United States Patent Application Publication	20250258965
Kind Code	A1
Publication Date	August 14, 2025
Inventor(s)	Kirschner; Yuval et al.

Detection of Security Attacks Through Die-Attach Pad

Abstract

An electronic device includes an Integrated Circuit (IC) and a package including a die-attach pad for connecting the IC. The IC includes (i) a measurement circuit configured to measure an electrical characteristic of the die-attach pad, and (ii) a security control circuit configured to initiate a responsive action responsively to detecting a deviation of the measured electrical characteristic of the die-attach pad from an initial measurement of the electrical characteristic.

Inventors: **Kirschner; Yuval (Even Yehuda, IL), Golan; Tamir (Kibbutz Givaat-Chaim Meuchad, IL)**

Applicant: **NUVOTON TECHNOLOGY CORPORATION** (Hsin-chu, TW)

Family ID: **1000007727777**

Appl. No.: **18/438481**

Filed: **February 11, 2024**

Publication Classification

Int. Cl.: **G06F21/87** (20130101); **G01R31/28** (20060101); **G06F21/55** (20130101)

U.S. Cl.:

CPC **G06F21/87** (20130101); **G01R31/2853** (20130101); **G06F21/554** (20130101);

Background/Summary

FIELD OF THE INVENTION

[0001] The present invention relates to security of integrated circuits, and particularly to methods and apparatuses to detect security attacks through the backend of an integrated circuit.

BACKGROUND OF THE INVENTION

[0002] To gain access to stored secrets, attackers of integrated circuits (ICs) in various leadframe packages sometimes attempt to physically access the IC from the backside.

[0003] Various techniques for securing ICs against backside attacks are known in the art. For example, “Si-Backside Protection Circuits Against Physical Security Attacks on Flip-Chip Devices”, Takuji et. al., IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 55, NO. 10, October 2020, presents a cryptographic key protection technique from physical security attacks through Si-backside of IC chip. The article proposes a backside buried metal (BBM) structure forming a meander wire pattern on the Si-backside detects unexpected disconnection of the meander and warns the malicious attempts to expose a vulnerable Si substrate. Moreover, the BBM meander also shields key information of cryptographic circuitry from both passive side-channel attacks and active laser fault injection.

[0004] U.S. Pat. No. 9,965,652 discloses security devices for protecting ICs from backside security attacks, including an N− well formed in a substrate, a P+ center disposed in the central region of the N− well, and a P+ ring surrounding the N− well. To prevent latch-up, a pair of inner and outer N+ rings is formed in the N− well. When a current source is applied to the P+ center, the current flows through a portion of the substrate and is picked up by the P+ ring. When an attacker mills the substrate or makes a trench in the substrate, the resistance of the substrate changes. By monitoring the voltage difference between the P+ center and P+ ring, the attempt to attack the die can be detected.

[0005] Lastly, In an Intel White Paper titled “Fault-Injection Countermeasures, Deployed at Scale” (Intel reference 0822/DCC/MZ/PDF), by Nemiroff and Tokunaga (August 2022), the authors detail a design, calibration, and validation methodology for a fault injection detection circuit, and describe how fault-injection attacks can impact circuit timing, the high-level design of the Tunable Replica Circuit (TRC), data gathering phase that occurs in HVM (high volume manufacturing), the methodology to create a calibration recipe, false positive testing, fault-injection testing and the final HVM production calibration flow.

SUMMARY OF THE INVENTION

[0006] An embodiment of the present invention that is described herein provides an electronic device including an Integrated Circuit (IC) and a package including a die-attach pad for connecting the IC. The IC includes (i) a measurement circuit configured to measure an electrical characteristic of the die-attach pad, and (ii) a security control circuit configured to initiate a responsive action responsively to detecting a deviation of the measured electrical characteristic of the die-attach pad from an initial measurement of the electrical characteristic.

[0007] In Some embodiments, the electrical characteristic of the die-attach pad includes a resistance between at least two wires that are bonded to the die-attach pad. In other embodiments, the electrical characteristic of the die-attach pad includes a capacitance between the die-attach pad and an electrical junction in the IC. In an example embodiment the electrical junction includes a metal deposition layer.

[0008] In a disclosed embodiment, the IC further includes a non-volatile memory (NVM), configured to store the initial measurement of the electrical characteristic of the die-attach pad. The NVM may be programmed with the initial measurement during manufacturing of the electronic device.

