

(51) International Patent Classification:
G06F 21/75 (2013.01)(21) International Application Number:
PCT/EP2022/063277(22) International Filing Date:
17 May 2022 (17.05.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2107032.1 17 May 2021 (17.05.2021) GB(71) Applicant: **NORDIC SEMICONDUCTOR ASA**
[NO/NO]; Otto Nielsens veg 12, 7052 Trondheim (NO).(72) Inventor: **PEDERSEN, Frode**; c/o Nordic Semiconductor
ASA, Otto Nielsens veg 12, 7052 Trondheim (NO).(74) Agent: **DEHNS**; St Bride's House, 10 Salisbury Square,
London, Greater London EC4Y 8JD (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, IQ, IR, IS, IT, JM, 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, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM,
ZW.

(54) Title: PROTECTION OF INTEGRATED CIRCUIT DEVICES

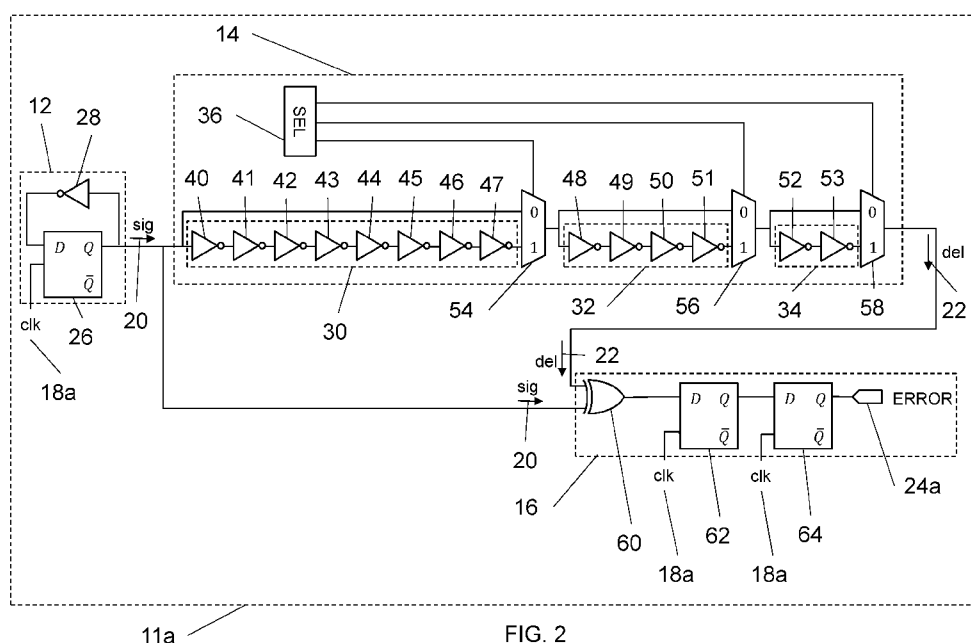


FIG. 2

(57) **Abstract:** An integrated circuit (2) comprises a circuit portion (6a) for detecting a low logic speed relative to a clock signal frequency. The circuit portion (6a) comprises an oscillator (10a) arranged to output a periodic clock signal (18a) and a detection circuit portion (11a) comprising a latch circuit portion (12), a delay circuit portion (14) and a comparison circuit portion (16). The latch circuit portion (12) outputs a first signal (20) that changes state once per clock cycle. The delay circuit portion (14) receives the first signal (20) and outputs a second signal (22) subject to a propagation delay compared to the first signal (20), the propagation delay being less than a period of the clock signal (18a) under normal operating conditions. The comparison circuit portion (16) compares the first signal (20) at the input and the second signal (22) at the output of the delay circuit portion (14) and outputs an error signal (24a) if the signals are indicative of low logic speed relative to the clock signal frequency.

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

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))*
-

Protection of integrated circuit devices

5 This invention relates to integrated circuits (ICs) and more particularly to the provision of measures which may help protect against unauthorised access to certain parts of such devices.

10 As ICs have become more complex and powerful, an increasing amount of attention has been paid to the risks posed by unauthorised access to certain parts – e.g. those which contain sensitive data or software or which can be used to exercise unauthorised control of a device incorporating the IC. Manufacturers therefore now routinely employ measures to discourage or prevent such access by hackers.

15 In recent years, hackers have started employing a type of physical attack on integrated circuits known as a glitch attack. A glitch attack involves forcing an integrated circuit to operate at a low logic speed relative to its internal clock frequency, either by applying a short duration pulse in order to rapidly drop supply
20 voltage or by increasing the clock frequency. In doing this, it becomes possible that logic signals will not reach an intended destination within an integrated circuit before a clock cycle is completed, thus allowing branches of code to be skipped – e.g. skipping part of an ‘if’ block to jump to an outcome.

25 The Applicant has recognised that glitch attacks pose a security threat to integrated circuits, and thus defence measures are desirable. Known defence designs utilise analogue devices to monitor the supply voltage directly in order to detect drops in supply voltage indicative of glitch attacks, or to monitor temperature in order to detect illegal temperature conditions indicative of glitch attacks. Alternatively, other
30 known defence designs utilise analogue devices to monitor the clock frequency directly in order to detect frequency spikes indicative of glitch attacks. The Applicant has recognised some shortcomings with known, analogue defence designs, namely that in order to detect very short duration low voltage pulses, like those used in glitch attacks, they require a lot of power. Additionally, traditional

- 2 -

designs can be expensive to produce and need to be tailored specifically to the integrated circuits they are designed to protect.

