(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 May 2020 (22.05.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/101867 A1

(51) International Patent Classification:
G01R 31/311 (2006.01) *G06F 21/76* (2013.01)

(21) International Application Number:
PCT/US2019/058254

(22) International Filing Date:
28 October 2019 (28.10.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/767,288	14 November 2018 (14.11.2018)	US
62/792,012	14 January 2019 (14.01.2019)	US
62/801,698	06 February 2019 (06.02.2019)	US
16/597,013	09 October 2019 (09.10.2019)	US

(71) Applicant: **MASSACHUSETTS INSTITUTE OF TECHNOLOGY** [US/US]; 77 Massachusetts Avenue, Cambridge, MA 02139 (US).

(72) Inventors: **BUSH, Kevin, B.**; 128 Plympton Road, Sudbury, MA 01776 (US). **HICKS, Matthew, D.**; 2003 Northside Drive, Blacksburg, VA 24060 (US). **TRIPPEL, Timothy, D.**; 526 Miami Club Court, Mishawaka, IN 46544 (US).

(74) Agent: **KIM, Do, Te** et al.; Daly, Crowley, Mofford & Durkee, LLP, One University Avenue, Suite 201B, Westwood, MA 02090 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

(54) Title: INTEGRATED CIRCUIT (IC) PORTHOLES AND RELATED TECHNIQUES

(57) Abstract: An integrated circuit (IC) structure includes a device layer including a security-critical wire and a metal layer disposed over the device layer. The metal layer includes at least one wire and an IC porthole. The IC porthole has a perimeter that defines a shape such that, when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes at least a segment of the security-critical wire, and the at least one wire in the metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

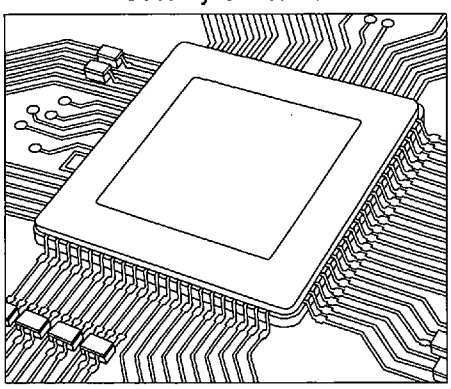


FIG. 4

WO 2020/101867 A1

INTEGRATED CIRCUIT (IC) PORTHOLES AND RELATED TECHNIQUES

FIELD

[0001] This disclosure relates generally to integrated circuit (IC) fabrication, and more particularly, to an IC structure and technique for detecting manipulations in an IC.

BACKGROUND

[0002] Since the inception of the integrated circuit (IC), the transistors and wires used to construct them have continued to shrink. While this shrinkage improves performance and density, it reduces trust. For example, increasing costs to build leading-edge integrated circuit (IC) fabrication facilities has resulted in the need for companies and even nation states to outsource the fabrication of high-performance ICs. However, outsourcing IC fabrication presents security threats including unauthorized fabrication-time modifications (sometimes referred to as "hardware trojans").

[0003] To detect hardware trojans post IC fabrication optical inspection techniques may be used. Such post-fabrication optical inspection techniques include focused ion beam (FIB) and/or scanning electron microscope (SEM) techniques. However, conventional IC designs include many layers of overlapping electrical interconnects making it challenging to conduct post-fabrication optical inspection of specific interconnects (e.g., wires).

SUMMARY

[0004] This Summary is provided to introduce a selection of concepts in simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key or essential features or combinations of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

[0005] In accordance with an embodiment, an integrated circuit (IC) structure includes a device layer having a security-critical wire disposed thereon and a metal

layer disposed over the device layer. The metal layer is provided having an opening therein. The opening is arranged above at least a segment of the security-critical wire.

[0006] With this particular arrangement, an IC structure which facilitates optical inspection of one or more security-critical signal paths is provided.

[0007] In embodiments, one or more translucent layers (e.g. optically translucent dielectric layers) may be disposed between the device later and the metal layer. As used herein, the translucent layer refers to a layer in an integrated circuit (IC) structure that allows light to pass though the layer.

[0008] In accordance with one illustrative embodiment provided to illustrate the broader concepts, systems, and techniques described herein, an integrated circuit (IC) structure includes a device layer including a security-critical wire, and a metal layer disposed over the device layer. The metal layer includes at least one wire and an IC porthole, the IC porthole having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one wire in the metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0009] In one aspect, the security-critical wire is a first security-critical wire, the IC porthole is a first IC porthole, and the IC structure further includes a second security-critical wire disposed on the device layer, and a second IC porthole defined in the metal layer. The second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in the metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole.

[0010] In one aspect, the metal layer is a first metal layer, the at least one wire is a first wire, the IC porthole is a first IC porthole, and the IC structure further includes a second metal layer disposed over the device layer. The second metal

layer includes at least one second wire and a second IC porthole, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one second wire in the second metal layer does not overlap the security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the first and second IC portholes.

[0011] In one aspect, the second IC porthole is aligned on top of the first IC porthole.

[0012] In one aspect, the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0013] In one aspect, spacing around the security-critical wire within the projection of the IC porthole perimeter is increased to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0014] In one aspect, the IC porthole perimeter is defined to include the security-critical wire.

[0015] In one aspect, the metal layer includes a metal fill, and further wherein the metal fill does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0016] According to another illustrative embodiment provided to illustrate the broader concepts described herein, a method includes providing a device layer including a security-critical wire and forming a metal layer over the device layer. The metal layer including at least one wire and an IC porthole, the IC porthole having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one wire in the metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0017] In one aspect, the security-critical wire is a first security-critical wire, the IC porthole is a first IC porthole, and the method further includes providing a second security-critical wire disposed on the device layer and defining a second IC porthole in the metal layer. The second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in the metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole.

[0018] In one aspect, the metal layer is a first metal layer, the at least one wire is a first wire, the IC porthole is a first IC porthole, and the method further includes disposing second metal layer over the device layer. The second metal layer including at least one second wire and a second IC porthole, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one second wire in the second metal layer does not overlap the security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the first and second IC portholes.

[0019] According to another illustrative embodiment provided to illustrate the broader concepts described herein, an integrated circuit (IC) structure includes a device layer including a security-critical wire, and one or more metal and interlayer dielectric layers disposed over the device layer. Each metal layer including at least one wire and an IC porthole, the IC porthole in each metal layer having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes a segment of the security-critical wire, wherein the at least one wire in each metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter defined in each metal layer to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole defined in each metal layer.

[0020] In one aspect, the security-critical wire is a first security-critical wire, the IC porthole in each metal layer is a first IC porthole, and the IC structure further includes a second security-critical wire disposed on the device layer, and a second IC porthole defined in each metal layer. The second IC porthole in each metal layer having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in each metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter defined in each metal layer to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole defined in each metal layer.

[0021] In one aspect, the security-critical wire is routed such that, within the projection of the IC porthole perimeter, the security-critical wire does not overlap any other wires, components, or metal fill in the IC structure.

[0022] In one aspect, the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The foregoing and other objects, features and advantages will be apparent from the following more particular description of the embodiments, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the embodiments.

[0024] Fig. 1 illustrates plan views of an example integrated circuit (IC) die having a trojan rogue wire connection observable through an IC porthole using post-fabrication optical inspection, in accordance with an embodiment of the present disclosure.

[0025] Fig. 2 illustrates plan views of an example IC die having multiple trojan rogue wire connections in multiple sections of the IC die, in accordance with an embodiment of the present disclosure. Fig. 2 also illustrates a plan view of a section

of the IC die including multiple IC portholes having varying wire widths and porthole widths, in accordance with an embodiment of the present disclosure.

[0026] Fig, 3 graphically illustrates porthole scalability using a plot of process technology vs. minimal metal pitch (MMP), in accordance with an embodiment of the present disclosure.

[0027] Fig. 4 illustrates a perspective view of an example security-critical IC having IC portholes provided therein, in accordance with an embodiment of the present disclosure.

[0028] Fig. 4A is an exploded perspective view of the security-critical IC of Fig. 4, in accordance with an embodiment of the present disclosure.

[0029] Fig. 5 is a cross-sectional view of the security-critical IC of Figs. 4 and 4A having portholes provided therein taken across line 5-5 of Fig. 4A, in accordance with an embodiment of the present disclosure.

[0030] Fig. 6A is a flow diagram illustrating an example IC design process for designing an IC, in accordance with an embodiment of the present disclosure.

[0031] Fig. 6B is a flow diagram illustrating an example place-and-route (PaR) sub-process of the IC design process of Fig. 6A, in accordance with an embodiment of the present disclosure.

[0032] Fig. 7 illustrates selected components of an example computing device that may be used to perform any of the techniques as variously described in the present disclosure, in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION

[0033] Concepts and techniques are disclosed that enable non-destructive and efficient post-fabrication optical inspection of wires or so-called interconnects within a multi-layer integrated circuit (IC). As will be appreciated in light of this disclosure, the techniques can be implemented using the concept of an IC porthole. Having determined or otherwise given a wire in an IC to be inspected post-fabrication, such as a security-critical wire, an IC porthole can be defined to allow for post-fabrication inspection of the wire or a segment of the wire. The defined IC may have a perimeter that defines a shape. The IC porthole can be defined during the place-and-route phase of an IC design workflow. Then, in designing the IC, the

wire is routed such that the segment of the wire within a projection of the perimeter of the IC porthole does not overlap any other wires, components, or metal fill. Post-fabrication of the IC, the IC porthole can be non-destructively imaged to determine whether the portholed wire (e.g., the wire or segment of the wire appearing within the projection of the IC porthole perimeter) has been manufactured to specification. Note that an IC porthole is not a physical hole within the IC or a layer of the IC. Rather, the IC porthole has a perimeter that defines a shape such that, when the perimeter of the IC porthole is projected onto a device layer of the IC, other than the wire of interest, no other wires, components, or metal fill are routed and/or placed above and/or below the wire of interest within the projection of the IC porthole in the design of the IC. Also note that the projection of the perimeter of an IC porthole can include an entire wire or a segment of the wire, such as a critical segment of the wire.

