(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6515100号
(P6515100)

(45)発行日　令和1年5月15日(2019.5.15)　(24)登録日　平成31年4月19日(2019.4.19)

(51)Int.Cl.　F I
H04L 9/10 (2006.01)　H04L 9/00 621Z
G06F 21/44 (2013.01)　G06F 21/44

請求項の数 15　(全 25 頁)

(21)出願番号　特願2016-536383(P2016-536383)
(86)(22)出願日　平成26年8月19日(2014.8.19)
(65)公表番号　特表2016-531515(P2016-531515A)
(43)公表日　平成28年10月6日(2016.10.6)
(86)国際出願番号　PCT/US2014/051718
(87)国際公開番号　WO2015/026838
(87)国際公開日　平成27年2月26日(2015.2.26)
審査請求日　平成29年7月26日(2017.7.26)
(31)優先権主張番号　13/975,082
(32)優先日　平成25年8月23日(2013.8.23)
(33)優先権主張国　米国(US)

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　シュウ・グオ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】侵襲的なクローンアタックに抵抗するためのメモリベースＰＵＦのマスキング演算への回路遅延ベース物理的クローン化不能関数（ＰＵＦ）の適用

(57)【特許請求の範囲】
【請求項１】
電子デバイスによって使用可能な方法であって、
前記電子デバイス内の複数のメモリセルを使用して第1の物理的クローン化不能関数を実施するステップと、
前記電子デバイス内の複数の回路遅延ベースパスを使用して第2の物理的クローン化不能関数を実施するステップと、
外部サーバからチャレンジを受け取るステップと、
第2のレスポンスを取得するために、前記第1の物理的クローン化不能関数にチャレンジ入力を適用するとともに、前記第2の物理的クローン化不能関数からの第1のレスポンスを使用するステップであって、前記第1のレスポンスが、
(a)前記チャレンジ入力を取得するために前記外部サーバからの前記チャレンジをマスキングすること、または
(b)前記第2のレスポンスを取得するために前記第1の物理的クローン化不能関数からのレスポンス出力をマスキングすることであって、前記外部サーバからの前記チャレンジが前記チャレンジ入力として使用される、ことのいずれかのために使用される、ステップと、
前記第1の物理的クローン化不能関数からの前記第2のレスポンスを前記外部サーバに送るステップとを含む方法。
【請求項２】

前記第1の物理的クローン化不能関数は、1つまたは複数のメモリセルに関する未初期化メモリセル状態を使用する、請求項1に記載の方法。

【請求項３】

前記複数の回路遅延ベースパスは、リング発振器であり、前記第2の物理的クローン化不能関数は、前記複数のリング発振器から2つのリング発振器を選択し前記2つのリング発振器間の周波数差分によって応答する第2のチャレンジを受け取る、請求項1に記載の方法。

【請求項４】

前記チャレンジは、前記第1の物理的クローン化不能関数に関する第1のチャレンジと、前記第2の物理的クローン化不能関数に関する第2のチャレンジとを含む、請求項1に記載の方法。

【請求項５】

前記第1のチャレンジは、前記第2のチャレンジへの予期されるレスポンスによってマスキングされたチャレンジである、請求項4に記載の方法。

【請求項６】

前記第1のチャレンジは、前記第1の物理的クローン化不能関数によって処理される前に前記第2の物理的クローン化不能関数からの前記第1のレスポンスによって修正される、請求項4に記載の方法。

【請求項７】

前記チャレンジは、前記第1の物理的クローン化不能関数に関する第1のチャレンジと、前記第2の物理的クローン化不能関数に関する第2のチャレンジとを含み、前記第2のチャレンジが第2の物理的クローン化不能関数によって使用されて前記第1のレスポンスが生成され、前記第1のレスポンスを使用して前記第1の物理的クローン化不能関数からの前記第2のレスポンスがマスキングされる、請求項1に記載の方法。

【請求項８】

前記第2の物理的クローン化不能関数からの前記第1のレスポンスをハッシングして中間レスポンスを得るステップと、

前記中間レスポンスを使用して前記第2のレスポンスをマスキングするステップとをさらに含む、請求項7に記載の方法。

【請求項９】

事前記憶されたデバイス識別子を、

(a)前記チャレンジが受け取られる前または

(b)前記第2のレスポンスを送るのと同時のいずれかのときに、前記電子デバイスから前記外部サーバに送ることをさらに含み、

前記デバイス識別子は前記電子デバイスを一意に識別する、請求項1に記載の方法。

【請求項１０】

電子デバイスであって、

第1の物理的クローン化不能関数として働く前記電子デバイス内の複数のメモリセルと、

第2の物理的クローン化不能関数を実施する前記電子デバイス内の複数の回路遅延ベースパスと、

外部サーバからチャレンジを受け取るための通信インターフェースと、

前記通信インターフェース、前記複数のメモリセル、および前記複数の回路遅延ベースパスに結合された処理回路であって、第2のレスポンスを取得するために、前記第1の物理的クローン化不能関数にチャレンジ入力を適用するとともに、前記第2の物理的クローン化不能関数からの第1のレスポンスを使用し、前記第1のレスポンスが、

(a)前記チャレンジ入力を取得するために前記外部サーバからの前記チャレンジをマスキングすること、または

(b)前記第1の物理的クローン化不能関数からのレスポンス出力をマスキングして、前記第2のレスポンスを取得することであって、前記外部サーバからの前記チャレンジが前

記チャレンジ入力として使用される、ことのいずれかのために使用される、処理回路とを備え、
前記通信インターフェースは、前記第1の物理的クローン化不能関数から前記外部サーバに前記第2のレスポンスを送るように構成される電子デバイス。
【請求項１１】
前記チャレンジは、前記第1の物理的クローン化不能関数に関する第1のチャレンジと、前記第2の物理的クローン化不能関数に関する第2のチャレンジとを含み、前記第1のチャレンジは、前記第2のチャレンジへの予期されるレスポンスによってマスキングされたチャレンジである、請求項10に記載の電子デバイス。
【請求項１２】
前記チャレンジは、前記第1の物理的クローン化不能関数に関する第1のチャレンジと、前記第2の物理的クローン化不能関数に関する第2のチャレンジとを含み、前記第1のチャレンジは、前記第1の物理的クローン化不能関数によって処理される前に前記第2の物理的クローン化不能関数からの前記第1のレスポンスによって修正される、請求項10に記載の電子デバイス。
【請求項１３】
前記チャレンジは、前記第1の物理的クローン化不能関数に関する第1のチャレンジと、前記第2の物理的クローン化不能関数に関する第2のチャレンジとを含み、前記第2のチャレンジが第2の物理的クローン化不能関数によって使用されて前記第1のレスポンスが生成され、前記第1のレスポンスを使用して前記第1の物理的クローン化不能関数からの前記第2のレスポンスがマスキングされる、請求項10に記載の電子デバイス。
【請求項１４】
前記処理回路は、
前記第2の物理的クローン化不能関数からの前記第1のレスポンスをハッシングして中間レスポンスを得ることと、
前記中間レスポンスを使用して前記第2のレスポンスをマスキングすることとを行うようにさらに構成される、請求項10に記載の電子デバイス。
【請求項１５】
1つまたは複数の命令が記憶された非一時的機械可読記憶媒体であって、前記命令は、請求項１０に記載の電子デバイス内の少なくとも1つの処理回路によって実行されたときに、少なくとも1つの処理回路に、請求項１から９のいずれか一項に記載の方法を実行させる、非一時的機械可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、物理的クローン化不能関数(PUF)を使用してメモリデバイスまたはそのようなメモリデバイスが組み込まれたデバイスを一意に識別することに関する。
【背景技術】
【０００２】
物理的クローン化不能関数(PUF)は、物理的な構成要素の固有のばらつきに基づいてハードウェアデバイスを一意に識別する機構を実現する。たとえば、複数のチップを製造する際、複雑な半導体製造プロセスによって、設計者の制御を超えたわずかなばらつきが導入される。たとえば、2つのチップが同じシリコンウェハから製造された場合でも、同一に設計された電気経路はおそらく、幅が数ナノメートル異なり、シリコンの表面における微視的な差によって、線の湾曲にごくわずかのばらつきが誘発される。これらの一意の特性は制御不能でかつ物理的デバイスに特有の特性であるので、これらの特性を定量化すると固有の識別子を生成することができる。リング発振器ベースPUF、アービタPUF、およびパス遅延分析ベースPUFなど、シリコンによる回路遅延のばらつきの調査および分析に基づいていくつかの異なる種類のPUFが提案されている。
【０００３】

あるPUFは、スタティックランダムアクセスメモリ(SRAM)の未初期化電源投入状態を利用して識別用の「フィンガープリント」を生成する。しかし、SRAM PUFは、クローン化アタックを受けやすい。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

したがって、現行のSRAM PUF設計のセキュリティを向上させてクローン化アタックおよび侵襲的なアタック全般に抵抗する必要がある。

【課題を解決するための手段】

【０００５】

クローン化アタックに抵抗しつつ一意に識別され得る電子デバイス(たとえば、プロセッサ、処理回路、メモリ、プログラマブル論理アレイ、チップ、半導体、メモリなど)が提供される。電子デバイスは、第1の物理的クローン化不能関数(PUF)として働く複数のメモリセルを電子デバイス内に含んでもよい。一例では、第1の物理的クローン化不能関数は、チャレンジに対するレスポンスとして、1つまたは複数のメモリセルに関する未初期化メモリセル状態を利用する。さらに、電子デバイス内の複数の回路遅延ベースパスは、第2の物理的クローン化不能関数を実施してもよい。一例では、複数の回路遅延ベースパスは、リング発振器であってもよく、第2の物理的クローン化不能関数は、複数のリング発振器から2つのリング発振器を選択し、2つのリング発振器間の周波数差分によって応答するチャレンジを受け取ってもよい。

【０００６】

通信インターフェースは、外部サーバからチャレンジを受け取る働きをしてもよい。処理回路が通信インターフェース、複数のメモリセル、および複数の回路遅延ベースパスに結合されてもよく、処理回路は、第2の物理的クローン化不能関数からの第1のレスポンスを使用して、(a)第1の物理的クローン化不能関数へのチャレンジ入力をマスキング/アンマスキングすること、(b)第1の物理的クローン化不能関数へのチャレンジ入力を生成すること、または(c)第1の物理的クローン化不能関数からのレスポンス出力をマスキングすることのいずれかを行うことによって第1の物理的クローン化不能関数にチャレンジを適用するように構成される。通信インターフェースは、第1の物理的クローン化不能関数から外部サーバに第2のレスポンスを送るように構成されてもよい。さらに、第1のレスポンスは、第2の物理的クローン化不能関数から外部サーバに送られてもよい。一例では、外部サーバは、第1の物理的クローン化不能関数に関するチャレンジおよびレスポンスの第1のデータベースと第2の物理的クローン化不能関数に関するチャレンジおよびレスポンスの第2のデータベースとを含んでもよく、外部サーバは、チャレンジを電子デバイスに送り、第2のレスポンスに基づいて電子デバイスを認証または識別する。

