



(51) International Patent Classification:

G06F 21/75 (2013.01) G09C 1/00 (2006.01)
G06F 21/87 (2013.01) H04L 9/00 (2006.01)

(21) International Application Number:

PCT/EP2021/069077

(22) International Filing Date:

08 July 2021 (08.07.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

20185298.5 10 July 2020 (10.07.2020) EP

(71) Applicant: NAGRAVISION S.A. [CH/CH]; 22-24, route de Genève, 1033 Cheseaux-sur-Lausanne (CH).

(72) Inventors: PELISSIER, Sylvain; c/o Nagravision SA, 22-24, route de Genève, 1033 Cheseaux-sur-Lausanne (CH). AUBRY, Pascal; c/o Nagravision SA, 22-24, route de Genève, 1033 Cheseaux-sur-Lausanne (CH).

(74) Agent: NOVAGRAAF INTERNATIONAL SA et al.; Chemin de l'Echo 3, 1213 Onex (CH).

(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, IT, 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.

(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))

(54) Title: INTEGRATED CIRCUIT DEVICE WITH PROTECTION AGAINST MALICIOUS ATTACKS

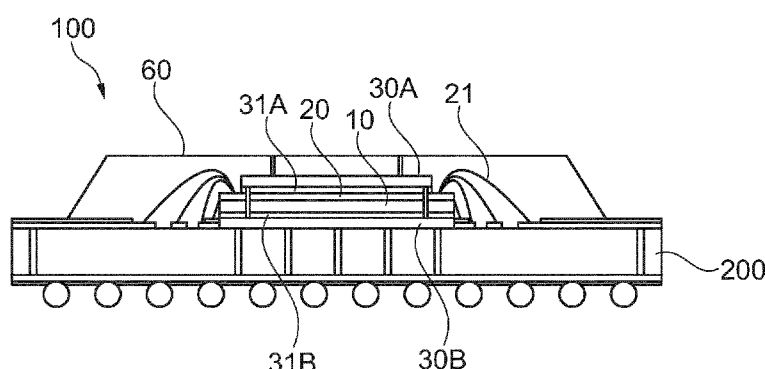


Fig. 1

(57) Abstract: Integrated circuit device with protection against malicious attacks The integrated circuit device (100) comprises a semiconductor substrate layer (10) and at least one active layer (20) including electronic components and supported by said semiconductor substrate layer (10). The semiconductor substrate layer (10) and the at least one active layer (20) are sandwiched between two protective layers (30A, 30B) acting as physical obstacles to prevent the passage of radiations. In addition, the two protective layers (30A, 30B) are electrically connected to a detection circuit (40) that can monitor an electrical information of the protective layers (30A, 30B) and detect a physical attack of at least one of the two protective layers (30A, 30B), based on the monitored electrical information.



INTEGRATED CIRCUIT DEVICE WITH PROTECTION AGAINST MALICIOUS ATTACKS

TECHNICAL FIELD

[0001] The present disclosure relates to the field of integrated circuit
5 protection against malicious attacks like side-channel attacks and fault attacks.

BACKGROUND

[0002] In computer security, security is typically provided by cryptographic algorithms that are designed to be extremely difficult to break mathematically.
10 Input and output messages are available to attackers, but the secret information (e.g. the secret key of an encryption algorithm) is not available. For well-studied algorithms, an attacker must perform a cryptanalysis requiring an unpractical amount of computational power to obtain the secret information.

15 [0003] However, it has been shown that hardware and software implementations of cryptographic algorithms or protocols are vulnerable to side channel attacks and fault attacks that do not require such a complex cryptanalysis. Both techniques can be used to obtain the secret information (e.g. secret key(s)) stored in an embedded device such as an integrated
20 circuit implementing cryptographic algorithm(s).

[0004] Side channel attacks are based on the principle that the secret information can leak through side channels. It can be defined as any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself. Side channels
25 are physical information leakages, for example the time needed to perform an encryption, the power consumed to the hardware implementation to execute an encryption algorithm, electromagnetic radiations emanating from the circuits executing the encryption or decryption, or even sound. The side

channel attacks have proven to be effective and require low cost and/or a reduced number of experiments.

[0005] Fault attacks consist in intentionally triggering computational faults in the cryptographic algorithms to obtain faulty outputs or fault behaviors, which
5 allow to obtain the secret information. Fault injections using for example a laser source or an electromagnetic source are used to alter the behavior of the cryptographic device and obtain information leakage under faulty environment. For example, Body Bias Injection (BBI) is a fault injection method that consists in applying a high voltage pulse on the circuit substrate
10 to induce faults.

[0006] WO 96/16378 A1 discloses a security device including a first integrated circuit having a memory area storing secret information and a second integrated circuit arranged above the first integrated circuit and covering the memory area (and any other sensible circuit) to form an obstacle
15 and prevent from access to the memory area. The two integrated circuits are joined together through an adhesive layer and are connected in order to communicate with each other. In operation, a periodical communication is established between the two integrated circuits to execute a mutual authentication procedure. If one of the two integrated circuits fails to
20 authenticate, the secret information is erased from the memory area. In order to access the memory area, an attacker needs to remove the second integrated circuit, which results in interrupting the connection between the two integrated circuits.

