

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2023-533547
(P2023-533547A)

(43)公表日 令和5年8月3日(2023.8.3)

(51)国際特許分類

F I

G 0 6 F 21/55 (2013.01) G 0 6 F 21/55 3 6 0

H 0 1 L 23/00 (2006.01) H 0 1 L 23/00 C

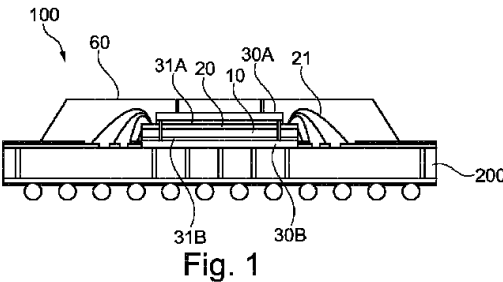
審査請求 未請求 予備審査請求 未請求 (全17頁)

(21)出願番号	特願2023-501255(P2023-501255)	(71)出願人	523005748
(86)(22)出願日	令和3年7月8日(2021.7.8)		ナグラビジョン ソシエテ ア レスポ
(85)翻訳文提出日	令和5年1月31日(2023.1.31)		ナビリテ リミテ
(86)国際出願番号	PCT/EP2021/069077		スイス 1 0 3 3 シュゾーシュールー
(87)国際公開番号	WO2022/008692		ローザンヌ ルート ドゥ ジュネーヴ 2
(87)国際公開日	令和4年1月13日(2022.1.13)		2-24
(31)優先権主張番号	20185298.5	(74)代理人	110002860
(32)優先日	令和2年7月10日(2020.7.10)		弁理士法人秀和特許事務所
(33)優先権主張国・地域又は機関	欧州特許庁(EP)	(72)発明者	ベリシエ, シルヴァン
(81)指定国・地域	AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA, RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR, GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC, 最終頁に続く		スイス 1 0 3 3 シュゾーシュールー
			ローザンヌ ルート ドゥ ジュネーヴ 2
			2-24 ナグラビジョン ソシエテ ア
			ノニム内
		(72)発明者	オーブリー, パスカル
			スイス 1 0 3 3 シュゾーシュールー
			最終頁に続く

(54)【発明の名称】 悪意のある攻撃に対する保護を有する集積回路デバイス

(57)【要約】

悪意のある攻撃に対する保護を有する集積回路デバイス。集積回路デバイス(100)は、半導体基板層(10)と、電子部品を含み、当該半導体基板層(10)によって支持される少なくとも1つの活性層(20)とを備える。半導体基板層(10)及び少なくとも1つの活性層(20)は、放射線の通過を妨げるための物理的障害物として作用する2つの保護層(30A、30B)の間に挟まれる。更に、2つの保護層(30A、30B)は、保護層(30A、30B)の電気情報を監視し、監視された電気情報に基づいて2つの保護層(30A、30B)のうちの少なくとも1つの物理的攻撃を検出することができる検出回路(40)に電気的に接続される。



【特許請求の範囲】

【請求項 1】

半導体基板層（１０）と、電子部品を含み、前記半導体基板層（１０）によって支持される少なくとも１つの活性層（２０）とを備える集積回路デバイス（１００）において、前記半導体基板層（１０）及び前記少なくとも１つの活性層（２０）が、放射線の通過を妨げる物理的障害物として作用する２つの保護層（３０Ａ、３０Ｂ）の間に挟まれ、前記保護層（３０Ａ、３０Ｂ）の電気情報を監視し、前記監視された電気情報に基づいて前記２つの保護層（３０Ａ、３０Ｂ）のうちの少なくとも１つの物理的攻撃を検出する検出回路（４０）に電氣的に接続されていることを特徴とする集積回路デバイス。

【請求項 2】

前記検出回路（４０）が、前記少なくとも１つの活性層（２０）内に集積されることを特徴とする、請求項 1 に記載のデバイス。

【請求項 3】

前記検出回路（４０）によって物理的攻撃が検出されると、電子的保護対策を実行するための信号を生成するように構成される電子保護回路（５０）を更に備える、請求項 1 又は 2 に記載のデバイス。

【請求項 4】

前記電子保護回路（５０）が、前記少なくとも１つの活性層（２０）内に集積されることを特徴とする、請求項 3 に記載のデバイス。

【請求項 5】

前記２つの保護層（３０Ａ、３０Ｂ）は、レーザ放射線、前記少なくとも１つの活性層からの電磁放射線、外部源によって生成される電磁放射線を含む群の放射線の通過を妨げるように構成されることを特徴とする、請求項 1 から 4 のいずれか一項に記載のデバイス。

【請求項 6】

前記２つの保護層が、金属、金属合金、又は半導体材料で作られていることを特徴とする、請求項 1 から 5 のいずれか一項に記載のデバイス。

【請求項 7】

前記保護層（３０Ａ、３０Ｂ）のうちの少なくとも１つがフルプレートであることを特徴とする、請求項 1 から 6 のいずれか一項に記載のデバイス。

【請求項 8】

前記保護層（３０Ａ、３０Ｂ）のうちの前記少なくとも１つが、平行線を形成する屈曲連続ワイヤで作られることを特徴とする、請求項 1 から 7 のいずれか一項に記載のデバイス。

