República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI 0715646-4 A2**

BRPI0715646A2

(22) Data de Depósito: 17/07/2007
(43) Data da Publicação: 26/03/2013
(RPI 2203)

(51) Int.Cl.:
G09C 1/00
H04L 9/06

(54) Título: APARELHO E MÉTODO DE PROCESSAMENTO POR CRIPTOGRAFIA, MÉTODO DE CONSTRUÇÃO DE ALGORITMO DE PROCESSAMENTO POR CRIPTOGRAFIA, E, PROGRAMA DE COMPUTADOR

(30) Prioridade Unionista: 28/07/2006 JP 2006-206376, 21/08/2006 JP 2006-224674, 21/08/2006 JP 2006-224674

(73) Titular(es): Sony Corporation

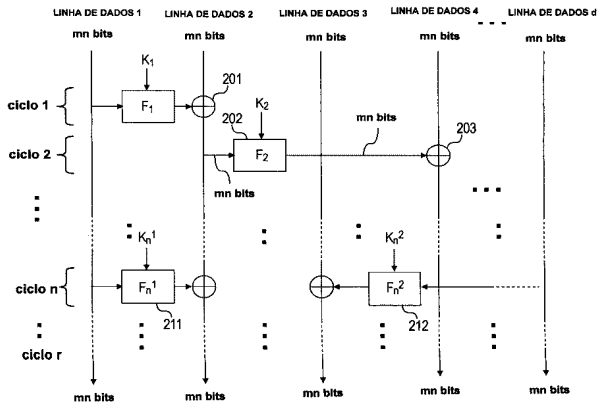
(72) Inventor(es): Kyoji Shibutani, Taizo Shirai

(74) Procurador(es): Momsen, Leonardos & Cia

(86) Pedido Internacional: PCT JP2007064089 de 17/07/2007

(87) Publicação Internacional: WO 2008/013076de 31/01/2008

(57) Resumo: APARELHO E MÉTODO DE PROCESSAMENTO POR CRIPTOGRAFIA, MÉTODO DE CONSTRUÇÃO DE ALGORITMO DE PROCESSAMENTO POR CRIPTOGRAFIA, E, PROGRAMA DE COMPUTADOR. Realizar uma configuração de processo de cifra de bloco de chave comum do tipo Feistel estendido para realização de um mecanismo de comutação de matriz de difusão (DSMF). Em uma configuração de processo criptográfico em que uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é estabelecida para um inteiro que satisfaça d ≥ 2 é aplicada, uma pluralidade de múltiplas matrizes diferentes são aplicadas, seletivamente, a processos de transformação linear realizados em seções de função-F. Uma pluralidade de matrizes diferentes satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado são selecionadas como as matrizes, o número mínimo de derivações correspondendo ás linhas de dados, cada um dos números mínimos de derivações correpondentes ás linhas de dados sendo baseados em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondendte na estrutura de Feistel estendida. De acordo com a presente invenção, cifra de bloco de chave comum com base na DSM com uma alta resistência à análise linear e análise diferencial é realizada.



"APARELHO E MÉTODO DE PROCESSAMENTO POR CRIPTOGRAFIA, MÉTODO DE CONSTRUÇÃO DE ALGORITMO DE PROCESSAMENTO POR CRIPTOGRAFIA, E, PROGRAMA DE COMPUTADOR"

Campo Técnico

A presente invenção se refere a um aparelho de processamento criptográfico, a um método de construção de algoritmo de processamento criptográfico e um programa de computador. Mais especificamente, a presente invenção se refere a um aparelho de processamento criptográfico, a um método de construção de algoritmo de processamento criptográfico e a um método de processamento criptográfico, que realizam processos de cifra de bloco de chave comum do tipo Feistel e um programa de computador.

Técnica Anterior

Atualmente, com o desenvolvimento da comunicação através de rede e do comércio eletrônico, a garantia de segurança na comunicação tem se tornado uma questão importante. Um método para garantir a segurança é a tecnologia criptográfica e a comunicação usando várias técnicas de criptografia é feita correntemente, na realidade.

Por exemplo, um sistema tem sido posto em uso prático, em que um módulo de processamento criptográfico é embutido em um dispositivo compacto, tal como um cartão de IC e em que a transmissão e a recepção de dados são realizadas entre o cartão de CI e uma leitora/impressora servindo como um aparelho de leitura e escrita de dados, assim, realizando um processo de autenticação ou de criptografia e descriptografia de dados recebidos e transmitidos.

Há vários algoritmos de processamento criptográfico, que são amplamente classificados em um esquema criptográfico de chave pública, em que uma chave de criptografia e uma chave de descriptografia são ajustadas como chaves diferentes, por exemplo, uma chave pública e uma chave

secreta, e um esquema criptográfico de chave comum.

O esquema criptográfico de chave comum tem vários algoritmos. Um deles é um esquema em que uma pluralidade de chaves são geradas com base em uma chave como um de em que um processo de transformação de dados em idade de blocos (tais como 64 bits ou 128 bits) é realizado repetidamente, usando a pluralidade de chaves geradas. Um algoritmo típico ao qual esse esquema de geração de chave e um processo de transformação de dados são aplicados é um esquema de cifra de blocos de chave comum.

Como um algoritmo de cifra de blocos de chave comum típico, por exemplo, um algoritmo de DES (Data Encryption Standard-Padrão de Criptografia de Dados), que é uma criptografia padrão dos EUA, é amplamente usado em vários campos.

O algoritmo de cifras de blocos de chave comum, tipificado pelo DES, pode ser dividido principalmente em seções de função de arredondamento que realizam transformação de entrada de dados e uma seção de programação de chaves que gera as chaves de arredondamento aplicadas em respectivos arredondamentos das seções de função de arredondamento (Função-F). Chaves de arredondamento (sub-chaves) que devem ser aplicadas nos respectivos arredondamentos das seções de função de arredondamento são geradas com base em uma chave mestre (uma chave principal) que é introduzida na seção de programação de chave e são aplicadas nas respectivas seções de função de arredondamento.

Uma estrutura de Feistel é conhecida como uma estrutura específica para a execução de um algoritmo ao qual essas funções de arredondamento são aplicadas. A estrutura de Feistel tem uma estrutura que transforma texto normal em texto cifrado através da simples repetição de funções de transformação que são chamadas funções de arredondamento. Exemplos de documentos descrevendo processos criptográficos aos quais as

estruturas de Feistel são aplicadas incluem o Documento de Não Patente 1 e o documento de Não Patente 2.

Contudo, por exemplo, um processo criptográfico de chave comum, ao qual a estrutura de Feistel é aplicada, tem um problema de vazamento de chaves devido à criptanálise. A análise diferencial (também chamada de criptanálise diferencial ou ataque diferencial), em que as chaves aplicadas nas respectivas funções de arredondamento são analisadas através da análise de múltiplos pedaços de dados de entrada (texto normal) tendo uma certa diferença e pedaços de dados de saída (texto cifrado) para os dados de entrada e análise linear (também chamada criptanálise linear ou ataque linear), em que a análise baseada no texto normal e no texto cifrado correspondente é realizada, têm sido conhecidas como técnicas típicas de criptanálise ou técnicas de ataque.

A análise fácil de chaves devido à criptanálise implica baixa segurança de um processo criptográfico usando as chaves. Em algoritmos criptográficos da técnica anterior, como os processos (matrizes de transformação) que são aplicados em seções de transformação linear de seções de função de arredondamento (função-F) são iguais um ao outro em arredondamentos de respectivos estágios, a análise é possível, resultando em uma fácil análise de chaves.

Como uma configuração para lidar com esse problema, tem sido proposta uma configuração em que duas ou mais matrizes diferentes são dispostas em seções em seções de transformação linear (função-F) em uma estrutura de Feistel. Essa técnica é chamada um mecanismo de comutação de matriz de difusão (DSM: Diffusion Switching Mechanism - Mecanismo de Comutação de Difusão, daqui em diante referido como "DSM"). A resistência aos ataques diferenciais ou ataques lineares pode ser acentuada usando esse DSM.

O mecanismo de comutação de matriz de difusão (DSM) é

proporcionado como uma configuração que pode ser aplicada a uma estrutura de Feistel típica, tendo duas linhas de dados. Em contraste, há uma estrutura de Feistel do tipo estendido, tendo três ou mais linhas de dados, que é diferente da estrutura de Feistel típica, tendo duas linhas de dados. Contudo, nenhuma configuração foi divulgada em que o mecanismo de comutação de matriz de difusão (DSM) mencionado acima é aplicado nessa estrutura de Feistel do tipo estendido, tendo três ou mais linhas de dados de modo que a resistência aos ataques diferenciais ou ataques lineares é acentuada.

Documento de Não Patente 1: K. Nyberg, "Extended Feistel structures", ASIACRYPT'96, SpringerVerlag, 1996, pp.91--104.

Documento de Não Patente 2: Yuliang Zheng, Tsutomu Matsumoto, Hideki Imai: On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. CRYPTO 1989: 461-480.

Descrição da Invenção

Problema Técnico

A presente invenção foi feita em vista dos problemas precedentes e ajuda a proporcionar um aparelho de processamento criptográfico, um método de construção de algoritmo de processamento criptográfico e um método de processamento criptográfico, que realizam algoritmos de cifra de blocos de chave comum com uma alta resistência à análise linear e à análise diferencial e um programa de computador.

Mais especificamente, as seções de função de arredondamento, às quais uma pluralidade de matrizes de transformação linear diferentes são aplicadas, são colocadas em uma estrutura de Feistel obtidas pela expansão de uma estrutura de Feistel, tendo duas linhas de dados, isto é, em uma estrutura de Feistel do tipo estendido, tendo qualquer número de linhas de dados que é igual ou maior do que dois, tal como três ou quatro, assim, ajudando a proporcionar um aparelho de processamento criptográfico, um método de

construção de algoritmo de processamento criptográfico e um método de processamento criptográfico, que realizam algoritmos de cifra de blocos de chave comum com uma alta resistência à análise diferencial, e um programa de computador.

Solução técnica

Um primeiro aspecto da presente invenção reside em: um aparelho de processamento criptográfico caracterizado por incluir uma seção de processamento criptográfico que realiza um processo de cifra de blocos de chave comum do tipo Feistel de repetição de uma função-F do tipo SP em uma pluralidade de arredondamentos, a função-F do tipo SP realizando um processo de transformação de dados que inclui um processo de transformação não linear e um processo de transformação linear, em que a seção de processamento criptográfico é configurada para realizar um processo criptográfico ao qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é ajustado para um inteiro que satisfaz $d \geq 2$ é aplicada, é configurada para aplicar, seletivamente, uma pluralidade de pelo menos duas ou mais matrizes diferentes aos processos de transformação linear que são realizados em funções-F em respectivos arredondamentos, a pluralidade de duas ou mais matrizes sendo uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações, correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondentes às linhas de dados sendo baseado em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida e é configurado de modo que a pluralidade de matrizes diferentes é disposta repetidamente nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

Além disso, em uma modalidade do algoritmo de processamento criptográfico da presente invenção, é caracterizado pelo fato de a pluralidade de matrizes diferentes, que são utilizadas na seção de processamento criptográfico, são uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_k^D]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_k^D(s(i))]$, correspondendo às linhas de dados, cada um dos números mínimos de derivações $[B_k^D(s(i))]$ correspondendo às linhas de dados que estão sendo calculadas com base em matrizes de transformação linear incluídas em duas funções-f contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a pluralidade de matrizes diferentes, que são utilizadas na seção de processamento criptográfico de uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2^L]$ para todas as linhas de dados é igual ou maior do que três, o número mínimo de derivações $[B_2^L]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_2^L(s(i))]$ correspondentes às linhas de dados, cada um dos números mínimos de derivações $[B_2^L(s(i))]$ correspondendo às linhas de dados sendo calculados com base nas matrizes de transformação linear incluídas em duas funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de, quando a pluralidade de matrizes diferentes são denotadas por n (onde n é um inteiro igual ou maior do que dois) matrizes diferentes, isto é, M_0, M_1, ...M_{n-1}, a seção de processamento criptográfico é configurada de modo que as

matrizes diferentes M_0, M_1, ...M_{n-1}, são dispostas repetidamente em uma ordem nas funções-F, que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a seção de processamento criptográfico ser configurada para realizar um processo criptográfico ao qual uma estrutura de Feistel estendida que realiza apenas uma função-F em um arredondamento é aplicada.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção ele é caracterizado pelo fato de a seção de processamento criptográfico ser configurada para realizar um processo criptográfico ao qual uma estrutura de Feistel estendida que realiza uma pluralidade de funções-F em um arredondamento é aplicada.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a seção de processamento criptográfico ser configurada para realizar, quando a é qualquer inteiro que satisfaça $a \geq 2$ e x é qualquer inteiro que satisfaça $x \geq 1$, um processo criptográfico ao qual uma estrutura de Feistel estendida, que utiliza um tipo de funções-F e que tem o número de linhas de dados: d, que é ajustado como $d = 2ax$ é aplicada, os tipos de a de funções-F que realizam processos diferentes de transformação linear, usando a pluralidade de matrizes diferentes e configurado para realizar igualmente x pedaços de cada um dos tipos (os tipos de a) de funções-F em um arredondamento.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a seção de processamento criptográfico ser configurada por incluir: uma unidade de realização de função-F que realiza funções-F que são realizadas em paralelo em um arredondamento; e uma unidade de controle

que realiza controle de entrada/saída de dados para a unidade de realização de função-F.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a seção de processamento criptográfico ser configurada por incluir: uma pluralidade de unidades de realização de função-F que realizam processos diferentes de transformação linear, usando a pluralidade de matrizes diferentes; e uma unidade de controle que muda uma seqüência de utilização da pluralidade de unidades de realização de função-F de acordo com uma configuração, em que a unidade de controle é configurada para realizar, seletivamente, qualquer um de processos criptográficos (a), (b1) e (b2), isto é,

a) um processo criptográfico usando uma estrutura de Feistel tendo o número de linhas de dados d que é ajustado como $d = 2$;

b1) um processo criptográfico usando uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$ e em que apenas uma função-F é permitida ser realizada em cada arredondamento; ou

b2) um processo criptográfico que usa uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$ e em que uma pluralidade de funções-F são permitidas serem realizadas em paralelo em cada arredondamento.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a unidade de controle ser configurada para selecionar um modo de processamento a ser realizado de acordo com um comprimento de bit de dados que deve ser submetido a um processo de criptografia ou descriptografia.

