

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6050523号
(P6050523)

(45) 発行日 平成28年12月21日 (2016.12.21)

(24) 登録日 平成28年12月2日 (2016.12.2)

(51) Int. Cl. F I
G O 6 F 21/79 (2013.01) G O 6 F 21/79

請求項の数 40 (全 23 頁)

(21) 出願番号	特願2015-552880 (P2015-552880)	(73) 特許権者	507364838
(86) (22) 出願日	平成26年1月14日 (2014.1.14)		クアルコム, インコーポレイテッド
(65) 公表番号	特表2016-507829 (P2016-507829A)		アメリカ合衆国 カリフォルニア 921
(43) 公表日	平成28年3月10日 (2016.3.10)		21 サン ディエゴ モアハウス ドラ
(86) 国際出願番号	PCT/US2014/011412		イブ 5775
(87) 国際公開番号	W02014/110550	(74) 代理人	100108453
(87) 国際公開日	平成26年7月17日 (2014.7.17)		弁理士 村山 靖彦
審査請求日	平成28年3月23日 (2016.3.23)	(74) 代理人	100163522
(31) 優先権主張番号	13/741, 248		弁理士 黒田 晋平
(32) 優先日	平成25年1月14日 (2013.1.14)	(72) 発明者	アサフ・アシュケナジ
(33) 優先権主張国	米国 (US)		アメリカ合衆国・カリフォルニア・921
早期審査対象出願			21・サン・ディエゴ・モアハウス・ドラ
			イブ・5775
		審査官	戸島 弘詩
			最終頁に続く

(54) 【発明の名称】 ワンタイムプログラマブル集積回路セキュリティ

(57) 【特許請求の範囲】

【請求項 1】

集積回路内のメモリアセットを保護する方法であって、
複数のワンタイムプログラマブル (OTP) メモリアレイの各々の値をサンプルするステップと、

前記複数の OTP メモリアレイの各 OTP メモリアレイの前記サンプル値を前記複数の OTP メモリアレイの他の各 OTP メモリアレイの前記サンプル値と、およびプログラムされていない OTP メモリアレイ値と比較するステップであって、前記プログラムされていない OTP メモリアレイ値が、製造時の OTP メモリアレイに関連付けられた同じ論理値のすべての n ビットに対応し、n が前記複数の OTP メモリアレイの各々の中のメモリデバイスの数である、ステップと、

各 OTP メモリアレイの前記サンプル値が他の各 OTP メモリアレイの前記サンプル値に等しいかどうかを判断するステップと、

各 OTP メモリアレイの前記サンプル値が他の各 OTP メモリアレイの前記サンプル値に等しく、各 OTP メモリアレイの前記サンプル値が前記プログラムされていない OTP メモリアレイ値に等しい場合に、集積回路動作障害が発生したと判断するステップと、

前記障害発生判断によって決定された、メモリへのアクセスによって前記集積回路を動作させるステップと

を含む方法。

【請求項 2】

10

20

前記集積回路動作障害が発生したと判断するステップが、
各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しくない場合に、前記障害が発生したと判断するステップと、
各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しく、各OTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しくない場合に、前記障害が発生しなかったと判断するステップと
をさらに含む、請求項1に記載の方法。

【請求項3】

前記プログラムされていないOTPメモリアレイ値がゼロである、請求項1に記載の方法。

【請求項4】

前記プログラムされていないOTPメモリアレイ値が $(2^n - 1)$ である、請求項1に記載の方法。

【請求項5】

セキュリティ信号の指示を決定するステップを含み、
前記障害が発生しなかったと判断された場合に、前記セキュリティ信号がセキュア動作モードを示し、

前記障害が発生したと判断された場合に、前記セキュリティ信号が非セキュア動作モードを示す、
請求項1に記載の方法。

【請求項6】

前記障害が発生したと判断された場合に、メモリへのアクセスが、セキュアメモリへの制限されたアクセスを含む、請求項1に記載の方法。

【請求項7】

前記集積回路をブートするステップが、前記障害発生判断によって影響されない、請求項1に記載の方法。

【請求項8】

前記集積回路がシステムオンチップを含む、請求項1に記載の方法。

【請求項9】

集積回路内のメモリアセットを保護する方法であって、
第1のワнтаイムプログラマブル(OTP)メモリアレイの値および第2のOTPメモリアレイの値をサンプルするステップと、

前記第1のOTPメモリアレイおよび前記第2のOTPメモリアレイの前記サンプル値を互いと、およびプログラムされていないOTPメモリアレイ値と比較するステップであって、前記プログラムされていないOTPメモリアレイ値が、製造時のOTPメモリアレイに関連付けられた同じ論理値のすべてのnビットに対応し、nが前記第1のOTPメモリアレイおよび前記第2のOTPメモリアレイの各々の中のメモリデバイス数である、ステップと、

前記第1のOTPメモリアレイの前記サンプル値が前記第2のOTPメモリアレイの前記サンプル値に等しいかどうかを判断するステップと、

前記第1のOTPメモリアレイの前記サンプル値が前記第2のOTPメモリアレイの前記サンプル値に等しく、前記第1のOTPメモリアレイおよび前記第2のOTPメモリアレイの各々の前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しい場合に、集積回路動作障害が発生したと判断するステップと、

前記障害発生判断によって決定された、メモリへのアクセスによって前記集積回路を動作させるステップと
を含む方法。

【請求項10】

前記集積回路動作障害が発生したと判断するステップが、
前記第1のOTPメモリアレイの前記サンプル値が前記第2のOTPメモリアレイの前記サンプル値に等しくない場合に、前記障害が発生したと判断するステップと、

前記第1のOTPメモリアレイの前記サンプル値が前記第2のOTPメモリアレイの前記サン

10

20

30

40

50

ル値に等しく、前記第1のOTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しくなく、前記第2のOTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しくない場合に、前記障害が発生しなかったと判断するステップと

をさらに含む、請求項9に記載の方法。

【請求項11】

前記プログラムされていないOTPメモリアレイ値がゼロである、請求項9に記載の方法。

【請求項12】

前記プログラムされていないOTPメモリアレイ値が (2^n-1) である、請求項9に記載の方法。

10

【請求項13】

セキュリティ信号の指示を決定するステップを含み、

前記障害が発生しなかったと判断された場合に、前記セキュリティ信号がセキュア動作モードを示し、

前記障害が発生したと判断された場合に、前記セキュリティ信号が非セキュア動作モードを示す、

請求項9に記載の方法。

【請求項14】

前記障害が発生したと判断された場合に、メモリへのアクセスが、セキュアメモリへの制限されたアクセスを含む、請求項9に記載の方法。

20

【請求項15】

前記集積回路をブートするステップが、前記障害発生を検出することによって影響されない、請求項9に記載の方法。

【請求項16】

前記集積回路がシステムオンチップを含む、請求項9に記載の方法。

【請求項17】

集積回路内のメモリアセットを保護するためのシステムであって、

複数のワнтаイムプログラマブル(OTP)メモリアレイと、

前記複数のOTPメモリアレイの各々の値をサンプルするように構成された回路と、

比較論理ブロックであって、

30

前記複数のOTPメモリアレイの各OTPメモリアレイの前記サンプル値を前記複数のOTPメモリアレイの他の各OTPメモリアレイの前記サンプル値と、およびプログラムされていないOTPメモリアレイ値と比較することであって、前記プログラムされていないOTPメモリアレイ値が、製造時のOTPメモリアレイに関連付けられた同じ論理値のすべてのnビットに対応し、nが前記複数のOTPメモリアレイの各々の中のメモリデバイス数である、比較することと、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しいかどうかを判断することであって、前記比較論理ブロックが、各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しく、各OTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しい場合に、障害が発生したと判断するように構成される、判断することと

40

を行うように構成された、比較論理ブロックと、

前記障害発生判断によって決定された、メモリへのアクセスによって前記集積回路を動作させるように構成された少なくとも1つの処理モジュールとを含むシステム。

【請求項18】

前記比較論理ブロックが、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しくない場合に、前記障害が発生したと判断し、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等し

50

く、各OTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しくない場合に、前記障害が発生しなかったと判断するようにさらに構成される、請求項17に記載のシステム。

【請求項19】

前記プログラムされていないOTPメモリアレイ値がゼロである、請求項17に記載のシステム。

【請求項20】

前記プログラムされていないOTPメモリアレイ値が $(2^n - 1)$ である、請求項17に記載のシステム。

【請求項21】

前記比較論理ブロックがセキュリティ信号の指示を決定するように構成され、
前記障害が発生しなかったと判断された場合に、前記セキュリティ信号がセキュア動作モードを示し、
前記障害が発生したと判断された場合に、前記セキュリティ信号が非セキュア動作モードを示す、
請求項17に記載のシステム。