The present invention aims at least partly to address the issues set out above and when viewed from a first aspect the invention provides an integrated circuit comprising a circuit portion for detecting a low logic speed relative to a clock signal frequency, the circuit portion comprising:

an oscillator arranged to output a periodic clock signal; and
a detection circuit portion comprising:

a latch circuit portion arranged to output a first signal that changes state once per clock cycle;

a delay circuit portion arranged to receive said first signal and output a second signal subject to a propagation delay compared to the first signal, said propagation delay being less than a period of the clock signal under normal operating conditions; and

a comparison circuit portion arranged to compare the first signal at the input and the second signal at the output of the delay circuit portion and output an error signal if the signals are indicative of low logic speed relative to the clock signal frequency.

Thus it will be seen by those skilled in the art that as the signal output by the latch circuit portion changes state once per clock signal, the present invention provides the ability to compare the propagation delay introduced by the delay circuit portion to the period of the clock signal. If the first and second signals are in the same state at the inputs of the comparison circuit portion, this means that sufficient time has passed since the most recent state switch of the first signal for the first signal to propagate through the delay circuit portion and then arrive (in the form of the second, delayed signal) at the comparison circuit portion before the state changes again. If the first and second signals are in different states at the inputs of the comparison circuit portion, this means that not enough time has passed since the most recent state switch of the first signal for the first signal to propagate through the delay circuit portion and then arrive (in the form of the second, delayed signal) at the comparison circuit portion.

- 3 -

Under normal operating conditions, the propagation delay introduced by the delay circuit portion is smaller than the period of the clock signal, and thus the comparison circuit portion does not output an error signal. When a glitch attack occurs, however, the propagation delay introduced by the delay circuit portion may increase, or the period of the clock signal may decrease, such that this is no longer the case, and thus the comparison circuit portion outputs an error signal to indicate this. This can arise for one of two reasons, namely that the supply voltage has decreased or the clock frequency has increased, both of which are methods used in glitch attacks. Low supply voltage diminishes the ability for logic elements in a circuit to draw power in order to drive an input voltage to a desired output voltage, thus lowering logic speed. In accordance with the invention, the lower logic speed affects the propagation delay introduced by the delay circuit portion, thus potentially triggering the error signal.

Whilst high clock frequency does not affect logic speed directly, glitch attacks rely on low logic speed when compared to clock frequency, so the same effect occurs – signals are prevented from reaching their intended destination within a single (decreased length) clock cycle.

Thus it will be understood by those skilled in the art that the present invention provides a circuit portion which may detect glitch attacks, or simply low logic speed relative to clock signal frequency. Advantageously, the circuit portion may be able to detect even short glitch attacks – e.g. those lasting only a single clock cycle. The integrated circuit (IC) may be able to detect the presence of a glitch attack before problems occur in the logic circuitry of the rest of the IC, and respond appropriately. The IC may, for example, cease or pause operation in response to the error signal as output by the detection circuit portion in order to protect from a glitch attack. The IC could also, by way of example, respond to the error signal by lowering the clock frequency (should that functionality be available) in order to allow more time for signals to propagate through logic circuitry between clock cycles.

The propagation delay could be any value less than the normal clock period but in a set of embodiments, the propagation delay introduced by the delay circuit portion is arranged to be greater than or equal to an inherent propagation delay introduced by a critical path of a logic circuit portion elsewhere in the IC, but preferably in the

- 4 -

same clock domain, under normal operating conditions. As used herein, the term “clock domain” is used to refer to a portion of circuitry that operates at a specific clock frequency – i.e. a portion of circuitry that uses the clock signal output by the oscillator, and the term “critical path” is used to refer to the path along which a
5 signal may propagate in a logic circuit portion which introduces the largest propagation delay.

In a set of embodiments, the propagation delay introduced by the delay circuit portion is arranged to be equal to the inherent propagation delay introduced by the
10 critical path of the logic circuit plus an error margin, e.g. 1%, 5%, 10%, 20%, etc., under normal operating conditions. By arranging the delay circuit portion to introduce a propagation delay that is greater than that introduced by the critical path, embodiments of the present invention provide the ability to protect the clock domain from a glitch attack by detecting the glitch attack and outputting an error
15 signal before any logic circuitry of the protected clock domain is affected. In a set of embodiments, the integrated circuit comprises a plurality of clock domains. The integrated circuit may comprise a detection circuit portion for each clock domain.

In a set of embodiments, the comparison circuit portion is arranged to compare the
20 first and second signals once per clock cycle, at the same time as the latch circuit portion is arranged to switch the state of its output signal (which may in some embodiments be a rising edge of the clock signal).

In a set of embodiments, the delay circuit portion comprises one or more delay
25 elements. Each delay element may comprise one or more standard cells – e.g. inverters or NOT gates. Preferably, the delay element(s) or the cells thereof have similar scaling characteristics with respect to voltage as those elsewhere in the integrated circuit – e.g. in the critical path. This means that the effect of low supply voltage on the propagation delay of the delay circuit portion will be indicative of the
30 effect of low supply voltage on the critical path.

Preferably, the delay circuit portion comprises a plurality of delay elements. In a set of such embodiments, the delay elements can be employed or bypassed to provide a configurable propagation delay. Each of the delay elements may introduce a
35 unique propagation delay to the first signal. In a set of embodiments for example,

- 5 -

the propagation delay introduced one of the delay elements is a unit delay, and the delays introduced by the other delay elements comprise increasing power of two multiples of the unit delay. This enables the total delay introduced by the delay circuit portion to be programmed to be any multiple of the unit delay up to a maximum where all the delay elements are employed. This could be achieved for example using a select register coupled with multiplexers, wherein each bit of the select register determines whether or not the corresponding delay element is bypassed or not. This allows a binary programmable delay proportional to the value of the select register.

