



- (51) International Patent Classification:
G09C 1/00 (2006.01) *H04L 9/32* (2006.01)
- (21) International Application Number:
PCT/EP2017/059987
- (22) International Filing Date:
26 April 2017 (26.04.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
1607614.3 29 April 2016 (29.04.2016) GB
- (71) Applicant: **THE QUEEN'S UNIVERSITY OF BELFAST** [GB/GB]; University Road, Belfast Antrim BT7 1NN (GB).
- (72) Inventors: **GU, Chongyan**; c/o 63 University Road, Belfast Antrim BT7 1NF (GB). **HANLEY, Neil**; c/o 63 University Road, Belfast Antrim BT7 1NF (GB).
- (74) Agent: **WALLACE, Alan**; FRKelly, 4 Mount Charles, Belfast Antrim BT7 1NZ (GB).
- (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: STRONG LIGHTWEIGHT FLIP-FLOP ARBITER PHYSICAL UNCLONABLE FUNCTION (PUF) FOR FPGA

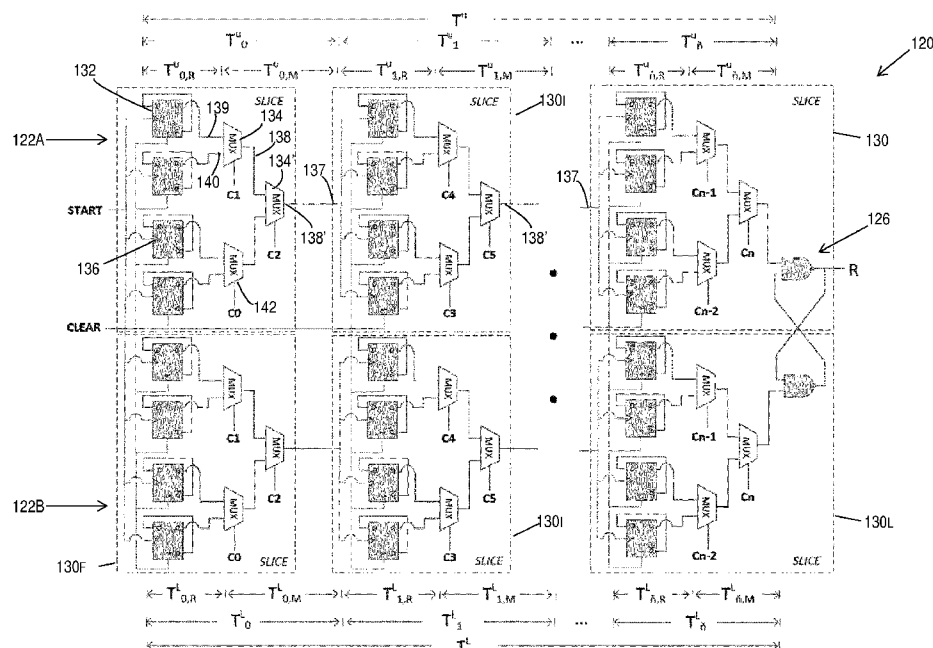


Fig. 3

(57) Abstract: A physical unclonable function (PUF) device comprising two chains of sub-cells that provide two parallel signal paths between an input and an arbiter that generates a response bit depending on the relative timing of the signals arriving on each signal path. Each sub-cell comprises flip flops and multiplexers, the multiplexers being controlled by a challenge input. The device is well suited for implementation on an FPGA, particularly such that a respective sub-cell is implemented in each FPGA slice. The device requires relatively low hardware resources while yielding good uniqueness and reliability results.



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))*

STRONG LIGHTWEIGHT FLIP-FLOP ARBITER PHYSICAL UNCLONABLE FUNCTION (PUF) FOR FPGA

Field of the Invention

5

The present invention relates to Physical Unclonable Functions (PUFs). The invention relates particularly to the implementation of Strong PUFs by an integrated circuit, especially but not exclusively a Field Programmable Gate Array (FPGA).

10 Background to the Invention

An important aspect of improving the trust-worthiness of semi-conductor devices, and semi-conductor based systems is enhancing their physical security. In particular there is a demand for semi-conductor devices to be resistant not only to computational attacks but also to physical attacks
15 such as reverse engineering.

A Physical Unclonable Function (PUF) is a function that is embodied in a physical structure such that when a physical stimulus is applied to the PUF it reacts unpredictably due to the interaction between the stimulus and the physical structure. This is a result of unpredictable physical characteristics
20 being introduced into the physical structure of the PUF during manufacture. The physical stimulus is typically referred to as a challenge and the reaction of the PUF is referred to as a response. A challenge and its respective response are called a challenge-response pair (C/R pair).

PUFs can be implemented to extract the physical properties of a variety of physical systems. For
25 example, it is possible to implement PUFs in integrated circuits (ICs). Silicon or other semi-conductor PUFs can be fabricated using, for example, existing ASIC fabrication processes and therefore can easily interface with ICs or can be built on the same die as other IC-based components. PUFs exploit uncontrollable process variations that occur during the fabrication of ICs. These variations make it impossible to manufacture any two identical devices with identical physical characteristics. Physical
30 Unclonable Functions (PUFs) are therefore able to generate signatures based on device manufacturing variations that are infeasible to control or reproduce.

A variety of semiconductor, in particular silicon, PUF implementations are known, including those categorized as delay-based PUFs, Ring Oscillator PUFs and memory-based PUFs. Delay-based
35 PUFs typically use variations in the propagation delay of identical circuits to derive a unique and secret response from the IC. A number of different architectures may be used such as Arbiter PUFs or Tristate Buffer PUFs. Ring Oscillator based PUFs compare the frequency outputs of otherwise identical oscillators, and Memory-based PUFs, which for example include SRAM PUFs and Butterfly PUFs, depend upon the unpredictable start up state of feedback based CMOS memory structures to
40 produce a secret response. Most CMOS based memory structures including flip-flops, SRAMs and latches, use a cross-coupled structure with a positive feedback to store the required logic.

Ideally, every PUF can generate a unique output for a fixed given input and so provides a means of authentication that can be used in many security, protection, and digital rights management applications.

