

【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 21 年 8 月 27 日 (2009.8.27)

【公開番号】特開 2008-51829 (P2008-51829A)  
 【公開日】平成 20 年 3 月 6 日 (2008.3.6)  
 【年通号数】公開・登録公報 2008-009  
 【出願番号】特願 2006-224674 (P2006-224674)  
 【国際特許分類】

G 0 9 C 1/00 (2006.01)

【 F I 】

G 0 9 C 1/00 6 1 0 B

【手続補正書】

【提出日】平成 21 年 7 月 10 日 (2009.7.10)

【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】

暗号処理装置であり、

非線形変換処理および線形変換処理を含むデータ変換処理を実行する S P 型 F 関数を複数ラウンド繰り返す F e i s t e l 型共通鍵ブロック暗号処理を実行する暗号処理部を有し、

前記暗号処理部は、

データ系列数：d を  $d - 2$  の整数とした拡張 F e i s t e l 構造を適用した暗号処理を実行する構成であり、各ラウンドにおける F 関数において実行する線形変換処理に、少なくとも 2 以上の複数の異なる行列を選択的に適用する構成を有し、

前記 2 以上の複数の異なる行列は、拡張 F e i s t e l 構造の各データ系列に inputs する F 関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記複数の異なる行列を、拡張 F e i s t e l 構造の各データ系列に inputs する F 関数に繰り返し配置した構成を有することを特徴とする暗号処理装置。

【請求項 2】

前記暗号処理部において利用される前記複数の異なる行列は、

拡張 F e i s t e l 構造の各データ系列  $s(i)$  に inputs する連続する  $k$  個 (ただし、 $k$  は 2 以上の整数) の F 関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数  $[B_k^D(s(i))]$  中から選択される全データ系列中の最小分岐数  $[B_k^D]$  が 3 以上となる条件を満足する複数の異なる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 3】

前記暗号処理部において利用される前記複数の異なる行列は、

拡張 F e i s t e l 構造の各データ系列  $s(i)$  に inputs する連続する 2 個の F 関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数  $[B_2^D(s(i))]$  中から選択される全データ系列中の最小分岐数  $[B_2^D]$  が 3 以上となる条件を満足する複数の異なる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 4】

前記暗号処理部において利用される前記複数の異なる行列は、

拡張  $F_{eistel}$  構造の各データ系列  $s(i)$  に入力する連続する 2 個の  $F$  関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数  $[B_2^L(s(i))]$  中から選択される全データ系列中の最小分岐数  $[B_2^L]$  が 3 以上となる条件を満足する複数の異なる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】

前記暗号処理部は、

前記複数の異なる行列を、 $n$  個（ただし、 $n$  は 2 以上の整数）の異なる行列、

$M_0, M_1, \dots, M_{n-1}$  としたとき、

これらの異なる行列  $M_0, M_1, \dots, M_{n-1}$  を、拡張  $F_{eistel}$  構造の各データ系列に入力する  $F$  関数に順番に繰り返し配置した構成を有す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 6】

前記暗号処理部は、

1 つのラウンドに 1 つの  $F$  関数のみを実行する拡張  $F_{eistel}$  構造を適用した暗号処理を実行する構成であることを特徴とする請求項 1 ~ 5 いずれかに記載の暗号処理装置。

【請求項 7】

前記暗号処理部は、

1 つのラウンドに複数の  $F$  関数を並列に実行する拡張  $F_{eistel}$  構造を適用した暗号処理を実行する構成であることを特徴とする請求項 1 ~ 5 いずれかに記載の暗号処理装置。

【請求項 8】

前記暗号処理部は、

$a$  2 の任意の整数、 $x$  1 の任意の整数としたとき、前記複数の異なる行列による異なる線形変換処理を実行する  $a$  種類の  $F$  関数を利用したデータ系列数： $d = 2ax$  の拡張  $F_{eistel}$  構造を適用した暗号処理を実行する構成であり、

1 つのラウンドにおいて、全種類（ $a$  種類）の  $F$  関数を均等に  $x$  個ずつ実行する構成であることを特徴とする請求項 1 ~ 5 いずれかに記載の暗号処理装置。

【請求項 9】

前記暗号処理部は、

1 つのラウンドにおいて並列に実行する  $ax$  個の  $F$  関数を実行する  $F$  関数実行部と、

前記  $F$  関数実行部に対するデータ入出力制御を実行する制御部とを備えた構成であることを特徴とする請求項 8 に記載の暗号処理装置。

【請求項 10】

前記暗号処理部は、

前記複数の異なる行列による異なる線形変換処理を実行する複数の  $F$  関数実行部と、

前記複数の  $F$  関数実行部の利用シーケンスを設定に応じて変更する制御部とを備え、

前記制御部は、

(a) データ系列数  $d = 2$  とした  $F_{eistel}$  構造による暗号処理、または、

(b1) データ系列数  $d$  2 の任意数とした拡張  $F_{eistel}$  構造であり、各ラウンドにおいて 1 つの  $F$  関数の実行のみを許容した暗号処理、または、

