



(51) International Patent Classification:

H01L 23/00 (2006.01) H01L 23/48 (2006.01)

H01L 23/552 (2006.01)

(21) International Application Number:

PCT/US2022/038921

(22) International Filing Date:

29 July 2022 (29.07.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/203,867 02 August 2021 (02.08.2021) US

(71) Applicant: INVENSAS BONDING TECHNOLOGIES, INC. [US/US]; 3025 Orchard Parkway, San Jose, California 95134 (US).

(72) Inventors: HABA, Belgacem; 3025 Orchard Parkway, San Jose, California 95134 (US). MIRKARIMI, Laura, Wills; 3025 Orchard Parkway, San Jose, California 95134 (US). AUBUCHON, Christopher; 3025 Orchard Parkway, San Jose, California 95134 (US). KATKAR, Rajesh; 3025 Orchard Parkway, San Jose, California 95134 (US).

(74) Agent: CHRISTENSEN, Michael, R.; 2040 Main Street, 14th Floor, Irvine, California 92614 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: PROTECTIVE SEMICONDUCTOR ELEMENTS FOR BONDED STRUCTURES

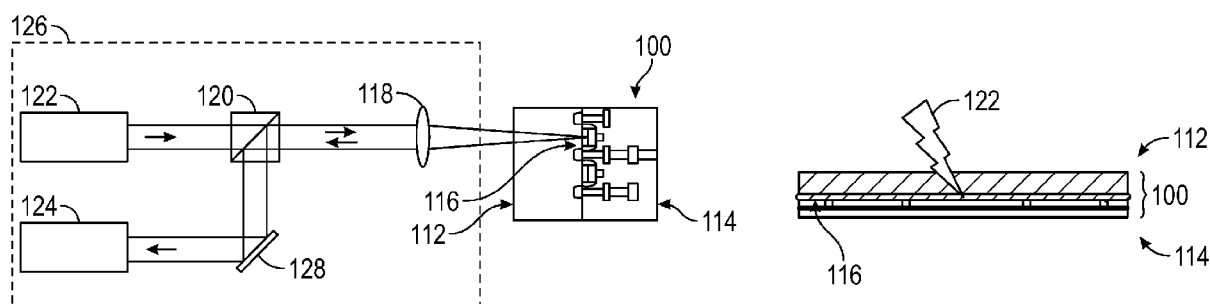


FIG. 1

(57) Abstract: A bonded structure with protective semiconductor elements including a semiconductor element with active circuitry and a protective element including an obstructive layer and/or a protective circuitry layer. The obstructive layer is configured to inhibit external access to at least a portion of the active circuitry. The protective circuitry layer is configured to detect or disrupt external access to the protective element and/or the active circuitry of the semiconductor element. The semiconductor element and the protective element are directly bonded without an adhesive along a bonding interface.

PROTECTIVE SEMICONDUCTOR ELEMENTS FOR BONDED STRUCTURES

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 63/203,867, filed August 02, 2021, the entire contents of which are hereby incorporated by reference in their entirety and for all purposes.

BACKGROUND

Field

[0002] The field relates to bonded structures comprising active and/or protective semiconductor elements and methods for forming the same.

Description of the Related Art

[0003] Semiconductor chips (*e.g.*, integrated device dies) may include active circuitry containing security-sensitive components which contain valuable and/or proprietary information, structures or devices. For example, such security-sensitive components may include an entity's intellectual property, software or hardware security (*e.g.*, encryption) features, privacy data, or any other components or data that the entity may wish to remain secure and hidden from third parties. For example, third party bad actors may utilize various techniques to attempt to access security-sensitive components for economic and/or geopolitical advantage. Accordingly, there remains a continuing need for improving the security of semiconductor chips from being accessed by third parties.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Figure 1 is an example illustration of optical imaging of a semiconductor chip.

[0005] Figure 2 is an example illustration of a focused ion beam (FIB) attack of a semiconductor chip.

[0006] Figure 3 is a schematic side sectional view showing an example solution to invasive chip attacks.

[0007] Figure 4A is a schematic side sectional view showing an example illustration of a protective chip incorporating a protective layer.

[0008] Figure 4B is a schematic side sectional view showing an example illustration of a protective chip incorporating a protective layer in conjunction with an obstructive layer.

[0009] Figure 5 is an example illustration of additional parameters of a protective chip.

DETAILED DESCRIPTION

[0010] As explained herein, third parties (such as third party bad actors) may attempt to access security-sensitive components on elements such as integrated device dies. In some elements, the security-sensitive components may be protected by a combination of netlist and non-volatile memory (NVM) data. However, third parties may attempt to hack the security-sensitive components by a combination of destructive and non-destructive techniques, e.g., through a variety of probing techniques (e.g. electro-optical probing) and/or delaying the element to expose, reverse engineer, or otherwise gain access to the security-sensitive components. In some cases, the third party may attempt to hack the security-sensitive components by pulsing electromagnetic (EM) waves onto active circuitry of the element, using fault injection techniques, employing near infrared (NIR) laser triggering or focused ion beam (FIB) modification of circuits, chemical etching techniques, and other physical, chemical, and/or electromagnetic hacking tools and even reverse engineering. These techniques can be used to physically access sensitive circuits of microdevices such as integrated circuits to directly read encrypted information, to trigger circuits to release information otherwise encrypted, to understand manufacturing processes, to extract enough information to be able to eventually replicate sensitive designs, or to completely bypass the security protocols to activate or use the chip without due permissions. For example, in some cases hackers may attempt to access the encryption key, which can be stored in the circuit design, in memory, or in a combination of both. Techniques can also be used to indirectly read sensitive information by analyzing the resultant output based upon fault injection inputs, and through recursive analysis determine the encryption key or data contents. It is challenging to structurally protect the security-sensitive components on elements.

[0011] Accordingly, it is important to provide improved security for elements (such as semiconductor integrated device dies) that include security-sensitive components. Various embodiments disclosed herein relate to a bonded structure including a first semiconductor element bonded to a second semiconductor element. The second semiconductor element can comprise a protective element including a plurality of layers disposed over active circuitry of the first semiconductor element and arranged to inhibit interrogation of the active circuitry.

[0012] Semiconductor chips face both hardware- and software-level attacks. In some cases, these can be combined in a single technique. For example, a hardware attack on a chip may be utilized to alter the logic of a software program by providing faulty data or affecting the logic circuits used to process data.

[0013] Many techniques are employed by attackers to compromise sensitive semiconductor chips. These may include physical tampering by etching, grinding, or other deencapsulation techniques to reveal the sensitive circuits of the chip. More sophisticated attacks may further employ optical probing of the sensitive circuits. Of these, focused ion beam (FIB) and laser probing are the most prevalent. Many protective countermeasures have been used and proposed in the past, with limited effectiveness as described in more detail below.

[0014] Figure 1 provides an overview of an optical imaging attack using laser probing. Optical probing techniques may be used to access active circuitry 116 (*e.g.*, electronic circuitry that includes at least one transistor) of a semiconductor chip 100 that includes sensitive circuitry (*e.g.*, circuitry that is vulnerable to a hacking attack). Optical probing techniques can enable an attacker to reconstruct sensitive circuitry, compromising the confidentiality and security of the sensitive circuitry. Optical probing techniques may be used to access active circuitry 116 from a back side 112 of the semiconductor element 100 as the optical probes 126 from the back side 112 are not blocked by any wiring or metallizations, unlike on the front side 114 of the semiconductor element 100. In the devices illustrated herein, the active circuitry 116 can be closer to the front side 114 of the semiconductor element than to the back side 112 of the element 100. For example, the active circuitry 116 can be patterned at or near the front side 114 of the element 100. The optical probe 126 includes a laser source 122, a beam splitter 120, a detector 124, and an objective lens 118. The laser source 122 can create and direct a laser beam to the beam splitter 120, which can split the beam into a first component that is directed through the objective lens 118 to the semiconductor element 100

and a second component that is directed to a mirror 128 and the detector 124. The back side optical intrusion techniques can also be used to monitor activity of a circuit, collecting bitstream information to retrieve encryption keys and compromise encrypted information. Laser probing may be performed, for example, by scanning a de-encapsulated chip with a near-infrared (NIR) laser to both image the circuits on the chip and capture waveform information of an active chip. By capturing variance in reflectivity of a circuit path over time caused by the shifting electromagnetic field of the circuit path, laser probing can be used to capture and reconstruct sensitive bitstream information. In some cases, laser probing may be intended to activate specific sets of sensitive transistors or circuits within a chip, which once activated during this type of hack may emit a small amount of IR that is in turn captured by the detector to identify the exact location of interest to hackers. In some cases, this attack may be used to compromise encryption keys. Additionally, imaging of sensitive circuits may allow an attacker to reconstruct sensitive algorithms and other data.

[0015] Preventing optical intrusion is thus important to ensuring the security of semiconductor chips containing security-sensitive components. Conventional techniques may include packaging semiconductor elements with protective casings. However, conventional packaging may be susceptible to grinding, chemical etching, and other package decapping processes that are relatively unsophisticated, leaving the sensitive circuitry exposed and susceptible to optical probing. It may thus be desirable to include protection against optical intrusions by bonding one or more protective elements directly to a semiconductor element, *e.g.*, an active chip having active circuitry 116 including sensitive circuitry. Semiconductor elements 100, such as integrated device dies or chips, may be mounted or stacked on other elements. For example, a semiconductor element 100 can be mounted to a carrier, such as a package substrate, an interposer, a reconstituted wafer or element, etc. As another example, a semiconductor element 100 can be stacked on top of another semiconductor element 100, *e.g.*, a first integrated device die can be stacked on a second integrated device die. In some arrangements, a through-substrate via (TSV) can extend vertically through a thickness of the semiconductor element 100 to transfer electrical signals through the semiconductor element 100, *e.g.*, from a first surface of the semiconductor element 100 to a second opposing surface of the semiconductor element 100.

[0016] To prevent optical imaging of a sensitive semiconductor chip 100, protective elements may thus be integrated into the chip itself, such as an occlusive or abrasive layer disposed over the sensitive semiconductor layer. Direct bonding of obstructive layers may be effective against conventional de-encapsulation techniques, preventing exposure of the sensitive circuit layers of the chip from grinding or etching. However, invasive attacks may be used to thwart these protective measures. As stated, many techniques are employed by attackers to compromise sensitive semiconductor chips. For example, hackers can recreate 2D activity maps of the active circuitry 116 by laser probing the chip. Further, an imaging attack may be utilized to break the bitstream encryption information found within. Thus the protective semiconductor elements described herein block or alter the reflected optical signals (e.g. IR) to help improve the security of the chip (e.g. semiconductor element 100) against non-contact tampering.

