine the usability of a PUF class P, where $puf_i \in P$, including i) intra-distance D_{intra}, where the hamming distance or the fractional hamming distance between two random evaluations y_{j1} and y_{j2} of a single PUF instance puf_i with the same challenge $x_k \in X_P$, and ii) inter-distance, where D_{inter} is the hamming distance or the fractional hamming distance between the evaluations y_{j1} and y_{j2} of two different PUF instances puf_{i1} and puf_{i2}, $i_1 \neq i_2$ for the same challenge $x_k \in X_P$.

[0028] A PUF class P should display certain basic properties. Informal quantifiers such as "easy," "hard," "high," and "low" are typically used to define the following

properties: i) constructibility, where constructing a random PUF instance puf_i should be relatively easy; ii) evaluability, where evaluating the response of any puf_i to a random challenge $x_k \in X_P$ should be relatively easy; iii) reproducibility, where when evaluated multiple times, a PUF should generate the same response to the same challenge with a relatively high probability (*i.e.*, a PUF instance should have a low D_{intra}); and iv) uniqueness, where the response of two different PUF instances to the same challenge should be highly dissimilar (*i.e.*, a PUF class should have a high D_{inter}).

[0029] Among other devices, certain memory devices incorporate PUF features. The static RAM (SRAM) PUF is one example of a memory-based PUF. An SRAM PUF uses the power-up state of an SRAM cell to generate a PUF response. An SRAM cell may be composed of a cross-coupled inverter latch designed to achieve symmetry between inverter pairs. Variations in process technology, however, may result in device mismatches specific to every SRAM cell. These mismatches result in a random but preferred power-up state for every cell. Thus, using the mismatches, the power-up state in SRAM cells may be employed to build an SRAM PUF. The latch PUF is another example of a memory-based PUF. In a latch PUF, the mismatch between two cross-coupled NOR gates is used to generate a PUF response. Further, nanoscale PUFs based on memristive crossbars with uncontrollable variations in the thickness, area, and concentration of oxygen vacancies of memristive elements have been proposed.

[0030] According to the embodiments described herein, the application of PUF features in magnetic memory cells and arrays are described. A magnetoresistive random access memory (MRAM) is one example of device which incorporates magnetic memory cells. The high density, endurance, thermal robustness, and radiation hardness of MRAM makes it a potential candidate for a universal memory used across platforms. The growing

popularity of MRAM devices calls for a greater role of the technology beyond storage purposes. One such application is in the authentication of integrated circuits.

[0031] According to aspects of the embodiments, the geometric variations in magnetic memory cells, such as magnetic tunnel junction (MTJ) cells, are used to generate a random PUF response. The PUF response is generated by destabilizing one or more MTJ cells, allowing them to relax, and then reading their associated responses. The MRAM PUF generates very high entropy, a low D_{intra}, and a high D_{inter}. It has also a relatively small footprint among silicon PUFs. Timing and control signals for the MRAM PUF are also provided along with power and delays associated with field driven and STT driven destabilization operations.

[0032] Turning to the drawings, various aspects of the embodiments are described in further detail.

[0033] FIG. 1 illustrates a system 100 for device authentication according to various example embodiments described herein. The system 100 includes a device 110, a network 150, and an authenticating system 160. Among other elements, the device 110 includes a memory 120 device and processing circuitry 130. The memory 120 device includes a memory array 122 formed from any suitable type or types of memory cells. In one embodiment, the memory array 122 includes, at least in part, an array of magnetic memory cells, such as MTJ cells. At least a portion 124 of the memory array 122 includes magnetic memory cells reserved for PUF functions.

[0034] The device 110 can be embodied as any device that includes processing circuitry and memory, such as a television, computer, set-top box, appliance, cellular telephone, camera, or other computing device, without limitation. The processing circuitry 130 includes a processor or processing circuit embodied in any suitable form. For example, the processing circuitry 130 may be embodied as one or more discrete logic

circuits having logic gates for implementing various logic functions, application specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs), general purpose processors, or other circuits or circuitry, without limitation.

[0035] The network 150 can include one or more local interfaces, local networks, local area networks (LANs), wide area networks (WANs), intranets, extranets, the Internet, or other networks, regardless of whether composed of wired, wireless, cable, satellite, other types of networks, or any combinations thereof. The authenticating system 160 can communicate with the device 110 over the network 150 using any suitable communications protocol.

[0036] The authenticating system 160 may be embodied as any computing system and is configured to authenticate the device 110 by issuing a challenge to the device 110 over the network 150. Upon receipt of the challenge, the processing circuitry 130 of the device 110 presents the challenge to the memory 120 device. The memory 120 device, in turn, processes the challenge by accessing one or more cells in the portion 124 of the memory array 122. The memory 120 device then returns the response from the one or more cells to the processing circuitry 130, and the processing circuitry 130 returns the response to the authenticating system 160 over the network 150. Once the response is received at the authenticating system 160, the authenticating system 160 is configured to compare the response received from the device 110 to an expected response for the original challenge with reference to the challenge / response database 162.

[0037] If the response received from the device 110 matches with the expected response, then the authenticating system 160 authenticates the device 110. Otherwise, the authenticating system 160 cannot authenticate the device 110. In this way, the authenticating system 160 (or other system) can confirm the identity, operating parameters, manufacturer, or other characteristics of the memory device 120 and/or the

device 110. For example, as a measure of quality or integrity assessment, a company can verify that their products were assembled with memory devices manufactured by a certain manufacturer, by presenting challenges to the memory devices and interfacing with a challenge / response database of the manufacturer to compare the responses. In other cases, the memory 120 device may be locked or unlocked based on the authentication.

[0038] FIG. 2 illustrates a memory device 200 including magnetic memory cells according to various example embodiments described herein. In that it includes magnetic memory cells reserved for PUF functions, the memory device 200 in FIG. 2 is similar to the memory device 120 in FIG. 1. As shown, the memory device 200 includes a memory array 210, banks of access transistors 220, sense amplifiers 230, a column decoder 240, a bitline (BL) driver 242, a row decoder 250, a wordline (WL) and digitline (DL) driver 252, a data bus (DX) 260, an address bus (AX) 262, control signal inputs 264, and an encrypter 280. The column decoder 240 and the row decoder 250 may be referred to, collectively, as a decoder. Similarly, the BL driver 242 and the WL and DL driver 252 may be referred to, collectively, as a driver. The logical control signal inputs to the drivers 242 and 252 include read enable (RE), write enable (WE), and authentication enable (AE) inputs. It should be appreciated that the illustration of the memory device 200 in FIG. 2 is provided by way of example and for discussion of representative memory devices. The illustration is not intended to be limiting as to the type or scope of memory devices with which the concepts described herein may be applied.

[0039] The memory array 210 includes an array of magnetic memory cells, such as MTJ cells, one of which is designated in FIG. 2 as MTJ cell 212. As described in further detail below with reference to FIG. 4, the MTJ cell 212 includes a free layer in which the orientation of magnetization is alterable and a fixed layer in which the magnetization is

fixed in a particular direction. The free layer can be relied upon to store data by manipulating its orientation of magnetization.

[0040] In the architecture shown in FIG. 2, the column decoders 240 and row decoders 250 are configured to decode a combination of the WL, DL, and BL lines for access to one or more magnetic memory cells in the memory array 210, such as the MTJ cell 212, with reference to the input of a logical address value on the address bus 262. In that context, once a combination of the WL, DL, and BL lines are decoded and electrically actuated, the MTJ cell 212 may be accessed, written to, and read from through the banks of access transistors 220, the sense amplifiers 230, and the data bus 260, as would be understood by those having skill in the art. Further, using the RE, WE, and AE logical control signal inputs, the memory device 200 may be operated in read, write, and authenticate modes as described herein.

[0041] As with the other MTJ cells in the memory array 210, energy minimum configurations arising from shape anisotropy are used to store data values of "0" and "1" in the MTJ cell 212. The orientation of magnetization in the free layer of the MTJ cell 212 generally aligns along an axis referred to as the easy axis of the cell. External magnetic fields (*e.g.*, "H" in FIG. 2) generated through current (*e.g.*, "I" in FIG. 2) passing through the BL 270 and DL 271 can flip the orientation of the magnetization in the free layer of the MTJ cell 212 along the easy axis to either parallel or anti-parallel orientations with respect to the reference layer, depending on the desired logic state (*e.g.*, "0" or "1"). The magnitudes of the magnetic fields can be selected to be large enough so that the MTJ cell 212 switches its logic state, but low enough so that the other magnetic memory cells in the memory array 210 do not switch. Alternatively, logic values may be written to or read from the MTJ cell 212 using spin transfer torque generated by current flowing through the MTJ cell 212.

[0042] FIGS. 3A-3C illustrate various energy landscapes of an MTJ cell. For a rectangular or elliptical geometry of an MTJ cell, two stable configurations are symmetrically positioned across an energy barrier at room temperature, as illustrated in FIG. 2A. However, when process variations affect the geometry of MTJ cells, each gets a random and unique tilt in its energy barrier, such as the examples as illustrated in FIGS. 2B and 2C. As a result, with process variations, the point A in FIG. 2A shifts to a new random location A' unique to each MTJ cell (*e.g.*, as in FIGS. 2A and 2B). Therefore, with variations, each MTJ cell in a memory array develops a preferred ground state which can be relied upon to incorporate MTJ PUF cells into a memory device. As further described below, the differences in tilt angles among various MTJ cells in a memory array generally follow a Gaussian distribution.

[0043] Turning to FIG. 4, the structure and logic states of the example MTJ cell 212 in the memory device 200 of FIG. 2 are further illustrated. It should be appreciated that the illustration of the MTJ cell 212 in FIG. 4 is provided by way of example and for discussion of representative memory cells. The illustration is not intended to be limiting as to the type or scope of memory cells with which the concepts described herein may be applied. Apart from the top electrode 410 and the bottom electrode 460, the MTJ cell 212 includes three main layers, including a free single-domain ferromagnetic layer 420, an insulating tunneling barrier 430, and a fixed single-domain ferromagnetic layer 440. In some cells, as illustrated in FIG. 4, the magnetic domain of the fixed layer 440 can remain fixed through exchange coupling from a pinning layer 450.

