



(51) International Patent Classification:

H03K 19/003 (2006.01) *H03K 23/00* (2006.01)

(21) International Application Number:

PCT/IB2018/001147

(22) International Filing Date:

03 July 2018 (03.07.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicants: **DOLPHIN INTEGRATION** [FR/FR]; 39, Avenue du Granier, 38240 Meylan (FR). **INSTITUT POLYTECHNIQUE DE GRENOBLE** [FR/FR]; 46 Avenue Félix Viallet, 38031 Grenoble Cedex 1 (FR).

(72) Inventors: **FESQUET, Laurent**; 4, Hameau du Haut Plaçage, 38360 Sassenage (FR). **CHERKAOUI, Abdelkarim**; 1584, chemin du Canet, 38950 Saint-Martin-Le-Vinoux (FR). **GIMENEZ, Grégoire**; 12, avenue Général Champon, 38000 Grenoble (FR). **FRISCH, Raphael**; 51, rue des Taillées, 38400 Saint Martin D'heres (FR).

(74) Agent: **CABINET BEAUMONT**; 4 Place Robert Schuman - B.P. 1529, 38025 Grenoble Cedex 1 (FR).

(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, JO, 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, 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,

(54) Title: CIRCUIT AND METHOD FOR PROTECTING ASYNCHRONOUS CIRCUITS

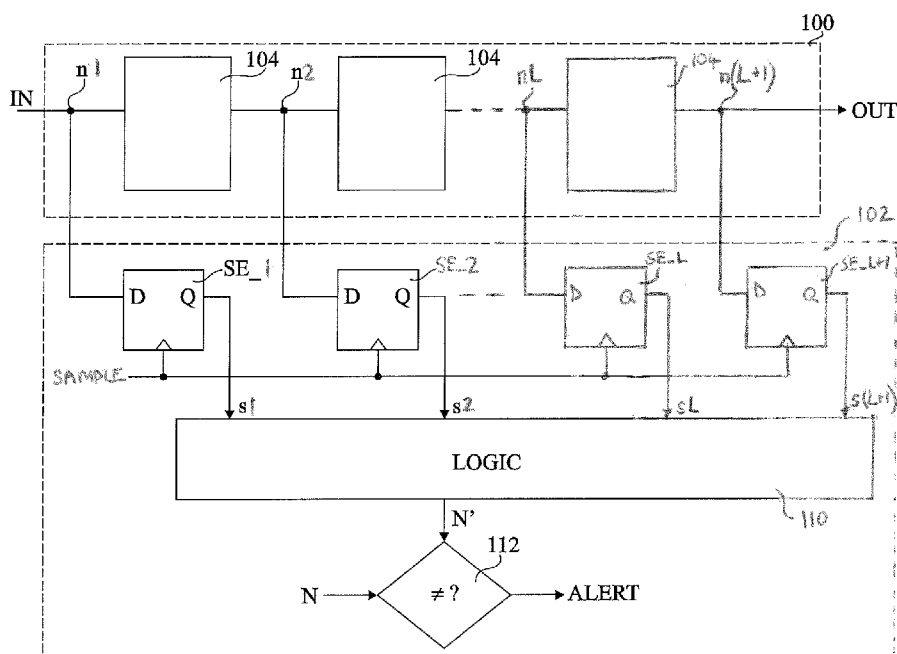


Fig 1

(57) Abstract: The present disclosure relates to a fault detection circuit comprising: sampling elements (SE₁ to SE_L) configured to sample signals present at a plurality of nodes (n₁ to n_L) of an asynchronous circuit (100); a logic circuit (110) configured to determine a number of tokens (N') in the asynchronous circuit based on the sampled signals; and a comparator (112) configured to compare the determined number of tokens with a reference value (N), a fault being detected based on said comparison.

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))*

Description

CIRCUIT AND METHOD FOR PROTECTING ASYNCHRONOUS CIRCUITS

[0001] Field

[0002] The present disclosure relates generally to the field of asynchronous circuits, and in particular to a circuit and method for protecting such circuits from faults.

[0003] Background

[0004] Asynchronous circuits are circuits that are locally synchronized, rather than being globally synchronized by a global signal. Generally, asynchronous circuits such as asynchronous pipelines or the like involve a propagation of asynchronous edges representing data events and control events, the control events often being referred to as tokens.

[0005] The tokens and/or data in an asynchronous circuit may be corrupted by physical phenomena, such as radiation provoking single event upsets (SEU) and/or intentionally in order to inject faults by someone wishing to modify the circuit operations for fraudulent purposes.

[0006] The duplication of circuits in order to introduce redundancy provides one counter-measure against potential data/token corruption. However, such a counter-measure has significant cost in terms of chip area and power consumption.

[0007] Summary

[0008] The embodiments described herein aim to at least partially address one or more problems in the prior art.

[0009] According to one aspect, there is provided a fault detection circuit comprising: sampling elements configured to sample signals present at a plurality of nodes of an asynchronous circuit; a logic circuit configured to determine

a number of tokens in the asynchronous circuit based on the sampled signals; and a comparator configured to compare the determined number of tokens with a reference value, a fault being detected based on said comparison.

[0010] According to one embodiment, the asynchronous circuit consists of a plurality of stages, each stage being configured to process one token at a time, a corresponding one of the sampling elements being configured to sample the signal present at an output node of each stage of the asynchronous circuit.

[0011] According to one embodiment, one or more of said nodes is an output of a logic circuit having its inputs coupled to a pair of input control and/or data lines, or to a pair of output control and/or data lines, of one or more stages.

[0012] According to one embodiment, each sampling element comprises at least a memorizing element, such as a flip-flop, latch, C-element, etc., each memorizing element having a data input coupled to a corresponding one of the plurality of nodes of the asynchronous circuit.

[0013] According to one embodiment, the logic circuit comprises a plurality of logic gates configured to detect differences in the logic states between adjacent ones of the plurality of nodes.

[0014] According to one embodiment, the asynchronous circuit forms a closed loop.

