(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 102 52 329 A1** 2004.05.27

(12) # Offenlegungsschrift

(21) Aktenzeichen: **102 52 329.0**
(22) Anmeldetag: **11.11.2002**
(43) Offenlegungstag: **27.05.2004**

(51) Int Cl.[7]: **G06F 12/14**
G06K 19/073

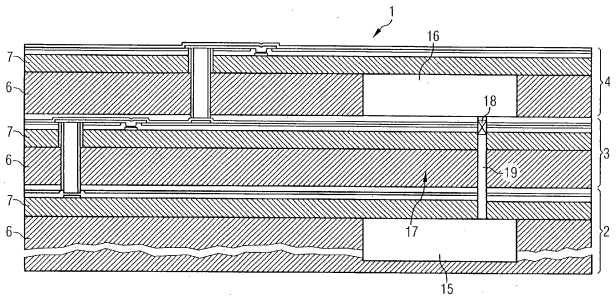
(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Effing, Wolfgang, 82205 Gilching, DE; Graßl, Thomas, Dr., 85354 Freising, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Chip mit Sicherheitssensor**

(57) Zusammenfassung: Ein gegen einen Angriff zu sichernder Datnspeicher 17 innerhalb eines Sicherheitschips 1 wird durch über und/oder unter dem Datenspeicherbereich angeordnete Hohlräume 15, 16 geschützt. Die Hohlräume werden mit einer geeigneten Sensorik 18, 19 überwacht. Die Sensorik reagiert und führt zum Löschen oder Zerstören des Datenspeicherbereichs, wenn der Hohlraum bei einem direkten Angriff auf den Datenspeicher physikalisch verletzt wird. Vorzugsweise herrscht in dem Hohlraum ein anderer Druck und/oder ist in dem Hohlraum ein anderer Stoff enthalten als in der Atmosphäre, so dass bei einem Angriff ein Druck und/oder Stoffausgleich mit der Atmosphäre stattfindet, der detektiert wird und zur Löschung der Zerstörung des Speicherbereichs führt.



Beschreibung

[0001] Die Erfindung betrifft einen Sicherheitschip mit einem gegen Ausspähen gesicherten Datenspeicher, insbesondere Schlüsselspeicher, umfassend eine Sicherheitseinrichtung zur Detektierung eines Zugriffsversuchs auf den Datenspeicher und, im Falle einer solchen Detektierung, zur Löschung des Datenspeichers.

[0002] Sicherheitschips im Sinne der vorliegenden Erfindung sind elektronische Chips mit sicherheitsrelevanten Strukturen, insbesondere solche mit einem Datenspeicher, auf dem sicherheitsrelevante Daten abgelegt sind, wie zum Beispiel ein individueller kryptographischer Schlüssel, eine PIN oder sonstige geheime Daten. Bevorzugte Chips finden beispielsweise in Chipkarten aller Art Verwendung. Die sicherheitsrelevanten Datenspeicher sind ein bevorzugtes Ausspähziel und müssen daher innerhalb des Chips besonders gegen Angriffe von außen geschützt werden. Es besteht beispielsweise die Gefahr, dass der Datenspeicher über in den Chip gebohrte Bohrungen kontaktiert und die Daten aus dem Speicher ausgelesen werden.

[0003] Zur Sicherung des Chips gegen Ausspähen sicherheitsrelevanter Daten sind bereits zahlreiche Maßnahmen vorgeschlagen worden.

[0004] Aufgabe der vorliegenden Erfindung ist es, eine Alternative zum Schutz eines Datenspeichers innerhalb eines Chips vorzuschlagen, um einen physikalischen Angriff auf den Chip detektieren und den Datenspeicher rechtzeitig löschen zu können.

[0005] Diese Aufgabe wird durch einen Sicherheitschip mit den Merkmalen des unabhängigen Anspruchs gelöst. In davon abhängigen Ansprüchen sind vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung angegeben.

[0006] Demnach sind in dem Chip ein oder mehrere Hohlräume vorgesehen. Das Hohlrauminnere wird auf eine charakteristische, auf einen äußeren Angriff zurückzuführende Zustandsänderung überwacht. Wird eine solche Veränderung detektiert, so wird unverzüglich die Löschung des gegen Ausspähen zu sichernden Datenspeichers veranlasst. Vorzugsweise bewirkt die Veränderung selbst, ohne zusätzliche Maßnahmen und insbesondere ohne den Einsatz zusätzlicher Energie, die Löschung oder sogar die Zerstörung des Datenspeichers.

[0007] Vorzugsweise sind die Sicherungshohlräume rund um den zu sichernden Datenspeicher vorgesehen, liegen aber zumindest direkt über und/oder unter und/oder neben dem Datenspeicher, um einen direkten physikalischen Zugriff auf den Datenspeicher, beispielsweise durch Anbohren, zu detektieren.

[0008] Das Anordnen des Hohlraums über und/oder unter dem Datenspeicher bietet sich besonders an, wenn der Sicherheitschip ein aus mehreren, elektronisch miteinander verbundenen Chiplagen bestehender Chipstapel ist. Die sicherheitsrelevanten Strukturen liegen dann in einer zentralen Schicht im Chipstapel, und einzelne oder alle Sicherungshohlräume liegen im Substratmaterial der an die betreffende Schicht angrenzenden Chiplagen über und unter dem Datenspeicher.

[0009] Sofern der sich auf den Hohlraumzustand auswirkende äußere Angriffsversuch nicht ohne weiteres zur Löschung oder Zerstörung des Speichers führt, sondern noch eine vorherige Auswertung tatsächlicher Messwertveränderungen erfordert, ist es vorteilhaft, die dazu notwendige Auswerteelektronik ebenfalls in einer Ebene unter oder zwischen die Sicherungshohlräume zu legen. Dadurch wird verhindert, dass eine Hohlraumebene von der darunter liegenden, zu sichernden Ebene getrennt werden kann, ohne dass ein derartiger Versuch bereits zum Löschen des Datenspeichers führt.