[0044] In the MTJ cell 212, the magnetic domain of the free layer 420 can freely precess. In other words, the orientation of magnetization in the free layer 420 is not fixed and can assume two stable orientations, referenced by the arrows M1 and M2 in FIG. 4. On the other hand, the fixed layer 440 has a fixed orientation of magnetization referenced

by the arrow MF. The orientation of magnetization of the free layer 420 can be rotated in response to electrical currents applied to the top electrode 410 and the bottom electrode 460, for example, which may be embodied as BL and DL lines, respectively, based on the architecture of the surrounding array. As described above, a logic value may be written to or read from the MTJ cell 212 using magnetic fields generated by current in the top electrode 410 and the bottom electrode 460 or by spin transfer torque generated by current flowing through the MTJ cell 212.

[0045] The first logic state of the MTJ cell 40 is established when the orientation of magnetization of the free layer 420 is substantially aligned or parallel with that of the fixed layer 440. For example, when the orientation of magnetization of the free layer 420 is in the M1 direction, a logic "0" state is stored in the MTJ cell 40. Conversely, a second logic state is established when the orientation of magnetization of the free layer 420 is antiparallel with that of the fixed layer 440. Thus, when the orientation of magnetization of the free layer 420 is in the M2 direction, a logic "1" state is stored in the MTJ cell 40. It is noted that, when current is passed though the MTJ cell 40, the logic "0" and logic "1" states have different resistance values. These values can be measured by a sense amplifier and compared against a reference value. The difference in resistances is captured by the term magnetoresistance.

[0046] To use a magnetic memory cell as a PUF, the identification of unique, intrinsic process variations among MTJ cells is relied upon in the embodiments described herein. To further illustrate this concept, FIG. 5 illustrates an example energy profile of a magnetic memory cell in which the cell is taken to a hard axis or maximum energy state. That is, the effective fields acting on the cell at the time of release from the hard axis or energy maximum position is shown. It should be appreciated that, when an MTJ cell is released from its energy maximum state, the net force acting on it determines with a finite

probability the preferred ground state that it is inclined to settle into. This inclination of the cell for one state increases with the increase in the easy axis tilt angle θ of the cell. In other words, with an increase in the easy axis tilt angle θ, a greater consistency in cell behavior can be expected. As applied to PUFs, any behavior of a cell that differs from its consistent behavior may be considered likelihood or probability for error. Thus, with increased easy axis tilt angle θ in MTJ cells, the more suitable the cells are as PUFs.

[0047] It is also noted that, in a device that makes use of spin transfer torque (STT), spin torque can be used to destabilize the free layer of an MTJ cell to generate a PUF response. In this case, the magnetic relaxation in the cell after the release of the torque would be the same as for field driven destabilization. The preferred ground state for the cell would again be decided by its unique geometric variations. The response from a PUF cell using STT can be read out with the help of tunnel magnetoresistance (TMR).

[0048] FIG. 6 illustrates an example error rate at 300 degrees kelvin (K) for MTJ PUF cells against tilt angle in easy axis. The arrows in FIG. 6 are representative of the orthogonal requirements of intrinsic process variations in MTJ cells for use as MTJ memory cells and MTJ PUF cells. At $\theta = 0$, the cells have good geometry and display a near equal probability to settle for either of the ground states. Such cells are best suited for memory cells. As θ increases, the cells display a greater probability to settle for their preferred intrinsic ground state. These cells are preferable as PUF cells. From FIG. 6, it can be seen that a high tilt angle in the energy barrier of an MTJ cell may be related to a lower error rate during PUF evaluation. In one embodiment, for a PUF cell, a reasonable tilt angle may be selected between about $-3^\circ \geq \theta \geq 3^\circ$. In this context, the selection process for PUF cells may include a step of filtering out low error rate cells.

[0049] In an MTJ cell, the pinning layer typically couples to some extent with the fixed layer through a spacer, such as a Ruthenium spacer, and reduces the impact of the

fixed layer on the free layer. When determining an appropriate thickness of the fixed layer (d_f) and an appropriate thickness of the pinning layer (d_p) in an MTJ cell, it is noted that the coupling between the free and fixed layers should be kept as close as possible to zero. When kept close to zero, the free layer acts as a single layer nanomagnet, without impact from the fixed layer. This is an important factor for PUF evaluation, because any error rate in PUF evaluation attributed to the impact of the fixed layer on the free layer can be reduced as much as possible.

[0050] With further regard to the impact of the fixed layer on the free layer, FIG. 7 illustrates a multilayer hysteresis plot of an MTJ cell according to various aspects of the embodiments described herein. For $d_f/d_p = 1.1$, curves 702 and 704, symmetry in the loop indicates zero coupling between the free and the fixed layers of the MTJ cell. The other hysteresis loops, $d_f + \sigma$, curves 712 and 714, and $d_f - \sigma$, curves 722 and 724, are generated for thicknesses of the fixed layer with $\sigma = 9\%$ in the conservative range.

[0051] According to aspects of the embodiments, the behavior of a PUF cell may be defined by Equation 1 below:

$$\frac{dM}{dt} = -\gamma M \times H_{eff} + \alpha M \times \frac{dM}{dt}, \qquad (1)$$

where M is the single-domain magnetization vector of the cell, H_{eff} is the effective magnetization field on the cell generated from a combination of anisotropy (NM), external fields (H_{Zeeman}), and thermal effects (H_{therm}), given by $H_{eff} = NM + H_{Zeeman} + H_{therm}$.

[0052] In Equation 2 below, N is the demagnetization tensor, which takes into account the shape anisotropy of the cell. For an ellipsoid with axes (a > b > c), N is given by a diagonal matrix provided by Equation 2, where each term of the diagonal matrix is

defined by Equation 3. H_{therm} is given by Equation 4. The terms in Equations (1)-(4) are defined in Table 1.

$$N = \begin{bmatrix} N_a & 0 & 0 \\ 0 & N_b & 0 \\ 0 & 0 & N_c \end{bmatrix} \quad (2)$$

$$N_i = \frac{1}{2} abc \int_0^\infty \left[(i^2 + \eta) \sqrt{(a^2 + \eta)(b^2 + \eta)(c^2 + \eta)} \right]^{-1} d\eta \quad (3)$$

$$H_{therm} = \frac{1}{\sqrt{V \Delta T}} \sqrt{\frac{2 k_B T \alpha}{\mu_0 \gamma M_S}} g(t), \quad (4)$$

[0053] In Equation 4, $g(t)$ is a Gaussian distributed random vector.

Symbols	Meaning
γ	Gyromagnetic ratio
α	Damping constant
V	Volume of cell
ΔT	Integration time step
k_B	Boltzmann constant
T	Absolute temperature
μ_0	Permeability of free space
M_S	Saturation magnetization

Table 1

[0054] Depending on the underlying technology, PUF cells may be destabilized (*i.e.*, $M = M_s$) either by current generated magnetic field or current induced STT. Below, both techniques for destabilization are discussed in the general framework of an MRAM array.

[0055] As discussed in further detail below, by fabricating, simulating, and testing MTJ cells, certain properties and behaviors of the MTJ cells have been analyzed with an aim toward use as PUF cells. It is noted at the outset that, by placing MTJ cells relatively far apart in an MRAM array, memory designers may ensure zero or near zero neighbor interaction between cells. This may be an important factor for PUF evaluation as it ensures high entropy among PUF response bits. For example, through micromagnetic simulations, dipolar coupling was observed between 90 × 60 nm^2 cells spaced 20 nm

apart, while the lack of effective coupling (*i.e.*, zero or near zero coupling) was observed between 90 × 60 nm^2 cells spaced 250 nm apart. However, any suitable cell spacing may be used among the embodiments.

[0056] FIG. 8 illustrates a scanning electron microscope image of an array 800 of MTJ PUF cells with variations in cell geometry, including a magnified 3 × 3 section of the array 800. To verify MTJ PUF cell behavior, the cells in FIG. 8 were fabricated in a 10 × 20 array to observe geometric variation and experimentally characterize the tilt angle and preferred ground state of the cells. The dimensions of each of the PUF cells in FIG. 8 are about 90 × 60 × 18 nm^3 with a vertical and horizontal spacing of 250 nm. The array 800 was used to determine the randomness in cell geometry and guide simulations to calculate the reproducibility and uniqueness in MTJ PUF cells. The array 800 was fabricated using standard electron beam lithography process. A Hitachi® SU-70 retrofitted with a nanometer pattern generation system (NPGS) and operating at 30kV was used to expose patterns on an Si wafer with a single layer of 50nm polymethyl methacrylate (PMMA) resist. Permalloy was evaporated at 0.3 $Å s^{-1}$ using a Varian® model 980-2462 electron beam evaporator (EBE). A Digital Instruments 3100 scanning probe microscope was utilized in magnetic force microscopy (MFM) mode for evaluation of the MTJ PUF cells. For topological measurements of the cells, the SEM was used.

[0057] For the MTJ PUF cells in FIG. 8, external magnetic fields were relied upon to destabilize the cells. When destabilized, each cell occupies its corresponding hard axis or saturation magnetization state. When released from this state (*i.e.*, $H_{Zeeman} = 0$), the cells start to relax in order to settle to their preferred ground states. The magnetic relaxation in the cells follows Equation 1 and is independent of the underlying destabilizing technique. The effective field H_{eff} acting on the relaxing cell is given by Equation 6 below, where M_x

($< M_y$) is a cell-specific random vector arising from the geometric variations in the cells and holds the key to the preferred ground state for the cell.

$$H_{eff} = \begin{bmatrix} H_x \\ H_y \\ H_z \end{bmatrix} = \begin{bmatrix} N_a & 0 & 0 \\ 0 & N_b & 0 \\ 0 & 0 & N_c \end{bmatrix} \begin{bmatrix} M_x \\ M_y \\ 0 \end{bmatrix} + H_{therm} \quad (6)$$

[0058] An entropy density function was relied upon to calculate randomness in the response of the MTJ PUF cells in the array 800. First, the cells were destabilized using an external magnetic field and then released. The cells were then MFM imaged. A high $\rho(y^n)$ indicates a high randomness among PUF cells. For the array 800 in FIG. 8, a $\rho(y^n)$ of 0.9997 was obtained, as outlined below in Table 2.

