【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28日(2007.6.28)

【公開番号】特開2006-72054(P2006-72054A)
【公開日】平成18年3月16日(2006.3.16)
【年通号数】公開・登録公報2006-011
【出願番号】特願2004-256465(P2004-256465)
【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5月10日(2007.5.10)
【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行列の逆行列から選択した第１行ベクトルと、
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行列の逆行列から選択した第２行ベクトルとが、
いずれの行ベクトルを選択した場合でも互いに線形独立であることを特徴とする暗号処理装置。
【請求項２】
前記暗号処理装置は、
前記排他的論理和部における排他的論理和結果を前記第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３】
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、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、正方ＭＤＳ（Ｍａｘｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）行列を適用した線形変換処理として実

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は、異なる正方ＭＤＳ行列：Ｌａ，Ｌｂが適用され、かつ該正方ＭＤＳ行列の逆行列：$Ｌａ^{－１}$，$Ｌｂ^{－１}$を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立であることを特徴とする暗号処理装置。
【請求項４】
前記暗号処理装置において、さらに、
前記逆行列：$Ｌａ^{－１}$，$Ｌｂ^{－１}$を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列が正方ＭＤＳ行列であることを特徴とする請求項３に記載の暗号処理装置。
【請求項５】
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２ｒ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ＭＤＳ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３に記載の暗号処理装置。
【請求項６】
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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立であることを特徴とする請求項３に記載の暗号処理装置。
【請求項７】
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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列も正方ＭＤＳ行列となることを特徴とする請求項３に記載の暗号処理装置。
【請求項８】
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行列の各々の逆行列は、該複数の正方ＭＤＳ行列を構成する要素を全て含むＭＤＳ行列Ｍから選択された列ベクトルによって構成される行列Ｍ'から抽出された行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３に記載の暗号処理装置。
【請求項９】
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的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行列の逆行列から選択し

た第１行ベクトルと、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行列の逆行列から選択した第２行ベクトルとは互いに線形独立であることを特徴とする暗号処理方法。

【請求項１０】

前記暗号処理方法は、

前記排他的論理和ステップにおける排他的論理和結果を前記第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９に記載の暗号処理方法。

【請求項１１】

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、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、正方ＭＤＳ（Ｍａｘｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）行列を適用した線形変換処理として実行し、

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は、異なる正方ＭＤＳ行列：Ｌａ，Ｌｂが適用され、かつ該正方ＭＤＳ行列の逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立であることを特徴とする暗号処理方法。

【請求項１２】

前記暗号処理方法において、さらに、

前記逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列が正方ＭＤＳ行列であることを特徴とする請求項１１に記載の暗号処理方法。

【請求項１３】

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２ｒの暗号処理アルゴリズムであり、

前記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$2 \leqq q \leqq r$のｑ種類の異なる正方ＭＤＳ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１１に記載の暗号処理方法。

【請求項１４】

前記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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列が線形独立であることを特徴とする請求項１１に記載の暗号処理方法。

【請求項１５】

前記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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列も正方ＭＤＳ行列となることを特徴とする請求項１１に記載の暗号処理方法。

【請求項１６】

前記Ｆ関数の線形変換処理において適用する異なる複数の行列の各々の逆行列は、該複数の正方ＭＤＳ行列を構成する要素を全て含むＭＤＳ行列Ｍから選択された列ベクトルによって構成される行列Ｍ'から抽出された行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１１に記載の暗号処理方法。

【請求項１７】

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的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行列の逆行列から選択した第１行ベクトルと、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行列の逆行列から選択した第２行ベクトルとは互いに線形独立であることを特徴とするコンピュータ・プログラム。
【請求項１８】
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するステップを有し、
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、正方ＭＤＳ（Ｍａｘｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）行列を適用した線形変換処理として実行する線形変換ステップであり、
前記線形変換ステップにおいて、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では、異なる正方ＭＤＳ行列：Ｌａ，Ｌｂが適用され、かつ該正方ＭＤＳ行列の逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立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】００１１
【補正方法】変更
【補正の内容】
【００１１】
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行列の逆行列から選択した第１行ベクトルと、

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行列の逆行列から選択した第２行ベクトルとが、

いずれの行ベクトルを選択した場合でも互いに線形独立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、前記暗号処理装置は、

前記排他的論理和部における排他的論理和結果を前記第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、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、正方ＭＤＳ（Ｍａｘｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）行列を適用した線形変換処理として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は、異なる正方ＭＤＳ行列：Ｌａ，Ｌｂが適用され、かつ該正方ＭＤＳ行列の逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立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】００１２
【補正方法】変更
【補正の内容】
【００１２】

さらに、本発明の暗号処理装置の一実施態様において、さらに、前記逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列が正方ＭＤＳ行列であることを特徴とする。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正の内容】
【００１３】

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２ｒ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$2 \leqq q \leqq r$のｑ種類の異なる正方ＭＤＳ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。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】変更
【補正の内容】
【００１４】

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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立であることを特徴とす

る。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正の内容】
【００１５】
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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列も正方ＭＤＳ行列となることを特徴とする。
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正の内容】
【００１６】
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Ｆ関数の線形変換部において適用する異なる複数の行列の各々の逆行列は、該複数の正方ＭＤＳ行列を構成する要素を全て含むＭＤＳ行列Ｍから選択された列ベクトルによって構成される行列Ｍ'から抽出された行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。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
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的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行列の逆行列から選択した第１行ベクトルと、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行列の逆行列から選択した第２行ベクトルとは互いに線形独立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、前記暗号処理方法は、前記排他

的論理和ステップにおける排他的論理和結果を前記第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、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、正方ＭＤＳ（Ｍａｘｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）行列を適用した線形変換処理として実行し、