Um segundo aspecto da presente invenção reside em: um método de processamento criptográfico para realizar um processo

criptográfico em um aparelho de processamento criptográfico, o método caracterizado pelo fato de incluir uma etapa de processamento criptográfico de realização de um processo de cifra de blocos de chave comum do tipo Feistel de repetição de uma função-F do tipo SP em uma pluralidade de arredondamentos em uma seção de processamento criptográfico, a função-F do tipo SP realizando um processo de transformação de dados, incluindo um processo de transformação não linear e um processo de transformação linear, em que a etapa de processamento criptográfico é uma etapa de realização de um processo criptográfico ao qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é ajustado para um inteiro que satisfaça $d \geq 2$ é aplicada e inclui uma etapa de operação de realização de operações em que uma pluralidade de pelo menos duas matrizes diferentes são aplicadas, seletivamente, aos processos de transformação linear que são realizados em funções-F em respectivos arredondamentos, em que uma pluralidade de matrizes diferentes que são aplicadas na etapa de operação, são uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo da derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseadas em matrizes de transformação linear, incluídas em funções-F, que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida e em que a etapa de operação é uma etapa de realização de operações de transformação linear com base na pluralidade de matrizes diferentes nas funções-F, que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a pluralidade de matrizes diferentes serem uma pluralidade de matrizes

diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2^L]$ para todas as linhas de dados é igual ou maior do que três, o número mínimo de derivações $[B_2^L]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_2^L(s(i))]$ correspondentes às linhas de dados, cada um dos números mínimos de derivações $[B_2^L(s(i))]$ correspondendo às linhas de dados sendo calculado com base nas matrizes de transformação linear incluídas em k (onde k é um inteiro igual ou maior do que dois) funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a pluralidade de matrizes diferentes serem uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2^L]$ para todas as linhas de dados é igual ou maior do que três, o número mínimo de derivações $[B_2^L]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_2^L(s(i))]$ correspondentes às linhas de dados, cada um dos números mínimos de derivações $[B_2^L(s(i))]$ correspondendo às linhas de dados sendo calculado com base nas matrizes de transformação linear incluídas em duas funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a pluralidade de matrizes diferentes serem uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2^L]$ para todas as linhas de dados é igual ou maior do que três, o número mínimo de derivações $[B_2^L]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_2^L(s(i))]$ correspondentes às linhas de dados, calculadas com base em matrizes de

transformação linear incluídas em duas funções-f contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

Além disso, em uma modalidade do aparelho de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de, quando a pluralidade de matrizes diferentes são denotadas por n (onde n é um inteiro igual ou maior do que dois) matrizes diferentes, isto é, M_0, M_1, ...M_{n-1}, a etapa de operação é uma etapa de realização, repetidamente, das matrizes diferentes M_0, M_1, ...M_{n-1}, em uma ordem nas funções-F, que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a etapa de processamento criptográfico ser uma etapa de realização de um processo criptográfico ao qual uma estrutura de Feistel estendida que realiza apenas uma função-F em um arredondamento é aplicada.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a etapa de processamento criptográfico ser uma etapa de realização de um processo criptográfico ao qual uma estrutura de Feistel estendida que realiza uma pluralidade de funções-F em paralelo em um arredondamento é aplicada.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a etapa de processamento criptográfico ser uma etapa de realização, quando a é qualquer inteiro que satisfaça $a \geq 2$ e x é qualquer inteiro que satisfaça $x \geq 1$, um processo criptográfico ao qual uma estrutura de Feistel estendida, que utiliza a tipos de funções-F e que tem o número de linhas de dados: d, que é ajustado como $d = 2ax$ é aplicada, os a tipos funções-F que realizam processos diferentes de transformação linear, usando a pluralidade de matrizes diferentes e uma etapa de realização igualmente x pedaços de cada um dos

tipos (os a tipos) de funções-F em um arredondamento.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a etapa de processamento criptográfico ser uma etapa de realização de um processo criptográfico em que uma unidade de realização de função-F que realiza ax funções-F que são realizadas em paralelo em um arredondamento é aplicada, de acordo com o controle realizado por uma unidade de controle que realiza controle de entrada/saída de dados para a unidade de realização de função-F.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a etapa de processamento criptográfico ser uma etapa de realização de um processo criptográfico pelo uso de uma pluralidade de unidades de realização de função-F que realizam processos diferentes de transformação linear, usando a pluralidade de matrizes diferentes e pelo uso de uma unidade de controle que muda uma seqüência de utilização da pluralidade de unidades de realização de função-F de acordo com uma configuração, em que a etapa de processamento criptográfico é uma etapa, de acordo com o controle realizado pela unidade de controle realizando, seletivamente, qualquer um de processos criptográficos (a), (b1) e (b2), isto é,

a) um processo criptográfico usando uma estrutura de Feistel tendo o número de linhas de dados d que é ajustado como $d = 2$;

b1) um processo criptográfico usando uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$ e em que apenas uma função-F é permitida ser realizada em cada arredondamento; ou

b2) um processo criptográfico que usa uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$ e em que uma pluralidade de funções-F são permitidas serem realizadas em paralelo em cada arredondamento.

Além disso, em uma modalidade do método de processamento criptográfico da presente invenção, ele é caracterizado pelo fato de a unidade de controle selecionar um modo de processamento a ser realizado de acordo com um comprimento de bit de dados que deve ser submetido a um processo de criptografia ou descriptografia.

Um terceiro aspecto da presente invenção reside em:

um método de construção de algoritmo de processamento criptográfico para construir um algoritmo de processamento criptográfico em um aparelho de processamento de informação, o método caracterizado por incluir:

uma etapa de determinação de matriz, em que uma configuração de algoritmo de processamento criptográfico, ao qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d, que é ajustado para um inteiro que satisfaça $d \geq 2$ é aplicado, uma unidade de controle proporcionada no aparelho de processamento de informação determina uma pluralidade de pelo menos duas ou mais matrizes diferentes que devem ser aplicadas aos processos de transformação linear realizados em funções-F em respectivos arredondamentos; e

uma etapa de configuração de matriz em que a unidade de controle dispões, repetidamente, a pluralidade de matrizes diferentes, que são determinadas na etapa de determinação de matriz, nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida, em que a etapa de determinação de matriz é uma etapa de realização de um processo de determinação, como a pluralidade de duas ou mais matrizes diferentes, como as matrizes a serem aplicadas, uma pluralidade de matrizes diferentes, satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações

correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear na estrutura de Feistel estendida.

Um quarto aspecto da presente invenção reside em:

um processamento criptográfico que faz com que um algoritmo de processamento criptográfico realize um processamento criptográfico, o programa caracterizado pelo fato de incluir uma etapa de processamento criptográfico, fazendo com que uma seção de processamento criptográfico realize um processo de cifra de blocos de chave comum do tipo Feistel, a função-F do tipo SP realizando um processo de transformação de dados, incluindo um processo de transformação não linear e um processo de transformação linear, em que a etapa de processamento criptográfico é uma etapa de fazer a seção de processamento criptográfico realizar um processo criptográfico ao qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é ajustado para um inteiro que satisfaça $d \geq 2$ é aplicada, e inclui uma etapa de operação de realização de operações em que uma pluralidade de pelo menos duas ou mais matrizes diferentes são aplicadas, seletivamente, aos processos de transformação linear, que são realizados em funções-F em respectivos arredondamentos, em que a pluralidade de matrizes diferentes, que são aplicadas na etapa de operação, são uma pluralidade de matrizes diferentes, satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados com base em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linhas de dados correspondente na estrutura de Feistel estendida, e em que a etapa de operação é uma etapa de realização de operações de transformação

linear com base na pluralidade de matrizes diferentes nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

Um quinto aspecto da presente invenção reside em:

um programa de computador que faz com que um aparelho de processamento de informação construa um algoritmo de processamento criptográfico, o programa caracterizado pelo fato de incluir: uma etapa de determinação de matriz, fazendo, em uma configuração de algoritmo de processamento criptográfico à qual uma estrutura de Feistel estendida, tendo um número de linha de dados: d que é ajustado para um inteiro que satisfaça d $\geq$ 2 é aplicada, uma unidade de controle proporcionada no aparelho de processamento de informação para determinar uma pluralidade de pelo menos duas ou mais matrizes diferentes que devem ser aplicadas aos processos de transformação linear realizados em funções-F em respectivos arredondamentos; e uma etapa de configuração de matriz fazendo com que a unidade de controle disponha, repetidamente, a pluralidade de matrizes diferentes, que são determinadas na etapa de determinação de matriz, nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida, em que a etapa de determinação de matriz é uma etapa de realização de um processo de determinação, como é uma etapa de realização de um processo de determinação, como a pluralidade de duas ou mais matrizes diferentes, como as matrizes a serem aplicadas, uma pluralidade de matrizes diferentes, satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear incluídas funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida.

Note que o programa de computador da presente invenção é um programa de computador que pode ser proporcionado usando um meio de armazenamento ou um meio de comunicação, por exemplo, um meio de gravação, tal como CD, um FD ou um MO ou um meio de comunicação, tal como uma rede, que proporciona um programa em um formato legível em computador para um sistema de computador capaz de executar vários códigos de programas. Esse programa é proporcionado em um formato legível em computador, pelo que um processo de acordo com o programa é realizado no sistema de computador.

Ainda outros objetivos, características e vantagens da presente invenção se tornarão evidentes de descrições mais detalhadas com base em modalidades da presente invenção, que serão descritas abaixo ou nos desenhos anexos.

Note que um "sistema" mencionado no relatório descritivo é configurado como um conjunto lógico de uma pluralidade de aparelhos e não está limitado a um sistema em que os aparelhos tendo respectivas configurações estão contidos na mesma caixa.

Efeitos Vantajosos

De acordo com uma configuração em uma modalidade da presente invenção, em um processo de cifra de blocos de chave comum do tipo Feistel, em que funções-F do tipo SPN, incluindo seções de transformação não linear e seções de transformação linear, são realizadas repetidamente em uma pluralidade de arredondamentos, seções de função de arredondamento, às quais matrizes diferentes de transformação linear são aplicadas, são ajustadas em uma estrutura de Feistel obtida pela expansão de uma estrutura de Feistel tendo duas linhas de dados, isto em, em uma estrutura de Feistel tendo qualquer número de linhas de dados que é igual ou maior do que dois, tais como três ou quatro, assim, realizando um mecanismo de comutação de matriz de difusão (DSM), de modo que um algoritmo de

cifra de blocos de chave comum pode ser construído e um processo criptográfico pode ser realizado com uma alta resistência à análise linear e à análise diferencial.

De acordo com uma configuração em uma modalidade da presente invenção, uma configuração é proporcionada, em que um processo criptográfico ao qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é ajustado para um inteiro que satisfaça $d \geq 2$ é aplicada é realizado e a configuração é proporcionada como uma configuração em que uma pluralidade de pelo menos duas matrizes diferentes são aplicadas, seletivamente, aos processos de transformação linear realizados em funções-F em respectivos arredondamentos. Uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, são ajustadas como a pluralidade de duas ou mais matrizes diferentes, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear, incluídas em funções-F, que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida e em que a etapa de operação é uma etapa de realização de operações de transformação linear com base na pluralidade de matrizes diferentes nas funções-F, que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida, assim, realizando o mecanismo de comutação de matriz de difusão (DSM), de modo que um algoritmo de cifra de blocos de chave comum pode ser construído e um processo criptográfico pode ser realizado com uma alta resistência à análise linear a à análise diferencial.

Além disso, de acordo com uma configuração em uma modalidade da presente invenção, uma configuração é proporcionada, em que

a ($a \geq 2$) tipos de funções-F realizam diferentes processos de transformação linear, usando uma pluralidade de matrizes diferentes, em que uma estrutura de Feistel estendida ($x \geq 1$) que utiliza as funções-F e que tem o número de linhas de dados: d que é ajustado como d-2ax e em que um processo criptográfico ao qual a estrutura de Feistel estendida é aplicada é realizado. A configuração é proporcionada como uma configuração em que, igualmente, x pedaços de cada um dos tipos (os a tipos) de funções-F são realizados em um arredondamento, pelo que um aparelho de processamento criptográfico compacto, em que nenhum circuito desnecessário é proporcionado, é realizado.

Além disso, de acordo com uma configuração em uma modalidade da presente invenção, uma pluralidade de unidades de realização de funções-F são configuradas para realizar diferentes processos de transformação linear, usando uma pluralidade de matrizes diferentes e uma configuração é proporcionada, em que uma seqüência de utilização da pluralidade de unidades de realização de função-F é mudada de acordo com uma configuração, pelo que um aparelho de processamento criptográfico é realizado, o qual pode realizar, seletivamente, qualquer um de processos criptográficos (a), (b1) e (b2), isto é,

a) um processo criptográfico usando uma estrutura de Feistel, tendo o número de linhas de dados d que é ajustado como $d = 2$;

b1) um processo criptográfico usando uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$ e em que apenas uma função-F é permitida ser realizada em cada arredondamento; ou

b2) um processo criptográfico que usa uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$ e em que uma pluralidade de funções-F são permitidas serem realizadas em paralelo em cada arredondamento.

Breve Descrição dos Desenhos

A figura 1 é um diagrama mostrando uma configuração de cifra de chave comum típica, tendo uma estrutura de Feistel.

A figura 2 é um diagrama descrevendo uma configuração de uma função-F que é ajustada como uma seção de função de arredondamento.

A figura 3 é um diagrama mostrando um algoritmo criptográfico do tipo Feistel, em que duas matrizes diferentes de transformação linear são utilizadas..

A figura 4 é um diagrama descrevendo o algoritmo criptográfico do tipo Feistel em que três matrizes diferentes de transformação linear são utilizadas.

A figura 5 é um diagrama descrevendo definições de uma estrutura de Feistel estendida.

A figura 6 é um diagrama mostrando um exemplo de uma estrutura de Feistel estendida, tendo sete linhas de dados (d = 7).

A figura 7 é um diagramas descrevendo definições de respectivas seções constituintes e dados de entrada/saída das respectivas seções constituintes de uma estrutura de Feistel estendida.

A figura 8 é um diagrama descrevendo a aplicação de DSM a uma estrutura de Feistel estendida ou a um tipo 1.

A figura 9 é um diagramas descrevendo a aplicação do DSM a uma estrutura de Feistel estendida ou a um tipo 2.

A figura 10 é um diagrama descrevendo a aplicação do DSM à estrutura de Feistel estendida ou a um tipo 1.

A figura 11 é um diagrama descrevendo a aplicação do DSM à estrutura de Feistel estendida ou a um tipo 2.

A figura 12 é um diagrama descrevendo uma configuração em que a eficiência da implementação é aperfeiçoada em uma estrutura de Feistel estendida.

A figura 13 é um diagrama descrevendo um exemplo de configuração de *hardware*, em que a eficiência da implementação é aperfeiçoada em uma estrutura de Feistel estendida.

A figura 14 é um diagrama descrevendo um exemplo de uma disposição para a implementação de modo eficiente de três tipos de funções-F.

A figura 15 é um diagrama mostrando uma configuração de cifra de blocos de 2mn bits que é proporcionada como uma estrutura de Feistel, tendo o número de linhas de dados que é estabelecido como d = 2.

A figura 16 é um diagrama mostrando uma estrutura de Feistel estendida, que satisfaz o mecanismo de comutação de matriz de difusão (DSM) e que tem o número de linhas de dados que é ajustado como d = 4.

A figura 17 é um diagrama descrevendo uma configuração de compartilhamento de circuito em que a cifra de blocos usando números diferentes de bits pode ser realizada.

A figura 18 é um diagrama descrevendo uma estrutura de Feistel à qual funções-F, isto é, três tipos de funções-F, F1, F2 e F3, são aplicadas e que tem o número de linhas de dados que é estabelecido como d = 2.

A figura 19 é um diagrama descrevendo um exemplo de uma configuração de um aparelho de processamento criptográfico que realiza os três tipos de funções-F, F1, F2 e F3.

A figura 20 é um diagrama mostrando um exemplo de uma configuração de um módulo de CI, servindo como um aparelho de processamento criptográfico, que realiza um processo criptográfico, de acordo com a presente invenção.

Melhores Modos para Realização da Invenção

Um algoritmo de processamento criptográfico e um método de processamento criptográfico e um programa de computador serão descritos

abaixo em detalhes. A descrição é feita na ordem dos cabeçalhos de seções como segue;

1. Estrutura de Feistel tendo Funções-F do Tipo SP

2. Função de Operação de Número de Derivações e função de Avaliação de Resistência

2-1. Função de Operação de Número de Derivações: Derivação ()

2-2. Índice de Avaliação de Resistência aos Ataques Diferenciais

2-3. Índice de Avaliação de Resistência aos Ataques Lineares

3. Método para Ajustar DSM para a Estrutura de Feistel Tendo Duas Linhas de Dados

4. Ajuste de DSM em Estrutura de Feistel estendida

4-1. Referência à Estrutura de Feistel estendida

4-2. Configuração para Acentuar a Resistência aos Ataques Diferenciais em Estrutura de Feistel estendida

4-2-1. Configuração para Selecionar Matrizes, que devem ser Ajustadas em Funções-F, que Fazem o Valor do Número Mínimo de Derivações B_2^D Igual ou Maior do que Três

4-2-2. Configuração para Selecionar Matrizes, que devem ser Ajustadas em Funções-F, que Fazem o Valor do Número Mínimo de Derivações B_K^D Igual ou Maior do que Três

4-3. Configuração para Acentuar a Resistência aos Ataques Lineares em Estrutura de Feistel estendida

4-3-1. Configuração para Selecionar Matrizes, que devem ser Ajustadas em Funções-F, que Fazem o Valor do Número Mínimo de Derivações B_2^L Igual ou Maior do que Três

5-1. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 1

5-2. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 2

6. Prova de Relações entre Números de Caixas-S Ativas em Estrutura de Feistel estendida de Cada Tipo e Números Mínimos de Derivações com Base em Matrizes de Transformação Linear em Funções-F

7. Configuração Aperfeiçoada para Implementação com Base em um Plano de Ajuste de Funções-F e Processo de Utilização de Funções-F

7-1. Método para Dispor Eficientemente Funções-F em Estrutura de Feistel estendida do Tipo 2

7-2. Associação de Componentes em Estrutura de Feistel e Estrutura de Feistel estendida

8. Sumário de Processos Criptográficos e Processos de Construção de Algoritmos Criptográficos da Presente Invenção

9. Exemplo de Configuração de Aparelho de Processamento Criptográfico

1. Estrutura de Feistel Tendo Funções-F do Tipo SP

Primeiro, uma estrutura de Feistel tendo funções-F do tipo SP será descrita. Uma estrutura de Feistel é conhecida como um desenho de cifra de blocos de chave comum. A estrutura de Feistel tem uma estrutura que transforma texto normal em texto cifrado através da repetição de uma unidade básica de processamento, que é referida como uma função de arredondamento.