(b2) データ系列数  $d$  2 の任意数とした拡張  $F_{eistel}$  構造であり、各ラウンドにおいて複数の  $F$  関数の並列実行を許容した暗号処理、

上記 (a), (b1), (b2) のいずれかの暗号処理を選択的に実行する構成であることを特徴とする請求項 1 ~ 5 いずれかに記載の暗号処理装置。

【請求項 11】

前記制御部は、

暗号化または復号処理の対象となるデータのビット長に応じて、実行する処理形態を選択する構成であることを特徴とする請求項 10 に記載の暗号処理装置。

## 【請求項 12】

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、

暗号処理部において、非線形変換処理および線形変換処理を含むデータ変換処理を実行する S P 型 F 関数を複数ラウンド繰り返す F e i s t e l 型共通鍵ブロック暗号処理を実行する暗号処理ステップを有し、

前記暗号処理ステップは、

データ系列数：d を  $d - 2$  の整数とした拡張 F e i s t e l 構造を適用した暗号処理を実行するステップであり、各ラウンドにおける F 関数において実行する線形変換処理に、少なくとも 2 以上の複数の異なる行列を選択的に適用した演算を実行する演算ステップを有し、

前記演算ステップにおいて適用する複数の異なる行列は、拡張 F e i s t e l 構造の各データ系列に入力する F 関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記演算ステップは、

拡張 F e i s t e l 構造の各データ系列に入力する F 関数において、前記複数の異なる行列に基づく線形変換演算を実行するステップであることを特徴とする暗号処理方法。

## 【請求項 13】

前記複数の異なる行列は、

拡張 F e i s t e l 構造の各データ系列  $s(i)$  に入力する連続する  $k$  個（ただし、 $k$  は 2 以上の整数）の F 関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数  $[B_k^D(s(i))]$  中から選択される全データ系列中の最小分岐数  $[B_k^D]$  が 3 以上となる条件を満足する複数の異なる行列であることを特徴とする請求項 12 に記載の暗号処理方法。

## 【請求項 14】

前記複数の異なる行列は、

拡張 F e i s t e l 構造の各データ系列  $s(i)$  に入力する連続する 2 個の F 関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数  $[B_2^D(s(i))]$  中から選択される全データ系列中の最小分岐数  $[B_2^D]$  が 3 以上となる条件を満足する複数の異なる行列であることを特徴とする請求項 12 に記載の暗号処理方法。

## 【請求項 15】

前記複数の異なる行列は、

拡張 F e i s t e l 構造の各データ系列  $s(i)$  に入力する連続する 2 個の F 関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数  $[B_2^L(s(i))]$  中から選択される全データ系列中の最小分岐数  $[B_2^L]$  が 3 以上となる条件を満足する複数の異なる行列であることを特徴とする請求項 12 に記載の暗号処理方法。

## 【請求項 16】

前記複数の異なる行列を、 $n$  個（ただし、 $n$  は 2 以上の整数）の異なる行列、

$M_0, M_1, \dots, M_{n-1}$  としたとき、

前記演算ステップは、

拡張 F e i s t e l 構造の各データ系列に入力する F 関数において、これらの異なる行列  $M_0, M_1, \dots, M_{n-1}$  を順番に繰り返し実行するステップであることを特徴とする請求項 12 に記載の暗号処理方法。

## 【請求項 17】

前記暗号処理ステップは、

1 つのラウンドに 1 つの F 関数のみを実行する拡張 F e i s t e l 構造を適用した暗号処理を実行するステップであることを特徴とする請求項 12 ~ 16 いずれかに記載の暗号処理方法。

## 【請求項 18】

情報処理装置において暗号処理アルゴリズムを構築する暗号処理アルゴリズム構築方法

であり、

情報処理装置における制御部が、データ系列数： $d$ を $d-2$ の整数とした拡張Feistel構造を適用した暗号処理アルゴリズムの構成において、各ラウンドにおけるF関数において実行する線形変換処理に適用する少なくとも2以上の複数の異なる行列を決定する行列決定ステップと、

前記制御部が、前記行列決定ステップにおいて決定した複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置する行列設定ステップを有し、

前記行列決定ステップは、

前記2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列を適用行列として決定する処理を実行するステップであることを特徴とする暗号処理アルゴリズム構築方法。

#### 【請求項19】

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、

暗号処理部において、非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行させる暗号処理ステップを有し、

前記暗号処理ステップは、

データ系列数： $d$ を $d-2$ の整数とした拡張Feistel構造を適用した暗号処理を実行させるステップであり、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用した演算を実行する演算ステップを含み、

前記演算ステップにおいて適用する複数の異なる行列は、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記演算ステップは、

拡張Feistel構造の各データ系列に入力するF関数において、前記複数の異なる行列に基づく線形変換演算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。

#### 【請求項20】

情報処理装置において暗号処理アルゴリズムを構築させるコンピュータ・プログラムであり、

情報処理装置における制御部に、データ系列数： $d$ を $d-2$ の整数とした拡張Feistel構造を適用した暗号処理アルゴリズムの構成において、各ラウンドにおけるF関数において実行する線形変換処理に適用する少なくとも2以上の複数の異なる行列を決定させる行列決定ステップと、