[0010] Es können auch mehrere Auswerteeinrichtungen in verschiedenen Chiplagen zur Auswertung detektierter Zustandsveränderungen desselben Hohlraums vorgesehen sein. Die jeweiligen Auswerteergebnisse sollten unter normalen Umständen identisch sein. Eine Abweichung der denselben Hohlraum betreffenden Auswerteergebnisse weist auf einen Angriff hin. Ist die Abweichung derart gravierend, dass auf einen äußeren Angriff geschlossen werden muss, so wird der zu schützende Datenspeicher unverzüglich gelöscht.

[0011] Um zu verhindern, dass Zustandsveränderungen, die nicht auf einen äußeren Angriff zurückzuführen sind, den Löschvorgang des Datenspeichers auslösen, können ein oder mehrere Sensoren und eine Ausgleichschaltung vorgesehen sein, um eine Messwertdrift auszugleichen.

[0012] Beispielsweise kann der Hohlraum ein unter Überdruck oder Unterdruck stehendes Fluid enthalten. Der Druck wird mittels einem Drucksensor überwacht. Bei Über- oder Unterschreiten eines vorbestimmten Grenzwertes reagiert die Auswerteschaltung und veranlasst das Löschen oder Zerstören des Datenspeichers. Dies geschieht beispielsweise, falls der Hohlraum angebohrt wird und dadurch ein Druckausgleich mit der Umgebung eintritt. Die Auswerteschaltung kann nun so eingerichtet sein, dass sie bei langsamen Druckveränderungen, wie sie temperaturbedingt auftreten, nicht reagiert. Stattdessen kann aber auch ein zusätzlicher Temperatursensor im Hohlraum angeordnet und eine Ausgleichsschaltung vorgesehen sein, um temperaturbedingte Druckschwankungen auf rechnerischem Wege zu berücksichtigen.

[0013] Es gibt zahlreiche Möglichkeiten, Zustandsänderungen des Hohlraums zu detektieren. Je nachdem, welche Eigenschaft bzw. welcher Parameter des Hohlraums überwacht wird, bieten sich wiederum unterschiedliche Sensoren zur Detektierung der jeweiligen Eigenschaft an. Die Sensoren können so ausgebildet sein, dass sie unmittelbar zur Löschung oder Zerstörung des Datenspeichers führen, oder dass sie lediglich ein Signal liefern, welches zunächst elektronisch ausgewertet wird, bevor daraufhin der

Datenspeicher gelöscht oder zerstört wird.

[0014] Interessante überprüfbare Eigenschaften des Hohlrauminneren sind beispielsweise elektrische, stoffliche, akustische, optische, dimensionale und Druckeigenschaften. Das Hohlrauminnere muss selbstverständlich so eingestellt sein, dass ein Angriff auf den Hohlraum, insbesondere ein Anbohren des Hohlraums, zu einer Veränderung der überprüften Eigenschaft führt, indem beispielsweise eine Druckveränderung oder ein Stoffaustausch oder eine Öffnung des Hohlraums zu einer Veränderung einer elektrischen, stofflichen, akustischen, optischen oder sonstigen Eigenschaft des Hohlrauminneren führt.

[0015] Nachfolgend wird die Erfindung anhand von Ausführungsbeispielen, teilweise unter Bezugnahme auf die begleitenden Zeichnungen, näher erläutert. Darin zeigen.

[0016] **Fig.** 1 einen Chipstapel mit drei Chiplagen und zwei. Hohlräumen,.

[0017] **Fig.** 2 einen Chipstapel mit zwei Chiplagen und einem Membrandrucksensor, und

[0018] **Fig.** 3 einen dielektrischen Hohlraumsensor,

[0019] **Fig.** 4 einen Chipstapel mit drei Chiplagen und einem chemisch reagierenden Flüssigkeitssensor.

[0020] **Fig.** 1 zeigt drei Chiplagen **2**, **3**, **4** eines Chipstapels **1**, die in üblicher Weise mittels Durchkontaktierungen **5** untereinander elektrisch leitend verbunden sind. Jede Chiplage **2**, **3**, **4** umfasst ein Siliziumsubstrat **6** mit einer Metallisierung **7**. In der Metallisierung **7** der mittleren Chiplage **3** sind die sicherheitsrelevanten Strukturen einschließlich eines zu sichernden Schlüsselspeichers realisiert. Der Schlüsselspeicher befindet sich beispielsweise direkt unterhalb des Hohlraums **9** der oberen Chiplage **4**. Die Hohlräume **8**, **9** sind als Sensoren ausgebildet oder besitzen Sensoren, mittels welchem Veränderungen am Hohlraum bzw. sich auf das Hohlrauminnere auswirkende Veränderungen detektierbar sind. Sofern ein Angriff auf den Schlüsselspeicher von einer Oberfläche des Chipstapels **1** geführt wird, beispielsweise durch Anbohren des Chipstapels, wird ein derartiger Angriff erkannt, sobald der dazwischen liegende Hohlraum angebohrt wird.

[0021] Der Hohlraum **9** in der oberen Chiplage **4** kann beispielsweise einen Drucksensor enthalten, der den Druck eines innerhalb des Hohlraums **9** befindlichen Gases misst. Dabei kann es sich um einen Überdruck oder einen Unterdruck handeln. Wird nun der Hohlraum **9** angebohrt, so stellt sich darin ein Druckgleichgewicht mit dem Atmosphärendruck der Umgebung ein. Der Drucksensor detektiert diese Druckänderung, so dass das Löschen oder Zerstören des Schlüsselspeichers unmittelbar veranlasst werden kann, noch bevor ein Kontaktieren und Auslesen des Schlüsselspeichers erfolgt.