A programmable delay is advantageous as it allows the use of the same detection circuit design even if the design of the protected domain is voltage scaled, as different select register values may be used for different voltage operating points. It also allows the use of the same detection circuit design for different clock domains regardless of the delay introduced by the actual critical path in each domain and regardless of the clock frequency in each domain. Additionally, it allows the detection circuit to be easily calibrated to an individual clock domain over a range of operating conditions. However, the programmable delay is not an essential feature of the present invention, as the same detection functionality may be achieved using bespoke delay circuit portions designed for specific clock domains.

In a set of embodiments having a plurality of delay elements, each delay element is arranged to output a non-inverted signal at its output relative to its input, and thus the second signal output by the delay circuit portion is arranged to be non-inverted relative to the first signal at the input of the delay circuit portion regardless of how many of the delay elements are employed. In a set of embodiments, each delay element comprises an even number of inverters connected in series. Where the delay elements comprises successive power of two multiples of a unit delay, each delay element may comprise twice as many inverters as its succeeding element.

In a set of embodiments, the comparison circuit portion comprises an XOR gate, the output of which is coupled to a first flip-flop, wherein the XOR gate takes the first signal as one of its inputs and the second signal as the other of its inputs. The XOR gate is therefore arranged to output a signal whereby the state of the output signal is dependent on whether the first and second signals are in the same state or

- 6 -

in different states. The first flip-flop takes the output of the XOR gate as its input, and is arranged to output the error signal if the output of the XOR gate indicates that the first and second signals are in different states when it is clocked – e.g. on a rising clock edge.

5

In some embodiments, the comparison circuit portion further comprises a second flip-flop, with the output of the first flip-flop being coupled to the input of the second flip-flop. The second flip-flop may mirror the output of the first flip-flop with a delay of one clock cycle. The Applicant has recognised that it is possible for a signal output by the XOR gate to arrive at the first flip-flop at exactly the same time as a rising clock edge, resulting in the first flip-flop entering a meta-stable state that may cause the output of the first flip-flop to be undefined. The second flip-flop may therefore be arranged to stabilise the output of the first flip-flop by capturing undefined signals output by the first flip-flop, as the output of the second flip-flop may settle to a defined state even if the output of the first flip-flop is undefined. This may help reduce the frequency of false detections by the detection circuit portion, and may prevent undefined signals from the first flip-flop propagating to further logic.

20 An embodiment of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig. 1 is a schematic block diagram of an integrated circuit comprising one or more clock domains and one or more detection circuit portions in accordance with an embodiment of the present invention; and

Fig. 2 is a more detailed schematic circuit diagram of a detection circuit portion of the embodiment of Fig. 1.

30 Fig. 1 is a schematic block diagram of an integrated circuit 2, comprising a power supply 4 and three clock domains 6a-c. It will be understood by those skilled in the art that the number of clock domains is not limited to three, but may be any number. Each clock domain 6a-c comprises an oscillator 10a-c, a logic circuit portion 8a-c, and a detection circuit portion 11a-c. The oscillators 10a-c are coupled to the respective logic circuit portions 8a-c and detection circuit portions 11a-c. The logic

35

- 7 -

circuit portions 8a-c are also coupled to the respective detection circuit portions 11a-c.

Each oscillator 10a-c outputs a periodic clock signal 18a-c to the respective logic circuit portion 8a-c and detection circuit portion 11a-c, each of which use the clock signal for timing purposes. It will be understood by those skilled in the art that the oscillators 10a-c may comprise any electronic oscillators arranged to output a periodic clock signal, including but not limited to a crystal oscillator, a CMOS ring oscillator, etc.

In this example, each detection circuit portion 11a-c outputs an error signal 24a-c to the respective logic circuit portion 8a-c if a low logic speed relative to the clock frequency is detected. The error signals 24a-c need not be transmitted to the respective logic circuit portions 8a-c, but may be transmitted to an external device or a different module within the integrated circuit 2. The error signals 24a-c are fed to the corresponding logic circuits 8a-c in order to instruct them to, for example, cease or pause operation. Alternatively, the error signals 24a-c may be fed to a module external to corresponding logic circuits 8a-c in order to, for example, make a record of the event and/or switch off the power supply, although switching off the power supply may be undesirable as this may require other powered logic to be kept alive in order to restore power when it is deemed safe.

In this example, the logic circuit portions 8a-c are coupled to each other so as to allow communication between clock domains. These couplings may further comprise a number of standard components used to transmit signals between clock domains of different frequencies, as is known in the art, but the description of these is omitted for the sake of brevity.

Each logic circuit 8a-c comprises a plurality of logic elements, which in turn may comprise any module found on an integrated circuit.

Fig. 2 is a schematic diagram illustrating the detection circuit portion 11a in more detail. The detection circuit portions 11b,c comprise the same circuitry as that shown in Fig. 2. The detection circuit portion 11a comprises a latch circuit portion 12, a delay circuit portion 14 and a comparison circuit portion 16. The output 20 of

- 8 -

the latch circuit portion 12 is coupled to the input of the delay circuit portion 14 and to one of the inputs of the comparison circuit portion 16. The output 22 of the delay circuit portion 14 is coupled to the other input of the comparison circuit portion 16.

5 The latch circuit portion 12 comprises a latch flip-flop 26 and an inverter 28. The clock input of the latch flip-flop 26 is coupled to the oscillator 10a (see Fig. 1), and thus the latch flip-flop 26 is clocked by the clock signal 18a. The inverter 28 acts as a feedback loop between the input and output of the latch flip-flop 26, causing the signal 20 output by the latch flip-flop 26 to alternate state once every clock cycle. In
10 this example, the signal output by the latch flip-flop 26 alternates state on every rising edge of the clock signal 18a. The output 20 of the latch flip-flop 26 is thus in the form of a square wave at half the frequency of the clock 10a.