[0017] Figure 2 illustrates an example FIB attack. FIB attacks may use a focused ion beam to ablate the surface of a de-encapsulated chip layer by layer, eliminating the protective elements to expose the sensitive semiconductor layer. For example, as shown in Figure 2, a target wire 204 may be exposed by ablation of intervening protective wires 202A, 202B. Ablation using the focused ion beam can form a hole 206 through the chip and protective wires 202A, 202B in a conical pattern having a depth d' . An FIB may then be used at lower intensity to provide high-precision imaging of the sensitive layers (e.g. wire 204). Additionally, the FIB may be used to alter the function of active chips, by inducing current flows, severing or altering traces that connect elements of the sensitive circuit. This may allow an attacker to modify and/or bypass protective structures within the sensitive semiconductor layer. Further, an FIB or laser probe may be used subsequent to ablation to capture bitstream information or image sensitive circuit elements.

[0018] With this invasive physical attack, hackers may access and directly monitor security critical nets of an IC and extract sensitive information. Attacks such as these typically happen on the front side of the chip but may also occur on the backside.

[0019] Figure 3 shows an illustrative example of protective measures employed to thwart imaging attacks of sensitive semiconductor chips. As shown in Figure 3, an active chip 310 may be bonded (e.g., directly bonded without an adhesive) to a protective chip 300 containing an obstructive layer 305. As shown, the protective chip 300 can be directly bonded

to a back side 112 of the active chip 310 that is opposite the front side 114 (which can comprise an active side nearer to the active circuitry 116 than the back side 112). In some configurations, the obstructive layer 305 may be an optically-occlusive layer designed to prevent laser probing, FIB or other hacking techniques of the active circuit layer 116 of the active chip 310, such as described in U.S. Patent Application No. 17/812,675, filed July 14, 2022, the entire contents of which are hereby incorporated. As shown in Figure 2 above, this provides limited protection against FIB attacks. A motivated attacker may, for example, identify a target region 204 of the active chip 310 and employ an FIB attack to remove the portions of the obstructive layer 305 covering the target area 204 of the chip 310, leaving it exposed to probing.

[0020] The obstructive layer 305 can comprise several layers, such as a plurality of metallized layers (e.g. 342A,B) spaced apart by an insulating material 343. In some embodiments, the metallized layers 342A,B and intervening insulating material 343 form a capacitive circuit with positive and negative terminals respectively connected to the two illustrated through-substrate vias (TSVs) 330.

[0021] As shown, a bond interface 315 may comprise a bond between a bonding layer 340A of the protective chip 300 and a bonding layer 340B of the active chip 310. The direct bond may comprise a nonconductive non-adhesive bond in which nonconductive layer 341A, 341B (e.g., dielectric materials) of the bonding layer 340A,B are directly bonded to one another. As shown, the protective chip 300 is bonded to the backside 312 of the active chip 310. Further, the obstructive layer 305 is located near the bonding layer 340A of the protective chip 310. In some embodiments, the direct bond may comprise a hybrid bond in which conductive contact features 350B of the active chip 310 are directly bonded to corresponding conductive contact features 350A of the protective chip 300, and in which nonconductive regions (e.g., nonconductive layer 341B) of the active chip 310 are directly bonded to corresponding nonconductive regions (e.g., a nonconductive layer 341A) of the protective chip 300. Further, the bonding layer 340A, 340B of each chip 300, 310 may comprise a plurality of conductive contact features 350A, B disposed in a nonconductive layers 341A, 341B, such as a dielectric layer (e.g., silicon oxide, silicon nitride, silicon oxynitrocarbide, etc.) The conductive contact features 350A, B may comprise conductive material, e.g., a metal such as copper prepared for direct hybrid bonding. The conductive contact features 350A of the protective chip 300 may be configured to mirror and/or correspond to the conductive contact features 350B of the active

chip 310. The pads may provide an electrical and/or mechanical connection between the protective and active chips. As used herein, the pads can comprise exposed ends of through substrate vias (TSVs) 330 or vertical interconnects 330 (*e.g.*, labeled as pad 350A) or discrete pads at least partially embedded in the field region (*e.g.*, labeled as pad 350B).

[0022] In some cases, an active chip 310 may be configured to detect alteration of a protective chip 300. For example, as shown in Figure 3, a protective chip 300 may be electrically connected to the active circuitry 116 of an active chip 310 by through-substrate vias (TSVs) 330 that may enable the active chip 310 to sense changes to the properties of the protective chip 300 caused by removal of material from the obstructive layer 305. In some embodiments the protective chip 300 may be electrically connected to the active chip 310 through a direct hybrid bond or other interconnect technology. The active chip 310 may be configured to measure the resistance or the capacitance of the obstructive layer 305 or other structures built within the protective chip. If a substantial change to the obstructive layer 305 or the structures takes place, the active chip 310 may then sense the change and disable sensitive circuit elements. However, a FIB attack may be very precise, and the portion of an obstructive layer 305 ablated by the FIB may be too small to create a measurable change in the electrical properties of the obstructive layer 305. Embodiments of the present disclosure are directed at bonded structures including protective chips 300 comprising protective layers resistant to invasive attacks bonded directly to active chips 310 that may comprise security-sensitive circuitry or circuit elements.

[0023] Figure 4A illustrates an example embodiment of the present disclosure directed at remedying the shortcomings of other solutions to protecting sensitive semiconductor chips 100 from sophisticated intrusions employing optical and/or invasive FIB attacks. As shown in Figures 4A and 4B, embodiments of the present disclosure may include a protective chip 300 comprising a protective circuitry layer 410, the protective chip 300 directly bonded to the active chip 310 (*e.g.*, to the back side 112 of the chip 310). The protective circuitry layer 410 can be configured to detect or disrupt external access to the protective element and/or the active circuitry of the semiconductor element. In some embodiments, for example as shown in Figure 4B, the disclosed embodiments can include an obstructive layer 305 and a separate protective circuitry layer 410, formed in the protective chip 300 which can be directly bonded to an active chip 310 (*e.g.*, the back side 112 of the chip

310) to protect an active circuitry 116 of the active chip 310. The active circuitry 116 is located near the front side 114 of the active chip 310 in the illustrated embodiment. As described above, non-bonded protective structures may be susceptible to removal via relatively easy removal techniques, such as grinding or etching. It may therefore be desirable to incorporate a protective chip 300 and active chip 310 into a bonded structure.

[0024] In some embodiments, a bond interface 315 may comprise a bond between a bonding layer 340A of the protective chip 300 and a bonding layer 340B of the active chip 310, which in the illustrated embodiments may be formed at or at least partially define the back side 112 of the chip 310. In some embodiments, the direct bond may comprise a nonconductive non-adhesive bond in which nonconductive material(s) (*e.g.*, dielectric and/or semiconductor materials 341A,B) of the elements are directly bonded to one another. In the illustrated embodiment, the direct bond may comprise a hybrid bond in which conductive contact features or pads 350A of the active chip 310 are also directly bonded to corresponding conductive contact features 350B of the protective chip 300, and in which nonconductive regions (*e.g.*, a bonding layer 340B) of the active chip 310 are directly bonded to corresponding nonconductive regions (*e.g.*, a bonding layer 340A) of the protective chip 300. As shown in Figure 4A, the bonding layer 315 of each chip may comprise a plurality of contact pads 350 disposed in a nonconductive material, such as a nonconductive or dielectric layer 341 (*e.g.*, silicon oxide, silicon nitride, silicon oxynitrocarbide, etc.). The contact pads 350 may comprise conductive material, *e.g.*, a metal such as copper. In these embodiments, the contact pads 350 of the protective chip 300 may be configured to mirror and/or correspond to the contact pads 350 of the active chip 310. The pads 350 may provide an electrical and/or mechanical connection between the protective 300 and active chips 310. Likewise, the contact pads 350 of the bonding layer 315 of the active chip 350 may be connected to the active circuitry 116 of the active chip 310 through TSVs 330. By bonding the contact pads 350A of the protective chip 300 to corresponding contact pads 350B of the active chip 310, in some embodiments the bonded structure may thus have an electrical connection between the active circuitry 116 of the active chip 310 and one or more layers of the protective chip 300. For example, a protective chip 300 may have vertical connectors (*e.g.* vertical interconnects) 360 providing electrical connections between the protective circuitry layer 410 and the contact pads 350 of the bonding layer 315. The protective circuitry layer 410 of the protective chip 300 may then be configured to

communicate through the TSVs 330 to the active layer 116 of the active chip 310 across the bond interface.

[0025] As shown in Figure 4A, the protective chip 300 may comprise a protective circuitry layer 410. The protective circuitry layer 410 described herein can be configured to detect or disrupt external access to at least one of the protective chip 300 and the active circuitry 116 of the active chip 310. In some embodiments, for example, the protective circuitry layer 410 may comprise circuitry, such as throw-away logic, that provides no functional processing to the active chip 310, but that may be configured to detect an intrusion by a hacker in order to protect the active circuitry 116 of the chip 310. In these embodiments, the circuitry in the protective circuitry layer 410 may be configured to mimic the appearance of sensitive active circuitry. For example, a protective chip 300 may incorporate a protective circuitry layer 410 comprising non-sensitive circuits to waste an attacker's time and prolong the analysis required to identify the sensitive areas of the active chip 310, which can disrupt external access to the active circuitry 116 of the chip 310. The protective circuitry layer 410 of the protective chip 300 shown herein may comprise an active circuitry layer. In such embodiments, the active protective circuitry layer 410 may comprise at least one transistor, *e.g.*, a plurality of transistors. In these embodiments, the protective circuitry layer 410 may contain circuits to provide additional, non-sensitive functionality to the active chip 310. In some embodiments, the inexpensive active circuitry in the protective circuitry layer 410 on the protective chip 300 may provide misleading or confusing data to an optical attack as the laser probe is reflected not from the active chip 310 that is to be protected but by the inexpensive low-logic circuitry in the protective circuitry layer 410 on the protective chip 300, which can disrupt external access to the chip 310. In these embodiments, an attacker employing FIB to drill down to the active chip 310 may cause the active chip 310 to disable or malfunction by ablating the intervening protective circuitry layer 410 of the protective chip 300. If one or more transistors of the protective circuitry layer 410 are destroyed or otherwise altered, the protective circuitry 410 can detect the external access and can transmit an alert to the active circuitry 116 of the chip 310 indicating an intrusion. In response, the active chip 310 can disable the functionality of the chip 310, cause the active circuitry 116 to self-destruct or be inactive, or to otherwise prevent external access to the circuitry 116. In some embodiments the protective circuitry layer 410 may comprise active circuitry configured to provide a signal or feedback to the active

circuitry 116 of the active chip 310. In these embodiments, any errors introduced into the protective layer 410 via ablation from an FIB may cause the signal from the protective layer 410 to cease or change, alerting the active chip 310 that the protective chip 300 has been tampered with. For example, the protective layer 410 may comprise active circuitry configured to provide an encrypted timing signal to the active chip 310. If the encrypted timing signal is modified by an external intrusion attempt, the active chip 310 can be alerted to the external access.

