(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5976308号
(P5976308)
(45)発行日　平成28年8月23日(2016.8.23)　(24)登録日　平成28年7月29日(2016.7.29)

(51)Int.Cl.　F I
G06F 21/81 (2013.01)　G06F 21/81

請求項の数 10　外国語出願　(全 9 頁)

(21)出願番号　特願2011-273503(P2011-273503)
(22)出願日　平成23年12月14日(2011.12.14)
(65)公開番号　特開2012-128860(P2012-128860A)
(43)公開日　平成24年7月5日(2012.7.5)
審査請求日　平成26年11月26日(2014.11.26)
(31)優先権主張番号　1060465
(32)優先日　平成22年12月14日(2010.12.14)
(33)優先権主張国　フランス(FR)

(73)特許権者　511304475
オベルチュール　テクノロジーズ
フランス国　９２３００　ルヴァロワ＝ペレ、５０　ケ　ミシュレ
(74)代理人　110000729
特許業務法人　ユニアス国際特許事務所
(72)発明者　ニコラ、モーリン
フランス国　９２３００　ルヴァロワ＝ペレ、５０　ケ　ミシュレ、オベルチュール　テクノロジーズ内
(72)発明者　クリストフ、ジロー
フランス国　９２３００　ルヴァロワ＝ペレ、５０　ケ　ミシュレ、オベルチュール　テクノロジーズ内

最終頁に続く

(54)【発明の名称】攻撃の場合のマイクロ回路カードの指令手段の電源の安全確保

(57)【特許請求の範囲】
【請求項１】
当該モジュールへの攻撃を検出するための手段と、
攻撃が検出されたときに、不揮発性メモリのセル（１１０、５１０）への書き込み動作を指令するために、プログラミング電圧（U_P）の印加可能なチャージポンプ（１２０）に充電することができる指令手段（１３０）と、
通常の動作の際に電力が供給され、攻撃が検出されたときにのみ前記チャージポンプ（１２０）へと電力を供給するように構成されたコンデンサ（１４０）とを備えており、
前記コンデンサ（１４０）が、攻撃が検出されたときに前記指令手段（１３０）にも電力を供給することを特徴とするモジュール（１００、５００、６００）。
【請求項２】
前記指令手段（１３０）が、フリップフロップ（１３２）及びＮＯＴゲート（１３４）を備えており、前記フリップフロップの出力が、通常の動作においては第１のレベルにあり、攻撃が検出されたときに第２のレベルにあり、前記第２のレベルが、前記書き込み動作の継続時間の全体において高のままであることを特徴とする請求項１に記載のモジュール（１００、５００、６００）。
【請求項３】
前記セル（１１０）が、ワン・タイム・プログラマブル（ＯＴＰ）セルであることを特徴とする請求項１又は２に記載のモジュール（１００）。
【請求項４】

前記セル（５１０）が、ＥＥＰＲＯＭメモリのセルであることを特徴とする請求項１又は２に記載のモジュール（５００、６００）。

【請求項５】

制御信号（ＳＣ）を含んでおり、

前記制御信号（ＳＣ）のレベル（ＮＨ、ＮＢ）が前記セル（５１０）の書き込み又はブランク状態を表わし、

前記制御信号（ＳＣ）が、攻撃が検出されたときに当該モジュール（５００）の重要信号（ＳＩＶ）を維持するために使用されることを特徴とする請求項４に記載のモジュール（５００）。

【請求項６】

前記重要信号（ＳＩＶ）が、リセット信号、クロック信号、又は当該モジュール（５００）の外部の機器に接続された入力／出力信号の中から選択されることを特徴とする請求項５に記載のモジュール（５００）。