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は、異なる正方ＭＤＳ行列：Ｌａ，Ｌｂが適用され、かつ該正方ＭＤＳ行列の逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立であることを特徴とする暗号処理方法にある。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】

さらに、本発明の暗号処理方法の一実施態様において、さらに、前記逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列が正方ＭＤＳ行列であることを特徴とする。

【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】
【００１９】

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２ｒの暗号処理アルゴリズムであり、前記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$2 \leqq q \leqq r$のｑ種類の異なる正方ＭＤＳ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。

【手続補正１１】
【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、本発明の暗号処理方法の一実施態様において、前記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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列が線形独立であることを特徴とする。

【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】

【００２１】
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ＭＤＳ行列の各々は、該複数の正方ＭＤＳ行列の逆行列を構成する行ベクトルから任意に選択したｍ個の行ベクトルによって構成する行列も正方ＭＤＳ行列となることを特徴とする。
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】変更
【補正の内容】
【００２２】
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Ｆ関数の線形変換処理において適用する異なる複数の行列の各々の逆行列は、該複数の正方ＭＤＳ行列を構成する要素を全て含むＭＤＳ行列Ｍから選択された列ベクトルによって構成される行列Ｍ'から抽出された行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。
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正の内容】
【００２３】
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的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行列の逆行列から選択した第１行ベクトルと、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行列の逆行列から選択した第２行ベクトルとは互いに線形独立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。
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するステップを有し、
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、正方ＭＤＳ（Ｍａｘ

ｉｍｕｍ　Ｄｉｓｔａｎｃｅ　Ｓｅｐａｒａｂｌｅ）行列を適用した線形変換処理として実行する線形変換ステップであり、

前記線形変換ステップにおいて、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では、異なる正方ＭＤＳ行列：Ｌａ，Ｌｂが適用され、かつ該正方ＭＤＳ行列の逆行列：La^{-1}，Lb^{-1}を構成する行ベクトルから任意に選択したｍ個の行ベクトルが線形独立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。

【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】０１２１
【補正方法】変更
【補正の内容】
【０１２１】

ステップＳ２２において、ｑ個のＧＦ（2^{n}）上のｍ次正方ＭＤＳ行列Ｌ１，Ｌ２，...，Ｌｑが生成した後、次に、以下の正方ＭＤＳ行列設定処理を実行する。

［ステップＳ２３］

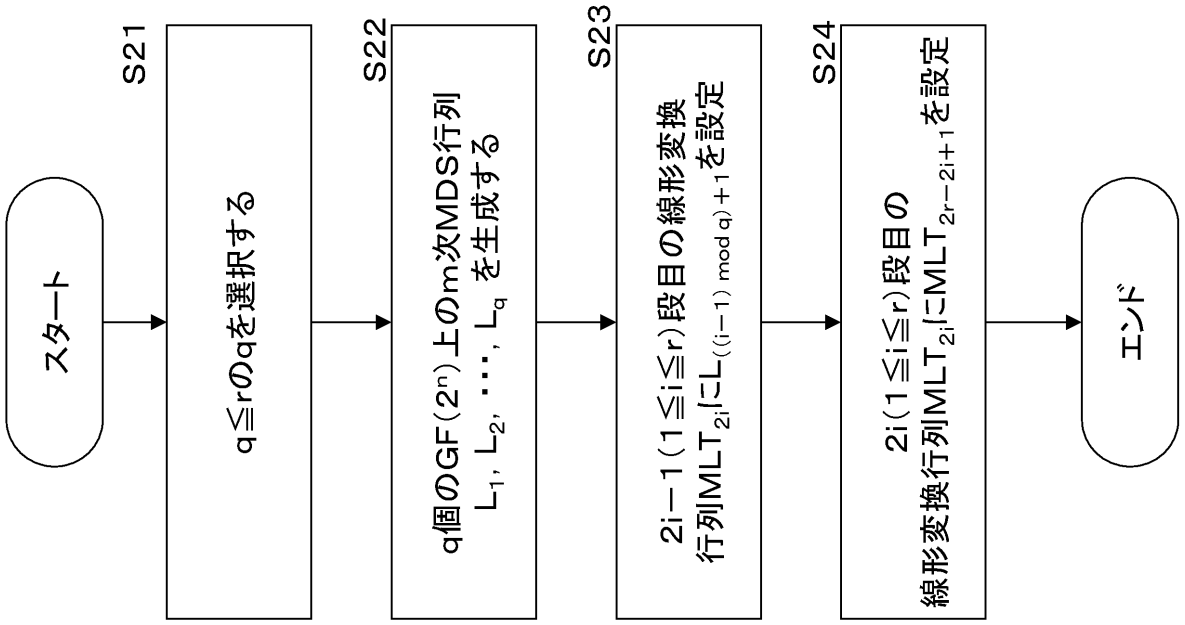
２ｉ－１（１≦ｉ≦ｒ）段目の線形変換行列MLT_{2i-1}にL$_{((i-1) \bmod q)+1}$を設定する。

［ステップＳ２４］

２ｉ（１≦ｉ≦ｒ）段目の線形変換行列に$MLT2_{i}$に$MLT_{2r-2i+1}$を設定する。

【手続補正１６】
【補正対象書類名】図面
【補正対象項目名】図１０
【補正方法】変更
【補正の内容】

【図１０】


スタート
S21
q≦rのqを選択する
S22
q個のGF(2^n)上のm次MDS行列 L1, L2, ・・・, Lq を生成する
S23
2i－1(1≦i≦r)段目の線形変換行列MLT2iにL((i－1) mod q)+1を設定
S24
2i(1≦i≦r)段目の線形変換行列MLT2iにMLT2r－2i+1を設定
エンド