(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2012-509585
(P2012-509585A)
(43)公表日　平成24年4月19日(2012.4.19)

(51)Int.Cl.		F I			テーマコード（参考）
H01L 23/00	***(2006.01)***	H01L	23/00	C	5B035
G06K 19/077	***(2006.01)***	G06K	19/00	K	
G06K 19/073	***(2006.01)***	G06K	19/00	P	

審査請求 未請求　予備審査請求 未請求　（全 17 頁）

(21)出願番号　特願2011-536917 (P2011-536917)
(86)(22)出願日　平成21年11月14日 (2009.11.14)
(85)翻訳文提出日　平成23年7月19日 (2011.7.19)
(86)国際出願番号　PCT/FR2009/001307
(87)国際公開番号　WO2010/058094
(87)国際公開日　平成22年5月27日 (2010.5.27)
(31)優先権主張番号　0806563
(32)優先日　平成20年11月21日 (2008.11.21)
(33)優先権主張国　フランス(FR)

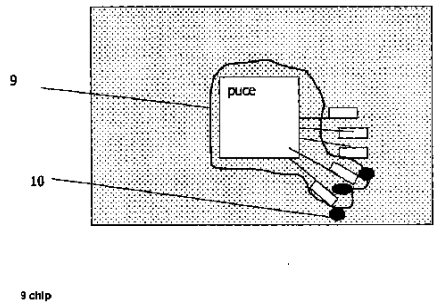
(71)出願人　511123784
イノバ　カード
フランス，エフ－１３６００　ラ　シオタ，カルチェ　ルマグワ，レ　フォロム　バー．ア，ゼッド．イ．アテリア　４
(74)代理人　100087701
弁理士　稲岡　耕作
(74)代理人　100101328
弁理士　川崎　実夫
(74)代理人　100136652
弁理士　河津　康一
(72)発明者　ロワゼル，ヤン
フランス，エフ－１３６００　ラ　シオタ，ラティセマー　ラ　リニュト　１１番地

最終頁に続く

(54)【発明の名称】物理的または化学的な侵入に対して電子集積回路ハウジングを保護する装置

(57)【要約】
【課題】従来技術において既知の保護システムの短所を克服可能な集積回路ハウジングの保護装置および方法を提案する。
【解決手段】基板上に配置された連結パッドに接続された入出力スタッドを備え、ハウジングにより保護された状態で基板に取り付けられた電子チップと、ハウジングの内部への機械的および／もしくは化学的侵入ならびに／または集積回路の機密領域へアクセスしようとする試みを検出可能な少なくとも１つの侵入検出手段と、を備えた電子集積回路であって、侵入検出手段が、検出回路を備えており、この検出回路は、集積回路の複数の機密領域のうちの１つの領域へアクセスしようとする如何なる試みによっても検出回路の電気的閉／開状態が変化するように、基板に内蔵および／または載置されるとともに、集積回路の機密領域のごく近傍を通過するように配置されていることを特徴とする電子集積回路。
【選択図】図５

FIGURE 5



【特許請求の範囲】
【請求項１】
基板（３）上に配置された連結パッド（６）に接続された入出力スタッド（２）を備え、ハウジングにより保護された状態で前記基板に取り付けられた電子チップ（１）と、
前記ハウジングの内部への機械的および／もしくは化学的侵入ならびに／または集積回路の機密領域へアクセスしようとする試みを検出可能な少なくとも１つの侵入検出手段（９、１０）と、を備えた電子集積回路であって、
前記侵入検出手段（９、１０）が、検出回路（９）を備えており、この検出回路（９）は、当該集積回路の複数の前記機密領域のうちの１つの領域へアクセスしようとする如何なる試みによっても当該検出回路（９）の電気的閉／開状態が変化するように、前記基板（３）に内蔵および／または載置されるとともに、当該集積回路の前記機密領域のごく近傍を通過するように配置されていることを特徴とする電子集積回路。
【請求項２】
前記検出回路が、脆弱領域（１０）を備えており、この脆弱領域は、前記機密領域の近傍における如何なる物理的または化学的なアクセスによっても破壊されるとともに当該回路への侵入が検出されるように前記機密領域のごく近傍に配置されていることを特徴とする、請求項１に記載の集積回路。
【請求項３】
前記脆弱領域が、前記機密領域の近傍に配置された導電性樹脂の小滴（１０）の形態で具現化されていることを特徴とする、請求項２に記載の集積回路。
【請求項４】
前記導電性樹脂の小滴（１０）が、およそ１０００μｍより小さなサイズを有し、５０μｍ前後の間隔で保護対象の前記機密領域から離間されていることを特徴とする、請求項３に記載の集積回路。
【請求項５】
前記検出回路（９）の前記脆弱領域（１０）が、当該集積回路の前記基板（３）中で不規則に分布していることを特徴とする、請求項１～４のいずれか１項に記載の集積回路。
【請求項６】
前記基板（３）が、導電性散在パターン、特に格子状のパターンを有し、前記機密領域に近接する当該散在パターンの複数の接合点が、導電性フィードスルーによって前記基板の表面まで持ち上げられるとともに脆弱領域（１０）を備えたことを特徴とする、請求項１～４のいずれか１項に記載の集積回路。
【請求項７】
前記侵入検出回路が、前記基板（３）に対する代替または追加として前記チップ（１）上に直接配置されており、前記チップの前記入出力スタッド（２）に接続されていることを特徴とする、請求項１～６のいずれか１項に記載の集積回路。
【請求項８】
前記検出回路が、導電性の液体による化学的攻撃によって前記機密領域の近傍において閉状態となり、その結果として当該化学的攻撃が検出されるように、前記機密領域の近傍において電気的に開放された回路の形態で具現化されていることを特徴とする、請求項１～７のいずれか１項に記載の集積回路。
【請求項９】
前記検出回路が、導電性の液体による化学的攻撃によって前記機密領域の近傍において開状態となり、その結果として当該化学的攻撃が検出されるように、前記機密領域の近傍において電気的に閉じられた回路の形態で具現化されていることを特徴とする、請求項１～７のいずれか１項に記載の集積回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、内部への物理的侵入を検出可能な集積回路用ハウジングの創製に関する。本