[0009] In an embodiment, the electronic device further includes a glue or a film for connecting the IC to the die-attach pad.

[0010] There is additionally provided, in accordance with an embodiment that is described herein, a method for securing an electronic device that includes an Integrated Circuit (IC) and a package including a die-attach pad for connecting the IC. The method includes measuring an electrical characteristic of the die-attach pad. A responsive action is initiated responsively to detecting a deviation of the measured electrical characteristic of the die-attach pad from an initial measurement

of the electrical characteristic.
[0011] The present invention will be more fully understood from the following detailed description of the embodiments thereof, taken together with the drawings in which:

Description

BRIEF DESCRIPTION OF THE DRAWINGS
[0012] FIG. **1** is a block diagram that schematically illustrates an electronic device with die-attach pad tamper protection, in accordance with an embodiment of the present invention;
[0013] FIG. **2** is a block diagram that schematically illustrates an electronic device with resistance-based tampering detection circuitry, in accordance with an embodiment that is disclosed herein;
[0014] FIG. **3** is a block diagram that schematically illustrates an electronic device with capacitance-based tampering detection circuitry, in accordance with an embodiment that is disclosed herein;
[0015] FIG. **4** is a flowchart that schematically illustrates a method for registering the electrical characteristics of the die-attach pad of an electronic device during manufacturing, in accordance with an embodiment that is disclosed herein; and
[0016] FIG. **5** is a flowchart **500** that schematically illustrates a method for on-line protection of an electronic device against die-attach tampering, in accordance with an embodiment that is disclosed herein.
DETAILED DESCRIPTION OF EMBODIMENTS
Overview
[0017] Security attacks on electronic devices are sometimes done through a die-attach pad that is connected to an IC that stores secret data.
[0018] We will refer hereinbelow to ICs that store secrets as security ICs. The secrets, such as encryption and authentication keys, are typically stored in memory, e.g., in a Non-Volatile Memory (NVM).
[0019] Security ICS may be attacked in a variety of techniques, such as fault injection methods, failure analysis and Focused Ion Beam (FIB) edits (and others). Most of those techniques are more easily done from the back-side of the IC; for example, Laser fault injection in advanced semiconductor processes is best done from the die back side, through the transparent substrate, rather than from the front side, through the opaque metal layers; FIB, too, is more easily done from the backside—in modern ICs there could be anywhere from six to ten (and sometimes even more) metal layers, making it hard to access the devices from the top-side, whereas, from the backside, as all signals start and end with metal-1 (the bottom metal layer), FIB is relatively easy.
[0020] Inexpensive lead-frame packages such as QFP, QFN and TSSOP are often used for security ICs. In those packages the die is glued on a central metal plate (called “die-attach pad”) and pads are bonded to surrounding pins.
[0021] In such packages, it is relatively easy to gain access from the package bottom to the die back side without damaging the chip, e.g., by drilling a hole in the bottom of the package, through the die-attach pad (and the glue), exposing the bottom of the die to attacks. In comparison, drilling a hole in a Ball Grid Array (BGA) package is not a feasible mode of attack, as it most likely damages the package and disconnects some of the pins.
[0022] Embodiments of the present invention that are disclosed herein provide for apparatuses and methods to detect attacks through the die-attach pad. In some embodiments, electrical characteristics of the die-attach pad are measured during IC production and stored in a non-volatile memory (NVM) thereon (referred to as reference electrical characteristics values). In an embodiment, the electrical characteristics comprise a resistance through the die-attach pad, and in another embodiment the electrical characteristics comprise a capacitance between the die-attach