Uma configuração básica da estrutura de Feistel será descrita com referência à figura 1. A figura 1 mostra um exemplo de uma estrutura de Feistel, tendo duas linhas de dados, tendo um número de arredondamento = r, que indica r arredondamentos. Note que o número de arredondamentos r é um parâmetro que é determinado em um estágio de desenho e que é um valor que pode ser mudado de acordo, por exemplo, com o comprimento de uma chave de entrada.

Na estrutura de Feistel mostrada na figura 1, é suposto que o comprimento do texto normal, que é introduzido como um alvo a ser criptografado é 2mn bits, onde m e n são ambos inteiros. Primeiro, o texto normal de 2mn bits é dividido em dois pedaços de dados de entrada de mn-bits P_L (Plain-Left-Normal Esquerdo) 101 e P_R (Plain-Right-Normal Direito) 102 e os dados de entrada P_L (Plain-Left-Normal Esquerdo) 101 e P_R (Plain-Right-Normal Direito) 102 são proporcionados como valores de entrada.

A estrutura de Feistel é representada usando a repetição da unidade básica de processamento, que é referida como uma função de arredondamento e uma função de transformação de dados incluída em cada arredondamento é referida como uma função-F 120. Na configuração mostrada na figura 1, um exemplo de uma configuração em que a função-F (função de arredondamento) 120 é repetida em r estágios é mostrado.

Por exemplo, no primeiro arredondamento, dados de entrada X de Mn-bits e chave de arredondamento K_1 de mn-bits 103, que é introduzida de uma seção de geração de chaves (não ilustrada) são introduzidos na função-F 120 e, após um processo de transformação de dados ser realizado na função-F 120, dados Y de mn-bits saem. Uma operação OR exclusivo é realizada em uma seção OR- exclusivo 104, usando os dados Y de saída e os outros dados de entrada que são introduzidos do estágio anterior (em um caso do primeiro estágio, dados de entrada p_L) e um resultado de operação de mn-bits é enviado para a função de arredondamento seguinte. Esse processo, isto é, um processo de criptografia em que a função-F é aplicada de modo a ser repetida apenas nos tempos correspondentes a um número determinado de arredondamentos (r), é completado e pedaços dos dados C_L (Cipher Left-Cifra Esquerda) divididos e C_R (Cipher Right-Cifra Direita), que são textos cifrados, saem. Com a configuração descrita acima, como um processo de descriptografia na estrutura de Feistel, é necessário apenas inverter a ordem de inserção de chaves de arredondamento e é concluído que não é necessário

configurar funções inversas.

Uma configuração da função-F 120, que é ajustada como uma função em cada arredondamento, é descrita com referência à figura 2. A Parte (a) da figura 2 é um diagrama mostrando entradas e uma saída da função-F 120 em um arredondamento e a parte (b) da figura 2 é um diagrama mostrando a configuração detalhada da função-F 120. Conforme mostrado na parte (b) da figura 2, a função-F 120 tem uma chamada configuração do tipo SP, em que uma camada de transformação não linear (uma camada de s) e uma camada de transformação linear (uma camada de P) são conectadas uma à outra.

A função-F 120, mostrada na figura 2 é uma função tendo uma configuração em que o comprimento dos bits de entrada/saída é m x n bits (m, n: inteiros). Na função-F do tipo SP, primeiro, OR exclusivo é realizado usando dados K_1 e dados X_1 de chave. A seguir, a camada de transformação não linear (a camada de S) é aplicada e, então, a camada de transformação linear (a camada de P) é aplicada.

Especificamente, a camada de transformação não linear (a camada de S) é uma camada em que m tabelas de transformação não linear com entradas de n-bits e saídas de n-bits, que são referidas como caixas-S 121, são dispostas e dados de mn-bits são divididos em pedaços de n-bits. Os pedaços de n-bits são introduzidos nas caixas-S 121 correspondentes e os dados são transformados. Em cada uma das caixas-S 121, um processo de transformação não linear, por exemplo, em que uma tabela de transformação é aplicada, é realizado.

A camada de transformação não linear (a camada de P) é configurada usando uma seção de transformação linear. A seção de transformação linear 122 toma um valor Z de saída de mn-bits, que é uma saída de dados das caixas-S 121, como uma entrada, e realiza transformação linear para a entrada a fim de sair um resultado de mn-bits. A seção de

transformação linear 122 realiza um processo de transformação linear, tal como um processo de permutação de posições de bits de entrada e saídas de um valor Y de saída de Mn-bits e dados de entrada que são proporcionados do estágio anterior e o resultado de OR exclusivo é proporcionado como um valor de entrada para uma função-F do arredondamento seguinte

Note que, em uma configuração de uma modalidade descrita acima, a transformação linear realizada na seção de transformação linear 122 servindo como a camada de transformação linear (a camada de P) é definida como transformação linear, que é realizada de modo que uma matriz de mn x mn definida em relação a GF(2) é aplicada e que, além disso, uma matriz incluída no i-ésimo arredondamento é referida como M_1. Note que é suposto que ambas as caixas-S, que servem como seções de transformação não linear e transformação linear na configuração na configuração descrita na presente invenção são objetivas

2. 2. Função de Operação de Número de Derivações e função de Avaliação de Resistência

A seguir, uma função de operação do número de elementos de vedação e uma função de avaliação de resistência, que são necessárias para compreender a presente invenção, serão descritas.

2-1. Função de Operação de Número de Derivações: Derivação ()

Uma função de operação do número de derivações: Derivação () para transformação de difusão ótima (Mapeamentos de Difusão Ótima), que é proporcionada como um exemplo de transformação linear que é realizada na seção de transformação linear 122, servindo como a camada de transformação linear (a camada de P) incluída na função-F descrita acima, é definida como segue:

Um mapeamento descrevendo a transformação linear de dados de nxa-bits para dados de nxb-bits é representado como segue:

$$\theta: \{0, 1\}na \rightarrow \{0, 1\}nb$$

O número de derivações: Derivação(θ) é definido para o mapeamento como segue:

$$Branchn(\theta) = min\alpha \neq 0\{hwn(\alpha) + hwn(\theta(\alpha))\}$$

Note que $min\alpha \neq 0\{X\alpha\}$ representa o valor mínimo entre todos $X\alpha$ satisfazendo $\alpha \neq 0$, e que hwn(Y) representa uma função de retorno do número de elementos (não zero) em que todos os n pedaços de bits de dados não são zero quando uma coluna Y de bits é delimitada e representada em unidades de n bits.

Note que, nesse caso, um mapeamento 9 que é proporcionado de modo que Branchn(θ) é b + 1 é definido como uma transformação de difusão ótima.

2-2. Índice de Avaliação de Resistência aos Ataques Diferenciais

Um processo criptográfico de chave comum em que uma estrutura de Feistel é aplicada tem um problema de vazamento de chaves devido à criptanálise. A análise diferencial (também chamada criptanálise diferencial ou ataque diferencial), em que chaves aplicadas em respectivas funções de arredondamento são analisadas pela análise de múltiplos pedaços de dados de entrada (texto normal) tendo uma certa diferença (ΔX) e pedaços de dados de saída (texto cifrado) para os dados de entrada e análise linear (também chamada criptanálise linear ou ataque linear), em que a análise baseada em texto normal e texto cifrado correspondente é realizada, têm sido conhecidas como técnicas típicas de criptanálise ou técnicas de ataque.

O número mínimo de caixas-S ativas diferenciais, incluídas em um curso diferencial que representa relações de conexão de diferenças pode ser aplicado como um índice para a avaliação da resistência aos ataques diferenciais.

Um curso diferencial é um curso em que valores diferenciais

específicos são designados para todos os pedaços de dados, excluindo pedaços de dados chave em funções de criptografia. Os valores diferenciais não são determinados arbitrariamente e os valores diferenciais obtidos antes/após processo de transformação estão relacionados um com o outro. Antes/após os processos de transformação linear, as relações entre diferenças de entrada e diferenças de saída são determinadas como relações de um para um, um conceito de probabilidades é introduzido. É suposto que as probabilidades para uma diferença de entrada e uma diferença de saída podem ser calculadas antecipadamente. A soma de todas as probabilidades para todas as saídas é um.Em uma estrutura de Feistel tendo funções-F do tipo SP, transformação não linear é realizada apenas em uma porção dos processos usando caixas-S.

Em conseqüência, neste caso, um curso diferencial tendo uma outra probabilidade que não zero representa um conjunto de pedaços de dados diferenciais que são proporcionados como valores diferenciais começando com um valor diferencial para texto normal (entrada) e terminando com um valor diferencial para texto cifrado (saída) e valores diferenciais que são proporcionados antes/após todas as caixas-S são valores diferenciais tendo outras probabilidades que não zero. Uma caixa-S, que é incluída em um curso diferencial tendo uma outra probabilidade que não zero e na qual um valor diferencial que não é zero é introduzido é referida como uma "caixa-S ativa diferencial". O número mínino entre os números de caixas-S ativas em todos os cursos diferenciais tendo outras probabilidades que não zero é referido como com "número mínimo de caixas-S ativas diferenciais" e o valor desse número é conhecido como um índice de segurança para ataques diferenciais. Note que não há ponto no ataque de um curso diferencial em que todos os valores diferenciais sejam zero porque a probabilidade do curso se torna um. Desse modo, o curso não será considerado baixo.

Em uma modalidade da presente invenção, uma configuração é

proporcionada, em que o número mínimo de caixas-S ativas diferenciais é assegurado como sendo grande, assim, acentuando a segurança para ataques diferenciais.

2-3. Índice de Avaliação de Resistência aos Ataques Lineares

Além disso, um número mínimo de caixas-S ativas lineares incluídas em um curso linear que representa relações de conexão de máscaras lineares (embora seja referido como uma "aproximação linear" na maioria dos casos, aqui, uma palavra “curso” é usada a fim de corresponder à diferença) podem ser aplicadas como um índice para a avaliação da resistência aos ataques lineares.

Um curso linear é um curso em que valores de máscaras lineares específicas são designados para todos os pedaços de dados, excluindo pedaços de dados de chave em funções de criptografia. Os valores de máscaras lineares não são determinados arbitrariamente e os valores lineares obtidos antes/após os processos de transformação estão relacionados um com outro. Antes/após processos de transformação linear, as relações entre valores de máscaras lineares de entrada e valores de máscaras lineares de saída são determinadas como relações de um para um. Embora, antes/após transformação não linear, as relações entre valores de máscaras lineares de entrada e valores de máscaras lineares de saída não sejam determinadas como relações de um para um, um conceito de probabilidades é introduzido. Um conjunto de um mais valores de máscaras lineares que pode ser dado como saída existe para um valor de máscara linear de entrada e probabilidades de que os respectivos valores de máscaras lineares sejam proporcionados como saída podem ser calculadas antecipadamente. A soma de todas as probabilidades para todas as saídas é um.

Em uma estrutura de Feistel tendo funções-F do tipo SP, transformação não linear é realizada apenas em uma porção dos processos usando caixas-S. Em conseqüência, neste caso, um curso linear tendo uma

outra probabilidade que não zero representa um conjunto de pedaços de dados de valores de máscaras de lineares que são proporcionados como valores lineares, começando com um valor linear para texto normal (entrada) e terminando com um valor linear para texto cifrado (saída) e valores lineares que são proporcionados antes/após todas as caixas-S são valores lineares tendo outras probabilidades que não zero. Uma caixa-S, que está incluída dentro de um curso linear tendo uma outra probabilidade que não zero e na qual um valor linear que não é zero é introduzido é referida como uma "Caixa-S ativa linear". O número mínimo entre os números de caixas-S ativas em todos os cursos lineares tendo outras probabilidades que não zero é referido como um "Número mínimo de caixas-S ativas lineares" e o valor desse número é conhecido como um índice de segurança para ataques lineares. Note que não há ponto no ataque de um curso de linear em que todos os valores de máscaras lineares sejam zero por causa da probabilidade do curso se tornar um. Desse modo, o curso não será considerado baixo.

Em uma modalidade da presente invenção, uma configuração é proporcionada em que o número mínimo de caixas-S ativas lineares é assegurado ser grande, assim, acentuando a segurança para ataques lineares.

3. Método para

Em uma modalidade da presente invenção, uma configuração é proporcionada, em que o número mínimo de caixas-S ativas e lineares é assegurado como sendo o grande e, assim, acentuando a segurança para ataques lineares.

3. Método para Ajustar DSM para a Estrutura de Feistel Tendo Duas Linhas de Dados

Como descrito previamente, uma configuração em que o mecanismo de comutação de matriz de difusão (DSM: Diffusion Switching Mechanism – Mecanismo de Comutação de Difusão), daqui em diante referido como "DSM") é aplicado tem sido proposta como uma configuração

para acentuar a resistência aos ataques diferenciais ou ataques lineares descritos acima em que uma estrutura de Feistel é aplicada. O DSM tem uma configuração em que duas ou mais matrizes diferentes são dispostas em seções de transformação linear de função de arredondamento (função-F) em uma estrutura de Feistel. Com o DSM, o número mínimo de caixas-S ativas lineares pode ser assegurado como sendo grande, pelo que a resistência aos ataques diferenciais ou ataques lineares pode ser acentuada.

Um esboço do DSM será descrito. Quando o mecanismo de comutação de matriz de difusão (DSM) é aplicado em uma estrutura de Feistel, uma pluralidade de matrizes diferentes são proporcionadas como matrizes que são aplicadas em seções de transformação linear (camadas de P) de seções de função de arredondamento (função-F), constituindo a estrutura de Feistel. Por exemplo, todas as matrizes aplicadas nos respectivos arredondamento na estrutura de Feistel, tendo r arredondamentos, conforme mostrado na figura 1, não são ajustadas como as mesmas matrizes de transformação linear e pelo menos dois ou mais tipos de matrizes são dispostos de acordo com uma regra específica.

Por exemplo, a figura 3 mostra um exemplo de uma estrutura de Feistel em que o mecanismo de comutação de matriz de difusão (DSM) é realizado usando duas matrizes de transformação linear M_0 e M_1 e a figura 4 mostra um exemplo de uma estrutura de Feistel em que o mecanismo de comutação de matriz de difusão (DSM) é realizado usando três matrizes de transformação linear M_0, M_1 e M_2.

No exemplo da estrutura de Feistel mostrado na figura 3, as duas matrizes de transformação linear M_0 e M_1 são configuradas como matrizes diferentes. Adicionalmente, no exemplo da estrutura de Feistel mostrado na figura 4, as três matrizes de transformação linear M_0, M_1 e M_2 são configuradas como matrizes diferentes.

A fim de realizar o mecanismo de comutação de matriz de

difusão (DSM), é necessário que as matrizes aplicadas satisfaçam condições predeterminadas. Uma das condições é uma restrição referente ao número de derivações (Branch) descritos acima. Essa restrição será descrita abaixo.

Com relação ao número de derivações em cada uma da pluralidade de matrizes diferentes M_0 a M_n aplicadas à transformação limiar realizada em seções de função de arredondamento de uma estrutura de Feistel, o número mínimo de derivações em uma matriz aplicada: B_1^D e os números mínimos de derivações correspondentes às matrizes de incidência de uma pluralidade de matrizes aplicadas: B_2^D, B_3^D e B_2^L são definidos como segue:

[Equação 1]

$$B_1^D = \min_i(Branch_n(M_i))$$

$$B_2^D = \min_i(Branch_n([M_i \mid M_{i+2}]))$$

$$B_3^D = \min_i(Branch_n([M_i \mid M_{i+2} \mid M_{i+4}]))$$

$$B_2^L = \min_i(Branch_n([{}^tM_i^{-1} \mid {}^tM_{i+2}^{-1}]))$$

Nas equações:

Mi denota uma matriz de transformação linear aplicada a um processo de transformação linear no i-ésimo arredondamento na estrutura de Feistel,

$[M_i|M_i+2|-]$ denota uma matriz de incidência obtida pela concatenação de respectivas matrizes $M_i|M_{i+2}|$-,

tM denota uma matriz transposta de uma matriz M e

M^{-1} denota uma matriz inversa da matriz M.

Nas equações descritas acima, especificamente: B_2^D, B_3^D e B_2^L denotam os valores mínimos dos números de derivações em matrizes obtidas pela conexão de matrizes incluídas em funções-F em dois ou três arredondamentos que são proporcionados consecutivamente na estrutura de Feistel.

Por exemplo, é conhecido que as respectivas matrizes são

ajustadas de modo que os respectivos números de derivações descritos acima satisfaçam as seguintes condições, isto é,

$$B_2^D > 3, B_3^D > 3 \text{ e } B_2^L > 3,$$

pelo que a resistência aos ataques diferenciais ou ataques lineares pode ser acentuada na estrutura de Feistel.

