(19) Deutsches Patent- und Markenamt

(10) **DE 10 2013 219 591 A1** 2015.04.16

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2013 219 591.5**
(22) Anmeldetag: **27.09.2013**
(43) Offenlegungstag: **16.04.2015**

(51) Int Cl.: ***G06K 19/00*** (2006.01)

(71) Anmelder:
Albert-Ludwigs-Universität Freiburg, 79098 Freiburg, DE

(74) Vertreter:
Grünecker Patent- und Rechtsanwälte PartG mbB, 80802 München, DE

(72) Erfinder:
Steiert, Matthias, 79111 Freiburg, DE; Wilde, Jürgen, Prof. Dr., 79189 Bad Krozingen, DE; Berndt, Michael, 79111 Freiburg, DE

(56) Ermittelter Stand der Technik:

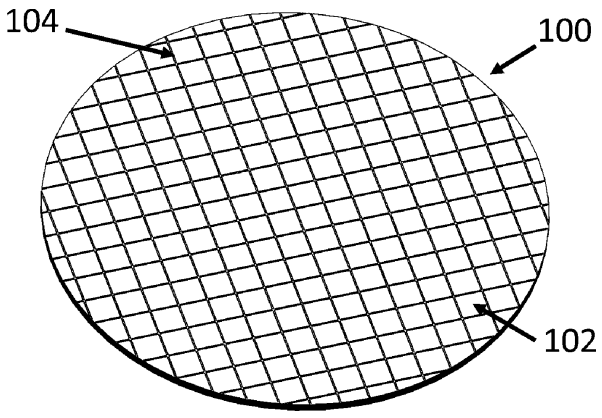
DE	**32 16 867**	**C2**
DE	**101 55 780**	**A1**
DE	**10 2012 204 553**	**A1**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **VERFAHREN ZUM AUTHENTIFIZIEREN MIKROELEKTRONISCHER BAUELEMENTE**

(57) Zusammenfassung: Verfahren zum Authentifizieren mikroelektronischer Bauelemente, wobei das Verfahren folgende Schritte umfasst: Digitalisieren mindestens eines vordefinierten intrinsischen Produktmerkmals für jedes zu authentifizierende mikroelektronische Bauelement, Erzeugen eines Testdatensatzes basierend auf dem digitalisierten Produktmerkmal, Vergleichen des Testdatensatzes mit einem Referenzdatensatz und Feststellen der Authentizität des mikroelektronischen Bauelements, wenn der Testdatensatz innerhalb eines vorgegebenen Rahmens mit dem Referenzdatensatz übereinstimmt, wobei der Referenzdatensatz erzeugt wird durch die folgenden Schritte:
Digitalisieren des mindestens einen vordefinierten intrinsischen Produktmerkmals für jedes zu authentifizierende mikroelektronische Bauelement,
Speichern des digitalisierten Produktmerkmals als Referenzdatensatz,
wobei das Produktmerkmal eine Material- und/oder Strukturveränderung umfasst, die beim Vereinzeln des mikroelektronischen Bauelements aus dem Waferverbund und/oder durch einen zusätzlich durchgeführten Prozessschritt der Vereinzelungstechnologie entsteht.



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf ein Verfahren zum Authentifizieren mikroelektronischer Bauelemente sowie auf eine Vorrichtung zum Durchführen des Verfahrens.

[0002] Die sichere Identifizierung, Authentifizierung und Unterscheidung zwischen originaler und gefälschter Elektronik ist für viele Produkte von wesentlicher Bedeutung. Beispielsweise können die Prinzipien der vorliegenden Erfindung im Zusammenhang mit Mikrosystemen, Mikrochips, Halbleiterchips, integrierten digitalen und analogen Schaltkreisen, mikromechanischen Bauteilen wie Drehratensensoren, Elektronikbauteilen, Printed Circuit Board (PCB)-Schaltungen, Elektronikbaugruppen, wie Motorsteuerungen oder automobilen Fahrerassistenzsystemen, sowie Elektronikgeräten sowohl im Industriebereich, beispielsweise Prozessüberwachungselektronik oder Mikrosensorik und Mikroaktorik, aber auch Messgeräten und Geräten des Consumerbereichs wie Computern, Mobiltelefonen, Fernsehern, digitalen Fotokameras, MP3-Spielern oder Spielekonsolen angewendet werden.

[0003] Die schnelle und zuverlässige Erkennung von gefälschter Elektronik stellt ein bislang ungelöstes Problem dar. Dabei entsteht durch gefälschte Elektronik nicht nur ein wirtschaftlicher Schaden, sondern die gefälschte Elektronik kann auch unmittelbar die Sicherheit des Anwenders gefährden, beispielsweise in sicherheitsrelevanten Bereichen wie Fahrerassistenzsystemen oder Sicherheitseinrichtungen in Industrieanlagen.

[0004] Bei der Problematik gefälschter Elektronik muss zwischen äußeren Eigenschaften und inneren Eigenschaften unterschieden werden. Als äußere Eigenschaft können insbesondere die erwartete elektrische Funktion der Elektronik, damit ist in der Regel ein bestimmtes elektrisches Verhalten an dafür vorgesehenen Ein- und Ausgangsverbindungen gemeint, sowie die äußere Erscheinungsform der elektronischen Komponente bezeichnet werden.

[0005] Im Gegensatz dazu können als innere Eigenschaften all jene Eigenschaften bezeichnet werden, die sich auf Betriebsanforderungen beziehen, beispielsweise Lebensdauer, Schockfestigkeit, Vibrationsfestigkeit, Einsatztemperatur usw. Die inneren Eigenschaften beziehen sich dabei in der Regel auf die Zuverlässigkeit der Elektronik und sie gewährleisten den sicheren Betrieb der Elektronik. Fälschungen von Elektronik beruhen meist auf der Kopie äußerer Eigenschaften, wohingegen die inneren Eigenschaften den entscheidenden technologischen Vorsprung der Originalhersteller markieren.