【請求項 9】

前記２つの保護層（３０Ａ、３０Ｂ）の各々が、前記検出回路（４０）に電氣的に接続される基本プレートのモザイクを備えることを特徴とする、請求項 1 から 8 のいずれか一項に記載のデバイス。

【請求項 10】

前記検出回路（４０）が、前記２つの保護層（３０Ａ、３０Ｂ）のそれぞれの電氣的値の間の相対的な値を測定するように構成されることを特徴とする、請求項 1 から 9 のいずれか一項に記載のデバイス。

【請求項 11】

前記検出回路（４０）が、前記２つの保護層（３０Ａ、３０Ｂ）の前記電気情報として、前記２つの保護層（３０Ａ、３０Ｂ）間の静電容量を測定するように構成されることを特徴とする、請求項 1 から 10 のいずれか一項に記載のデバイス。

【請求項 12】

前記検出回路（４０）が、前記２つの保護層（３０Ａ、３０Ｂ）の前記電気情報として、前記２つの保護層（３０Ａ、３０Ｂ）間の電気抵抗の差を測定するように構成されることを特徴とする、請求項 1 から 10 のいずれか一項に記載のデバイス。

10

20

30

40

50

【請求項 1 3】

前記検出回路（40）が、許容範囲外の、基準値からの前記監視された電気情報の偏差を検出するように構成されることを特徴とする、請求項 1 から 1 2 のいずれか一項に記載のデバイス。

【請求項 1 4】

前記 2 つの保護層（30 A、30 B）が、電気絶縁体として機能する 2 つのそれぞれの接合層（31 A、31 B）を介して、前記半導体基板層（10）及び前記少なくとも 1 つの活性層（20）に接合されることを特徴とする、請求項 1 から 1 3 のいずれか一項に記載のデバイス。

【請求項 1 5】

請求項 1 から 1 4 のいずれか一項に記載の集積回路デバイスを含む製品。

【発明の詳細な説明】**【技術分野】****【0001】**

本開示は、サイドチャネル攻撃及び障害攻撃のような悪意のある攻撃に対する集積回路保護の分野に関する。

【背景技術】**【0002】**

コンピュータセキュリティにおいて、セキュリティは、典型的には、数学的に破ることが極めて困難であるように設計された暗号アルゴリズムによって提供される。攻撃者は入出力メッセージを利用できるが、秘密情報（例えば、暗号化アルゴリズムの秘密鍵）は利用できない。よく研究されたアルゴリズムの場合、攻撃者は、秘密情報を得るために実用的でない量の計算能力を必要とする暗号解析を実行しなければならない。

【0003】

しかしながら、暗号アルゴリズム又はプロトコルのハードウェア実装及びソフトウェア実装は、そのような複雑な暗号解析を必要としないサイドチャネル攻撃及び障害攻撃に対して脆弱であることが示されている。両方の技術を使用して、1 つ以上の暗号アルゴリズムを実装する集積回路などの埋め込みデバイスに記憶された秘密情報（例えば、1 つ以上の秘密鍵）を得ることができる。

【0004】

サイドチャネル攻撃は、秘密情報がサイドチャネルを介して漏洩し得るという原理に基づく。これは、実装されたアルゴリズム自体の弱点ではなく、コンピュータシステムの実装から得られる情報に基づく任意の攻撃として定義することができる。サイドチャネルとは、例えば、暗号化を実行するのに必要な時間、暗号化アルゴリズムを実行するためにハードウェア実装に消費される電力、暗号化又は復号化を実行する回路から発される電磁放射線、或いは音などの物理的な情報漏洩である。サイドチャネル攻撃は、効果的であり、低コスト及び／又は実験回数の低減を必要とすることが証明されている。

【0005】

障害攻撃は、暗号アルゴリズムにおける計算上の障害を意図的にトリガして、秘密情報を得ることを可能にする障害出力又は障害挙動を得ることにある。例えばレーザ源又は電磁源を使用する障害注入は、暗号デバイスの挙動を変更し、障害環境下での情報漏洩を発生させるために使用される。例えば、ボディバイアス注入（BBI）は、高電圧パルス回路基板に印加して障害を誘発することからなる障害注入方法である。

【0006】

国際公開第 96 / 16378（A1）号は、秘密情報を記憶するメモリ領域を有する第 1 の集積回路と、第 1 の集積回路の上に配置され、メモリ領域（及び任意の他の感知回路）を覆って障害物を形成し、メモリ領域へのアクセスを妨げる第 2 の集積回路とを含むセキュリティデバイスを開示している。2 つの集積回路は、接着層を介して互いに接合され、互いに通信するために接続される。動作中、相互認証手順を実行するために、2 つの集積回路の間で周期的通信が確立される。2 つの集積回路のうちの 1 つが認証に失敗した場

10

20

30

40

50

合、秘密情報はメモリ領域から消去される。メモリ領域にアクセスするために、攻撃者は第2の集積回路を除去する必要がある、結果として、2つの集積回路間の接続が遮断される。

