(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2007 051 788 A1** 2009.05.14

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2007 051 788.4**
(22) Anmeldetag: **30.10.2007**
(43) Offenlegungstag: **14.05.2009**

(51) Int Cl.[8]: ***H01L 31/0216*** (2006.01)
H01L 23/552 (2006.01)

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Finkenzeller, Klaus, 85774 Unterföhring, DE;
Baldischweiler, Michael, 81825 München, DE;
Stocker, Thomas, 81739 München, DE

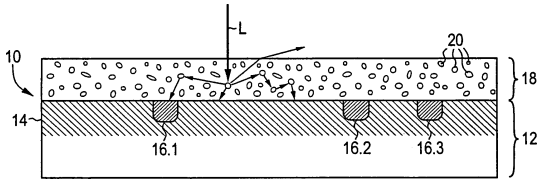
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 198 55 209 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Halbleiterchip mit einer Schutzschicht und Verfahren zum Betrieb eines Halbleiterchip**

(57) Zusammenfassung: Ein Halbleiterchip (10) weist eine integrierte Schaltung (14), mindestens einen Lichtsensor (16.x) und eine Schutzschicht (18) auf. Die Schutzschicht (18) ist als Diffusor für in die Schutzschicht (18) einfallendes Licht (L) ausgebildet. Durch die Diffusionswirkung der Schutzschicht (18) wird das bei einem Lichtangriff einfallende Licht (L) flächig verteilt. Damit wird sichergestellt oder zumindest die Wahrscheinlichkeit erhöht, dass ein gerichteter Lichtangriff von mindestens einem Lichtsensor (16.x) erkannt wird. Die Erfindung stellt ferner ein Halbleiterbauteil, einen tragbaren Datenträger und ein Verfahren zum Betrieb eines Halbleiterchips bereit.



Beschreibung

[0001] Die Erfindung betrifft allgemein das technische Gebiet der integrierten Schaltungen und insbesondere das Gebiet der Sicherung eines Halbleiterchip gegen Angriffe.

[0002] Mikrocontroller und andere Halbleiterchips mit komplexen Funktionen werden für eine Vielzahl sicherheitskritischer Anwendungen eingesetzt, beispielsweise bei Finanztransaktionen oder bei der Zugangskontrolle oder bei der elektronischen Verschlüsselung oder Signatur von Dokumenten. Bei derartigen Anwendungen kann durch eine unbefugte Ausspähung oder Manipulation der im Chip gespeicherten Daten bzw. der durch den Chip ausgeführten Verfahren hoher Schaden entstehen. Besonders gefährdet sind Chips, die sich im unüberwachten Besitz des Anwenders befinden, wie dies z. B. bei Chipkarten (Smart Cards) oder Chipmodulen oft der Fall ist.

[0003] Es sind diverse Angriffsverfahren zur Ausspähung und/oder Manipulation von Mikrocontrollern und anderen Halbleiterchips bekannt. Eine an sich bekannte Klasse von Angriffen sind so genannte Fehlerangriffe (Fault Attacks), bei denen die Programmausführung und/oder der Speicherinhalt eines Halbleiterchip durch externe Einwirkung gestört wird. Beispielsweise wird bei einem so genannten Lichtangriff intensives Licht auf den freigelegten Halbleiterchip gestrahlt. Die dadurch bewirkte Störung der regulären Chipfunktion kann die Sicherheit der vom Halbleiterchip ausgeführten Verfahren bzw. der auf dem Chip gespeicherten Daten kompromittieren, wenn z. B. der Chip als Folge der Lichteinstrahlung fehlerhaft verschlüsselte Daten ausgibt, deren Analyse Rückschlüsse auf einen geheimen Schlüssel zuläßt.

[0004] EP 1 429 227 A2 zeigt einen Mikrocontroller für eine Chipkarte, bei dem Lichtsensoren in ein Speicherfeld integriert sind. Wenn ein Lichtsensor eine irreguläre Lichteinstrahlung erkennt, können beispielsweise interne Aktionen des Mikrocontrollers gestoppt werden. Teile der Lichtsensoren sind mit einer Metallschicht abgedeckt.

[0005] WO 00/11719 A1 beschreibt einen Halbleiterchip mit einer elektrisch leitenden Schutzschicht, die mit einem elektrischen Schutzsensor verbunden ist. Der Schutzsensor vermag eine Manipulation des Halbleiterchip durch ein FIB-Verfahren (FIB = focused ion beam) aufgrund der dabei in der Schutzschicht hervorgerufenen elektrischen Spannung zu erkennen.

[0006] WO 2006/058510 A1 offenbart einen Halbleiterchip mit einer Passivierungsschicht, die aus einem Polymer mit eingebetteten mineralisch-keramischen Nanopartikeln besteht. Durch diese Ausgestaltung soll die Wärmeübertragung von dem Halbleiterchip auf ein angrenzendes Kunststoffgehäuse verbessert werden.

[0007] EP 1 410 319 B1 offenbart einen tragbaren Datenträger mit einer Sicherheitseinrichtung. Die Sicherheitseinrichtung sendet ein Sicherheitssignal, das von einem im Körper des Datenträgers integrierten Beeinflussungsmittel beeinflusst wird. Wenn keine korrekte Beeinflussung erkannt wird, sperrt ein Sperrmittel einen sicherheitskritischen Betriebszustand.

[0008] Bei einem Halbleiterchip mit Lichtsensoren – wie z. B. dem oben bereits gewürdigten Mikrocontroller gemäß EP 1 429 227 A2 – besteht das Problem, dass aus wirtschaftlichen und praktischen Gründen die Anzahl und Dichte der Lichtsensoren beschränkt ist. Ein Angreifer kann daher möglicherweise einen ausreichend fein fokussierten Lichtstrahl an den Lichtsensoren vorbei auf andere kritische Teile des Mikrocontrollers richten und somit einen erfolgreichen Lichtangriff ausführen.

[0009] Die Erfindung hat demgemäß die Aufgabe, eine Technik bereitzustellen, die es ermöglicht, einen Lichtangriff auf einen mit mindestens einem Lichtsensor ausgestatteten Halbleiterchip mit hoher Sicherheit zu erkennen.

[0010] Erfindungsgemäß wird diese Aufgabe ganz oder zum Teil gelöst durch einen Halbleiterchip mit den Merkmalen des Anspruchs 1, ein Halbleiterbauteil mit den Merkmalen des Anspruchs 9, einen tragbaren Datenträger gemäß Anspruch 12 und ein Verfahren zum Betrieb eines Halbleiterchip nach Anspruch 13. Die abhängigen Ansprüche betreffen optionale Merkmale einiger Ausgestaltungen der Erfindung.