[0007] US 5,881,155 A discloses a security device for preventing access to
25 secret information stored in a semiconductor chip (protected chip) comprising a second semiconductor chip (protective chip). The two chips are coupled to each other by communication terminals. A semiconductor resin having a non-homogeneous resistivity is sandwiched between the protected chip and the protective chip. The protective chip has means that measure a plurality of
30 resistances through the resin and means for determining an encryption key

(“resistive key”) by processing the measured resistances. When the security device is initialized, the measuring means measure a certain number of resistances through the semi-conductor resin. The measured values of resistance are then processed to determine the resistive key that is
5 communicated to the protected chip through communication terminals in order to encrypt and decrypt information. In this configuration, a physical attack on the protected chip would not provide access the secret information (resistive key). In addition, it presupposes access to the active surface of the chip and therefore destruction of the semiconductor layer, which permanently
10 prevents from reconstruction of the resistive key.

[0008] WO 99/12204 A1 discloses a security integrated circuit comprising an active layer and a complementary layer, joined together through an intermediate sealing layer. The “active” layer includes a substrate sub-layer in a semi-conductor material and, above the substrate sub-layer, an active sub-
15 layer integrating electronic circuits and having memory. This active layer is thinned. The complementary layer is made of a semi-conductor material. The intermediate sealing layer is made of an electrically insulating material. When an attacker wants to access the integrated circuits, he needs to separate the complementary layer from the active layer by applying traction forces. As the
20 active layer is thinned and thus weakened, such traction forces would inevitably break the active layer, which would make impossible to extract the secret information.

[0009] The security devices of the prior art are complicated to implement and design. Moreover, they provide a protection against physical attacks only
25 from one side of the chip. However, it has recently been shown that attacks from both sides of the chip are feasible. Furthermore, the security devices of the prior art are designed to prevent reading secret information from memory but not to provide an efficient protection against side-channel attacks, electromagnetic fault attacks or body biasing injection attacks.

30 [0010] There is a need to improve the situation.

SUMMARY

[0011]The present disclosure concerns an integrated circuit device comprising a semiconductor substrate layer and at least one active layer including electronic components and supported by said semiconductor substrate layer, characterized in that the semiconductor substrate layer and the at least one active layer are sandwiched between two protective layers acting as physical obstacles to prevent the passage of radiations and electrically connected to a detection circuit for monitoring an electrical information of the protective layers and detecting a physical attack of at least one of the two protective layers, based on the monitored electrical information, in order to protect the at least one active layer against a malicious attack,

[0012]According to the present disclosure, the integrated circuit device uses a protection or shield layer on both sides of the chip (integrated circuit). The two protective layers act as physical obstacles that prevent the passage of internal and/or external radiations. Such a configuration creates a protection that can be compared to a “Faraday cage” effect. It prevents from intrusive attacks using radiations, for example a laser beam or an electromagnetic glitch, coming from both sides of the chip. It also prevents from side-channel attacks based on the detection of the electromagnetic radiations emanating from the active layer(s).

[0013]Additionally, in case that an attacker tries to get rid of all or part of one of the protective layers, the detection circuit detects the attack based on the monitored electrical information of the protective layers, and triggers an electronic countermeasure of protection, for example a memory wipe.

[0014]Thus, in the present disclosure, the protective layers act as physical shields to protect the integrated circuit(s) against attacks using radiations and are also used as a trigger to activate an electronic countermeasure of protection in case that the integrated circuit device is physically attacked by digging a protective layer. Thus, the present disclosure combines a physical

protection and an electronic countermeasure of protection, both allowing to protect the active layer(s) against malicious attacks. The physical protection is actually used as a trigger to execute the electronic countermeasure.

[0015] Advantageously, the detection circuit is integrated within the at least
5 one active layer.

[0016] The integrated circuit device can further comprise an electronic protection circuit configured to generate a signal for executing an electronic protection countermeasure when a physical attack is detected by the detection circuit.

10 [0017] Advantageously, the electronic protection circuit is integrated within the at least one active layer.

[0018] The two protective layers can be configured to prevent the passage of internal and external radiations of the group including laser radiations, electromagnetic emanations from the at least one active layer,
15 electromagnetic radiations produced by an external source (i.e. external to the integrated circuit device).

[0019] The two protective layers can be made of metal, or metal alloy, or a semi-conductor material.

[0020] In a first embodiment, the integrated circuit device is designed for wire
20 bonding.

[0021] In a second embodiment, the integrated circuit device is a flip chip system.

[0022] One of the two protective layers or each of the two protective layers can be a full plate.

25 [0023] In a first variant, one of the two protective layers or each of the two protective layers is made of a bent continuous wire forming parallel lines. Optionally, this bent continuous wire can be supported by a printed circuit board.

[0024] In another embodiment, the protective layers comprise a mosaic of elementary plates electrically connected to the detection circuit.

[0025] The detection circuit can be configured to measure a relative value between respective electrical values of the two protective layers.

- 5 [0026] In a first example, the detection circuit is configured to measure a capacitance between the two protective layers, as said electrical information of the two protective layers.

- [0027] In a second example, the detection circuit is configured to measure a difference of electrical resistance between the two protective layers, as said
10 electrical information of the two protective layers.

[0028] The detection circuit is configured to detect a deviation of the monitored electrical information from a reference value, out of a tolerance range.

- [0029] Optionally, the two protective layers are joined to the semiconductor
15 substrate layer and the at least one active layer, through two respective joining layers functioning as electrical insulators.