PUFs	D_{intra}	D_{inter}	$\rho(y^n) \leq$	Area (μm^2)
SRAM	0.078	0.49	0.94	51.99
Latch	0.26	0.3	0.71	531.25
D F/F	0.19	0.39	0.81	765.63
Arbiter	0.07	0.46	0.5-0.9	690.56
Ring Osc	0.099	0.46	0.86	7774.2
MRAM	0.0225	0.47	0.99	5.5

Table 2

[0059] As for constructability, an MRAM PUF can rely upon the geometric variations in the MRAM cells. The metal lines in MRAM technology can be used to supply the required current for destabilizing the MTJ PUF cells when required for authentication. Thus, the integration of PUF features in MRAM devices does not require any significant processing steps beyond those currently used in conventional MRAM devices. Only certain hardware and current drivers beyond those currently found in conventional MRAM devices are needed to supply the destabilizing current.

[0060] Evaluating an MRAM PUF includes (i) destabilizing one or more MTJ PUF cells, (ii) releasing the cells, and, once the cells have relaxed and settled to their ground states, reading out their PUF responses using standard MRAM read techniques. In an

MRAM, the contents of a cell are read by sensing the differential voltage generated from the comparison between the cell resistance and a reference value.

[0061] The measure of reproducibility in a PUF is called the intra-distance D_{intra}. Stochastic Landau-Lifshitz–Gilbert (LLG) simulations were relied upon over the array 800 in FIG. 8 to evaluate D_{intra}. SEM images of fabricated cells were relied upon to generate masks in the LLG simulator. A total of 20 SEM images of cells were selected. FIG. 9A illustrates a SEM image of an MTJ PUF cell from the array 800 in FIG. 8A. The LLG mask of the MTJ PUF cell in FIG. 9A is illustrated in FIG. 9B. The masks were discretized into cubes of 3 nm sides. The region in the mask bounded by the cell periphery was filled with the same material used in the cell fabrication and the adjoining spaces were regarded as a vacuum to ensure that the simulations closely emulate cell behavior in free space. Stochastic LLG simulations were carried out at 300 degrees K with the easy axis of the cells oriented along the y-axis.

[0062] At the start of every simulation, the magnetic moment of each MTJ PUF cell was initialized or destabilized uniformly along the hard axis, as illustrated in FIG. 9C. The simulations were then run until the cell settled to its ground state, as illustrated in FIG. 9D. The procedures outlined among FIGS. 9A-D were repeated 40 times for the 20 selected MTJ PUF cells in FIG. 8. The direction that am MTJ PUF cell settled the majority of time was assumed to be its preferred settling state, and any inconsistency was regarded as error. Of the 20 cells measured, 16 were consistent in settling behavior. Of the 4 remaining, 3 showed some inconsistency in settling while 1 always remained stuck in the vortex state. After discarding the outlier cell, a total of 18 errors were recorded from 800 runs, yielding an average D_{intra} of 0.0225, as outlined in Table 2 above.

[0063] As for uniqueness, the inter-distance D_{inter} is the measure for uniqueness in the PUF instance. Through stochastic LLG simulations over three 4 x 5 subsets of fabricated

arrays, D_{inter} for an MRAM PUF was obtained. Masks for the cells were created in the same manner as the intra-distance simulations. The mask generation and simulation procedure was similar to the previous case. At the start of every simulation, the magnetic moments of every cell were initialized along the hard axis, and then released. Sufficient time was given to allow the cells to settle to their ground state. A 20-bit binary string obtained from reading the array in a raster fashion represented response from each array. The D_{inter} was calculated using the fractional hamming distance between each pairwise 20-bit response string. The values were then averaged to obtain an average D_{inter} of 0.47, as outlined in Table 2 above.

[0064] As for device size or area, an MRAM PUF has a significantly smaller footprint in comparison to other silicon PUFs. Table 2 above compares the area between different 64-bit PUFs. Generally, it is noted that the area overhead for the MJT PUF is minimal and can be divided into two categories: (i) current drivers to generate the required current for destabilizing the cells, and (ii) multiplexers to select between PUF and normal memory read/write voltage levels.

[0065] For the desired reproducibility in the MRAM PUF response, it is noted that MTJ PUF cells with tilt angles of about $-3^\circ \geq \theta \geq 3^\circ$ are preferred. A multiple evaluation step can be used to carry out this selection. Stochastic LLG simulations were performed over these specific cells ($-3^\circ \geq \theta \geq 3^\circ$) to analyze their robustness and suggest enhancements based on cell geometry. Each reported error rate E was obtained by calculating the normalized hamming distance over 100 simulations for each θ_i. The results will be symmetrical for $\theta \leq -3^\circ$. For a n-bit PUF, the error rate E is related to D_{intra} as $D_{intra} = \frac{1}{n}\sum_{i=1}^{n}\varepsilon_i$, where ε_i is the error of PUR i of n.

[0066] As for robustness against temperature, FIG. 10A illustrates error rate in MTJ PUF cells at different temperatures. With an increase of 50 degrees K over room temperature, a maximum increase in error rate of only 0.03 is observed at $\theta = 4^{\circ}$. On the other hand, the error rate decreases with decreasing temperature. Further, FIG. 10B illustrates error rate in MTJ PUF cells with thickness variation in fixed layer. The thickness variation was modeled with the help of a resultant coupling field on the free layer. In both cases, a cell size of 90 x 60 x 5 nm^3 was simulated. It is noted that variations in the fixed layer cause non-zero coupling on the free layer of the MTJs (*e.g.*, FIG. 7). This variation was emulated through a highly conservative coupling field of ±250 Oersted on the free layer. In FIG. 10B, it is clearly evident that the MRAM PUF is robust to the variations in the thicknesses of the fixed layer of the MTJs.

[0067] As to enhanced robustness with geometry, the goal is to identify different geometrical aspects of cells to increase the margin ($N_aM_x - H_{thermx}$) for the cells. This implies either (i) increasing N_a, which is a function of shape anisotropy (a/b) of the cell or (ii) decreasing σ_{Htherm}, which is a function of the overall volume ($V=abc$) of the cell (Equation 5). Increasing the volume at constant aspect ratio decreases the σ_{Htherm} term and therefore increases the ($N_aM_x–H_{thermx}$) margin. As to increasing the cell thickness at constant area, FIG. 10C illustrates error rate in MTJ PUF cells at 300 degrees K for different thicknesses of the free layer. A sharp fall in error rate by as high as 0.24 is seen at $\theta = 5^{\circ}$ when the thickness is increased from 2 nm to 5 nm. A considerable drop in error rate by 0.11 at $\theta = 5^{\circ}$ is also observed for thickness increase from 2 nm to 3 nm.

[0068] As to increasing the cell area at constant thickness, FIG. 10D illustrates error rate in PUF cells at 300 degrees K for different cell areas with same 3:2 aspect ratio. A maximum error reduction by 0.1 is obtained at $\theta = 3^{\circ}$, when the cell area is increased from

90 x 60 nm^2 to 120x80 nm^2. As to decreasing the aspect ratio at constant volume, this increases N_a while keeping σ_{Htherm} constant. However, as seen from FIG. 10E, this method is not very effective in enhancing the PUF robustness. Therefore, increasing the thickness by even 1 nm seems to be the most effective way to improve the robustness of MTJ PUF cells.

[0069] Table 3 summarizes the delay and current associated with the response generation and response read out phase of a STT-MRAM PUF clocked with field and STT current.

Response generation			
MRAM		STT-MRAM	
Delay (τ_D)	5ns	Delay	5ns
DL current (I_D)	4mA	SL current	170μA
WL voltage	0	WL voltage @ VDD=1V	1V
Avg. power @ VDD = 1V for row of x cells	4mW	Avg. power @ VDD = 1V for row of x cells	170x μW
Response Readout			
Delay (τ_X)	5ns	Delay	5ns
BL current	30μA	BL current	30μA

Table 3

[0070] FIG. 11 illustrates a process 1100 for generating a PUF response to an authentication challenge. Although the process 1100 is described below as being performed by the memory device 200 in FIG. 2, the process 1100 can be performed by other memory devices.

[0071] At reference numeral 1102, the process 1100 includes receiving an authentication challenge at the memory device 200 (FIG. 2). As one example, receiving the authentication challenge may include the memory device 200 receiving a logical address signal and a logical authentication enable signal. For additional example context, FIG. 12 illustrates timing signals used for the process of generating a PUF response to an authentication challenge are illustrated. Receipt of the logical address signal is shown at

reference numeral 1202, and receipt of the logical authentication enable signal is shown at reference numeral 1204.

[0072] The logical address signal can be associated with a certain PUF challenge, and the PUF challenge may be associated with one or more MTJ cells, such as the MTJ cell 212, in the memory device 200. In this context, it should be appreciated that, by incorporating PUF features, the memory device 200 can be capable of providing a unique response to any number of unique authentication challenges, where each authentication challenge is associated with a unique logical address signal. As further described below, because the memory device 200 decodes each unique logical address signal to access a particular MTJ cell or group of MTJ cells, each unique logical address signal is associated with a unique response to a unique authentication challenge.

[0073] At reference numeral 1104, the process 1100 includes the column decoder 240 and the row decoder 250 of the memory device 200 decoding a location of one or more MTJ cells associated with the PUF challenge in the memory array 210 based on the logical address signal received at reference numeral 1102. As part of the decoding, the column decoder 240 and the row decoder 250 identify which BL, WL, and DL lines should be actuated for access to the MTJ cell or cells.

[0074] At reference numeral 1106, the process 1100 includes destabilizing the MTJ cell or cells associated with the PUF challenge for a predetermined period of time. To destabilize the MTJ cell or cells, one or both of the drivers 242 and driver 252 supply a source current pulse of suitable magnitude and duration to take the MTJ cell or cells to their hard axis. Here, it is noted that the step of destabilizing at reference numeral 1106 does not occur during normal read and write operations of the memory array 210, as the write and read portions of the timing diagram in FIG. 12 show. Thus, it should be appreciated that the memory device 200 is configured to perform the destabilizing,

releasing, and reading at reference numerals 1104, 1106, and 1108 in response to the logical authentication enable signal received at reference numeral 1102.