【請求項22】

前記障害が発生したと判断された場合に、メモリへのアクセスが、セキュアメモリへの制限されたアクセスを含む、請求項17に記載のシステム。

【請求項23】

前記集積回路が前記障害発生判断によって影響されないルーチンによってブートされる、請求項17に記載のシステム。

【請求項24】

前記集積回路がシステムオンチップを含む、請求項17に記載のシステム。

【請求項25】

集積回路内のメモリアセットを保護するためのシステムであって、
複数のワнтаイムプログラマブル(OTP)メモリアレイの各々の値をサンプルするための手段と、
前記複数のOTPメモリアレイの各OTPメモリアレイの前記サンプル値を前記複数のOTPメモリアレイの他の各OTPメモリアレイの前記サンプル値と、およびプログラムされていないOTPメモリアレイ値と比較するための手段であって、前記プログラムされていないOTPメモリアレイ値が、製造時のOTPメモリアレイに関連付けられた同じ論理値のすべてのnビットに対応し、nが前記複数のOTPメモリアレイの各々の中のメモリデバイス数である、手段と、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しいかどうかを判断するための手段と、

第1のOTPメモリアレイの前記サンプル値が第2のOTPメモリアレイの前記サンプル値に等しく、前記第1のOTPメモリアレイおよび前記第2のOTPメモリアレイの各々の前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しい場合に、集積回路動作障害が発生したと判断するための手段と、

前記障害発生判断によって決定された、メモリへのアクセスによって前記集積回路を動作させるための手段と
を含むシステム。

【請求項26】

前記集積回路動作障害が発生したと判断するための前記手段が、
各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しくない場合に、前記集積回路動作障害が発生したと判断するための手段と、
各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しく、各OTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しくない場合に、前記集積回路動作障害が発生しなかったと判断するための手段と

を含む、請求項25に記載のシステム。

【請求項 2 7】

前記プログラムされていないOTPメモリアレイ値がゼロである、請求項25に記載のシステム。

【請求項 2 8】

前記プログラムされていないOTPメモリアレイ値が $(2^n - 1)$ である、請求項25に記載のシステム。

【請求項 2 9】

セキュリティ信号の指示を決定するための手段を含み、

前記障害が発生しなかったと判断された場合に、前記セキュリティ信号がセキュア動作モードを示し、

前記障害が発生したと判断された場合に、前記セキュリティ信号が非セキュア動作モードを示す、

請求項25に記載のシステム。

【請求項 3 0】

前記障害が発生したと判断された場合に、メモリへのアクセスが、セキュアメモリへの制限されたアクセスを含む、請求項25に記載のシステム。

【請求項 3 1】

前記集積回路をブートするステップが、前記障害発生判断によって影響されない、請求項25に記載のシステム。

【請求項 3 2】

前記集積回路がシステムオンチップを含む、請求項25に記載のシステム。

【請求項 3 3】

プロセッサ可読非一時的記憶媒体に常駐し、1つまたは複数のプロセッサによって実行可能なプロセッサ可読命令を含むコンピュータプログラムであって、前記プロセッサ可読命令が、

回路に複数のワнтаイムプログラマブル(OTP)メモリアレイの各々の値をサンプルさせ

、

比較論理ブロックに、

前記複数のOTPメモリアレイの各OTPメモリアレイの前記サンプル値を前記複数のOTPメモリアレイの他の各OTPメモリアレイの前記サンプル値と、およびプログラムされていないOTPメモリアレイ値と比較することであって、前記プログラムされていないOTPメモリアレイ値が、製造時のOTPメモリアレイに関連付けられた同じ論理値のすべてのnビットに対応し、nが前記複数のOTPメモリアレイの各々の中のメモリデバイス数である、比較することと、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しいかどうかを判断することであって、前記プロセッサ可読命令が、前記比較論理ブロックに、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しく、各OTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ値に等しい場合に、障害が発生したと判断させる、判断することとを行わせ、

前記障害発生判断によって決定された、メモリへのアクセスによって前記集積回路を動作させる

ためのものである、コンピュータプログラム。

【請求項 3 4】

前記比較論理ブロックに、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しくない場合に、前記障害が発生したと判断させ、

各OTPメモリアレイの前記サンプル値が他の各OTPメモリアレイの前記サンプル値に等しく、各OTPメモリアレイの前記サンプル値が前記プログラムされていないOTPメモリアレイ

値に等しくない場合に、障害が発生しなかったと判断させるためのプロセッサ可読命令をさらに含む、請求項33に記載のコンピュータプログラム。

【請求項35】

前記プログラムされていないOTPメモリアレイ値がゼロである、請求項33に記載のコンピュータプログラム。

【請求項36】

前記プログラムされていないOTPメモリアレイ値が (2^n-1) である、請求項33に記載のコンピュータプログラム。

【請求項37】

前記比較論理ブロックにセキュリティ信号の指示を決定させるためのプロセッサ可読命令を含み、

前記障害が発生しなかったと判断された場合に、前記セキュリティ信号がセキュア動作モードを示し、

前記障害が発生したと判断された場合に、前記セキュリティ信号が非セキュア動作モードを示す、
請求項33に記載のコンピュータプログラム。

【請求項38】

前記障害が発生したと判断された場合に、メモリへのアクセスが、セキュアメモリへの制限されたアクセスを含む、請求項33に記載のコンピュータプログラム。

【請求項39】

前記集積回路が前記障害発生判断によって影響されないルーチンによってブートされる、請求項33に記載のコンピュータプログラム。

【請求項40】

前記集積回路がシステムオンチップを含む、請求項33に記載のコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ワンタイムプログラマブル集積回路セキュリティに関する。

【背景技術】

【0002】

集積回路(IC)を含む電子システムは、秘密にし、ハッカー攻撃から保護することをユーザが望むまたはそうする必要があるプロビジョニングされたデータを記憶するために、ICのセキュアメモリ、たとえば、セキュアランダムアクセスメモリ(RAM)を利用することが多い。一般に、プロビジョニングされたデータは、製造後にICメモリに記憶された任意のデータであり得る。セキュアメモリに記憶されたプロビジョニングされたデータは、たとえば、限定はしないが、コード、キー、パスワード、アカウント情報、個人情報、プロプライエタリ情報、および連絡先情報を含むことができる。例示的な電子システム、またはエンドデバイスは、セットトップボックス、パーソナルコンピュータ、ラップトップコンピュータ、ハンドヘルドデバイス、タブレット、およびモデムを含む。セキュアメモリに記憶されたそのようなプロビジョニングされたデータは、セキュアメモリに無許可でアクセスできるように設計されたハッカー攻撃を受けやすい場合がある。セキュアメモリ内のプロビジョニングされたデータを保護するために、システムオンチップ(SoC)ICを含むことができるICは、ハードウェア組込み型セキュリティシーケンスを利用して、ICがハッカー攻撃の対象になっているかどうかを判断することができるセキュリティシステムを内蔵することができる。ICが攻撃された場合、セキュリティシステムは、ICがセキュアメモリおよびセキュアメモリに記憶されたプロビジョニングされたデータへのアクセスをブロックまたは制限することを可能にし得る。

【0003】

ハードウェア組込み型セキュリティシーケンスは、ワンタイムプログラマブル(OTP)メ

メモリを使用して実装され得る。OTPメモリは、少なくとも1つのOTPメモリデバイスと、限定はしないが、プログラマブルデバイスのプログラムされた状態をサンプルおよびキャプチャするサンプル/キャプチャ回路を含む任意の関連する電子回路とを含む。複数のOTPメモリデバイスおよび関連する電子回路は、OTPメモリアレイを構成する。OTPメモリデバイスは、1回プログラムすることができ、再プログラムすることはできない。OTPメモリデバイスの例はヒューズおよびアンチヒューズである。

