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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 February 2015 (26.02.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/026838 A1

(51) International Patent Classification:
G06F 7/58 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/US2014/051718

(22) International Filing Date:
19 August 2014 (19.08.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/975,082 23 August 2013 (23.08.2013) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventors: **GUO, Xu**; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **JACOBSON, David M.**; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **YANG, Yafei**; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **DREW, Adam J.**; 5775 Morehouse Drive, San Digeo, California 92121-1714 (US). **ROSENBERG, Brain Marc**; 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(74) Agent: **LOZA, Julio**; Loza & Loza, LLP, 305 North Second Avenue #127, Upland, California 91786 (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, LT, 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, 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))*

Published:

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

(54) Title: APPLYING CIRCUIT DELAY-BASED PHYSICALLY UNCLONABLE FUNCTIONS (PUFS) FOR MASKING OPERATION OF MEMORY-BASED PUFS TO RESIST INVASIVE AND CLONE ATTACKS

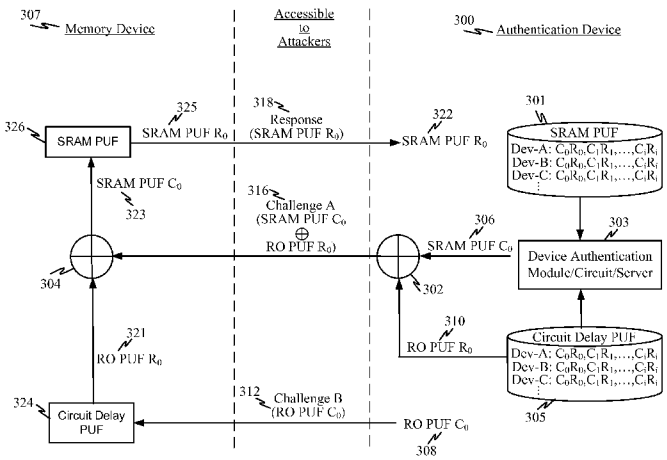


FIG. 3

(57) Abstract: One feature pertains to generating a unique identifier for an electronic device by combining static random access memory (SRAM) PUFs and circuit delay based PUFs (e.g., ring oscillator (RO) PUFs, arbiter PUFs, etc.). The circuit delay based PUFs may be used to conceal either a challenge to, and/or response from, the SRAM PUFs, thereby inhibiting an attacker from being able to clone a memory devices response.

WO 2015/026838 A1

APPLYING CIRCUIT DELAY-BASED PHYSICALLY UNCLONABLE FUNCTIONS (PUFS) FOR MASKING OPERATION OF MEMORY-BASED PUFS TO RESIST INVASIVE AND CLONE ATTACKS

BACKGROUND

Field

[0001] The present disclosure pertains to the use of physically unclonable functions (PUFs) to uniquely identify a memory device or device into which such memory device is integrated.

Background

[0002] Physical Unclonable functions (PUFs) provide a mechanism to uniquely identify a hardware device based on intrinsic variations of physical components. When multiple chips are manufactured, the complex semiconductor manufacturing process introduces slight variations that are beyond the control of the designer. For instance, even if two chips are manufactured from the same silicon wafer, electrical paths designed to be the same will probably differ in width by a few nanometers; microscopic differences in the surface of the silicon will induce almost trivial variations in the curvature of lines. As these unique characteristics are uncontrollable and inherent to the physical device, quantifying them can produce an intrinsic identifier. Several different types of PUFs have been proposed based on exploration and analysis of silicon variations in circuit delays, such as ring oscillator based PUFs, arbiter PUFs, and path delay analysis based PUFs.

[0003] One PUF makes use of the uninitialized power-up state of a static random access memory (SRAM) to generate an identifying "fingerprint". However, the SRAM PUFs are susceptible to cloning attacks.

[0004] Consequently, there is a need to improve the security of current SRAM PUF designs to resist cloning attacks and invasive attacks in general.

SUMMARY

[0005] An electronic device (e.g., processor, processing circuit, memory, programmable logic array, chip, semiconductor, memory, etc.) is provided which can be uniquely identified while being resistant to cloning attack. The electronic device may

include a plurality of memory cells within the electronic device serving as a first physically unclonable function (PUF). In one example, the first physically unclonable function may use the uninitialized memory cell states for one or more memory cells as a response to the challenge. Additionally, a plurality of circuit delay based paths within the electronic device may implement a second physically unclonable function. In one example, the plurality of circuit delay based paths may be ring oscillators and the second physically unclonable function may receive a challenge that selects two ring oscillators from the plurality of ring oscillators and responds with a frequency differential between the two ring oscillators.

[0006] A communication interface may serve to receive a challenge from an external server. A processing circuit may be coupled to the communication interface, the plurality of memory cells, and the plurality of circuit delay based paths, wherein the processing circuit is adapted to apply the challenge to the first physical unclonable function by using a first response from the second physically unclonable function to either: (a) mask/unmask a challenge input to the first physically unclonable function, (b) generate the challenge input to the first physical unclonable function, or (c) mask a response output from the first physically unclonable function. The communication interface may be adapted to send a second response from the first physically unclonable function to the external server. Additionally, the first response may be sent from the second physically unclonable function to the external server. In one example, the external server may include a first database of challenges and responses for the first physically unclonable function and a second database of challenges and responses for the second physically unclonable function, where the external server sends the challenge to the electronic device and authenticates or identifies the electronic device based on the second response.

[0007] In one example, the challenge may include a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function. In one implementation, the first challenge may be a challenge masked by an expected response to second challenge. In another implementation, the first challenge may be modified by the first response from the second physically unclonable function prior to processing by the first physically unclonable function.

[0008] In another example, the received challenge may be used by the second physically unclonable function to generate the first response which is then used as a

second challenge by the first physically unclonable function to generate the second response.

[0009] In yet another example, the challenge may include a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function, the second challenge is used by the second physically unclonable function to generate the first response which is used to mask the second response from the first physically unclonable function. The first response from the second physically unclonable function may be hashed to obtain an intermediate response. The second response may then be masked using the intermediate response.

[0010] In other instances, the challenge may be received as part of at least one of: an authentication process of the electronic device, an identification process of the electronic device, and/or a key generation process within the electronic device.

[0011] In some implementations, the electronic device may have previously received one or more challenges and provided (e.g., to a data collector) one or more corresponding responses during a pre-deployment or manufacturing phase.

[0012] Additionally, a pre-stored device identifier may be sent from the electronic device to the external server either: (a) before the challenge is received, or (b) concurrent with sending the second response, wherein the device identifier uniquely identifies the electronic device.

[0013] A data collector device is also provided that obtains (e.g., receives or assigns) a device identifier associated with an electronic device during a pre-deployment or manufacturing stage of the electronic device. The data collector device may then generate and send one or more challenges to the electronic device. As a result, the data collector device may receive one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device. The device identifier, challenges, and corresponding responses are stored for subsequent authentication of the electronic device. This process may be repeated for each of a plurality of electronic devices. Note that the challenges sent to the electronic devices may be the same for all devices, may be randomly generated for each electronic device, and/or may be a subset of possible challenges.

[0014] Similarly an authentication device is provided that authenticates an electronic device based on the responses from distinct types of physically unclonable

functions. The authentication device receives a device identifier associated with the electronic device. It then sends one or more challenges to the electronic device. In response, the authentication device receives one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device. The pre-stored responses specific to the electronic device may be identified using the electronic device identifier. The electronic device may then be authenticated by comparing the pre-stored responses and the received one or more responses for the electronic device. The challenges may be selected from a plurality of challenges for which responses where previously obtained from the electronic device. The pre-stored responses may have been obtained at a manufacturing stage or pre-deployment stage of the electronic device. The device identifier may be received prior to sending the one or more challenges. The device identifier may be received along with receiving the one or more responses.

[0015] The challenge may include a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function. The first challenge may be a challenge masked by an expected response to second challenge. The one or more challenges may include a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function, the one or more responses include a first response from the first physically unclonable function and a second response from the second physically unclonable function, the electronic device is successfully authenticated if the first response matches a first pre-stored response corresponding to the first challenge and the second response matches a second pre-stored response corresponding to the second challenge.

[0016] The one or more challenges include a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function, the one or more responses include a first response from the first physically unclonable function and a second response from the second physically unclonable function. Additionally, an intermediate challenge may be obtained by unmasking the first challenge with the second response. The received first response may be compared to the pre-stored response associated with the intermediate challenge.

[0017] In yet another example, the one or more challenges include a first challenge for a second physically unclonable function, the one or more responses include a first

response from the first physically unclonable function. An intermediate challenge may be obtained by retrieving a pre-stored intermediate response corresponding to the first challenge. The received first response may be compared to a pre-stored intermediate response corresponding to the intermediate challenge.

[0018] In yet another example, the one or more challenges include a first challenge for a first physically unclonble function and a second challenge for a second physically unclonable function, the one or more responses include a first response. An intermediate response may be obtained by unmasking the first response with a pre-stored second response corresponding to the second challenge. The intermediate response is compared to a pre-stored response associated with the first challenge.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] FIG. 1 is a block diagram illustrating an exemplary way of generating a unique mapping of responses for a memory device based on a SRAM PUF and a Circuit Delay Based PUF.

[0020] FIG. 2 is a block diagram illustrating an exemplary way of verifying or identifying a particular memory device using previously obtained characteristic responses for the memory device which combines a SRAM PUF and a Circuit Delay Based PUF.

[0021] FIG. 3 is a block diagram illustrates a first example of how an SRAM PUF and a Circuit Delay PUF may be combined to prevent an attacker from being able to clone a memory device.

[0022] FIG. 4 is a block diagram illustrates a second example of how a SRAM PUF and a circuit delay PUF may be combined to prevent an attacker from being able to clone a memory device.

[0023] FIG. 5 is a block diagram illustrates a third example of how an SRAM PUF and Circuit Delay PUF may be combined to prevent an attacker from being able to clone a memory device.

[0024] FIG. 6 is a block diagram illustrating a fourth example of how SRAM PUF and RO PUF may be combined to prevent an attacker from being able to clone a memory device.

[0025] FIG. 7 is a block diagram illustrating a data collector device according to one example.

[0026] FIG. 8 illustrates a method operational in a data collector device for obtaining characteristic information from an electronic device.

[0027] FIG. 9 is a block diagram illustrating an exemplary authentication device adapted to authenticate an electronic device based on responses from multiple physically unclonable functions within each electronic device.

[0028] FIG. 10 illustrates a method operational in an authentication device for authenticating an electronic device based on responses from a plurality of physically unclonable functions.

[0029] FIG. 11 is a block diagram illustrating an exemplary electronic device having multiple physically unclonable functions.

[0030] FIG. 12 illustrates a method operational in an electronic device for authenticating itself with an authentication device based on a response from a plurality of physically unclonable functions.

DETAILED DESCRIPTION

[0031] In the following description, specific details are given to provide a thorough understanding of the various aspects of the disclosure. However, it will be understood by one of ordinary skill in the art that the aspects may be practiced without these specific details. For example, circuits may be shown in block diagrams in order to avoid obscuring the aspects in unnecessary detail. In other instances, well-known circuits, structures and techniques may not be shown in detail in order not to obscure the aspects of the disclosure.

[0032] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any implementation or aspect described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other aspects of the disclosure. Likewise, the term "aspects" does not require that all aspects of the disclosure include the discussed feature, advantage or mode of operation.

Overview

[0033] One feature provides for generating a unique identifier by combining static random access memory (SRAM) PUFs and circuit delay based PUFs (e.g., ring

oscillator (RO) PUFs, arbiter PUFs, etc.). SRAM PUFs by themselves may be susceptible to cloning attacks that use failure analysis tools (e.g., a Focused Ion Beam (FIB)). Therefore, circuit delay based PUFs may be used to conceal either a challenge to, and/or response from, the SRAM PUFs, thereby inhibiting an attacker from being able to clone a memory device's response.

Combining SRAM and Circuit Delay Based Physically Unclonable Functions (PUFs)

[0034] A Physical Unclonable Function (PUF) is a challenge-response mechanism exploiting manufacturing process variations within circuits to obtain a unique identifier. In one example, the relation between a challenge and the corresponding response is determined by complex, statistical variations in logic components and interconnects in a circuit (e.g., integrated circuit). Two types of PUFs include, for example, an SRAM PUF and a circuit delay PUF (e.g., Ring Oscillator PUF).

[0035] An SRAM PUF exploits the uninitialized power-up state of a static random access memory (SRAM) to generate an identifying "fingerprint" for a memory device or an electronic device into which the memory device is integrated. While SRAM cell design is symmetrical, the manufacturing process deviations lead to a small asymmetry between SRAM cells, resulting in a preferred/biased state (0 or 1) during startup. This preference or bias of uninitialized SRAM cells may be used to uniquely identify a memory device.

[0036] However, recent advances in failure analysis attacks using a Focused Ion Beam (FIB) threaten the security of memory-based PUFs. A circuit edit attack could produce a hardware clone with identical SRAM PUF response to an original device.

[0037] Circuit delay based PUFs exploit systematic variations between oscillation circuits caused by fabrication/manufacturing imperfections. While fabrication/manufacturing processes seek to avoid such variations in circuit delay based PUFs, they are always present to some extent and are actually useful to identify devices/chips. In one example of a circuit delay based PUF, a plurality of ring oscillators may be concurrently used and the outputs of at least two ring oscillators are sent to one or more switches (multiplexers). The challenge may serve as input to the ring oscillators (e.g., challenge serves to select two ring oscillators) and the output from

two selected ring oscillators 204 are represented as a first frequency and a second frequency. Because of differences between the selected ring oscillators, their frequencies will be different (i.e., resulting in a frequency differential). The RO PUF output (response) is created by a pair-wise comparison of the ring oscillator frequencies (e.g., difference between first and second frequency).

[0038] However, implementing a sizable circuit delay based PUF takes up much needed space in an integrated circuit.