[0011] Die Erfindung beruht auf der Grundidee, eine Schutzschicht für den Halbleiterchip vorzusehen, die als Diffusor für in die Schutzschicht einfallendes Licht ausgebildet ist. Von außen einfallendes Licht wird somit, selbst wenn es nur punktförmig auf die Schutzschicht auftrifft, durch die Schutzschicht flächig verteilt. Je nach den optischen Eigenschaften der Schutzschicht und der Anzahl und Verteilung der Lichtsensoren wird damit sichergestellt oder zumindest die Wahrscheinlichkeit erhöht, dass ein gerichteter Lichtangriff von dem Lichtsensor oder zumindest einem der Lichtsensoren erkannt wird. Der Lichtsensor kann daraufhin eine geeignete Sicherheitsfunktion aktivieren, also z. B. die integrierte Schaltung in einen Ruhezustand versetzen oder eine Datenausgabe unterdrücken.

[0012] In der Wortwahl des vorliegenden Dokuments soll unter Licht jede elektromagnetische Strahlung verstanden werden, die zur Ausführung eines

Lichtangriffs geeignet ist, also insbesondere sichtbares Licht sowie Ultraviolett- und Infrarot-Licht.

[0013] Die integrierte Schaltung des erfindungsgemäßen Halbleiterchip stellt Funktionen eines Prozessors und/oder eines Speichers bereit. Dies heißt jedoch weder, dass die Schaltung keine anderen Funktionen aufweisen darf, noch, dass die Schaltung alle Funktionen eines Prozessors oder Speichers bieten muss. Insbesondere kann es sich bei der Schaltung um einen Mikrocontroller handeln, der beispielsweise zur Verwendung in Chipkarten oder Chipmodulen vorgesehen ist.

[0014] Die Funktion der Schutzschicht als Diffusor kann auf jedem beliebigen physikalischen Effekt beruhen. In vielen Ausführungsbeispielen wird das in die Schutzschicht einfallende Licht hauptsächlich gestreut; es kann jedoch in anderen Ausgestaltungen auch gebrochen und/oder gebeugt und/oder reflektiert und/oder durch eine Interferenz abgelenkt werden.

[0015] Allgemein kann die Diffusionswirkung der Schutzschicht durch beliebige optisch aktive Flächen oder Bereiche hervorgerufen werden, beispielsweise durch mindestens eine Grenzfläche – z. B. eine Oberfläche der Schutzschicht oder eine Grenzfläche im Inneren der Schutzschicht – oder durch Einschlüsse – z. B. kleine Hohlräume – in der Schutzschicht. In vielen Ausgestaltungen sind in der Schutzschicht Partikel vorgesehen. Solche Partikel können beispielsweise aus Glas oder einem anderen geeigneten Material bestehen.

[0016] In manchen Ausgestaltungen sind die Partikel so genannte Nanopartikel. Beispielsweise kann der durchschnittliche mittlere Durchmesser der Partikel zwischen 1 nm und 1000 nm oder zwischen 1 nm und 100 nm betragen. In manchen Ausführungsformen sind die Partikel hinsichtlich Material und Größe so ausgebildet, dass sie in einer klaren Schutzschicht mit bloßem Auge nicht sichtbar sind. Dies ist z. B. bei Nano-Glaspartikeln in der Regel der Fall.

[0017] Die als Diffusor wirkende Schutzschicht kann prinzipiell jede Schicht oder Kombination von Schichten sein, die den Halbleiterchip ganz oder teilweise bedeckt. Besonders kostengünstig sind Ausgestaltungen, bei denen die bei Halbleiterchips übliche Passivierungsschicht auch als Diffusor-Schutzschicht wirkt.

[0018] In manchen Ausführungsformen ist eine aktive Überwachung der Schutzschicht vorgesehen. Hierzu kann der Halbleiterchip beispielsweise mindestens eine Lichtquelle aufweisen, wobei das von der Lichtquelle in die Schutzschicht eingestrahlte Licht dort diffus zu mindestens einem Lichtsensor geleitet wird. Hierdurch lassen sich in manchen Ausgestaltungen Kenndaten über die Lichtleiteigenschaften der Schutzschicht bestimmen, die als individuelles Merkmal des einzelnen Halbleiterchip oder als generisches Merkmal einer Serie von Halbleiterchips verwendet werden können.

[0019] Die Erfindung umfasst ferner ein Halbleiterbauteil mit einem Halbleiterchip, der zumindest zum Teil von Vergussmasse umgeben ist. Die Vergussmasse weist Partikel auf, die bei einer Hochfrequenz-Einstrahlung in Resonanz geraten. Eine Überwachungsschaltung ist dazu eingerichtet, ein Hochfrequenz-Sendesignal zu erzeugen und die durch dieses Sendesignal hervorgerufene Resonanz der Partikel zu messen. Bei derartigen Ausgestaltungen lässt sich eine an der Vergussmasse vorgenommene Manipulation zuverlässig erkennen, so dass z. B. eine geeignete Sicherheitsfunktion aktiviert werden kann.

[0020] Der erfindungsgemäße tragbare Datenträger ist in manchen Ausführungsformen als Chipkarte (Smart Card) oder Chipmodul (z. B. als SIM oder MMC oder RFID-Tag oder Schlüsselgriff) ausgebildet.

[0021] Weitere Merkmale, Vorteile und Aufgaben der Erfindung gehen aus der folgenden genauen Beschreibung mehrerer Ausführungsbeispiele und Ausführungsvarianten hervor. Es wird auf die schematischen Zeichnungen verwiesen, in denen zeigen:

[0022] Fig. 1 einen Querschnitt durch einen Halbleiterchip nach einem Ausführungsbeispiel der Erfindung,

[0023] Fig. 2 eine Draufsicht auf einen Halbleiterchip in einem abgewandelten Ausführungsbeispiel,

[0024] Fig. 3 einen Querschnitt entlang der Linie III-III in Fig. 2,

[0025] Fig. 4 einen Querschnitt durch ein Halbleiterbauteil nach einem weiteren Ausführungsbeispiel,

[0026] Fig. 5 eine vergrößerte schematische Darstellung einer Überwachungsschaltung in dem Ausführungsbeispiel von Fig. 4, und

[0027] Fig. 6 eine schematische Darstellung eines komplexen Merkmals des Halbleiterbauteils in dem Ausführungsbeispiel von Fig. 4 und Fig. 5.

[0028] In Fig. 1 ist ein Halbleiterchip **10** gezeigt, der im vorliegenden Ausführungsbeispiel zur Verwendung in einem tragbaren Datenträger – z. B. in einer Chipkarte oder einem Chipmodul – vorgesehen ist. Der Hableiterchip **10** weist ein beispielsweise aus Silizium gefertigtes Substrat **12** auf, in dem in an sich bekannter Weise eine integrierte Schaltung **14** aus-

gebildet ist. Im vorliegenden Ausführungsbeispiel bildet die integrierte Schaltung **14** einen Mikrocontroller, der einen Prozessorkern und mehrere in unterschiedlichen Technologien ausgestaltete Speicherfelder – z. B. ROM, RAM und EEPROM – aufweist.