5

Authentication using PUFs typically involves a challenge-response cycle. Authentication schemes typically require a "Strong" PUF, which has a complex input/output relationship and can generate multiple challenge-response pairs (C/R pairs). The Arbiter PUF is an example of a Strong PUF.

However, known Arbiter PUFs suffer from poor uniqueness and repeatability properties, and are
10 difficult to implement on a Field Programmable Gate Array (FPGA). They also consume excessive FPGA resources to achieve sufficient bit-lengths. In particular, known Arbiter PUFs, which use an n -stage differential delay line and a latch arbiter to generate a 1-bit response, are difficult to achieve on FPGA devices as they require the delay lines to be balanced.

15 It would be desirable therefore to provide a Strong PUF that mitigates the problems outlined above.

Summary of the Invention

A first aspect of the invention provides an integrated circuit for implementing a physical unclonable
20 function, said integrated circuit comprising:

at least one cell having a cell activation input for receiving a cell activation signal, and a response output for providing a response data bit, the, or each, cell further comprising:

an arbiter device having a first input, a second input, an arbiter output, and being configured to produce an arbiter output signal at said arbiter output depending on the relative timing of signals
25 received in use at said first and second inputs, said arbiter output being connected to said response output;

at least one sub-cell connected between said cell activation input and said first input of said arbiter device to create a first signal path between said cell activation input and said arbiter device;

at least one sub-cell connected between said cell activation input and said second input of
30 said arbiter device to create a second signal path between said cell activation input and said arbiter device,

wherein each sub-cell comprises:

a sub-cell activation input;

a sub-cell output;

35 at least two flip flops, each flip flop having a flip flop activation input and a flip flop output, each flip flop activation input being connected to said sub-cell activation input;

and at least one multiplexer connected between said at least two flip flops and said sub-cell output, said at least one multiplexer being operable by at least one selection control input to connect a selected one of said flip flop outputs to said sub-cell output depending on the value of a challenge
40 input provided in use to said at least one selection control input.

Preferably said at least one sub-cell connected between said cell activation input and said first input of said arbiter device comprises a plurality of said sub-cells connected together in a first chain, and said at least one sub-cell connected between said cell activation input and said second input of said arbiter device comprises a plurality of said sub-cells connected together in a second chain, and
5 wherein the sub-cell activation input of a respective first sub-cell in each of said chains is connected to said cell activation input, and the sub-cell output of a respective last sub-cell in each of said chains is connected to the respective one of said first and second arbiter inputs.

Preferably in each of said first and second chains, the sub-cell output of the, or each, sub-cell other
10 than the last sub-cell is connected to the sub-cell activation input of the next sub-cell in the respective chain. Preferably in each of said first and second chains, the sub-cell activation input of the, or each, sub-cell other than the first sub-cell is connected to the sub-cell output of the previous sub-cell in the respective chain.

In preferred embodiments said at least one sub-cell connected between said cell activation input and said first input of said arbiter device comprises a single one of said sub-cells having its sub-cell activation input connected to said cell activation input, and its sub-cell output connected to said first
15 arbiter input, and wherein said at least one sub-cell connected between said cell activation input and said second input of said arbiter device comprises a single one of said sub-cells having its sub-cell
20 activation input connected to said cell activation input, and its sub-cell output connected to said second arbiter input.

Preferably the respective flip flop activation inputs of each flip flop in a respective sub-cell are connected together.
25

Typically said at least one multiplexer comprises a single multiplexer having a respective multiplexer input for each flip flop output of the respective sub-cell, and a single multiplexer output for connecting said selected flip flop output to said sub-cell output.

Said at least one multiplexer typically comprises a plurality of multiplexers connected together in a multi-stage hierarchy in which a plurality of multiplexers in a first stage collectively have a respective multiplexer input connected to a respective flip flop output, and a single multiplexer in a last stage has a single output connected to said sub-cell output, and wherein the output of each multiplexer in the, or each, stage other than said last stage is connected to a respective multiplexer input of the
30 subsequent stage. Conveniently the, or each, multiplexer is a 2-to-1 multiplexer usually with a single
35 bit selector control input.

In preferred embodiments, in each sub-cell, said flip flops are provided in one or more sets of two, a respective multiplexer being provided for the, or each, set, the respective multiplexer having first and
40 second inputs connected to the respective output of each flip flop in the respective set. In a particularly preferred embodiment, each sub-cell comprises four flip flops.

Preferably each sub-cell comprises a hierarchy of 2-to-1 multiplexers, the hierarchy comprising a first stage having two 2-to-1 multiplexers, and a second stage comprising a single 2-to-1 multiplexer, each input of each multiplexer in the first stage being connected to a respective flip flop output, each
5 input of the multiplexer of the second stage being connected to a respective first stage multiplexer output, and the output of the second stage multiplexer being connected to the sub-cell output.

Typically said cell has a reset input for receiving a reset signal, said flip flops having a reset input for receiving said reset signal or a derivative thereof.

10

Said arbiter device may comprise first and second cross-coupled NAND gates.

In typical embodiments the, or each, respective multiplexer is configured, in use, such that corresponding sub-cells in said first and second signal paths are configured identically.

15

Said integrated circuit may be a Field Programmable Gate Array (FPGA) comprising logic resources arranged in a plurality of slices, and wherein each sub-cell is implemented in a respective one of said slices.

20 In typical embodiments, the integrated circuit comprises a plurality of instances of said cell, each generating a respective response bit.

A second aspect of the invention provides an authentication system comprising the integrated circuit of the first aspect and a reader device, said reader device being configured to send at least one
25 multi-bit challenge to said integrated circuit and to receive a corresponding response from the integrated circuit, wherein said at least one multi-bit challenge provides said challenge input and said response comprises the corresponding respective response data bit generated by said at least one cell.

30 A third aspect of the invention provides an authentication method using then authentication system of the second aspect of the invention, said method comprising sending at least one multi-bit challenge to said integrated circuit; providing at least one bit of said challenge to each of said sub-cells as said challenge input; providing a response to said challenge, said response comprising the corresponding respective response data bit generated by said at least one cell.

35

The preferred method includes providing a respective one or more bits of said challenge to each sub-cell. Preferably the method includes providing said at least one challenge to said at least one sub-cell of each of said first and second signal paths simultaneously. The method typically includes providing corresponding sub-cells in said first and second signal paths with the same respective one
40 or more bits of said challenge.

