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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 December 2013 (12.12.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/184562 A1

(51) International Patent Classification:
G06F 9/455 (2006.01) *G06F 17/50* (2006.01)

(21) International Application Number:
PCT/US2013/043864

(22) International Filing Date:
3 June 2013 (03.06.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/655,689 5 June 2012 (05.06.2012) US

(71) Applicant: **BOARD OF REGENTS, THE UNIVERSITY OF TEXAS SYSTEM**; 201 West 7th Street, Austin, TX 78701 (US).

(72) Inventor: **ORSHANSKY, Michael**; 1 University Station C8800, Aces Building 5.442, Austin, TX 78712-0323 (US).

(74) Agent: **VOIGT, Robert, A., Jr.**; Winstead, P.C., P.O. Box 131851, Dallas, TX 75313 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: PHYSICALLY UNCLONABLE FUNCTIONS BASED ON NON-LINEARITY

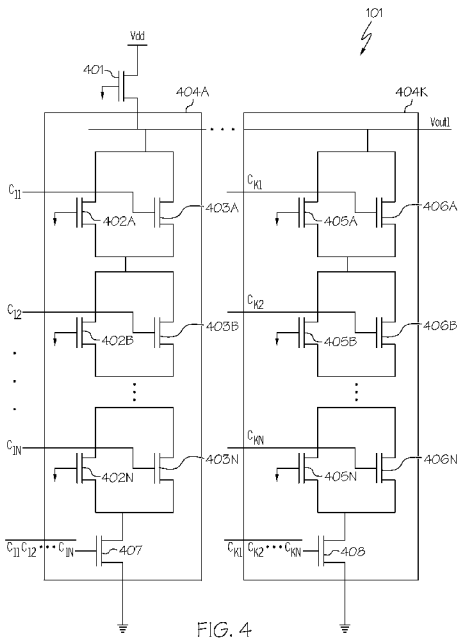


FIG. 4

(57) Abstract: An electronic circuit for implementing a physically unclonable function. The electronic circuit includes duplicate circuits, referred to as "circuit primitives," that generate a first and a second output voltage based on the received input, referred to as a "challenge." The electronic circuit further includes a comparator coupled to the circuit primitives and generates an output based on the difference between the first and second output voltages. While the circuit primitives contain duplicate circuitry, the circuit primitives may generate a different output voltage due to a particular set of transistors in the circuit primitives operating in the sub-threshold region whose gates are tied to ground and whose sub-threshold current, the magnitude of which is random based on the threshold voltage variation of the set of transistors, is used to affect the value of the output voltage.

WO 2013/184562 A1

PHYSICALLY UNCLONABLE FUNCTIONS BASED ON NON-LINEARITY

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application Serial No. 61/655,689, "Physically Unclonable Functions Based on Non-Linearity of Sub-Threshold Operation and Drain-Induced Barrier Lowering Effect," filed on June 5, 2012, which is incorporated by reference herein in its entirety.

TECHNICAL FIELD

[0002] The present invention relates generally to physically unclonable functions, and more particularly to highly secure strong Physically Unclonable Functions (PUFs) based on the strong non-linearity of the Field-Effect Transistor (FET) operation in the sub-threshold region and the Drain-Induced Barrier Lowering (DIBL) effect.

BACKGROUND

[0003] A Physically Unclonable Function (PUF) exploits variations, such as stochastic process variations in manufacturing, to generate secret keys used in cryptographic operations, chip authentication, and even random number generation. A device that supports a PUF yields different responses (e.g., binary responses) to different inputs, referred to as "challenges." Authentication of a device using a PUF is performed by supplying a challenge input to the device to which the response of an authentic device is known. The response is a result of a function that, by definition, is not clonable. For example, a PUF may result from stochastic process variations in the production of otherwise identical devices. As a result of the process variations, the otherwise identical devices may respond with a different series of bits in response to a set of challenge input bits.

[0004] Currently, the most widely adopted silicon-based PUFs are based on establishing timing races and relying on arbiters to produce a rich set of responses. The PUF circuit can use random variations in the delay of circuit components to achieve an unpredictable mapping of challenges and responses. For example, given an input challenge, a race condition is set up in the circuit, and two transitions that propagate along different paths are compared to see which comes first. An arbiter, typically implemented as a latch, produces a logical "1" or a "0", depending on which

transition comes first. When a circuit with the same layout mask is fabricated to result in different chips, the mapping between challenges and responses implemented by the circuit is different for each chip due to the random variations of delays.

[0005] Unfortunately, such PUFs show a vulnerability to machine-learning attacks due to the linear separability of the output function as a result of the additive nature of the timing delay along the paths.

BRIEF SUMMARY

[0006] In one embodiment of the present invention, an electronic circuit for implementing a Physically Unclonable Function (PUF) comprises a first and a second circuit primitive configured to generate a first and a second output voltage, respectively, where the first and second circuit primitives are duplicates of one another. The electronic circuit further comprises a challenge inputted to the first and second circuit primitives. Furthermore, the electronic circuit comprises a comparator coupled to the first and second circuit primitives, where the comparator generates an output based on a difference between the first and second output voltages. Each of the first and second circuit primitives comprises one or more circuit blocks. Each of the one or more circuit blocks comprises a first plurality of series-connected transistors that operate in a sub-threshold region, where a gate of each of the first plurality of series-connected transistors is tied to ground or to an internal node and where a drain of a first transistor of the first plurality of series-connected transistors is coupled to an output node. Furthermore, each of the one or more circuit blocks comprises a second plurality of transistors that are in parallel to the first plurality of series-connected transistors, where a drain of a first transistor of the second plurality of transistors is coupled to the output node and where a gate of each of the second plurality of transistors receives a value of one bit of the challenge. Furthermore, the electronic circuit comprises a first transistor coupled to a source of a second transistor of the first plurality of series-connected transistors and coupled to a source of a second transistor of the second plurality of transistors in response to having two or more circuit blocks, where the first transistor is controlled by an input that corresponds to a logical operation of each value for each bit of the challenge. Each of the first and second output voltages of the first and second circuit primitives, respectively, is determined based on current that flows through the first plurality of series-connected transistors of the first and second circuit primitives, respectively, whose magnitude is random based on a threshold voltage variation of the first plurality of series-connected transistors.