[0029] In dem Halbleiterchip **10** sind ferner Lichtsensoren **16.1**, **16.2**, **16.3**, ... ausgebildet, die im folgenden zusammenfassend mit **16.x** bezeichnet werden. Die Lichtsensoren **16.x** sind in dem in Fig. 1 gezeigten Ausführungsbeispiel in der Fläche der integrierten Schaltung **14** räumlich verteilt angeordnet. Die Anzahl der Lichtsensoren **16.x** und ihre Anordnung kann in unterschiedlichen Ausgestaltungen unterschiedlich gewählt werden; im Extremfall kann ein einziger Lichtsensor ausreichen.

[0030] Jeder der Lichtsensoren **16.x** ist dazu eingerichtet, einfallendes Licht zu erkennen. Übersteigt die Stärke des einfallenden Lichts einen vorgegebenen Schwellwert, so wird ein Lichtangriff vermutet. Der Lichtsensor **16.x** aktiviert dann eine Sicherheitsfunktion der integrierten Schaltung **14**. Je nach den Funktionen der integrierten Schaltung **14** kann diese Sicherheitsfunktion beispielsweise bewirken, dass ein Speicherbereich gelöscht wird, oder dass eine Hardware-Unterbrechung (Interrupt) ausgelöst wird oder ein Speicherbit (Flog) gesetzt wird. Wenn es sich bei der integrierten Schaltung **14** um einen Mikrocontroller handelt, kann dieser in Reaktion auf die Lichtangriffserkennung beispielsweise ein gerade ausgeführtes Programm abbrechen oder in eine Endlosschleife springen oder geplante Ausgaben unterdrücken.

[0031] Im Stand der Technik ist die Nutzung von Lichtsensoren zur Lichtangriffserkennung bei einem Halbleiterchip an sich bekannt. Eine Besonderheit des in Fig. 1 gezeigten Ausführungsbeispiels ist jedoch, dass der Halbleiterchip **10** durch eine Schutzschicht **18** abgedeckt ist, die als Diffusor für in die Schutzschicht **18** einfallendes Licht wirkt. Beispielsweise kann die Schutzschicht **18** eine Passivierungsschicht des Halbleiterchip **10** sein, in der sich Glaspartikel in Nanometer-Größe befinden; einige dieser Partikel sind in Fig. 1 mit dem Bezugszeichen **20** gezeigt.

[0032] In unterschiedlichen Ausführungsformen der Erfindung braucht die Schutzschicht **18** nicht notwendigerweise eine Passivierungsschicht zu sein, sondern kann zusätzlich zu einer herkömmlichen Passivierungsschicht – die eine Oxidation der Schaltungsstrukturen des Halbleiterchip **10** verhindert – vorgesehen sein. Die Schutzschicht **18** braucht dann nicht notwendigerweise die gesamte integrierte Schaltung **14** zu bedecken, sondern kann auf kritische Bereiche beschränkt sein. Ferner kann die Schutzschicht **18** in manchen Ausgestaltungen ihrerseits mehrere übereinander angeordnete Teilschichten und/oder mehrere nebeneinander angeordnete Bereiche aufweisen.

[0033] In Fig. 1 ist ein gebündelter Lichtstrahl L – beispielsweise ein kohärenter Laserstrahl – gezeigt, der auf den Halbleiterchip **10** gerichtet ist und in die Schutzschicht **18** eindringt. Bei einem Halbleiterchip nach dem Stand der Technik, der eine klare Passivierungsschicht aufweist, würde der Lichtstrahl L die Passivierungsschicht durchdringen und auf die Oberfläche der integrierten Schaltung **14** auftreffen. Da der Lichtstrahl L in diesem Fall an der Auftreffstelle nach wie vor gebündelt wäre, ist nicht sicher, ob einer der Lichtsensoren **16.x** ansprechen würde.

[0034] Bei dem in Fig. 1 gezeigten Ausführungsbeispiel wird der Lichtstrahl L dagegen an den Partikeln **20** in unterschiedliche Richtungen abgelenkt, also beispielsweise gestreut. Das sich somit in der Schutzschicht **18** ergebende Streulicht ist in Fig. 1 durch dünne Pfeile dargestellt. Der ursprünglich gebündelte Lichtstrahl L wird dadurch flächenmäßig aufgeweitet, so dass er zumindest einen der Lichtsensoren **16.x** – in Fig. 1 beispielsweise den Lichtsensor **16.1** – erreicht. Die Sicherheitsfunktion des Halbleiterchip **10** wird somit auch im Falle eines Lichtangriffs mit einem gebündelten Lichtstrahl L zuverlässig aktiviert.

[0035] Die entscheidende Eigenschaft der Schutzschicht **18** ist ihre Diffusionswirkung für in die Schutzschicht **18** einfallendes Licht. Diese Wirkung wird im oben beschriebenen Ausführungsbeispiel durch die Partikel **20** in der ansonsten klaren Schutzschicht **18** erreicht, wobei die Partikel **20** eine Größe von beispielsweise 1 nm–100 nm aufweisen und mit bloßem Auge nicht sichtbar sind. In Ausführungsvarianten können jedoch andere Mittel zum Erzielen der gewünschten Diffusionswirkung vorgesehen sein, z. B. eine raue Grenzfläche oder Einschlüsse in der Schutzschicht **18**. Die Diffusion kann prinzipiell auf beliebigen physikalischen Effekten, beispielsweise einer Streuung und/oder Brechung und/oder Beugung und/oder Reflexion und/oder Interferenz beruhen.

[0036] Insgesamt ergibt sich bei dem in Fig. 1 gezeigten Ausführungsbeispiel – je nach dem Grad der Diffusionswirkung und der Dicke der Schutzschicht **18** – eine besonders zuverlässige Lichtangriffserkennung und/oder eine Einsparung hinsichtlich der Anzahl der benötigten Lichtsensoren **16.x**.

[0037] Bei dem gerade beschriebenen Ausführungsbeispiel besteht die theoretische Möglichkeit, dass ein Angreifer die Schutzschicht **18** durch chemische Mittel entfernt, bevor der Lichtangriff ausgeführt wird. Ein solcher Angriff ist jedoch insbesondere dann nicht einfach, wenn die Schutzschicht **18** auch als Passivierungsschicht dient, weil in diesem Fall die freigelegte integrierte Schaltung **14** dem Luftsauer-

stoff ausgesetzt wäre und damit in kurzer Zeit funktionsunfähig werden würde.

[0038] In dem in Fig. 2 und Fig. 3 gezeigten Ausführungsbeispiel wird die gerade beschriebene Angriffsmöglichkeit durch eine aktive Überwachung der Schutzschicht **18** verhindert. Hierzu wird zumindest einer der Lichtsensoren **16.x** – z. B. der Lichtsensor **16.2** – als Lichtquelle betrieben. Das von dieser Lichtquelle in die Schutzschicht **18** eingestrahlte Licht wird, wie in Fig. 3 gezeigt, von den Partikeln **20** gestreut oder auf sonstige Weise in diffuses Licht umgewandelt. Ein Teil dieses diffusen Lichts trifft auf andere Lichtsensoren **16.x**, z. B. den Lichtsensor **16.3** in Fig. 3. Offensichtlich tritt dieser Effekt nicht auf, wenn die Schutzschicht **18** entfernt worden ist. Der Effekt kann daher zur Überwachung der Schutzschicht **18** und zur Erkennung des oben beschriebenen Angriffs verwendet werden.