【請求項７】

制御信号（ＳＣ）を含んでおり、

前記制御信号（ＳＣ）のレベル（ＮＨ、ＮＢ）が前記セル（５１０）の書き込み又はブランク状態を表わし、

前記制御信号（ＳＣ）が、当該モジュールの重要部品（１５０）への電力の供給を制御するスイッチ（Ｔ３）に対する指令に使用されることを特徴とする請求項４に記載のモジュール（６００）。

【請求項８】

前記スイッチ（Ｔ３）が、ＰＭＯＳトランジスタであることを特徴とする請求項７に記載のモジュール（６００）。

【請求項９】

前記重要部品が、プロセッサ（１５０）であることを特徴とする請求項７に記載のモジュール（６００）。

【請求項１０】

IS0 7816規格によるマイクロ回路カードで構成される請求項１に記載のモジュール（１００、５００、６００）。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電子モジュールの保護の分野に位置する。

【背景技術】

【０００２】

この発明は、特に、マイクロ回路カード（例えばIS0 7816規格によるもの）の保護に適用されるが、これに限られるわけではない。

【０００３】

故障注入攻撃（fault injection attack）に対するマイクロ回路カードの保護の範囲において、以下のような対策が知られている。混乱が検出されたときにカードの不揮発性メモリの予約領域に所定の値を書き込み、この領域の内容を各々の指令の開始時にカードによってチェックする。そして、チェックしたこの内容が、前記所定の値に等しい場合には、カードが指令の実行を拒絶し、カードが使用不可能になる。

【０００４】

公知の様相では、不揮発性メモリへの書き込み動作に先立ってチャージポンプの充電が必須であり、結果としてカードの電流消費の極めて顕著な増加が必然的に生じる。

【０００５】

この急激な変化は、カードと直列に接続された抵抗器を使用する単純電力解析（ＳＰＡ）によって観測可能である。

【０００６】

従って、チャージポンプの充電検出モジュールを利用できる攻撃者にとってみれば、通常の動作においてはあり得ない電力消費の増加を検出し、すなわちカードの自身を動作不可能にしようとする試みの現れを検出したときに、前記領域への前記所定の値の書き込みを防止すべくカードへの電源を速やかに遮断することで、上述の攻撃対策を回避できてしまう。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

本発明は、この問題に対する解決策を提供する。

【課題を解決するための手段】

【０００８】

より正確には、本発明は、

モジュールへの攻撃を検出するための手段と、

攻撃が検出されたときに、不揮発性メモリのセルへの書き込み動作を指令するために、プログラミング電圧の印加可能なチャージポンプに充電することができる指令手段と、

通常の動作の際に電力が供給され、攻撃が検出されたときにのみ前記チャージポンプへと電力を供給するように構成されたコンデンサと、を備えるモジュールに関する。

【０００９】

このモジュールは、前記コンデンサが、攻撃が検出されたときに前記指令手段にも電力を供給することを特徴とする。

【００１０】

本発明によれば、極めて好都合なことに、コンデンサの放電をマイクロ回路カードの電力消費の解析によって検出することが不可能である。

【００１１】

攻撃が検出されたときに、コンデンサは指令手段にも電力を供給する。このため、マイクロ回路カードへの電力の供給を遮断しようとする攻撃は、効果的なものではなくなるだろう。

【００１２】

本発明の一特定の実施の形態においては、指令手段が、フリップフロップ及びＮＯＴゲートを備えており、ゲートの出力が、通常の動作においては第１の通常レベルにあり、攻撃が検出されたときに第２のレベルにある。

【００１３】

不揮発性メモリのセルは、ワン・タイム・プログラマブル（ＯＴＰ）セル又はＥＥＰＲＯＭメモリのセルとすることができる。

【００１４】

本発明の一特定の実施の形態においては、このモジュールが、制御信号を含んでおり、この制御信号のレベルが、ＥＥＰＲＯＭセルの書き込み又はブランク状態を表わす。この制御信号は、攻撃が検出されたときに当該モジュールの重要信号を維持するために使用される。