[0039] According to one feature, an SRAM PUF and a circuit delay based PUF are combined within an electronic device (e.g., memory device, semiconductor device, etc.) to enhance the security of the SRAM PUF.

[0040] FIG. 1 is a block diagram illustrating an exemplary way of generating a unique mapping of responses for a memory device based on a SRAM PUF and a Circuit Delay Based PUF, e.g., Ring Oscillator (RO) PUF. This block diagram illustrates the process of querying and collecting challenge/response characteristics for a memory device 102 (e.g., chip, semiconductor device, etc.) comprising an SRAM PUF 105 and a Circuit Delay PUF 122 (e.g., implemented as a ring oscillator bank).

[0041] In one example, the SRAM PUF may be implemented from all or parts of the SRAM cells of the memory device 102. In particular, the SRAM PUF 105 makes use of biasing in uninitialized memory cells 104 of the SRAM 106. For instance, during a manufacturing stage, the uninitialized SRAM 106 may be queried such that for each challenge 110 (e.g., memory address), a corresponding response 112 (e.g., logical 0 or 1) is obtained. For example, for each memory address within the SRAM 106 the uninitialized value/state for the memory cell 104 associated with that memory address is obtained. For a plurality of challenges 110, a plurality of responses 112 are obtained. In other approaches, just a subset of the memory addresses may be queried. In this manner, a mapping of uninitialized values to addresses is built for the SRAM 106 and may be stored in a database 114 (e.g., as challenges and corresponding responses). That is, a database of SRAM PUF challenges/responses 114 may be built for each memory device (chip), for example, during a manufacturing or quality control process. For instance, for a Device-A a first set of challenges/responses $[C_0R_0,C_1R_1,\ldots,C_iR_i]$ is obtained, for a Device-B a second set of challenges/responses $[C_0R_0,C_1R_1,\ldots,C_iR_i]$ is obtained, and for a Device-C a third set of challenges challenges/responses $[C_0R_0,C_1R_1,\ldots,C_iR_i]$ is obtained. Note that in some implementations, the challenges

$[C_0,C_1,\ldots,C_i]$ for all devices may be the same, but the responses would be different. In other implementations, the challenges $[C_0,C_1,\ldots,C_i]$ for each device may be randomly selected, so different devices receive different challenges.

[0042] In one example, the circuit delay PUF 120 may be implemented as a Ring Oscillator (RO) PUF 122 which makes use of a plurality of ring oscillators 123 and their frequency variations to generate a unique signature/response. For instance, for a given challenge 124 (e.g., selection of two ring oscillator inputs/outputs) a corresponding response (e.g., a frequency difference between the two selected ring oscillators) is obtained. In this manner, a circuit delay PUF database 128 of challenges and corresponding responses are obtained.

[0043] Because uninitialized memory cell states of the SRAM 106 are susceptible to being cloned by a focused ion beam (FIB) attack, using just the SRAM PUF 105 to provide a unique identifier for the memory device 102 is insecure. However, unlike the SRAM PUF 105, the circuit delay PUF 120 (e.g., RO PUF 122) is not susceptible to being cloned, but using a large number of RO PUFs is undesirable as they take up space on a chip. Consequently, a relatively small number of ring oscillators 123 may be combined with SRAM PUF 105 on a memory device 102 (e.g., chip, semiconductor, etc.) to thwart against cloning attacks on the SRAM PUF 102.

[0044] In order to associate the challenges/responses with each device, a device identifier 108 (e.g., serial number, ID number, etc.) may be stored at the device 102 and known to, or stored at, the databases 114 and 128. That is, the device identifier 108 for each memory device 102 may be stored and associated with the corresponding challenges and/or responses for that memory device 102.

[0045] FIG. 2 is a block diagram illustrating an exemplary way of verifying or identifying a particular memory device using previously obtained characteristic responses for the memory device which combines a SRAM PUF and a Circuit Delay Based PUF, e.g., Ring Oscillator (RO) PUF. During operation, a device verification module/circuit 202 (e.g., implemented by a verifier or authentication device/server) may query the memory device 102 with a challenge 204 to obtain a response 206 which can be verified using the combination of SRAM PUF database 114 and Circuit Delay PUF database 128. The response 206 may serve to verify the identity of the memory device or to authenticate the memory device 102. Note that this technique may also serve to generate a unique identifier/signature for the memory device.

[0046] Note that, in one example, the memory device 102 may provide its pre-stored/pre-assigned device identifier 108 to the device authentication module/circuit/server 202. The device authentication module/circuit/server 202 may then retrieve one or more challenges previously stored for that device identifier 108 and sends 204 them to the memory device 102. Alternatively, the device identifier 108 is provided by the electronic device along with any responses to challenges (e.g., where the same challenges are used for all electronic devices). Upon receipt of the response 206, the device authentication module/circuit/server 202 compares the received response 206 to the corresponding previously stored response(s) in the SRAM PUF 114 and Circuit Delay PUF 128 to ascertain whether there is a match.

[0047] During this verification stage, the challenge 204 and response 206 may be accessed or accessible to an attacker. Therefore, various features provide for protecting challenges 204 and/or responses 206 to/from the memory device 102 in order to inhibit an attacker from cloning the memory device 102.

[0048] In one example, the circuit delay PUF 120 (e.g., a delay-based PUF) is tamper-resistant. While a focused ion beam (FIB) attack may expose the responses of memory cells of the SRAM PUF 105, it does not provide information about the circuit delay PUF 120 (e.g., ring oscillators). In fact, the process used to clone/attack the memory device 102 may be sufficiently invasive that it may change the response of the circuit delay PUF 120 (e.g., ring oscillators), thereby exposing the attack and causing a failure of authentication/identification of the memory device 102.

[0049] There are various ways to combine the SRAM PUF 105 and circuit delay PUF 120 to inhibit an attacker from cloning of the memory device 102 even when the challenges 204 and responses 206 are accessible to the attacker.

Combining SRAM and RO Physically Unclonable Functions (PUFs) to Mask Challenges

[0050] FIG. 3 is a block diagram illustrates a first example of how an SRAM PUF 326 and a Circuit Delay PUF 324 may be combined to prevent an attacker from being able to clone a memory device 307. In this example, an authentication device 300 may include a device authentication module/circuit/server 303, a SRAM PUF database 301, and a Circuit Delay PUF database 305. The SRAM PUF database 301 may be generated for a memory cell region of the memory device 307 during manufacturing by,

for example, sending a plurality of challenges (e.g., memory addresses) to the memory cell region and obtaining corresponding responses (e.g., uninitialized memory cell states/values). Similarly, the Circuit Delay PUF database 305 may be generated for a plurality of ring oscillator within the memory device 307 during manufacturing by, for example, sending a plurality of challenges (e.g., selection of two ring oscillators) to the ring oscillators and obtaining a corresponding responses (e.g., frequency differential between two selected ring oscillators).

[0051] In this example, when the device authentication module/circuit/server 303 subsequently tries to authenticate the memory device 307, it sends a challenge (comprising Challenge A 316 and Challenge B 312) to the memory device 307. The challenge A 316 may comprise an SRAM PUF challenge C_0 306 and a RO PUF response R_0 310 that have been combined by a XOR operation 302. Because this Challenge A 316 may be accessible by an attacker, one aspect obscures the actual SRAM PUF challenge C_0 306 by masking (e.g., XORing) it with a corresponding RO PUF response R_0 310 (obtained from the Circuit Delay PUF database 305) to generate the transmitted (exposed) challenge A 316. Additionally, challenge B 312 which includes an RO PUF challenge C_0 308, corresponding to the RO PUF response R_0 310, is also sent from the authentication device 300 to the memory device 307.

[0052] At the memory device 307, the RO PUF challenge C_0 312 is used to generate a RO PUF response R_0 321 from the circuit delay PUF 324. Challenge A 316 is then XORed 304 with the RO PUF response R_0 321 to obtain the actual (clear) SRAM PUF challenge C_0 323 which may be used as the challenge for the SRAM PUF 326. The SRAM PUF 326 then generates a response SRAM PUF R_0 325. In this manner, a response from the memory device 307 to the authentication device 300 may include SRAM PUF response R_0 318.

[0053] At the authentication device 300, the received response SRAM PUF R_0 322 may be used to compare to the stored responses in the SRAM PUF database 301 and Circuit Delay PUF 305 and ascertain whether they match. Note that since the RO PUF response R_0 310 is already known or stored in the circuit delay PUF database 305, the authentication device 300 is able to use it to mask the SRAM PUC challenge C_0 306 with it.

[0054] FIG. 4 is a block diagram illustrates a second example of how a SRAM PUF 426 and a circuit delay PUF 424 may be combined to prevent an attacker from being

able to clone a memory device 407. Unlike the example in FIG. 3, in this example the SRAM PUF challenge C_0 406 and RO PUF challenge C_0 408 are sent on the clear from the device authentication module/circuit/server 403 to the memory device 407. In this example, an authentication device 400 may include a device authentication module/circuit/server 403, a SRAM PUF database 401, and a Circuit Delay PUF database 405. The SRAM PUF database 401 may be generated for a memory cell region of the memory device 407 during manufacturing by, for example, sending a plurality of challenges (e.g., memory addresses) to the memory cell region and obtaining corresponding responses (e.g., uninitialized memory cell states/values). Similarly, the Circuit Delay PUF database 405 may be generated for a plurality of ring oscillator within the memory device 407 during manufacturing by, for example, sending a plurality of challenges (e.g., selection of two ring oscillators) to the ring oscillators and obtaining a corresponding responses (e.g., frequency differential between two selected ring oscillators).

[0055] In this example, when the device authentication module/circuit/server 403 subsequently tries to authenticate the memory device 407, it sends a challenge (comprising Challenge A 416 and Challenge B 412) to the memory device 407. The challenge A 416 may comprise an SRAM PUF challenge C_0 406. The challenge B 412 includes an RO PUF challenge C_0 408, corresponding to the RO PUF response R_0 410, is also sent from the authentication device 400 to the memory device 407.

[0056] While challenge A 416 may be accessible by an attacker, one aspect modifies the actual SRAM PUF challenge C_0 406 to a modified SRAM PUF challenge C_0' 423 by a XORing operation 404 at the memory device 407. At the memory device 407, the RO PUF challenge C_0 412 is used to generate a RO PUF response R_0 421 from the circuit delay PUF 424. Challenge A 416 (i.e., SRAM PUF challenge C_0 406) is then XORed 404 with the RO PUF response R_0 421 to obtain a modified SRAM PUF challenge C_0' 423 which may be used as the challenge for the SRAM PUF 426. The SRAM PUF 426 then generates a SRAM PUF response R_0' 425 that is returned (as response A 418) to the authentication device 400. In this manner, a response from the memory device 407 to the authentication device 400 may include SRAM PUF response R_0 418.

[0057] In this approach, the RO PUF response R_0 421 is used to modify the actual challenge to the memory cell region 426. Because an attacker is unable to reproduce the

RO PUF response R_0 421, it does not know the modified SRAM PUF challenge C_0' 423 used to produce the response SRAM PUF response R_0' 425.

[0058] At the authentication device 400, the device authentication module/circuit/server 403 may verify the SRAM PUF response R_0' 422. This may be done, for example, by XORing 402 the SRAM PUF challenge C_0 406 with the RO PUF response R_0 420 (obtained from the circuit delay PUF database 405) to obtain a local version of the modified SRAM PUF challenge C_0' 427. The local version of the modified SRAM PUF challenge C_0' 427 can then be used to lookup the corresponding response in the SRAM PUF database 401 and compare that response to the received response SRAM PUF response R_0' 422.

[0059] FIG. 5 is a block diagram illustrates a third example of how an SRAM PUF 526 and Circuit Delay 524 PUF may be combined to prevent an attacker from being able to clone a memory device. In this example, a authentication device 500 may include a device authentication module/circuit/server 503, a SRAM PUF database 501, and a Circuit Delay PUF database 505. The SRAM PUF database 501 may be generated for a memory cell region of the memory device 507 during manufacturing by, for example, sending a plurality of challenges (e.g., memory addresses) to the memory cell region and obtaining corresponding responses (e.g., uninitialized memory cell states/values). Similarly, the Circuit Delay PUF database 505 may be generated for a plurality of ring oscillator within the memory device 507 during manufacturing by, for example, sending a plurality of challenges (e.g., selection of two ring oscillators) to the ring oscillators and obtaining a corresponding responses (e.g., frequency differential between two selected ring oscillators).

[0060] In this example, when the device authentication module/circuit/server 503 subsequently tries to authenticate the memory device 507, it sends a challenge 512, comprising an RO PUF challenge C_0 508, having a corresponding RO PUF response R_0.

[0061] While RO PUF challenge C_0 512 may be accessible by an attacker, the Circuit Delay PUF 524 cannot be replicated by the attacker. At the memory device 507, the RO PUF challenge C_0 512 is used to generate a RO PUF response R_0 521 from the circuit delay PUF 524. This RO PUF response R_0 521 is then used as the SRAM PUF challenge C_0 523 into the SRAM PUF 526 to obtain the RO PUF response R_0 525. In an alternative approach, the RO PUF response R_0 521 may be used to generate the challenge SRAM PUF C_0 523 (e.g., by mapping or converting the RO PUF response R_0

521 into a memory address). The SRAM PUF response R_0 518 is sent to the authentication device 500

[0062] In this approach, the RO PUF response R_0 521 is used to modify the actual challenge to the SRAM PUF 526. Because an attacker is unable to reproduce the RO PUF response R_0 521, it does not know the SRAM PUF challenge C_0 523 used to produce the response SRAM PUF response R_0 525.