[0015] According to a further aspect, there is provided a true random number generator comprising: a self-timed ring implemented by a closed loop asynchronous circuit; and the above fault detection circuit.

[0016] According to a further aspect, there is provided a secure asynchronous circuit comprising: an open-loop asynchronous circuit; an input circuit configured to detect

tokens entering the asynchronous circuit; an output circuit configured to detect tokens exiting the asynchronous circuit; and the above fault detection circuit.

[0017] According to one embodiment, the secure asynchronous circuit further comprises a reference value generation circuit for generating the reference value based on the number of tokens detected by the input and output circuits.

[0018] According to one embodiment, the reference value generation circuit is an up/down counter configured to increment a count value when a token entering the asynchronous circuit is detected and to decrement the count value when a token exiting the asynchronous circuit is detected.

[0019] According to a further aspect, there is provided a method of protecting an asynchronous circuit from faults, the method comprising: sampling signals present at a plurality of nodes of the asynchronous circuit; determining, by a logic circuit, a number of tokens in the asynchronous circuit based on the sampled signals; and comparing the determined number of tokens with a reference value, a fault being detected based on said comparison.

[0020] Brief disclosure of the drawings

[0021] The foregoing features and advantages, as well as others, will be described in detail in the following description of specific embodiments given by way of illustration and not limitation with reference to the accompanying drawings, in which:

[0022] [Fig. 1] Figure 1 schematically illustrates an asynchronous circuit and a fault detection circuit according to an example embodiment of the present disclosure;

[0023] [Fig. 2A] Figure 2A schematically illustrates an asynchronous half-buffer according to an example embodiment;

[0024] [Fig. 2B] Figure 2B represents 4-phase encoding according to an example embodiment;

[0025] [Fig. 2C] Figure 2C represents 2-phase encoding according to an example embodiment;

[0026] [Fig. 3] Figure 3 schematically illustrates a logic circuit of Figure 1 in more detail according to an example embodiment;

[0027] [Fig. 4] Figure 4 schematically illustrates a self-timed ring based true random number generator according to an example embodiment of the present disclosure;

[0028] [Fig. 5] Figure 5 is a graph representing operation of the circuit of Figure 4 according to example embodiment;

[0029] [Fig. 6] Figure 6 schematically illustrates an open-loop asynchronous circuit and a fault detection circuit according to a further example embodiment of the present disclosure; and

[0030] [Fig. 7] Figure 7 is a flow diagram representing operations in a method of fault detection in an asynchronous circuit according to an example embodiment of the present disclosure.

[0031] Detailed disclosure

[0032] Like features have been designated by like references in the various figures. In particular, the structural and/or functional features that are common among the various embodiments may have the same references and may dispose identical structural, dimensional and material properties.

[0033] Unless indicated otherwise, when reference is made to two elements connected together, this signifies a direct connection without any intermediate elements other than conductors, and when reference is made to two elements linked or coupled together, this signifies that these two elements

can be connected or they can be linked or coupled via one or more other elements.

[0034] Throughout the present disclosure, the following terms are assumed to have the following definitions:

[0035] asynchronous circuit - a circuit in which the timing of events is not linked to a common clock signal;

[0036] token - a state transition of a data signal or control signal that propagates through an asynchronous circuit; and

[0037] stage - an asynchronous circuit block that can contain one token at a time.

[0038] Figure 1 schematically illustrates an asynchronous circuit 100 and a fault detection circuit 102 according to an example embodiment of the present disclosure.

[0039] The asynchronous circuit for example comprises stages 104 coupled in series, each stage processing one token at the time. In particular, as known by those skilled in the art, the propagation of control and data signals in asynchronous circuits may involve a handshake protocol in which each stage cannot accept a new data or control event until a current data event has been processed and sent to a subsequent stage. In some cases, a stage waits for an acknowledgement signal from the subsequent stage before accepting a new data event by asserting its own acknowledgement signal. In other cases, it may be possible for a stage to accept new data before it has received the acknowledgement signal from the subsequent stage.

[0040] While in the example of Figure 1 the stages of the asynchronous circuit 100 are coupled in series, it will be apparent to those skilled in the art that one or more stages could alternatively or additionally be coupled in parallel with each other, for example using non-linear asynchronous components such as fork and join.

[0041] Input, output and intermediate nodes n_1 to $n_{(L+1)}$ at the inputs and outputs of each of the stages 104 of the asynchronous circuit 100 are for example coupled to the fault detection circuit 102. The number $L+1$ of nodes will depend on the number of stages L in the asynchronous circuit. In the example of Figure 1, both the input and output of the asynchronous circuit are treated as nodes coupled to the fault detection circuit 102. In alternative embodiments, for example in the case of a closed-loop asynchronous circuit discussed in more detail below, only one of the input and output is for example treated as such a node, and thus there are L nodes rather than $L+1$.

[0042] The fault detection circuit 102 for example comprise a sampling circuit for sampling the signals at the nodes n_1 to $n_{(L+1)}$. In the example of Figure 1, this sampling circuit is formed of sampling elements SE_1 to SE_{L+1} each implemented by a flip-flop. Each node n_1 to $n_{(L+1)}$ of the asynchronous circuit 100 is for example associated with a dedicated flip-flop. In alternative embodiments, a different type of sampling circuit could be used, such as latches or a sample and hold circuit based on a capacitance.

[0043] The flip-flops SE_1 to SE_{L+1} are for example D-type flip-flops, and capture the node tokens based on a common sampling signal $SAMPLE$. In some embodiments, this sampling signal $SAMPLE$ is provided by an external unit or by one or more of the nodes n_1 to $n_{(L+1)}$ of the asynchronous circuit. The sampling signal $SAMPLE$ could also be generated by a combination of the signals at a plurality of the nodes n_1 to $n_{(L+1)}$, the signals for example being combined by an XOR tree.