発明は特に、たとえばハウジング内への侵入を受けた場合における集積回路に含まれる秘密の破壊等の物理的攻撃を受けた場合の集積回路に含まれる可能性がある秘密の保護に適用される。

【背景技術】

【０００２】

定義：

用語に関して言えば、チップは、シリコンウェハーから切り出された実際の集積回路を表す。

基板は、外側接続部またはスタッドと「チップ」自体との接続を可能にする小型プリント回路基板（ＰＣＢ：Ｐｒｉｎｔｅｄ　Ｃｉｒｃｕｉｔ　Ｂｏａｒｄ）を表す。

【０００３】

コンポーネントは、基板、チップ、およびそれらすべてを覆うハウジングから成るアセンブリを表す。

プリント回路基板（ＰＣＢ）は、コンポーネントが載置された電子基板を表す。

チップは通常、「ダイアタッチ」として知られている作業の間に（いわゆる「フリップチップ」技術の場合を除いて）基板上に載置され、導電性のエポキシ接着剤で接着される。

【０００４】

接続、特に、基板と「チップ」との間の接続は、選択した技術に応じて多様に構成される。たとえば従来は、導電性ワイヤを用いて基板をチップに接続するワイヤ接続が行われる。この場合、導電性ワイヤは、基板側のパッドおよびチップ側のスタッドに載せられる。「フリップチップ」として知られている技術の場合は、コンポーネントの下および基板上の溶接された導電性ボールによってチップと基板とを電気的に接続している。

【０００５】

また、コンポーネントとプリント回路基板（ＰＣＢ）との間の電気的接続についても、たとえばボールグリッドアレイ（ＢＧＡ：Ｂａｌｌ　Ｇｒｉｄ　Ａｒｒａｙ）として知られているパッケージ上の導電性ボールを介する方法等、選択した技術に応じて多様に構成される。

このようなフリップチップ方式ではないＢＧＡチップを考えると、プリント回路基板（ＰＣＢ）からの任意の信号、特に機密信号は、ボール、基板、スタッドを通り、相互接続ワイヤ、およびスタッドを通って、最終的にチップの内部へ伝達される。

従来技術：

情報のセキュリティを確保するための複数種類の集積回路が存在しており、近年、電子システムまたはコンピュータシステムのセキュリティは、セキュリティ機能を実行する集積回路に基づいて確保するのが一般的である。

【０００６】

その周知例としては、チップカードが挙げられる。チップカードは、キー等の機密情報の保護機能を有する集積回路を備えている。このキーは、たとえば銀行取引、電話料金、または遠隔購買取引等の安全を確保するものである。

ただし、チップカード用の集積回路には、入出力ピンが１つしか存在しない。したがって、このピンを流れるデータの暗号化は容易であり、ハウジングそれ自体の安全確保には役立たない。

【０００７】

セキュリティを確保するための回路の別の例としては、ＴＰＭ（Ｔｒｕｓｔｅｄ　Ｐｌａｔｆｏｒｍ　Ｍｏｄｕｌｅ）が挙げられる。近年、このＴＰＭは、大手コンピュータ会社の主導により、ほぼすべての専門家用ラップトップ型コンピュータに提供されており、おそらく将来的には、世界中で販売されるすべてのパソコンに装備されることになるであろう。

