



(51) International Patent Classification:

G06F 21/71 (2013.01)

G06F 21/76 (2013.01)

Published:

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

(21) International Application Number:

PCT/US2018/057565

(22) International Filing Date:

25 October 2018 (25.10.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: HEWLETT-PACKARD DEVELOPMENT

COMPANY, L.P. [US/US]; 10300 Energy Drive, Spring, Texas 77389 (US).

(72) Inventors: BELGARRIC, Pierre; HP Inc UK Limited, Filton Road Stoke Gifford, Pt., Bristol Bristol BS34 8QZ (GB). PLAQUIN, David; HP Inc UK Limited, Filton Road Stoke Gifford, Pt., Bristol South Gloucestershire BS34 8QZ (GB). COHEN, Eugene; 11311 Chinden Blvd., Boise, Idaho 83714-0021 (US). GUNNING, Chris R; 11311 Chinden Blvd., Boise, Idaho 83714-0021 (US).

(74) Agent: WOODWORTH, Jeffrey C. et al.; HP Inc., 3390 E. Harmony Road - MS 35, Fort Collins, Colorado 80528 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: INTEGRATED CIRCUIT(S) WITH ANTI-GLITCH CANARY CIRCUIT(S)

(57) Abstract: An IC comprising functional circuit to perform primary functions of the IC is provided. The functional circuit is to enable electrical signals to propagate through it within a timing constraint of the functional circuit. The IC comprises at least one canary circuit used for detecting glitch attacks on the circuit. Electrical signals are to propagate through the canary circuit(s) within a defined timing constraint of the canary circuit(s). The canary circuit is to provide a signal path designed such that in the event of a timing constraint of the functional circuit(s) is violated due to a glitch attack, also the timing constraint of the canary circuit(s) is violated.



INTEGRATED CIRCUIT(S) WITH ANTI-GLITCH CANARY CIRCUIT(S)

BACKGROUND

[0001] An integrated circuit is a circuit in which all or some of the circuit elements are inseparably associated and electrically interconnected so that it is considered to be indivisible for the purposes of construction and commerce. The integrated circuit comprises functional circuit(s), which perform primary functions of the integrated circuit. Such primary functions are, for example, to store data and to provide access to that data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Features and advantages of examples will be described, by way of example only, in the following detailed description with reference to the accompanying drawings in which like reference numerals correspond to similar, though perhaps not identical, components. For the sake of brevity, reference numerals or features having a previously described function may or may not be described in connection with other drawings in which they appear.

[0003] Figure 1 shows a schematic block diagram of an integrated circuit equipped with functional circuits and canary circuits under normal operation;

[0004] Figure 2 shows a schematic block diagram on the integrated circuit of Figure 1 when the integrated circuit suffers a glitch attack;

[0005] Figure 3 shows a schematic block diagram on an exemplary distribution of canary circuits and functional circuits over an exemplary integrated circuit;

[0006] Figure 4 shows schematic examples of time constraint violations and non-violations of canary circuits and functional circuits.

[0007] Figure 5 shows schematic examples of a functional circuit and of a strict and a restrictive canary circuits with their respective signal propagation time relative to a

clock pulse width.

[0008] Figure 6 shows a schematic block diagram of a canary circuit with a signal path including a series connection of standard logic gates;

[0009] Figure 7 shows a schematic block diagram of an integrated circuit, equipped with anti-clock-glitch canary circuits, which suffers a glitch attack on the integrated circuit's clock signal input;

[0010] Figure 8 shows a schematic block diagram of an integrated circuit, equipped with anti-voltage-glitch canary circuits, which suffers a glitch attack on the integrated circuit's voltage signal input;

[0011] Figure 9 shows a schematic block diagram of an integrated circuit, equipped with anti-voltage-glitch and anti-clock-glitch canary circuits, which suffers a glitch attack on the integrated circuit's power/voltage signal and clock signal inputs;

[0012] Figure 10 shows a schematic block diagram of an integrated circuit equipped with strict and a relaxed canary circuits, with the strict canary circuit responding to a glitch attack

[0013] Figure 11 shows a schematic block diagram of an integrated circuit equipped with strict and a relaxed canary circuits, with the strict and the relaxed canary circuit responding to a glitch attack

[0014] Figure 12 shows an exemplary integrated circuit with a canary circuit placed adjacent to input and output of a cryptographic engine circuit;

[0015] Figure 13 shows an exemplary integrated circuit with a canary circuit placed adjacent to a storage medium on which a firmware signature is stored;

[0016] Figure 14 provides a flow chart of an exemplary method of handling a glitch attack on an integrated circuit;

[0017] Figure 15 provides a flow chart of exemplary counteractions 80 triggered by the monitoring logic 8.

[0018] Figure 16 provides a flow chart of exemplary counteractions 80 triggered by the monitoring logic 8 different to those counteractions illustrated in Fig. 15.

[0019] Throughout the drawings, identical reference numbers designate similar, but not necessarily identical, elements. The figures are not necessarily to scale, and the size of some parts may be exaggerated to more clearly illustrate the example shown. Moreover the drawings provide examples and/or implementations consistent with the description; however, the description is not limited to the examples and/or implementations provided in the drawings.

DETAILED DESCRIPTION

[0020] Examples provided herein include an integrated circuit and a method of handling a glitch attack on an integrated circuit. Integrated circuits are increasingly subject to hardware associated attacks based on tampering with input signals of the circuit. This enables an attacker to read out sensitive data, to circumvent authenticity checks etc. An often-used hardware associated attack is a so-called glitch attack which is based on disrupting a power/voltage or clock input of an integrated circuit, such that timing constraints of an integrated circuit are violated and security related functions of the chip might therefore fail.

[0021] The primary function of an integrated circuit, mentioned in the background section is, in some examples, the main purpose of the integrated circuit. As such, for example, when the main purpose of the integrated circuit is to store data and to provide access to that data, the functional circuits are, for example, reading/writing circuits for a data storage. The functional circuit may also correspond to the integrated circuit main logic. The integrated circuit has a power/voltage input and a clock input.

[0022] The at least one functional circuit enables signals to propagate through the at least one functional circuit in accordance with a timing constraint of the at least one functional circuit. Signal propagation through a circuit is understood herein as the signal entering an input of the circuit, passing through the circuit's interior logic and leaving the

circuit at its output. The timing constraint of the functional circuit is, for example, a timing constraint of the hardware logic gates (especially CMOS gates). To work properly, the clock period of a clock signal for the integrated circuit is high enough for registers in the circuits to stabilize to the correct value.

[0023] The timing constraint of the at least one functional circuit, for example, ensures that electrical signals propagate fast enough through the circuit such that register-values of the at least one functional circuit stabilize before a clock signal edge and at each clock signal edge, the register value of the functional circuit is the correct one.

[0024] In addition to the at least one functional circuit, the integrated circuit also comprises at least one canary circuit. The at least one canary circuit is to be used in the detection of glitch attacks. In some examples, the at least one canary circuit serves as a detector for said glitch attacks.

[0025] A glitch attack is based on perturbing the inputs (power/voltage, clock, etc.) of an integrated circuit with a glitch (disrupting the signal with a short spike). This may interfere with the logic of the integrated circuit. It can lead to the attacker successfully tampering with the integrity of the system or its data, or to get access to secret or sensitive data, for example by

- Bypassing security mechanism such as secure boot and execute their own software (and then access any credentials stored within the chip)
- Force leakage of information and perform cryptanalysis to deduce the value of some secret data (e.g. keys).

[0026] The at least one canary circuit also enables electrical signals to propagate through the at least one canary circuit according to at least one defined timing constraint of the canary circuit. The defined timing constraint of the canary circuit ensures also here, for example, that electrical signals propagate fast enough through the circuit such that register values of the canary circuit stabilize before a clock signal edge and at each clock signal edge, the register value of the canary circuit is the correct one.

[0027] As the at least one canary circuit and the at least one functional circuit, for example, face the same clock signal and the same power/voltage input the timing

constraint of the canary circuit and the timing constraint of the at least one functional circuit is, for example, the same design constraint, namely that signal propagate fast enough through the circuit that register values in the circuit are settled and correct at each clock signal edge.

[0028] The at least one canary circuit is to provide at least one signal path designed such that in the event of a timing constraint of the at least one functional circuit is violated due to a glitch attack, also the timing constraint of the at least one canary circuit is violated. The signal path of the at least one canary circuit is, for example, a digital logic path through which signals propagate just within the timing constraint of the at least one canary circuit.

[0029] As such, the canary circuits may exhibit the longest propagation paths in the integrated circuit. At least, in some examples, the propagation time of a signal through the canary circuit is equal to or longer than the signal propagation time of a time critical functional circuit (which is a circuit through which signals propagate just within the timing constraint of the functional circuit).

[0030] Glitch attacks on the clock input (e.g. inserting a short spike on the clock) cause a timing constraint violation of the at least one functional circuit as well as the at least one canary circuit. This is the case as due to disrupting the clock signal, the clock signal edge might arrive earlier – such that register values of the at least one canary circuit and of the at least one functional circuit do not have settled upon arrival of said clock signal edge.

[0031] Glitch attacks on the power/voltage input may cause signal propagation speed to be decreased, which in turn, also leads to a violation of the timing constraint both of the at least one canary circuit and the at least one functional circuit.

[0032] The at least one violation of the timing constraint of the at least one canary circuit is counted as a detection of a glitch attack.

[0033] In some examples, the at least one canary circuit is to send at least one intrusion-detection signal to a monitoring logic in response to the timing constraint of the at least one canary circuit being violated. The monitoring logic can be a part of the same

integrated circuit as the at least one canary circuit and the at least one functional circuit.

[0034] The monitoring logic is, for example, to cause at least one counteraction against a glitch attack in response to receiving said at least one intrusion detection signal.

[0035] In some examples, a plurality of canary circuits are distributed over the integrated circuit.

[0036] In some examples, the at least one canary circuit is implemented in a block of the integrated circuit which is separate to the at least one functional circuit. The canary circuits are, for example, discrete circuit elements and are, for example, disjoint from the at least one functional circuit.

[0037] To ensure that, for example, local variations within an integrated circuit, such as manufacturing differences of CMOS switches or local EM field effects are not the cause of a timing constraint violation of a canary circuit but indeed an attack also afflicting the at least one functional circuit, there is, for example, a sufficient difference between the signal propagation paths of the functional circuits and the signal propagation paths of the canary circuits in terms of time criticality. Time criticality refers herein to the difference of a propagation time through a circuit in relation to the clock signal period – circuits with a high propagation time that finish signal processing only a short time before a clock signal edge are more time critical than such that finish signal processing well before the clock edge.

[0038] By distributing a plurality of canary circuits over the integrated circuit, it is also easier to avoid invasive glitch attacks as spots for an invasive glitch attack to be successful are limited.

[0039] In some examples, the integrated circuit comprises a plurality of canary circuits and at least a part of the canary circuits is to provide a signal path designed such that when the timing constraint of the at least one canary circuit is violated, the timing constraint of the at least one functional circuit is not yet violated.

[0040] Nonetheless, the signal path of such canary circuit provides a signal path with a signal propagation time as such that in the event of a glitch attack tampering with

the timing constraint the at least one functional circuit - performing the primary functions
- also the timing constraint of the canary circuit is violated.

[0041] Hence, a violation of timing constraint of the functional circuit means a violation of the defined timing constraint of these canary circuits but a timing constraint violation of those canary circuits does not necessarily indicate that the at least one functional circuit is compromised.