[0044] The flip-flops SE_1 to SE_{L+1} have their data inputs D coupled to the corresponding nodes n_1 to $n_{(L+1)}$, and their data outputs Q , which respectively provide samples s_1 to $s_{(L+1)}$, coupled to a logic circuit (LOGIC) 110. The circuit

110 for example generates a number N' representing the number of tokens present in the asynchronous circuit 100 based on the signals sampled by the sampling circuit. The number N' is compared by a comparator 112 to a reference value N . In the case that these values do not match, this for example is interpreted as an indication of a fault injected, or otherwise occurring, in the asynchronous circuit 100. Indeed, a fault will cause a state transition at a node of the asynchronous circuit, and will thus either add a token, or remove a token, from the circuit. An alert signal ALERT is for example generated upon every fault detection, in other words whenever N' is not equal to N . Alternatively or additionally, an ALERT signal could be generated when the difference between N' and N is greater than a threshold, the threshold for example being set at 2 or a higher value.

[0045] The nodes n_1 to $n_{(L+1)}$ of the asynchronous circuit may correspond directly to nodes on the lines between the stages, or may involve a logic function applied to more than one of the lines (in some implementation/protocol, internal point can also be used and combined with the inputs/outputs of the stage), as will now be described in more detail with reference to Figures 2A to 2C. Indeed, the nodes are for example selected or generated such that the signals at these nodes transition at each new token.

[0046] Figure 2A schematically illustrates a half-buffer 200 formed of a pair of C-elements 202, 204. Such a half-buffer for example forms part of each stage of the asynchronous circuit 100 of Figure 1, and controls the progression of data through the circuit.

[0047] The C-element 202 has one of its inputs coupled to a data input line 206 receiving an input data signal $I.0$, and its other input coupled to a data input line 208 receiving a data input signal $I.1$. The other inputs of the C-elements 202

and 204 are coupled to an acknowledgement line 210 receiving an acknowledgement signal O_ack. The outputs of the C-elements 202, 204 are coupled to output data lines 212 and 214 respectively, the line 212 providing an output data signal O.0, and the line 214 providing an output data signal O.1. The lines 212 and 214 are also coupled to respective inputs of a two-input NOR gate 216, which provides at its output an acknowledgement signal I_ack on an acknowledgement line 218.

[0048] Each C-element 202, 204 for example has an operation defined by the following truth table, where the input signals are referenced A and B, and the output signal is referenced Z:

[0049] [Tableaux 1]

A	B	Z
0	0	0
0	1	Z-1
1	0	Z-1
1	1	1

[0050] In other words, when the values of the input signals A and B are at the same logic level, the output signal Z is set to this logic level. When the values of the input signals A and B are at different logic levels from each other, the circuit is in a standby state in which the output signal Z remains unchanged.

[0051] Referring again to Figure 2A, a data bit is transmitted on the input data lines 206, 208 and on the output data lines 212, 214 using a 4-phase protocol according to which:

- logic states "01" on the lines I.0 and I.1 respectively or on the lines O.0 and O.1 respectively for example transmits a logical "1" bit;

- logic states "10" on the lines I.0 and I.1 respectively or on the lines O.0 and O.1 respectively for example transmits a logical "0" bit;

- logic states "00" on the lines I.0 and I.1 or on the lines O.0 and O.1 for example indicates an idle state in which no data is transmitted; and

- logic states "11" on the lines I.0 and I.1 or on the lines O.0 and O.1 is for example a forbidden state.

[0052] The nodes of the stage 200 that form part of the nodes n_1 to $n(L+1)$ may correspond to the data input lines 206 and 208 combined by an OR gate (not illustrated in Figure 2A), and to the data output lines 212 and 214 combined by an OR gate (also not illustrated in Figure 2A), or to the acknowledgement input and output lines 210, 218 directly.

[0053] In other embodiments, different protocols can be implemented for transmitting data events on two data lines, as will now be described with reference to Figures 2B and 2C.

[0054] Figure 2B represents the 4-phase encoding implemented in Figure 2A, in which, in an idle state, both data lines are at a low state, and one or the other data line is brought to a high state to transmit either a "0" or a "1" bit. Two high states is a forbidden state. If a stage i is based on this protocol, the input node n_i for example corresponds to a logic OR applied to the data input lines, and the output node $n(i+1)$ of the stage for example corresponds to a logic OR applied to the data output lines.

[0055] Figure 2C represents 2-phase encoding in which a "0" bit is transmitted by maintaining a first of the data lines at a low state, and toggling the second data line between

high and low states on each data event. A "1" bit is transmitted by maintaining the first data line at a high state, and toggling the second data line between high and low states on each data event. If a stage I is based on this protocol, the input node n_i for example corresponds to a logic XOR applied to the data input lines, and the output node $n(i+1)$ of the stage for example corresponds to a logic XOR applied to the data output lines.

[0056] Figure 3 schematically illustrates the logic circuit 110 according to an example embodiment. In the example of Figure 3, the samples s_1 to $s(L+1)$ generated by the sampling elements SE_1 to SE_{L+1} are provided in pairs to $L+1$ XOR gates 302. In particular, each i th XOR gate, for i from 1 to $L+1$, performs the exclusive OR operation on the samples $s(i-1)$ and s_i . Thus the XOR gates 302 detect the presence of transitions, i.e. tokens, between on the $(i-1)$ th sample and the i th sample. The outputs of the XOR gates 302 are coupled to a hash code generation circuit (HASH CODE GEN) 304, which for example generates a fixed length code N' representing the number of detected tokens. In some embodiments, the hash code is a Hamming weight, although other algorithms could be applied.

[0057] Rather than using XOR gates 302 to detect tokens held in each stage, other logic functions could be used, depending on the protocol. For example, in the case of the 4-phase protocol, an AND gate with one inverted input could be used, as will be understood by those skilled in the art.

