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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 December 2024 (12.12.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/253590 A1

(51) International Patent Classification:
G06F 21/44 (2013.01) *G06F 21/73* (2013.01)
H04L 9/32 (2006.01) *G11C 11/40* (2006.01)

(21) International Application Number:
PCT/SG2024/050378

(22) International Filing Date:
07 June 2024 (07.06.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10202301638W 09 June 2023 (09.06.2023) SG

(71) Applicant: **NATIONAL UNIVERSITY OF SINGAPORE** [SG/SG]; 21 Lower Kent Ridge Road, Singapore 119077 (SG).

(72) Inventors: **BASU, Joydeep**; c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **TANEJA, Sachin**; c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **KONANDUR RAJANNA, Viveka**; c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **WANG, Tianqi**; c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG). **ALIOTO, Massimo**; c/o National University of Singapore, College of Design and Engineering, Department of Electrical and Computer Engineering, 21 Lower Kent Ridge Road, Singapore 119077 (SG).

(74) Agent: **OWEN, Man Hon Samuel**; Marks & Clerk Singapore LLP, Tanjong Pagar Post Office, P. O. Box 636, Singapore 910816 (SG).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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:
— *of inventorship (Rule 4.17(iv))*

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

(54) Title: METHODS AND SYSTEMS FOR GENERATING PHYSICAL UNCLONABLE FUNCTIONS

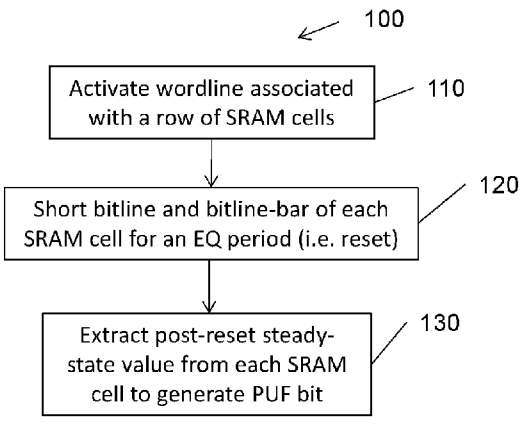


FIG.1

(57) Abstract: In a described embodiment, a method for generating a Physically Unclonable Function (PUF) bit from a Static Random-Access Memory (SRAM) cell is disclosed The method comprises activating a wordline (WL) associated with the SRAM cell for a wordline time period; equalizing the SRAM cell by shorting a bitline (BL) and bitline-bar (BLb) of the SRAM cell during the activation of the wordline for an equalization (EQ) time period to force the SRAM cell into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and extracting a post-reset steady-state value associated with a post-reset steady- state from the SRAM cell to generate the PUF bit, the post-reset steady-state value being read out after the wordline time period ends.

WO 2024/253590 A1

METHODS AND SYSTEMS FOR GENERATING PHYSICAL UNCLONABLE FUNCTIONS

Technical Field

The present application pertains generally to generating Physically Unclonable Functions (PUF), and in particular systems and methods for generating Physically Unclonable Function (PUF) bits from Static Random-Access Memory (SRAM) cells.

Background

The need for chip authentication and remote attestation has driven the demand for low-cost low-power physically unclonable functions (PUF) in resource-constrained secure systems.

SRAM PUFs are currently an industry standard given their high density, though their relatively poor stability reduces PUF array utilization under common stabilization techniques like masking, and requires extensive (and expensive) testing-time corner coverage.

The inclusion of PUFs as key building blocks in secure resource-constrained systems has led to the demand for low-cost low-power solutions with high density and high PUF array utilization under masking or other bit stabilization techniques.

To suppress the typically dominant area and energy of error correcting code (ECC) post-processing, PUF stabilization techniques were proposed to achieve ECC-less operation while meeting a required bit error rate (BER) target, such as self-checking/healing, and hot carrier injection burn-in, at the cost of increased circuit complexity and testing time.

As further solutions to increase array utilization (i.e., ratio of total PUF bits and the total cell count), PUFs delivering multiple bits per cell are considered, along with simultaneous reuse of unstable bits for true random number generator (TRNG), although their post-enhancement instability disallows ECC-less operation.

Regarding SRAM PUFs, they are widely adopted in industrial products thanks to the reuse of ubiquitously available SRAMs and their density, although their typically high native instability further exacerbates the above challenges.

Accordingly, state-of-the-art SRAM PUFs require expensive addition of ECC, high post-stabilization energy/bit (pJ/bit range), additional testing time and cost, additional relatively high supply voltages, and no SRAM design reuse due to custom bitcell requirement.

Therefore, it is desirable to provide a method and system that leverages PUF generation to address the disadvantages or limitations of the existing technologies or, at the very least, provide the public with a useful alternative.

Summary

The present disclosure aims to provide new and useful systems and methods for generating Physically Unclonable Functions (PUF), and in particular systems and methods for generating Physically Unclonable Function (PUF) bits from Static Random-Access Memory (SRAM) cells.

In a first aspect, the present invention proposes a method for generating a Physically Unclonable Function (PUF) bit from a Static Random Access Memory (SRAM) cell, the method comprising: activating a wordline (WL) associated with the SRAM cell for a wordline time period; equalizing the SRAM cell by shorting a bitline (BL) and bitline-bar (BLb) of the SRAM cell during the activation of the wordline for an equalization (EQ) time period to force the SRAM cell into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and extracting a post-reset steady-state value associated with a post-reset steady-state from the SRAM cell to generate the PUF bit, the post-reset steady-state value being read out after the wordline time period ends.

In an embodiment, the method may be applied to a pair of SRAM cells, wherein to extract a second PUF bit from the pair of SRAM cells, the method may further comprise: determining if a first SRAM cell of the pair of SRAM cells reaches its post-reset steady-state earlier than a second SRAM cell of the pair of SRAM cells, or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and forming the second PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the method may further comprise: extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and comparing the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

In some embodiments, the PUF bit is read at the end of the wordline time period.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row of SRAM cells, and wherein the method is adapted to extract PUF bits from every SRAM cell in the row of SRAM cells.

In a second aspect, the present invention proposes a method for generating a single or multiple Physically Unclonable Function (PUF) bit(s) from a pair of Static Random-Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells. The method comprises: activating a wordline (WL) associated with the pair of SRAM cells for a wordline time period; equalizing the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value optionally yielding the or a first PUF bit and being read out after the wordline time period ends; determining if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and forming the PUF bit, or a second PUF bit, based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In an aspect, the present invention proposes a method for generating a single or multiple Physically Unclonable Function (PUF) bit(s) from a pair of Static Random-Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells. The method comprises: activating a wordline (WL) associated with the pair of SRAM cells for a wordline time period; equalizing the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM

cells, the post-reset steady-state value optionally yielding the or a first PUF bit and being read out after the wordline time period ends; and forming the PUF bit, or a second PUF bit, based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, the method includes the step of determining if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the method may further comprise: extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and comparing the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row of SRAM cells, and wherein the method is adapted to extract bits from every SRAM cell in the row of SRAM cells.

In a third aspect, the present invention proposes a method for generating one or more Physically Unclonable Function (PUF) bits from a pair of Static Random-Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells. The method comprises: activating a wordline (WL) associated with the pair of SRAM cells for a wordline time period; equalizing the SRAM cells by shorting their

corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value being read out after the wordline time period ends; determining if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; digitizing the difference of the post-reset resolution time period of the SRAM cells being compared into one or more discrete level(s); and forming the one or more PUF bits corresponding to the digitized discrete level(s), and based on the determination in relation to the resolution time periods of the first and second SRAM cells.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row of SRAM cells, and wherein the system is adapted to extract bits from every SRAM cell.

In a fourth aspect, the present invention proposes a method for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random-Access Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell in a row of SRAM cells. The method comprises: activating a wordline (WL) associated with the row of SRAM cells for a wordline time period; equalizing the SRAM cells within the row by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit corresponding to each SRAM cell, the post-reset steady-state value being read out after the wordline time period ends.

In some embodiments, to extract a second PUF bit, the method may further comprise: determining if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and forming the second PUF bit based on the determination

in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the method may further comprise: extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and comparing the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row, and wherein the method is adapted to extract bits from every SRAM cell in the row of SRAM cells.

In a fifth aspect, the present invention proposes a system for generating a Physically Unclonable Function (PUF) bit from a Static Random Access Memory (SRAM) cell, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to: activate a wordline (WL) associated with the SRAM cell for a wordline time period; equalize the SRAM cell by shorting a bitline (BL) and bitline-bar (BLb) of the SRAM cell during the activation of the wordline for an equalization (EQ) time period to force the SRAM cell into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and extract a post-reset steady-state value associated with a post-reset steady-state from the SRAM cell to generate the PUF bit, the post-reset steady-state value being read out after the wordline time period ends.

In some embodiments, to extract a second PUF bit from the pair of SRAM cells, the data storage further stores computer program instructions operable to cause the processor to: determine if a first SRAM cell of the pair of SRAM cells reaches its post-reset steady-state earlier than a second SRAM cell of the pair of SRAM cells, or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and form the second PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the data storage further stores computer program instructions operable to cause the processor to: extract a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and compare the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the system is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

In some embodiments, the PUF bit is read at the end of the wordline time period.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row of SRAM cells, and wherein the system is adapted to extract bits from every SRAM cell in the row of SRAM cells.

In a sixth aspect, the present invention proposes a system for generating a Physically Unclonable Function (PUF) bit from a pair of Static Random Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of

SRAM cells, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to: activate a wordline (WL) associated with the pair of SRAM cells for a wordline time period; equalize the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; extract a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value being read out after the wordline time period ends; determine if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and form the PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the data storage further stores computer program instructions operable to cause the processor to: extract a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and compare the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the system is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row of SRAM cells, and wherein the system is adapted to extract bits from every SRAM cell in the row of SRAM cells.

In a seventh aspect, the present invention proposes a system for generating one or more Physically Unclonable Function (PUF) bits from a pair of Static Random Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to: activating a wordline (WL) associated with the pair of SRAM cells for a wordline time period; equalizing the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value being read out after the wordline time period ends; determining if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; digitizing the difference of the post-reset resolution time period of the SRAM cells being compared into one or more discrete level(s); and forming the one or more PUF bits corresponding to the digitized discrete level(s), and based on the determination in relation to the resolution time periods of the first and second SRAM cells.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row of SRAM cells, and wherein the system is adapted to extract bits from every SRAM cell.

In an eighth aspect, the present invention proposes a system for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random Access Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell in a row of SRAM cells, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to: activate a wordline (WL) associated with the

row of SRAM cells for a wordline time period; equalize the SRAM cells within the row by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and extract a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit corresponding to each SRAM cell, the post-reset steady-state value being read out after the wordline time period ends.

In some embodiments, to extract a second PUF bit the data storage further stores computer program instructions operable to cause the processor to: determine if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and form the second PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the data storage further stores computer program instructions operable to cause the processor to: extract a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and compare the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the system is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row, and wherein the system is adapted to extract bits from every SRAM cell in the row of SRAM cells.

In a ninth aspect, the present invention proposes a method for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random-Access Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell in a row of SRAM cells. The method comprises activating a wordline (WL) associated with the row of SRAM cells for a wordline activation or time period; equalizing the SRAM cells within the row by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; disabling or deactivating EQ to remove the shorting of bitline and bitline-bar of each SRAM cell, thereby allowing the bitcell to settle to a natural state set or determined by internal mismatch or internal variation between the first and second SRAM cells; and extracting a post-reset steady-state value associated with a or the post-reset steady-state from each of the SRAM cells to generate a first PUF bit, the post-reset steady-state value being read out after the wordline time period ends.

In some embodiments, to extract a second PUF bit, the method may further comprise determining if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period of the respective SRAM cell; and forming the second PUF bit based on the above determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution, instead of the 1-bit resolution used above for the extraction of a second PUF bit.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell or vice-versa, the method may further comprise extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period, and/or after the equalization is disabled or deactivated; and comparing the first transient time

value with the second transient time value, the first SRAM cell is determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution, instead of the 1-bit resolution used above for the extraction of a second PUF bit.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline activation or time period.

