(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6359035号
(P6359035)
(45)発行日　平成30年7月18日(2018.7.18)　(24)登録日　平成30年6月29日(2018.6.29)

(51)Int.Cl.　　F I
H04L 9/10 (2006.01)　　H04L 9/00 621Z
G01R 31/30 (2006.01)　　G01R 31/30

請求項の数 44　(全 25 頁)

(21)出願番号	特願2015-557029 (P2015-557029)
(86)(22)出願日	平成26年2月5日 (2014.2.5)
(65)公表番号	特表2016-508003 (P2016-508003A)
(43)公表日	平成28年3月10日 (2016.3.10)
(86)国際出願番号	PCT/US2014/014896
(87)国際公開番号	WO2014/124023
(87)国際公開日	平成26年8月14日 (2014.8.14)
審査請求日	平成28年2月24日 (2016.2.24)
審判番号	不服2016-17983 (P2016-17983/J1)
審判請求日	平成28年12月1日 (2016.12.1)
(31)優先権主張番号	13/764,507
(32)優先日	平成25年2月11日 (2013.2.11)
(33)優先権主張国	米国 (US)

早期審査対象出願

(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】リング発振器ベースの物理的複製不可関数および年齢検知回路を使用した集積回路識別およびディペンダビリティ検証

(57)【特許請求の範囲】
【請求項１】
集積回路であって、
部分的に、物理的複製不可関数(PUF)を実装するように構成される第1の複数のリング発振器と、
部分的に、前記集積回路の年齢を提供する年齢センサ回路を実装するように構成される第2の複数のリング発振器と、
前記第1の複数のリング発振器および前記第2の複数のリング発振器と結合される、リング発振器選択回路と
を備え、
前記リング発振器選択回路が、前記第1の複数のリング発振器および/または前記第2の複数のリング発振器のうちから、少なくとも2つのリング発振器を選択するように適合され、
前記リング発振器選択回路が前記PUFおよび前記年齢センサ回路によって共通に共有される、集積回路。
【請求項２】
前記2つのリング発振器出力を受け取って比較し、出力信号を生成するように適合される出力機能回路
をさらに備える、請求項1に記載の集積回路。
【請求項３】

前記第1の複数のリング発振器および前記第2の複数のリング発振器が、少なくとも1つの共通に共有されるリング発振器を含む、請求項1に記載の集積回路。

【請求項４】

前記リング発振器選択回路が、前記第1の複数のリング発振器および前記第2の複数のリング発振器から出力を受け取る2つ以上の選択スイッチを含み、前記選択スイッチが前記少なくとも2つのリング発振器出力を選択する、請求項1に記載の集積回路。

【請求項５】

前記リング発振器選択回路が、処理回路により受け取られるチャレンジに応答して、前記少なくとも2つのリング発振器出力を選択する、請求項1に記載の集積回路。

【請求項６】

前記リング発振器選択回路が、前記チャレンジに応答して前記処理回路に前記少なくとも2つのリング発振器出力を提供する、請求項5に記載の集積回路。

【請求項７】

前記第1の複数のリング発振器が、

前記第1の複数のリング発振器のうちの少なくとも2つのリング発振器を選択的にイネーブルにすること

により、前記物理的複製不可関数を実装し、前記第1の複数のリング発振器の間の製造ばらつきに起因する周波数ばらつきが固有の識別子を生成する、請求項1に記載の集積回路。

【請求項８】

選択的にイネーブルにされる前記2つのリング発振器は、互いから少なくとも10μm離れて配置される、請求項7に記載の集積回路。

【請求項９】

前記第2の複数のリング発振器が、

前記第2の複数のリング発振器のうちの第1のリング発振器を連続的に稼働すること、

年齢検出が確認されているのでない限り、前記第2の複数のリング発振器のうちの第2のリング発振器をアイドル状態に維持すること、および

前記第1のリング発振器と前記第2のリング発振器との間の周波数差分測定を実施することによる回路年齢情報を確認すること、

により前記年齢センサ回路を実装する、請求項1に記載の集積回路。

【請求項１０】

前記第2の複数のリング発振器のうちの前記第1および第2のリング発振器が、各々の10μm以内に配置される、請求項9に記載の集積回路。

【請求項１１】

前記第2の複数のリング発振器のうちの連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対が、前記集積回路の様々な部分にわたって分散され、連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の前記対が配置される前記集積回路の前記部分の局所的な回路信頼性情報を生成する、請求項9に記載の集積回路。

【請求項１２】

集積回路を製造する方法であって、

部分的に、物理的複製不可関数(PUF)を実装するように構成される第1の複数のリング発振器を提供するステップと、

部分的に、前記集積回路の年齢を提供する年齢センサ回路を実装するように構成される第2の複数のリング発振器を提供するステップと、

リング発振器選択回路を提供するステップと、

前記リング発振器選択回路を前記第1の複数のリング発振器および前記第2の複数のリング発振器と結合するステップと

を含み、

前記リング発振器選択回路が、前記第1の複数のリング発振器および/または前記第2の

複数のリング発振器のうちから、少なくとも2つのリング発振器を選択するように適合され、
前記リング発振器選択回路を、前記PUFと前記年齢センサ回路との間で共有する、方法。
【請求項１３】
前記2つのリング発振器出力を受け取って比較し、出力信号を生成するように適合される出力機能回路を提供するステップをさらに含む、請求項12に記載の方法。
【請求項１４】
前記第1の複数のリング発振器と前記第2の複数のリング発振器との間で少なくとも1つのリング発振器を共有するステップをさらに含む、請求項12に記載の方法。
【請求項１５】
前記リング発振器選択回路が、前記第1の複数のリング発振器および前記第2の複数のリング発振器から出力を受け取るように適合される2つ以上の選択スイッチを含み、前記選択スイッチが前記少なくとも2つのリング発振器出力を選択する、請求項12に記載の方法。
【請求項１６】
前記リング発振器選択回路が、処理回路により受け取られるチャレンジに応答して、前記少なくとも2つのリング発振器出力を選択するように適合される、請求項12に記載の方法。
【請求項１７】
前記リング発振器選択回路が、前記チャレンジに応答して、前記少なくとも2つのリング発振器出力を前記処理回路に提供するように適合される、請求項16に記載の方法。
【請求項１８】
前記第1の複数のリング発振器が、
前記第1の複数のリング発振器のうちの少なくとも2つのリング発振器を選択的にイネーブルにすること
により、前記物理的複製不可関数を実装するように適合され、前記第1の複数のリング発振器の間の製造ばらつきに起因する周波数ばらつきが固有の識別子を生成する、請求項12に記載の方法。
【請求項１９】
選択的にイネーブルにされるように適合される前記2つのリング発振器は、互いから少なくとも10μm離れて配置される、請求項18に記載の方法。
【請求項２０】
前記第2の複数のリング発振器が、
前記第2の複数のリング発振器のうちの第1のリング発振器を連続的に稼働すること、
年齢検出が確認されているのでない限り、前記第2の複数のリング発振器のうちの第2のリング発振器をアイドル状態に維持すること、および
前記第1のリング発振器と前記第2のリング発振器との間の周波数差分測定を実施することによる回路年齢情報を確認すること
により前記年齢センサ回路を実装するように適合される、請求項12に記載の方法。
【請求項２１】
前記第2の複数のリング発振器のうちの前記第1および第2のリング発振器が、各々の10μm以内に配置される、請求項20に記載の方法。
【請求項２２】
前記第2の複数のリング発振器のうちの連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対を、前記集積回路の様々な部分にわたって分散し、連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の前記対が配置される前記集積回路の前記部分の局所的な回路信頼性情報を生成するステップ
をさらに含む、請求項20に記載の方法。
【請求項２３】

集積回路であって、
物理的複製不可関数(PUF)を実装するための手段と、
前記集積回路の年齢を提供する年齢センサ回路を実装するための手段と、
前記PUFを実装するための前記手段および前記年齢センサ回路を実装するための前記手段に結合される信号を選択するための手段と
を備え、
選択するための前記手段が、前記PUFを実装するための前記手段および前記年齢センサ回路を実装するための前記手段のうちの少なくとも1つから出力される、少なくとも2つの信号を選択するように適合され、
選択するための前記手段が前記PUFを実装するための前記手段および前記年齢センサ回路を実装するための前記手段によって共通に共有される、集積回路。
【請求項２４】
信号を比較するための手段をさらに備え、比較するための前記手段は、前記PUFを実装するための前記手段および前記年齢センサ回路を実装するための前記手段のうちの前記少なくとも1つから出力される前記2つの信号を受け取って比較するように適合されて、比較するための前記手段が出力信号を生成する、請求項23に記載の集積回路。
【請求項２５】
前記PUFを実装するための前記手段および前記年齢センサ回路を実装するための前記手段が、少なくとも1つの共通に共有されるリング発振器を含む、請求項23に記載の集積回路。
【請求項２６】
前記PUFを実装するための前記手段が、
前記PUFを実装するための前記手段の少なくとも2つのリング発振器を選択的にイネーブルにすること
により実施され、前記PUFを実装するための前記手段間の製造ばらつきに起因する周波数ばらつきが固有の識別子を生成する、請求項23に記載の集積回路。
【請求項２７】
前記年齢センサ回路を実装するための前記手段が、
前記年齢センサ回路を実装するための前記手段の第1のリング発振器を連続的に稼働すること、
年齢検出が確認されているのでない限り、前記年齢センサ回路を実装するための前記手段の第2のリング発振器をアイドル状態に維持すること、および
前記第1のリング発振器と前記第2のリング発振器との間の周波数差分測定を実施することによる回路年齢情報を確認すること
により実施される、請求項23に記載の集積回路。
【請求項２８】
前記年齢センサ回路を実装するための前記手段の連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対は、前記集積回路の様々な部分にわたって分散され、連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の前記対が配置される前記集積回路の前記部分の局所的な回路信頼性情報を生成する、請求項27に記載の集積回路。
【請求項２９】
その上に1つまたは複数の命令が記憶されるコンピュータ可読記憶媒体であって、少なくとも1つのプロセッサにより実行されると、前記プロセッサに、
第1の複数のリング発振器を有する物理的複製不可関数(PUF)を実装させ、
集積回路の年齢を提供する第2の複数のリング発振器を有する年齢センサ回路を実装させ、
前記第1の複数のリング発振器および前記第2の複数のリング発振器と結合されるリング発振器選択回路を使用して、前記第1の複数のリング発振器および/または前記第2の複数のリング発振器のうちから、少なくとも2つのリング発振器を選択させ、