【０００８】

複雑で堅牢な回路、特にＴＰＭ回路は、チップカード用の回路よりもはるかに多くの入

出力部を備えている（ＴＰＭの場合は２８ピン）。このため、コンポーネントの安全確保には、攻撃者による情報取得または所望の値への情報の変換を不可能とするため、これら多数の入出力部を流れる機密情報を保護することが必要である。したがって、チップカード用の回路には好適な暗号化ソリューションが、複雑で堅牢な回路に対してはもはや好適ではないことが分かる。これは、２０個前後またはそれ以上の信号を実時間で暗号化および復号化するのに必要な演算能力が、所要の性能およびコストの観点からは実現困難なためである。

【０００９】

したがって、多数の入出力部を備えた複雑な回路の安全を確保するための新たなソリューションが必要である。

さらに、集積回路を物理的および電気的に分析する装置の急速な進歩が指摘されている。これらの装置としては特に、走査型電子顕微鏡、集束イオンビーム（ＦＩＢ：Ｆｏｃａｌｉｚｅｄ　Ｉｏｎ　Ｂｅａｍ）装置、または接合部の光子放出を分析する装置（「Ｅｍｉｓｃｏｐｅ」としても知られている）等が挙げられる。

【００１０】

これらの機器類は、基本的には集積回路の開発を目的としたものであるが、回路のセキュリティに攻撃を仕掛ける手段としても利用可能である。

ただし、これに関しては、これらのすべての装置において、攻撃の実行前にハウジングを開放しておく必要があることに留意することが重要である。

したがって、この問題に対処する１つの方法として、物理的な侵入に対して回路のハウジングを保護することにより回路全体を保護する方式がある。ハウジングの保護は、「チップオンボード」型のパッケージの場合、または堅牢なコンポーネントがチップカードのマイクロモジュールである場合、たとえば樹脂被膜を集積回路の上面に堆積させる等、場合によっては比較的容易である。

【００１１】

この方式は、仏国特許出願公開第２，８８８，９７５号明細書で採用されており、チップ全体を覆うようにチップ各面に配置された保護層でチップの全表面を覆うものである。当然のことながら、このような構造は、保護すべき表面積を考えると高価である。また、保護手段の迂回（バイパス）に必要なのは、位置が明確で一目瞭然の保護層を除去することだけであるため、あまり効果が得られない。

【００１２】

ただし、このような保護は、支持部上への回路載置時に堆積させた樹脂被膜の除去および実際の集積回路（チップ）へのアクセスが、簡単な化学的攻撃のみで可能となるため、効果がない。

集積回路を支持部上へ最終的に搭載する際に回路作製者が付加的な保護を設けた場合、別の実施態様においては、物理的な侵入に対するハウジングの保護がより複雑となる。たとえば、様々な種類のキャップまたはカバー（樹脂被膜、金属キャップ）等の被膜で回路を覆うことが知られている。後者は非常に簡単な場合があり、受動的な保護に過ぎないことから、最小限の機械的保護を与えるものである。

【００１３】

より精巧な外部保護手段も知られており、セキュリティ機構を用いた確認によりカバー内への如何なる侵入をも検出することを意図した電気信号が伝達する導電回路の形態もある。この場合、導電回路は一般に、アクセスを防止可能な材料（樹脂、ジェル等）の中に配置されている。高水準のセキュリティを提供するこのような被膜の代表的な一例としては、Ｗ．Ｌ．Ｇｏｒｅ＆Ａｓｓｏｃｉａｔｅｓ社の「ｔａｍｐｅｒ－ｒｅｓｐｏｎｄｅｎｔ　ｓｅｃｕｒｉｔｙ　ｅｎｃｌｏｓｕｒｅ」と呼ばれる製品がある。ただし、この外部保護の選択肢は、最終製品への集積を行う回路作製者にとっては大きな障害となる。実際のところ、以下のような問題点がある。