In some embodiments, the SRAM cell comprises 6-transistors (6T) SRAM cell.

In some embodiments, the wordline activation or time period and the equalization activation or time period are initialized at the same time, or the equalization is activated earlier than the wordline activation or time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row, and the method is adapted to extract bits from every SRAM cell or cells.

In a tenth aspect, the present invention proposes a method for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random-Access Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell in a row of SRAM cells. The method comprises activating a wordline (WL) associated with the row of SRAM cells for a wordline time period; equalizing the SRAM cells within the row by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit, the post-reset steady-state value being read out after the wordline time period ends.

In some embodiments, to extract a second PUF bit, the method may further comprise determining if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and forming the second PUF bit based on the above determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves

earlier than the second SRAM cell and a value of "0" (alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In some embodiments, the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution, instead of the 1-bit resolution used above for the extraction of a second PUF bit.

In some embodiments, to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell or vice-versa, the method may further comprise extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and comparing the first transient time value with the second transient time value, the first SRAM cell is determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

In some embodiments, the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution, instead of the 1-bit resolution used above for the extraction of a second PUF bit.

In some embodiments, the first PUF bit and the second PUF bit are read at the end of the wordline time period.

In some embodiments, the SRAM cell comprises a 6-transistors (6T) SRAM cell.

In some embodiments, the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

In some embodiments, the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row, and the method is adapted to extract bits from every SRAM cell or cells.

In an eleventh aspect, the present invention proposes a system comprising a processor and a data storage storing computer program instructions operable to cause the processor to carry out any one or more of the method steps of the first to tenth aspects as described herein.

The above description is provided as an overview of some implementations of the present disclosure. Further description of those implementations, and other implementations, are described in more detail below.

Brief Description of the Drawings

Embodiments of the invention will now be explained for the sake of example only, with reference to the following figures in which:

FIG.1 illustrates a flow chart of an example embodiment of a method according to the invention disclosed herein;

FIG.2A and 2B illustrate flow charts of alternative example embodiments of a method according to the invention disclosed herein;

FIG.3 illustrates circuit diagrams according to an example embodiment of the invention disclosed herein;

FIG.4A illustrates a timing diagram of conventional operation of SRAM cells in a read mode;

FIG.4B illustrates a timing diagram of SRAM cells according to an example embodiment of the invention disclosed herein;

FIG.5A illustrates a circuit diagram of an SRAM cell in operation according to prior art methods of PUF bit extraction;

FIG.5B illustrates a circuit diagram of an SRAM cell in operation according to an example embodiment of the invention disclosed herein;

FIG.6A shows a graph of improvements in bit error rate for the example embodiments of the invention disclosed herein;

FIG.6B shows a graph of improvements in unstable bit percentage for the example embodiments of the invention disclosed herein;

FIG.6C shows a graph of improvements in noise performance for the example embodiments of the invention disclosed herein;

Fig.7 illustrates stability and entropy performance of the example embodiments of the invention disclosed herein; and

Fig.8 illustrates various performance parameters of the example embodiments of the invention disclosed herein.

Detailed Description

Embodiments will now be discussed with reference to the accompanying FIGs, which depict one or more exemplary embodiments. These embodiments are described in sufficient detail to enable those skilled in the art to practice the embodiment, and it is to be understood that mechanical, logical, and other changes may be made without departing from the spirit or scope of the embodiments or the invention. Therefore, embodiments may be implemented in many different forms and should not be construed as limited to the embodiments set forth herein, shown in the FIGs, and/or described below.

As used in this disclosure, the terms "device," "module," "system," "apparatus," or the like are generally intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution. For example, a component or a module may be, but is not limited to being, a process running on a processor, a processor, an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a controller and the controller can be a component or a module. One or more components/modules may reside within a process and/or thread of execution and a component may be localized on one computer and/or distributed between two or more computers.

Herein, the term "PUF" refers to a physical or physically unclonable function, and may be considered a digital fingerprint originating from a physical device, based on conditions and/or inputs to the device. The PUF may serve as a unique identifier, and may be an output of the physical device that cannot be reproduced or cloned in a physical way (i.e., by making another physical device using the same technology), due to inherent and unique variations occurring in the production of the physical device. For example, an SRAM (static random-access memory) cell in a row of SRAM cells in a memory chip may comprise unique fluctuations and variations occurring during the semiconductor manufacturing process that result in a unique output from that cell. Across a row of SRAM cells, this may result in a unique identifier that may be repeatably obtained based on conditions and/or inputs to the device.

Furthermore, the claimed subject matter may be implemented as a method, apparatus, or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof to control a computer to implement the disclosed subject matter. For instance, the claimed subject matter may be implemented as a computer-readable medium embedded with a computer executable program, which encompasses a computer program accessible from any computer-readable storage device or storage media. For example, computer readable media can include but are not limited to magnetic storage devices (e.g., hard disk, floppy disk, magnetic strips, etc.), optical disks (e.g.,

compact disk (CD), digital versatile disk (DVD), etc.), smart cards, and flash memory devices (e.g., card, stick, key drive, etc.).

Unless otherwise defined, all terms (including technical and scientific terms) used herein are to be interpreted as is customary in the art. It will be further understood that terms in common usage should also be interpreted as is customary in the relevant art.

Physical unclonable function(s) (PUFs) are a key building block in recent secure resource-constrained systems (e.g. IoT devices) which may require low-cost low-power solutions with high density and high PUF array utilization, together with masking or other bit stabilization techniques. To suppress the typically dominant area and energy of error correcting code (ECC) post-processing, aggressive PUF stabilization techniques are used to achieve ECC-less operation while meeting the required bit error rate target, such as self-checking/healing and hot carrier injection burn-in, at the cost of increased circuit complexity and testing time. SRAM cell based PUFs are widely adopted in industrial products thanks to the reuse of ubiquitously available SRAMs and their density, although their typically high native instability further exacerbates the above challenges. Accordingly, state-of-the-art SRAM PUFs require expensive addition of ECC, high post-stabilization energy/bit, additional testing time and cost, additional relatively high supply voltages, and no SRAM design reuse due to custom bitcell requirement. Additional background details are provided in J. Basu, S. Taneja, V. K. Rajanna, T. Wang and M. Alioto, "*ECC-Less Multi-Level SRAM Physically Unclonable Function and 127% PUF-to-Memory Capacity Ratio with No Bitcell Modification in 28nm*," 2023 IEEE Symposium on VLSI Technology and Circuits (VLSI Technology and Circuits), Kyoto, Japan, 2023, pp. 1-2, which is incorporated by reference herein.

The invention as described herein may address the above commercial challenges by proposing a method and system for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random-Access Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell in a row of SRAM cells. In an example embodiment, the invention as described herein may result in an ECC-less commercial 6T SRAM based PUF yielding 2 PUF bits/bitcell.

Further, the proposed invention may be implemented on a standard-cell-based design that allows fully automated digital design flow for uncomplicated adoption and system integration with no need of SRAM cell modification.

FIG.1 illustrates a flow chart of an example embodiment of a method 100 according to the invention disclosed herein. In an example embodiment, a method is proposed for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random-Access

Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell, for example, the post-reset steady-state value from each SRAM cell in a row of SRAM cells.

In an example embodiment, the method may comprise the step 110 of activating a wordline (WL) associated with the row of SRAM cells for a wordline time period. Next, the SRAM cells may be equalized within the row at step 120 by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period. This may force each of the SRAM cells into a metastable (reset) state.

In an example embodiment the steps of activating the wordline 110 and equalization 120 may be reversed, for example, the equalization step 120 may occur before the wordline step 110. It will be understood that the order of activation of wordline and equalization could be reversed, occur sequentially or simultaneously in any order.

The method as described herein may require the equalization (EQ) time period to overlap with the wordline (WL) time period.

In an example embodiment (not shown), the equalization activation step 120 may be separated into two steps. In a first step, the equalization may be activated, by shorting the corresponding bitline (BL) and bitline-bar (BLb) of respective SRAM cells, during the activation of the wordline. In a second step, the equalization may be deactivated, by removing or deactivating or disabling the shorting of the corresponding bitline and bitline-bar of each SRAM cell. In an example embodiment, the equalization may be activated as a pulse, and may be activated for a shorter time than the wordline activation as described herein. It will be understood that the equalisation period may cause a reset action of a respective SRAM cell, which may lead to a post-reset steady-state that may be determined by inherent and unique variations occurring in the production of the physical device. For example, as set out above, an SRAM cell in a row of SRAM cells in a memory chip may comprise unique fluctuations and variations occurring during the semiconductor manufacturing process that result in a unique output from that cell upon reset.

The method may next comprise extracting at step 130 a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit (for example bit1), the post-reset steady-state value being read out after the wordline time period ends.

FIG.2A illustrates a flow chart of an example embodiment of a method 200 according to the invention disclosed herein. In an example embodiment, the method as described herein may comprise extracting a second PUF bit (for example bit2). The method may comprise steps 110

to 130 as described above in relation to FIG.1, i.e. the step 210 of activating a wordline associated with the row of SRAM cells for a wordline time period; equalizing within the row at step 220 by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization time period; and extracting at step 230 a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit.

As described above in relation to FIG.1, in an example embodiment the FIG.2 steps of activating the wordline 210 and equalization 220 may be reversed, for example, the equalization step 120 may occur before the wordline step 110. It will be understood that the order of activation of wordline and equalization could be reversed, occur sequentially or simultaneously in any order.

The method as described herein may require the equalization (EQ) time period to overlap with the wordline (WL) time period.

In an example embodiment (not shown), the FIG.2 equalization activation step 220 may be separated into two steps. In a first step, the equalization may be activated, by shorting the corresponding bitline (BL) and bitline-bar (BLb) of respective SRAM cells, during the activation of the wordline. In a second step, the equalization may be deactivated, by removing or deactivating or disabling the shorting of the corresponding bitline and bitline-bar of each SRAM cell. In an example embodiment, the equalization may be activated as a pulse, and may be activated for a shorter time than the wordline activation as described herein. It will be understood that the equalisation period may cause a reset action of a respective SRAM cell, which may lead to a post-reset steady-state that may be determined by inherent and unique variations occurring in the production of the physical device. For example, as set out above, an SRAM cell in a row of SRAM cells in a memory chip may comprise unique fluctuations and variations occurring during the semiconductor manufacturing process that result in a unique output from that cell upon reset.

The method described in FIG.2A may further comprise a differential comparison of SRAM bitcells (for any pair of bitcells in a row). In an example embodiment, the differential comparison may include determining at step 240 if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell, or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is identified as a resolution time period. Next, the method may comprise forming, generating or extracting the second PUF bit at step 250 based on the above determination in relation to the resolution time periods of the first and second SRAM cells. In an example embodiment, the second PUF bit is assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and

a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

In an example embodiment, the method as described herein may allow extraction of further additional PUF bits (for example, bit3, bit4, etc...) by digitizing the difference of the post-reset resolution time periods of the SRAM cells being compared with a higher resolution, instead of the 1-bit resolution used above for the extraction of a second PUF bit (for example bit2).

FIG.2B illustrates a flow chart of an example embodiment of a method 201 according to the invention disclosed herein. The method may comprise steps 210 to 250 as described above in relation to FIG.2A, i.e. the step 211 of activating a wordline associated with the row of SRAM cells for a wordline time period; equalizing within the row at step 221 by shorting their (i.e. the respective SRAM cells) corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization time period; extracting at step 231 a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit; determining if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell, or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is identified as a resolution time period; and generating the second PUF bit at step 251 based on the above determination in relation to the resolution time periods of the first and second SRAM cells.

The method described in FIG.2B may further comprise additional steps 241 and 242 as illustrated. For example, the step of determining if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, (i.e. corresponding to step 240 in FIG.2A) may comprise additional sub-steps 241 and 242. For example, firstly, the method may comprise the step 241 of extracting a first transient time value associated with a resolution of the first SRAM cell, and a second transient time value associated with a resolution of the second SRAM cell. In an example embodiment, the first and second transient time values being each measured from the time immediately after the equalization time period, i.e. when the equalization is deactivated.