前記リング発振器選択回路が、前記PUFおよび前記年齢センサ回路によって共通に共有される、コンピュータ可読記憶媒体。

【請求項３０】

前記第1の複数のリング発振器および前記第2の複数のリング発振器が、少なくとも1つの共通に共有されるリング発振器を含む、請求項29に記載のコンピュータ可読記憶媒体。

【請求項３１】

バスに結合される複数の構成要素であって、各構成要素が、(a)固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)、および(b)対応する構成要素についての回路年齢情報を提供する年齢センサ回路を実装するように構成されるリング発振器の配列を有する構成要素と、

バスに結合される処理回路であって、

前記1つまたは複数の構成要素についての年齢情報を獲得すること、

前記構成要素のうちの少なくとも1つについての前記固有の識別子またはキーを獲得すること、および/または

異なる構成要素からのリング発振器の2つ以上の配列から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成すること

のうちの少なくとも1つを実施するように適合される処理回路と

を備える、電子デバイス。

【請求項３２】

リング発振器の各配列が、前記PUFを実装するための第1の複数のリング発振器と、前記年齢センサ回路を実装するための第2の複数のリング発振器とを含む、請求項31に記載の電子デバイス。

【請求項３３】

前記第1の複数のリング発振器および前記第2の複数のリング発振器が、少なくとも1つの共通に共有されるリング発振器を含む、請求項32に記載の電子デバイス。

【請求項３４】

各構成要素が、前記処理回路により受け取られたチャレンジに応答して、少なくとも2つのリング発振器出力を選択する選択回路をさらに備える、請求項32に記載の電子デバイス。

【請求項３５】

各構成要素が、前記2つのリング発振器出力を受け取って比較し、前記比較に基づいて出力信号を生成し、前記出力信号を前記処理回路に提供するように適合される出力機能回路をさらに備える、請求項34に記載の電子デバイス。

【請求項３６】

前記選択回路が、前記2つのリング発振器出力を前記処理回路に提供する、請求項34に記載の電子デバイス。

【請求項３７】

電子デバイスを製造する方法であって、

バスを提供するステップと、

処理回路を提供するステップと、

複数の構成要素を提供するステップであって、各構成要素が、(a)固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)、および(b)対応する構成要素についての回路年齢情報を提供する年齢センサ回路を実装するように構成されるリング発振器の配列を有するステップと、

前記複数の構成要素を前記バスに結合させるステップと、

前記処理回路を前記バスに結合させるステップと

を含み、処理回路が、

前記1つまたは複数の構成要素についての年齢情報を獲得すること、

前記構成要素のうちの少なくとも1つについての前記固有の識別子またはキーを獲得すること、および/または

異なる構成要素からのリング発振器の2つ以上の配列から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成すること
のうちの少なくとも1つを実施するように適合される、方法。
【請求項３８】
リング発振器の各配列が、前記PUFを実装するための第1の複数のリング発振器と、前記年齢センサ回路を実装するための第2の複数のリング発振器とを含む、請求項37に記載の方法。
【請求項３９】
前記第1の複数のリング発振器および前記第2の複数のリング発振器が、少なくとも1つの共通に共有されるリング発振器を含む、請求項38に記載の方法。
【請求項４０】
各構成要素が、前記処理回路により受け取られたチャレンジに応答して、少なくとも2つのリング発振器出力を選択する選択回路をさらに備える、請求項38に記載の方法。
【請求項４１】
各構成要素が、前記2つのリング発振器出力を比較し、前記比較に基づいて出力信号を生成し、前記出力信号を前記処理回路に提供するように適合される出力機能回路をさらに備える、請求項40に記載の方法。
【請求項４２】
前記選択回路が、前記2つのリング発振器出力を前記処理回路に提供する、請求項40に記載の方法。
【請求項４３】
通信するための手段に結合される複数の構成要素であって、各構成要素が、固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)を実装するための手段、および対応する構成要素についての回路年齢情報を提供するための手段を有する構成要素と、
通信するための前記手段への処理をするための手段であって、
前記1つまたは複数の構成要素についての年齢情報を獲得すること、
前記構成要素のうちの少なくとも1つについての前記固有の識別子またはキーを獲得すること、および/または
異なる構成要素からの前記PUFを実装するための2つ以上の手段および異なる構成要素から回路年齢情報を提供するための手段から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成すること
のうちの少なくとも1つを実施するように適合される手段と
を備える、電子デバイス。
【請求項４４】
その上に1つまたは複数の命令が記憶されるコンピュータ可読記憶媒体であって、前記命令が、少なくとも1つのプロセッサにより実行されると、前記プロセッサに、
バスに結合され、それぞれがリング発振器の配列を有する複数の構成要素に、(a)固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)、および(b)対応する構成要素についての回路年齢情報を提供する年齢センサ回路を実装させることと、
前記バスに結合される処理回路に、
前記1つまたは複数の構成要素についての年齢情報を獲得すること、
前記構成要素のうちの少なくとも1つについての前記固有の識別子またはキーを獲得すること、および/または
異なる構成要素からのリング発振器の2つ以上の配列から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成することを行わせることと
を行わせる、コンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
様々な特徴は、集積回路に関し、より詳細には、リング発振器ベースの物理的複製不可

関数および年齢検知回路(age detection circuitry)を使用する集積回路(IC)識別(ID)およびICディペンダビリティ(dependability)検証に関する。

【背景技術】

【０００２】

広範囲にわたるコンピューティングの時代では、ソフトウェア著作権保護、偽造IC(すなわち、チップ)、およびシステム信頼性(reliability)について、多くのセキュリティ問題が存在する。ソフトウェア保護は、ソフトウェアの無認可複製を防止するために使用される、コンピュータセキュリティ技法の一群である。言い換えれば、ソフトウェアは、ユーザがソフトウェアを使用するために適正に認可されているのかどうかを判定することができ、その場合にのみ稼働しなければならない。ソフトウェア保護に関する別の問題は、ソフトウェアが稼働しているチップまたはプラットフォームが偽造チップであるかどうかをどのように識別するかである。偽造チップは、業界全体にわたって急増してきており、電子機器のサプライチェーンに対するリスクである。その結果、電子機器のサプライチェーンにおいて、偽造チップの使用を識別し制限することが極めて重要である。

【０００３】

オンチップの物理的複製不可関数(PUF: Physical Unclonable Function)は、IC内部の製造プロセスばらつきを利用する、チップ固有のチャレンジ応答機構(challenge-response mechanism)である。チャレンジと対応する応答との間の関係は、IC中のロジックおよび相互接続における、複雑で統計的なばらつきにより決定される。IC中の異なるPUF実装形態は、従来技術中に見いだすことができる。たとえば、リング発振器ベースのPUFは、同一にレイアウトされるリング発振器の周波数にランダムだが統計的なばらつきを引き起こす、ICの製造プロセスばらつきを利用する。

【０００４】

図1は、従来技術に見いだされる、リング発振器ベースのPUF回路102の一例を図示する概略ブロック図である。複数のリング発振器(RO: ring oscillator)104は、並行してイネーブルにすることができ、それらの出力は、2つ以上のスイッチ(マルチプレクサ)106、108に送られる。チャレンジは、次に各スイッチ106、108に複数のRO104から単一のROを選択させる、スイッチ106、108への入力としての役割を果たす。スイッチ106、108へ送られるチャレンジは、各スイッチ106、108が異なるROを選択するように設計される。選択されるROは、それぞれを同一に作るような試みでそれぞれが製造されたが、半導体レベルでのわずかな製造ばらつきに起因して、それらに関係するわずかに異なる共振周波数をそれぞれが有する。PUF出力応答は、カウンタ110および112により測定/記憶されるような、これらの選択されるリング発振器の周波数の、対比較114により生成される。たとえば、第1のカウンタ110が第2のカウンタ112よりも高い周波数を検出する場合、論理「1」を生成してよく、そうでない場合、論理「0」を生成してよい。このやり方では、なされる比較はチャレンジ/応答機構を表し、選択されるRO対がチャレンジであり、RO周波数比較結果が応答である。

【０００５】

理想的には、チャレンジとして選択される各RO対は、固有の応答を生成することになる。生成される応答は、チャレンジ入力に基づいて前もって決定することが可能であるべきでない。さらに、PUF中への同じチャレンジ入力が、毎回同じ応答出力を生成するべきである。しかし、とりわけ、時間の経過および使用につれて、これらの特性のうちの1つまたは複数が、真のままでない場合がある。たとえば、時間の経過につれて、使いすぎに起因して1つのROの周波数が遅くなる場合があり、同じチャレンジ入力が、異なる応答出力を生成する場合がある(たとえば、論理「1」が「0」へと反転する場合がある)。

【０００６】

上に記載されたもののようなROベースのPUF回路が使用されて、チップ識別子番号を生成することができる。しかし、単にこのやり方で生成されるチップ識別子番号に単に依拠するチップ識別セキュリティシステムは、本質的に制限される。

【０００７】

CMOSプロセス技術は、積極的なスケーリングのロードマップに従い続けているので、信頼できる回路を設計することは、各技術的な里程標で一層難しくなった。ナノスケールのCMOSデバイスで電界が増加し続けるので、バイアス温度不安定性(BTI: bias temperature instability)、ホットキャリア注入(HCI: hot carrier injection)、および絶縁膜経時破壊(TDDB: time-dependent dielectric breakdown)などの信頼性問題がより一般化した。これらのチャレンジの最も緊急のものの1つは、PMOSトランジスタのSi-SiO界面内のトラップ生成により引き起こされる負バイアス温度不安定性(NBTI: negative bias temperature instability)である。その結果、デジタル回路劣化の正確な測定は、経年変化耐性のある回路の設計の鍵となる態様である。