・上記のように保護されたコンポーネントの集積は当然のことながら、付加的な要素（たとえばキャップ等）、キャップを設けるための付加的な工具、ならびにキャップの搭載お

よび樹脂の乾燥のための付加的な時間を要するため、実現するのがより複雑である。
・製造コストは、必要な材料および製造工程を追加する必要があるため、高くなる。
・最終製品の生産収率にマイナスの影響がある。
・最終製品の機能変更により、この保護を再考する場合があるため、セキュリティの観点からリスクが高くなる。
・外部保護の認証は、研究所の認定によって行う必要がある。
【先行技術文献】
【特許文献】
【００１４】
【特許文献１】仏国特許出願公開第２，８８８，９７５号明細書
【発明の概要】
【発明が解決しようとする課題】
【００１５】
発明の目的：
本発明の一般的な目的は、従来技術において既知の保護システムの短所を克服可能な集積回路ハウジングの保護装置および方法を提案することにある。
本発明のより具体的な別の目的は、集積回路ハウジングを簡単かつ効果的に保護することによって、集積回路の機密領域へのアクセスにつながるハウジングの如何なる開放をも検出可能な装置を提案することにある。
【００１６】
本発明のさらに別の目的は、安価に生産可能な保護装置を提案することにある。
【課題を解決するための手段】
【００１７】
発明の概要：
本発明の原理は、導電性材料を含む脆弱要素を特定のパターンで配置したことにある。この脆弱要素は、侵入検出回路と連続的に導入されている。
したがって、前述の仏国特許出願公開第２，８８８，９７５号明細書とは対照的に、機密領域のごく近い周囲、すなわち、機密情報の伝達に使用される可能性が高い領域のみを保護することを目的とする。この目的のため、非常に小さな径の小滴または脆弱領域を機密領域の周囲に形成する。これらの小滴は、基板に配置または内蔵された電気回路によって互いに接続されている。また、小滴は非常に小さく、攻撃者が予測できないように配置されているため、機密領域の近傍における如何なる機械的または化学的な侵入によっても、１もしくは複数の小滴または後者を接続する回路が必然的に破壊されることになる。
【００１８】
検出回路は、その電気的な連続性の確認を可能とする信号を伝達する。使用する信号は、静的または動的（すなわち、常時変化する形状）等、複数の形状（形態）であってもよい。検出回路の電気的な連続性は、たとえばその入力と出力とを比較することによって確認する。このような確認を行った場合および侵入行為の検出があり得る場合の対処は、セキュリティ方針に基づいて決定する。たとえば、考えられる１つの対処としては、集積回路に格納されたキーの消去が挙げられる。
【００１９】
この原理を実現するため、本発明は、基板上に配置された連結パッドに接続された入出力スタッドを備え、ハウジングにより保護された状態で基板に取り付けられた電子チップと、ハウジングの内部への機械的および／もしくは化学的侵入ならびに／または集積回路の機密領域へアクセスしようとする試みを検出可能な少なくとも１つの侵入検出手段と、を備えた電子集積回路であって、上記侵入検出手段が、集積回路の複数の機密領域のうちの１つの領域へアクセスしようとする如何なる試みによっても、検出回路の電気的状態（閉／開）が変化するように、基板に内蔵および／または載置されるとともに、集積回路の機密領域のごく近傍を通過するように配置された検出回路を備えたことを特徴とする電子集積回路に関する。

【００２０】
この目的のため、上記検出回路は、上記機密領域のごく近傍に配置された脆弱領域を備えている。これにより、機密領域の近傍における如何なる物理的または化学的なアクセスによっても、隣接する脆弱領域が破壊されるとともに、回路への侵入が検出されるようになる。
上記脆弱領域は、上記機密領域の近傍に配置された導電性樹脂の小滴の形態で具現化されていると都合が良い。
【００２１】
また、上記導電性樹脂の小滴は、およそ１０００μｍより小さなサイズを有し、５０μｍ前後の間隔で保護対象の上記機密領域から離間されていると好ましい。
本発明の一実施形態によれば、上記検出回路の脆弱領域は、集積回路の基板中または基板上で不規則に分布している。
別の実施形態として、上記検出回路の脆弱領域は、導電性散在パターンとして特に格子状の形態で、基板上に分布している。そして、上記機密領域に近接する当該散在パターンの複数の接合点は、導電性フィードスルーによって基板表面まで持ち上げられるとともに脆弱領域を備えている。
【００２２】
本発明の一実施形態によれば、上記侵入検出回路は、基板に対する代替または追加としてチップ上に直接配置されており、当該チップの入出力スタッドに接続されている。
上記検出回路は、導電性の液体による化学的攻撃によって上記機密領域の近傍において閉状態となり、その結果として当該化学的攻撃が検出されるように、機密領域の近傍において電気的に開放された回路の形態で具現化されていると都合が良い。
【００２３】
変形例として、上記検出回路は、導電性の液体による化学的攻撃によって上記機密領域の近傍において開状態となり、その結果として当該化学的攻撃が検出されるように、機密領域の近傍において電気的に閉じた回路の形態で具現化されている。
本発明は、以下の詳細な説明および図面を参照すれば理解がより深まるであろう。
【図面の簡単な説明】
【００２４】
【図１】支持部に接続された基板上に搭載された集積回路ハウジングの従来構造の正面の断面を示す概略図である。
【図２】基板上にチップを搭載し、チップと基板とを相互接続配線および連結パッドによってワイヤ接続した状態の正面の断面を示す詳細図である。
【図３】図２に示す装置の平面図である。
【図４】本発明に係る侵入検出回路を含むこと以外は図２と類似する装置の正面の断面を示す図である。
【図５】図４に示す装置の平面図である。
【発明を実施するための形態】
【００２５】
まず、図１を参照する。図１は、シリコンウェハーから切り出すことによって得られる単一チップであって、当該チップと周囲環境とを電気的に接続するための電気的なスタッドまたは端子２を備えた単一チップ１を示している。このチップは、基板３（任意の種類の絶縁材料）に取り付けられている。基板３は、ボールをマトリクス配置したＢＧＡ５によってプリント回路基板４に溶接されている。プリント回路基板４は、適当な直径のランドを備えている（図示せず）。ボールとボールとの間隔は通常、ミリメートルのオーダーである。チップ１のスタッド２とプリント回路基板４の導電パターン（トラック）との間の電気的な連結は、はんだボール５によって形成している。
【００２６】
図２および図３にさらに詳しく示すように、チップ１のスタッド２は、一般的に金またはアルミニウム製の導電性ワイヤ７を介して基板３のパッド６に接続されている。また、