[0006] Bislang ist kein nicht fälschbares äußeres Merkmal bekannt und daher ist die sichere Erkennung von Fälschungen anhand äußerer Merkmale ein ungelöstes Problem. Eine zuverlässige Erkennung gefälschter Elektronik erfordert gegenwärtig immer aufwendige Analysenmethoden, die innere Eigenschaften untersuchen, beispielsweise durch die Bestimmung von Materialzusammensetzungen.

[0007] Eine in vielen technischen Bereichen übliche Methode der Fälschungssicherung ist das zusätzliche künstliche Ein- oder Anbringen potentiell fälschungssicherer äußerer Merkmale. Dabei sind diese sekundären Sicherheitselemente nicht produkteigen, vielmehr handelt es sich beispielsweise um Sticker, Lacke, Materialpartikel, Materialschichtabscheidungen oder codierte Ziffernfolgen, die an dem Produkt angebracht oder aufgebracht sind. Derartige Sicherheitselemente sind beispielsweise aus der DE 10 2009 033 221 A1, der DE 3843076 A1, der DE 198 10 134 A1, der EP 1 934 950 A1, der EP 1 748 902 A1, der EP 1 674 286 A1, der EP 1 327 531 A1, der EP 919 916 B1, der US 6,022,429, der US 6,264, 296, der US 6,685,312, der US 6,932, 527, der US 6,979,141 sowie der US 7,037,013 bekannt.

[0008] Bei einigen dieser sekundären Sicherheitselemente beruht die Fälschungssicherung auf der nicht beeinflussbaren und absichtlich herbeigeführten Entstehung stochastischer Strukturen. Diese Strukturen werden mit diversen Methoden für jedes Sicherheitselement einzeln digitalisiert und gespeichert. Ein solches Sicherheitselement kann zu einem späteren Zeitpunkt durch einen Vergleich mit den gespeicherten Daten wiedererkannt werden. Ein mit einem derartigen sekundären Sicherheitselement versehenes Produkt ist der Idee nach ebenfalls wieder erkennbar. Ein ähnliches Vorgehen ist bei der Personenerkennung hinlänglich bekannt, etwa als Vergleich von Fingerabdrücken oder durch die Iriserkennung.

[0009] Ein wesentlicher Nachteil derartiger sekundärer Sicherheitselemente besteht darin, dass auch hier letztlich nicht das Produkt selbst fälschungssicher ist, sondern die Fälschungssicherheit nur indirekt durch das nichtprodukteigene Sicherheitselement gegeben ist. Die Fälschungssicherheit ist damit unmittelbar von der tatsächlichen Fälschungssicherheit der eingesetzten Sicherheitselemente abhängig. Durch die aus dem Stand der Technik bekannten Verfahren der Fälschungssicherung unter Nutzung sekundärer Sicherheitselemente wird oftmals nur der Fälscheraufwand erhöht, ohne die Fälschung abschließend unmöglich zu machen.

[0010] Wird beispielsweise die Struktur eines bereits in Umlauf gebrachten sekundären Sicherheitselements bekannt, so besteht prinzipiell die Möglich-

keit, diese Struktur mit Fälschermethoden so nachzubilden, dass für einen Laien die Fälschung nicht augenscheinlich ist. Dann wird das Vorhandensein einer Fälschung erst erkannt, wenn die gleiche Struktur zeitgleich in Erscheinung tritt oder ein Fälschungsexperte das gefälschte Sicherheitselement anhand anderer Eigenschaften, etwa Materialeigenschaften, erkennt. Im Falle von Elektronik besteht damit weiterhin das Risiko, dass sich Fälschungen unerkannt in Umlauf befinden. Bei der Fälschungssicherheit durch sekundäre Sicherheitselemente bleibt die abschließende Identifizierung und Authentifizierung weiterhin die Aufgabe entsprechender Fälschungsexperten unter Verwendung aufwändiger Analysemethoden.

[0011] Es besteht daher nach wie vor das Bedürfnis nach einem Verfahren, das die schnelle und zuverlässige Unterscheidung und Erkennung von Fälschungen und originaler elektronischer Bauelemente auf der Basis unfälschbarer intrinsischer Merkmale erlaubt und die Fälschung von Elektronik a priori unmöglich macht.

[0012] Diese Aufgabe wird durch den Gegenstand der unabhängigen Patentansprüche gelöst. Vorteilhafte Weiterbildungen sind Gegenstand der abhängigen Patentansprüche.

[0013] Die vorliegende Erfindung basiert auf der Idee, intrinsische und a priori fälschungssichere Material- oder Strukturveränderungen, die eine eigentlich unerwünschte Folge des Prozesses der Wafervereinzelung sind, zur Authentifizierung mikroelektronischer Bauelemente zu nutzen.

[0014] Bei der Fertigung mikroelektronischer und mikromechanischer Bauteile stellt die Chipvereinzelung der fertig prozessierten Bauteile, die sich noch im Verbund eines gemeinsamen Wafers befinden, einen an sich bekannten Prozess dar. Beispielsweise wird häufig mit Hilfe einer Diamantsäge eine Wafervereinzelung vorgenommen.

[0015] Neben dem Wafersägen stellt das sogenannte „Stealth Dicing“ eine alternative Technologie zur Wafervereinzelung dar. Dabei erfolgt eine Amorphisierung des Wafermaterials mittels eines Laserstrahls, wodurch mechanische Spannungen in dem Wafer induziert werden. Die so erzeugten Sollbruchstellen bewirken bei Expansion des Wafers auf einer Folie die Vereinzelung der Chips entlang der durch den Laserstrahl definierten Linien. Beim Stealth Dicing wird effektiv kein Material abgetragen, sodass die Notwendigkeit von flüssigen Medien während des Vereinzelungsprozesses zum Abtransport von überschüssigem Material entfällt.