Note que os respectivos subscritos e sobrescritos de B_1^D, B_2^D, B_3^D, e B_2^L têm os seguintes significados;

Isto é, n de B_n^D denota o número de matrizes que são conectadas uma à outra, D de B_n^D denota uma condição para ter resistência aos ataques diferenciais e L de B_n^L denota uma condição para ter resistência aos ataques lineares.

4. Ajuste de DSM em Estrutura de Feistel estendida

Na presente invenção, uma configuração é proposta em que o mecanismo de comutação de matriz de difusão (DSM) é realizado em uma estrutura de Feistel tendo qualquer número de linhas de dados que sejam duas ou mais linhas de dados, por exemplo, três linhas ou quatro linhas, em lugar de na estrutura de Feistel tendo duas linhas de dados. A configuração será descrita abaixo em detalhes.

Uma estrutura de Feistel a ser descrita na presente invenção é uma estrutura de Feistel estendida em que o número de divisões que é o número de linhas de dados é denotado por d para generalização, embora seja o mesmo que a estrutura de Feistel descrita acima, tendo duas linhas de dados em que funções-F do tipo SP são usadas, onde d é um inteiro que é igual ou maior do que dois.

Embora a configuração em que o mecanismo de comutação de matriz de difusão (DSM) é aplicado à estrutura de Feistel no caso limitado em que o número de linhas de dados = 2 tem sido proposto como descrito acima, um método não é conhecido em que a resistência seja acentuada através da aplicação do DSM a uma estrutura de Feistel estendida, tendo o número de

linhas de dados d que é ajustado para qualquer número d que satisfaça $d \geq 2$. Na presente invenção, uma configuração é realizada em que a resistência aos ataques diferenciais ou ataques lineares é acentuada pela aplicação do mecanismo de comutação de matriz de difusão (DSM) a uma estrutura de Feistel estendida tendo número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$.

Exemplos específicos de configurações e processos da presente invenção serão descritos abaixo.

4-1. Referência à Estrutura de Feistel estendida

Definições de estrutura de Feistel estendida serão descritas com referência à figura 5. No relatório descritivo, uma estrutura de Feistel estendida é definida como segue:

1. Tem d (d é igual ou maior do que dois) linhas de dados e o tamanho de cada uma das linhas de dados é mn bits.

2. O tamanho de entrada/saída de uma função-F é mn bits

3. Tem arredondamentos que são referidos como unidades de processamento. Uma linha de dados ou uma pluralidade de linhas de dados são submetidas a um processo de transformação usando uma função-F em um arredondamento. O resultado é submetido a OR-exclusivo usando outra linha de dados. Contudo, quando duas ou mais funções-F são incluídas em um arredondamento, linhas de dados duplicadas não existem como linhas de dados que servem como entradas/saídas de todos as funções-F.

Um exemplo da estrutura de Feistel estendida que é construída de acordo com as definições descritas acima será descrito com referência à figura 5.

A definição 1 mencionada acima:

Tem d (d é igual ou maior do que dois) linhas de dados e o tamanho de cada uma das linhas de dados é mn bits.

A definição é descrita com referência á figura 5; A definição

significa que, na figura 5, o tamanho da entrada /saída de cada linha de dados, isto é, de cada uma das linhas de dados 1 a d é de mn bits e o número total de bits para uma entrada/saída é dmn bits.

A definição 2 descrita acima:

O tamanho de entrada/saída de uma função-F é mn bits

A definição é descrita com referência à figura 5; Por exemplo, mn bits que são a saída como um resultado de operação de uma seção de operação de OR-exclusivo (XOR) 201, servindo como um estágio superior, são introduzidos em uma função-F 202 via uma linha de dados 2. Além disso, uma chave de arredondamento K é introduzida e um processo de operação é realizado. Esse processo de operação é o processo que foi descrito com referência à parte (b) da figura 2 e inclui transformação não linear realizada nas caixas-S e um processo de transformação linear, em que a matrizes de transformação linear Mi é aplicada, que é realizado na seção de transformação linear. A saída da função-F 202 é Mn bits e é introduzida em uma seção de operação OR-exclusivo (XOR) 203 de uma linha de dados 4.

A definição 3 descrita acima:

Tem arredondamentos que são referidos como unidades de processamento. Uma linha de dados ou uma pluralidade de linhas de dados são submetidas a um processo de transformação usando uma função-F em um arredondamento. O resultado é submetido a OR-exclusivo usando outra linha de dados. Contudo, quando duas ou mais funções-F são incluídas em um arredondamento, linhas de dados duplicadas não existem como linhas de dados que servem como entradas/saídas de todos as funções-F.

A definição é descrita com referência à figura 5. A figura 5 mostra uma estrutura de Feistel estendida tendo uma configuração de r-arredondamentos. Uma ou mais funções-F são incluídas em cada arredondamento e o resultado é submetido a OR-exclusivo, usando outra linha de dados. Com referência a um arredondamento n mostrado na figura 5, uma

pluralidade de funções-F são incluídas em um arredondamento e são uma função-F 211 e uma função-F 212 mostrada na figura 5.

Como descrito acima, quando uma pluralidade de funções-F são incluídas em um arredondamento, linhas de entrada/saída das respectivas funções-F são linhas de dados diferentes uma da outra e são ajustadas de modo que as linhas de dados duplicadas não sejam aplicadas como as linhas de dados de entrada/saída.

Uma linha de dados de entrada da função-F 211, mostrada na figura 5 é uma linha de dados 1 e uma linha de dados de saída da função-F 211 é uma linha de dados 2.

Uma linha de dados de entrada da função-F 212 é qualquer uma das linhas de dados 5 ou mais e uma linha de dados de saída da função-F 212 é uma linha de dados 3.

As linhas de dados de entrada/saída são ajustadas de modo a não serem duplicadas.

Note que, conforme mostrado na figura 5, no relatório descritivo, uma função-F é denotada por [F] e uma chave de arredondamento é denotada por [K]. Subscritos e sobrescritos que são ajustados para os respectivos identificadores F e K têm os seguintes significados:

Isto é, i de F_i^n ou K_i^n denota um arredondamento e n denota um número de identificação de uma função-F ou uma chave de arredondamento no mesmo arredondamento.

Note que uma matriz de transformação linear que é aplicada em uma seção de transformação linear de uma função-F em cada arredondamento é denotada por [M] na descrição dada abaixo, embora não esteja ilustrada. Como no caso descrito acima, um subscrito e um sobrescrito que devem ser ajustados para M ter os seguintes significados.

Isto é, i de M_i^n denota um arredondamento e n denota um número de identificação de uma matriz de transformação linear para uma

correspondente de uma pluralidade de funções-F que são estabelecidas no mesmo arredondamento.

A figura 6 mostra um exemplo de uma estrutura de Feistel estendida que satisfaz as definições descritas acima e que tem sete linhas de dados (d = 7). Note que, na figura 6, embora símbolos de seções de operação de OR-exclusivo para saídas de respectivas funções-F e respectivas linhas de dados são omitidas, a estrutura de Feistel estendida tem uma configuração em que as operações de OR-exclusivo (XOR), usando entradas correspondentes são realizadas em respectivos pontos de interseção das saídas das respectivas funções-F e das respectivas linhas de dados e em que os resultados das operações de OR-exclusivo (XOR) saem em uma direção para baixo das mesmas linhas de dados. No exemplo mostrado na figura 6, um arredondamento i+4, um arredondamento i+5, um arredondamento i+9 e um arredondamento i+10 são arredondamentos que são proporcionados de tal maneira que duas ou mais funções-F são incluídas em um arredondamento. Com relação às funções-F [F] e às chaves de arredondamento [K] proporcionadas nesses arredondamentos, números denotando números de identificação das funções-F ou das chaves de arredondamento nos mesmos arredondamentos são proporcionados nos cantos de topo direitos.

Quando uma estrutura de Feistel, tendo o número de linhas d que é estabelecido como d = 2, é construída de acordo com as definições descritas acima de 1 a 3, ela é proporcionada como uma estrutura de Feistel tendo duas linhas de dados, isto é, a estrutura de Feistel que foi previamente descrita com referência à figura 1. Em outras palavras, uma estrutura de conexão em que funções-F são introduzidas alternadamente em duas respectivas linhas é proporcionada. Contudo, em um caso de uma estrutura de Feistel estendida tendo três ou mais linhas de dados, uma estrutura de conexão não é determinada unicamente, uma vez que uma pluralidade de linhas de dados que podem ser selecionadas como entradas e saídas de

funções-F existem. Em outras palavras, quanto maior é d em uma estrutura de Feistel estendida, maior é o número de locais em que as funções-F podem ser estabelecidas. A flexibilidade com que as funções-F podem ser estabelecidas é aumentada exponencialmente.

Na presente invenção, uma configuração é proposta em que o mecanismo de comutação de matriz de difusão (DSM: Diffusion Switching Mechanism – Mecanismo de Comutação de Difusão) que acentua a resistência aos ataques diferenciais ou ataques lineares é realizado nessa estrutura de Feistel estendida.

Em uma estrutura de Feistel em que o número de linhas d é estabelecido como d = 2, por exemplo, conforme mostrado na figura 3 ou na figura 4, duas matrizes diferentes de transformação linear M_0 e M_1, ou três matrizes diferentes de transformação linear M_0, M_1 e M_2 são proporcionadas como matrizes aplicadas em seções de transformação linear (camadas de P) de seções de função de arredondamento (função-F), constituindo uma estrutura de Feistel, pelo que o DSM é realizado. Contudo, a fim de realizar o DSM, é necessário que matrizes aplicadas satisfaçam condições predeterminadas. Uma das condições é uma restrição referente ao número de derivações (Branch) descrito acima.

Em uma estrutura de Feistel estendida tendo o número de linhas de dados d que é estabelecido como

d: qualquer inteiro que satisfaça $d \geq 2$,

antes, uma descrição de uma configuração para realização do DSM, definições de respectivas seções constituintes de uma estrutura de Feistel estendida, usada na descrição dada abaixo, serão descritas com referência à figura 7.

A figura 7 é um diagrama em que apenas uma linha de dados é extraída e mostrada dentre linhas de dados que constituem uma estrutura de Feistel estendida, por exemplo, conforme mostrado na figura 6. Conforme

mostrado na figura 7, pode ser compreendido que dados que são introduzidos em uma linha de dados são submetidos a OR-exclusivo (XOR), usando uma ou mais saídas de funções-F que, então, eles saem. Isso é aplicado a qualquer linha de dados incluída na estrutura de Feistel estendida.

Na figura 7, um estado é mostrado em que saídas de uma pluralidade de funções-F [$F_{s(i),\ 1}$, $F_{s(i),\ 2}$, ...] são adicionadas, usando operações de OR-exclusivo (XOR) para uma linha de dados [s(i)].

Note que cada uma das linhas de dados incluídas na estrutura de Feistel estendida é referida como S(i) ($1 \leq i \leq d$). As funções-F que são introduzidas na linha de dados S(i) são referidas como $F_{s(i),\ 1}$, $F_{s(i),\ 2}$, ... na ordem em que elas são introduzidas na linha de dados S(i) das anteriores.

Adicionalmente, os dados de entrada que são introduzidos na linha de dados s(i) são denotados por $W_{s(i),\ 0}$.

Os dados obtidos após uma saída de uma função-F $F_{s(i),\ j}$ são submetidos ao OR-exclusivo por $W_{s(i),\ j}$.

Além disso, os dados de entrada que são introduzidos na função-F $F_{s(i),\ j}$ são denotados por $X_{s(i),\ j}$.

Embora cada $X_{s(i),\ j}$ sejam dados que pertencem a outra linha que não a linha de dados s(i), aqui, é suposto que a linha à qual cada $X_{s(i),\ j}$ pertence não importa.

Nesse caso, pode ser considerado que a estrutura de Feistel estendida tem uma configuração em que as d linhas de dados são conectadas uma à outra.

Uma configuração para a realização do DSM em uma estrutura de Feistel estendida, isto é, daqui em diante, uma configuração para realizar o DSM em uma estrutura de Feistel estendida tendo o d seguinte, será descrita abaixo. d: qualquer inteiro que satisfaça $d \geq 2$.

A descrição é feita na ordem dos cabeçalhos de seções como segue:

(4-2. Configuração para Acentuar a Resistência aos Ataques Diferenciais em Estrutura de Feistel estendida)

(4-3. Configuração para Acentuar a Resistência aos Ataques Lineares em Estrutura de Feistel estendida)

As respectivas configurações serão descritas seqüencialmente.

(4-2. Configuração para Acentuar a Resistência aos Ataques Diferenciais em Estrutura de Feistel estendida)

Primeiro, uma configuração para acentuar a resistência aos ataques diferenciais em uma estrutura de Feistel estendida será descrita.

Como descrito acima, ataques diferenciais são ataques em que chaves aplicadas em respectivas funções de arredondamento são analisadas através de análise de múltiplos pedaços de dados de entrada (texto normal), tendo uma certa diferença (ΔX) e pedaços de dados de saída (texto cifrado) para os dados de entrada. O número mínimo de caixas-S ativas diferenciais incluídas em um curso diferencial que representa as relações de conexão de diferenças pode ser aplicado como um índice para avaliar a resistência aos ataques diferenciais.

Um curso diferencial inclui valores diferenciais em pedaços de dados, excluindo pedaços de dados de chave em funções de criptografia. Antes/após os processos de transformação linear, as relações entre as diferenças de entrada e as diferenças de saída são determinadas como relações de uma para uma. Embora antes/após processos de transformação não linear, as relações entre diferenças de entrada e diferenças de saída não são determinadas como relações de uma para uma, as probabilidade de ocorrência de diferenças de saída para uma diferença de entrada são calculadas. A soma de todas as probabilidades para todas as saídas é um.

Em uma estrutura de Feistel tendo funções-F do tipo SP, transformação não linear é realizada usando apenas caixas-S. Nesse caso, um curso diferencial, tendo uma outra probabilidade que não zero representa um

conjunto de pedaços de dados diferenciais que são proporcionados como valores diferenciais, começando com um valor diferencial para texto normal (entrada) e terminando com um valor diferencial para texto cifrado (saída) e valores diferenciais que são proporcionados antes/após todas as caixas-S terem outras probabilidades que não zero. Uma caixa-S, que é incluída em um curso diferencial tendo uma outra probabilidade que não zero, e na qual um valor diferencial que não é zero é introduzido, é referida como uma "caixa-S ativa diferencial".

O número mínimo entre os números de caixas-S ativas em todos os cursos diferenciais tendo outras probabilidades que não zero é referido como "o número mínimo de caixas-S ativas diferenciais" e o valor desse número é usado como um índice de segurança para ataques diferenciais.

Tornar grande o número mínimo de caixas-S ativas diferenciais leva à acentuação de resistência aos ataques diferenciais. Uma técnica para a construção de uma estrutura de DSM para tornar grande o número mínimo de caixas-S ativas diferenciais em uma estrutura de Feistel estendida, tendo número de linhas de dados d que é estabelecido para qualquer inteiro que satisfaça $d \geq 2$ será descrita baixo.

Uma matriz de transformação linear usada em uma função-F $[F_{s(i),\ x}]$ incluída em uma estrutura de Feistel estendida é denotada por $[M_{s(i),\ x}]$. Nesse caso, uma equação $B_2^D(s(i))$ para calcular o número de derivações, em que a função de operação do número de derivações: Branch() é aplicada, é definida como segue;

[Equação 2]

$$B_2^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1}]))$$

A equação mencionada acima é uma equação para calcular o valor mínimo do número de derivações em uma matriz de incidência $[M_{s(i),\ j}|M_{s(i),\ j+1}]$ de duas matrizes de transformação linear $[M_{s(i),\ j},\ M_{s(i),\ j+1}]$ que são usadas em duas funções-F $[F_{s(i),\ j},\ F_{s(i),\ j+1}]$ que ficam adjacentes uma à outra e

que são introduzidas em qualquer linha de dados s(i), constituindo a estrutura de Feistel estendida.

Em qualquer linha de dados s(i), constituindo a estrutura de Feistel estendida, [j] que corresponde ao número de funções-F, que são introduzidas na linha de dados s(i), do estágio de topo, é ajustada para qualquer j e dados $[W_{s(i),\ j}]$ na linha de dados s(i) serão considerados.