【０００８】

図2は、従来技術に見いだされる、IC年齢センサ回路(IC age sensor circuit)200の概略ブロック図を図示する。2つのRO202、204出力は、RO202、204間の周波数差f_{diff}を決定する、位相比較器206に結合される。第1のRO202(たとえば、RO_{STR})は、それが、チップの定格電源電圧V_{DD}よりも高い、電源電圧レベルV_{DD_STR}でほとんど常に電源投入される(すなわち、それは連続的に動作する)ので、「ストレスを受ける」。対照的に、第2のRO204(たとえば、RO_{REF})は、典型的には、電源切断される(すなわち、それは動作しない)。次いで、測定を希望する時間期間に、両方のROは、定格電源電圧V_{DD}で動作され(すなわち、オンにされ)、RO202、204間の周波数差が位相比較器206により測定される。経時的に、ストレスを受けるRO202の動作周波数は、ストレスを受けないRO204の動作周波数と比較して減少することになる(すなわち、f_{diff}が増加することになる)。IC年齢センサ回路200の年齢、したがって今度はセンサ回路200があるより大きい回路の年齢を、次いで、f_{diff}が経時的に増加する量を分析することにより決定することができる。

【発明の概要】

【発明が解決しようとする課題】

【０００９】

上に記載された回路の各々は、ICの活性表面上の貴重なチップ面積を占有する。したがって、そのようなシステムを実装するために必要なチップ面積を減少した、PUFセキュリティ回路およびIC年齢センサ回路によりもたらされる利益を抽出することが可能な改善された回路設計が有益である。さらに、偽造チップを識別し、チップの健全性を監視する(すなわち、チップ年齢を検出する)、システムの能力を増加させる必要が常にある。

【課題を解決するための手段】

【００１０】

1つの特徴は、部分的に、物理的複製不可関数(PUF)を実装するように構成される第1の複数のリング発振器と、部分的に、年齢センサ回路を実装するように構成される第2の複数のリング発振器と、第1の複数のリング発振器および第2の複数のリング発振器と結合される、リング発振器選択回路とを備え、リング発振器選択回路が、第1の複数のリング発振器および/または第2の複数のリング発振器のうちの少なくとも1つから、少なくとも2つのリング発振器出力を選択するように適合され、リング発振器選択回路がPUFおよび年齢センサ回路によって共通に共有される、集積回路を提供する。一態様によれば、集積回路は、2つのリング発振器出力を受け取って比較し、出力信号を生成するように適合される出力機能回路をさらに備える。別の態様によれば、第1の複数のリング発振器および第2の複数のリング発振器は、少なくとも1つの共通に共有されるリング発振器を含む。さらに別の態様によれば、選択回路は、第1の複数のリング発振器および第2の複数のリング発振器から出力を受け取る、2つ以上の選択スイッチを含み、選択スイッチが少なくとも2つのリング発振器出力を選択する。

【００１１】

一態様によれば、選択回路は、処理回路により受け取られるチャレンジに応答して、少なくとも2つのリング発振器出力を選択する。別の態様によれば、選択回路は、チャレンジに応答して処理回路に少なくとも2つのリング発振器出力を提供する。さらに別の態様によれば、第1の複数のリング発振器は、第1の複数のリング発振器のうちの少なくとも2

つのリング発振器を選択的にイネーブルにすることにより、物理的複製不可関数を実装し、第1の複数のリング発振器の間の製造ばらつきに起因する周波数ばらつきが固有の識別子を生成する。別の態様によれば、選択的にイネーブルにされる2つのリング発振器は、互いから少なくとも10μm離れて配置される。

【００１２】

一態様によれば、第2の複数のリング発振器は、第2の複数のリング発振器のうちの第1のリング発振器を連続的に稼働すること、年齢検出が確認されているのでない限り第2の複数のリング発振器のうちの第2のリング発振器をアイドル状態に維持すること、および第1のリング発振器と第2のリング発振器との間の周波数差分測定(differential frequency measurement)を実施することによる回路年齢情報を確認することにより年齢センサ回路を実装する。別の態様によれば、第2の複数のリング発振器のうちの第1および第2のリング発振器は、各々の10μm以内に配置される。さらに別の態様によれば、第2の複数のリング発振器のうちの連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対は、集積回路の様々な部分にわたって分散され、連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対が配置される集積回路の部分の局所的な回路信頼性情報を生成する。

【００１３】

別の特徴は、集積回路を製造する方法を提供し、方法は、部分的に、物理的複製不可関数(PUF)を実装するように構成される第1の複数のリング発振器を提供するステップと、部分的に、年齢センサ回路を実装するように構成される第2の複数のリング発振器を提供するステップと、リング発振器選択回路を提供するステップと、リング発振器選択回路を第1の複数のリング発振器および第2の複数のリング発振器と結合するステップとを含み、リング発振器選択回路は、第1の複数のリング発振器および/または第2の複数のリング発振器のうちの少なくとも1つから、少なくとも2つのリング発振器出力を選択するように適合され、リング発振器選択回路を、PUFと年齢センサ回路との間で共有する。一態様によれば、方法は、2つのリング発振器出力を受け取って比較し、出力信号を生成するように適合される出力機能回路を提供するステップをさらに含む。別の態様によれば、方法は、第1の複数のリング発振器と第2の複数のリング発振器との間で少なくとも1つのリング発振器を共有するステップをさらに含む。さらに別の態様によれば、選択回路は、第1の複数のリング発振器および第2の複数のリング発振器から出力を受け取るように適合される、2つ以上の選択スイッチを含み、選択スイッチが少なくとも2つのリング発振器出力を選択する。別の態様によれば、選択回路は、処理回路により受け取られるチャレンジに応答して、少なくとも2つのリング発振器出力を選択するように適合される。

【００１４】

一態様によれば、選択回路は、チャレンジに応答して、少なくとも2つのリング発振器出力を処理回路に提供するように適合される。別の態様によれば、第1の複数のリング発振器は、第1の複数のリング発振器のうちの少なくとも2つのリング発振器を選択的にイネーブルにすることにより、物理的複製不可関数を実装するように適合され、第1の複数のリング発振器の間の製造ばらつきに起因する周波数ばらつきが固有の識別子を生成する。さらに別の態様によれば、第2の複数のリング発振器は、第2の複数のリング発振器のうちの第1のリング発振器を連続的に稼働すること、年齢検出が確認されているのでない限り第2の複数のリング発振器のうちの第2のリング発振器をアイドル状態に維持すること、および第1のリング発振器と第2のリング発振器との間の周波数差分測定を実施することによる回路年齢情報を確認することにより年齢センサ回路を実装するように適合される。さらに別の態様によれば、方法は、第2の複数のリング発振器のうちの連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対を、集積回路の様々な部分にわたって分散し、連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対が配置される集積回路の部分の局所的な回路信頼性情報を生成するステップをさらに含む。

【００１５】

別の特徴は、物理的複製不可関数(PUF)を実装するための手段と、年齢センサ回路を実装するための手段と、PUFを実装するための手段および年齢センサ回路を実装するための手段に結合される信号を選択するための手段とを備える集積回路であって、選択するための手段が、PUFを実装するための手段および年齢センサ回路を実装するための手段のうちの少なくとも1つから出力される、少なくとも2つの信号を選択するように適合され、選択するための手段がPUFを実装するための手段および年齢センサ回路を実装するための手段によって共通に共有される、集積回路を提供する。一態様によれば、集積回路は、信号を比較するための手段をさらに備え、比較するための手段は、PUFを実装するための手段および年齢センサ回路を実装するための手段のうちの少なくとも1つから出力される2つの信号を受け取って比較するように適合されて、比較するための手段が出力信号を生成する。別の態様によれば、PUFを実装するための手段および年齢センサ回路を実装するための手段が、少なくとも1つの共通に共有されるリング発振器を含む。さらに別の態様によれば、PUFを実装するための手段が、PUFを実装するための手段の少なくとも2つのリング発振器を選択的にイネーブルにすることにより実施され、第1の複数のリング発振器の間の製造ばらつきに起因する周波数ばらつきが固有の識別子を生成する。

【００１６】

一態様によれば、年齢センサ回路を実装するための手段は、年齢センサ回路を実装するための手段の第1のリング発振器を連続的に稼働すること、年齢検出が確認されているのでない限り年齢センサ回路を実装するための手段の第2のリング発振器をアイドル状態に維持すること、および第1のリング発振器と第2のリング発振器との間の周波数差分測定を実施することによる回路年齢情報を確認することにより実施される。別の態様によれば、年齢センサ回路を実装するための手段の連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対は、集積回路の様々な部分にわたって分散され、連続的に稼働しているリング発振器とアイドル状態にされるリング発振器の対が配置される集積回路の部分の局所的な回路信頼性情報を生成する。

【００１７】

別の特徴は、その上に1つまたは複数の命令が記憶されるコンピュータ可読記憶媒体を提供し、少なくとも1つのプロセッサにより実行されると、プロセッサに、第1の複数のリング発振器を有する物理的複製不可関数(PUF)を実装させ、第2の複数のリング発振器を有する年齢センサ回路を実装させ、第1の複数のリング発振器および第2の複数のリング発振器と結合されるリング発振器選択回路を使用して、第1の複数のリング発振器および/または第2の複数のリング発振器のうちの少なくとも1つから、少なくとも2つのリング発振器出力を選択させ、リング発振器選択回路が、PUFおよび年齢センサ回路によって共通に共有される。