[0007] The foregoing has outlined rather generally the features and technical advantages of one or more embodiments of the present invention in order that the detailed description of the present invention that follows may be better understood. Additional features and advantages of the

present invention will be described hereinafter which may form the subject of the claims of the present invention.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0008] A better understanding of the present invention can be obtained when the following detailed description is considered in conjunction with the following drawings, in which:

[0009] Figure 1 illustrates an electronic circuit implementing a Physically Unclonable Function (PUF) for generating non-linear responses produced by the physics of the Field-Effect Transistors (FETs) of the duplicate circuit primitives at the nanometer scale in accordance with an embodiment of the present invention;

[0010] Figure 2 illustrates one embodiment of the circuit primitive that is used in the electronic circuit depicted in Figure 1;

[0011] Figure 3 illustrates an alternative embodiment of the circuit primitive that is used in the electronic circuit depicted in Figure 1; and

[0012] Figure 4 illustrates a further alternative embodiment of the circuit primitive that is used in the electronic circuit depicted in Figure 1.

DETAILED DESCRIPTION

[0013] In the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced without such specific details. In other instances, well-known circuits have been shown in block diagram form in order not to obscure the present invention in unnecessary detail. For the most part, details considering timing considerations and the like have been omitted inasmuch as such details are not necessary to obtain a complete understanding of the present invention and are within the skills of persons of ordinary skill in the relevant art.

[0014] As stated in the Background section, currently, the most widely adopted strong silicon-based PUFs (those with a large number of challenge-response pairs) are based on establishing timing races and relying on arbiters to produce a rich set of responses. The PUF circuit can use random variations in the delay of circuit components to achieve an unpredictable mapping of challenges and responses. For example, given an input challenge, a race condition is set up in the circuit, and two transitions that propagate along different paths are compared to see which comes first. An arbiter, typically implemented as a latch, produces a logical "1" or a "0", depending on which transition comes first. When a circuit with the same layout mask is fabricated, and the result of fabrication is a set of different chips, the input-output mapping implemented by the circuit is different for each chip due to the random variations of delays. Unfortunately, such PUFs show a vulnerability to machine-learning attacks due to the linear separability of the output function as a result of the additive nature of the timing delay along the paths.

[0015] The principles of the present invention provide a PUF that is less vulnerable to machine-learning attacks by relying on the non-linearity of the responses produced by the physics of the Field-Effect Transistors (FETs) at the nanometer scale. Namely, the strong non-linear behavior of the FET in the sub-threshold region of its operation and also the Drain-Induced Barrier Lowering (DIBL) effect are used to inject strong non-linearity into the response of the PUF. Non-linearity is based on the fact that in the sub-threshold region of FET operation, current is an exponential function of threshold voltages which exhibit strong random intrinsic variability. An additional non-linearity is due to exponential dependence of current on drain-to-source voltage

due to DIBL. DIBL refers to the reduction of threshold voltage of the transistor at higher drain voltages. The generated voltages from the duplicate circuit primitives of the electronic circuit implementing a PUF are compared to produce a random binary response as discussed below in connection with Figures 1-4.

[0016] Figure 1 illustrates an electronic circuit implementing a PUF for generating non-linear responses produced by the physics of the FETs of the duplicate circuit primitives at the nanometer scale. Figure 2 illustrates one embodiment of the circuit primitive that is used in the electronic circuit depicted in Figure 1. Figure 3 illustrates an alternative embodiment of the circuit primitive that is used in the electronic circuit depicted in Figure 1. Figure 4 illustrates a further alternative embodiment of the circuit primitive that is used in the electronic circuit depicted in Figure 1.

[0017] Prior to discussing the electronic circuit implementing a PUF for generating non-linear responses produced by the physics of the FETs of the duplicate circuit primitives at the nanometer scale, a discussion of "strong" and "weak" PUFs is deemed appropriate.

[0018] Multiple realizations of PUFs have been proposed. The key distinction that defines PUF constructions is based on the rate at which the number of Challenge-Response Pairs (CRPs) grows with the size of the physical realization of the PUF itself. Two major categories of PUFs in this regard are the Weak PUFs and Strong PUFs. Weak PUFs are PUFs that are characterized by a small number of CRPs. Strong PUFs are systems with a large number of CRPs, which typically grow exponentially with the size of the PUF. The exponential size of the CRP set makes it impossible to record the responses for a PUF of a reasonable size or even to measure all the CRPs within a finite amount of time.

[0019] Strong PUFs are essential for public authentication security protocols in which the number of CRPs needs to be large such that the same CRPs are not re-used for authentication (preventing the adversary of simply capturing the CRPs transmitted in plain text and using them for subsequent attacks). However, for a strong PUF to be an effective security primitive, the CRPs need to be un-predictable: given a certain set of known CRPs, it should not be possible to predict the unobserved CRPs with any reasonable probability. If that is not the case, an adversary can stage an attack based on building a model of the PUF.

[0020] In weak PUFs, the number of CRPs grows linearly with the PUF physical size. Therefore, an important implicit feature of weak PUFs is that each CRP depends on a single realization of a random variable (property) which is not shared. That makes it impossible to build a model of this PUF and makes weak PUFs resilient to model-building attacks.

[0021] The principles of the present invention described herein relate to a strong PUF that is based on the essential non-linearity of responses produced by the physics of the FETs at the nanometer scale as discussed below.

[0022] Referring to Figure 1, Figure 1 illustrates an electronic circuit 100 implementing a PUF for generating non-linear responses produced by the physics of the FETs of the duplicate circuit primitives at the nanometer scale in accordance with an embodiment of the present invention. Circuit 100 generates an output binary response by comparing the output response, V_{out1} and V_{out2}, of the duplicate circuit primitives 101A, 101B, respectively, using a comparator 102. Both circuit primitives 101A, 101B are operated with the same challenge input (identified as C_0, C_1 and C_2 in Figure 1). Circuit primitives 101A, 101B may collectively or individually be referred to as circuit primitives 101 or circuit primitive 101, respectively. While each circuit primitive 101 contains duplicate circuitry, circuit primitives 101A, 101B may generate a different output voltage due to a particular set of transistors operating in the sub-threshold region whose gates are tied to ground and whose sub-threshold leakage current, the magnitude of which is random based on the threshold voltage variation of the set of transistors, is used to affect the value of the output voltage as discussed further below.

[0023] The voltage difference (ΔV) between the two output voltages (V_{out1} and V_{out2}) of circuit primitives 101A, 101B depends on the values of the bits of the challenge input and the realizations of the random threshold voltages. For the ideal comparator, the produced binary output of comparator 102 will match perfectly the sign of ΔV for any magnitude of the voltage difference. The real comparators are analog circuits and are characterized by the non-ideality, known as the offset voltage. That effectively determines the resolution of comparator 102. It is noted that one of ordinary skill in the art would know how to build a comparator in such a way that its offset voltage is sufficiently small so that it does not detrimentally impact the security properties of the PUF of the present invention.

[0024] While Figure 1 illustrates two circuit primitives 101, electronic circuit 100 may include any number of circuit primitives 101 operating on any number of bits of a challenge input. Figure 1 is not to be limited in scope to the depicted number of circuit primitives 101 and number of bits of the challenge input.