[0016] Ein weiterer Spaltvorgang, der zum Vereinzeln der Chips genutzt wird, ist aus der DE 197 30 028 C2 bekannt. Hier wird ein Initialschnitt als Auskerbung durch einen Laser so erzeugt, dass es zu einem selbsttätigen Spaltvorgang und damit zum Trennen der Halbleiterchips in der Trennlinienrichtung führt.

[0017] Es ist außerdem bekannt, gemäß dem Ablationslaserschneiden einen Oberflächenbereich des Wafers mit Hilfe eines Laserstrahls zu verdampfen und so durch entsprechenden Materialabtrag das Trennen der einzelnen Chips zu bewerkstelligen. Die Ablationsmethode ist in etlichen Verfahrensprinzipien wieder zu finden, beispielsweise dem Wasserstrahl-Laserschneiden, wobei die Grundidee des Materialabtrags durch Verdampfung bestehen bleibt.

[0018] Weiterhin ist unter der Bezeichnung TLS (thermal laser separation) ein Trennverfahren bekannt, bei dem mit Hilfe einer punktförmigen Lasererhitzung Druckspannungen erzeugt werden, die bei Abkühlung mit Hilfe eines Aerosols oder Gases zu Zugspannungen führen, wodurch es anschließend zu einem Aufspalten entlang einer entsprechenden Bruchlinie kommt.

[0019] Jedes der angewendeten Vereinzelungsverfahren führt zu ganz typischen und für jeden Chip einzigartigen strukturellen Veränderungen. So bilden sich in Folge des Sägens Ausmuschelungen („Chipping“), während das Laserschneiden und das Stealth Dicing zu charakteristischen Profilen an den Grenzflächen der vereinzelten Chips führen.

[0020] Die Erfinder der vorliegenden Erfindung haben erkannt, dass derartige Kantenfehler und Oberflächenschäden an den Flankenoberflächen für jedes Bauelement einzigartig sind und zur Authentifizierung des jeweiligen Bauelements genutzt werden können, sofern sie aufgezeichnet und in Form eines Referenzdatensatzes abgespeichert werden.

[0021] Die erwähnten Vereinzelungsverfahren basieren auf mechanischen, thermischen und chemischen Wirkprinzipien und verursachen entsprechend ihrer Wirkprinzipien ganz typische Schadensbilder. Bei den mechanischen Verfahren sind hauptsächlich Ausbrüche an den Chipkanten typisch, während bei thermischen und chemischen Verfahren anstelle der mechanischen Oberflächenschäden Defekte an den Flankenoberflächen erkennbar sind, die sich aus geschmolzenem und wiedererstarrtem Silizium oder Materialrückständen von Ätzprozessen ergeben. Weiterhin treten bei den thermischen Verfahren Mikrorisse auf, die von den Schadbereichen in das Chipvolumen hineinragen. Schließlich sind auch Materialverspannungen möglich, die durch die Vereinzelung entstehen und für jeden Chip einzigartig sind.

[0022] Auch polykristalline Materialanlagerungen oder Versetzungen und andere Störungen im Kristall-

gitter können als Authentifizierungsmerkmale gemäß der vorliegenden Erfindung genutzt werden.

[0023] Entsprechend dem zu detektierenden Produktmerkmal wird ein geeignetes Verfahren zum Erfassen und Katalogisieren der Authentifizierungsmerkmale verwendet. Beispielsweise können lichtmikroskopische Verfahren, spannungsoptische Verfahren, röntgenmikroskopische Verfahren oder Röntgenbeugungsverfahren eingesetzt werden. So sind mikroskopische Verfahren, etwa Lichtmikroskopie, Röntgenmikroskopie und Ultraschallmikroskopie, dazu geeignet Risse und Abplatzungen zu detektieren. Interne Verspannungen und Versetzungen in der Kristallstruktur können dagegen mittels spannungsoptischer Verfahren, Röntgenbeugung oder Raman-Spektroskopie detektiert werden.

[0024] Für den Fall, dass die zur Authentifizierung verwendeten Produktmerkmale in einer Draufsicht erfassbar sind, also beispielsweise bei dem sogenannten Chipping oder bei inneren Verspannungen, die über spannungsoptische Verfahren aufgezeichnet werden können, kann in vorteilhafter Weise die Erfassung der einzelnen Produktmerkmale für alle Chips eines Wafers unmittelbar nach der Wafer-Vereinzelung vorgenommen werden, wenn alle Chips im Waferverbund noch auf der Sägefolie im Sägerahmen eingespannt sind. Produktmerkmale, die sich auf Veränderungen und Profile der Flanken des Chips beziehen, können beispielsweise während des Pick-and-Place Vorgangs aufgezeichnet werden, wobei als Pick and Place der Vorgang des Aufnehmens eines Chips und Platzieren auf einem Chipträgersubstrat bezeichnet wird.

[0025] Weiterhin ist es vorteilhaft, wenn die aufgezeichneten Produktmerkmale im Betrieb zerstörungsfrei für eine Authentifizierung ausgelesen werden können. Da in der Anwendung die zu authentifizierenden Chips in aller Regel gehäust sind, kann die Authentifizierung später nur dann zerstörungsfrei erfolgen, wenn beispielsweise eine Röntgen- oder Ultraschallmikroskopie verwendet werden kann und bereits die Aufzeichnung des Referenzdatensatzes in vorteilhafter Weise am gehäusten Chip durchgeführt wird.

