【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６部門第２区分
【発行日】平成19年6月14日(2007.6.14)

【公開番号】特開2005-107078(P2005-107078A)
【公開日】平成17年4月21日(2005.4.21)
【年通号数】公開・登録公報2005-016
【出願番号】特願2003-339364(P2003-339364)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６１０Ａ

【手続補正書】
【提出日】平成19年4月26日(2007.4.26)
【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】
入力情報を非線形変換し、第１非線形変換情報を出力する第１非線形変換部と、当該第１非線形変換情報を線形変換して第１線形変換情報を出力する第１線形変換部とを有する第１暗号処理部と、
入力情報を非線形変換し、第２非線形変換情報を出力する第２非線形変換部と、当該第２非線形変換情報を線形変換して第２線形変換情報を出力する第２線形変換部とを有する第２暗号処理部と、
前記第２暗号処理部からの出力と、前記第１暗号処理部からの出力とが入力される排他的論理和部を備え、
前記第１非線形変換情報を第１列ベクトルで示すと共に前記第１線形変換情報を第２列ベクトルで示した場合に、当該第１列ベクトルを当該第２列ベクトルに変換する第１行列と、
前記第２非線形変換情報を第３列ベクトルで示すと共に前記第２線形変換情報を第４列ベクトルで示した場合に、当該第３列ベクトルを当該第４列ベクトルに変換する第２行列とは、
互いに異なる行列であることを特徴とする暗号処理装置。
【請求項２】
前記第１行列から選択した第１列ベクトルと、
前記第２行列から選択した第２列ベクトルとは、
いずれの列ベクトルを選択した場合であっても、互いに線形独立であることを特徴とする請求項１に記載の暗号処理装置。
【請求項３】
前記暗号処理装置は、
前記排他論理和部における排他論理和結果を前記前記第１暗号処理部または前記第２暗号処理部に再度入力し、前記第１暗号処理部および前記第２暗号処理部における暗号処理を繰り返し実行する構成であることを特徴とする請求項１に記載の暗号処理装置。
【請求項４】
前記第１線形変換部および前記第２線形変換部は、ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理を実行する構成であり、

前記第１線形変換部および前記第２線形変換部において線形変換に適用する前記第１行列と前記第２行列は、行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルが互いに線形独立となるｍ次行列であることを特徴とする請求項１に記載の暗号処理装置。
【請求項５】
Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行する暗号処理装置であり、
非線形変換部および線形変換部を有するＳＰＮ型のＦ関数を、複数ラウンド繰り返し実行する構成を有し、
前記複数ラウンド各々に対応するＦ関数の線形変換部は、
正方行列を適用した線形変換処理を実行する構成であり、少なくとも連続する偶数ラウンドおよび連続する奇数ラウンドの各々において異なる正方行列を適用した線形変換処理を実行する構成であることを特徴とする暗号処理装置。
【請求項６】
前記Ｆ関数の線形変換部は、
全ての偶数ラウンドおよび全ての奇数ラウンドにおいて異なる正方行列をそれぞれ適用した線形変換処理を実行する構成であることを特徴とする請求項５に記載の暗号処理装置。
【請求項７】
前記Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理のアルゴリズムは、ラウンド数Ｒの暗号処理アルゴリズムであり、
前記Ｆ関数の線形変換部は、
ｒ個の全ての偶数ラウンドおよびｒ個の全ての奇数ラウンドにおいてｒ種類の異なる正方行列を順次適用した線形変換処理を実行する構成であることを特徴とする請求項５に記載の暗号処理装置。
【請求項８】
前記Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理のアルゴリズムは、ラウンド数Ｒの暗号処理アルゴリズムであり、
前記Ｆ関数の線形変換部は、
ｒ個の全ての偶数ラウンドおよびｒ個の全ての奇数ラウンドにおいて２≦ｑ＜ｒのｑ種類の異なる正方行列を順次繰り返し適用した線形変換処理を実行する構成であることを特徴とする請求項５に記載の暗号処理装置。
【請求項９】
前記Ｆ関数の線形変換部は、ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理を実行する構成であり、
前記Ｆ関数の線形変換部において適用する異なる複数の正方行列の各々は、
前記複数の正方行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルによって構成する行列が線形独立である正方行列として設定したことを特徴とする請求項５に記載の暗号処理装置。
【請求項１０】
前記Ｆ関数の線形変換部は、ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理を実行する構成であり、
前記Ｆ関数の線形変換部において適用する異なる複数の正方行列の各々は、
前記複数の正方行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルによって構成する行列も正方行列となる正方行列として設定したことを特徴とする請求項５に記載の暗号処理装置。
【請求項１１】
前記Ｆ関数の線形変換部において適用する異なる複数の正方行列の各々は、
前記異なる正方行列を構成する要素を全て含む正方行列Ｍから選択された行ベクトルによって構成される行列Ｍ'から抽出された列ベクトルによって構成される行列によって構成されていることを特徴とする請求項５に記載の暗号処理装置。
【請求項１２】