各パッド６は、基板３に集積された回路８を介してボール５に接続されている。したがって、連結パッド６に伝わった信号は、基板中に存在する回路８によってＢＧＡの対応するボール５へと伝達される。

【００２７】

次に、図４を参照する。図４は、脆弱領域を備えた本発明に係る侵入検出回路９を含むこと以外は図２と類似する装置の正面の断面を示す図である。検出回路９は、基板３に内蔵もしくは載置されるか、または一部が基板に内蔵され一部が基板上に載置されている。この検出回路９、特に脆弱要素と対応する部分には、コンポーネント上の機密要素の完全性確保および保護の役割がある。また、これらの機密要素は、特に、機密データを含む記憶装置、または機密信号を伝達するその他のチップもしくは回路である。

【００２８】

検出回路９は、特に検出用小滴１０の形態で具現化された脆弱要素に向かって上に延びている。当業者であれば、当然のことながら脆弱要素のその他の実施形態も想到される。小滴は、機密と見なされる連結パッド６に近接して基板３の表面に堆積されているため、機密領域への如何なる物理的または化学的な攻撃によっても、最も近い脆弱要素が破壊されることになる。これにより、検出回路に接続された警報器が起動することになる。

【００２９】

図５に示すように、検出回路９は、検出用小滴を互いに接続しているため、回路または１つの検出用小滴への如何なる攻撃によっても回路９が切断される。これにより、警報、たとえばチップ１の記憶装置に格納された秘密の破壊に使用可能なものが発生する。

検出回路９は、基板３の内層に埋め込まれているのが好ましく、この場合は、アクセス不可能と見なされる。そして、この回路は、導電性フィードスルー（図示せず）を介して基板３の表面まで「上に延び」ている。このように、１つの小滴によって２つのフィードスルーと小滴群とが接続されていることにより、検出回路は閉じた状態となる。機密領域への侵入の検出効果を十分に確保するため、小滴１０および連結パッド６、ならびにそれぞれの相互接続配線は、製造コストへの要求を考慮して、可能な限りサイズを抑える必要があることは言うまでもない。

【００３０】

したがって、現在の回路形成技術で容易に実現可能な寸法は、小滴１０については直径５００μｍ前後、連結パッド６については２００μｍ前後、検出回路９の相互接続配線については３５μｍ前後である。また、小滴の堆積精度は２５μｍ前後であり、小滴１０と保護対象の最も近い連結パッド６との間の距離は５０μｍ前後である。

なお、チップ１を基板３上に接着するのに使用する製品は一般に、注射器によって小滴状またはパターン状に基板表面に堆積される。このような製品としては、たとえば「ａｂｌｅｓｔｉｋ　ａｂｌｅｂｏｎｄ　（登録商標）　ｅｐｏｘｙ　８２９０」という商標名で知られている導電性樹脂が挙げられる。小滴を堆積させるこの方法および工具は、導電性樹脂の小滴１０を基板３上に堆積させる場合にも使用可能である。

【００３１】

前述の通り、基板上に配置されたチップを有するコンポーネントの最機密領域は、脆弱要素、たとえば導電性材料の小滴１０の形態で具現化されたものを近接させることによって保護される。以下では、特にコンポーネントへの機械的および／または化学的な攻撃に際して、所望の脆弱性を得るいくつかの方法を述べる。