 The delay circuit portion 14 comprises three delay elements 30, 32 and 34; three
15 two-input multiplexers 54, 56 and 58; and a three-bit select register 36, wherein each bit of the select register 36 is coupled to the control input of one of the multiplexers 54, 56 or 58. The first of the delay elements 30 comprises eight inverters 40-47 connected in series; the second delay element 32 comprises four inverters 48-51 connected in series; and the third delay element 34 comprises two
20 inverters 52 and 53 connected in series. The number of delay elements, and therefore the number of multiplexers and size of the select register 36 is not limited to three, but may be any number. It will also be understood that the number of inverters in each of the delay elements 30, 32 and 34 is not limited to that given in this example, but may be any number. Additionally, the delay elements 30, 32 and
25 34 are not limited to the order shown in Fig. 2, but could be arranged in any convenient order.

 One input of the first multiplexer 54 is coupled to the input of the first delay element 30 (i.e. the signal 20 which is also input to the first inverter 40 of the first delay
30 element 30) and the other input of the first multiplexer 54 is coupled to the output of the first delay element 30 (i.e. the output of the last inverter 47 of the first delay element 30). One input of the second multiplexer 56 is coupled to the input of the second delay element 32 (i.e. the output of the first multiplexer which is also input to the first inverter 48 of the second delay element 32) and the other input of the
35 second multiplexer 56 is coupled to the output of the second delay element 32 (i.e.

the output of the last inverter 51 of the second delay element 30). One input of the third multiplexer 58 is coupled to the input of the third delay element 34 (i.e. the output of the second multiplexer 56 which is input to the first inverter 52 of the third delay element 34) and the other input of the third multiplexer 58 is coupled to the output of the third delay element 34 (i.e. the output of the last inverter 53 of the third delay element 34). This multiplexer arrangement enables each of the delay elements 30, 32 and 34 to be individually bypassed depending on the state of the bit of the select register 36 that is coupled to the respective control input of each multiplexer 54, 56 and 58.

The number of inverters in each of the delay elements 30, 32 and 34 is even, resulting in the delayed signal 22 being non-inverted relative to the signal 20 after propagation through delay circuit portion 14.

The comparison circuit portion 16 comprises an XOR gate 60, a detection flip-flop 62 and a stabilising flip-flop 64 connected in series. One input of the XOR gate 60 is coupled to the output 20 of the latch circuit portion 12 (i.e. the output of the latch flip-flop 26) and the other input is coupled to the output 22 of the delay circuit portion 14 (i.e. the output of the third multiplexer 58). The XOR gate is therefore arranged to compare the signal 20 output by the latch circuit portion 12 and the delayed version of the signal 22 output by the delay circuit portion 14. The XOR gate 60 therefore outputs a logic 0 if the signal 20 and delayed version of the signal 22 are in the same state, and a logic 1 if the signal 20 and delayed version of the signal 22 are in different states.

The output of the XOR gate 60 is coupled to the input of the detection flip-flop 62. The clock input of the detection flip-flop 62 is clocked by the clock signal 18a, as output by the oscillator 10a (see Fig. 1). The output of the detection flip-flop 64 is coupled to the input of the stabilisation flip-flop 64 which is also clocked by the common clock signal 18a output by the oscillator 10a.

Operation of the detection circuit portion 11a will now be described. As described previously, the signal 20 output by the latch circuit portion alternates state once per clock cycle. As the output of the latch circuit portion 12 is directly coupled to the input of the comparison circuit portion 16, the comparison circuit portion 16 receives

- 10 -

the signal 20 at one of its inputs substantially without delay. The delay circuit portion 14 similarly receives the signal 20 at its input (i.e. at the input of the first inverter 40 of the first delay element 30) substantially without delay.

5 The signal 20 then propagates through the first inverter 40 of the first delay element 30. When this happens, the inverter 40 drives the signal at its output to the opposite state of the signal 20 at its input, drawing power from the power supply 4 to do so (see Fig. 1). The speed at which the inverter 40 is able to drive the signal 20 at its input to the opposite state at its output is dependent upon the supply voltage. The
10 inverter 40 therefore introduces a propagation delay to the signal 20, the magnitude of the propagation delay introduced being dependent on the supply voltage. The next inverter 41 then receives the signal output by the first inverter 40 at its input, and the process is repeated. Each of the subsequent inverters 42-47 then repeat the same process. It will be understood by those skilled in the art that, as there are
15 eight inverters 40-47 (i.e. an even number) within the first delay element 30, the signal output by the last inverter 47 is non-inverted relative to the signal 20 at the input of the first inverter 40, and delayed with a propagation delay that is dependent on supply voltage, the propagation delay being introduced as a result of the signal 20 propagating through the inverters 40-47.

20

In the same way that the inverters 40-47 introduce a propagation delay to the signals at their output relative to the signals at their input, the logic elements within the logic circuit 8a also introduce a propagation delay to the signals at their output relative to the signals at their inputs. The propagation delays introduced by the logic
25 elements within the logic circuit 8a are similarly dependent on supply voltage, in the same way that the propagation delays introduced by the inverters 40-47 are dependent on supply voltage. As a result, it will be seen by those skilled in the art that the propagation delay introduced by the inverters 40-47 is therefore dependent on logic speed, wherein the term 'logic speed' is used to describe the rate at which
30 a signal propagates through the logic elements within the logic circuit 8a. As the supply voltage provided by the power supply 4 decreases, the logic speed of the logic circuit 8a decreases accordingly. At the same time, as the supply voltage provided by the power supply 4 decreases, the propagation delay introduced by each inverter 40-47 of the first delay element 30 increases accordingly.