【０００７】

一例では、チャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと、第2の物理的クローン化不能関数に関する第2のチャレンジとを含んでもよい。一実装形態では、第1のチャレンジは、第2のチャレンジへの予期されるレスポンスによってマスキングされたチャレンジであってもよい。別の実装形態では、第1のチャレンジは、第1の物理的クローン化不能関数によって処理される前に第2の物理的クローン化不能関数からの第1のレスポンスによって修正されてもよい。

【０００８】

別の例では、受け取ったチャレンジが第2の物理的クローン化不能関数によって使用されて第1のレスポンスが生成され、次に、第1のレスポンスが第1の物理的クローン化不能関数によって第2のチャレンジとして使用されて第2のレスポンスが生成されてもよい。

【０００９】

さらに別の例では、チャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと、第2の物理的クローン化不能関数に関する第2のチャレンジとを含んでもよく、第2のチャレンジが第2の物理的クローン化不能関数によって使用されて第1のレスポンス

が生成され、第1のレスポンスを使用して第1の物理的クローン化不能関数からの第2のレスポンスがマスキングされる。第2の物理的クローン化不能関数からの第1のレスポンスはハッシングされて中間レスポンスが得られる。第2のレスポンスは次いで、中間レスポンスを使用してマスキングされる。

【００１０】

他の例では、チャレンジは、電子デバイスの認証プロセス、電子デバイスの識別プロセス、および/または電子デバイス内のキー生成プロセスのうちの少なくとも1つの一部として受け取られてもよい。

【００１１】

いくつかの実装形態では、電子デバイスは、すでに展開前段階または製造段階中に1つまたは複数のチャレンジを受け取っており、1つまたは複数の対応するレスポンスを(たとえば、データコレクタに)供給している。

【００１２】

さらに、事前に記憶されたデバイス識別子が、(a)チャレンジが受け取られる前または(b)第2のレスポンスを送るのと同時のいずれかのときに電子デバイスから外部サーバに送られてもよく、デバイス識別子は電子デバイスを一意に識別する。

【００１３】

電子デバイスの展開前段階または製造段階中に電子デバイスに関連するデバイス識別子を得る(たとえば、受け取るかまたは割り当てる)データコレクタデバイスも設けられる。データコレクタデバイスは次いで、1つまたは複数のチャレンジを生成して電子デバイスに送ってもよい。その結果、データコレクタデバイスは、電子デバイスから1つまたは複数のレスポンスを受け取ってもよく、1つまたは複数のレスポンスは、電子デバイスにおいて2つ以上の異なる種類の物理的クローン化不能関数から生成される特性情報を含む。デバイス識別子、チャレンジ、および対応するレスポンスは、後で電子デバイスを認証できるように記憶される。このプロセスは、複数の電子デバイスの各々について繰り返されてもよい。電子デバイスに送られるチャレンジがすべてのデバイスについて同じであってもよく、電子デバイスごとに無作為に生成されてもよく、ならびに/あるいはあり得るチャレンジのサブセットであってもよいことに留意されたい。

【００１４】

同様に、様々な種類の物理的クローン化不能関数からのレスポンスに基づいて電子デバイスを認証する認証デバイスが設けられる。認証デバイスは、電子デバイスに関連するデバイス識別子を受け取る。認証デバイスは次いで、1つまたは複数のチャレンジを電子デバイスに送る。それに応答して、認証デバイスは、電子デバイスから1つまたは複数のレスポンスを受け取り、1つまたは複数のレスポンスは、電子デバイスにおいて2つ以上の異なる種類の物理的クローン化不能関数から生成される特性情報を含む。電子デバイスに固有の事前に記憶されたレスポンスは、電子デバイス識別子を使用して識別されてもよい。電子デバイスは次いで、電子デバイスに関する事前に記憶されたレスポンスと受け取った1つまたは複数のレスポンスを比較することによって認証されてもよい。チャレンジは、電子デバイスから事前にレスポンスが得られた複数のチャレンジから選択されてもよい。事前に記憶されたレスポンスは、電子デバイスの製造段階または展開前段階において得られていてもよい。デバイス識別子は、1つまたは複数のチャレンジを送る前に受け取られていてもよい。デバイス識別子は、1つまたは複数のレスポンスを受け取るのとともに受け取られていてもよい。

【００１５】

チャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと、第2の物理的クローン化不能関数に関する第2のチャレンジとを含んでもよい。第1のチャレンジは、第2のチャレンジへの予期されるレスポンスによってマスキングされたチャレンジであってもよい。1つまたは複数のチャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと第2の物理的クローン化不能関数に関する第2のチャレンジとを含んでもよく、1つまたは複数のレスポンスは、第1の物理的クローン化不能関数からの第1のレス

ポンスと第2の物理的クローン化不能関数からの第2のレスポンスとを含み、電子デバイスは、第1のレスポンスが第1のチャレンジに対応する事前に記憶された第1のレスポンスと一致し、第2のレスポンスが第2のチャレンジに対応する事前に記憶された第2のレスポンスと一致する場合に首尾よく認証される。

【００１６】

1つまたは複数のチャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと第2の物理的クローン化不能関数に関する第2のチャレンジとを含み、1つまたは複数のレスポンスは、第1の物理的クローン化不能関数からの第1のレスポンスと第2の物理的クローン化不能関数からの第2のレスポンスとを含む。さらに、第1のチャレンジを第2のレスポンスによってアンマスキングすることによって中間チャレンジが得られてもよい。受け取った第1のレスポンスは、中間チャレンジに関連する事前に記憶されたレスポンスと比較されてもよい。

【００１７】

さらに別の例では、1つまたは複数のチャレンジは、第2の物理的クローン化不能関数に関する第1のチャレンジを含み、1つまたは複数のレスポンスは、第1の物理的クローン化不能関数からの第1のレスポンスを含む。第1のチャレンジに対応する事前に記憶された中間レスポンスを取り込むことによって中間チャレンジを得ることができる。受け取った第1のレスポンスは、中間チャレンジに対応する事前に記憶された中間レスポンスと比較されてもよい。

【００１８】

さらに別の例では、1つまたは複数のチャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと第2の物理的クローン化不能関数に関する第2のチャレンジとを含み、1つまたは複数のレスポンスは第1のレスポンスを含む。第2のチャレンジに対応する事前に記憶された第2のレスポンスによって第1のレスポンスをアンマスキングすることによって中間レスポンスを得ることができる。中間レスポンスは、第1のチャレンジに関連する事前に記憶されたレスポンスと比較される。

【図面の簡単な説明】

【００１９】

【図１】SRAM PUFおよび回路遅延ベースPUFに基づいてメモリデバイスに関するレスポンスの一意のマッピングを生成する例示的な方法を示すブロック図である。

【図２】SRAM PUFおよび回路遅延ベースPUFを組み合わせるメモリデバイスに関する事前に得られた特徴的なレスポンスを使用して特定のメモリデバイスを検証または識別する例示的な方法を示すブロック図である。

【図３】攻撃者がメモリデバイスをクローン化できないようにするにはSRAM PUFと回路遅延PUFをどのように組み合わせたらよいかについての第1の例を示すブロック図である。

【図４】攻撃者がメモリデバイスをクローン化できないようにするにはSRAM PUFと回路遅延PUFをどのように組み合わせたらよいかについての第2の例を示すブロック図である。

【図５】攻撃者がメモリデバイスをクローン化できないようにするにはSRAM PUFと回路遅延PUFをどのように組み合わせたらよいかについての第3の例を示すブロック図である。

【図６】攻撃者がメモリデバイスをクローン化できないようにするにはSRAM PUFとRO PUFをどのように組み合わせたらよいかについての第4の例を示すブロック図である。

【図７】一例によるデータコレクタデバイスを示すブロック図である。

【図８】電子デバイスから特性情報を得るためのデータコレクタデバイスにおいて使用可能な方法を示す図である。

【図９】各電子デバイス内の複数の物理的クローン化不能関数からのレスポンスに基づいて電子デバイスを認証するように構成された例示的な認証デバイスを示すブロック図である。

【図１０】複数の物理的クローン化不能関数からのレスポンスに基づいて電子デバイスを認証するための認証デバイスにおいて使用可能な方法を示す図である。

【図１１】複数の物理的クローン化不能関数を有する例示的な電子デバイスを示すブロッ

ク図である。
【図１２】複数の物理的クローン化不能関数からのレスポンスに基づいて認証デバイスによって電子デバイス自体を認証するための電子デバイスにおいて使用可能な方法を示す図である。
【発明を実施するための形態】
【００２０】
以下の説明では、本開示の様々な態様の完全な理解をもたらすために具体的な詳細が与えられる。しかしながら、態様はこれらの具体的な詳細を伴わずに実践され得ることが当業者によって理解されるであろう。たとえば、態様が不要な詳細で不明瞭になることを回避するために、回路はブロック図で示されることがある。他の場合には、本開示の態様を不明瞭にしないために、よく知られている回路、構造、および技法は、詳細に示されないことがある。
【００２１】
「例示的」という用語は、本明細書では「一例、事例、または実例として役立つ」ことを意味するように使用される。「例示的」として本明細書に記載の任意の実装形態または態様は、必ずしも本開示の他の態様よりも好ましいまたは有利であると解釈されるべきではない。同様に、「諸態様」という用語は、本開示のすべての態様が、議論される特徴、利点、または動作のモードを含むことを必要としない。
【００２２】
概要
一特徴は、スタティックランダムアクセスメモリ(SRAM) PUFと回路遅延ベースPUF(たとえば、リング発振器(RO)PUF、アービタPUFなど)を組み合わせることによって一意の識別子を生成するのを可能にする。それ自体によるSRAM PUFは、障害解析ツール(たとえば、集束イオンビーム(FIB))を使用するクローン化アタックを受けることがある。したがって、回路遅延ベースPUFを使用してSRAM PUFへのチャレンジおよび/またはSRAM PUFからのレスポンスを隠し、それによって攻撃者がメモリデバイスのレスポンスをクローン化できないようにしてもよい。
【００２３】
SRAM物理的クローン化不能関数(PUF)と回路遅延ベース物理的クローン化不能関数(PUF)の組合せ
物理的クローン化不能関数(PUF)は、回路内の製造プロセスばらつきを利用して一意の識別子を得るチャレンジ-レスポンス機構である。一例では、チャレンジとそれに対応するレスポンスとの間の関係は、回路(たとえば、集積回路)内の論理構成要素および配線の複雑な統計量的ばらつきによって決定される。2種類のPUFには、たとえば、SRAM PUFおよび回路遅延PUF(たとえば、リング発振器PUF)が含まれる。
【００２４】
SRAM PUFは、スタティックランダムアクセスメモリ(SRAM)の未初期化電源投入状態を利用して、メモリデバイスまたはメモリデバイスが組み込まれた電子デバイスに関する識別用「フィンガープリント」を生成する。SRAMセル設計は対称性を有するが、製造プロセスばらつきによってSRAMセル間にわずかな非対称性が生じ、立ち上げ時に優先/偏り状態(0または1)が生じる。未初期化SRAMセルのこの優先または偏りを使用してメモリデバイスを一意に識別してもよい。
【００２５】
しかし、集束イオンビーム(FIB)を使用する障害解析アタックにおける最近の高度化によって、メモリベースPUFのセキュリティが脅かされている。回路編集アタックは、元のデバイスに対する同一のSRAM PUFレスポンスを有するハードウェアクローンを生成することができる。
【００２６】
回路遅延ベースPUFは、製作/製造上の欠陥によって生じる発振回路間の体系的なばらつきを利用する。製作/製造プロセスは回路遅延ベースPUFにおけるそのようなばらつきを回