[0063] At the authentication device 500, the device authentication module/circuit/server 503 may obtain, from the Circuit Delay PUF 505, a RO PUF response R_0 520 corresponding to the sent RO PUF challenge C_0 508. This RO PUF response R_0 520 may serve as the SRAM PUF challenge C_0 527. The device authentication module/circuit/server 403 may verify the SRAM PUF response R_0 422. The SRAM PUF challenge C_0 527 can then be used to lookup the corresponding response in the SRAM PUF database 501 and compare that response to the received response SRAM PUF response R_0 522.

[0064] In the approaches illustrated in FIGS. 3, 4, and 5, the device authentication module/circuit/server 303, 403, and/or 503 has access to the challenge and response pairs for both the SRAM PUF and RO PUF. Therefore, the device authentication module/circuit/server 303, 403, and/or 503 is able to verify the operations performed by the memory device 307, 407, and 507 and verify the response(s).

Combining SRAM and RO Physically Unclonable Functions (PUFs) to Mask Responses

[0065] In an alternative approach protects the SRAM PUF response from a memory device by use of a RO PUF.

[0066] FIG. 6 is a block diagram illustrating a fourth example of how SRAM PUF 626 and RO PUF 624 may be combined to prevent an attacker from being able to clone a memory device 607. In this example, an authentication device 600 may include a device authentication module/circuit/server 603, a SRAM PUF database 601, and a RO PUF database 605. The SRAM PUF database 601 may be generated for a memory cell region of the memory device 607 during manufacturing by, for example, sending a plurality of challenges (e.g., memory addresses) to the memory cell region and obtaining corresponding responses (e.g., uninitialized memory cell states/values). Similarly, the Circuit Delay PUF database 605 may be generated for a plurality of ring

oscillator within the memory device 607 during manufacturing by, for example, sending a plurality of challenges (e.g., selection of two ring oscillators) to the ring oscillators and obtaining a corresponding responses (e.g., frequency differential between two selected ring oscillators).

[0067] In this example, when the device authentication module/circuit/server 603 subsequently tries to authenticate the memory device 607, it sends a challenge (comprising Challenge A 616 and Challenge B 612) to the memory device 607. The challenge A 616 may comprise an SRAM PUF challenge C_0 606. The challenge B 612 includes an RO PUF challenge C_0 608 is also sent from the authentication device 600 to the memory device 607.

[0068] At the memory device 604, the RO PUF challenge C_0 612 is used to generate a RO PUF response R_0 621 from the circuit delay PUF 624. The SRAM PUF challenge C_0 616 is processed by the SRAM PUF 626 to generate a SRAM PUF response R_0 623. A hash 619 of the RO PUF response R_0 621 is then obtained as RO PUF response R_0' 625. The RO PUF response R_0' 625 is then XORed 604 with the SRAM PUF R_0 623 to obtain a combined response 618 (e.g., SRAM PUF R_0 XOR RO PUF response R_0') that is transmitted back to the device authentication module/circuit/server 603. In this manner, the SRAM PUF response R_0 623 from the SRAM PUF 626 the authentication device 600 can be protected during transmission.

[0069] At the authentication device 600, the device authentication module/circuit/server 603 may verify that the response 618 corresponds to the sent challenges SRAM PUF C_0 606 and RO PUF C_0 608. For instance, using the circuit delay PUF database 605, the RO PUF response R_0 620 corresponding to the sent RO PUF challenge C_0 608 is obtained. Then, the device authentication module/circuit/server 603 may obtain the SRAM PUF response R_0 627 by hashing 617 the RO PUF response R_0 620 and XORing 602 that result with the response 618 to obtain the SRAM PUF response R_0 627. The SRAM PUF response R_0 627 can then be used to lookup the corresponding response expected for the SRAM PUF challenge C_0 606 in the SRAM PUF database 601. If the responses match, then the memory device 607 is successfully authenticated or identified.

Exemplary Data Collector Device and Method Operational Therein

[0070] FIG. 7 is a block diagram illustrating a data collector device according to one example. The data collector device 702 may be adapted to collect and store information that uniquely characterizes electronic devices (e.g., chips, semiconductors, memory devices, etc.). For example, during a manufacturing stage, quality control stage, and/or pre-deployment stage, the data collector device 702 may be adapted to send challenges and receive responses to each electronic device and stores the received information for later use in authenticating/identifying each electronic device.

[0071] The data collector device 702 may include a processing circuit 704, a storage device 706, a communication interface 708, and/or a machine-readable medium 710. The communication interface 708 may include a transmitter/receiver circuit 718 that permits the data collector device 702 to communicate (e.g., wired or wirelessly) with one or more electronic devices.

[0072] The processing circuit 704 may include a device identifier circuit/module 722 adapted to obtain a unique identifier for each electronic device and store such unique identifier in a device identifier database 716 in the storage device 706. The processing circuit 704 may also include a challenge generator circuit/module 720 adapted to generate and send out one or more challenges to an electronic device. For instance, the challenges may be memory addresses (e.g., for a SRAM PUF) or ring oscillator pairs (e.g., for a RO PUF). The processing circuit 704 may also include an SRAM PUF collection circuit/module 726 adapted to collect responses from an SRAM PUF in an electronic device in response to one or more challenges sent. The processing circuit 704 may also include a circuit delay PUF collection circuit/module 726 adapted to collect responses from a circuit delay PUF in an electronic device in response to one or more challenges sent.

[0073] The machine-readable medium 710 may include or store device identifier instructions 730 (e.g., to cause the processing circuit to obtain a device identifier from an electronic device being queried), challenge generator instructions 728 (e.g., to cause the processing circuit to generate/send random or pre-generated challenges to the SRAM PUF and/or circuit delay PUF of the electronic device being queried), SRAM PUF collection instructions 732 (e.g., to cause the processing circuit to collect responses from the SRAM PUF of the electronic device being queried), and/or circuit delay PUF collection instructions 734 (e.g., to cause the processing circuit to collect responses from the circuit delay PUF of the electronic device being queried). Note that, in one

example, the circuit delay PUF may be a tamper-resistant PUF. By contrast, the SRAM PUF has been shown to be susceptible to various attacks (e.g., Focused Ion Beam (FIB) attacks, circuit edit attacks, etc.).

[0074] The data collector device 702 may be adapted to perform one or more of the steps or functions illustrated in FIGS. 1-6.

[0075] FIG. 8 illustrates a method operational in a data collector device for obtaining characteristic information from an electronic device. The data collector device may obtain (e.g., receive or assign) a device identifier associated with an electronic device during a pre-deployment or manufacturing stage 802. The data collector device may then generate and send one or more challenges to the electronic device 804. As a result, the data collector device may receive one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device 806. The device identifier, challenges, and corresponding responses are stored for subsequent authentication of the electronic device 808. This process may be repeated for each of a plurality of electronic devices. Note that the challenges sent to the electronic devices may be the same for all devices, may be randomly generated for each electronic device, and/or may be a subset of possible challenges.

Exemplary Authentication Device and Method Operational Therein

[0076] FIG. 9 is a block diagram illustrating an exemplary authentication device adapted to authenticate an electronic device based on responses from multiple physically unclonable functions within each electronic device. The authentication device 902 may be adapted to query an electronic device (e.g., chip, semiconductor, memory devices, etc.) and attempt to identify the electronic device based on a device identifier (e.g., obtained from the electronic device) and authenticate the electronic device by performing a query involving challenges to an SRAM PUF and circuit delay PUF in the electronic device. The authentication device 902 may include a processing circuit 904, a storage device 906, a communication interface 908, and/or a machine-readable medium 910. The communication interface 908 may include a transmitter/receiver circuit 918 that permits the authentication device 902 to communicate (e.g., wired or wirelessly) with one or more electronic devices.

[0077] The processing circuit 904 may include a device identifier circuit/module 922 adapted to obtain a unique device identifier from an electronic device. Using the obtained device identifier, an authentication circuit/module 936 may check a device identifier database 916 (in the storage device 906) for the corresponding challenge/response information associated with that device identifier. The authentication circuit/module 936 in cooperation with a SRAM PUF verification circuit/module 924 and circuit delay PUF verification circuit/module 926 may then send one or more of the corresponding challenges to the electronic device and obtains one or more responses to the challenges. Note that, in one example, the circuit delay PUF may be a tamper-resistant PUF. By contrast, the SRAM PUF has been shown to be susceptible to various attacks (e.g., Focused Ion Beam (FIB) attacks, circuit edit attacks, etc.).

[0078] The responses, in conjunction with the challenges, may be used by the SRAM PUF verification circuit/module 924 and circuit delay PUF verification circuit/module 926 to ascertain, from a SRAM PUF database 914 (in the storage device 906) and a circuit delay PUF database 912 (in the storage device 906), respectively, whether they correctly match the expected response (i.e., match the responses corresponding to the challenges in the databases 914 and 916). If the received responses match the previously stored corresponding responses, the authentication circuit/module 936 may conclude that the electronic device is successfully authenticated. Such successful authentication may be a probabilistic match, where as long as a threshold percentage or number of responses are correctly matched, a successful match may be concluded.

[0079] The machine-readable medium 910 may include or store device identifier instructions 930 (e.g., to cause the processing circuit to obtain a device identifier from an electronic device being verified), SRAM PUF verification instructions 932 (e.g., to cause the processing circuit to verify responses from the SRAM PUF of the electronic device being verified), circuit delay PUF verification instructions 934 (e.g., to cause the processing circuit to verify responses from the circuit delay PUF of the electronic device being verified), and/or authentication instructions 938 to ascertain whether both SRAM PUF and circuit delay PUF verification has been successful.

[0080] The data collector device 902 may be adapted to perform one or more of the steps or functions illustrated in FIGS. 1-6.

[0081] FIG. 10 illustrates a method operational in an authentication device for authenticating an electronic device based on responses from a plurality of physically unclonable functions. The authentication device may obtain (e.g., request or receive) a device identifier associated with an electronic device during a post-deployment stage 1002. The authentication device may obtain and send one or more challenges to the electronic device 1004. For example, the challenges may be a pre-defined set of challenges utilized for all electronic devices. Alternatively, the challenges may be a specific subset of challenges for the electronic device obtained from a database using the device identifier. As a result of sending the one or more challenges, the authentication device may receive one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device 1006. In various implementations, the authentication device may operate as illustrated and described with reference to FIGS. 1, 2, 3, 4, 5, and/or 6.

[0082] The device identifier may be used to identify pre-stored challenges and corresponding responses specific to the electronic device 1008. The authentication device may then authenticate the electronic device by comparing the pre-stored responses and the received one or more responses for the electronic device 1010. Successful authentication occurs when the received one or more responses match the pre-stored responses for the electronic device. Successful authentication may be a probabilistic match, where as long as a threshold percentage or number of responses are correctly matched, a successful match may be concluded. This process may be repeated for each of a plurality of electronic devices. Since physically unclonable functions are used by each electronic device, the one or more responses will be distinct even if the same challenge is used for all devices.

Exemplary Electronic Device and Method Operational Therein

[0083] FIG. 11 is a block diagram illustrating an exemplary electronic device having multiple physically unclonable functions. The electronic device 1102 may be a chip, semiconductor, memory devices, etc., and adapted to provide a device identifier and respond to challenges to an SRAM PUF and circuit delay PUF in the electronic device. The electronic device 1102 may include a processing circuit 1104, a device identifier 1116 (in a storage device), a delay-based PUF circuit 1112 (e.g., plurality of

oscillator ring circuits), a static random access memory 1116 (which may be used as an SRAM PUF), a communication interface 1108, and/or a machine-readable medium 1110. The communication interface 1108 may include a transmitter/receiver circuit 1118 that permits the electronic device 1102 to communicate (e.g., wired or wirelessly) with one or more data collector and/or authentication devices.

[0084] The processing circuit 1104 may include a device identifier circuit/module 1122 adapted to provide its unique device identifier 1116 to a data collector and/or authentication device. The processing circuit may also include a SRAM PUF Response circuit/module 1124 and a circuit delay PUF Response circuit/module 1126 that are adapted to obtain responses to received challenges and send the responses to a data collector device and authentication devices. Note that, in one example, the circuit delay PUF may be a tamper-resistant PUF. By contrast, the SRAM PUF has been shown to be susceptible to various attacks (e.g., Focused Ion Beam (FIB) attacks, circuit edit attacks, etc.).

[0085] The SRAM PUF Response circuit/module 1124 may send received challenges to the static random access memory 1114 to obtain responses. For example, responses may be the uninitialized states of one or more memory cells of the static random access memory 1114. Similarly, the circuit delay PUF Response circuit/module 1126 may send received challenges to the delay-based PUF circuit 1112 to obtain responses.

[0086] The machine-readable medium 1110 may include or store device identifier instructions 1130 (e.g., to cause the processing circuit to obtain the device identifier 1116 for the electronic device), SRAM PUF response instructions 1132 (e.g., to cause the processing circuit to obtain responses from the static random access memory 1114 of the electronic device), and/or circuit delay PUF response instructions 1134 (e.g., to cause the processing circuit to obtain responses from the circuit delay PUF of the electronic device).

[0087] The electronic device 1102 may be adapted to perform one or more of the steps or functions illustrated in FIGS. 1-6.

[0088] FIG. 12 illustrates a method operational in an electronic device for authenticating itself with an authentication device based on a response from a plurality of physically unclonable functions. The electronic device may have received one or

more challenges and provided one or more corresponding responses during a pre-deployment or manufacturing phase.

[0089] The electronic device implements a first physically unclonable function using a plurality of memory cells within the electronic device 1204. In one example, the first physically unclonable function may use the uninitialized memory cell states for one or more memory cells as a response to the challenge.

[0090] The electronic device may also implement a second physically unclonable function using a plurality of circuit delay based paths within the electronic device 1206. In one example, the plurality of circuit delay based paths and/or is otherwise tamper-resistant. The term "tamper-resistant" refers to an implementation or type of a PUF that when an attempt is made to tamper with it to predict, ascertain, and/or read its response or output, this causes the response and/or output to change. For example, an attempt to physically tamper with a ring oscillator or circuit delay path type oscillator would cause the response for the ring oscillator or circuit delay path to be altered (e.g., output frequency changes).