前記Ｆ関数の線形変換部において適用する異なる複数の正方行列の各々は、
リードソロモン符号生成行列に基づいて生成された正方行列であることを特徴とする請求項５に記載の暗号処理装置。
【請求項１３】
暗号処理装置において暗号処理を実行する暗号処理方法であり、
第１暗号処理部の第１非線形変換部において入力情報を非線形変換して第１非線形変換情報を出力し、第１暗号処理部の第１線形変換部において当該第１非線形変換情報を線形変換して第１線形変換情報を出力する第１暗号処理ステップと、
第２暗号処理部の第２非線形変換部において入力情報を非線形変換して第２非線形変換情報を出力し、第２暗号処理部の第２線形変換部において当該第２非線形変換情報を線形変換して第２線形変換情報を出力する第２暗号処理ステップと、
排他的論理和部が、前記第２暗号処理部からの出力と、前記第１暗号処理部からの出力とを入力して排他論理和処理を実行する排他的論理和ステップとを有し、
前記第１暗号処理ステップの第１線形変換処理は、前記第１非線形変換情報を第１列ベクトルで示すと共に前記第１線形変換情報を第２列ベクトルで示した場合に、当該第１列ベクトルを当該第２列ベクトルに変換する第１行列を適用した第１線形変換処理実行ステップであり、
前記第２暗号処理ステップの第２線形変換処理は、前記第２非線形変換情報を第３列ベクトルで示すと共に前記第２線形変換情報を第４列ベクトルで示した場合に、当該第３列ベクトルを当該第４列ベクトルに変換する第２行列を適用した第２線形変換処理実行ステップであり、
前記第１線形変換処理実行ステップにおいて適用する前記第１行列と第２線形変換処理実行ステップにおいて適用する前記第２行列とは互いに異なる行列であることを特徴とする暗号処理方法。
【請求項１４】
前記第１行列から選択した第１列ベクトルと、
前記第２行列から選択した第２列ベクトルとは、
いずれの列ベクトルを選択した場合であっても、互いに線形独立であることを特徴とする請求項１３に記載の暗号処理方法。
【請求項１５】
前記暗号処理方法は、
前記排他論理和ステップにおける排他論理和結果を前記前記第１暗号処理部または前記第２暗号処理部に再度入力し、前記第１暗号処理ステップおよび前記第２暗号処理ステップの暗号処理を繰り返し実行することを特徴とする請求項１３に記載の暗号処理方法。
【請求項１６】
前記第１線形変換部および前記第２線形変換部における線形変換処理は、ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理を実行するステップであり、
前記第１線形変換部および前記第２線形変換部において線形変換に適用する前記第１行列と前記第２行列は、行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルが互いに線形独立さなるｍ次行列であることを特徴とする請求項１３に記載の暗号処理方法。
【請求項１７】
Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行する暗号処理方法であり、
非線形変換処理および線形変換処理を実行するＳＰＮ型のＦ関数を、複数ラウンド繰り返し実行し、
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
正方行列を適用した線形変換処理を実行するとともに、
少なくとも連続する偶数ラウンドおよび連続する奇数ラウンドの各々において異なる正方行列を適用した線形変換処理を実行することを特徴とする暗号処理方法。