この考え方では、チップまたはハウジングの基板上にある信号へのアクセスを試みる攻撃者が、まず第一に不活性層（通常は成形用樹脂）を化学的および／または機械的に除去する必要があるという保護原理が期待される。この不活性層を除去する動作によって、少なくとも１つの脆弱要素が破壊され、攻撃の検出動作が起動することになる。

【００３２】

機械的脆弱性の導入に関しては、微細小滴１０を堆積させる場合と同様に、微小サイズの脆弱領域を堆積させる場合に特有の方式である。これは、小滴のサイズを小さくすると、機密要素へアクセスするための如何なる機械加工アプローチ（たとえばフライス加工、

ドリル加工等）に対しても感度が高くなるためであり、この機密要素への如何なる攻撃によっても、小滴の引裂が発生する可能性は極めて高くなる。

【００３３】

化学的脆弱性の導入に関しては、たとえば代表的には小滴１０である脆弱要素の化学組成とハウジングの化学組成とが類似するものとすることが可能である。化学的攻撃はチップと基板とを内蔵および保護する、コンポーネントのハウジング（図示せず）を破壊することであるため、このような攻撃に対して敏感になることになる。

このように、ハウジングに対する化学的攻撃は、ハウジングの溶解と同時またはそれ以前に脆弱要素を破壊または劣化させることになる。この結果、検出回路が反応して攻撃が検出される。

【００３４】

別の解決手段として、ハウジングの化学組成と脆弱要素の化学組成とが類似しない場合は、導電性の脆弱要素と絶縁性の脆弱要素とを混合する。この種の実施態様の一例としては、導電性エポキシ樹脂および絶縁性エポキシ樹脂を使用する。これにより、絶縁性エポキシ樹脂を除去しようとすると、導電性エポキシ樹脂も除去されることになる。樹脂を堆積させるための工具（ニードル）が集積回路の封入ラインで既存かつ利用可能であるため、エポキシ樹脂の使用は、非常に興味深い解決手段である。

【００３５】

化学的攻撃を困難にする最後の手段としては、攻撃者が脆弱要素および／またはハウジングを攻撃する際の製品の選択肢を狭めることが挙げられる。これは、ハウジングの化学組成として多量のシリカを含む場合、有機溶媒の効果がなくなるためである。したがって、これらの条件下では、樹脂を破壊して集積回路を攻撃するのに通常使用される発煙硝酸等の製品のみが使用可能である。硝酸、導電性を確保するのに十分な濃度を有するその他任意の酸、または任意の導電性溶液を考慮して、閉じていない状態の回路を用いた検出機構をハウジング内に設ければ十分である。これにより、攻撃用溶液の流動性および導電性のため、この導電性溶液が拡散すると、検出回路が閉じた状態となって攻撃が報知されるという効果を奏することになる。

【００３６】

脆弱要素は、当該要素のために確保された接続点の位置を除いて、電気的に絶縁された表面上に堆積される。

また、脆弱要素の位置および／または散在は、個別に規定されるべきセキュリティの水準および最適な技術的選択に応じて、大きく異なっていてもよい。

たとえば、各脆弱要素１０は、近接して機密領域を保護するため、当該領域の近くに配置されていてもよい。ワイヤ相互接続を利用する場合は、チップに接続するワイヤの基板への連結点である連結パッドを保護する必要がある。したがって、脆弱要素は、これら連結パッドに可能な限り近づけて堆積される。脆弱要素は、連結パッドに接触させるのが理想的である。こうすれば、攻撃を試みる者は、検出されることなく連結パッドにアクセスして攻撃を仕掛けることが非常に難しくなる。

【００３７】

以上のことから、脆弱要素の散在は、通常「メッシュ」と呼ばれるパターン状であってもよい。これは、程度の差はあるものの、綿密に編み込んだネットワークの一種であって、基板の全体または一部にわたって散在している。これにより、基板中を伝達する信号の保護が可能となる。また、回路がこのように形成されることにより、回路中を伝わる信号の変形により、如何なる侵入も検出可能となる。

【００３８】

脆弱要素の別の散在パターンとしては、基板上に脆弱要素の微小ドットを散在させたパターンが挙げられる。たとえば、脆弱要素は、基板全体に不規則に分布させてもよいし、または、特に機密性が高く保護すべき部分のみに分布させてもよい。このパターンの場合、検出回路の大部分は基板中に埋め込まれ、わずかな点のみが外部に現れることになる。そして、これらの点には、導電性小滴等の脆弱要素が堆積される。検出回路がこのように

