【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29年9月7日(2017.9.7)

【公表番号】特表2016-531515(P2016-531515A)
【公表日】平成28年10月6日(2016.10.6)
【年通号数】公開・登録公報2016-058
【出願番号】特願2016-536383(P2016-536383)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｇ０６Ｆ　21/44　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ｚ
Ｇ０６Ｆ　21/44

【手続補正書】
【提出日】平成29年7月26日(2017.7.26)
【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】
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/アン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、前記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2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/アン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のいずれかのために使用され、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、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つのプロセッサに、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。