【００１８】

別の特徴は、バスに結合される複数の構成要素を備える電子デバイスを提供し、各構成要素は、(a)固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)、および(b)対応する構成要素についての回路年齢情報を提供する年齢センサ回路を実装するように構成されるリング発振器の配列、ならびにバスに結合される処理回路を有し、処理回路は、1つまたは複数の構成要素についての年齢情報を獲得すること、構成要素のうちの少なくとも1つについての固有の識別子またはキーを獲得すること、および/または異なる構成要素からのリング発振器の2つ以上の配列から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成することのうちの少なくとも1つを実施するように適合される。一態様によれば、リング発振器の各配列は、PUFを実装するための第1の複数のリング発振器と、年齢センサ回路を実装するための第2の複数のリング発振器とを含む。別の態様によれば、各構成要素は、処理回路により受け取られたチャレンジに応答して、少なくとも2つのリング発振器出力を選択する選択回路をさらに備える。さらに別の態様によれば、各構成要素は、2つのリング発振器出力を受け取って比較し、比較に基づいて出力信号を生成し、出力信号を処理回路に提供するように適合される出力機能回路をさらに備える。別の態様によれば、選択回路は、2つのリング発振器出力を処理回路に提供

する。
【００１９】
別の特徴は、電子デバイスを製造する方法を提供し、方法は、バスを提供するステップと、処理回路を提供するステップと、複数の構成要素を提供するステップであって、各構成要素が、(a)固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)、および(b)対応する構成要素についての回路年齢情報を提供する年齢センサ回路を実装するように構成されるリング発振器の配列を有するステップと、複数の構成要素をバスに結合させるステップと、処理回路をバスに結合させるステップとを含み、処理回路が、1つまたは複数の構成要素についての年齢情報を獲得すること、構成要素のうちの少なくとも1つについての固有の識別子またはキーを獲得すること、および/または異なる構成要素からのリング発振器の2つ以上の配列から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成することのうちの少なくとも1つを実施するように適合される。
【００２０】
別の特徴は、通信するための手段に結合される複数の構成要素を含む電子デバイスを提供し、各構成要素は、固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)を実装するための手段、および対応する構成要素についての回路年齢情報を提供するための手段、ならびに通信するための手段への処理をするための手段を有し、処理するための手段が、1つまたは複数の構成要素についての年齢情報を獲得すること、構成要素のうちの少なくとも1つについての固有の識別子またはキーを獲得すること、および/または異なる構成要素からのPUFを実装するための2つ以上の手段および回路年齢情報を提供するための手段から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成することのうちの少なくとも1つを実施するように適合される。
【００２１】
別の特徴は、その上に1つまたは複数の命令が記憶されるコンピュータ可読記憶媒体を提供し、命令は、少なくとも1つのプロセッサにより実行されると、プロセッサに、バスに結合され、それぞれがリング発振器の配列を有する複数の構成要素に、(a)固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)、および(b)対応する構成要素についての回路年齢情報を提供する年齢センサ回路を実装させることと、バスに結合される処理回路に、1つまたは複数の構成要素についての年齢情報を獲得すること、構成要素のうちの少なくとも1つについての固有の識別子またはキーを獲得すること、および/または異なる構成要素からのリング発振器の2つ以上の配列から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成することを行わせることとを行わせる。
【図面の簡単な説明】
【００２２】
【図１】従来技術に見いだされる、リング発振器ベースのPUF回路の一例を図示する概略ブロック図である。
【図２】従来技術に見いだされる、IC年齢センサ回路を図示する概略ブロック図である。
【図３】例示的なチップ識別およびチップ健全性監視装置を図示する高レベル概略図である。
【図４】リング発振器を図示する概略ブロック図である。
【図５】PUFおよび年齢センサ回路を図示する概略ブロック図である。
【図６】チップ識別およびチップ健全性監視装置を図示する概略ブロック図である。
【図７】電子デバイスを図示する概略ブロック図である。
【図８】集積回路を製造する方法を図示する図である。
【図９】電子デバイスを製造する方法を図示する図である。
【発明を実施するための形態】
【００２３】
以下の記載において、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、これらの具体的な詳細なしで態様を実施できることを、当業者な

ら理解するであろう。たとえば、態様を不必要な詳細さで不明瞭にすることを回避するために、回路を、ブロック図で示す場合がある。他の事例では、本開示の態様を不明瞭にしないために、良く知られた回路、構造、および技法を詳細に示さない場合がある。

【００２４】

「例示的な」という用語は、本明細書では、「例、事例、または説明として働く」ということを意味するように使用される。本明細書で「例示的な」と記載される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、「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、または動作モードを含むことを要求しない。本明細書で使用される、「チップ健全性監視」または「健全性監視」という用語は、単に、ICおよび/またはIC内のモジュールの経年変化および/または使用に起因して、ICおよび/またはIC内のモジュールの信頼性および/またはディペンダビリティ問題を検出することを言う。

【００２５】

概要

一実装形態は、チップ年齢検出および(たとえば、固有の識別子/キーを生成するための)PUF機能の両方を提供するリング発振器(RO)ベースの回路を提供する。すなわち、年齢検出センサおよびPUFは、1つまたは複数のリング発振器チェーンおよび/または選択器回路を共有することにより、同じリング発振器回路配列で実装することができる。共通の、または共有される回路に、これらのセキュリティおよびチップ健全性監視機能の両方を一体化することによって、ダイ内に必要とされる面積を減少させる。

【００２６】

別の態様は、ホストシステム内の複数の構成要素中に、そのような二重目的のリング発振器回路を実装することを可能にする。ホストシステムは、したがって、個別の構成要素を監視し、システムの全体的な健全性を判定することが可能であり、異なる構成要素の2つ以上のそのようなリング発振器回路からの出力を組み合わせることにより、(たとえば、キー、識別子など)セキュリティ構成要素を構築することもできる。

【００２７】

例示的な機構

図3は、本開示の一態様に従う例示的なチップ識別およびチップ健全性監視装置300の高レベル概略図を図示する。装置300は、PUFおよび年齢センサ回路302、処理回路304、および/またはメモリ回路306を含むことができる。

【００２８】

PUFおよび年齢センサ回路302は、RO配列310、RO選択器回路312(たとえば、信号を選択するための手段)、および出力機能回路314(たとえば、信号を比較するための手段)を含む。RO配列310は、複数のRO316を含む。RO316の第1のグループはPUFモジュール318に関連付けされてよく、一方RO316の第2のグループはチップ年齢センサモジュール320に関連付けされてよい。特に、RO316のうちの1つまたは複数は、(同じ3つのROを両方が含む、モジュール318、320の重なった点線により示されるように)PUFモジュール318およびチップ年齢センサモジュール320の両方に関連付けされる。RO配列310中に示され、各モジュール318、320に関連付けされるRO316の数は、単に例示である。

【００２９】

RO配列310の複数のRO316の各々は、その周波数を表す出力322a、322b、322c、…、322nを有する。これらの周波数出力は、RO選択器回路312の中に入力される。RO選択器回路312は、複数のRO周波数出力322a、322b、322c、…、322nのうちの2つ(または、2つ以上)のRO周波数324a、324bを選択する。たとえば、選択器回路312は、RO周波数324a、324bを選択する1つまたは複数のスイッチ(たとえば、マルチプレクサ)を含んでよい。RO周波数324a、324bは、次いで、2つ(または、2つ以上)の周波数324a、324bを分析して出力応答326を生成する、出力機能回路314内に入力される。一態様では、出力機能回路314は、2つ(または、2つ以上)の入力周波数324a、324bのどちらがより高いのかに依存して、その出力信号(たとえば、論理「1」または「0」)を変える、単純な比較器回路であってよい。他の態様

では、出力機能回路314は、それが2つ(または、2つ以上)の入力周波数324a、324bに他の分析を実施して出力ストリング326を生成するように、ますます複雑であってよい。

【００３０】

とりわけ、処理回路304は、PUFおよび年齢センサ回路302への入力としての役割を果たすチャレンジ328を生成する。詳細には、チャレンジ328は、RO周波数出力322a、322b、322c、…、322nのどの2つ(または、2つ以上)を、出力324a、324bとして選択するかをRO選択器回路312に命令するデータを含む。チャレンジ328は、RO配列310中のRO316の選択を、イネーブルまたはディセーブル(たとえば、電源投入または電源切断)にするデータも含んでよい。一例では、チャレンジ328は、PUFおよび年齢センサ回路302に対し、そのPUF機能を利用して、識別値を生成する要求であってよい。別の例によれば、チャレンジ328は、PUFおよび年齢センサ回路302に対し、その回路年齢検知機能を利用して、チップ健全性監視情報を提供する要求であってよい。両方の場合で、処理回路304は、そのチャレンジ328に対し、PUFおよび年齢センサ回路302からの応答326を受け取る。

【００３１】

一例によれば、メモリ回路306は、たとえば、チップ識別子330および/またはチップ年齢値332を記憶する、読取り専用メモリ(ROM)であってよい。メモリチップ306は、処理回路304に通信可能に結合されてよい(334)。たとえば、処理回路304は、PUFおよび年齢センサ回路302にチップ識別チャレンジ328を発行してよい。PUFおよび年齢センサ回路302は、そのPUF機能を使用して、PUFおよび年齢センサ回路302があるICまたはICサブモジュールに固有である応答326としての、チップ識別値を生成してよい。処理回路304は、次いで、チップ識別値応答326を、メモリ306に記憶されるチップ識別子330と比較してよい。2つが一致する場合、ICおよび/または処理回路304上で実行される他のソフトウェアは、正常に動作し続けてよく、他の場合、エラーメッセージを生成してよく、ICおよび/または処理回路304の動作を停止してよい。別の例として、処理回路304は、PUFおよび年齢センサ回路302に健全性監視チャレンジ328を発行してよい。PUFおよび年齢センサ回路302は、その健全性監視機能を使用して、処理回路304に回路年齢情報応答326を提供してよい。処理回路304は、次いで、回路年齢情報応答326を、メモリ306内に記憶される使用期限年数(expiration age)332と比較してよい。回路年齢情報応答326の値が使用期限年数332を超えない場合、ICおよび/または処理回路304上で実行される他のソフトウェアは、正常に動作し続けてよく、他の場合、エラーメッセージを生成してよく、ICおよび/または処理回路304の動作を停止してよい。