[0039] In unterschiedlichen Ausführungsformen können einige oder alle Lichtsensoren **16.x** so ausgestaltet sein, dass sie wahlweise auch als Lichtquellen verwendbar sind. Es sind jedoch auch Ausführungsformen möglich, in denen eine oder mehrere Lichtquellen als separate Bauteile – zusätzlich zu den Lichtsensoren **16.x** – vorgesehen sind.

[0040] Das Ausmaß der diffusen Lichtleitung in der Schutzschicht **18** hängt von den Eigenschaften der Schutzschicht **18** – insbesondere ihrer Dicke und der zufälligen Verteilung der darin enthaltenen Partikel **20** – ab. Wenn in einer Ausführungsform eine Schutzschicht **18** mit besonders guten und gleichförmigen Diffusionseigenschaften verwendet wird, ist es ein Merkmal aller Halbleiterchips **10** dieser Ausführungsform, dass ein von einer Lichtquelle ausgesandter Lichtimpuls von allen anderen Lichtsensoren **16.x** erkannt wird. Das Vorhandensein dieses Merkmals kann durch ein für alle Halbleiterchips **10** fest vorgegebenes Verfahren überprüft werden, bei dem z. B. der Reihe nach jeder der Lichtsensoren **16.x** als Lichtquelle aktiviert wird und überprüft wird, ob alle anderen Lichtsensoren **16.x** den Lichtimpuls empfangen.

[0041] In anderen Ausgestaltungen weist die Schutzschicht **18** weniger gute, aber für alle Halbleiterchips **10** ungefähr gleiche Diffusionseigenschaften auf. Auch in diesem Fall kann ein fest vorgegebenes Verfahren zum Erkennen von Manipulationen an der Schutzschicht **18** verwendet werden. Bei diesem Verfahren wird beispielsweise überprüft, ob ein von einer Lichtquelle ausgestrahlter Lichtimpuls von allen umliegenden Lichtsensoren **16.x** empfangen wird.

[0042] Ferner sind Ausgestaltungen möglich, bei denen die Diffusionseigenschaften der Schutzschicht **18** für jeden Halbleiterchip **10** individuell unterschiedlich sind. Dies kann beispielsweise durch eine zufällige und relativ ungleichmäßige Verteilung der Partikel **20** in der Schutzschicht **18** bewirkt werden. So erstreckt sich z. B. das in Fig. 2 gezeigte Streulicht innerhalb der Schutzschicht **18** nicht gleichmäßig in alle Richtungen von dem als Lichtquelle wirkenden Lichtsensor **16.2**, sondern breitet sich in Richtung zum Lichtsensor **16.1** weiter als in Richtung zum Lichtsensor **16.3** aus.

[0043] Derartige ungleichmäßige Diffusionseigenschaften der Schutzschicht **18** werden in manchen Ausführungsformen der Erfindung zur Ermittlung eines Merkmals verwendet, das für den jeweiligen Halbleiterchip **10** individuell ist. Weil dieses Merkmal beispielsweise auf der zufälligen Verteilung der Partikel **20** in der Schutzschicht **18** beruht, ist es nicht duplizierbar. In unterschiedlichen Ausgestaltungen kann das individuelle Merkmal z. B. zur Erkennung von Manipulationen an der Schutzschicht **18** und/oder als Sicherheitsmerkmal zur Identifikation des Halbleiterchip **10** verwendet werden.

[0044] Um das individuelle Merkmal zu bestimmen, werden die vorhandenen Lichtquellen – z. B. einer oder mehrere der Lichtsensoren **16.x** – der Reihe nach aktiviert, und das jeweils von den anderen Lichtsensoren **16.x** empfangene Streulicht wird gemessen. Hierbei kann eine binäre Messung – also ein Vergleich mit einem vorgegebenen Schwellwert – oder eine Messung in mehr als zwei – beispielsweise 16 oder 256 – Stufen erfolgen. Die so ermittelten Messwerte oder Streulichtstärken für die einzelnen Lichtquellen ergeben Kenndaten, die für die Diffusionseigenschaften der Schutzschicht **18** charakteristisch sind. Diese Kenndaten können gespeichert, mit vorab ermittelten und gespeicherten Kenndaten verglichen, oder unmittelbar weiterverwendet werden.

[0045] Wenn die Kenndaten zur Erkennung von Manipulationen der Schutzschicht **18** verwendet werden sollen, müssen Referenzwerte vorliegen, die beispielsweise bei der Herstellung des Halbleiterchip **10** oder bei der Initialisierung oder Personalisierung ermittelt werden. Diese Referenzwerte werden im Halbleiterchip **10** unveränderlich gespeichert. Während des späteren Betriebs des Halbleiterchips **10** werden aktuelle Kenndaten nach dem oben beschriebenen Verfahren ermittelt und mit den gespeicherten Werten verglichen. In manchen Ausgestaltungen werden bei dem Vergleich zulässige Abweichungen der gemessenen Werte – die z. B. durch Alterung oder Spannungsschwankungen hervorgerufen werden können – berücksichtigt.

[0046] Wenn die gespeicherten Kenndaten und die aktuell ermittelten Werte identisch sind oder sich nur in geringem Maße unterscheiden, kann eine Manipulation der Schutzschicht **18** mit hoher Wahrscheinlichkeit ausgeschlossen werden. Falls dagegen eine erhebliche Abweichung auftritt, wird eine Sicherheits-

funktion – z. B. eine der oben bereits genannten Funktionen – aktiviert.

[0047] Statt oder zusätzlich zu der gerade beschriebenen Nutzung des individuellen Merkmals zur Manipulationserkennung können die Kenndaten zur eindeutigen Identifikation des Halbleiterchip **10** verwendet werden. Beispielsweise können die jeweils aktuell ermittelten Kenndaten in die Berechnung eines geheimen Schlüssels oder eines Kennworts oder einer Signatur des Halbleiterchip **10** eingehen. Hierzu können z. B. die Kenndaten mit einer für den Halbleiterchip **10** individuellen Seriennummer verknüpft werden. Auch hier werden vorzugsweise geeignete Vorkehrungen getroffen – z. B. eine fehlerkorrigierende Prüfsumme –, um leichte Variationen der jeweils gemessenen Werte auszugleichen. Insgesamt ergibt sich somit ein Sicherheitsmerkmal des Halbleiterchip **10**, das mit dem MM-Modul einer Kunststoffkarte vergleichbar ist.

[0048] Die Grundidee der Ausgestaltung gemäß Fig. 2 und Fig. 3 ist somit, dass der Halbleiterchip **10** Licht ausstrahlt und die Wechselwirkung dieses Lichts mit der Schutzschicht **18** überwacht wird. In weiteren Ausführungsformen der Erfindung wird diese Grundidee dadurch variiert, dass nicht Licht, sondern elektromagnetische Wellen in einem anderen Frequenzbereich ausgestrahlt werden, und dass die Wechselwirkung dieser Wellen mit Partikeln in einer Vergussmasse überwacht wird. Eine derartige Ausgestaltung eines Halbleiterbauteils **22** ist in Fig. 4 gezeigt.