As described previously, the control input of the first multiplexer 54 is coupled to one of the bits of the select register 36. In this example, if the value held in the associated bit is a logic 0, the first multiplexer 54 outputs the signal at the input of the first delay element 30 (i.e. the signal 20 without propagation delay introduced); if
5 the value held in the associated bit is a logic 1, the first multiplexer 54 outputs the signal at the output of the first delay element 30 (i.e. the signal 20 with a propagation delay introduced by the first delay element 30). It will therefore be appreciated by those skilled in the art that the associated bit within the select register 36 may be used to select whether or not the first delay element 30 is
10 bypassed during the propagation of the signal 20 through the delay circuit portion 14.

The signal output by the first multiplexer 54 is then input to the first inverter 48 of the second delay circuit portion 32, as well as to one of the inputs of the second
15 multiplexer 56. The first inverter 48 and subsequent inverters 49-51 of the second delay element 32 then invert and introduce propagation delay to the signals at their inputs in the same way as that described with reference to the first inverter 40 of the first delay element 30. As there are four inverters 48-51 (i.e. an even number) within the second delay element 32, the signal output by the last inverter 51 is non-
20 inverted relative to the signal at the input of the first inverter 48 and delayed by a propagation delay that is dependent on supply voltage, the propagation delay being introduced as a result of the signal propagating through the inverters 48-51. It will also be understood by those skilled in the art that the propagation delay introduced by the second delay element 32 is half of that introduced by the first delay element
25 30, as the second delay element 32 comprises half as many inverters as the first delay element 30.

As described previously, the control input of the second multiplexer 56 is coupled to another of the bits of the select register 36. In this example, if the value held in the
30 associated bit is a logic 0, the second multiplexer 56 outputs the signal at the input of the second delay element 32 (i.e. the signal output by the first multiplexer 54 without propagation delay introduced); if the value held in the associated bit is a logic 1, the second multiplexer 56 outputs the signal at the output of the second delay element 32 (i.e. the signal output by the first multiplexer 54 with a propagation
35 delay introduced by the second delay element 32). It will therefore be appreciated

- 12 -

by those skilled in the art that the associated bit within the select register 36 may be used to select whether or not the second delay element 32 is bypassed during the propagation of the signal 20 through the delay circuit portion 14.

- 5 The signal output by the second multiplexer 56 is then input to the first inverter 52 of the third delay circuit portion 34, as well as to one of the inputs of the third multiplexer 58. The first inverter 52 and subsequent inverter 53 of the third delay element 34 then invert and introduce propagation delay to the signals at their inputs in the same way as that described with reference to the first inverter 40 of the first
- 10 delay element 30. Again, as there are two inverters 52-53 within the third delay element 34, the signal output by the last inverter 53 is non-inverted relative to the signal at the input of the first inverter 52, and the propagation delay introduced by the third delay element 34 is half of that introduced by the second delay element 32.
- 15 As described previously, the control input of the third multiplexer 58 is coupled to the remaining bit of the select register 36 to allow the third delay element 34 to be bypassed depending on the value of that bit.

20 The arrangement of the delay circuit portion 14 shown in Fig. 2 therefore provides a binary programmable propagation delay that is proportional to the value stored in the select register 36. The value stored in the select register 36 is selected such that the propagation delay introduced by the delay circuit portion is representative of the propagation delay introduced by the critical path of the corresponding logic circuit portion 8a plus some safety margin, e.g. 10%. By having the delay circuit

25 portion 14 introduce a delay representative of, but greater than, the critical path of the corresponding logic circuit 8a, a signal will fail to propagate through the delay circuit portion 14 within a designated time period before a signal will fail to propagate through the critical path of the corresponding logic circuit 8a within the same time period when the supply voltage is decreasing. This means that a glitch

30 attack on the integrated circuit will affect the detection portion 11a before it affects any of the functional logic 8a.

35 The XOR gate 60 of the comparison circuit portion 16 receives the signal 20 at one of its inputs and receives the delayed signal 22 output by the delay circuit portion 14 at the other of its inputs. As described previously, the XOR gate 60 outputs a logic 0

if the signal 20 and delayed signal 22 are in the same state, and a logic 1 if the signal 20 and delayed signal 22 are in different states.

5 The signal output by the XOR gate 60 is input to the detection flip-flop 62. In this example, the detection flip-flop 62 captures the signal output by the XOR gate 60 on each rising edge of the clock signal 18a. Thus, the detection flip-flop 62 outputs a logic 1 only if the non-delayed signal 20 and delayed signal 22 are in different states on a rising clock edge of the clock signal 18a.

10 If the non-delayed signal 20 and delayed signal 22 are in the same state at the inputs of the XOR gate 60, this means that sufficient time has elapsed since the last change of the signal 20 for it fully to propagate through the delay circuit portion 14. If the non-delayed signal 20 and delayed signal 22 are in different states at the inputs of the XOR gate 60, this means that insufficient time has elapsed since the last change of the signal 20 for it fully to propagate through the delay circuit portion 14. As the detection flip-flop 62 captures the signal output by the XOR gate 60 on each rising clock edge, and the signal 20 alternates once per clock cycle (as described with reference to the latch circuit portion 12), this means that the detection flip-flop 62 outputs a logic 1 on a rising clock edge if the signal 20 did not fully propagate through delay circuit portion 14 within a single clock cycle. If, however, the signal 20 successfully propagates through the delay circuit portion 14 within a single clock cycle, as should be the case during normal operation of the integrated circuit 2, then the detection flip-flop 62 outputs a logic 0 on a rising clock edge. It will be appreciated by those skilled in the art that the detection flip-flop 62 may, in other examples, capture the signal output by the XOR gate 60 on a falling clock edge if appropriate changes are made to the latch circuit portion 12.