[0026] In the illustrated embodiments, the active circuitry of the protective circuitry layer 410 may comprise one or more transistors. In various embodiments, the operational processing circuitry of the active chip 310 can use advanced processes for forming the transistors used in the active chip 310, while the active circuitry of the protective chip 300 (*e.g.*, in the protective circuitry layer 410) can be fabricated using less expensive and less advanced processing technologies, since the protective chip 300 may only utilize basic functionality without the need for advanced circuitry. As an example, the operational processing circuitry 116 of the active chip 310 can use advanced processes, such as an advanced, sub-22nm node process. By contrast, the active circuitry layer of the protective circuitry layer 410 of the protective element 300 or chip may comprise transistors using a legacy node process with larger feature sizes, such as 65nm and larger. In the illustrated embodiments, the protective circuitry layer 410 can be disposed within (*e.g.*, entirely within) the body of the protective element 300. In some embodiments, the transistors in the protective element 300 may serve to provide a warning to the active chip 310 when the protective chip 300 has been tampered with. In some embodiments, the active circuitry (*e.g.*, including one or more transistors) in the protective circuitry layer 410 of the protective element 300 may initiate or cause the sensitive circuitry 116 of the active chip 310 to stop working or functioning in a normal manner. Thus, the protective circuitry 410 inhibits ablative attacks from an FIB. The protective materials used in the protective chip 300, including the materials used in the obstructive layer 305 and protective circuitry layer 410, may include but are not limited to the protective materials described in U.S. Patent Application No. 16/844,932, filed April 9, 2020, U.S. Patent Application No. 16/844941, filed April 9, 2020, U.S. Patent Application No. 16/881621, filed May 22, 2020, and U.S. Patent Application No. 16/846177, filed April 10,

2020, the entire contents of each of which are incorporated by reference herein in their entirety and for all purposes.

[0027] As shown in Figure 4B, the protective chip 300 may further comprise an obstructive layer 305 separate and spaced apart vertically from the protective circuitry layer 410. In some embodiments, the obstructive layer 305 may comprise a plurality of metallization layers 342A,B, separated by an insulation layer 343, that renders the layer 305 opaque to the radiation of a laser probe. In other embodiments, the obstructive layer 305 may comprise an optical filter. In order to increase the cost of analyzing a sensitive chip, it may be desirable to provide misleading or confusing data to an attacker in order to slow the analysis process. In lieu of merely blocking optical signals, it may thus be beneficial to alter the signals. An optical filter may be used to alter the optical signal. For example, in some embodiments an optical filter may comprise a refractive filter. In these embodiments, the obstructive layer 305 may cause an attacker's laser probe to generate inaccurate measurements. As described in U.S. Application No. 17/812,675, which is incorporated by reference herein, the obstructive layer can change the direction of an incoming or outgoing beam (e.g. refract), focus or de-focus (e.g. lensing) the beam, scatter the beam, diffuse the beam, diffract the beam (e.g., a grating), phase/wavelength shift the beam, etc. Thus, the metallization layers 342A,B refer to light-blocking or light-modifying materials that block or modify incident light utilized when attempting to hack sensitive circuitry.

[0028] In some embodiments, the connective contact pads or features (e.g. 350A) of the bonding layer 315 of the protective chip 300 may be further connected by through-semiconductor vias vertical connectors 360 to one or more occlusive layers of the protective chip 300, as shown in the embodiment of Figure 4B. Additionally or alternatively, as shown in Figure 4B, an obstructive layer 305 of the protective chip 300 may be connected to the active layer 116 of the active chip 310 and/or a protective circuitry layer 410 of the protective chip 300. For example, the obstructive layer 305 of the protective chip 300 may be electrically connected to the protective layer 410 of the protective chip 300 by one or more vertical interconnects 360.

[0029] Figure 4B shows the obstructive layer 305 electrically connected to the circuitry 116 of the active chip 310 by way of the contact pads 350A, 350B and TSVs 330 formed in the active chip. In some embodiments, the obstructive layer 305 may further

comprise a detection circuit. In these embodiments, the active chip 310 may be configured to respond to changes to one or more properties of the detection circuit in the obstructive layer 305 through the TSVs 330. In some embodiments, the detection circuit may be configured to enable detection of the resistance of the obstructive layer 305 or a part of the obstructive layer 305 of the protective chip 300. Additionally or alternatively, the detection circuit may be configured to enable detecting the capacitance of the obstructive layer 305 or a part of the obstructive layer 305 of the protective chip 300. In these embodiments, the active chip 310 may be able to respond to removal of sufficiently large portions of the protective chip 300. For example, an FIB probe may be used to ablate portions of the obstructive layer 305 of the protective chip 300 to expose the sensitive semiconductor layer of the active chip 310. By removing these portions of the protective chip 300, the FIB may alter the capacitance and/or resistance or impedance of the obstructive layer 305 of the protective chip 300 to a degree detectable by the detection circuits. In these embodiments, the active chip 310 may be configured to shut down when it detects changes to the obstructive layer 305 of the protective chip 300. Additionally or alternatively, the active chip 310 may be configured to emit an alert signal when it detects changes to the obstructive layer 305 of the protective chip 300. The obstructive layer 305 of the protective chip 300 may be additionally or alternatively connected to the protective circuitry layer 410 of the protective chip 300 by additional vertical connectors 360. In these embodiments, the protective layer 410 of the protective chip 300 may be further configured to respond to changes to the properties of the obstructive layer 305 of the protective chip 300. In some embodiments, the protective circuitry layer 410 of the protective chip 300 may be configured to disable the active chip 310 when changes to the protective chip 300 are detected.

[0030] As shown in Figure 4B, the obstructive layer 305 of the protective chip 300 may be disposed between the protective layer 410 of the protective chip 300 and the active layer 116 of the active chip 310. It should be understood by one skilled in the art that this is for illustrative purposes only. In other embodiments, the protective layer 410 of the protective chip 300 may be between an obstructive layer 305 of the protective chip 300 and the active layer of the active chip 310. Further, in some embodiments the protective chip 300 may have multiple protective layers 410. Additionally or alternatively, the protective chip 300 may have multiple obstructive layers 305. In these embodiments, the layers may be disposed in the

protective chip 300 in any order. As shown, the protective chip 300 is bonded to the backside 112 of the active chip 310. In some embodiments, the protective circuitry layer 410 of the protective element 300 and the obstructive layer 305 of the protective element 300 are spaced apart (i.e. distance d) from one another along a direction transverse to the bonding interface 315. In some embodiments, the obstruction layer 305 may be located on either the protective chip 300, the active chip 310, or both.

[0031] Figure 5 illustrates additional considerations in the configuration of the protective chip 300. As described in more detail above, the precision of an FIB may enable an attacker to drill through an obstructive layer 305 of a bonded structure without ablating a detectable portion of the obstructive material. However, the aspect ratio of FIBs is fairly shallow. Consequently, as shown in Figure 2 above, the FIB widens as the distance from the focal point increases. As shown in Figure 5, in order to ensure an FIB attack is detectable, in some embodiments the obstructive layer 305 of the protective chip 300 may be disposed at a minimum distance (i.e. D) from the sensitive semiconductor layer 116 of the active chip 310, where distance D describes a distance transverse to the bonding interface 315. This may ensure that an FIB attack used to expose a portion of the active chip 310 will ablate sufficient material of the obstructive layer 305 of the protective chip 300 to be detectable. In some embodiments, the spacing or distance D between the obstructive layer 305 of the protective element 300 and the active circuitry 116 of the semiconductor element or active chip 310 is at least 20 micrometers. In some embodiments, the distance D can be between 20 micrometers and 100 micrometers, for example, between 50 micrometers and 100 micrometers. In some embodiments, the distance D can be between 100 micrometers and 500 micrometers. In some embodiments, the protective chip 300 may also comprise a protective circuitry layer 410 comprising an active circuitry layer. In these embodiments, the protective element 300 may be contain circuits to provide additional, non-sensitive functionality to the active chip 310. Further, in some other embodiments the protective chip 300 may comprise multiple obstructive layer 305s. In addition to adding distance between the top obstructive layer 305 and the active layer 116 of the active chip 310, in these embodiments an FIB attack would need to ablate through the multiple obstructive layers 305 in order to expose the sensitive semiconductor layer (e.g., active circuitry 116) of the active chip 310. Accordingly, in various embodiments the obstructive layer 305 of the protective chip 300 may be disposed at a minimum distance

from the semiconductor layer of the active chip 310, as the increased distance D requires increased ablation of the protective chip 300. An advantage of including protective circuitry (*e.g.*, active circuitry including transistors and/or passive circuitry such as a capacitor) in the protective element is that this may force a counterfeiter to make a larger hole when ablating the material of the protective element, which in turn will increase the chance of triggering a warning to the active chip 310.

[0032] Although the illustrated embodiments herein (*e.g.* FIGS. 3-5) show the protective element 300 bonded to the back side 112 of the semiconductor element 310, in other embodiments, the protective element 300 can additionally or alternatively be bonded to the front side 314 to provide front side protection of the circuitry. Accordingly, in some embodiments, the bonded structure may include a second protective element 300 directly bonded to a front side of the semiconductor element 310 without an adhesive along a second bonding interface 315, the second protective element 300 including a second obstructive layer 305 configured to inhibit external access to at least the frontside 114 of the semiconductor element 310; and a second protective circuitry layer 410 disposed within the protective element 300, the protective circuit layer 410 configured to detect or disrupt external access to the front side 114 of the semiconductor element 300.

Examples of Direct Bonding Methods and Directly Bonded Structures

[0033] Various embodiments disclosed herein relate to directly bonded structures in which two elements can be directly bonded to one another without an intervening adhesive. Two or more semiconductor elements (such as integrated device dies, wafers, etc., *e.g.* elements 300, 310) may be stacked on or bonded to one another to form a bonded structure. Conductive contact features or pads (*e.g.* 350A,B) of one element may be electrically connected to corresponding conductive contact features (*e.g.* 350A,B) of another element. Any suitable number of elements can be stacked in the bonded structure.

[0034] In some embodiments, the elements are directly bonded to one another without an adhesive. In various embodiments, a non-conductive or dielectric material (*e.g.* 341A) of a first element (*e.g.*, a protective or occlusive element) can be directly bonded to a corresponding non-conductive or dielectric field region (*e.g.* 341B) of a second element (*e.g.*,

an active chip) without an adhesive. The non-conductive material can be referred to as a nonconductive bonding region or bonding layer of the first element. In some embodiments, the non-conductive material of the first element can be directly bonded to the corresponding non-conductive material of the second element using dielectric-to-dielectric bonding techniques. For example, dielectric-to-dielectric bonds may be formed without an adhesive using the direct bonding techniques disclosed at least in U.S. Patent Nos. 9,564,414; 9,391,143; and 10,434,749, the entire contents of each of which are incorporated by reference herein in their entirety and for all purposes.