[0091] A challenge may be received from an external server 1208. The challenge may be applied to the first physical unclonable function by using a first response from the second physically unclonable function to either: (a) mask/unmask a challenge input to the first physically unclonable function, (b) generate the challenge input to the first physical unclonable function, or (c) mask a response output from the first physically unclonable function 1210. In one example, the first challenge may identify memory addresses within the plurality of memory cells. In another example, the challenge may select two ring oscillators from the plurality of ring oscillators in the second physically unclonable function and responds with a frequency differential between the two ring oscillators. The challenge may be received as part of at least one of: an authentication process of the electronic device, an identification process of the electronic device, and/or a key generation process within the electronic device.

[0092] The first response from the second physically unclonable function and/or a second response from the first physically unclonable function may then be sent to the external server 1212. The external server may include a first database of challenges and responses for the first physically unclonable function and a second database of challenges and responses for the second physically unclonable function, where the

external server sends the challenge to the electronic device and authenticates or identifies the electronic device based on the second response.

[0093] An indicator may be received that the response was successfully verified by the external server 1214. For instance, upon successful authentication, the electronic device may receive an indicator that it has gained access to a network and/or data.

[0094] In one example, the challenge includes a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function. For instance, the first challenge may be a challenge masked by an expected response to second challenge (as illustrated in FIG. 3). In another instance, the first challenge may be modified by the first response from the second physically unclonable function prior to processing by the first physically unclonable function (as illustrated in FIG. 4).

[0095] In yet another example, the received challenge may be used by the second physically unclonable function to generate the first response which is then used as a second challenge by the first physically unclonable function to generate the second response (as illustrated in FIG. 5).

[0096] In another implementation, the challenge may include a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function, the second challenge may be used by the second physically unclonable function to generate the first response which is used to mask the second response from the first physically unclonable function (as illustrated in FIG. 6). The method may further include: (a) hashing the first response from the second physically unclonable function to obtain an intermediate response; and/or (b) masking the second response using the intermediate response.

[0097] In one example, a pre-stored device identifier may also be pre-provisioned within the electronic device 1202. It may send the pre-stored device identifier from the electronic device to the external server either: (a) before the challenge is received, or (b) concurrent with sending the second response. The device identifier uniquely identifies the electronic device.

[0098] One or more of the components, steps, features, and/or functions illustrated in FIGS. 1 – 12 may be rearranged and/or combined into a single component, step, feature or function or embodied in several components, steps, or functions. Additional elements, components, steps, and/or functions may also be added without departing

from the invention. The apparatus, devices, and/or components illustrated in FIGS. 1 – 7, 9, and 11 may be configured to perform one or more of the methods, features, or steps described in FIGS. 8, 10 and 12. The algorithms described herein may also be efficiently implemented in software and/or embedded in hardware.

[0099] Moreover, in one aspect of the disclosure, the processing circuit 704, 904 and 1104 illustrated in FIGS. 7, 9 and 11 may be specialized processors (e.g., an application specific integrated circuit (e.g., ASIC)) that are specifically designed and/or hard-wired to perform the algorithms, methods, and/or steps described in FIGS. 8, 10, and 12, respectively. Thus, such a specialized processor (e.g., ASIC) may be one example of a means for executing the algorithms, methods, and/or steps described in FIGS. 8, 10, and 12.

[00100] Also, it is noted that the aspects of the present disclosure may be described as a process that is depicted as a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[00101] Moreover, a storage medium may represent one or more devices for storing data, including read-only memory (ROM), random access memory (RAM), magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine-readable mediums and, processor-readable mediums, and/or computer-readable mediums for storing information. The terms "machine-readable medium", "computer-readable medium", and/or "processor-readable medium" may include, but are not limited to non-transitory mediums such as portable or fixed storage devices, optical storage devices, and various other mediums capable of storing, containing or carrying instruction(s) and/or data. Thus, the various methods described herein may be fully or partially implemented by instructions and/or data that may be stored in a "machine-readable medium", "computer-readable medium", and/or "processor-readable medium" and executed by one or more processors, machines and/or devices.

[00102] Furthermore, aspects of the disclosure may be implemented by hardware, software, firmware, middleware, microcode, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine-readable medium such as a storage medium or other storage(s). A processor may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

[00103] The various illustrative logical blocks, modules, circuits, elements, and/or components described in connection with the examples disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic component, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing components, e.g., a combination of a DSP and a microprocessor, a number of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[00104] The methods or algorithms described in connection with the examples disclosed herein may be embodied directly in hardware, in a software module executable by a processor, or in a combination of both, in the form of processing unit, programming instructions, or other directions, and may be contained in a single device or distributed across multiple devices. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. A storage medium may be coupled to the processor such that the processor can read

information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor.

[00105] Those of skill in the art would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the aspects disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system.

[00106] The various features of the invention described herein can be implemented in different systems without departing from the invention. It should be noted that the foregoing aspects of the disclosure are merely examples and are not to be construed as limiting the invention. The description of the aspects of the present disclosure is intended to be illustrative, and not to limit the scope of the claims. As such, the present teachings can be readily applied to other types of apparatuses and many alternatives, modifications, and variations will be apparent to those skilled in the art.

CLAIMS

WHAT IS CLAIMED IS:

1. A method operational by an electronic device, comprising:

implementing a first physically unclonable function using a plurality of memory cells within the electronic device;

implementing a second physically unclonable function using a plurality of circuit delay based paths within the electronic device;

receiving a challenge from an external server;

applying the challenge to the first physical unclonable function by using a first response from the second physically unclonable function to either:

(a) mask/unmask a challenge input to the first physically unclonable function,

(b) generate the challenge input to the first physical unclonable function, or

(c) mask a response output from the first physically unclonable function; and

sending a second response from the first physically unclonable function to the external server.

2. The method of claim 1, further comprising:

sending the first response from the second physically unclonable function to the external server.

3. The method of claim 1, wherein the first physically unclonable function uses the uninitialized memory cell states for one or more memory cells as a response to the challenge.

4. The method of claim 1, wherein the plurality of circuit delay based paths are ring oscillators and the second physically unclonable function receives a challenge that selects two ring oscillators from the plurality of ring oscillators and responds with a frequency differential between the two ring oscillators.

5. The method of claim 1, wherein the external server includes a first database of challenges and responses for the first physically unclonable function and a second database of challenges and responses for the second physically unclonable function, where the external server sends the challenge to the electronic device and authenticates or identifies the electronic device based on the second response.

6. The method of claim 1, wherein the challenge includes a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function.

7. The method of claim 6, wherein the first challenge is a challenge masked by an expected response to second challenge.

8. The method of claim 6, wherein the first challenge is modified by the first response from the second physically unclonable function prior to processing by the first physically unclonable function.

9. The method of claim 1, wherein the received challenge is used by the second physically unclonable function to generate the first response which is then used as a second challenge by the first physically unclonable function to generate the second response.

10. The method of claim 1, wherein the challenge includes a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function, the second challenge is used by the second physically unclonable function to generate the first response which is used to mask the second response from the first physically unclonable function.

11. The method of claim 10, further comprising:

hashing the first response from the second physically unclonable function to obtain an intermediate response; and

masking the second response using the intermediate response.

12. The method of claim 1, wherein the challenge is received as part of at least one of: an authentication process of the electronic device, an identification process of the electronic device, and/or a key generation process within the electronic device.

13. The method of claim 1, wherein the electronic device received one or more challenges and provided one or more corresponding responses during a pre-deployment or manufacturing phase.

14. The method of claim 1, further comprising:

sending a pre-stored device identifier from the electronic device to the external server either:

(a) before the challenge is received, or

(b) concurrent with sending the second response,

wherein the device identifier uniquely identifies the electronic device.

15. An electronic device, comprising:

a plurality of memory cells within the electronic device serving as a first physically unclonable function;

a plurality of circuit delay based paths within the electronic device implementing a second physically unclonable function;

a communication interface to receive a challenge from an external server;

a processing circuit coupled to the communication interface, the plurality of memory cells, and the plurality of circuit delay based paths, wherein the processing circuit is adapted to apply the challenge to the first physical unclonable function by using a first response from the second physically unclonable function to either:

(a) mask/unmask a challenge input to the first physically unclonable function,

(b) generate the challenge input to the first physical unclonable function, or

(c) mask a response output from the first physically unclonable function; and

the communication interface adapted to send a second response from the first physically unclonable function to the external server.

16. The electronic device of claim 15, further comprising:

sending the first response from the second physically unclonable function to the external server.

17. The electronic device of claim 15, wherein the first physically unclonable function uses the uninitialized memory cell states for one or more memory cells as a response to the challenge.

18. The electronic device of claim 15, wherein the plurality of circuit delay based paths are ring oscillators and the second physically unclonable function receives a challenge that selects two ring oscillators from the plurality of ring oscillators and responds with a frequency differential between the two ring oscillators.

19. The electronic device of claim 15, wherein the external server includes a first database of challenges and responses for the first physically unclonable function and a second database of challenges and responses for the second physically unclonable function, where the external server sends the challenge to the electronic device and authenticates or identifies the electronic device based on the second response.

20. The electronic device of claim 15, wherein the challenge includes a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function.

21. The electronic device of claim 20, wherein the first challenge is a challenge masked by an expected response to second challenge.

22. The electronic device of claim 20, wherein the first challenge is modified by the first response from the second physically unclonable function prior to processing by the first physically unclonable function.

23. The electronic device of claim 15, wherein the received challenge is used by the second physically unclonable function to generate the first response which is then used

as a second challenge by the first physically unclonable function to generate the second response.

24. The electronic device of claim 15, wherein the challenge includes a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function, the second challenge is used by the second physically unclonable function to generate the first response which is used to mask the second response from the first physically unclonable function.

25. The electronic device of claim 24, wherein the processing circuit is further adapted to:

hash the first response from the second physically unclonable function to obtain an intermediate response; and

mask the second response using the intermediate response.

26. The electronic device of claim 15, wherein the challenge is received as part of at least one of: an authentication process of the electronic device, an identification process of the electronic device, and/or a key generation process within the electronic device.

27. The electronic device of claim 15, wherein the processing circuit is further adapted to send a pre-stored device identifier from the electronic device to the external server by either:

(a) before the challenge is received, or

(b) concurrent with sending the second response,

wherein the device identifier uniquely identifies the electronic device.

28. An electronic device, comprising:

means for implementing a first physically unclonable function using a plurality of memory cells within the electronic device;

means for implementing a second physically unclonable function using a plurality of circuit delay based paths within the electronic device;

means for receiving a challenge from an external server;

means for applying the challenge to the first physical unclonable function by using a first response from the second physically unclonable function to either:

(a) mask/unmask a challenge input to the first physically unclonable function,

(b) generate the challenge input to the first physical unclonable function, or

(c) mask a response output from the first physically unclonable function; and

means for sending a second response from the first physically unclonable function to the external server.

29. The electronic device of claim 28, wherein the challenge includes a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function.

30. The electronic device of claim 29, wherein the first challenge is a challenge masked by an expected response to second challenge.

31. The electronic device of claim 29, wherein the first challenge is modified by the first response from the second physically unclonable function prior to processing by the first physically unclonable function.

32. The electronic device of claim 29, wherein the received challenge is used by the second physically unclonable function to generate the first response which is then used as a second challenge by the first physically unclonable function to generate the second response.

33. The electronic device of claim 28, wherein the challenge includes a first challenge for the first physically unclonable function and a second challenge for the second physically unclonable function, the second challenge is used by the second physically unclonable function to generate the first response which is used to mask the second response from the first physically unclonable function.

34. A non-transitory machine-readable storage medium having one or more instructions stored thereon, which when executed by at least one processor causes the at least one processor to:

implement a first physically unclonable function using a plurality of memory cells within the electronic device;

implement a second physically unclonable function using a plurality of circuit delay based paths within the electronic device;

receive a challenge from an external server;

apply the challenge to the first physical unclonable function by using a first response from the second physically unclonable function to either:

(a) mask/unmask a challenge input to the first physically unclonable function,

(b) generate the challenge input to the first physical unclonable function, or

(c) mask a response output from the first physically unclonable function; and

send a second response from the first physically unclonable function to the external server.

35. A method operational by an authentication device, comprising:

receiving a device identifier associated with an electronic device;

sending one or more challenges to the electronic device;

receiving one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device;

identifying pre-stored responses specific to the electronic device using the electronic device identifier; and

authenticating the electronic device by comparing the pre-stored responses and the received one or more responses for the electronic device.

36. The method of claim 35, wherein the challenges are selected from a plurality of challenges for which responses where previously obtained from the electronic device.

37. The method of claim 35, wherein the pre-stored responses were obtained at a manufacturing stage or pre-deployment stage of the electronic device.

38. The method of claim 35, wherein the device identifier is received prior to sending the one or more challenges.

39. The method of claim 35, wherein the device identifier is received along with receiving the one or more responses.

40. The method of claim 35, wherein the challenge includes a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function.

41. The method of claim 40, wherein the first challenge is a challenge masked by an expected response to second challenge.

42. The method of claim 40, wherein the one or more challenges include a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function, the one or more responses include a first response from the first physically unclonable function and a second response from the second physically unclonable function, the electronic device is successfully authenticated if the first response matches a first pre-stored response corresponding to the first challenge and the second response matches a second pre-stored response corresponding to the second challenge.

43. The method of claim 40, wherein the one or more challenges include a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function, the one or more responses include a first response from the first physically unclonable function and a second response from the second physically unclonable function, and further comprising:

obtaining an intermediate challenge by unmasking the first challenge with the second response, and comparing the received first response to the pre-stored response associated with the intermediate challenge.

44. The method of claim 35, wherein the one or more challenges include a first challenge for a second physically unclonable function, the one or more responses include a first response from the first physically unclonable function, and further comprising:

obtaining an intermediate challenge by retrieving a pre-stored intermediate response corresponding to the first challenge, and comparing the received first response to a pre-stored intermediate response corresponding to the intermediate challenge.