[0042] In some examples, the integrated circuit comprises at least one strict canary circuit, wherein the strict canary circuit provides a signal path such that when the timing constraint of the strict canary circuit is violated, the timing constraint of the at least one functional circuit is not violated and there is at least one relaxed canary circuit that provides a signal path with a signal propagation time closer to a signal propagation time of the at least one functional circuit than a signal propagation time of the strict canary circuit.

[0043] The signal propagation time through a relaxed canary circuit is typically shorter than those through a strict canary circuit – for which a timing constraint violation occurs more easily.

[0044] In some examples, when only the timing constraint of the at least one strict canary circuit is violated, wherein the monitoring logic is to cause counteractions by informing an integrated circuit main logic and the integrated circuit main logic is to perform the at least one counteraction against the glitch attack. This is the case as timing constraint violation of at least one strict canary circuit only indicates that the functional circuit(s) (that could also correspond to the main logic of the integrated circuit) is/are not compromised.

[0045]

In some examples, when the timing constraint both of the at least one strict canary circuit and the at least one relaxed canary circuit is violated, the monitoring logic is to perform the at least one counteraction against the glitch attack. Timing constraint violations of both sorts of canary circuits (strict and relaxed) indicate that the functional circuits and

therewith the main logic of the integrated circuit is very likely compromised so that counteractions are to be performed by the monitoring logic itself instead of by the functional circuit.

[0046] In some examples, where the at least one canary circuit comprises standard logic gates is to perform calculation operations. In some examples, when a result of the calculation operations performed does not match an expected result of the calculation operation, a violation of a timing constraint of the at least one canary circuit is deemed to have occurred.

[0047] Standard logic gates are gates corresponding to logical operations such as "AND", "OR", "NOT", "XOR", "NAND" and so forth.

[0048] By connecting such logic gates with each other, calculation tasks that require a signal propagation time through the canary circuit as needed can be created. To provide an example, a calculation task is chosen that yields a processing time such that the result is available just before the clock-signal edge so that under normal conditions the timing constraint of the canary circuit is not violated, but said timing constrain is violated in the event of a glitch attack on the integrated circuit.

[0049] In some examples, the standard logic gates in the signal path of the canary circuit comprise a succession of inverters. Inverters are logical gates performing a "NOT" or negation operation. This succession of inverters is, for example, connected to a plurality of other logical gates to form said signal path. The usage of standard logic gates in the signal path makes it possible to embed the canary circuit at the integrated circuit's core logic.

[0050] In some examples, the at least one canary circuit is to provide a signal path as such that the timing constraint is violated as a consequence of at least one glitch present in a voltage signal for the integrated circuit. The glitch present in a voltage signal for the integrated circuit corresponds to a glitch present in the power signal for the integrated circuit.

[0051] In these examples, the signal path is to provide a propagation time through the at least one canary circuit that allows register bits to settle within the canary circuit with such a distance in time (further referred to herein also as "time buffer") to the clock-

signal edge, such that the timing constraint of the canary circuit is not violated by natural voltage, temperature or manufacturing differences on the integrated circuit but is certainly violated as a consequence of glitch in the clock-signal, e.g.. a clock edge shift to an earlier time. Canary circuits with such a signal path are also referred to herein as "anti clock-glitch canary circuits".

[0052] In other examples, the at least one canary circuit is to provide a signal path as such that the timing constraint is violated as a consequence of at least one glitch present in a voltage signal for the integrated circuit. As mentioned above, a glitch in the voltage signal corresponds to a glitch in the power signal.

[0053] For these examples, the signal path of the at least one canary circuit is chosen such as explained above for the anti-clock glitch canary circuit but with the difference that the signal path of the circuit yields a time buffer so that said timing constraint is violated by a glitch present in the power/voltage input but not said rather natural local fluctuations. Canary circuits with such a signal path are also referred to herein as "anti voltage-glitch canary circuits".

[0054] The above-mentioned time buffer is designed differently for anti clock-glitch canary circuits than for anti voltage-glitch canary circuits. This is the case as slowing down signal speed, as it is the case for a glitch attack on the integrated circuit's voltage input, may cause violations of a (canary) circuits timing constraint on a significantly higher or lower timescale than violations caused by a glitch introduced into the clock signal for the integrated circuit. An anti clock-glitch canary circuit, for example, with a signal path to detect (high) timing constraint violations, providing therefore a comparable short signal path, would not be able to detect (smaller) timing constraint violations caused by a glitch introduced into the circuit's input voltage.

[0055] In some examples the integrated circuit therefore comprises at least one anti clock-glitch canary circuit and at least one anti-voltage glitch canary circuit to reliably detect glitch attacks on the integrated circuit's power/voltage input and glitch attacks on the integrated circuit's clock input.

[0056] In some examples, the integrated circuit comprises a cryptographic engine and wherein the at least one canary circuit is placed in the integrated circuit adjacent to at

least one of the input and the output of said cryptographic engine. The cryptographic engine is an example for a functional circuit which is monitored by the at least one canary circuit for glitch attack detection.

[0057] By placing the canary circuits this way, they face the same local variations as the ports of the cryptographic engine, which makes the detection accurate for this engine and diminishes the risk of a successful invasive glitch attack. An invasive glitch attacker would most likely also affect the canary circuit by its attack not only the cryptographic engine as the at least one canary circuit is placed close to the cryptographic engine. The cryptographic engine is a sensitive place as tampering with said cryptographic engine may result in deducing the value of an encryption key.

[0058] In some examples, the integrated circuit comprises a storage medium on which a firmware-signature is stored and wherein the at least one canary circuit is placed adjacent to circuits for accessing said storage medium on which the firmware signature is stored.

[0059] The firmware signature's storage place is sensitive as the firmware signature could be retrieved by unauthorized persons due to a successful glitch attack. This could, for example, enable those persons to provide a non-authentic firmware with said signature.

[0060] In this example, the canary circuit also "sees" the same local variations as the firmware-signature storage when placed like that and invasive glitch attacks are unlikely to succeed are attackers would most likely also tamper with the adjacent placed canary circuit not only with the firmware storage.

[0061] In some embodiments, the monitoring logic is a chip monitoring logic and wherein the counteractions against the glitch attack performed by this monitoring logic comprises notifying a main logic of the integrated circuit.

[0062] The monitoring logic is to notify the integrated circuits main logic upon receiving the intrusion detection signal send by the at least one canary circuit.

[0063] The integrated circuit's main logic is to block access to the integrated circuit or disable parts of the integrated circuit. upon being notified.

[0064] Those blocking or disabling actions could be at least one of (i) blocking access to at least one memory of the integrated circuit and (ii) disconnecting a network connection of a host device of the integrated circuit.

[0065] By blocking to a memory of the integrated circuit, sensitive data cannot be read out from said memory or sensitive data cannot be overwritten by an attacker. The memory of the integrated circuit could be one of the above mentioned functional circuits. By disconnecting a network connection of a host device of the integrated circuit, it is ensured that after a security breach caused by a glitch attack no other device of the network is affected.

[0066] Furthermore, access to the hard drive controller, to the PCI controller or any other subsystem may be blocked.

[0067] In some examples, the integrated circuit comprises at least one microchip and the counteractions against the glitch attack are chip-wide actions. Those chip-wide actions comprise at least one of the following: (i) reset, (ii) hold, (iii) data wipe.

[0068] Those chip-wide actions are either performed by the monitoring unit itself or by another entity of the integrated circuit.

[0069] In the course of the counteraction "reset" the chip is set to a default state. In the course of the counteraction "hold" – further processing of chip operations is stopped. In the course of the counteraction "data wipe", all data is erased from the chip.

[0070] The examples described herein also relate to a method of handling a glitch attack on an integrated circuit. The method comprises:

Performing primary functions of the integrated circuit by at least one functional circuit, wherein the at least one functional circuit enables electric signals to propagate through the at least one functional circuit in accordance with a timing constraint of the at least one functional circuit,

detecting a glitch attack, wherein detecting the glitch attack comprises:

checking whether or not a defined timing constraint of at least one canary circuit is violated, the at least one canary circuit being a circuit comprised by the integrated

circuit, wherein the at least one canary circuit enables electrical signals to propagate through the at least one canary circuit in accordance with the defined timing constraint,

wherein the at least one canary circuit provides a signal path designed such that in the event of a timing constraint of the at least one functional circuit is violated due to a glitch attack, also the defined timing constraint of the at least one canary circuit is violated,

reacting to a detected glitch attack, wherein reacting to the detected glitch attack comprises:

sending at least one intrusion-detection signal to a monitoring logic in response to the timing constraint of the at least one canary circuit being violated,

causing - by the monitoring logic - at least one counteraction against a glitch attack in response to receiving said at least one intrusion-detection signal.

[0071] The method of handling a glitch attack and reacting to a glitch attack comprises any of the functions described in conjunction with examples pertaining to the integrated circuit disclosed herein.

[0072] Referring to figure 1, the exemplary integrated circuit 100 comprises two functional circuits 1 and two canary circuits 2. The functional circuits 1 are to perform primary functions of the integrated circuit, such as a cryptographic operation using a private key, storing information etc. The canary circuits 2 are used in detecting glitch attacks 200 (see Figs. 2, 5, 6 and 7) on the integrated circuit 100. The integrated circuit 100, for example, comprises at least one micro-chip. The exemplary canary circuits 2 are located on each of those chips or only on such chips that perform critical operations for data security, such as encryption etc.

[0073] The exemplary integrated circuit 100 is supplied with a clock signal 4 at a clock input 14 with a supply voltage/power at a power/voltage input 15.

[0074] Electrical signals 6 are to propagate through the functional circuits 1 in accordance with a timing constraint of the functional circuit 1.

[0075] The canary circuits 2 provide a signal path 3 for electrical signals 6 to propagate within the timing constraints of the canary circuit 2. The signal path 3 is designed such that in the event of a glitch attack (which is further described in conjunction with figure 2 below) – in response to the timing constraint of the functional circuit 1 is violated, also the timing constraint of the canary circuits 2 is violated.

[0076] This is the case, as propagating through a signal path 3 of the canary circuits 2 needs more time or the same time than propagating through, for example, the functional circuit 1 with the longest signal path, which is, a time critical circuit. The signal path of the canary circuits 2 is chosen - by design of signal path 3 - that signals propagate just within the timing constraints of the canary circuits 2.

[0077] Any glitch attack which violates the timing constraints of a function circuit 1, e.g. the above-mentioned time critical circuit, consequently also violates the timing constraints of at least one of the canary circuits 2.

[0078] A violation of a timing constraint of at least one canary circuit 2 corresponds to the detection of a glitch attack by the canary circuit(s) 2. The integrated circuit 1 further comprises a monitoring logic 8 to cause counteractions 80 (see Figs. 11 and 12) against the glitch attack and a main logic of the integrated circuit 30.

[0079] It is noted here that the functional circuit 1 and the main logic of the integrated circuit 30 might be the same or separate circuits.

[0080] Fig. 2 shows an exemplary glitch attack 200. The glitch attack 200 can be, for example, directed to at least one of (i) the voltage signal 5 and (ii) the clock signal 4. When the glitch attack 200 is directed to the clock signal 4, for example, a glitch 20 is introduced into the clock signal by introducing a spike into the clock pulse, with the consequence that a clock edge is timed earlier than intended. The timing constraints of at least one of the functional circuits 1 is thereby violated. Hence, for example, if an authentication procedure is interrupted that way, access might be granted to the attacker although authentication was never successful.

[0081] Similarly, the glitch 20 introduced into the voltage signal slows down signal propagation speed through the functional circuits 1. Due to the slow signal

propagation speed also here security related processes, performed by functional circuits 1 can be sabotaged.