[0075] In various embodiments, the destabilizing at reference numeral 1102 can be achieved through a current generated magnetic field or current induced STT, as described herein. For a current generated magnetic field, the DL driver 252 sources a current pulse of magnitude I_D for duration τ_D. The values of I_D and τ_D may vary depending upon various factors, such as the temperature of the memory array 210, the sizing of the MTJ cells, the thicknesses of one or more of the free, tunneling barrier, or fixed layers of the MTJ cells, or other physical or operating characteristics of the memory array 210. Generally, the value of I_D may be selected so as to ensure that the MTJ cells are is taken to a hard axis or maximum energy state, as described above with reference to FIG. 5, for example. One example of values of I_D and τ_D is provided above in Table 3. Table 3 also includes an example value for current induced STT. With reference to FIG. 12, destabilizing the MTJ cell or cells associated with the PUF challenge for a predetermined period of time τ_D is shown at reference number 1206.

[0076] Referring again to FIG. 11, at reference numeral 1108, the process 1100 includes releasing the one or more MTJ cells associated with the PUF challenge. For example, the releasing includes the DL driver 252 releasing the current pulse of magnitude I_D. At reference numeral 1110, the process 1100 includes reading the settling state of the one or more MTJ cells. For example, for each of the MTJ cells, a current is passed through the MTJ cell, and the sense amplifiers 230 sense a differential voltage across the MTJ cell. The differential voltage is representative of the magnetoresistance of the MTJ cell after destabilizing and settling. As described herein, the settling state magnetoresistance of an MTJ cell is relied upon for determining a unique response to the authentication challenge received at reference numeral 1102. To the extent that multiple

MTJ cells are accessed during an authentication challenge, the readings from the individual cells may be concatenated, aggregated, or assembled together in any suitable form as a single response to the authentication challenge.

[0077] According to one aspect of the embodiments, the reading at reference numeral 1110 occurs at a predetermined time τ_X after the releasing at reference numeral 1108, as noted at reference numeral 1208 in FIG. 12. The value of τ_X may vary depending upon various factors, such as the temperature of the memory array 210, the sizing of the MTJ cells, the thickness of one or more of the free, tunneling barrier, or fixed layers of the MTJ cells, or other physical or operating characteristics of the memory array 210. However, the value of τ_X is generally independent of how the MTJ cells associated with the PUF challenge were destabilized.

[0078] At reference numeral 1112, the process 1100 includes encrypting the settling state values of the one or more MTJ cells read at reference numeral 1110. For example, the encrypter 280 is configured to encrypt the settling state values received from the MTJ cells, however aggregated or assembled together, and encrypt the values into an encrypted response result. In some embodiments, the encrypting at reference numeral 1112 may be omitted from the process 1100.

[0079] At reference numeral 1114, the process 1100 includes providing a value representative of the settling state values of the MTJ cells read at reference numeral 1110 as a response to the authentication challenge received at reference numeral 1102. In embodiments where the settling state values are encrypted, the value provided at reference numeral 1114 may be encrypted. At this point, consistent with the description provided above with reference to FIG. 1, an authenticating system can compare the response to the authentication challenge with an expected response, to authenticate the memory device 200 or any other suitable purpose.

[0080] Although the flowchart or process diagram in FIG. 11 illustrates a specific order, it is noted that the order can differ from that which is depicted. For example, an order of execution of two or more blocks can be scrambled relative to the order shown. Also, two or more blocks shown in succession in FIG. 11 can be executed concurrently or with partial concurrence. Further, in some embodiments, one or more of the blocks shown in FIG. 11 can be skipped or omitted.

[0081] Although embodiments have been described herein in detail, the descriptions are by way of example. The features of the embodiments described herein are representative and, in alternative embodiments, certain features and elements may be added or omitted. Additionally, modifications to aspects of the embodiments described herein may be made by those skilled in the art without departing from the spirit and scope of the present invention defined in the following claims, the scope of which are to be accorded the broadest interpretation so as to encompass modifications and equivalent structures.

CLAIMS

At least the following is claimed:

1. A method of using a magnetic tunnel junction (MTJ) cell as a physically unclonable function (PUF), comprising:

destabilizing the MTJ cell for a predetermined period of time;

releasing the MTJ cell after the destabilizing;

reading a settling state of the MTJ cell; and

providing a value representative of the settling state as a response of the PUF.

2. The method of claim 1, further comprising:

receiving a logical address signal associated with a PUF challenge;

based on the logical address signal, decoding a location of the MTJ cell in an array of MTJ cells;

receiving a logical authentication enable signal; and

performing the destabilizing, releasing, and reading in response to the logical authentication enable signal.

3. The method of claim 2, wherein the decoding comprises decoding at least a bitline and a wordline of the MTJ cell to access the MTJ cell in the array of MTJ cells based on the logical address signal.

4. The method of claim 1, wherein the destabilizing comprises taking the MTJ cell to a hard axis maximum energy state by applying a magnetic field to the MTJ

cell.

5. The method of claim 1, wherein the destabilizing comprises destabilizing the MTJ cell using a current pulse of predetermined magnitude and for the predetermined period of time through at least one of a bitline, a wordline, or a digitline associated with the MTJ cell.

6. The method of claim 1, wherein the reading comprises sensing a differential voltage across the MTJ cell at a predetermined period of time after the releasing to allow the MTJ cell to settle to a settling state.

7. The method of claim 6, wherein providing the value representative of the settling state comprises at least one of encoding or encrypting a value representative of the differential voltage as the value representative of the settling state.

8. The method of claim 1, wherein the MTJ cell comprises a plurality of MTJ cells, and providing a value representative of the settling state comprises providing a value representative of settling states of each of the plurality of MTJ cells.

9. A memory device including a physically unclonable function (PUF), comprising:

a memory array, the memory array including a magnetic tunnel junction (MTJ) cell selected for use as a PUF;

an address decoder configured to decode at least a bitline and a wordline to access the MTJ cell in the memory array based on a logical address signal associated

with the MTJ cell; and

driver circuitry configured, in response to a logical authentication enable signal, to:

destabilize the MTJ cell for a predetermined period of time;

release the MTJ cell;

read a settling state of the MTJ cell; and

provide, over a data bus, a logical value representative of the settling state as a response of the PUF.

10. The memory device of claim 9, wherein, to destabilize the MTJ cell, the driver circuitry is configured to take the MTJ cell to a hard axis maximum energy state by applying a magnetic field to the MTJ cell.

11. The memory device of claim 9, wherein, to destabilize the MTJ cell, the driver circuitry is configured to apply a current pulse of predetermined magnitude and for the predetermined period of time through at least one of the bitline, the wordline, or a digitline associated with the MTJ cell.

12. The memory device of claim 9, wherein, to read the settling state of the MTJ cell, the driver circuitry is configured to sense a differential voltage across the MTJ cell at a predetermined period of time after the releasing, to allow the MTJ cell to settle to a settling state.

13. The memory device of claim 9, wherein the MTJ cell comprises a plurality of MTJ cells, and the driver circuitry is configured to provide the value

representative of the settling state based on settling states of each of the plurality of MTJ cells.

14. A method of using a magnetic memory cell as a physically unclonable function (PUF), comprising:

destabilizing the magnetic memory cell for a predetermined period of time;

releasing the magnetic memory cell after the destabilizing;

reading a settling state of the magnetic memory cell at a predetermined period of time after the releasing; and

providing a value representative of the settling state as a response of the PUF.

15. The method of claim 14, further comprising:

receiving a logical address signal associated with a PUF challenge;

based on the logical address signal, decoding a location of the magnetic memory cell in an array of magnetic memory cells;

receiving a logical authentication enable signal; and

performing the destabilizing, releasing, and reading in response to the logical authentication enable signal.

16. The method of claim 15, wherein the decoding comprises decoding at least a bitline and a wordline of the magnetic memory cell to access the magnetic memory cell in the array of magnetic memory cells based on the logical address signal.

17. The method of claim 14, wherein the destabilizing comprises taking the magnetic memory cell to a hard axis maximum energy state by applying a magnetic field to the magnetic memory cell.

18. The method of claim 14, wherein the destabilizing comprises destabilizing the MTJ cell using a current pulse of predetermined magnitude and for the predetermined period of time through at least one of a bitline, a wordline, or a digitline associated with the MTJ cell.

19. The method of claim 14, wherein the reading comprises sensing a differential voltage across the MTJ cell after the releasing, to allow the MTJ cell to settle to a settling state.

20. The method of claim 19, wherein providing the value representative of the settling state at least one of encoding or encrypting a value representative of the differential voltage as the value representative of the settling state.