【００１５】

この重要信号を、リセット信号、クロック信号、又は当該モジュールの外部の機器に接続される入力／出力信号の中から選択することができる。

【００１６】

別の実施の形態においては、前記制御信号が、当該モジュールの重要部品への電力の供給を制御するスイッチに対する指令に使用される。

【００１７】

前記重要部品は、例えばプロセッサで構成することができる。

【００１８】

前記スイッチは、ＰＭＯＳトランジスタとすることができる。

【００１９】

本発明の一特定の実施の形態においては、当該モジュールが、IS0 7816規格によるマイクロ回路カードである。

【図面の簡単な説明】

【００２０】

【図１】本発明の第１の実施の形態によるモジュール１００を示している。

【図２】本発明の別の実施の形態によるマイクロ回路カード５００を示している。

【図３】本発明の別の実施の形態によるマイクロ回路カード６００を示している。

【発明を実施するための形態】

【００２１】

本発明の他の特徴及び利点が、添付の図面（決して本発明を限定しようとするものではない３つの実施の形態を示している）を参照しつつ以下に提示される説明から、明らかになるであろう。

【００２２】

図１に、本発明の第１の実施の形態によるモジュール１００を示す。このモジュールは、この例では、IS0 7816規格によるマイクロ回路カードで構成されている。

【００２３】

このマイクロ回路カードは、セル１１０からなる不揮発性メモリを備えており、このセルは、１回だけプログラム可能である。このセルは、ＯＴＰ（One Time Programmable）セルという名前で当業者に知られている。

【００２４】

本発明によれば、ＯＴＰセル１１０は、マイクロ回路カード１００に対する悪意のある攻撃の検出を表わす変数を保存すべく、変更されるように設計されている。そのような攻撃については、例えば或る動作を２回実行して対応する出力を比較することによって検出することができるが、個々の攻撃の検出は本発明の主題ではない。

【００２５】

公知の様相で、マイクロ回路カード１００は、ＯＴＰセル１１０へと値を書き込むように実現されたチャージポンプ１２０を備えている。不揮発性メモリへの書き込みに先立って、セル１１０にプログラミング電圧U_pを印加するために、チャージポンプ１２０の充電が行われる。この充電に伴い、マイクロ回路カードの電流消費が極めて顕著に増加する。

【００２６】

この急激な変化を、例えば抵抗器をマイクロ回路カード１００に直列に接続することによって、例えばＳＰＡ（単純電力解析）によって観測することができる。

【００２７】

マイクロ回路カード１００は、ＯＴＰセル１１０への変数の書き込みを指令するための手段１３０を備えている。より正確には、この手段は、通常動作においては第１のレベル（低レベルＮＢ）にあり、攻撃が検出されたときは第２のレベル（高レベルＮＨ）にある指令（信号）ＣＯＭを生成する。

【００２８】

ここで説明される実施の形態においては、この指令手段が、Ｄ型フリップフロップ１３２と、ＮＯＴゲート１３４とを備えている。Ｄ型フリップフロップ１３２が、ＯＴＰセル１１０への書き込み動作を制御するビットに相当する。

【００２９】

換言すると、この例においては、攻撃が検出されると、Ｄ型フリップフロップ１３２の出力が低レベル（ＮＢ）から高レベル（ＮＨ）へと反転される。

【００３０】

本発明によれば、マイクロ回路カードが、電圧ＶＣＣが通常の動作において供給されるコンデンサ１４０を備えている。

【００３１】

ここで説明される実施の形態においては、コンデンサ１４０の一方のリード線がスイッ

チＴ１へと接続されており、通常の動作においてはこのスイッチＴ１が導通されてコンデンサ１４０が充電される。このスイッチＴ１は、Ｄ型フリップフロップ１３２の出力へと直接接続されたＰＭＯＳトランジスタで構成されており、このＤ型フリップフロップ１３２は通常の動作において低レベル（ＮＢ）にある