[0058] Figure 4 schematically illustrates a self-timed ring (STR) based true random number generator (STRNG) 400 according to an example embodiment of the present disclosure. Such a circuit is for example described in more detail in the French patent published as FR 2 986 679, and in the publication entitled "Self-timed Ring based True Random Number Generator: threat model and countermeasures", G. Gimenez et al., 2017

IEEE 2nd International Verification and Security Workshop (IVSW), the contents of these documents being hereby incorporated by reference to the extent permitted by the law.

[0059] The generator 400 for example comprises a self-timed ring 402 formed by an asynchronous circuit comprising stages S1 to SL. As represented for the first stage S1 of the ring, each *i*th stage, for *i* from 1 to L, is for example implemented by a C-element having an input Fi, an inverted input Ri and an output Ci. Furthermore, each *i*th stage Si for example has its output coupled to the input F(*i*+1) of the stage S(*i*+1) and to the inverted input R(*i*-1) of the stage S(*i*-1), where the stage S(*i*-1) for the first stage S1 is the stage SL, and the stage S(*i*+1) for the Lth stage is the stage S1. The number L of stages is for example equal to an integer equal to or greater than 3.

[0060] Random values are extracted from the self-timed ring by an entropy extractor 404. The circuit 404 is configured to sample the outputs C1 to CL of the stages S1 to SL using respective sampling elements SE_0' to SE_L'. The sampling elements SE_0' to SE_L' each for example correspond to a flip-flop clocked by a sampling signal SAMPLE', which for example indicates each time a random value is to be extracted. The sampled signals at the outputs of the sampling elements SE_1' to SE_L' are combined, for example using an XOR tree 406, to generate a random output signal OUTPUT for example corresponding to a single bit stream.

[0061] Figure 5 is a graph representing an example of the operation of the circuit of Figure 4, based on events at nodes C(*j*-1), Cj and Cj+1 re-indexed to correspond to three consecutive events around a significant edge of the sampling signal SAMPLE'. Shaded regions in Figure 5 around the edge of the signal SAMPLE' and around each event represent the range of jitter variations, which have a normal distribution. Thus,

when the jitter variations are larger than the mean phase difference $\Delta\phi$ between consecutive events, the signal C_j is sampled in its uncertainty zone, implying the generation of a random value.

[0062] The fault detection circuit 102 of Figure 1 can be used in conjunction with the embodiment of Figure 4, for example by treating the inputs F_1 to F_L as the nodes n_1 to n_L of the asynchronous circuit to be sampled by the fault detection circuit 102. In some cases, the sampling elements SE_1 to SE_L of the fault detection circuit 102 and the sampling elements SE_1' to SE_L' of the entropy extractor 404 could be implemented by a same set of flip-flops or latches, and thus the number tokens can for example be verified upon each random value extraction.

[0063] Thus Figures 4 and 5 correspond to a case of a closed-loop system in which the number of tokens circulating in the loop is initially defined and then remains fixed during operation. In the case of the self-timed ring of Figure 4, the number of tokens is for example chosen in order to respect a certain minimum occupancy, as described in more detail in the above-referenced publication by G. Gimenez et al. Thus the reference number N is for example fixed. Furthermore, it should be noted that the correct behavior of the generator of Figure 4 is dependent on the number of tokens circulating in the self-timed ring. Thanks to the fault detection circuit described herein, the number of tokens can for example be verified at regular intervals.

[0064] In the case of open-loop asynchronous circuits, the number of tokens in the asynchronous circuit at a given time may vary based on the number of tokens entering and exiting the circuit.

[0065] Figure 6 schematically illustrates a secure asynchronous circuit 600 comprising the asynchronous circuit

100, which in this example is an open-loop circuit, and the fault detection circuit 102, according to a further example embodiment of the present disclosure.

[0066] In the embodiment of Figure 6, an input circuit (IN DETECT) 602 is provided for detecting the number of tokens entering the asynchronous circuit 100. Furthermore, an output circuit (OUT DETECT) 604 is provided for detecting the number of tokens exiting the asynchronous circuit 100. With respect to the detection circuit 102 of Figure 1, the detection circuit 102 of Figure 6 additionally comprises circuitry for determining the reference value N based on the tokens entering and exiting the asynchronous circuit. For example, this circuitry comprises an up/down counter (UP/DN COUNTER) 606, which increments a count value each time a token is detected by the circuit 602 as entering the asynchronous circuit 100, and which decrements the count value each time a token is detected by the circuit 604 as exiting the asynchronous circuit 100.

[0067] As shown in example of Figure 6, this count value may directly provide the reference value N representing the number of tokens in the asynchronous circuit 100, if for example the number of tokens in this circuit 100 is initially zero. Alternatively, the value of N could be calculated differently, for example as the sum of the initial value of N' detected in the circuit 100 and the count value generated by the up/down counter 606. Of course, the values of N' and N may additionally be condensed by a hash algorithm or the like, as described above in relation with Figure 1.

[0068] In some embodiments, the output count value generated by the up/down counter 606 is sampled by a flip-flop 608 based on the same signal SAMPLE used to sample the nodes of the asynchronous circuit 100.

[0069] Figure 7 is a flow diagram representing operations in a method of fault detection in an asynchronous circuit according to an example embodiment of the present disclosure.

[0070] In an operation 701, the number of tokens N' in an asynchronous circuit is determined. As described above with reference to Figures 1 and 3, this is for example achieved by sampling the signal at a node between each stage of the asynchronous circuit. In some embodiments, tokens are then detected using XOR gates or other logic gates to compare the signals at adjacent nodes in order to detect transitions that occur between the nodes.

[0071] Depending on the type of asynchronous circuit, operations 702 and 703 may be implemented in parallel with operation 701. Operations 702 and 703 respectively involve monitoring the number of tokens entering and exiting the asynchronous circuit. As described in relation with Figure 6 above, these operations are for example performed when the asynchronous circuit is not a closed loop, but rather an open loop in which the rate that tokens enter the circuit may vary with respect to the rate that tokens exit the circuit, leading to a natural variation in the number of tokens in the circuit.