Next, the method as illustrated in FIG.2B may compare the first transient time value with the second transient time value at step 242. In an example embodiment at 242, the first SRAM cell is determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value. Alternatively, in an example embodiment (not shown), the second SRAM cell is determined to reach its post-reset steady-state earlier than the first SRAM cell if the second transient time value is smaller than the first transient time value (i.e. vice-versa).

It will be understood that differential comparison of the SRAM cells or bitcells, for example that described herein in relation to steps 240 (in FIG.2A), and 241, 242, (in FIG.2B), can be made for any pair of bitcells (e.g. typically adjacent bitcells, but this is not required) which allows bit extraction from every bitcell (not half of them as in some prior art methods).

Further, in the example embodiment as disclosed herein it will be understood that each bit of the type "PUF bit-1", or first PUF bit, is generated or extracted from each SRAM cell of the SRAM row or array. For example, the PUF bits extracted or generated at step 130 in FIG.1 may be extracted or generated from each SRAM cell. In addition, each bit of type "PUF bit-2", or second PUF bit, is generated or extracted from a pair of SRAM cells in a row as described herein, for example at steps 250 and 251 in FIGs.2A and 2B, utilising the transient time value differences between first and second SRAM cells reaching their respective post-reset steady-state condition.

In an example embodiment, the first PUF bit, i.e. extracted or generated at step 130 in FIG.1, or 230/231 in FIGs.2A and 2B, may be read out after the end of the wordline time period (i.e. steady state). The optional second, and optional subsequent, PUF bits (i.e. transient), such as those extracted or generated at steps 250 and 251 in FIGs.2A and 2B, may be extracted before the end of the wordline time period by digitizing the post-reset resolution time difference between the two considered bitcells. In an example embodiment, the PUF bits may be read out (i.e., digitally transferred to the output) after the end of the wordline time period.

In an example embodiment, the systems and methods as disclosed herein may be adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution, instead of the 1-bit resolution described above for the extraction of a second PUF bit. Put another way, the digitization of the resolution time difference as described herein may allow the generation and/or extraction of more than the second PUF bit (e.g., a third or fourth PUF bit, etc.) by increasing the bit resolution of the digitisation of the difference in the post-reset resolution time period of the SRAM cells being compared.

In an example embodiment, the method as described herein may read the first PUF bit and the second PUF bit at the end of the wordline time period.

Although the system and methods described herein refer to an SRAM cell, it will be understood that said systems and methods can be applied over an array of SRAM cells to achieve a plurality of PUF bits.

In an example embodiment, the SRAM cell comprises a 6-transistors (6T) SRAM cell. However, it will be understood that the systems and methods as disclosed herein may be

operable to generate a PUF based on SRAM of any configuration and/or layout. For example, the systems and methods of the present disclosure can operate in 4T SRAM cell(s) (which are a symmetrical structure, similar to the 6T SRAM cells as described herein).

In an example embodiment, the wordline time period and the equalization time period are initialized at the same time, however, in an alternative embodiment the equalization time period is started earlier than the wordline time period. It will be understood that in the methods and systems of the present disclosure, it may be necessary to create an overlap between the wordline time period and the equalization time period, but wordline time period and the equalization time period do not need to start at the same time. For example, the equalization time period can start earlier or simultaneously with the wordline time period for determining a time overlap to induce the reset process as described herein.

In an example embodiment the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row. In this way, the method as described herein may be adapted to extract bits from every SRAM cell(s).

FIG.3 illustrates an example embodiment of a circuit diagram of a 6T SRAM bitcell 300, i.e. bit1[i] generation as descried herein (where i = 1, 2, 3, ... may denote the index number of a particular SRAM cell in the row of bitcells). In the example embodiment, the bitcell comprises a wordline (WL) indicated by reference 301, and voltage nodes including bitline (BL) indicated by reference 302, bitline bar (BLb) indicated by reference 303, and storage nodes Q indicated by reference 304 and Qb indicated by reference 305. In the example embodiment, corresponding bitline capacitances C_{BL}, indicated by reference 306, and C_{BLb}, indicated by reference 307, are shown. The equalisation transistor EQ 308 is shown, which may be a conventional column level transistor, and may be configured to pulse (enable) the equalization signal EQ to provide for a reset state as described herein.

The example embodiment of FIG.3 may provide for a PUF generation or extraction based on bitcell reset and polarity-independent arbiter as part of pitch-matched column peripheral circuity. In this example embodiment, the first PUF bit1 from each bitcell may be extracted from a post-reset state of the bitcell (i.e., post-reset values at storage nodes Q and Qb), such as bitcell bit1 300 as described herein, rather than a conventional or prior art power-up extraction of a PUF bit.

Alternatively, or in addition, a second bit, bit2, may be generated from a resolution time of two bitcells. In an example embodiment shown in FIG.3 at 310, first and second bitline inputs (from two cells) may be used to generate a second PUF bit, bit2, as described herein. Bitline input BL_i, indicated by reference 311, and bitline bar input BLb_i, indicated by reference 312, may comprise the first input. Similarly, bitline input BL_{i+1}, indicated by reference 313, and bitline bar

input BLb_{i+1}, indicated by reference 314, may comprise the second input. Both inputs may be provided to separate resolution identifiers 321 and 322, which may comprise resolution to edge converters. In this example embodiment, the resolution time of each bitcell of a pair of bitcells *i*, and *i+1*, may be digitized via respective resolution to edge converters 321 and 322, where bitline and bitline bar of each respective bitcell are sent to respective resolution identifiers 321 and 322. In an example embodiment, the output of each resolution identifiers 321 and 322 may feed into an arbiter 323, for example a NAND arbiter, to produce a second bit, bit2, based on a resolution time difference between a pair of bitcells, for example bitcells *i*, and *i+1*.

In FIG.3, circuit 330 represents an example embodiment of a resolution identifier, such as 321, 322 as set out herein. In an example embodiment, the resolution identifier may comprise a resolution to edge converter.

In an example embodiment, resolution identifier 330 may comprise a resolution to edge converter circuit as shown. In an example embodiment, circuit 330 may generate a rising-edge whenever a corresponding bitcell resolves. In an example embodiment this may be independent of the polarity of resolution of the bitcell. Whilst the circuit 330 shown in FIG.3 is an example circuit implementation to generate a rising edge on bitcell resolution, it will be understood that alternative circuit implementations may be utilised to obtain the resolution identification or detection as described herein.

In an example embodiment, the resolution identifier circuit 330 may be provided as an additional modification to the periphery of a conventional SRAM. Alternatively, or in addition, the resolution identifier circuit may be implemented as part of the SRAM device, or provided as a separate circuit for generating a rising edge on bitcell resolution, to allow identification of a resolution of a bitcell.

For a pair of bitcells, the two generated rising edges may be fed to the arbiter 323 which can then determine which rising edge occurred (i.e., rose) earlier. In an example embodiment, at a PUF bitcell reset phase, bitcells within each row may be reset by activating the respective wordlines, and simultaneously shorting the two respective bitlines via a column-level equalization transistor. In an example embodiment, this may be accomplished by pulsing the equalization signal EQ for a short time. This may advantageously avoid the need for an accurate initialization voltage, whilst providing an initialised state from where a PUF may be extracted.

In an example embodiment, at a resolution phase the EQ may be disabled, and each bitcell may settle to a natural state set due to inherent internal mismatch of the device as explained herein. In this way, the bitcell may be available for PUF readout at the end of the access.

The above-described overlapping activation of wordlines (WL) and equalization (EQ) may enable improved stability over conventional or prior art power-up state SRAM PUFs, in which wordlines may be instead activated only after equalization completion for readout.

In the invention as described herein, such stabilization may require a minor change in the control signal timing, and may expose bitcells to a much larger bitline capacitance compared to their intrinsic capacitance seen in power-up state resolution. Advantageously, the higher capacitance seen by the bitcell during resolution may suppress noise and therefore improve PUF bit1 stability and repeatability.

FIG.4A illustrates a conventional read mode SRAM timing, and FIG.4B illustrates an example embodiment of timing of the systems and methods of the invention as disclosed herein. In an example embodiment, the invention as disclosed herein may induce metastability and successive mismatch-driven resolution.

FIG.4A illustrates a conventional timing diagram 400 showing a conventional or prior art timing for SRAM read mode. As shown at 410, the equalisation 430 and wordline 420 do not overlap. In a conventional read out mode, the wordline 420 may be activated only when equalisation 430 of the SRAM cell(s) is completed.

FIG.4B illustrates an example embodiment of a modified timing diagram 401 for PUF bitcell reset according to an example embodiment of the invention as disclosed herein. FIG.4B illustrates an example of a modified timing, i.e. modified over the conventional timing in FIG.4A. The timing illustrated in FIG.4B may be for PUF bitcell reset and PUF bit1 and bit2 generation as described herein. The example of FIG.4B may provide for PUF bit generation from a fabrication induced mismatch dependent post-reset steady state of the SRAM cell, and/or a transient or resolution completion order of SRAM cells, as described herein.

FIG.4B illustrates timing for a pair of SRAM cells, showing a start time for PUF bit generation 402, and an end time when PUF bit(s) are read 403, which may be a completion time where PUF bit(s) are read, generated, and/or extracted. FIG.4B shows timing of a pair of cells, comprising cell *i*, denoted with reference 441, and SRAM cell *i+1*, denoted with reference 451, which may be adjacent cells in an SRAM bitcell array as described herein. In this example, as wordline 421 and equalisation 431 are both activated such that there is an overlap, cells *i* (441) and *i+1* (451) enter a reset phase, or metastable state 461. In this example, the wordline is activated, and the equalisation is activated for a time such that the wordline and equalisation pulses overlap. As indicated at 411, the equalisation time is provided by activating an equalisation pulse, i.e. equalisation or reset of Q, Qb, BL and BLb.

Following the activated overlap of both the wordline 421 and equalisation 431, after some time the bitcells enter a resolution phase 471. In an example embodiment, the resolution phase 471 may correspond with the deactivation of the equalisation pulse as illustrated in FIG.4B. In this example embodiment, cell *i* (441) resolves high, as shown by reference 442, and provides a PUF bit of value 1 (or alternatively, 0), i.e. $Q_i = 1$, and bit1[i] = 1. Put another way, the bit1 value of bitcell *i* may equal the steady state value of said bitcell after resolution (in this case a 1). In contrast, in this example embodiment cell *i+1* (451) resolves low, as shown by reference 452, and provides a PUF bit of value 0 (or alternatively 1), i.e. $Q_{i+1} = 0$, and bit1[i+1] = 0. Put another way, the bit1 value of bitcell *i+1* may equal the steady state value of said bitcell after resolution (in this case a 0). In this way, a first or bit1 PUF bit or set of PUF bits may be extracted or generated from the SRAM cell array as described herein, in this case the extraction of two PUF bits from the resolution steady state value after equalisation or reset of a pair of bitcells.

FIG.4B also describes the generation or extraction of bit2, or a second PUF bit as described herein. In this example embodiment, the timing diagram indicates that the resolution of bitcell *i* (441) occurs earlier than the resolution of bitcell *i+1* (451). This is indicated by resolution point of bitcell *i* (441), indicated by reference 443, occurring before the resolution of bitcell *i+1* (451), indicated by reference 453. It will be understood that this resolution identification is independent of the actual resolution state of either bitcell (i.e. resolving high or low). In this example, the resolution of bitcell *i* (441) before bitcell *i+1* (451) is assigned a bit2 value of 1 (alternatively 0). In an alternative scenario, had bitcell *i+1* (451) resolved before bitcell *i*, (441) then the assigned bit2 value would be 0 (or alternatively 1). In this way, a second or bit2 PUF bit or set of PUF bits may be extracted or generated from the SRAM cell array. Put another way, bit2 or a second PUF bit may be generated or extracted from the post-reset transient response of a bitcell pair, i.e. order of resolution completion between bitcells or which bitcell in the pair resolves earlier.