pad and a metal deposition in the IC.
[0023] In embodiments, the IC comprises a measurement circuit that measures the electrical characteristics of the die-attach pad, and a security control circuit (SCC) that compares the measured electrical characteristics to the reference value and, according to a deviation measure, may take protective actions (e.g., erase stored secrets). In an embodiment, the measurement takes place once, when the IC is turned on, protecting against die-attach tampering that was done when the IC was powered-off; in other embodiments, the SCC continuously measures the electrical characteristics, to provide protection again die-attach tampering done when the IC is powered on or off.
[0024] The embodiments disclosed herein provide relatively inexpensive protection, as no additional IC fabrication steps are added. Moreover, since the die-attach pad, which is the target of the attack is directly examined, a more reliable attack protection may be achieved (when compared to indirect protection, relying on indirect effects).
System Description
[0025] In some embodiments, electronic devices comprise an IC that is connected to the IC package through a Die-Attach Pad. Such electronic devices may be prone to attacks ("hacking") through the die-attach pad. For example, an attacker may drill or otherwise puncture the die-attach pad, to gain access to the IC and read secret information that may be stored therein.
[0026] FIG. **1** is a block diagram that schematically illustrates an electronic device **100** with die-attach pad tamper protection, in accordance with an embodiment of the present invention. Electronic Device **100** comprises an integrated circuit (IC) **102** that is connected to a package (not shown) through a Die-Attach Pad **104**. The IC is typically connected to the die-attach pad **104** using a suitable glue or film.
[0027] Any tampering with the die-attach pad, including puncturing using a laser beam, an electron-beam, a mechanical drill, or others is bound to change some electrical characteristics of the die-attach pad (examples that will be described below include change in resistance and/or capacitance).
[0028] IC **102** comprises an Electrical Characteristic Measurement circuit **106**, configured to measure the electrical characteristics of the die-attach pad, and a Non-Volatile Memory (NVM) **108**, configured to store a reference value of the electrical characteristics. In some embodiments, the NVM is programmed during the manufacturing process of the electronic device, as part of a final test and/or calibration process; in embodiments, during manufacturing, electrical measurement circuit **102** measures the electrical characteristics, and a testing equipment writes the measured value (referred to as "reference value") in the NVM. In other embodiments, the reference electrical characteristics value may be measured by a test equipment.
[0029] IC **102** further comprises a Security Control Circuit (SCC) **110** that is configured to find a deviation of the electrical characteristics measured by the electrical measurement circuit and the reference value stored in the NVM; if the deviation is greater than a predefined threshold, the SCC is configured to protect sensitive data in the IC, for example, by erasing all stored secrets. In some embodiments, the SCC is operative during device startup, and protects against die-attach drilling that is done while the electronic device is not powered. In other embodiments, the SCC is continually operative (when powered), providing protection also against in-vivo attacks.
[0030] As will be shown below (with reference to FIGS. **2** and **3**), in some embodiments the measurement of the electrical characteristics utilizes a clock in IC **102**. In embodiments, since an attacker can typically stop the clock, the deviation when the clock is stopped will be above the predefined threshold, and the protection mechanism will not be compromised.
[0031] In an embodiment, a user may, during Printed Circuit-Board (PCB) manufacturing, solder the die-attach pad directly on the PCB, modifying the die-attach pad electrical characteristics (e.g., lowering the resistance by providing a parallel path). In this case, the reference value stored in the NVM should be updated as part of the PCB manufacturing process.