Preferred embodiments provide an FPGA-based Strong PUF that is robust and lightweight. Advantageously, the PUF, or more particularly each PUF logic cell, comprises two identical groups of flip flops and MUXes. The generation of the response depends on generating a race condition between two identical delay paths created by each group of flip flops and MUXes. A hard-macro of a 1-bit Strong PUF design may be utilised to ensure balanced routing and low resource usage.

Further advantageous aspects of the invention will be apparent to those ordinarily skilled in the art upon review of the following description of a specific embodiment.

10 Brief Description of the Drawings

An embodiment of the invention is now described by way of example and with reference to the accompanying drawings in which:

15 Figure 1 is a block diagram of an example PUF based authentication system embodying one aspect of the invention;

Figure 2 is a block diagram of an Arbiter PUF;

20 Figure 3 is a block diagram of a preferred Strong PUF embodying the invention; and

Figure 4 shows equations that describe the challenge and response relationship of the PUF of Figure 3.

25 Detailed Description of the Drawings

Referring now to Figure 1 of the drawings there is shown, generally indicated as 10, a PUF based authentication system embodying one aspect of the invention. The system 10 comprises a PUF device 12, a reader 14 and a data store 16. The PUF device 12, which may be referred to as a silicon, or semiconductor, PUF, comprises a PUF embodied on an IC, and performs as a pseudo-random function that is unique to the integrated circuit. The PUF device 12 is included in a target device whose authenticity it is desired to verify.

The PUF 12 and the reader 14 communicate with each other in accordance with an authentication protocol. During authentication of the PUF 12, the PUF 12 receives an input data value C (the “challenge”) from the reader 14 and returns an unpredictable output data value R (the “response”), or a function thereof. The use of (any) PUF for authentication in the manner of Figure 1 is only one example of many ways to use a PUF. For example, in alternative embodiments either one or both of C and R may be masked by a masking function.

In preferred embodiments, each challenge comprises a respective multi-bit data value. Each response preferably also comprises a respective multi-bit data value. Due to manufacturing variations, the physical structure of each PUF 12 is unique such that it implements a respective pseudo-random function. Hence, the response generated by the PUF 12 is dependent on its physical characteristics and, more particularly, on one or more physical characteristics that result from its manufacturing process. The data store 16, which typically comprises a database, holds data representing a plurality of challenges and their corresponding responses (in respective challenge-response data sets referred to hereinafter as challenge-response pairs (C/R pairs)) for the or each PUF 12 supported by the system 10. This data can be gathered empirically during a registration phase and subsequently used to authenticate the PUF 12, or other article with which the PUF 12 is associated. For example, the PUF 12 may be incorporated into product packaging to allow authentication of the product. In Figure 1, only one PUF 12 is shown. In practice the system 10 may include a plurality of PUFs in that the reader 14 and database 16 may be used in the authentication of a plurality of PUFs, each of which for example is incorporated into respective packaging or other article.

A Strong PUF has a complex challenge-response behaviour and supports a plurality of possible challenges. A Strong PUF is assumed to be effective if it is impossible to determine or attack all the C/R pairs in a given time frame, for example, a few days or weeks. Figure 1 shows a block diagram of an arbiter based PUF, or Arbiter PUF, generally indicated as 20, which is an example of a delay based PUF. The PUF 20 comprises first and second parallel, n -stage (i.e. multi-stage) chains 22A, 22B of multiplexers 24, each chain 22A, 22B feeding an arbiter device 26, typically a flip-flop, to form 1-bit of an n -bit PUF.

Each stage of each chain 22A, 22B comprises a respective multiplexers 24A, 24B each having first and second selectable inputs, an output and a control input for determining which of the selectable inputs is provided at the output. In use a respective bit (C_1 to C_N) of the challenge is used for each stage, such that the respective challenge bit is provided to the control inputs of the multiplexers of the respective stage. Typically, the number of bits in the challenge is the same as the number of stages in the chains. The outputs of each multiplexer of each stage are provided to a respective input of each of the multiplexers in the following stage, except in the case of the final stage where the outputs of each multiplexer are provided to the arbiter device 26. The PUF 20 has an activation input provided to each input of each multiplexer of the first stage. In use, a step or state transition input signal is provided to the activation input as an activation signal, which signal propagates along the chains 22A, 22B to reach the arbiter 26. The arbiter 26 generates a response R_i bit depending on the relative timing of the signals received at its respective inputs.

The arrangement is such that, depending on the value of the challenge bit at each stage, each stage is configured as either cross-connect (so that the output of the multiplexer of each chain is provided to an input of the multiplexer of the next stage in the other chain) or straight-through connection (so that so that the output of the multiplexer of each chain is provided to an input of the multiplexer of the

next stage in its respective chain). The arbiter 26 compares the arrival time of its two inputs racing against each other, when enabled, to generate the response bit, which should differ between devices due to variability effects.

- 5 In an FPGA, logic resources are provided in groups known as slices to create configurable logic blocks such that the FPGA, or part of it, can be configured to provide the desired functionality of any particular design. Typically a slice contains a fixed set of logic resources that may comprise a plurality of Look-up tables (LUTs), flip-flops, multiplexers and/or logic gates. A problem in the design of arbiter based PUFs, particularly when implemented on an FPGA, is how to achieve balanced
- 10 paths from the activation input to the arbiter device 26.

Referring now to Figure 3, there is shown, generally indicated as 120, a schematic representation of a PUF logic cell embodying one aspect of the invention. As is described in more detail below, the cell 120 may be used to implement a Strong PUF, in particular an arbiter type PUF but more generally a

15 delay type PUF. The cell 120 generates a single bit output R from a multi-bit challenge C. To implement a PUF with a multi-bit response, multiple instances of the cell 120 are provided. For example an array of N asynchronous elementary 1-bit cells 120 are provided to implement a PUF having an N -bit response R.