[0035] In various embodiments, hybrid direct bonds can be formed without an intervening adhesive. For example, dielectric bonding surfaces can be polished to a high degree of smoothness. The bonding surfaces can be cleaned and exposed to a plasma and/or etchants to activate the surfaces. In some embodiments, the surfaces can be terminated with a species after activation or during activation (*e.g.*, during the plasma and/or etch processes). Without being limited by theory, in some embodiments, the activation process can be performed to break chemical bonds at the bonding surface, and the termination process can provide additional chemical species at the bonding surface that improves the bonding energy during direct bonding. In some embodiments, the activation and termination are provided in the same step, *e.g.*, a plasma or wet etchant to activate and terminate the surfaces. In other embodiments, the bonding surface can be terminated in a separate treatment to provide the additional species for direct bonding. In various embodiments, the terminating species can comprise nitrogen. Further, in some embodiments, the bonding surfaces can be exposed to fluorine. For example, there may be one or multiple fluorine peaks near layer and/or bonding interfaces. Thus, in the directly bonded structures, the bonding interface between two dielectric materials can comprise a very smooth interface with higher nitrogen content and/or fluorine peaks at the bonding interface. Additional examples of activation and/or termination treatments may be found throughout U.S. Patent Nos. 9,564,414; 9,391,143; and 10,434,749, the entire contents of each of which are incorporated by reference herein in their entirety and for all purposes.

[0036] In various embodiments, conductive contact pads of the first element can also be directly bonded to corresponding conductive contact pads of the second element. For example, a hybrid bonding technique can be used to provide conductor-to-conductor direct bonds along a bond interface (*e.g.* 315) that includes covalently direct bonded dielectric-to-

dielectric surfaces, prepared as described above. In various embodiments, the conductor-to-conductor (e.g., contact pad to contact pad) direct bonds and the dielectric-to-dielectric hybrid bonds can be formed using the direct bonding techniques disclosed at least in U.S. Patent Nos. 9,716,033 and 9,852,988, the entire contents of each of which are incorporated by reference herein in their entirety and for all purposes.

[0037] For example, dielectric bonding surfaces can be prepared and directly bonded to one another without an intervening adhesive as explained above. Conductive contact pads (which may be surrounded by nonconductive dielectric field regions) may also directly bond to one another without an intervening adhesive. In some embodiments, the respective contact pads can be recessed below exterior (e.g., upper) surfaces of the dielectric field or nonconductive bonding regions, for example, recessed by less than 30 nm, less than 20 nm, less than 15 nm, or less than 10 nm, for example, recessed in a range of 2 nm to 20 nm, or in a range of 4 nm to 10 nm. The nonconductive bonding regions can be directly bonded to one another without an adhesive at room temperature in some embodiments and, subsequently, the bonded structure can be annealed. Upon annealing, the contact pads can expand and contact one another to form a metal-to-metal direct bond. Beneficially, the use of hybrid bonding techniques, such as Direct Bond Interconnect, or DBI®, available commercially from Xperi of San Jose, CA, can enable high density of pads connected across the direct bond interface (e.g., small or fine pitches for regular arrays). In some embodiments, the pitch of the bonding pads, or conductive traces embedded in the bonding surface of one of the bonded elements, may be less 40 microns or less than 10 microns or even less than 2 microns. For some applications the ratio of the pitch of the bonding pads to one of the dimensions of the bonding pad is less than 5, or less than 3 and sometimes desirably less than 2. In other applications the width of the conductive traces embedded in the bonding surface of one of the bonded elements may range between 0.3 to 3 microns. In various embodiments, the contact pads and/or traces can comprise copper, although other metals may be suitable.

[0038] Thus, in direct bonding processes, a first element can be directly bonded to a second element without an intervening adhesive. In some arrangements, the first element can comprise a singulated element, such as a singulated integrated device die or singulated protective element. In other arrangements, the first element can comprise a carrier or substrate (e.g., a wafer) that includes a plurality (e.g., tens, hundreds, or more) of device regions that,

when singulated, form a plurality of integrated device dies. Similarly, the second element can comprise a singulated element, such as a singulated integrated device die. In other arrangements, the second element can comprise a carrier or substrate (*e.g.*, a wafer).

[0039] As explained herein, the first and second elements can be directly bonded to one another without an adhesive, which is different from a deposition process. In one application, a width of the first element in the bonded structure can be similar to a width of the second element. In some other embodiments, a width of the first element in the bonded structure can be different from a width of the second element. The width or area of the larger element in the bonded structure may be at least 10% larger than the width or area of the smaller element. The first and second elements can accordingly comprise non-deposited elements. Further, directly bonded structures, unlike deposited layers, can include a defect region along the bond interface in which nanovoids are present. The nanovoids may be formed due to activation of the bonding surfaces (*e.g.*, exposure to a plasma). As explained above, the bond interface can include concentration of materials from the activation and/or last chemical treatment processes. For example, in embodiments that utilize a nitrogen plasma for activation, a nitrogen peak can be formed at the bond interface. In embodiments that utilize an oxygen plasma for activation, an oxygen peak can be formed at the bond interface. In some embodiments, the bond interface can comprise silicon oxynitride, silicon oxycarbonitride, or silicon carbonitride. As explained herein, the direct bond can comprise a covalent bond, which is stronger than van Der Waals bonds. The bonding layers can also comprise polished surfaces that are planarized to a high degree of smoothness.

[0040] In various embodiments, the metal-to-metal bonds between the contact pads can be joined such that copper grains grow into each other across the bond interface. In some embodiments, the copper can have grains oriented along the crystal plane for improved copper diffusion across the bond interface. The bond interface can extend substantially entirely to at least a portion of the bonded contact pads, such that there is substantially no gap between the nonconductive bonding regions at or near the bonded contact pads. In some embodiments, a barrier layer may be provided under the contact pads (*e.g.*, which may include copper). In other embodiments, however, there may be no barrier layer under the contact pads, for example, as described in US 2019/0096741, which is incorporated by reference herein in its entirety and for all purposes.

[0041] In one aspect, a bonded structure is provided. The bonded structure includes a semiconductor element, including active circuitry (e.g. 116). The bonded structure also includes a protective element directly bonded to the semiconductor element without an adhesive along a bonding interface. The protective element includes an obstructive layer (i.e. 305) configured to inhibit external access to at least a portion of the active circuitry. The protective element may also include, additionally or alternatively, a protective circuitry layer (e.g. 410) disposed within it, and the protective circuitry layer is configured to detect or disrupt external access to the protective element, the active circuitry of the semiconductor element, or both.

[0042] In some embodiments, the obstructive layer of the protective element and the active circuitry of the semiconductor element are spaced apart from one another relative to the bonding interface. In some embodiments, the spacing between the obstructive layer of the protective element and the active circuitry of the semiconductor element is between 50 micrometers and 100 micrometers. In some embodiments, the protective circuitry layer of the protective element and the obstructive layer of the protective element are spaced apart from one another along a direction transverse to the bonding interface. In some embodiments, the spacing between the protective circuitry layer and the obstructive layer of the protective element is at least 20 micrometers. In some embodiments, the protective circuitry layer of the protective element is disposed between the obstructive layer of the protective element and the bond interface. In some embodiments, the obstructive layer of the protective element is disposed between the protective circuitry layer of the protective element and the bond interface. In some embodiments, the obstructive layer of the protective element includes an occlusive layer configured to occlude a predefined area of the semiconductor element in the plane parallel to the layer's surface. In some embodiments, the protective element includes a bonding layer directly bonded to a bonding layer of the semiconductor element. In some embodiments, the bonding layer of the protective element is metallized in a pattern that matches at least a portion of a metallization pattern of a bonding layer of the protective element. In some embodiments, the bonding layer of the semiconductor element includes a number of contact pads disposed in a nonconductive layer, and the bonding layer of the protective element includes a number of contact pads disposed in a nonconductive layer directly bonded to the contact pads of the semiconductor element. In some embodiments, the bonding layer of the

protective element and the protective circuitry layer of the protective element are connected through one or more vertical interconnects (e.g. 360). In some embodiments, the obstructive layer of the protective element includes a detection circuit configured to detect external access of the protective element. In some embodiments, the detection circuit includes a passive electronic circuit element configured to detect external access. In some embodiments, the passive electronic circuit includes a capacitive circuit element, a resistive circuit element, or both. In some embodiments, the passive electronic circuit element includes a resistive element comprising a patterned trace. In some embodiments, the passive electronic circuit element includes a capacitive element comprising a plurality of traces separated by an insulating material. In some embodiments, the detection circuit includes active circuitry. In some embodiments, a vertical interconnect extends from the detection circuit to a contact pad of the protective element. In some embodiments, a vertical interconnect extends from the detection circuit to the protective circuitry layer of the protective element. In some embodiments, one or more contact pads of the protective element are bonded to a contact pad at an active side of the semiconductor element. In some embodiments, the protective circuitry layer of the protective element includes a passive electronic circuit configured to mimic the appearance of active circuitry. In some embodiments, the protective circuitry layer of the protective element includes active circuitry. In some embodiments, the active circuitry of the protective circuitry layer is configured to emit an encrypted timing signal. In some embodiments, the active circuitry of the protective circuitry layer is configured to detect changes to the protective circuitry layer. In some embodiments, the active circuitry of the protective circuitry layer is configured to disable the active circuitry of the semiconductor when it detects a change to the protective circuitry layer. In some embodiments, the protective circuitry layer is configured to emit an alarm signal when the active circuitry of the protective circuitry layer detects a change to the protective circuitry layer. In some embodiments, a vertical interconnect extends from the protective circuitry layer to a contact pad of the protective element. In some embodiments, the protective element is directly bonded to a back side (e.g. 112) of the semiconductor element opposite an active side (e.g. 114), and a through semiconductor via (e.g. 330) extends from a contact pad at or near the active side of the semiconductor element to a contact pad of the protective element providing electrical communication between the semiconductor element

and the protective circuitry layer of the protective element. In some embodiments, the protective circuitry layer is completely embedded within the protective element.

[0043] In another aspect, a method is provided for forming a bonded structure. The method includes directly bonding a semiconductor element to a protective element without an adhesive. The semiconductor element includes active circuitry, and the protective element includes an obstructive layer configured to inhibit external access to a portion of the active circuitry and a protective layer configured to detect or disrupt external access to the protective element, the semiconductor element, or both.