[0030] The present disclosure also concerns a product including an integrated circuit device.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0031] Other features, purposes and advantages of the disclosure will
20 become more explicit by means of reading the detailed statement of the non-restrictive embodiments made with reference to the accompanying drawings.

[0032] Figure 1 shows an integrated circuit device according to a first embodiment.

- [0033] Figure 2 shows an integrated circuit device according to a second
25 embodiment.

[0034] Figure 3 shows an electronic circuit providing an electronic protection to the integrated circuit device.

[0035] Figures 4A, 4B show a first variant of the integrated circuit device according to the first embodiment.

- 5 [0036] Figure 5 shows second variant of the integrated circuit device according to the first embodiment.

[0037] Figure 6 shows a third embodiment of the integrated circuit device.

[0038] Figure 7 is an organigram illustrating the operation of the integrated circuit device according to the first embodiment.

DETAILED DESCRIPTION

- 10 [0039] The present disclosure concerns an integrated circuit device that is designed to provide protection against malicious attacks, especially side channel attacks and fault attacks.

- [0040] An integrated circuit device is a mix of hardware and software implementations that can be designed to execute cryptographic algorithms
15 and/or protocols. These hardware and software implementations are vulnerable to side channel attacks and fault attacks (e.g. fault attacks with a laser beam or glitch electromagnetic attacks). Such attacks can be based on the use of radiations to inject a fault into the integrated circuit device and alter its behavior, or on the detection of radiations emanating from the circuit(s).
- 20 The present disclosure aims to provide protection against attacks using an external source of radiation(s) (e.g. laser or electromagnetic glitch) directed towards the circuit(s) and attacks based on the detection of radiations emanating from the circuit(s).

- [0041] As well known by the person skilled in the art, the integrated circuit
25 device 100 comprises a plurality of overlapping layers including a semiconductor substrate layer 10 and at least one active layer 20. The semiconductor substrate layer 10 is made of a semiconductor material. The

active layer(s) 20 include electronic components, such as semiconductor components. They also include conductive track(s). One or more electronic circuits or devices can be integrated in these active layer(s).

[0042] In the present disclosure, the semiconductor substrate layer 10 and
5 the active layer(s) 20 are sandwiched between two protective or 'shield' layers 30A, 30B acting as physical obstacles to prevent the passage of internal and external radiations. The protective layers are disposed on both sides (top and bottom in figure 1 or 2) of the stack of layers 10, 20. They constitute additional overlapping layers. These protective layers are designed
10 to prevent passage of radiations, such as laser radiations and electromagnetic radiations. They produce an effect that can be compared to a 'Faraday cage' effect for protecting the integrated circuit device 100 (especially the active layer(s)). For example, a laser beam emitted by an external source (i.e. external to the integrated circuit device) and directed
15 towards the integrated circuit device hits one of the protective layers and is blocked by this protective layer. In case of an electromagnetic fault injection on one side of the integrated circuit device, the electromagnetic field hits the protective layer arranged on this side and is distributed over it like a Faraday cage, without disrupting the active layer(s). Furthermore, the protective layers
20 absorb radiations coming from the circuit(s) such as the electromagnetic emanations from the circuit(s). As a result, it is very difficult, or even impossible, to obtain a secret information by a side channel attack.

[0043] The thickness of each protective layer 30A, 30B can be adapted to provide an efficient protection. Its value can depend on one or more
25 parameters such as the material of the protective layer and a required size for the integrated circuit device and be determined experimentally. For example, this thickness can be comprised between 50 and 200 μm for a given material of the protective layers, in order to offer a good protection and a reduced size. However, for another material, a lesser thickness (e.g. 30 μm) could be
30 efficient too. A thickness higher than 200 μm could also be applied, if there is

no requirement on the size of the integrated circuit device. For example, the thickness of each protective layer could be equal to 500 μm .

[0044] The protective layers 30A, 30B can be made of a metal, for example copper or aluminum or gold or platinum. Alternatively, they are made of a metal alloy, such as stainless steel (e.g. 300 grade stainless steel), or a semiconductor material.

[0045] The protective layers 30A, 30B offer a strong passive protection against side channel attacks, laser attacks and electromagnetic attacks such as electromagnetic fault attacks and Body Biased Injection attacks. Indeed, these shield layers 30A, 30B retain most, if not all, of the electromagnetic emanations on both sides of the integrated circuit device 100, rendering very difficult to acquire side-channel data. They also retain any laser beam directed towards the active layer(s), and most of the electromagnetic signals or needles towards the active layer(s), rendering very difficult to disturb the integrated circuit operation.

[0046] Joining or interface layers 31A, 31B can be interposed between the protective layers 30A, 30B, respectively, and the layers 10 and 20, in order to facilitate the adhesion of the protective layers. These joining layers 31A, 31B have the function of joining the protective layer 30A with the active layer(s) 20 and the protective layer 30B with the semiconductor substrate layer 10. They can be made of a specific glue, well known by the person skilled in the art. The material of the joining layers can be an electrically insulating material, as well known by the person skilled in the art. The protective layers 30A, 30B could be joined to the layers 10 and 20 in another way.

