

【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 18 年 5 月 11 日 (2006.5.11)

【公開番号】特開 2001-144743 (P2001-144743A)

【公開日】平成 13 年 5 月 25 日 (2001.5.25)

【出願番号】特願 平 11-320946

【国際特許分類】

**H 0 4 L 9/08 (2006.01)**

**H 0 4 L 9/32 (2006.01)**

【F I】

H 0 4 L 9/00 6 0 1 Z

H 0 4 L 9/00 6 7 3 D

H 0 4 L 9/00 6 7 3 A

【手続補正書】

【提出日】平成 18 年 3 月 13 日 (2006.3.13)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

前記生体情報読み取り手段で読み取られ生成される生体コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

前記暗号鍵生成手段で生体コードに基づいて生成される暗号鍵と同じ暗号鍵を生成する鍵生成用コードを出力する鍵生成用コード出力手段と、

を有することを特徴とする暗号鍵生成装置。

【請求項 2】

前記暗号鍵生成装置は、さらに、

前記生体情報読み取り手段で読み取られ生成される生体コードを変換する変換コード生成手段を有し、

前記鍵生成用コード出力手段は、前記変換コード生成手段において生成される変換コードを出力する構成を有することを特徴とする請求項 1 に記載の暗号鍵生成装置。

【請求項 3】

前記暗号鍵生成装置は、さらに、

鍵生成用コードを入力する鍵生成用コード入力手段を有し、

前記暗号鍵生成手段は、前記生体情報読み取り手段で読み取られ生成される生体コード、または前記鍵生成用コード入力手段から入力される鍵生成用コードのいずれか一方のコードに基づいて暗号化処理または復号化処理に適用する暗号鍵を生成する構成を有することを特徴とする請求項 1 に記載の暗号鍵生成装置。

【請求項 4】

前記暗号鍵生成装置は、さらに、

前記鍵生成用コード入力手段からの入力コードを再変換するコード再変換手段を有し、

前記暗号鍵生成手段は、前記生体情報読み取り手段で読み取られ生成される生体コード、または前記鍵生成用コード入力手段から入力され、前記コード再変換手段で再変換されて生成される鍵生成用コードのいずれか一方のコードに基づいて暗号化処理または復号化

処理に適用する暗号鍵を生成する構成を有することを特徴とする請求項 3 に記載の暗号鍵生成装置。

【請求項 5】

前記暗号鍵生成装置は、さらに、

前記変換コード生成手段、および前記コード再変換手段において各入力コードに対して適用する関数を書換えるための関数書換手段を有することを特徴とする請求項 4 に記載の暗号鍵生成装置。

【請求項 6】

前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNA パターンのいずれか、または指紋、眼底像、声紋、DNA パターンの 2 以上の生体情報の組み合わせであることを特徴とする請求項 1 に記載の暗号鍵生成装置。

【請求項 7】

前記生体情報読み取り手段の読み取る生体情報は指紋情報であり、

前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする請求項 1 に記載の暗号鍵生成装置。

【請求項 8】

前記暗号鍵生成手段の生成する暗号鍵は、共通鍵暗号化方式における共通鍵、公開鍵暗号化方式における公開鍵、秘密鍵のいずれかであることを特徴とする請求項 1 に記載の暗号鍵生成装置。

【請求項 9】

前記暗号鍵生成装置は、さらに、

パスワードを入力するパスワード入力手段と、

前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段とを有し、

前記鍵生成用コード出力手段は、前記中間コード生成手段の生成する中間コードを出力し、

前記暗号鍵生成手段は、前記中間コード生成手段の生成する中間コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する構成を有することを特徴とする請求項 1 に記載の暗号鍵生成装置。

【請求項 10】

前記鍵生成用コード出力手段は、データ表示手段であることを特徴とする請求項 1 に記載の暗号鍵生成装置。

【請求項 11】

前記鍵生成用コード入力手段は、キーボードであることを特徴とする請求項 3 に記載の暗号鍵生成装置。

【請求項 12】

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

前記生体情報読み取り手段で読み取られ生成される生体コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

前記暗号鍵生成手段で生体コードに基づいて生成される暗号鍵と同じ暗号鍵を生成する鍵生成用コードを出力する鍵生成用コード出力手段と、

暗号化すべきデータを入力するデータ入力手段と、

前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの暗号化処理を実行する暗号化手段と、

前記暗号化手段において暗号化したデータを出力するデータ出力手段と、

を有することを特徴とする暗号化装置。

**【請求項 1 3】**

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

前記生体コードに基づいて生成される暗号鍵と同じ暗号鍵を生成する鍵生成用コードを入力する鍵生成用コード入力手段と、

前記生体情報読み取り手段で読み取られ生成される生体コード、または鍵生成用コード入力手段において入力される鍵生成用コードのいずれかを選択的に入力し、該入力コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