【0004】

例示的なヒューズOTPメモリアレイでは、アレイ内の各ヒューズデバイスは2つの状態のうちの1つで存在することができる。最初のプログラムされていない状態では、ヒューズデバイスは、電流の伝導を可能にする電氣的接続の線として機能することができる。プログラミング電圧または電流が印加されると、各ヒューズデバイスをプログラムされた状態に変換することができ、この状態では、ヒューズデバイスは、ヒューズを通る電流の伝導を制限する開回路として機能することができる。プログラミング電圧または電流は、ヒューズを構成するデバイスに依存する。たとえば、ヒューズがトランジスタによって形成されている場合、プログラミング電圧はトランジスタの動作電圧よりもわずかに高い電圧とすることができる。プログラミング電圧は、ヒューズデバイスの電気特性および/またはヒューズデバイスの構成材料を恒久的に変更することができる。値は、アレイ内の個々のヒューズデバイスを選択的にプログラムする、または「焼く(burning)」ことによって、ヒューズOTPメモリアレイにプログラムされ得る。

【0005】

ヒューズOTPメモリアレイ内のヒューズデバイスの状態の読出しまたはサンプリング中に、各ヒューズは、関連する電子回路によってサンプルおよびキャプチャされ得る「0」または「1」の論理値に対応することができる。たとえば、プログラムされていないヒューズは論理値「0」に対応することができ、プログラムされたヒューズは論理値「1」に対応することができる。まとめると、アレイ内のプログラムされたヒューズデバイスおよびプログラムされていないヒューズデバイスの対応する論理値は、アレイ値を決定することができる。このアレイ値は、ハードウェア組込み型セキュリティシーケンスに対応することができる。

【0006】

OTPメモリアレイを含むICが製造されるとき、プログラムされていないOTPメモリアレイは、すべてのプログラムされていないデバイスを含み得る。一般に、プログラムされていないOTPメモリアレイを備えるICは「バージンチップ」と呼ばれる。プログラムされていないOTPメモリアレイ内のすべてのプログラマブル要素のサンプル状態は、同じ論理値に対応することができる。たとえば、プログラムされていないOTPデバイスが論理値「0」に対応することができる場合、バージンチップのOTPメモリアレイ内の各プログラマブルデバイスのサンプル状態は「0」とすることができる。この場合、プログラムされていないまたはバージンチップOTPメモリアレイ値はゼロとすることができる。別の例では、プログラムされていないOTPデバイスが論理値「1」に対応することができる場合、バージンチップのOTPメモリアレイ内の各プログラマブルデバイスのサンプル状態は「1」とすることができる。この場合、プログラムされていないまたはバージンチップOTPメモリアレイ値は $(2^n - 1)$ (たとえば、2のn乗-1)とすることができ、指数nはOTPメモリアレイ内のプログラマブルデバイスの数に等しいビットの数であり、nは1よりも大きいまたはそれに等しい値を有することができる。

【0007】

ICへのハッカー攻撃の1つのタイプはグリッチ攻撃として知られている。グリッチ攻撃は、悪意をもって利用され得るIC性能の障害を引き起こし得るIC動作パラメータの物理的な外乱であり得る。物理的な外乱は、たとえば、動作電圧の変動、チップ温度の変化、印加される電界、および付随する電磁放射によって実現され得る。グリッチ攻撃によって生じる例示的な障害として、たとえば、セキュアメモリ、処理ルーチン、および/またはICの任意の他の機能、機能要素、もしくは態様を保護するように設計されたICセキュリティ

システムを無効化またはバイパスしようとして、ハードウェア組込み型セキュリティシーケンスがスプーフィングされる可能性がある。

【0008】

OTPメモリアレイを含むICへの例示的なグリッチ攻撃では、チップの物理的状态が変更される場合があり、その結果、プログラマブルデバイス状態のサンプリング中に、各プログラマブルデバイスの状態に対応する論理値を「0」または「1」と一義的に解釈することができない。グリッチ攻撃によって生じる例示的な障害として、シーケンス、たとえば、セキュリティシーケンスでプログラムされたOTPメモリアレイのサンプルOTPメモリアレイ値は、プログラムされたシーケンスに等しくない場合があり、むしろ、スプーフィングされた値であり得る。上記の例示的な攻撃では、OTPメモリアレイは、ヒューズOTPメモリアレイ、アンチヒューズOTPメモリアレイ、または任意の他のタイプのOTPメモリアレイもしくはデバイスであり得る。

10

【0009】

一実施形態では、ICは、サンプルOTPメモリアレイ値を使用して、IC性能の障害が発生したかどうかを判断することによって、セキュアメモリ内のプロビジョニングされたデータを保護することができる。障害が発生したと判断された場合、セキュアメモリへのアクセスが制限またはブロックされ得る。結果として、その後、少なくともグリッチ攻撃を開始したハッカーによってセキュアメモリ内のプロビジョニングされたデータが悪用され得る確率が低減され得る。

20

【発明の概要】

【課題を解決するための手段】

【0010】

本開示による集積回路内のメモリアセットを保護する方法の一例は、複数のOTPメモリアレイの各々の値をサンプルするステップと、各OTPメモリアレイのサンプル値を他の各OTPメモリアレイのサンプル値と、およびプログラムされていないOTPメモリアレイ値と比較するステップと、比較されたサンプル値に基づいて、集積回路性能障害が発生したかどうかを判断するステップと、集積回路をブートするステップと、障害発生判断によって決定されたメモリへのアクセスによって集積回路を動作させるステップとを含む。

【0011】

そのような方法の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。障害が発生したかどうかを判断するステップは、少なくとも1つのOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しく、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しくない場合に、障害が発生したと判断するステップを含み得る。障害が発生したかどうかを判断するステップは、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しく、各OTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しくない場合に、障害が発生しなかったと判断するステップを含み得る。プログラムされていないOTPメモリアレイ値はゼロであってもよい。プログラムされていないOTPメモリアレイ値は $(2^n - 1)$ であってもよく、 n はビットの数であり得る。

30

【0012】

本方法の例示的な実装形態は、セキュリティ信号の指示を決定するステップを含み得る。セキュリティ信号は、障害が発生しなかったと判断された場合に、セキュア動作モードを示し得る。セキュリティ信号は、障害が発生したと判断された場合に、非セキュア動作モードを示し得る。メモリへのアクセスは、障害が発生したと判断された場合に、セキュアメモリへの制限されたアクセスを含み得る。集積回路をブートするステップは、障害発生判断によって影響され得ない。集積回路はシステムオンチップであり得る。

40

【0013】

本開示による集積回路内のメモリアセットを保護する方法の一例は、第1のOTPメモリアレイの値および第2のOTPメモリアレイの値をサンプルするステップと、第1のOTPメモリアレイおよび第2のOTPメモリアレイのサンプル値を互いと、およびプログラムされていない

50

OTPメモリアレイ値と比較するステップと、比較されたサンプル値に基づいて、集積回路性能障害が発生したかどうかを判断するステップと、集積回路をブートするステップと、障害発生判断によって決定されたメモリへのアクセスによって集積回路を動作させるステップとを含み得る。

【0014】

そのような方法の実装形態は、以下の特徴のうちの1つまたは複数を含み得る。障害が発生したかどうかを判断するステップは、第1のOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しい場合、または第2のOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しい場合、または第1のOTPメモリアレイと第2のOTPメモリアレイの両方のサンプル値がプログラムされていないOTPメモリアレイ値に等しい場合に、障害が発生したと判断するステップを含み得る。障害が発生したかどうかを判断するステップは、第1のOTPメモリアレイのサンプル値が第2のOTPメモリアレイのサンプル値に等しくない場合に、障害が発生したと判断するステップを含み得る。障害が発生したかどうかを判断するステップは、第1のOTPメモリアレイのサンプル値が第2のOTPメモリアレイのサンプル値に等しく、第1のOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しくなく、第2のOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しくない場合に、障害が発生しなかったと判断するステップを含み得る。プログラムされていないOTPメモリアレイ値はゼロであってもよい。プログラムされていないOTPメモリアレイ値は (2^n-1) であってもよく、 n はビットの数であり得る。

【0015】

本方法の例示的な実装形態は、セキュリティ信号の指示を決定するステップを含み得る。セキュリティ信号は、障害が発生しなかったと判断された場合に、セキュア動作モードを示し得る。セキュリティ信号は、障害が発生したと判断された場合に、非セキュア動作モードを示し得る。メモリへのアクセスは、障害が発生したと判断された場合に、セキュアメモリへの制限されたアクセスを含み得る。集積回路をブートするステップは、障害発生判断によって影響され得ない。集積回路はシステムオンチップであり得る。