[0049] Bei dem in Fig. 4 dargestellten Halbleiterbauteil **22** ist ein Halbleiterchip **10'** auf einem Träger **24** – beispielsweise einem Kartenkörper einer Chipkarte – angebracht. Der Halbleiterchip **10** weist ein Silizium-Substrat **12'**, eine in dem Substrat **12'** ausgebildete integrierte Schaltung **14** und eine die integrierte Schaltung **14'** abdeckende Schutzschicht **18'** auf. In unterschiedlichen Ausgestaltungen kann der Halbleiterchip **10'** entweder gemäß den oben beschriebenen Ausführungsbeispielen – also z. B. mit einer Licht streuenden Schutzschicht **18'** – oder mit einer herkömmlichen Passivierungsschicht als Schutzschicht **18'** ausgestaltet sein.

[0050] Auf der Schutzschicht **18'** ist eine Antenne **26** angeordnet, deren Funktion unten noch genauer beschrieben wird. Eine Vergussmasse **28** umgibt den Halbleiterchip **10'** und schützt ihn gegen Umwelteinflüsse und Angriffe, wie beispielsweise mechanische Manipulationsversuche oder Lichtangriffe. In Ausführungsalternativen kann die Antenne **26** auch zwischen zwei Lagen der Vergussmasse **28** eingebettet sein oder als Teil der Schaltungsstrukturen der integrierten Schaltung **14'** ausgebildet sein.

[0051] Die Vergussmasse **28** besteht typischerweise aus einem anorganischen Material, das sich z. B. durch einen Ätzvorgang mit geeigneten chemischen Mitteln entfernen lässt. Hierdurch würde der von der Vergussmasse **28** geschützte Halbleiterchip **10'** freigelegt und damit potentiellen Angriffen – z. B. Lichtangriffen – ausgesetzt werden.

[0052] Die hier beschriebenen Ausführungsbeispiele weisen daher einen Mechanismus auf, mit dem sich eine Manipulation der Vergussmasse **28** – z. B. deren vollständiges oder teilweises Abtragen – erkennen lässt. Hierzu enthält die Vergussmasse **28** eine Vielzahl von Partikeln, von denen in Fig. 4 einige mit dem Bezugszeichen **30** gezeigt sind. Die Partikel **30** sind so ausgestaltet, dass sie in Wechselwirkung mit einem von der Antenne **26** abgestrahlten Hochfrequenz-Wechselfeld treten können.

[0053] Beispielsweise können die Partikel **30** aus einem Material mit elektrischer und/oder magnetischer Leitfähigkeit bestehen und eine an die Wellenlänge angepasste Größe aufweisen. In dem hier beschriebenen Ausführungsbeispiel sind die Partikel **30** dünne Metallfäden mit einer Länge im Bereich einiger Mikrometer. Bei der Herstellung des Halbleiterbauteils **22** werden diese Partikel **30** der flüssigen Vergussmasse **28** beigemengt, bevor die Vergussmasse **28** auf den Halbleiterchip **10'** aufgetragen wird. In der ausgehärteten Vergussmasse **28** sind die Partikel **30** dann zufällig verteilt und zufällig orientiert.

[0054] Eine Überwachungsschaltung **32** ist in dem Halbleiterchip **10'** als Teil der integrierten Schaltung **14'** oder als davon getrennte Baugruppe ausgebildet. Wie in Fig. 5 gezeigt ist, weist die Überwachungsschaltung **32** einen Hochfrequenz-Oszillator **34** auf, der über eine Antennenleitung **36** mit der Antenne **26** verbunden ist. Eine als Teil der Überwachungsschaltung **32** ausgebildete Messeinrichtung **38** weist einen an die Antennenleitung **36** gekoppelten Richtkoppler **40**, einen Gleichrichter **42** und einen Analog/Digital-Wandler **44** auf.

[0055] Beim Betrieb der Überwachungsschaltung **32** erzeugt der Hochfrequenz-Oszillator **34** Frequenzen im Bereich von beispielsweise 10 GHz oder höher. In besonders einfachen Ausgestaltungen kann der Oszillator **34** auf eine einzige feste Frequenz eingestellt sein. Bevorzugt ist der Oszillator **34** jedoch ein frequenzvariabler Oszillator, der in einer Anzahl von Schritten – z. B. zwei oder vier oder sechzehn oder mehr Schritten – oder kontinuierlich abstimmbar ist. Das vom Oszillator **34** erzeugte Sendesignal wird über die Antennenleitung **36** in die Antenne **26** eingespeist. Es versteht sich, dass die Antenne **26** an den Frequenzbereich des Oszillators **26** angepasst ist (Impedanzanpassung).

[0056] Die Größe und Form der Partikel **30** ist so gewählt, dass die Partikel **30** im Frequenzbereich des

Oszillators **34** in elektrische Resonanz geraten. In manchen Ausgestaltungen ist in die Vergussmasse **28** eine Mischung von Partikeln **30** unterschiedlicher Größen – z. B. unterschiedlicher Längen – eingebracht, so dass unterschiedliche Resonanzfrequenzen erzeugt werden und sich ein charakteristisches Ansprechverhalten auf unterschiedliche Oszillatorfrequenzen ergibt.

[0057] Durch die in den Partikeln **30** hervorgerufene Resonanz wird in die Antenne **26** Hochfrequenz-Leistung eingekoppelt, die von der Antenne **26** zur Antennenleitung **36** zurückläuft und dort vom Richtkoppler **40** ausgekoppelt wird. Die ausgekoppelte Rücklaufleistung wird vom Gleichrichter **42** in eine Gleichspannung umgewandelt. Diese Gleichspannung, die proportional zum Resonanzgrad in den Partikeln **30** ist, wird vom Analog/Digital-Wandler **44** erfasst und in einen Digitalwert umgewandelt. Das so ermittelte Resonanzverhalten der Vergussmasse **28** stellt ein Merkmal des Halbleiterbauteils **22** dar, auf dessen Grundlage Manipulationen an der Vergussmasse **28** – insbesondere deren vollständiges oder teilweises Abtragen – erkannt werden können.

[0058] In vielen Ausgestaltungen besteht das Merkmal aus Kenndaten zum Resonanzverhalten der Vergussmasse **28** bei mehreren unterschiedlichen Anregungsfrequenzen. Beispielsweise kann zur Ermittlung des Merkmals vorgesehen sein, dass der Oszillator **34** einen vorgegebenen Frequenzbereich durchläuft, wobei der Oszillator **34** in mehreren diskreten Frequenzschritten stufenweise zwischen den einzelnen vorgesehenen Frequenzen umgeschaltet wird. Fig. 6 zeigt beispielhaft solche Frequenzschritte f_1, f_2, ..., f_7. Für jede dieser diskreten Messfrequenzen ermittelt die Messeinrichtung **38** auf die oben beschriebene Weise den Leistungsrückfluss von der Antenne **26**. In dem Maße, wie einige oder alle der Partikel **30** bei einer bestimmten Messfrequenz in Resonanz geraten, wird auf Grund der von den Partikeln **30** reflektierten Leistung ein erhöhter Leistungsrückfluss von der Antenne **26** gemessen.