Os dados de entrada/saída $[W_{s(i),\ j}]$ e $[W_{s(i),\ j+2}]$ intercalam porções de entrada das duas funções-F $[F_{s(i),\ j+1}]$ e $[F_{s(i),\ j+2}]$, que são introduzidas na linha de dados s(i) para a linha de dados s(i). Com referência aos dados de entrada/saída $[W_{s(i),\ j}]$ e $[W_{s(i),\ j+2}]$ na linha de dados s(i), o seguinte caso é considerado:

$$Ws(i), j = 0$$

$$Ws(i), j+2 = 0$$

Nesse caso, entre os respectivos valores diferenciais de entrada $[AX_{s(i),\ j+1}]$ e $[AX_{s(i),\ j+2}]$ para as funções-F $[F_{s(i),\ j+1}]$ e $[F_{s(i),\ j+2}]$ adjacentes uma à outra dentre as funções-F, que são introduzidas na linha de dados s(i), a seguinte relação se mantém:

[Equação 3]

$$hw_n(\Delta X_{s(i),j+1}) + hw_n(\Delta X_{s(i),j+2}) \geq B_2^D(s(i))$$

Note que, na relação mencionada acima, hw denota peso e o lado esquerdo da relação mencionada acima representa o número de elementos não zero em dados diferenciais de entrada das funções-F, isto é, a soma dos números de caixas-S ativas. Assegurar que esse número seja um grande valor é uma condição em que a acentuação da resistência aos ataques diferenciais pode ser esperada. Em conseqüência, se outras condições que não a condição são as mesmas, é concluído que é preferível que matrizes nas respectivas funções-F, constituindo a estrutura de Feistel estendida sejam selecionadas de modo a tornarem $B_2^D(s(i))$ tão grande quanto possível.

Em criptografia do tipo Feistel Estendido na técnica anterior, uma configuração em que uma matriz de transformação linear é utilizada em seções de transformação linear em todas as funções-F é uma configuração geral.

Contudo, quando as duas matrizes de transformação linear $[M_{s(i),\ j}]$ e $[M_{s(i),\ j+1}]$ que são usadas nas duas funções-F $[F_{s(i),\ j},\ F_{s(i),\ j+1}]$ adjacentes uma à outra, que são introduzidas na linha de dados s(i), são as mesmas matrizes, a equação descrita acima para calcular o número de derivações: Branch () é aplicada, isto é, $B_2^D(s(i))$, se torna dois, que é o valor mínimo. Desse modo, um efeito B_2^D de acentuação de resistência não pode ser esperado.

Adicionalmente, mesmo em um caso em que matrizes diferentes são usadas, quando duas matrizes são selecionadas sem cuidados, há um caso em que $B_2^D(s(i))$ se torna dois.

$B_2^D(s(i))$, que é definido pela equação descrita acima para calcular o número de derivações, é feito para ser um número muito maior de derivações, pelo que um número mínimo localizado de caixas-S ativas diferenciais é assegurado ser grande, de modo que a resistência aos ataques diferenciais pode ser acentuada. Em conseqüência, por exemplo, matrizes são selecionadas de modo a tornarem $B_2^D(s(i))$ igual ou maior do que três, pelo que a resistência aos ataques diferenciais podem ser acentuados.

$B_2^D(s(i))$ é calculado para cada uma das linhas de dados na estrutura de Feistel estendida. O valor mínimo dentre os valores calculados é denotado por B_2^D. Um método para selecionar matrizes nas funções-F de modo a tornar B_2^D igual ou maior do que três será descrito.

(4-2-1. Configuração para Selecionar Matrizes, que devem ser Ajustadas em Funções-F, que Fazem o Valor do Número Mínimo de Derivações B_2^D Igual ou Maior do que Três)

Primeiro, será descrito abaixo que tornar o número mínimo de

derivações $[B_2^D]$, que é o número mínimo entre os números mínimos de derivações $[B_2^D(s(i))]$ calculado para todas as linhas de dados na estrutura de Feistel estendida, igual ou maior do que três pode ser realizado pelo fornecimento de pelo menos dois tipos de matrizes.

Primeiro, duas matrizes diferentes $[A_0]$ e $[A_1]$ são preparadas, as quais tornam o número de derivações em uma matriz de incidência $[A_0|A_1]$ das duas matrizes diferentes $[A_0]$ e $[A_1]$ igual ou maior do que três, isto em que satisfazem como segue:

$$Branch_n([A_0|A_1]) \geq 3$$

A seguir, matrizes de transformação linear das seções de transformação linear da pluralidade de funções-F, que são introduzidas na linha de dados s(i) na estrutura de Feistel estendida, são estabelecidas como segue:

A_0 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da primeira função-F $F_{s(i),\ 1}$.

A_1 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da segunda função-F $F_{s(i),\ 2}$.

A_0 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da terceira função-F $F_{s(i),\ 3}$.

Dessa maneira, as duas matrizes diferentes $[A_0]$ e $[A_1]$ são dispostas alternadamente nessa ordem do topo para a pluralidade de funções-F, que são introduzidas na linha de dados s(i).

Quando as matrizes de transformação linear são estabelecidas dessa maneira, a equação descrita acima para calcular o valor mínimo do número de derivações na matriz de incidência $[M_{s(i),\ j}|M_{s(i),\ j+1}]$ das duas matrizes de transformação linear $[M_{s(i),\ j},\ M_{s(i),\ j+1}]$ que são usadas nas duas funções-F $[F_{s(i),\ j},\ F_{s(i),\ j+1}]$ adjacentes uma à outra, que são introduzidas em qualquer linha de dados s(i) é proporcionada como segue:

[Equação 4]

$$B_2^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1}])) \geq 3$$

Em outras palavras, é assegurado que o número mínimo de derivações é igual ou maior do que três.

Como é óbvio, quando as matrizes $[A_0]$ e $[A_1]$ são permutadas, o mesmo efeito é obtido. Adicionalmente, quando as matrizes são similarmente estabelecidas para cada uma das linhas de dados s(i) na estrutura de Feistel estendida B_2^D pode ser feito igual ou maior do que três, simplesmente pelo uso das duas matrizes.

$$Branch_n([A_0|A_1]) \geq 3$$

Dessa maneira, as duas matrizes diferentes $[A_0]$ e $[A_1]$, que satisfazem a relação dada acima são preparadas e as respectivas matrizes são estabelecidas de modo a serem dispostas alternadamente nas funções-F que são introduzidas nas respectivas linhas de dados s(i) na estrutura de Feistel estendida, pelo que o valor do número mínimo de derivações B_2^L pode ser feito igual ou maior do que três. A acentuação da resistência aos ataques diferenciais pelo uso do mecanismo de comutação de matriz de difusão (DSM) pode ser realizada.

Um exemplo em que as duas matrizes diferentes $[A_0]$ e $[A_1]$ são aplicadas foi descrito acima.

Em seguida, um exemplo será descrito abaixo, em que matrizes diferentes são generalizadas usando qualquer número [k] que seja igual ou maior do que dois.

Uma matriz de transformação linear usada em uma função-F $[F_{s(i),\,j}]$ incluída em uma estrutura de Feistel estendida é denotada por $[M_{s(i),\,j}]$. Nesse caso, uma equação $B_2^D(s(i))$ para o cálculo do número de derivações, em que a função de operação do numero de derivações: Branch () é aplicada, é definido como

[Equação 5]

$$B_k^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1} \mid M_{s(i),j+2} \mid \cdots \mid M_{s(i),j+k-1}]))$$

A equação mencionada acima é uma equação para cálculo do valor mínimo do número de derivações do número de derivações em uma matriz de incidência $[M_{s(i),\ j}|M_{s(i),\ j+1}|\ldots|M_{s(i),\ j+k-1}]$ of k matrizes de transformação linear $[M_{s(i),\ j},\ M_{s(i),\ j+1},\ \ldots,\ M_{s(i),\ j+k-1}]$ que são usadas em k funções-F $[F_{s(i),\ j},\ F_{s(i),\ j+1},\ \ldots,\ F_{s(i),\ j+k-1}]$ que ficam adjacentes uma à outra e que são introduzidas em qualquer linha de dados s(i) constituindo a estrutura de Feistel estendida.

Em qualquer linha de dados s(i) constituindo a estrutura de Feistel estendida, [j] que corresponde ao número de funções-F, que são introduzidas na linha de dados s(i) do estágio superior é ajustado para qualquer j e dados $[W_{s(i)},\ j]$ na linha de dados s(i) serão considerados.

Dados de entrada/saída $[W_{s(i)},\ j]$ e $[W_{s(i)},\ j+k]$ intercalam porções de entrada das funções-F $[F_{s(i),\ j+1}]\ldots\ [F_{s(i),\ j+k}]$, que são introduzidas na linha de dados s(i) para a linha de dados s(i). Com relação aos dados de entrada/saída $[W_{s(i)},\ j]$ e $[W_{s(i)},\ j+k]$ na linha de dados s(i), o seguinte caso é considerado:

$$Ws(i),\ j = 0$$

$$Ws(i),\ j+k = 0$$

Nesse caso, entre os respectivos valores diferenciais de entrada $[AX_{s(i),\ j+1}]\ldots\ [AX_{s(i),\ j+k}]$ para as k funções-F $[F_{s(i),\ j+1}]\ldots\ [F_{s(i),\ j+k}]$ adjacentes uma à outra dentre as funções-F, que são introduzidas na linha de dados s(i), a seguinte relação é obtida:

[Equação 6]

$$\sum_{l=j+1}^{j+k} hw_n(\Delta X_{s(i),l}) \geq B_k^D(s(i))$$

Além disso, na relação mencionada acima,

hw denota peso e o lado esquerdo da relação mencionada

acima representa o número de elementos não zero em dados diferenciais de entrada das funções-F, isto é, a soma dos números de caixas-S ativas. Assegurar que esse número seja um grande valor é uma condição em que a acentuação da resistência aos ataques diferenciais pode ser esperada. Em conseqüência, se outras condições que não a condição são as mesmas, é concluído que é preferível que matrizes nas respectivas funções-F, constituindo a estrutura de Feistel estendida sejam selecionadas de modo a tornarem $B_k^D(s(i))$ tão grande quanto possível.

Contudo, mesmo quando apenas um par das mesmas matrizes existe nas k matrizes de transformação linear $[M_{s(i),\ j}] \ldots [M_{s(i),\ j+k-1}]$ que são usadas nas k funções-F $[F_{s(i),\ j}] \ldots [F_{s(i),\ j+k-1}]$ adjacentes uma à outra, que são introduzidas na linha de dados s(i), a equação descrita acima para calcular o número de derivações, em que a função de operação do número de derivações: Branch () é aplicada, isto é, $B_k^D(s(i))$ se torna dois, que o valor mínimo. Desse modo, um efeito de acentuação de resistência não pode ser esperado.

Adicionalmente, mesmo em um caso em que matrizes diferentes são usadas como as k matrizes de transformação linear $[M_{s(i),\ j}] \ldots [M_{s(i),\ j+k-1}]$, quando matrizes são selecionadas sem cuidados, há um caso em que $B_k^D(s(i))$ se torna dois.

$B_k^D(s(i))$, que é definido pela equação descrita acima para calcular o número de derivações, é feito ser um número muito maior de derivações, pelo que um número mínimo localizado de caixas-S ativas lineares é assegurado ser grande, de modo que a resistência aos ataques diferenciais pode ser acentuada. Em conseqüência, por exemplo, matrizes são selecionadas de modo a tornarem $B_k^D(s(i))$ igual ou maior do que três, pelo que a resistência aos ataques diferenciais pode ser acentuada.

$B_k^D(s(i))$ é calculado para cada uma das linhas de dados na estrutura de Feistel estendida. O valor mínimo dentre os valores calculados é

denotado por B_k^D. Um método para selecionar matrizes nas funções-F de modo a tornar B_k^D igual ou maior do que três será descrito.

4-2-2. Configuração para Selecionar Matrizes, que devem ser Ajustadas em Funções-F, que Fazem o Valor do Número Mínimo de Derivações B_K^D Igual ou Maior do que Três

Será descrito abaixo que tornar o número mínimo de derivações $[B_k^D]$, que é o número mínimo entre os números mínimos de derivações $[B_k^D(s(i))]$ calculados para todas as linhas de dados na Estrutura Feistel estendida igual ou maior do que três pode ser realizado pelo fornecimento de pelo menos k tipos de matrizes.

Primeiro, k matrizes diferentes $[A_0]$, $[A_1]$, $[A_2]$, ...$[A_{k-1}]$ são preparadas, as quais tornam o número de derivações de uma matriz de incidência $[A_0|A_1|...|A_{k-1}]$ das k matrizes diferentes $[A_0]$, $[A_1]$, $[A_2]$, ...$[A_{k-1}]$ igual ou maior do que três, isto é, que satisfazem como segue:

$$Branch_n([A_0|A_1|...|A_{k-1}]) \geq 3$$

Em seguida, matrizes de transformação linear das seções de transformação linear da pluralidade de funções-F, que são introduzidas na linha de dados s(i) na estrutura de Feistel estendida, são estabelecidas como segue:

A_0 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da primeira função-F $F_{s(i),\ 1}$.

A_1 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da segunda função-F $F_{s(i),\ 2}$.

A_2 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da terceira função-F $F_{s(i),\ 3}$.

A_{k-1} é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da k-ésima função-F $F_{s(i),\ k}$.

A_0 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da

k +1 -ésima função-F $F_{s(i),\ k+1}$.

A_1 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da k+2 - ésima função-F $F_{s(i),\ k+2}$.

Dessa maneira as k matrizes diferentes $[A_0]$, $[A_1]$, $[A_2]$, ...$[A_{k-1}]$ são dispostas repetidamente nessa ordem desde cima para a pluralidade de funções-F, que são introduzidas na linha de dados s(i).

Quando as matrizes de transformação linear $[A_0]$, $[A_1]$, $[A_2]$, ...$[A_{k-1}]$ são ajustadas dessa maneira, a equação descrita acima para calcular o valor mínimo do número de derivações na matriz de incidência $[M_{s(i),\ j}|M_{s(i),\ j+1}|...M_{s(i),\ j+k-1}]$ das k matrizes de transformação linear $[M_{s(i),\ j}, M_{s(i),\ j+1}, ...M_{s(i),\ j+k-1}]$ que são usadas nas k funções-F $[F_{s(i),\ j}, F_{s(i),\ j+1}...F_{s(i),\ j+k-1}]$ adjacentes uma à outra, que são introduzidas em qualquer linha de dados s(i), é proporcionada como segue:

[Equação 7]

$$B_k^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1} \mid M_{s(i),j+2} \mid \cdots \mid M_{s(i),j+k-1}])) \geq 3$$

Em outras palavras, é assegurado que o número mínimo de derivações é igual ou maior do que três.

Como é óbvio, quando as matrizes $[A_0]$, $[A_1]$,

$[A_2]$,...$[A_{k-1}]$ são permutadas, o mesmo efeito é obtido. Adicionalmente, quando as matrizes são similarmente ajustadas para cada uma das linhas de dados s(i) na estrutura de Feistel estendida, B_2^D pode ser feito igual ou maior do que três, simplesmente pelo uso de k matrizes.

Branchn([A0|A1|...|Ak-1]) ≥ 3

Dessa maneira, as KSs (chave) matrizes diferentes, $[A_0]$, $[A_1]$,

$[A_2]$,...$[A_{k-1}]$ satisfazendo a relação dada acima são preparadas e as respectivas matrizes são ajustadas de modo a serem dispostas repetidamente em uma ordem nas funções-F que são introduzidas nas respectivas linhas de dados s(i) na estrutura de Feistel estendida, pelo que o valor do número mínimo de derivações B_k^D podem ser iguais ou maior do que

três. A acentuação da resistência aos ataques diferenciais pelo uso de mecanismo de comutação de matriz de difusão (DSM) pode ser realizado.

Note que, com relação à seleção de um valor de K, quando k é pelo menos igual ou maior do que dois, um efeito pode ser esperado. Quanto maior é o k, maior é a faixa garantida. Desse modo, a acentuação de resistência pode ser mais esperada. Contudo, em contraste, como o número mínimo de tipos de matrizes necessárias é aumentado, há uma probabilidade de que esse k não seja adequado para uma implementação eficiente. Desse modo, o valor de k é um valor que será selecionado de acordo com uma situação em um estágio de desenho.

4-3. Configuração para Acentuar a Resistência aos Ataques Lineares em Estrutura de Feistel estendida.

A seguir, uma configuração para acentuar a resistência aos ataques lineares em uma estrutura de Feistel estendida será descrita.