【００３２】

チャージポンプ１２０も、指令手段１３０によって制御される。指令手段１３０は、通常の動作の間はチャージポンプ１２０への電力の供給を阻止する。

【００３３】

より正確には、ここで説明される実施の形態においては、チャージポンプ１２０の一方のリード線が、通常の動作において非導通であるスイッチＴ２に接続されている。このスイッチＴ２は、ＰＭＯＳトランジスタで構成され、このＰＭＯＳトランジスタは、ＮＯＴゲート１３４を介してＤ型フリップフロップ１３２の出力へと接続されている。

【００３４】

本発明によれば、コンデンサ１４０が、攻撃が検出されたときにのみチャージポンプ１２０への電力供給を行うように設計されている。ここで説明される実施の形態においては、コンデンサ１４０の一方のリード線が、スイッチＴ２へと接続されている。

【００３５】

攻撃が検出されたとき、Ｄ型フリップフロップ１３２の出力が高レベル（ＮＨ）へと反転することで、スイッチＴ２の導通、コンデンサ１４０によるチャージポンプ１２０への充電、及びＯＴＰセル１１０への書き込み動作がもたらされる。

【００３６】

ここで説明される実施の形態においては、マイクロ回路カードのプロセッサ１５０が、ＯＴＰセルの中身をソフトウェアにて監視（ポーリング、割り込みなど）し、攻撃に応答する動作を実行するが、そのような動作は本発明の一部を構成するものではない。

【００３７】

公知の様相で、ＯＴＰセル１１０のレジスタへの書き込みを正しく行うためには、Ｄ型フリップフロップの出力が、書き込み動作の全体にわたって高レベル（ＮＨ）のままであることが必要である。

【００３８】

しかしながら、攻撃者にとって、例えばＥＭＡ（電磁気解析）を使用して、コンデンサ１４０からチャージポンプ１２０への放電の開始を検出し、マイクロ回路カード１００への電力の供給を遮断して、Ｄ型フリップフロップの出力を乱し、つまりＯＴＰセル１１０への書き込み作業を邪魔することが可能である。