[0082] To prevent the glitch attack 200 from succeeding, the integrated circuit 1 is provided with the above described canary circuits 2. As a consequence of the glitch attack 200, not only the timing constraints of the functional circuits 1 are violated, but at the same time also the timing constraints of the canary circuits 2 are violated. The canary circuits 2 are to react to this violated by sending at least one intrusion detection signal 7 to the monitoring circuit 8. The monitoring circuit 8 is to cause at least one counteraction against the glitch attack 200. The at least one counteraction comprises for example notifying the integrated circuit main logic 30, which then, e.g. blocks access to a memory or disconnects the network connection of the integrated circuit (or the host device of the integrated circuit) or initiating chip-wide actions such as hold, reset or data wipe.

[0083] Hence, although the timing constraints of at least one functional circuit is violated, an attacker cannot seize the merits of the glitch attack 200 as this is prevented by the at least one counteraction 80 (see Figs. 11 and 12).

[0084] Fig. 3 shows a schematic block diagram of an exemplary distribution of functional circuits 1 and canary circuits 2 an exemplary integrated circuit 100. The integrated circuit 100 can, for example, be equipped the same further elements (monitoring logic 8, integrated circuit main logic 30) as the integrated circuit illustrated by Figs. 1 or 2.

[0085] The two canary circuits 2 of the integrated circuit 100 are distributed over the integrated circuit 100 as illustrated by Fig. 3. The canary circuits 2 are implemented in blocks of the integrated circuit 100 that are separate to the three functional circuits 1. Hence, the canary circuits 2 are discrete and not necessarily connected to the functional circuits 1. As the canary circuits 2 are designed as blocks separate to the functional circuits 1 they do not have to be included into design considerations for the functional circuits 1.

[0086] Fig. 4 shows a schematic block diagram of situation in which the timing constraint of a functional circuit 1 is violated 402 and a situation in which said timing constraint is not violated 401 and a situation in which the timing constraint of a canary

circuit is violated 502 and a situation in which the timing constraint of a canary circuit is not violated 502. When a violation of the timing constraint of the functional circuit 402 occurs, the clock signal 4 edge arrives before the electrical signal 6 (the circuit's input signals) have propagated to the functional circuit's output and hence have been processed completely and register values of said circuit have settled to the correct value. When the clock signal edge 4, however, arrives before the electrical signal 6 is processed (and said register values have settled) the timing constraint of the functional circuit is violated 402.

[0087] Violations and non-violations of constraints of the canary circuit 502, 501 also correspond to the signal 6 propagating fast enough through the signal path 3 such as register values are settled before the clock signal edge arrives (situation 501) or too slow such that the register values are not settled upon arrival of the clock-signal edge (situation 502).

[0088] Fig. 5 is schematic examples of a functional circuit and of a strict and a restrictive canary circuits with their respective signal propagation time relative to a clock pulse width.

[0089] Functional circuit 1 shows no timing constraint violation in situation 601, as signals can propagate through the functional circuit 1 before the edge of clock signal 4 arrives. The signal propagation time is indicated by the length of the boxes representing the functional circuit 1 and the relaxed and strict canary circuits 2a, 2b respectively, the clock pulse width by the shape of clock pulse 4.

[0090] The functional circuit 1 is, for example, guarded by a strict canary circuit 2b and a relaxed canary circuit 2a, having signal paths 3a, 3b respectively. In the case a glitch attack on the voltage occurs, the voltage pulse 4 is shortened, as explained above. The strict canary circuit 2b is very sensitive with regard to such a pulse-shortening as the signal propagates through the circuit right before the arrival of the clock signal edge 4, as shown in situation 602. However, there is more buffer for a signal to propagate through the functional circuit 1 before the clock signal 4 arrives (see situation 601). Hence, the timing constraint of the strict canary circuit 2b might be violated with the timing constraint of the functional circuit 1 not being violated. However, if the timing constraint of the functional circuit is violated, then also the timing constraint of the strict canary

circuit 2b is violated.

[0091] However, the signal propagation path 3a of the relaxed canary circuit 2a is shorter than the signal propagation path 3b of said strict canary circuit 2b. Therefore, timing constraints are more relaxed for the relaxed canary circuit 2a. The length of signal propagation path of relaxed canary circuit 2a is closer to the length of signal propagation path of the functional circuit 1 the corresponding signal path length of the strict canary circuit 2b. This means but also that if the timing constraint of the relaxed canary circuit 2a is violated, the timing constraint of the functional circuit 1 is very likely also violated, as in this example, relaxed canary circuit 2a and functional circuit 1 nearly face the same timing constraint (see comparison of situation 601 and 603).

[0092] Fig. 6 is a schematic block diagram of a single canary circuit 2. The canary circuit 2 has an exemplary signal path 3. In the example illustrated by Fig. 4, the signal path is constituted by standard logic circuits 9. The standard logic circuits 9 are chosen as such that the path 3 provides a propagation time for a signal that is close to violating the timing constraint of the canary circuit 9. This propagation time can be bigger or equal to the propagation time of a rather time critical functional circuit 1 of integrated circuit 100. Still, the propagation time is chosen with a time buffer to the timing constraint of the canary circuit as such that the above-mentioned impacts of local variations between the functional circuits 1 to be monitored and the canary circuits 2 on signal propagation time do not cause false positive glitch attack 200 (see Figs. 2, 5-7) detections.

[0093] In the example illustrated by Fig. 5, standard logic gates 6 in the form of a chain of an "AND" gate and a succession of three inverters (which are "NOT" gates) are implemented. Whenever a glitch attack occurs, there will not be enough time to go through all those logic elements before the clock signal edge, which makes the outcome of a calculation necessarily wrong. A wrong calculation result thereby indicates a timing constraint violation and consequently a glitch attack. Checking whether the calculations match the expected result or not is, for example, performed by a matching circuit attached to a canary circuit 2 (not shown) or it is performed by the canary circuits 2 themselves.

[0094] Fig. 7 provides a schematic view on the integrated circuit of Fig. 2, with the difference that a glitch 20' is introduced only into the clock signal 4, when the

integrated circuit 100 suffers the glitch attack 200. Furthermore, the integrated circuit 100' is equipped with an anti-clock glitch canary circuit 2', providing a signal path 3' that is chosen such that the timing constraint of said canary circuit 2' is violated as a consequence of the glitch 20' present in the clock signal. The exemplary signal path 3' thereby provides a propagation time with enough time buffer to the timing constraint of the canary circuit 2' to be not yet violated by natural signal deviations or local chip variations but to be certainly violated by a clock-edge shift to an earlier time in the form of the voltage glitch 20'. Such a violation corresponds to the detection of a glitch attack on the clock input 14 of the integrated circuit 100.

[0095] Fig. 8 provides a schematic view on the integrated circuit of Fig. 2, with the difference that a glitch 20'' is introduced only into the voltage signal 5 in the course of a glitch attack 200. Furthermore, the integrated circuit 100 is equipped with an anti voltage-glitch canary circuit 2'', providing a signal path 3'' that is chosen such that the timing constraint of said canary circuit 2'' is violated as a consequence of the glitch 20'' present in the voltage signal. The exemplary signal path 3'' thereby provides a propagation time with enough time buffer to the timing constraint of the canary circuit 2'' to be not yet violated by natural signal deviations or local chip variations but to be certainly violated by a voltage drop in the form of the voltage glitch 20''. Such a violation corresponds to the detection of a glitch attack on the voltage input 15 of the integrated circuit 100.

[0096] Fig. 9 provides a schematic block diagram of an integrated circuit 100 equipped with both anti voltage-glitch canary circuits 3'' and anti clock-glitch canary circuits 3' to address a voltage glitch 20'' as well as a clock glitch 20'. The detection of a voltage or clock glitch by the canary circuits 3', 3'' triggers the actions as described in conjunction with Figs. 14, 15 and 16.

[0097] Fig. 10 is a schematic block diagram of an integrated circuit 100 equipped with a strict canary circuit 2b and a relaxed canary circuit 2a. In the scenario shown in Fig. 10 only the strict canary circuit 2b suffers a timing constraint violation but this is not the case for the relaxed canary circuit 2a, the timing constraint of which is aligned with the timing constraint of the functional circuit 1. This is interpreted as a glitch attack that has occurred but has not tempered with the functional circuit 1 (or the main logic 30 if identical) yet.

[0098] Hence, upon receiving the intrusion detection signal 7, the monitoring logic 8 causes a counteraction 70 to be performed by the main logic 30, such as those illustrated in Fig. 15.

[0099] Fig. 11 shows the integrated circuit of Fig. 12 in a different scenario. In this scenario the timing constraints both of the relaxed canary circuit 2a and the strict canary circuit 2b are violated. This is interpreted as a glitch attack being present which has most likely already tempered with the functional circuit 1 (which could also be identical to the main logic 30). In this scenario, counteractions are performed by the monitoring logic 8 itself. Examples for these counteractions are illustrated in Fig. 16.

[0100] Fig. 12 provides a schematic block diagram of an integrated circuit 100 with canary circuits 2 located close to a sensitive place of said integrated circuit 100.

[0101] In the integrated circuit 100 in which a canary circuit 2, providing a signal path 3 is located adjacent to the input of a cryptographic engine 50. The effects and reasons for such a placement of the cryptographic engine have been already discussed above.

[0102] Fig. 13 also provides a schematic block diagram of an integrated circuit 100 with canary circuits located close to a sensitive place of the integrated circuit 100.

[0103] In this example, the canary circuit 2, providing path 3, is located adjacent to a memory 60 on which a firmware signature is stored. The effect and the reason for this placement has also already been discussed above.

[0104] Fig. 14 provides a flowchart of a method of handling a glitch attack on an integrated circuit. At reference numeral S1 primary functions of an integrated circuit 100, such as encryption, reading out data etc., are performed. In this activity, signals propagate through at least one functional circuit 1.

[0105] It is continuously checked at reference numeral S2 if the timing constraints of the canary circuits is violated to detect possible glitch attacks 20. Checking if the timing constraint of the canary circuits is violated comprises checking whether calculation results obtained by the canary circuits 2 are equal to expected results. These

calculation results are obtained, for example, by standard logic gates as illustrated by Fig. 6.

[0106] When it is found out that the calculation results do not match the expected results at reference numeral S2.2, this is counted as a glitch attack 20 detected at reference numeral S2.4. If, however, the calculation results do match the expected result at reference numeral S2.3, this is counted as no glitch attack being detected at reference numeral S2.5.

[0107] In response to a glitch attack being detected at reference numeral S2.4 it is reacted to the glitch attack at reference numeral 20. Reacting to the glitch attack comprises sending an intrusion-detection signal 7 to the monitoring logic 8 at reference numeral S3.1.

[0108] Fig. 15 provides a flowchart of counteractions against a glitch attack 200. Counteractions 80 are triggered by the monitoring logic 8.

[0109] The counteractions 80 triggered by the monitoring logic 8 at reference numeral S3.2 comprise notifying the main logic 30. The main logic's 30 actions comprise at least one of (i) block access to the hard drive controller at reference numeral S3.2.1.1 and (ii) block access to the PCI controller or other subsystems at reference numeral S3.2.1.2 or other actions the block access to the integrated circuit or disable a part of the integrated circuit.

[0110] Fig. 13 provides a flow chart of different counteractions 80 triggered by the monitoring logic 8 at reference numeral S3.2.

[0111] Those counteractions are chip wide actions at reference numeral S3.2.2. Those chip-wide actions comprise at least one of (i) reset chip at reference numeral S3.2.2.1, (ii) hold chip at reference numeral S3.2.2.2 and (iii) a data wipe of the chip at reference numeral S3.2.2.3.