【0007】

米国特許第5,881,155号は、第2の半導体チップ（保護チップ）を備える半導体チップ（被保護チップ）に記憶された秘密情報へのアクセスを妨げるためのセキュリティデバイスを開示している。2つのチップは、通信端子によって互いに結合される。不均一な抵抗率を有する半導体樹脂が、被保護チップと保護チップとの間に挟まれている。保護チップは、樹脂を介して複数の抵抗を測定する手段と、測定された抵抗を処理することによって暗号鍵（「抵抗鍵」）を決定する手段とを有する。セキュリティデバイスが初期化されると、測定手段は半導体樹脂を介して一定数の抵抗を測定する。次に、測定された抵抗値は、情報を暗号化及び復号化するために通信端子を介して保護された船舶に通信される抵抗鍵を決定するために処理される。この構成では、被保護チップに対する物理的攻撃は、秘密情報（抵抗鍵）へのアクセスを提供しない。更に、これは、チップの活性表面へのアクセス、したがって半導体層の破壊を前提とし、抵抗鍵の再構成を恒久的に妨げる。

10

【0008】

国際公開第99/12204（A1）号は、中間封止層を介して互いに接合された活性層及び相補層を備えるセキュリティ集積回路を開示している。「活性」層は、半導体材料内の基板副層と、基板副層の上に、電子回路を集積しメモリを有する活性副層とを含む。この活性層を薄膜化する。相補層は半導体材料で作られる。中間封止層は、電気絶縁材料で作られる。攻撃者が集積回路にアクセスすることを望むとすると、攻撃者は、牽引力を印加することによって相補層を活性層から分離する必要がある。活性層が薄膜化し、したがって弱まると、そのような牽引力は必然的に活性層を破り、秘密情報を抽出することを不可能にする。

20

【0009】

従来技術のセキュリティデバイスは、実装及び設計が複雑である。更に、それらは、チップの一方の側からのみの物理的攻撃に対する保護を提供する。しかしながら、チップの両側からの攻撃が可能であることが最近示された。更に、従来技術のセキュリティデバイスは、メモリから秘密情報を読み出すことを妨げるように設計されているが、サイドチャネル攻撃、電磁障害攻撃、又はボディバイアス注入攻撃に対する効率的な保護を提供しない。

30

【0010】

状況を改善する必要がある。

【発明の概要】

【0011】

本開示は、半導体基板層と、電子部品を含み、当該半導体基板層によって支持される少なくとも1つの活性層とを備える集積回路デバイスにおいて、半導体基板層及び少なくとも1つの活性層が、放射線の通過を妨げる物理的障害物として作用する2つの保護層の間に挟まれ、少なくとも1つの活性層を悪意のある攻撃に対して保護するために、保護層の電気情報を監視し、監視された電気情報に基づいて2つの保護層のうちの少なくとも1つの物理的攻撃を検出する検出回路に電氣的に接続されることを特徴とする集積回路デバイスに関する。

40

【0012】

本開示によれば、集積回路デバイスは、チップ（集積回路）の両側に保護層又はシールド層を使用する。2つの保護層は、内部放射線及び／又は外部放射線の通過を妨げる物理的障害物として作用する。そのような構成は、「ファラデーケージ」効果と比較することができる保護を作り出す。それは、チップの両側から来る放射線、例えばレーザビーム又は電磁グリッチを使用する侵入攻撃を妨げる。それはまた、1つ以上の活性層から発される電磁放射線の検出に基づくサイドチャネル攻撃を妨げる。

50

【0013】

更に、攻撃者が保護層のうちの1つの、全部又は一部を除去しようとする場合、検出回路は、保護層の監視された電気情報に基づいて攻撃を検出し、保護の電子的対策、例えばメモリワイプをトリガする。

【0014】

したがって、本開示では、保護層は、放射線を使用する攻撃に対して1つ以上の集積回路を保護するための物理的シールドとして作用し、集積回路デバイスが保護層を掘ることによって物理的に攻撃された場合に保護の電子的対策を起動するためのトリガとしても使用される。したがって、本開示は、物理的保護と保護の電子的対策とを組み合わせ、両方とも、悪意のある攻撃に対して活性層を保護することを可能にする。物理的保護は、電子的対策を実行するトリガとして実際に使用される。

10

【0015】

有利には、検出回路は、少なくとも1つの活性層内に集積される。

【0016】

集積回路デバイスは、検出回路によって物理的攻撃が検出されると、電子的保護対策を実行するための信号を生成するように構成される電子保護回路を更に備えることができる。

【0017】

有利には、電子保護回路は、少なくとも1つの活性層内に集積される。

【0018】

2つの保護層は、レーザ放射線、少なくとも1つの活性層からの電磁放射線、外部源（すなわち、集積回路デバイスの外部）によって生成される電磁放射線を含む群の内部放射線及び外部放射線の通過を妨げるように構成することができる。

20

【0019】

2つの保護層は、金属、金属合金、又は半導体材料で作られ得る。

【0020】

第1の実施形態では、集積回路デバイスはワイヤボンディング用に設計される。

【0021】

第2の実施形態では、集積回路デバイスはフリップチップシステムである。

【0022】

2つの保護層のうちの1つ、又は2つの保護層の各々は、フルプレートであり得る。

30

【0023】

第1の変形形態では、2つの保護層のうちの1つ又は2つの保護層の各々は、平行線を形成する屈曲連続ワイヤで作られる。任意選択的に、この屈曲連続ワイヤは、プリント回路基板によって支持することができる。