[0025] Embodiments of circuit primitives 101A, 101B are discussed below in connection with Figures 2-4.

[0026] Figure 2 illustrates an embodiment of the present invention of circuit primitive 101 (Figure 1) used in circuit 100 (Figure 1). Referring to Figure 2, in conjunction with Figure 1, circuit primitive 101 includes an n-type transistor 201 with its drain coupled to Vdd (the voltage level of the power source). The gate of transistor 201 is coupled to ground. The source of transistor 201 is coupled to the output voltage node (e.g., V_{out1} for circuit primitive 101A) and to the drains of n-type transistors 202A-202N, where N is a positive integer, that operate in the sub-threshold region with their gate voltages tied to ground. In one embodiment, N is equal to the number of bits of the challenge input as shown in Figure 1. For example, if there are three bits in the challenge input (e.g., C_0, C_1 and C_2), then N is equal to three. N-type transistors 202A-202N may collectively or individually be referred to as n-type transistors 202 or n-type transistor 202, respectively. The drains of transistors 202 are coupled to the output voltage node (e.g., V_{out1} for circuit primitive 101A). The sources of n-type transistors 202 are coupled to n-type transistors 203A-203N, 204A-204N, where N is a positive integer, which act as switch transistors (explained in further detail below). Transistors 203A-203N may collectively or individually be referred to as n-type transistors 203 or n-type transistor 203, respectively. Transistors 204A-204N may collectively or individually be referred to as n-type transistors 204 or n-type transistor 204, respectively. The drains of n-type transistors 203 are coupled to the sources of n-type transistors 202. The drains of n-type transistors 204 are coupled to the sources of n-type transistors 202 and their sources are coupled to the output node (e.g., V_{out1} for circuit primitive 101A). The gates of transistors 203 receive a challenge input (e.g., C_0, C_1, $C_{2...}C_N$). Furthermore, the gates of transistors 204 receive the complement of the challenge input (e.g., C_0', C_1', C_2'…C_N').

[0027] As illustrated in Figure 2, circuit primitive 101 is based on a parallel combination of currents flowing through transistors 202. As discussed above, transistors 202 operate in the sub-threshold region (region where the transistor is being operated below the threshold voltage, such as when the gate-to-source voltage is less than the transistor threshold voltage) with the gate voltages at ground. When transistors 202 operate in the sub-threshold region, current, referred to as the sub-threshold current, flows between the source and drain of the transistor even when the transistor is nominally off/deactivated (transistors 202 are said to be deactivated when their gate voltages are tied to ground). Transistor 201 acts as a load device and also operates in the sub-threshold region (its gate voltage (Vg)=0 as well). Specifically, to ensure that circuit primitive 101 correctly operates, careful sizing of transistors 202, 203 and 204 is needed. For example, to ensure that only transistors 202 exhibit stochastic threshold voltage variation (i.e., to ensure that only transistors 202 exhibit randomness), they are made at a minimum size (e.g., width (W)=Wmin and length (L)=Lmin) in order to maximize their threshold voltage variability. The switch transistors 203, 204 additionally need to provide negligible resistance in the on-state (i.e., when they are activated) but essentially eliminate the sub-threshold leakage current through the given branch when they are in the off-state (i.e., when they are deactivated). That can be achieved by making the channel length much longer than that of transistors 202 since the sub-threshold current is exponentially dependent on the channel length. In one embodiment, the length of switch transistors 203, 204 is approximately at least between 2-50 times the length of transistors 202 such that their sub-threshold leakage current is practically zero, in comparison to that of transistors 202, during the off-state. Furthermore, in one embodiment, the width of transistor 201 is at least between 10-1,000 times the width of transistors 202. Depending on the value of the challenge input bit (e.g., 0 or logical value of 1), the current whose magnitude is random either flows through a branch or is zero. For example, when the value of challenge input C_0 is 0, then transistor 203A is deactivated and transistor 204A is activated and the current through this specific branch is effectively eliminated altogether and it does not contribute to the value of the output voltage at the output node (e.g., V_{out1} for circuit primitive 101A). If, however, the value of challenge input C_0 is 1, then transistor 203A is activated and transistor 204A is deactivated, and current flows to ground. The current that flows is attributed to the sub-threshold leakage current from transistor 202A operating in the sub-threshold region. The amount of such a current is variable. Based on the values of the bits of the challenge input, zero

or more transistors 204 will be activated allowing sub-threshold leakage current from transistors 202 to flow in their branch(es) operating in the sub-threshold region to contribute to the voltage value at the output node (e.g., V_{out1} for circuit primitive 101A). The voltage at the output node (e.g., V_{out1} for circuit primitive 101A) is determined by the entire set of currents that flow through all the branches and is determined by the challenge input as well as the random realizations of the threshold voltages.

[0028] A duplicate circuit primitive 101 as the one shown in Figure 2 is provided to generate a voltage value at the other output node (e.g., V_{out2}), such as the output node of circuit primitive 101B shown in Figure 1. Due to the randomness of the threshold voltage of transistors 202, the amount of current that is generated by circuit primitives 101A, 101B (and the voltage value at its output node) will vary even though the circuit primitives 101 have the same circuitry with the same input value (challenge). As a result, comparator 102 compares the two different voltage outputs and generates a random binary output. Device 100 has 2^N possible output values.

[0029] Another embodiment of circuit primitive 101 is provided below in connection with Figure 3. Figure 3 illustrates an alternative embodiment of the present invention of circuit primitive 101 (Figure 1) used in circuit 100 (Figure 1). Referring to Figure 3, in conjunction with Figure 1, circuit primitive 101 includes an n-type transistor 301 with its drain coupled to Vdd (the voltage level of the power source). The gate of transistor 301 is coupled to ground. The source of transistor 301 is coupled to the output voltage node (e.g., V_{out1} for circuit primitive 101A) and to the drain of the first n-type transistor 302A in a series of connected n-type transistors 302A-302C that operate in the sub-threshold region with their gate voltages tied to ground. N-type transistors 302A-302C may collectively or individually be referred to as n-type transistors 302 or n-type transistor 302, respectively. In one embodiment, the number of n-type transistors 302 is equal to the number of bits of the challenge input as shown in Figure 1. For example, if there are three bits in the challenge input (e.g., C_0, C_1 and C_2), then there will be three n-type transistors 302. Hence, while Figure 3 illustrates three n-type transistors 302, circuit primitive 101 of Figure 3 may include any number of n-type transistors 302 that equals the number of bits in the challenge input.

[0030] The sources of all the series connected n-type transistors 302A-302B except the last n-type transistor 302C in the series connected n-type transistors 302 are connected to the drains of the following n-type transistors 302B-302C, respectively, in the series connected n-type transistors 302. The source of the last n-type transistor 302C in the series connected n-type transistors 302 is connected to ground.