[0026] Gemäß einer weiteren vorteilhaften Ausgestaltung wird ein digitales Überlagerungsmuster berechnet und gespeichert, welches durch die Kombination verschiedener Material- oder Strukturveränderungen und durch digitalisierte Daten mit und ohne Gehäuse sowie mit den verschiedenen Ausleseverfahren gewonnener Daten entsteht. In vorteilhafter Weise ermöglicht dies eine gewisse Unabhängigkeit von den jeweiligen Ausleseverfahren und der Situation, in welcher der Originalitätsnachweis erbracht werden soll.

[0027] Gemäß einer weiteren Ausführungsform werden gezielt nur bestimmte Bereiche der Chipkante, der Chipseitenfläche oder des Chipvolumens zur Identifizierung herangezogen, beispielsweise Bereiche mit besonders eindeutigen Material- oder Strukturveränderungen, etwa im Bereich der Chipecken. In vorteilhafter Weise kann auf diese Weise das Erstellen der Test- und Referenzdatensätze beschleunigt und die Datensatzgröße reduziert werden.

[0028] Um das Auslesen der Produktmerkmale noch weiter zu vereinfachen, können die Material- oder Strukturveränderungen durch weitere Maßnahmen ergänzt werden. Substanzen können beispielsweise in Risse, Mikrorisse oder Materialausbrüche an den Kanten gefüllt werden, um hierdurch beispielsweise den Röntgenkontrast oder den Ultraschallkontrast zu erhöhen oder die Eigenspannungen zu verstärken.

[0029] Gemäß einer weiteren vorteilhaften Ausführungsform können aber die Material- und Strukturveränderungen auch während der Vereinzelung in definierten Bereichen gezielt verstärkt eingebracht werden. Beispielsweise kann bei laserbasierten Vereinzelungsvefahren bereichsweise mit höherer Leistung vereinzelt werden oder beim Stealth Dicing zusätzliche Strukturierungslinien eingebracht werden. Auch beim Wafersägen können zusätzliche Sägelinien eingefügt werden, die ausschließlich für die Authentifizierung genutzt werden.

[0030] Gemäß einer Ausführungsvariante wird die vollständige durch das gewählte Ausleseverfahren zugängliche Information als Referenzdatensatz gespeichert. Beispielsweise können mikroskopisch gewonnene Bilder gespeichert werden und die spätere Authentifizierung durch Bildkorrelation erfolgen. Hierdurch wird der Eindeutigkeitsbereich, mit dem ein Chip wieder erkannt werden kann, maximal.

[0031] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung wird nach dem Auslesevorgang durch geeignete Methoden der digitalen Datenverarbeitung die Datenmenge komprimiert. Beispielsweise kann der durch die Vereinzelung beschädigte Teil des Chips in definierte Bereiche unterteilt und ein Grenzwert festgelegt werden, der sich auf die zur Authentifizierung verwendeten Produktmerkmale bezieht. Etwa kann eine Ausbruchtiefe des Chippings oder eine Spannungshöhe der Eigenspannungen definiert werden. Jene Bereiche, die den Grenzwert übersteigen, werden beispielsweise mit 1 und jene, die darunter liegen, beispielsweise mit 0 digitalisiert. Bei festgelegter Bereichsreihenfolge entsteht so eine auf das Produktmerkmal und einen Chip bezogene Zahlenfolge. Hierdurch wird das Datenaufkommen reduziert und die Authentifizierung beschleunigt.

[0032] Zum besseren Verständnis der vorliegenden Erfindung wird diese anhand der in den nachfol-

genden Figuren dargestellten Ausführungsbeispiele näher erläutert. Dabei können einige Merkmale oder Merkmalskombinationen aus den gezeigten und beschriebenen unterschiedlichen Ausführungsformen für sich genommen eigenständige, erfinderische oder erfindungsgemäße Lösungen darstellen.

[0033] Es zeigen:

[0034] Fig. 1 eine schematische Darstellung eines Wafers mit getrennten, aber noch nicht vereinzelten elektronischen Bauelementen;

[0035] Fig. 2 eine schematische Darstellung eines vereinzelten Bauelements mit Ausbrüchen;

[0036] Fig. 3 eine schematische Darstellung zur Erläuterung von Flankendefekten;

[0037] Fig. 4 eine schematische Darstellung eines zusätzlich eingebrachten fälschungssicheren Produktmerkmals;

[0038] Fig. 5 eine schematische Darstellung zur Erläuterung eines möglichen Digitalisierungsverfahrens.

[0039] Die vorliegende Erfindung wird nachfolgend mit Bezug auf die Figuren näher erläutert. **Fig.** 1 zeigt zunächst schematisch und nicht maßstäblich einen Wafer **100**, der eine Vielzahl von elektronischen Bauelementen **102** umfasst. Die gemeinsam in dem Waferprozess hergestellten Bauelemente **102** müssen mit Hilfe eines Vereinzelungsverfahrens von einander getrennt werden, um anschließend einer Aufbau- und Verbindungstechnik zum Kontaktieren und Gehäusen zugeführt zu werden. Dabei werden die einzelnen Bauelemente **102**, die nachfolgend auch als „Chip“ bezeichnet werden, entlang von rasterförmig aufgebrachten Trennlinien **104** vereinzelt. Die Trennlinien **104** stellen dabei entsprechend dem verwendeten Vereinzelungsverfahren entweder eine reine Bruchstelle oder aber einen Sägegraben dar.