[0047] The protective layers 30A, 30B are electrically connected to a detection circuit 40, as schematically represented in figure 3. This detection circuit or device 40 has the function of monitoring an electrical information of the protective layers 30A, 30B and detecting a physical attack of at least one of the two protective layers 30A, 30B, based on the monitored electrical information. The detection circuit 40 is integrated in the active layer(s) 20 of

the integrated circuit device 100. Each protective layer 30A, 30B is connected to the detection circuit 40 through one or more TSV (Through Silicon Via).

[0048] More precisely, the detection circuit 40 can be configured to monitor a relative electrical value between the two protective layers 30A, 30B. Such a relative value is expected to remain constant, or almost constant, over time. In particular, a change of temperature of the integrated circuit device 100 should not have an impact on this relative value.

[0049] The relative electrical value can be a capacitance between the two protective layers 30A, 30B. Alternatively, the relative electrical value can be a difference of electrical resistances between the two protective layers.

[0050] The detection circuit 40 is configured to measure this relative electrical value between the two protective layers 30A, 30B, and monitor it by determining whether or not it remains constant, or almost constant, over time in order to detect a physical attack. To this end, a tolerance range including a reference value can be used by the detection circuit 40. A variation of the monitored relative electrical value within this tolerance range can be accepted, while a variation of the monitored relative electrical value out of the tolerance can be detected as a physical attack by the detection circuit 40. In other words, if the measured relative electrical value is within this tolerance range, it is considered to remain constant (or almost constant) and no physical attack is detected. But, if the measured relative electrical value is out of the tolerance range, it is considered not to remain constant and a physical attack is detected. The tolerance range could be characterized by experiments in order to allow an efficient detection of attacks and avoid false detections. For example (only), a variation of plus or minus 10% compared to a reference value, can be tolerated (considered as "almost constant"). However, this value of $\pm 10\%$ is only an example. Another tolerance range could be determined as appropriate, for example $\pm 5\%$ or $\pm 30\%$ compared to the reference value, or any other values determined experimentally suitable for efficient detection of attacks and avoidance of false detections.

[0051] The integrated circuit device 100 further comprises an electronic protection circuit 50, as represented in figure 3. This protection circuit 50 is connected to the detection circuit 40. In operation, when the integrated circuit device is physically attacked, by digging one of the protective layers 30, this
5 physical attack is detected by the detection circuit 40 and signaled to the protection circuit 50. Consequently, the protection circuit 50 generates a control signal for executing an electronic protection countermeasure. For example, the control signal is a command to erase one or more memories, or to block the operation (functioning) of the integrated circuit device, or any
10 other countermeasure intended to protect secret or sensible information of the integrated circuit device 100.

[0052] Thanks to the detection circuit 40 and protection circuit 50, the protective layers 30A, 30B are not only used as a passive protection to block laser or electromagnetic signals going into the integrated circuit (chip) or
15 electromagnetic emanations outside the chip but also as components that trigger an active countermeasure when the integrated circuit device 100 undergoes a physical attack and the attacker tries to get rid of all or part of one of the protection layers 30A, 30B.

[0053] The integrated circuit device 100 can also comprise a mold cap 60
20 covering the set of overlapping layers 10, 20, 30A, 30B, 31A, 31B.

[0054] The integrated circuit device 100 can be supported by a carrier 200. This carrier 200 can support conductive tracks to which the circuit(s) of the integrated circuit device 100 are connected. Such a configuration allows a redistribution of the conductive tracks in order to facilitate the connection of
25 the integrated circuit device 100 to other electronic devices. This carrier 200 can be supported by another larger carrier (not represented) supporting other electronic components or devices. The electrical connection between the carrier 200 and the larger carrier can use solder ball terminals, as shown in figures 1 and 2.

30 **First Embodiment**

[0055] Figure 1 shows a first embodiment of the integrated circuit device 100 that is designed for wire bonding. The integrated circuit device 100 is a wire-bond package. This embodiment is compliant with the above disclosure. The characteristics specific to this first embodiment will now be described with
5 reference to figure 1.

[0056] As the first embodiment of the integrated circuit device 100 is designed for wire bonding, a plurality of connection wires 21, for example in Au, connect the circuit(s) of the active layer(s) 20 to conductive tracks supported by the carrier 200 for a redistribution of the connections, as well known by the
10 person skilled in the art. The layers of the integrated circuit device 100 overlap each other from the carrier 200 to the mold cap 60 (i.e., from bottom to top in figure 1), in the following order: protective layer 30B, joining layer 31B, semiconductor substrate layer 10, active layer(s) 20, joining layer 31A and protective layer 30A.

15 [0057] According to the first embodiment, the protective layers 30A, 30B are two plates, advantageously two full plates.

[0058] The operation of the integrated circuit device 100 (for example the one represented in figure 1) will now be described with reference to figure 7.

[0059] The two protective layers 30A, 30B act as physical obstacles to
20 prevent the passage of radiations. They prevent the passage of radiations, such as a laser beam or electromagnetic radiations. In case that an attacker attacks the integrated circuit device 100 by directing a laser beam towards the active layer(s) from an external laser source, this laser beam is stopped by one of the protective layers 30A, 30B. In case of a glitch electromagnetic
25 attack from one side of the integrated circuit device 100, the electromagnetic field generated in the vicinity of the protective layers 30 disposed on this side is blocked by this protective layer and does not disturb the active layer(s) 20. Furthermore, in case of a side channel attack, the protective layers 30A, 30B stop the electromagnetic emanations generated by the circuit(s) in operation,

in such a way that an attacker cannot capture these electromagnetic emanations in order to obtain secret information.