[0031] The drain of the first n-type transistor 302A in the series connected n-type transistors 302 is coupled to the output voltage node V_{out1}.

[0032] Circuit primitive 101 of Figure 3 further includes a series connected n-type switch transistors 303A-303C that are in parallel to n-type transistors 302. N-type transistors 303A-303C may collectively or individually be referred to as n-type transistors 303 or n-type transistor 303, respectively. In one embodiment, the number of n-type transistors 303 is equal to the number of bits in the challenge input as shown in Figure 1. For example, if there are three bits in the challenge input (e.g., C_0, C_1 and C_2), then there will be three n-type transistors 303. Hence, while Figure 3 illustrates three n-type transistors 303, circuit primitive 101 of Figure 3 may include any number of n-type transistors 303 that equals the number of bits in the challenge input.

[0033] The sources of all the series connected n-type transistors 303A-303B except the last n-type transistor 303C in the series connected n-type transistors 303 are connected to the drains of the following n-type transistors 303B-303C, respectively, and to the drains of n-type transistors 302B-302C, respectively, in the series connected n-type transistors 302, 303. The source of the last n-type transistor 303C in the series connected n-type transistors 303 is connected to ground.

[0034] The drain of the first n-type transistor 303A in the series connected n-type transistors 303 is coupled to the output voltage node V_{out1}.

[0035] The gates of n-type transistors 303 receive the values of the challenge input (e.g., C_0, C_1 and C_2) as shown in Figure 3.

[0036] As illustrated in Figure 3, circuit primitive 101 is based on a series combination of transistors 302. As discussed above, transistors 302 operate in the sub-threshold region (region where the transistor is being operated below the threshold voltage, such as when the gate-to-

supply voltage is less than the transistor threshold voltage) with the gate voltages at ground. When transistors 302 operate in the sub-threshold region, current, referred to as the sub-threshold leakage current, flows between the source and drain of the transistor even when the transistor is nominally off/deactivated (transistors 302 are said to be deactivated when the gate voltages are tied to ground). Transistor 301 acts as a load device and also operates in the sub-threshold region (its Vg=0 as well). To ensure the correct operation of circuit primitive 101, careful sizing of transistors 302, 303 is needed. Specifically, to ensure that only transistors 302 exhibit stochastic threshold voltage variation (i.e., to ensure that only transistors 302 exhibit randomness), they are made at a minimum size (e.g., width (W)=Wmin and length (L)=Lmin) in order to maximize their threshold voltage variability. The role of switch transistors 303 is to set the voltage between the drain and source of transistor 303, and by extension of transistor 302, in the sub-threshold regions to zero. At the same time, when switch transistor 303 is deactivated, its sub-threshold current needs to be negligible compared to the sub-threshold leakage current of the corresponding transistor 302 in parallel with transistor 303. As a result, in one embodiment, the length of transistors 303 is approximately at least between 2-50 times the length of transistors 302 such that their sub-threshold leakage current is practically zero compared to the current of transistors 302 during the off-state of transistors 303. Furthermore, in one embodiment, the width of transistor 301 is at least between 10-1,000 times the width of transistors 302.

[0037] Depending on the value of the challenge input bit (e.g., 0 or logical value of 1), transistor 302, whose threshold voltage is random, either is part of the pull-down network or is effectively "removed" in that its contribution to the branch current is eliminated. For example, when the value of challenge input C_0 is 0, then transistor 303A is deactivated and the sub-threshold leakage current of the corresponding transistor 302A in parallel with transistor 303A flows thereby affecting the voltage value of the output node V_{out1}. The amount of the sub-threshold leakage current is variable due to the randomness of the threshold voltage of transistors 302. If, however, the value of challenge input C_0 is 1, then transistor 303A is activated, and current flows through transistor 303A to the next series connected transistors 302B, 303B. Based on the values of the challenge input bits, zero or more transistors 303 will be deactivated allowing sub-threshold leakage current from transistors 302 to flow in their branch(es) operating in the sub-threshold region to contribute to the voltage value at the output node V_{out1}.

[0038] A duplicate circuit primitive 101 as the one shown in Figure 3 is provided to generate a voltage value at the other output node, e.g., V_{out2}, such as the output node for circuit primitive 101B shown in Figure 1. Due to the randomness of the threshold voltage of transistors 302, the amount of current that is generated by circuit primitives 101A, 101B (and the voltage value at its output node) will vary even though the circuit primitives 101 have the same circuitry with the same input value (challenge). As a result, comparator 102 compares the two different voltage outputs and generates a random binary output.

[0039] Another embodiment of circuit primitive 101 is provided below in connection with Figure 4. Figure 4 illustrates a further alternative embodiment of the present invention of circuit primitive 101 that is used in circuit 100 depicted in Figure 1.

[0040] Referring to Figure 4, circuit primitives 101 shown in Figures 2 and 3 are special cases of circuit primitive 101 shown in Figure 4. One of the differences between circuit primitive 101 of Figure 4 and circuit primitive 101 of Figure 3 is that circuit primitive 101 of Figure 4 includes a footer transistor 407, 408 (discussed further below) that is controlled by an input that corresponds to the NAND logical operation of the values of the challenge input bits.

[0041] As illustrated in Figure 4, circuit primitive 101 of Figure 4 is an array composed of K columns and N rows of a unit cell, where K and N are positive integer numbers. The unit cell consists of a stochastic sub-threshold n-type transistor. A transistor is referred to as a stochastic transistor if it exhibits strong variability in response to randomness of its threshold voltage. This is achieved by sizing the transistor appropriately. The general dependence is that smaller transistors exhibit more variability. A non-stochastic switch transistor is arranged in parallel to the stochastic transistor. A transistor is referred to as a non-stochastic transistor if it does not exhibit strong variability in response to randomness of its threshold voltage. This is achieved by sizing the transistor to be significantly larger than the minimum-sized transistor. When K is equal to 1, then circuit primitive 101 of Figure 4 will resemble circuit primitive 101 of Figure 3 though in the preferred embodiment of the invention for K = 1, the footer transistors 407 (408 and on) will be omitted. When N is equal to 1, then circuit primitive 101 of Figure 4 will resemble circuit primitive 101 of Figure 2.

[0042] As illustrated in Figure 4, circuit primitive 101 of Figure 4 is an array composed of K columns and N rows of a unit cell, where K and N are positive integer numbers. The unit cell consists of a stochastic sub-threshold n-type transistor. A non-stochastic switch transistor is arranged in parallel to the stochastic transistor. When K is equal to 1, then circuit primitive 101 of Figure 4 will resemble circuit primitive 101 of Figure 3. When N is equal to 1, then circuit primitive 101 of Figure 4 will resemble circuit primitive 101 of Figure 2.