【請求項１８】
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
全ての偶数ラウンドおよび全ての奇数ラウンドにおいて異なる正方行列をそれぞれ適用した線形変換処理を実行することを特徴とする請求項１７に記載の暗号処理方法。
【請求項１９】
前記暗号処理方法は、
ラウンド数ＲのＦｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行し、
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
ｒ個の全ての偶数ラウンドおよびｒ個の全ての奇数ラウンドにおいてｒ種類の異なる正方行列を順次適用した線形変換処理を実行することを特徴とする請求項１７に記載の暗号処理方法。
【請求項２０】
前記暗号処理方法は、
ラウンド数ＲのＦｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行し、
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
ｒ個の全ての偶数ラウンドおよびｒ個の全ての奇数ラウンドにおいて$2 \leqq q < r$のｑ種類の異なる正方行列を順次繰り返し適用した線形変換処理を実行することを特徴とする請求項１７に記載の暗号処理方法。
【請求項２１】
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理であり、
前記複数ラウンド各々に対応するＦ関数の線形変換処理において適用する異なる複数の正方行列の各々は、該複数の正方行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルによって構成する行列が線形独立である正方行列であることを特徴とする請求項１７に記載の暗号処理方法。
【請求項２２】
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理であり、
前記複数ラウンド各々に対応するＦ関数の線形変換処理において適用する異なる複数の正方行列の各々は、前記複数の正方行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルによって構成する行列も正方行列となる正方行列であることを特徴とする請求項１７に記載の暗号処理方法。
【請求項２３】
前記複数ラウンド各々に対応するＦ関数の線形変換処理において適用する異なる複数の正方行列の各々は、前記複数の正方行列を構成する要素を全て含む正方行列Ｍから選択された行ベクトルによって構成される行列Ｍ'から抽出された列ベクトルによって構成される行列によって構成されていることを特徴とする請求項１７に記載の暗号処理方法。
【請求項２４】
前記Ｆ関数の線形変換部において適用する異なる複数の正方行列の各々は、
リードソロモン符号生成行列に基づいて生成された正方行列であることを特徴とする請求項１７に記載の暗号処理方法。
【請求項２５】
暗号処理装置において暗号処理を実行させるコンピュータ・プログラムであり、
第１暗号処理部の第１非線形変換部に入力情報を非線形変換させて第１非線形変換情報を出力させ、第１暗号処理部の第１線形変換部に当該第１非線形変換情報を線形変換させて第１線形変換情報を出力させる第１暗号処理ステップと、
第２暗号処理部の第２非線形変換部に入力情報を非線形変換させて第２非線形変換情報を出力させ、第２暗号処理部の第２線形変換部に当該第２非線形変換情報を線形変換させ