[0060] The detection circuit 40 measures a relative electrical value between the two protective layers 30A, 30B, in a step S1. Such a monitoring can be
5 done over the lifetime of the integrated circuit device 100 when the integrated circuit device 100 is powered. For example, the two protective layers 30A, 30B are considered as two capacitors and the difference C between the respective capacitance values of the two protective layers 30A, 30B is measured. As the measured electrical value is a 'relative' value between the
10 two protective layers, it is expected to be constant (or almost constant) over time. Even if the temperature increases both capacitors will be similarly impacted. It should not be modified by a change of temperature. However, a small variation could be tolerated within a tolerance range with respect to a reference value (for example plus or minus 10% with respect to the reference
15 value). In a step of monitoring S2, the measured relative electrical value (e.g. difference of capacitances C) between the two protective layers 30A, 30B is monitored in order to determine whether or not it deviates from the reference value referenced as ' C_0 ' out of the tolerance range. The detection circuit 40 determines if the measured relative electrical value C remains constant
20 compared to the reference value C_0 or within the predefined tolerance range. If so (branch Y in figure 7), the detection device 40 repeats the steps S1 and S2. No physical attack is detected.

[0061] In case of a physical attack of the integrated circuit device 100, the attacker should dig into at least one of the two protective layers before
25 accessing the active layer(s). In that case, the detection circuit 40 detects that the measured relative electrical value C changes and deviates from the reference value out of the tolerance range, in the step S2 (branch N in figure 7). As a result, the detection circuit 40 generates an alert signal, in a step S3, and transmits it to the electronic protection circuit 50, in a step S4. For
30 example (only), an alert signal is generated by the detection circuit 40 when

the monitored relative electrical value increases or decreases by more than 10% compared to the reference value.

[0062] Upon reception of the alert signal, the electronic protection circuit 50 controls the execution of an electronic countermeasure to protect the integrated circuit device 100, in a step S5. The countermeasure can be one or more of the following actions: erasing one or more memories of the integrated circuit device 100, blocking the operation of the integrated circuit device 100, or any other electronic countermeasure known by the skilled person.

[0063] Instead of the capacitance, the difference between the respective resistance values of the two protective layers 30A, 30B could be measured and monitored. Alternatively, any other electrical property of the two protective layers 30A, 30B that is expected to remain constant or almost constant over time, even in case of a change of temperature, could be measured and monitored by the detection circuit 40.

[0064] As previously explained, the protective layers 30A, 30B provide a physical and passive protection against attacks like side-channel attacks and fault attacks. As a result, an attacker needs to get rid of all or part of at least one of the two protective layers 30A, 30B. Drilling a hole in one of the protective layers 30, or integrally removing one of the protective layers 30, will have the effect of triggering a security mechanism that executes a countermeasure like a memory wipe. The security mechanism could be of any kind and the present disclosure is not limited to some specific countermeasures.

Variant 1 of the first embodiment

[0065] In a variant of the first embodiment, at least one of the two protective layers 30A, 30B (i.e., either one of them or both of them) can be made of a single continuous wire 32 that is bent in order to form parallel lines.

[0066] Figures 4A and 4B illustrates an example of this first variant of the first embodiment. In this example, the structure of the integrated circuit device 100 is similar to the structure of the first embodiment, but one bent continuous wire 32A, 32B is used to replace each protective plate and acts as the protective or shield layer 30A, 30B. The bent continuous wire 32, 32B can be joined to the active layer(s) or the semiconductor substrate layer through a joining (interface) layer 31A, 31B, as previously described in the first embodiment. Thus, each bent wire 32A, 32B extends over the corresponding joining layer 31A, 31B.

10 [0067] Figure 4A is a top view of the overlapping layers 30A, 31A, 20, 10, 31B, 30B of the integrated circuit device 100. It shows the protective layer 30A formed by the single bent wire 32A. Figure 4B shows a side view of the overlapping layers 30A, 31A, 20, 10, 31B, 30B.

[0068] In each protective layer 30A, 30B, the parallel lines of wire are very close to each other. The space between two adjacent lines can be very small, for example a few microns.

[0069] Each bent wire 32A (32B) forms a shield that protects the integrated circuit device against attacks, similarly to a full plate. In addition, the fact that the shield is provided by a single wire facilitates the detection in case of an attack of the shield. Indeed, it is very easy to detect whether or not the wire has been cut.

Variant 2 of the first embodiment

[0070] A second variant of the first embodiment is similar to the first variant described above embodiment and only differs from it in that each bent continuous wire 32A (32B) is supported by a printed circuit board (PCB) 33 (referred as 33A for one side and 33B for the other side of the integrated circuit device). The printed circuit board 33A (33B) forms an intermediate layer between the protective layer 30A (30B) and the joining layer 31A (31B). The wire 32A (32B) is printed on the corresponding PCB 33A (33B). This allows to improve the physical protection. The protection against the different

attacks provided by such a configuration is very close to the protection provided by a full plate.

[0071] The printed circuit board carrying a bent continuous wire can be provided on one side or on both sides of the integrated circuit device.

- 5 [0072] The first and second variant of the protective layers could be used in an integrated circuit device according to the first embodiment but also in an integrated circuit device provided with another interface for interconnection to an external circuitry suitable to receive this kind of protective layer(s).