[0043] As further illustrated in Figure 4, circuit primitive 101 of Figure 4 includes an n-type transistor 401 that is functionally similar to n-type transistor 301 of Figure 3. Furthermore, circuit primitive 101 includes parallel circuit blocks 404A-404K, where K is a positive integer number, with the circuitry that is functionally similar to the circuitry of transistors 302, 303 of circuit primitive 101 of Figure 3 with the additional footer transistors 407, 408. Circuit blocks 404A-404K may collectively or individually be referred to as circuit blocks 404 or circuit block 404. While Figure 4 illustrates two circuit blocks 404, circuit primitive 101 may include any number of circuit blocks 404.

[0044] Circuit block 404A includes a series connected n-type transistors 402A-402N, where N is a positive integer number, that are functionally similar to the series connected n-type transistors 302 of circuit primitive 101 of Figure 3. Furthermore, circuit block 404A includes a series connected n-type transistors 403A-403N, where N is a positive integer number, that are functionally similar to the series connected n-type transistors 303 of circuit primitive 101 of Figure 3. N-type transistors 402A-402N may collectively or individually be referred to as n-type transistors 402 or n-type transistor 402, respectively. N-type transistors 403A-403N may collectively or individually be referred to as n-type transistors 403 or n-type transistor 403, respectively. N-type transistors 402 are in parallel with n-type transistors 403. In one embodiment, the number of n-type transistors 402, 403 corresponds to the number of bits in the challenge input. In one embodiment, the number of n-type transistors 402, 403 does not correspond to the number of bits in the challenge input. In one embodiment, n-type transistors 402 are configured similarly as n-type transistors 302 of Figure 3 and will not be discussed in further detail herein for sake of brevity. Furthermore, in one embodiment, n-type transistors 403 are configured similarly as n-type transistors 303 of Figure 3 and will not be discussed in further detail herein for sake of brevity. In one embodiment, the body terminal of stochastic transistors

402 is tied to an internal node of the array as opposed to being tied to ground as shown in Figure 4.

[0045] Circuit block 404A additionally includes a footer transistor 407 that is coupled to the sources of n-type transistors 402N, 403N. The input of footer transistor 407 is controlled by an input that corresponds to the NAND logical operation of the values of the challenge input bits ($C_{11}C_{12}...C_{1N}$, where the first number in the subscript of the challenge input represents the column and the second number in the subscript of the challenge input represents the row). By having footer transistor 407, the node at footer transistor 407 is prevented from being shorted to ground. For example, if all the challenge input bits have the logical value of "1," then the input of footer transistor 407 corresponds to zero thereby preventing the node of footer transistor 407 from being shorted to ground.

[0046] As discussed above, circuit primitive 101 of Figure 4 includes K columns or K circuit blocks configured similarly as circuit block 404A. For example, series connected n-type transistors 405A-405N of circuit block 404K, where N is a positive integer number, are functionally similar to the series connected n-type transistors 402 of circuit block 404A. Furthermore, series connected n-type transistors 406A-406N of circuit block 404K, where N is a positive integer number, are functionally similar to the series connected n-type transistors 403 of circuit block 404A. N-type transistors 405A-405N may collectively or individually be referred to as n-type transistors 405 or n-type transistor 405, respectively. N-type transistors 406A-406N may collectively or individually be referred to as n-type transistors 406 or n-type transistor 406, respectively. N-type transistors 405 are in parallel with n-type transistors 406. In one embodiment, the number of n-type transistors 405, 406 corresponds to the number of bits in the challenge input. In one embodiment, the number of n-type transistors 405, 406 does not correspond to the number of bits in the challenge input. Circuit block 404K additionally includes a footer transistor 408 that is functionally similar to footer transistor 407 of circuit block 404A.

[0047] In circuit primitive 101 of Figure 4, based on the values of the challenge input bits, zero or more transistors 403, 406 will be deactivated allowing sub-threshold leakage current from transistors 402, 405 to flow in their branch(es) operating in the sub-threshold region to contribute to the voltage value at the output node V_{out1}. The randomness of the voltage value produced at

the output node originates in the randomness of the threshold voltage of transistors 402, 405. While the foregoing only discusses the functionality of blocks 404A and 404K, each block 404 of circuit primitive 101 (has a total of K blocks 404) performs functionally the same.

[0048] A duplicate circuit primitive 101 as the one shown in Figure 4 is provided to generate a voltage value at the other output node (e.g., V_{out2}), such as the output node for circuit primitive 101B shown in Figure 1. Due to the randomness of the threshold voltage of transistors 402, 405, the amount of current that is generated by circuit primitives 101A, 101B (and the voltage value at its output node) will vary even though the circuit primitives 101 have the same circuitry with the same conditional input values. As a result, comparator 102 compares the two different voltage outputs and generates a random binary output.

[0049] As a result of the foregoing, circuit 100 (Figure 1) is less vulnerable to machine-learning attacks by relying on the non-linearity of the responses produced by the physics of the FETs at the nanometer scale. Non-linearity is based on the fact that in the sub-threshold region of FET operation, current is an exponential function of threshold voltages which exhibit strong random intrinsic variability. Also, the Drain-Induced Barrier Lowering (DIBL) effect is used to inject strong non-linearity into the response of circuit 100. This additional non-linearity is due to exponential dependence of current on drain-to-source voltage due to DIBL. The generated voltages from the duplicate circuit primitives 101 of circuit 100 implementing a PUF are compared to produce a random binary response.

[0050] It is noted that one of ordinary skill in the art would recognize that circuit 100 and circuit primitives 101 of Figures 1-4 may be configured with different circuitry providing the same functionality as discussed above. For example, n-type logic, e.g., n-type transistors, may be replaced with p-type logic, e.g., p-type transistors.

[0051] While this disclosure mentioned non-linearity in sub-threshold channel current, other mechanisms of strong non-linearity in terminal current-voltage relationships of solid-state field-effect transistors can be used. Those include non-linearities due to gate insulator (e.g., oxide) tunneling current, gate-induced drain leakage, body effect, and other non-linearities well-known to one of ordinary skill in the art.

[0052] It is also noted that the present invention fundamentally exploits the functional behavior of solid-state devices in which terminal current-voltage relationships exhibit strong non-linearity. Therefore, alternative solid-state devices can be used as direct substitutes for the silicon FETs used to illustrate the present invention. Alternative solid-state devices include non-silicon field-effect transistors (those using III-V semiconductor materials or carbon nanotubes), bipolar junction transistors, tunneling field-effect transistors and others.