【0024】

別の実施形態では、保護層は、検出回路に電氣的に接続される基本プレートのモザイクを備える。

【0025】

検出回路は、2つの保護層のそれぞれの電氣的値の間の相対的な値を測定するように構成することができる。

40

【0026】

第1の例では、検出回路は、2つの保護層の当該電気情報として、2つの保護層間の静電容量を測定するように構成される。

【0027】

第2の例では、検出回路は、2つの保護層の当該電気情報として、2つの保護層間の電気抵抗の差を測定するように構成される。

【0028】

検出回路は、許容範囲外の、基準値からの監視された電気情報の偏差を検出するように構成される。

50

【0029】

任意選択的に、2つの保護層は、電気絶縁体として機能する2つのそれぞれの接合層を介して、半導体基板層及び少なくとも1つの活性層に接合される。

【0030】

本開示はまた、集積回路デバイスを含む製品に関する。

【図面の簡単な説明】

【0031】

本開示の他の特徴、目的、及び利点は、添付の図面を参照してなされた非限定的な実施形態の詳細な記述を読むことによってより明確になるであろう。

【図1】第1の実施形態による集積回路デバイスを示す。

10

【図2】第2の実施形態による集積回路デバイスを示す。

【図3】集積回路デバイスに電子的保護を提供する電子回路を示す。

【図4A】第1の実施形態による集積回路デバイスの第1の変形形態を示す。

【図4B】第1の実施形態による集積回路デバイスの第1の変形形態を示す。

【図5】第1の実施形態による集積回路デバイスの第2の変形形態を示す。

【図6】集積回路デバイスの第3の実施形態を示す。

【図7】第1の実施形態による集積回路デバイスの動作を示す構成図である。

【発明を実施するための形態】

【0032】

本開示は、悪意のある攻撃、特にサイドチャネル攻撃及び障害攻撃に対する保護を提供するように設計された集積回路デバイスに関する。

20

【0033】

集積回路デバイスは、暗号アルゴリズム及び／又はプロトコルを実行するように設計され得るハードウェア実装及びソフトウェア実装の混合である。これらのハードウェア実装及びソフトウェア実装は、サイドチャネル攻撃及び障害攻撃（例えば、レーザビームによる障害攻撃又はグリッチ電磁攻撃）に対して脆弱である。そのような攻撃は、集積回路デバイスに障害を注入してその挙動を変更するための放射線の使用、又は1つ以上の回路から発される放射線の検出に基づくことができる。本開示は、1つ以上の回路に向けられた1つ以上の外部放射源（例えば、レーザ又は電磁グリッチ）を使用する攻撃、及び1つ以上の回路から発される放射線の検出に基づく攻撃に対する保護を提供することを目的とする。

30

【0034】

当業者によく知られているように、集積回路デバイス100は、半導体基板層10と少なくとも1つの活性層20とを含む複数の重なり合う層を備える。半導体基板層10は、半導体材料で作られる。1つ以上の活性層20は、半導体部品などの電子部品を含む。それらはまた、1つ以上の導体トラックを含む。1つ以上の電子回路又はデバイスは、これらの1つ以上の活性層に集積され得る。

【0035】

本開示では、半導体基板層10及び1つ以上の活性層20は、内部放射線及び外部放射線の通過を妨げるための物理的障害物として作用する2つの保護層又は「シールド」層30A、30Bの間に挟まれる。保護層は、層10、20のスタックの両側（図1又は図2の上部及び底部）に配置される。それらは、追加の重なり合う層を構成する。これらの保護層は、レーザ放射線及び電磁放射線などの放射線の通過を妨げるように設計されている。それらは、集積回路デバイス100（特に、1つ以上の活性層）を保護するための「ファラデーケージ」効果と比較し得る効果をもたらす。例えば、外部源（すなわち、集積回路デバイスの外部）によって放射され、集積回路デバイスに向けられたレーザビームは、保護層うちの1つに当たり、この保護層によって遮断される。集積回路デバイスの一方の側での電磁障害注入の場合、電磁場は、この側に配置された保護層に当たり、1つ以上の活性層を破壊することなく、ファラデーケージのように保護層にわたって分布する。更に、保護層は、1つ以上の回路からの電磁放射線などの1つ以上の回路から来る放射線を吸

40

50

収する。結果として、サイドチャネル攻撃によって秘密情報を得ることは非常に困難であるか、不可能でさえある。

【0036】

各保護層30A、30Bの厚さは、効率的な保護を提供するように適合させることができる。その値は、保護層の材料及び集積回路デバイスに必要なサイズなどの1つ以上のパラメータに依存し、実験的に決定することができる。例えば、この厚さは、良好な保護及びサイズの低減を提供するために、保護層の所与の材料について50pmと200pmとの間に含まれ得る。しかしながら、別の材料の場合、より薄い厚さ（例えば、30pm）も効率的であり得る。集積回路デバイスのサイズに対する要件がない場合には、200pmよりも厚い厚さを適用することもできる。例えば、各保護層の厚さは、500pmに等しくなり得る。

10

【0037】

保護層30A、30Bは、金属、例えば銅、アルミニウム、金又は白金で作られ得る。或いは、それらは、ステンレス鋼（例えば、300グレードのステンレス鋼）などの金属合金、又は半導体材料で作られる。

【0038】

保護層30A、30Bは、サイドチャネル攻撃、レーザ攻撃、及び電磁障害攻撃やボディバイアス注入攻撃などの電磁攻撃に対して強力な受動保護を提供する。実際、これらのシールド層30A、30Bは、集積回路デバイス100の両側の電磁放射線の全部ではないにしても大部分を保持し、サイドチャネルデータを取得することを非常に困難にする。それらはまた、1つ以上の活性層に向けられた任意のレーザビーム、及び1つ以上の活性層に向けられた電磁信号又はニードルの大部分を保持し、集積回路動作を妨げることを非常に困難にする。