避しようとするが、そのようなばらつきは常にある程度存在し、デバイス./チップを識別するうえで実際に有用である。回路遅延ベースPUFの一例では、複数のリング発振器が併用されてもよく、少なくとも2つのリング発振器の出力が1つまたは複数のスイッチ(マルチプレクサ)に送られる。チャレンジは、リング発振器への入力として働くことができ(たとえば、チャレンジは2つのリング発振器を選択する働きをし)、2つの選択されたリング発振器204からの出力は、第1の周波数および第2の周波数として表される。選択されるリング発振器間の違いに起因して、リング発振器の周波数が異なる(すなわち、周波数差分が生じる)。RO PUF出力(レスポンス)は、リング発振器周波数を対ごとに比較することによって作成される(たとえば、第1と第2の周波数の差)。

【００２７】

しかし、サイズ変更可能な回路遅延ベースPUFを実装すると、集積回路内の必要な空間として広い空間が占有される。

【００２８】

一特徴によれば、SRAM PUFと回路遅延ベースPUFが、SRAM PUFのセキュリティを強化するように電子デバイス(たとえば、メモリデバイス、半導体デバイスなど)内で組み合わされる。

【００２９】

図1は、SRAM PUFおよび回路遅延ベースPUF、たとえば、リング発振器(RO)PUFに基づいてメモリデバイスに関するレスポンスの一意のマッピングを生成する例示的な方法を示すブロック図である。このブロック図は、SRAM PUF 105と回路遅延PUF 122(たとえば、リング発振器バンクとして実装される)とを備えるメモリデバイス102(たとえば、チップ、半導体デバイスなど)に関するチャレンジ/レスポンス特性を問い合わせて収集するプロセスを示す。

【００３０】

一例では、SRAM PUFは、メモリデバイス102のSRAMセルのすべてによって実装されてもまたはその一部によって実装されてもよい。特に、SRAM PUF 105は、SRAM 106の未初期化メモリセル104における偏りを利用する。たとえば、製造段階中に、チャレンジ110(たとえば、メモリアドレス)ごとに、対応するレスポンス112(たとえば、論理0または1)が得られるように、未初期化SRAM 106が問合せを受けてもよい。たとえば、SRAM 106内のメモリアドレスごとに、そのメモリアドレスに関連するメモリセル104の未初期化値/状態が得られる。複数のチャレンジ110に関して、複数のレスポンス112が得られる。他の手法では、メモリアドレスのサブセットのみが問合せを受けてもよい。このようにして、未初期化値のアドレスへのマッピングが、SRAM 106に関して構成され、データベース114に(たとえば、チャレンジおよび対応するレスポンスとして)記憶されてもよい。すなわち、SRAM PUFチャレンジ/レスポンスのデータベース114が、たとえば、製造プロセスまたは品質管理プロセス中にメモリデバイス(チップ)ごとに構成されてもよい。たとえば、デバイスAの場合、チャレンジ/レスポンスの第1の組$[C_0R_0,C_1R_1,..,C_iR_i]$が得られ、デバイスBの場合、チャレンジ/レスポンスの第2の組$[C_0R_0,C_1R_1,..,C_iR_i]$が得られ、デバイスCの場合、チャレンジ/レスポンスの第3の組$[C_0R_0,C_1R_1,..,C_iR_i]$が得られる。いくつかの実装形態では、すべてのデバイスに関するチャレンジ$[C_0,C_1,..,C_i]$が同じであってもよいが、レスポンスはそれぞれ異なることに留意されたい。他の実装形態では、デバイスごとのチャレンジ$[C_0,C_1,..,C_i]$が無作為に選択されてもよく、したがって、様々なデバイスがそれぞれに異なるチャレンジを受け取る。

【００３１】

一例では、回路遅延PUF 120は、複数のリング発振器123およびその周波数変動を利用して一意のシグネチャ/レスポンスを生成するリング発振器(RO)PUF 122として実装されてもよい。たとえば、所与のチャレンジ124に関して(たとえば、2つのリング発振器入力/出力の選択)、対応するレスポンス(たとえば、2つの選択されたリング発振器間の周波数差)が得られる。このようにして、チャレンジおよび対応するレスポンスの回路遅延PUFデータベース128が得られる。

【００３２】
SRAM 106の未初期化メモリセル状態は集束イオンビーム(FIB)アタックによるクローン化を受けやすいので、SRAM PUF 105のみを使用してメモリデバイス102の一意の識別子を供給するのは安全ではない。しかし、SRAM PUF 105とは異なり、回路遅延PUF 120(たとえば、RO PUF 122)は、クローン化を受けにくいが、多数のRO PUFを使用すると、チップ上の空間が占有されるので望ましくない。したがって、SRAM PUF 102上のクローン化アタックを妨害するには、比較的少数のリング発振器123をメモリデバイス102(たとえば、チップ、半導体など)上のSRAM PUF 105と組み合わせればよい。
【００３３】
チャレンジ/レスポンスを各デバイスに関連付けるには、デバイス識別子108(たとえば、通し番号、ID番号など)をデバイス102に記憶させ、データベース114および128に通知するかまたは記憶させればよい。すなわち、メモリデバイス102ごとのデバイス識別子108は、記憶され、そのメモリデバイス102の対応するチャレンジおよび/またはレスポンスに関連付けられてもよい。
【００３４】
図2は、SRAM PUFと回路遅延ベースPUF、たとえば、リング発振器(RO)PUFを組み合わせるメモリデバイスに関する事前に得られた特徴的なレスポンスを使用して特定のメモリデバイスを検証または識別する例示的な方法を示すブロック図である。動作時には、デバイス検証モジュール/回路202(たとえば、ベリファイアまたは認証デバイス/サーバによって実装される)がチャレンジ204によってメモリデバイス102に問い合わせてレスポンス206を得てもよく、レスポンス206は、SRAM PUFデータベース114と回路遅延PUFデータベース128の組合せを使用して検証され得る。レスポンス206は、メモリデバイスの識別情報を検証する働きをしてもよく、またはメモリデバイス102を認証する働きをしてもよい。この技法がメモリデバイスに関する一意の識別子/シグネチャを生成する働きをしてもよいことに留意されたい。
【００３５】
一例では、メモリデバイス102がその事前に記憶され/事前割り当てされたデバイス識別子108をデバイス認証モジュール/回路/サーバ202に供給してもよいことに留意されたい。デバイス認証モジュール/回路/サーバ202は次いで、そのデバイス識別子108に関して事前に記憶された1つまたは複数のチャレンジを取り込んでメモリデバイス102に送ってもよい(204)。代替的に、デバイス識別子108は、電子デバイスによってチャレンジへのあらゆるレスポンスとともに供給される(たとえば、すべての電子デバイスに同じチャレンジが使用される)。デバイス認証モジュール/回路/サーバ202は、レスポンス206を受け取ると、受け取ったレスポンス206をSRAM PUF 114および回路遅延PUF 128内の対応する事前に記憶されたレスポンスと比較して一致するかどうかを確認する。
【００３６】
この検証段階中に、チャレンジ204およびレスポンス206は攻撃者からアクセスされるかまたはアクセス可能になることがある。したがって、様々な機能によって、メモリデバイス102との間のチャレンジ204および/またはレスポンス206を保護して攻撃者がメモリデバイス102をクローン化するのを抑制することが可能である。
【００３７】
一例では、回路遅延PUF 120(たとえば、遅延ベースPUF)は不正使用防止可能である。集束イオンビーム(FIB)アタックではSRAM PUF 105のメモリセルのレスポンスがアタックにさらされる恐れがあるが、回路遅延PUF 120(たとえば、リング発振器)に関する情報は得られない。実際は、メモリデバイス102をクローン化/アタックするのに使用されるプロセスは、回路遅延PUF 120(たとえば、リング発振器)のレスポンスが変更され得る程、侵襲的であり、それによって、アタックにさらされ、メモリデバイス102の認証/識別が失敗する恐れがある。
【００３８】
SRAM PUF 105と回路遅延PUF 120を組み合わせ、チャレンジ204およびレスポンス206が

攻撃者からアクセス可能であるときでも攻撃者がメモリデバイス102をクローン化するのを抑制するための様々な方法がある。

【００３９】

SRAM物理的クローン化不能関数(PUF)とRO物理的クローン化不能関数(PUF)を組み合わせてチャレンジをマスキングすること

図3は、攻撃者がメモリデバイス307をクローン化できないようにするにはSRAM PUF 326と回路遅延PUF 324をどのように組み合わせたらよいかについての第1の例を示すブロック図である。この例では、認証デバイス300が、デバイス認証モジュール/回路/サーバ303と、SRAM PUFデータベース301と、回路遅延PUFデータベース305とを含んでもよい。SRAM PUFデータベース301は、たとえば、複数のチャレンジ(たとえば、メモリアドレス)をメモリセル領域に送り、対応するレスポンス(たとえば、未初期化メモリセル状態/値)を得ることによって、製造時にメモリデバイス307のメモリセル領域に関して生成されてもよい。同様に、回路遅延PUFデータベース305は、たとえば、複数のチャレンジ(たとえば、2つのリング発振器の選択)をリング発振器に送り、対応するレスポンス(たとえば、2つの選択されたリング発振器間の周波数差分)を得ることによって、製造時にメモリデバイス307内の複数のリング発振器に関して生成されてもよい。

【００４０】

この例では、デバイス認証モジュール/回路/サーバ303は、その後メモリデバイス307の認証を試みるときに、(チャレンジA 316とチャレンジB 312とを含む)チャレンジをメモリデバイス307に送る。チャレンジA 316は、XOR演算302によって組み合わされたSRAM PUFチャレンジ$C_0$306とRO PUFレスポンス$R_0$310とを備えてもよい。このチャレンジA 316は攻撃者からアクセス可能になり得るので、一態様では、実際のSRAM PUFチャレンジ$C_0$306を(回路遅延PUFデータベース305から得られる)対応するRO PUFレスポンス$R_0$310によってマスキングして(たとえば、XOR演算を行って)送られる(アタックにさらされる)チャレンジA 316を生成することによって実際のSRAM PUFチャレンジ$C_0$306を不明瞭にする。さらに、RO PUFレスポンス$R_0$310に対応するRO PUFチャレンジ$C_0$308を含むチャレンジB 312も認証デバイス300からメモリデバイス307に送られる。