[0053] The descriptions of the various embodiments of the present invention have been presented for purposes of illustration, but are not intended to be exhaustive or limited to the embodiments disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the described embodiments. The terminology used herein was chosen to best explain the principles of the embodiments, the practical application or technical improvement over technologies found in the marketplace, or to enable others of ordinary skill in the art to understand the embodiments disclosed herein.

CLAIMS:

1. An electronic circuit for implementing a Physically Unclonable Function (PUF), the electronic circuit comprising:

a first and a second circuit primitive configured to generate a first and a second output voltage, respectively, wherein said first and second circuit primitives are duplicates of one another;

a challenge inputted to said first and second circuit primitives; and

a comparator coupled to said first and second circuit primitives, wherein said comparator generates an output based on a difference between said first and second output voltages;

wherein each of said first and second circuit primitives comprises:

one or more circuit blocks, wherein each of said one or more circuit blocks comprises:

a first plurality of series-connected transistors that operate in a sub-threshold region, wherein a gate of each of said first plurality of series-connected transistors is tied to ground or to an internal node, wherein a drain of a first transistor of said first plurality of series-connected transistors is coupled to an output node; and

a second plurality of transistors that are in parallel to said first plurality of series-connected transistors, wherein a drain of a first transistor of said second plurality of transistors is coupled to said output node, wherein a gate of each of said second plurality of transistors receives a value of one bit of said challenge;

a first transistor coupled to a source of a second transistor of said first plurality of series-connected transistors and coupled to a source of a second transistor of said second plurality of transistors in response to having two or more of said circuit blocks, wherein said first transistor is controlled by an input that corresponds to a logical operation of each value for each bit of said challenge;

wherein each of said first and second output voltages of said first and second circuit primitives, respectively, is determined based on current that flows through said first plurality of series-connected transistors of said first and second circuit primitives, respectively, whose magnitude is random based on a threshold voltage variation of said first plurality of series-connected transistors.

2. The electronic circuit as recited in claim 1, wherein each of said first and second circuit primitives further comprises:

a second transistor functioning as a load device that operates in said sub-threshold region, wherein said second transistor has its gate tied to said ground, wherein a source of said second transistor is coupled to said output node.

3. The electronic circuit as recited in claim 2, wherein said load device has a width between 10-1,000 times greater than a width of each of said first plurality of series-connected transistors.

4. The electronic circuit as recited in claim 1, wherein a number of said plurality of series-connected transistors corresponds to a number of bits of said challenge.

5. The electronic circuit as recited in claim 1, wherein a number of said second plurality of transistors corresponds to a number of bits of said challenge.

6. The electronic circuit as recited in claim 1, wherein a length of each of said second plurality of transistors is at least 2-50 times greater than a length of each of said first plurality of series-connected transistors.

7. The electronic circuit as recited in claim 1, wherein a number of said plurality of series-connected transistors does not corresponds to a number of bits of said challenge.

8. The electronic circuit as recited in claim 1, wherein a number of said plurality of series-connected transistors does not correspond to a number of bits of said challenge.

9. The electronic circuit as recited in claim 1, wherein a number of said second plurality of transistors does not correspond to a number of bits of said challenge.