[0040] Wie bereits erwähnt bilden alle verwendeten Vereinzelungsverfahren entlang der Trennlinien **104** aber auch durch das Vollmaterial der Chips **102** verlaufend, ganz typische und für den jeweiligen Chip **102** individuelle Schadensbilder aus. Eine Übersicht über derartige Schadensbilder ist z. B. aus den folgenden beiden Fachartikeln zu entnehmen: M. Steiert, J. Wilde: "Chip-Side-Healing as a Basis for Robust Bare-Chip Assemblies", Proc. of the 63rd IEEE Electronic Components and Technology Conference, Mai 2013, Las Vegas, pp.1054,1059, ISBN 978-1-4799-0233-0, doi: 10.1109/ECTC.2013.6575703, und M. Steiert, J. Wilde: "New Probabilistic Reliability Model Describing the Risk of Chip Fracture in the Chip-On-Board Technology", Proc. of the 4th IEEE Electronic System-Integration Technology Conference (ESTC), Sept. 2012, Amsterdam, pp.1-6, ISBN 978-1-4673-4645-0, doi: 10.1109/ESTC.2012.6542094.

[0041] Beispiele für Wafervereinzelungsverfahren mit besonders geeigneten typischen Defekten sind das Diamantritzen, Sägen, Stealth Dicing, Water Jet Laser Dicing, Deep Reactive Ion Etching (DRIE) and TLS Dicing (thermal laser separation dicing). Insbesondere sind entsprechend dem verwendeten Verfahren die Chipkanten und Flankenoberflächen durch typische Schadensbilder individuell unterscheidbar. Wie bereits erwähnt, basieren die Verfahren auf mechanischen, thermischen und chemischen Wirkprinzipien. Das Diamantritzen und Sägen sind Beispiele für mechanische Vereinzelungstechniken, während das Stealth Dicing, das Water Jet Laser Dicing und das TLS Dicing thermische Verfahren sind. Das Deep Reactive Ion Etching beruht auf einem chemischen Materialabtrag.

[0042] Wie schematisch in **Fig.** 2 dargestellt, verursachen die mechanischen Verfahren Ausbrüche an den Chipkanten. Bei thermischen und chemischen Verfahren treten anstelle mechanischer Oberflächenschäden **106** vorzugsweise an den Kanten des Chips **102** Defekte an den Flankenoberflächen (s. **Fig.** 3) auf. Die Defekte an den Flankenoberflächen **108** ergeben sich beispielsweise aus geschmolzenem und wiedererstarrtem Substratmaterial (z.B. Silizium) oder Materialrückständen von Ätzprozessen. Bei thermischen Verfahren sind außerdem Mikrorisse zu beobachten, die von den Schadbereichen in das Chipvolumen hineinragen. Alle diese Schadensbilder sind individuell unverwechselbar und unfälschbar an dem vereinzelten Chip **102** vorhanden.

[0043] Erfindungsgemäß wird für jeden der Chips **102** ein Referenzdatensatz generiert, der für eine spätere Authentifizierung in digitaler Form die Information über einen Teil des typischen Schadensbildes beinhaltet. So können beispielsweise mit Hilfe von optischen oder röntgenoptischen Mikroskopaufnahmen Bilder von bestimmten und genau definierten Bereichen aufgezeichnet werden und so abgespeichert werden, dass sie für eine spätere Authentifizierung dem jeweiligen Chip zugeordnet zur Verfügung stehen.

[0044] Mit Methoden der digitalen Datenverarbeitung, beispielsweise der Mustererkennung, können anschließend die relevanten Informationen selektiert und die Datenmenge verkleinert werden. Beispielsweise kann bei gesägten Chips die Chipkante in Bereiche **114** eingeteilt werden mit einer definierten Betrachtungsbreite der Kante von ca. 30 µm. Des Weiteren wird nun ein Grenzwert **116** für die Chippingtiefe festgelegt, beispielsweise 5 µm.

[0045] Befindet sich nun in einem der definierten Bereiche ein Chipping mit einer Tiefe, die diesen Grenzwert überschreitet, so wird dieser z.B. mit 1, andernfalls mit einer 0 digitalisiert. Werden die so gewonnenen Digitalisierungen entsprechend der Bereichspositionen an der Chipkante zu einer Zahl formiert, so entsteht eine dem Chip eindeutig zugewiesene Zahlenfolge **118**. Werden auf diese Weise beispielsweise **50** Bereiche definiert und digitalisiert, so ist die Wahrscheinlichkeit, dass zwei Chips dieselbe Zahlenfolge aufweisen mit

$$\frac{1}{2^{100}}$$

gegeben. Eine derartige Digitalisierung ist vom eigentlichen Ausleseverfahren unabhängig.

[0046] Der Referenzdatensatz kann beispielsweise in einem entsprechend vorgesehenen Speicherbereich des zu authentfizierenden Bauelements abgespeichert sein, wenn dieses Datenspeichermöglichkeiten beinhaltet. Für Bauteile, die keine direkten Speichermöglichkeiten beinhalten, muss der Referenzdatensatz eindeutig zugeordnet in externen Speichern abgelegt werden und für eine spätere Authentifizierung zugänglich sein.

[0047] Wie bereits erwähnt sind die verwendeten Material- oder Strukturveränderungen im Grunde unerwünschte Folge des Prozesses der Wafervereinzelung und entstehen zufällig entlang der Chipkanten, Chipseitenflächen und in einem Volumen hinter der Chipseitenfläche durch die mechanische, thermische und/oder chemische Belastung, die während des Vereinzelungsprozesses auf den späteren Chip und den Wafer einwirken. Diese Merkmale sind aber a priori fälschungssicher und verhalten sich zu dem einzelnen Chip wie die Iris zu einem menschlichen Auge oder der Fingerabdruck zu einer Person.

[0048] Dadurch, dass dieses eindeutige Produktmerkmal für jeden Chip digitalisiert und anschließend gespeichert wird, ist jederzeit durch eine erneute Aufnahme und Digitalisierung der Merkmale und einen Abgleich mit den bereits gespeicherten Daten, ein zuverlässige Identifizierung des Chips möglich. Wird der Chip in einer Elektronikbaugruppe eingesetzt, dann ist die Baugruppe durch den darin enthaltenen Chip eindeutig identfizierbar. Somit sind durch die Erfassung eines einzelnen Chips auch höhere Integrationsstufe eindeutig authentifizierbar.