【００４１】

メモリデバイス307において、RO PUFチャレンジ$C_0$312は、回路遅延PUF 324からRO PUFレスポンス$R_0$321を生成するのに使用される。チャレンジA 316は次いで、RO PUFレスポンス$R_0$321とXOR演算され(304)、SRAM PUF 326に関するチャレンジとして使用することのできる実際の(クリア)SRAM PUFチャレンジ$C_0$323が得られる。SRAM PUF 326は次いで、レスポンスSRAM PUF $R_0$325を生成する。このようにして、メモリデバイス307から認証デバイス300へのレスポンスは、SRAM PUFレスポンス$R_0$318を含んでもよい。

【００４２】

認証デバイス300において、受け取ったレスポンスSRAM PUF $R_0$322を使用してSRAM PUFデータベース301および回路遅延PUF 305内の記憶されたレスポンスを比較してそれらが一致するかどうかを確認してもよい。RO PUFレスポンス$R_0$310がすでに知られているかまたは回路遅延PUFデータベース305に記憶されているので、認証デバイス300がRO PUFレスポンス$R_0$310を使用してSRAM PUFチャレンジ$C_0$306をマスキングすることができることに留意されたい。

【００４３】

図4は、攻撃者がメモリデバイス407をクローン化できないようにするにはSRAM PUF 426と回路遅延PUF 424をどのように組み合わせたらよいかについての第2の例を示すブロック図である。図3の例とは異なり、この例では、SRAM PUFチャレンジ$C_0$406およびRO PUFチャレンジ$C_0$408がデバイス認証モジュール/回路/サーバ403からメモリデバイス407に平文で送られる。この例では、認証デバイス400が、デバイス認証モジュール/回路/サーバ403と、SRAM PUFデータベース401と、回路遅延PUFデータベース405とを含んでもよい。SRAM PUFデータベース401は、たとえば、複数のチャレンジ(たとえば、メモリアドレス)をメモリセル領域に送り、対応するレスポンス(たとえば、未初期化メモリセル状態/値)を得るこ

とによって、製造時にメモリデバイス407のメモリセル領域に関して生成されてもよい。同様に、回路遅延PUFデータベース405は、たとえば、複数のチャレンジ(たとえば、2つのリング発振器の選択)をリング発振器に送り、対応するレスポンス(たとえば、2つの選択されたリング発振器間の周波数差分)を得ることによって、製造時にメモリデバイス407内の複数のリング発振器に関して生成されてもよい。

【００４４】

この例では、デバイス認証モジュール/回路/サーバ403は、その後メモリデバイス407の認証を試みるときに、(チャレンジA 416とチャレンジB 412とを含む)チャレンジをメモリデバイス407に送る。チャレンジA 416はSRAM PUFチャレンジ$C_0$406を含んでもよい。チャレンジB 412は、RO PUFレスポンス$R_0$410に対応するRO PUFチャレンジ$C_0$408を含み、同じく認証デバイス400からメモリデバイス407に送られる。

【００４５】

チャレンジA 416は攻撃者からアクセス可能になり得るので、一態様では、メモリデバイス407においてXOR演算を行う(404)ことによって実際のSRAM PUFチャレンジ$C_0$406を修正SRAM PUFチャレンジC_0'423に修正する。メモリデバイス407において、RO PUFチャレンジ$C_0$412は、回路遅延PUF 424からRO PUFレスポンス$R_0$421を生成するのに使用される。チャレンジA 416(すなわち、SRAM PUFチャレンジ$C_0$406)は次いで、RO PUFレスポンス$R_0$421とXOR演算され(404)、SRAM PUF 426に関するチャレンジとして使用することのできる修正SRAM PUFチャレンジC_0'423が得られる。SRAM PUF 426は次いで、認証デバイス400に(レスポンスA 418として)返されるSRAM PUFレスポンスR_0'425を生成する。このようにして、メモリデバイス407から認証デバイス400へのレスポンスは、SRAM PUFレスポンス$R_0$418を含んでもよい。

【００４６】

この手法では、実際のチャレンジをメモリセル領域426に修正するためにRO PUFレスポンス$R_0$421が使用される。攻撃者はRO PUFレスポンス$R_0$421を再生することができないので、攻撃者には、レスポンスSRAM PUFレスポンスR_0'425を生成するのに使用される修正SRAM PUFチャレンジC_0'423はわからない。

【００４７】

認証デバイス400において、デバイス認証モジュール/回路/サーバ403は、SRAM PUFレスポンスR_0'422を検証してもよい。このことは、たとえば、SRAM PUFチャレンジ$C_0$406と(回路遅延PUFデータベース405から得られる)RO PUFレスポンス$R_0$420とのXOR演算を行って(402)修正SRAM PUFチャレンジC_0'427のローカルバージョンを得ることによって行われてもよい。次いで、修正SRAM PUFチャレンジC_0'427のローカルバージョンを使用してSRAM PUFデータベース401において対応するレスポンスを探索しそのレスポンスを受け取ったレスポンスSRAM PUFレスポンスR_0'422と比較してもよい。

【００４８】

図5は、攻撃者がメモリデバイスをクローン化できないようにするにはSRAM PUF 526と回路遅延524 PUFをどのように組み合わせたらよいかについての第3の例を示すブロック図である。この例では、認証デバイス500が、デバイス認証モジュール/回路/サーバ503と、SRAM PUFデータベース501と、回路遅延PUFデータベース505とを含んでもよい。SRAM PUFデータベース501は、たとえば、複数のチャレンジ(たとえば、メモリアドレス)をメモリセル領域に送り、対応するレスポンス(たとえば、未初期化メモリセル状態/値)を得ることによって、製造時にメモリデバイス507のメモリセル領域に関して生成されてもよい。同様に、回路遅延PUFデータベース505は、たとえば、複数のチャレンジ(たとえば、2つのリング発振器の選択)をリング発振器に送り、対応するレスポンス(たとえば、2つの選択されたリング発振器間の周波数差分)を得ることによって、製造時にメモリデバイス507内の複数のリング発振器に関して生成されてもよい。

【００４９】

この例では、デバイス認証モジュール/回路/サーバ503は、その後メモリデバイス507の認証を試みるときに、対応するRO PUFレスポンスR_0を有するRO PUFチャレンジ$C_0$508を含

むチャレンジ512を送る。

【００５０】

RO PUFチャレンジ$C_0$512は攻撃者によってアクセス可能であるが、回路遅延PUF 524を攻撃者によって複製することはできない。メモリデバイス507において、RO PUFチャレンジ$C_0$512は、回路遅延PUF 524からRO PUFレスポンス$R_0$521を生成するのに使用される。このRO PUFレスポンス$R_0$521は次に、SRAM PUF 526へのSRAM PUFチャレンジ$C_0$523として使用され、RO PUFレスポンス$R_0$525が得られる。代替手法では、RO PUFレスポンス$R_0$521を使用して(たとえば、RO PUFレスポンス$R_0$521をメモリアドレスにマッピングまたは変換することによって)チャレンジSRAM PUF $C_0$523を生成してもよい。SRAM PUFレスポンス$R_0$518は認証デバイス500に送られる。

【００５１】

この手法では、実際のチャレンジをSRAM PUF 526に修正するためにRO PUFレスポンス$R_0$521が使用される。攻撃者はRO PUFレスポンス$R_0$521を再生することができないので、攻撃者には、レスポンスSRAM PUFレスポンス$R_0$525を生成するのに使用されるSRAM PUFチャレンジ$C_0$523はわからない。

【００５２】

認証デバイス500において、デバイス認証モジュール/回路/サーバ503は、送られたRO PUFチャレンジ$C_0$508に対応するRO PUFレスポンス$R_0$520を回路遅延PUF 505から得てもよい。このRO PUFレスポンス$R_0$520は、SRAM PUFチャレンジ$C_0$527として働いてもよい。デバイス認証モジュール/回路/サーバ403は、SRAM PUFレスポンス$R_0$422を検証してもよい。次いで、SRAM PUFチャレンジ$C_0$527を使用してSRAM PUFデータベース501において対応するレスポンスを探索しそのレスポンスを受け取ったレスポンスSRAM PUFレスポンス$R_0$522と比較してもよい。

【００５３】

図3、図4、および図5に示す手法では、デバイス認証モジュール/回路/サーバ303、403、および/または503は、SRAM PUFとRO PUFの両方に関するチャレンジとレスポンスの対にアクセスすることができる。したがって、デバイス認証モジュール/回路/サーバ303、403、および/または503は、メモリデバイス307、407、および507によって実行された演算を検証し、レスポンスを検証することができる。

【００５４】

SRAM物理的クローン化不能関数(PUF)とRO物理的クローン化不能関数(PUF)を組み合わせてレスポンスをマスキングすること

代替手法では、RO PUFを使用することによってSRAM PUFレスポンスをメモリデバイスから保護する。

【００５５】

図6は、攻撃者がメモリデバイス607をクローン化できないようにするにはSRAM PUF 626とRO PUF 624をどのように組み合わせたらよいかについての第4の例を示すブロック図である。この例では、認証デバイス600が、デバイス認証モジュール/回路/サーバ603と、SRAM PUFデータベース601と、RO PUFデータベース605とを含んでもよい。SRAM PUFデータベース601は、たとえば、複数のチャレンジ(たとえば、メモリアドレス)をメモリセル領域に送り、対応するレスポンス(たとえば、未初期化メモリセル状態/値)を得ることによって、製造時にメモリデバイス607のメモリセル領域に関して生成されてもよい。同様に、回路遅延PUFデータベース605は、たとえば、複数のチャレンジ(たとえば、2つのリング発振器の選択)をリング発振器に送り、対応するレスポンス(たとえば、2つの選択されたリング発振器間の周波数差分)を得ることによって、製造時にメモリデバイス607内の複数のリング発振器に関して生成されてもよい。

【００５６】

この例では、デバイス認証モジュール/回路/サーバ603は、その後メモリデバイス607の認証を試みるときに、(チャレンジA 616とチャレンジB 612とを含む)チャレンジをメモリデバイス607に送る。チャレンジA 616はSRAM PUFチャレンジ$C_0$606を含んでもよい。チャ

レンジB 612は、RO PUFチャレンジ$C_0$608を含み、同じく認証デバイス600からメモリデバイス607に送られる。

【００５７】

メモリデバイス604において、RO PUFチャレンジ$C_0$612は、回路遅延PUF 624からRO PUFレスポンス$R_0$621を生成するのに使用される。SRAM PUFチャレンジ$C_0$616は、SRAM PUFレスポンス$R_0$623を生成するようにSRAM PUF 626によって処理される。次いで、RO PUFレスポンス$R_0$621のハッシュ619がRO PUFレスポンスR_0'625として得られる。RO PUFレスポンスR_0'625は次いで、SRAM PUF $R_0$623とXOR演算され(604)、デバイス認証モジュール/回路/サーバ603に送り返される組み合わされたレスポンス618(たとえば、SRAM PUF R_0 XOR RO PUFレスポンスR_0')が得られる。このようにして、SRAM PUF 626からのSRAM PUFレスポンス$R_0$623によって送信時に認証デバイス600を保護することができる。