【0016】

本開示による集積回路内のメモリアセットを保護するためのシステムの一例は、複数のOTPメモリアレイと、複数のOTPメモリアレイの各々の値をサンプルするように構成された回路と、各OTPメモリアレイのサンプル値を他の各OTPメモリアレイのサンプル値と、およびプログラムされていないOTPメモリアレイ値と比較し、比較されたサンプル値に基づいて、集積回路性能障害が発生したかどうかを判断するように構成された比較論理ブロックと、集積回路をブートし、障害発生判断によって決定されたメモリへのアクセスによって集積回路を動作させるように構成された少なくとも1つの処理モジュールとを含み得る。

【0017】

本システムの例示的な実装形態は、少なくとも1つのOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しい場合に、障害が発生したと判断し、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しくない場合に、障害が発生したと判断し、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しく、各OTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しくない場合に、障害が発生しなかったと判断するように構成された比較論理ブロックを含み得る。プログラムされていないOTPメモリアレイ値はゼロであってもよい。プログラムされていないOTPメモリアレイ値は (2^n-1) であってもよく、 n はビットの数であり得る。

【0018】

本システムの一例は、セキュリティ信号の指示を決定するように構成された比較論理ブロックを含み得る。セキュリティ信号は、障害が発生しなかったと判断された場合に、セキュア動作モードを示し得る。セキュリティ信号は、障害が発生したと判断された場合に、非セキュア動作モードを示し得る。メモリへのアクセスは、障害が発生したと判断され

た場合に、セキュアメモリへの制限されたアクセスを含み得る。集積回路をブートするステップは、障害発生判断によって影響され得ない。集積回路はシステムオンチップであり得る。

【0019】

本開示による集積回路内のメモリアセットを保護するためのシステムの一例は、複数のOTPメモリアレイの各々の値をサンプルするための手段と、複数のOTPメモリアレイのうちの各OTPメモリアレイのサンプル値を複数のOTPメモリアレイのうちの他の各OTPメモリアレイのサンプル値と、およびプログラムされていないOTPメモリアレイ値と比較するための手段と、比較されたサンプル値に基づいて、集積回路性能障害発生を検出するための手段と、集積回路をブートするための手段と、障害発生判断によって決定されたメモリへのアクセスによって集積回路を動作させるための手段とを含み得る。

10

【0020】

本システムの例示的な実装形態は、少なくとも1つのOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しい場合に、障害が発生したと判断するステップと、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しくない場合に、障害が発生したと判断するステップと、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しく、各OTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しくない場合に、障害が発生しなかったと判断するステップとを含み得る。プログラムされていないOTPメモリアレイ値はゼロであってもよい。プログラムされていないOTPメモリアレイ値は $(2^n - 1)$ であってもよく、 n はビット

20

【0021】

本システムの一例は、セキュリティ信号の指示を決定するための手段を含み得る。セキュリティ信号は、障害が発生しなかったと判断された場合に、セキュア動作モードを示し得る。セキュリティ信号は、障害が発生したと判断された場合に、非セキュア動作モードを示し得る。メモリへのアクセスは、障害が発生したと判断された場合に、セキュアメモリへの制限されたアクセスを含み得る。集積回路をブートするステップは、障害発生判断によって影響され得ない。集積回路はシステムオンチップであり得る。

【0022】

本開示によるプロセッサ可読非一時的記憶媒体に常駐するコンピュータプログラム製品の一例は、回路に複数のOTPメモリアレイの各々の値をサンプルさせ、比較論理ブロックに各OTPメモリアレイのサンプル値を他の各OTPメモリアレイのサンプル値と、およびプログラムされていないOTPメモリアレイ値と比較させ、比較されたサンプル値に基づいて、集積回路性能障害が発生したかどうかを判断させ、集積回路をブートし、障害発生判断によって決定されたメモリへのアクセスによって集積回路を動作させるための、1つまたは複数のプロセッサによって実行可能なプロセッサ可読命令を含み得る。

30

【0023】

本コンピュータプログラム製品の例示的な実装形態は、比較論理ブロックに、少なくとも1つのOTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しい場合に、障害が発生したと判断させ、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しくない場合に、障害が発生したと判断させ、各OTPメモリアレイのサンプル値が他の各OTPメモリアレイのサンプル値に等しく、各OTPメモリアレイのサンプル値がプログラムされていないOTPメモリアレイ値に等しくない場合に、障害が発生しなかったと判断させるためのプロセッサ可読命令を含み得る。プログラムされていないOTPメモリアレイ値はゼロであってもよい。プログラムされていないOTPメモリアレイ値は $(2^n - 1)$ であってもよく、 n はビットの数であり得る。

40

【0024】

本コンピュータプログラム製品の一例は、比較論理ブロックに、セキュリティ信号の指示を決定させるためのプロセッサ可読命令を含み得る。セキュリティ信号は、障害が発生しなかったと判断された場合に、セキュア動作モードを示し得る。セキュリティ信号は、

50

障害が発生したと判断された場合に、非セキュア動作モードを示し得る。メモリへのアクセスは、障害が発生したと判断された場合に、セキュアメモリへの制限されたアクセスを含み得る。集積回路をブートするステップは、障害発生判断によって影響され得ない。集積回路はシステムオンチップであり得る。

【0025】

本発明の実装形態によれば、以下の機能のうちの1つまたは複数が提供され得る。集積回路へのグリッチ攻撃は、障害が発生したと判断することによって検出され得る。2つ以上のOTPアレイの値は互いと、およびプログラムされていないOTPアレイ値と比較され得る。障害が発生したと比較結果が判断した場合、集積回路内のメモリアセットが保護され得る。集積回路をブートすることは、障害が発生したという判断によって影響されない。本発明自体とともに、本発明のこれらおよび他の機能は、以下の図、詳細な説明および特許請求の範囲を検討した後に、より十分に理解されよう。他の機能が提供されてよく、本開示によるすべての実装形態が、説明する機能のすべてはもちろん、それらのいずれかを提供しなければならないわけではない。さらに、上記で言及された効果が言及されたもの以外の手段によって達成される可能性があり、言及された項目/技法は必ずしも言及された効果を生じるとは限らない。

【図面の簡単な説明】

【0026】

【図1】2つのヒューズOTPメモリアレイを含むSoC内のハードウェア組込み型セキュリティシステムの一実施形態を示すブロック図である。

【図2】2つのヒューズOTPメモリアレイを含むハードウェア組込み型セキュリティ方法のためのプロセス図である。

【図3】M個のOTPメモリアレイを含むハードウェア組込み型セキュリティ方法のためのプロセス図である。

【発明を実施するための形態】

【0027】

本発明の実施形態は、ハードウェア組込み型セキュリティシステムを利用して、たとえば、グリッチ攻撃によって引き起こされるSoC性能の障害の発生を検出または判断するための技法を提供する。しかしながら、以下で説明する技法は例示的なものであり、本開示による他の実装形態が可能であるので、本発明を限定するものではない。説明する技法は、方法、装置、またはシステムとして実装され得、コンピュータ可読媒体で具現化され得る。

【0028】

SoCが電源投入されるかリセットされるときに、ヒューズOTPメモリアレイ値がサンプルされる。ヒューズOTPメモリアレイの値は、プログラムされていないまたはバージンチップヒューズOTPメモリアレイ値とおよび1つまたは複数の他のヒューズOTPメモリアレイの値と比較される。ヒューズOTPメモリアレイ値の各々が等しく、アレイ値がプログラムされていない値に等しくない場合、障害が発生しなかったと判断され、SoCはグリッチ攻撃の対象ではなかったと判断され、セキュリティ信号はセキュア動作モードを示すように設定される。ヒューズOTPメモリアレイのアレイ値がすべて等しくないか、またはアレイ値のうちの少なくとも1つがプログラムされていない値に等しい場合、障害が発生したと判断され、SoCはグリッチ攻撃の対象であったと判断され、セキュリティ信号は非セキュア動作モードを示すように設定される。SoCはセキュア動作モードと非セキュア動作モードの両方についての同じ手順に従ってブートされる。SoCがブートされた後、非セキュア動作モードで、SoCは、セキュリティ信号指示に応答して、セキュアメモリへの制限された、ブロックされた、または他の方法で制御されたアクセス、およびセキュアメモリに記憶された任意のプロビジョニングされたデータによって動作する。セキュア動作モードでは、SoCは、セキュアメモリへのアクセス、およびセキュアメモリに記憶された任意のプロビジョニングされたデータによって動作する。セキュア動作モードでは、セキュアメモリへのアクセスの程度、レベル、またはタイプおよびセキュアメモリに記憶された任意のプ