[0022] Beispielsweise kann der Drucksensor so ausgebildet sein, dass er diskrete Druckmesswerte an eine Auswertelektronik liefert, die bei Überschreiten des vorgegebenen Grenzwertes den Schlüsselspeicher aktiv löscht. Diese Auswerteelektronik liegt vorzugsweise nicht in der Chiplage **4**, da ansonsten die Gefahr bestünde, dass die Chiplage **4** mit dem Hohlraumsensor vom Chipstapel **1** getrennt werden und den Zugriff auf den Schlüsselspeicher in der Chiplage **3** freigeben könnte. Daher befindet sich die Auswerteschaltung zur Druckmessung vorzugsweise zusammen mit dem zu schützenden Datenspeicher in der mittleren Chiplage **3** unterhalb des Hohlraums **9** der oberen Chiplage **4**.

[0023] Ein für diese Zwecke geeigneter, in der Massenproduktion herstellbarer Membrandrucksensor für die Chipintegration ist beispielsweise vom Fraunhofer-Institut für Mikroelektronische Schaltungen und Systeme (IMS) entwickelt worden. Ein solcher Sensor könnte angrenzend an den Hohlraum **9** realisiert werden. Dabei handelt es sich um einen Vakuumspaltkondensator, dessen Kapazität sich durch druckbedingte Verlagerung der Membran verändert (Fraunhofer-Institut für Mikroelektronische Schaltungen und Systeme, Duisburg – Dresden, IMS-APS „Absolute Pressure Sensor Family", 5/97 und 06/98).

[0024] **Fig.** 2 zeigt eine alternative Ausführungsform zur Realisierung eines Drucksensors. Dargestellt sind die obersten beiden Chiplagen **3**, **4** eines Chipstapels. In diesem Fall ist der Hohlraum in zwei Hohlraumkammern **9a**, **9b** unterteilt, die durch eine Membran **10** voneinander getrennt sind. Der Hohlraum **9a** enthält eine Flüssigkeit und grenzt an die Metallisierung **7** der den Schlüsselspeicher **11** enthaltenden Chiplage **7** an. Jedoch deckt die Membran **10** den Schlüsselspeicher **11** unter normalen Bedingungen gegenüber der im Hohlraum **9a** enthaltenen Flüssigkeit ab. Zu diesem Zweck ist der Hohlraum **9b** mit einem unter Überdruck stehenden Fluid gefüllt. Wird nun der unter Überdruck stehende Hohlraum **9b** von außen geöffnet, so findet ein Druckausgleich mit der Umgebung statt, der letztendlich zur Überflutung des Schlüsselspeichers **11** mit der im Hohlraum **9a** enthaltenen Flüssigkeit führt. Je nach Art dieser Flüssigkeit, kann die Überflutung verschiedene Konsequenzen haben. Beispielsweise kann es sich um eine zerstörende, insbesondere ätzende, Flüssigkeit handeln, durch die der Schlüsselspeicher physikalisch zerstört wird. Anstelle einer Flüssigkeit kann im Hohlraum **9a** auch ein Gas mit entsprechender Wirkung enthalten sein.

[0025] Anstelle der unmittelbaren Überwachung des Hohlrauminnendrucks kann dessen Unversehrtheit auch mittelbar anhand der elektrischen Eigenschaften des Hohlrauminneren, wie beispielsweise Dielektrizitätseigenschaften oder elektrische Leitfähigkeit, überprüft werden.

[0026] So kann der Hohlraum beispielsweise mit einem Elektrolyt gefüllt sein und ein oder mehrere unterschiedliche Sensoren enthalten, die das Vorhandensein des Elektrolyts anhand der elektrischen Leitfähigkeit des Hohlrauminneren detektieren. Wird der Hohlraum im Falle eines Angriffs auf den Chip zerstört, so fließt das Elektrolyt aus und die elektrische

Leitfähigkeit geht verloren. Die Auswerteeinrichtung wird daraufhin das Löschen des Datenspeichers veranlassen.

[0027] Andererseits kann der Hohlraum als Kondensator ausgebildet sein, wobei das Hohlrauminnere das Dielektrikum bildet. Der Hohlraum ist zu diesem Zweck mit einem speziellen Gas oder einer speziellen Flüssigkeit gefüllt, oder aber evakuiert, so dass aufgrund der speziellen Dielektrizitätseigenschaften die Kapazität des Kondensators vorgegeben ist. Derartige dielektrische Gas- oder Flüssigkeitssensoren sind in der Chiptechnologie als Interdigitalkondensatoren bekannt. Beispielsweise kann der Hohlraum mit Heteropolysyloxan gefüllt sein.

[0028] In der einfachsten Ausführung ist ein solcher dielektrischer Gas- oder Flüssigkeitssensor als Plattenkondensator ausgebildet. Diese Variante ist sehr einfach zu realisieren, indem der Hohlraum **9** lediglich an die beiden Metallisierungen **7** der beiden aneinander angrenzenden Chiplagen **3**, **4** anzugrenzen braucht. Die Metallisierungen **7** sind in dem an den Hohlraum angrenzenden Bereich dementsprechend als Kondensatorplatten realisiert. Vorzugsweise sind die Metallisierungsschichten mäanderförmig strukturiert.

[0029] Anstatt die Kondensatorplatten parallel zu einer Chipebene vorzusehen, können sie auch senkrecht dazu, beispielsweise als Gräben, realisiert sein. In **Fig.** 3 ist ein besonderes Ausführungsbeispiel eines derartigen dielektrischen Sensors gezeigt, welches in einen Hohlraum des Chips integriert werden kann. Die Integration kann waagerecht parallel zu einer Chipebene oder senkrecht erfolgen. Bei diesem speziellen Ausführungsbeispiel bilden die Kondensatorplatten **12**, **13** einen mäanderförmigen Zwischenraum **14**, der beispielsweise mit dem vorgenannten Heteropolysyloxan gefüllt ist.