20

【0039】

保護層の接着を容易にするために、接合層又は界面層31A、31Bを、それぞれ保護層30A、30Bと層10、20との間に挿入することができる。これらの接合層31A、31Bは、保護層30Aと1つ以上の活性層20とを接合し、保護層30Bと半導体基板層10とを接合する機能を有する。それらは、当業者によく知られている特定の接着剤で作られ得る。接合層の材料は、当業者によく知られているように、電気絶縁材料とすることができる。保護層30A、30Bは、別の方法で層10、20に接合することができる。

30

【0040】

保護層30A、30Bは、図3に概略的に示されるように、検出回路40に電氣的に接続される。この検出回路又は検出デバイス40は、保護層30A、30Bの電気情報を監視し、監視された電気情報に基づいて2つの保護層30A、30Bのうちの少なくとも1つの物理的攻撃を検出する機能を有する。検出回路40は、集積回路デバイス100の1つ以上の活性層20に集積される。各保護層30A、30Bは、1つ以上のTSV（シリコン貫通電極）を介して検出回路40に接続される。

【0041】

より正確には、検出回路40は、2つの保護層30A、30B間の相対的な電氣的値を監視するように構成することができる。そのような相対的な値は、経時的に一定又はほぼ一定のままであると予想される。特に、集積回路デバイス100の温度の変化は、この相対的な値に影響を与えるべきではない。

40

【0042】

相対的な電氣的値は、2つの保護層30A、30B間の静電容量であり得る。或いは、相対的な電氣的値は、2つの保護層間の電気抵抗の差であり得る。

【0043】

検出回路40は、物理的攻撃を検出するために、2つの保護層30A、30B間のこの相対的な電氣的値を測定し、それが経時的に一定又はほぼ一定のままであるか否かを判定することによってそれを監視するように構成される。このために、基準値を含む許容範囲

50

が、検出回路 40 によって使用され得る。この許容範囲内の監視された相対的な電氣的値の変動は受け入れることができ、許容範囲外の監視された相対的な電氣的値の変動は、検出回路 40 によって物理的攻撃として検出することができる。言い換えれば、測定された相対的な電氣的値がこの許容範囲内にある場合、それは一定（又はほぼ一定）のままであると見なされ、物理的攻撃は検出されない。しかし、測定された相対的な電氣的値が許容範囲外である場合、それは一定のままではないと見なされ、物理的攻撃が検出される。許容範囲は、攻撃の効率的な検出を可能にし、誤検出を回避するために、実験によって特徴付けることができる。例えば（あくまでも）、基準値と比較して $\pm 10\%$ の変動が許容され得る（「ほぼ一定」と見なされる）。しかしながら、この $\pm 10\%$ の値は一例に過ぎない。別の許容範囲、例えば、基準値と比較して $\pm 5\%$ 若しくは $\pm 30\%$ 、又は攻撃の効率的な検出及び誤検出の回避に実験的に適切であると判定された任意の他の値を適宜判定することができる。

10

【0044】

集積回路デバイス 100 は、図 3 に示されるように、電子保護回路 50 を更に備える。この保護回路 50 は、検出回路 40 に接続される。動作中、集積回路デバイスが、保護層 30 うちの 1 つを掘ることによって物理的に攻撃されると、この物理的攻撃は、検出回路 40 によって検出され、保護回路 50 に信号が送られる。これにより、保護回路 50 は、電子的保護対策を実行するための制御信号を生成する。例えば、制御信号は、1 つ以上のメモリを消去する、又は集積回路デバイスの動作（機能）を遮断するためのコマンド、又は集積回路デバイス 100 の秘密情報又は機密情報を保護することを目的とした任意の他の対策である。

20

【0045】

検出回路 40 及び保護回路 50 のおかげで、保護層 30 A、30 B は、集積回路（チップ）に入るレーザ又は電磁信号又はチップ外部の電磁放射線を遮断するための受動保護として使用されるだけでなく、集積回路デバイス 100 が物理的攻撃を受け、攻撃者が保護層 30 A、30 B のうちの 1 つの、全部又は一部を除去しようとする、能動的対策をトリガする構成要素としても使用される。

【0046】

集積回路デバイス 100 はまた、1 組の重なり合う層 10、20、30 A、30 B、31 A、31 B を覆うモールドキャップ 60 を備え得る。

30

【0047】

集積回路デバイス 100 は、キャリア 200 によって支持され得る。このキャリア 200 は、集積回路デバイス 100 の 1 つ以上の回路が接続される導体トラックを支持することができる。そのような構成は、集積回路デバイス 100 の他の電子デバイスへの接続を容易にするために、導体トラックの再分布を可能にする。このキャリア 200 は、他の電子部品又は電子デバイスを支持する別のより大きなキャリア（不図示）によって支持することができる。キャリア 200 とより大きなキャリアとの間の電氣的接続は、図 1 及び図 2 に示すように、はんだボール端子を使用することができる。

【0048】

第 1 の実施形態

40

図 1 は、ワイヤボンディング用に設計された集積回路デバイス 100 の第 1 の実施形態を示す。集積回路デバイス 100 は、ワイヤボンディングパッケージである。この実施形態は、上記の開示に準拠する。次に、この第 1 の実施形態に特有の特徴を図 1 を参照して説明する。