て第２線形変換情報を出力させる第２暗号処理ステップと、
排他的論理和部に、前記第２暗号処理部からの出力と、前記第１暗号処理部からの出力とを入力して排他論理和処理を実行させる排他的論理和ステップとを有し、
前記第１暗号処理ステップの第１線形変換処理は、前記第１非線形変換情報を第１列ベクトルで示すと共に前記第１線形変換情報を第２列ベクトルで示した場合に、当該第１列ベクトルを当該第２列ベクトルに変換する第１行列を適用した第１線形変換処理実行ステップであり、
前記第２暗号処理ステップの第２線形変換処理は、前記第２非線形変換情報を第３列ベクトルで示すと共に前記第２線形変換情報を第４列ベクトルで示した場合に、当該第３列ベクトルを当該第４列ベクトルに変換する第２行列を適用した第２線形変換処理実行ステップであり、
前記第１線形変換処理実行ステップにおいて適用する前記第１行列と第２線形変換処理実行ステップにおいて適用する前記第２行列とは互いに異なる行列として設定したことを特徴とするコンピュータ・プログラム。
【請求項２６】
Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行するコンピュータ・プログラムであり、
非線形変換処理および線形変換処理を実行するＳＰＮ型のＦ関数を、複数ラウンド繰り返し実行し、
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
正方行列を適用した線形変換処理を実行するとともに、
少なくとも連続する偶数ラウンドおよび連続する奇数ラウンドの各々において異なる正方行列を適用した線形変換処理を実行するステップであることを特徴とするコンピュータ・プログラム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
本発明の第１の側面は、
入力情報を非線形変換し、第１非線形変換情報を出力する第１非線形変換部と、当該第１非線形変換情報を線形変換して第１線形変換情報を出力する第１線形変換部とを有する第１暗号処理部と、
入力情報を非線形変換し、第２非線形変換情報を出力する第２非線形変換部と、当該第２非線形変換情報を線形変換して第２線形変換情報を出力する第２線形変換部とを有する第２暗号処理部と、
前記第２暗号処理部からの出力と、前記第１暗号処理部からの出力とが入力される排他的論理和部を備え、
前記第１非線形変換情報を第１列ベクトルで示すと共に前記第１線形変換情報を第２列ベクトルで示した場合に、当該第１列ベクトルを当該第２列ベクトルに変換する第１行列と、
前記第２非線形変換情報を第３列ベクトルで示すと共に前記第２線形変換情報を第４列ベクトルで示した場合に、当該第３列ベクトルを当該第４列ベクトルに変換する第２行列とは、
互いに異なる行列であることを特徴とする暗号処理装置にある。
さらに、本発明の暗号処理装置の一実施態様において、前記第１行列から選択した第１列ベクトルと、前記第２行列から選択した第２列ベクトルとは、いずれの列ベクトルを選択した場合であっても、互いに線形独立であることを特徴とする。
さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理装置は、前記排他

論理和部における排他論理和結果を前記前記第１暗号処理部または前記第２暗号処理部に再度入力し、前記第１暗号処理部および前記第２暗号処理部における暗号処理を繰り返し実行する構成であることを特徴とする。

さらに、本発明の暗号処理装置の一実施態様において、前記第１線形変換部および前記第２線形変換部は、ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理を実行する構成であり、前記第１線形変換部および前記第２線形変換部において線形変換に適用する前記第１行列と前記第２行列は、行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルが互いに線形独立となるｍ次行列であることを特徴とする。

さらに、本発明の第２の側面は、

Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行する暗号処理装置であり、

非線形変換部および線形変換部を有するＳＰＮ型のＦ関数を、複数ラウンド繰り返し実行する構成を有し、

前記複数ラウンド各々に対応するＦ関数の線形変換部は、

正方行列を適用した線形変換処理を実行する構成であり、少なくとも連続する偶数ラウンドおよび連続する奇数ラウンドの各々において異なる正方行列を適用した線形変換処理を実行する構成であることを特徴とする暗号処理装置にある。

【手続補正３】

【補正対象書類名】明細書

【補正対象項目名】００２０

【補正方法】変更

【補正の内容】

【００２０】

さらに、本発明の第３の側面は、

暗号処理装置において暗号処理を実行する暗号処理方法であり、

第１暗号処理部の第１非線形変換部において入力情報を非線形変換して第１非線形変換情報を出力し、第１暗号処理部の第１線形変換部において当該第１非線形変換情報を線形変換して第１線形変換情報を出力する第１暗号処理ステップと、

第２暗号処理部の第２非線形変換部において入力情報を非線形変換して第２非線形変換情報を出力し、第２暗号処理部の第２線形変換部において当該第２非線形変換情報を線形変換して第２線形変換情報を出力する第２暗号処理ステップと、

排他的論理和部が、前記第２暗号処理部からの出力と、前記第１暗号処理部からの出力とを入力して排他論理和処理を実行する排他的論理和ステップとを有し、

前記第１暗号処理ステップの第１線形変換処理は、前記第１非線形変換情報を第１列ベクトルで示すと共に前記第１線形変換情報を第２列ベクトルで示した場合に、当該第１列ベクトルを当該第２列ベクトルに変換する第１行列を適用した第１線形変換処理実行ステップであり、

前記第２暗号処理ステップの第２線形変換処理は、前記第２非線形変換情報を第３列ベクトルで示すと共に前記第２線形変換情報を第４列ベクトルで示した場合に、当該第３列ベクトルを当該第４列ベクトルに変換する第２行列を適用した第２線形変換処理実行ステップであり、