[0059] Durch die gerade beschriebene Messung bei mehreren Einzelfrequenzen ergibt sich ein komplexes Merkmal, wie es in Fig. 6 beispielhaft mit gemessenen Amplituden "a" gezeigt ist. Dieses komplexe Merkmal, das auch als "elektronischer Fingerabdruck" angesehen werden kann, ist für das konkrete Halbleiterbauteil **22** – insbesondere für die Anordnung der Vergussmasse **28** und die darin verteilten Partikel **30** – individuell und charakteristisch.

[0060] Die Überwachungsschaltung **32** führt selbsttätig oder gesteuert von dem Halbleiterchip **10'** einen Überwachungsvorgang aus, bei dem dieses charakteristische Merkmal ermittelt und ausgewertet wird. Ähnlich wie bei den oben beschriebenen Ausgestaltungen gemäß Fig. 2 und Fig. 3 kann auch in den vorliegend beschriebenen Ausführungsbeispielen das Merkmal entweder nach einem vorab festgelegten, für alle Halbleiterbauteile einer Serie einheitlichen Verfahren oder durch einen Vergleich mit für das einzelne Halbleiterbauteil **22** individuellen Kenndaten ausgewertet werden. Der Überwachungsvorgang kann z. B. in vorbestimmten Zeitintervallen oder ansprechend auf vorbestimmte Ereignisse angestoßen werden.

[0061] In einer besonders einfachen Ausgestaltung wird lediglich überprüft, ob bei einer oder mehreren Frequenzen des Oszillators **34** eine Resonanz stattfindet, die einen oder mehrere fest vorgegebene/n Grenzwert/e übersteigt. Hierdurch lässt sich zwar eine Entfernung der Vergussmasse **28** erkennen, nicht jedoch eine Manipulation, bei der die ursprüngliche Vergussmasse **28** durch eine andere Vergussmasse mit ähnlichen Eigenschaften ersetzt wird.

[0062] Um die Überwachungsgenauigkeit zu verbessern, ist daher in manchen Ausgestaltungen vorgesehen, bei der Produktion des Halbleiterbauteils **22** eine Messreihe durchzuführen, bei der das individuelle Merkmal auf die oben beschriebene Weise ermittelt wird. Die gemessenen Werte können dann als individuelle Kenndaten in einen nichtflüchtigen Speicher des Halbleiterbauteils **22** eingetragen werden. Diese Kenndaten bilden einen Referenzwert für die Kombination von Halbleiterchip **10** und Vergussmasse **28**.

[0063] In diesen Ausführungsformen wird dann bei dem während des Betriebs des Halbleiterbauteils **22** ausgeführten Überwachungsvorgang das individuelle Merkmal – beispielsweise das in Fig. 6 gezeigte Resonanzprofil – erneut ermittelt und mit den abgespeicherten Werten verglichen. In manchen Ausführungsformen wird hierbei nicht das vollständige Messspektrum durchlaufen, sondern es werden nur auf einigen – z. B. zufällig ausgewählten – Frequenzen Messungen durchgeführt.

[0064] Ergeben sich bei dem Vergleich der aktuellen Messwerte mit den gespeicherten Daten zu große Abweichungen, so wird eine Manipulation oder Beschädigung der Vergussmasse **28** angenommen. Die Überwachungsschaltung **32** aktiviert dann eine Sicherheitsfunktion des Halbleiterchip **10'**. Wie bereits oben beschrieben, kann die Sicherheitsfunktion beispielsweise eine Unterbrechung oder einen Rücksetzvorgang auslösen oder ein gerade ausgeführtes Programm abbrechen oder den Programmfluss in eine Endlosschleife springen lassen.

[0065] Statt oder zusätzlich zu der gerade beschriebenen Nutzung des individuellen Merkmals zur Manipulationserkennung können die jeweils aktuell aus dem Resonanzprofil ermittelten Kenndaten zur eindeutigen Identifikation des Halbleiterbauteils **22** ver-

wendet werden, wie dies oben bereits im Zusammenhang mit der Ausgestaltung gemäß Fig. 2 und Fig. 3 beschrieben wurde.

[0066] Es versteht sich, dass die hier beschriebenen Ausführungsformen und Ausführungsvarianten lediglich als Beispiele zu sehen sind. Weitere Abwandlungen und Kombinationen der hier beschriebenen Merkmale sind für den Fachmann unmittelbar ersichtlich. Dies betrifft insbesondere Kombinationen derjenigen Merkmale, die im vorliegenden Dokument in Zusammenhang mit unterschiedlichen Ausführungsbeispielen beschrieben worden sind.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- EP 1429227 A2 **[0004, 0008]**
- WO 00/11719 A1 **[0005]**
- WO 2006/058510 A1 **[0006]**
- EP 1410319 B1 **[0007]**

Patentansprüche

1. Halbleiterchip (**10**) mit:
– einer integrierten Schaltung (**14**), die Funktionen eines Prozessors und/oder eines Speichers bereitstellt, und
– mindestens einem Lichtsensor (**16.x**), der dazu eingerichtet ist, einen Lichtangriff zu erkennen und ansprechend auf das Erkennen des Lichtangriffs eine Sicherheitsfunktion der integrierten Schaltung (**14**) zu aktivieren, wobei
– der Halbleiterchip (**10**) zumindest zum Teil durch eine Schutzschicht (**18**) abgedeckt ist,
dadurch gekennzeichnet, dass
– die Schutzschicht (**18**) als Diffusor für in die Schutzschicht (**18**) einfallendes Licht (L) ausgebildet ist.

2. Halbleiterchip (**10**) nach Anspruch 1, dadurch gekennzeichnet, dass die Wirkung der Schutzschicht (**18**) als Diffusor auf einer Streuung und/oder Brechung und/oder Beugung und/oder Reflexion und/oder Interferenz beruht.

3. Halbleiterchip (**10**) nach Anspruch 1 oder Anspruch 2, dadurch gekennzeichnet, dass die Schutzschicht (**18**) Partikel (**20**) aufweist, die dazu eingerichtet sind, das in die Schutzschicht (**18**) einfallende Licht (L) in unterschiedliche Richtungen abzulenken.

4. Halbleiterchip (**10**) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Partikel (**20**) Nanopartikel und/oder Glaspartikel sind.

5. Halbleiterchip (**10**) nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Schutzschicht (**18**) eine Passivierungsschicht des Halbleiterchip (**10**) ist.