ロビジョニングされたデータはセキュリティ信号指示に応答して制限されないが、セキュリティ信号指示以外のパラメータに応答して制限され、ブロックされ、または他の方法で制御され得る。この手順は、SoCが電源投入されるかリセットされるたびに繰り返される。

【0029】

図1を参照すると、SoC内のメモリアセットを保護するためのハードウェア組込み型セキュリティシステム100の一実施形態を示すブロック図が示されている。システム100は例示的なものであり、別のタイプのIC内にあってもよく、SoCに限定されない。システム100は限定的なものではなく、たとえば、構成要素を追加する、削除する、または、並べ替えることによって変更され得る。

10

【0030】

システム100は、図1には図示されていない電子システム、またはエンドデバイスの一部であり得る。エンドデバイスは、ICを含む任意の電子システム、たとえば、セットトップボックス、パーソナルコンピュータ、ラップトップコンピュータ、ハンドヘルドデバイス、タブレット、およびモデムであり得る。

【0031】

一実施形態では、システム100は、OTPメモリアレイブロック120、比較論理ブロック140、処理モジュール170、非セキュアメモリ184、およびセキュアメモリ188を含むことができる。OTPメモリアレイブロック120は、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128の2つのヒューズOTPメモリアレイを含むことができる。ヒューズOTPメモリアレイA 124は、n個のヒューズデバイス121(nは1よりも大きいまたはそれに等しい整数である)およびサンプル/キャプチャ回路123を含むことができる。同様に、ヒューズOTPメモリアレイB 128は、n個のヒューズデバイス125(nはヒューズOTPメモリアレイA 124と同じ値である)およびサンプル/キャプチャ回路127を含むことができる。図1に示すヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128の構成要素は例示的なものであり、限定的なものではなく、両方のヒューズOTPメモリアレイは図示されていない他の構成要素も含み得る。

20

【0032】

サンプル/キャプチャ回路123および127は、n個のヒューズデバイス121および125のプログラムされた/プログラムされていない状態に対応する論理値をそれぞれサンプルおよびキャプチャすることができる。

30

【0033】

一実施形態では、プログラムされていないヒューズは「0」の論理値に対応し得、プログラムされたヒューズは「1」の論理値に対応し得る。いくつかの例示的な実装形態では、プログラムされていないヒューズは「1」の論理値に対応し得、プログラムされたヒューズは「0」の論理値に対応し得る。一実施形態では、OTPメモリアレイブロック120は、プログラムされていないヒューズOTPデバイスを「1」の論理値に対応させ、プログラムされたヒューズOTPデバイスを「0」の論理値に対応させ得る、1つまたは複数のインバータデバイスを含み得る。例示的な適用例では、OTPメモリアレイブロック120は、アンチヒューズデバイスまたは任意の他のタイプのOTPデバイスを含み得る。

40

【0034】

OTPメモリアレイブロック120は、ビット線バスA 134およびビット線バスB 138の2つのビット線バスを介して比較論理ブロック140に結合され得る。各ビット線バス134および138は、それぞれヒューズOTPメモリアレイ124および128からn個の信号を搬送することができる。n個の信号の各々は、n個のヒューズOTPデバイスのうちの1つのサンプルおよび/またはキャプチャされた論理値に対応することができる。

【0035】

比較論理ブロックは処理モジュール170に結合され得る。セキュリティ信号160は、電気的接続または信号を伝播するように構成された任意の他のタイプの接続を介して比較論理ブロック140から処理モジュール170に送られ得る。

50

【0036】

処理モジュール170は、ランダムアクセスメモリ(RAM)または任意の他のタイプのICメモリを含み得るメモリブロック184および188に結合され得る。メモリブロック184は非セキュアメモリであってもよく、メモリブロック188はセキュアメモリであってもよい。非セキュアメモリ184とセキュアメモリ188の両方はプロビジョニングされたデータを含み得る。

【0037】

図1に示すシステム100の要素間の接続は例示的なものである。要素間の追加の接続が使用され得る。図1に示す要素と、図1に図示されないが、ハードウェア組込み型セキュリティシステムおよび/またはSoCもしくは他のICに含まれる他の要素との間の接続も存在し得る。図示されない1つまたは複数の他のプロセッサがシステム100に含まれ得る。

10

【0038】

システム100のセキュアメモリブロック188、または処理モジュール170がアクセス可能な他のセキュアメモリに記憶され得るプロビジョニングされたデータを保護するために、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128は、チップ製造後に、たとえば、システム100を含む電子システムまたはエンドデバイスの製造中に、同一のセキュリティシーケンスでプログラムされ得る。

【0039】

一実施形態では、OTPメモリアレイブロック120は、バージンチップのプログラムされていないOTPメモリアレイについて、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128内のすべてのプログラムされていないヒューズデバイスのサンプル状態がすべて「0」の同じ論理値に対応し得るように構成された、ヒューズOTPデバイスを含むことができる。したがって、n個のプログラムされていないヒューズデバイスの場合、ヒューズOTPメモリアレイA 124のサンプル状態はゼロのnビット値に対応し得る。同様に、ヒューズOTPメモリアレイB 128のサンプル状態はゼロのnビット値に対応し得る。特定の例示的な実装形態では、プログラムされていないOTPデバイスのサンプル状態は「1」の論理値に対応し得、プログラムされたOTPデバイスのサンプル状態は「0」の論理値に対応し得る。したがって、そのような例示的な実装形態では、OTPメモリアレイブロック120内の各OTPメモリアレイのサンプルnビット値は、論理値「1」のすべてのnビットに対応する($2^n - 1$)であり得る。nの値によって決定される($2^n - 1$)というこの非ゼロ値は、バージンチップのプログラムされていないOTPメモリアレイ値であり得る。

20

30

【0040】

一実施形態では、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128は、同一のセキュリティシーケンスでプログラムされ得る。セキュリティシーケンスをヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128にプログラムすることは、OTPメモリアレイ内のヒューズを選択的にプログラムすることによって実装され得る。プログラミングの後、ヒューズOTPメモリアレイA 124のサンプルアレイ値はヒューズOTPメモリアレイB 128のサンプルアレイ値と同一であり得る。さらに、サンプルアレイ値はプログラムされていないバージンチップOTPメモリアレイ値に等しくなくてもよい。

40

【0041】

一実施形態では、SoCを含むシステム100が電源投入されるかリセットされるとき、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128について、ヒューズOTPメモリアレイA 124のn個のヒューズデバイス121のヒューズ状態およびヒューズOTPメモリアレイB 128のn個のヒューズデバイス125のヒューズ状態が、それぞれサンプル/キャプチャ回路123および127によってサンプルおよびキャプチャされ得る。ヒューズOTPメモリアレイA 124のサンプルアレイ値は、ビット線バスA 134を介して比較論理ブロック140に送られ得る。同様に、ヒューズOTPメモリアレイB 128のサンプルアレイ値は、ビット線バスB 138を介して比較論理ブロック140に送られ得る。

【0042】

50

比較論理ブロック140は、デジタル論理回路145を含むことができる。デジタル論理回路145は、限定はしないが、ANDゲート、NANDゲート、ORゲート、NORゲート、XORゲートおよびそれらの任意の組合せを含むことができる。一実施形態では、デジタル論理回路145は、各ヒューズOTPメモリアレイ124および128のサンプル値をプログラムされていないバージンチップアレイ値と比較することができ、ヒューズOTPメモリアレイA 124のサンプル値をヒューズOTPメモリアレイB 128のサンプル値と比較することもできる。これらの比較に基づいて、比較論理ブロック140は、たとえば、グリッチ攻撃による障害が発生したかどうかを判断することができる。

【0043】

いくつかの実装形態では、各アレイのプログラムされていないバージンチップ値はゼロであり得る。この場合、各ヒューズOTPメモリアレイ124および128のサンプル値がデジタル論理回路145によってゼロと比較され得る。他の例示的な実装形態では、n個の要素の各アレイのプログラムされていないバージンチップ値は (2^n-1) であり得る。そのような実装形態では、各ヒューズOTPメモリアレイ124および128のサンプル値は (2^n-1) と比較され得る。

【0044】

特定の実装形態では、比較論理ブロック140は、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128のサンプル値が同一であり、非ゼロである場合に、障害が発生しなかったと判断することができる。この場合、ヒューズOTPメモリアレイA 124とヒューズOTPメモリアレイB 128の両方のサンプル値は、ヒューズOTPメモリアレイA 124とヒューズOTPメモリアレイB 128の両方にプログラムされ得る同一のセキュリティシーケンスに対応し得る。別の特定の実装形態では、比較論理ブロック140は、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128のサンプル値が同一であり、 (2^n-1) に等しくない場合に、障害が発生しなかったと判断することができる。