Como previamente descrito, o número mínimo de caixas-S ativas lineares incluídas em um curso linear que representa relações de conexão de máscaras lineares (embora seja referido como uma "aproximação linear", na maioria dos casos, aqui, uma palavra "curso" é usada a fim de corresponder à diferença) pode ser aplicado como um índice para avaliar a resistência aos ataques lineares. Um curso linear é um curso em que valores específicos de máscaras lineares são designados para todos os pedaços de dados, excluindo de dados de chave em funções de criptografia. Antes/após os processos de transformação linear, as relações entre valores de máscaras lineares de entrada e valores de máscaras lineares de saída são determinadas como relações de um para um. Embora antes/após processos de transformação não linear as relações entre valores de máscaras lineares de entrada e valores de máscaras lineares de saída não sejam determinadas como relações de um para um, probabilidades de ocorrência de máscaras lineares de saída para uma máscara linear de entrada são calculadas. A soma de todas as probabilidades

para todas as saídas é um.

Em uma estrutura de Feistel, tendo funções-F do tipo SP, transformação não linear é realizada apenas em uma porção dos processos usando caixas-S. Em conseqüência, neste caso, um curso linear, tendo uma outra probabilidade que não zero, representa um conjunto de pedaços de dados de valores de máscaras lineares que são proporcionados como valores lineares, começando com um valor linear para texto normal (entrada) e terminando com um valor linear para texto cifrado (saída) e valores lineares que são proporcionados antes/após todas as caixas-S são valores lineares tendo outras probabilidades que não se quer. Uma caixa-S que é incluída em um curso linear, tendo uma outra probabilidade que não zero e à qual um valor linear que não é zero é introduzido, é referida como uma "Caixa-S ativa linear". O número mínimo entre os números de caixas-S ativas em todos os cursos lineares tendo outras probabilidades que não zero é referido como um "número mínimo de caixas-S ativas lineares" e o valor desse número é usado como um índice de segurança para ataques lineares.

Tornar grande o número mínimo de caixas-S ativas lineares leva à acentuação da resistência aos ataques lineares. Uma técnica para a construção de uma estrutura de DSM para tornar grande o número mínimo de caixas-S ativas lineares em uma estrutura de Feistel estendida, tendo o número de linhas de dados d que é estabelecido para qualquer inteiro que satisfaça $d > 2$ será descrita abaixo.

Uma matriz de transformação linear usada em uma função-F $[F_{s(i),\ x}]$ incluída em uma estrutura de Feistel estendida é denotada por $[M_{s(i),\ x}]$. Neste caso, uma equação $B_2^L(s(i))$ para calcular o número de derivações, em que a função de operação do número de derivações: Branch () é aplicada, é definida como segue:

[Equação 8]

$$B_2^L(s(i)) = \min_j(Branch_n([{}^tM^{-1}_{s(i),j} | {}^tM^{-1}_{s(i),j+1}]))$$

A equação mencionada acima é uma equação para calcular o valor mínimo de derivações em uma matriz de incidência $[{}^{t}M^{-1}{}_{s(i),\ j}|{}^{t}M^{-1}{}_{s(i),\ j+1}]$ de matrizes transpostas $[{}^{t}M^{-1}{}_{s(i),\ j}]$ e $[{}^{t}M^{-1}{}_{s(i),\ j+1}]$ de matrizes inversas de duas respectivas matrizes de transformação linear $[M_{s(i),\ j}]$ e $[M_{s(i),\ j+1}]$ que são usadas em duas funções-F $[F_{s(i),\ j}, F_{s(i),\ j+1}]$, que ficam adjacentes uma à outra e que são introduzidas em qualquer linha de dados s(i), constituindo a estrutura de Feistel estendida.

Em qualquer linha de dados s(i), constituindo a estrutura de Feistel estendida, [j] que corresponde ao número de funções-F, que são introduzidas na linha de dados s(i), do estágio superior é ajustado para qualquer j e, para um certo j, os seguintes são definidos:

uma entrada para a j-ésima função-F: $X_{s(i),\ j}$

um resultado obtido por OR-exclusivo (XOR) de uma saída da j-ésima função-F e dados na linha de dados s(i): $W_{s(i),\ j}$

uma entrada para a j+1- ésima função-F: $X_{s(i),\ j+1}$

Máscaras lineares para esses respectivos pedaços de dados são definidas como segue:

ΓXs(i), j

ΓWs(i), j

ΓXs(i), j+1

Nesse caso, se pelo menos qualquer uma das máscaras lineares não for zero, a seguinte relação é satisfeita

[Equação 9]

$$hw_n(\Gamma X_{s(i),j}) + hw(\Gamma W_{s(i),j}) + hw(\Gamma X_{s(i),j+1}) \geq B_2^L(s(i))$$

Em outras palavras, a relação mencionada acima é satisfeita. Isso significa que quanto maior o valor do lado esquerdo da relação mencionada acima, maior o número localizado de caixas-S ativas lineares. Em conseqüência, é concluído que é preferível que as matrizes sejam selecionadas de modo a tornar $B_2{}^{L}$(s(i)) grande.

Contudo, quando as duas matrizes de transformação linear [Ms(i), j] e [Ms(i), j+1], que são usadas nas duas funções-F [$F_{s(i),\ j}$, $F_{s(i),\ j+1}$], adjacentes uma à outra, que são introduzidas na linha de dados s(i), são as mesmas matrizes, a equação descrita acima para calcular o número de derivações, isto é, $B_2^L(s(i))$, se torna dois, que é o valor mínimo. Desse modo, um efeito de acentuação da resistência não pode ser esperado. $B_2^L(s(i))$ é feito para se tornar uma derivação muito maior, pelo que um valor mínimo de caixas-S ativas lineares é assegurado ser grande, de modo que a resistência aos ataques lineares pode ser acentuada. Assim, por exemplo, as matrizes são selecionadas de modo a tornar $B_2^L(s(i))$ igual ou maior do que três, pelo que a resistência aos ataques lineares pode ser acentuada.

$B_2^L(s(i))$ é calculado para cada uma das linhas de dados na estrutura de Feistel estendida. O valor mínimo dentre os valores calculados é denotado por B_2^L. Um método para selecionar matrizes nas funções-F de modo a tornar B_2^L igual a um ou maior do que três será descrito.

(4-3-1. Configuração para Selecionar Matrizes, que devem ser Ajustadas em Funções-F, que Fazem o Valor do Número Mínimo de Derivações B_2^L Igual ou Maior do que Três)

Será descrito abaixo que fazer o número mínimo de derivações $[B_2^L]$, que é o número mínimo entre os números mínimos de derivações $[B_2^L(s(i))]$ calculado para todas as linhas de dados na estrutura de Feistel estendida, igual ou maior do que três, pode ser realizado pelo fornecimento de pelo menos dois tipos de matrizes.

Primeiro, duas matrizes diferentes $[A_0]$ e $[A_1]$ são preparadas, as quais tornam o número de derivações em uma matriz de incidência $[{}^tA_0^{-1}|{}^tA_1^{-1}]$ das duas matrizes diferentes $[A_0]$ e $[A_1]$ igual ou maior do que três, isto é, que satisfazem como segue:

$$Branch_n([{}^tA_0^{-1}|{}^tA_1^{-1}]) \geq 3$$

A seguir, matrizes de transformação linear das seções de

transformação linear da pluralidade de funções-F, que são introduzidas na linha de dados s(i) na estrutura de Feistel estendida, são estabelecidas como segue:

A_0 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da primeira função-F $F_{s(i),\ 1}$.

A_1 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da segunda função-F $F_{s(i),\ 2}$.

A_0 é estabelecido como a matriz de transformação linear que é ajustada na seção de transformação linear da terceira função-F $F_{s(i),\ 3}$.

Dessa maneira, as duas matrizes diferentes $[A_0]$ e $[A_1]$ são dispostas alternadamente nessa ordem do topo para a pluralidade de funções-F, que são introduzidas na linha de dados s(i).

Quando as matrizes de transformação linear são estabelecidas dessa maneira, a equação descrita acima para calcular o valor mínimo do número de derivações na matriz de incidência $[{}^tM^{-1}{}_{s(i),\ j}|{}^tM^{-1}{}_{s(i),\ j+1}]$ das matrizes transpostas $[{}^tM^{-1}{}_{s(i),\ j}]$ e $[{}^tM^{-1}{}_{s(i),\ j+1}]$ das matrizes inversas das duas respectivas matrizes de transformação linear $[M_{s(i),\ j}]$ e $[M_{s(i),\ j+1}]$ que são usadas nas duas funções-F $[F_{s(i),\ j},\ F_{s(i),\ j+1}]$ adjacentes uma à outra, que são introduzidas em qualquer linha de dados s(i), é proporcionada como segue:

[Equação 10]

$$B_2^L(s(i)) = \min_j(Branch_n([{}^tM^{-1}_{s(i),j}|{}^tM^{-1}_{s(i),j+1}])) \geq 3$$

Em outras palavras, é assegurado que o número mínimo de derivações é igual ou maior do que três.

Como é óbvio, quando as matrizes $[A_0]$ e $[A_1]$ são permutadas, o mesmo efeito é obtido. Adicionalmente, quando as matrizes são similarmente estabelecidas para cada uma das linhas de dados s(i) na estrutura de Feistel estendida $B_2{}^L$ pode ser feito igual ou maior do que três, simplesmente pelo uso das duas matrizes.

$$Branch_n([{}^tA_0{}^{-1}|{}^tA_1{}^{-1}]) > 3$$

Dessa maneira, as duas matrizes diferentes $[A_0]$ e $[A_1]$, que satisfazem a relação dada acima são preparadas e as respectivas matrizes são estabelecidas de modo a serem dispostas alternadamente nas funções-F que são introduzidas nas respectivas linhas de dados s(i) na estrutura de Feistel estendida, pelo que o valor do número mínimo de derivações B_2^L pode ser feito igual ou maior do que três. A acentuação da resistência aos ataques diferenciais pelo uso do mecanismo de comutação de matriz de difusão (DSM) pode ser realizada.

[5. Configuração em Que DSM é Utilizado para Estrutura de Feistel estendida, Tendo Forma Específica]

Como descrito acima, a tecnologia de DSM é aplicada nas estruturas de Feistel estendido, tendo o número de linhas de dados d que é ajustado para qualquer inteiro que satisfaça $d \geq 2$, pelo que a resistência aos ataques diferenciais ou ataques lineares pode ser acentuada. As estruturas de Feistel estendido específicas em que um índice de segurança para ataques diferenciais ou ataques lineares pode ser assegurado em um alto nível serão descritas abaixo.

Como previamente descrito com referência às figuras 5 e 6, as estruturas de Feistel estendido, tendo o número de linhas de dados d que é ajustado para qualquer inteiro que satisfaça $d \geq 2$ têm várias configurações, como uma configuração em que uma pluralidade de funções-F podem ser realizadas em paralelo em um arredondamento. As estruturas de Feistel estendido serão amplamente classificadas em dois tipos (um tipo 1 e um tipo 2) e uma estrutura de Feistel estendida específica em que um índice de segurança para ataques diferenciais ou ataques lineares pode ser assegurado em um alto nível será descrita abaixo para cada tipo.

5-1. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 1

Primeiro, a aplicação de DSM à Estrutura de Feistel estendida

do Tipo 1 será descrita com referência à figura 8.

É suposto que a estrutura de Feistel estendida do tipo 1 tem os seguintes parâmetros.

Parâmetros:

(a) O número de divisões para um pedaço de dados: d (onde d é igual ou maior do que três).

(b) o comprimento de um pedaço de dados de entrada/saída: dmn bits.

(c) o comprimento de pedaços de dados divididos: mn bits.

(d) o número de funções-F por arredondamento: 1.

Conforme mostrado na figura 8, uma função-F é aplicada aos dados de mn- bits em uma linha de dados proporcionada na extremidade esquerda, mostrada na figura 8, em cada arredondamento, e o resultado do processo da função-F sai para uma linha de dados imediatamente adjacente e é submetido a OR-exclusivo. Note que os operadores de OR-exclusivo são omitidos na figura 8.

Conforme mostrado na figura 8, uma configuração é proporcionada, em que a linha de dados proporcionados na extremidade esquerda é usada para realizar entrada de dados para as funções-F em cada arredondamento, e em que a linha de dados proporcionada na extremidade esquerda é movida para a extremidade direita e as outras linhas de dados que não a linha de dados são desviadas para a esquerda por um, no arredondamento seguinte.

Uma configuração para acentuar a resistência aos ataques diferenciais e aos ataques lineares através da aplicação de DSM à estrutura de Feistel estendida em que uma função-F é realizada em cada arredondamento dessa maneira será descrita.

Em [4-2 Configuração para Acentuar a Resistência aos Ataques Diferenciais em Estrutura de Feistel estendida] que foi previamente

descrita, foi descrito que $B_2^D(s(i))$ é calculado para cada linha de dados em uma estrutura de Feistel estendida, que o valor mínimo entre os valores calculados é definido como B_2^D e que as matrizes em funções-F são selecionadas de modo a fazer B_2^D igual ou maior do que três, pelo que a resistência aos ataques diferenciais pode ser acentuada.

Além disso, em [4-3. Configuração para Acentuar a Resistência aos Ataques Lineares em Estrutura de Feistel estendida] que foi previamente descrita, foi descrito que $B_2^L(s(i))$ é calculado para cada linha de dados em uma estrutura de Feistel estendida, que o valor mínimo entre os valores calculados é definido como as B_2^L e que as matrizes em funções-F são selecionadas de modo a tornar B_2^L igual ou maior do que três, pelo que a resistência aos ataques lineares pode ser acentuada.

Em adição a B_2^D e B_2^L, além disso, o número mínimo de derivações entre o número de derivações em matrizes de transformação linear em funções-F incluídas na estrutura de Feistel estendida do tipo 1, conforme mostrado na figura 8, é denotado por B_1^D.

Neste caso, quando o número de caixas-S ativas diferenciais incluídas em p arredondamentos contínuos na estrutura de Feistel estendida do tipo 1, conforme mostrado na figura 8, é denotado por ActD(p) e o número de caixas-S ativas lineares é denotado por ActL(p), existem as seguintes relações:

$$ActD(3d) \geq B_1^D + B_2^D$$

$$ActL(3d) \geq 2B_2^L$$

Nas relações mencionadas acima:

ActD(3d) denota o número de caixas-S ativas diferenciais incluídas em 3d arredondamentos contínuos; e

ActL(3d) denota o número de caixas-S ativas lineares incluídas em 3d arredondamentos contínuos.

Essas relações mantidas serão descritas abaixo.

Conforme descrito acima, pela utilização das matrizes que tornam grandes B_1^D, B_2^D, e B_2^L , o número de caixas-S ativas pode ser assegurado como sendo grande e, em conseqüência, a resistência aos ataques diferenciais e aos ataques lineares pode ser acentuada.

Note que é conhecido que um valor teórico máximo de B_1^D, B_2^D ou B_2^L é m + 1.

Fazendo referência às relações mencionadas acima, isto é,

$$ActD(3d) \geq B_1^D + B_2^D \text{ e}$$

$$ActL(3d) \geq 2B_2^L,$$

O número mínimo de derivações B_2^D ou B_2^L, que foram previamente descritas, é incluído nos lados direito das relações. Tornar grandes os números mínimos de derivações contribui para assegurar que o número de caixas-S ativas seja grande e efetivo para acentuar a resistência aos ataques diferenciais e aos ataques lineares. Em conseqüência, na configuração da estrutura de Feistel estendida do tipo 1, conforme mostrado na figura 8, uma configuração em que o número mínimo de derivações B_2^D ou B_2^L, que foram previamente descritas, é tornado igual ou maior do que 3 é efetiva e, com a configuração, a resistência aos ataques diferenciais e aos ataques lineares pode ser assegurada em um nível maior do que aqueles na técnica anterior.

5-2. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 2

5-2. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 2

A seguir, a aplicação do DSM à estrutura de Feistel estendida de um tipo 2 será descrita com referência à figura 9.

É suposto que a estrutura de Feistel estendida do tipo 2 tem os seguintes parâmetros.

Parâmetros:

(a) o número de divisões para um pedaço de dados: d (onde d é um número par igual ou maior do que quatro)

(b) o comprimento de um pedaço de dados de entrada/saída: dmn bits.

(c) o comprimento de pedaços de dados divididos: mn bits

(d) o número de funções-F por arredondamento: d/2.

Conforme mostrado na figura 9, funções-F são aplicadas às linhas de dados de Mn-bits proporcionadas como linhas de dados com números ímpares da extremidade esquerda em cada arredondamento e os resultados dos processos das funções-F saem para linhas de dados imediatamente adjacentes e são submetidos ao OR-exclusivo. Note que os operadores do OR-exclusivo são omitidos na figura 9.

Conforme mostrado na figura 9, uma configuração é proporcionada em que a linha de dados proporcionada na extremidade esquerda é usada para realizar entrada de dados para as funções-F em cada arredondamento e em que a linha de dados proporcionada na extremidade esquerda é movida para a extremidade direita e as outras linhas de dados que não a linha de dados são deslocadas para a esquerda por um no arredondamento do texto.