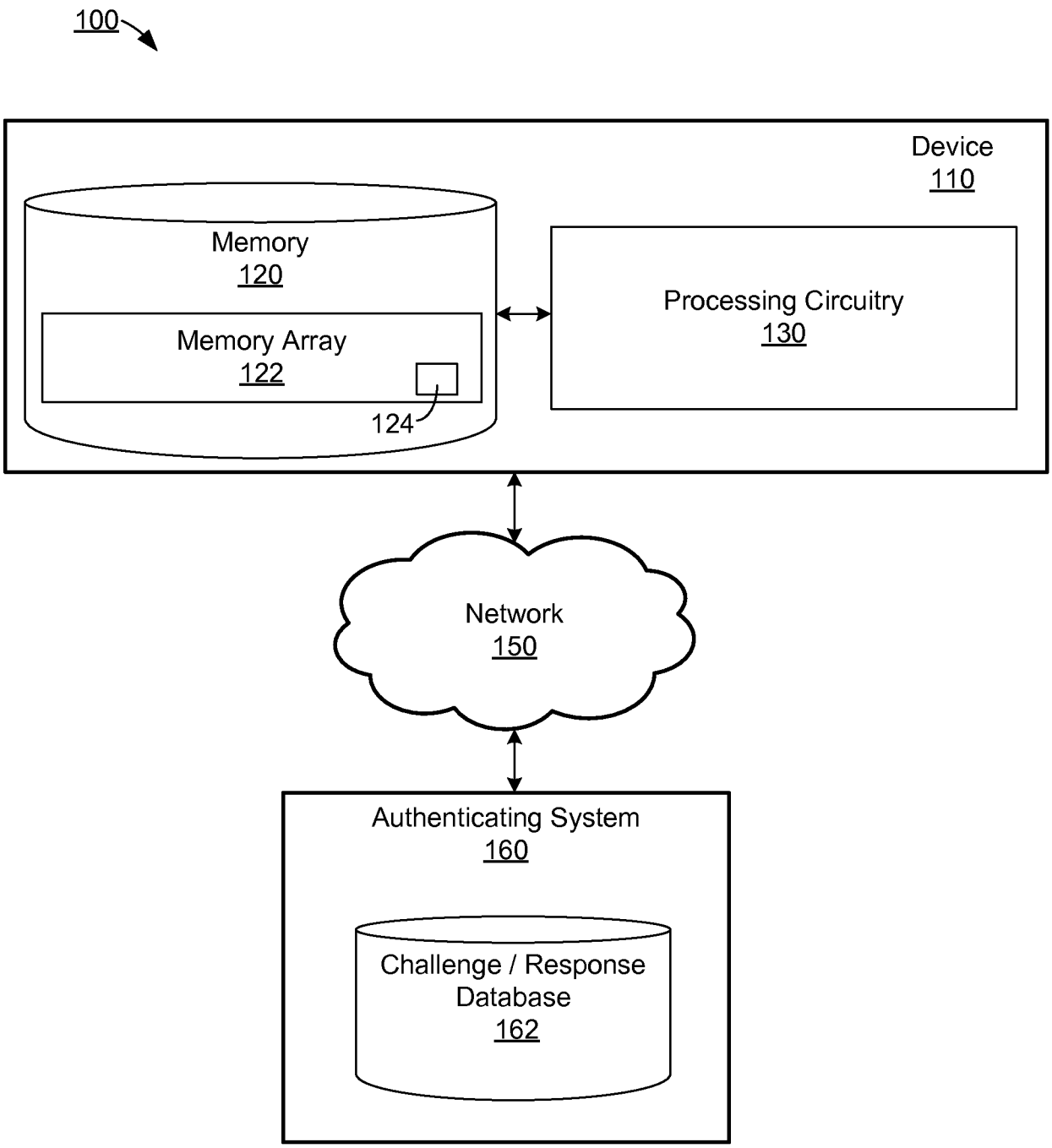
100
Device
110
Memory
120
Memory Array
122
124
Processing Circuitry
130
Network
150
Authenticating System
160
Challenge / Response
Database
162

FIG. 1

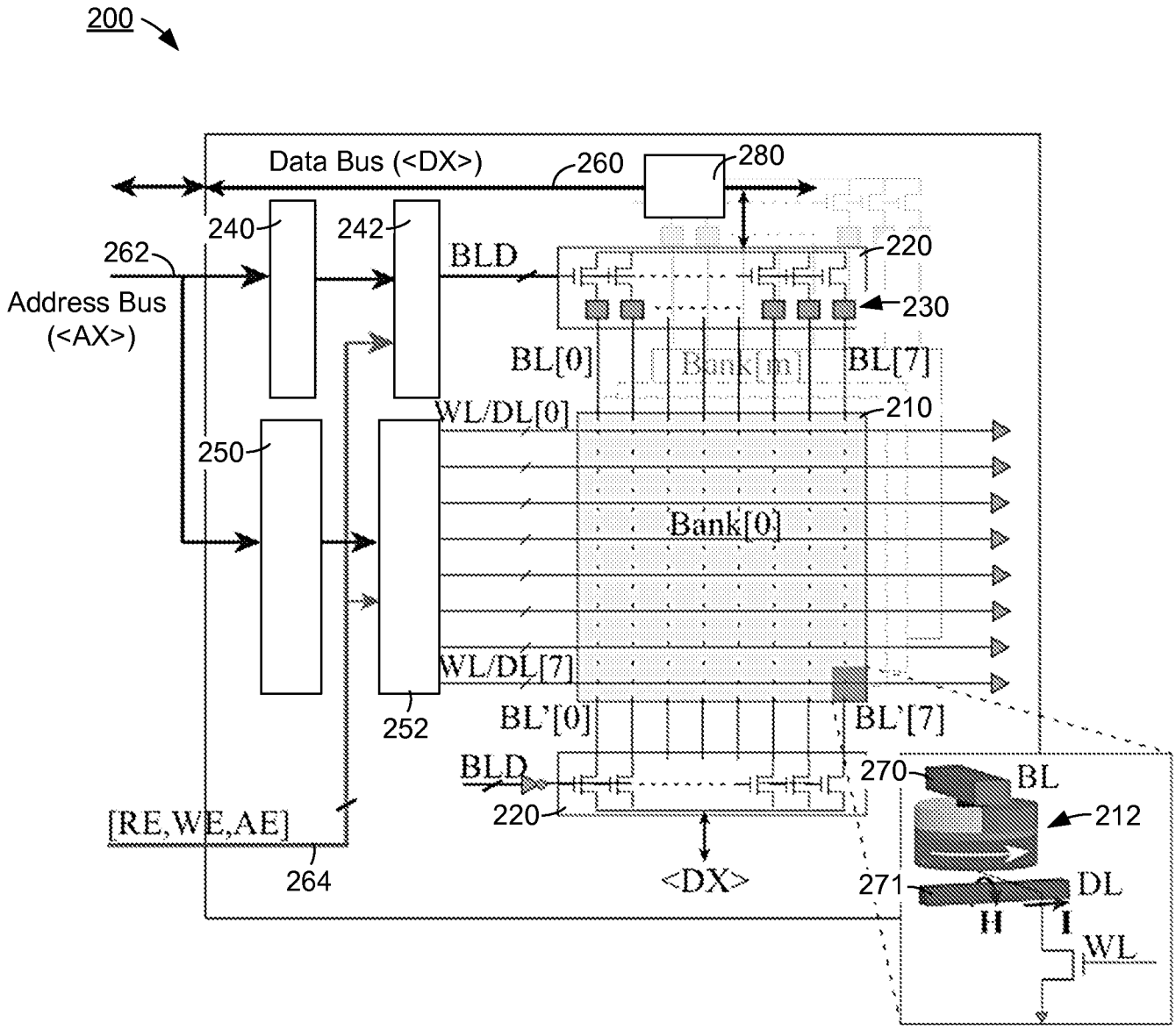
200
Data Bus (<DX>)
260
280
240
242
262
Address Bus
(<AX>)
BLD
220
230
BL[0]
Bank[m]
BL[7]
WL/DL[0]
210
250
Bank[0]
WL/DL[7]
BL'[0]
BL'[7]
252
BLD
270
BL
220
212
[RE,WE,AE]
<DX>
271
DL
264
H
I
WL

FIG. 2

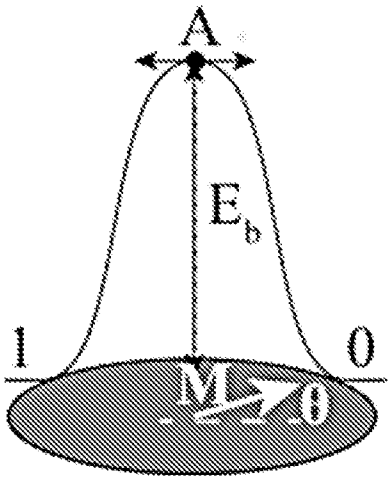

FIG. 3A

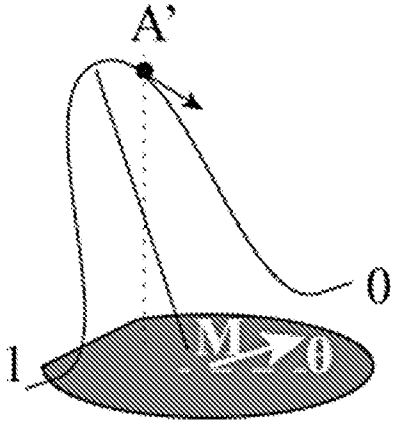

FIG. 3B

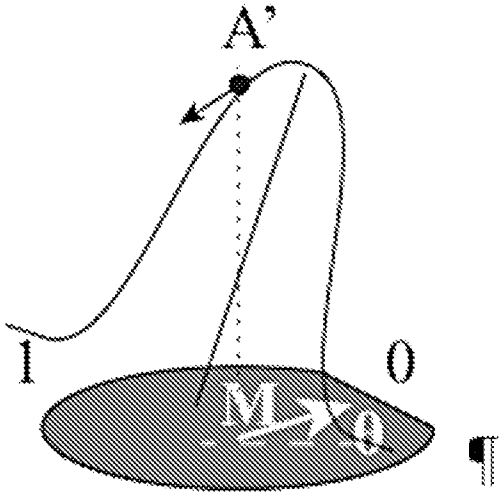

FIG. 3C

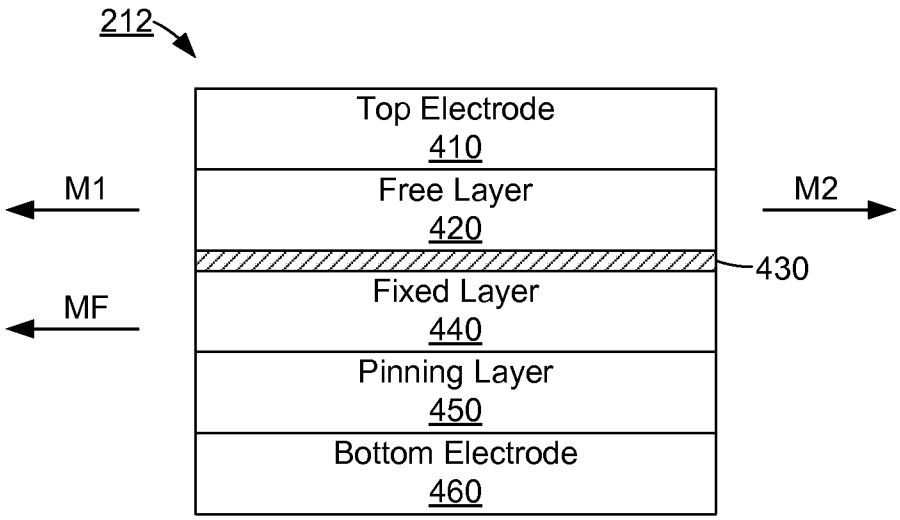
212
Top Electrode
410
M1
Free Layer
420
M2
430
MF
Fixed Layer
440
Pinning Layer
450
Bottom Electrode
460