[0112] It is to be understood that the examples disclosed herein are provided for illustrative purposes and are not to be construed as limiting the scope of the present disclosure.

Claims:

1. An integrated circuit comprising:
A functional circuit to perform primary functions of the integrated circuit, wherein the functional circuit is to enable electrical signals to propagate through the functional circuit in accordance with a timing constraint of the functional circuit,
a canary circuit to be used in a detection of glitch attacks on the integrated circuit, where the canary circuit is to enable electrical signals to propagate through the canary circuit in accordance with a defined timing constraint of the canary circuit,
where the canary circuit is to provide a signal path designed such that in the event of the timing constraint of the functional circuit is violated due to a glitch attack, also the defined timing constraint of the canary circuit is violated.
2. The integrated circuit of claim 1, where the canary circuit is to send an intrusion-detection signal to a monitoring logic in response to the defined timing constraint of the canary circuit being violated and where the monitoring logic is to cause or to perform a counteraction against a glitch attack in response to receiving said intrusion-detection signal.
3. The integrated circuit of claim 1, where a plurality of canary circuits are distributed over the integrated circuit.
4. The integrated circuit of claim 1, wherein the canary circuit is implemented in a block of the integrated circuit which is separate to the functional circuit.
5. The integrated circuit of claim 1, wherein the integrated circuit comprises a plurality of canary circuits and at least a part of the canary circuits is to provide a signal path designed such that when the timing constraint of the canary circuit is violated, the timing constraint of the functional circuit is not yet violated.
6. The integrated circuit of claim 1, wherein the integrated circuit comprises a strict canary circuit, wherein the strict canary circuit provides a signal path such that when the timing constraint of the strict canary circuit is violated, the timing constraint of the

functional circuit is not yet violated and there is a relaxed canary circuit that provides a signal path with a signal propagation time closer to a signal propagation time of the functional circuit than a signal propagation time of the strict canary circuit.

7. The integrated circuit of claim 1, wherein the integrated circuit comprises a strict canary circuit, wherein the strict canary circuit provides a signal path such that when the timing constraint of the strict canary circuit is violated, the timing constraint of the functional circuit is not yet violated and there is a relaxed canary circuit that provides a signal path with a signal propagation time closer to a signal propagation time of the functional circuit than a signal propagation time of the strict canary circuit wherein when the timing constraint of the strict canary circuit is violated and the timing constraint of the relaxed canary circuit is not yet violated, the monitoring logic is to cause counteractions by informing an integrated circuit main logic and the integrated circuit main logic is to perform the counteraction against the glitch attack.

8. The integrated circuit of claim 1, wherein the integrated circuit comprises a strict canary circuit, wherein the strict canary circuit provides a signal path such that when the timing constraint of the strict canary circuit is violated, the timing constraint of the functional circuit is not yet violated and there is a relaxed canary circuit that provides a signal path with a signal propagation time closer to a signal propagation time of the functional circuit than a signal propagation time of the strict canary circuit, wherein when the timing constraint both of the strict canary circuit and the relaxed canary circuit is violated, the monitoring logic is to perform the counteraction against the glitch attack.

9. The integrated circuit of claim 1, where the canary circuit comprises standard logic gates and is to perform calculation operations

wherein a violation of a timing constraint of the canary circuit is deemed to have occurred in response to a result of the calculations not matching an expected result of the calculation.

10. The integrated circuit of claim 1, where a canary circuit comprises standard logic gates, including a succession of inverters, to perform calculation operations, where a violation of a timing constraint of the canary circuit is deemed to have occurred in

response to a result of the calculations not matching an expected result of the calculation.

11. The integrated circuit of claim 1, where the canary circuit is to provide a signal path as such that the timing constraint is violated as a consequence of a glitch present in a clock signal for the integrated circuit.

12. The integrated circuit of claim 1, where the canary circuit is to provide a signal path as such that the timing constraint is violated as a consequence of a glitch present in a voltage signal for the integrated circuit.

13. The integrated circuit of claim 1, where the integrated circuit comprises an anti clock-glitch canary circuit and an anti voltage-glitch canary circuit, wherein the anti clock-glitch canary circuit is to provide a signal path as such that the timing constraint is violated as a consequence of a glitch present in a clock signal for the integrated circuit and wherein the canary circuit is to provide a signal path as such that the timing constraint is violated as a consequence of a glitch present in a voltage signal for the integrated circuit.

14. The integrated circuit of claim 1, where the integrated circuit comprises a cryptographic engine and wherein the canary circuit is placed in the integrated circuit adjacent to at least one of the input and the output of said cryptographic engine, or where the integrated circuit comprises a storage medium on which a firmware-signature is stored and wherein the at least one canary circuit is placed adjacent to circuits for accessing said storage medium on which the firmware signature is stored.

15. A method of handling a glitch attack on an integrated circuit, the method comprising:

performing primary functions of the integrated circuit by a functional circuit, wherein the functional circuit enables electric signals to propagate through the functional circuit in accordance with a timing constraint of the functional circuit,

detecting a glitch attack, wherein detecting the glitch attack comprises:

checking whether or not a defined timing constraint of the canary circuit is violated, the canary circuit being a circuit comprised by the integrated circuit, wherein

the canary circuit enables electrical signals to propagate through the canary circuit in accordance with the defined timing constraint,

wherein the canary circuit provides a signal path designed such that in the event of the timing constraint of the at least one functional circuit is violated due to a glitch attack, also the defined timing constraint of the canary circuit is violated.