形成されることにより、当該回路中を伝わる信号の変形により、如何なる侵入も検出可能となる。

【００３９】

第３の実施例としては、基板ではなくチップを直接保護する形態が挙げられる。チップは通常、絶縁性のパッシベーション層で覆われている。これにより、導電性の脆弱要素をチップ表面上に堆積させることができる。そして、検出回路との接続は、チップのスタッド２で行う。非常に簡単な実施態様としては、連続する２つのスタッド間の接続がある。このような検出回路であれば、これら２つのスタッドの近傍に配置された第３の機密スタッドを保護することができる。この種の製品の利点は、脆弱要素を堆積させることによる２つのスタッドの接続が、容易に実現可能であることである。また、チップ表面上の任意の位置にパッシベーション開口を形成し、小滴を堆積させることも可能である。

【００４０】

検出回路の第４の実施例としては、初期的には開放状態にあるが攻撃液体（たとえば発煙硝酸等）の流動性および導電性によって閉じられる回路を用いて、上述の溶液と同様に、攻撃液体の導電性を利用してチップを直接保護する形態が挙げられる。これは、チップ表面上に分散して１または複数の開回路を構成するスタッドの形態で実現可能である。これらの開回路は、攻撃液体が拡がると、その流動性および導電性によって閉じた状態となる。表面上のスタッドの密度は可変であり、高密度とすることで液体による化学的攻撃を完全に防止するようにしてもよい。

【００４１】

この最後の解決手段には、２つの効果がある。第１の効果として、ハウジング内ではチップが基板よりも高いため、ハウジングへの攻撃は、チップ表面上に配置されたセンサーによって早く検出される。第２の効果として、この機構は、チップへの物理的な侵入に対する保護も可能とする。また、理想的には、現在一般的なラティス等の機構と併せて使用してもよい。

発明の効果：

本発明により得られた集積回路の保護方法および集積回路は、設定した目的を満足する。提案した解決手段では、機密領域の近傍に脆弱要素を使用しているため、集積回路で利用している技術に関わらず、集積回路に対する実質的にすべての侵入攻撃に対抗可能である。

【００４２】

また、この解決手段により、集積回路のハウジング領域の保護を補強できるため、セキュリティを容易に利用かつ保証可能である。

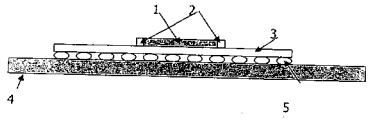
さらに、たとえば脆弱要素がエポキシ樹脂製である場合等は、樹脂堆積用の工具が既存であり十分使いこなすことができるため、別の機能に使用する場合、すなわち検出回路を形成し、侵入に対して閉じた状態となるように導電性小滴を堆積させる場合であっても、ほとんどコストが掛からずに高い生産収率が得られるものと考えられる。

発明の用途：

本発明の複数の利点を考慮すると、上述の解決手段は、たとえばボイスオーバーＩＰ電話、ネットワーク上での機密データの送信（認証、ＶＰＮ技術）、安全な認証トークン（「セキュアＵＳＢキー」）、セキュリティ専用コンポーネント、暗号演算用コンポーネント等の応用向け機密コンポーネント等、広範な用途を対象とした集積回路に適用可能である。

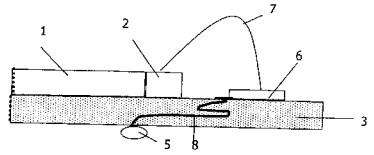
【図１】

図１



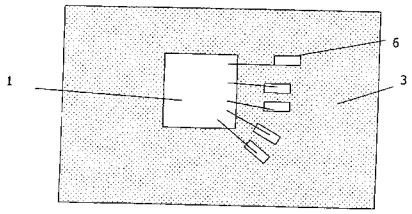
【図２】

図２



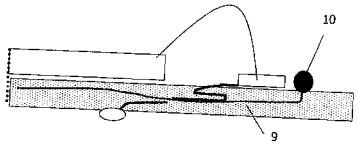
【図３】

図３



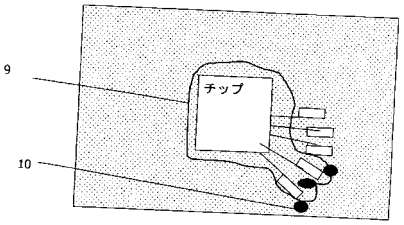
【図４】

図４



【図５】

図５



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/001307

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K19/073 H01L23/58 G08B13/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K H01L G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	FR 2 888 975 A (ATMEL CORP [US]) 26 January 2007 (2007-01-26) page 4, lines 19-31; figures 1-3 page 5, line 8 - line 19	1-3,5-6, 8-9 4
X Y A	FR 2 872 610 A (COMMISSARIAT ENERGIE ATOMIQUE [FR]) 6 January 2006 (2006-01-06) page 8, lines 5-10; figure 2 page 8, lines 30,31 page 9, lines 1,2	7 1-3,5-6, 8-9 4
Y	FR 2 864 667 A (COMMISSARIAT ENERGIE ATOMIQUE [FR]) 1 July 2005 (2005-07-01) page 15, lines 26-30; figures 1,4,5	1,5-6, 8-9