[0030] Es ist auch möglich, die Unversehrtheit des Hohlraums zu überwachen, indem detektiert wird, welcher Stoff sich im Hohlraum befindet. Eine solche Prüfung kann sich auf die Art des Hohlraumfüllstoffs und/oder die Menge des Hohlraumfüllstoffs, im Falle einer Flüssigkeit beispielsweise auf die Füllstandshöhe, erstrecken. Sie kann sich auch darauf beziehen, ob sich ein Fremdkörper, beispielsweise im Falle eines Bohrangriffs die Bohrerspitze, im Hohlraum befindet.

[0031] Die Art des Hohlraumfüllstoffs lässt sich mittels entsprechenden Sensoren, insbesondere Gassensoren zur Detektierung eines bestimmten Gases, realisieren. Im Falle eines Angriffs wird ein Stoffaustausch mit der Umgebung stattfinden. Dies wird vom Sensor detektiert.

[0032] Die Art des Hohlraumfüllstoffs lässt sich auch optoelektronisch prüfen, indem beispielsweise der Brechungsindex und/oder die Farbe des gasförmigen oder flüssigen Füllstoffs detektiert wird. Dazu können beispielsweise faseroptische Lichtsensoren in einem optoelektronischen Aufbau verwendet werden. Derartige Lichtsensoren erfordern eine eigene Lichtquelle.

[0033] Auch der Füllstand des Hohlraums lässt sich optoelektronisch unter Einsatz einer eigenen Lichtquelle überwachen. Mittels Lichtsensoren lassen sich auch Dimensionseigenschaften, nämlich beispielsweise die Hohlraumwandabstände durch Abstandsmessungen, überwachen. Sogar das Eindringen eines Fremdkörpers in den Hohlraum lässt sich mittels Lichtsensoren unter Einsatz einer eigenen Lichtquelle überwachen, wenn nämlich die Lichtsensoren als Lichtschranke ausgebildet sind. In den drei vorgenannten Fällen ist es auch ohne Bedeutung, welcher konkrete Stoff sich in dem Hohlraum befindet.

[0034] Vorstehend wurden bereits einige Beispiele genannt, wie spezielle Eigenschaften des Hohlrauminneren optoelektronisch unter Einsatz einer eigenen Lichtquelle detektierbar sind. Vorteilhaft ist es aber, wenn auf den Einsatz einer Lichtquelle verzichtet werden kann. Eine alternative Ausführung sieht daher vor, einfache Lichtsensoren in den Hohlraum zu integrieren. Sobald bei einem Angriff auf den Chip Licht in den Hohlraum fällt, sendet der Lichtsensor ein Signal an die Auswerteelektronik zur Löschung des Datenspeichers. Allerdings schützt diese Maßnahme nicht vor einem Angriff im Dunkeln. Die Kombination mehrerer unterschiedlicher Sensoren, seien es Lichtsensoren oder Sensoren anderer Art ist daher sinnvoll.

[0035] Auch die Akustik des Hohlrauminneren kann als Kriterium zur Überprüfung herangezogen werden. Die Akustik ändert sich unter anderem bei einer Änderung des Hohlrauminnendrucks. Als Akustiksensoren können beispielsweise im Vakuum betriebene mechanische Resonatoren eingesetzt werden, wie sie in Beschleunigungssensoren für Airbags verwendet werden. Diese Sensoren werden in Resonanz betrieben, und ihre Amplitude wird überwacht, welche durch eine Änderung des Vakuums stark beeinflusst wird. Zur Realisierung dieser Variante ist der Hohlraum zu evakuieren. Im Falle eines Angriffs, bei dem der Hohlraum geöffnet wird, findet ein Druckausgleich statt, der vom Akustiksensor unmittelbar detektiert wird und zur Löschung des Datenspeichers führt.

[0036] Aus den vorgenannten Beispielen ergibt sich, dass der Hohlraum in fast allen Fällen mit einem besonderen Fluid gefüllt ist. Die Besonderheit besteht darin, dass das Fluid im Vergleich zur Atmosphäre einen anderen Druck (Überdruck oder Unterdruck) und/ oder einen anderen Stoff (Flüssigkeit oder besonderes Gas) enthält. Ein Angriff auf den Chip unter Verletzung des Hohlraums führt zu einem Druckausgleich und/oder einem Stoffaustausch mit der Umgebung. Dieser Druckausgleich bzw. Stoffaustausch kann mittels einem oder unterschiedlichen Sensoren aufgrund unterschiedlichster physikalischer Phänomene detektiert werden. Die einzigen Ausnahmen werden durch die Varianten gebildet, bei denen Lichtsensoren zur Detektierung eines Lichteinfalls oder Fremdkörpers im Hohlraum eingesetzt

werden, oder bei denen die Hohlraumdimensionen oder der Füllstand mittels Lichtsensoren überwacht werden. In diesen Fällen kommt es auf Druckverhältnisse und/oder Stoffeigenschaften nicht an.

[0037] Die vorgenannten Ausführungsbeispiele erfordern jeweils eine Auswerteschaltung, über die der Schlüsselspeicher im Angriffsfall aktiv gelöscht wird. Dies wiederum erfordert den Einsatz zusätzlicher Energie. Diese Energie zum Löschen des Datenspeichers stammt üblicherweise von einer externen Spannungsquelle. Wird diese externe Spannungsquelle unterbrochen, so kann der Schlüsselspeicher im Falle eines Angriffs nicht gelöscht werden. Nachfolgend werden Ausführungsbeispiele erläutert, bei denen zum Löschen des Datenspeichers eine externe Spannungsquelle nicht benötigt wird. Vielmehr ist in diesen Fällen die Spannungsquelle im Sicherheitschip integriert.