前記第１線形変換処理実行ステップにおいて適用する前記第１行列と第２線形変換処理実行ステップにおいて適用する前記第２行列とは互いに異なる行列であることを特徴とする暗号処理方法にある。

さらに、本発明の暗号処理方法の一実施態様において、前記第１行列から選択した第１列ベクトルと、前記第２行列から選択した第２列ベクトルとは、いずれの列ベクトルを選択した場合であっても、互いに線形独立であることを特徴とする。

さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理方法は、前記排他論理和ステップにおける排他論理和結果を前記前記第１暗号処理部または前記第２暗号処理部に再度入力し、前記第１暗号処理ステップおよび前記第２暗号処理ステップの暗号処

理を繰り返し実行することを特徴とする。
さらに、本発明の暗号処理方法の一実施態様において、前記第１線形変換部および前記第２線形変換部における線形変換処理は、ｍ個の非線形変換部各々の出力するｎビット、総計ｍｎビットの入力に対する線形変換処理を実行するステップであり、前記第１線形変換部および前記第２線形変換部において線形変換に適用する前記第１行列と前記第２行列は、行列を構成する列ベクトルから任意に選択したｍ個の列ベクトルが互いに線形独立なるｍ次行列であることを特徴とする。
さらに、本発明の第４の側面は、
Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行する暗号処理方法であり、
非線形変換処理および線形変換処理を実行するＳＰＮ型のＦ関数を、複数ラウンド繰り返し実行し、
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
正方行列を適用した線形変換処理を実行するとともに、
少なくとも連続する偶数ラウンドおよび連続する奇数ラウンドの各々において異なる正方行列を適用した線形変換処理を実行することを特徴とする暗号処理方法にある。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正の内容】
【００２８】
さらに、本発明の第５の側面は、
暗号処理装置において暗号処理を実行させるコンピュータ・プログラムであり、
第１暗号処理部の第１非線形変換部に入力情報を非線形変換させて第１非線形変換情報を出力させ、第１暗号処理部の第１線形変換部に当該第１非線形変換情報を線形変換させて第１線形変換情報を出力させる第１暗号処理ステップと、
第２暗号処理部の第２非線形変換部に入力情報を非線形変換させて第２非線形変換情報を出力させ、第２暗号処理部の第２線形変換部に当該第２非線形変換情報を線形変換させて第２線形変換情報を出力させる第２暗号処理ステップと、
排他的論理和部に、前記第２暗号処理部からの出力と、前記第１暗号処理部からの出力とを入力して排他論理和処理を実行させる排他的論理和ステップとを有し、
前記第１暗号処理ステップの第１線形変換処理は、前記第１非線形変換情報を第１列ベクトルで示すと共に前記第１線形変換情報を第２列ベクトルで示した場合に、当該第１列ベクトルを当該第２列ベクトルに変換する第１行列を適用した第１線形変換処理実行ステップであり、
前記第２暗号処理ステップの第２線形変換処理は、前記第２非線形変換情報を第３列ベクトルで示すと共に前記第２線形変換情報を第４列ベクトルで示した場合に、当該第３列ベクトルを当該第４列ベクトルに変換する第２行列を適用した第２線形変換処理実行ステップであり、
前記第１線形変換処理実行ステップにおいて適用する前記第１行列と第２線形変換処理実行ステップにおいて適用する前記第２行列とは互いに異なる行列として設定したことを特徴とするコンピュータ・プログラムにある。
さらに、本発明の第６の側面は、
Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理を実行するコンピュータ・プログラムであり、
非線形変換処理および線形変換処理を実行するＳＰＮ型のＦ関数を、複数ラウンド繰り返し実行し、
前記複数ラウンド各々に対応するＦ関数の線形変換処理は、
正方行列を適用した線形変換処理を実行するとともに、
少なくとも連続する偶数ラウンドおよび連続する奇数ラウンドの各々において異なる正

方行列を適用した線形変換処理を実行するステップであることを特徴とするコンピュータ・プログラムにある。