- 20 In preferred embodiments, the cell 120 comprises a plurality of sub-cells 130 arranged in an array comprising first and second parallel chains 122A, 122B of at least two sub-cells 130 per chain (although in other embodiments each chain may comprise only one sub-cell). Each chain 122A, 122B has a first sub-cell 130_F, a last sub-cell 130_L and typically at least one other sub-cell 130_i intermediate the first and last sub cells. Each sub-cell 130 has input and an output, the output of
- 25 each sub-cell 130 in each chain being connected to the input of the next sub-cell 130 in the respective chain, with the exception of the last sub-cell 130_L the output of which is used to provide the response bit R. More particularly, the respective outputs of the last sub-cell 130_L of each chain are provided to an arbiter device 126, preferably an asynchronous arbiter. The arbiter 126 generates a single bit output R the value of which, i.e. logic 1 or logic 0 in this case, depends on the relative
- 30 timing of the respective signals provided to it by each chain 122A, 122B. In the illustrated embodiment, the arbiter 126 comprises first and second cross coupled NAND gates, but could alternatively comprise any suitable alternative circuit or device, e.g. a flip flop. The input of the first sub-cell 130_F of each chain receives an activation signal *START*, which is typically a step signal, e.g. a transition from logic 0 to logic 1 or vice versa.

35

- Each sub-cell 130 comprises at least two flip flops 132 and at least one multiplexer (MUX) 134. Each flip flop has an activation (or clock) input 136 and an output Q. In use, the activation inputs 136 receive the same input signal and to this end may be connected together. In the case of the first sub-cell 130_F of each chain, the common input signal is the activation signal *START*. For the other sub-
- 40 cells of each chain the input signal is the output signal provided by the preceding sub-cell 130 in the respective chain 122A, 122B. Each MUX 134 has an output 138, first and second selectable inputs

139, 140 and a control input 142 the value of which determines which of the selectable inputs 139, 140 is provided as the output 138. In use, the START signal is provided to each chain 122A, 122B simultaneously and so the activation inputs 136 of the first sub-cell 130 in each chain are conveniently connected together to provide the activation input for the sub-cell.

5

In preferred embodiments, in each sub-cell 130 the flip flops 132 are provided in multiples of two, a respective MUX 134 being provided for each set of two flip flops 132, and wherein the respective outputs Q of each flip flop 132 in the respective set are provided as the respective selectable inputs 139, 140 of the respective MUX 134. In addition, the sets of two flip flops are preferably provided in multiples of two, a respective additional MUX 134' being provided for each group of flip flop sets, wherein the respective outputs 138 of each MUX 134 of the respective group are provided as the respective selectable inputs 139, 140 of the respective MUX 134'. More generally, for each group of two MUXes 134, a further MUX 134' is provided to receive the respective output of each of the two MUXes 134 as its selectable inputs. It will be apparent therefore that two or more stages of MUXes may be provided until a last stage is reached having only one MUX 134'. The output of the last MUX 134' provides the output of the respective sub-cell 130.

In the illustrated embodiment, each sub-cell 130 has four flip flops 132, arranged in two sets of two, each set providing the selectable inputs 139, 140 to a respective MUX 134, the outputs of which provide the selectable inputs 139, 140 to the last MUX 134' which provides the output of the sub-cell 130. As such there are two stages of MUXes. In a simpler embodiment, the sub-cell may comprise only two flip flops 132 feeding a single MUX 134. More generally, in preferred embodiments each sub-cell 130 has 2^n flip flops 132 followed by n MUX stages each MUX stage having $n-x$ MUXes 134 where $x=1$ to n from the first stage to the last.

25

The control input for each MUX 134 is provided by a respective bit of the challenge. The same challenge (i.e. a selected one of the available challenges) is applied to each chain 122A, 122B simultaneously. In the simple embodiment (not illustrated) where there are only two flip flops 132 and one MUX 134 in each sub-cell 130, a respective single bit of the challenge is provided to each sub-cell 130. As such each chain 122A, 122B may comprise the same number of sub-cells 130 as there are bits in the challenge. In preferred embodiments however, each sub-cell includes more than one MUX and so more than one bits of the challenge are provided to each sub-cell. In the illustrated embodiment a respective three bits of the challenge are provided to each sub-cell 130, e.g. bits C0, C1 and C2 to the first sub-cell 130, bits C3, C4 and C5 to the second sub-cell and so on. The same challenge bit(s) are provided to the corresponding sub-cell 130 in each chain 122A, 122B. Accordingly, each corresponding sub-cell in each chain is configured in the same way by its multiplexers.

It will be apparent that the flip flops and MUXes of each sub-cell 130 in a given chain 122A, 122B, create a signal, or delay, path (indicated in Figure 3 as T^U and T^L respectively) for the respective chain 122A, 122B between its input (i.e. the input of the first cell 130F in the chain) and the

40

respective input of the arbiter 126. Depending on the control input values (i.e. the value of the respective challenge bit C_i) provided to the MUXes, the MUXes 134 in each sub-cell 130 select which of the flip flops 132 in the respective sub-cell 130 form part of the respective delay path. In preferred embodiments, the MUXes 134 are arranged in a multi-stage hierarchy in which a plurality of MUXes in a first stage receive inputs from the flip flops and provide outputs to a fewer number of MUXes in the next stage, and so on until a single last stage MUX provides the output of the sub-cell 130. This may be described as a cascaded hierarchy of multiplexers, in which the output of the multiplexers in each (higher) stage in the hierarchy feed an input of a respective multiplexer in the subsequent (lower) stage of the hierarchy (where each higher stage has more multiplexers than the subsequent lower stage) until the last (lowest) stage comprises a single multiplexer with a single output. The number of multiplexers in the first stage of the hierarchy depends on the type of multiplexer (in particular how many inputs it has) and on the number of flip flops in the sub-cell. There may be one or more stages in the hierarchy, as required.

In preferred embodiments, the MUXes 134 are multiple input single output multiplexers. In particular, the MUXes 134 are preferably 2-to-1 MUXes with a single bit control input. In alternative embodiments, MUXes with more than 2 inputs and a multi-bit control input may alternatively be used. For example, in the embodiment of Figure 3, the 2 stage MUX hierarchy may be replaced by a single 4-to-1 MUX with a 2 bit control input. Such an embodiment requires fewer MUX control bits per sub-cell 130 than the embodiment of Figure 3, which may be compensated for by using shorter challenges or longer chains 122A, 122B.