The signal 20 not being able to fully propagate through the delay circuit portion 14 within a single clock cycle indicates that the logic speed of the first clock domain 6a is too slow relative to the clock frequency of the first oscillator 10a (as signals propagating through the logic circuit portion 8a may not reach their intended destinations within the space of a single clock cycle). This may occur as a result of a glitch attack. The output of the detection flip-flop 62 indicates whether or not this is the case. If a logic 0 is output by the detection flip-flop 62, then this indicates normal operation: the signal 20 was able to fully propagate through the delay circuit

- 14 -

portion 14. If a logic 1 is output by the detection flip-flop 62, then this indicates a slow logic speed relative to the clock frequency (as the signal 20 was not able to fully propagate through the delay circuit portion 14), which may be caused by a glitch attack.

5

The signal output by the detection flip-flop 62 is received at the input of the stabilising flip-flop 64. The stabilising flip-flop 64 counteracts the effect of meta-stability in the detection flip-flop 62, e.g. if an edge of a signal output by the XOR gate 60 arrives at the detection flip-flop 62 at exactly the same time as a rising clock edge, which can cause the detection flip-flop 62 to enter a meta-stable state. The term 'meta-stable state', as used herein, is used to describe the state of the detection flip-flop 62 when edges of the input and clock signals arrive at substantially the same time such that it becomes possible for the detection flip-flop 62 to output an undefined signal (i.e. neither a logic 1 nor a logic 0).

15

The stabilising flip-flop 64 is provided in order to prevent meta-stability in the detection flip-flop 62 causing an undefined signal from propagating through any subsequent logic. The stabilising flip-flop 64 mirrors the signal output by detection flip-flop 62, one clock cycle later. For example, if the detection flip-flop 62 outputs a logic 1 on a rising clock edge, the stabilising flip-flop 64 will output a logic 1 one clock cycle later. If the detection flip-flop 62 then changes its output to a logic 0, the stabilising flip-flop will change its output to a logic 0 one clock cycle later. If the detection flip-flop 62 outputs an undefined signal as a result of meta-stability, the stabilising flip-flop 64 will prevent the undefined signal from propagating any further – the stabilising flip-flop 64 will output either a logic 1 or a logic 0, dependent on the undefined signal at its input, but will not output an undefined signal itself. As the output of the stabilising flip-flop 64 is the error signal 24a output of the detection circuit portion 11a, this therefore prevents the error signal 24a from being undefined. If the output of the flip-flop 64 is high for even a single cycle, it can be inferred that a glitch must have occurred.

30

Thus it will be understood that the detection circuit 11a outputs an error signal 24a if the signal 20 does not fully propagate through the delay circuit portion 14 within a single clock cycle. As the propagation delay introduced by the delay circuit portion 14 is representative of the critical path of the corresponding logic circuit 8a, plus

35

- 15 -

some error margin, this means that the error signal 24a will be output at the same time or before a signal is not able to propagate along the critical path of the corresponding logic circuit 8a in the event of a decreasing supply voltage from the power supply 4. Hence, the detection circuit 11a is able to detect a low logic speed
5 relative to the clock frequency, which may arise as a result of a glitch attack which may be as short as a single cycle, at the same time as or before failure occurs in the corresponding logic circuit 8a.

As previously mentioned, the error signal may be reported to the logic 8a of another
10 module to allow appropriate action to be taken such as recording a suspicious event, pausing operation, power cycling the circuit, preventing operation etc.

CLAIMS

1. An integrated circuit comprising a circuit portion for detecting a low logic speed relative to a clock signal frequency, the circuit portion comprising:
an oscillator arranged to output a periodic clock signal; and
5 a detection circuit portion comprising:
a latch circuit portion arranged to output a first signal that changes state once per clock cycle;
a delay circuit portion arranged to receive said first signal and output a second signal subject to a propagation delay compared to the first signal,
10 said propagation delay being less than a period of the clock signal under normal operating conditions; and
a comparison circuit portion arranged to compare the first signal at the input and the second signal at the output of the delay circuit portion and output an error signal if the signals are indicative of low logic speed relative
15 to the clock signal frequency.
2. The integrated circuit as claimed in claim 1, arranged to compare the propagation delay to the period of the clock signal.
- 20 3. The integrated circuit as claimed in claim 1 or 2, arranged such that the propagation delay is dependent on a supply voltage provided thereto.
4. The integrated circuit as claimed in any preceding claim, wherein the delay circuit portion comprises a plurality of logic gates.
- 25 5. The integrated circuit as claimed in any preceding claim, arranged such that the propagation delay is greater than or equal to an inherent propagation delay introduced by a critical path of a logic circuit portion elsewhere in the integrated circuit.
- 30 6. The integrated circuit as claimed in claim 5, wherein the logic circuit portion is clocked by the periodic clock signal.