[0049] **Fig.** 4 zeigt eine schematische Darstellung eines weiteren Ausführungsbeispiels, bei dem ein Chip **102** neben den zur Vereinzelung erforderlichen Flanken **108** zusätzlich mit einer nur wenige Mikrometer tief ins Material eingebrachten Sägegrube **110** gekennzeichnet wird. Dadurch entsteht das unfälschbare Authentifizierungsmerkmal, wobei entlang dieser Sägekante nicht getrennt wird.

[0050] Ein solcher zusätzlicher Sägekanal **110** hat den Vorteil, dass er beispielsweise mit Hilfe eines Glaswafers **112**, der anodisch aufgebondet ist, abgedeckt werden kann. Durch die transparente Abdeckung **112** hindurch bleibt das zuvor eingebrachte fälschungssichere Merkmal mikroskopisch zugänglich, ist aber gegen spätere Beschädigungen geschützt.

[0051] Alternativ kann statt des Glaswafers **112** auch ein im sichtbaren Bereich nicht transparentes Material, wie beispielsweise Silizium, verwendet werden, das im Infrarotbereich aber transparent ist.

[0052] Nach dem Aufbringen des zusätzlichen Sägekanals **110** sowie der eigentlichen Trennlinien **104** kann der durch den Chip **102** und die Abdeckung **112** gebildete Verbund vereinzelt werden, sodass die zuvor eingebrachten Authentifizierungsmerkmale sich dann beispielsweise in der Mitte des Chips **102** befinden. Durch ein derartiges Vorgehen sind die individuellen Produktmerkmale zum einen geschützt, können zum anderen aber auch nicht mehr nachträglich manipuliert oder unkenntlich gemacht werden, ohne den Chip komplett zu zerstören, da eine anodische Bondverbindung nicht mehr zerstörungsfrei aufgetrennt werden kann.

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

- DE 102009033221 A1 [0007]
- DE 3843076 A1 [0007]
- DE 19810134 A1 [0007]
- EP 1934950 A1 [0007]
- EP 1748902 A1 [0007]
- EP 1674286 A1 [0007]
- EP 1327531 A1 [0007]
- EP 919916 B1 [0007]
- US 6022429 [0007]
- US 6264296 [0007]
- US 6685312 [0007]
- US 6932527 [0007]
- US 6979141 [0007]
- US 7037013 [0007]
- DE 19730028 C2 [0016]

Zitierte Nicht-Patentliteratur

- M. Steiert, J. Wilde: "Chip-Side-Healing as a Basis for Robust Bare-Chip Assemblies", Proc. of the 63rd IEEE Electronic Components and Technology Conference, Mai 2013, Las Vegas, pp.1054,1059, ISBN 978-1-4799-0233-0, doi: 10.1109/ECTC.2013.6575703 [0040]
- M. Steiert, J. Wilde: "New Probabilistic Reliability Model Describing the Risk of Chip Fracture in the Chip-On-Board Technology", Proc. of the 4th IEEE Electronic System-Integration Technology Conference (ESTC), Sept. 2012, Amsterdam, pp.1-6, ISBN 978-1-4673-4645-0, doi: 10.1109/ESTC.2012.6542094 [0040]

Patentansprüche

1. Verfahren zum Authentifizieren mikroelektronischer Bauelemente, wobei das Verfahren folgende Schritte umfasst:
Digitalisieren mindestens eines vordefinierten intrinsischen Produktmerkmals für jedes zu authentifizierende mikroelektronische Bauelement,
Erzeugen eines Testdatensatzes basierend auf dem digitalisierten Produktmerkmal,
Vergleichen des Testdatensatzes mit einem Referenzdatensatz und Feststellen der Authentizität des mikroelektronischen Bauelements, wenn der Testdatensatz innerhalb eines vorgegebenen Rahmens mit dem Referenzdatensatz übereinstimmt, wobei der Referenzdatensatz erzeugt wird durch die folgenden Schritte:
Digitalisieren des mindestens einen vordefinierten intrinsischen Produktmerkmals für jedes zu authentifizierende mikroelektronische Bauelement,
Speichern des digitalisierten Produktmerkmals als Referenzdatensatz,
wobei das Produktmerkmal eine Material- und/oder Strukturveränderung umfasst, die beim Vereinzeln des mikroelektronischen Bauelements aus dem Waferverbund und/oder durch einen zusätzlich durchgeführten Prozessschritt der Vereinzelungstechnologie entsteht.

2. Verfahren nach Anspruch 1, wobei der Testdatensatz gespeichert wird.

3. Verfahren nach Anspruch 1 oder 2, wobei der Schritt des Digitalisierens die Überführung einer bildgebenden Erfassung des Produktmerkmals beinhaltet.

4. Verfahren nach Anspruch 3, wobei der Schritt des Digitalisierens lichtmikroskopische Verfahren, spannungsoptische Verfahren, röntgenmikroskopische Verfahren oder Röntgenbeugungsverfahren oder eine Ultraschallmikroskopie umfasst.

5. Verfahren nach einem der vorangehenden Ansprüche, wobei das Produktmerkmal Absplitterungen an einer Schneidkante, Mikrorissstrukturen oder Bruch- und Schleifprofile an einer Trennfläche oder inneren mechanischen Verspannungen umfasst.

6. Verfahren nach einem der vorangehenden Ansprüche, wobei der Referenzdatensatz während eines Herstellungsprozesses oder während eines davon getrennten Registrierungsprozesses erzeugt wird.

7. Verfahren nach einem der vorangehenden Ansprüche, wobei die Material- und/oder Strukturveränderungen durch Anbringen und/oder Einbringen weiterer Substanzen ergänzt werden.