[0038] Gemäß einer ersten Variante befindet sich zwischen zwei Hohlräumen eine Piezomembran. Alternativ kann ein Hohlraum durch eine Piezomembran in zwei Hohlraumkammern unterteilt sein. Die Piezomembran wird durch einen Überdruck oder einen Unterdruck in einem Hohlraum bzw. einer Hohlraumkammer vorgespannt. Aufgrund der Flexibilität der Piezomembran stellt sich derselbe Über- bzw. Unterdruck in dem anderen Hohlraum bzw. der anderen Hohlraumkammer ein. Wird einer der Hohlräume bzw. Hohlraumkammern beschädigt, so tritt ein Druckausgleich mit der Umgebungsatmosphäre ein. Dadurch entspannt sich die Membran schlagartig und gibt einen Energiestoß ab, der zum Löschen oder Zerstören des Datenspeichers unmittelbar eingesetzt wird. Eine Auswertelektronik ist bei dieser Variante hinfällig.

[0039] Gemäß einer zweiten Variante kann die Energie zum Löschen oder Zerstören des Datenspeichers elektrolytisch gewonnen werden. Dazu befinden sich in eng benachbarten Hohlräumen oder in aneinander angrenzenden Hohlraumkammern zwei Elektrolyte, die bei Kontakt miteinander reagieren und über eine entsprechende elektronische Schaltung zu einem Stromfluss führen. Dieser Stromfluss wird wiederum zum Löschen des Schlüsselspeichers eingesetzt.

[0040] Die Art und Weise, wie die beiden Elektrolyte im Falle eines Angriffs miteinander in Kontakt kommen können, ist vielfältig. Beispielsweise können die Hohlräume bzw. Hohlraumkammern durch eine mäanderförmige oder kammartige Trennwand voneinander getrennt sein, so dass diese Trennwand im Falle eines Bohrangriffs zwangsläufig getroffen und gestört wird.

[0041] Alternativ dazu kann beispielsweise wieder ein Druckausgleich dazu genutzt werden, eine Fluidverbindung zwischen den beiden Kammern herzustellen. Bezugnehmend auf **Fig.** 2 könnten beispielsweise die linken und rechten Kammerabschnitte der Hohlraumkammer **9a** mit unterschiedlichen Elektrolyten gefüllt und durch die durch den Überdruck in der Hohlraumkammer **9b** vorgespannte Membran **10** voneinander getrennt sein. Bei Druckausgleich in der Hohlraumkammer **9b** werden sich die beiden Elektrolyte mischen und zu einem Stromfluss führen, der zum Löschen des Datenspeichers **11** verwendet werden kann.

[0042] Anstatt die chipintern erzeugte Energie zum Löschen des Datenspeichers einzusetzen, kann sie auch zur physikalischen Zerstörung des Datenspeichers eingesetzt werden. Beispielsweise kann mittels der vorbeschriebenen Piezomembran ein aktiv schaltbares Ventil geschaltet werden, um ein zerstörendes Fluids auf den Schlüsselspeicherbereich zu pumpen. Dabei kann es sich beispielsweise um eine ätzende Flüssigkeit handeln, mit der ätzbare Strukturen des zu löschenden Schlüsselspeichers zerstört werden.

[0043] Alternativ kann die Energie zur Öffnung eines Ventils zwischen zwei Hohlräumen genutzt werden, die mit zwei heftig miteinander reagierenden Stoffen gefüllt sind und die, zumindest nach Öffnung des Ventils, in Kontakt mit dem Schlüsselspeicherbereich kommen. Die beiden Stoffe können chemisch unter Freisetzung von Energie miteinander reagieren, so dass der Schlüsselspeicher chemisch und/oder thermisch zerstört wird. Der Schalter zum Öffnen des Ventils kann auch ein passiver Schalter sein, beispielsweise ein druckempfindlicher Schalter. In diesem Falle würde eine Druckveränderung in einem der beiden Hohlräume zur Öffnung des die Hohlräume verbindenden Ventils führen.

[0044] Dies ist in **Fig.** 4 dargestellt. Gezeigt sind wiederum drei Chiplagen **2**, **3**, **4** eines mehrschichtigen Chips **1** mit einem Schlüsselspeicherbereich **17** in der inneren Chiplage **3**. Unmittelbar über und unter dem Schlüsselspeicherbereich **17** liegen Hohlräume **15**, **16**, die mit unterschiedlichen Flüssigkeiten gefüllt sind. Der Hohlrauminnendruck jeder dieser beiden Hohlräume **15**, **16** unterscheidet sich vom Umgebungsdruck. Die Hohlräume **15**, **16** sind durch eine Verbindungsleitung **19** miteinander verbunden. Ein Ventil **18** in der Verbindungsleitung **19** verhindert jedoch den Kontakt der in den beiden Hohlräumen **15** ,**16** enthaltenen Flüssigkeit. Bei dem Ventil **18** handelt es sich um ein passives, druckempfindliches Ventil, welches öffnet, sobald in einem der beiden angrenzenden Hohlräume **15**, **16** ein Druckausgleich mit der Atmosphäre eintritt. Nach dem Öffnen des Ventils **18** gelangen die beiden Flüssigkeiten innerhalb der Verbindungsleitung **19** in Kontakt und reagieren chemisch miteinander. Bei dieser Reaktion kann Energie freigesetzt werden. Der an die Verbindungsleitung **19** angrenzende Schlüsselspeicherbereich **17** kann dabei chemisch und/oder thermisch zerstört werden.

Patentansprüche

1. Sicherheitschip (**1**) mit einem Datenspeicher (**11**; **17**), insbesondere Schlüsselspeicher, und einer

Sicherungseinrichtung (**8**, **9**; **12-14**; **15**, **16**, **18**, **19**) zur Detektierung eines Zugriffsversuchs auf den Datenspeicher und, im Falle einer solchen Detektierung, zur Löschung des Datenspeichers, dadurch gekennzeichnet, dass die Sicherungseinrichtung mindestens einen Hohlraum (**8**, **9**; **9a**, **9b**; **15**, **16**) und ein Sensorsystem umfasst, welches aufgrund einer charakteristischen Zustandsänderung im Hohlraum die Löschung des Datenspeichers bewirkt.