In the example embodiment of FIG.4B, resolution order may be evaluated or determined by outputs of resolution identifiers (481 and 491) which may comprise a polarity-independent arbiter, for example 310 as shown in FIG.3, having output Arb[i], which in an example embodiment may be part of the pitch-matched column peripheral circuitry.

In an example embodiment, the order of resolution evaluated by identifiers 481 and 491 may determine the PUF bit value for a pair of SRAM bitcells as described herein. For example, if resolution identifier 481 for bitcell *i* (441) indicates a resolution in a time domain before resolution identifier 491 for bitcell *i+1* (451), as shown at reference 472, then the generated or extracted PUF bit may be designated 1 (or alternatively 0) as described above. Put another

way, the order of resolution completion of bitcell *i* (441) and bitcell *i+1* (451) sets the value of bit2, in this example embodiment as a 1, i.e. Arb[i] = 1, and hence bit2[i] = 1, but it will be understood this resolution order could be assigned a 0 in the alternative.

It will be understood that resolution timing comparison can occur between multiple SRAM cells in an array, such that bit1 and bit2 (and additional bits as required) PUF bits may be generated from every bitcell of the SRAM array as described herein.

In addition, as described herein, an example embodiment of the invention may be adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution, instead of the 1-bit resolution described above for the extraction of a second PUF bit, bit2. Put another way, the digitization by identifiers 481 and 491 which may comprise a polarity independent arbiter as described herein, occurs at a time period indicated by reference 472, and provides a single further PUF bit, i.e. bit2. However, it will be understood that the digitization of the resolution time difference 472 could be separated into multiple levels, for example, resolution time difference 472 could be digitized or separated or segregated into multiple potential bit identifiers, depending on the resolution time between bitcells. Put another way, the time difference 472 may be digitized into one or more discrete time partitions or discrete levels. In this way, the resolution time difference as described herein may allow the generation and/or extraction of more than the second PUF bit, bit2, (e.g., a third PUF bit, bit3, fourth PUF bit, bit4, etc.) by increasing the bit resolution of the digitisation of the difference in the post-reset resolution time difference periods 472 of the SRAM cells being compared.

The methods and systems as described herein may therefore provide for the simultaneous extraction and/or generation of multiple PUF bits, for example bit1 and bit2 as described herein, from the same reset operation of an SRAM cell.

It will be understood that the values and timings provided herein are for exemplary purposes only, and the resolution state of each SRAM cell may be assigned a corresponding PUF value as required.

FIG.5A shows an example embodiment of a conventional or prior art bitcell circuit operation 500. FIG.5B illustrates an example embodiment of a bitcell circuit operation 501 according to an embodiment of the invention as disclosed herein. The conventional or prior art PUF generating bitcell shown in FIG.5A illustrates a power-up readout condition where the PUF bit is generated as the power-up state of the cross-coupled latch (570), and includes the wordline (pass) transistors 520, 530, and EQ transistor 540 in the OFF-state condition. This is shown in FIG.5A by transistors 520 and 530 being in the OFF state, as well as EQ transistor 540

being in the OFF state. This condition leads to the small internal capacitances (580) loading the latch (570), which results in increased noise effects and therefore increased error rate of the extraction of the PUF bits.

In contrast, in the example embodiment of FIG.5B, the respective wordline may be activated, as shown by transistors 521 and 531 being in an ON state, and the bitlines may be shorted, by activating the EQ transistor 541, for example by a short EQ pulse to short the bitlines via EQ transistor 541 as described herein. In this example embodiment, the bitline capacitance 561 may be large (compared to that of the internal capacitances 580 in conventional power-up condition PUF generation of FIG.5A) and loads the latch 571 during its resolution from the metastable state when the EQ transistor 541 is turned off, which may lead to noise suppression as outlined herein, and improved error rate associated with extraction of one or more PUF bits.

It will be understood that the internal capacitance indicated at 580, 581 and the bitline capacitance indicated at 560, 561 are always present in the circuits 500 and 501 of FIGs.5A and 5B, respectively. However, due to the mode of operation of the circuit 500 in FIG.5A, only the small internal capacitance 580 influences the latch 570. In contrast, in an example embodiment, the circuit 501 of FIG.5B comprises a large bitline capacitance 561, as a result of the operation of circuit 501 as outlined above, including wordline and EQ activation. In the embodiment of 501 and FIG.5B, both the large bitline capacitance 561, and the small internal capacitance 581 may be present. However, the larger bitline capacitance 561 may have a dominating effect on the latch resolution, which may load the latch during resolution when the EQ is turned off, leading to noise suppression and improved error rate.

As illustrated in FIGs.6A to C, the invention as described herein may lead to PUF generation with improved performance and/or reliability. For example, the graph 600 in FIG.6A illustrates cumulative bit error rate (BER) 610 versus number of PUF evaluations 620 for a prior art power-up PUF method 630 (dashed line above) and the proposed post-reset state readout of the invention as described herein 640 (solid line below). In FIG.6A, graph 600, a drop in BER 650 is observed, and it is clear that the post-reset state readout method of the invention as described herein (640, solid line below) may provide an increase in stability by over four times compared to a conventional or prior art power-up PUF state readout (630, dashed line above, see e.g. circuit 500 shown in FIG.5A for conventional method, and circuit 501 shown in FIG.5B for method according to an embodiment of the invention as claimed herein).

The percentage of unstable bits may also reduce as bitline capacitance is increased, as shown in the graph 660 in FIG.6B, which shows post-reset readout stability 670 versus bitline capacitance 680. The graph 660 of FIG.6B illustrates that the percentage of unstable PUF bits

reduces 690 with increasing bitline capacitance. This may lead to improvements provided by the invention, which may provide for an increase in load capacitance for the cross-coupled latch within the SRAM cell, and therefore reduction in unstable bits as described herein.

As set out above, FIG.5B illustrates an example reset process of the system and methods as described herein, which may expose each bitcell to full bitline capacitance. This may be much larger than the intrinsic capacitance seen in conventional power-up SRAM PUF readout (i.e. as shown in FIG.5A). This may result in the post-reset readout of the methods and systems disclosed herein being significantly more stable than power-up conventional methods. Such stability improvement may be more pronounced at larger bitline capacitances, as shown in graph 691 of FIG.6C, which shows noise power spectral density (PSD) measured around reset (metastable point) at bitcell output, hence showing RMS noise reduction with increased bitline capacitance C_{BL}.

In an example embodiment, supply voltage reduction may further amplify the dominance of mismatch over noise. Similarly, higher bitline capacitances (e.g., more array rows) may further improve stability, as shown by the noise analysis in FIG.6C.

A further advantage of the invention as described herein is that the methods and systems described herein may allow bitcells to be selectively reset in specific rows in a single cycle. In this way, it may be possible to allow coexistence of PUF bits and storage bits within the same bank, with no need for SRAM bank power-down and flushing. This is in contrast to prior art conventional power-up PUF methods, which would require a power cycle to extract a PUF on power up.

In an example embodiment, bit1 is extracted from the steady-state post-reset value of each bitcell as described herein. In an example embodiment, bit2 may be simultaneously extracted from the post-reset transient as illustrated in FIG.4A and 4B, and described above.

In an example embodiment as described herein, the resolution time of each accessed PUF bitcell is compared with another bitcell, such as an adjacent bitcell in an array, and bit2 is defined by whether the earliest resolution occurs in the former or the latter bitcell. In this way, all bitcells in the array contribute to the PUF capacity, for example by being regularly compared with the adjacent bitcell. Since the order of occurrence of the resolution in the two bitcells is unknown upfront, a polarity-independent arbiter may assess the order independently of the direction taken by the bitline voltage in the resolution phase. The steady-state mechanisms introduced for both bit1 and bit2 are not tied to a specific bitcell design, and can hence reuse existing bitcell designs, which may be desirable from a design and qualification effort standpoint.

FIG.7 Illustrates stability and entropy performance of example embodiments of the systems and methods disclosed herein. Graph 710 illustrates native BER and percentage of unstable bits vs. PUF evaluations at nominal conditions. Graph 720 illustrates native BER and percentage of unstable bits vs. temperature. Graph 730 illustrates native BER and percentage of unstable bits vs. supply voltage V_{DD}, showing stability with supply voltage fluctuations. The diagram 740 illustrates bit1 and bit2 speckle patterns of 5k bits showing the random distribution of the generated '1' and '0' bits, together with Hamming Distance (HD) and Correlation values indicating the independence of the generated PUF bit1 and bit2. In an example embodiment, the speckle diagrams at 740 may qualitatively indicate that the generated "1" and "0" bits are randomly distributed without any spatial correlation; while the Correlation(bit1, bit2) value in 740 (i.e. correlation (bit1, bit2) = 0.0077) indicates the independence of the generated bits.

From FIG.7, the measured unstable bit ratio of bit1 (bit2) of 4.2% (22%) degrades to 9.1% (28%) across voltage fluctuations (0.65 V ± 0.05 V – as shown in graph 730) and 7.6% (36.8%) across temperatures (0 – 70 °C – as shown in graph 720). BER is improved to better than 1.5E-7 (2.2E-7) for bit1 (bit2) by masking only 12.5% (60.1% of the extra bits) unstable cells in the worst case. Overall, these results confirm ECC-less PUF operation for the two bits across voltage and temperature fluctuations, while retaining stability for 87.5% of bit1 and 39.9% of bit2. Being bit1 the most stable followed by bit2, their array utilization may be progressively lower due to the need for more pronounced masking to suppress errors, but each additional PUF bit still adds a significant net contribution to the overall PUF capacity. Overall, the proposed 2-bit/bitcell PUF achieves ECC-less operation at a PUF capacity that is >127% of memory capacity, and can be further improved by adding other conventional stabilization methods (e.g., TMV, SMV) to use less masking. More broadly, the above-100% PUF/SRAM capacity ratio fundamentally eliminates the need for aggressive masking ratio reduction down to near-zero to achieve adequate array utilization, which is well known to be challenging.

In an example embodiment, a prototype system was developed in 28-nm CMOS technology, and the PUF performance has been proven by silicon measurement results.

In an example embodiment, a 6T SRAM-based PUF macro is provided that may exhibit 2 PUF bits/bitcell to achieve a capacity well above the SRAM storage capacity and ECC-less operation for low-cost and low-power systems, and applicability to ubiquitously available SRAMs.

In an example embodiment, the first bit may be generated from post-reset state with column-level stabilization technique based on properly-timed bitline pair shorting for PUF bit noise mitigation, while minimally modifying the periphery and keeping the 6T bitcell array unaltered.

The second PUF bit may be extracted from each bitcell pair by digitizing the resolution time difference through an arbiter in column periphery. The proposed fully-digital and pitch-matched architecture is fully compatible with memory compiler automated SRAM generation at no additional testing time.

FIG.8 illustrates stability and entropy performance of example embodiments of the systems and methods disclosed herein. Graph 810 illustrates measured PUF bit1 and bit2 bias along SRAM columns at nominal condition after masking and XOR, confirming no significant skew due to column-level periphery., Graph 820 illustrates intra-PUF Hamming Distance and inter-PUF Hamming Distance. Graphs 830 and 840 illustrate autocorrelation function of PUF bit-1 830 (i.e. bit1 as described herein) and PUF bit-2 840 (i.e. bit2 as described herein). Table 850 illustrates NIST randomness test results for verifying the quality of the generated PUF bits.