8. Verfahren nach einem der vorangehenden Ansprüche, wobei die Material- und/oder Strukturveränderungen während der Vereinzelung in definierten Bereichen gezielt verstärkt eingebracht werden.

9. Verfahren nach Anspruch 8, wobei die mikroelektronischen Bauelemente bei laserbasierten Vereinzelungsverfahren bereichsweise mit höherer Leistung vereinzelt werden oder beim Stealth Dicing zusätzliche Strukturierungslinien eingebracht werden.

10. Verfahren nach einem der vorangehenden Ansprüche, wobei in dem Schritt des Digitalisierens ein digitales Überlagerungsmuster berechnet und gespeichert wird, welches durch die Kombination verschiedener Material- oder Strukturveränderungen und durch digitalisierte Daten mit und ohne Gehäuse sowie der mit den verschiedenen Ausleseverfahren gewonnnen Daten entsteht.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Schritt des Digitalisierens mindestens eines intrinsischen Produktmerkmals für jedes zu authentifizierende mikroelektronische Bauelement umfasst:
Vergleich eines Messwerts, der das intrinsische Produktmerkmal widerspiegelt, mit einem vorgegebenen Schwellenwert für eine Vielzahl von Messpunkten in einem definierten Bereich des mikroelektronischen Bauelements,
Zuweisen eines Kennwertes zu jedem Messwert, entsprechend dem Vergleichsergebnis,
Zusammenfassen der Kennwerte zu dem Referenzdatensatz.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