45. The method of claim 35, wherein the one or more challenges include a first challenge for a first physically unclonble function and a second challenge for a second physically unclonable function, the one or more responses include a first response, and further comprising:

obtaining an intermediate response by unmasking the first response with a pre-stored second response corresponding to the second challenge, and comparing the intermediate response to s pre-stored response associated with the first challenge.

46. An authentication device, comprising:

a communication interface to communicate with an electronic device;

a processing circuit coupled to the communication interface, wherein the processing circuit is adapted to:

receive a device identifier associated with the electronic device;

send one or more challenges to the electronic device;

receive one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device;

identify pre-stored responses specific to the electronic device using the electronic device identifier; and

authenticate the electronic device by comparing the pre-stored responses and the received one or more responses for the electronic device.

47. The authentication device of claim 46, wherein the challenges are selected from a plurality of challenges for which responses where previously obtained from the electronic device.

48. The authentication device of claim 46, wherein the challenge includes a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function.

49. The authentication device of claim 48, wherein the first challenge is a challenge masked by an expected response to second challenge.

50. The authentication device of claim 48, wherein the one or more challenges include a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function, the one or more responses include a first response from the first physically unclonable function and a second response from the second physically unclonable function, the electronic device is successfully authenticated if the first response matches a first pre-stored response corresponding to the first challenge and the second response matches a second pre-stored response corresponding to the second challenge.

51. The authentication device of claim 46, wherein the one or more challenges include a first challenge for a first physically unclonable function and a second challenge for a second physically unclonable function, the one or more responses include a first response from the first physically unclonable function and a second response from the second physically unclonable function, and the processing circuit is further adapted to:

obtain an intermediate challenge by unmasking the first challenge with the second response, and comparing the received first response to the pre-stored response associated with the intermediate challenge.

52. The authentication device of claim 46, wherein the one or more challenges include a first challenge for a second physically unclonable function, the one or more

RECTIFIED SHEET (RULE 91) ISA/EP

responses include a first response from the first physically unclonable function, and and the processing circuit is further adapted to:

obtain an intermediate challenge by retrieving a pre-stored intermediate response corresponding to the first challenge, and comparing the received first response to a pre-stored intermediate response corresponding to the intermediate challenge.

53. The authentication device of claim 46, wherein the one or more challenges include a first challenge for a first physically unclonble function and a second challenge for a second physically unclonable function, the one or more responses include a first response, and the processing circuit is further adapted to:

obtain an intermediate response by unmasking the first response with a pre-stored second response corresponding to the second challenge, and comparing the intermediate response to s pre-stored response associated with the first challenge.

54. An authentication device, comprising:

means for receiving a device identifier associated with an electronic device;

means for sending one or more challenges to the electronic device;

means for receiving one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device;

means for identifying pre-stored responses specific to the electronic device using the electronic device identifier; and

means for authenticating the electronic device by comparing the pre-stored responses and the received one or more responses for the electronic device.

55. A non-transitory machine-readable storage medium having one or more instructions stored thereon, which when executed by at least one processor causes the at least one processor to: receiving a device identifier associated with an electronic device;

send one or more challenges to an electronic device;

receive one or more responses from the electronic device, the one or more responses including characteristic information generated from two or more distinct types of physically unclonable functions in the electronic device;

identify pre-stored responses specific to the electronic device using the electronic device identifier; and

authenticate the electronic device by comparing the pre-stored responses and the received one or more responses for the electronic device.

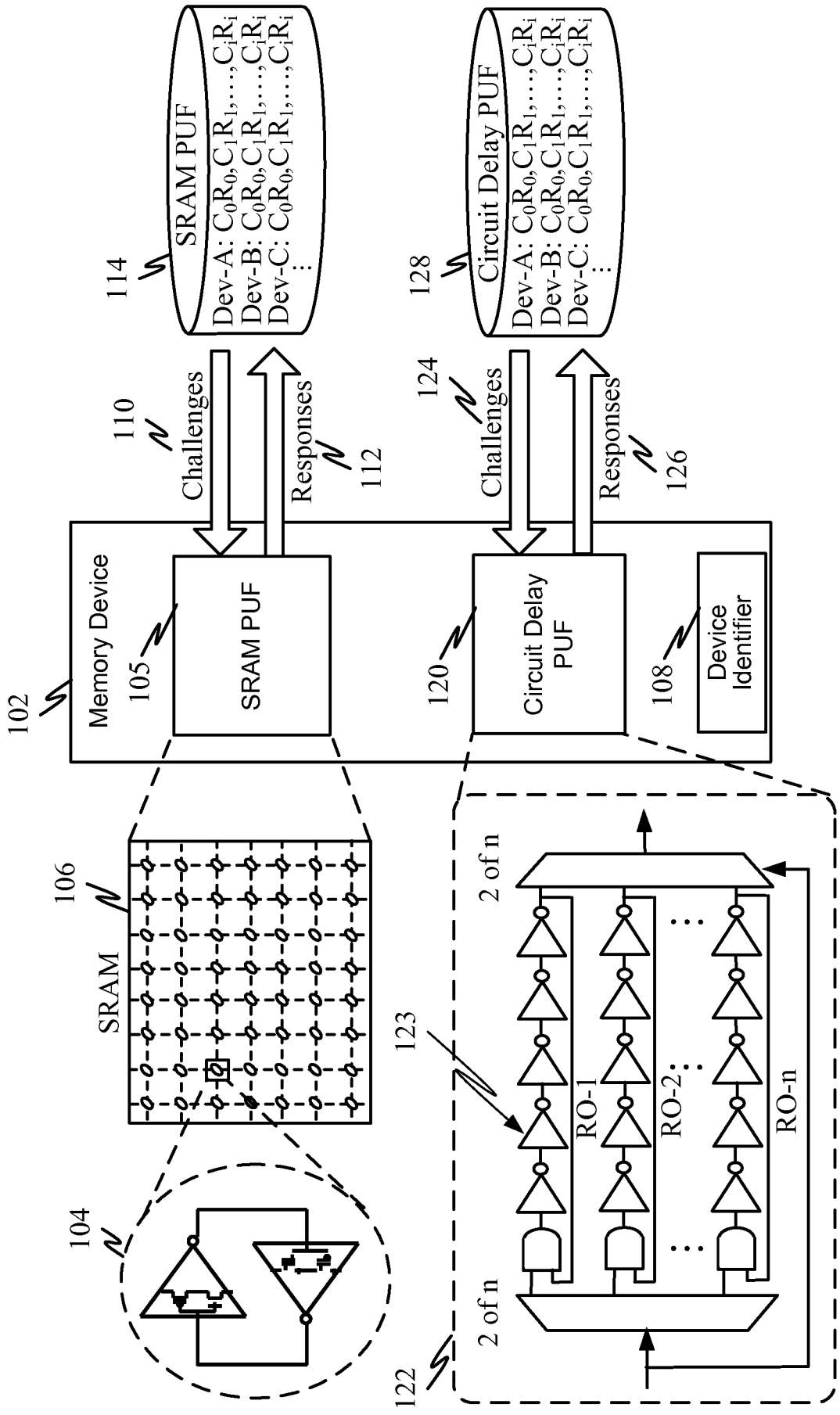

SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
114
Circuit Delay PUF
128
110
Challenges
112
Responses
124
126
102
Memory Device
105
SRAM PUF
120
Circuit Delay PUF
108
Device Identifier
106
SRAM
104
123
2 of n
RO-1
RO-2
RO-n
122

FIG. 1

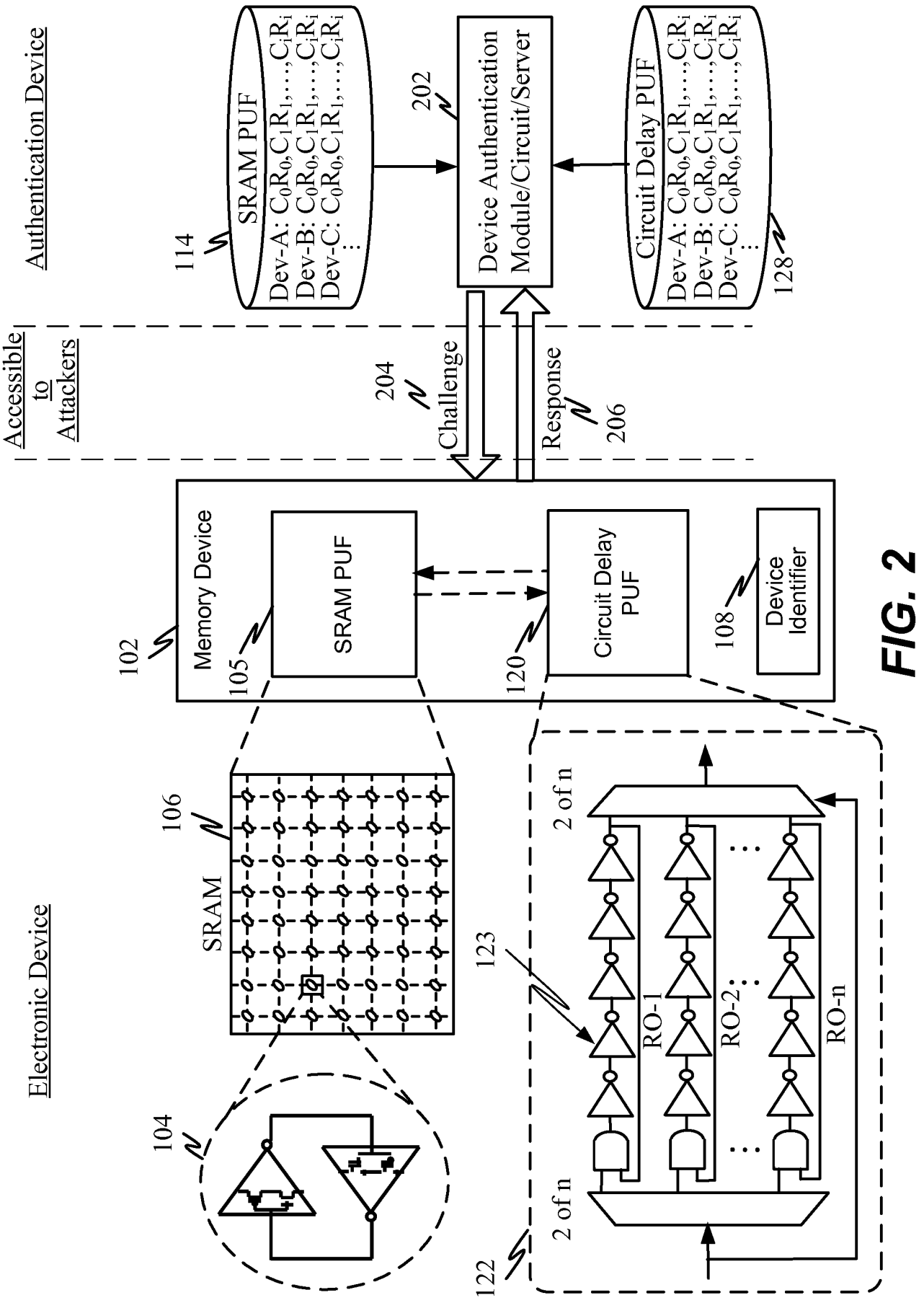

Authentication Device
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
114
202
Device Authentication Module/Circuit/Server
Circuit Delay PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
128
Accessible to Attackers
204
Challenge
Response
206
Memory Device
102
SRAM PUF
105
Circuit Delay PUF
120
Device Identifier
108
Electronic Device
SRAM
106
104
123
2 of n
2 of n
RO-1
RO-2
RO-n
122