【0045】

一実施形態では、比較論理ブロック140は、ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128のサンプル値が同一でない場合に、障害が発生したと判断することができる。上記で説明したように、たとえば、グリッチ攻撃によって障害が発生した場合、ヒューズOTPメモリアレイA 124および/またはヒューズOTPメモリアレイB 128のサンプル値がスプーフィングされる可能性があり、したがって、同一でもなく、プログラムされたセキュリティシーケンスに等しくもない可能性がある。

【0046】

特定の実装形態では、比較論理ブロック140は、ヒューズOTPメモリアレイA 124のサンプル値および/またはヒューズOTPメモリアレイB 128のサンプル値がゼロに等しい場合に、障害が発生したと判断することができる。この場合は、バージンチップに対応し得る。

【0047】

特定の実装形態では、比較論理ブロック140は、ヒューズOTPメモリアレイA 124のサンプル値および/またはヒューズOTPメモリアレイB 128のサンプル値が (2^n-1) に対応する場合に、障害が発生したと判断することができる。この場合は、バージンチップに対応し得る。

【0048】

バージンチップの場合、障害が発生したという判断に関してフォールスポジティブが実現され得る。比較論理ブロック140は、ヒューズOTPメモリアレイのサンプル値についての上記で説明した比較基準に基づいて、たとえば、グリッチ攻撃による障害が、そのような障害または攻撃がない場合でさえ、発生したことを示し得る。たとえば、バージンチップのセキュアメモリは、保護が必要とされるおよび/または所望されるプロビジョニングされたデータを含まないことがあるため、バージンチップのセキュアメモリへのブロックされたまたは制限されたアクセスがチップの動作において重要でなくてもよいので、そのようなフォールスポジティブな結果は軽減される。

【0049】

障害発生判断に基づいて、比較論理ブロック140は、セキュア動作モードまたは非セキュア動作モードを示すことができるセキュリティ信号160を生成することができる。障害が発生したと比較論理ブロック140が判断した場合、セキュリティ信号160は非セキュア動作モードを示すことができる。バージンチップは障害の発生に関してフォールスポジティブを生成する可能性があるので、セキュリティ信号160はバージンチップの場合に非セキュア動作モードを示すことがある。障害が発生しなかったと比較論理ブロック140が判断した場合、セキュリティ信号160はセキュア動作モードを示すことができる。

【0050】

セキュリティ信号160は、比較論理ブロック160によって処理モジュール170に送られ得る。一実施形態では、処理モジュール170は、セキュア動作モードまたは非セキュア動作モードのセキュリティ信号指示にかかわらず、同じ処理ルーチンに従ってSoCをブートすることができる。プロセッサをブートするルーチンは、セキュアメモリ188への制限されたまたはブロックされたアクセスによって影響され得ない。特定の適用例では、処理モジュール170はSoCのデバイスまたは機能を試験し得る。プロセッサを試験するルーチンは、セキュアメモリ188への制限されたまたはブロックされたアクセスによって影響され得ない。したがって、少なくともSoCをブートすることおよび試験することは、セキュリティ信号指示によって影響され得ない。

【0051】

SoCがブートされると、SoCはセキュリティ信号指示によって決定されたメモリへのアクセスによって動作することができる。セキュリティ信号160がセキュア動作モードを示す場合、SoCは、非セキュアメモリ184およびセキュアメモリ188に記憶され得るプロビジョニングされたデータとともに、非セキュアメモリ184、セキュアメモリ188、およびSoC動作で使用される任意の他のメモリにアクセスすることができる。一実施形態では、セキュア動作モードでは、セキュアメモリへのアクセスおよびセキュアメモリに記憶された任意のプロビジョニングされたデータは、無制限であり得る。特定の実施形態では、セキュア動作モードでは、セキュアメモリへのアクセスおよびセキュアメモリに記憶された任意のプロビジョニングされたデータは、セキュリティ信号指示を除くパラメータに応答して制限され、ブロックされ、または他の方法で制御され得る。逆に、セキュリティ信号160が非セキュア動作モードを示す場合、セキュリティ信号指示に応答して、SoCは、セキュアメモリ188に記憶され得るプロビジョニングされたデータとともにセキュアメモリ188へのアクセスを制限またはブロックし得る。

【0052】

一実施形態では、バージンチップの場合にフォールスポジティブによって生成された非セキュア動作モードのセキュリティ信号指示は、SoCをブートすることおよび試験することに影響を及ぼし得ない。たとえば、バージンチップはセキュアメモリ188にプロビジョニングされたデータを含まないことがあるので、SoC動作中にセキュアメモリ188へのアクセスがないこと、またはセキュアメモリ188への制限されたアクセスは無関係であり得る。

【0053】

システム100を含む電子システムまたはエンドデバイスの製造中に、セキュリティシーケンスはOTPメモリアレイブロック120にプログラムされ得る。その後、プロビジョニングされたデータがセキュアメモリ188に記憶されると、システム100はプログラムされたセキュリティシーケンスを使用して、たとえば、グリッチ攻撃、ハッカー攻撃、または他の物理的な外乱による障害発生を判断することができる。検出されたまたは判断された障害発生に応答して、システム100は、セキュアメモリ188へのアクセスをブロックまたは制限することによって、セキュアメモリ188およびセキュアメモリ188に記憶され得る任意のプロビジョニングされたデータを保護することができる。

【0054】

動作時、図1をさらに参照しながら図2を参照すると、システム100を使用するハードウェア組込み型セキュリティ方法200は図示された段階を含んでいる。しかしながら、方法2

10

20

30

40

50

00は例示的なものにすぎず、限定的なものではない。方法200は、たとえば、段階を追加する、削除する、または、並べ替えることによって変更され得る。

【0055】

方法200は、ヒューズOTPメモリアレイをサンプルすること220、サンプルヒューズOTPメモリアレイ値を比較すること240、障害の発生を判断すること260、SoCをブートすること270、およびSoCを動作させること280を含む。

【0056】

段階220で、SoCが電源投入されるかリセットされるときに、OTPメモリアレイブロック120の構成要素である(constituent)OTPメモリアレイのヒューズデバイス状態がサンプルおよびキャプチャされる。段階224で、ヒューズOTPメモリアレイA 124のn個のヒューズデバイス121のヒューズ状態が図1に示すサンプル/キャプチャ回路123によってサンプルおよびキャプチャされる。同様に、段階226で、ヒューズOTPメモリアレイB 128のn個のヒューズデバイス125のヒューズ状態が図1に示すサンプル/キャプチャ回路127によってサンプルおよびキャプチャされる。

【0057】

段階240で、デジタル論理回路145を使用して、ビット線バスA 134およびビット線バスB 138によって比較論理ブロック140に与えられたサンプルヒューズOTPメモリアレイ値が互いとおよびバージンチップまたはプログラムされていないOTPメモリアレイ値と比較される。一実施形態では、ゼロのサンプルアレイ値はバージンチップ値に対応する。いくつかの適用例では、「1」の値のすべてのnビットの場合、 $(2^n - 1)$ のサンプルnビットアレイ値はバージンチップ値に対応する。

【0058】

段階260で、障害の発生が判断され得る。ヒューズOTPメモリアレイA 124および/またはヒューズOTPメモリアレイB 128のサンプル値がバージンチップを示す場合(すなわち、様々な実施形態では、両方のアレイのすべてのn個のヒューズデバイス121および125について、すべて「1」またはすべて「0」のいずれか)、段階264で、障害が発生したと判断される。このバージンチップの場合、障害検出はフォールスポジティブである。ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128のサンプル値が同一でない場合、段階266で、障害が発生したと判断される。ヒューズOTPメモリアレイA 124およびヒューズOTPメモリアレイB 128のサンプル値が同一であり、バージンチップを示さない場合、段階268で、障害が発生しなかったと判断される。段階264、266、および268は相互排他的であるので、方法200の段階260でこれらの状態のうちの1つのみが存在し得る。

【0059】

加えて、段階260で、セキュリティ信号160が比較論理ブロック140によって生成され、その結果、セキュリティ信号160の指示は、たとえば、グリッチ攻撃、ハッカー攻撃、または他の物理的な外乱によって引き起こされた障害発生の判断によって決定される。障害が発生したと判断された場合に非セキュア動作モードのセキュリティ信号指示が生成され、障害が発生しなかったと判断された場合にセキュア動作モードのセキュリティ信号指示が生成される。