FIG. 4

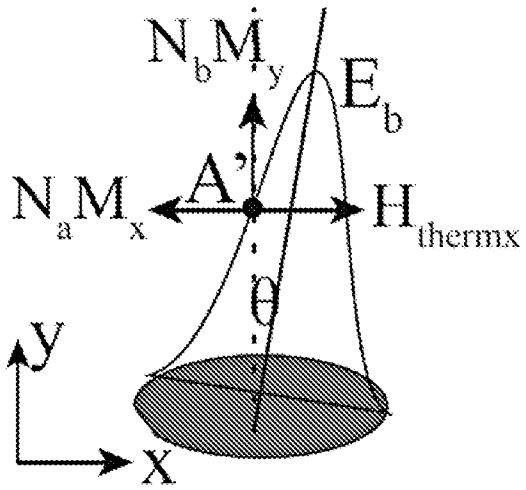
$N_b M_y$
E_b
A'
$N_a M_x$
H_{thermx}
θ
y
x

FIG. 5

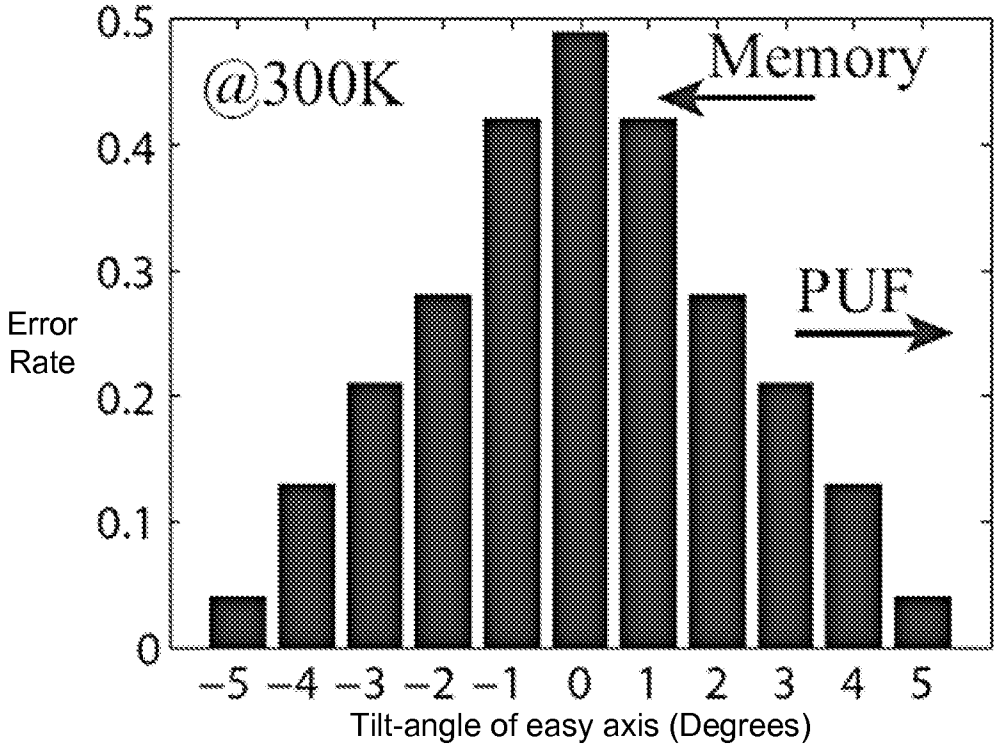
0.5
0.4
0.3
0.2
0.1
0
Error Rate
@300K
Memory
PUF
−5 −4 −3 −2 −1 0 1 2 3 4 5
Tilt-angle of easy axis (Degrees)

FIG. 6

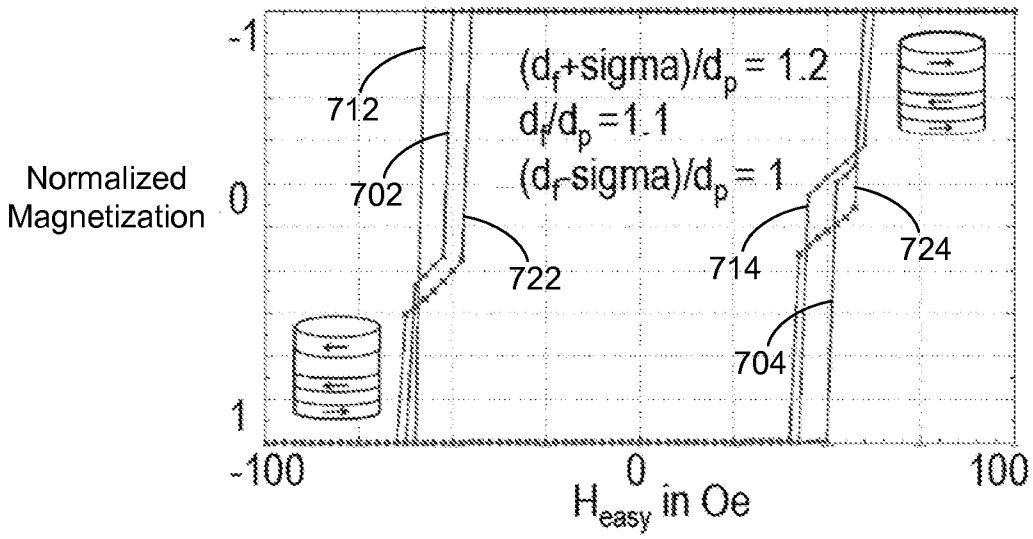
Normalized Magnetization
-1
0
1
-100
0
100
H_{easy} in Oe
$(d_f+sigma)/d_p = 1.2$
$d_f/d_p = 1.1$
$(d_f-sigma)/d_p = 1$
712
702
722
714
724
704