- 17 -

7. The integrated circuit as claimed in any preceding claim, wherein the comparison circuit portion is arranged to compare the first and second signals once per clock cycle.
- 5 8. The integrated circuit as claimed in any preceding claim, wherein the latch circuit portion is arranged to switch the state of its output signal on a rising edge of the clock signal, and the comparison circuit portion is arranged to compare the first and second signals on a rising edge of the clock signal.
- 10 9. The integrated circuit as claimed in any preceding claim, wherein the delay circuit portion comprises a plurality of delay elements.
10. The integrated circuit as claimed in claim 9, arranged such that each delay element has similar scaling characteristics with respect to voltage as logic elements
15 in a critical path of a logic circuit portion elsewhere in the integrated circuit.
11. The integrated circuit as claimed in claim 9 or 10, arranged such that each delay element can be employed or bypassed in order to provide a configurable propagation delay.
20
12. The integrated circuit as claimed in any of claims 9 to 11, arranged such that each delay element introduces a unique propagation delay to the first signal.
13. The integrated circuit as claimed in any of claims 9 to 12, arranged such that
25 the propagation delay introduced by one of the delay elements comprises a unit delay, and the delays introduced by the other delay elements comprise increasing power of two multiples of the unit delay.
14. The integrated circuit as claimed in any of claims 9 to 13, arranged such that
30 each delay element outputs a non-inverted signal at its output relative to its input.
15. The integrated circuit as claimed in any of claims 9 to 14, wherein each delay element comprises an even number of inverters connected in series.

16. The integrated circuit as claimed in any preceding claim, wherein the comparison circuit portion comprises a logic gate, an output of which is coupled to an input of a first flip-flop clocked by the periodic clock signal, the logic gate taking the first signal as one of its inputs and the second signal as the other of its inputs.
- 5
17. The integrated circuit as claimed in claim 16, wherein the logic gate is arranged to output a third signal, the state of which is dependent on whether the first and second signals are in the same state or in different states.
- 10
18. The integrated circuit as claimed in claim 16 or 17, arranged such that the first flip-flop outputs the error signal when the output of the logic gate indicates that the first and second signals are in different states, when the first flip-flop is clocked.
- 15
19. The integrated circuit as claimed in any of claims 16 to 18, wherein the comparison circuit portion further comprises a second flip-flop clocked by the periodic clock signal, the output of the first flip-flop being coupled to an input of the second flip-flop, wherein the second flip-flop is arranged to mirror the output of the first flip-flop with a delay of one clock cycle and output the error signal.