In preferred embodiments, the cell 120 is arranged to receive a reset signal CLEAR which resets all of the flip flops 132 in all of the sub-cells 130 to a reset state. Typically, each flip flop 132 has a reset input for receiving the reset signal. In use all of the flip flops in at least the first sub-cells 130_F are preferably reset simultaneously and so, conveniently, the reset inputs of the relevant flip flops 132 are connected together.

In preferred embodiments, the architecture and configuration of each sub-cell 130 is the same (other than the provision of the arbiter at the end of the chains) and the configuration of each parallel chain 122A, 122B is the same. Therefore the respective delay path provided by each chain is substantially identical, e.g. subject to variations caused by fabrication rather than architecture/configuration.

For FPGA implementation the flip flops are D flip flop since that is what is typically available on an FPGA. However, in alternative embodiments, e.g. for an ASIC implementation, other types of flip flops, for example JK flip flops may be used with minor circuit modifications.

In the illustrated embodiment, on reset $Q = 0$, and $Q_{inv} = 1$ for all flip-flops 132. As Q_{inv} is connected to D, on the activation of the clock signal $Q = D = Q_{inv} = 1$ (which is the value of Q_{inv} at the clock edge, immediately after the clock edge $Q_{inv} = 0$, but by now $Q=1$). As Q is connected to the next

stage activation signal, this allows the rising edge to “flow” through the system by sequentially changing all Q from 0=>1.

In the illustrated embodiment, to generate a single bit response, R , n MUXes 134 and

- 5 $4n/3$ flip flops 132 are cascaded in each of the two paths provided by the respective chains 122A, 122B, where the value of n depends on the number of sub-cells 130 in the chains (there are 3 MUXes in each sub-cell in this example and so the value of n is three times the number of sub-cells in the chains).
- 10 In use, the flip flops 132 in the first sub-cells 132_F are first reset by *CLEAR* and then activated by the rising edge of the *START* signal, which is fed into the respective activation inputs 136. Depending on the control input values (i.e. the value of the respective challenge bit C_i) provided to the MUXes 134, the MUXes 134 in the respective sub-cell 130 select are used to select one of the flip flops 132 of the respective sub-cell 130 to form part of the delay path for the respective chain 122A, 122B. The
- 15 output of the sub cell 130_F is fed into the activation input of the next sub-cell 130 and so on, until the last sub-cell 130_L . The last cells 130_L of the chains 122A, 122B together contained the arbiter 126, conveniently in the form of cross-coupled NAND gates. The arbiter 126 determines which delay path, T^U or T^L , is faster, returning an output R of either one or zero depending on the relative timing of the signals reaching it via the respective chains 122A, 122B. T^U and T^L respectively represent the upper
- 20 and lower delay paths used in the generation of each 1-bit response.

The sub-cells 130 of each chain operate asynchronously in that their respective flip flops are not operated by a common clock signal. Instead the clock (control) input of the first sub-cell 130_F is fed by the *START* signal, while the clock (control) input of the subsequent sub-cell(s) are fed by the

25 output of the preceding sub-cell 130.

The output R generated by the cell 120 may serve as a single bit PUF response, or as a single bit of a multi-bit PUF response. To generate an N -bit PUF response, a PUF logic circuit may be provided which comprises a plurality (N) of instances of the cell 120, each instance produce a respective

30 single bit of the N -bit response.

When multiple cells 120 are provided to give an N -bit PUF response, the cells 120 may be connected together to receive the *START* signal simultaneously and/or to receive the challenge bits simultaneously. Alternatively, the cells 120 can operate asynchronously and/or receive different

35 challenges if required. Alternatively still, a single cell 120 may be used to generate an n -bit response R_n from a single challenge C by applying a function, e.g. a random one-way function, to the challenge before supplying it to the cell 120 to generate successive bits of the response. For example: $R_1 = \text{PUF}(C)$; $R_2 = \text{PUF}(F(C))$; $R_3 = \text{PUF}(F(F(C)))$ and so on, where F is a random one-way function. In any case, the input challenge need not be the same for all cells 120, i.e. some or all cells

40 may receive the same challenge, or all cells may receive a different challenge.

The challenge and response relationship of a Strong PUF implemented using the cells 120 can be described by equation [1] of Figure 4, wherein T^U and T^L are as defined in equations [2] and [3], where T_i^U , T_i^L are respectively the delay times of the i -th slices in the upper and lower delay paths, $T_{i,M}^U$ and $T_{i,R}^U$ are respectively the delay times of the MUX and flip flops (including delays between
 5 said components) in the i -th sub-cells 130 in the upper delay paths (chain 122A), and $T_{i,M}^L$ and $T_{i,R}^L$ are respectively the delay times of the MUX and flip flops of the i -th sub-cell 130 in the lower delay paths (chain 122B). Equation [1] may therefore be re-written as equation [4] of Figure 4.

Advantageously, a PUF device that uses one or more PUF logic cells embodying the present
 10 invention, including one or more instances of the cell 120, is implemented on an integrated circuit (IC), typically an FPGA. In preferred embodiments, the common logic resources required by each sub-cell are typically available on a single FPGA slice (although the arbiter may be provided on a separate slice). Conveniently therefore, each sub-cell 130 may be implemented by a respective (separate) slice of the FPGA. This facilitates the provision of balanced routing in each slice and
 15 therefore throughout the PUF, which helps to ensure a robust PUF response. In contrast traditional Arbiter type PUFs are non-trivial to implement on an FPGA due to restrictions when performing the routing, which can significantly bias the PUF response if poorly balanced.

By way of example, an Artix-7 XC7A100TFPGA (trade mark) FPGA device may be used, which has
 20 15850 slices. To generate a 1-bit response from a 64 bit challenge using the proposed Strong PUF design of Figure 3 requires only 44 slices. 42 slices are used to implement 4 flip-flops and 3 MUXes per slice, while the last two slices implement the extra cross-coupled NAND gates of the final stages also. The MUXes and/or cross coupled NAND gates can be implemented using a LUT, dedicated internal slice MUXs as convenient. Each slice of the Xilinx Artix-7 FPGA has 4 flip-flops, which allows
 25 for the 4 flip-flops of the proposed PUF cell to be placed in a single slice. For the generation of each 1-bit response R from a 64 bit challenge, the 44 slices may be implemented as a hard macro; hence, to generate a 64-bit response, a maximum of 64 hard macros and 64×44 slices are required. It will be understood that the logic architecture of Figure 3 may equally suit other FPGA devices, and that the logic architecture of alternative embodiments may be adapted to facilitate
 30 implementation on any available FPGA device.