【００５８】

認証デバイス600において、デバイス認証モジュール/回路/サーバ603は、レスポンス618が送られたチャレンジSRAM PUF $C_0$606およびRO PUF $C_0$608に対応することを検証してもよい。たとえば、回路遅延PUFデータベース605を使用して、送られたRO PUFチャレンジ$C_0$608に対応するRO PUFレスポンス$R_0$620が得られる。次いで、デバイス認証モジュール/回路/サーバ603は、RO PUFレスポンス$R_0$620をハッシングし(617)、その結果とレスポンス618をXOR演算して(602)、SRAM PUFレスポンス$R_0$627を得ることによってSRAM PUFレスポンス$R_0$627を得ることができる。SRAM PUFレスポンス$R_0$627を使用してSRAM PUFデータベース601内のSRAM PUFチャレンジ$C_0$606に関して予期される対応するレスポンスを探索することができる。レスポンスが一致する場合、メモリデバイス607は首尾よく認証または識別される。

【００５９】

例示的なデータコレクタデバイスおよびデータコレクタデバイスにおいて使用可能な方法

図7は、一例によるデータコレクタデバイスを示すブロック図である。データコレクタデバイス702は、電子デバイス(たとえば、チップ、半導体、メモリデバイスなど)を一意に特徴付ける情報を収集して記憶するように構成されてもよい。たとえば、製造段階、品質管理段階、および/または展開前段階の間、データコレクタデバイス702は、各電子デバイスに対してチャレンジを送ってレスポンスを受け取り、受け取った情報を後で各電子デバイスを認証/識別する際に使用できるように記憶するように構成されてもよい。

【００６０】

データコレクタデバイス702は、処理回路704、記憶デバイス706、通信インターフェース708、および/または機械可読媒体710を含み得る。通信インターフェース708は、データコレクタデバイス702が1つまたは複数の電子デバイスと(たとえば、有線によってまたはワイヤレスに)通信するのを可能にする送信機/受信機回路718を含んでもよい。

【００６１】

処理回路704は、電子デバイスごとの一意の識別子を得てそのような一意の識別子を記憶デバイス706内のデバイス識別子データベース716に記憶するように構成されたデバイス識別子回路/モジュール722を含んでもよい。処理回路704は、1つまたは複数のチャレンジを生成して電子デバイスに送出するように構成されたチャレンジ生成回路/モジュール720を含んでもよい。たとえば、チャレンジは、(たとえば、SRAM PUFに関する)メモリアドレスまたは(たとえば、RO PUFに関する)リング発振器対であってもよい。処理回路704は、送られた1つまたは複数のチャレンジに応答して電子デバイス内のSRAM PUFからのレスポンスを収集するように構成されたSRAM PUF収集回路/モジュール726を含んでもよい。処理回路704は、送られた1つまたは複数のチャレンジに応答して電子デバイス内の回路遅延PUFからのレスポンスを収集するように構成された回路遅延PUF収集回路/モジュール726を含んでもよい。

【００６２】

機械可読媒体710は、(たとえば、処理回路に問合せ中の電子デバイスからデバイス識別子を得させるための)デバイス識別子命令730、(たとえば、処理回路にランダムなチャレ

ンジまたは事前生成されたチャレンジを生成させて問合せ中の電子デバイスのSRAM PUFおよび/または回路遅延PUFに送らせるための)チャレンジ生成命令728、(たとえば、処理回路に問合せ中の電子デバイスのSRAM PUFからのレスポンスを収集させるための)SRAM PUF収集命令732、ならびに/あるいは(たとえば、処理回路に問合せ中の電子デバイスの回路遅延PUFからレスポンスを収集させるための)回路遅延PUF収集命令734を含むかまたは記憶してもよい。一例では、回路遅延PUFが不正使用防止PUFであってもよいことに留意されたい。対照的に、SRAM PUFは様々なアタック(たとえば、集束イオンビーム(FIB)アタック、回路編集アタックなど)を受けやすいように示されている。

【００６３】

データコレクタデバイス702は、図1～図6に示すステップまたは関数のうちの1つまたは複数を実行するように構成されてもよい。

【００６４】

図8は、電子デバイスから特性情報を得るためのデータコレクタデバイスにおいて使用可能な方法を示す図である。データコレクタデバイスは、電子デバイスの展開前段階または製造段階中に電子デバイスに関連するデバイス識別子を得てもよい(たとえば、受け取るかまたは割り当ててもよい)(802)。データコレクタデバイスは次いで、1つまたは複数のチャレンジを生成して電子デバイスに送ってもよい(804)。その結果、データコレクタデバイスは、電子デバイスから1つまたは複数のレスポンスを受け取ってもよく、1つまたは複数のレスポンスは、電子デバイス806において2つ以上の異なる種類の物理的クローン化不能関数から生成される特性情報を含む。デバイス識別子、チャレンジ、および対応するレスポンスは、後で電子デバイスを認証できるように記憶される(808)。このプロセスは、複数の電子デバイスの各々について繰り返されてもよい。電子デバイスに送られるチャレンジがすべてのデバイスについて同じであってもよく、電子デバイスごとに無作為に生成されてもよく、ならびに/あるいはあり得るチャレンジのサブセットであってもよいことに留意されたい。

【００６５】

例示的な認証デバイスおよび認証デバイスにおいて使用可能な方法

図9は、各電子デバイス内の複数の物理的クローン化不能関数からのレスポンスに基づいて電子デバイスを認証するように構成された例示的な認証デバイスを示すブロック図である。認証デバイス902は、電子デバイス(たとえば、チップ、半導体、メモリデバイスなど)に問い合わせ、(電子デバイスから得られる)デバイス識別子に基づいて電子デバイスを識別し、電子デバイス内のSRAM PUFおよび回路遅延PUFへのチャレンジを含む問合せを実行することによって電子デバイスを認証することを試みるように構成されてもよい。認証デバイス902は、処理回路904、記憶デバイス906、通信インターフェース908、および/または機械可読媒体910を含み得る。通信インターフェース908は、認証デバイス902が1つまたは複数の電子デバイスと(たとえば、有線によってまたはワイヤレスに)通信するのを可能にする送信機/受信機回路918を含んでもよい。

【００６６】

処理回路904は、電子デバイスから一意のデバイス識別子を得るように構成されたデバイス識別子回路/モジュール922を含んでもよい。認証回路/モジュール936は、得られたデバイス識別子を使用して、そのデバイス識別子に関連する対応するチャレンジ/レスポンス情報の有無に関して(記憶デバイス906内の)デバイス識別子データベース916をチェックしてもよい。認証回路/モジュール936は次いで、SRAM PUF検証回路/モジュール924および回路遅延PUF検証回路/モジュール926と協働して、対応するチャレンジのうちの1つまたは複数を電子デバイスに送ってもよく、チャレンジに対する1つまたは複数のレスポンスを得る。一例では、回路遅延PUFが不正使用防止PUFであってもよいことに留意されたい。対照的に、SRAM PUFは様々なアタック(たとえば、集束イオンビーム(FIB)アタック、回路編集アタックなど)を受けやすいように示されている。

【００６７】

レスポンスは、チャレンジとともに、それぞれ(記憶デバイス906内の)SRAM PUFデータ

ベース914および(記憶デバイス906内の)回路遅延PUFデータベース912から、予期されるレスポンスに正しく一致するか(すなわち、データベース914および916内のチャレンジに対応するレスポンスと一致する)どうかを確認するために、SRAM PUF検証回路/モジュール924および回路遅延PUF検証回路/モジュール926によって使用されてもよい。受け取ったレスポンスが事前に記憶された対応するレスポンスと一致する場合、認証回路/モジュール936は、電子デバイスが首尾よく認証されたと結論付けてもよい。そのような認証の成功は確率的な一致であってもよく、しきい値率またはしきい値数のレスポンスが正しく一致する限り、首尾よく一致したと結論付けられてもよい。

【００６８】

機械可読媒体910は、(たとえば、処理回路に検証中の電子デバイスからデバイス識別子を得させるための)デバイス識別子命令930、(たとえば、処理回路に検証中の電子デバイスのSRAM PUFからのレスポンスを検証させるための)SRAM PUF検証命令932、(たとえば、処理回路に検証中の電子デバイスの回路遅延PUFからのレスポンスを検証させるための)回路遅延PUF検証命令934、ならびに/あるいはSRAM PUF検証と回路遅延PUF検証の両方が成功したかどうかを確認するための認証命令938を含むかまたは記憶してもよい。

【００６９】

データコレクタデバイス902は、図1～図6に示すステップまたは関数のうちの1つまたは複数を実行するように構成されてもよい。

【００７０】

図10は、複数の物理的クローン化不能関数からのレスポンスに基づいて電子デバイスを認証するための認証デバイスにおいて使用可能な方法を示す。認証デバイスは、展開後段階中に電子デバイスに関連するデバイス識別子を得てもよい(たとえば、要求するかまたは受け取ってもよい)(1002)。認証デバイスは次いで、1つまたは複数のチャレンジを得て電子デバイスに送ってもよい(1004)。たとえば、チャレンジは、すべての電子デバイスに利用されるあらかじめ規定された1組のチャレンジであってもよい。代替的に、チャレンジは、デバイス識別子を使用してデータベースから得られる電子デバイスに関するチャレンジの特定のサブセットであってもよい。認証デバイスは、1つまたは複数のチャレンジを送った結果として、電子デバイスから1つまたは複数のレスポンスを受け取ってもよく、1つまたは複数のレスポンスは、電子デバイスにおいて2つ以上の異なる種類の物理的クローン化不能関数から生成される特性情報を含む(1006)。様々な実装形態では、認証デバイスは、図1、図2、図3、図4、図5、および/または図6に例示し、図1、図2、図3、図4、図5、および/または図6を参照して説明したように動作してもよい。

【００７１】

デバイス識別子を使用して電子デバイスに特有の事前に記憶されたチャレンジおよび対応するレスポンスを識別してもよい(1008)。認証デバイスは次いで、電子デバイスに関する事前に記憶されたレスポンスと受け取った1つまたは複数のレスポンスを比較することによって電子デバイスを認証してもよい(1010)。電子デバイスに関して受け取った1つまたは複数のレスポンスが事前に記憶されたレスポンスと一致するときに認証が成功する。認証の成功は確率的な一致であってもよく、しきい値率またはしきい値数のレスポンスが正しく一致する限り、首尾よく一致したと結論付けられてもよい。このプロセスは、複数の電子デバイスの各々について繰り返されてもよい。物理的クローン化不能関数は各電子デバイスによって使用されるので、1つまたは複数のレスポンスは、すべてのデバイスに同じチャレンジが使用される場合でも異なる。

【００７２】

例示的な電子デバイスおよび電子デバイスにおいて使用可能な方法

図11は、複数の物理的クローン化不能関数を有する例示的な電子デバイスを示すブロック図である。電子デバイス1102は、チップ、半導体、メモリデバイスなどであってもよく、デバイス識別子を供給し、電子デバイス内のSRAM PUFおよび回路遅延PUFへのチャレンジに応答するように構成されてもよい。電子デバイス1102は、処理回路1104、(記憶デバイス内の)デバイス識別子1116、遅延ベースPUF回路1112(たとえば、複数の発振器リング