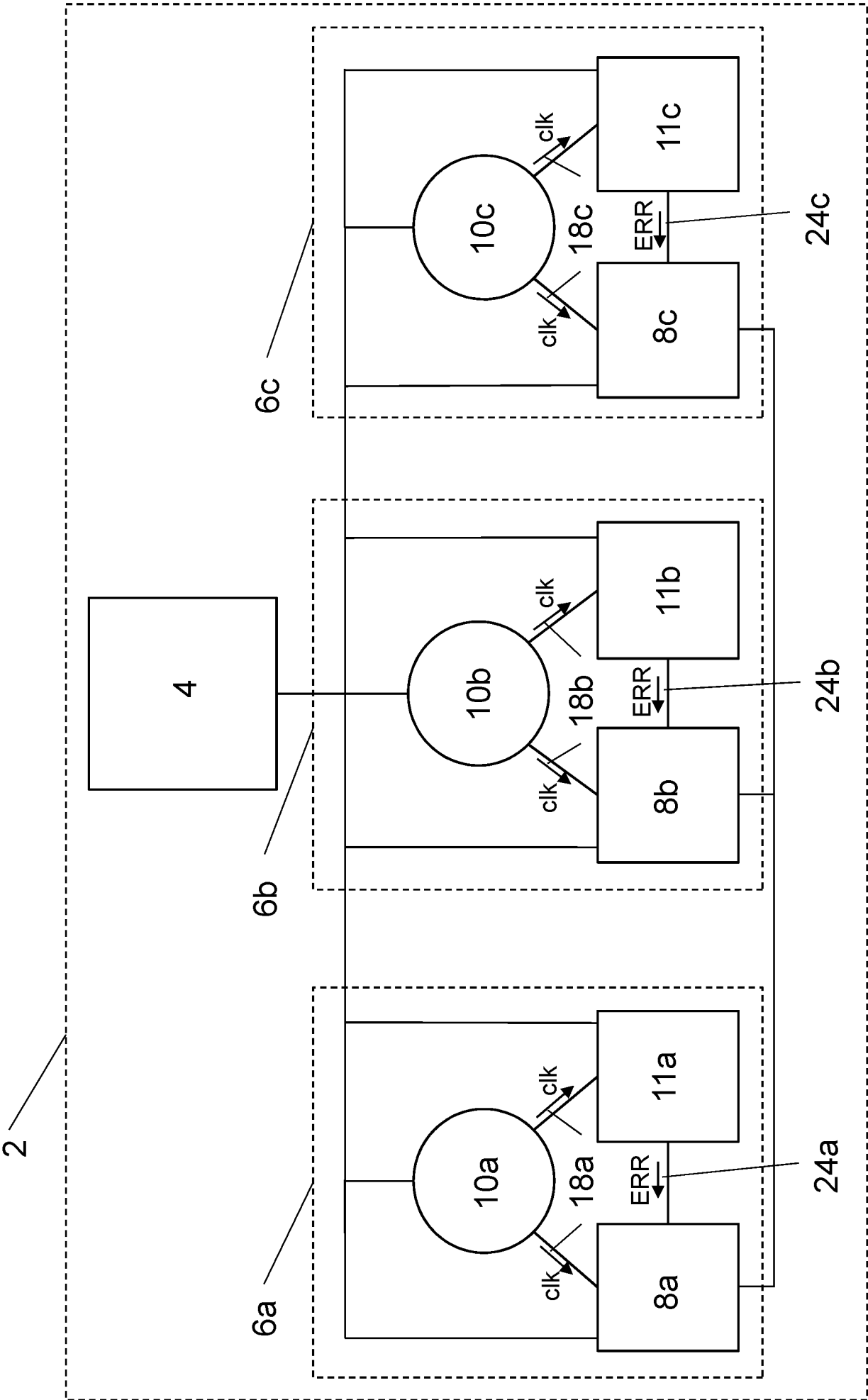


FIG. 1

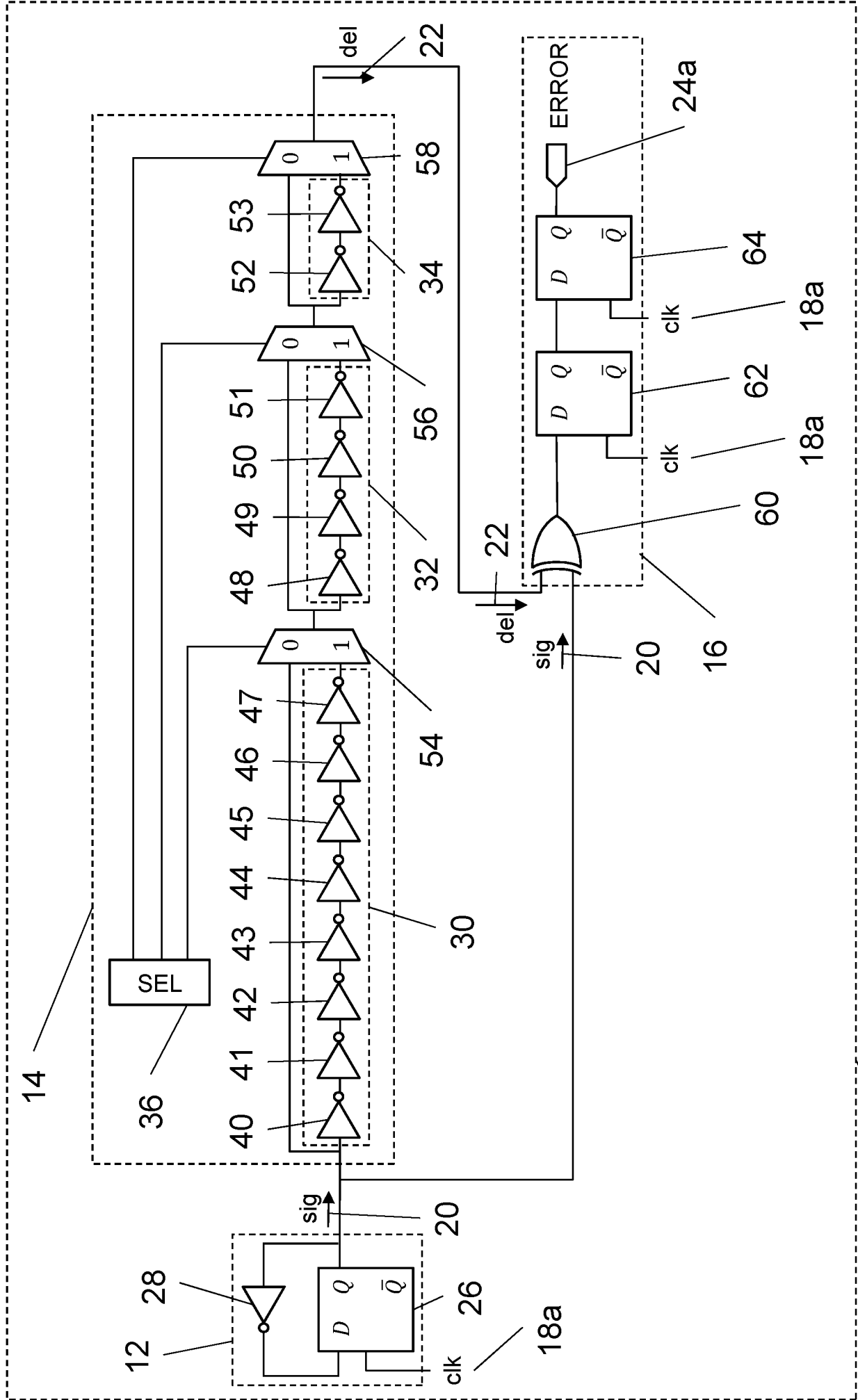


FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2022/063277

A. CLASSIFICATION OF SUBJECT MATTER INV. G06F21/75 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/402929 A1 (LENTZ ANDREAS [DE] ET AL) 24 December 2020 (2020-12-24) paragraphs [0017] - [0021], [0028], [0032], [0036], [0043]; figures 3,4 -----	1-19
X	US 2020/081062 A1 (GOH BENG-HENG [SG]) 12 March 2020 (2020-03-12) paragraphs [0051] - [0063] -----	1-19
X	BERINGUIER-BOHER NOEMIE ET AL: "Voltage Glitch Attacks on Mixed-Signal Systems", 2014 17TH EUROMICRO CONFERENCE ON DIGITAL SYSTEM DESIGN, IEEE, 27 August 2014 (2014-08-27), pages 379-386, XP032665127, DOI: 10.1109/DSD.2014.14 Section II.B; Section IV; Fig. 6 and 7; figures 6,7 -----	1-19
-/--		
☒ 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 6 September 2022		Date of mailing of the international search report 15/09/2022
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 Dingel, Janis

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2022/063277

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NIDHAL SELMANE ET AL: "WDDL is Protected against Setup Time Violation Attacks", FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY (FDTC), 2009 WORKSHOP ON, IEEE, PISCATAWAY, NJ, USA, 6 September 2009 (2009-09-06), pages 73-83, XP031627631, ISBN: 978-1-4244-4972-9 Abstract; Section V.B; figure 14 -----	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2022/063277

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2020402929	A1	24-12-2020	NONE	

US 2020081062	A1	12-03-2020	NONE	