復号化すべきデータを入力するデータ入力手段と、

前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの復号化処理を実行する復号化手段と、

前記復号化手段において復号化したデータを出力するデータ出力手段と、

を有することを特徴とする復号化装置。

**【請求項 1 4】**

前記復号化装置は、さらに、鍵生成用コードを出力する鍵生成用コード出力手段を有することを特徴とする請求項 1 3 記載の復号化装置。

**【請求項 1 5】**

前記復号化装置は、さらに、

前記鍵生成用コード入力手段からの入力コードを再変換するコード再変換手段を有し、

前記暗号鍵生成手段は、前記生体情報読み取り手段で読み取られ生成される生体コード、または前記鍵生成用コード入力手段から入力され、前記コード再変換手段で再変換されて生成される鍵生成用コードのいずれか一方のコードを選択的に入力し、該入力コードに基づいて復号化処理に適用する復号化鍵を生成する構成を有することを特徴とする請求項 1 3 に記載の復号化装置。

**【請求項 1 6】**

前記復号化装置は、さらに、前記生体情報読み取り手段で読み取られ生成される生体コードを変換する変換コード生成手段を有し、前記鍵生成用コード出力手段は、前記変換コード生成手段において生成される生体コードに基づく変換コードを出力する構成を有することを特徴とする請求項 1 4 に記載の復号化装置。

**【請求項 1 7】**

前記復号化装置は、さらに、

前記変換コード生成手段、および前記コード再変換手段において各入力コードに対して適用する関数を書換えるための関数書換手段を有することを特徴とする請求項 1 6 に記載の復号化装置。

**【請求項 1 8】** 前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNA パターンのいずれか、または指紋、眼底像、声紋、DNA パターンの 2 以上の生体情報の組み合わせであることを特徴とする請求項 1 3 に記載の復号化装置。

**【請求項 1 9】**

前記生体情報読み取り手段の読み取る生体情報は指紋情報であり、

前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする請求項 1 3 に記載の復号化装置。

**【請求項 2 0】**

前記復号化装置は、さらに、

パスワードを入力するパスワード入力手段と、

前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段とを有し、

前記鍵生成用コード出力手段は、前記中間コード生成手段の生成する中間コードを出力し、

前記暗号鍵生成手段は、前記中間コード生成手段の生成する中間コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する構成を有することを特徴とする請求項 1 4 に記載の復号化装置。

【請求項 2 1】

前記鍵生成用コード出力手段は、データ表示手段であることを特徴とする請求項 1 3 に記載の復号化装置。

【請求項 2 2】

前記鍵生成用コード入力手段は、キーボードであることを特徴とする請求項 1 3 に記載の復号化装置。

【請求項 2 3】

暗号化処理または復号化処理に使用する暗号鍵を生成する暗号鍵生成方法において、生体情報に基づくコードを入力するコード入力ステップと、

前記コード入力ステップで入力されるコードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

前記暗号鍵生成ステップで入力コードに基づいて生成される暗号鍵と同じ暗号鍵を生成する鍵生成用コードを出力する鍵生成用コード出力ステップと、

を有することを特徴とする暗号鍵生成方法。

【請求項 2 4】

生体情報に基づくコードを入力するコード入力ステップと、

前記コード入力ステップで入力されるコードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

前記暗号鍵生成ステップで生体情報に基づくコードに基づいて生成される暗号鍵と同じ暗号鍵を生成する鍵生成用コードを出力する鍵生成用コード出力ステップと、

暗号化すべきデータを入力するデータ入力ステップと、

前記暗号鍵生成ステップにおいて生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの暗号化処理を実行する暗号化処理ステップと、

前記暗号化処理ステップにおいて暗号化したデータを出力するデータ出力ステップと、を有することを特徴とする暗号化方法。

【請求項 2 5】

暗号化処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、

前記コンピュータ・プログラムは、

生体情報に基づくコードを入力するコード入力ステップと、

前記コード入力ステップで入力されるコードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

前記暗号鍵生成ステップで生体情報に基づくコードに基づいて生成される暗号鍵と同じ暗号鍵を生成する鍵生成用コードを出力する鍵生成用コード出力ステップと、

暗号化すべきデータを入力するデータ入力ステップと、前記暗号鍵生成ステップにおいて生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの暗号化処理を実行する暗号化処理ステップと、

前記暗号化処理ステップにおいて暗号化したデータを出力するデータ出力ステップと、を有することを特徴とするプログラム提供媒体。