FIG.8 shows in graph 820 that the inter-PUF (intra-PUF) Hamming distance mean for bit1 and bit2 is 50.11% and 50.09% (1.87% and 2.95%), and the resulting identifiability of 27X and 17X, which confirm that there are no fundamental differences among the two PUF bits, i.e. bit1 and bit2 as described herein. This may mean that both bit1 and bit2 can be reliably used in authentication and identification. From FIG.8, graph 830 and 840, no spatial pattern is noticeable across the array bitcells for the two bits, i.e. bit1 and bit2 as evidenced by the low value of the autocorrelation function at 95% confidence of 0.0225 and 0.0242, respectively. The two bits, i.e. bit1 and bit2, are also essentially uncorrelated and hence fully contribute to the overall entropy, as the phi (correlation) coefficient between bit1 and bit2 is lower than 0.0077. From a statistical quality perspective, FIG.8 graph 810 shows that the 0/1 bias across columns is close to ideal and hence centered around 50% with low 2.7-3.5% standard deviation under simple XOR post-processing, confirming that the column-level circuitry does not introduce any significant bias in any of the two bits.

In the example embodiment, the 28-nm testchip implementation of an 8 kbit/bank SRAM macro is compared with the relevant state of the art through measurements of five dice. Compared to prior SRAM PUFs, the proposed SRAM macro enables the extraction of two PUF bits per bitcell. The 2-bit extraction leads to an area/bit of 442 F^2 (F=min feature size) under the available logic rule-based commodity bitcell, and would expectedly further improve with pushed-rule bitcells in mass-produced products. Based on the BER better than 1.537E-7 for bit1 (2.172E-7 for bit2) (i.e., zero errors across all environmental conditions and dice), the proposed SRAM PUF is uniquely able to operate without ECC as opposed to other SRAM PUFs, while simultaneously not requiring extra testing time (e.g., burn-in) and custom bitcell for stabilization, and using only masking (masking ratio of 12.5% and 60.1% for the two bits). The energy/bit is higher than the ECC-less SRAM with custom bitcell in some prior SRAM

PUF implementations, and is expectedly much lower than the energy of SRAM PUFs when the pJ/bit penalty of ECC is included. Overall, the proposed SRAM PUF leads to a >127% PUF/SRAM ratio. Combined with the above stabilization techniques, the proposed PUF simultaneously achieves ECC-less operation while using the SRAM capacity in full and exceeding it.

In an example embodiment, the bitcell as described herein, may comprise a six-transistor (6T) Static Random-Access Memory (SRAM). In an example embodiment, the invention may comprise a Physically Unclonable Function (PUF) macro capable of generating 2 PUF bits per SRAM bitcell. This may yield a PUF capacity well above the SRAM storage capacity with no requirement to modify the SRAM cell.

In an example embodiment, the first PUF bit is generated from a steady-state post-reset bitcell state, with a column-level stabilization technique based on properly-timed bitline pair shorting for PUF bit noise mitigation, while minimally modifying the periphery and keeping the 6T bitcell array unaltered. Advantageously, the PUF bit may have >4X higher stability than conventional power-up based SRAM PUF. The second PUF bit may be extracted simultaneously from the post-reset transient response of each bitcell pair by digitizing the resolution time difference through an arbiter in column periphery.

The methods and systems as disclosed herein may comprise a fully-digital and pitch-matched SRAM PUF architecture, which may be compatible with memory compiler automated SRAM generation with no additional testing time.

In an example embodiment, the methods and systems as disclosed herein may provide for above-storage capacity and bitcell stability, which may enable ECC-less operation of the PUF. This may be advantageous for low-cost and low-power systems, for example those utilizing ubiquitously available SRAMs.

Non-limiting advantages of the methods and systems as disclosed herein may include:

High PUF stability - Improved stability achieved over conventional power-up state SRAM PUFs by using a minor change in the control signal timing and exposing the SRAM bitcells to the much larger bitline capacitance compared to their intrinsic capacitance seen in power-up state resolution. The higher capacitance suppresses noise during cell resolution, and hence, may improve PUF bit stability by up to around >4X over conventional power-up state readout. Supply voltage reduction further amplifies the dominance of mismatch over noise.

Above-storage capacity - Two PUF bits may be generated from each SRAM bitcell. Additionally, the enhanced PUF stability may lead to reduced masking requirement. These

features may contribute to a high PUF to memory capacity ratio (i.e., high bit density and high PUF array utilization).

SRAM design reuse – The methods and systems described herein reuse the ubiquitously available SRAMs. Modification of the conventional 6T SRAM bitcell design (i.e., a custom bitcell design) may not be required.

Simplified circuitry - The proposed methods and systems as disclosed herein may avoid the need for aggressive PUF stabilization techniques that are used to achieve ECC-less operation while meeting the required bit error rate (BER) target, such as self-checking/healing and hot carrier injection burn-in, at the cost of increased circuit complexity, testing time and cost.

ECC-less operation - The typically dominant area and energy of error correcting code (ECC) post-processing is made redundant leading to a low-cost low-power solution.

Coexistence of PUF bits and storage bits - Bitcells can be selectively reset in specific rows in a single cycle, thus allowing coexistence of PUF bits and storage bits within the same memory bank with no need for SRAM bank power-down and flushing as opposed to power-up SRAM PUF.

Fully-automated standard-cell based design - The proposed fully-digital and pitch-matched architecture is fully compatible with memory compiler automated SRAM generation. Automated placement and routing (PNR) in a single design iteration avoids manual optimization and iterative PNR.

Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the art that many variations of the embodiments can be made within the spirit and scope of the invention as defined by the claims. Moreover, features of one or more embodiments may be mixed and matched with features of one or more other embodiments.

Claims

1. A method for generating a Physically Unclonable Function (PUF) bit from a Static Random-Access Memory (SRAM) cell, the method comprising:

activating a wordline (WL) associated with the SRAM cell for a wordline time period;

equalizing the SRAM cell by shorting a bitline (BL) and bitline-bar (BLb) of the SRAM cell during the activation of the wordline for an equalization (EQ) time period to force the SRAM cell into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and

extracting a post-reset steady-state value associated with a post-reset steady-state from the SRAM cell to generate the PUF bit, the post-reset steady-state value being read out after the wordline time period ends.

2. The method of claim 1, applied to a pair of SRAM cells, wherein to extract a second PUF bit from the pair of SRAM cells, the method further comprises:

determining if a first SRAM cell of the pair of SRAM cells reaches its post-reset steady-state earlier than a second SRAM cell of the pair of SRAM cells, or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and

forming the second PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

3. The method of claim 2, wherein to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the method further comprises:

extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and

comparing the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

4. The method of claim 2 or claim 3, wherein the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

5. The method of claim 1, wherein the PUF bit is read at the end of the wordline time period, or wherein the first PUF bit and the second PUF bit are read at the end of the wordline time period.

6. A method for generating a Physically Unclonable Function (PUF) bit from a pair of Static Random-Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells, the method comprising:

activating a wordline (WL) associated with the pair of SRAM cells for a wordline time period;

equalizing the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period;

determining if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and

forming the PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of “1” (or alternatively “0”) if the first SRAM cell resolves earlier than the second SRAM cell and a value of “0” (or alternatively “1”) if the second SRAM cell resolves earlier than the first SRAM cell.

7. The method of claim 6, further comprising the step of extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value being read out after the wordline time period ends.

8. The method of claim 6 or claim 7, wherein to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the method further comprises:

extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and

comparing the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

9. The method of any one of claims 6 to 8, wherein the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

10. A method for generating one or more Physically Unclonable Function (PUF) bits from a pair of Static Random-Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells, the method comprising:

activating a wordline (WL) associated with the pair of SRAM cells for a wordline time period;

equalizing the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period;

extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value being read out after the wordline time period ends;

determining if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period;

digitizing the difference of the post-reset resolution time period of the SRAM cells being compared into one or more discrete level(s); and

forming the one or more PUF bits corresponding to the digitized discrete level(s), and based on the determination in relation to the resolution time periods of the first and second SRAM cells.

11. A method for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random-Access Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell in a row of SRAM cells, the method comprising:

activating a wordline (WL) associated with the row of SRAM cells for a wordline time period;

equalizing the SRAM cells within the row by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and

extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit corresponding to each SRAM cell, the post-reset steady-state value being read out after the wordline time period ends.

12. The method of claim 11, wherein to extract a second PUF bit, the method further comprises:

determining if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and

forming the second PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of “1” (or alternatively “0”) if the first SRAM cell resolves earlier than the second SRAM cell and a value of “0” (or alternatively “1”) if the second SRAM cell resolves earlier than the first SRAM cell.

13. The method of claim 12, wherein to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the method further comprises:

extracting a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and

comparing the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

14. The method of claim 12 or claim 13, wherein the method is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

15. The method of any one of claims 6 to 14, wherein the first PUF bit and the second PUF bit are read at the end of the wordline time period.

16. The method of any one of the preceding claims, wherein the SRAM cell comprises a 6-transistors (6T) SRAM cell.

17. The method of any one of the preceding claims, wherein the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

18. The method of any one of claims 2 to 17, wherein the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row of SRAM cells, and wherein the method is adapted to extract bits from every SRAM cell in the row of SRAM cells.

19. A system for generating a Physically Unclonable Function (PUF) bit from a Static Random-Access Memory (SRAM) cell, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to:

activate a wordline (WL) associated with the SRAM cell for a wordline time period;

equalize the SRAM cell by shorting a bitline (BL) and bitline-bar (BLb) of the SRAM cell during the activation of the wordline for an equalization (EQ) time period to force the SRAM cell into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and

extract a post-reset steady-state value associated with a post-reset steady-state from the SRAM cell to generate the PUF bit, the post-reset steady-state value being read out after the wordline time period ends.

20. The system of claim 19, further comprising a pair of SRAM cells, wherein to extract a second PUF bit from the pair of SRAM cells, the data storage further stores computer program instructions operable to cause the processor to:

determine if a first SRAM cell of the pair of SRAM cells reaches its post-reset steady-state earlier than a second SRAM cell of the pair of SRAM cells, or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and

form the second PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

21. A system for generating a Physically Unclonable Function (PUF) bit from a pair of Static Random-Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to:

activate a wordline (WL) associated with the pair of SRAM cells for a wordline time period;

equalize the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each

of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period;

extract a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value being read out after the wordline time period ends;

determine if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and

form the PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of "1" (or alternatively "0") if the first SRAM cell resolves earlier than the second SRAM cell and a value of "0" (or alternatively "1") if the second SRAM cell resolves earlier than the first SRAM cell.

22. A system for generating one or more Physically Unclonable Function (PUF) bits from a pair of Static Random-Access Memory (SRAM) cells, based on differential comparison of a first SRAM cell and a second SRAM cell of the pair of SRAM cells, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to:

activating a wordline (WL) associated with the pair of SRAM cells for a wordline time period;

equalizing the SRAM cells by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period;

extracting a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells, the post-reset steady-state value being read out after the wordline time period ends;

determining if the first SRAM cell reaches a post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period;

digitizing the difference of the post-reset resolution time period of the SRAM cells being compared into one or more discrete level(s); and

forming the one or more PUF bits corresponding to the digitized discrete level(s), and based on the determination in relation to the resolution time periods of the first and second SRAM cells.

23. A system for generating one or multiple Physically Unclonable Function (PUF) bits from each Static Random-Access Memory (SRAM) cell, based on differential comparison of a first SRAM cell and a second SRAM cell in a row of SRAM cells, the system comprising a processor and a data storage storing computer program instructions operable to cause the processor to:

activate a wordline (WL) associated with the row of SRAM cells for a wordline time period;

equalize the SRAM cells within the row by shorting their corresponding bitline (BL) and bitline-bar (BLb) during the activation of the wordline for an equalization (EQ) time period to force each of the SRAM cells into a metastable (reset) state, wherein the equalization time period overlaps with the wordline time period; and

extract a post-reset steady-state value associated with a post-reset steady-state from each of the SRAM cells to generate a first PUF bit corresponding to each SRAM cell, the post-reset steady-state value being read out after the wordline time period ends.