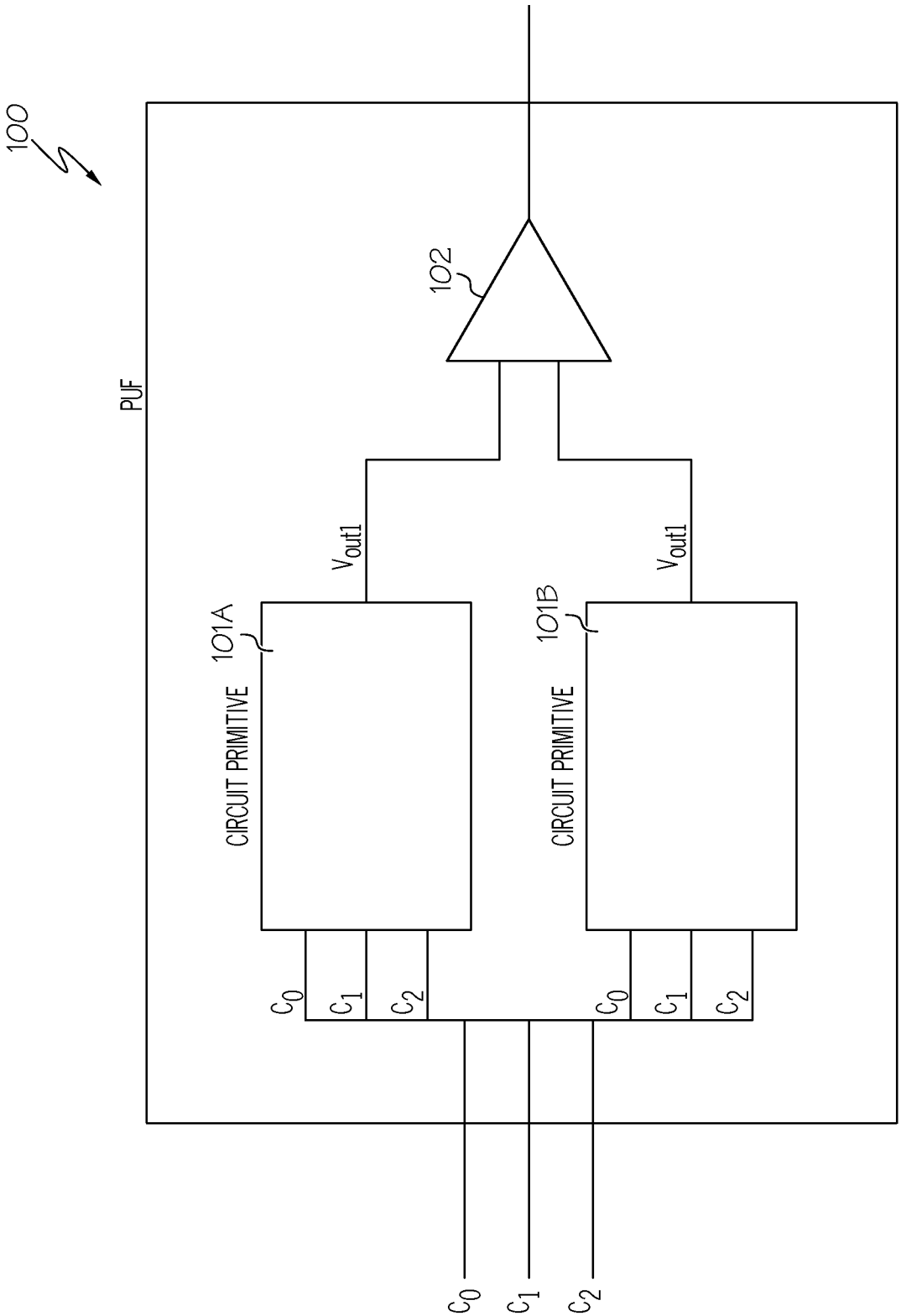

100
PUF
102
V_{out1}
V_{out1}
101A
101B
CIRCUIT PRIMITIVE
CIRCUIT PRIMITIVE
C_0
C_1
C_2
C_0
C_1
C_2
C_0
C_1
C_2

FIG. 1

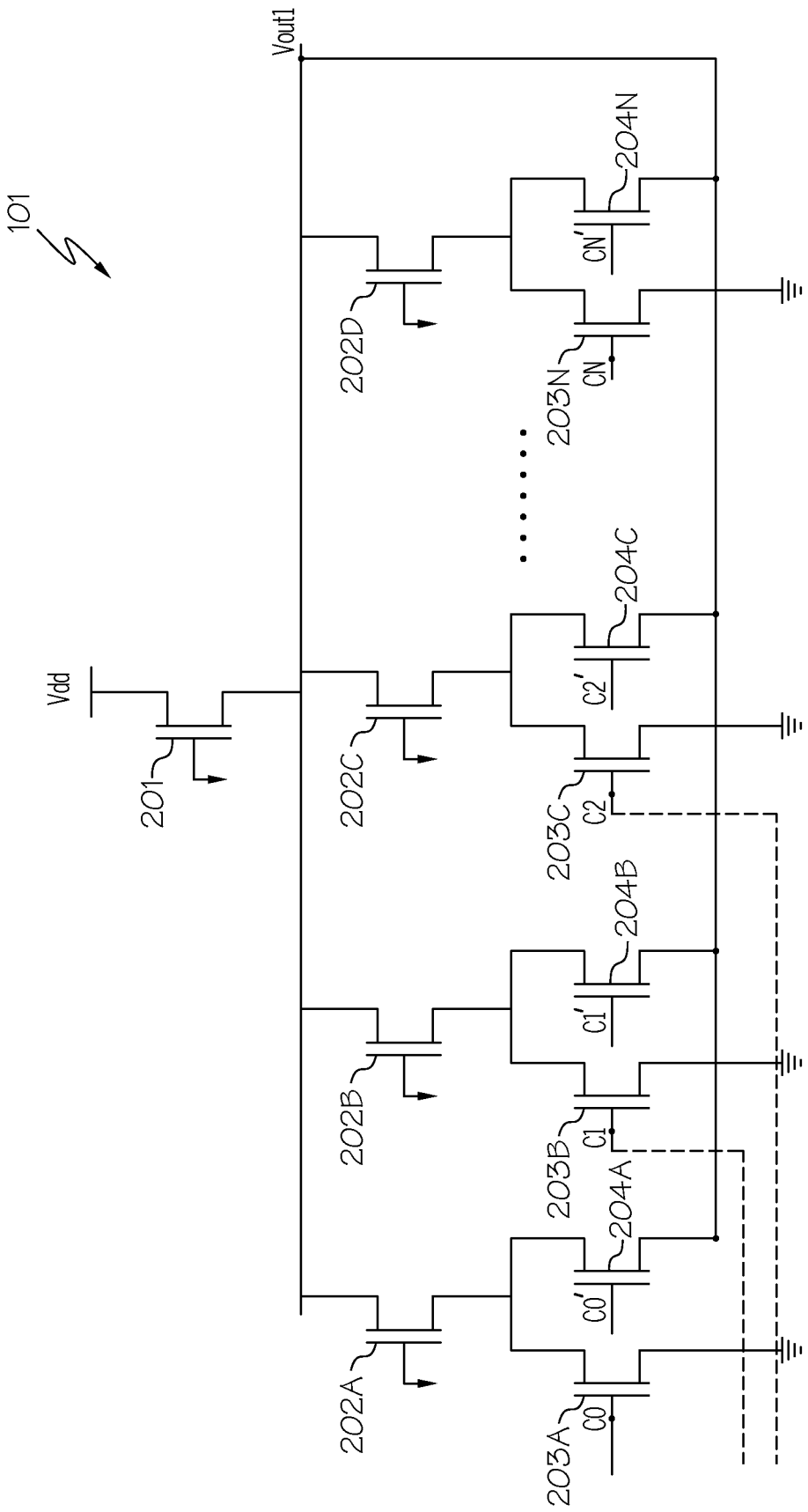

101
Vout1
Vdd
201
202A
202B
202C
202D
203A
203B
203C
203N
204A
204B
204C
204N
C0
C1
C2
CN
C0'
C1'
C2'
CN'

FIG. 2

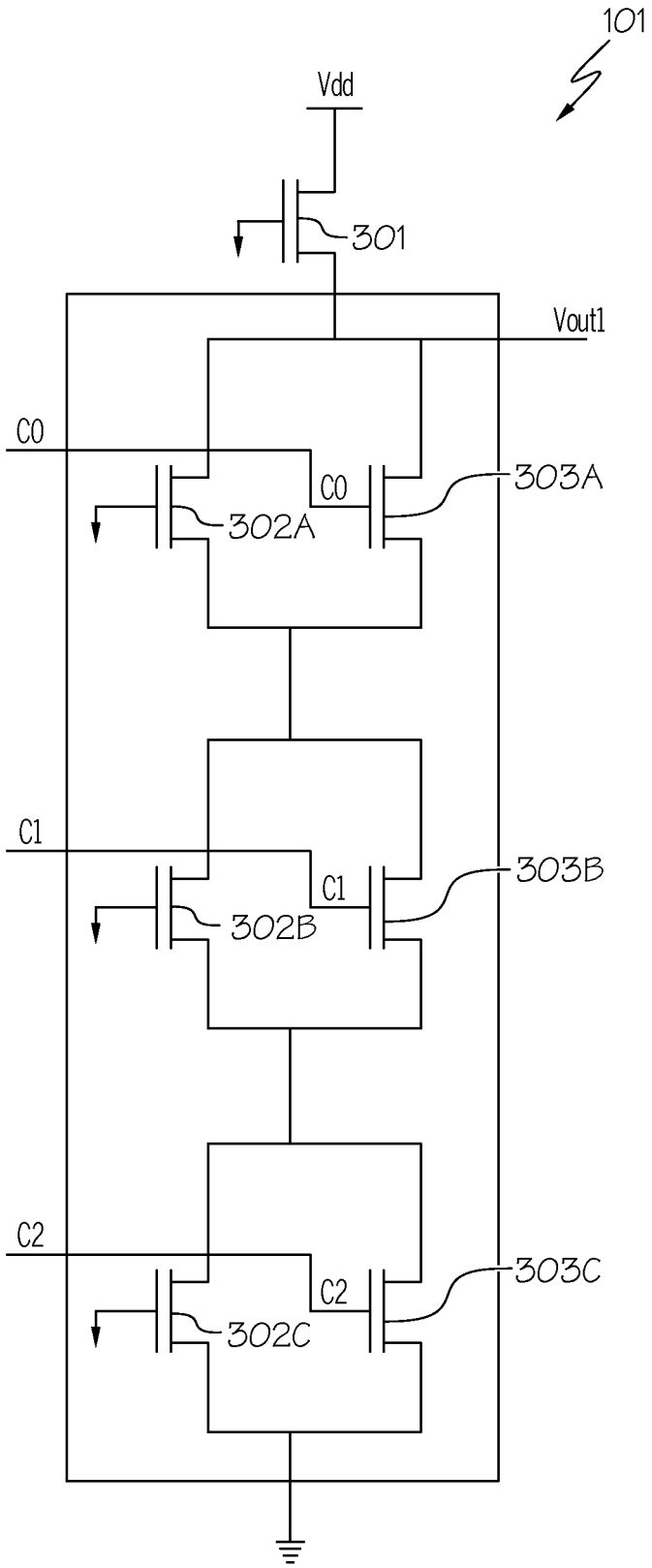

101
Vdd
301
Vout1
C0
C0
303A
302A
C1
C1
303B
302B
C2
C2
303C
302C

FIG. 3

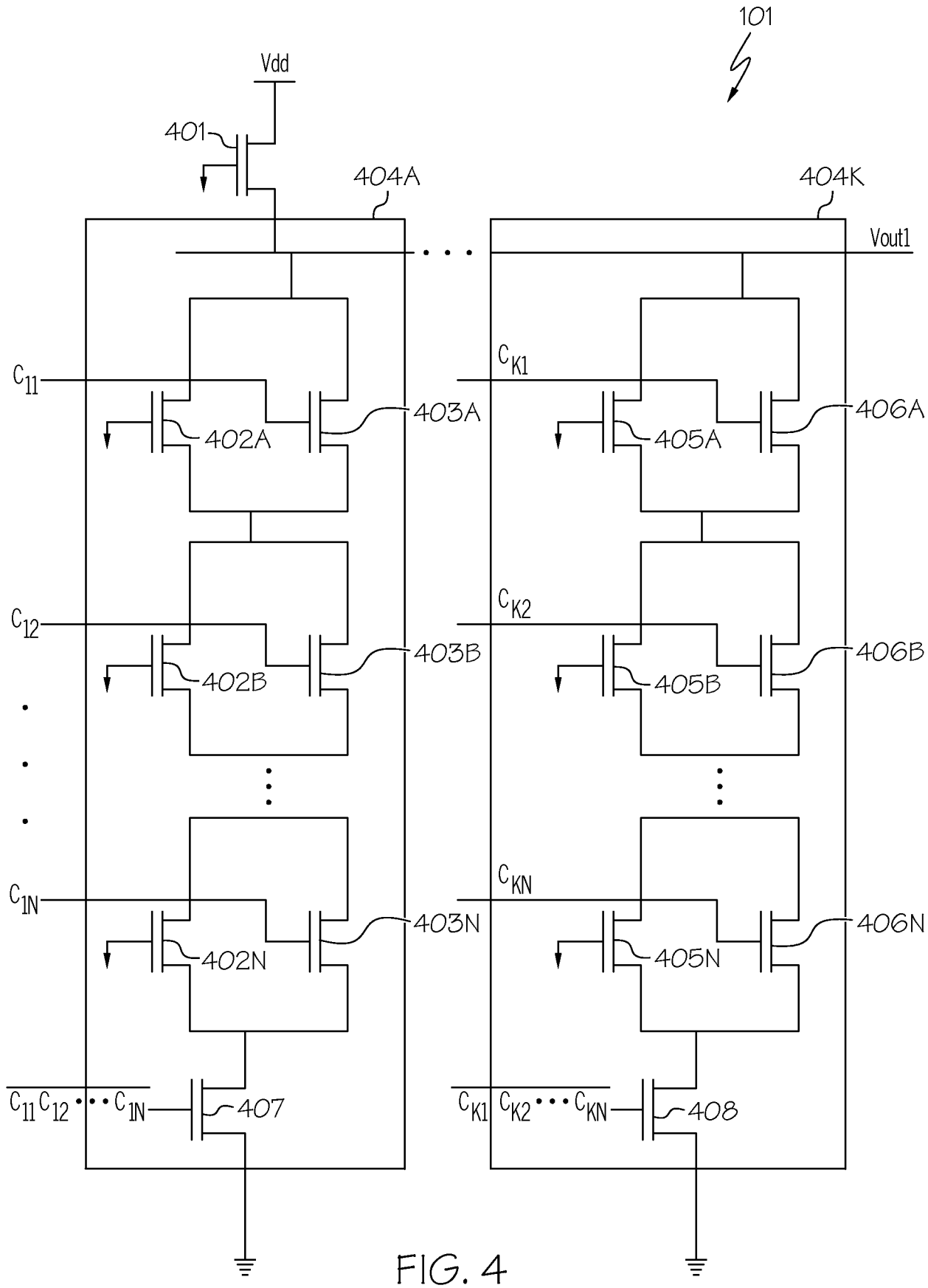

101
Vdd
401
404A
404K
Vout1
C11
C12
C1N
CK1
CK2
CKN
402A
402B
402N
403A
403B
403N
405A
405B
405N
406A
406B
406N
407
408

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US13/43864

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 9/455, 17/50 (2013.01)
USPC - 716/101; 365/148, 703/14
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) Classification(s): G06F 9/455, 17/50 (2013.01)
USPC Classification(s): 365/148, 154, 184, 187, 188; 716/101, 110, 111, 116, 136; 700/52; 703/14, 16

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)
MicroPatent (US-G, US-A, EP-A, EP-B, WO, JP-bib, DE-C,B, DE-A, DE-T, DE-U, GB-A, FR-A); DialogPro (Derwent, INSPEC, NTIS, PASCAL, Current Contents Search, Dissertation Abstracts Online, Inside Conferences); IP.com; IEEE; Search Terms: unclonable, circuit, threshold, voltage, comparator

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011/0317829 A1 (FICKE, J et al.), December 29, 2011, Figure 1, paragraphs [0014]-[0016], [0024]	1-9
A	WO 2012/045627 A1 (SCHRIJEN, G. et al.), April 12, 2012, Page 21, lines 24-32, page 27, lines 10-32, Figure 1	1-9
A	WO 2012/069545 A2 (SIMONS, P. et al.) May 31; 2012, Page 15, lines 10-20, page 17, lines 15-32, Figure 2, Figure 5	1-9

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
19 September 2013 (19.09.2013)	08 OCT 2013

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)