2. Sicherheitschip nach Anspruch 1, dadurch gekennzeichnet, dass der mindestens eine Hohlraum direkt über und/oder unter und/oder neben dem Datenspeicher liegt.

3. Sicherheitschip nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Sicherheitschip (**1**) aus einem Chipstapel mit zwei oder mehr untereinander elektrisch verbundenen, übereinanderliegenden Chiplagen (**2**, **3**, **4**) besteht.

4. Sicherheitschip nach Anspruch 3, dadurch gekennzeichnet, dass mindestens ein Hohlraum in einer anderen Chiplage (**4**) liegt als der Datenspeicher (**11**; **17**).

5. Sicherheitschip nach Anspruch 3 oder 4, dadurch gekennzeichnet, dass das Sensorsystem in mindestens zwei Chiplagen jeweils eine elektronische Auswerteeinrichtung zum Auswerten des aktuellen Zustands oder einer Zustandsänderung im Hohlraum besitzt und desweiteren eine Vergleichseinrichtung besitzt, mit der Auswerteergebnisse der mindestens zwei Auswerteeinrichtungen verglichen werden.

6. Sicherheitschip nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass eine elektronische Auswerteeinrichtung des Sensorsystems zum Auswerten des aktuellen Zustands oder einer Zustandsänderung im Hohlraum direkt über und/ oder unter dem mindestens einen Hohlraum liegt.

7. Sicherheitschip nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Sensorsystem mindestens einen Sensor zum Erfassen einer oder mehrere Eigenschaften des Hohlrauminneren umfasst, ausgewählt aus der folgenden Gruppe von Eigenschaften:
– elektrische Eigenschaften, wie beispielsweise Die-elektrizität oder elektrische Leitfähigkeit,
– stoffliche Eigenschaften, wie zum Beispiel Art des Hohlraumfüllstoffs, Menge des Hohlraumfüllstoffs, Füllstandshöhe oder Fremdkörper im Hohlraum,
– Druckeigenschaften, wie zum Beispiel Überdruck oder Unterdruck im Vergleich zum Atmosphärendruck,
– optische Eigenschaften, wie zum Beispiel Helligkeit, Brechungsindex oder Farbe,
– akustische Eigenschaften, wie zum Beispiel Resonanzeigenschaften, und
– Dimensionseigenschaften, wie zum Beispiel Wandungsabstände.

8. Sicherheitschip nach Anspruch 7, gekennzeichnet durch mindestens einen weiteren Sensor und eine Ausgleichschaltung zum Erfassen der Umgebungsbedingungen, insbesondere der Atmosphärentemperatur, und zum Ausgleichen einer Messwertdrift des mindestens einen Sensors.

9. Sicherheitschip nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass der Hohlraum mit einem Fluid gefüllt ist.

10. Sicherheitschip nach Anspruch 9, dadurch gekennzeichnet, dass das Fluid im Vergleich zum Atmosphärendruck einem höheren oder niedrigeren Druck unterliegt.

11. Sicherheitschip nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass das Fluid sich seiner Art nach von Umgebungsluft in charakteristischer Weise unterscheidet.

12. Sicherheitschip nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass das Sensorsystem eine Einrichtung zum Löschen oder Zerstören des Datenspeichers ohne Zuführung von Fremdenergie umfasst.

13. Sicherheitschip nach Anspruch 12, dadurch gekennzeichnet, dass das Sensorsystem eine Piezomembran umfasst, welche zwei Kammern des mindestens einen Hohlraums voneinander trennt und bei schlagartiger Änderung ihres Spannungszustands einen Energiestoß abgibt, der zum Löschen oder Zerstören des Datenspeichers dient.

14. Sicherheitschip nach Anspruch 12, dadurch gekennzeichnet, dass zwei benachbarte Hohlräume (**9a**; **15**, **16**) jeweils eine Substanz enthalten, die bei einer charakteristischen Zustandsänderung in mindestens einem der beiden Hohlräume oder in einem dritten Hohlraum (**10**) miteinander in Kontakt kommen und miteinander reagieren, wodurch die Löschung oder Zerstörung des Datenspeichers bewirkt wird.

15. Sicherheitschip nach Anspruch 14, dadurch gekennzeichnet, dass die beiden Hohlräume durch einen drucksensitiven Mechanismus (**10**; **18**) voneinander getrennt sind, der bei einer Druckveränderung in mindestens einem der Hohlräume (**9b**; **15**, **16**) eine Verbindung zwischen den beiden Hohlräumen herstellt.

16. Sicherheitschip nach Anspruch 14, dadurch gekennzeichnet, dass die beiden Hohlräume durch eine mäanderförmige oder kammartige Wandung

voneinander getrennt sind.

17. Sicherheitschip nach einem der Ansprüche 14 bis 16, dadurch gekennzeichnet, dass die beiden Hohlräume (**9a**; **15**, **16**) jeweils ein Elektrolyt enthalten, welche bei Kontakt zu einem Stromfluss führen, welcher zum Löschen oder Zerstören des Datenspeichers dient.

18. Sicherheitschip nach einem der Ansprüche 14 bis 17, dadurch gekennzeichnet, dass die in den beiden Hohlräumen enthaltenen Substanzen chemisch oder exotherm miteinander reagieren und der Datenspeicher dadurch chemisch oder thermisch zerstört wird.