前記制御部に、前記行列決定ステップにおいて決定した複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置させる行列設定ステップを有し、

前記行列決定ステップは、

前記2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列を適用行列として決定する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】 0 0 3 2  
 【補正方法】 削除  
 【補正の内容】  
 【手続補正 3】  
 【補正対象書類名】 明細書  
 【補正対象項目名】 0 0 3 3  
 【補正方法】 削除  
 【補正の内容】  
 【手続補正 4】  
 【補正対象書類名】 明細書  
 【補正対象項目名】 0 0 3 4  
 【補正方法】 削除  
 【補正の内容】  
 【手続補正 5】  
 【補正対象書類名】 明細書  
 【補正対象項目名】 0 0 3 5  
 【補正方法】 削除  
 【補正の内容】  
 【手続補正 6】  
 【補正対象書類名】 明細書  
 【補正対象項目名】 0 0 3 6  
 【補正方法】 削除  
 【補正の内容】  
 【手続補正 7】  
 【補正対象書類名】 明細書  
 【補正対象項目名】 0 1 9 5  
 【補正方法】 変更  
 【補正の内容】  
 【 0 1 9 5 】

図 1 1 において、F 関数を識別するための番号は証明をわかりやすくするために新たに導入したものであり、2 つの数字を使って F 関数の位置を決定している。

$F_{i,j}$  の  $i$  は、ラウンド数 ( $1 = 1$ , 2 ラウンド、 $2 = 3$ , 4 ラウンド...) を示し、 $j$  は、2 つのラウンドにおける F 関数の位置を示している。なお、 $j$  が 0, 2, 4, の偶数であれば、先行ラウンドにおける F 関数であり、 $j$  が 1, 3, 5, の奇数であれば、後続ラウンドにおける F 関数である。なお、F 関数  $F_{i,j}$  に含まれる線形変換行列を  $[M_{i,j}]$  と呼ぶものとする。

【手続補正 8】  
 【補正対象書類名】 明細書  
 【補正対象項目名】 0 2 4 0  
 【補正方法】 変更  
 【補正の内容】  
 【 0 2 4 0 】

さらに、データ系列数  $d = 12$  の場合は 1 つのラウンドに存在する 6 つの F 関数を  $F_1$ ,  $F_2$ ,  $F_3$  各々 2 つずつの設定とする。また、データ系列数  $d = 18$  の場合は、1 つのラウンドに設定する 9 つの F 関数について、 $F_1$ ,  $F_2$ ,  $F_3$  を 3 つずつの設定とする。これらを一般化して、データ系列数  $d = 6x$  の場合には、各ラウンドに設定する F 関数を  $F_1$ ,  $F_2$ ,  $F_3$  の各々が  $x$  個ずつとなるようにする。すなわち、各ラウンドにおいて、異なる F 関数が均等に利用される構成とする。

【手続補正 9】  
 【補正対象書類名】 明細書

【補正対象項目名】 0 2 5 8

【補正方法】 変更

【補正の内容】

【 0 2 5 8 】

このような３種類の F 関数  $F_1$  ,  $F_2$  ,  $F_3$  を実行する暗号処理装置の構成例を図 19 に示す。図 19 に示す暗号処理装置 280 は、F 関数  $F_1$  を実行する第 1 F 関数 ( $F_1$ ) 専用処理回路 281 と、F 関数  $F_2$  を実行する第 2 F 関数 ( $F_2$ ) 専用処理回路 282 と、F 関数  $F_3$  を実行する第 3 F 関数 ( $F_3$ ) 専用処理回路 283 と、制御回路 284、および補助回路 285 から構成される。第 1 F 関数 ( $F_1$ ) 専用処理回路 281 と、第 2 F 関数 ( $F_2$ ) 専用処理回路 282 と、第 3 F 関数 ( $F_3$ ) 専用処理回路 283 とは並列に動作可能な構成である。制御回路 284 は、各処理部に対するデータ入出力制御を行うとともに、Feistel 構造選択処理を実行する。補助回路 285 は F 関数以外の演算処理などを実行する。

【手続補正 10】

【補正対象書類名】 明細書

【補正対象項目名】 0 2 6 1

【補正方法】 変更

【補正の内容】

【 0 2 6 1 】

上述したように、拡散行列切り替え機構 (DSM) を満足する線形変換行列を実行する複数の異なる F 関数を決定し、これらの各 F 関数を実装して、F 関数を適用した処理シーケンスを変更することで、

(a) データ系列数 (分割数)  $d = 2$  とした Feistel 構造

(b1) データ系列数 (分割数)  $d = 2$  の任意数とした拡張 Feistel 構造であり、各ラウンドにおいて 1 つの F 関数の実行のみを許容したタイプ 1、

(b2) データ系列数 (分割数)  $d = 2$  の任意数とした拡張 Feistel 構造であり、各ラウンドにおいて複数の F 関数の並列実行を許容したタイプ 2、

これらのいずれかの構造に基づく暗号処理を 選択的 に実行する構成が実現され、暗号化処理または復号処理における処理ビット数を変更可能な装置が実現される。