[0034] As noted above, there are a number of non-trivial and unresolved issues associated with post-fabrication detection of fabrication-time attacks to an IC. Post-fabrication detection techniques attempt to search for unwanted modifications to a circuit design post-fabrication. However, post-fabrication techniques become more challenging as device dimensions continue to scale down, increasing the size and complexity of IC designs. In such complex designs, stealthy hardware trojans, which may include only one or two additional circuit components, can be hidden in the sea of millions and, in some cases, billions of circuit components, yet have a significant impact on the overall state of the circuit.

[0035] Thus, and in accordance with one embodiment, techniques are provided for forming IC portholes in an IC for post-fabrication optical inspection of wires within an IC. In some embodiments, an IC porthole is formed or otherwise generated to facilitate post-fabrication optical inspection of a security-critical wire within the IC. As used herein, the term “security-critical wire” refers to a wire within an IC that is likely to be a target of an IC fabrication time attack, such as by a hardware trojan or other malicious modification to the circuitry of the IC. For example, a security-critical wire is a wire within the IC to which a rogue hardware trojan wire would attach to. In some example cases, a security-critical wire connects or operatively couples security-critical components in the IC. In one specific embodiment, a security-critical wire within an IC design is identified. The

components connected to the security-critical wire are then positioned where route-densities are relatively low in the IC design, such as towards the out-skirts of an IC die. An IC porthole having a perimeter that defines a shape can be defined such that, when the perimeter of the IC porthole is projected onto a device layer, the projection of the IC porthole perimeter includes at least a segment of the security-critical wire in the IC design. The security-critical wire can then be routed such that, within the projection of the defined IC porthole perimeter, the security-critical wire does not overlap any other wires, components, or metal fill in the IC design. In some embodiments, the projection of the IC porthole perimeter may include the entire security-critical wire. In any case, the remaining components and wiring within the IC design are positioned and/or routed such that they do not overlap the security-critical wire within the projection of the IC porthole perimeter. It will be appreciated in light of this disclosure that an IC design can include multiple IC portholes. It will also be appreciated in light of this disclosure that a projection of a perimeter of an IC porthole can include one or more security-critical wires and, in some cases, segments or portions of one or more security-critical wires.

[0036] In some example embodiments, the size of the security-critical wires within a projection of an IC porthole perimeter can be increased. Increasing the size of the security-critical wires, such as the widths of the security-critical wires, may allow for or otherwise assist in the post-fabrication optical inspection of such security-critical wires. Additionally or alternatively, the spacing around the security-critical wires within a projection of an IC porthole perimeter can be increased. Similar to increasing the size of a security-critical wire, increasing the spacing around a security-critical wire may assist in the post-fabrication optical inspection of the security-critical wire.

[0037] In other embodiments, a security-critical wire within a projection of an IC porthole perimeter can be surrounded with device placement and routing blockage constraints. Device placement blockage constraints may define “keep-out” zones on the device layer, and routing blockage constraints may define “keep-out” zones on the routing metal layers. Such device placement and routing blockage constraints may further enhance security of the security-critical wire. Numerous configurations and modifications will be apparent in light of this disclosure.

[0038] It is noted that designations such "above" or "below" or "top" or "bottom" or "top side" or "bottom side" are not intended to necessarily implicate a limitation as to orientation of the embodiments described herein. Rather, such terminology is simply used in a relative sense to consistently describe a structure as it exists in any one particular orientation and as illustrated herein.

[0039] Turning now to the figures, Fig. 1 illustrates plan views of an example integrated circuit (IC) die having a trojan rogue wire connection observable through an IC porthole using post-fabrication optical inspection, in accordance with an embodiment of the present disclosure. As can be seen, an IC die 104 can be of a security-critical IC 102. Security-critical IC 102 may be an IC that includes security-critical components that may be the target of a fabrication-time attack. As such, in some example cases, security-critical IC 102 may be an IC of a central processing unit (CPU), a microcontroller, a digital signal processor (DSP), a system on a chip (SoC), an application-specific integrated circuit (ASIC), a Field-Programmable Gate Array (FPGA), Complex Instruction Set Computer (CISC), Reduced Instruction Set Computer (RISC), multi core, or any other digital or analog circuitry configured to interpret and/or to execute program instructions and/or to process data, whether loaded from memory or implemented directly in hardware. Outsourcing fabrication of such complex security-critical ICs 102 make them vulnerable to fabrication-time attacks.

[0040] Still referring to Fig. 1, IC die 104 may be a multi-layer structure of semiconducting material on which the functional components of security-critical IC 102 is fabricated. As shown, IC die 104 includes an IC die section 106. IC die section 106 is a section or portion of IC die 104 towards the outskirts of IC die 104. Specifically, IC die section 106 is a section at the top edge of IC die 104. As can be seen in the exploded view of IC die section 106, IC die section 106 includes an IC die sub-section 108. IC die sub-section 108 is a section or portion of IC die section 106 towards the bottom-right corner of IC die section 106. As shown in the exploded view of IC die subsection 108, IC die subsection 108 can include multiple IC portholes 110. For example, in the illustrated embodiment, IC die subsection 108 may be a section of IC die 104 that includes security-critical wires, and IC portholes 110 can be generated in the vicinity of or around the security-critical wires. Within a projection of a perimeter of each IC porthole 110, the security-critical wire (or

security-critical wires) within a projection of a particular IC porthole 110 perimeter is routed such that the security-critical wire does not overlap any other wires, components, or metal fill in any metal or interconnect layer of IC die 104. Likewise, any other wire, component, or metal fill that may be in any metal or interconnect layer of IC die 104 is routed to not overlap the security-critical wire (or security-critical wires) within the projection of IC porthole 110 perimeter. The end result is that IC portholes 110 allow for or otherwise permit post-fabrication optical inspection of the security-critical wires within IC portholes 110 due to the translucent nature of the interlayer dielectric materials in IC die 104. As will be appreciated in light of this disclosure, while a specific number of IC portholes are shown in Fig. 1 for illustration purposes, the claimed invention is not limited to any particular number of IC portholes. Rather, any appropriate number of IC portholes may be generated to permit post-fabrication optical inspection of security-critical wires within the projection of the respective perimeters of the generated IC portholes. Also, while the IC portholes are shown as being generated towards the outskirts of the IC die in Fig. 1 for illustration purposes, the placement or location of the IC portholes need not be so limited. Indeed, in some embodiments, a security-critical wire may be located towards the middle or center of the IC die and an IC porthole can be generated in the vicinity of or around such security-critical wire, for instance. As will be appreciated, numerous configurations can be implemented and the present disclosure is not intended to be limited to any particular one.

[0041] Fig. 2 illustrates plan views of an example IC die having multiple trojan rogue wire connections in multiple sections of the IC die, in accordance with an embodiment of the present disclosure. As can be seen, an IC die 202 can be of a security-critical IC and include a first section 204 and a second section 206. For example, in the illustrated embodiment, first section 204 of IC die 202 may include one or more security-critical wires, and IC die 202 may have been maliciously modified during the fabrication process to include a trojan rogue wire connection to the security-critical wire in first section 204. Similarly, second section 206 of IC die 202 may also include one or more security-critical wires, and IC die 202 may have been maliciously modified during the fabrication process to include a trojan rogue wire connection to the security-critical wire in second section 206. As can be seen in the exploded view of first section 204, first section 204 includes an IC porthole

210 that allows for post-fabrication optical inspection and detection of the trojan rogue wire maliciously included in first section 204 of IC die 202. In contrast, as can be seen in the exploded view of second section 206, the trojan rogue wire maliciously included in a section 212 of second section 206 is not observable through post-fabrication optical inspection because of the lack of an IC porthole. That is, an IC porthole was not generated in or near section 212 of second section 206 during the design of IC die 202 and, as a result, an IC porthole is not present for post-fabrication optical inspection and detection of the trojan rogue wire maliciously included in second section 206 of IC die 202.

[0042] As can be seen, Fig. 2 also illustrates a plan view of a third section 208 of IC die 202 including multiple IC portholes having varying wire widths and porthole widths, in accordance with an embodiment of the present disclosure. For example, in some embodiments and as can be seen on the exploded view of third section 208, the widths of the security-critical wires may be varied to allow for post-fabrication optical inspection of the security-critical wires. In such embodiments, varying the width of a security-critical wire may result in or otherwise cause a need to appropriately vary the spacing surrounding the security-critical wire. For example, increasing the width of a wire decreases resistance and allows the wire to carry more current. When the spacing between the wider wire and an adjacent wire is not sufficient (e.g., too small), cross-coupling capacitance is increased, which results in an increase in cross-talk observed in the adjacent wire as a result of driving the wider wire (e.g., main wide wire). To compensate, manufacturing design rules may specify that spacing between adjacent wires increase when wire widths are increased.

[0043] In some embodiments, the width of a security-critical wire may need to be increased based on the capabilities of the available post-fabrication optical die imaging techniques. As explained above, this may cause a need to increase the spacing surrounding the security-critical wire. In an example implementation of the IC porthole concept in an IC die of an open source OpenRISC processor OR1200, the security-critical wire may be increased from a default width of 140 nanometers (nm) to about 350 nm, and the spacing surrounding the security-critical wire may be increased from about 160 nm to about 500 nm. As can be seen in the exploded view of third section 208, the respective dimensions of the IC portholes can be

based on the dimension of the security-critical wire included within the IC porthole. For example, in the above example of the OpenRISC processor OR1200, the width or smaller dimension of the rectangle-shaped IC porthole can be a minimum of about 1.35 microns (i.e., 500nm + 500nm + 350nm). It will be appreciated that, depending on the available process technology and optical imaging capabilities, a designer can make the wire width and spacings as small or large as desired. It will also be appreciated that reducing the wire and spacing widths, while still being able to image the wires through the IC portholes, reduces the area overhead of including IC portholes in an IC layout.

