【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3月2日(2017.3.2)

【公表番号】特表2016-532349(P2016-532349A)
【公表日】平成28年10月13日(2016.10.13)
【年通号数】公開・登録公報2016-059
【出願番号】特願2016-518720(P2016-518720)
【国際特許分類】
Ｈ０４Ｌ　9/10　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６２１Ｚ
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成29年1月25日(2017.1.25)
【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】
認証デバイスによって使用可能な方法であって、
電子デバイスに関連するデバイス識別子を受け取るステップと、
前記電子デバイスにおいて物理的クローン化不能関数(PUF)から生成される特性情報を含む第1の物理的クローン化不能関数データセットを、前記電子デバイスから受け取るステップと、
前記デバイス識別子を使用して、前記電子デバイスに対応する事前に記憶されたPUFデータセットを識別するステップと、
前記事前に記憶されたPUFデータセットと前記電子デバイスに対する前記第1のPUFデータセットとを相関させることによって前記電子デバイスを認証するステップとを含み、そのような相関が、前記相関において系統的ばらつきとランダムなばらつきとを区別する、前記事前に記憶されたPUFデータセットの要素と前記第1のPUFデータセットの要素との間のパターンまたは分布相関に基づく、方法。
【請求項２】
前記第1のPUFデータセットを受け取る前に前記電子デバイスにデータセット要求を送るステップをさらに含む、請求項1に記載の方法。
【請求項３】
前記データセット要求が、新しい特性情報が探索される、前記事前に記憶されたデータセットに対応する要素を識別する、請求項2に記載の方法。
【請求項４】
前記デバイス識別子に基づいて前記データセット要求を得るステップをさらに含む、請求項2に記載の方法。
【請求項５】
前記事前に記憶されたPUFデータセットが、前記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る、請求項1に記載の方法。
【請求項６】
前記物理的クローン化不能関数から生成された前記特性情報が、前記物理的クローン化

不能関数の個別の要素に対する情報を含む、請求項1に記載の方法。
【請求項７】
前記物理的クローン化不能関数から生成された前記特性情報が、前記物理的クローン化不能関数の個別のリング発振器に対する周波数値を含む、請求項1に記載の方法。
【請求項８】
前記事前に記憶されたPUFデータセットと前記電子デバイスに対する前記第1のPUFデータセットとを相関させるステップが、前記事前に記憶されたPUFデータセットおよび前記第1のPUFデータセットにわたるピアソンの積率相関係数を得るステップを含む、請求項1に記載の方法。
【請求項９】
前記相関係数がしきい値より大きい場合、前記電子デバイスが首尾よく認証される、請求項8に記載の方法。
【請求項１０】
認証が成功する場合、
前記電子デバイスによって後で送られた他のデータセットとの相関のために、前記事前に記憶されたPUFデータセットと併せて前記第1のPUFデータセットを記憶するステップをさらに含む、請求項1に記載の方法。
【請求項１１】
前記電子デバイスによって送られた全ての首尾よく認証されたデータセットのサブセットだけが、前記電子デバイスによって後で送られた前記他のデータセットとの相関のために前記認証デバイスによって記憶される、請求項10に記載の方法。
【請求項１２】
電子デバイスと通信す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に結合された処理回路とを備え、前記処理回路が、
前記電子デバイスに関連するデバイス識別子を受け取ることと、
前記電子デバイスにおいて物理的クローン化不能関数(PUF)から生成される特性情報を含む第1の物理的クローン化不能関数データセットを、前記電子デバイスから受け取ることと、
前記デバイス識別子を使用して、前記電子デバイスに対応する事前に記憶されたPUFデータセットを識別することと、
前記事前に記憶されたPUFデータセットと前記電子デバイスに対する前記第1のPUFデータセットとを相関させることによって前記電子デバイスを認証することとを行うように構成され、そのような相関が、前記相関において系統的ばらつきとランダムなばらつきとを区別する、前記事前に記憶されたPUFデータセットの要素と前記第1のPUFデータセットの要素との間のパターンまたは分布相関に基づく、認証デバイス。
【請求項１３】
前記処理回路が、さらに、
前記第1のPUFデータセットを受け取る前に前記電子デバイスにデータセット要求を送るように構成される、請求項12に記載の認証デバイス。
【請求項１４】
前記データセット要求が、新しい特性情報が探索される、前記事前に記憶されたデータセットに対応する要素を識別する、請求項13に記載の認証デバイス。
【請求項１５】
前記処理回路が、さらに、
前記デバイス識別子に基づいて前記データセット要求を得るように構成される、請求項13に記載の認証デバイス。
【請求項１６】
前記事前に記憶されたPUFデータセットが、前記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る、請求項12に記載の認証デバイス。
【請求項１７】