6. Halbleiterchip (**10**) nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der Halbleiterchip (**10**) mindestens eine Lichtquelle aufweist, die dazu eingerichtet ist, Licht in die Schutzschicht (**18**) einzustrahlen, und dass die Schutzschicht (**18**) dazu eingerichtet ist, das von der mindestens einen Lichtquelle in die Schutzschicht (**18**) eingestrahlte Licht zumindest zum Teil zu dem Lichtsensor bzw. mindestens einem der Lichtsensoren (**16.x**) zu leiten.

7. Halbleiterchip (**10**) nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der Halbleiterchip (**10**) mehrere Lichtsensoren (**16.x**) aufweist und dazu eingerichtet ist, ein Merkmal des Halbleiterchip (**10**) zu bestimmen, indem die Lichtquelle bzw. mindestens eine der Lichtquellen aktiviert wird/werden, die Lichteinstrahlung an den Lichtsensoren (**16.x**) bestimmt wird, und das Merkmal in Abhängigkeit von der Lichteinstrahlung an den Lichtsensoren (**16.x**) bestimmt wird.

8. Halbleiterchip (**10**) nach Anspruch 7, dadurch gekennzeichnet, dass im Halbleiterchip (**10**) Kenndaten gespeichert sind, die durch ein zu einem früheren Zeitpunkt erfolgtes Aktivieren der Lichtquelle bzw. mindestens einer der Lichtquellen und Bestimmen der Lichteinstrahlung an den Lichtsensoren (**16.x**) ermittelt wurden.

9. Halbleiterbauteil (**22**) mit:
– einem Halbleiterchip (**10'**),
– einer Antenne (**26**),
– Vergussmasse (**28**), die den Halbleiterchip (**10'**) und/oder die Antenne (**26**) zumindest zum Teil umgibt, wobei die Vergussmasse (**28**) Partikel (**30**) aufweist, die dazu eingerichtet sind, bei einer Hochfrequenz-Einstrahlung in Resonanz zu geraten, und
– mindestens einer an die Antenne (**26**) angeschlossenen Überwachungsschaltung (**32**), die dazu eingerichtet ist, ein Hochfrequenz-Sendesignal zu erzeugen und die durch dieses Sendesignal hervorgerufene Resonanz der Partikel (**30**) zu messen.

10. Halbleiterbauteil (**22**) nach Anspruch 9, dadurch gekennzeichnet, dass die Überwachungsschaltung (**32**) einen frequenzvariablen Hochfrequenz-Oszillator (**34**) und eine Messeinrichtung (**38**) für von der Antenne (**26**) aufgenommene Rücklaufleistung aufweist.

11. Halbleiterbauteil (**22**) nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der Halbleiterchip (**10'**) gemäß einem der Ansprüche 1 bis 8 ausgebildet ist.

12. Tragbarer Datenträger, insbesondere Chipkarte oder Chipmodul, mit einem Halbleiterchip (**10**) nach einem der Ansprüche 1 bis 8 und/oder einem Halbleiterbauteil (**22**) nach einem der Ansprüche 9 bis 11.

13. Verfahren zum Betrieb eines Halbleiterchip (**10**), bei dem ein Merkmal des Halbleiterchip (**10**) ermittelt wird, wobei der Halbleiterchip (**10**) mindestens eine Lichtquelle und eine Mehrzahl von Lichtsensoren (**16.x**) aufweist und der Halbleiterchip (**10**) zumindest zum Teil durch eine Schutzschicht (**18**) abgedeckt ist, die als Diffusor für in die Schutzschicht (**18**) einfallendes Licht ausgebildet ist, mit den Schritten:
– Aktivieren der Lichtquelle bzw. mindestens einer der Lichtquellen zum Aussenden von Licht in die Schutzschicht (**18**), so dass die Schutzschicht (**18**) das in die Schutzschicht (**18**) eingestrahlte Licht zumindest zum Teil an zumindest einen der Lichtsensoren (**16.x**) leitet,
– Bestimmen der Lichteinstrahlung an den Lichtsensoren (**16.x**), und
– Ermitteln des Merkmals in Abhängigkeit von der Lichteinstrahlung an den Lichtsensoren (**16.x**).

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass das Merkmal nach einem fest

vorgegebenen Verfahren überprüft wird, um eine Manipulation der Schutzschicht (**18**) zu erkennen.

15. Verfahren nach Anspruch 13 oder Anspruch 14, dadurch gekennzeichnet, dass das Merkmal mit im Halbleiterchip (**10**) gespeicherten Kenndaten verglichen wird, um eine Manipulation der Schutzschicht (**18**) zu erkennen.

16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, dass die Kenndaten durch ein zu einem früheren Zeitpunkt erfolgtes Aktivieren der Lichtquelle bzw. mindestens einer der Lichtquellen und Bestimmen der Lichteinstrahlung an den Lichtsensoren (**16.x**) ermittelt wurden.

17. Verfahren nach einem der Ansprüche 13 bis 16, dadurch gekennzeichnet, dass das Merkmal ein für den Halbleiterchip (**10**) individuelles Merkmal ist.

18. Verfahren nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, dass der Halbleiterchip (**10**) gemäß einem der Ansprüche 1 bis 8 ausgebildet ist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