【0049】

集積回路デバイス 100 の第 1 の実施形態はワイヤボンディング用に設計されているので、当業者によく知られているように、例えば金（Au）の複数の接続ワイヤ 21 が、活性層 20 の 1 つ以上の回路を、接続の再分布のためにキャリア 200 によって支持された導体トラックに接続する。集積回路デバイス 100 の層は、キャリア 200 からモールドキャップ 60 に向かって（すなわち、図 1 の底部から上部に向かって）、保護層 30 B、

50

接合層 31B、半導体基板層 10、活性層 20、接合層 31A、及び保護層 30A の順で互いに重なり合う。

【0050】

第1の実施形態によれば、保護層 30A、30B は、2つのプレート、有利には2つのフルプレートである。

【0051】

次に、集積回路デバイス 100（例えば、図1に示されるデバイス）の動作について、図7を参照して説明する。

【0052】

2つの保護層 30A、30B は、放射線の通過を妨げる物理的障害物として作用する。それらは、レーザビーム又は電磁放射線などの放射線の通過を妨げる。攻撃者が、外部レーザ源からレーザビームを1つ以上の活性層に向けることによって集積回路デバイス 100 を攻撃する場合、このレーザビームは、保護層 30A、30B のうちの1つによって止められる。集積回路デバイス 100 の一方の側からのグリッチ電磁攻撃の場合、この側に配置された保護層 30 の近傍で生成される電磁場は、この保護層によって遮断され、1つ以上の活性層 20 を妨げない。更に、サイドチャネル攻撃の場合、保護層 30A、30B は、攻撃者が秘密情報を得るためにこれらの電磁放射線を捕捉することができないように、動作中の1つ以上の回路によって生成される電磁放射線を止める。

【0053】

検出回路 40 は、ステップ S1 において、2つの保護層 30A、30B 間の相対的な電気的値を測定する。そのような監視は、集積回路デバイス 100 が電力供給されていると、集積回路デバイス 100 の寿命にわたって行うことができる。例えば、2つの保護層 30A、30B を2つのコンデンサと見なし、2つの保護層 30A、30B 間のそれぞれの静電容量値の差 C を測定する。測定された電気的値は、2つの保護層間の「相対的」な値であるので、経時的に一定（又はほぼ一定）であることが予想される。温度が上昇しても、両方のコンデンサは同様に影響を受けるので、温度の変化によって変更されるべきではない。しかしながら、小さな変動は、基準値に対する許容範囲内（例えば、基準値に対して $\pm 10\%$ ）で許容され得る。監視ステップ S2 において、2つの保護層 30A、30B 間の測定された相対的な電気的値（例えば、静電容量 C の差）が、「C₀」として参照される基準値から許容範囲外に逸脱しているか否かを判定するために監視される。検出回路 40 は、測定された相対的な電気的値 C が基準値 C₀ と比較して一定のままであるか否か、又は所定の許容範囲内にあるか否かを判定する。そうである（図7の分岐 Y の）場合、検出デバイス 40 は、ステップ S1 及びステップ S2 を繰り返す。物理的攻撃は検出されない。

【0054】

集積回路デバイス 100 の物理的攻撃の場合、攻撃者は、1つ以上の活性層にアクセスする前に、2つの保護層のうちの少なくとも1つに侵入しなければならない。その場合、検出回路 40 は、ステップ S2（図7の分岐 N）において、測定された相対的な電気的値 C が変化し、基準値から許容範囲外に逸脱することを検出する。結果として、ステップ S3 において、検出回路 40 は警報信号を生成し、ステップ S4 において、それを電子保護回路 50 に送信する。例えば（あくまでも）、監視された相対的な電気的値が基準値と比較して 10% を超えて増加又は減少すると、検出回路 40 によって警報信号が生成される。

【0055】

電子保護回路 50 は、警報信号を受信すると、ステップ S5 において、集積回路デバイス 100 を保護するための電子的対策の実行を制御する。対策は、集積回路デバイス 100 の1つ又は複数のメモリを消去すること、集積回路デバイス 100 の動作を遮断すること、又は当業者に知られている任意の他の電子的対策のうちの1つ以上の動作であり得る。

【0056】

静電容量の代わりに、２つの保護層３０Ａ、３０Ｂのそれぞれの抵抗値の間の差を測定し、監視することができる。或いは、温度が変化した場合であっても、経時的に一定又はほぼ一定のままであると予想される２つの保護層３０Ａ、３０Ｂの任意の他の電気的特性を、検出回路４０によって測定及び監視することができる。

【００５７】

前述したように、保護層３０Ａ、３０Ｂは、サイドチャネル攻撃及び障害攻撃のような攻撃に対する物理的及び受動保護を提供する。結果として、攻撃者は、２つの保護層３０Ａ、３０Ｂのうちの少なくとも１つの、全部又は一部を除去する必要がある。保護層３０のうちの１つに穴を開けること、又は保護層３０のうちの１つを一体的に除去することは、メモリワイプのような対策を実行するセキュリティメカニズムをトリガする効果を有する。セキュリティメカニズムは任意の種類のものであってもよく、本開示はいくつかの特定の対策に限定されない。

【００５８】

第１の実施形態の変形形態１

第１の実施形態の変形形態では、２つの保護層３０Ａ、３０Ｂのうちの少なくとも１つ（すなわち、保護層の一方又は両方のいずれか）は、平行線を形成するために屈曲された単一の連続ワイヤ３２で作られ得る。