FIG. 2

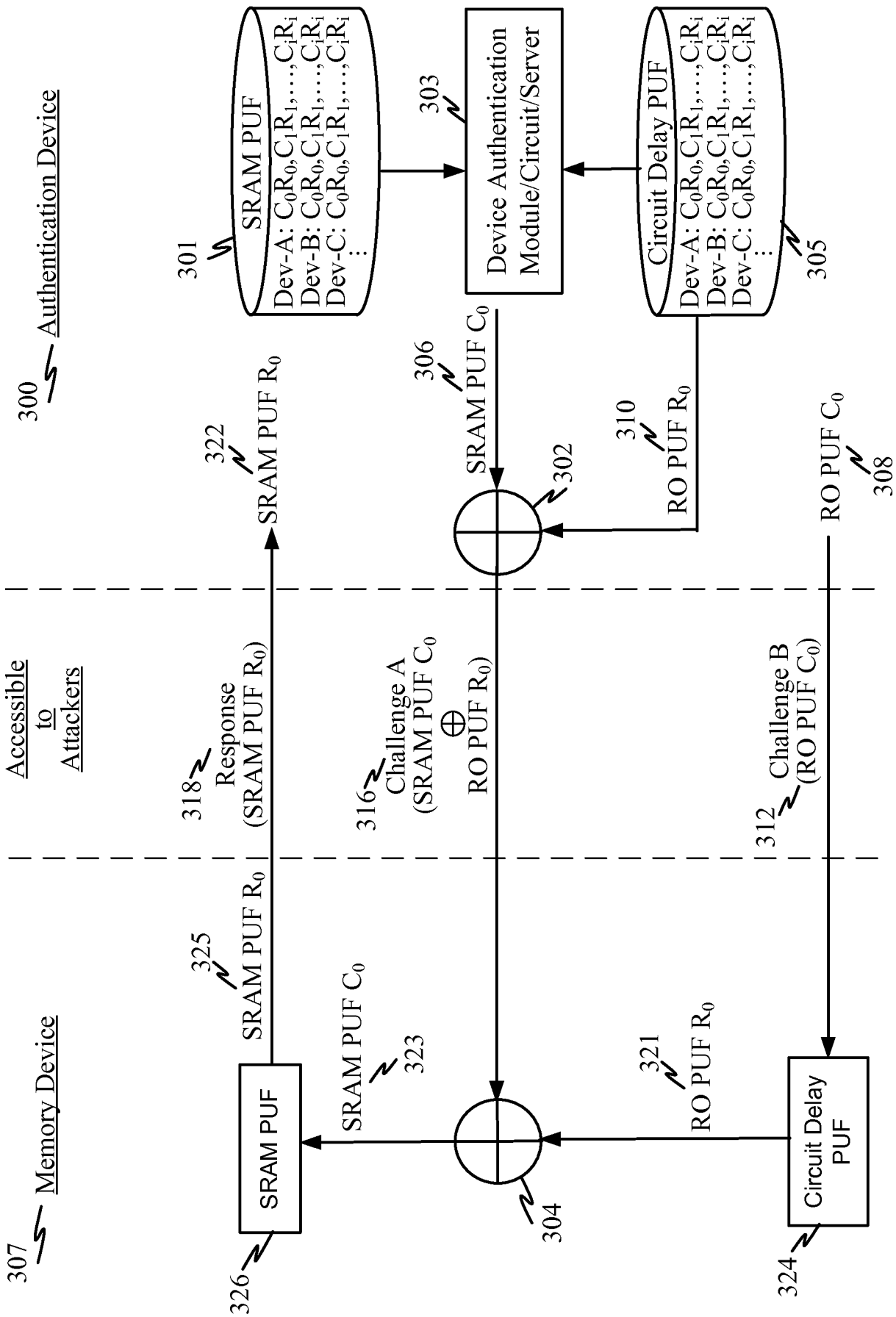

300 Authentication Device
301
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
303
Device Authentication Module/Circuit/Server
305
Circuit Delay PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
322 SRAM PUF R_0
306 SRAM PUF C_0
310 RO PUF R_0
308 RO PUF C_0
302
Accessible to Attackers
318 Response (SRAM PUF R_0)
316 Challenge A (SRAM PUF C_0 ⊕ RO PUF R_0)
312 Challenge B (RO PUF C_0)
325 SRAM PUF R_0
323 SRAM PUF C_0
321 RO PUF R_0
307 Memory Device
SRAM PUF
Circuit Delay PUF
326
304
324

FIG. 3

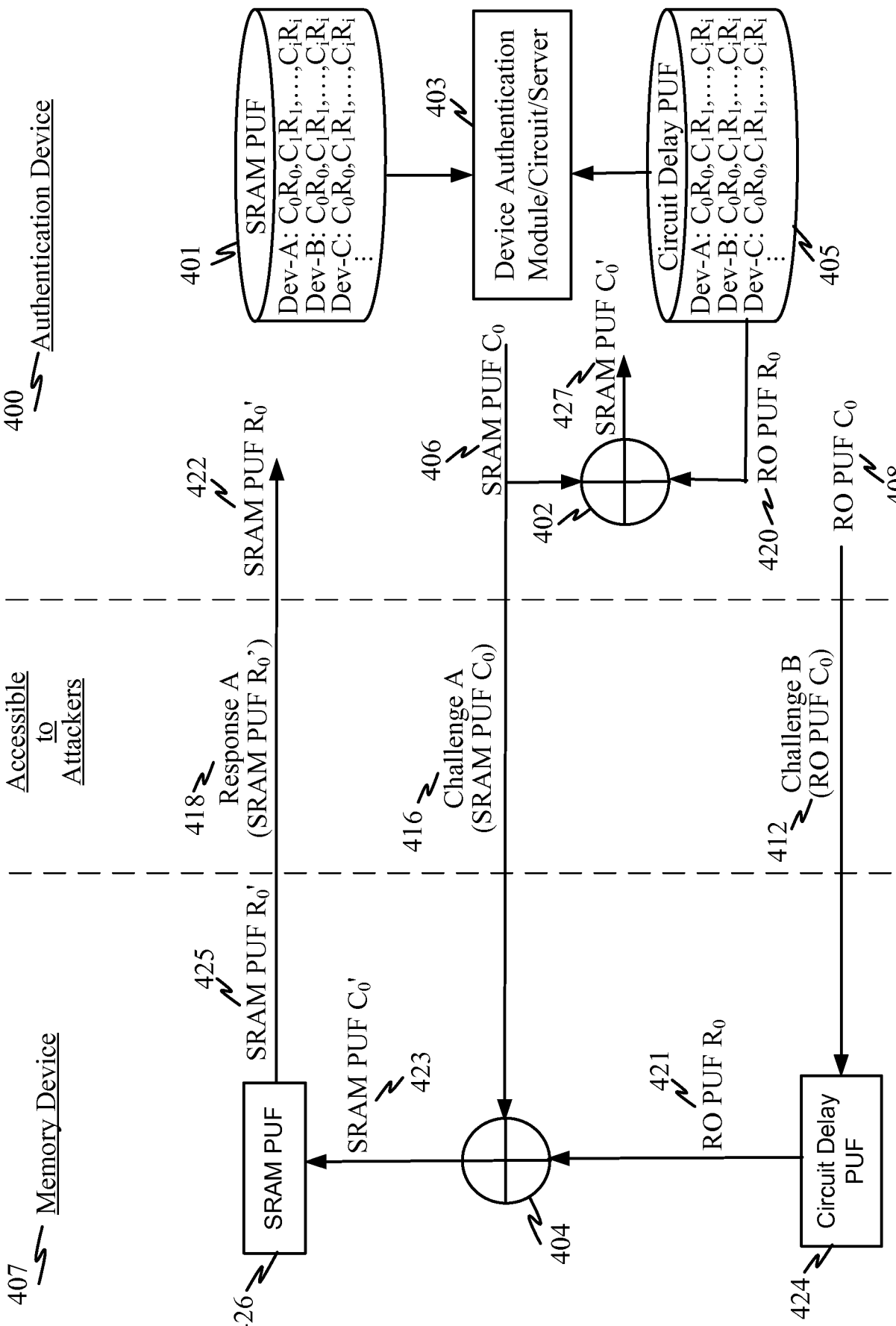

400 Authentication Device
401 SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
403 Device Authentication Module/Circuit/Server
405 Circuit Delay PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
422 SRAM PUF R_0'
406 SRAM PUF C_0
427 SRAM PUF C_0'
402
420 RO PUF R_0
RO PUF C_0 408
Accessible to Attackers
418 Response A (SRAM PUF R_0')
416 Challenge A (SRAM PUF C_0)
412 Challenge B (RO PUF C_0)
425 SRAM PUF R_0'
SRAM PUF C_0' 423
421 RO PUF R_0
407 Memory Device
SRAM PUF 426
404
Circuit Delay PUF 424

FIG. 4

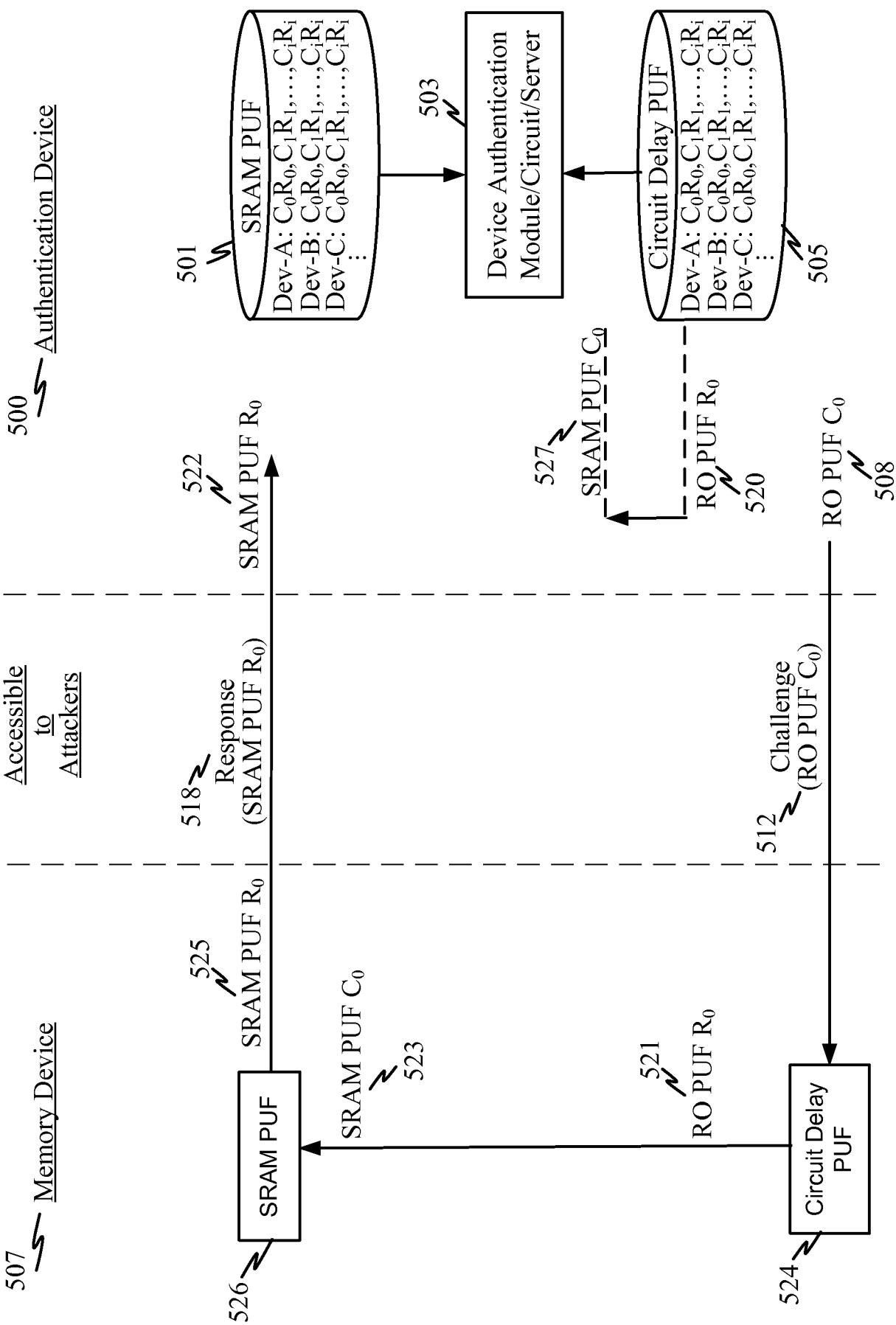

500 Authentication Device
501
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
503
Device Authentication Module/Circuit/Server
505
Circuit Delay PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
522
SRAM PUF R_0
527
SRAM PUF C_0
RO PUF R_0
520
RO PUF C_0
508
Accessible to Attackers
518
Response (SRAM PUF R_0)
512
Challenge (RO PUF C_0)
525
SRAM PUF R_0
SRAM PUF C_0
523
521
RO PUF R_0
507 Memory Device
SRAM PUF
526
Circuit Delay PUF
524

FIG. 5

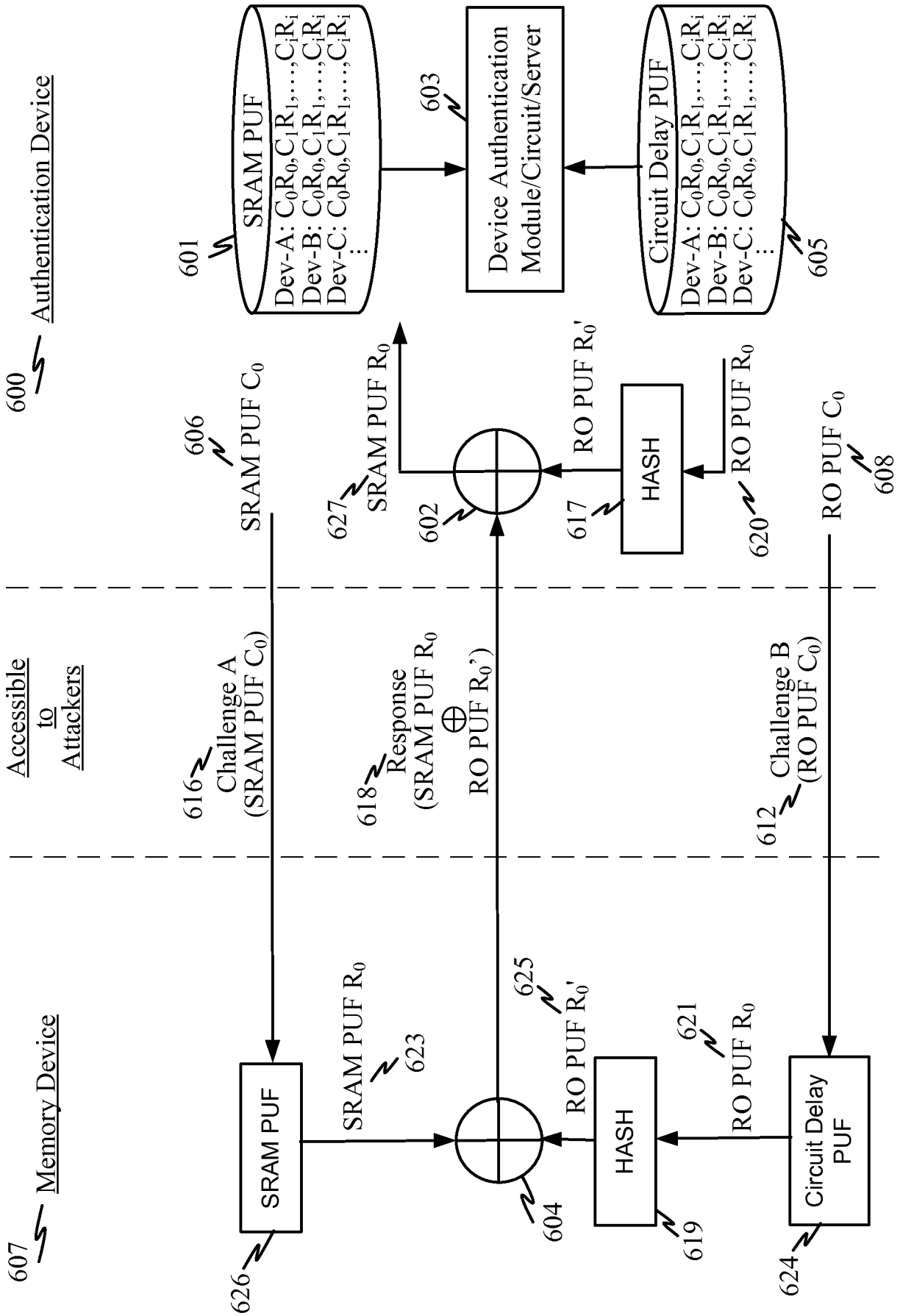

600 Authentication Device
601 SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
603 Device Authentication Module/Circuit/Server
605 Circuit Delay PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
606 SRAM PUF C_0
627 SRAM PUF R_0
602
RO PUF R_0'
617 HASH
620 RO PUF R_0
RO PUF C_0 608
Accessible to Attackers
616 Challenge A (SRAM PUF C_0)
618 Response (SRAM PUF R_0 ⊕ RO PUF R_0')
612 Challenge B (RO PUF C_0)
607 Memory Device
SRAM PUF 626
SRAM PUF R_0 623
625 RO PUF R_0'
604
HASH 619
621 RO PUF R_0
Circuit Delay PUF 624