[0072] Following operation 701, the determined number of tokens N' is compared with a reference value N . In a closed-loop circuit, this reference value N may be fixed. In an open-loop circuit, this reference value N may be based on the number of input and output tokens determined in operations 702 and 703. In either case, the values N' and N could be binary values directly equal to the number of tokens, or they could be condensed values, for example generated using a hash algorithm.

[0073] In an operation 705, it is determined whether N' is equal to N . If so, the method for example returns to operation 701, and is repeated at a next significant edge of the

sampling signal SAMPLE. Alternatively, if the values N' and N do not match, an alert can for example be generated in an operation 706 before the method returns to operation 701. It will be apparent to those skilled in the art that the comparison performed by the comparator 112 could be implemented by a logic circuit, or by software code executed by a computer processor.

[0074] An advantage of the embodiments described herein is that an asynchronous circuit can be protected from faults caused by fault injection, SEUs, etc., in a simple and effective manner. Furthermore, an advantage of the embodiment of Figure 6 is that it permits the method to be applied to open-loop circuits in which the number of tokens expected in the circuit varies.

[0075] Various embodiments and variants have been described. Those skilled in the art will understand that certain features of these embodiments can be combined and other variants will readily occur to those skilled in the art. In particular, while in the example embodiments each stage of the asynchronous circuit comprises a half-buffer, in alternative embodiments other types of buffering circuits could be used. In addition, the logic circuit 110 may comprise XOR gates as represented in Figure 3, or could be implemented using different types of logic circuitry. The implementation of the logic circuit 110 will depend on the class of asynchronous circuit and the particular protocols that are employed.

[0076] Furthermore, in some embodiments, the asynchronous circuit 100 could be split into two or more sub-circuits, each of which can be monitored independently by the fault detection circuit described herein. One or more of these sub-circuits could also not be monitored at all.

Claims

1. A fault detection circuit comprising:

sampling elements (SE₁ to SE_{L+1}) configured to sample signals present at a plurality of nodes (n₁ to n_L) of an asynchronous circuit (100);

a logic circuit (110) configured to determine a number of tokens (N') in the asynchronous circuit based on the sampled signals; and

a comparator (112) configured to compare the determined number of tokens with a reference value (N), a fault being detected based on said comparison.

2. The fault detection circuit of claim 1, wherein the asynchronous circuit (100) consists of a plurality of stages (104), each stage being configured to process one token at a time, a corresponding one of the sampling elements being configured to sample the signal present at an output node of each stage of the asynchronous circuit.

3. The fault detection circuit of claim 2, wherein one or more of said nodes is an output of a logic circuit having its inputs coupled to a pair of input control and/or data lines, or to a pair of output control and/or data lines, of one or more stages.

4. The fault detection circuit of any of claims 1 to 3, wherein each sampling element (SE₁ to SE_L) comprises a memorizing element, such as a flip-flop, latch or C-element, each memorizing element having a data input coupled to a corresponding one of the plurality of nodes of the asynchronous circuit.

5. The fault detection circuit of any of claims 1 to 4, wherein the logic circuit (110) comprises a plurality of logic

gates (302) configured to detect differences in the logic states between adjacent ones of the plurality of nodes (n1 to nL).

6. The fault detection circuit of any of claims 1 to 5, wherein the asynchronous circuit forms a closed loop.

7. A true random number generator comprising:

a self-timed ring implemented by a closed loop asynchronous circuit; and

the fault detection circuit of claim 6.

8. A secure asynchronous circuit (600) comprising:

an open-loop asynchronous circuit (100);

an input circuit (602) configured to detect tokens entering the asynchronous circuit (100);

an output circuit (604) configured to detect tokens exiting the asynchronous circuit (100); and

the fault detection circuit of any of claims 1 to 4.

9. The secure asynchronous circuit of claim 8, further comprising a reference value generation circuit for generating the reference value (N) based on the number of tokens detected by the input and output circuits (602, 604).

10. The secure asynchronous circuit of claim 9, wherein the reference value generation circuit is an up/down counter (606) configured to increment a count value when a token entering the asynchronous circuit is detected and to decrement the count value when a token exiting the asynchronous circuit is detected.