回路)、スタティックランダムアクセスメモリ1116(SRAM PUFとして使用されてもよい)、通信インターフェース1108、および/または機械可読媒体1110を含んでもよい。通信インターフェース1108は、電子デバイス1102が1つまたは複数のデータコレクタデバイスおよび/または認証デバイスと(たとえば、有線によってまたはワイヤレスに)通信するのを可能にする送信機/受信機回路1118を含んでもよい。

【００７３】

処理回路1104は、一意のデバイス識別子1116をデータコレクタデバイスおよび/または認証デバイスに供給するように構成されたデバイス識別子回路/モジュール1122を含んでもよい。処理回路は、受け取ったチャレンジに対するレスポンスを得て、レスポンスをデータコレクタデバイスおよび認証デバイスに送るように構成されたSRAM PUFレスポンス回路/モジュール1124と回路遅延PUFレスポンス回路/モジュール1126とを含んでもよい。一例では、回路遅延PUFが不正使用防止PUFであってもよいことに留意されたい。対照的に、SRAM PUFは様々なアタック(たとえば、集束イオンビーム(FIB)アタック、回路編集アタックなど)を受けやすいように示されている。

【００７４】

SRAM PUFレスポンス回路/モジュール1124は、受け取ったチャレンジをスタティックランダムアクセスメモリ1114に送ってレスポンスを得てもよい。たとえば、レスポンスは、スタティックランダムアクセスメモリ1114の1つまたは複数のメモリセルの未初期化状態であってもよい。同様に、回路遅延PUFレスポンス回路/モジュール1126は、受け取ったチャレンジを遅延ベースPUF回路1112に送ってレスポンスを得てもよい。

【００７５】

機械可読媒体1110は、(たとえば、処理回路に電子デバイスに関するデバイス識別子1116を得させるための)デバイス識別子命令1130、(たとえば、処理回路に電子デバイスのスタティックランダムアクセスメモリ1114からのレスポンスを得させるための)SRAM PUFレスポンス命令1132、および/または(たとえば、処理回路に電子デバイスの回路遅延PUFからのレスポンスを得させるための)回路遅延PUFレスポンス命令1134を含むかまたは記憶してもよい。

【００７６】

電子デバイス1102は、図1～図6に示すステップまたは関数のうちの1つまたは複数を実行するように構成されてもよい。

【００７７】

図12は、複数の物理的クローン化不能関数からのレスポンスに基づいて認証デバイスによって電子デバイス自体を認証するための電子デバイスにおいて使用可能な方法を示す。電子デバイスは、すでに展開前段階または製造段階中に1つまたは複数のチャレンジを受け取っており、1つまたは複数の対応するレスポンスを供給している。

【００７８】

電子デバイスは、電子デバイス内の複数のメモリセルを使用して第1の物理的クローン化不能関数を実施する(1204)。一例では、第1の物理的クローン化不能関数は、チャレンジに対するレスポンスとして、1つまたは複数のメモリセルに関する未初期化メモリセル状態を利用する。

【００７９】

電子デバイスは、電子デバイス内の複数の回路遅延ベースパスを使用して第2の物理的クローン化不能関数を実施してもよい(1206)。一例では、複数の回路遅延ベースパスは場合によっては不正使用防止可能である。「不正使用防止」という用語は、不正使用が試みられたときにそのレスポンスまたは出力の予想、確認、および/または読取りを行い、これによってレスポンスおよび/または出力を変更するPUFの実装形態または種類を指す。たとえば、リング発振器または回路遅延パス式発振器を物理的に不正使用することを試みると、リング発振器または回路遅延パスに関するレスポンスが変更される(たとえば、出力周波数が変化する)。

【００８０】

チャレンジが外部サーバから受け取られることがある(1208)。このチャレンジは、第2の物理的クローン化不能関数からの第1のレスポンスを使用して、(a)第1の物理的クローン化不能関数へのチャレンジ入力をマスキング/アンマスキングすること、(b)第1の物理的クローン化不能関数へのチャレンジ入力を生成すること、または(c)第1の物理的クローン化不能関数からのレスポンス出力をマスキングすることのいずれかを行うことによって第1の物理的クローン化不能関数に適用されてもよい(1210)。一例では、第1のチャレンジは、複数のメモリセル内のメモリアドレスを識別してもよい。別の例では、チャレンジは、第2の物理的クローン化不能関数における複数のリング発振器から2つのリング発振器を選択し、2つのリング発振器間の周波数差分によって応答してもよい。チャレンジは、電子デバイスの認証プロセス、電子デバイスの識別プロセス、および/または電子デバイス内のキー生成プロセスのうちの少なくとも1つの一部として受け取られてもよい。

【００８１】

次に、第2の物理的クローン化不能関数からの第1のレスポンスおよび/または第1の物理的クローン化不能関数からの第2のレスポンスを外部サーバに送ってもよい(1212)。外部サーバは、第1の物理的クローン化不能関数に関するチャレンジおよびレスポンスの第1のデータベースと第2の物理的クローン化不能関数に関するチャレンジおよびレスポンスの第2のデータベースとを含んでもよく、外部サーバは、チャレンジを電子デバイスに送り、第2のレスポンスに基づいて電子デバイスを認証または識別する。

【００８２】

レスポンスが外部サーバによって首尾よく検証されたことを示すインジケータが受け取られてもよい(1214)。たとえば、電子デバイスは、首尾よく認証されたときに、ネットワークおよび/またはデータにアクセス可能になったことを示すインジケータを受け取ることができる。

【００８３】

一例では、チャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと、第2の物理的クローン化不能関数に関する第2のチャレンジとを含んでもよい。たとえば、第1のチャレンジは、(図3に示すように)第2のチャレンジへの予期されるレスポンスによってマスキングされたチャレンジであってもよい。別の例では、第1のチャレンジは、(図4に示すように)第1の物理的クローン化不能関数によって処理される前に第2の物理的クローン化不能関数からの第1のレスポンスによって修正されてもよい。

【００８４】

さらに別の例では、(図5に示すように)受け取ったチャレンジが第2の物理的クローン化不能関数によって使用されて第1のレスポンスが生成され、次に、第1のレスポンスが第1の物理的クローン化不能関数によって第2のチャレンジとして使用されて第2のレスポンスが生成されてもよい。

【００８５】

さらに別の実装形態では、チャレンジは、第1の物理的クローン化不能関数に関する第1のチャレンジと、第2の物理的クローン化不能関数に関する第2のチャレンジとを含んでもよく、(図6に示すように)第2のチャレンジが第2の物理的クローン化不能関数によって使用されて第1のレスポンスが生成され、第1のレスポンスを使用して第1の物理的クローン化不能関数からの第2のレスポンスがマスキングされてもよい。この方法は、(a)第2の物理的クローン化不能関数からの第1のレスポンスをハッシングして中間レスポンスを得ること、および/または(b)中間レスポンスを使用して第2のレスポンスをマスキングすることをさらに含んでもよい。

【００８６】

一例では、事前に記憶されたデバイス識別子が電子デバイス内に事前プロビジョニングされてもよい(1202)。この例では、(a)チャレンジが受け取られる前または(b)第2のレスポンスを送るのと同時のいずれかのときに、事前に記憶されたデバイス識別子を電子デバイスから外部サーバに送ってもよい。デバイス識別子は電子デバイスを一意に識別する。

【００８７】

図1～図12に示す構成要素、ステップ、特徴および/または機能のうちの1つまたは複数は、単一の構成要素、ステップ、特徴または機能として再構成されならびに/あるいは組み合わされるか、あるいは、いくつかの構成要素、ステップ、または機能として具現化され得る。追加の要素、構成要素、ステップ、および/または機能は、また、本発明から逸脱することなく加えられ得る。図1～図7、図9、および図11に示す装置、デバイス、および/または構成要素は、図8、図10、および図12に記載した方法、特徴、またはステップのうちの1つまたは複数を実行するように構成され得る。また、本明細書で説明されたアルゴリズムは、効率的にソフトウェアに実装されてもよく、かつ/またはハードウェアに組み込まれてもよい。

【００８８】

その上、本開示の一態様では、図7、図9、および図11に示す処理回路704、904、および1104は、特に、それぞれ図8、図10、および図12で説明したアルゴリズム、方法、および/またはステップを実行するように特に設計されならびに/あるいは配線される専用プロセッサ(たとえば、特定用途向け集積回路(ASIC))であり得る。したがって、そのような専用プロセッサ(たとえば、ASIC)は、図8、図10、および/または図12で説明したアルゴリズム、方法、および/またはステップを実行するための手段の一例であり得る。

【００８９】

また、本開示の態様は、フローチャート、フロー図、構造図またはブロック図として示されるプロセスとして説明され得ることに留意されたい。フローチャートは動作を逐次プロセスとして説明し得るが、動作の多くは並行してまたは同時に実行され得る。さらに、動作の順序を並び替えてもよい。プロセスは、その動作が完了したとき、終了する。プロセスは、メソッド、関数、プロシージャ、サブルーチン、サブプログラムなどに対応することができる。プロセスが関数に対応するときには、その終了は、呼び出す側の関数またはメイン関数への関数のリターンに対応する。

【００９０】

その上、記憶媒体は、読取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、磁気ディスク記憶媒体、光学記憶媒体、フラッシュメモリデバイスおよび/もしくは他の機械可読媒体、およびプロセッサ可読媒体、ならびに/または情報を記憶するためのコンピュータ可読媒体を含む、データを記憶するための1つもしくは複数のデバイスを表し得る。「機械可読媒体」、「コンピュータ可読媒体」、および/または「プロセッサ可読媒体」という用語は、ポータブルもしくは固定ストレージデバイス、光ストレージデバイス、ならびに、命令および/またはデータを記憶、格納または搬送することが可能な様々な他の媒体のような非一時的媒体を含み得るが、これらに限定されない。したがって、本明細書で説明される様々な方法は、「機械可読媒体」、「コンピュータ可読媒体」および/または「プロセッサ可読媒体」に記憶され、1つもしくは複数のプロセッサ、機械および/またはデバイスによって実行され得る命令および/またはデータによって、完全にまたは部分的に実装され得る。

【００９１】

さらに、本開示の態様は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、またはそれらの任意の組合せによって実装され得る。ソフトウェア、ファームウェア、ミドルウェアまたはマイクロコードで実装されるとき、必要なタスクを実行するプログラムコードまたはコードセグメントは、記憶媒体または他のストレージのような機械可読媒体に記憶され得る。プロセッサは必要なタスクを実行することができる。コードセグメントは、手順、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、あるいは命令、データ構造、またはプログラムステートメントの任意の組合せを表すことができる。コードセグメントは、情報、データ、引数、パラメータ、またはメモリ内容を渡す、および/または受信することによって、別のコードセグメントまたはハードウェア回路に結合され得る。情報、引数、パラメータ、データ等は、メモリ共有、メッセージパッシング、トークンパッシング、ネットワーク送信等を含む任意の適切な手段を介して渡されてもよく、転送または送信