FIG. 6

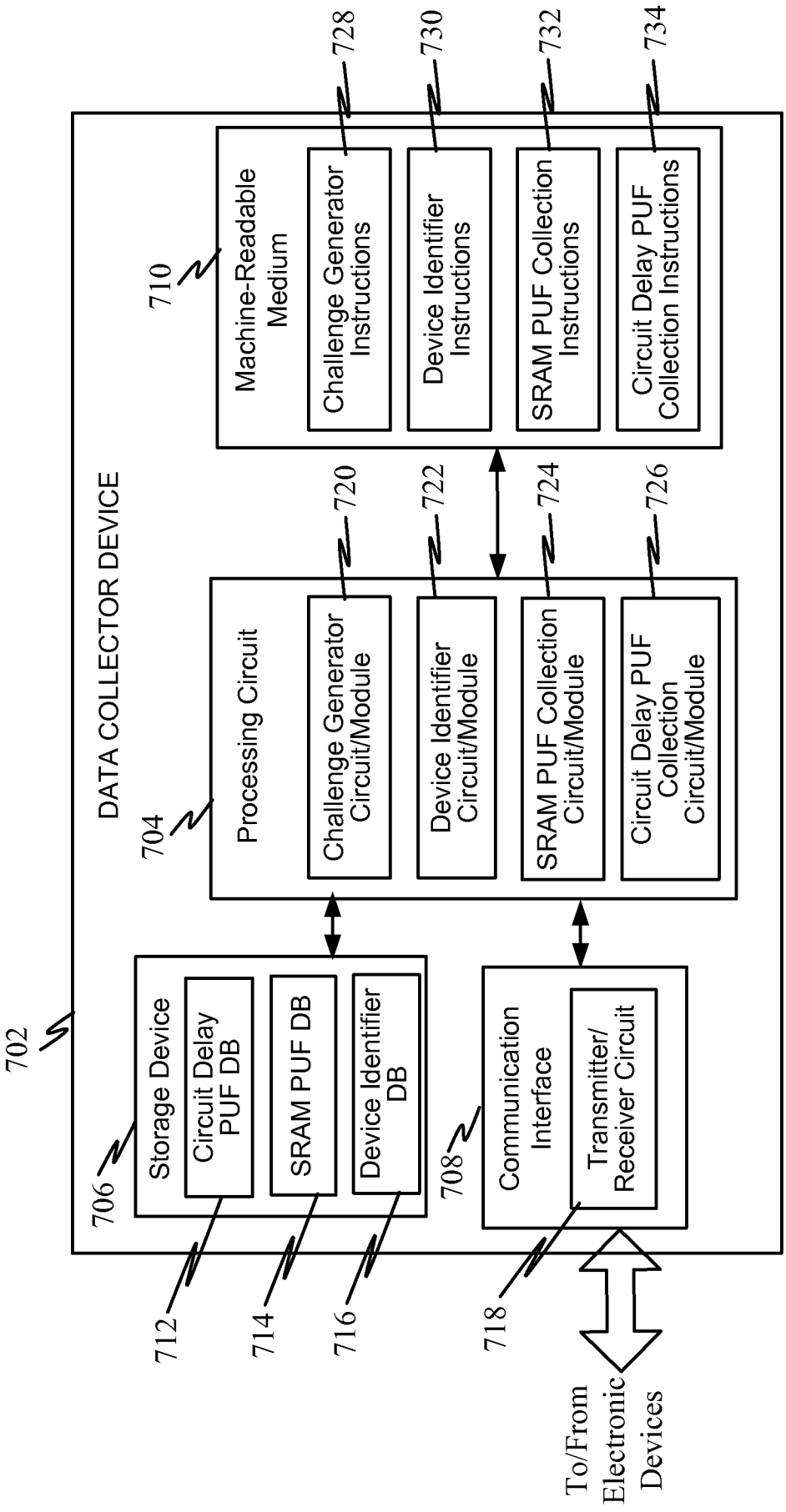
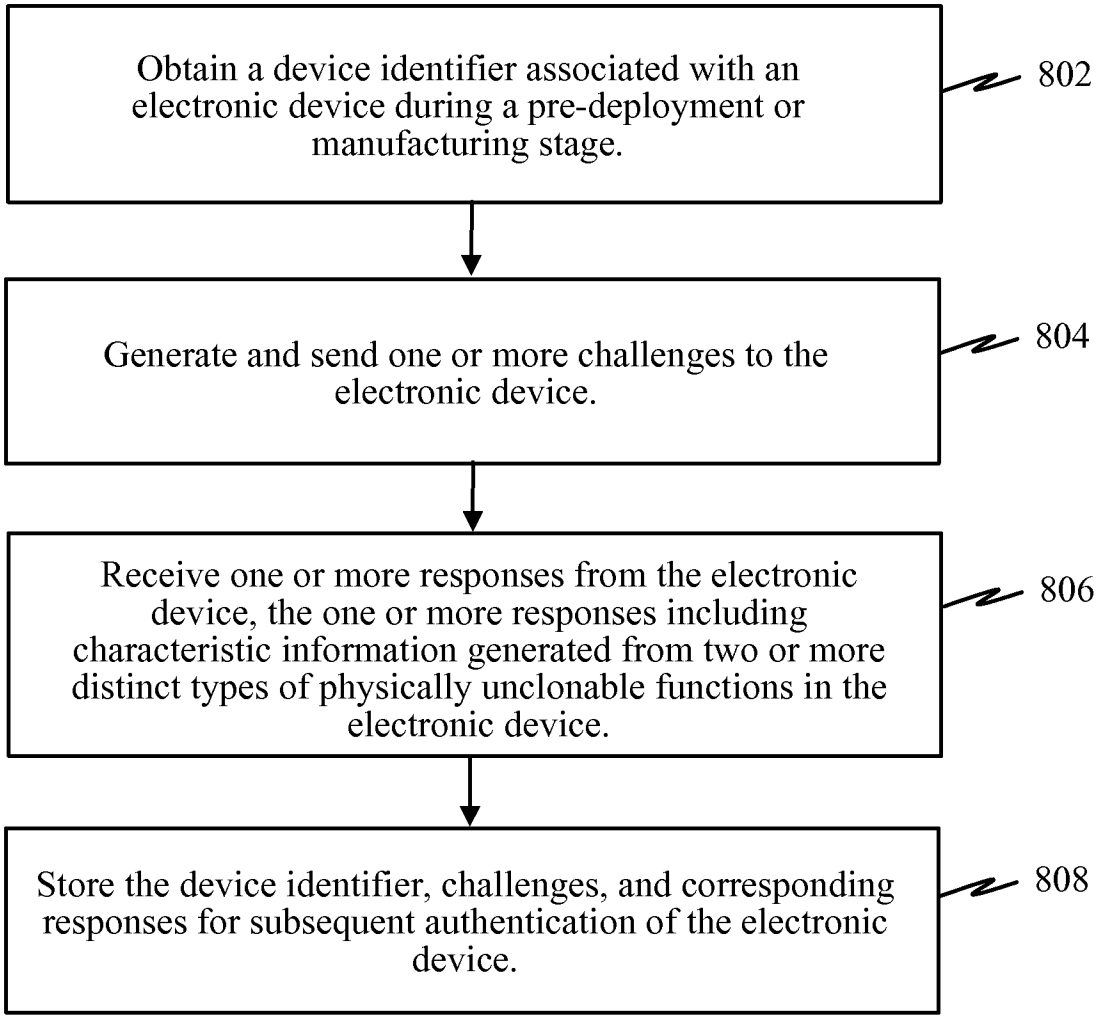

DATA COLLECTOR DEVICE
702
Machine-Readable Medium
710
Challenge Generator Instructions
728
Device Identifier Instructions
730
SRAM PUF Collection Instructions
732
Circuit Delay PUF Collection Instructions
734
Processing Circuit
704
Challenge Generator Circuit/Module
720
Device Identifier Circuit/Module
722
SRAM PUF Collection Circuit/Module
724
Circuit Delay PUF Collection Circuit/Module
726
Storage Device
706
Circuit Delay PUF DB
SRAM PUF DB
Device Identifier DB
Communication Interface
708
Transmitter/ Receiver Circuit
712
714
716
718
To/From Electronic Devices

FIG. 7



Method Operational on Data Collector Device

FIG. 8

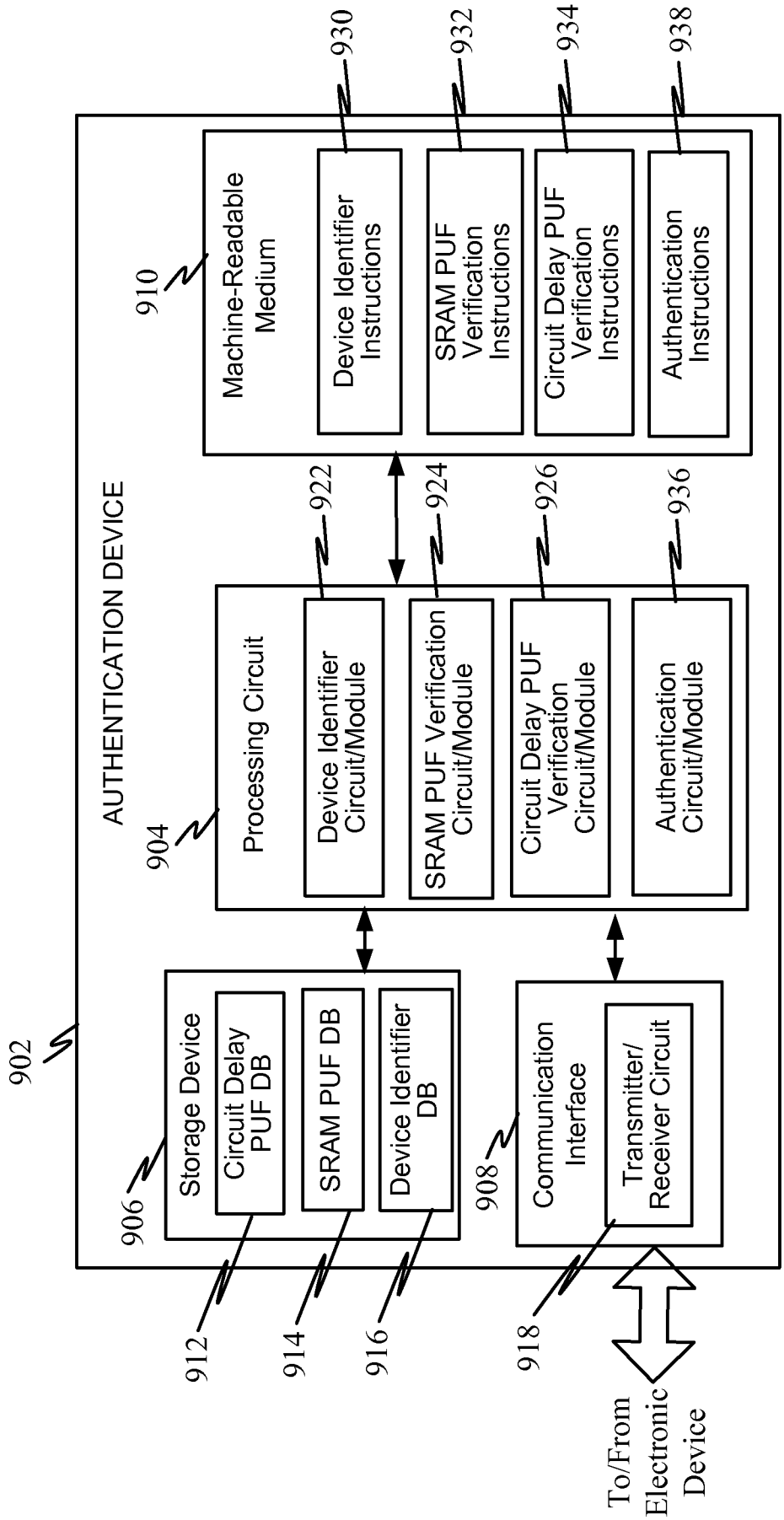
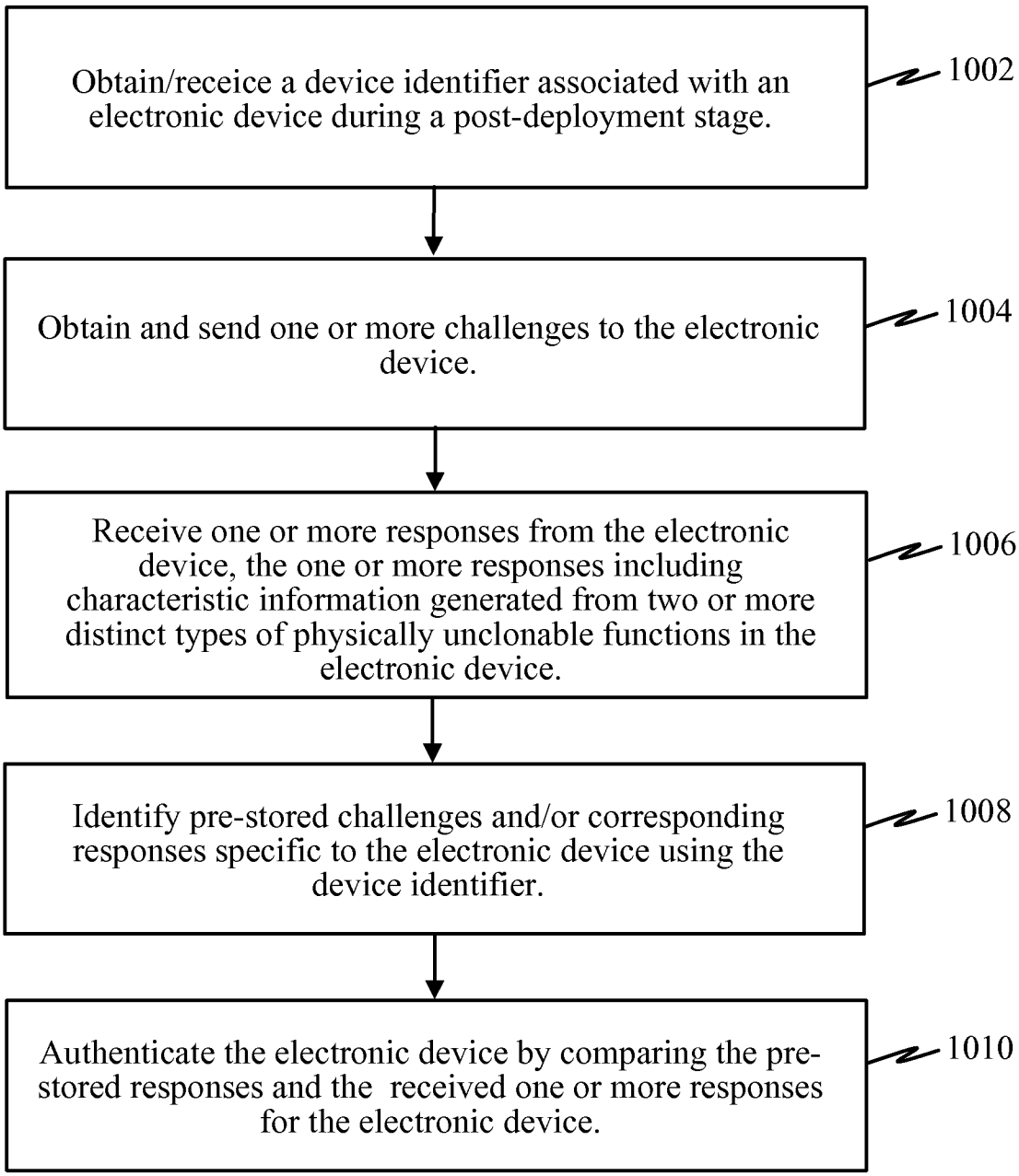