19. Sicherheitschip nach Anspruch 12, dadurch gekennzeichnet, dass das Sensorsystem eine Membran (**10**) umfasst, welche zwei Kammern (**9a**, **9b**) des Hohlraums voneinander und von dem Datenspeicher (**11**) trennt, wobei eine Druckveränderung zumindest in einer der Kammern (**9b**) dazu führt, dass der Datenspeicher mit einer Kammer (**9a**) in Verbindung kommt, wodurch der Datenspeicher (**11**) von der darin enthaltenen Substanz überflutet wird.

20. Chipkarte umfassend einen Sicherheitschip nach einem der Ansprüche 1 bis 19.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

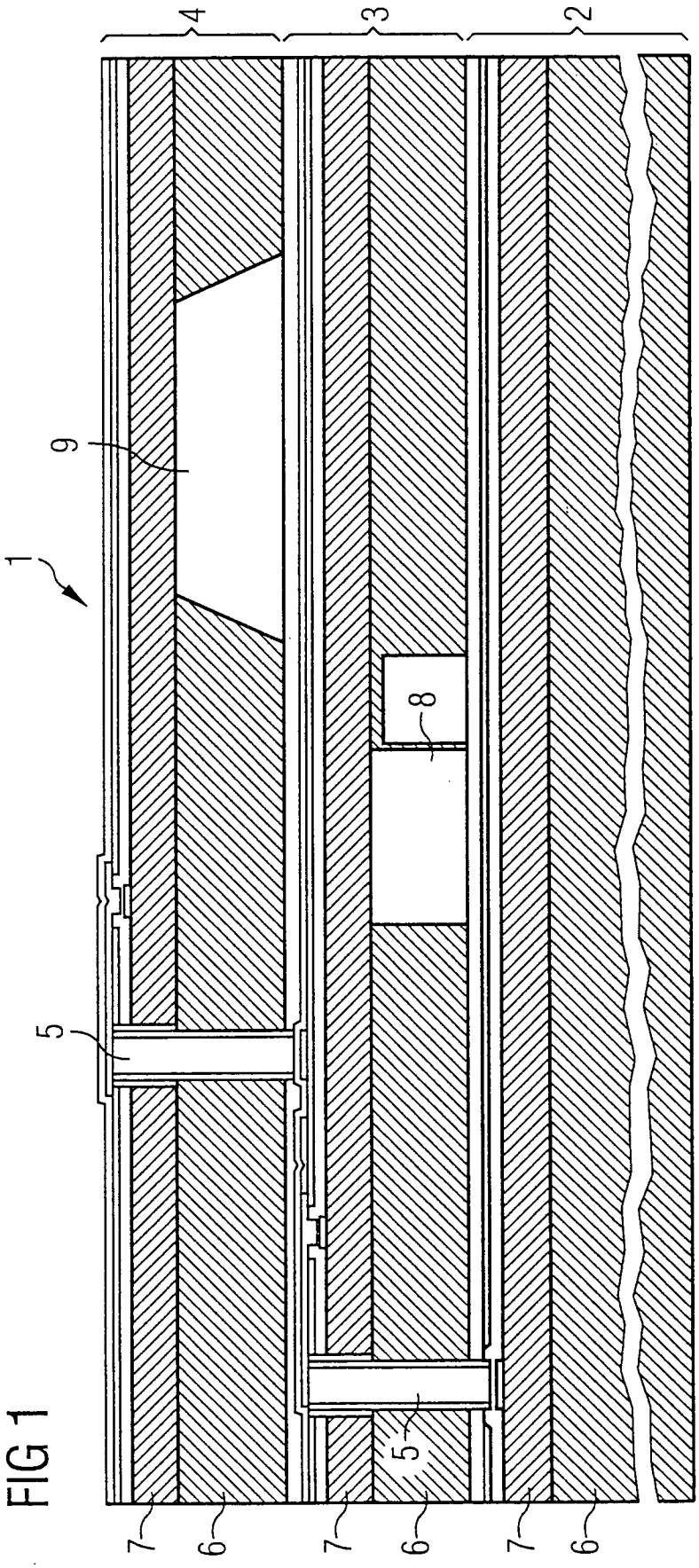


FIG 1

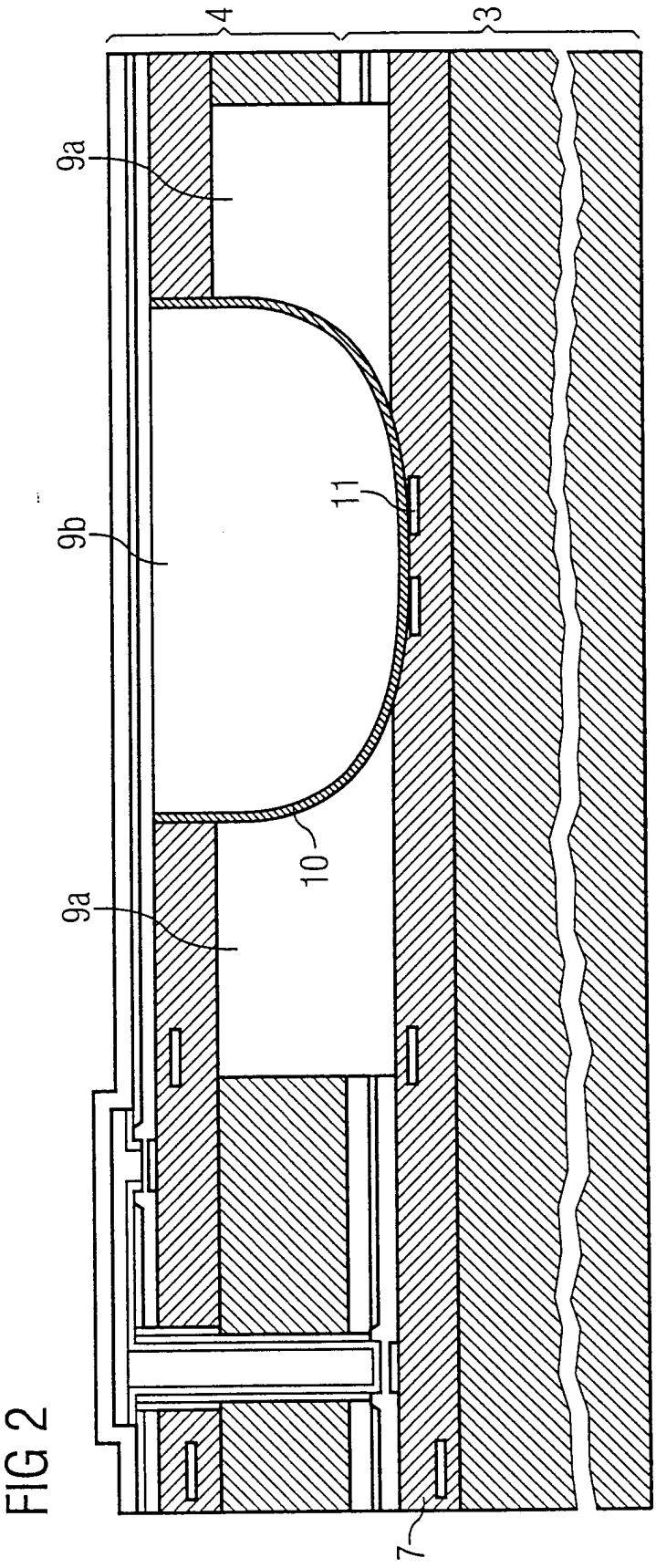


FIG 2

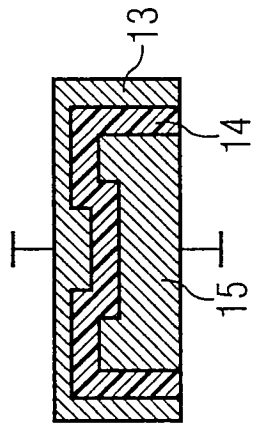


FIG 3

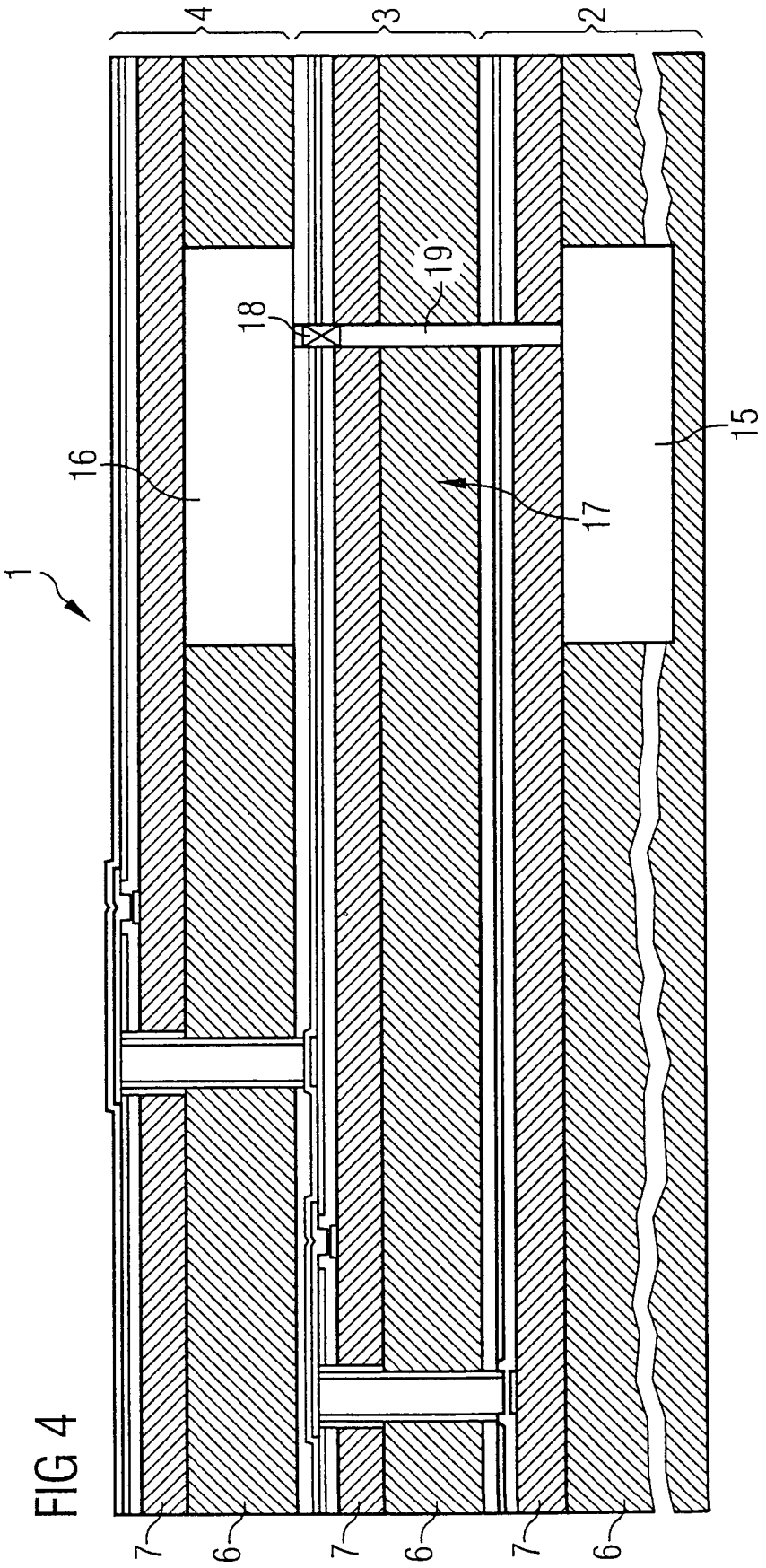


FIG 4