【００５９】

図４Ａ及び図４Ｂは、第１の実施形態のこの第１の変形形態の一例を示す。この例では、集積回路デバイス１００の構造は、第１の実施形態の構造と同様であるが、１つの屈曲連続ワイヤ３２Ａ、３２Ｂが、各保護プレートを置き換えるために使用され、保護層又はシールド層３０Ａ、３０Ｂとして作用する。屈曲連続ワイヤ３２、３２Ｂは、第１の実施形態で前述したように、接合（界面）層３１Ａ、３１Ｂを介して１つ以上の活性層又は半導体基板層に接合することができる。したがって、各屈曲ワイヤ３２Ａ、３２Ｂは、対応する接合層３１Ａ、３１Ｂにわたって延在している。

【００６０】

図４Ａは、集積回路デバイス１００の重なり合う層３０Ａ、３１Ａ、２０、１０、３１Ｂ、３０Ｂの上面図である。これは、単一の屈曲ワイヤ３２Ａによって形成された保護層３０Ａを示している。図４Ｂは、重なり合う層３０Ａ、３１Ａ、２０、１０、３１Ｂ、３０Ｂの側面図を示す。

【００６１】

各保護層３０Ａ、３０Ｂにおいて、ワイヤの平行線は互いに非常に近接している。２つの隣接する線の間の空間は、非常に小さく、例えば数ミクロンであり得る。

【００６２】

各屈曲ワイヤ３２Ａ（３２Ｂ）は、フルプレートと同様に、攻撃に対して集積回路デバイスを保護するシールドを形成する。更に、シールドが単一のワイヤによって提供されるという事実は、シールドの攻撃の場合の検出を容易にする。実際、ワイヤが切断されたか否かを検出することは非常に容易である。

【００６３】

第１の実施形態の変形形態２

第１の実施形態の第２の変形形態は、上述の実施形態の第１の変形形態と同様であるが、各屈曲連続ワイヤ３２Ａ（３２Ｂ）がプリント回路基板（ＰＣＢ）３３（集積回路デバイスの一方の側を３３Ａ、他方の側を３３Ｂと呼ぶ）によって支持されている点のみが異なる。プリント回路基板３３Ａ（３３Ｂ）は、保護層３０Ａ（３０Ｂ）と接合層３１Ａ（３１Ｂ）との間の中間層を形成する。ワイヤ３２Ａ（３２Ｂ）は、対応するＰＣＢ ３３Ａ（３３Ｂ）上にプリントされる。これは、物理的保護を改善することを可能にする。そのような構成によって提供される異なる攻撃に対する保護は、フルプレートによって提供される保護に非常に近い。

【００６４】

屈曲連続ワイヤを担持するプリント回路基板は、集積回路デバイスの一方の側又は両側

10

20

30

40

50

に備えることができる。

【0065】

保護層の第1の変形形態及び第2の変形形態は、第1の実施形態による集積回路デバイスにおいて使用することができるが、この種類の1つ以上の保護層を受け入れるのに適した外部回路への相互接続のための別のインターフェースを備える集積回路デバイスにおいても使用することができる。

【0066】

第2の実施形態

集積回路デバイスの第2の実施形態は、第1の実施形態と同様であるが、図2に示すように、フリップチップシステムである点でこの第1の実施形態とは異なる。

10

【0067】

はんだボール端子70は、1つ以上の活性層の接続端子の再分布のために、キャリア200によって支持される導体トラックに1つ以上の活性層20の1つ以上の回路を接続する。重なり合う層は、キャリア200からモールドキャップ60に向かって（図2の底部から上部に向かって）、保護層30A、接合層30A、活性層20、半導体基板層10、接合層31B、及び保護層31Bの順に配置される。当業者によく知られているように、図2には示されていない円筒形の（例えば、銅で作られた）導体ポストが、はんだボール端子70と1つ以上の活性層20の接続端子との間に挿入され、保護層30Aに備えられ穴を通して配置される。

【0068】

第2の実施形態による集積回路デバイスの動作は、第1の実施形態による集積回路デバイスの動作と同様である。

20

【0069】

第3の実施形態

第3の実施形態では、各保護層30は、図6に示す基本プレート34Aのような基本プレートのモザイクを備える。各基本プレート34Aは、例えばTSVによって、検出回路40に電氣的に接続される。2つの保護層30A、30Bは同一である。これは、第1の保護層30Aの各基本プレート34Aが、第2の保護層30Bの対応する基本プレート34Bに面することを意味する。互いに対向する2つの対応する基本プレート34A、34Bは結合される。

30

【0070】

動作中、検出回路40は、基本プレート34A、34Bの各対について、2つの結合された基本プレート間の相対的な電氣的値を測定する。例えば、検出回路40は、2つの結合された基本プレート間の静電容量、又は2つの結合された基本プレートのそれぞれの抵抗間の差を測定するように構成される。

【0071】

保護層のそのような構成は、ワイヤボンダパッケージ（第1の実施形態）、フリップチップシステム（第2の実施形態）、又は外部回路への相互接続のための別の種類のインターフェースを備える集積回路デバイスの別のパッケージの集積回路デバイスにおいて使用することができる。