902
AUTHENTICATION DEVICE
910
Machine-Readable Medium
930
Device Identifier Instructions
932
SRAM PUF Verification Instructions
934
Circuit Delay PUF Verification Instructions
938
Authentication Instructions
904
Processing Circuit
922
Device Identifier Circuit/Module
924
SRAM PUF Verification Circuit/Module
926
Circuit Delay PUF Verification Circuit/Module
936
Authentication Circuit/Module
906
Storage Device
Circuit Delay PUF DB
SRAM PUF DB
Device Identifier DB
908
Communication Interface
Transmitter/ Receiver Circuit
912
914
916
918
To/From Electronic Device

FIG. 9



Method Operational on Authentication Device

FIG. 10

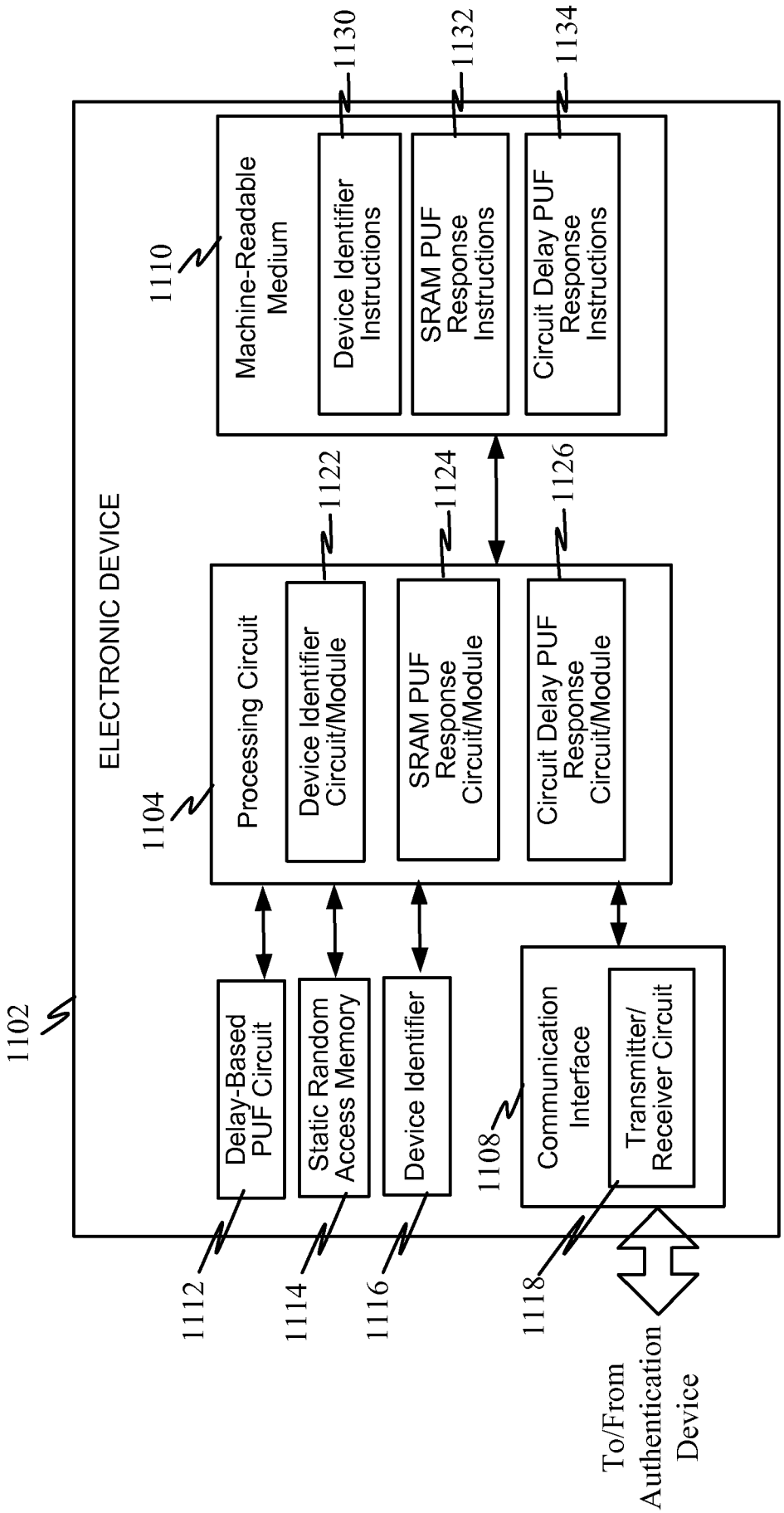
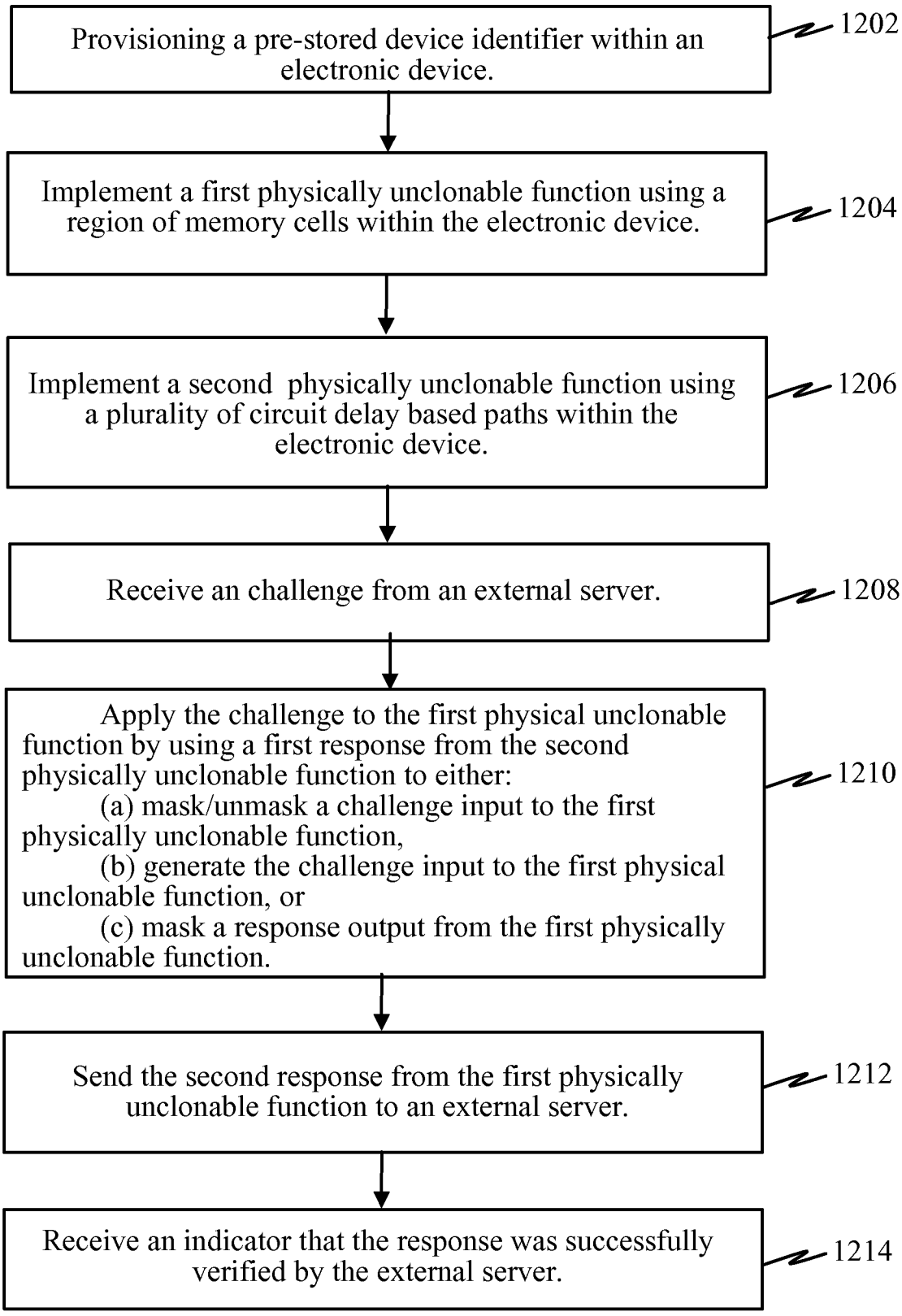

ELECTRONIC DEVICE
1102
Machine-Readable Medium
1110
Device Identifier Instructions
1130
SRAM PUF Response Instructions
1132
Circuit Delay PUF Response Instructions
1134
Processing Circuit
1104
Device Identifier Circuit/Module
1122
SRAM PUF Response Circuit/Module
1124
Circuit Delay PUF Response Circuit/Module
1126
Delay-Based PUF Circuit
1112
Static Random Access Memory
1114
Device Identifier
1116
Communication Interface
1108
Transmitter/ Receiver Circuit
1118
To/From Authentication Device

FIG. 11



Method Operational by Electronic Device

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/051718

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/58 H04L9/32
ADD.

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)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 615 571 A1 (GEMALTO SA [FR]) 17 July 2013 (2013-07-17) paragraphs [0006], [0042] - [0053] -----	1-54
A	Roel Maes ET AL: "Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions" In: "Towards Hardware-Intrinsic Security", 1 January 2010 (2010-01-01), Springer Berlin Heidelberg, Berlin, Heidelberg, XP055149570, ISSN: 1619-7100 ISBN: 978-3-64-214452-3 pages 1-36, DOI: 10.1007/978-3-642-14452-3_1, sections 2.1, 3.3.2, 3.4.1, 5.1, 5.2 ----- -/--	1-54

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* 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
31 October 2014	06/11/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Prins, Leendert

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/051718

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HOLCOMB D E ET AL: "Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers", IEEE TRANSACTIONS ON COMPUTERS, IEEE SERVICE CENTER, LOS ALAMITOS, CA, US, vol. 57, no. 11, 1 November 2008 (2008-11-01), pages 1-14, XP007918251, ISSN: 0018-9340 abstract	1-54
A	DE 10 2012 216677 B3 (SIEMENS AG [DE]) 13 June 2013 (2013-06-13) abstract	1-54

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/051718

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2615571 A1	17-07-2013	EP 2615571 A1	17-07-2013
		WO 2013107593 A1	25-07-2013
DE 102012216677 B3	13-06-2013	DE 102012216677 B3	13-06-2013
		WO 2014044510 A1	27-03-2014