[0044] Fig. 3 graphically illustrates porthole scalability using a plot of process technology vs. minimal metal pitch (MMP), in accordance with an embodiment of the present disclosure. It will be appreciated that MMP shrinks with process technology advancements. For example, and as can be seen in the plot of Fig. 3, as the process technology advances from 130 nm to 10 nm technology, the MMP shrinks from about 350 nm to in the range of about 36 nm to about 48 nm. The MMP defines the distance between the centers of two adjacent wires on the lowest routing layer for a given process technology. Namely, MMP = minimum wire width + minimum wire spacing, where the minimum wire spacing is between two adjacent IC wires. Note that at 10 to 14 nm. process nodes, the MMP is within the capabilities of optical imaging techniques, as indicated by the dashed line in the plot of Fig. 3. In some example cases, 50 nm feature resolution is possible with conventional optical scanning objectives. Note that only optical feature detection, and not resolution, is necessary to detect the presence of a rogue trojan wire within an IC porthole.

[0045] Fig. 4 illustrates a perspective view of an example security-critical IC having IC portholes provided therein, in accordance with an embodiment of the present disclosure. For example, the security-critical IC may be an IC such as security-critical IC 102 of Fig. 1.

[0046] Fig. 4A is an exploded perspective view of the security-critical IC of Fig. 4, in accordance with an embodiment of the present disclosure. Specifically, Fig. 4A shows a three-dimensional view of an integrated circuit structure of the security-critical IC of Fig. 4. As can be seen, the structure includes two metal structures or layers (404 and 406) in a vertically stacked arrangement above a

device layer 402. For example, device layer 402 can include the circuit components (e.g., placement of the digital logic gates), and metal layers 404 and 406 can include the routing of the wires to connect the circuit components on the device layers, such as device layer 402, for example. In this context, a metal layer may include any signal layer that includes metal that may obstruct a security-critical wire from view during post fabrication optical inspection. An interlayer dielectric structure or layer separates each of the metal and device layers and can include the vias that are used to connect wires on adjacent layers. As can be seen, an interlayer dielectric layer 403 is formed above device layer 402 and separates device layer 402 and metal layer 404, and an interlayer dielectric layer 405 is formed above metal layer 404 and separates metal layer 404 and metal layer 406. In addition, an interlayer dielectric layer 407 is formed above metal layer 406. Although two distinct metal structures or layers are shown, other embodiments may have fewer metal layers or more metal layers, as will be appreciated.

[0047] As can be further seen in Fig. 4A, device layer 402 includes a security-critical wire 408 (e.g., security-critical wire 408 is included in or otherwise disposed on device layer 402). To allow for post-fabrication inspection of security-critical wire 408, an IC porthole is defined within the integrated circuit structure. In an embodiment, the IC porthole has a perimeter that defines a shape, such as, by way of example, circular, square, rectangular, oval, any regular geometric shape, or any irregular geometric shape, such that, when the perimeter of the IC porthole is projected onto a device layer, such as device layer 402, the projection of the IC porthole perimeter includes at least a segment of security-critical wire 408. For example, in one implementation, the IC porthole has a perimeter that defines a substantially rectangular shape. The substantially rectangular shape may follow the perimeter or outline of the segment of the security-critical wire being portholed. In particular, an IC porthole having a perimeter that defines a shape is defined in each of the device and metal layers such that, when the metal layers are stacked above the device layer, the projection of the IC porthole perimeters in each of the layers includes at least a segment the security-critical wire. In addition, the projections of the defined IC porthole perimeters are aligned or substantially aligned on top of one another when the metal layers are stacked above the device layer. Alignment of the

projections of the IC porthole perimeters in the stacked layers allows for optical viewing of the included security-critical wire through the aligned IC portholes.

[0048] For example and as can be seen in Fig. 4A, an IC porthole 410 is defined in metal layer 404 to have a perimeter that defines a shape such that, when the perimeter of IC porthole 410 is projected onto device layer 402, the projection of IC porthole 410 perimeter includes at least a segment of security-critical wire 408. Similarly, an IC porthole 412 is defined in metal layer 406 to have a perimeter that defines a shape such that, when the perimeter of IC porthole 412 is projected onto device layer 402, the projection of IC porthole 412 includes at least a segment of security-critical wire 408. When metal layers 404 and 406 are stacked above device layer 402, the projections of the respective perimeters of IC portholes 410 and 412 are aligned on top of one another as well as a projection of a perimeter of an IC porthole (not shown) that is defined in device layer 402 to include at least a segment of security-critical wire 408. In device layer 402, the segment of security-critical wire 408 within perimeter of the defined IC porthole (not shown) can be routed such that security-critical wire 408 does not overlap any other wires, components, or metal fill. In metal layer 404, any metal fill and wiring within the perimeter of IC porthole 410 is positioned and/or routed such that they do not overlap security-critical wire 408. Similarly, in metal layer 406, any metal fill and wiring within the perimeter of IC porthole 412 is positioned and/or routed such that they do not overlap security-critical wire 408. The alignment of the projections of the respective perimeters of IC portholes 410 and 412 with the projection of the perimeter of the IC porthole (not shown) defined in device layer 402 to include at least a segment of security-critical wire 408 allows for post-fabrication optical inspection of security-critical wire 408 through IC portholes 410 and 412. Note that IC portholes need not be defined in the interlayer dielectric layers because of the translucent nature of the interlayer dielectric materials.

[0049] Also, as will be appreciated in light of this disclosure, additional IC portholes may be defined within the integrated circuit structure. For example, and as can be further seen in Fig. 4A, an IC porthole 414 is defined in metal layer 404 and an IC porthole 416 is defined in metal layer 406. IC portholes 414 and 416 have a respective perimeter that defines a shape such that, when the perimeters of IC portholes 414 and 416 are projected onto device layer 402, the projection of the

respective perimeters of IC portholes 414 and 416 includes at least a segment of a security-critical wire (not shown) in device layer 402. This security-critical wire may be distinct from security-critical wire 408. When metal layers 404 and 406 are stacked above device layer 402, the projections of the respective perimeters of IC portholes 414 and 416 are aligned on top of one another such that optical viewing of the segment of the security-critical wire within the projections of the respective perimeters of IC portholes 414 and 416 is possible.

[0050] Fig. 5 is a cross-sectional view of the security-critical IC of Figs. 4 and 4A having portholes provided therein taken across line 5-5 of Fig. 4A, in accordance with an embodiment of the present disclosure. Specifically, Fig. 5 shows the integrated circuit structure of the security-critical IC of Figs. 4 and 4A taken across line 5-5 of Fig. 4A. As can be seen, when metal layers 404 and 406 are stacked above device layer 402, the projections of the respective perimeters of IC portholes 410 and 412 defined in respective metal layers 404 and 406 are aligned on top of one another above at least a segment of security-critical wire 408. Alignment of IC portholes 410 and 412 in a manner as to include at least a segment of security-critical wire 408 allows for post-fabrication optical viewing and inspection of security-critical wire 408 through IC portholes 410 and 412.

[0051] Fig. 6A is a flow diagram illustrating an example IC design process 600 for designing an IC, in accordance with an embodiment of the present disclosure. The embodiments disclosed herein, including process 600 and a sub-process 650 of Fig. 6B further described below, can be implemented using and/or in various forms of hardware, software, firmware, and/or special purpose processors. For example, in one embodiment, a non-transitory computer readable medium has instructions encoded thereon that, when executed by one or more processors, cause one or more of the IC design methodologies described herein to be implemented. The instructions can be encoded using any suitable programming language, such as C, C++, object-oriented C, JavaScript, Visual Basic .NET, BASIC, or alternatively, using custom or proprietary instruction sets. Such instructions can be provided in the form of one or more computer software applications that are tangibly embodied on a memory device, and that can be executed by a computer having any suitable architecture. In one embodiment, some of the operations of process 600 and the operations of sub-process 650 of Fig. 6B

can be implemented, for example, using and/or as part of a Computer Aided Design (CAD) tool suitable for use in designing an IC. A computer system, such as a workstation, desktop computer, server, laptop, handheld computer, tablet computer (e.g., the iPad™ tablet computer), or other form of computing or telecommunications device that is capable of communication and that has sufficient processor power and memory capacity can then be used to execute the CAD tool and/or perform the operations described in this disclosure.

[0052] As will be further appreciated in light of this disclosure, for this and other processes and methods disclosed herein, the functions performed in the processes and methods may be implemented in differing order. Additionally or alternatively, two or more operations may be performed at the same time or otherwise in an overlapping contemporaneous fashion. Furthermore, the outlined actions and operations are only provided as examples, and some of the actions and operations may be optional, combined into fewer actions and operations, or expanded into additional actions and operations without detracting from the essence of the disclosed embodiments.

[0053] With reference to process 600 of Fig. 6A, at operation 602, high-level descriptions of an IC are written. In one example implementation, the high-level description can be written using a suitable Hardware Description Language (HDL), such as Verilog or Very High Speed Integrated Circuits HDL (VHDL), to name two examples. Note that the written description is of an IC that is to be configured with one or more IC portholes.

[0054] At operation 604, the high-level descriptions of the IC are synthesized into a gate-level netlist. The netlist may include information regarding the electronic components used in the IC, cells used, interconnections, area used, as well as other details. The netlist may also include information regarding the constraints that are applied to ensure that the design satisfies the desired performance specifications (e.g., required functionality, speed, etc.). In the example implementation of the high-level descriptions of the IC being written using HDL, the HDL code can be "compiled" into a gate-level netlist.