24. The system of claim 23, wherein to extract a second PUF bit the data storage further stores computer program instructions operable to cause the processor to:

determine if the first SRAM cell reaches its post-reset steady-state earlier than the second SRAM cell or vice-versa, wherein a time taken for a SRAM cell to reach its post-reset steady state is a resolution time period; and

form the second PUF bit based on the determination in relation to the resolution time periods of the first and second SRAM cells, the second PUF bit being assigned a value of “1” (or alternatively “0”) if the first SRAM cell resolves earlier than the second SRAM cell and a value of “0” (or alternatively “1”) if the second SRAM cell resolves earlier than the first SRAM cell.

25. The system of any one of claims 20 to 24, wherein to determine if the first SRAM cell reaches the steady-state earlier than the second SRAM cell, or vice-versa, the data storage further stores computer program instructions operable to cause the processor to:

extract a first transient time value associated with a resolution of the first SRAM cell and a second transient time value associated with a resolution of the second SRAM cell, the first and second transient time values being each measured from the time immediately after the equalization time period; and

compare the first transient time value with the second transient time value, the first SRAM cell determined to reach its post-reset steady-state earlier than the second SRAM cell if the first transient time value is smaller than the second transient time value (and vice-versa).

26. The system of any one of claims 20 to 25, wherein the system is adapted to allow extraction of further additional PUF bits by digitizing the difference of the post-reset resolution time period of the SRAM cells being compared with a higher resolution.

27. The system of any one of claims 20 to 26, wherein the first PUF bit and the second PUF bit are read at the end of the wordline time period.

28. The system of any one of claims 19 to 27, wherein the SRAM cell comprises a 6-transistors (6T) SRAM cell.

29. The system of any one of claims 19 to 28, wherein the wordline time period and the equalization time period are initialized at the same time, or the equalization time period is started earlier than the wordline time period.

30. The system of any one of claims 19 to 29, wherein the first SRAM cell and the second SRAM cell are in adjacent columns or are separated by one or more columns in the same row, and wherein the system is adapted to extract bits from every SRAM cell in the row of SRAM cells.

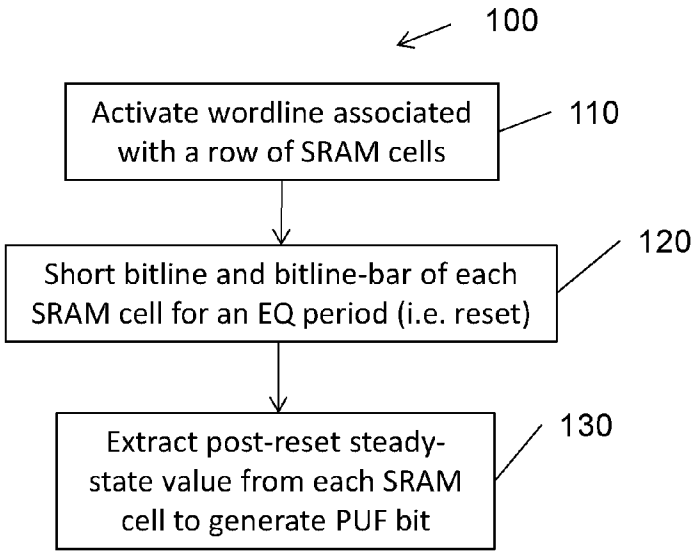

100
Activate wordline associated with a row of SRAM cells
110
Short bitline and bitline-bar of each SRAM cell for an EQ period (i.e. reset)
120
Extract post-reset steady-state value from each SRAM cell to generate PUF bit
130

FIG.1

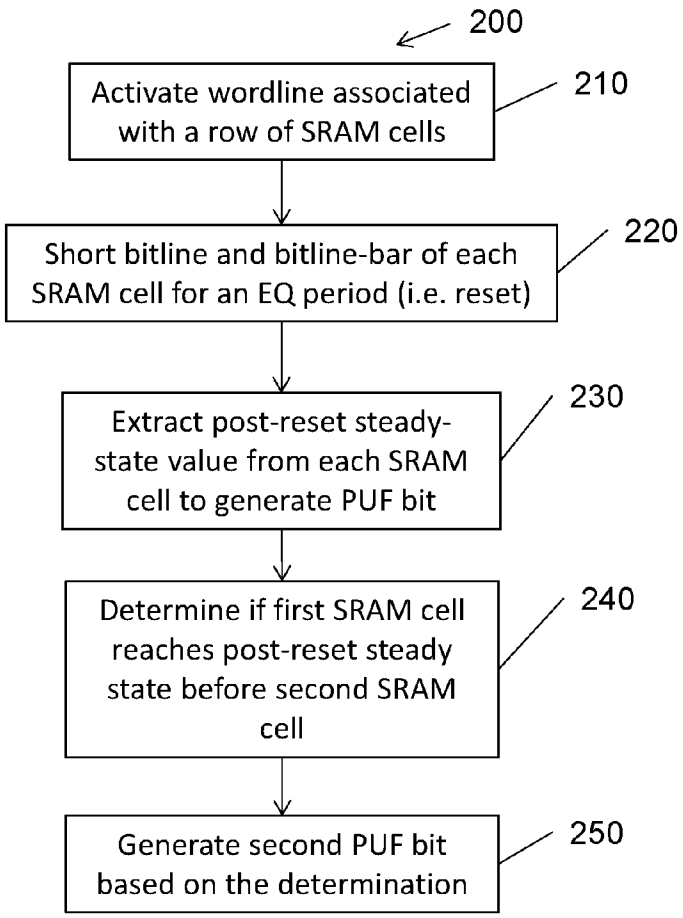

200
Activate wordline associated with a row of SRAM cells
210
Short bitline and bitline-bar of each SRAM cell for an EQ period (i.e. reset)
220
Extract post-reset steady-state value from each SRAM cell to generate PUF bit
230
Determine if first SRAM cell reaches post-reset steady state before second SRAM cell
240
Generate second PUF bit based on the determination
250

FIG.2A

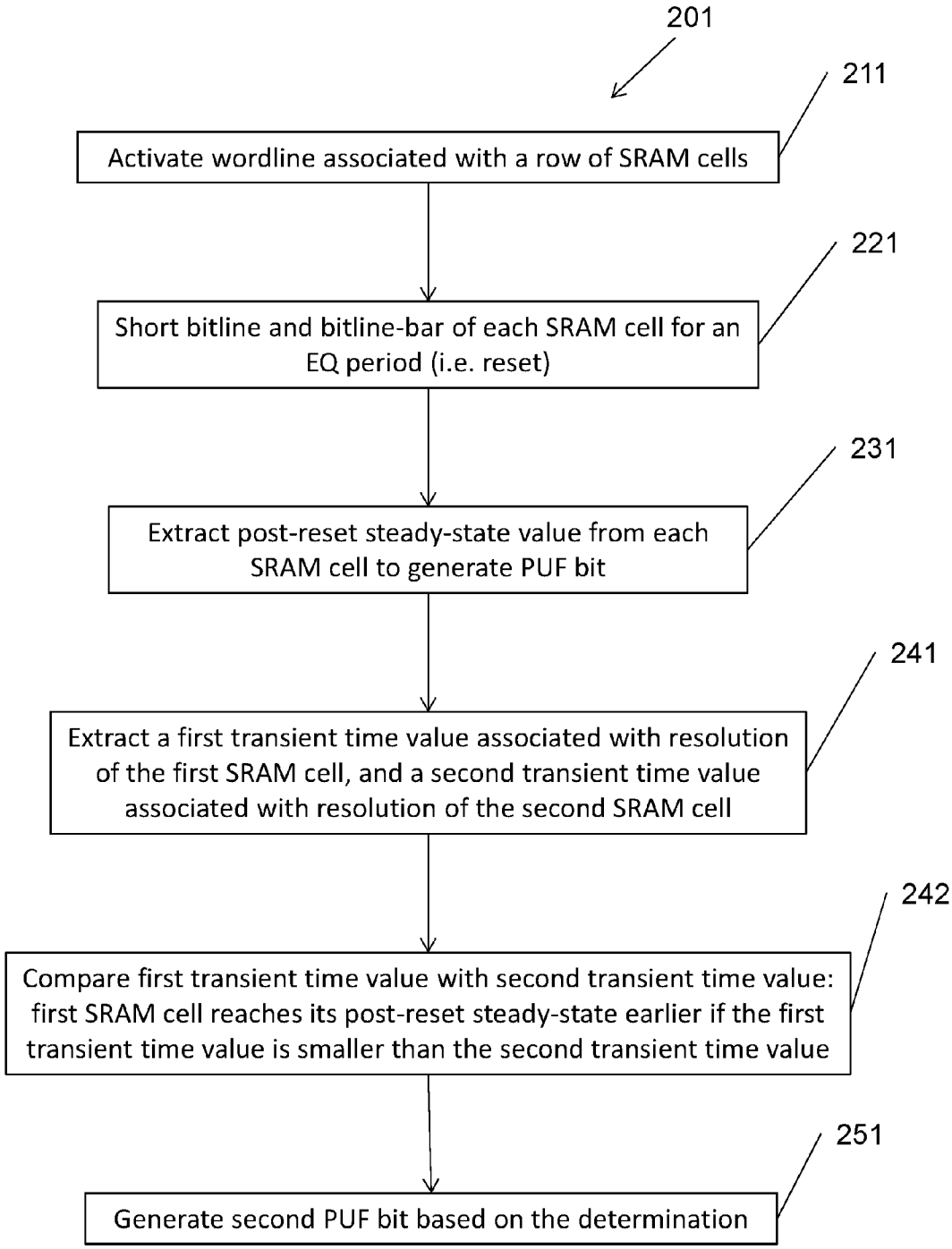
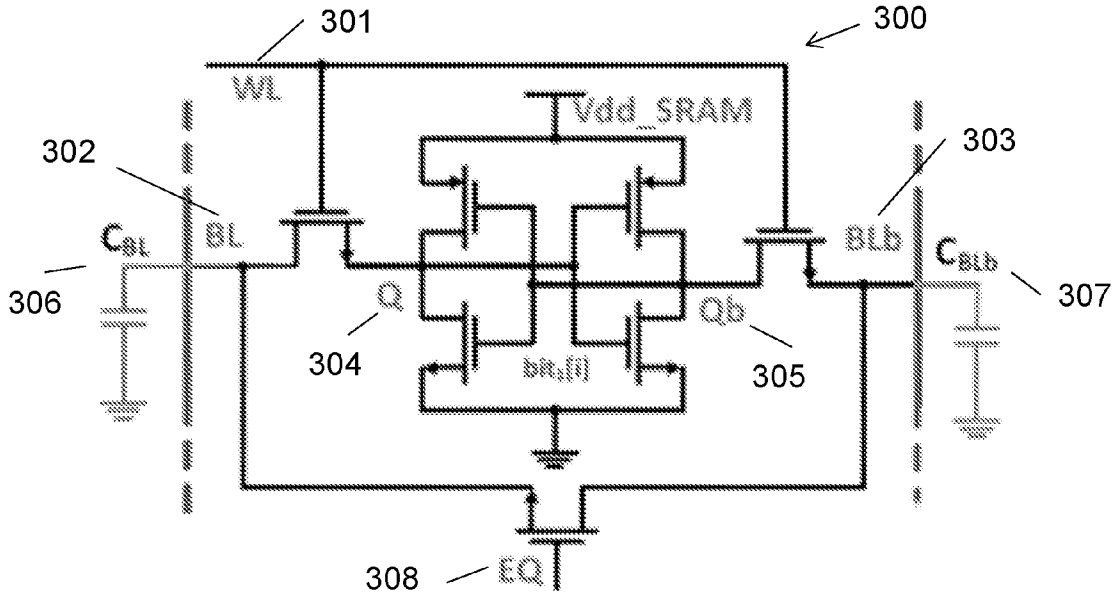
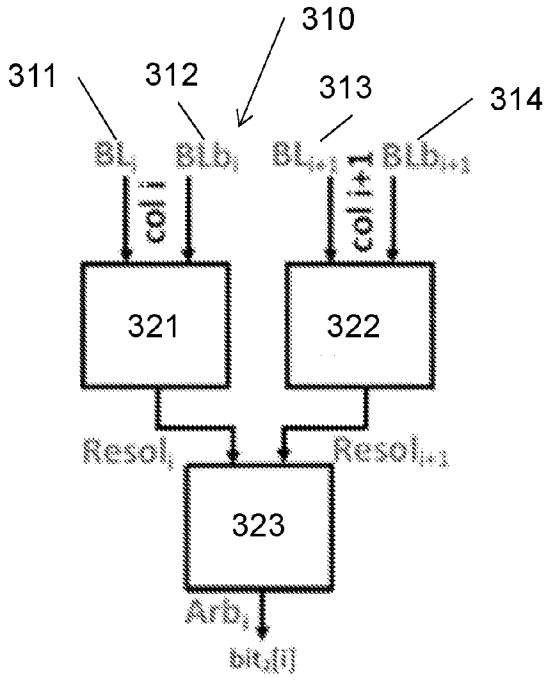