【0060】

段階270で、セキュリティ信号160の指示にかかわらず、同じ処理ルーチンを使用して、SoCが処理モジュール170によってブートされる。SoCは、非セキュア動作モードとセキュア動作モードの両方において、同じルーチンまたは手順に従ってブートすることができる。SoCのブートルーチンはセキュアメモリ188へのアクセスを必要としなくてもよい。例示的な実装形態では、SoC構成要素も段階270で試験され得る。試験ルーチンはセキュアメモリ188へのアクセスを必要としなくてもよい。試験ルーチンまたは手順は非セキュア動作モードとセキュア動作モードの両方で同じであり得る。

【0061】

段階280で、SoCはセキュリティ信号160の指示によって決定されたセキュアメモリ188へのアクセスによって動作する。非セキュア動作モードの場合、SoCはセキュアメモリ188へ

のブロックされたまたは制限されたアクセスによって動作し、それによって、セキュアメモリ188に記憶され得るプロビジョニングされたデータを保護する。逆に、セキュア動作モードの場合、SoCはセキュアメモリ188へのアクセスおよびセキュアメモリ188に記憶され得るプロビジョニングされたデータによって動作する。一実施形態では、セキュア動作モードでは、セキュアメモリへのアクセスおよびセキュアメモリに記憶された任意のプロビジョニングされたデータは、無制限であり得る。特定の実施形態では、セキュア動作モードでは、セキュアメモリへのアクセスおよびセキュアメモリに記憶された任意のプロビジョニングされたデータは、セキュリティ信号指示を除くパラメータに応答して制限され、ブロックされ、または他の方法で制御され得る。

【0062】

10

図1に関して上記で説明したように、ブートルーチンおよび試験ルーチンはセキュアメモリ188へのブロックされたアクセスによって影響され得ないので、バージンチップに関連付けられたフォールスポジティブの負の影響は軽減される。加えて、バージンチップのセキュアメモリ188はプロビジョニングされたデータを含まないことがあり、したがって、セキュアメモリ188へのアクセスがないことはバージンチップには無関係であり得る。

【0063】

一実施形態では、方法200はSoCが電源投入されるリセットされるたびに繰り返すことができる。

【0064】

図1をさらに参照すると、一実施形態では、OTPメモリアレイブロック120は、複数のM個のヒューズOTPメモリアレイおよび関連するサンプル/キャプチャ回路を含むことができ、Mは2よりも大きいかまたはそれに等しい整数である。M個のヒューズOTPメモリアレイの各ヒューズOTPメモリアレイはn個のヒューズデバイスを含むことができ、nは1よりも大きいかまたはそれに等しい整数であり、すべてのM個のヒューズOTPメモリアレイに対して同じ値を有する。特定の適用例では、OTPメモリアレイブロック120は、アンチヒューズOTPデバイスまたは任意の他のタイプのOTPデバイスを利用するM個のOTPメモリアレイを含むことができる。

20

【0065】

一実施形態では、OTPメモリアレイブロック120は、M個のビット線バスを介して比較論理ブロック140に結合され得る。各ビット線バスはM個のOTPメモリアレイのうちの1つからn個の信号を搬送することができる。

30

【0066】

一実施形態では、比較論理ブロック140のデジタル論理回路145は、M個のヒューズOTPメモリアレイの各々のサンプル値をプログラムされていないバージンチップアレイ値とおおよび残りの(M-1)個のヒューズOTPメモリアレイの各々と比較することができる。図1を参照して上記で説明したように、この比較に基づいて、比較論理ブロック140は障害が発生したかどうかを判断することができる。

【0067】

一実施形態では、比較論理ブロック140は、M個のヒューズOTPメモリアレイのサンプル値が同一であり、バージンチップ値に等しくない場合に、障害が発生しなかったと判断することができる。電子システムまたはエンドデバイスの製造中に、同一のセキュリティシーケンスがすべてのM個のヒューズOTPメモリアレイにプログラムされ得る。障害がない場合、M個のヒューズOTPメモリアレイのサンプル値はすべて、プログラムされたセキュリティシーケンスに等しくなり得る。

40

【0068】

いくつかの実装形態では、各アレイのプログラムされていないバージンチップ値はゼロであり得る。この場合、M個のヒューズOTPメモリアレイの各々のサンプル値はデジタル論理回路145によってゼロと比較され得る。他の例示的な実装形態では、各アレイのプログラムされていないバージンチップ値は $(2^n - 1)$ であり得る。そのような実装形態では、M個のヒューズOTPメモリアレイの各々のサンプル値は $(2^n - 1)$ と比較され得る。

50

【0069】

一実施形態では、比較論理ブロック140は、すべてのM個のヒューズOTPメモリアレイのサンプル値が同一でないすなわち等しくない場合、またはM個のヒューズOTPメモリアレイのうちの少なくとも1つのサンプル値がゼロに等しい場合に、障害が発生したと判断することができる。この後者の場合はバージンチップに対応し得る。上記で説明したように、障害が発生した場合、M個のヒューズOTPメモリアレイのいずれかまたはすべてのサンプル値がスプーフィングされる可能性があり、したがって、同一でもなく、プログラムされたセキュリティシーケンスに等しくもない可能性がある。

【0070】

一実装形態では、比較論理ブロック140は、M個のヒューズOTPメモリアレイのサンプル値が同一でない場合、またはM個のヒューズOTPメモリアレイのうちの少なくとも1つのサンプル値が $(2^n - 1)$ に等しい場合に、障害が発生したと判断することができる。この後者の場合はプログラムされていないバージンチップに対応し得る。

【0071】

動作時、図1をさらに参照しながら図3を参照すると、ハードウェア組込み型セキュリティ方法300は図示された段階を含んでいる。しかしながら、方法300は例示的なものにすぎず、限定的なものではない。方法300は、たとえば、段階を追加する、削除する、または、並べ替えることによって変更され得る。

【0072】

複数のM個のヒューズOTPメモリアレイおよび関連するサンプル/キャプチャ回路を含む(Mは2よりも大きいまたはそれに等しい整数である)上記で説明したシステム100の一実施形態を使用してSoCチップでの障害の発生を識別するための方法実施形態300は、方法200に類似し得るが、方法200に依存しなくてもよい。

【0073】

方法300は、M個のヒューズOTPメモリアレイの値をサンプルすること320、各ヒューズOTPメモリアレイのサンプル値を他の各ヒューズOTPメモリアレイのサンプル値と比較すること340、障害の発生を判断すること360、SoCをブートすること370、およびSoCを動作させること380を含む。

【0074】

段階320で、SoCが電源投入されるリセットされるときに、OTPメモリアレイブロック120内のM個のヒューズOTPメモリアレイのn個のヒューズデバイス状態がサンプルおよびキャプチャされ得る。

【0075】

一実施形態では、段階340で、デジタル論理回路145を使用して、M個のビット線バスによって比較論理ブロック140に与えられたサンプルヒューズOTPメモリアレイ値が互いと、およびプログラムされていないバージンチップOTPメモリアレイ値と比較される。

【0076】

一実施形態では、段階360で、障害の発生が判断される。M個のヒューズOTPメモリアレイのうちの少なくとも1つのサンプル値がバージンチップを示す場合(すなわち、様々な実施形態では、ゼロのアレイ値または $(2^n - 1)$ のアレイ値のいずれか)、段階364で、障害が発生したと判断される。バージンチップの場合、障害検出はフォールスポジティブである。M個のヒューズOTPメモリアレイのサンプル値が同一ではなく、バージンチップ値に等しくない場合、段階366で、障害が発生したと判断される。M個のヒューズOTPメモリアレイのサンプル値が同一であり、バージンチップを示さない場合、段階368で、障害が発生しなかったと判断される。段階364、366、および368は相互排他的であるので、方法実施形態300の段階360でこれらの状態のうちの1つのみが存在し得る。

【0077】

M個のヒューズOTPメモリアレイを利用する方法実施形態300では、段階370および380は、それぞれ図2に示す方法200の段階270および280に関して上記で説明したように進む。

【0078】

他の実施形態は、本発明の範囲および趣旨の範囲内である。たとえば、ソフトウェアの性質により、上記で説明した機能は、ソフトウェア、ハードウェア、ファームウェア、ハードワイヤリング、またはこれらの任意の組合せを使用して実装され得る。機能を実装する機構はまた、機能の一部が異なる物理的ロケーションで実装されるように分散された状態を含む、様々な位置に物理的に位置していてもよい。