Uma configuração para acentuar a resistência aos ataques diferenciais e aos ataques lineares através da aplicação do DSM à estrutura de Feistel estendida, em que d/2 funções-F são realizadas em cada arredondamento, dessa maneira, será descrita.

Em [4-2. Configuração para Acentuar a Resistência aos Ataques Diferenciais em Estrutura de Feistel estendida] que foi previamente descrita, foi descrito que $B_2^D(s(i))$ é calculado para cada linha de dados em uma estrutura de Feistel estendida, que o valor mínimo entre os valores calculados é definido como B_2^D e que matrizes em funções-F são selecionadas de modo a tornarem B_2^D igual ou maior do que três, pelo que a resistência aos

ataques diferenciais pode ser acentuada.

Além disso, em [4-3. Configuração para Acentuar a Resistência aos Ataques Lineares em Estrutura de Feistel estendida] que foi previamente descrita, foi descrito que $B_2^L(s(i))$ é calculado para cada linha de dados em uma estrutura de Feistel estendida, que o valor mínimo entre os valores calculados é definido como B_2^L e que matrizes em funções-F são selecionadas de modo a tornarem B_2^L igual ou maior do que três, pelo que a resistência aos ataques lineares pode ser acentuada.

Em adição a B_2^D e B_2^L, além disso, o número mínimo de derivações entre o número de derivações em matrizes de transformação linear em funções-F incluídas na estrutura de Feistel estendida do tipo 2, conforme mostrado na figura 9, é denotado por B_1^D.

Neste caso, quando o número de caixas-S ativas diferenciais incluídas em p arredondamentos contínuos na estrutura de Feistel estendida do tipo 2, conforme mostrado na figura 9, é denotado por ActD(p) e o número de caixas-S ativas lineares é denotado por ActL(p), existem as seguintes relações:

$$ActD(6) \geq B_1^D + B_2^D$$

$$ActL(6) \geq 2B_2^L$$

Nas relações mencionadas acima:

ActD(6) denota o número de caixas-S ativas diferenciais incluídas em seis arredondamentos contínuos; e

ActL(3d) denota o número de caixas-S ativas lineares incluídas em 3d arredondamentos contínuos.

Prova de que essas relações se mantêm será descrita abaixo.

Conforme descrito acima, pela utilização das matrizes que tornam grandes B_1^D, B_2^D, e B_2^L , o número de caixas-S ativas pode ser assegurado como sendo grande e, em conseqüência, a resistência aos ataques diferenciais e aos ataques lineares pode ser acentuada.

Note que é conhecido que um valor teórico máximo de B_1^D, B_2^D ou B_2^L é m + 1.

Fazendo referência às relações mencionadas acima, isto é,

$$ActD(6) \geq B_1^D + B_2^D \text{ e}$$

$$ActL(6) \geq 2B_2^L,$$

O número mínimo de derivações B_2^D ou B_2^L, que foram previamente descritas, é incluído nos lados direito das relações. Tornar grandes os números mínimos de derivações contribui para assegurar que o número de caixas-S ativas seja grande e efetivo para acentuar a resistência aos ataques diferenciais e aos ataques lineares. Em conseqüência, na configuração da estrutura de Feistel estendida do tipo 2, conforme mostrado na figura 9, uma configuração em que o número mínimo de derivações B_2^D ou B_2^L, que foram previamente descritas, é tornado igual ou maior do que três é efetiva e, com a configuração, a resistência aos ataques diferenciais e aos ataques lineares pode ser assegurada em um nível maior do que aqueles na técnica anterior.

[6. Prova de Relações entre Números de Caixas-S Ativas em Estrutura de Feistel estendida de Cada Tipo e Números Mínimos de Derivações com Base em Matrizes de Transformação Linear em Funções-F]

A seguir, a prova de relações entre os números de caixas-S ativas e os números mínimos de derivações com base em matrizes de transformação linear em funções-F, que foram descritas nos cabeçalhos das seções

[5-1. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 1] e

[5-2. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 2]

[6-1. Prova de Relações entre Números de Caixas-S Ativas em Estrutura de Feistel estendida de Cada Tipo e Números Mínimos de

Derivações com Base em Matrizes de Transformação Linear em Funções-F]

Primeiro, a prova de relações entre os números de caixas-S ativas na estrutura de Feistel estendida do tipo 1, que foram descritas previamente com referência à figura 8 e os números mínimos de derivações com base em matrizes de transformação linear em funções-F será descrita.

Em outras palavras, em um caso em que o número de caixas-S ativas diferenciais incluídas em p arredondamentos contínuos na estrutura de Feistel estendida do tipo 1 é denotado por ActD(p) e em que o número de caixas-S ativas lineares é denotado por ActL(p), existem as seguintes relações:

$$\mathrm{ActD}(3d) \geq B_1^{D} + B_2^{D}$$

$$\mathrm{ActL}(3d) \geq 2B_2^{L}$$

A prova de que essas relações se mantêm será descrita abaixo.

Quando a configuração da estrutura de Feistel estendida do tipo 1, que foi descrita previamente com referência a figura 8, é mostrada em outra forma, ela pode ser mostrada como uma configuração mostrada na figura 10. Embora a configuração seja mostrada na figura 8 de tal maneira que as respectivas linhas de dados são permitidas em uma base de arredondamento por arredondamento, de modo que uma linha de dados que é usada para realizar a entrada para uma função-F é colocada na extremidade esquerda, permutação das linhas de dados em uma base de arredondamento por arredondamento não é realizada na figura 10 e cada uma das linhas de dados é mostrada como uma linha. Na figura 10, os arredondamentos de 1 a 6d são mostrados. Embora d arredondamentos (arredondamentos de 1 a d, d+1 a 2d,..., 5d+1 a 6d) sejam mostrados de tal maneira que eles são dispostos em uma linha horizontal, esses arredondamentos não são realizados em paralelo e os respectivos arredondamentos, por exemplo, os arredondamentos de 1 a d, são realizados em seqüência.

Adicionalmente, embora operações de OR-exclusivo que são

realizadas em interseções de saídas de funções-F e as respectivas linhas de dados são omitidas na Figura 10, as operações de OR-exclusivo (XOR) são realizadas nas interseções de saídas de funções-F e as respectivas linhas de dados e os resultados são proporcionados como entradas para as funções-F do arredondamento seguinte.

Na configuração da estrutura de Feistel estendida do tipo 1, será provado que as relações seguintes, que foram previamente descritas em [5-1, Aplicação de DSM à estrutura de Feistel estendida do Tipo 1], se mantêm:

$$\mathrm{ActD}(3d) \geq B_1^{D} + B_2^{D}$$

$$\mathrm{ActL}(3d) \geq 2B_2^{L}$$

Nas relações:

ActD(3d) e ActL(3d) denotam o número de caixas-S ativas diferenciais e o número de caixas-S ativas lineares incluídas em 3d arredondamentos contínuos na estrutura de Feistel estendida do tipo 1, que é mostrado na figura 8 ou na figura 10.

B_1^{D} denota o número mínimo de derivações entre os números de derivações nas matrizes de transformação linear nas funções-F incluídas na estrutura de Feistel estendida do tipo 1.

B_2^{D} e B_2^{L} denotam o número mínimo de derivações em uma matriz de incidência xs matrizes de transformação linear e o número mínimo de derivações em uma matriz de incidência das matrizes transpostas, respectivamente, que foram previamente descritas em (4-2) e (4-3), em funções-F contínuas, que são introduzidas em uma linha de dados incluída em uma estrutura de Feistel estendida.

$B1^{D}$, B_2^{D}, e B_2^{L} são definidos como segue: [Equação 11]

$$B_1^{D} = \min_i(Branch_n(M_i))$$

$$B_2^{D} = \min_i(Branch_n([M_i \mid M_{i+d}]))$$

$$B_2^L = \min_i(Branch_n([{}^tM_i^{-1}|{}^tM_{i+d}^{-1}]))$$

Note que, nas definições mencionadas acima, a relação a seguir se mantém:

$$B_1{}^D \geq B_2{}^D$$

Adicionalmente, o número de caixas-S ativas diferenciais, incluídas na k-ésima função-F na estrutura de Feistel estendida do tipo 1, que é mostrado na figura 8 ou na figura 10, é denotado por D_k e o número de caixas-S ativas lineares é denotado por L_K

(Prova 1. Prova de ActD(3d) > $B_1{}^D + B_2{}^D$)

Primeiro, será provado que ActD(3d) > $B_1{}^D + B_2{}^D$ se mantém.

Em outras palavras, será provado que o número de caixas-S ativas diferenciais incluídas em 3d arredondamentos contínuos na estrutura de Feistel estendida do tipo 1, que é mostrado na figura 8 ou na figura 10, é igual ou maior do que $B_1{}^D + B_2{}^D$.

É considerado um caso em que uma diferença (AX), obtida usando uma entrada que não é zero, é proporcionada na estrutura de Feistel estendida do tipo 1. Nesse caso, a estrutura de Feistel estendida do tipo 1 tem as quatro características a seguir:

(Característica 1) - uma caixa-S ativa diferencial, que não é zero, existe em pelo menos um arredondamento dentre d arredondamentos contínuos.

(Característica 2)-se $D_k = 0$ se mantém, $D_{k-d+1} = D_k + 1$ se mantém.

(Característica 3)-se $D_k * 0$ se mantém, $D_{k-d+1} + D_k + D_k + 1 > B_1{}^D$ se mantém.

(Característica 4)-se $D_k + D_{k+d} * 0$ se mantém, $D_{k-d+1} + D_k + D_{k+d} + D_{k+d+1} > B_2{}^D$ se mantém.

Através da utilização das quatro características dadas acima, será provado que:

$ActD(3d) > B_1^D + B_2^D$ se mantém, isto é,

Será provado que "o número de caixas-S ativas diferenciais incluídas em 3d arredondamentos contínuos é igual ou maior do que $B_1^D + B_2^D$".

É suposto que o i-ésimo ao i+3d-ésimo arredondamentos são arredondamentos alvo.

Caso 1: um caso é suposto em que uma caixa-S ativa que não é zero existe nos $B_1^D + B_2^D$" arredondamentos.

Quando é suposto que um arredondamento em que uma caixa-S ativa que não é zero existe é o k-ésimo arredondamento, é indicado que $Dk \neq 0$ se mantém.

Caso 1-1: além do Caso 1, quando $Dk+d-1 \neq 0$ se mantém, os seguintes se mantêm:

De acordo com a característica 3, $Dk + Dk+1 + Dkd+ 1 \geq B_1^D$

De acordo com a característica 4, $Dk+d-1 + Dk-2d + Dk-1 + Dk+d \geq B2$

Desse modo, o seguinte é obtido:

[Equação 12]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

Caso 1-2: em adição ao Caso 1, quando $Dk+1 \neq 0$ se mantém, os seguintes se mantêm:

De acordo com a característica 3, $Dk+1 + Dk+2 + Dk-d+2 \geq B_1^D$

De acordo com a característica 4, $Dk + Dk-d+1 + Dk+d + Dk+d+1 \geq B_2^D$.

Assim, o seguinte é obtido

[Equação 13]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

Caso 1-3: em adição ao caso 1, quando $D_{k+d-1} = 0$ e $D_{k+1} = 0$ se mantêm, os seguintes se mantêm:

De acordo com a característica 2, $D_k = D_{k+d} \neq 0$;

De acordo com a característica 3, Dk+d + Dk+d+1 + Dk+1 ≥ B_2^D

De acordo com a característica 3, Dk+d + Dk+d+1 + Dk+1 ≥ $B2^D$

Como $D_{k+1} = 0$ se mantém, o seguinte é obtido:

[Equação 14]

$$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$

Caso 2: é suposto um caso em que nenhuma caixa-S ativa que não seja zero exista nos i+d+2 a i+2d-1 arredondamentos.

De acordo com a característica 1, Di+d+1 ≠ 0 ou Di+2d ≠ 0 se mantém

Caso 2-1: quando $D_{i+2d} = 0$ se mantém, embora D_{i+d+1} * 0 se mantenha, os seguintes se mantêm:

de acordo com a característica 2, Di+d+1 = Di+2d+1 ≠ 0 de acordo com a característica 3, Di+d+1 + Di+d+2 + Di+2 ≥ B_1^D

de acordo com a característica 3, Di+2d+1 + Di+2d+2 + Di+d+2 ≥ B_1^D.

Como $D_{i+d+2} = 0$ se mantém, o seguinte é obtido:

[Equação 15]

$$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$

Caso 2-2: quando $D_{i+2d} \neq 0$ se mantém, o seguinte se mantém:

De acordo com a característica 2, $D_{i+2d} = D_{i+d} \neq 0$, de acordo com a característica 3, $D_{i+d} + D_{i+d+1} + D_{i+1} > B_1^D$ de acordo com a característica 3, $D_{i+2d} + D_{i+2d+1} + D_{i+d+1} > B_1^D$.

Como $D_{i+d+1} = 0$ se mantém, o seguinte é obtido:

[Equação 16]

$$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$

Caso 2-3: quando $D_{i+d+1} \neq 0$ e $D_{i+2d} \neq 0$ se mantém, os seguintes se mantêm:

de acordo com a característica 3, $D_{i+d+1} + D_{i+d+2} + D_{i+2} > B_1^D$

de acordo com a característica 3, $D_{i+2d} + D_{i+2d+1} + D_{i+d} + D_{i+1} > B_2^D$

Desse modo, o seguinte é obtido:

[Equação 17]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

Quando o Caso 1 e o Caso 2 são resumidos, é provado que o seguinte se mantém:

[Equação 18]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

Em outras palavras, o seguinte se mantém:

$$\text{ActD}(3d) > B_1^D + B_2^D$$

Foi provado que o número de caixas-S ativas diferenciais incluídas nos 3d arredondamentos contínuos na estrutura de Feistel estendida do tipo 1, que é mostrado na figura 8 ou na figura 10 é igual ou maior do que $B_1^D + B_2^D$.

(Prova 2. Prova de $\text{ActL}(3d) > 2B_2^L$)

A seguir, será provado que $\text{ActL}(3d) > 2B_2^L$) se mantém.

Em outras palavras, será provado que o número de caixas-S ativas lineares incluídas em 3d arredondamentos contínuos na estrutura de Feistel estendida do tipo 1, que é mostrado na figura 8 ou na figura 10, é igual ou maior do que $2B_2^L$.

Note que, como descrito acima, B_2^L é definido como segue:

[Equação 19]

$$B_2^L = \min_i(Branch_n([{}^tM_i^{-1}|{}^tM_{i+d}^{-1}]))$$

Adicionalmente, o número de caixas-S ativas lineares incluídas na k- ésima função-F é denotada por L_k.

Quando uma máscara linear obtida usando uma entrada que não é zero é proporcionada na estrutura de Feistel estendida do tipo 1, a estrutura de Feistel estendida do tipo 1 tem as duas características a seguir:

(Característica 5) uma caixa-S ativa linear que não é zero existe em pelo menos um arredondamento dentre d arredondamentos contínuos.

(Característica 6) $L_k + L_{k+1} + L_{k+d} > B_2^L$ ou $L_k + L_{k+1} + Lk+d = 0$ se mantém. Note que, quando $L_k + L_{k+1} + L_{k+d} > B_2^L$ se mantém, dois ou mais termos incluídos no lado esquerdo não se tornam simultaneamente zero.

Através da utilização de duas características dadas acima, será provado que:

$ActL(3d) > 2B_2^L$, se mantém, isto é,

será provado que "o número de caixas-S ativas lineares incluídas em 3d arredondamentos contínuos é igual ou maior do que $2B_2^L$".

É suposto que os i+1-ésimo ao i+3d-ésimo são arredondamentos alvo.

Caso 1: é suposto um caso em que uma caixa-S ativa que não é zero existe nos i+d+2-ésimo ao i+2d-ésimo arredondamentos. Quando é suposto que um arredondamento em que uma caixa-S ativa que não é zero existe é o k-ésimo arredondamento, é indicado que $L_k \neq 0$ se mantém.

Caso 1-1: em adição ao Caso 1, quando $L_{k+d} \neq 0$ ou $L_{k-1} \neq 0$ se mantém, o seguinte se mantém:

de acordo com a característica 6, $L_k + L_{k+d} + L_{k+1} > B_2^L$

de acordo com a característica 6, $L_{k-1} + L_{k-1-d} + Lk\text{-}d \neq B2L$.