FIG. 7

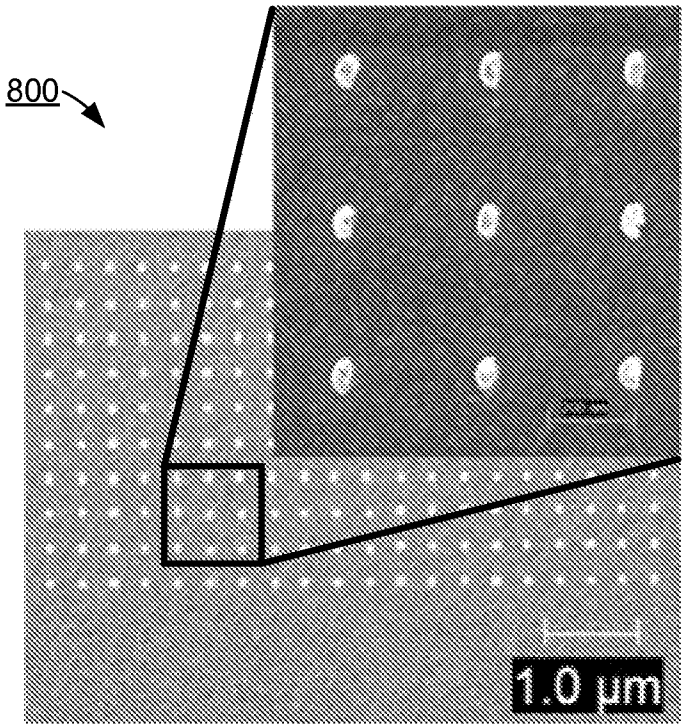

FIG. 8

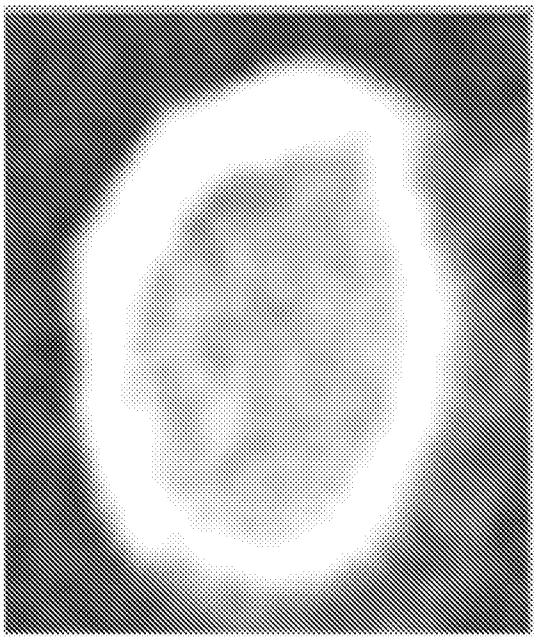

FIG. 9A

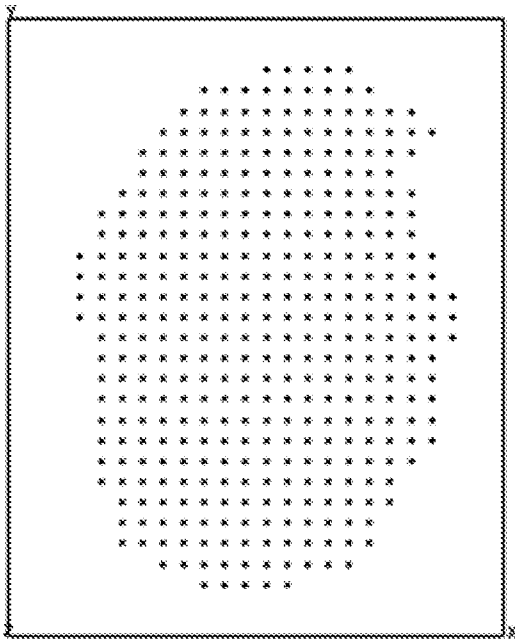

FIG. 9B

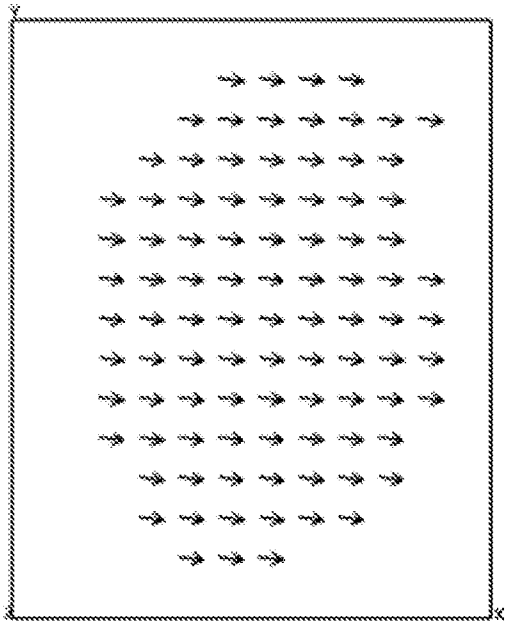

FIG. 9C

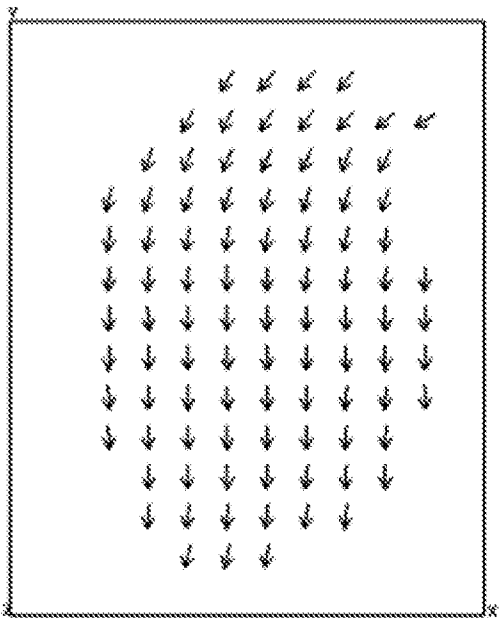

FIG. 9D

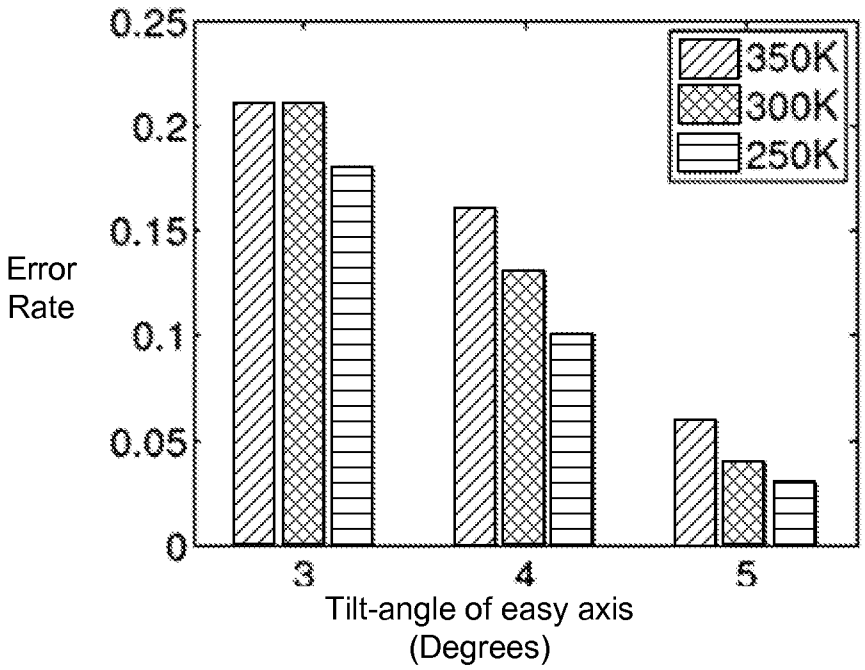

FIG. 10A

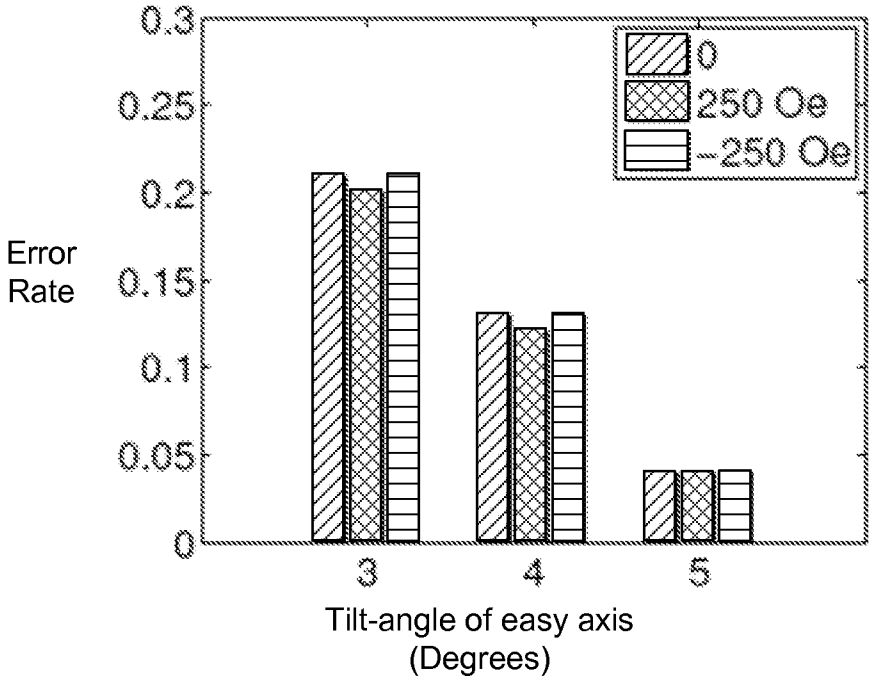

FIG. 10B

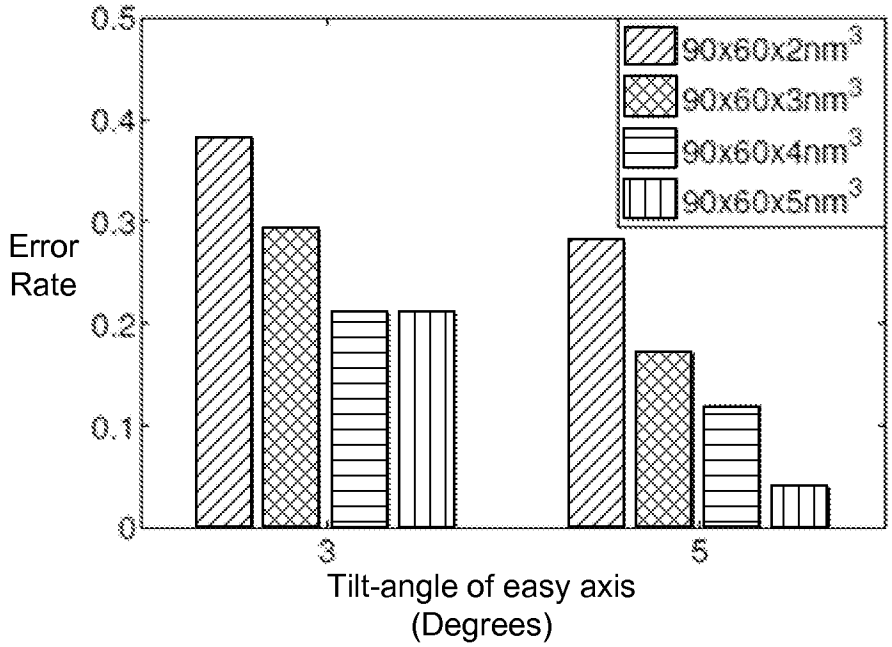

FIG. 10C

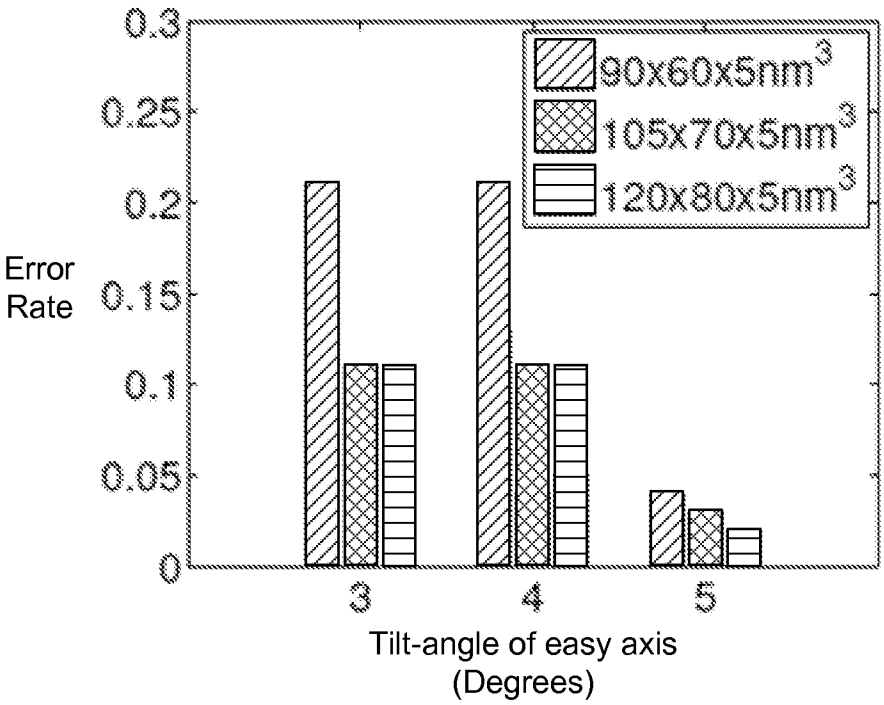

FIG. 10D

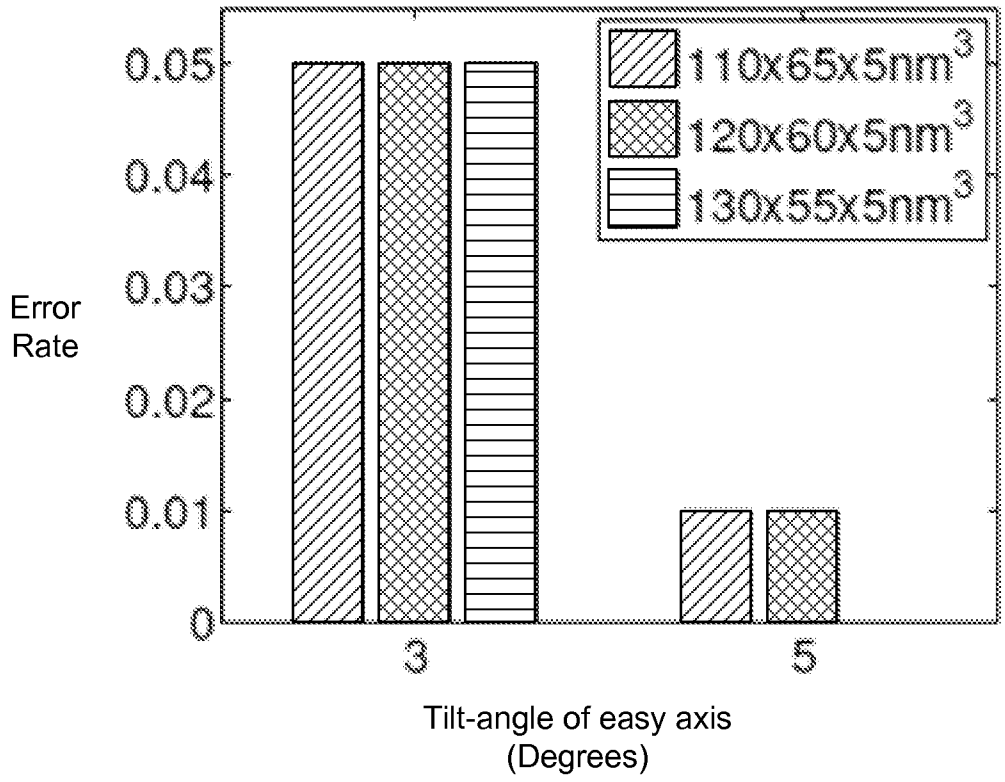
0.05
0.04
0.03
0.02
0.01
0
Error Rate
110x65x5nm3
120x60x5nm3
130x55x5nm3
3
5
Tilt-angle of easy axis (Degrees)

FIG. 10E

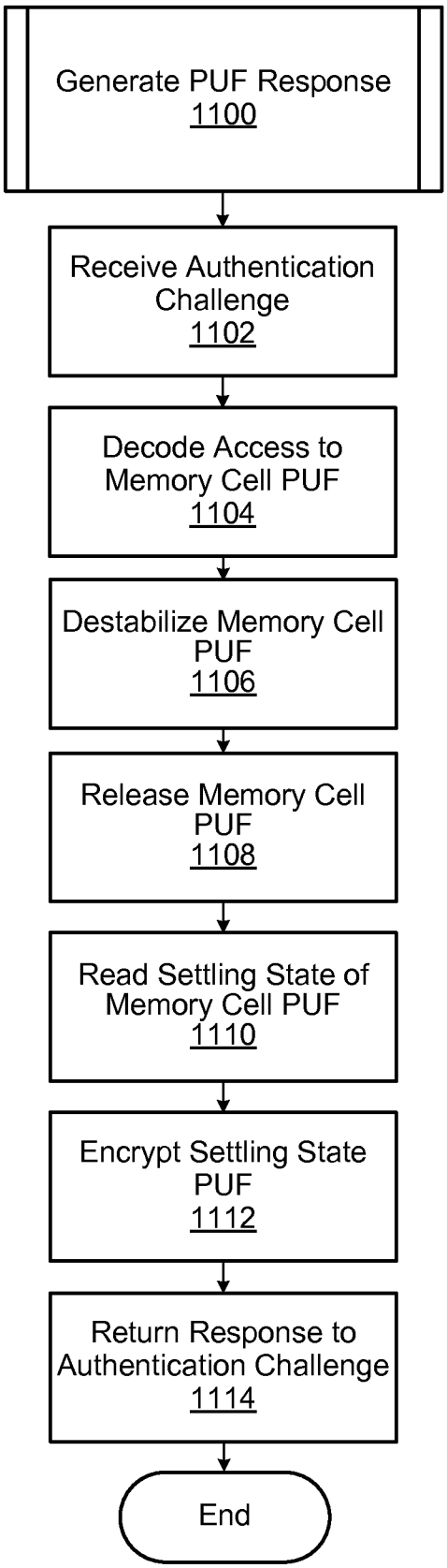
Generate PUF Response
1100
Receive Authentication Challenge
1102
Decode Access to Memory Cell PUF
1104
Destabilize Memory Cell PUF
1106
Release Memory Cell PUF
1108
Read Settling State of Memory Cell PUF
1110
Encrypt Settling State PUF
1112
Return Response to Authentication Challenge
1114
End

FIG. 11

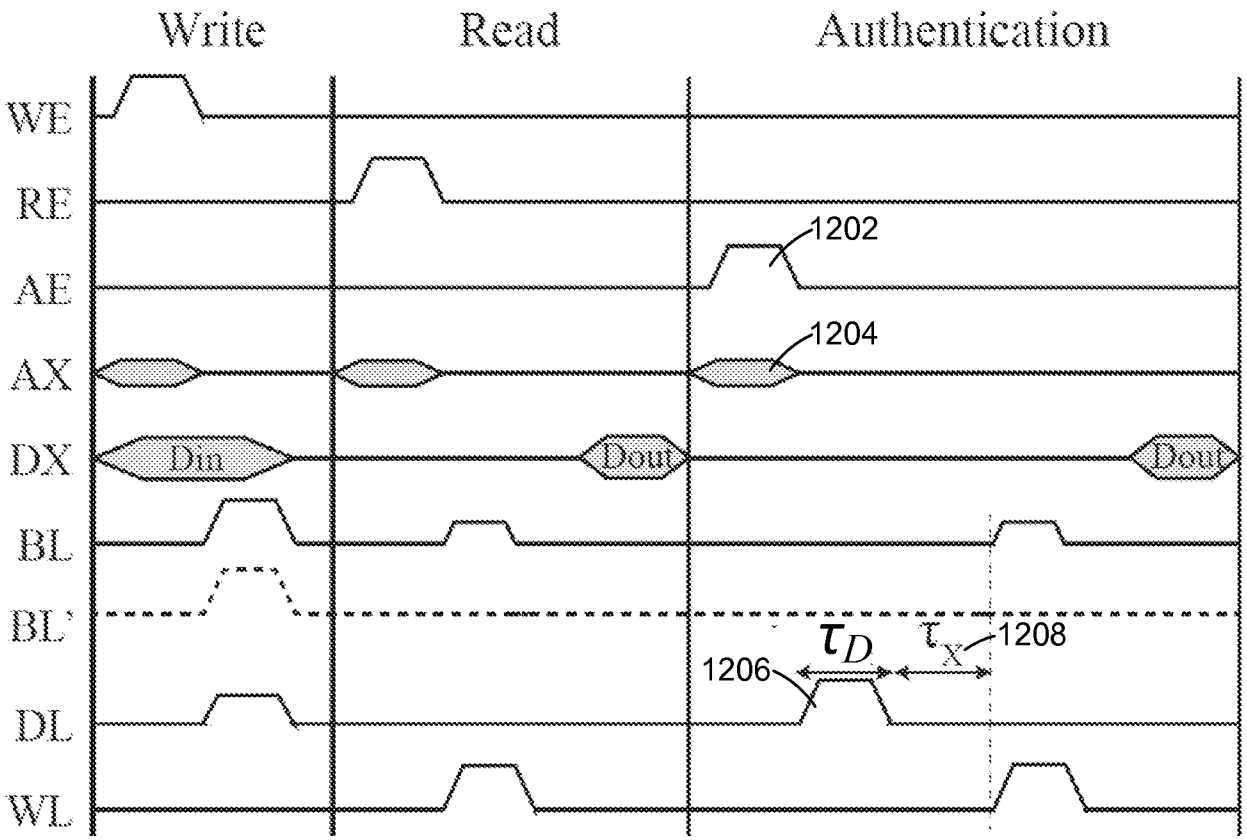
Write
Read
Authentication
WE
RE
AE
AX
DX
BL
BL'
DL
WL
Din
Dout
Dout
1202
1204
1206
1208
τ_D
τ_X

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 15/32914

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G11C 16/04 (2015.01)
CPC - G11C 16/10; H01L 27/115; G11C 16/12
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