【００３２】

図4は、一態様に従うリング発振器400の概略ブロック図を図示する。RO400は、ANDゲート402および奇数のインバータ404a、404b、…、404nを含む。ANDゲート402は、少なくとも2つの入力端子406、408および出力端子410を有する。ANDゲートの出力端子410は、第1のインバータ404aへの入力であってよい。インバータ404a、404b、…は、次いで、示されるように直列に接続される。RO400の出力412は、次いで、ANDゲートの入力端子のうちの1つ406に結合される。他の入力端子408は、たとえば、図3に示される処理回路304と同様の処理回路により制御され得るイネーブル信号に結合される。図4を参照すると、RO400が十分に電力供給され、イネーブル信号がハイ(たとえば、論理値「1」)である場合、RO出力412は、論理値間で行ったり来たりしてトグル動作する(すなわち、「1」と「0」との間で行ったり来たりしてトグル動作する)ことになる。

【００３３】

図5は、一態様に従う、PUFおよび年齢センサ回路302の概略ブロック図を図示する。回路302は、複数のRO502、504、506、508、510、第1のスイッチ512、第2のスイッチ514、第1のカウンタ516、第2のカウンタ518、および比較器520を含む。図3および図5を参照すると、複数のRO502、504、506、508、510は、たとえば、RO配列310であってよい。スイッチ512、514は、たとえば、RO選択器312であってよい。同様に、カウンタ516、518、および比較器520は、たとえば、出力機能回路314であってよい。RO502、504、506、508、510は、たとえば、図4に示されるRO400であってよい。

【００３４】
図示される例では、RO502、504、506、508、510は、それらの機能に応じて3つのタイプに分類/グループ化され得る。第1のグループは、回路302のPUF機能のために主に使用される、第1の複数のRO502、504、506(たとえば、PUFを実装するための手段)からなる。N個のそのようなRO502、504、506があってよく、Nは、2以上の任意の正の整数である。単に1つの例として、Nは、512、1024、または2048であってよい。特に、PUF RO502、504、506は、図5に示される1つまたは複数のイネーブル信号(すなわち、$Enable_{PUF\_1}$、$Enable_{PUF\_2}$、$Enable_{PUF\_3}$)を使用して、選択的にイネーブルにされ得る(すなわち、時々オンにされ、時々オフにされる)。

【００３５】
第2のグループは、健全性監視のために主に使用される、少なくとも1つのRO508からなる。このRO508は、極めて大部分の時間イネーブルにされ、したがって、「ストレスを受けるRO」と標示される。一態様では、ストレスを受けるRO508は、PUF RO502、504、506などの他の回路により利用される定格電源電圧V_{DD}よりも高い、電源電圧V_{DD_STR}を利用してよい。別の態様では、ストレスを受けるRO508は、他のPUF RO502、504、506により使用される同じ定格電源電圧V_{DD}を利用してよい。第3のグループは、健全性監視のために主に使用される、少なくとも1つのRO510からなる。このRO510は、極めて大部分の時間ディセーブルにされ、したがって、「アイドル状態の基準RO」と標示される。ストレスを受けるRO508およびアイドル状態の基準RO510は、第2の複数のROと考えられてよく、年齢センサ回路を実装するための手段である。

【００３６】
動作の1つのモードでは、回路302は、そのPUF機能を利用して、キーまたは識別子を生成することができる。たとえば、回路302は、図3に示される処理回路304などの処理回路から、チップ識別子またはキー生成チャレンジ522を受け取ってよい。図5を参照すると、チャレンジ522は、複数のPUF RO502、504、506のうちの2つのPUF ROが、適切なイネーブル信号(たとえば、$Enable_{PUF\_1}$、$Enable_{PUF\_2}$、…、$Enable_{PUF_N}$のうちの2つ)をオンにすることにより、選択的に活動化される/イネーブルにされることを引き起こし得る。チャレンジ522は、2つのスイッチ512、514が、選択的に活動化される/イネーブルにされる複数の出力524、526、528のうちの2つの異なるRO出力を選択して通過させることも引き起こすことになる。したがって、各スイッチ512、514は、カウンタ516、518に1つのPUF RO信号530、532を提供する。RO出力530、532の周波数は、それらの対応するカウンタ316、318の値を増加させる働きをする。選択されるPUF RO間の小さい差異に起因して、RO出力530、532は、わずかに異なる周波数を有することになる。そのため、カウンタ516、518は、異なる速度で変化し、所定の時間期間後に異なるカウンタ値を有することになる。カウンタ516、518は、次いで、比較回路520により比較され、出力信号534が比較に基づいて生成される。たとえば、第1のカウンタ516の値が第2のカウンタ518の値よりも大きい場合に論理「1」が生成されてよく、他の場合に論理「0」が生成されてよい。このプロセスは、複数回実施されてよく、識別子または十分な長さのキー(たとえば、ビットストリング)が生成されるまで、比較のために、場合によっては異なるPUF RO502、504、506を毎回選択する。

【００３７】
別の動作のモードでは、回路302は、その健全性監視機能を利用して、回路302があるICまたはICサブモジュールの回路年齢情報を提供することができる。たとえば、回路302は、図3に示される処理回路304などの処理回路から、チップ年齢要求チャレンジ522を受け取ってよい。図5を参照して、チャレンジ522は、ストレスを受けるRO508およびアイドル状態の基準RO510が、測定状態に入ることを引き起こしてよい。測定状態の期間に、ストレスを受けるRO508は、イネーブルにされ(すなわち、依然として動作し)続けてよいが、それが通常は、ストレス電源電圧V_{DD_STR}を使用していた場合に、それは定格電源電圧V_{DD}を利用してよい(さもなければ、その電源電圧はV_{DD}のままである)。さらに、アイドル状態の基準RO510は、それが動作可能になるように、$Enable_{AS_Ref}$を介してイネーブルにさ

れる(すなわち、それは、定格電源電圧V_{DD}を使用して電源投入される)。チャレンジ522は、2つのスイッチ512、514が、ストレスを受けるRO508およびアイドル状態の基準RO510の出力を選択して通過させることも引き起こすことになる。ストレスを受けるRO508がほとんどの時間動作したままであるという事実に起因して、その発振周波数は経時的に減少し、一方アイドル状態の基準RO510の発振周波数は、それが通常電源切断されるので、比較的同じ状態のままでいる。したがって、ストレスを受けるRO508とアイドル状態の基準RO510との間の出力周波数差は、時間の経過とともに増加する。これら2つのRO508、510の出力530、532は、次いで、カウンタ516、518、および比較器520に提供され、その結果、出力応答信号534が生成され得る。たとえば、この場合、カウンタ値516、518間の実際の差異が出力534であり、2つのRO508、510間の周波数差の推定を可能にすることができる。値の差は、経験的に獲得された(たとえば、図3中のメモリ回路306に記憶される)データと比較され、ICまたはICサブモジュール全体の回路年齢情報を確認する(ascertain)ことができる。

【００３８】

PUF RO502、504、506は、(たとえば、ほとんど常に電源投入されるストレスを受けるRO508と異なり)、単に選択的にイネーブルにされ、電力を節約することができるが、それらの発振周波数は、使用のために経時的にやはり減少し得る。したがって、2つのPUF ROの出力周波数間の差は、互いに対して経時的に変化し得る。この差は、極めて十分となることができ、そのため、以前には他のPUF ROと比較してより低い発振周波数を有していた1つのPUF ROが、同じPUF ROと比較してわずかに高い発振周波数を後で有することができる。したがって、これら2つのPUF RO間の比較を引き起こすチャレンジ522は、出力応答534の変化(たとえば、出力534におけるビットフリップ)をもたらし得る。したがって、回路302の健全性監視機能を使用して、どのPUF ROが、その元の発振周波数にあまりにも大きい変化を受け、その結果、それらがもはや信頼できない(すなわち、それらは、他のPUF ROと比較して出力534においてビットフリップを引き起こしやすい)ことを検出することができる。

【００３９】

したがって、別の動作のモードによれば、回路302は、その健全性監視機能を利用して、選択されるPUF RO502、504、506経路の信頼性情報を提供することができる。たとえば、回路302は、図3に示される処理回路304などの処理回路から、経路信頼性要求チャレンジ522を受け取ってよい。図5を参照して、チャレンジ522は、所望のPUF RO、たとえばPUF RO504が、$Enable_{PUF_2}$を介してイネーブルにされること、アイドル状態の基準RO510が測定状態に入ること(すなわち、RO510が$Enable_{AS_Ref}$を介して電源投入されること)を引き起こすことができる。チャレンジ522は、2つのスイッチ512、514が、PUF RO504およびアイドル状態の基準RO510の出力を選択して通過させることも引き起こすことになる。PUF RO504の発振周波数が経時的に(使用のために)減少し、アイドル状態の基準RO510の発振周波数が実質的に同じままであるという事実に起因して、PUF RO504とアイドル状態の基準RO510との間の周波数差は、やはり経時的に増大する。これら2つのRO504、510の出力530、532は、次いで、カウンタ516、518、および比較器520に提供され、その結果、出力応答信号534が生成され得る。たとえば、この場合、カウンタ値516、518間の実際の差異が出力534であり、2つのRO504、510間の周波数差の推定を可能にすることができる。値の差を、2つのRO504、510の元々獲得され記憶された周波数差の値と比較することができ、予測されるPUF RO504の経路信頼性問題についての、すべての有意な変化を評価することができる。

【００４０】

図5は、単一のストレスを受けるRO508および単一の基準RO510を図示する。しかし、PUFおよび年齢センサ回路302は、複数のストレスを受けるROおよび複数の基準ROを備えてよい。たとえば、複数のストレスを受けるROおよび/または基準ROが、ICの様々な物理的な部分にわたって分散されてよい。ICの異なる部分は異なるストレスを受ける可能性があるので、ICのいくつかの部分が、より顕著な経年変化効果を経験する可能性がある。たとえ