【0079】

情報および信号は、様々な異なる技術および技法のいずれかを使用して表され得ることが、当業者には理解されよう。たとえば、上記の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁界もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表され得る。

10

【0080】

さらに、本明細書の開示に関して説明した様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることが、当業者には理解されよう。ハードウェアおよびソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップを、概してそれらの機能に関して上記で説明した。そのような機能がハードウェアとして実装されるか、またはソフトウェアとして実装されるかは、具体的な適用例および全体的なシステムに課される設計制約に依存する。当業者は、説明した機能を具体的な適用例ごとに様々な方法で実装し得るが、そのような実装の決定は、本開示の範囲からの逸脱をもたらすものと解釈されるべきではない。

20

【0081】

本明細書の開示に関して説明した様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明した機能を実施するように設計されたそれらの任意の組合せを用いて実装あるいは実施され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であり得る。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPおよびマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装され得る。

30

【0082】

本明細書の開示に関して説明する方法またはアルゴリズムのステップは、直接ハードウェアで実施されるか、プロセッサによって実行されるソフトウェアモジュールで実施されるか、またはその2つの組合せで実施され得る。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体に存在し得る。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替として、記憶媒体はプロセッサと一体であり得る。プロセッサおよび記憶媒体はASIC内に存在し得る。ASICはユーザ端末内に存在し得る。代替として、プロセッサおよび記憶媒体は、ユーザ端末内に個別構成要素として存在し得る。

40

【0083】

1つまたは複数の例示的な設計では、説明した機能は、ハードウェア、ソフトウェア、ファームウェア、または任意のそれらの組合せで実装され得る。機能は、ソフトウェアで実装される場合、1つもしくは複数の命令またはコードとしてコンピュータ可読媒体上に記憶され、あるいはコンピュータ可読媒体を介して送信され得る。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を可能にする任意の媒体を

50

含む、コンピュータ記憶媒体と通信媒体の両方を含む。記憶媒体は、ある場所から別の場所へのコンピュータプログラムの転送を可能にする任意の媒体を含む。記憶媒体は、汎用または専用コンピュータによってアクセスできる任意の利用可能な媒体とすることができる。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または、命令またはデータ構造の形態の所望のプログラムコード手段を搬送または記憶するために使用され得、汎用もしくは専用コンピュータまたは汎用もしくは専用プロセッサによってアクセスされ得る、任意の他の媒体を含み得る。また、任意の接続はコンピュータ可読媒体と適切に呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用する場合、ディスク(disk)およびディスク(disc)は、コンパクトディスク(CD)、レーザーディスク(登録商標)、光ディスク、デジタル多用途ディスク(DVD)、フロッピー(登録商標)ディスク、およびブルーレイディスクを含み、ディスク(disk)は、通常、磁氣的にデータを再生するが、ディスク(disc)は、レーザーで光学的にデータを再生する。上記の組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。

10

【0084】

20

本開示の前述の説明は、任意の当業者が本開示を作成または使用できるように提供されている。本開示への様々な修正が当業者には容易に明らかになり、本明細書で定義する一般原理は、本開示の範囲を逸脱することなく他の変形形態に適用され得る。したがって、本開示は、本明細書で説明する例および設計に限定されるものではなく、本明細書で開示する原理および新規の特徴に一致する最大の範囲を与えられるものである。

【0085】

さらに、上記の説明は本発明を指すが、この説明は2つ以上の発明を含み得る。

【0086】

特許請求の範囲を含め、本明細書で使用する場合、特に明記しない限り、機能または動作が項目または条件「に基づく」という文言は、機能または動作が述べられた項目または条件に基づくこと、また、述べられた項目または条件に加えて1つまたは複数の項目および/または条件に基づき得ることを意味する。

30

【符号の説明】**【0087】**

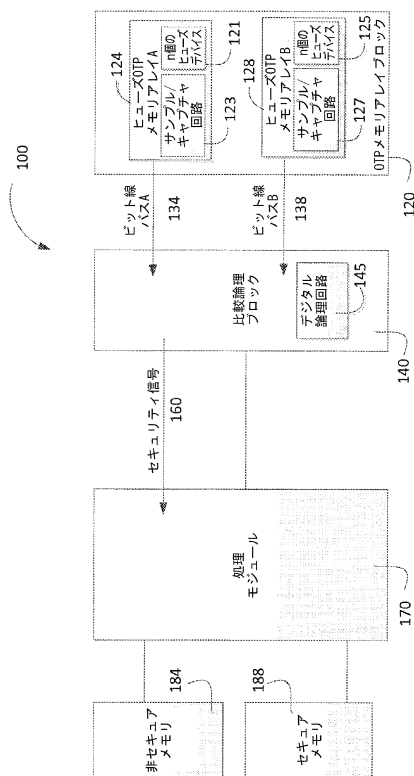
- 100 システム
- 120 OTPメモリアレイブロック
- 121 n個のヒューズデバイス
- 123 サンプル/キャプチャ回路
- 124 ヒューズOTPメモリアレイA
- 125 n個のヒューズデバイス
- 127 サンプル/キャプチャ回路
- 128 ヒューズOTPメモリアレイB
- 134 ビット線バスA
- 138 ビット線バスB
- 140 比較論理ブロック
- 145 デジタル論理回路
- 160 セキュリティ信号
- 170 処理モジュール
- 184 非セキュアメモリ
- 188 セキュアメモリ

40

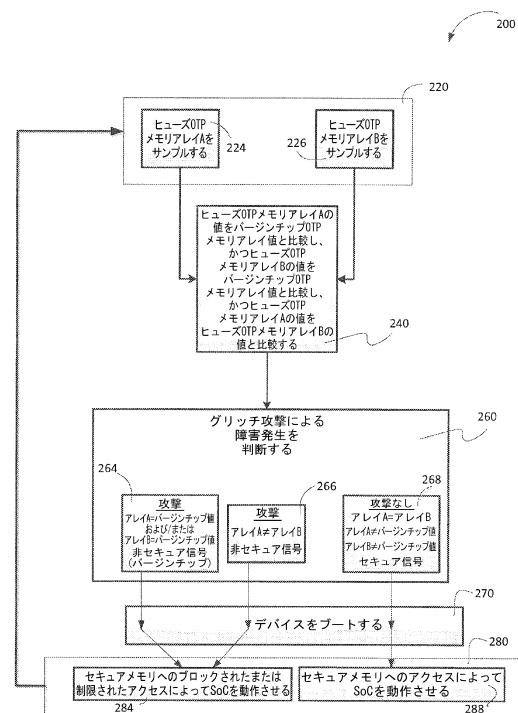
50

200 方法
300 方法

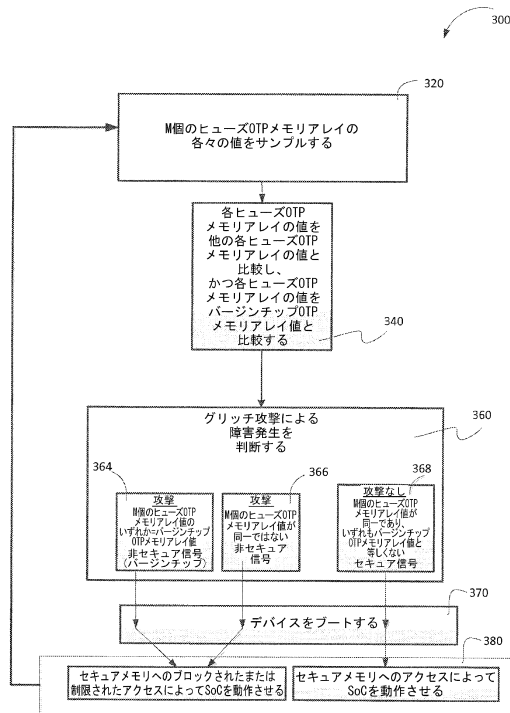
【図 1】



【図 2】



【図 3】



フロントページの続き

- (56)参考文献 米国特許第09262259 (US, B1)
米国特許第07398554 (US, B1)
米国特許第06944083 (US, B1)
米国特許出願公開第2014/0140162 (US, A1)
特開平05-189987 (JP, A)
特開2003-263618 (JP, A)
米国特許出願公開第2010/0250943 (US, A1)
特開2011-204319 (JP, A)
特開2011-210316 (JP, A)
特開昭61-211754 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
G06F12/14, 21/00, 11/28, 11/30
G11C17/00
G09K19/00