されてもよい。

【００９２】

本明細書に開示された例に関連して説明される様々な例示的な論理ブロック、モジュール、回路、要素、および/または構成要素は、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)または他のプログラマブル論理構成要素、個別ゲートまたはトランジスタ論理、個別ハードウェア構成要素、あるいは本明細書に記載の機能を実行するように設計されたそれらの任意の組合せで実装または実行され得る。汎用プロセッサはマイクロプロセッサでよいが、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、または状態機械でもよい。プロセッサはまた、コンピューティングコンポーネントの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、いくつかのマイクロプロセッサ、DSPコアと連係した1つまたは複数のマイクロプロセッサ、あるいは他の任意のそのような構成として実装され得る。

【００９３】

本明細書で開示される例に関連して説明される方法またはアルゴリズムを、ハードウェアで直接に、プロセッサによって実行可能なソフトウェアモジュールで、またはその両方の組合せで、処理ユニット、プログラミング命令、または他のディレクティブの形で実施することができ、単一のデバイス内に含めるか、複数のデバイスにまたがって分散させることができる。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既知の任意の他の形の記憶媒体に存在することができる。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、記憶媒体を、プロセッサに結合することができる。代替案では、記憶媒体を、プロセッサと一体とすることができる。

【００９４】

当業者は、本明細書で開示される諸態様に関連して説明される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を、電子ハードウェア、コンピュータソフトウェア、またはその両方の組合せとして実施できることを、さらに了解するはずである。ハードウェアとソフトウェアとのこの相互交換可能性を明瞭に示すために、様々な例示的なコンポーネント、ブロック、モジュール、回路、およびステップが、上では全般的にその機能性に関して説明された。そのような機能性が、ハードウェアまたはソフトウェアのどちらとして実施されるのかは、具体的な応用と、システム全体に課せられる設計制約とに依存する。

【００９５】

本明細書に記載の本発明の様々な特徴は、本発明から逸脱することなく、異なるシステムで実施され得る。本開示の前述の態様は、単に例であり、本発明を限定するものとして解釈されるべきではないことに留意すべきである。本開示の態様の説明は、例示であることを意図しており、特許請求の範囲を限定することを意図していない。したがって、本教示は、他のタイプの装置に容易に適用されることが可能であり、多くの代替形態、変更形態、および変形形態が当業者には明らかであろう。

【符号の説明】

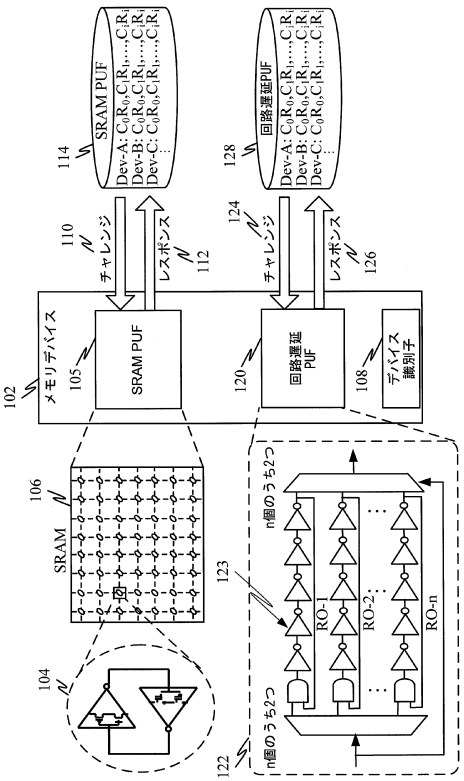
【００９６】

102　メモリデバイス
104　メモリセル
106　SRAM
108　デバイス識別子
110　チャレンジ
112　レスポンス
114　データベース
120　回路遅延PUF

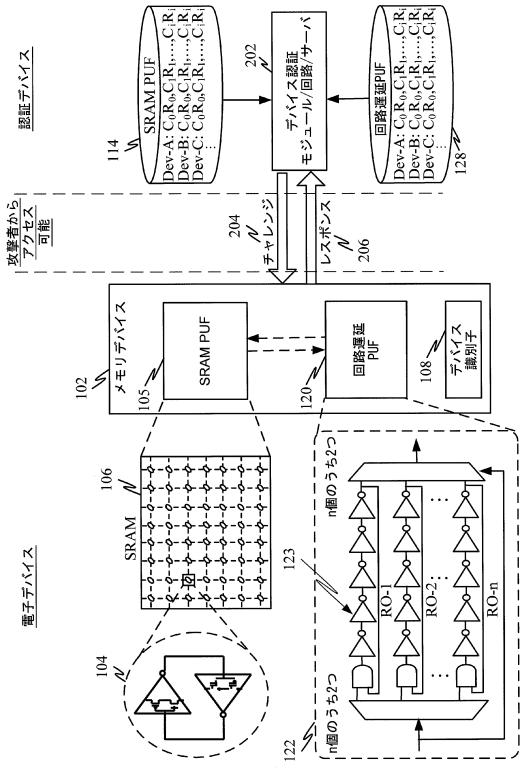
123 リング発振器
124 チャレンジ
128 回路遅延PUFデータベース
202 デバイス認証モジュール/回路/サーバ
204 リング発振器
206 レスポンス
300 認証デバイス
302 XOR演算
303 デバイス認証モジュール/回路/サーバ
305 回路遅延PUFデータベース
307 メモリデバイス
312 チャレンジ
316 チャレンジ
318 レスポンス
324 回路遅延PUF
400 認証デバイス
403 デバイス認証モジュール/回路/サーバ
404 XOR演算
405 回路遅延PUFデータベース
407 メモリデバイス
416 チャレンジ
418 レスポンス
424 回路遅延PUF
426 メモリセル領域
500 認証デバイス
503 デバイス認証モジュール/回路/サーバ
505 回路遅延PUFデータベース
507 メモリデバイス
512 チャレンジ
518 レスポンス
524 回路遅延PUF
600 認証デバイス
603 デバイス認証モジュール/回路/サーバ
604 メモリデバイス
605 RO PUFデータベース
607 メモリデバイス
612 チャレンジ
616 チャレンジ
618 レスポンス
619 ハッシュ
624 回路遅延PUF
625 RO PUFレスポンス
702 データコレクタデバイス
704 処理回路
706 記憶デバイス
708 通信インターフェース
710 機械可読媒体
712 回路遅延PUFデータベース
714 SRAM PUFデータベース
716 デバイス識別子データベース

718 送信機/受信機回路
720 チャレンジ生成回路/モジュール
722 デバイス識別子回路/モジュール
724 SRAM PUF収集回路/モジュール
726 回路遅延PUF収集回路/モジュール
728 チャレンジ生成命令
730 デバイス識別子命令
732 SRAM PUF収集命令
734 回路遅延PUF収集命令
902 認証デバイス
904 処理回路
906 記憶デバイス
908 通信インターフェース
910 機械可読媒体
912 回路遅延PUFデータベース
914 データベース
916 デバイス識別子データベース
918 送信機/受信機回路
922 デバイス識別子回路/モジュール
924 SRAM PUF検証回路/モジュール
926 回路遅延PUF検証回路/モジュール
930 デバイス識別子命令
932 SRAM PUF検証命令
934 回路遅延PUF検証命令
936 認証回路/モジュール
938 認証命令
1102 電子デバイス
1104 処理回路
1108 通信インターフェース
1110 機械可読媒体
1112 遅延ベースPUF回路
1114 スタティックランダムアクセスメモリ
1116 デバイス識別子
1118 送信機/受信機回路
1122 デバイス識別子回路/モジュール
1124 SRAM PUFレスポンス回路/モジュール
1126 回路遅延PUFレスポンス回路/モジュール
1130 デバイス識別子命令
1132 SRAM PUFレスポンス命令
1134 回路遅延PUFレスポンス命令

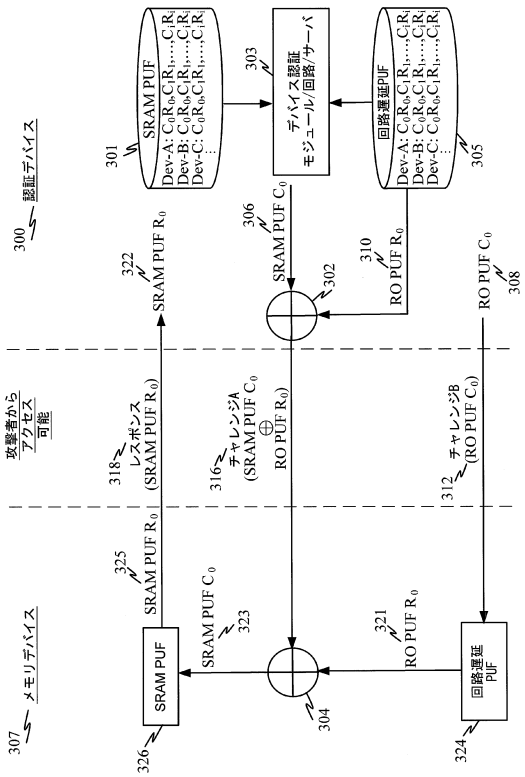
【図１】


SRAM PUF
回路遅延PUF
チャレンジ
レスポンス
メモリデバイス
SRAM PUF
回路遅延 PUF
デバイス識別子
SRAM
RO-1
RO-2
RO-n
n個のうち2つ

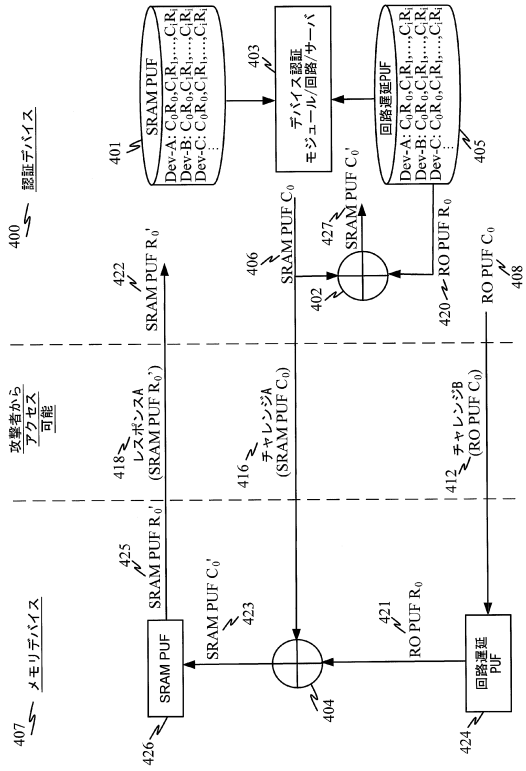
【図２】


認証デバイス
攻撃者からアクセス可能
デバイス認証 モジュール/回路/サーバ
チャレンジ
レスポンス
SRAM PUF
回路遅延PUF
メモリデバイス
SRAM PUF
回路遅延 PUF
デバイス識別子
SRAM
電子デバイス
RO-1
RO-2
RO-n
n個のうち2つ