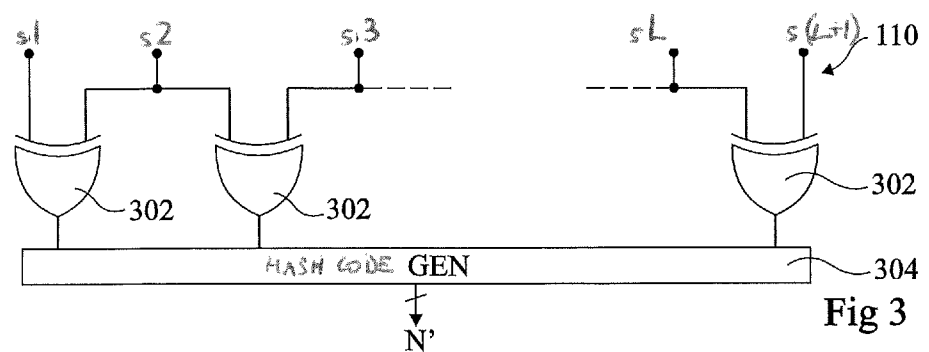
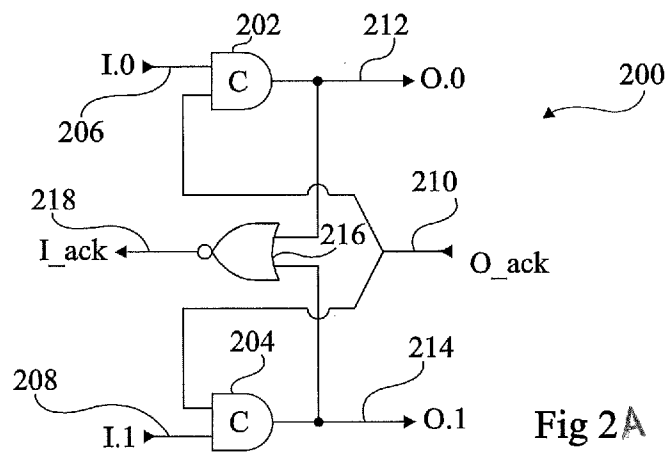
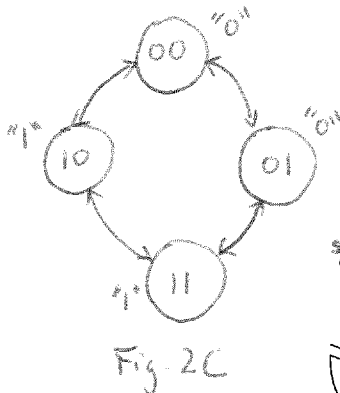
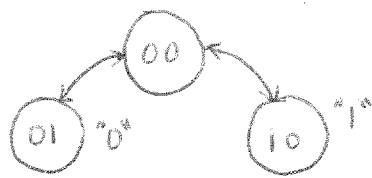
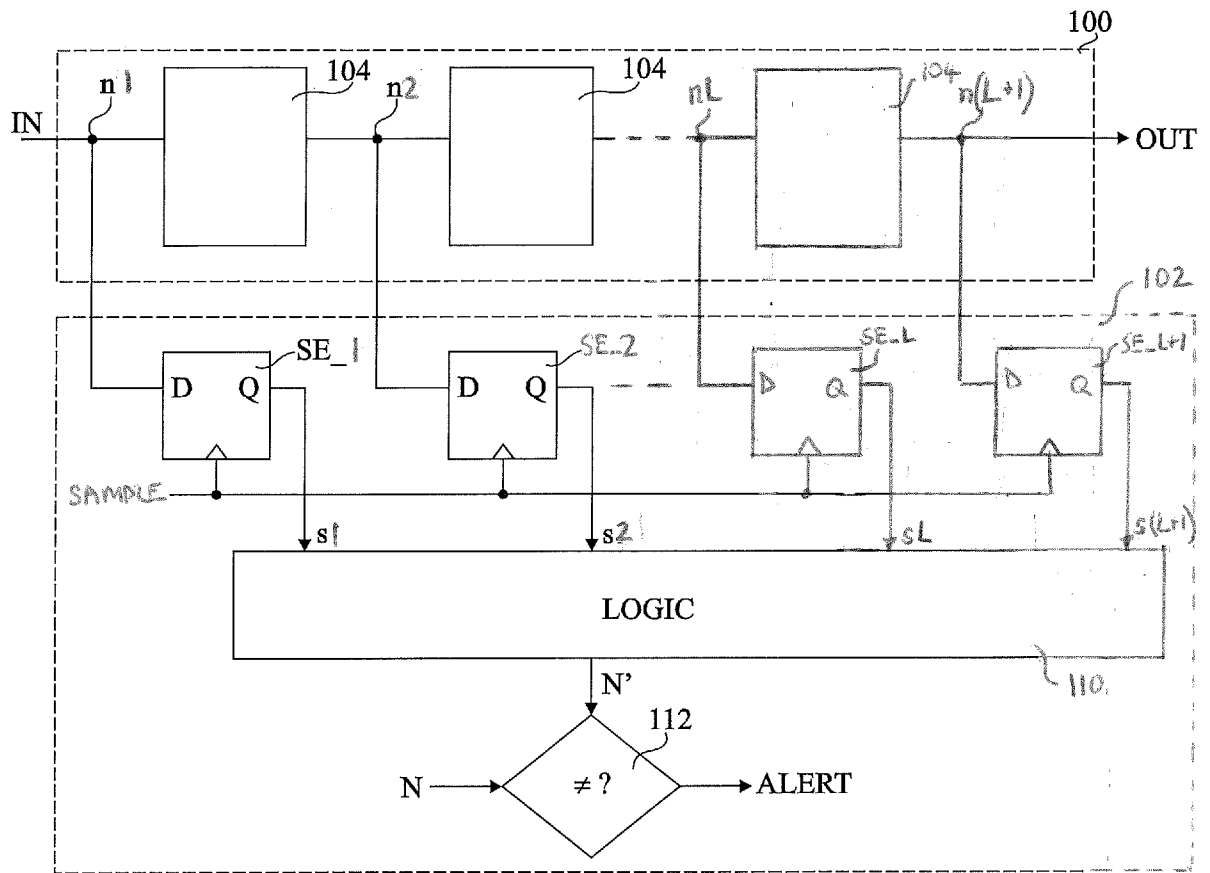
11. A method of protecting an asynchronous circuit from faults, the method comprising:

sampling signals present at a plurality of nodes (n1 to nL) of the asynchronous circuit (100);

determining, by a logic circuit (110), a number of tokens (N') in the asynchronous circuit based on the sampled signals; and

comparing the determined number of tokens with a reference value (N), a fault being detected based on said comparison.