40

【0072】

変形形態では、基本プレート34A（34B）は、前述したように、プリント回路基板によって支持され得る。

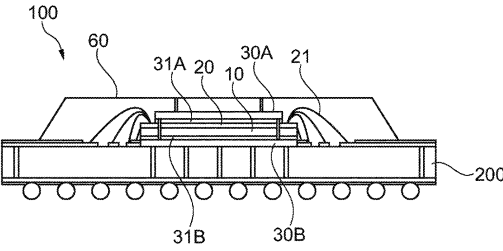
【0073】

集積回路デバイス100は、製品に集積され得る。本開示はまた、そのような製品に関する。

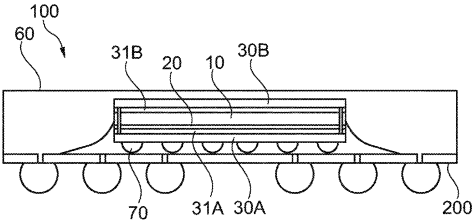
50

【図面】

【図 1】

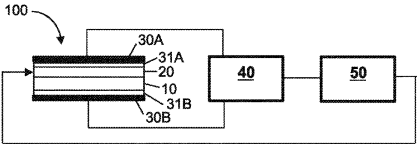


【図 2】

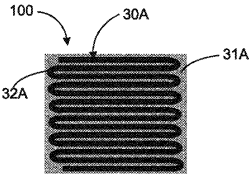


10

【図 3】

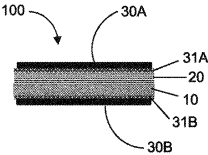


【図 4 A】

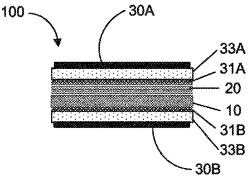


20

【図 4 B】



【図 5】

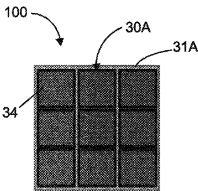


30

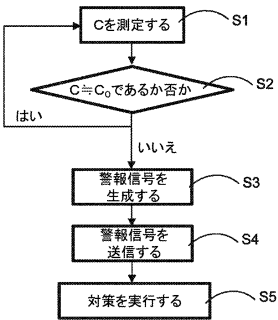
40

50

【図 6】



【図 7】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/069077

A. CLASSIFICATION OF SUBJECT MATTER INV. G06F21/75 G06F21/87 G09C1/00 H04L9/00 ADD.		
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) G06F G09C H04L		
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 practicable, search terms used) EPO-Internal, WPI Data, COMPENDEX, IBM-TDB		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2019/055307 A1 (CRYPTOGRAPHY RES INC [US]) 21 March 2019 (2019-03-21) paragraph [0037] - paragraph [0053] figures 3,4a,4b,4c	1-15
A	EP 3 291 293 A1 (STMICROELECTRONICS (CROLLES 2) SAS [FR]) 7 March 2018 (2018-03-07) paragraph [0030] - paragraph [0031]	1-15
A	US 2018/308808 A1 (KIRSCHNER YUVAL [IL] ET AL) 25 October 2018 (2018-10-25) paragraph [0016] - paragraph [0032]	1-15
A	FR 3 035 267 A1 (COMMISSARIAT ENERGIE ATOMIQUE [FR]) 21 October 2016 (2016-10-21) page 10, line 16 - page 14, line 30	1-15
-/--		
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 12 October 2021		Date of mailing of the international search report 20/10/2021
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Bec, Thierry

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/069077

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007 227498 A (MATSUSHITA ELECTRIC IND CO LTD) 6 September 2007 (2007-09-06) paragraph [0008] - paragraph [0015] -----	1-15
A	WO 2007/086046 A2 (NDS LTD [GB]; WALKER JOHN [GB]; MANTIN ITSIK [IL]) 2 August 2007 (2007-08-02) figures 10-12 page 29, line 27 - page 34, line 21 -----	1-15

1

10

20

30

40

50

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2021/069077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2019055307 A1	21-03-2019	CN 111095534 A EP 3682471 A1 US 2021035924 A1 WO 2019055307 A1	01-05-2020 22-07-2020 04-02-2021 21-03-2019
EP 3291293 A1	07-03-2018	CN 107799474 A CN 206992080 U EP 3291293 A1 FR 3055471 A1 US 2018061781 A1	13-03-2018 09-02-2018 07-03-2018 02-03-2018 01-03-2018
US 2018308808 A1	25-10-2018	JP 6635276 B2 JP 2018186271 A TW 201839652 A US 2018308808 A1	22-01-2020 22-11-2018 01-11-2018 25-10-2018
FR 3035267 A1	21-10-2016	CN 106067460 A EP 3086368 A2 FR 3035267 A1 US 2016307855 A1	02-11-2016 26-10-2016 21-10-2016 20-10-2016
JP 2007227498 A	06-09-2007	NONE	
WO 2007086046 A2	02-08-2007	CN 102063584 A EP 1977481 A2 EP 2615641 A2 HK 1129772 A1 HK 1157508 A1 IL 192916 A US 2009001821 A1 WO 2007086046 A2	18-05-2011 08-10-2008 17-07-2013 04-12-2009 29-06-2012 31-07-2012 01-01-2009 02-08-2007

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,N
E,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,
CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JO,JP,K
E,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,N
G,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,
TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW
ローザンヌ ルート ドゥ ジュネーヴ 22-24 ナグラビジョン ソシエテ アノニム内