[0055] At operation 606, the gate-level netlist is placed-and-routed (PaR) onto a physical layout, such as for example a physical geometric blueprint, of the IC. In brief, the placement phase of PaR includes determining where to place all the

electronic components, circuity, and logic elements in the layout, and the routing phase of PaR includes determining the exact design of all the wires needed to connect the placed components, circuitry, and logic elements. In one example implementation, the layout of the IC can be encoded in a Graphics Database System II (GDSII) file. The PaR sub-process is further described below with respect to Fig. 6B.

[0056] At operation 608, a semiconductor device fabrication is performed to create an IC die based on the layout of the IC (e.g., the layout encoded in a GDSII file).

[0057] At operation 610, the fabricated IC die is packaged or otherwise encapsulated in a supporting case that prevents physical damage and corrosion. The supporting case, which is also known as a "package", supports the electrical contacts which connect the device to a circuit board.

[0058] Fig. 6B is a flow diagram illustrating an example place-and-route (PaR) sub-process 650 of IC design process 600 of Fig. 6A, in accordance with an embodiment of the present disclosure. In brief, process 650 includes converting the circuit representations of the IC components (e.g., electronic components, circuitry, interconnects, etc.) into geometric representations (i.e., IC layout) of shapes which, when manufactured in the corresponding layers of materials, ensure the functioning of the components.

[0059] With reference to process 650, at operation 652, floor planning is performed to create a schematic representation of the tentative placement of the major functional blocks of the IC. For example, an IC floor plan may be generated that includes a core area and an input/output (I/O) pad ring surrounding the chip core area. The core area may include a placement grid, and circuit components may be placed and routed within the placement grid. Power and ground trees may be routed to provide power and/or ground rails to placement sites in the core area. The placement and routing may be optimized to adhere to design and performance objectives.

[0060] At operation 654, security-critical placement is performed to place the security-critical components (e.g., devices and/or standard cells connected to security-critical wires) on the placement grid. In an embodiment, the security-critical components may be placed within the placement grid in a manner that reduces and,

in some cases, minimizes, routing wire lengths and power consumption, and increases performance.

[0061] At operation 656, security-critical routing is performed to connect the security-critical components. At operation 658, IC porthole(s) placement is performed. In an embodiment, IC porthole(s) placement may include placement of device placement blockage constraints (e.g., "keep-out" zones) on the device layer and routing blockage constraints (e.g., "keep-out" zones) on the routing metal layers above and below the segments of the security-critical wires and components that are being portholed. The security-critical wires and components may be marked or otherwise identified (e.g., marked as "fixed") to prevent movement of the security-critical wires and components during subsequent place and route operations.

[0062] At operation 660, remaining placement is performed to place the remaining non-security-critical cells (e.g., standard cells such as logic gates) within the core area. In an embodiment, the non-security-critical standard cells may be placed within the placement grid in a manner that reduces and, in some cases, minimizes, routing wire lengths and power consumption, and increases performance.

[0063] At operation 662, clock tree synthesis is performed to route and connect the clock tree to all sequential components in the IC design. Clock tree synthesis may include generating a balanced clock tree in such a manner as to, for example, reduce the skew and latency, maintain symmetrical clock tree structure and to cover the necessary components (e.g., devices that require clocks, such as flip-flops) in the design.

[0064] At operation 664, remaining routing is performed to connect the non-security-critical components. For example, wires may be routed between the standard cells.

[0065] At operation 666, the remaining (e.g., empty) placement sites may be filled with filler capacitor cells to achieve device uniformity. This may improve manufacturability and provide distributed decoupling capacitors to improve switching performance. Timing, design rules, and other verification tests may be run to ensure the IC device functions properly under the desired performance and operating margins.

[0066] Fig. 7 illustrates selected components of an example computing device 700 that may be used to perform any of the techniques as variously described in the present disclosure, in accordance with an embodiment of the present disclosure. In some embodiments, computing device 700 may be configured to implement or direct one or more operations associated with some or all of the components and/or modules of a CAD tool suitable or otherwise configured to perform IC design process 600. For example, such CAD tools may be implemented in and/or using computing device 700. In one example case, for instance, such CAD tools may be stored on a data store 708, loaded in memory 706, and executable by a processor 702.

[0067] In some embodiments, computing device 700 may be any computer system, such as a workstation, desktop computer, server, laptop, handheld computer, tablet computer (e.g., the iPad™ tablet computer), mobile computing or communication device (e.g., the iPhone™ mobile communication device, the Android™ mobile communication device, and the like), or other form of computing or telecommunications device that is capable of communication and that has sufficient processor power and memory capacity to perform the operations described in this disclosure. In some embodiments, a distributed computational system may be provided comprising multiple of such computing devices. As shown in Fig. 7, computing device 700 includes processor 702, a communication module 704, memory 706, and data store 708. Processor 702, communication module 704, memory 706, and data store 708 may be communicatively coupled. In various embodiments, additional components (not illustrated, such as a display, communication interface, input/output interface, etc.) or a subset of the illustrated components can be employed without deviating from the scope of the present disclosure.

[0068] Processor 702 may be designed to control the operations of the various other components of computing device 700. Processor 702 may include any processing unit suitable for use in computing device 700, such as a single core or multi-core processor. In general, processor 702 may include any suitable special-purpose or general-purpose computer, computing entity, or computing or processing device including various computer hardware, or firmware, and may be configured to execute instructions, such as program instructions, stored on any

applicable computer-readable storage media. For example, processor 702 may include a microprocessor, a central processing unit (CPU), a microcontroller, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a Field-Programmable Gate Array (FPGA), Complex Instruction Set Computer (CISC), Reduced Instruction Set Computer (RISC), multi core, or any other digital or analog circuitry configured to interpret and/or to execute program instructions and/or to process data, whether loaded from memory or implemented directly in hardware. Although illustrated as a single processor in Fig. 7, processor 702 may include any number of processors and/or processor cores configured to, individually or collectively, perform or direct performance of any number of operations described in the present disclosure.

[0069] In some embodiments, processor 702 may be configured to interpret and/or execute program instructions and/or process data stored in memory 706, data store 708, or memory 706 and data store 708. In some embodiments, processor 702 may fetch program instructions from data store 708 and load the program instructions in memory 706. After the program instructions are loaded into memory 706, processor 702 may execute the program instructions.

[0070] For example, in some embodiments, any one or more of the components and/or modules of the CAD tool suitable or otherwise configured to perform IC design process 600 or any of the other embodiments and/or examples described herein may be included in data store 708 as program instructions 710. For example, in such embodiments, program instructions 710 cause computing device 700 to implement functionality in accordance with the various embodiments and/or examples described herein. Processor 702 may fetch some or all of program instructions 710 from data store 708 and may load the fetched program instructions 710 in memory 706. Subsequent to loading the fetched program instructions 710 into memory 708, processor 702 may execute program instructions 710 such that the CAD tool runs on computing device 700 as variously described herein.

[0071] In some embodiments, virtualization may be employed in computing device 700 so that infrastructure and resources in computing device 700 may be shared dynamically. For example, a virtual machine may be provided to handle a process running on multiple processors so that the process appears to be using

only one computing resource rather than multiple computing resources. Multiple virtual machines may also be used with one processor.

[0072] Communication module 704 can be any appropriate network chip or chipset which allows for wired or wireless communication via a network, such as, by way of example, a local area network (e.g., a home-based or office network), a wide area network (e.g., the Internet), a peer-to-peer network (e.g., a Bluetooth connection), or a combination of such networks, whether public, private, or both. Communication module 704 can also be configured to provide intra-device communications via a bus or an interconnect.

[0073] Memory 706 may include computer-readable storage media configured for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable storage media may include any available media that may be accessed by a general-purpose or special-purpose computer, such as processor 702. By way of example, and not limitation, such computer-readable storage media may include non-transitory computer-readable storage media including Random Access Memory (RAM), Dynamic Random Access Memory (DRAM), Synchronized Dynamic Random Access Memory (SDRAM), Static Random Access Memory (SRAM), non-volatile memory (NVM), or any other suitable storage medium which may be used to carry or store particular program code in the form of computer-executable instructions or data structures and which may be accessed by a general-purpose or special-purpose computer. Combinations of the above may also be included within the scope of computer-readable storage media.

[0074] Data store 708 may include any type of computer-readable storage media configured for short-term or long-term storage of data. By way of example, and not limitation, such computer-readable storage media may include a hard drive, solid-state drive, Read-Only Memory (ROM), Electrically Erasable Programmable Read-Only Memory (EEPROM), Compact Disc Read-Only Memory (CD-ROM) or other optical disk storage, magnetic disk storage or other magnetic storage devices, flash memory devices (e.g., solid state memory devices), non-volatile memory (NVM), or any other storage medium, including those provided above in conjunction with memory 706, which may be used to carry or store particular program code in the form of computer-readable and computer-executable instructions, software or

data structures for implementing the various embodiments as disclosed herein and which may be accessed by a general-purpose or special-purpose computer. Combinations of the above may also be included within the scope of computer-readable storage media. Computer-executable instructions may include, for example, instructions and data configured to cause processor 702 to perform a certain operation or group of operations. Data store 708 may be provided on computing device 700 or provided separately or remotely from computing device 700.

[0075] The following examples pertain to further embodiments, from which numerous permutations and configurations will be apparent.

[0076] Example 1 includes an integrated circuit structure including: a device layer including a security-critical wire; and a metal layer disposed over the device layer, the metal layer including at least one wire and an IC porthole, the IC porthole having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one wire in the metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0077] Example 2 includes the subject matter of Example 1, wherein the security-critical wire is a first security-critical wire, the IC porthole is a first IC porthole, and further including a second security-critical wire disposed on the device layer; and a second IC porthole defined in the metal layer, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in the metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole.

