【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成28年4月21日(2016.4.21)

【公表番号】特表2016-508003(P2016-508003A)
【公表日】平成28年3月10日(2016.3.10)
【年通号数】公開・登録公報2016-015
【出願番号】特願2015-557029(P2015-557029)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｇ０１Ｒ　31/30　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ｚ
Ｇ０１Ｒ　31/30

【手続補正書】
【提出日】平成28年2月24日(2016.2.24)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
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、
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、
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、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、
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】
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、
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、
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、
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。