前記物理的クローン化不能関数から生成された前記特性情報が、前記物理的クローン化不能関数の個別の要素に対する情報を含む、請求項12に記載の認証デバイス。
【請求項１８】
前記物理的クローン化不能関数から生成された前記特性情報が、前記物理的クローン化不能関数の個別のリング発振器に対する周波数値を含む、請求項12に記載の認証デバイス。
【請求項１９】
前記事前に記憶されたPUFデータセットと前記電子デバイスに対する前記第1のPUFデータセットとを相関させるステップが、前記事前に記憶されたPUFデータセットおよび前記第1のPUFデータセットにわたるピアソンの積率相関係数を得るステップを含む、請求項12に記載の認証デバイス。
【請求項２０】
認証が成功する場合、前記処理回路が、さらに、
前記電子デバイスによって後で送られた他のデータセットとの相関のために、前記事前に記憶されたPUFデータセットと併せて前記第1のPUFデータセットを記憶するように構成される、請求項12に記載の認証デバイス。
【請求項２１】
前記電子デバイスによって送られた全ての首尾よく認証されたデータセットのサブセットだけが、前記電子デバイスによって後で送られた前記他のデータセットとの相関のために前記認証デバイスによって記憶される、請求項20に記載の認証デバイス。
【請求項２２】
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、前記命令が、少なくとも1つのプロセッサによって実行されたときに、前記少なくとも1つのプロセッサに、
電子デバイスに関連するデバイス識別子を受け取ることと、
前記電子デバイスにおいて物理的クローン化不能関数(PUF)から生成される特性情報を含む第1の物理的クローン化不能関数データセットを、前記電子デバイスから受け取ることと、
前記デバイス識別子を使用して、前記電子デバイスに対応する事前に記憶されたPUFデータセットを識別することと、
前記事前に記憶されたPUFデータセットと前記電子デバイスに対する前記第1のPUFデータセットとを相関させることによって前記電子デバイスを認証することとを行わせ、そのような相関が、前記相関において系統的ばらつきとランダムなばらつきとを区別する、前記事前に記憶されたPUFデータセットの要素と前記第1のPUFデータセットの要素との間のパターンまたは分布相関に基づく、非一時的機械可読記憶媒体。
【請求項２３】
認証が成功する場合、前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、
前記電子デバイスによって後で送られた他のデータセットとの相関のために、前記事前に記憶されたPUFデータセットと併せて前記第1のPUFデータセットを記憶させる、請求項22に記載の非一時的機械可読記憶媒体。
【請求項２４】
前記電子デバイスによって送られた全ての首尾よく認証されたデータセットのサブセットだけが、前記電子デバイスによって後で送られた前記他のデータセットとの相関のために認証デバイスによって記憶される、請求項23に記載の非一時的機械可読記憶媒体。
【請求項２５】
前記電子デバイスを認証するステップは、前記事前に記憶されたPUFデータセットおよび前記電子デバイスに対する前記第1のPUFデータセットの系統的ばらつきを相関させるステップをさらに含む、請求項１に記載の方法。
【請求項２６】

要素間の前記パターンまたは分布相関は、前記事前に記憶されたPUFデータセットおよび前記第1のPUFデータセットの要素のアレイ間の依存関係の測度を含む、請求項１に記載の方法。