Second embodiment

- 10 [0073] A second embodiment of the integrated circuit device is similar to the first embodiment but differs from this first embodiment in that it is a flip chip system, as shown in figure 2.

- [0074] Solder ball terminals 70 connect the circuit(s) of the active layer(s) 20 to conductive tracks supported by the carrier 200, for a redistribution of connection terminals of the active layer(s). The overlapping layers are arranged from the carrier 200 to the mold cap 60 (from bottom to top in figure 2) in the following order : protective layer 30A, joining layer 30A, active layer(s) 20, semiconductor substrate layer 10, joining layer 31B and protective layer 31B. Cylindrical conductive posts (e.g. made of copper), not represented in figure 2, are interposed between the solder ball terminals 70 and the connection terminals of the active layer(s) 20 and arranged through holes provided in the protective layer 30A, as well known by the skilled person.
- 15
20

- [0075] The operation of the integrated circuit device according to the second embodiment is similar to the operation of the integrated circuit device according the first embodiment.
- 25

Third embodiment

[0076] In a third embodiment, each protective layer 30 comprises a mosaic of elementary plates, as the elementary plates 34A shown in figure 6. Each

elementary plate 34A is electrically connected to the detection circuit 40, for example by TSV. The two protective layers 30A and 30B are identical. It means that each elementary plate 34A of the first protective layer 30A faces a corresponding elementary plate 34B of the second protective layer 30B.

- 5 The two corresponding elementary plates 34A, 34B facing each other are coupled.

[0077] In operation, the detection circuit 40 measures a relative electrical value between the two coupled elementary plates for each pair of elementary plates 34A, 34B. For example, the detection circuit 40 is configured to
10 measure a capacitance between the two coupled elementary plates or a difference between the respective resistances of the two coupled elementary plates.

[0078] Such a configuration of the protective layers could be used in an integrated circuit device in a wire bond package (first embodiment), or in a flip
15 chip system (second embodiment), or in another package of integrated circuit device provided with another type of interface for interconnection to an external circuitry.

[0079] In a variant, the elementary plates 34A (34B) could be supported by a printed circuit board, as previously described.

- 20 [0080] The integrated circuit device 100 can be integrated in a product. The present disclosure also concerns such a product.

CLAIMS

1. An integrated circuit device (100) comprising a semiconductor substrate layer (10) and at least one active layer (20) including electronic components and supported by said semiconductor substrate layer (10),
5 characterized in that the semiconductor substrate layer (10) and the at least one active layer (20) are sandwiched between two protective layers (30A, 30B) acting as physical obstacles to prevent the passage of radiations and electrically connected to a detection circuit (40) for monitoring an electrical information of the protective layers (30A, 30B) and detecting a physical attack
10 of at least one of the two protective layers (30A, 30B), based on the monitored electrical information.
2. The device according to claim 1, characterized in that the detection circuit (40) is integrated within the at least one active layer (20).
3. The device according to claim 1 or 2, further comprising an electronic
15 protection circuit (50) configured to generate a signal for executing an electronic protection countermeasure, when a physical attack is detected by the detection circuit (40).
4. The device according to claim 3, characterized in that the electronic protection circuit (50) is integrated within the at least one active layer (20).
- 20 5. The device according to any of claims 1 to 4, characterized in that the two protective layers (30A, 30B) are configured to prevent the passage of radiations of the group including laser radiations, electromagnetic emanations from the at least one active layer, electromagnetic radiations produced by an external source.
- 25 6. The device according to any of claims 1 to 5, characterized in that the two protective layers are made of metal, or a metal alloy, or a semi-conductor material.
7. The device according to any of claims 1 to 6, characterized in that at least one of the protective layers (30A, 30B) is a full plate.

8. The device according to any of claims 1 to 7, characterized in that the at least one of the protective layers (30A, 30B) is made of a bent continuous wire forming parallel lines.
9. The device according to any of claims 1 to 8, characterized in that
5 each of the two protective layers (30A, 30B) comprises a mosaic of elementary plates electrically connected to the detection circuit (40).
10. The device according to any of claims 1 to 9, characterized in that the detection circuit (40) is configured to measure a relative value between respective electrical values of the two protective layers (30A, 30B).
- 10 11. The device according to any of claims 1 to 10, characterized in that the detection circuit (40) is configured to measure a capacitance between the two protective layers (30A, 30B), as said electrical information of the two protective layers (30A, 30B).
12. The device according to any of claims 1 to 10, characterized in that
15 the detection circuit (40) is configured to measure a difference of electrical resistances between the two protective layers (30A, 30B), as said electrical information of the two protective layers (30A, 30B).
13. The device according to any of claims 1 to 12, characterized in that the detection circuit (40) is configured to detect a deviation of the monitored
20 electrical information from a reference value, out of a tolerance range.
14. The device according to any of claims 1 to 13, characterized in that the two protective layers (30A, 30B) are joined to the semiconductor substrate layer (10) and the at least one active layer (20), through two respective joining layers (31A, 31B) functioning as electrical insulators.
- 25 15. A product including an integrated circuit device according to any of claims 1 to 14.