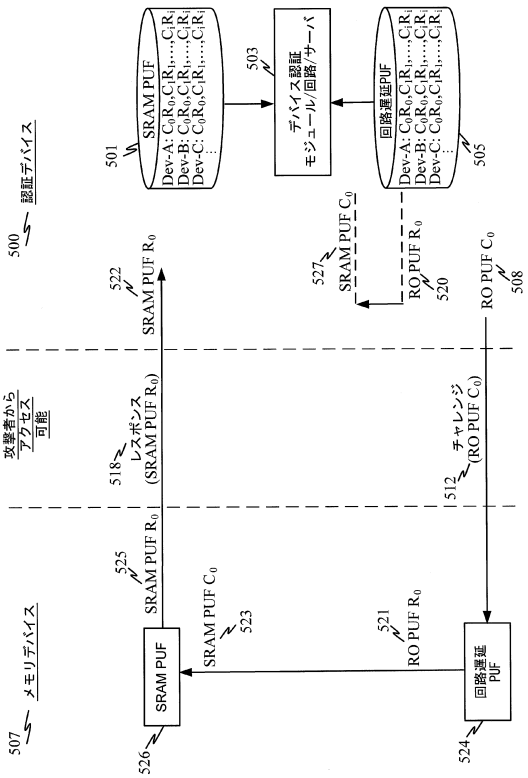
【図３】


認証デバイス
攻撃者からアクセス可能
SRAM PUF
デバイス認証 モジュール/回路/サーバ
回路遅延PUF
SRAM PUF R0
SRAM PUF C0
RO PUF R0
RO PUF C0
レスポンス (SRAM PUF R0)
チャレンジA (SRAM PUF C0 ⊕ RO PUF R0)
チャレンジB (RO PUF C0)
メモリデバイス
SRAM PUF
回路遅延 PUF

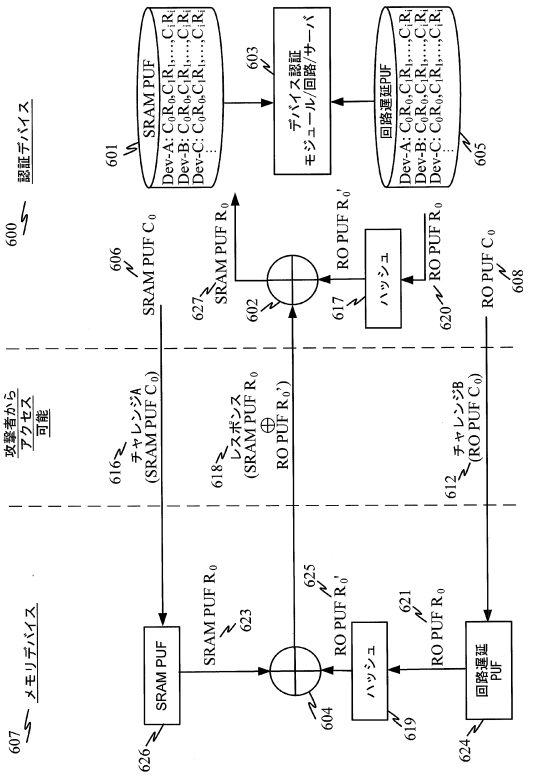
【図４】


認証デバイス
攻撃者からアクセス可能
SRAM PUF
デバイス認証 モジュール/回路/サーバ
回路遅延PUF
SRAM PUF R0'
SRAM PUF C0'
SRAM PUF C0
RO PUF R0
RO PUF C0
レスポンスA (SRAM PUF R0')
チャレンジA (SRAM PUF C0')
チャレンジB (RO PUF C0)
メモリデバイス
SRAM PUF
回路遅延 PUF

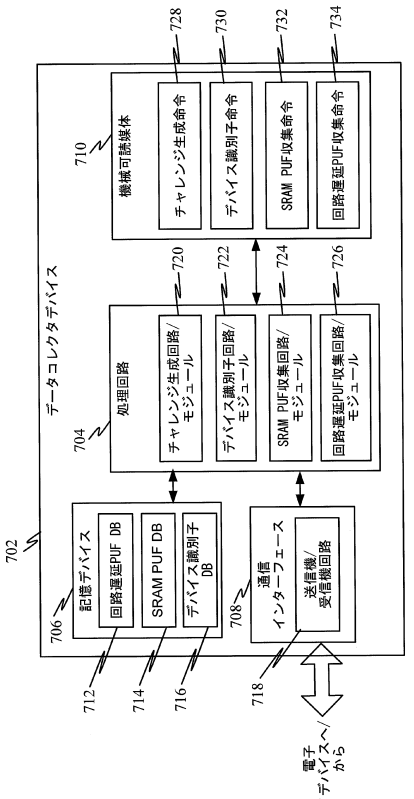
【図５】



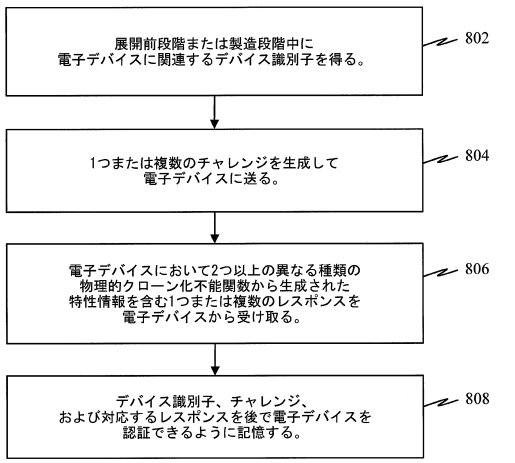
【図６】



【図７】

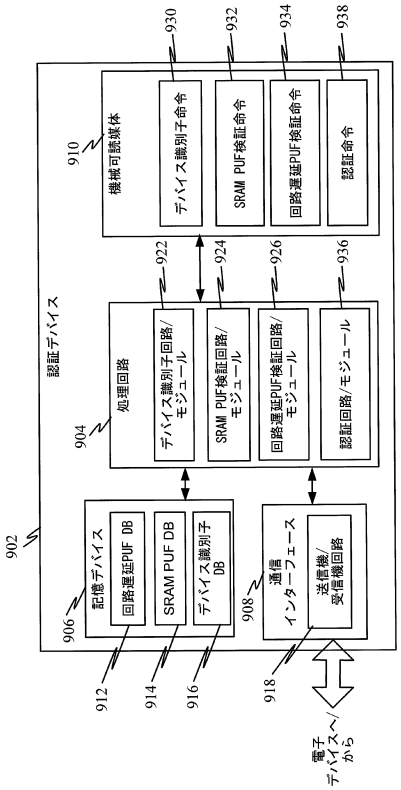


【図８】

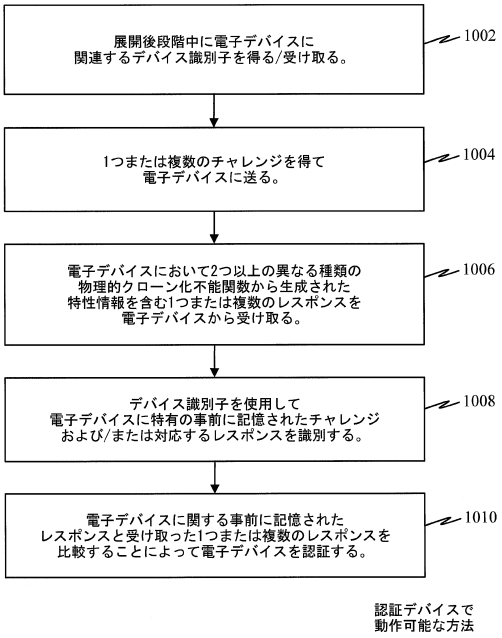


データコレクタデバイスで動作可能な方法

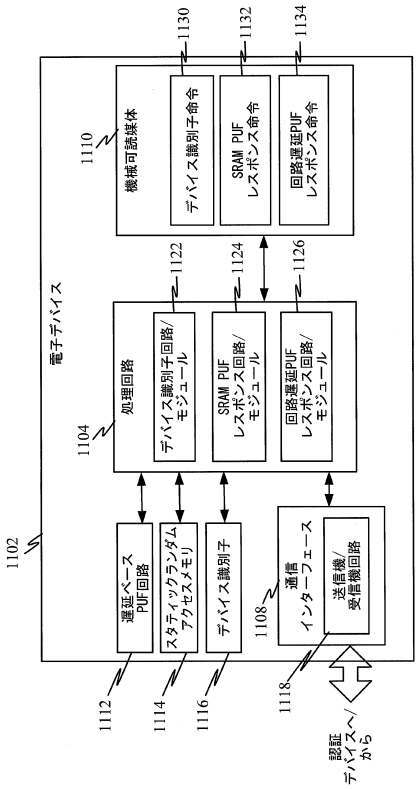
【図９】



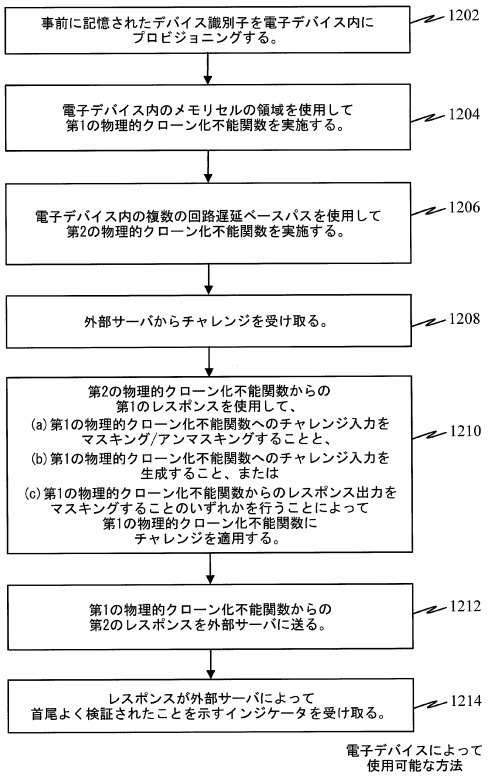
【図１０】



【図１１】



【図１２】



フロントページの続き

(72)発明者　デイヴィッド・エム・ジェイコブソン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ヤフェイ・ヤン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　アダム・ジェー・ドリュー
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ブライアン・マーク・ローゼンバーグ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　青木　重徳

(56)参考文献　欧州特許出願公開第０２６１５５７１（ＥＰ，Ａ１）
特表２００８－５１６４７２（ＪＰ，Ａ）
特開２００３－１９８５２８（ＪＰ，Ａ）
米国特許第０８５１６２６９（ＵＳ，Ｂ１）
米国特許出願公開第２０１２／０１３１３４０（ＵＳ，Ａ１）
欧州特許出願公開第０２６２６８１６（ＥＰ，Ａ１）
山本　大　ほか，ラッチの乱数出力位置を利用したＰＵＦによるＩＤ生成／認証システムの信頼性向上手法，２０１１年　暗号と情報セキュリティシンポジウム概要集，日本，２０１１年　暗号と情報セキュリティシンポジウム実行委員会，２０１１年　1月２５日，２Ｄ１－１，ｐｐ．１－８

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１０
Ｇ０６Ｆ　　２１／４４