ば、ICの異なる区域は、異なるダイのプロセスばらつき、異なる温度変動、および/または異なる電源電圧変動を経験する可能性がある。これらの効果は、ICの特定の区域に配置されるいくつかの回路構成要素に、追加のストレスを引き起こす可能性がある。したがって、ICの異なる部分/区域にストレスを受けるROおよび基準RO(RO508、510など)を配置することは、配置される区域に局所的な経時変化を数量化する助けになる場合があり、深刻な経年変化を受けてもはや信頼できないPUF ROの不具合のあるキーまたは識別子の生成を検出する助けになる場合がある。一態様によれば、ストレスを受けるROおよび基準ROの対は、互いに非常に近接して(たとえば、10μm未満離れて)配置され、最初の周波数差を最小化することができる。別の態様によれば、ストレスを受けるROおよび基準ROの対は、それらが遠い(たとえば、10μm以上離れる)ように配置および/または選択されてよい。

【００４１】

さらに、複数のPUF RO502、504、506が、ICの様々な部分に配置されてよい。2つの異なるPUF ROが比較のために選択されて、上に記載されたように、キー/識別子ビットを生成するとき、選択されるPUF ROは、ICの異なる部分から来てよい。すなわち、チャレンジ522は、互いの直ぐそばに物理的にレイアウトされる2つのPUF ROの代わりに、互いから少なくとも一定の閾値の距離だけ物理的に離れて配置される2つの異なるPUF ROを具体的に選択してよい。上述の段落に記載されたように、ICの異なる区域は、異なるダイのプロセスばらつき、異なる温度変動、および/または異なる電源電圧変動を経験する可能性がある。したがって、互いから物理的に遠い2つのPUF ROは、互いから物理的に近い(たとえば、互いに直ぐそばの)2つのPUF ROよりも、それらの動作周波数間により大きい差を有する可能性がある。というのは、前者の対は、より大きい製造ばらつきを経験する可能性があるからである。したがって、2つのPUF ROは、それらの動作周波数がより良好に識別可能となることができる可能性を増加させるため、ICの異なる部分からキー/識別子生成のために選択されてよい。たとえば、選択される2つのPUF ROは、IC上で少なくとも、10μm、50μm、100μm、200μm、500μm、または1000μm離れてよい。

【００４２】

図6は、別の態様に従う、チップ識別およびチップ健全性監視装置600の概略ブロック図を図示する。図3に示される装置300のように、図6に図示される装置600は、PUFおよび年齢センサ回路602、処理回路604、およびメモリ回路606をやはり含み、図3の装置300と同じ動作を実施する。図6に示されるPUFおよび年齢センサ回路602は、図6のPUFおよび年齢センサ回路602が、カウンタおよび比較器を含む場合がある(図3および図5参照)出力機能回路314を欠いていることを除いて、図3のPUFおよび年齢センサ回路302と同一である。PUFおよび年齢センサ回路602は、RO配列610、RO選択器回路612を含む。RO選択器回路612は、PUFおよび年齢センサ回路602と別個の回路であってよい処理回路604に、2つ(または2つ以上)のRO出力624a、624bを応答として出力する。処理回路302は、図6のPUFおよび年齢センサ回路602のための出力機能回路314により実行されるものと同じ機能を実施してよい。

【００４３】

図7は、一態様に従う電子デバイス700の概略ブロック図を図示する。電子デバイス700は、モバイルフォンおよびコンピュータなどの、ICを有する任意のデジタル電子デバイスであってよい。電子デバイス700は、複数の回路モジュール702、704、706、708、処理回路720、メモリ回路722、他のプロセッサ724、および上述の回路を相互接続する1つまたは複数のバス710を含む。(本明細書で、「構成要素」とも呼ばれる)回路モジュール702、704、706、708は、電子デバイス700のため異なる機能を実施する別個のICであってよい。たとえば、回路A702は、マルチメディアサブシステム回路であってよく、回路B704は、暗号処理回路であってよく、回路C706は、モデム回路であってよく、回路N708は低電力オーディオ回路であってよい。もちろん、電子デバイス700は、多くのさらなる回路モジュールを有してよい。

【００４４】

図示される例では、各回路モジュール702、704、706、708は、それ自体のPUFおよび年齢センサ回路(PUF/ASC)712、714、716、718を含む。PUF/ASC712、714、716、718は、図3

に示されたPUFおよび年齢センサ回路302または図6に示されたPUFおよび年齢センサ回路602のいずれかであってよい。各回路モジュール702、704、706、708がそれ自体のPUF/ASC712、714、716、718を含むので、各回路モジュール702、704、706、708は、電子デバイスの処理回路720にキー/識別子および/または健全性監視情報を生成し提供することができる(両矢印の点線がモジュール702、704、706、708と処理回路720との間の通信を示す)。処理回路720は、メモリ回路722に記憶されたデータに対する応答を検証してよい。

【００４５】

一例によれば、PUF/ASC712、714、716、718は、図3に示されたPUFおよび年齢センサ回路302と同一である。この場合、処理回路720は、各PUF/ASC712、714、716、718にチャレンジを送信することができ、PUF/ASC712、714、716、718は、それ自体が必要なRO周波数比較を実施して、処理回路720に応答を送り返すことになる。たとえば、PUF/ASC712、714、716、718は、チップ識別子またはキー生成チャレンジに応答して、キーまたは識別子ストリングを生成することができる。別の例として、PUF/ASC712、714、716、718は、チップ年齢/健全性要求チャレンジに応答して、回路年齢情報を提供することができる。そのような、局所的に生成される出力応答処理方式は、たとえば、モジュール702、704、706、708の数が多い(たとえば、5以上である)場合、モジュール702、704、706、708と処理回路720との間のバス710経由の通信が最小化するように使用することができる。

【００４６】

別の例によれば、PUF/ASC712、714、716、718は、図6に示されたPUFおよび年齢センサ回路602と同一である。この場合、処理回路720は、各PUF/ASC712、714、716、718にチャレンジを送信することができ、これに応じて、処理回路720は、PUF/ASC712、714、716、718から2つ(または2つ以上)のRO出力を受け取ることになる。次いで、処理回路720は、必要なRO周波数比較を実施することになる。たとえば、PUF/ASC712、714、716、718は、チップ識別子またはキー生成チャレンジに応答して、処理回路720に2つのRO出力を提供することができる。処理回路720は、次いで、それが受け取ったこれらのRO出力に基づいてそれ自体でキーまたは識別子ストリングを生成することになる。そのような、中心に配置される出力応答処理方式は、たとえば、モジュール702、704、706、708の数が少ない(たとえば、4以下である)場合、モジュール702、704、706、708から処理回路720へのRO出力を通信することは、タイミングおよび/または電力消費の観点から面倒なものとはならないので、使用することができる。

【００４７】

各チップ上のPUF/ASC712、714、716、718のそのような分散型システムは、回路モジュール702、704、706、708のうちのいずれか1つが年齢に起因して信頼できない可能性があるかどうかを処理回路720が判定することを可能にする。それは、ただ1つの代わりにいくつかの異なるPUF/ASC712、714、716、718からの応答に基づいて、処理回路720がキーまたは識別子(たとえば、第2の固有識別子またはキー)を生成することも可能にする。これは、より大きいエントロピーおよびより安全なキーまたは識別子生成を可能にする。

【００４８】

図8は、本開示の一態様に従う、集積回路を製造する方法800を図示する。最初に、部分的に、物理的複製不可関数(PUF)を実装するように構成される第1の複数のリング発振器が提供される(802)。次いで、部分的に、年齢センサ回路を実装するように構成される第2の複数のリング発振器が提供される(804)。次いで、リング発振器選択回路が提供される(806)。次いで、リング発振器選択回路が第1の複数のリング発振器および第2の複数のリング発振器に結合され、第1の複数のリング発振器および/または第2の複数のリング発振器のうちの少なくとも1つから少なくとも2つのリング発振器出力を選択するように、リング発振器選択回路が適合される(808)。最後に、リング発振器選択回路は、PUFと年齢センサ回路との間で共有される(810)。

【００４９】

図9は、本開示の一態様に従う、電子デバイスを製造する方法900を図示する。最初に、バスおよび処理回路が提供される(902)。次いで、複数の構成要素が提供され、各構成要

素は、(a)固有の識別子またはキーの生成を支援する物理的複製不可関数(PUF)、および(b)対応する構成要素についての回路年齢情報を提供する年齢センサ回路を実装するように構成されるリング発振器の配列を有する(904)。次いで、複数の構成要素は、バスに結合される(906)。次いで、処理回路がやはりバスに結合され、処理回路は、1つまたは複数の構成要素についての年齢情報を獲得すること、構成要素のうちの少なくとも1つについての固有の識別子またはキーを獲得すること、および/または異なる構成要素からのリング発振器の2つ以上の配列から獲得される情報を組み合わせることにより第2の固有の識別子またはキーを生成することのうちの少なくとも1つを実施するように適合される(908)。

【００５０】

図3～図9に図示された構成要素、ステップ、特徴、および/もしくは機能のうちの1つまたは複数は、単一の構成要素、ステップ、特徴もしくは機能に再構成ならびに/または組み合わされ、またはいくつかの構成要素、ステップ、もしくは機能に具現化されてよい。追加の要素、構成要素、ステップ、および/または機能が、本発明から逸脱することなく、追加されてもよい。図3～図7に図示された装置、デバイス、および/または構成要素は、図8および図9に記載された方法、特徴、またはステップのうちの1つまたは複数を実施するように構成され得る。本明細書に記載されるアルゴリズムは、ソフトウェアに効率的に実装されて、および/またはハードウェアに内蔵されてもよい。

【００５１】

さらに、本開示の一態様では、図3および図6に図示された処理回路304、604は、図8に記載されたアルゴリズム、方法、および/またはステップを実施するため、具体的に設計される、および/または配線接続される、専用プロセッサ(たとえば、特定用途向け集積回路(たとえば、ASIC))であってよい。すなわち、そのような専門プロセッサ(たとえば、ASIC)は、図8に記載されたアルゴリズム、方法、および/またはステップを実行するための手段のうちの一例であってよい。さらに、本開示の別の態様では、図7に図示されたプロセッサ724は、図9に記載されたアルゴリズム、方法、および/またはステップを実施するため、具体的に設計される、および/または配線接続される、専用プロセッサ(たとえば、特定用途向け集積回路(たとえば、ASIC))であってよい。すなわち、そのような専門プロセッサ(たとえば、ASIC)は、図9に記載されたアルゴリズム、方法、および/またはステップを実行するための手段のうちの一例であってよい。