[0032] Thus, in embodiments, secret data stored in the IC are protected against physical attacks through the die-attach pad, that change the electrical characteristics of the die-attach pad beyond a preset threshold.
[0033] FIG. **2** is a block diagram that schematically illustrates an electronic device **200** with resistance-based tampering detection circuitry, in accordance with an embodiment that is disclosed herein. An IC **202** is connected to a die-attach pad **204**. IC **202** comprises a Resistance-Measurement Circuit **206**. In an example embodiment, the Resistance-Measurement Circuit comprises a current source that sources current through the measured resistance, and an analog to digital converter that converts the voltage on the resistance to digital representation.
[0034] Resistance-Measurement Circuit **206** is connected through a Pad **208**A and a wire **210**A to a first location **212**A on the die-attach pad, and, through a pad **208**B and a wire **210**B to a second location **212**B on the die-attach pad. The resistance measurement circuit, thus, measures a resistance **214** through the die-attach pad. In embodiments, locations **212**A and **212**B on the die-attach pad are remote from each other, typically on two opposite corners or at the centers of two opposite sides of the die-attach pad.
[0035] It should be noted that, since the tamper-detection criterion is a deviation between two measurements, the resistance measurement circuit does not have to be either linear or precise, as long as the readouts are consistent.
[0036] In some embodiments, since the resistance of wires **210**A and **210**B is typically larger than the resistance **214** of the die-attach pad, multiple parallel wires are used to connect the measurement circuit to the die-attach pad. In other embodiments, a die-attach pad with higher sheet-resistance is used, e.g., using different material with lower conductivity, or using a thinner profile.
[0037] FIG. **3** is a block diagram that schematically illustrates an electronic device **300** with capacitance-based tampering detection circuitry, in accordance with an embodiment that is disclosed herein. An IC **302** is connected (e.g. to a galvanically floating die-attach pad **304**. IC **302** comprises a Capacitance-Measurement Circuit **306** that is connected to a floating node **308** (typically an electrically isolated metal deposition area) and, through a bond **310** and a wire **312**, to a bond **314** on the die-attach pad **304**. The capacitance measurement circuit is configured to measure the capacitance between the floating node and the die-attach pad.
[0038] Since the tamper-detection criterion is a deviation between two measurements, the capacitance measurement should be consistent and sensitive, but does not have to be either linear or precise. In some embodiments, capacitance measurement circuit **306** comprises a current source that charges (or discharges) the capacitance; in other embodiments, a simpler (albeit less accurate) circuit that charges (or discharges) the capacitance through a voltage source in series with a resistance is employed. In some embodiment, the voltage on the capacitance is measured after a preset time (derived, for example, from an on-chip clock). In yet other embodiments, the capacitance measurement circuit measures a time (e.g., counts clock cycles) until the voltage on the capacitance reaches a preset level.
[0039] In embodiments, since the variance between the capacitances of the metal layers to the die-attach pad is small, floating node **308** may comprise any metal layer.
[0040] Alternatively, in an embodiment, the Redistribution Layer (RDL), covering most of the area above the chip (excluding metal pads and power routing), which is used as a top-side shield against FIB/laser attacks, can also be used as the capacitance top plate. The distance between the RDL and the die-attach pad, or the die thickness, typically comprises 7 mil of silicon and 0.5 mil of epoxy; in embodiments, die thickness is trimmed down to 5 mil of silicon and 0.5 mil of epoxy, and, in yet other embodiments, to 3 mil+film (film is used as an alternative to liquid glue). At a gap size of 3.5 mil, the capacitances of a 1 mm.sup.2 capacitor and 1 cm.sup.2 capacitors are, respectively, 0.1 pF and 10 pF.
[0041] The configurations of electronic device **200** and **300** illustrated in FIGS. **3** and **4** are

examples that are cited merely for the sake of conceptual clarity. Other configurations may be used in alternative embodiments. In some embodiments, for example, the die-attach pad is connected to ground (in the IC and/or in the board), and can be used as the negative node of the capacitance measurement, while a floating metal plate implemented inside the IC is used as the positive node,. In other embodiments both the resistance and the capacitance are measured. In an embodiment, the capacitance between the die-attach pad and the ground is measured (and, hence, floating node **308** is not needed).

[0042] FIG. **4** is a flowchart **400** that schematically illustrates a method for registering the electrical characteristics of the die-attach pad of an electronic device during manufacturing, in accordance with an embodiment that is disclosed herein. The method is executed by a test-equipment that is used during the final test of the electronic device.

[0043] The flowchart starts at a Measure-Electrical-Characteristics operation **402**, wherein the test equipment measures the electrical characteristics of the die-attach pad (e.g., resistance, or capacitance). In some embodiments, the test equipment directly measures the characteristics; in other embodiments, the test equipment activates the characteristics measurement circuit in the device (e.g., electrical characteristics measurement circuit **106**, FIG. **1**).

[0044] Next, in a Write Measurement Value operation **404**, the test equipment writes the measurement results of operation **402** in a non-volatile memory (e.g., NVM **108**, FIG. **1**) of the electronic device. After operation **404** the flowchart ends.

[0045] FIG. **5** is a flowchart **500** that schematically illustrates a method for on-line protection of an electronic device against die-attach tampering, in accordance with an embodiment that is disclosed herein. The method is executed by SCC **110** and Electrical Characteristics Measurement Circuit **106** (FIG. **1**).

[0046] The flowchart is initiated at power-up and continues as long as power is applied to the electronic device. The flowchart starts at a Measure-Electrical-Characteristics operation **502**, wherein the Electrical Characteristics Measurement Circuit **106** measures the electrical characteristics of the die-attach pad (e.g., resistance, or capacitance). Next, in a Calculate-Deviation operation **504**, the SCC compares the measured value to the reference value (stored, for example, in NVM **108**, FIG. **1**); in some embodiments the deviation is the absolute value of the difference between the measured and the reference values; in other embodiment, a relative deviation measure is used, e.g., the absolute difference divided by the reference value.