[0078] Example 3 includes the subject matter of any of Examples 1 and 2, wherein the metal layer is a first metal layer, the at least one wire is a first wire, the IC porthole is a first IC porthole, and further including a second metal layer disposed

over the device layer, the second metal layer including at least one second wire and a second IC porthole, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one second wire in the second metal layer does not overlap the security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the first and second IC portholes.

[0079] Example 4 includes the subject matter of Example 3, wherein the second IC porthole is aligned on top of the first IC porthole.

[0080] Example 5 includes the subject matter of any of Examples 1 through 4, wherein the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0081] Example 6 includes the subject matter of any of Examples 1 through 5, wherein spacing around the security-critical wire within the projection of the IC porthole perimeter is increased to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0082] Example 7 includes the subject matter of any of Examples 1 through 6, wherein the IC porthole perimeter is defined to include the security-critical wire.

[0083] Example 8 includes the subject matter of any of Examples 1 through 7, wherein the metal layer includes a metal fill, and further wherein the metal fill does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0084] Example 9 includes the subject matter of any of Examples 1 through 8, wherein the post-fabrication optical inspection is non-destructive.

[0085] Example 10 includes a method for forming an integrated circuit (IC) structure, the method including: providing a device layer including a security-critical wire; and forming a metal layer over the device layer, the metal layer including at least one wire and an IC porthole, the IC porthole having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes at least a segment of the

security-critical wire, wherein the at least one wire in the metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0086] Example 11 includes the subject matter of Example 10, wherein the security-critical wire is a first security-critical wire, the IC porthole is a first IC porthole, and the method further including: providing a second security-critical wire disposed on the device layer; and defining a second IC porthole in the metal layer, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in the metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole.

[0087] Example 12 includes the subject matter of any of Examples 10 and 11, wherein the metal layer is a first metal layer, the at least one wire is a first wire, the IC porthole is a first IC porthole, and the method further including disposing second metal layer over the device layer, the second metal layer including at least one second wire and a second IC porthole, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one second wire in the second metal layer does not overlap the security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the first and second IC portholes.

[0088] Example 13 includes the subject matter of Example 12, wherein the second IC porthole is aligned on top of the first IC porthole.

[0089] Example 14 includes the subject matter of any of Examples 10 through 13, wherein the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0090] Example 15 includes the subject matter of any of Examples 10 through 14, wherein spacing around the security-critical wire within the projection of the IC porthole perimeter is increased to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0091] Example 16 includes the subject matter of any of Examples 10 through 15, wherein the IC porthole is defined to include the security-critical wire.

[0092] Example 17 includes the subject matter of any of Examples 10 through 16, wherein the metal layer includes a metal fill, and further wherein the metal fill does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0093] Example 18 includes the subject matter of any of Examples 10 through 17, wherein the post-fabrication optical inspection is non-destructive.

[0094] Example 19 includes an integrated circuit (IC) structure including: a device layer including a security-critical wire; and one or more metal and interlayer dielectric layers disposed over the device layer, each metal layer including at least one wire and an IC porthole, the IC porthole in each metal layer having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes a segment of the security-critical wire, wherein the at least one wire in each metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter defined in each metal layer to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole defined in each metal layer.

[0095] Example 20 includes the subject matter of Example 19, wherein the security-critical wire is a first security-critical wire, the IC porthole in each metal layer is a first IC porthole, and further including: a second security-critical wire disposed on the device layer; and a second IC porthole defined in each metal layer, the second IC porthole in each metal layer having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in each metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter defined in each metal layer to thereby allow post-fabrication

optical inspection of the second security-critical wire through the second IC porthole defined in each metal layer.

[0096] Example 21 includes the subject matter of any of Examples 19 and 20, wherein the security-critical wire is routed such that, within the projection of the IC porthole perimeter, the security-critical wire does not overlap any other wires, components, or metal fill in the IC structure.

[0097] Example 22 includes the subject matter of any of Examples 19 through 21, wherein the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0098] Example 23 includes the subject matter of any of Examples 19 through 22, wherein spacing around the security-critical wire within the projection of the IC porthole perimeter is increased to thereby allow non-destructive post-fabrication optical inspection of the security-critical wire through the IC porthole.

[0099] Example 24 includes the subject matter of any of Examples 19 through 23, wherein the projection of the IC porthole perimeters in each metal layer is defined to include a segment of the security-critical wire.

[00100] Terms used in the present disclosure and in the appended claims (e.g., bodies of the appended claims) are generally intended as “open” terms (e.g., the term “including” should be interpreted as “including, but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes, but is not limited to,” etc.).

[00101] Additionally, if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases "at least one" and "one or more" to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles "a" or "an" limits any particular claim containing such introduced claim recitation to embodiments containing only one such recitation, even when the same claim includes the introductory phrases "one or more" or "at least one" and indefinite articles such as "a" or "an" (e.g., “a” and/or

“an” should be interpreted to mean “at least one” or “one or more”); the same holds true for the use of definite articles used to introduce claim recitations.

[00102] In addition, even if a specific number of an introduced claim recitation is explicitly recited, such recitation should be interpreted to mean at least the recited number (e.g., the bare recitation of "two widgets," without other modifiers, means at least two widgets, or two or more widgets). Furthermore, in those instances where a convention analogous to “at least one of A, B, and C, etc.” or “one or more of A, B, and C, etc.” is used, in general such a construction is intended to include A alone, B alone, C alone, A and B together, A and C together, B and C together, or A, B, and C together, etc.

[00103] All examples and conditional language recited in the present disclosure are intended for pedagogical examples to aid the reader in understanding the present disclosure, and are to be construed as being without limitation to such specifically recited examples and conditions. Although example embodiments of the present disclosure have been described in detail, various changes, substitutions, and alterations could be made hereto without departing from the spirit and scope of the present disclosure. Accordingly, it is intended that the scope of the present disclosure be limited not by this detailed description, but rather by the claims appended hereto.

CLAIMS

What is claimed is:

1. An integrated circuit (IC) structure, comprising:

a device layer including a security-critical wire; and

a metal layer disposed over the device layer, the metal layer including at least one wire and an IC porthole, the IC porthole having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one wire in the metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

2. The IC structure of claim 1, wherein the security-critical wire is a first security-critical wire, the IC porthole is a first IC porthole, and further comprising:

a second security-critical wire disposed on the device layer; and

a second IC porthole defined in the metal layer, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in the metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole.

3. The IC structure of claim 1, wherein the metal layer is a first metal layer, the at least one wire is a first wire, the IC porthole is a first IC porthole, and further comprising:

a second metal layer disposed over the device layer, the second metal layer including at least one second wire and a second IC porthole, the second IC porthole having a perimeter that defines a shape such that

when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one second wire in the second metal layer does not overlap the security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the first and second IC portholes.

4. The IC structure of claim 3, wherein the second IC porthole is aligned on top of the first IC porthole.

5. The IC structure of claim 1, wherein the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

6. The IC structure of claim 1, wherein spacing around the security-critical wire within the projection of the IC porthole perimeter is increased to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

7. The IC structure of claim 1, wherein the IC porthole perimeter is defined to include the security-critical wire.

8. The IC structure of claim 1, wherein the metal layer includes a metal fill, and further wherein the metal fill does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

9. A method for forming an integrated circuit (IC) structure, the method comprising:

providing a device layer including a security-critical wire; and

forming a metal layer over the device layer, the metal layer including at least one wire and an IC porthole, the IC porthole having a perimeter that defines a shape such that when the perimeter of the IC porthole is

projected onto the device layer, the projection of the IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one wire in the metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

10. The method of claim 9, wherein the security-critical wire is a first security-critical wire, the IC porthole is a first IC porthole, and the method further comprising:

providing a second security-critical wire disposed on the device layer; and

defining a second IC porthole in the metal layer, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in the metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole.

11. The method of claim 9, wherein the metal layer is a first metal layer, the at least one wire is a first wire, the IC porthole is a first IC porthole, and the method further comprising:

disposing second metal layer over the device layer, the second metal layer including at least one second wire and a second IC porthole, the second IC porthole having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the security-critical wire, wherein the at least one second wire in the second metal layer does not overlap the security-critical wire within the projection of the second IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the first and second IC portholes.

12. The method of claim 11, wherein the second IC porthole is aligned on top of the first IC porthole.

13. The method of claim 9, wherein the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

14. The method of claim 9, wherein spacing around the security-critical wire within the projection of the IC porthole perimeter is increased to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

15. The method of claim 9, wherein the IC porthole perimeter is defined to include the security-critical wire.

16. The method of claim 9, wherein the metal layer includes a metal fill, and further wherein the metal fill does not overlap the security-critical wire within the projection of the IC porthole perimeter to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

17. An integrated circuit (IC) structure, comprising:

a device layer including a security-critical wire; and

one or more metal and interlayer dielectric layers disposed over the device layer, each metal layer including at least one wire and an IC porthole, the IC porthole in each metal layer having a perimeter that defines a shape such that when the perimeter of the IC porthole is projected onto the device layer, the projection of the IC porthole perimeter includes a segment of the security-critical wire, wherein the at least one wire in each metal layer does not overlap the security-critical wire within the projection of the IC porthole perimeter defined in each metal layer to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole defined in each metal layer.

18. The IC structure of claim 17, wherein the security-critical wire is a first security-critical wire, the IC porthole in each metal layer is a first IC porthole, and further comprising:

a second security-critical wire disposed on the device layer; and

a second IC porthole defined in each metal layer, the second IC porthole in each metal layer having a perimeter that defines a shape such that when the perimeter of the second IC porthole is projected onto the device layer, the projection of the second IC porthole perimeter includes at least a segment of the second security-critical wire, wherein the at least one wire in each metal layer does not overlap the second security-critical wire within the projection of the second IC porthole perimeter defined in each metal layer to thereby allow post-fabrication optical inspection of the second security-critical wire through the second IC porthole defined in each metal layer.