【００５２】

また、本開示の態様は、フローチャート、流れ図、構造図、またはブロック図として描かれるプロセスとして記載され得るということに留意されたい。フローチャートは、動作を連続的なプロセスとして記載する場合があるが、動作の多くは、並列または同時に実施され得る。加えて、動作の順番が再構成されてよい。プロセスは、その動作が完了したら、終了される。プロセスは、方法、機能、プロシージャ、サブルーチン、サブプログラムなどに対応し得る。プロセスが機能に対応するとき、その終了は、呼び出している機能または主機能への機能の復帰に対応する。

【００５３】

さらに、記憶媒体は、情報を記憶するための、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、光学的記憶媒体、フラッシュメモリデバイスならびに/または他の機械可読媒体、および、プロセッサ可読媒体、および/もしくは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つまたは複数のデバイスを表してよい。「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、限定するものではないが、携帯または固定記憶デバイス、光学的記憶デバイス、ならびに命令および/またはデータを記憶、含有、または運搬することが可能な、様々な他の媒体などの非一時的媒体を含んでよい。したがって、本明細書に記載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」に記憶され得る命令および/またはデータにより完全に、または部分的に実装されて、1つまたは複数のプロセッサ、機械、および/またはデバイスにより実行され得る。

【００５４】
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り実装され得る。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、必要なタスクを実施するための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記憶装置などの機械可読媒体に記憶されてよい。プロセッサは、必要なタスクを実施してよい。コードセグメントは、プロシージャ、機能、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、または命令、データ構造、もしくはプログラムステートメントの任意の組合せを表してよい。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こと、および/または受け取ることにより、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、データなどは、メモリ共有、メッセージ輸送、トークン輸送、ネットワーク伝送などを含む任意の好適な手段を介して、渡され、転送され、または伝送され得る。

【００５５】
本明細書に開示される例に関連して記載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)もしくは他のプログラム可能論理構成要素、ディスクリートゲートもしくはトランジスタロジック、ディスクリートハードウェア構成要素、または本明細書に記載された機能を実施するように設計されるそれらの任意の組合せで、実装または実施され得る。汎用プロセッサは、マイクロプロセッサであってよいが、代替的に、プロセッサは、任意の従来型プロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってよい。プロセッサは、たとえば、DSPとマイクロプロセッサの組合せ、いくつかのマイクロプロセッサ、DSPコアと組み合わせた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いった、コンピューティング構成要素の組合せとしても実装され得る。

【００５６】
本明細書に開示される例に関連して記載される方法またはアルゴリズムは、ハードウェアで直接的に、プロセッサによる実行可能なソフトウェアモジュールで、または両方の組合せで、処理ユニット、プログラミング命令、または他の指示の形で具現化されてよく、単一のデバイスに含まれ、または複数のデバイスにわたって分散されてよい。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記憶媒体の任意の他の形で常駐することができる。記憶媒体は、プロセッサが記憶媒体から情報を読み込み、記憶媒体へ情報を書き込むことができるように、プロセッサと結合されてよい。代替として、記憶媒体は、プロセッサと一体であってよい。

【００５７】
本明細書に開示された態様に関連して記載した、様々な例示の論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子的ハードウェア、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できることを当業者ならさらに理解するであろう。ハードウェアとソフトウェアのこの互換性を明確に示すため、様々な例示の構成要素、ブロック、モジュール、回路、およびステップが、一般的にそれらの機能性の点で上に記載されてきた。そのような機能性がハードウェアまたはソフトウェアとして実装されるかどうかは、特定の用途および全体的なシステムに課せられる設計制約に依存する。

【００５８】
本明細書に記載される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に実装することができる。本開示の上述の態様は、単に例であり、本発明を制限するものと解釈されるべきでないことに留意されたい。本開示の態様の記載は、例示であることが意図され、特許請求の範囲を制限する意図はない。そのため、本教示は、他のタイプの装置に容易に適用でき、多くの代替形態、修正形態および変形形態が当業者に明らかと

なるであろう。

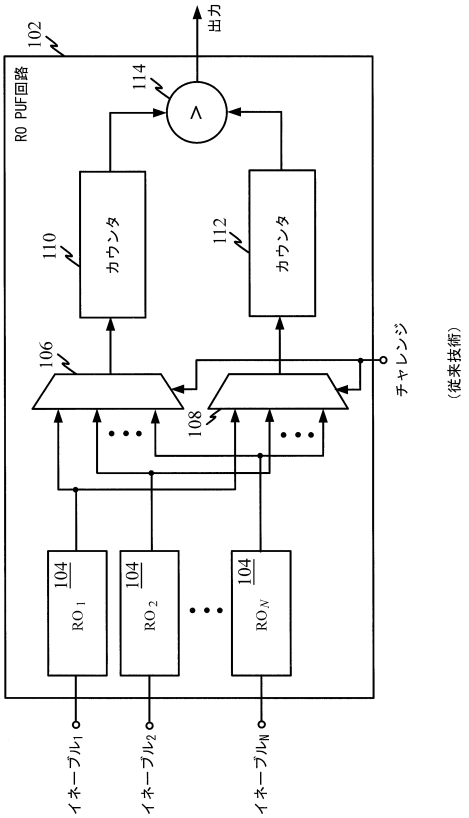
【符号の説明】

【００５９】

102　リング発振器ベースのPUF回路、RO PUF回路
104　リング発振器、RO
106　スイッチ、マルチプレクサ
108　スイッチ、マルチプレクサ
110　カウンタ
112　カウンタ
114　対比較
200　IC年齢センサ回路
202　RO
204　RO
206　位相比較器
300　チップ識別およびチップ健全性監視装置
302　PUFおよび年齢センサ回路
304　処理回路
306　メモリ回路
310　RO配列
312　RO選択器回路
314　出力機能回路
316　RO
318　PUFモジュール
320　チップ年齢センサモジュール
322a　RO周波数出力
322b　RO周波数出力
322c　RO周波数出力
322n　RO周波数出力
324a　RO周波数、入力周波数、出力
324b　RO周波数、入力周波数、出力
326　出力応答、出力ストリング、チップ識別値応答、回路年齢情報応答
328　チップ識別チャレンジ、健全性監視チャレンジ、チャレンジ
330　チップ識別子
332　チップ年齢値、使用期限年数
400　リング発振器、RO
402　ANDゲート
404a　インバータ
404b　インバータ
404c　インバータ
404n　インバータ
406　入力端子
408　入力端子
410　出力端子
412　RO出力
502　PUF RO
504　PUF RO
506　PUF RO
508　ストレスを受けるRO
510　アイドル状態の基準RO
512　第1のスイッチ

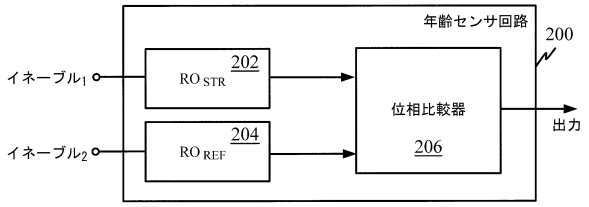
514 第2のスイッチ
516 第1のカウンタ
518 第2のカウンタ
520 比較器
522 チップ識別子またはキー生成チャレンジ
524 出力
526 出力
528 出力
530 PUF RO信号、RO出力
532 PUF RO信号、RO出力
534 RO出力、出力信号、出力応答信号
600 チップ識別およびチップ健全性監視装置
602 PUFおよび年齢センサ回路
604 処理回路
606 メモリ回路
610 RO配列
612 RO選択器回路
624a RO出力
624b RO出力
700 電子デバイス
702 回路モジュール、回路A
704 回路モジュール、回路B
706 回路モジュール、回路C
708 回路モジュール、回路N
710 バス
712 PUFおよび年齢センサ回路、PUF/ASC
714 PUFおよび年齢センサ回路、PUF/ASC
716 PUFおよび年齢センサ回路、PUF/ASC
718 PUFおよび年齢センサ回路、PUF/ASC
720 処理回路
722 メモリ回路
724 他のプロセッサ