201
211
Activate wordline associated with a row of SRAM cells
221
Short bitline and bitline-bar of each SRAM cell for an EQ period (i.e. reset)
231
Extract post-reset steady-state value from each SRAM cell to generate PUF bit
241
Extract a first transient time value associated with resolution of the first SRAM cell, and a second transient time value associated with resolution of the second SRAM cell
242
Compare first transient time value with second transient time value: first SRAM cell reaches its post-reset steady-state earlier if the first transient time value is smaller than the second transient time value
251
Generate second PUF bit based on the determination

FIG.2B


301
300
WL
Vdd_SRAM
302
303
BL
BLb
C_{BL}
C_{BLb}
306
307
Q
Qb
304
305
$bit_i[i]$
308
EQ


310
311
312
313
314
BL_i
BLb_i
BL_{i+1}
BLb_{i+1}
col i
col i+1
321
322
$Resol_i$
$Resol_{i+1}$
323
Arb_i
$bit_i[i]$

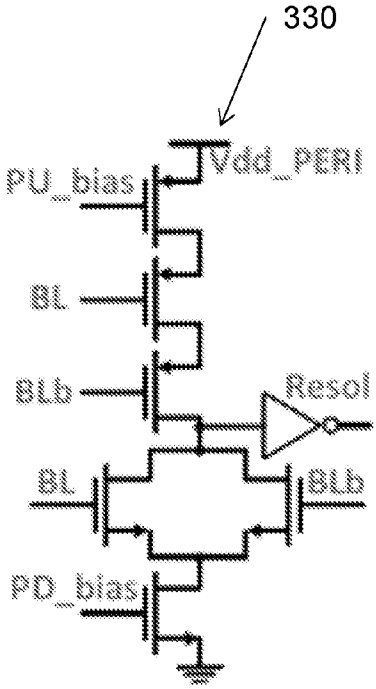

330
Vdd_PERI
PU_bias
BL
BLb
Resol
BL
BLb
PD_bias

FIG. 3

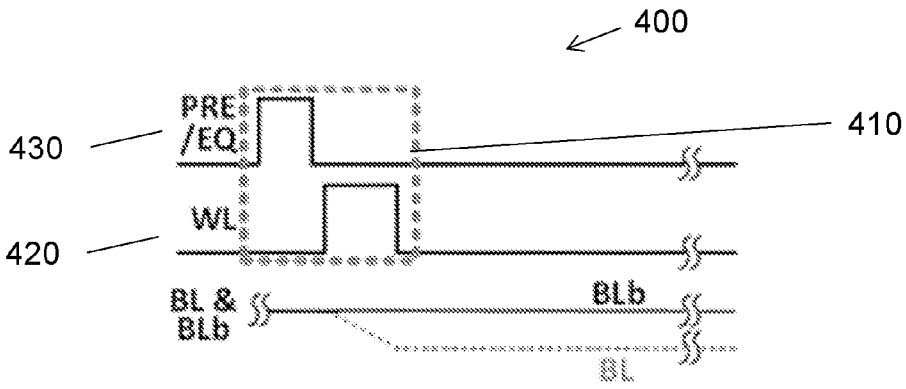

400
PRE /EQ
430
410
WL
420
BL & BLb
BLb
BL

FIG. 4A

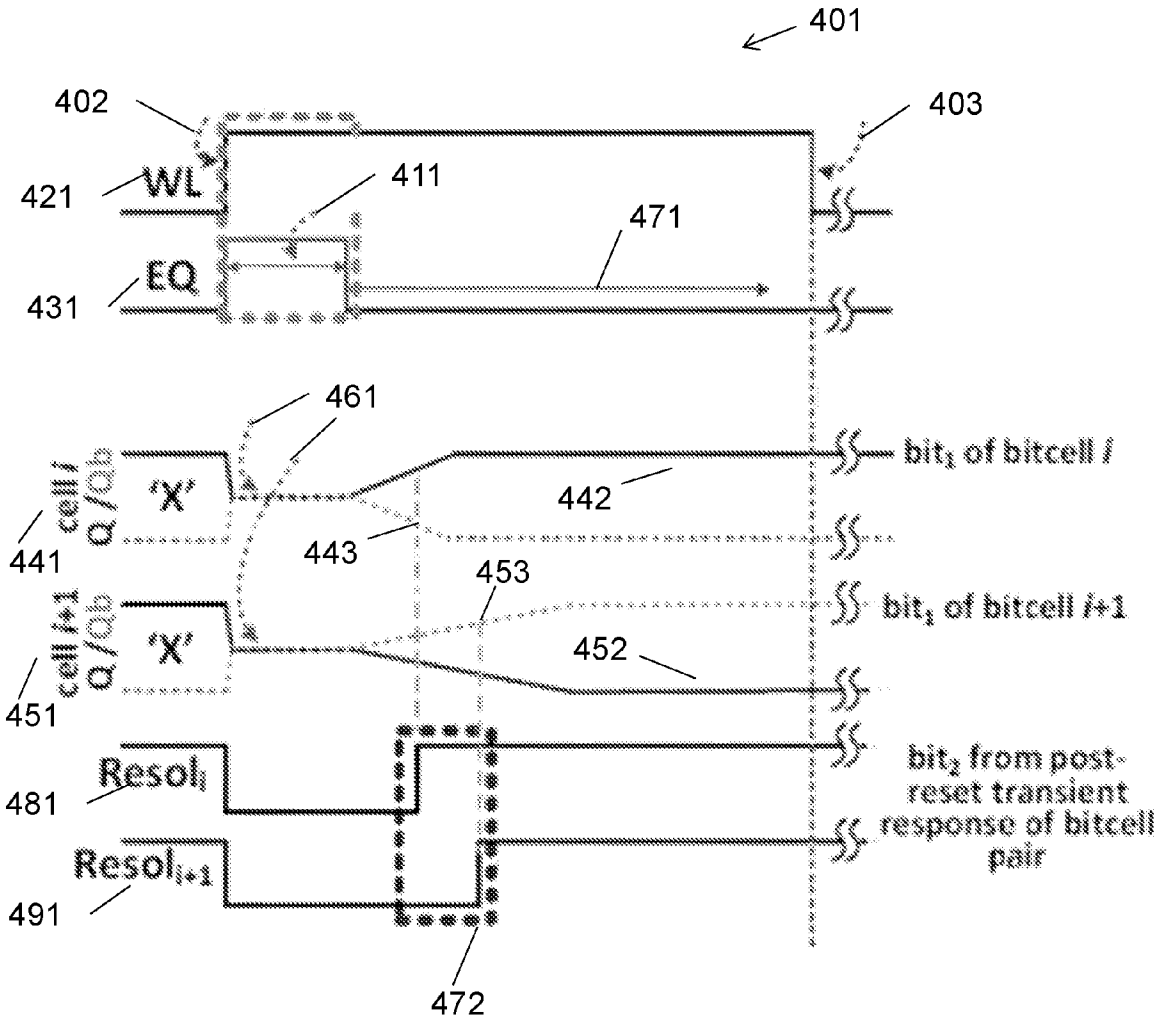

401
402
403
421
WL
411
471
431
EQ
461
cell i Q /Qb
'X'
441
bit1 of bitcell i
442
443
453
cell i+1 Q /Qb
'X'
bit1 of bitcell i+1
452
451
Resoli
481
bit2 from post-reset transient response of bitcell pair
Resoli+1
491
472