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

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

Date of the actual completion of the International search	Date of mailing of the international search report
8 March 2010	12/03/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Manet, Pascal

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/001307

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 801 999 A (GEMPLUS CARD INT [FR]) 8 June 2001 (2001-06-08) page 4, lines 10-18; figure 1 page 7, lines 11-14	1-2,9
Y	GB 2 363 233 A (IBM [US]) 12 December 2001 (2001-12-12) page 3, lines 24-27; figure 1	1-2,9
A	YVES FOUILLET: "Plate-forme microfluidique discrète et électromouillage" 18ÈME CONGRÈS FRANÇAIS DE MÉCANIQUE (CFM'07), GRENOBLE - FRANCE, [Online] 1 January 2007 (2007-01-01), pages 1-6, XP007912047 Retrieved from the Internet: URL:http://documents.irevues.inist.fr/handle/2042/6829> abstract; figure 2	4

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2009/001307

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2888975 A	26-01-2007	CN 101258552 A	03-09-2008
		US 2007018334 A1	25-01-2007
FR 2872610 A	06-01-2006	WO 2006013302 A1	09-02-2006
FR 2864667 A	01-07-2005	AT 370464 T	15-09-2007
		DE 602004008339 T2	08-05-2008
		EP 1700256 A1	13-09-2006
		WO 2005069210 A1	28-07-2005
		JP 2007535022 T	29-11-2007
		US 2007121575 A1	31-05-2007
FR 2801999 A	08-06-2001	NONE	
GB 2363233 A	12-12-2001	US 2001056542 A1	27-12-2001

Form PCT/ISA/210 (patent family annex) (April 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/001307

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06K19/073 H01L23/58 G08B13/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06K H01L G08B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y A	FR 2 888 975 A (ATMEL CORP [US]) 26 janvier 2007 (2007-01-26) page 4, ligne 19-31; figures 1-3 page 5, ligne 8 - ligne 19	1-3,5-6, 8-9 4
X Y A	FR 2 872 610 A (COMMISSARIAT ENERGIE ATOMIQUE [FR]) 6 janvier 2006 (2006-01-06) page 8, ligne 5-10; figure 2 page 8, ligne 30,31 page 9, ligne 1,2	7 1-3,5-6, 8-9 4
Y	FR 2 864 667 A (COMMISSARIAT ENERGIE ATOMIQUE [FR]) 1 juillet 2005 (2005-07-01) page 15, ligne 26-30; figures 1,4,5	1,5-6, 8-9

-/—

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 mars 2010	12/03/2010

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Manet, Pascal

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/001307

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	FR 2 801 999 A (GEMPLUS CARD INT [FR]) 8 juin 2001 (2001-06-08) page 4, ligne 10-18; figure 1 page 7, ligne 11-14	1-2,9
Y	GB 2 363 233 A (IBM [US]) 12 décembre 2001 (2001-12-12) page 3, ligne 24-27; figure 1	1-2,9
A	YVES FOUILLET: "Plate-forme microfluidique discrète et électromouillage" 18ÈME CONGRÈS FRANÇAIS DE MÉCANIQUE (CFM'07), GRENOBLE - FRANCE, [Online] 1 janvier 2007 (2007-01-01), pages 1-6, XP007912047 Extrait de l'Internet: URL:http://documents.irevues.inist.fr/handle/2042/6829> abrégé; figure 2	4

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2009/001307

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR 2888975	A	26-01-2007	CN	101258552 A	03-09-2008
			US	2007018334 A1	25-01-2007
FR 2872610	A	06-01-2006	WO	2006013302 A1	09-02-2006
FR 2864667	A	01-07-2005	AT	370464 T	15-09-2007
			DE	602004008339 T2	08-05-2008
			EP	1700256 A1	13-09-2006
			WO	2005069210 A1	28-07-2005
			JP	2007535022 T	29-11-2007
			US	2007121575 A1	31-05-2007
FR 2801999	A	08-06-2001	AUCUN		
GB 2363233	A	12-12-2001	US	2001056542 A1	27-12-2001

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ジーグ, ルノー
フランス, エフ－１３７１０ フュヴォー, シュマン デ ラ ユロット １１番地
(72)発明者 トレムレット, クリストフ
フランス, エフ－１３４００ オーバーニュ, ルー デ リオン １２番地

Ｆターム(参考) 5B035 BA03 BB09 CA08 CA38