【００３９】

本発明は、コンデンサ１４０から指令手段１３０にも電力を供給することによって、この問題を解決する。

【００４０】

本発明によれば、極めて好都合なことに、コンデンサ１４０の放電を、マイクロ回路カードの電力消費を解析することによって検出することは不可能である。

【００４１】

従って、ここで説明される実施の形態においては、コンデンサ１４０が、Ｄ型フリップフロップ１３２及びＮＯＴゲート１３４へと電力を供給する。

【００４２】

フリップフロップ１３２への書き込みを、プロセッサ１５０又は他のハードウェア部品によって行うことができる。

【００４３】

一変種（図示されていない）においては、このフリップフロップが、プロセッサ１５０の特定のレジスタの１ビットであってよい。

【００４４】

図２に、本発明の別の実施の形態によるマイクロ回路カード５００を示す。

【００４５】
この図において、マイクロ回路カード５００の構成要素のうちで、図１のマイクロ回路カード１００の構成要素と同様の構成要素には、同じ参照符号を付している。
【００４６】
この実施の形態においては、マイクロ回路カード５００の不揮発性メモリが、ＥＥＰＲＯＭセル５１０である。この実施の形態の原理は、攻撃が検出されたときにチャージポンプ１２０へと電力を供給することによってＥＥＰＲＯＭセル５１０への書き込み動作を開始させ、ＥＥＰＲＯＭメモリへの書き込み動作が実行されるときに、通常モードにおいては高レベルにある制御信号ＳＣを低レベルへと反転させることにある。
【００４７】
ここで説明される実施の形態においては、攻撃が検出されたときにマイクロ回路カード５００の重要信号ＳＩＶを維持するために、制御信号ＳＣは、これらの信号ＳＣ、ＳＩＶをＡＮＤゲートによって結合させることによって使用される。
【００４８】
この重要信号は、例えばリセット信号（ＲＥＳＥＴ）、クロック信号（ＣＬＯＣＫ）、又はこのマイクロ回路カードの読み取り機に接続される入力／出力（ＩＯ）信号の中から選択することができる。
【００４９】
このＡＮＤゲートからもたらされる信号ＳＩＶＳが、本発明によって保護される重要信号である。
【００５０】
ここで説明される実施の形態においては、ＥＥＰＲＯＭセル５１０のドレインｄが、チャージポンプ１２０の出力及び制御信号ＳＣへと接続され、これによって制御信号ＳＣのレベルがＥＥＰＲＯＭセル５１０の書き込み又はブランク状態を表わす。
【００５１】
通常の動作においては、ＥＥＰＲＯＭセル５１０がブランクであり、ソースｓとドレインｄとの間に高いインピーダンスを有し、ゲートが接地されている。つまり、このＥＥＰＲＯＭセル５１０は、開いたスイッチと同様に振る舞い、電流が通過することがない。
【００５２】
第１のリード線が電圧ＶＣＣへと接続され、他方のリード線がドレインｄへと接続された抵抗器５２０が、信号ＳＣを高レベルに保持することを可能にする。
【００５３】
この通常動作モードにおいて、チャージポンプ１２０は、チャージポンプ１２０の出力に配置された第１のダイオード５３０によって保護されている。
【００５４】
指令手段１３０によって攻撃が検出されたとき、スイッチＴ２が導通状態になり、チャージポンプ１２０が、プログラミング電圧U_P（例えば、１５Ｖ程度である）をＥＥＰＲＯＭセル５１０のドレインｄへと出力する。
【００５５】
これにより、公知の様相で、ＥＥＰＲＯＭ５１０の浮遊ゲートｇｆが正に充電され、書き込み動作がＥＥＰＲＯＭ５１０へと実行され、負になる閾値電圧（ゲート－ソース間）の低下が引き起こされる。
【００５６】
書き込み動作の継続時間の全体にわたって、プログラミング電圧U_Pが電圧ＶＣＣよりも高いことに注目することが重要である。制御信号ＳＣを、書き込み動作の継続時間の全体にわたって、U_Pレベルにではなく、ＶＣＣレベルに維持するために、マイクロ回路カード５００は、ＥＥＰＲＯＭ５１０のドレインｄと制御信号ＳＣを引き出すための抵抗器５２０との間に直列に配置された第２のダイオード５４０を備えている。
【００５７】
この第２のダイオード５４０は、制御信号ＳＣの後方に位置する論理回路を保護するた

めに、チャージポンプ１２０の出力の制御信号ＳＣへの接続を防止する。

【００５８】

ひとたびＥＥＰＲＯＭへの書き込み動作が完了すると、ＥＥＰＲＯＭは導通状態（ゲートと０Ｖであるソースとの間の電圧が、閾値電圧よりも大きくなる）になり、ソースｓとドレインｄとの間のインピーダンスが、抵抗器５２０と比べて低くなる。