[0044] In some embodiments, the method includes forming the protective element such that the obstructive layer of the protective element and the protective layer of the protective element are spaced apart from one another along a direction transverse to the bonding interface. In some embodiments, the method includes forming the protective element such that the spacing between the obstructive layer and the protective layer is at least 20 micrometers. In some embodiments, the method includes forming the protective element such that the spacing between the obstructive layer of the protective element and the active circuitry of the protective element is at least 20 micrometers. In some embodiments, the method includes forming the protective element to include a bonding layer, forming the semiconductor element to include a bonding layer, and bonding the bonding layer of the protective element to the bonding layer of the semiconductor element. In some embodiments, the method includes forming the protective element such that the bonding layer of the protective element is metallized to match a metallization pattern of the semiconductor element. In some embodiments, the method includes forming the protective element such that the bonding layer of the protective element includes a number of contact pads disposed in a nonconductive layer configured to mirror a plurality of contact pads of the bonding layer of the semiconductor element. In some embodiments, the method includes forming the protective element such that the obstructive layer includes a detection circuit configured to detect external access to the protective element. In some embodiments, the method includes forming the protective element to include a vertical interconnect extending from the detection circuit to a contact pad of the protective element. In some embodiments, the method includes directly bonding the protective element to a back side of the semiconductor element that is directly opposite an active side of the semiconductor element, and forming the semiconductor element to include a through

semiconductor via (TSV) extending from a contact pad at or near the active side of the semiconductor to a contact pad of the protective element such that the TSV provides electrical communication between the semiconductor element and the detection circuit. In some embodiments, the method includes forming the protective element to include a vertical interconnect extending from the detection circuit to the protective layer of the protective element, and a second vertical interconnect extending from the protective layer of the protective element to a contact pad of the protective element. In some embodiments, the method includes forming the protective circuitry layer to include a passive electronic circuit configured to mimic the appearance of active circuitry. In some embodiments, the method includes forming the protective circuitry layer to include active circuitry. In some embodiments, the method includes configuring the active circuitry of the protective circuitry layer to emit an encrypted timing signal. In some embodiments, the method includes configuring the active circuitry of the protective circuitry layer to detect changes to the protective circuitry layer. In some embodiments, the method includes configuring the active circuitry of the protective circuitry layer to disable the active circuitry of the semiconductor element when the active circuitry of the protective circuitry layer detects a change to the protective circuitry layer. In some embodiments, the method includes configuring the active circuitry of the protective circuitry layer to emit an alarm signal when the active circuitry of the protective circuitry layer detects a change to the protective circuitry layer. In some embodiments, the method includes forming the protective element to include a vertical interconnect extending from the protective circuitry layer to a contact pad of the protective element. In some embodiments, the method includes directly bonding the protective element to a back side of the semiconductor element that is directly opposite an active side of the semiconductor element, and forming the semiconductor element to include a through semiconductor via (TSV) extending from a contact pad at or near the active side of the semiconductor to a contact pad of the protective element such that the TSV provides electrical communication between the semiconductor element and the protective layer of the protective element. In some embodiments, the method includes forming the protective element such that the protective circuitry layer is completely embedded within the protective element.

[0045] In another aspect, a bonded structure is provided. The bonded structure includes a semiconductor element that includes active circuitry, and a protective element that

is directly bonded to the semiconductor element without an adhesive along a bonding interface. The protective element includes a protective circuitry layer configured to detect or disrupt external access to the protective element, the active circuitry of the semiconductor element, or both.

[0046] In some embodiments, the protective layer of the protective element and the active circuitry of the semiconductor element are spaced apart from one another along a direction transverse to the bonding interface. In some embodiments, the spacing between the obstructive layer of the protective element and the active circuitry of the semiconductor element is at least 20 micrometers. In some embodiments, the protective element includes a bonding layer, and the semiconductor element includes a bonding layer directly bonded to the bonding layer of the protective element. In some embodiments, the bonding layer of the protective element is metallized to match a metallization pattern of the semiconductor element. In some embodiments, the bonding layer of the semiconductor element includes a number of contact pads disposed in a nonconductive layer, and the bonding layer of the protective element includes a number of contact pads disposed in a nonconductive layer directly bonded to the contact pads of the semiconductor element. In some embodiments, the protective layer of the protective element includes a passive electronic circuit configured to mimic the appearance of active circuitry. In some embodiments, the protective layer of the protective element includes active circuitry. In some embodiments, the active circuitry of the protective circuitry layer is configured to emit an encrypted timing signal. In some embodiments, the active circuitry of the protective circuitry layer is configured to detect changes to the protective element. In some embodiments, the active circuitry of the protective circuitry layer is configured to disable the active circuitry of the semiconductor element when the active circuitry of the protective circuitry layer detects a change to the protective element. In some embodiments, the protective circuitry layer is configured to emit an alarm signal when it detects a change to the protective element. In some embodiments, the bonded structure includes a vertical interconnect extending from the protective layer of the protective element to a contact pad of the protective element. In some embodiments, the protective element is directly bonded to a back side of the semiconductor element opposite an active side, and a through semiconductor via (TSV) extends from a contact pad at or near the active side of the semiconductor element to a contact pad of the protective element, such that the TSV provides electrical communication between

the semiconductor element and the protective layer of the protective element. In some embodiments, the protective circuitry layer of the protective element is completely embedded within the protective element.

[0047] Unless the context clearly requires otherwise, throughout the description and the claims, the words “comprise,” “comprising,” “include,” “including” and the like are to be construed in an inclusive sense, as opposed to an exclusive or exhaustive sense; that is to say, in the sense of “including, but not limited to.” The word “coupled”, as generally used herein, refers to two or more elements that may be either directly connected, or connected by way of one or more intermediate elements. Likewise, the word “connected”, as generally used herein, refers to two or more elements that may be either directly connected, or connected by way of one or more intermediate elements. Additionally, the words “herein,” “above,” “below,” and words of similar import, when used in this application, shall refer to this application as a whole and not to any particular portions of this application. Moreover, as used herein, when a first element is described as being “on” or “over” a second element, the first element may be directly on or over the second element, such that the first and second elements directly contact, or the first element may be indirectly on or over the second element such that one or more elements intervene between the first and second elements. Where the context permits, words in the above Detailed Description using the singular or plural number may also include the plural or singular number respectively. The word “or” in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list, and any combination of the items in the list.

[0048] Moreover, conditional language used herein, such as, among others, “can,” “could,” “might,” “may,” “e.g.,” “for example,” “such as” and the like, unless specifically stated otherwise, or otherwise understood within the context as used, is generally intended to convey that certain embodiments include, while other embodiments do not include, certain features, elements and/or states. Thus, such conditional language is not generally intended to imply that features, elements and/or states are in any way required for one or more embodiments.

[0049] While certain embodiments have been described, these embodiments have been presented by way of example only, and are not intended to limit the scope of the disclosure. Indeed, the novel apparatus, methods, and systems described herein may be

embodied in a variety of other forms; furthermore, various omissions, substitutions and changes in the form of the methods and systems described herein may be made without departing from the spirit of the disclosure. For example, while blocks are presented in a given arrangement, alternative embodiments may perform similar functionalities with different components and/or circuit topologies, and some blocks may be deleted, moved, added, subdivided, combined, and/or modified. Each of these blocks may be implemented in a variety of different ways. Any suitable combination of the elements and acts of the various embodiments described above can be combined to provide further embodiments. The accompanying claims and their equivalents are intended to cover such forms or modifications as would fall within the scope and spirit of the disclosure.

WHAT IS CLAIMED IS:

1. A bonded structure comprising:
a semiconductor element comprising active circuitry; and
a protective element directly bonded to the semiconductor element without an adhesive along a bonding interface, the protective element comprising:
an obstructive layer configured to inhibit external access to at least a portion of the active circuitry; and
a protective circuitry layer disposed within the protective element, the protective circuit layer configured to detect or disrupt external access to the active circuitry of the semiconductor element.
2. The bonded structure of claim 1, wherein the protective element is directly bonded to a back side of the semiconductor element opposite an active front side of the semiconductor element, the active circuitry of the semiconductor element disposed closer to the active front side than to the back side.
3. The bonded structure of claim 1, wherein the obstructive layer of the protective element and the active circuitry of the semiconductor element are spaced apart from one another along a direction transverse to the bonding interface.
4. The bonded structure of claim 1, wherein the spacing between the obstructive layer of the protective element and the active circuitry of the semiconductor element is at least 20 micrometers.
5. The bonded structure of claim 1, wherein the spacing between the obstructive layer of the protective element and the active circuitry of the semiconductor element is between 50 micrometers and 100 micrometers.
6. The bonded structure of claim 1, wherein the protective circuitry layer of the protective element and the obstructive layer of the protective element are spaced apart from one another along a direction transverse to the bonding interface.

7. The bonded structure of claim 6, wherein the spacing between the protective circuitry layer of the protective element and the obstructive layer of the protective element is at least 20 micrometers.

8. The bonded structure of claim 1, wherein the protective circuitry layer of the protective element is disposed between the obstructive layer of the protective element and the bond interface.

9. The bonded structure of claim 1, wherein the obstructive layer of the protective element is disposed between the protective circuitry layer of the protective element and the bond interface.

10. The bonded structure of claim 1, wherein the obstructive layer of the protective element further comprises an occlusive layer configured to occlude a predefined area of the semiconductor element in the plane parallel to the layer's surface.

11. The bonded structure of claim 1, wherein the protective element further comprises a bonding layer, and wherein the protective element further comprises a bonding layer directly bonded to the bonding layer of the semiconductor element.

12. The bonded structure of claim 11, wherein the bonding layer of the protective element is metallized to match at least a portion of a metallization pattern of the bonding layer of the semiconductor element.

13. The bonded structure of claim 12, wherein the bonding layer of the semiconductor element comprises a plurality of contact pads disposed in a nonconductive layer, and wherein the bonding layer of the protective element comprises a plurality of contact pads disposed in a nonconductive layer directly bonded to the contact pads of the semiconductor element.

14. The bonded structure of claim 10, wherein the bonding layer of the protective element and the protective circuitry layer of the protective element are connected through at least one vertical interconnect.

15. The bonded structure of any one of claims 1 to 14 wherein the obstructive layer of the protective element comprises a detection circuit configured to detect external access of the protective element.

16. The bonded structure of claim 15, wherein the detection circuit comprises a passive electronic circuit element configured to detect the external access.

17. The bonded structure of claim 16, wherein the passive electronic circuit comprises at least one of a capacitive circuit element and a resistive circuit element.

18. The bonded structure of claim 17, wherein the passive electronic circuit element comprises the resistive element, and wherein the resistive element further comprises a patterned trace.

19. The bonded structure of claim 17, wherein the passive electronic circuit element comprises the capacitive element, and wherein the capacitive element further comprises a plurality of traces separated by an insulating material.

20. The bonded structure of claim 15, wherein the detection circuit further comprises active circuitry.

21. The bonded structure of any one of claims 15 to 20, further comprising a vertical interconnect extending from the detection circuit to a contact pad of the protective element.

22. The bonded structure of any one of claims 15 to 20, further comprising a vertical interconnect extending from the detection circuit to the protective circuitry layer of the protective element.