Preferred embodiments of the invention may for example be implemented on a Xilinx Artix-7 (trade mark) FPGA, or other FPGA, and have a relatively small hardware resource requirement compared to known Strong PUF designs. PUFs embodying the invention also yield relatively good uniqueness
 35 and reliability results compared to known Strong PUF designs. For example, to generate a 1-bit response from a 64 bit challenge, the design only requires 44 slices of the Artix-7 FPGA.

The invention is not limited to the embodiment(s) described herein but can be amended or modified without departing from the scope of the present invention.

CLAIMS:

1. An integrated circuit for implementing a physical unclonable function, said integrated circuit comprising:
 - 5 at least one cell having a cell activation input for receiving a cell activation signal, and a response output for providing a response data bit, the, or each, cell further comprising:
 - an arbiter device having a first input, a second input, an arbiter output, and being configured to produce an arbiter output signal at said arbiter output depending on the relative timing of signals received in use at said first and second inputs, said arbiter output being connected to said response
 - 10 output;
 - at least one sub-cell connected between said cell activation input and said first input of said arbiter device to create a first signal path between said cell activation input and said arbiter device;
 - at least one sub-cell connected between said cell activation input and said second input of said arbiter device to create a second signal path between said cell activation input and said arbiter
 - 15 device,
 - wherein each sub-cell comprises:
 - a sub-cell activation input;
 - a sub-cell output;
 - at least two flip flops, each flip flop having a flip flop activation input and a flip flop output,
 - 20 each flip flop activation input being connected to said sub-cell activation input;
 - and at least one multiplexer connected between said at least two flip flops and said sub-cell output, said at least one multiplexer being operable by at least one selection control input to connect a selected one of said flip flop outputs to said sub-cell output depending on the value of a challenge input provided in use to said at least one selection control input.
 - 25
2. The integrated circuit of claim 1, wherein said at least one sub-cell connected between said cell activation input and said first input of said arbiter device comprises a plurality of said sub-cells connected together in a first chain, and said at least one sub-cell connected between said cell activation input and said second input of said arbiter device comprises a plurality of said sub-cells
- 30 connected together in a second chain, and wherein the sub-cell activation input of a respective first sub-cell in each of said chains is connected to said cell activation input, and the sub-cell output of a respective last sub-cell in each of said chains is connected to the respective one of said first and second arbiter inputs.
- 35 3. The integrated circuit of claim 2, wherein in each of said first and second chains, the sub-cell output of the, or each, sub-cell other than the last sub-cell is connected to the sub-cell activation input of the next sub-cell in the respective chain.
4. The integrated circuit of claim 2 or 3, wherein in each of said first and second chains, the sub-cell
- 40 activation input of the, or each, sub-cell other than the first sub-cell is connected to the sub-cell output of the previous sub-cell in the respective chain.

5. The integrated circuit of claim 1, wherein said at least one sub-cell connected between said cell activation input and said first input of said arbiter device comprises a single one of said sub-cells
5 having its sub-cell activation input connected to said cell activation input, and its sub-cell output connected to said first arbiter input, and wherein said at least one sub-cell connected between said cell activation input and said second input of said arbiter device comprises a single one of said sub-cells having its sub-cell activation input connected to said cell activation input, and its sub-cell output connected to said second arbiter input.
- 10 6. The integrated circuit of any preceding claim, wherein the respective flip flop activation inputs of each flip flop in a respective sub-cell are connected together.
7. The integrated circuit of any preceding claim, wherein said at least one multiplexer comprises a
15 single multiplexer having a respective multiplexer input for each flip flop output of the respective sub-cell, and a single multiplexer output for connecting said selected flip flop output to said sub-cell output.
8. The integrated circuit of any one of claims 1 to 6, wherein said at least one multiplexer comprises
20 a plurality of multiplexers connected together in a multi-stage hierarchy in which a plurality of multiplexers in a first stage collectively have a respective multiplexer input connected to a respective flip flop output, and a single multiplexer in a last stage has a single output connected to said sub-cell output, and wherein the output of each multiplexer in the, or each, stage other than said last stage is connected to a respective multiplexer input of the subsequent stage.
- 25 9. The integrated circuit of any preceding claim, wherein the, or each, multiplexer is a 2-to-1 multiplexer.
10. The integrated circuit of claim 9, wherein the, or each, multiplexer has a single bit selector
30 control input.
11. The integrated circuit of claim 9 or 10, wherein, in each sub-cell, said flip flops are provided in one or more sets of two, a respective multiplexer being provided for the, or each, set, the respective multiplexer having first and second inputs connected to the respective output of each flip flop in the
35 respective set.
12. The integrated circuit of any preceding claim, wherein each sub-cell comprises four flip flops.
13. The integrated circuit of claim 12, wherein each sub-cell comprises a hierarchy of 2-to-1
40 multiplexers, the hierarchy comprising a first stage having two 2-to-1 multiplexers, and a second stage comprising a single 2-to-1 multiplexer, each input of each multiplexer in the first stage being

connected to a respective flip flop output, each input of the multiplexer of the second stage being connected to a respective first stage multiplexer output, and the output of the second stage multiplexer being connected to the sub-cell output.

5 14. The integrated circuit of any preceding claim, wherein said cell has a reset input for receiving a reset signal, said flip flops having a reset input for receiving said reset signal or a derivative thereof.

15. The integrated circuit of any preceding claim, wherein said arbiter device comprises first and second cross-coupled NAND gates.

10

16. The integrated circuit of any preceding claim, wherein the, or each, respective multiplexer is configured, in use, such that corresponding sub-cells in said first and second signal paths are configured identically.

15 17. The integrated circuit of any preceding claim, wherein said integrated circuit is a Field Programmable Gate Array (FPGA) comprising logic resources arranged in a plurality of slices, and wherein each sub-cell is implemented in a respective one of said slices.

18. The integrated circuit of any preceding claim, comprising a plurality of instances of said cell, each
20 generating a respective response bit.