【００５９】

結果として、制御信号ＳＣが低レベルへと反転し、このレベルを論理的に監視することによって攻撃を検出することができる。

【００６０】

図３に、本発明の別の実施の形態によるマイクロ回路カード６００を示す。

【００６１】

この図において、マイクロ回路カード６００の構成要素のうちで、図２のマイクロ回路カード５００の構成要素と同様の構成要素には、同じ参照符号を付している。

【００６２】

この実施の形態においては、マイクロ回路カード６００が、図２の制御信号ＳＣに対して相補的な制御信号ＳＣを生成するためのＮＯＴゲート５６０を有している。

【００６３】

換言すると、この実施の形態においては、制御信号ＳＣが、通常の動作において低レベル（ＮＢ）にあり、攻撃が検出された場合に高レベル（ＮＨ）にある。

【００６４】

この制御信号ＳＣが、カードの重要な構成要素（この例ではプロセッサ１５０）への電力の供給を遮断することができるスイッチを制御する。

【００６５】

ここで説明される実施の形態においては、このスイッチが、ＰＭＯＳトランジスタＴ３で構成される。

【００６６】

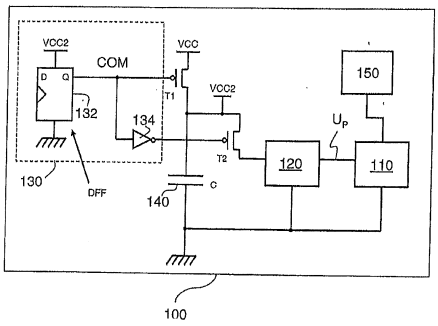
より正確には、図３の実施の形態においては、マイクロ回路カード６００が、制御信号ＳＣによって制御されるトランジスタＴ３を備えている。この制御内容は、以下の通りである。通常の動作においては、制御信号ＳＣが低レベルにあり、ＣＰＵ１５０に電圧ＶＣＣが供給される。そして、攻撃が検出された場合には、制御信号ＳＣが高レベルへと反転し、ＣＰＵ１５０にはもはや電力が供給されない。

【符号の説明】

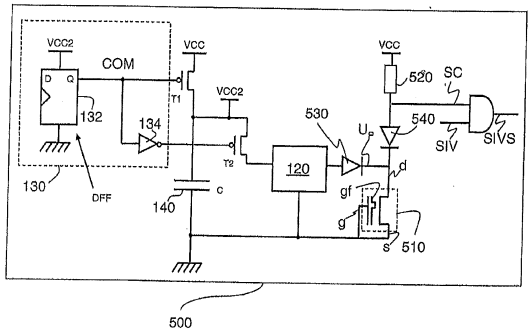
【００６７】

１００：　モジュール（マイクロ回路カード）
１１０：　セル（ＯＴＰセル）
１２０：　チャージポンプ
１３０：　変数書込指令手段
１３２：　Ｄ型フリップフロップ
１３４：　ＮＯＴゲート
１４０：　コンデンサ
１５０：　プロセッサ
５００：　マイクロ回路カード
５１０：　ＥＥＰＲＯＭセル
５２０：　抵抗器
５３０：　第１のダイオード
５４０：　第２のダイオード
５６０：　ＮＯＴゲート
６００：　マイクロ回路カード

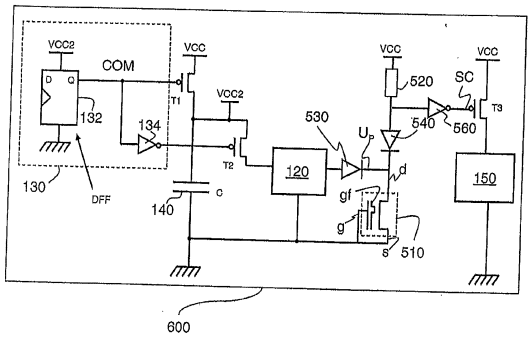
【図１】


VCC2
COM
VCC
150
D Q
132
T1
VCC2
134
U_P
T2
120
110
130
DFF
140
C
100

【図２】


VCC2
COM
VCC
VCC
520
SC
D Q
132
T1
VCC2
530
U_P
540
SIV
SIVS
134
T2
120
d
130
DFF
140
C
gf
g
s
510
500

【図３】


VCC2
COM
VCC
VCC
520
SC
VCC
D Q
132
T1
VCC2
530
U_P
540
T3
560
134
T2
120
150
d
130
DFF
140
C
gf
g
s
510
600

フロントページの続き

審査官　打出　義尚

(56)参考文献　特開２０１０－０６８５２３（ＪＰ，Ａ）
欧州特許出願公開第０１１１３３８６（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／８１