23. The bonded structure of Claim 21, wherein the contact pad of the protective element is directly bonded to a contact pad at an active side of the semiconductor element.

24. The bonded structure of any one of claims 1 to 23, wherein the protective circuitry layer of the protective element further comprises a passive electronic circuit configured to mimic the appearance of active circuitry.

25. The bonded structure of any one of claims 1 to 23, wherein the protective circuitry layer of the protective element further comprises second active circuitry.

26. The bonded structure of claim 25, wherein the second active circuitry of the protective circuitry layer is configured to emit an encrypted timing signal.

27. The bonded structure of claim 25, wherein the second active circuitry of the protective circuitry layer is configured to detect changes to the protective circuitry layer.

28. The bonded structure of claim 27, wherein the second active circuitry of the protective circuitry layer is configured to disable the active circuitry of the semiconductor when the active circuitry of the protective circuitry layer detects a physical change to the protective circuitry layer.

29. The bonded structure of claim 27, wherein the protective circuitry layer is configured to emit an alarm signal when the second active circuitry of the protective circuitry layer detects a change to the protective circuitry layer.

30. The bonded structure of any one of claims 25 to 29, further comprising a vertical interconnect extending from the protective circuitry layer of the protective element to a contact pad of the protective element.

31. The bonded structure of claim 30, further comprising a through semiconductor via (TSV) extending from a contact pad at or near the active side of the semiconductor element to the contact pad of the protective element, the TSV providing electrical communication between the semiconductor element and the protective circuitry layer of the protective element.

32. The bonded structure of any one of claims 1 to 31, wherein the protective circuitry layer of the protective element is completely embedded within the protective element.

33. A method of forming a bonded structure, the method comprising:
directly bonding a semiconductor element to a protective element without an adhesive, the semiconductor element comprising active circuitry, and the protective element comprising an obstructive layer and a protective circuitry layer disposed within the protective element, the obstructive layer configured to inhibit external access to at least a portion of the active circuitry and the protective circuitry layer configured to detect or disrupt external access to the active circuitry of the semiconductor element.

34. The method of claim 33, further comprising:
forming the protective element such that the obstructive layer of the protective element and the protective layer of the protective element are spaced apart from one another along a direction transverse to the bonding interface.

35. The method of claim 34, further comprising:
forming the protective element such that the spacing between the obstructive layer of the protective element and the protective layer of the protective element is at least 20 micrometers.

36. The method of claim 34, further comprising:
forming the protective element such that the spacing between the obstructive layer of the protective element and the active circuitry of the semiconductor element is at least 20 micrometers.

37. The method of any one of claims 33 to 36, further comprising:
forming the protective element to comprise a bonding layer;
forming the semiconductor element to comprise a bonding layer; and
bonding the bonding layer of the protective element to the bonding layer of the semiconductor element.

38. The method of claim 37, further comprising:

forming the protective element such that the bonding layer of the protective element is metallized to match a metallization pattern of the semiconductor element.

39. The method of claim 38, further comprising:

forming the protective element such that the bonding layer of the protective element comprises a plurality of contact pads disposed in a nonconductive layer, the contact pads configured to mirror a plurality of contact pads of the bonding layer of the semiconductor element.

40. The method of any one of claims 33 to 39 further comprising:

forming the protective element such that the obstructive layer comprises a detection circuit configured to detect external access of the protective element.

41. The method of claim 40, further comprising:

forming the protective element to include a vertical interconnect extending from the detection circuit to a contact pad of the protective element.

42. The method of claim 41, further comprising:

directly bonding the protective element to a back side of the semiconductor element that is directly opposite an active side of the semiconductor element, wherein the active circuitry of the semiconductor element is disposed at or near the active side of the semiconductor element and further comprises a through semiconductor via (TSV) extending from a contact pad at or near the active side of the semiconductor element to the contact pad of the protective element, the TSV providing electrical communication between the semiconductor element and the detection circuit.

43. The method of claim 40, further comprising:

forming the protective element to include a first vertical interconnect extending from the detection circuit to the protective layer of the protective element, and a second

vertical interconnect extending from the protective layer of the protective element to a contact pad of the protective element.

44. The method of any one of claims 33 to 43, further comprising:

forming the protective circuitry layer to comprise a passive electronic circuit configured to mimic the appearance of active circuitry.

45. The method of any one of claims 33 to 43, further comprising:

forming the protective circuitry layer to comprise second active circuitry.

46. The method of claim 45, further comprising:

configuring the second active circuitry of the protective circuitry layer to emit an encrypted timing signal.

47. The method of claim 45, further comprising:

configuring the second active circuitry of the protective circuitry layer to detect changes to the protective circuitry layer.

48. The method of claim 47, further comprising:

configuring the second active circuitry of the protective circuitry layer to disable the active circuitry of the semiconductor element when the active circuitry of the protective circuitry layer detects changes to the protective circuitry layer.

49. The method of claim 47, further comprising:

configuring the second active circuitry of the protective circuitry layer to emit an alarm signal when the active circuitry of the protective circuitry layer detects a change to the protective circuitry layer.

50. The method of any one of claims 45 to 49, further comprising:

forming the protective element to include a vertical interconnect extending from the protective circuitry layer of the protective element to a contact pad of the protective element.

51. The method of claim 50, further comprising:

directly bonding the protective element to a back side of the semiconductor element that is directly opposite an active side of the semiconductor element, wherein the active circuitry of the semiconductor element is disposed at or near the active side of the semiconductor element and further comprises a through semiconductor via (TSV) extending from a contact pad at or near the active side of the semiconductor element to the contact pad of the protective element, the TSV providing electrical communication between the semiconductor element and the protective layer of the protective element.

52. The method of any one of claims 33 to 51, further comprising:

forming the protective element such that the protective circuitry layer is completely embedded within the protective element.

53. A bonded structure comprising:

a semiconductor element comprising first active circuitry; and

a protective element directly bonded to the semiconductor element without an adhesive along a bonding interface, the protective element comprising a protective circuitry layer disposed within the protective element, the protective circuit layer having second active circuitry configured to detect or disrupt external access to the first active circuitry of the semiconductor element.

54. The bonded structure of claim 53, wherein the protective element is directly bonded to a back side of the semiconductor element opposite an active front side of the semiconductor element, the first active circuitry of the semiconductor element disposed closer to the active front side than to the back side.

55. The bonded structure of claim 53, wherein the protective layer of the protective element and the active circuitry of the semiconductor element are spaced apart from one another along a direction transverse to the bonding interface.

56. The bonded structure of claim 55, wherein the spacing between the obstructive layer of the protective element and the active circuitry of the semiconductor element is at least 20 micrometers.

57. The bonded structure of any of claims 53 to 56, wherein the protective element further comprises a bonding layer, and wherein the semiconductor element further comprises a bonding layer directly bonded to the bonding layer of the first semiconductor element.

58. The bonded structure of claim 57, wherein the bonding layer of protective element is metallized to match a metallization pattern of the semiconductor element.

59. The bonded structure of claim 58, wherein the bonding layer of the semiconductor element comprises a plurality of contact pads disposed in a nonconductive layer, and wherein the bonding layer of the protective element comprises a plurality of contact pads disposed in a nonconductive layer directly bonded to the contact pads of the semiconductor element.

60. The bonded structure of any one of claims 53 to 59, wherein the protective layer of the protective element further comprises a passive electronic circuit configured to mimic the appearance of active circuitry.

61. The bonded structure of any one of claims 53 to 59, wherein the protective layer of the protective element further comprises second active circuitry.

62. The bonded structure of claim 61, wherein the second active circuitry of the protective circuitry layer is configured to emit an encrypted timing signal.

63. The bonded structure of claim 61, wherein the second active circuitry of the protective circuitry layer is configured to detect changes to the protective element.

64. The bonded structure of claim 63, wherein the second active circuitry of the protective circuitry layer is configured to disable the active circuitry of the semiconductor element when the active circuitry of the protective circuitry layer detects a change to the protective element.

65. The bonded structure of claim 63, wherein the protective circuitry layer is configured to emit an alarm signal when the second active circuitry of the protective circuitry layer detects a change to the protective element.

66. The bonded structure of any one of claims 61 or 65, further comprising a vertical interconnect extending from the protective layer of the protective element to a contact pad of the protective element.

67. The bonded structure of claim 66, wherein the protective element is directly bonded to a back side of the semiconductor element opposite an active side, the bonded structure further comprising a through semiconductor via (TSV) extending from a contact pad at or near the active side of the semiconductor element to the contact pad of the protective element, the TSV providing electrical communication between the semiconductor element and the protective layer of the protective element.

68. The bonded structure of any one of claims 53 to 67, wherein the protective circuitry layer of the protective element is completely embedded within the protective element.

69. A bonded structure comprising:

a semiconductor element comprising active circuitry; and

a protective element directly bonded to a back side of the semiconductor element without an adhesive along a bonding interface, the protective element comprising:

an obstructive layer configured to inhibit external access to the active circuitry of the semiconductor element; and

a protective circuitry layer disposed within the protective element, the protective circuit layer configured to detect or disrupt external access to the active circuitry of the semiconductor element.

70. The bonded structure of claims 69, further comprising a second protective element directly bonded to a front side of the semiconductor element without an adhesive along a second bonding interface, the second protective element comprising:

a second obstructive layer configured to inhibit external access to at least the frontside of the semiconductor element; and

a second protective circuitry layer disposed within the protective element, the protective circuit layer configured to detect or disrupt external access to the front side of the semiconductor element.

71. The bonded structure of claim 69, wherein the protective circuitry layer of the protective element is disposed between the obstructive layer of the protective element and the bond interface.

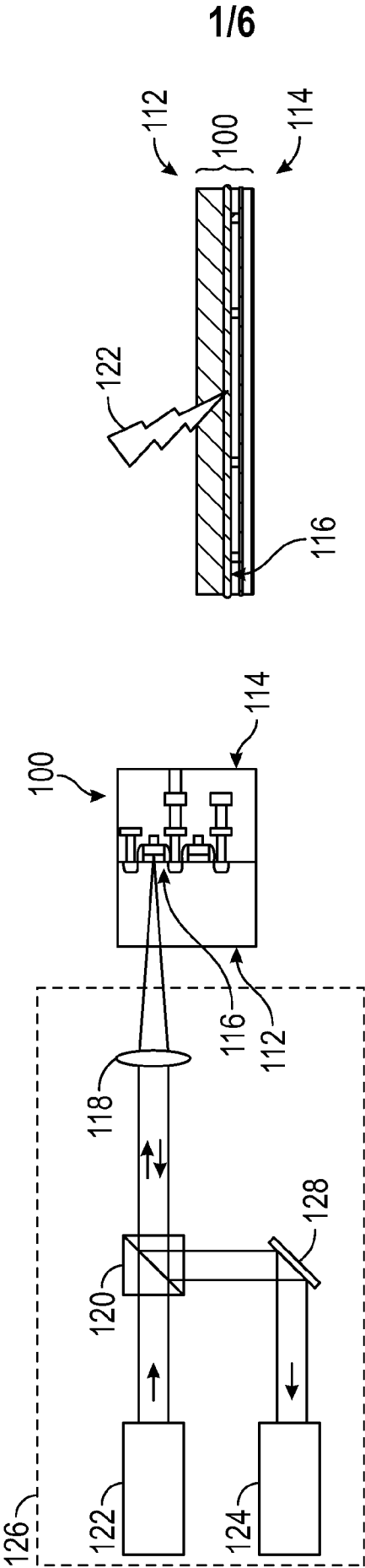
72. The bonded structure of claim 69, wherein the obstructive layer of the protective element is disposed between the protective circuitry layer of the protective element and the bond interface.