19. An authentication system comprising an integrated circuit as claimed in any preceding claim and a reader device, said reader device being configured to send at least one multi-bit challenge to said integrated circuit and to receive a corresponding response from the integrated circuit, wherein said at
25 least one multi-bit challenge provides said challenge input and said response comprises the corresponding respective response data bit generated by said at least one cell.

20. An authentication method using an authentication system as claimed in claim 19, said method comprising sending at least one multi-bit challenge to said integrated circuit; providing at least one bit
30 of said challenge to each of said sub-cells as said challenge input; providing a response to said challenge, said response comprising the corresponding respective response data bit generated by said at least one cell.

21. The method of claim 20, including providing a respective one or more bits of said challenge to
35 each sub-cell.

22. The method of claim 20 or 21, including providing said at least one challenge to said at least one sub-cell of each of said first and second signal paths simultaneously.

40 23. The method of any one of claims 20 to 21, including providing corresponding sub-cells in said first and second signal paths with the same respective one or more bits of said challenge.

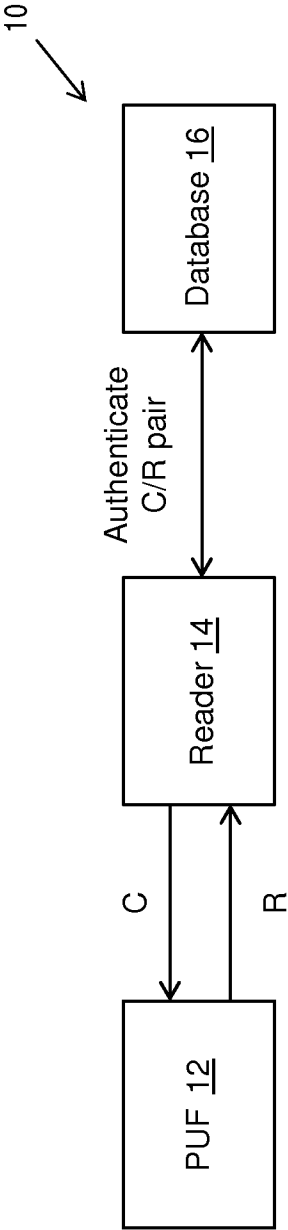


Fig. 1

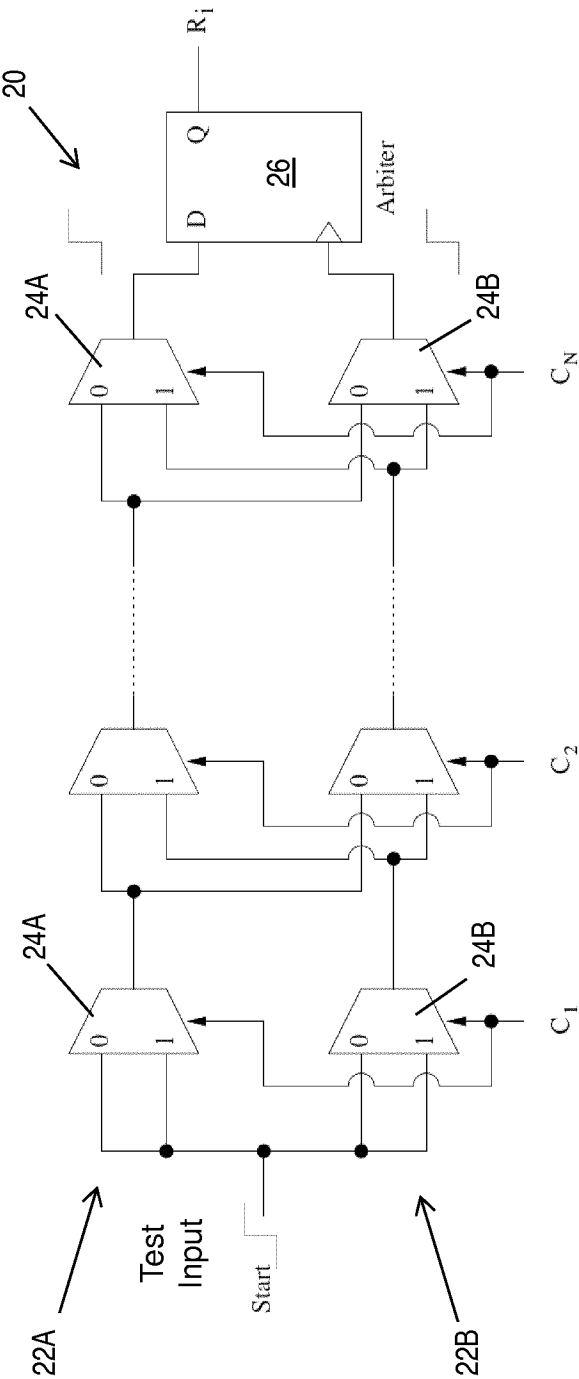


Fig. 2

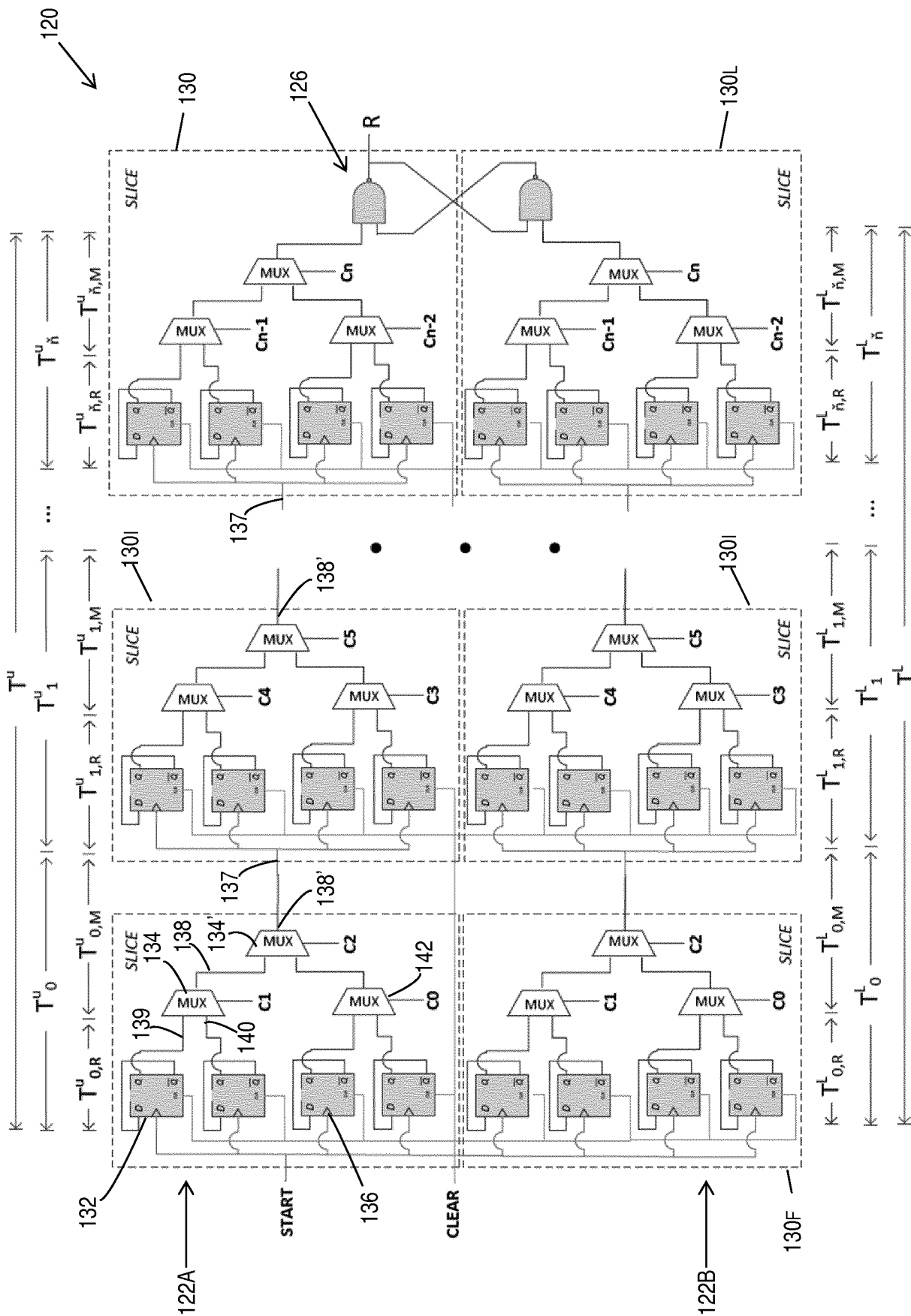


Fig. 3

$$T^U - T_L \overset{r=0}{\underset{r=1}{\geq}} 0$$

[1]

$$\begin{aligned} T^U &= T_0^U + T_1^U + T_2^U + \dots + T_{\tilde{n}}^U \\ &= T_{0,M}^U + T_{0,R}^U + T_{1,M}^U + T_{1,R}^U + T_{2,M}^U + T_{2,R}^U + \dots + T_{\tilde{n},M}^U + T_{\tilde{n},R}^U \end{aligned}$$

[2]

$$\begin{aligned} T^L &= T_0^L + T_1^L + T_2^L + \dots + T_{\tilde{n}}^L \\ &= T_{0,M}^L + T_{0,R}^L + T_{1,M}^L + T_{1,R}^L + T_{2,M}^L + T_{2,R}^L + \dots + T_{\tilde{n},M}^L + T_{\tilde{n},R}^L \end{aligned}$$

[3]

where:

$$\tilde{n} = \frac{n}{\text{\#MUXES in the slice}}$$

[4]

$$\sum_{i=1}^{\tilde{n}} (T_{i,M}^U - T_{i,M}^L) + \sum_{i=1}^{\tilde{n}} (T_{i,R}^U - T_{i,R}^L) \overset{r=0}{\underset{r=1}{\geq}} 0$$

[5]

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/059987