【図１】



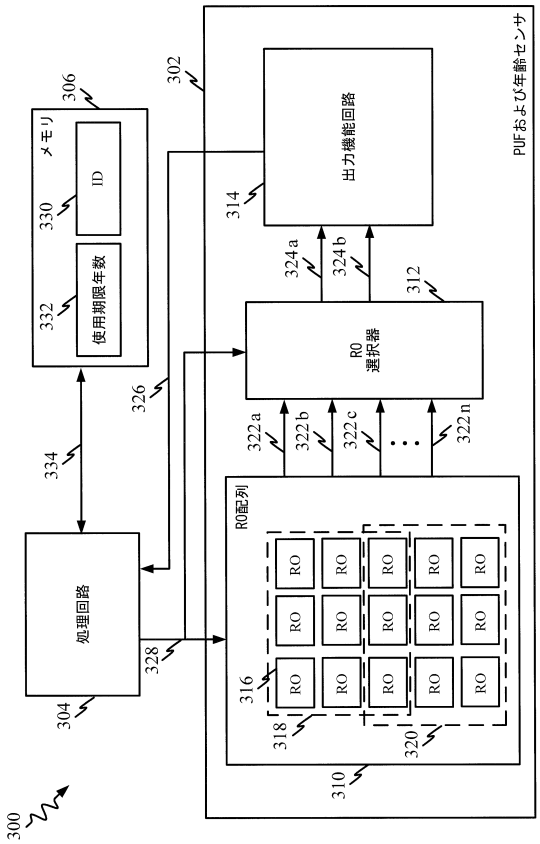
（従来技術）

【図２】

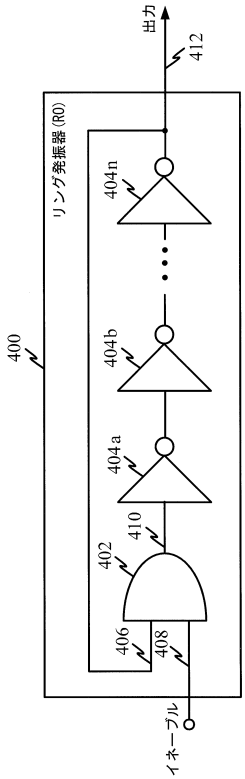


（従来技術）

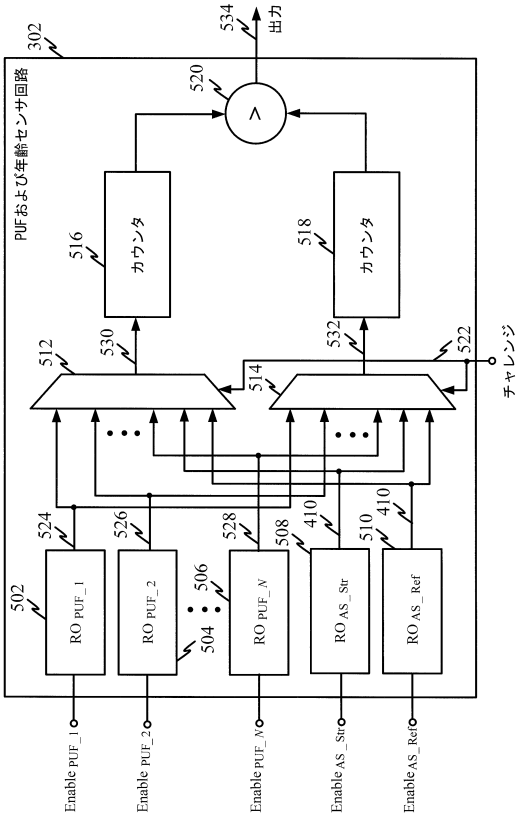
【図３】



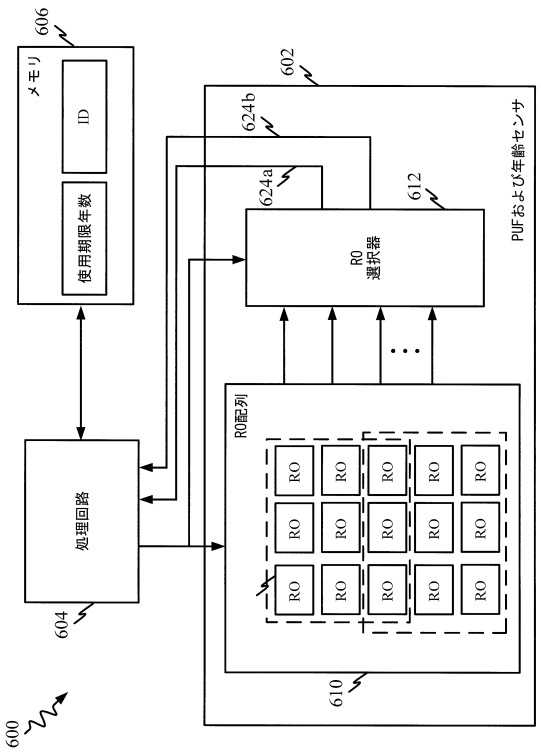
【図４】



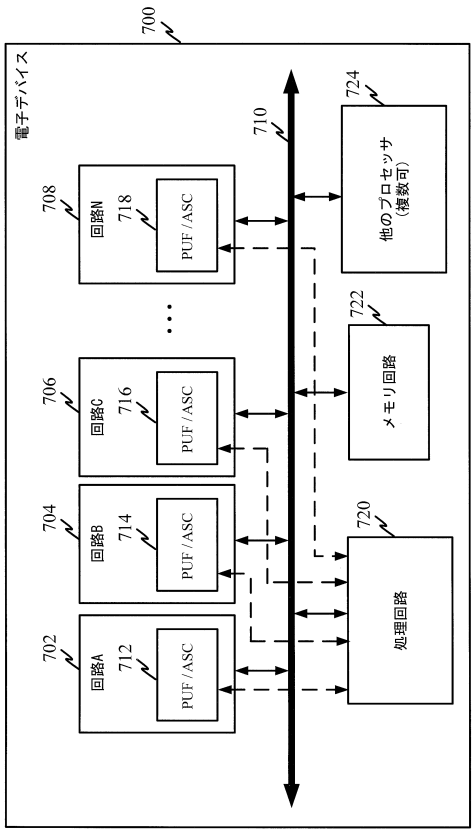
【図５】


302
PUFおよび年齢センサ回路
534
出力
520
>
516
カウンタ
518
カウンタ
512
530
532
522
チャレンジ
514
524
526
528
508
410
510
410
502
RO PUF_1
RO PUF_2
504
506
RO PUF_N
RO AS_Str
RO AS_Ref
Enable PUF_1
Enable PUF_2
Enable PUF_N
Enable AS_Str
Enable AS_Ref

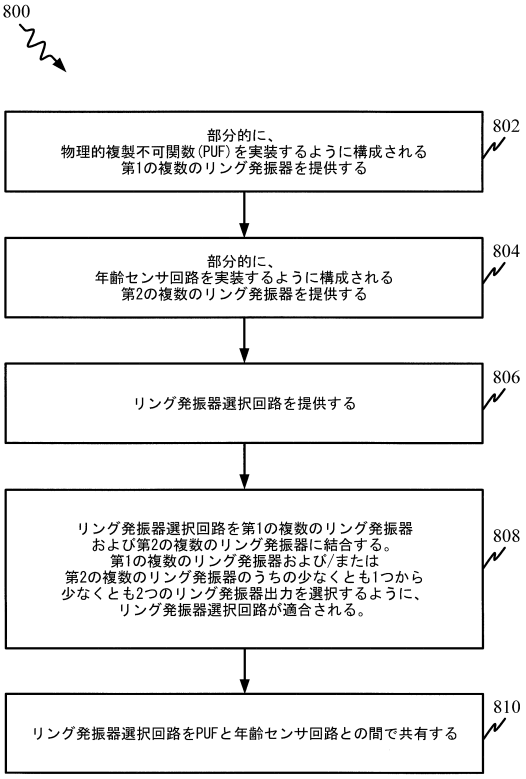
【図６】


606
メモリ
ID
使用期限年数
602
624b
624a
612
RO
選択器
PUFおよび年齢センサ
RO配列
RO
処理回路
604
610
600

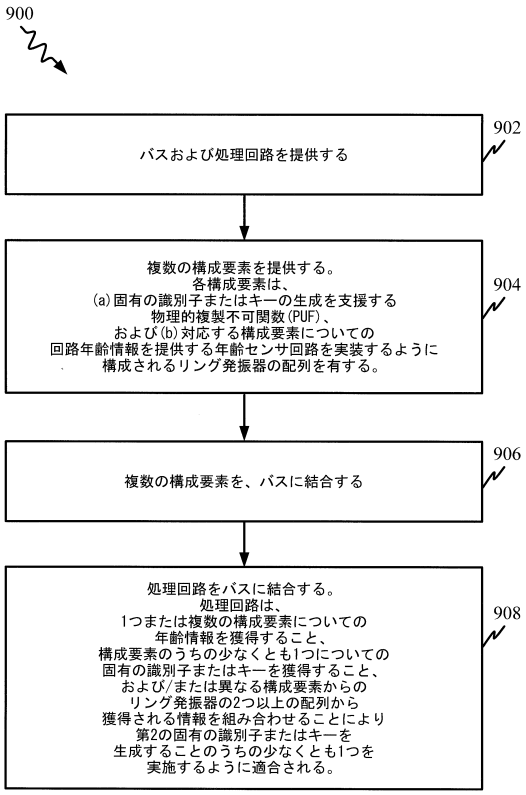
【図７】


700
電子デバイス
710
724
他のプロセッサ
(複数可)
708
回路N
718
PUF/ASC
722
メモリ回路
706
回路C
716
PUF/ASC
704
回路B
714
PUF/ASC
720
処理回路
702
回路A
712
PUF/ASC

【図８】


800
部分的に、
物理的複製不可関数(PUF)を実装するように構成される
第1の複数のリング発振器を提供する
802
部分的に、
年齢センサ回路を実装するように構成される
第2の複数のリング発振器を提供する
804
リング発振器選択回路を提供する
806
リング発振器選択回路を第1の複数のリング発振器
および第2の複数のリング発振器に結合する。
第1の複数のリング発振器および/または
第2の複数のリング発振器のうちの少なくとも1つから
少なくとも2つのリング発振器出力を選択するように、
リング発振器選択回路が適合される。
808
リング発振器選択回路をPUFと年齢センサ回路との間で共有する
810

【図９】


900
バスおよび処理回路を提供する
902
複数の構成要素を提供する。
各構成要素は、
(a)固有の識別子またはキーの生成を支援する
物理的複製不可関数(PUF)、
および(b)対応する構成要素についての
回路年齢情報を提供する年齢センサ回路を実装するように
構成されるリング発振器の配列を有する。
904
複数の構成要素を、バスに結合する
906
処理回路をバスに結合する。
処理回路は、
1つまたは複数の構成要素についての
年齢情報を獲得すること、
構成要素のうちの少なくとも1つについての
固有の識別子またはキーを獲得すること、
および/または異なる構成要素からの
リング発振器の2つ以上の配列から
獲得される情報を組み合わせることにより
第2の固有の識別子またはキーを
生成することのうちの少なくとも1つを
実施するように適合される。
908

フロントページの続き

(72)発明者　ブライアン・エム・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

合議体
審判長　高木　進
審判官　石井　茂和
審判官　須田　勝巳

(56)参考文献　国際公開第２００８／０５６６１２（WO，Ａ１）
国際公開第２０１１／０２７５５３（WO，Ａ１）
特開２００９－０１６５８６（ＪＰ，Ａ）
特表２００８－５０３８８２（ＪＰ，Ａ）
特表２００８－５０３８８３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/00 621Z，G01R 31/30