1/3

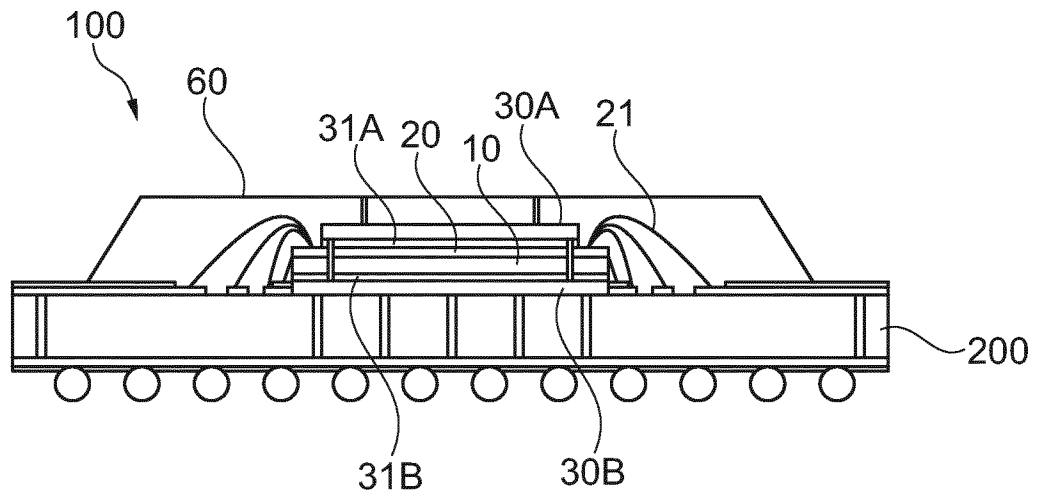


Fig. 1

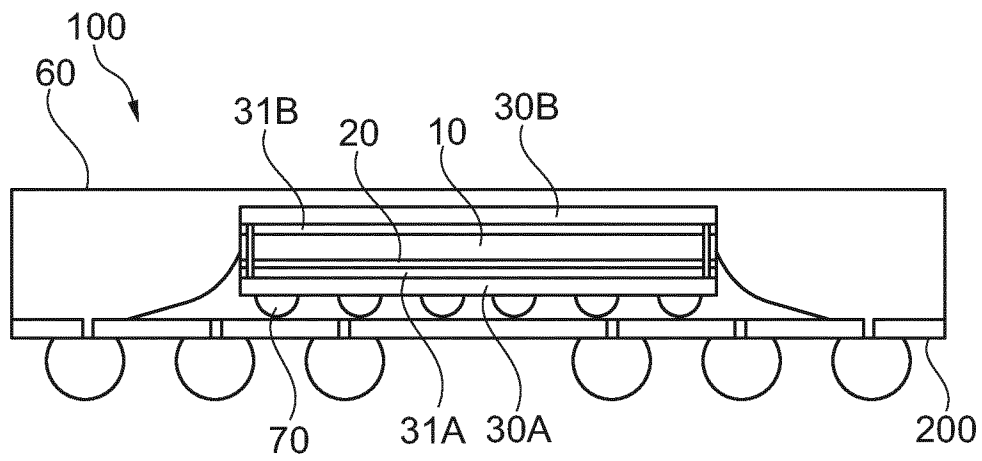


Fig. 2

2/3

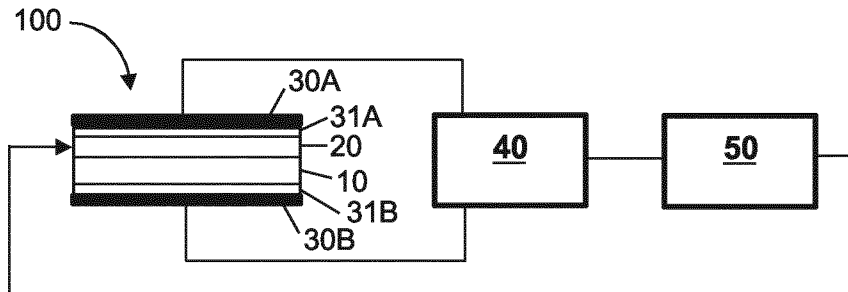


Fig. 3

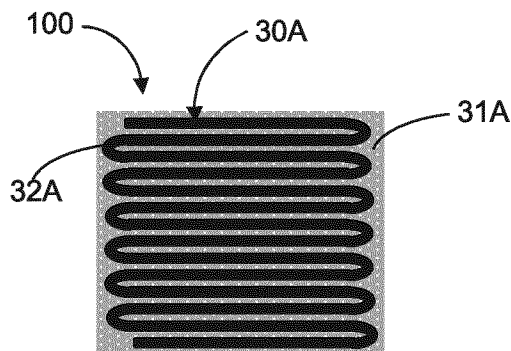


Fig. 4A

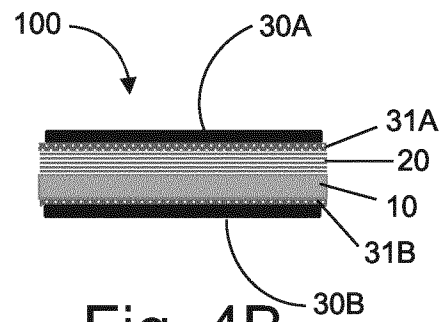


Fig. 4B

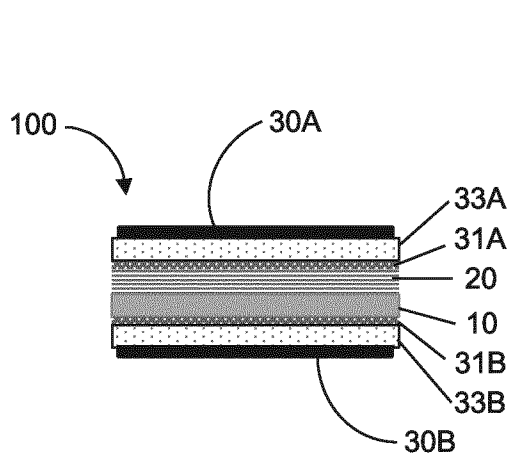


Fig. 5

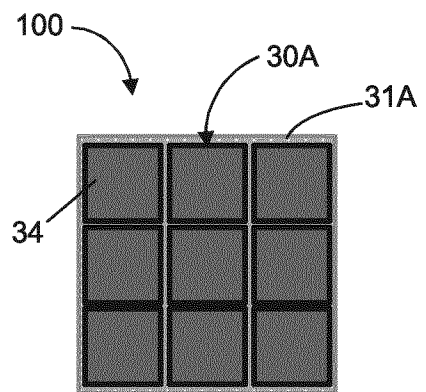


Fig. 6

3/3

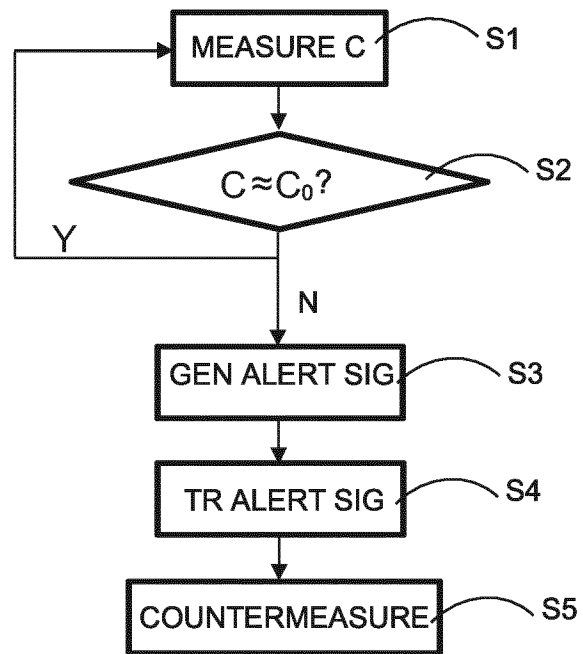


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/069077

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/75 G06F21/87 G09C1/00 H04L9/00
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F G09C H04L

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2019/055307 A1 (CRYPTOGRAPHY RES INC [US]) 21 March 2019 (2019-03-21) paragraph [0037] - paragraph [0053] figures 3,4a,4b,4c -----	1-15
A	EP 3 291 293 A1 (STMICROELECTRONICS (CROLES 2) SAS [FR]) 7 March 2018 (2018-03-07) paragraph [0030] - paragraph [0031] -----	1-15
A	US 2018/308808 A1 (KIRSCHNER YUVAL [IL] ET AL) 25 October 2018 (2018-10-25) paragraph [0016] - paragraph [0032] -----	1-15
A	FR 3 035 267 A1 (COMMISSARIAT ENERGIE ATOMIQUE [FR]) 21 October 2016 (2016-10-21) page 10, line 16 - page 14, line 30 ----- -/-	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

"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

12 October 2021

Date of mailing of the international search report

20/10/2021

Name and mailing address of the ISA/