19. The IC structure of claim 17, wherein the security-critical wire is routed such that, within the projection of the IC porthole perimeter, the security-critical wire does not overlap any other wires, components, or metal fill in the IC structure.

20. The IC structure of claim 17, wherein the security-critical wire within the projection of the IC porthole perimeter is of an increased width to thereby allow post-fabrication optical inspection of the security-critical wire through the IC porthole.

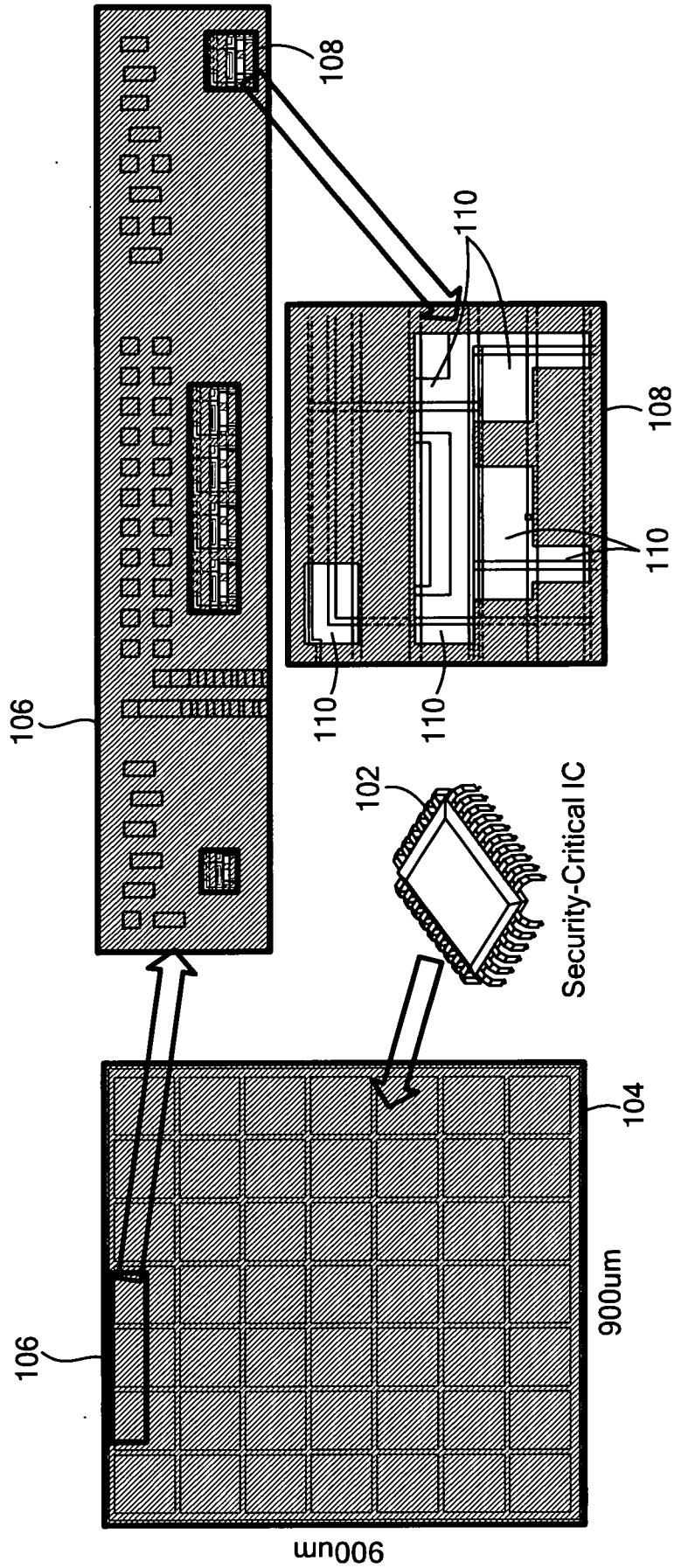

108
110
108
110
110
110
106
102
Security-Critical IC
104
106
900um
900um

FIG. 1

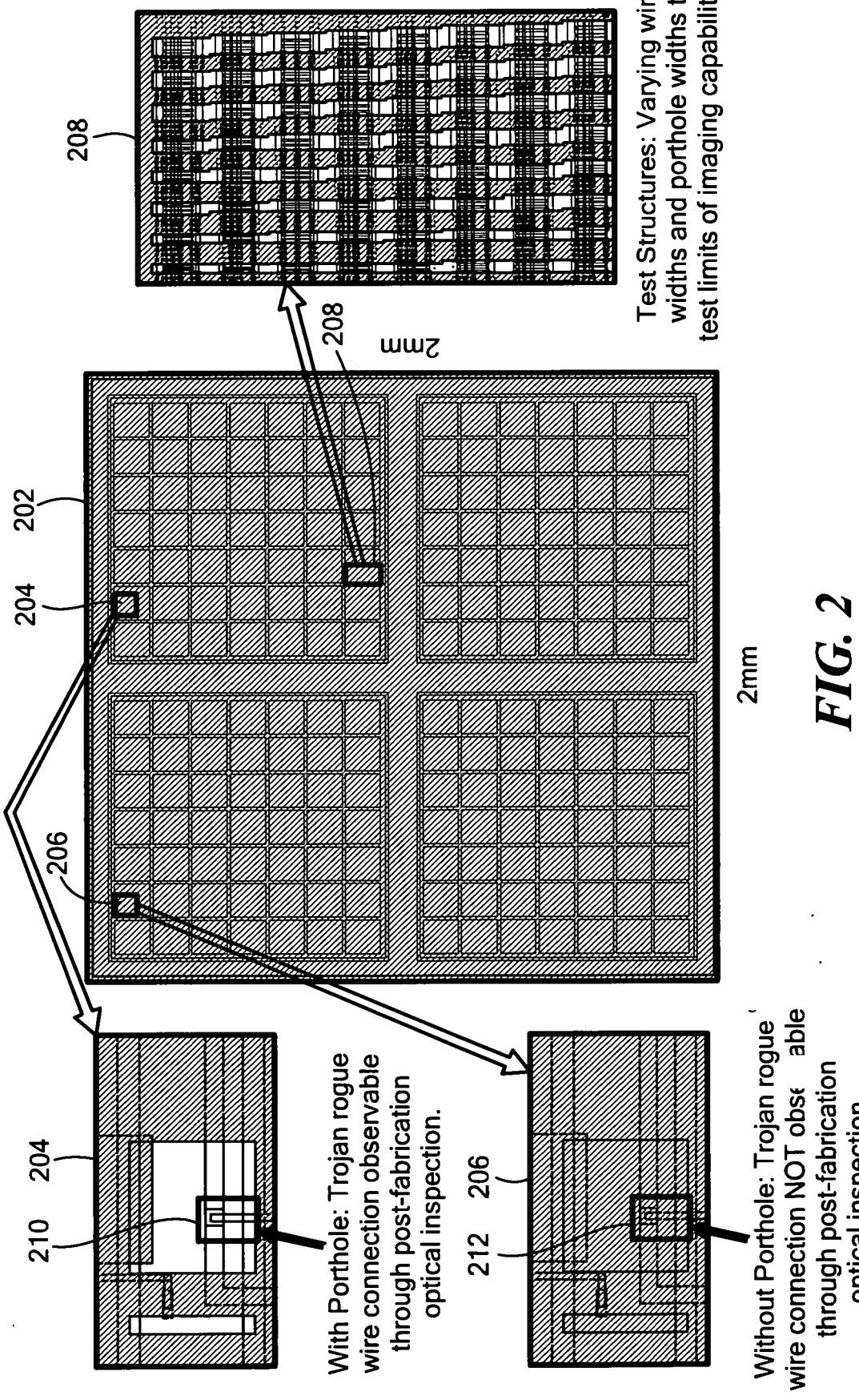

208
Test Structures: Varying wire widths and porthole widths to test limits of imaging capabilities
208
2mm
202
204
206
2mm
204
210
With Porthole: Trojan rogue wire connection observable through post-fabrication optical inspection.
206
212
Without Porthole: Trojan rogue wire connection NOT obst able through post-fabrication optical inspection.