CPC: G11C 16/10; H01L 27/115; G11C 16/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC: G11C 16/0475, G11C 16/0483; USPC: 365/185.28; 365/50; 365/129; IPC(8): G11C 16/04 (keyword limited - see search terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Google; Google Scholar
Terms: memory, storage, mram, magnetic, magnetoresistive, tunnel, junction, cell, array, physical, unclonable, puf, challenge, state, mode, steady, equilibrium, address, bit, line, word, stable, read, release, field, value, encryption, unpredictable, random.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/0067890 A1 (Zhu et al.) 06 March 2014 (06.03.2014), entire document, especially abstract, para [0019], [0020], [0025], [0026], [0038]	1-20
Y	US 2013/0194886 A1 (Schrijen et al.) 01 August 2013 (01.08.2013), entire document, especially abstract, para [0009], [0012], [0019], [0048], [0142], [0155], [0158], [0182], [0214].	1-20
Y	US 2012/0106235 A1 (Christensen et al.) 03 May 2012 (03.05.2012), entire document, especially abstract, para [0001], [0003], [0005], [0019], [0023].	3, 5, 9-13, 16, 18
Y	US 2013/0141137 A1 (Krutzik et al.) 06 June 2013 (06.06.2013), entire document, especially abstract, para [0008], [0013].	7, 20
A	US 2013/0254636 A1 (Kirkpatrick et al.) 26 September 2013 (26.09.2013), entire document.	1-20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 August 2015 (05.08.2015)	03 SEP 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)