FIG. 4B

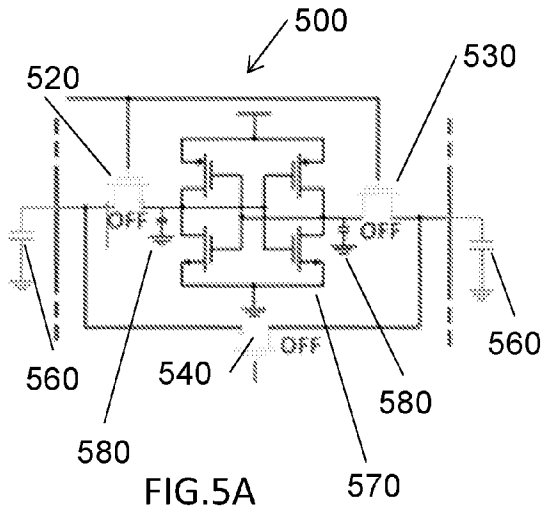


FIG.5A

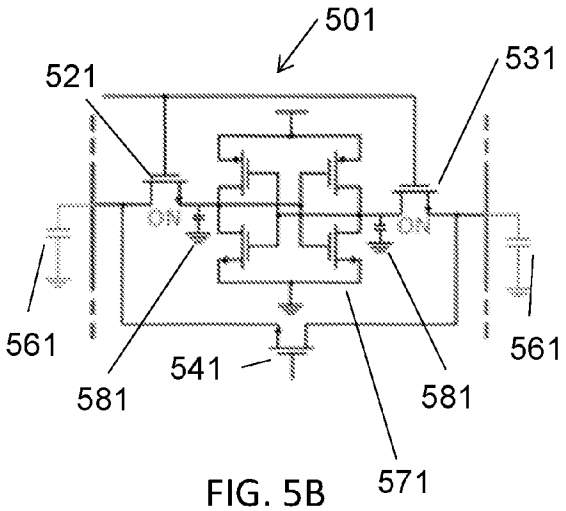


FIG. 5B

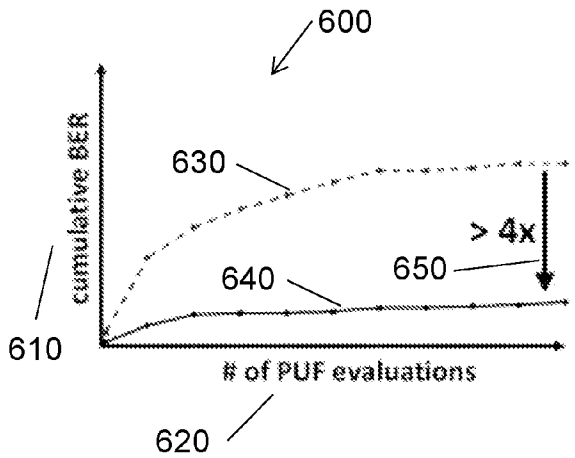


FIG.6A

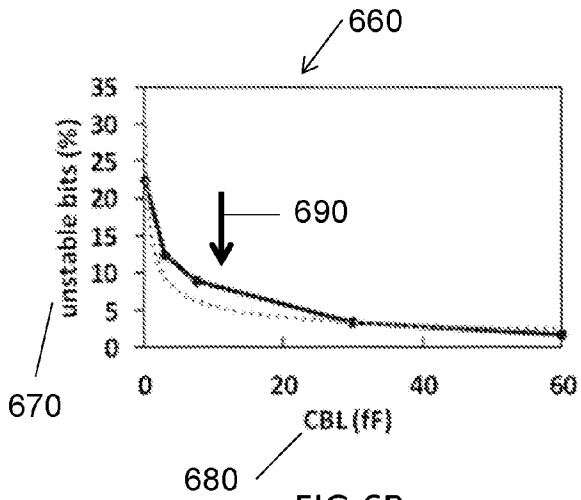


FIG.6B

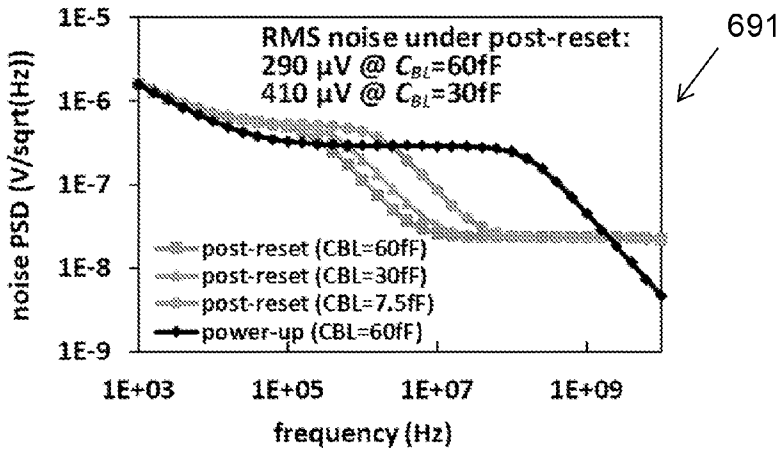


FIG.6C

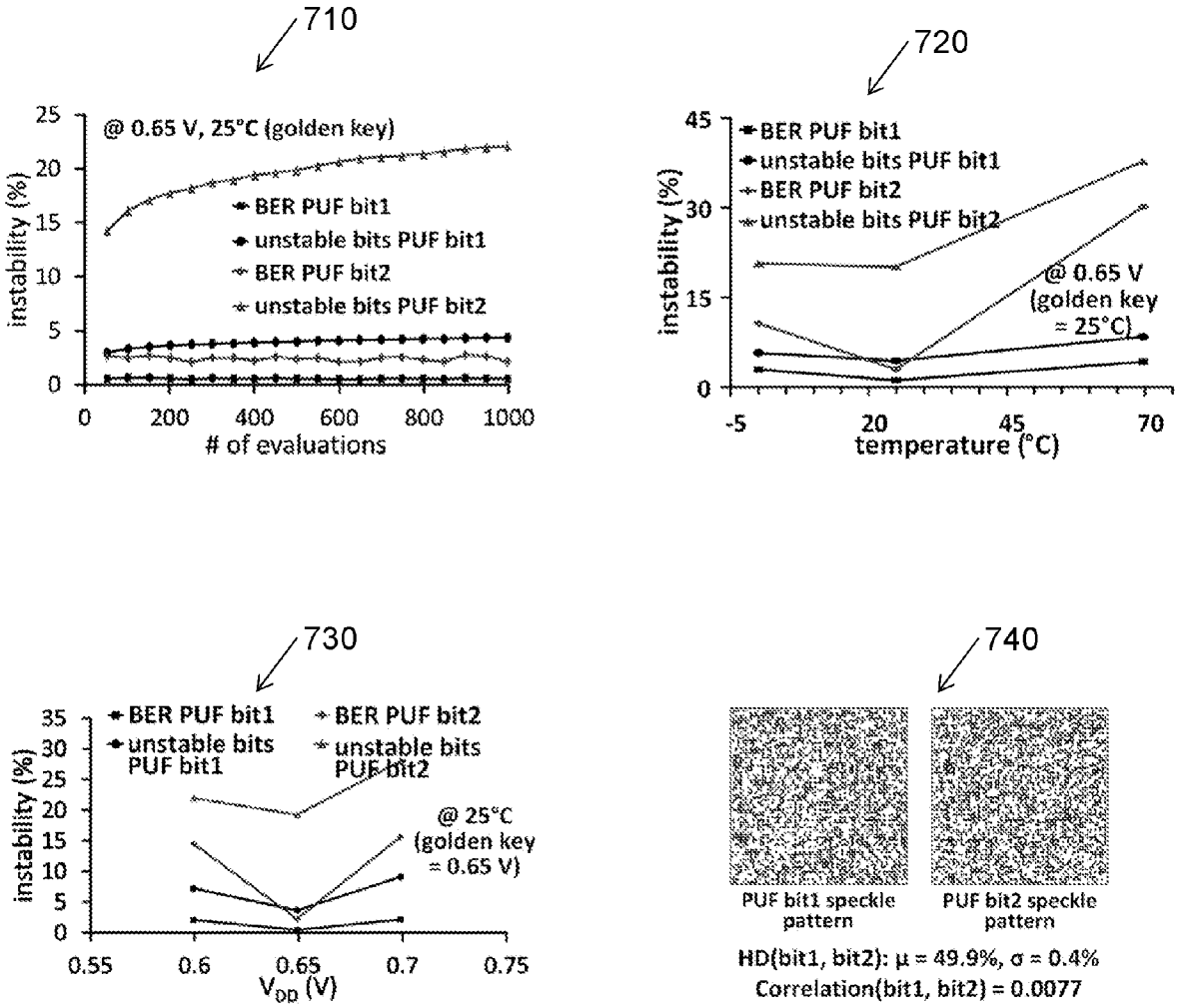
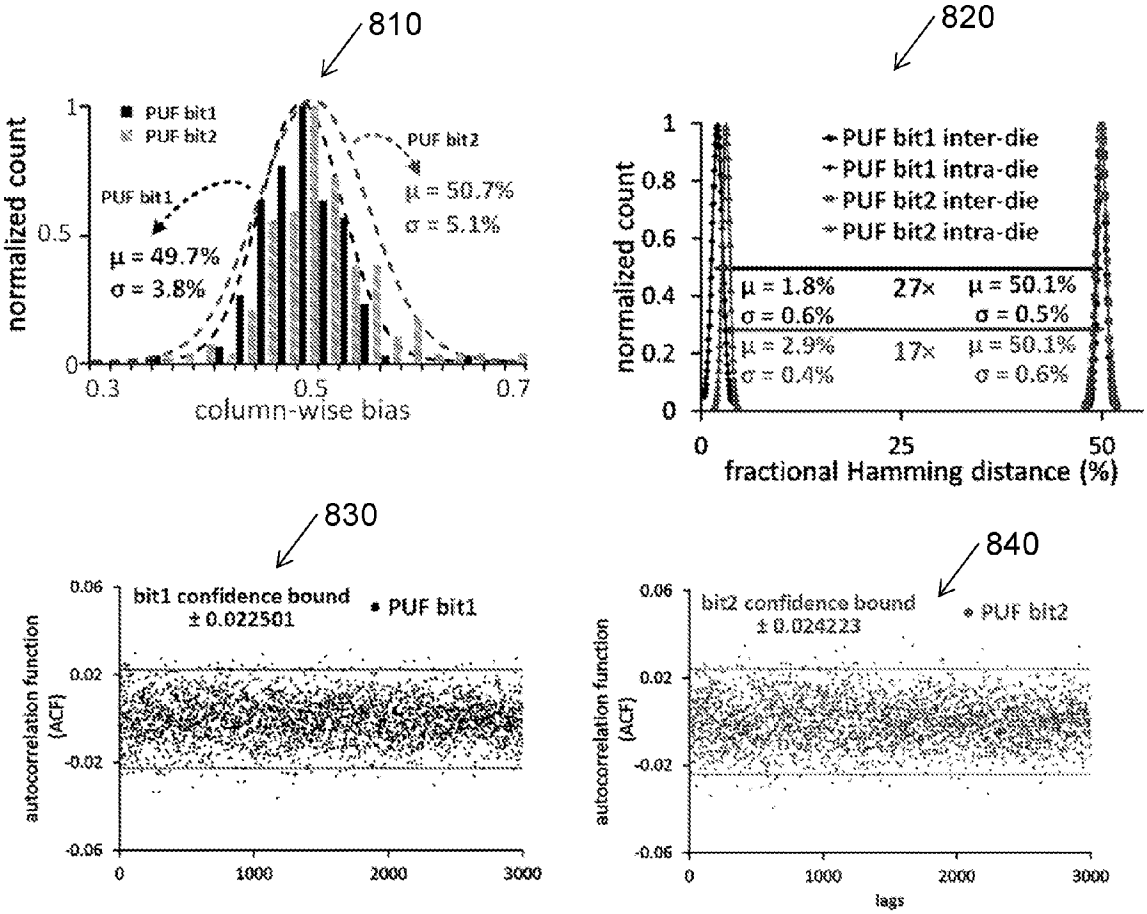

710
@ 0.65 V, 25°C (golden key)
BER PUF bit1
unstable bits PUF bit1
BER PUF bit2
unstable bits PUF bit2
instability (%)
# of evaluations
720
BER PUF bit1
unstable bits PUF bit1
BER PUF bit2
unstable bits PUF bit2
@ 0.65 V (golden key = 25°C)
instability (%)
temperature (°C)
730
BER PUF bit1
unstable bits PUF bit1
BER PUF bit2
unstable bits PUF bit2
@ 25°C (golden key = 0.65 V)
instability (%)
V_DD (V)
740
PUF bit1 speckle pattern
PUF bit2 speckle pattern
HD(bit1, bit2): μ = 49.9%, σ = 0.4%
Correlation(bit1, bit2) = 0.0077

FIG. 7



850

NIST SP 800-22 Randomness Tests				
Test Name	Stream Length	bit1 Avg. P-Value	bit2 Avg. P-Value	Pass?
Frequency	6000	0.36	0.11	pass
Block Frequency	6000 (M=128)	0.46	0.41	pass
Runs	6000	0.40	0.10	pass
Longest Runs	6000	0.30	0.30	pass
Rank	6000	0.40	0.37	pass
Cumulative Sums	6000	0.35	0.09	pass
FFT	6000	0.38	0.39	pass
Non-Overlapping...	6000 (m=9)	0.51	0.52	pass
Overlapping...	6000 (m=9)	0.45	0.51	pass
Serial	6000 (m=9)	0.48	0.64	pass
Approx. Entropy	6000 (m=6)	0.20	0.38	pass

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2024/050378

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44 (2013.01) ***H04L 9/32 (2006.01)*** *G06F 21/73 (2013.01)* *G11C 11/40 (2006.01)*

According to International Patent Classification (IPC)

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F, H04L, G11C

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)

FAMPAT, Google Scholar, IEEE Xplore: physically unclonable function, PUF, static random-access memory, SRAM, generate, extract, wordline, bitline, equalization, short, time, period, duration, width, post-reset, metastable, second, pair, and related terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2019/0229933 A1 (LI, X. ET AL.) 25 July 2019 Para. [0021]-[0022], Fig. 2-3	1-30
A	US 2020/0084052 A1 (O'CONNELL, C. M.) 12 March 2020 Whole document	
A	WO 2022/159031 A1 (NAT UNIV SINGAPORE) 28 July 2022 Whole document	
P,X	BASU, J. ET AL., ECC-Less Multi-Level SRAM Physically Unclonable Function and 127% PUF-to-Memory Capacity Ratio with No Bitcell Modification in 28nm. *2023 IEEE Symposium on VLSI Technology and Circuits*, 24 July 2023, pages 1-2 [Retrieved on 2024-08-08] <DOI:10.23919/VLSITECHNOLOGYANDCIR57934.2023.10185261> Whole document	1-30

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

"D" document cited by the applicant in the international application

"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
22/08/2024 *(day/month/year)*	26/08/2024 *(day/month/year)*

Name and mailing address of the ISA/SG

Intellectual Property Office of Singapore
1 Paya Lebar Link, #11-03
PLQ 1, Paya Lebar Quarter
Singapore 408533

Email: pct@ipos.gov.sg

Authorized officer

Fang Zheng (Dr)

IPOS Customer Service Tel. No.: (+65) 6339 8616

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG2024/050378

Note: This Annex lists known patent family members relating to the patent documents cited in this International Search Report. This Authority is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019/0229933 A1	25/07/2019	NONE	
US 2020/0084052 A1	12/03/2020	NONE	
WO 2022/159031 A1	28/07/2022	US 2024/0078087 A1 EP 4282121 A1	07/03/2024 29/11/2023