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

Authorized officer

Bec, Thierry

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/069077

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007 227498 A (MATSUSHITA ELECTRIC IND CO LTD) 6 September 2007 (2007-09-06) paragraph [0008] - paragraph [0015] -----	1-15
A	WO 2007/086046 A2 (NDS LTD [GB]; WALKER JOHN [GB]; MANTIN ITSIK [IL]) 2 August 2007 (2007-08-02) figures 10-12 page 29, line 27 - page 34, line 21 -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2021/069077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2019055307 A1	21-03-2019	CN 111095534 A EP 3682471 A1 US 2021035924 A1 WO 2019055307 A1	01-05-2020 22-07-2020 04-02-2021 21-03-2019
EP 3291293 A1	07-03-2018	CN 107799474 A CN 206992080 U EP 3291293 A1 FR 3055471 A1 US 2018061781 A1	13-03-2018 09-02-2018 07-03-2018 02-03-2018 01-03-2018
US 2018308808 A1	25-10-2018	JP 6635276 B2 JP 2018186271 A TW 201839652 A US 2018308808 A1	22-01-2020 22-11-2018 01-11-2018 25-10-2018
FR 3035267 A1	21-10-2016	CN 106067460 A EP 3086368 A2 FR 3035267 A1 US 2016307855 A1	02-11-2016 26-10-2016 21-10-2016 20-10-2016
JP 2007227498 A	06-09-2007	NONE	
WO 2007086046 A2	02-08-2007	CN 102063584 A EP 1977481 A2 EP 2615641 A2 HK 1129772 A1 HK 1157508 A1 IL 192916 A US 2009001821 A1 WO 2007086046 A2	18-05-2011 08-10-2008 17-07-2013 04-12-2009 29-06-2012 31-07-2012 01-01-2009 02-08-2007