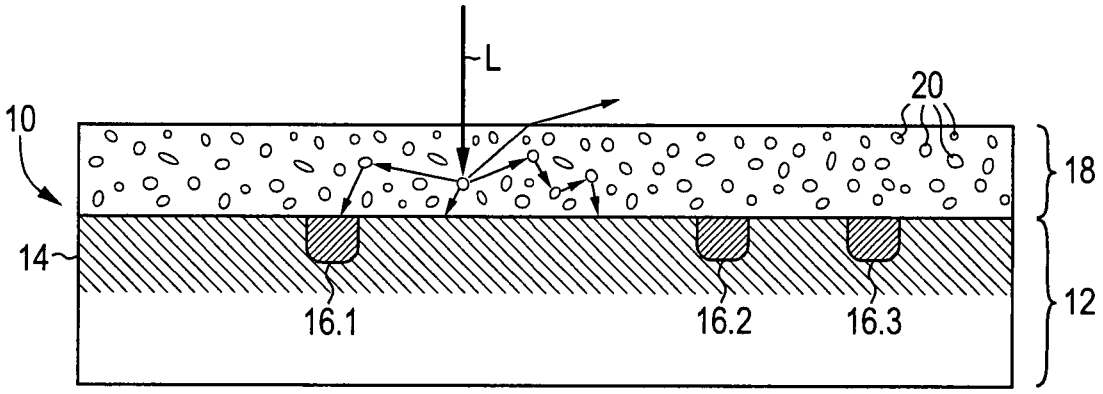


Fig. 1

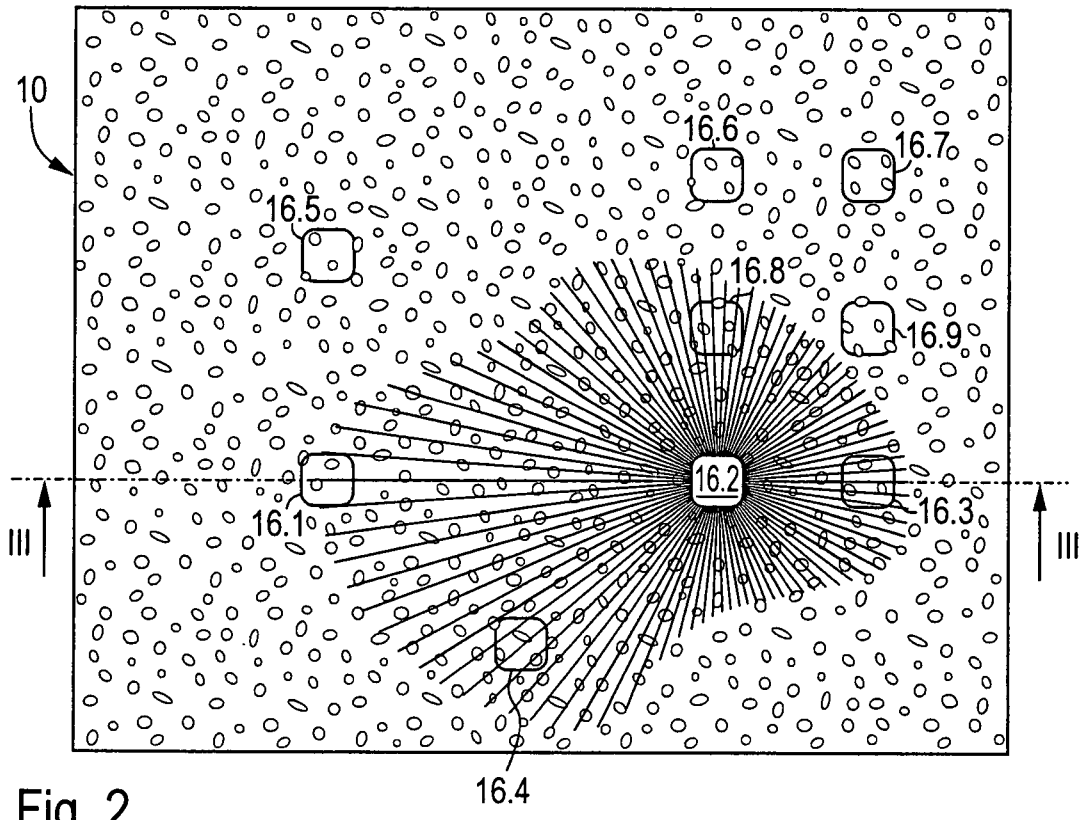


Fig. 2

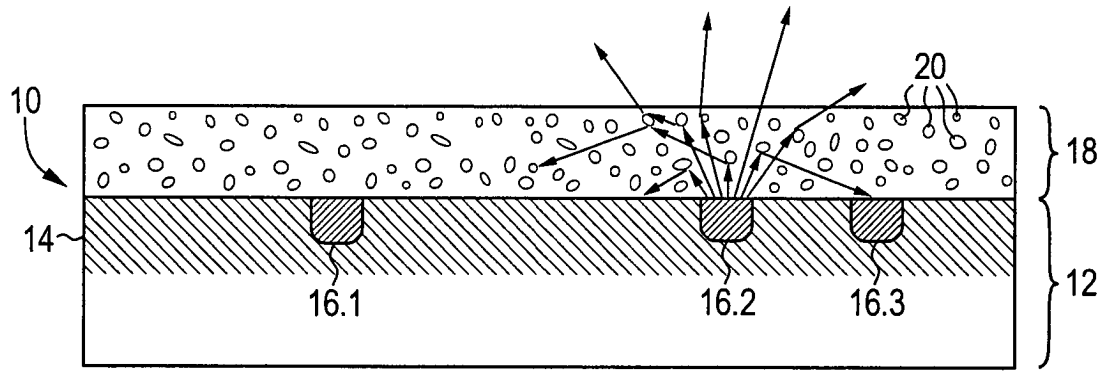


Fig. 3

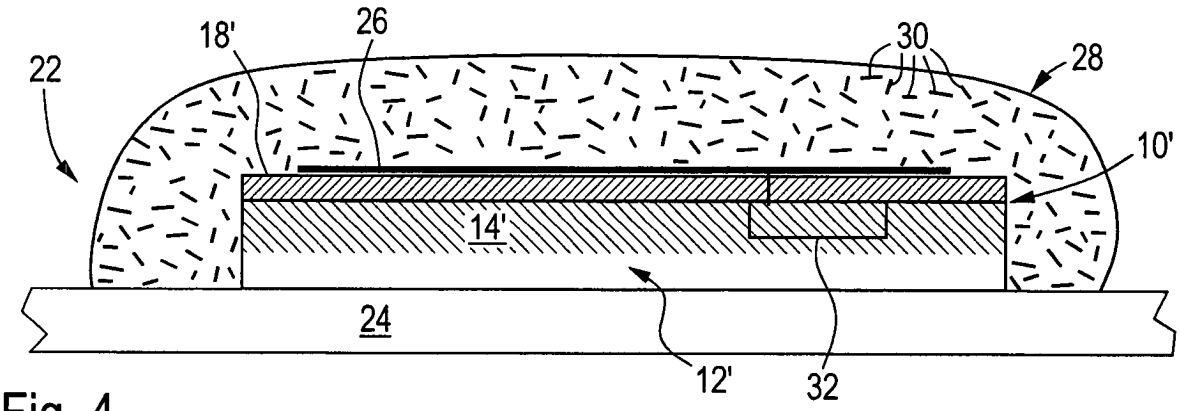


Fig. 4

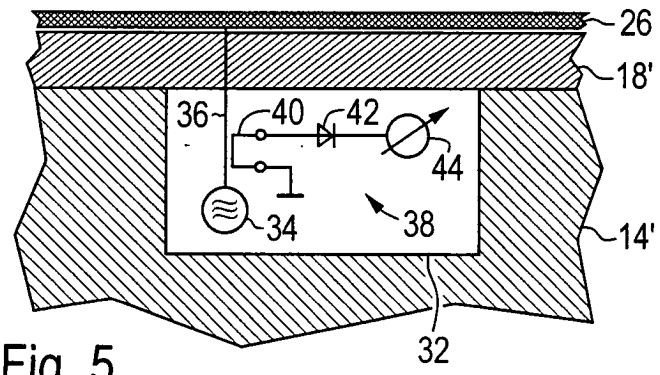


Fig. 5

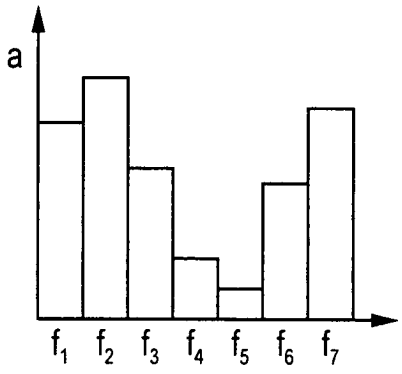


Fig. 6