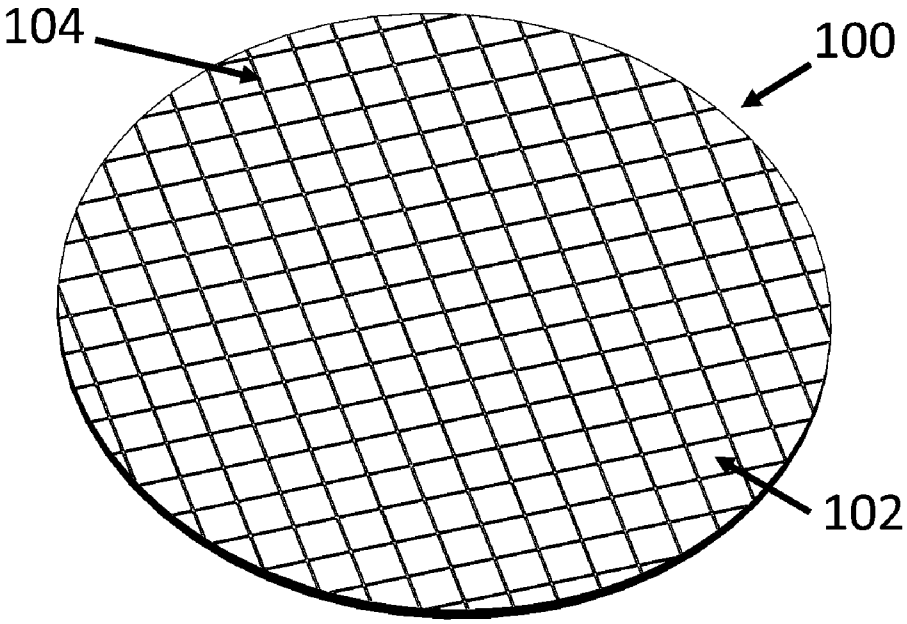


FIG. 1

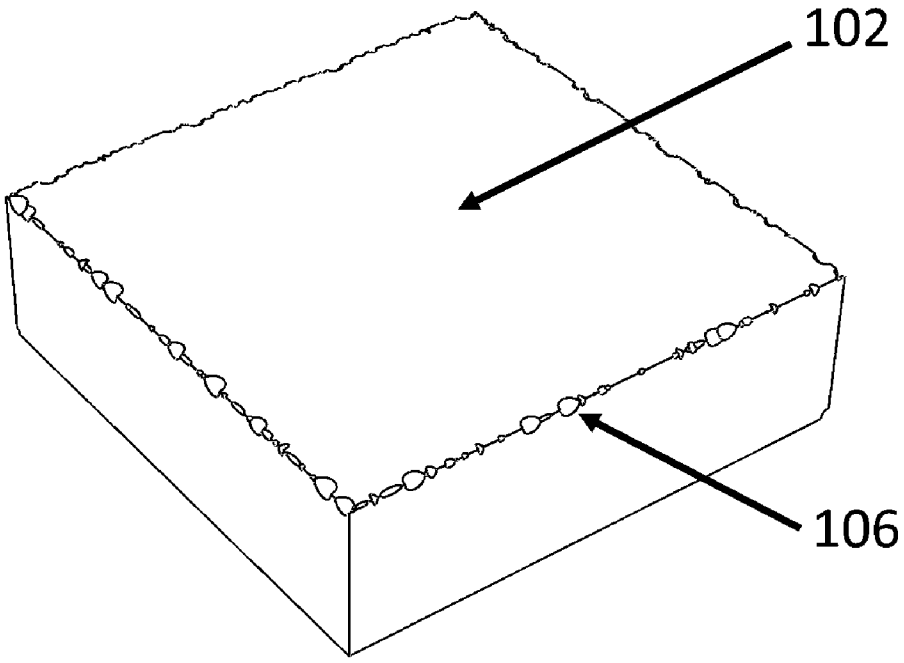


FIG. 2

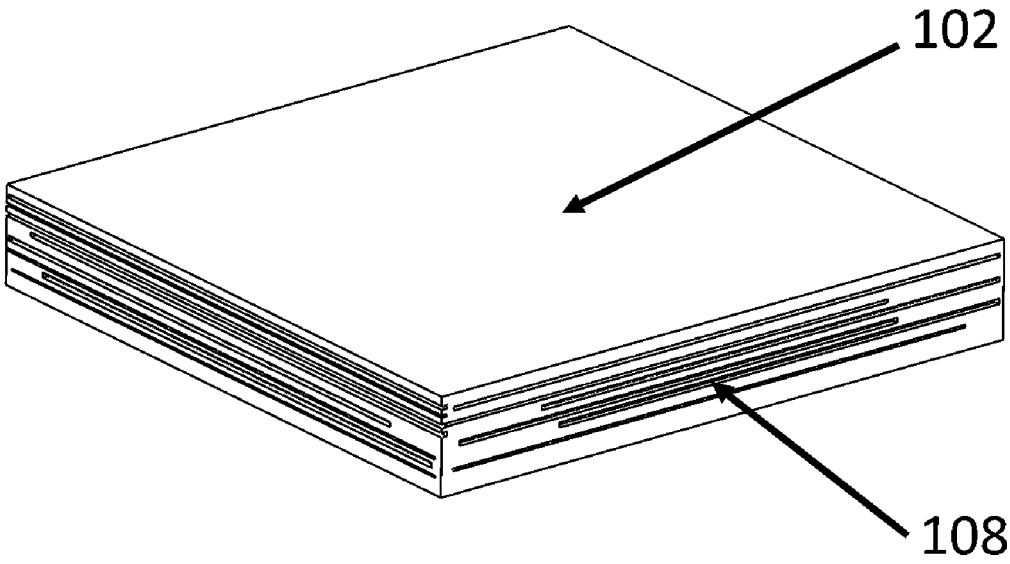


FIG. 3

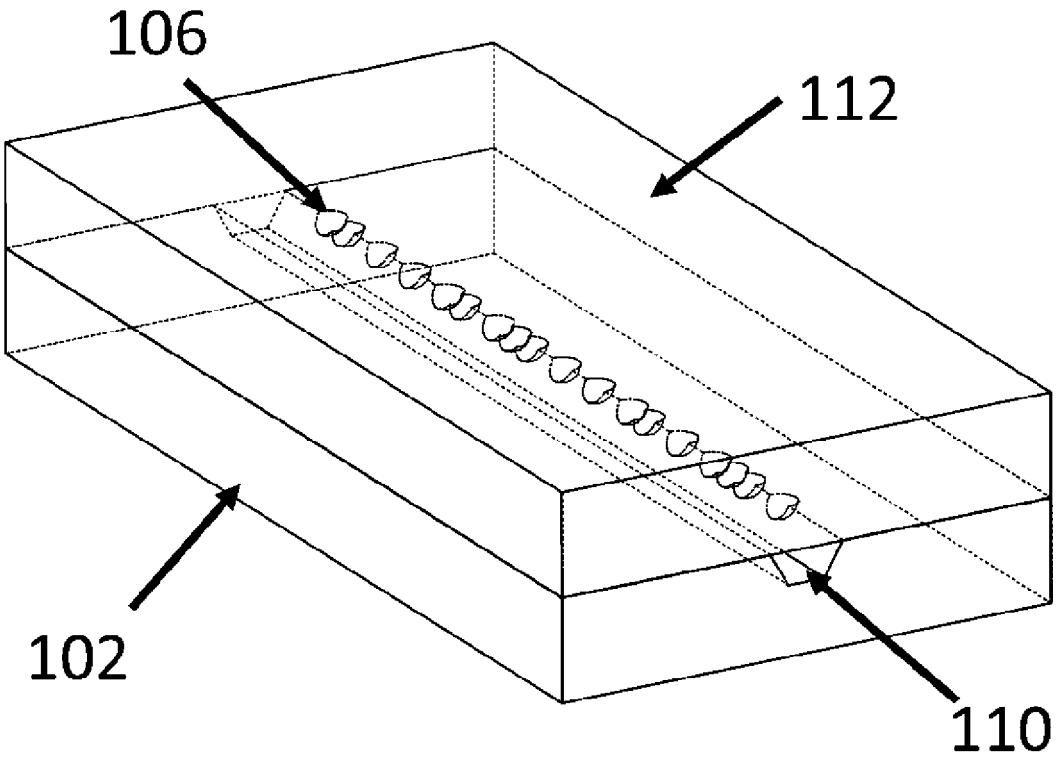


FIG. 4

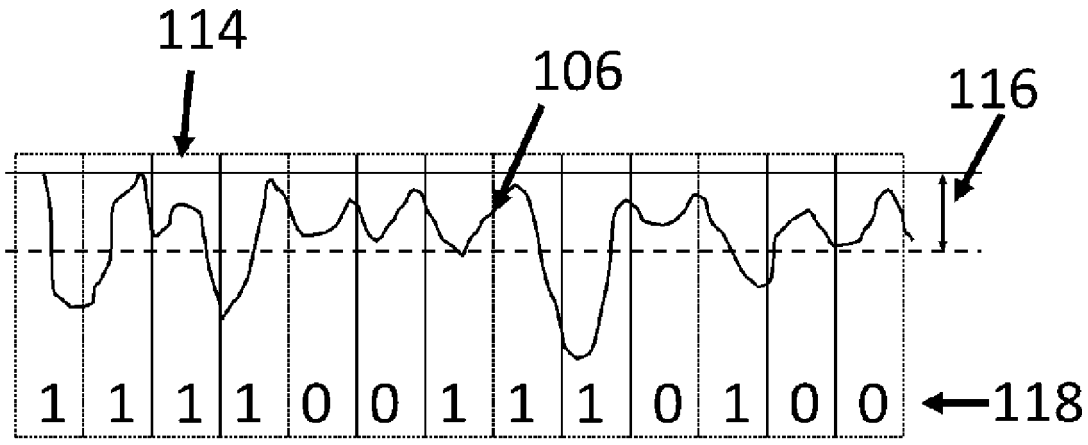


FIG. 5