73. A bonded structure comprising:

a semiconductor element comprising active circuitry; and

a protective element directly bonded to a back side of the semiconductor element without an adhesive along a bonding interface, the protective element comprising an obstructive layer configured to inhibit external access to the active circuitry of the semiconductor element, wherein the obstructive layer is vertically separated from the active circuitry by a distance of at least 20 microns.

74. The bonded structure of claim 73, further comprising a protective circuitry layer disposed within the protective element, the protective circuit layer configured to detect or disrupt external access to the active circuitry of the semiconductor element.



2/6

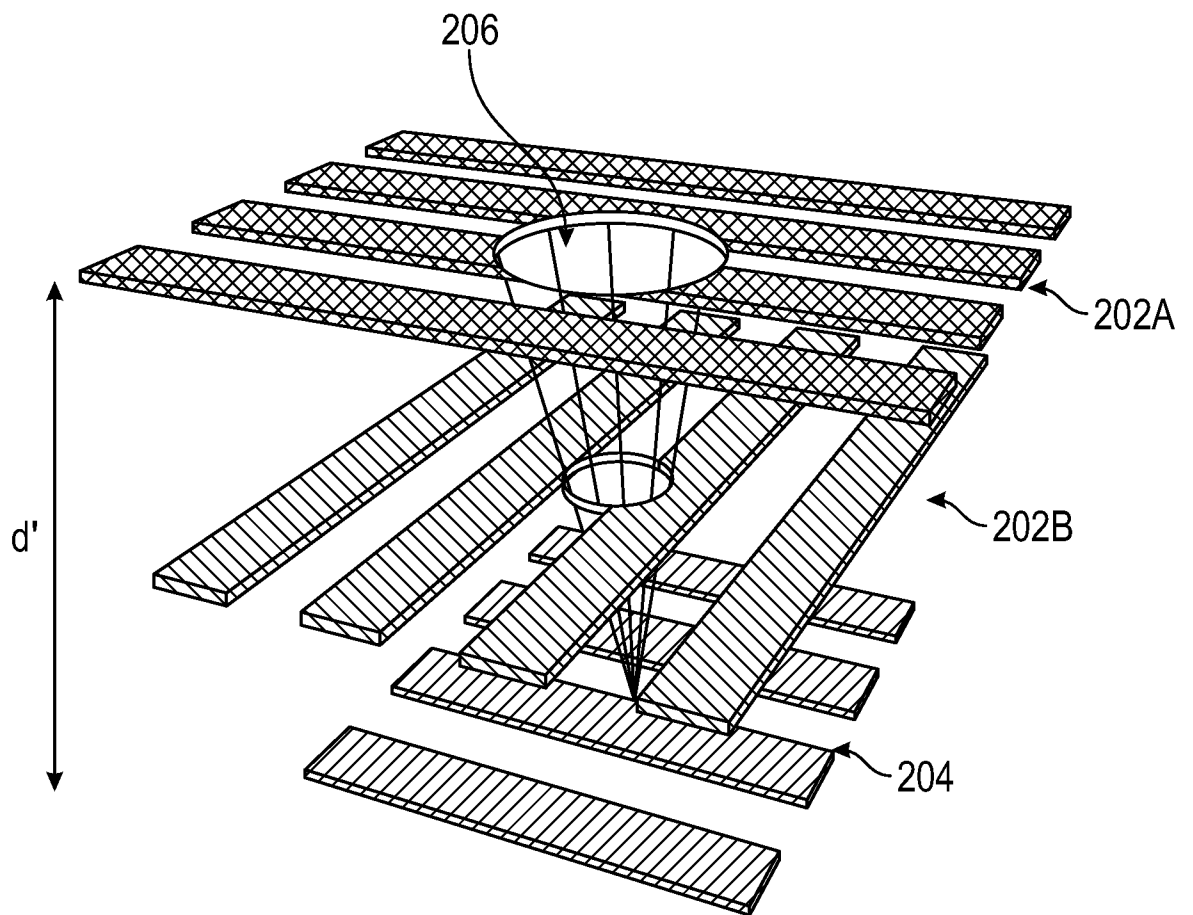


FIG. 2

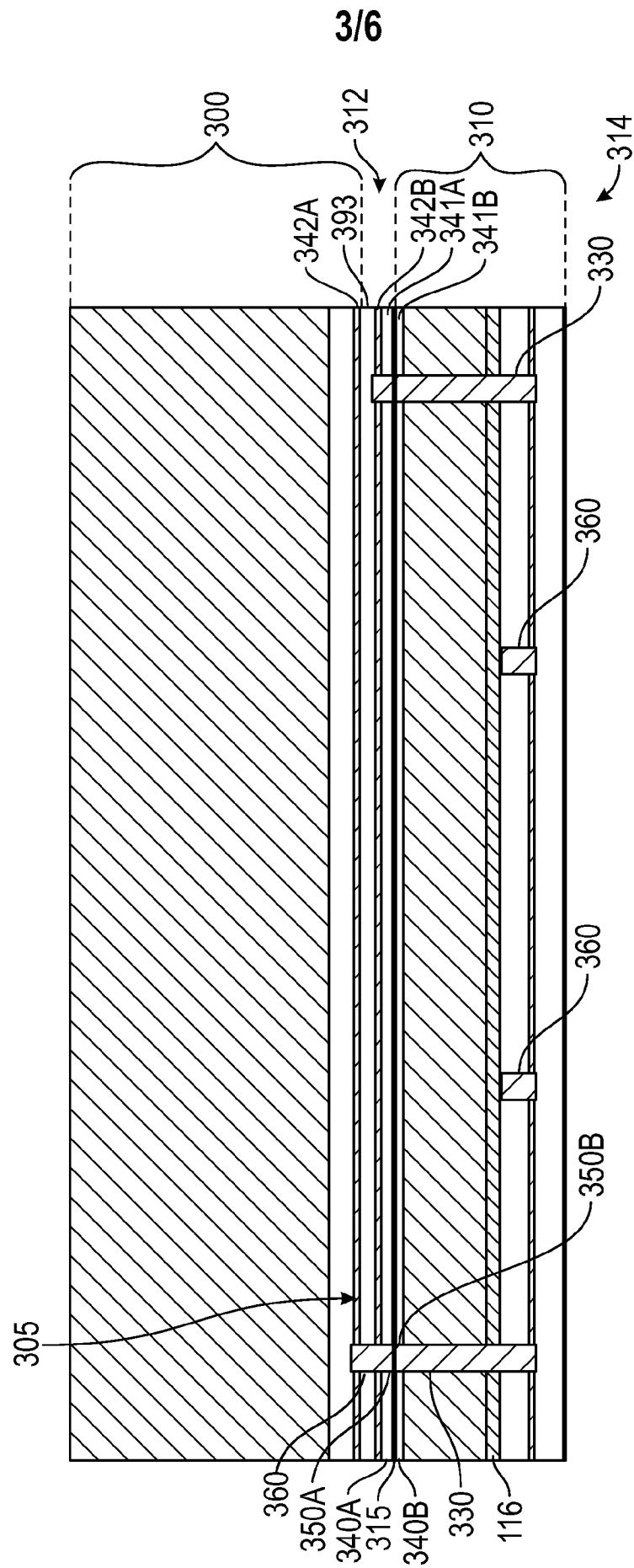


FIG. 3

4/6

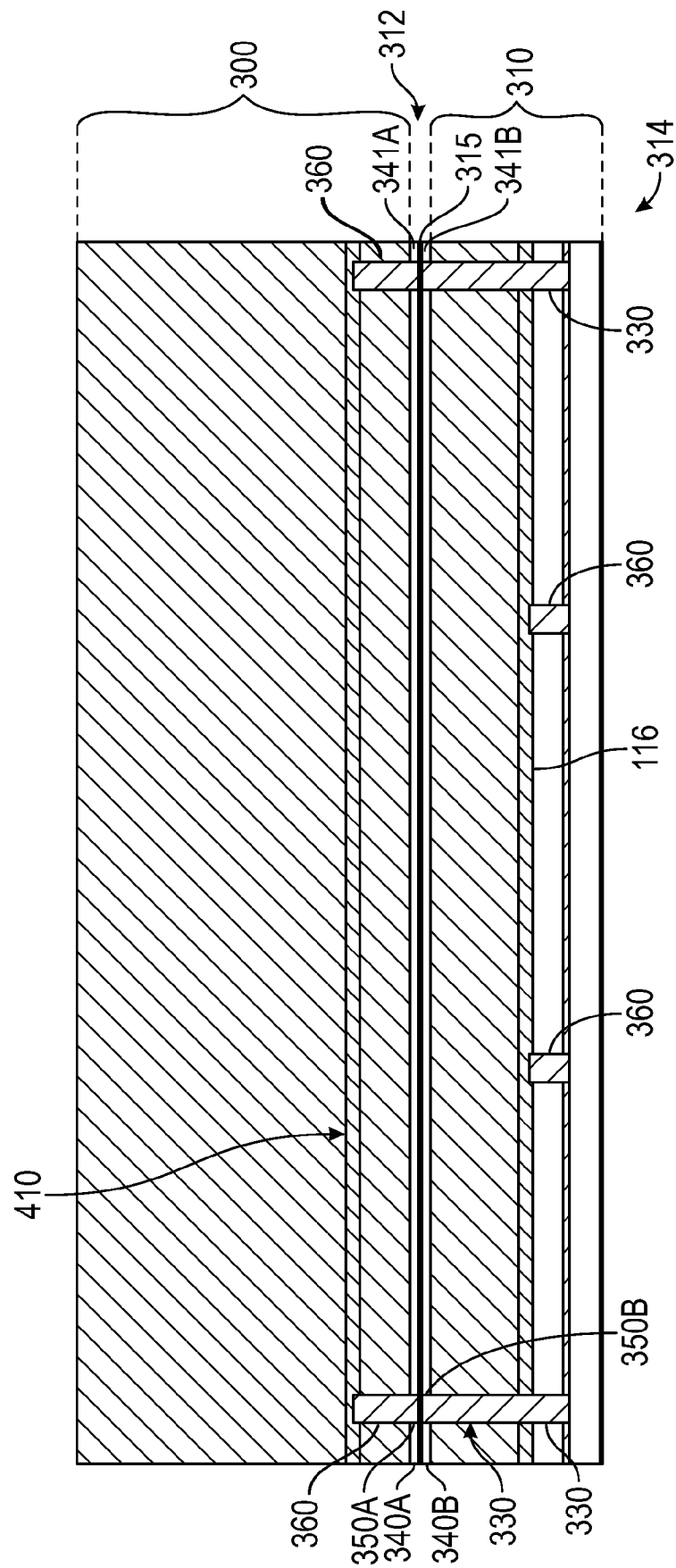


FIG. 4A

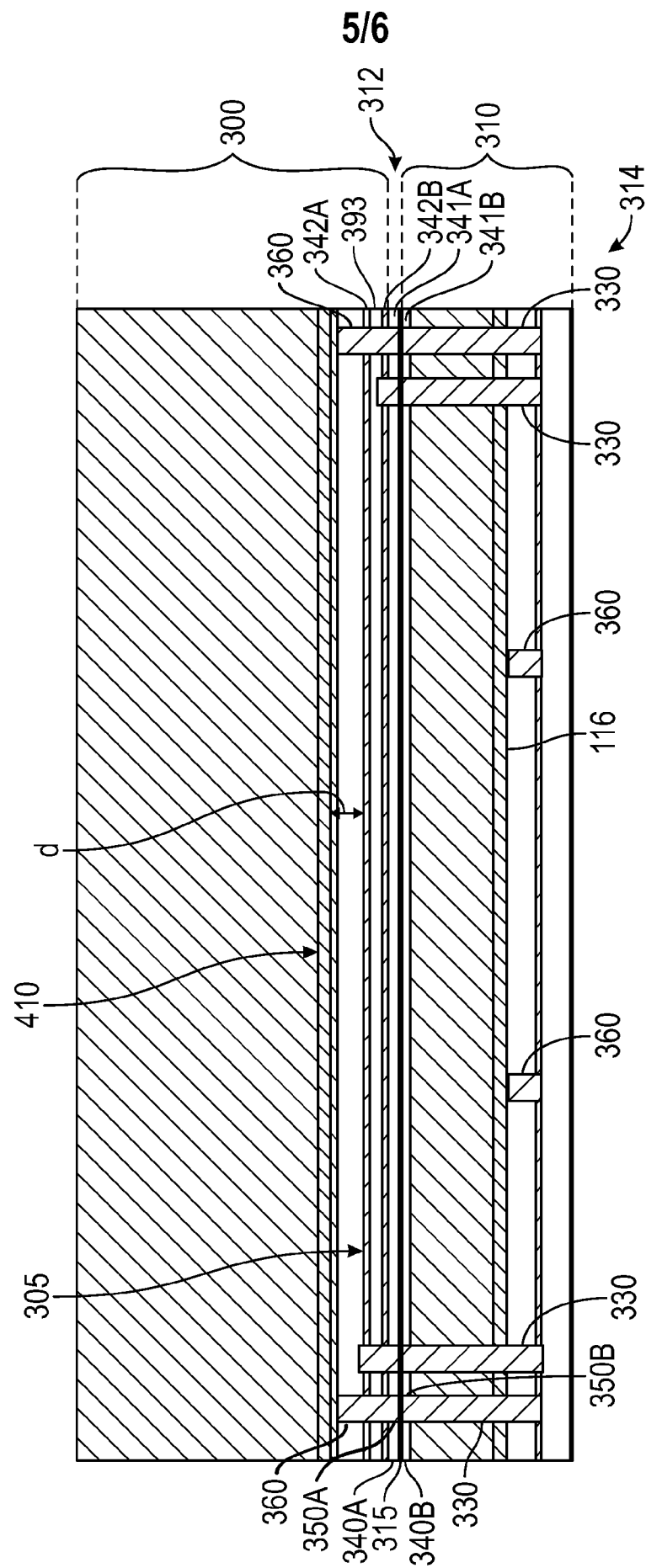


FIG. 4B

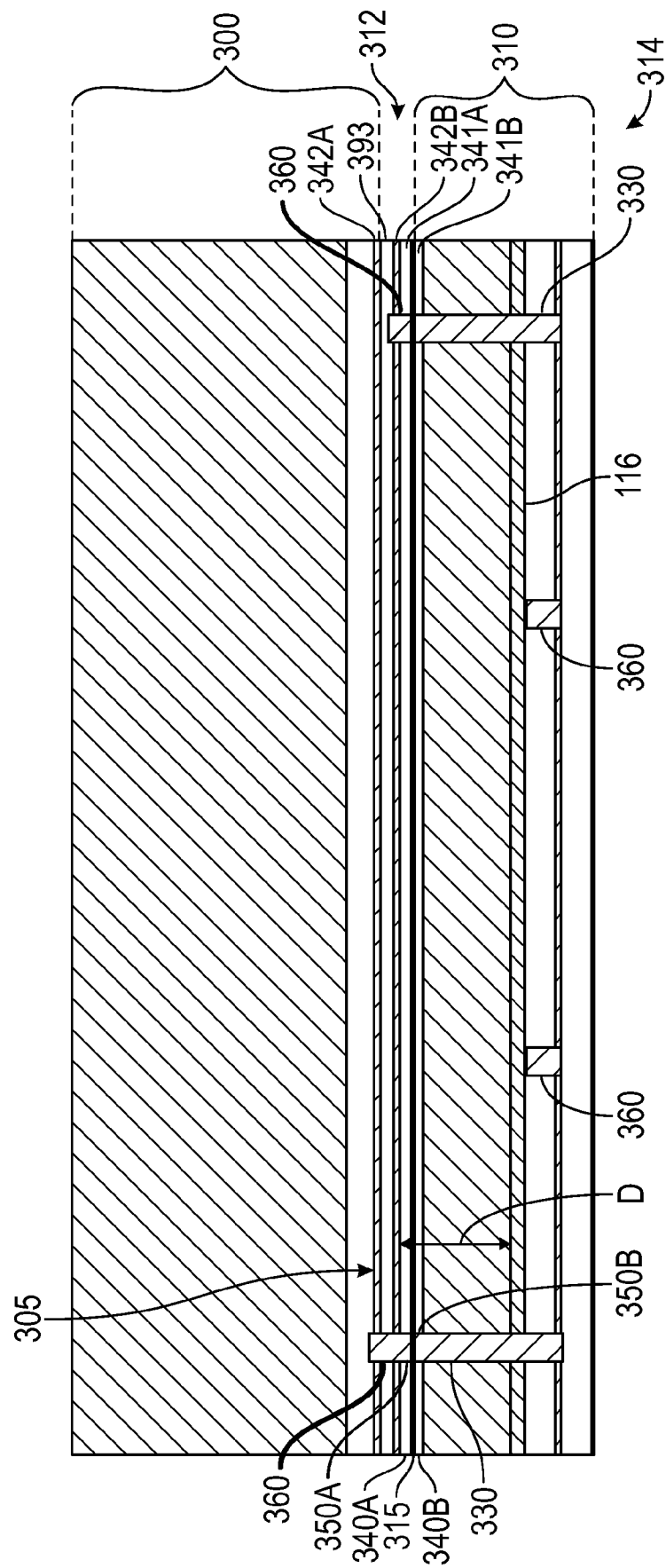


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2022/038921

A. CLASSIFICATION OF SUBJECT MATTER H01L 23/00(2006.01)i; H01L 23/552(2006.01)i; H01L 23/48(2006.01)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) H01L 23/00(2006.01); G01R 31/28(2006.01); G06F 21/55(2013.01); G06F 21/75(2013.01); H01L 21/66(2006.01); H01L 23/528(2006.01); H01L 23/58(2006.01) Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean utility models and applications for utility models Japanese utility models and applications for utility models Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKOMPASS(KIPO internal) & Keywords: semiconductor, protective element, bonding, external access, protective circuitry layer		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2020-0328164 A1 (INVENSAS BONDING TECHNOLOGIES, INC.) 15 October 2020 (2020-10-15) paragraphs [0018]-[0049], claim 1 and figures 1-6B	1-20,33-39,53-59,69-74
Y	US 2020-0371154 A1 (INVENSAS BONDING TECHNOLOGIES, INC.) 26 November 2020 (2020-11-26) paragraphs [0029], [0035] and figure 2B	1-20,33-39,53-59,69-74
A	US 2018-0308808 A1 (NUVOTON TECHNOLOGY CORPORATION) 25 October 2018 (2018-10-25) paragraphs [0016]-[0067] and figures 1-3	1-20,33-39,53-59,69-74