⋮



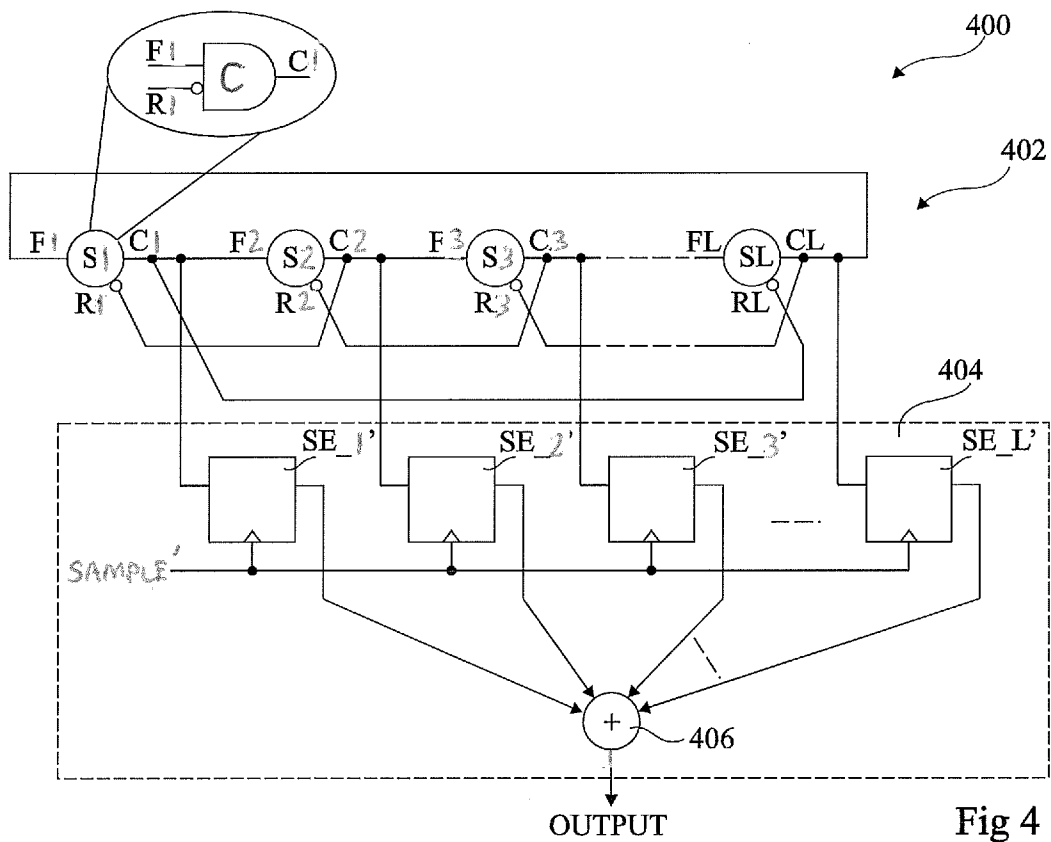


Fig 4

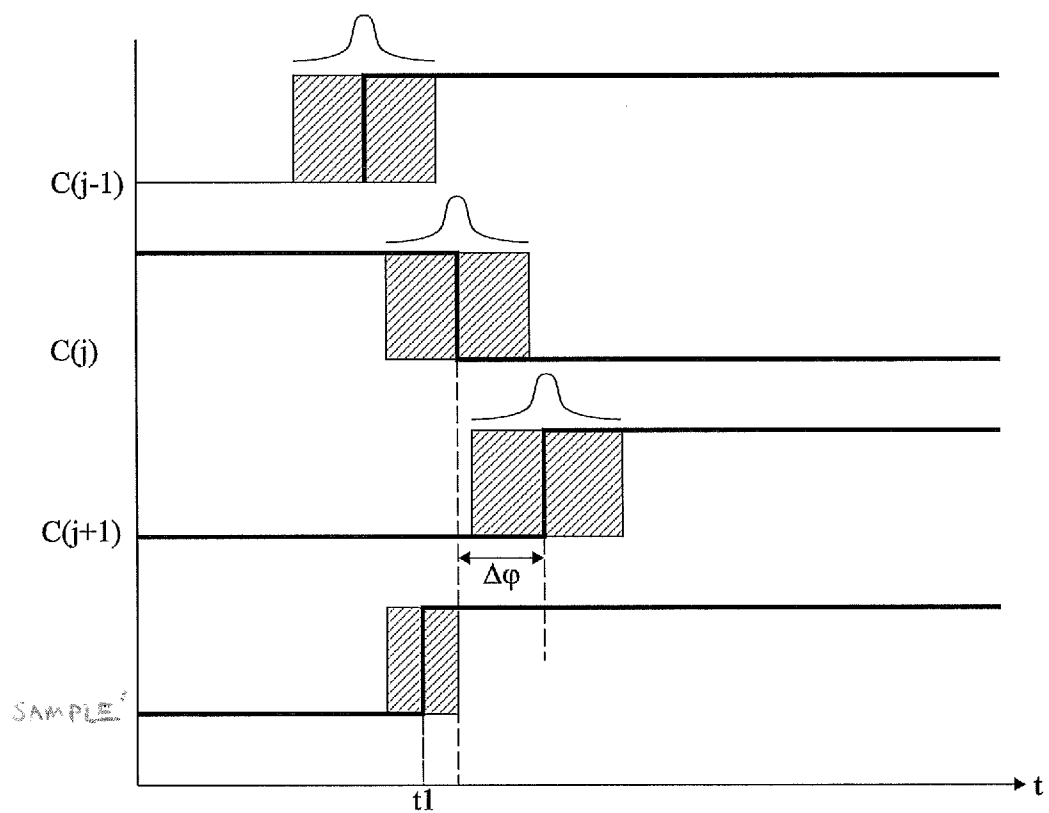


Fig 5

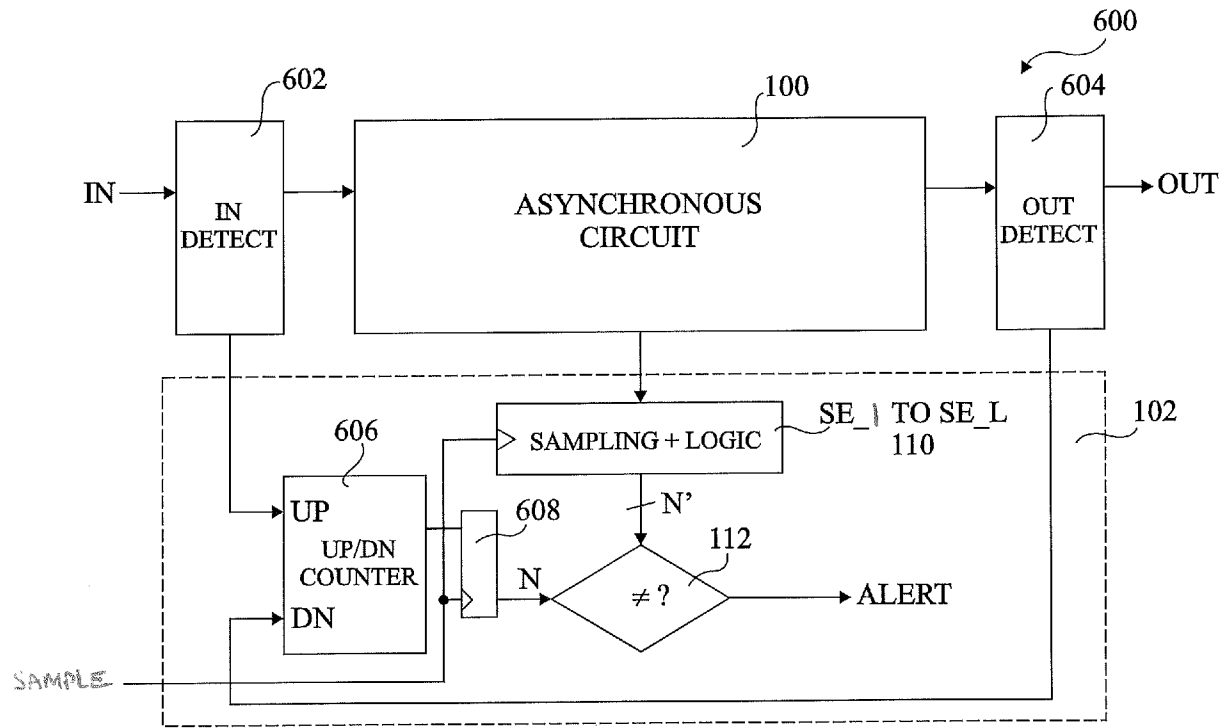


Fig 6

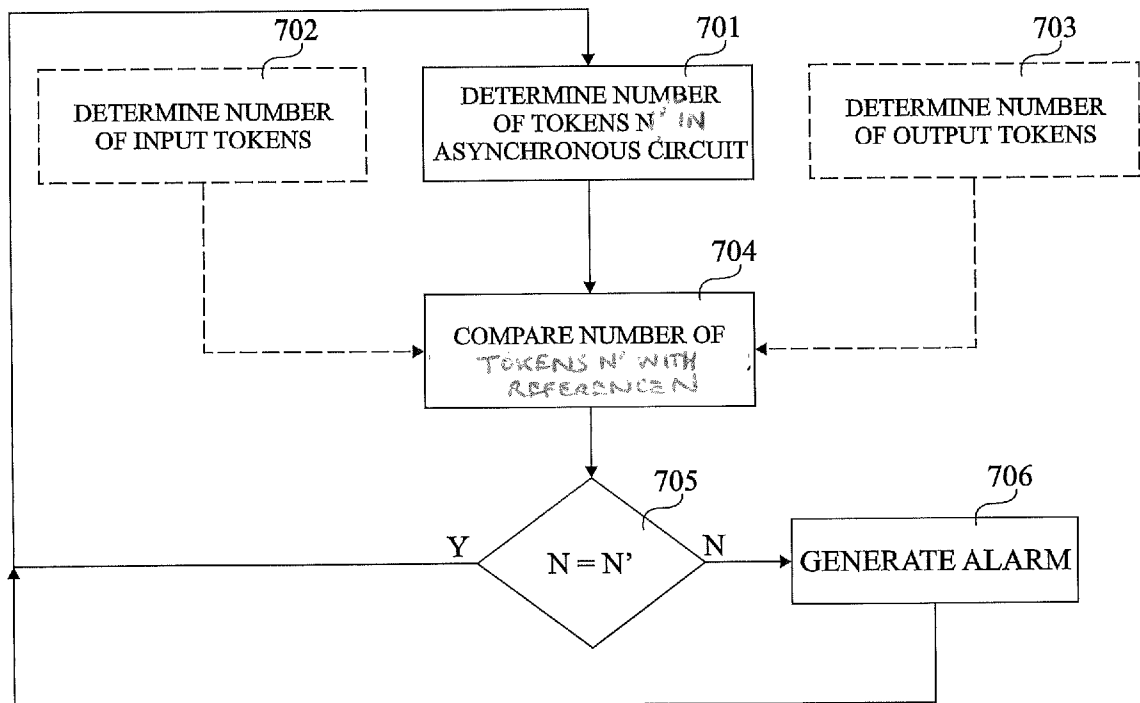


Fig 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2018/001147

A. CLASSIFICATION OF SUBJECT MATTER
INV. H03K19/003 H03K23/00
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)
H03K G06F

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)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 900 078 B1 (MANOHAR RAJIT [US] ET AL) 1 March 2011 (2011-03-01)	1-6,11
Y	column 2, line 12 - column 15, line 5; figures 1-10	7-10

X	WO 03/069485 A2 (FULCRUM MICROSYSTEMS INC [US]) 21 August 2003 (2003-08-21)	1-6,11
A	page 12, line 24 - page 31, line 21; figures 1-12	7-10

Y	FR 2 986 679 A1 (INST POLYTECHNIQUE GRENOBLE [FR]; CENTRE NAT RECH SCIENT [FR]; UNIV JE) 9 August 2013 (2013-08-09)	7-10
	cited in the application	
A	page 2, line 13 - page 23, line 19; figures 1-6	1-6,11



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

22 March 2019

Date of mailing of the international search report

01/04/2019

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

Kassner, Holger

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2018/001147

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 7900078	B1	01-03-2011	US 7900078 B1	01-03-2011
			US 2011130171 A1	02-06-2011

WO 03069485	A2	21-08-2003	AT 401607 T	15-08-2008
			AU 2003215211 A1	04-09-2003
			EP 1474748 A2	10-11-2004
			JP 4520742 B2	11-08-2010
			JP 2005518018 A	16-06-2005
			US 2003159078 A1	21-08-2003
			US 2003165158 A1	04-09-2003
			WO 03069485 A2	21-08-2003

FR 2986679	A1	09-08-2013	NONE	