FIG. 2

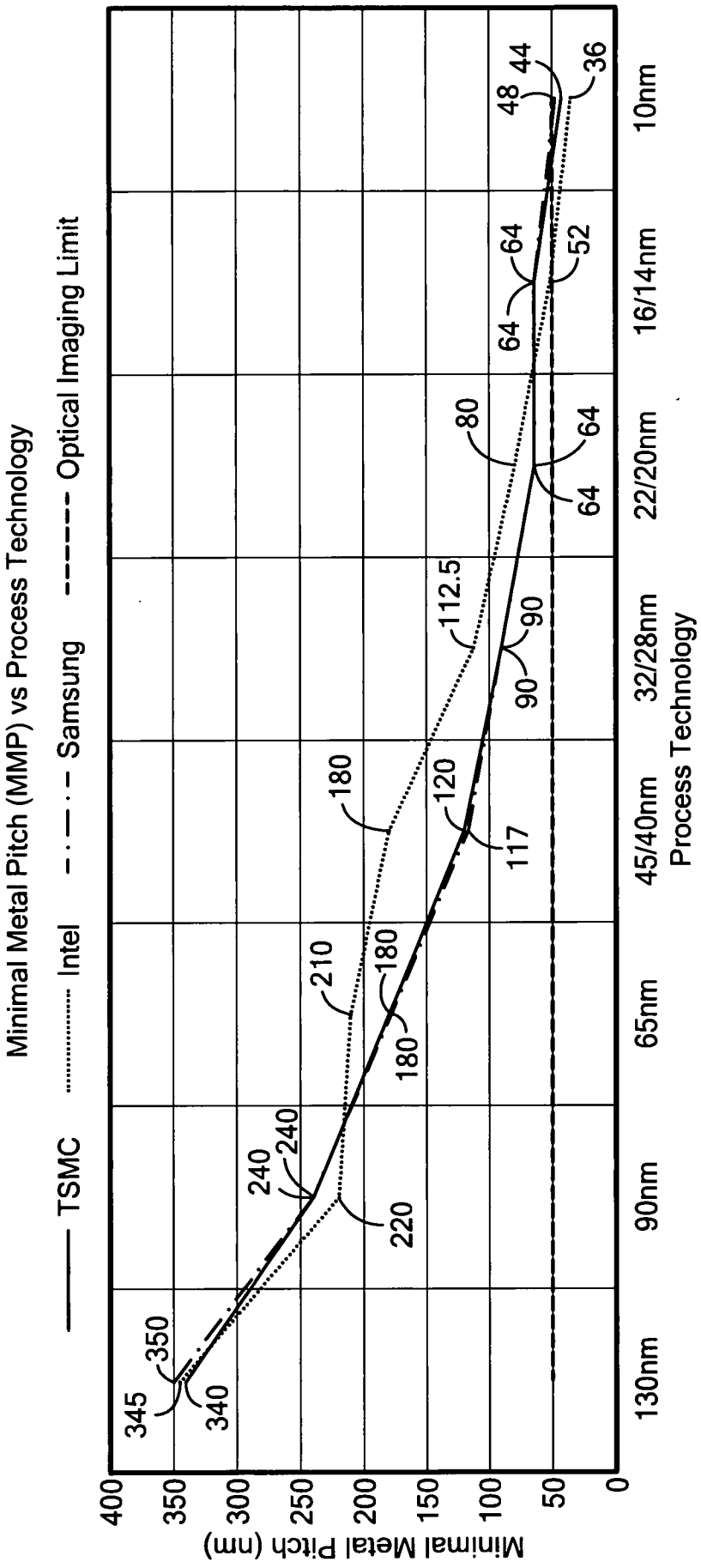

Minimal Metal Pitch (MMP) vs Process Technology
TSMC
Intel
Samsung
Optical Imaging Limit
Minimal Metal Pitch (nm)
400
350
300
250
200
150
100
50
0
130nm
90nm
65nm
45/40nm
32/28nm
22/20nm
16/14nm
10nm
Process Technology
345
350
340
240
240
210
220
180
180
180
120
117
112.5
90
90
80
64
64
64
64
52
48
44
36

FIG. 3

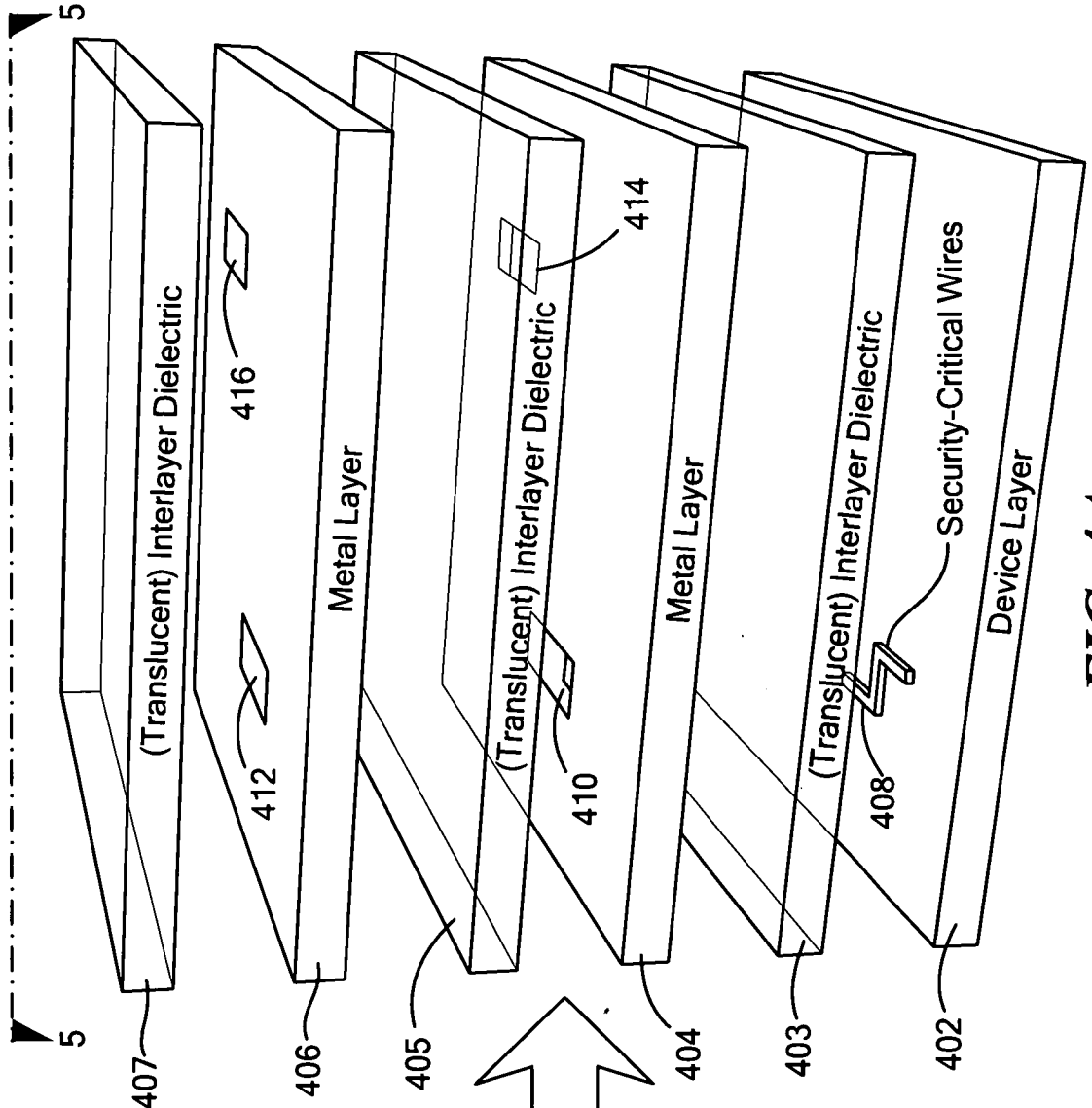

5
5
(Translucent) Interlayer Dielectric
Metal Layer
(Translucent) Interlayer Dielectric
Metal Layer
(Translucent) Interlayer Dielectric
Security-Critical Wires
Device Layer
407
406
405
404
403
402
412
416
410
414
408