A	US 9455233 B1 (FREESCALE SEMICONDUCTOR, INC.) 27 September 2016 (2016-09-27) claims 1-17 and figures 1-2	1-20,33-39,53-59,69-74
A	KR 10-2020-0141783 A (INDUSTRY-ACADEMIC COOPERATION FOUNDATION, YONSEI UNIVERSITY) 21 December 2020 (2020-12-21) paragraphs [0024]-[0094] and figures 1-13	1-20,33-39,53-59,69-74
☐ 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 "D" document cited by the applicant in the international application "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 25 November 2022		Date of mailing of the international search report 25 November 2022
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon 35208, Republic of Korea Facsimile No. +82-42-481-8578		Authorized officer JANG, Gi Jeong Telephone No. +82-42-481-8364

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2022/038921

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: **23,26-29,31,41-43,46-49,51,62-65,67**
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

Claims 23, 26-29, 31, 41-43, 46-49, 51, 62-65, 67 are regarded to be unclear because they refer to claims which do not comply with PCT Rule 6.4(a).

3. ☒ Claims Nos.: **21,22,24,25,30,32,40,44,45,50,52,60,61,66,68**
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/US2022/038921

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2020-0328164	A1	15 October 2020	CN	113646881	A	12 November 2021
				CN	113678243	A	19 November 2021
				KR	10-2021-0139461	A	22 November 2021
				KR	10-2021-0139483	A	22 November 2021
				US	11205625	B2	21 December 2021
				US	11373963	B2	28 June 2022
				US	2020-0328162	A1	15 October 2020
				US	2020-0328165	A1	15 October 2020
				WO	2020-210676	A1	15 October 2020
				WO	2020-210703	A1	15 October 2020
US	2020-0371154	A1	26 November 2020	None			
US	2018-0308808	A1	25 October 2018	JP	2018-186271	A	22 November 2018
				JP	6635276	B2	22 January 2020
				TW	201839652	A	01 November 2018
				TW	I665581	B	11 July 2019
				US	10249579	B2	02 April 2019
US	9455233	B1	27 September 2016	None			
KR	10-2020-0141783	A	21 December 2020	KR	10-2245773	B1	27 April 2021
				US	11387196	B2	12 July 2022
				US	2020-0395315	A1	17 December 2020