[0047] The SCC then, at a Compare Deviation operation **506**, compared the deviation to a preset threshold. If the deviation is not greater than the threshold, the flowchart will reenter operation **502**, to reexamine the electrical characteristics (and, thus, provide continuous protection). If, in operation **506**, the deviation is larger than the threshold, the flowchart will enter a Destroy-Secrets operation **508**, wherein the SCC destroys some or all the stored secrets (alternatively, or additionally the SCC) may, in some embodiments, permanently disable access to the stored secrets). After operation **508** the IC operation will abort.

[0048] The configurations of flowcharts **400**, **500** illustrated in FIGS. **3**, **4** and described above are example configurations. Other configurations may be used in alternative embodiments. For example, in some embodiments, the SCC executes flowchart **500** only once, right after power-up and, in operation **506**, if the deviation is not larger than the threshold, the SCC exits (this approach saves power consumption, but provides protection against off-power tampering of the die-attach pad only).

[0049] In some embodiments, a package that does not require a die-attach pad is used (e.g., a BGA package); instead, the package is modified to include a metal plate that covers most, or all, of the IC substrate area; the metal plate is used for attack detection, similarly to the use of the die-attach pad described above.

[0050] The configurations of electronic devices **100**, **200** and **300**, including resistance measurement circuit **206** and capacitance measurement circuit **306**, and the methods of flowcharts

400 and **500**, illustrated in FIGS. **1** through **5** and described hereinabove are example configurations and methods that are shown purely for the sake of conceptual clarity. Any other suitable system configurations and methods can be used in alternative embodiments. The different elements of electronic circuit **100**, may be implemented in an integrated circuit, such as an application specific integrated circuit (ASIC) or a field-programmable gate-array (FPGA).

[0051] It will thus be appreciated that the embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and sub-combinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art. Documents incorporated by reference in the present patent application are to be considered an integral part of the application except that to the extent any terms are defined in these incorporated documents in a manner that conflicts with the definitions made explicitly or implicitly in the present specification, only the definitions in the present specification should be considered.

Claims

1. An electronic device, comprising: an Integrated Circuit (IC); and a package comprising a die-attach pad for connecting the IC, wherein the IC comprises: a measurement circuit, configured to measure an electrical characteristic of the die-attach pad; and a security control circuit, configured to initiate a responsive action responsively to detecting a deviation of the measured electrical characteristic of the die-attach pad from an initial measurement of the electrical characteristic.

2. The electronic device according to claim 1, wherein the electrical characteristic of the die-attach pad comprises a resistance between at least two wires that are bonded to the die-attach pad.

3. The electronic device according to claim 1, wherein the electrical characteristic of the die-attach pad comprises a capacitance between the die-attach pad and an electrical junction in the IC.

4. The electronic device according to claim 3, wherein the electrical junction comprises a metal deposition layer.

5. The electronic device according to claim 1, wherein the IC further comprises a non-volatile memory (NVM), configured to store the initial measurement of the electrical characteristic of the die-attach pad.

6. The electronic device according to claim 5, wherein the NVM is programmed with the initial measurement during manufacturing of the electronic device.

7. The electronic device according to claim 1, further comprising a glue or a film for connecting the IC to the die-attach pad.

8. A method for securing an electronic device that includes an Integrated Circuit (IC) and a package comprising a die-attach pad for connecting the IC, the method comprising: measuring an electrical characteristic of the die-attach pad; and initiating a responsive action responsively to detecting a deviation of the measured electrical characteristic of the die-attach pad from an initial measurement of the electrical characteristic.

9. The method according to claim 8, wherein measuring the electrical characteristic of the die-attach pad comprises measuring a resistance between at least two wires that are bonded to the die-attach pad.

10. The method according to claim 8, wherein measuring the electrical characteristic of the die-attach pad comprises measuring a capacitance between the die-attach pad and an electrical junction in the IC.

11. The method according to claim 10, wherein the electrical junction comprises a metal deposition layer.

12. The method according to claim 8, further comprising storing the initial measurement of the

electrical characteristic of the die-attach pad in a non-volatile memory (NVM) in the IC.

13. The method according to claim 12, wherein storing the initial measurement comprises programming the NVM with the initial measurement during manufacturing of the electronic device.

14. The method according to claim 8, further comprising a glue or a film for connecting the IC to the die-attach pad.