FIG. 4A

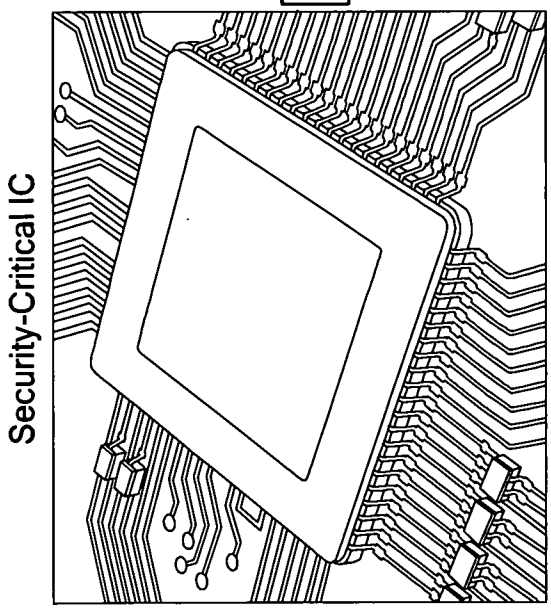

Security-Critical IC

FIG. 4

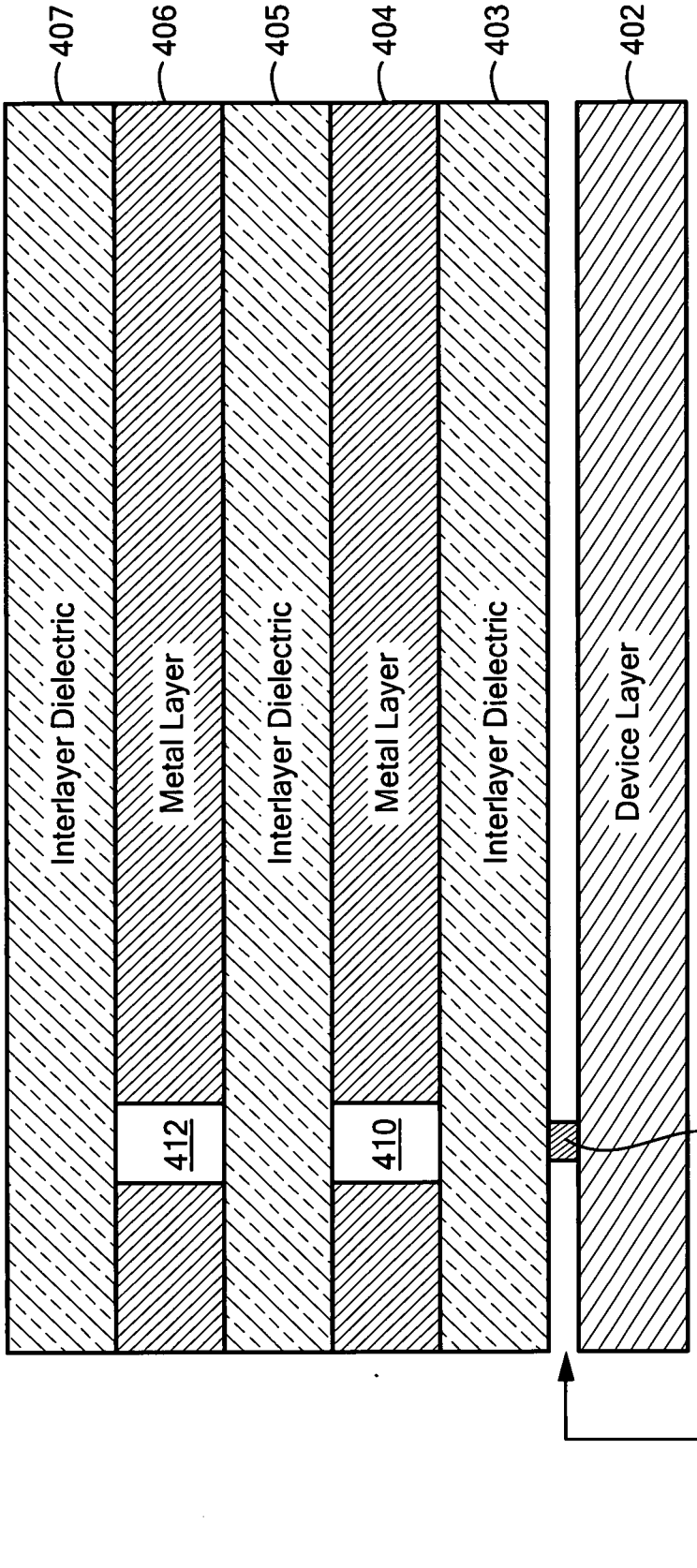

407
406
405
404
403
402
Interlayer Dielectric
Metal Layer
Interlayer Dielectric
Metal Layer
Interlayer Dielectric
Device Layer
412
410
408
Exaggerated metal layer to provide clarity in showing the "security critical wire"

FIG. 5

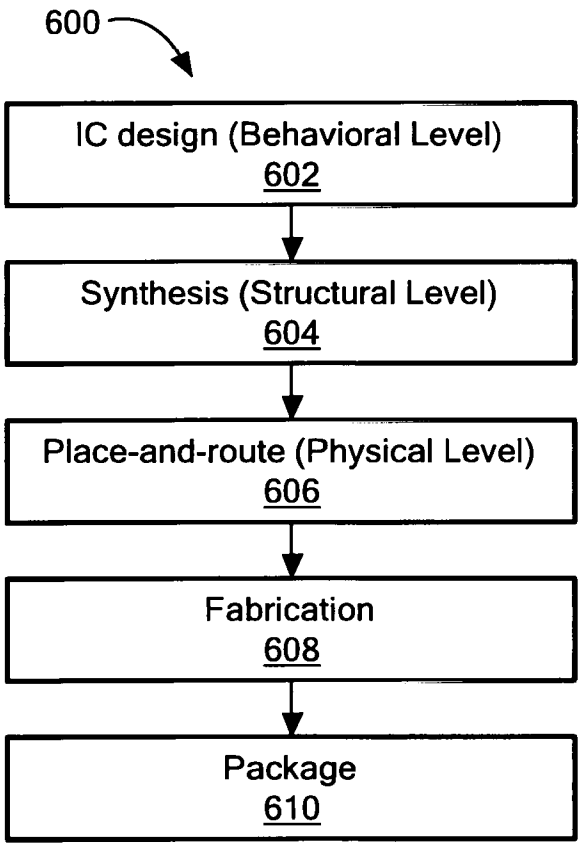

600
IC design (Behavioral Level)
602
Synthesis (Structural Level)
604
Place-and-route (Physical Level)
606
Fabrication
608
Package
610

FIG. 6A

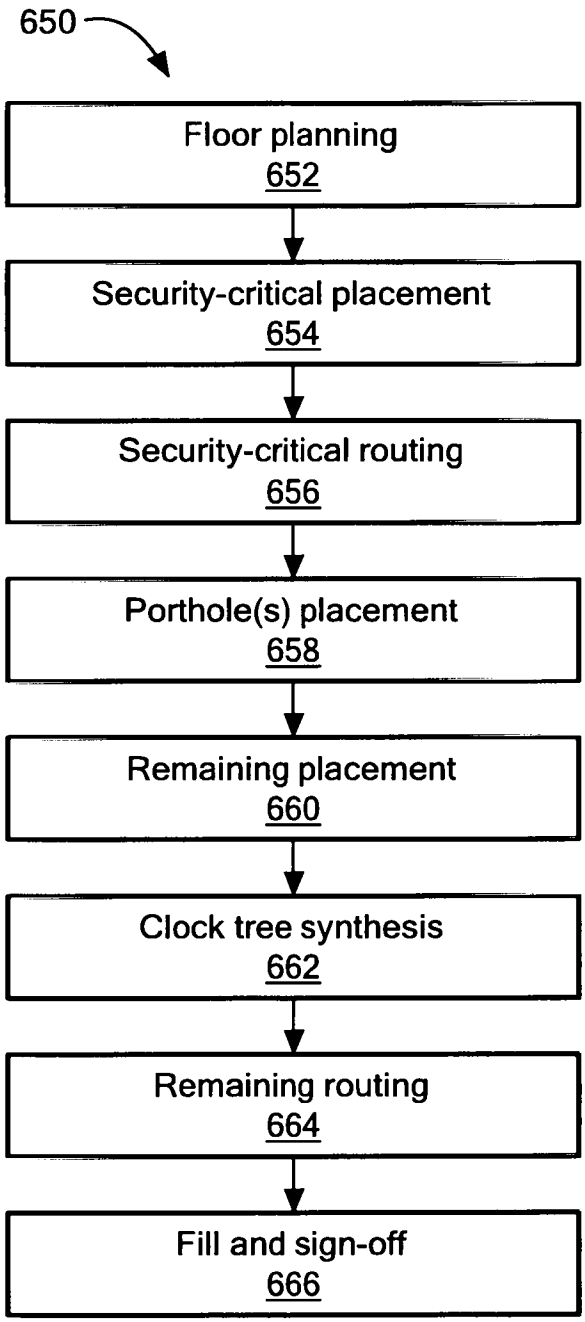

650
Floor planning
652
Security-critical placement
654
Security-critical routing
656
Porthole(s) placement
658
Remaining placement
660
Clock tree synthesis
662
Remaining routing
664
Fill and sign-off
666

FIG. 6B

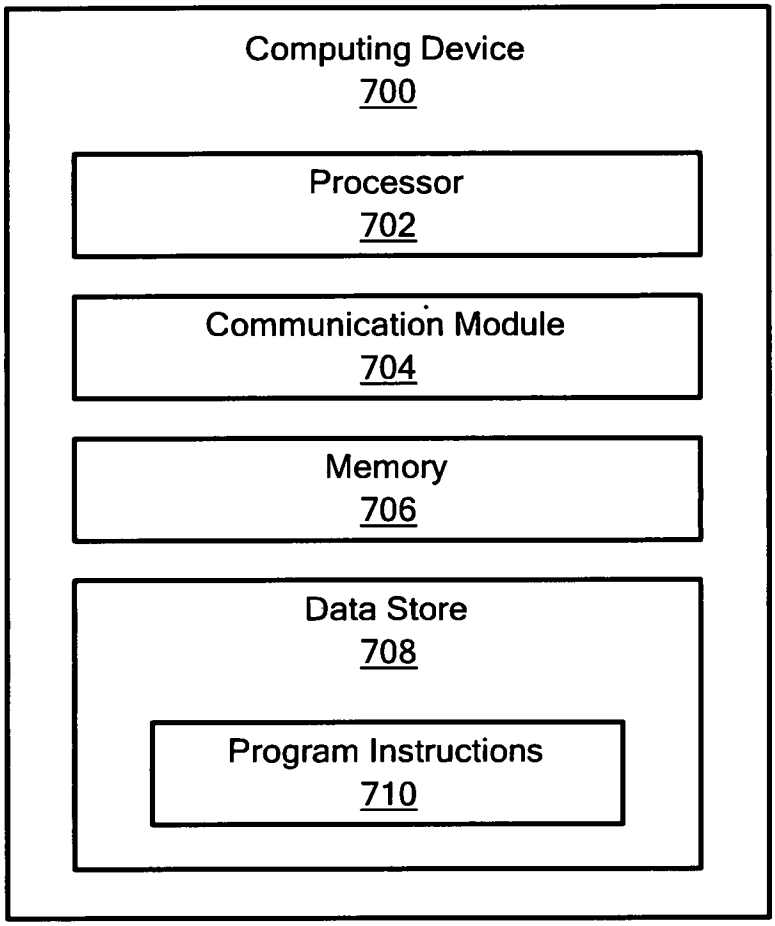

Computing Device
700
Processor
702
Communication Module
704
Memory
706
Data Store
708
Program Instructions
710

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/058254

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G01R 31/311; G06F 21/76 (2019.01)
CPC - G01R 31/311; G06F 21/56; G06F 21/76 (2019.08)

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)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 326/8; 326/15; 382/141; 382/145; 382/147; 726/34; 726/35; 726/36 (keyword delimited)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018/0211377 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 26 July 2018 (26.07.2018) entire document	1-20
A	US 2011/0002528 A1 (BAJURA et al) 06 January 2011 (06.01.2011) entire document	1-20
A	US 2011/0026806 A1 (BERNSTEIN et al) 03 February 2011 (03.02.2011) entire document	1-20
A	US 2013/0312122 A1 (ARORA et al) 21 November 2013 (21.11.2013) entire document	1-20
A	US 2012/0033810 A1 (DEVADAS et al) 09 February 2012 (09.02.2012) entire document	1-20
A	US 2003/0218475 A1 (GAMMEL) 27 November 2003 (27.11.2003) entire document	1-20
A	US 6,251,773 B1 (HARTSWICK et al) 26 June 2001 (26.06.2001) entire document	1-20
A	US 2016/0098561 A1 (NOKOMIS, INC.) 07 April 2016 (07.04.2016) entire document	1-20
A	US 2010/0031064 A1 (WALMSLEY) 04 February 2010 (04.02.2010) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 December 2019	03 JAN 2020
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774