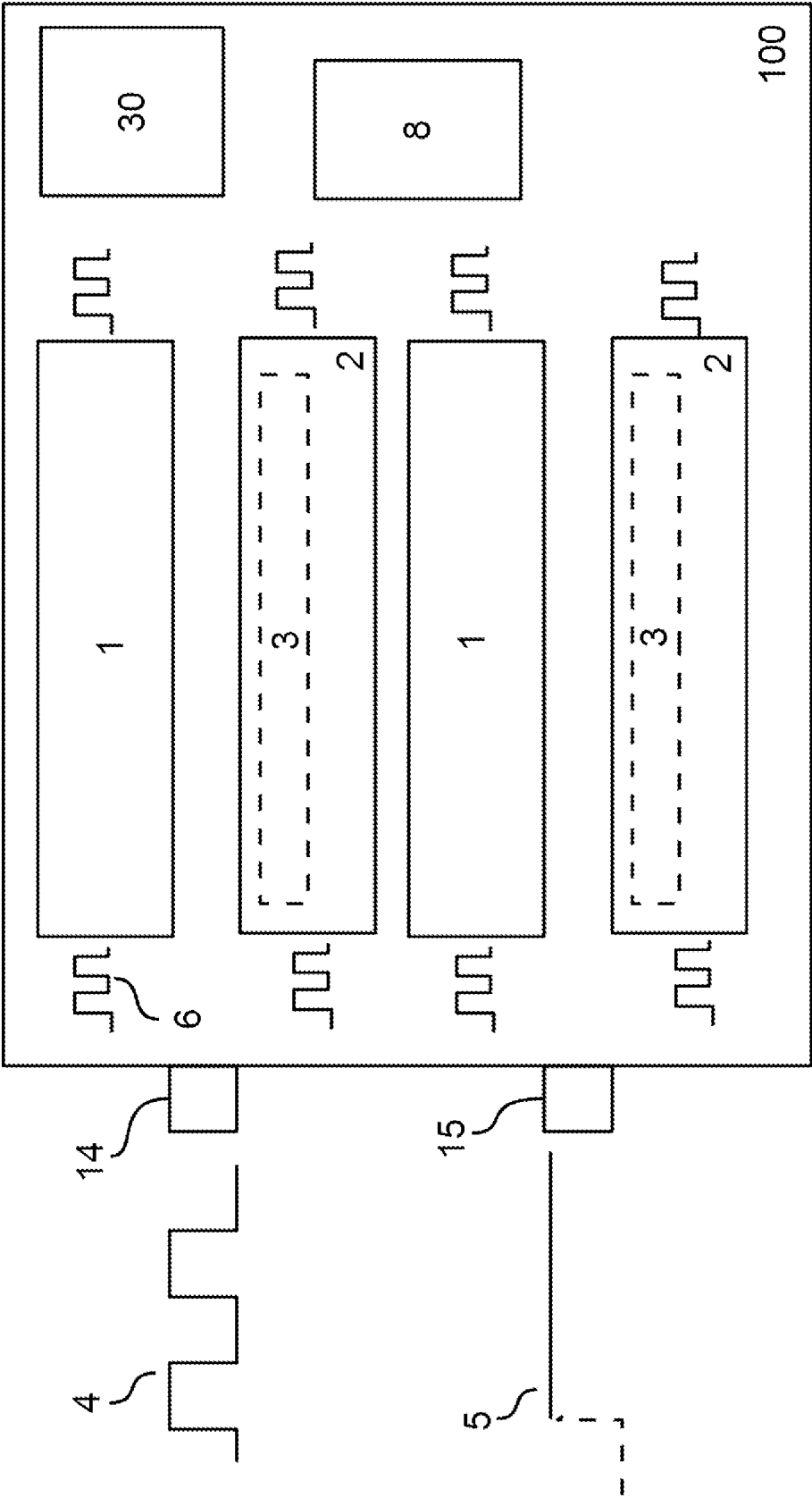


FIG. 1

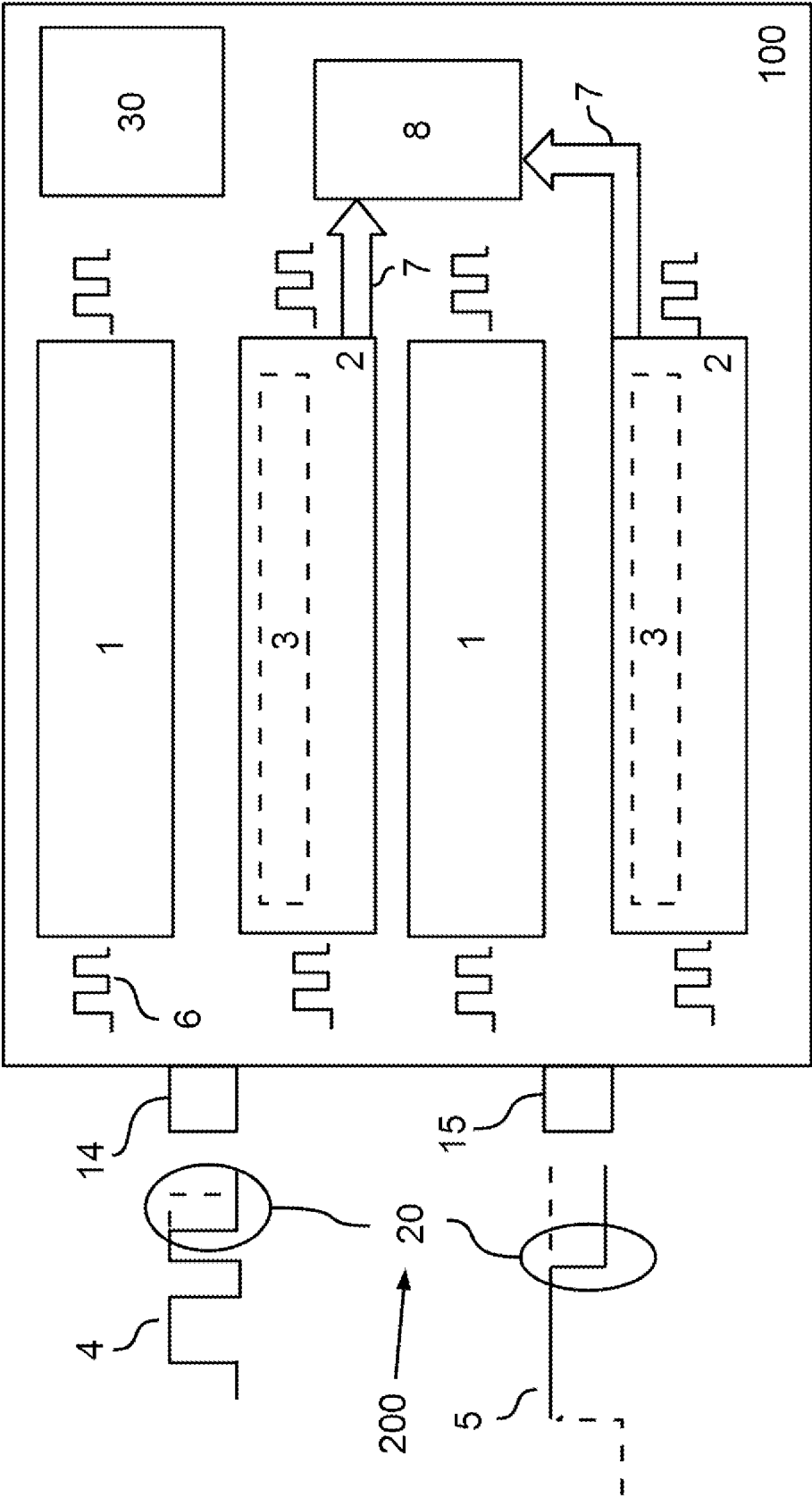


FIG. 2

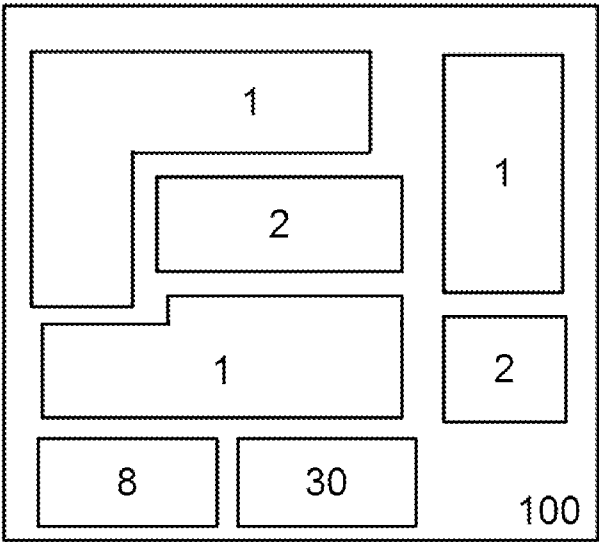


FIG. 3

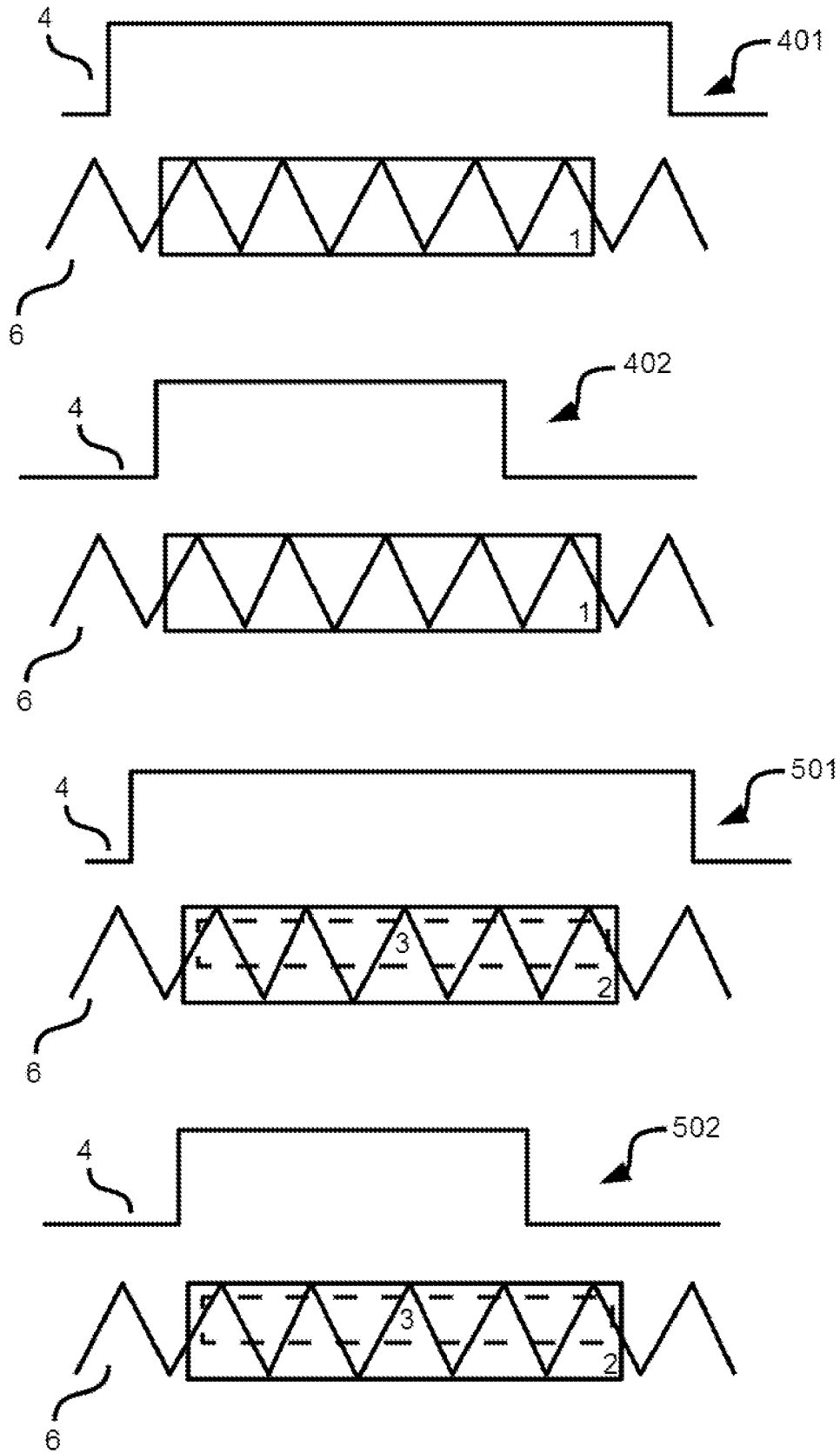


FIG. 4

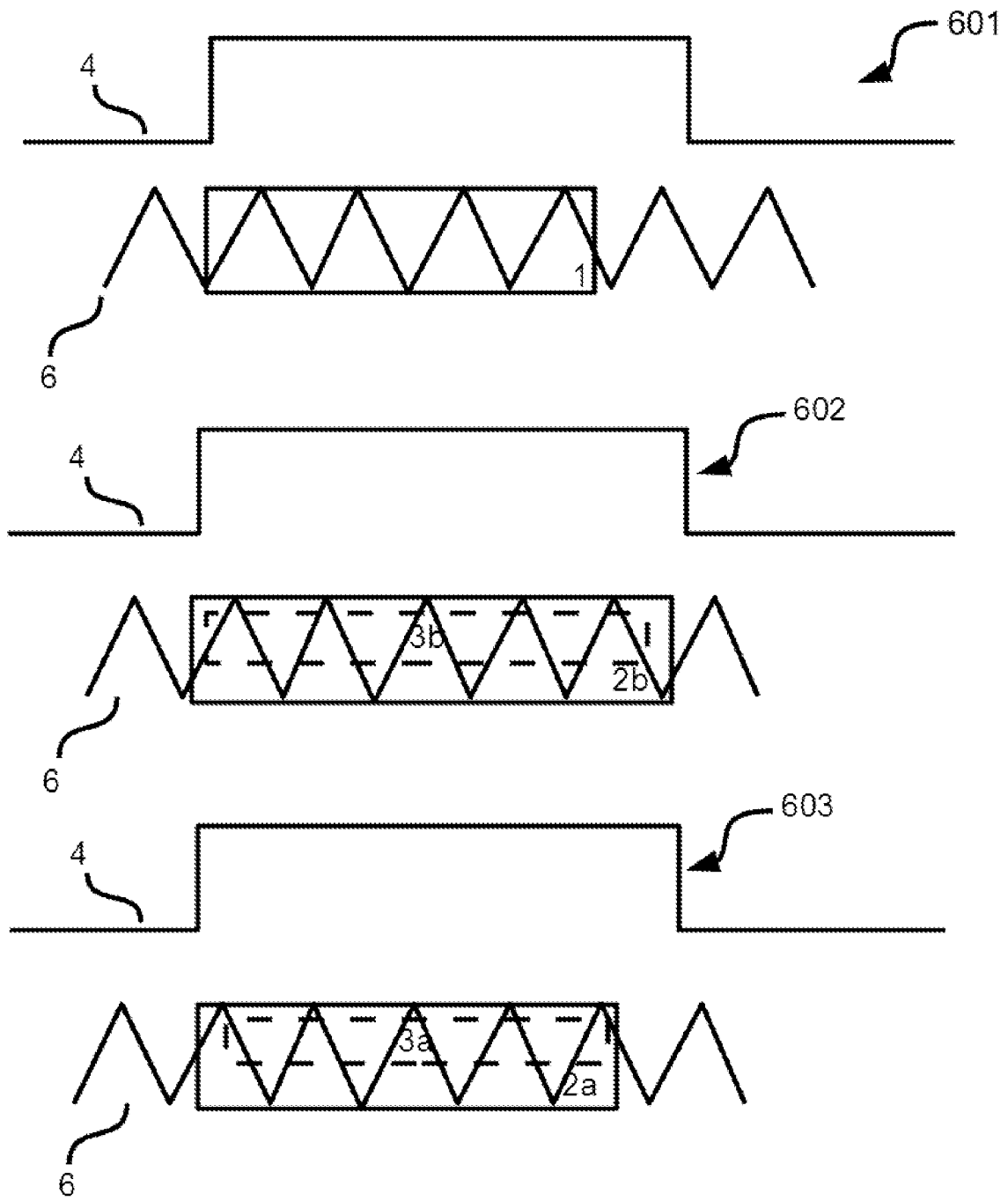


FIG. 5

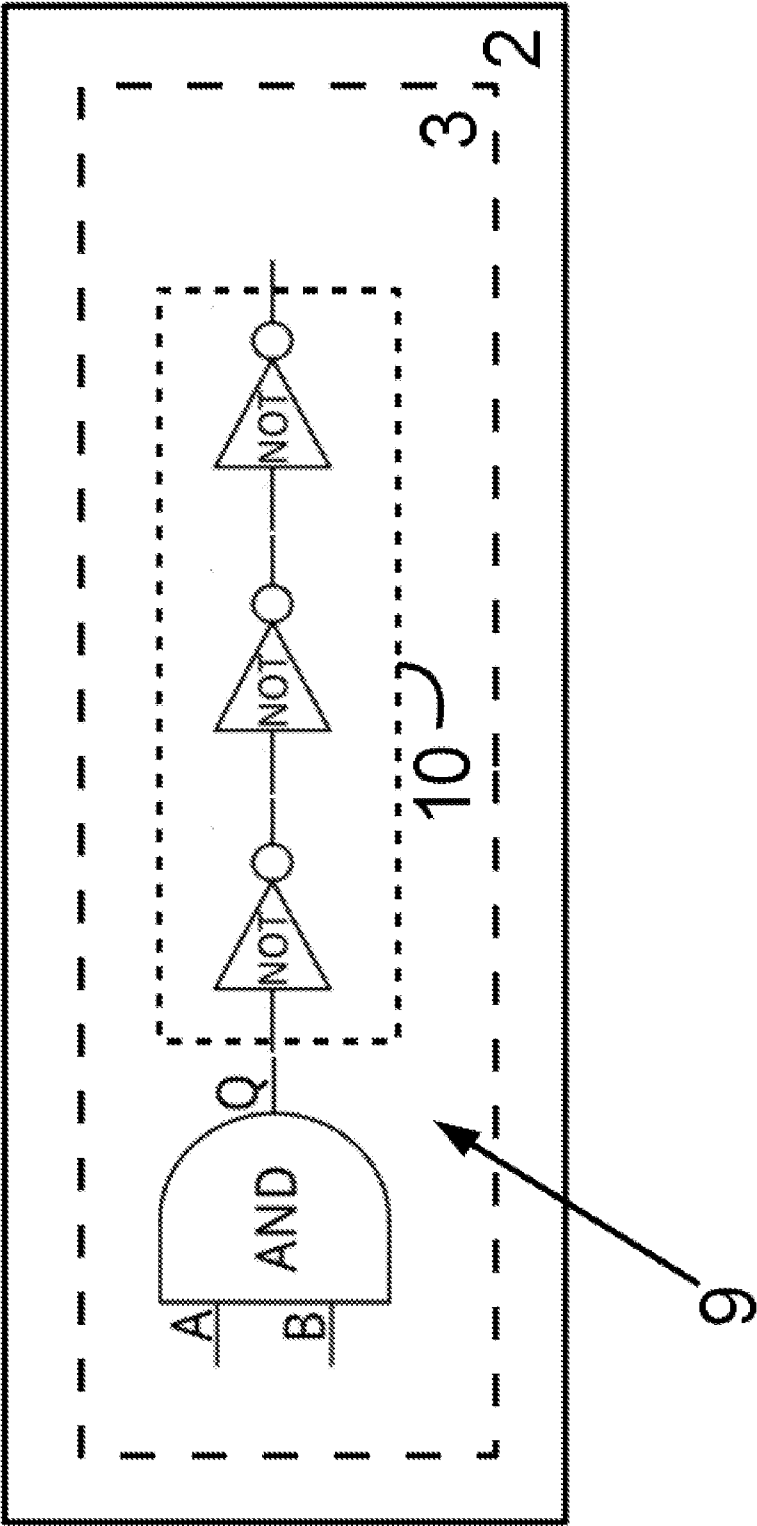


FIG. 6

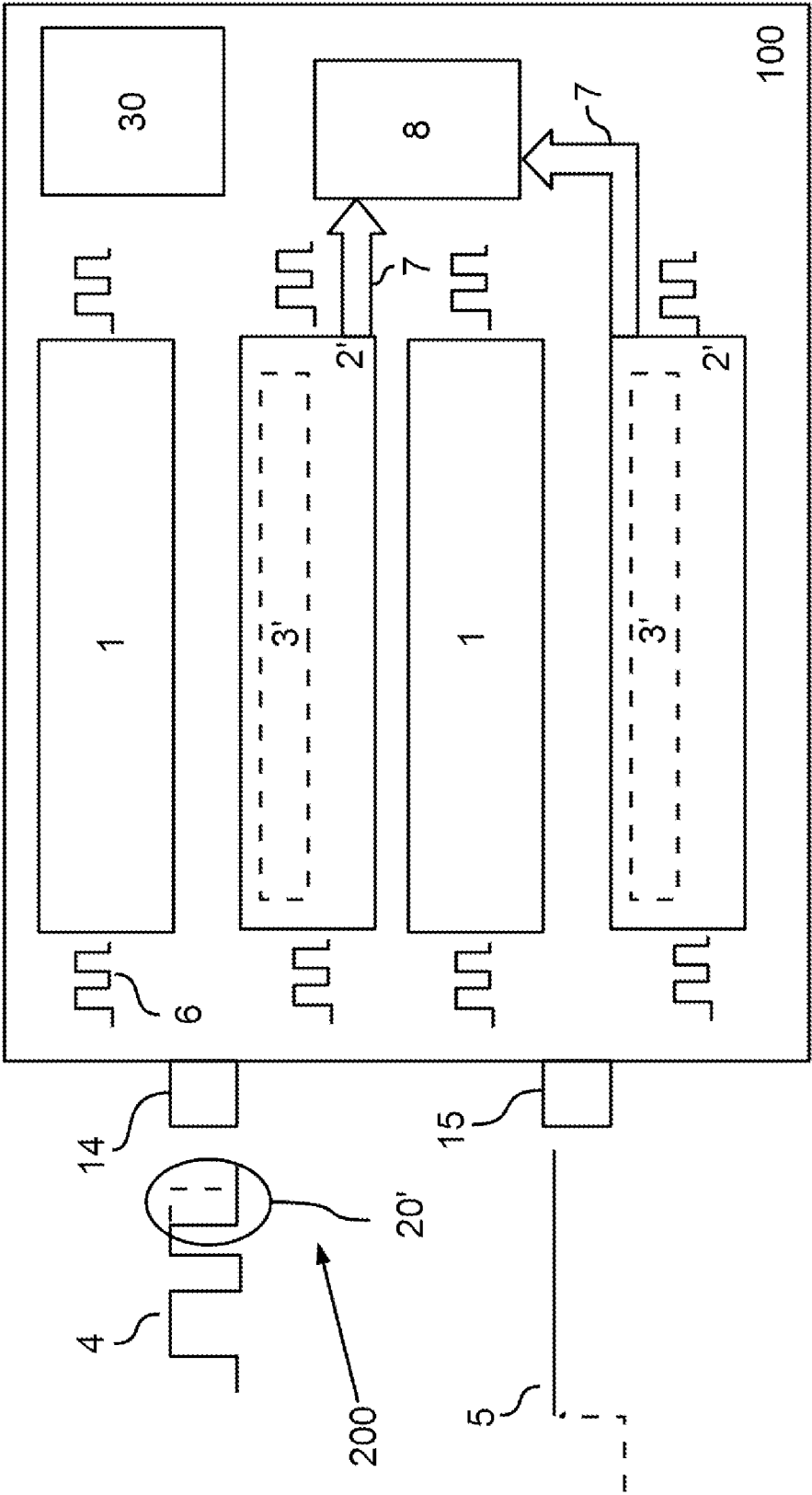


FIG. 7

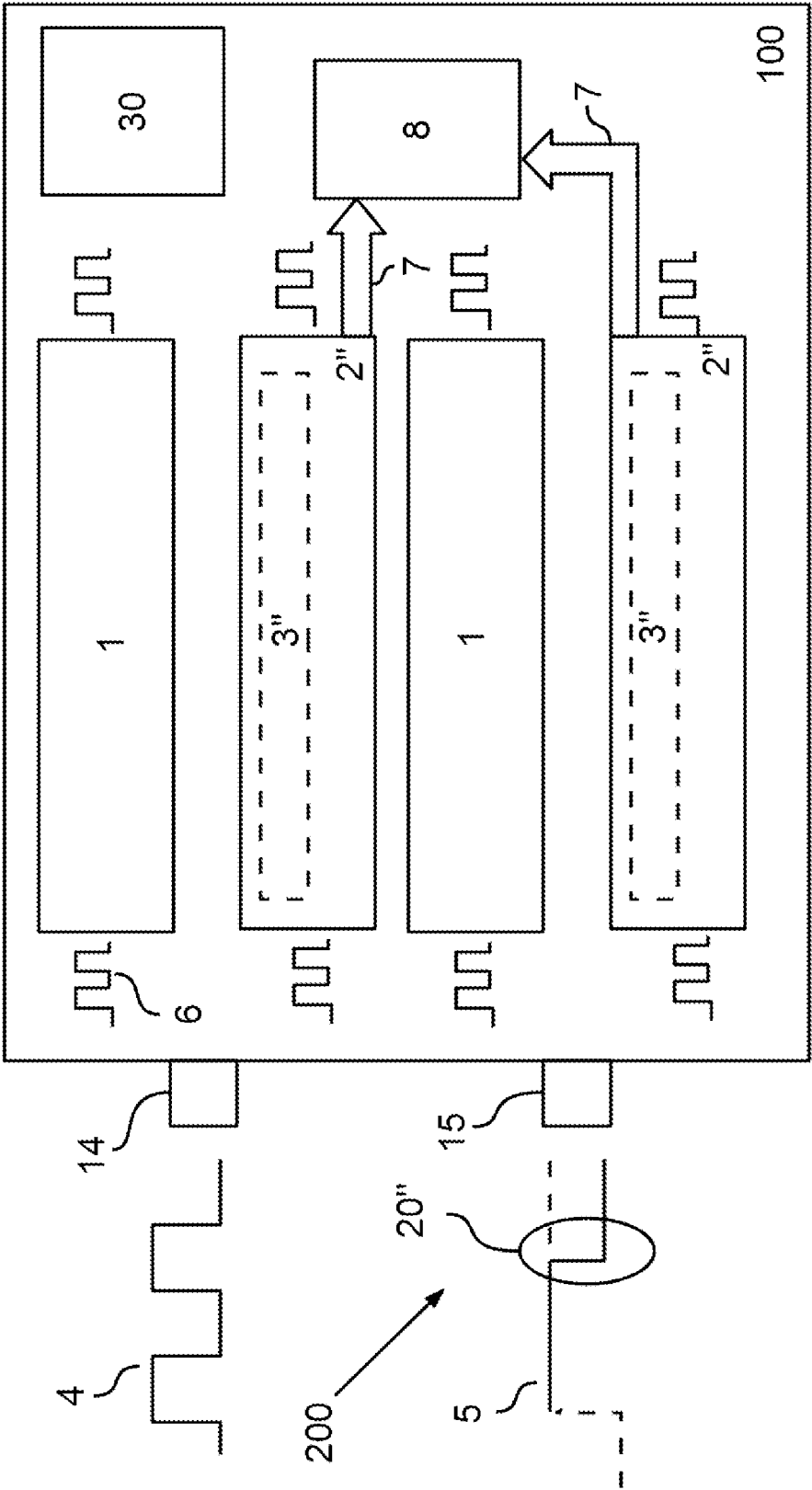


FIG. 8

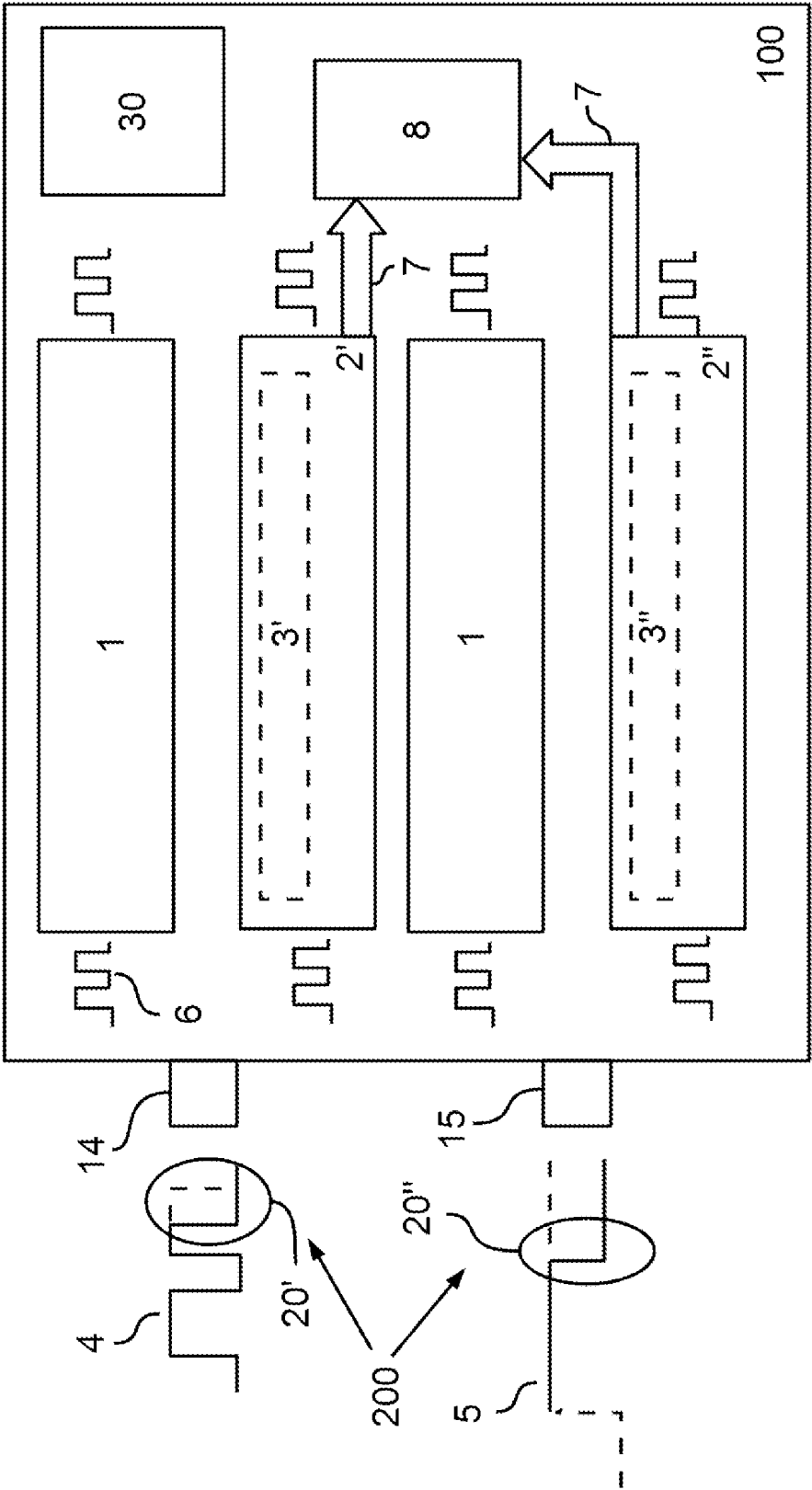


FIG. 9

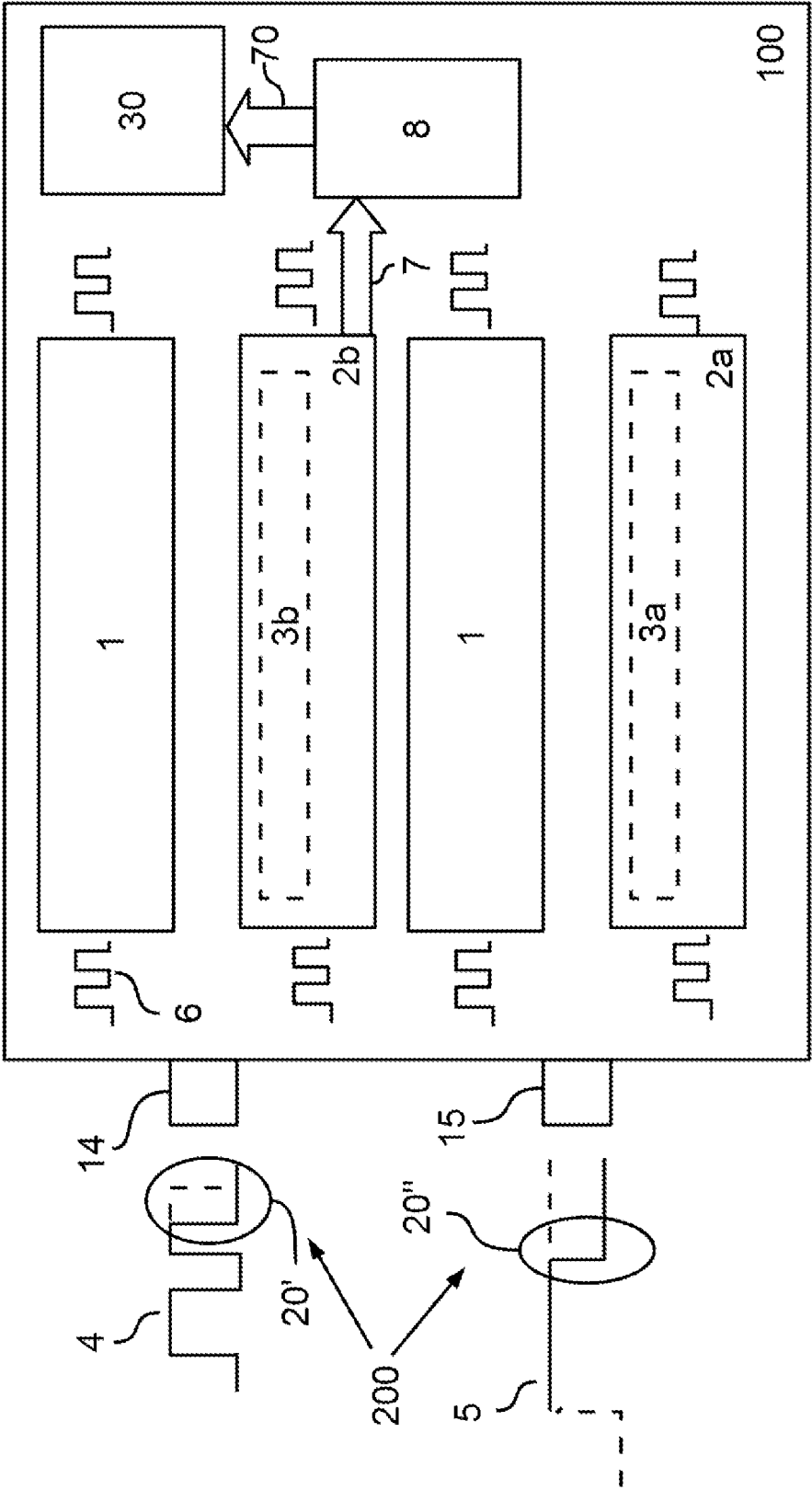


FIG. 10

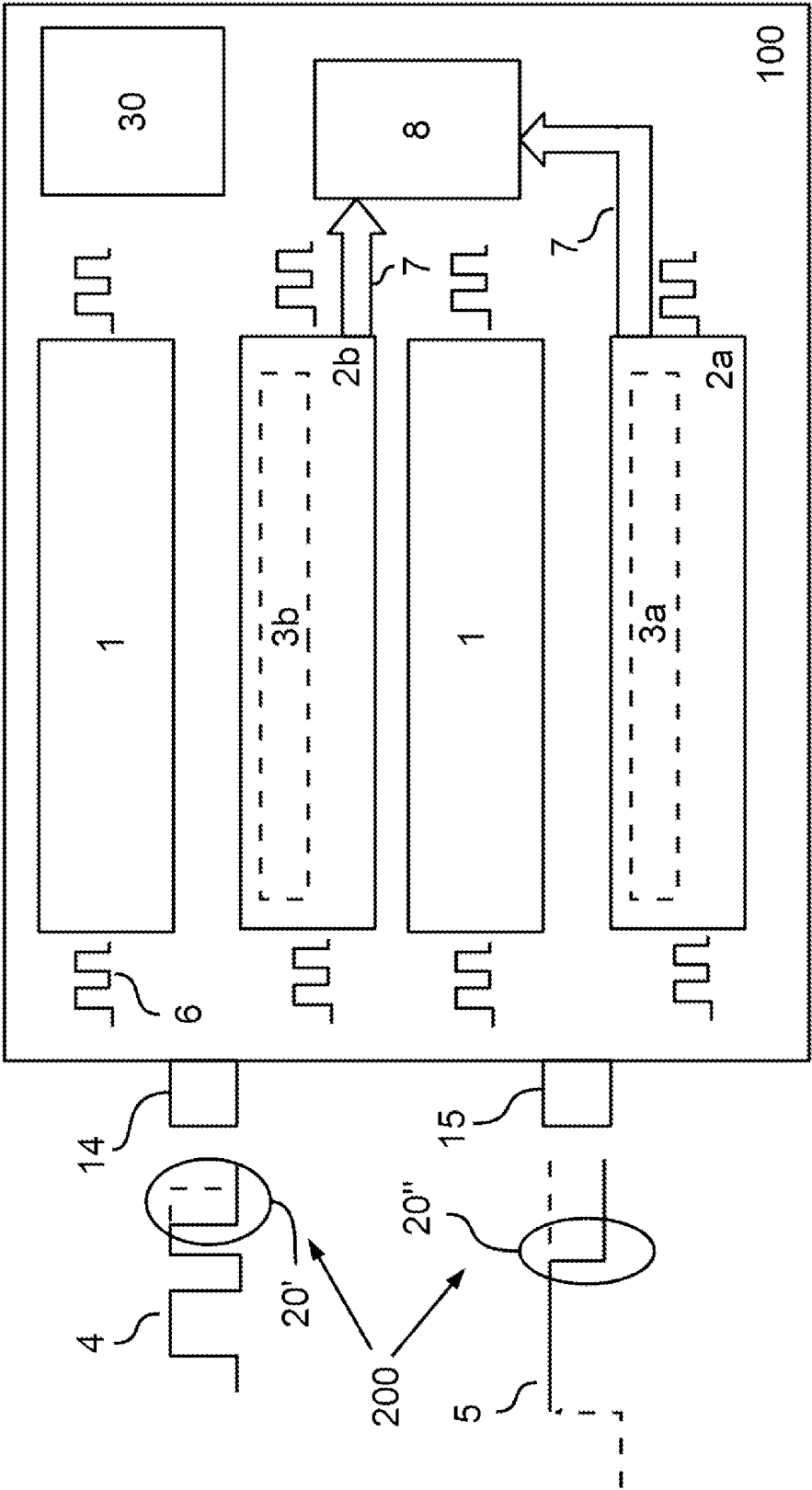


FIG. 11

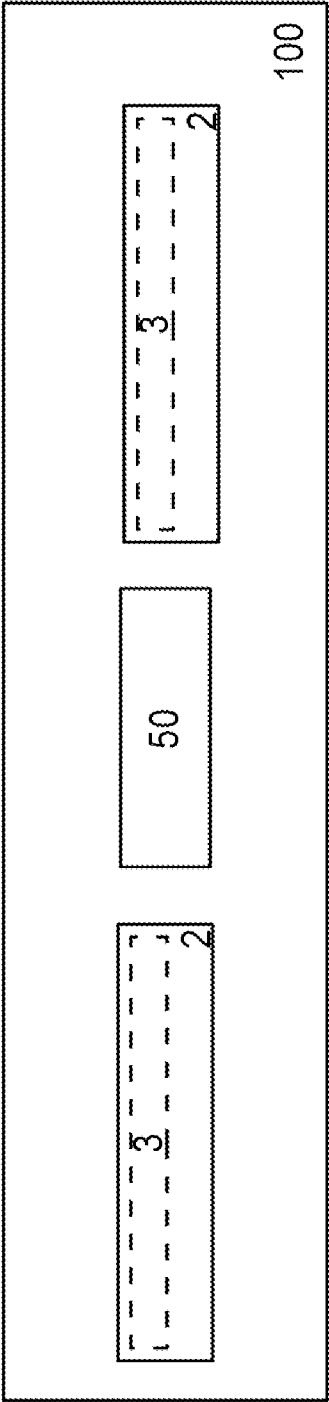


FIG. 12

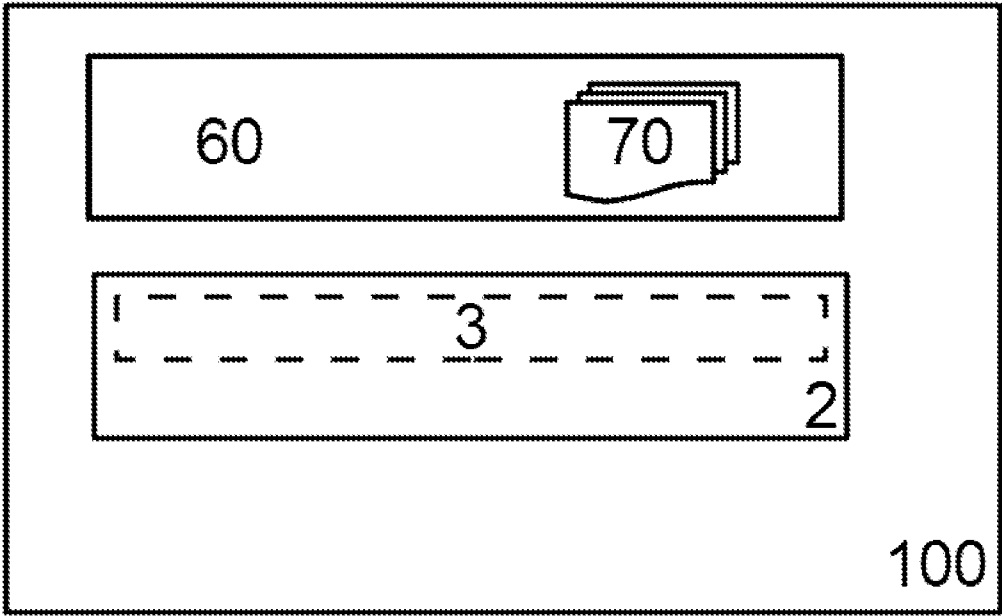