A. CLASSIFICATION OF SUBJECT MATTER
INV. G09C1/00 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G09C H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHONGYAN GU ET AL: "Ultra-compact and robust FPGA-based PUF identification generator", THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC. (IEEE) CONFERENCE PROCEEDINGS, 1 May 2015 (2015-05-01), page 934, XP055388330, Piscataway	1-19
Y	paragraph [0002]	19-23
Y	GB 2 507 988 A (UNIV BELFAST [GB]) 21 May 2014 (2014-05-21) page 6, line 4 - page 9, line 24 ----- -/-	19-23



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

"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

5 July 2017

Date of mailing of the international search report

13/07/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bec, Thierry

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/059987

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CORTES MARIO ET AL: "Improving the statistical variability of delay-based physical unclonable functions", 2015 28TH SYMPOSIUM ON INTEGRATED CIRCUITS AND SYSTEMS DESIGN (SBCCI), ACM, 31 August 2015 (2015-08-31), pages 1-7, XP032894663, [retrieved on 2016-04-26] paragraph [0002] - paragraph [0004] -----	1-18
X	DURGA PRASAD SAHOO ET AL: "Architectural Bias: a Novel Statistical Metric to Evaluate Arbiter PUF Variants", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20160125:082704, 23 January 2016 (2016-01-23), pages 1-14, XP061020031, [retrieved on 2016-01-23] paragraph [00IV] -----	1-18
A	SHAHIN TAJIK ET AL: "Physical Characterization of Arbiter PUFs", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20141010:142847, 6 October 2014 (2014-10-06), pages 1-18, XP061017075, [retrieved on 2014-10-06] paragraphs [0002], [0005] -----	1-23
A	US 2013/047209 A1 (SATO AKASHI [JP] ET AL) 21 February 2013 (2013-02-21) figures 1-6 paragraph [0049] - paragraph [0075] -----	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/059987

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2507988	A	21-05-2014	EP 2920909 A1 23-09-2015
			GB 2507988 A 21-05-2014
			US 2015278505 A1 01-10-2015
			WO 2014076151 A1 22-05-2014

US 2013047209	A1	21-02-2013	CN 102812472 A 05-12-2012
			JP 5499358 B2 21-05-2014
			JP 2011198317 A 06-10-2011
			US 2013047209 A1 21-02-2013
			WO 2011118548 A1 29-09-2011