FIG. 13

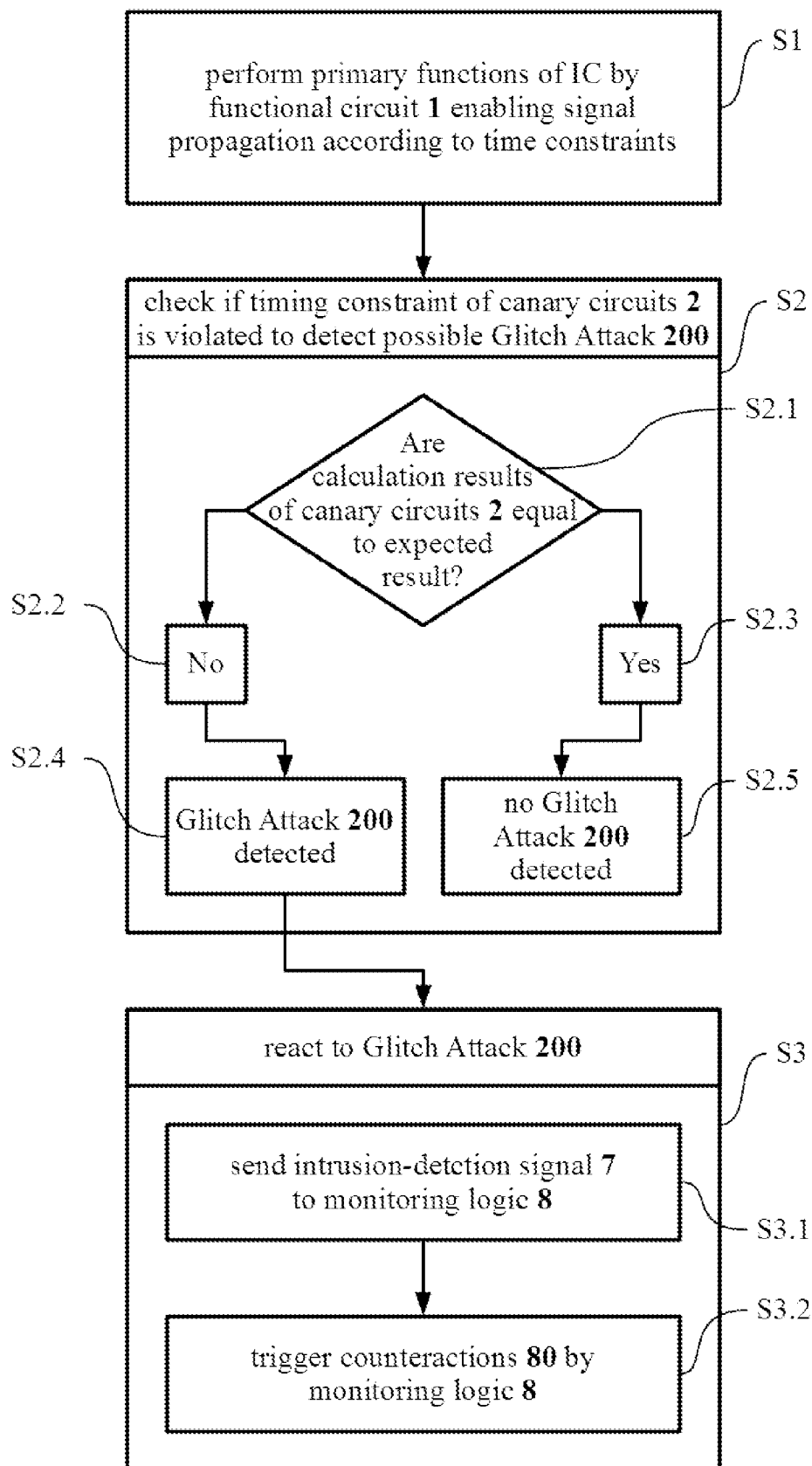


FIG. 14

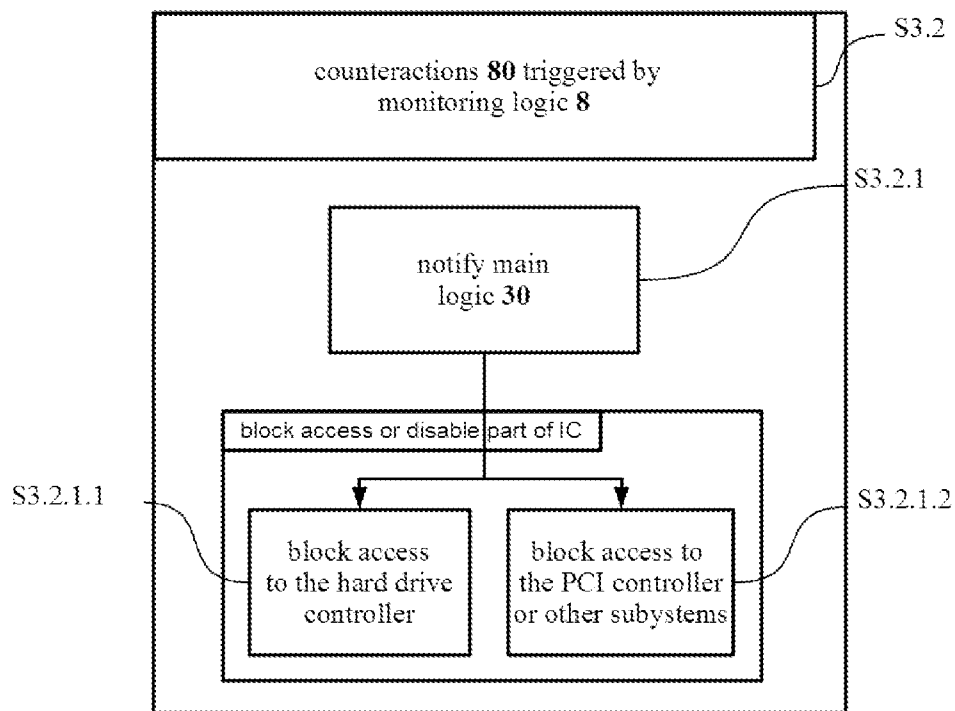


FIG. 15

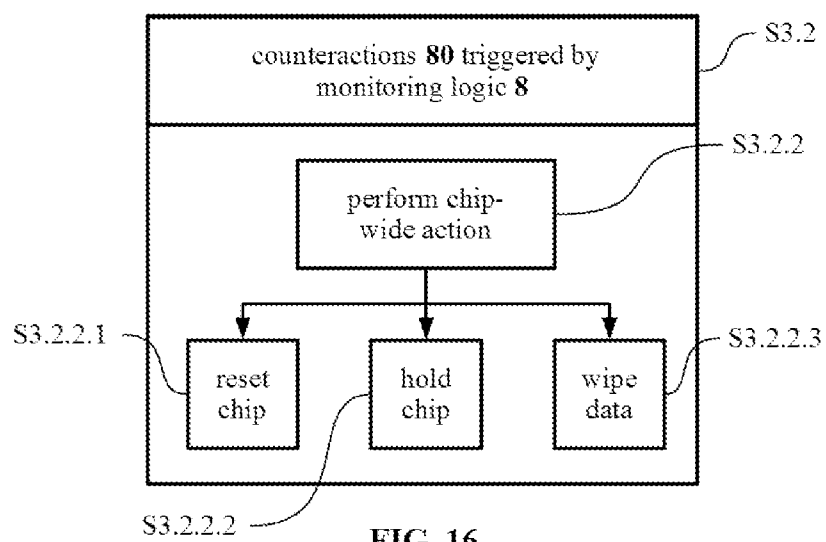


FIG. 16

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2018/057565

A. CLASSIFICATION OF SUBJECT MATTER <i>G06F 21/71 (2013.01)</i> <i>G06F 21/76 (2013.01)</i>		
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 21/00-21/76, B41J 2/00-2/05, G01R 35/00, 31/00-31/28, H04L 9/00, H04N 1/00-1/405, G06K 19/00-19/073, G11C 16/00-16/22, 5/00-5/14, H03K 17/00-17/22, 5/00-5/01, H01L 23/00-23/58, H03H 1/00-1/02		
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)		
PatSearch (RUPTO internal), USPTO, PAJ, Esp@cenet, DWPI, EAPATIS, PATENTSCOPE, Information Retrieval System of FIPS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/0052962 A1 (SILVERBROOK RESEARCH PTY LTD) 09.03.2006, abstract, [0643], [0896]-[0897], [1492], [1506]-[1510], [1534], [1544]-[1548], [1697], [4426]-[4428], [5189], [5222], [5386]	1-15
A	US 7085979 B2 (SAMSUNG ELECTRONICS CO LTD) 01.08.2006	1-15
A	CN 2718783 Y (SHANGHAI HUAHONG IC CO LTD) 17.08.2005	1-15
☐ 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	“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
“E”	earlier document but published on or after the international filing date	“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
“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)	“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
“O”	document referring to an oral disclosure, use, exhibition or other means	“&” document member of the same patent family
“P”	document published prior to the international filing date but later than the priority date claimed	
Date of the actual completion of the international search		Date of mailing of the international search report
15 July 2019 (15.07.2019)		08 August 2019 (08.08.2019)
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37		Authorized officer A. Tokarev Telephone No. (499) 240-25-91