Desse modo, o seguinte é obtido:

[Equação 20]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

Caso 1-2: em adição ao caso 1, quando $L_{k+d} = 0$ e $L_{k-1} = 0$ se mantêm, o seguinte se mantém:

de acordo com a característica 6, $L_{k-d+1} * 0$

de acordo com a característica 6, $L_k + L_{k-1} + L_{k+d-1} > B_2^L$

de acordo com a característica 6, $L_{k-d+1} + L_{k+1} + L_{k-d+2} > B_2^L$

Nesse caso, se $d > 4$ se mantém, o seguinte é obtido:

[Equação 21].

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

Se $d = 3$ se mantém, já é conhecido que $L_{k-1} = 0$ se mantém, embora L_{k-1} seja duplicado.

Desse modo, similarmente, o seguinte é obtido:

[Equação 22]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

Caso 2: é suposto um caso em que uma caixa-S ativa que não seja zero não existe nos i+d+2-ésimo a i+2d-1-ésimo arredondamentos. Os seguintes se mantêm:

de acordo com a característica 1, $L_{i+d+1} \neq 0$

de acordo com a característica 6, $L_{i+d} \neq 0$

de acordo com a característica 6, $L_{i+d+1} + L_{i+d+2} + Li+2d+1 -$ B2

de acordo com a característica 6, $L_{i+d} + L_{i+d-1} + L_{i+2d-} 1 \neq B2^{L}$

Nesse caso, se d > 4 se mantém, o seguinte é obtido.

[Equação 23]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

Se d = 3 se mantém, já é conhecido que $L_{i+5} = 0$ se mantém, embora L_{i+5} seja duplicado.

Desse modo, similarmente, o seguinte é obtido:

[Equação 24]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

Quando o Caso 1 e o Caso 2 dados acima são resumidos, é provado que o seguinte se mantém:

[Equação 25]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

Em outras palavras, o seguinte se mantém:

$$ActL(3d) > 2B_2^{L},$$

Foi provado que o número de caixas-S ativas lineares incluídas em 3d arredondamentos contínuos na estrutura de Feistel estendida do tipo 1, que é mostrado na figura 8 ou na figura 10, é igual ou maior do que $2B_2^{L}$.

[6-2. Prova de Relações entre Números de Caixas-S Ativas em Estrutura de Feistel estendida do Tipo 2 e Números Mínimos de Derivações com Base em Matrizes de Transformação Linear em Funções-F]

A seguir, a Prova de Relações entre Números de Caixas-S Ativas em Estrutura de Feistel estendida do Tipo 2, que foi descrito na figura 9, e Números Mínimos de Derivações com Base em Matrizes de

Transformação Linear em Funções-F será descrita.

Em outras palavras, em um caso em que o número de caixas-S ativas diferenciais incluídas em p arredondamentos contínuos na estrutura de Feistel estendida do tipo 2 é denotado por ActD(p) e em que o número de caixas-S ativas lineares é denotado por ActL(p), existem as seguintes relações:

$$ActD(6) \geq B_1^D + B_2^D$$

$$ActL(6) \geq 2B_2^L$$

Será provado que essas relações se mantêm.

Quando a configuração da estrutura de Feistel estendida do tipo 2, que foi previamente descrita com referência à figura 9, é mostrada de outra forma, ela pode ser mostrada como uma configuração mostrada na figura 11. Embora a configuração seja mostrada na figura 9 de tal maneira que respectivas linhas de dados são permutadas em uma base de arredondamento por arredondamento, a permutação das linhas de dados não é realizada na figura 11 e cada uma das linhas de dados é mostrada como uma linha. Na figura 11, arredondamentos de 1 a 12 são mostrados de tal maneira que eles são dispostos em uma linha horizontal. Por exemplo, F1, 1, F1, 3, ... , e F1, d-1, selecionadas dentre as funções-F F1, 0 a F1, d-1, que são mostradas em uma linha horizontal para os arredondamentos de 1 a 2 mostrados na figura 11, que são funções-F selecionadas alternadamente (setas de saída são dirigidas para cima), são realizadas no primeiro arredondamento em paralelo. No segundo arredondamento a seguir, $F_{1,\ 1}$, $F_{1,\ 3}$, ... e $F_{1,\ d-1}$ restantes, que são funções-F selecionadas alternadamente (as setas de saída são dirigidas para baixo) são realizadas em paralelo.

Na figura 11, números usados para identificar cada uma das funções-F são introduzidos recentemente, a fim de compreender facilmente a prova e uma posição da função-F é determinada usando os dois números.

Isto é, i de $F_{i,\ j}$ denota um número de arredondamento (1 = 1 e

2 arredondamentos, 2 = 3 e 4 arredondamentos...) e Y denota- de uma função-F em dois arredondamentos. Note que, quando j é um número par, que é 0, 2 ou 4, a função-F é proporcionada para um arredondamento precedente e que, quando j é um número ímpar, que é 1, 3 ou 5, a função-F é proporcionada para o arredondamento seguinte. Note que, quando uma matriz de transformação linear incluída na função-F $F_{i,j}$ é referido como $[M_{i,j}]$.

Na configuração da estrutura de Feistel estendida do tipo 2, será provado que as seguintes relações, que foram previamente descritas em (5-2, Aplicação de DSM à Estrutura de Feistel estendida do Tipo 2) se mantêm:

$$ActD(6) \geq B_1^D + B_2^D$$

$$ActL(6) \geq 2B_2^L$$

Nas relações, ActD(6) e ActL(6) denotam o número de caixas-S ativas diferenciais e o número de caixas-S ativas lineares, respectivamente, incluídas em seis arredondamentos contínuos na estrutura de Feistel estendida do tipo 2, que é mostrado na figura 9 ou na figura 11.

B_1^D denota o número mínimo de derivações entre o número de derivações nas matrizes de transformação linear nas funções-F incluídas na estrutura de Feistel estendida do tipo 2.

B_2^D e B_2^L denotam o número mínimo de derivações em uma matriz de incidência de matrizes de transformação linear e o número mínimo de derivações em uma matriz de incidência de matrizes transpostas de matrizes inversas das matrizes de transformação linear, respectivamente, que foram previamente descritas em (4-2) e (4-3), em funções-F contínuas que são introduzidas em uma linha de dados incluída em uma estrutura de Feistel estendida.

B_1^D, B_2^D, e B_2^L são definidos como segue:

[Equação 26]

$$B_1^D = \min_{i,j}(Branch_n(M_{i,j}))$$

$$B_2^D = \min_{i,j}(Branch_n([M_{i,j} \mid M_{i+1,j}]))$$

$$B_2^L = \min_{i,j}(Branch_n([{}^tM_{i,j}^{-1} \mid {}^tM_{i+1,j}^{-1}]))$$

Note que, nas definições acima, as seguintes relações se mantêm:

$$B_1^D > B_2^D$$

Adicionalmente, o número de caixas-S ativas incluídas em $F_{p,q}$ é denotado por $D_{p,q}$. Note que, na descrição a seguir, quando uma porção denotada pelo subscrito q tem um valor negativo ou um valor igual ou maior do que d, uma operação de resíduo (q modo d) é realizada, usando d, assim, corrigindo a porção de modo que $0 < q < d$ sempre se mantém.

(Prova 3. Prova de $ActD(6) > B_1^D + B_2^D$)

Primeiro, será provado que $ActD(6) > B_1^D + B_2^D$) se mantém.

Em outras palavras, será provado que o número de caixas-S ativas diferenciais, incluídas em seis arredondamentos contínuos na estrutura de Feistel estendida do tipo 2, que é mostrado na figura 9 ou na figura ou 11, é igual ou maior do que $B_1^D + B_2^D$.

É considerado um caso em que uma diferença (AX), obtida usando uma entrada que não é zero, é proporcionada na estrutura de Feistel estendida do tipo 2. Nesse caso, a estrutura de Feistel estendida do tipo 2 tem as quatro características a seguir:

(Característica 1) Uma caixa-S ativa diferencial que não é zero existe em $F_{p,q}$ ($p = i$, q e {0,...d-1}) para um certo i.

(Característica 2) Se $D_{p,q} = 0$ se mantém,

Dp-1, q+1 = Dp, q+1 se mantém (onde q é um número par), e

Dp, q+1 = Dp+1, q+1 se mantém (onde q é um número ímpar)

(Característica 3) Se $D_{p,\,q} \neq 0$ se mantém,

D_p, q + D_p-1, q+1 + D_p, q+1 ≥ $B1^D$ se mantém (onde q é um número par), e

D_p, q + D_p, q+1 + D_p+1, q+1 ≥ $B1^D$ se mantém (onde q é um número ímpar).

(Característica 4) Se $D_{p,\,q} + D_{p+1,\,q} \neq 0$ se mantém,

Dp, q + Dp+1, q + *Dp-1,* q+1 + Dp+1, q+1 ≥ B2D se mantém (onde q é um número par) e

Dp, q + Dp+1, q + Dp, q+1 + Dp+2, q+1 ≥ B2D se mantém (onde q é um número ímpar).

Através da utilização das quatro características dadas acima , será provado que

$$\mathrm{ActD}(6) > B_1^D + B_2^D,$$

Se mantém, isto é, será provado que "o número total de caixas-S ativas diferenciais incluídas em 3d funções-F contínuas $F_{p,\,q}$ satisfazendo p G {i, i+1, i+2}, q G {0, 1,...d-1} para qualquer inteiro i que é igual ou maior do que um é igual ou maior do que $B_1^D + B_2^D$".

É suposto que, quando um elemento que não é zero é selecionado, arbitrariamente dentre $D_{p,\,q}$ (p = i + 1, q G {0,...d-1}), ele satisfaz $D_{j,\,k} \neq 0$. É indicado, de acordo com a (característica 1) mencionada acima, que ele sempre existe.

Caso 1: quando $D_{j,\,k-1} \neq 0$ se mantém, os seguintes se mantêm:

De acordo com a Característica 3,

Dj, k + *Dj-1,* k+1 + Dj, k+1 ≥ B_1^D (onde k é um número par)

Dj, k + Dj, k+1 + Dj+1, k+1 ≥ $B1^D$ (onde k é um número ímpar)

De acordo com a Característica 4,

Dj-1, k-1 + Dj, k-1 + Dj-1, k + Dj+1, k ≥ B2D (onde k é um número par)

Dj, k-1 + Dj+1, k-1 + Dj-1, k + Dj+1, k ≥ B2D (onde k é um número ímpar)

Desse modo, o seguinte se mantém:

[Equação 27]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

Caso 2: quando $D_{j,\,k+1} \neq 0$ se mantém, os seguintes se mantêm:

De acordo com a Característica 3,

Dj, k+1 + Dj, k+2 + Dj+1, k+2 ≥ $B1^D$ (onde k é um número par)

Dj, k+1 + Dj-1, k+2 + Dj, k+2 ≥ $B1^D$ (onde k é um número ímpar)

De acordo com a Característica 4,

Dj, k + Dj+1, k + Dj-1, k+1 + Dj+1, k+1 ≥ $B2^D$ (onde k é um número par)

Dj-1, k + Dj, k + Dj-1, k+1 + Dj+1, k+1 ≥ $B2^D$ (onde k é um número ímpar)

Desse modo, o seguinte se mantém:

[Equação 28]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

Caso 3: quando $D_{j,\,k-1} = 0$ e $D_{j,\,k+1} = 0$ se mantém, os seguintes se mantêm:

De acordo com a característica 2, como $D_{j,\,k-1} = 0$ se mantém,

Dj+1, k = Dj, k ≠ 0 (onde k é um número par)

$Dj-_{1,\,k}$ = Dj, k ≠ 0 (onde k é um número ímpar)

De acordo com a característica 3,

$Dj,_{\,k}$ + $Dj-_{1,\,k+1}$ + $Dj,_{\,k+1}$ ≥ $B_1{}^D$ (onde k é um número par)

Dj, k + Dj, k+1 + Dj+1, k+1 ≥ $B1^D$ (onde k é um número ímpar)

Ainda de acordo com a característica 3,

Dj+1, k + Dj, k+1 + Dj+1, k+1 ≥ $B1^D$ (onde k é um número par)

Dj-1, k + Dj-1, k+1 + Dj, k+1 ≥ $B1^D$ (onde k é um número ímpar)

Desse modo, como $D_{j,\ k+1} = 0$ se mantém, o seguinte se mantém:

[Equação 29]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

Quando os casos dados acima são resumidos, o seguinte é provado:

[Equação 30]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

Em outras palavras, o seguinte se mantém:

ActD(6) ≥ $B_1^D + B_2^D$

Foi provado que o número de caixas-S ativas diferenciais incluídas em seis arredondamentos contínuos na estrutura de Feistel estendida do tipo 2, que é mostrado na figura 9 ou na figura 11 é igual ou maior do que ActD(6) ≥ $B_1^D + B_2^D$

(Prova 4. Prova de ActL(6) ≥ $2B_2^L$)

A seguir, será provado que ActL(6) ≥ $2B_2^L$ se mantém.

Em outras palavras, será provado que o número de caixas-S ativas lineares incluídas em seis arredondamentos contínuos na estrutura de Feistel estendida do tipo 2, que é mostrado na figura9 ou na figura 11, é igual ou maior do que $2B_2^L$.

Note que, como descrito acima, B_2^L é definido como segue:

[Equação 31]

$$B_2^L = \min_{i,j}(Branch_n([{}^tM_{i,j}^{-1}|{}^tM_{i+1,j}^{-1}]))$$

Adicionalmente, o número de caixas-S ativas lineares incluídas na f-ésima função-F é denotado por Lp, q.

Quando uma máscara linear obtida usando uma entrada que não é zero é proporcionada na estrutura de Feistel estendida do tipo 2, a estrutura de Feistel estendida do tipo 2 tem as duas características a seguir:

(Característica 5) Uma caixa-S ativa diferencial que não é zero existe em $F_{p,\,q}$ (p = i, q e {0,...d-1}) para um certo i.

(Característica 6)

Lj, k + Lj+1, k + Lj, k+1 ≥ B2 ou Lj, k + Lj+1, k + Lj, k+1 = 0 se mantém (onde k é um número par) e

Lj, k + Lj+1, k + Lj+1, k+1 ≥ B2 ou Lj, k + Lj+1, k + Lj+1, k+1 = 0 se mantém (onde k é um número ímpar).

Note que, quando uma relação é representada em uma forma $L_a + L_b + L_c \geq B_2^L$, dois ou mais termos incluídos no lado esquerdo não se torna simultaneamente zero.

Através da utilização das duas características dadas acima, será provado que

$$\text{ActL}(6) \geq 2B_2^L,$$

se mantém, isto é,

Será provado que "o número de caixas-S ativas lineares incluídas em 3d funções-F, $F_{p,\,q}$ satisfazendo p e {i, i+1, i+2), q ∈ {0, 1, ... d-1} para qualquer inteiro i que seja igual ou maior do que um é igual ou maior do que $2B_2^L$".

É suposto que, quando um elemento que não é zero é selecionado arbitrariamente dentre Lp, q (p = i + 1, q ∈ {0, ... ,d-1}), satisfaz $L_{j,\,k} \neq 0$. É indicado, de acordo com a característica 5, que esse $L_{j,\,k}$ sempre

existe.

Os seguintes se mantêm:

de acordo com a característica 6,

$Lj\text{-}_{1,\,k} + L_{j,\,k} + Lj\text{-}_{1,\,k+1} \geq B_2^L$ (onde k é um número par)

$Lj,\ k + Lj+1,\ k + Lj+1,\ k+1 \geq B2^L$ (onde k é um número ímpar)

Caso 1: quando $L_{j,\,k\text{-}1} \neq 0$ se mantém, os seguintes se mantêm: de acordo com a característica 6,

$Lj,\ _{k\text{-}1} + L_{j+1,\,k\text{-}1} + L_{j+1,\,k} \geq B_2^L$ (onde k é um número par)

Lj-1, k-1 + Lj, k-1 + Lj-1, k $\geq B2^L$ (onde k é um número ímpar).

Desse modo, nesse caso, o seguinte se mantém:

[Equação 32]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} L_{p,q} \geq B_2^L$$

Caso 2: quando Lj, k-1 = 0 mantém, os seguintes se mantêm;

De acordo com a característica 6,

Lj-1, k-1 ≠ 0 (onde k é um número par)

Lj+1, k-1 ≠ 0 (onde k é um número ímpar)

Desse modo, o seguinte se mantém:

Lj-1, k-2 + Lj, k-2 + Lj-1, k-1 $\geq B2^L$ (onde k é um número par)

$Lj,\ k\text{-}2 + L_{j+1,\,k\text{-}2} + L_{j+1,\,k\text{-}1} \geq B_2L$ (onde k é um número ímpar)

Como d > 4 se mantém nesse caso, então, o seguinte se mantém:

[Equação 33]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} L_{p,q} \geq B_2^L$$

Quando o caso 1 e o caso 2 dados acima são resumidos, é

provado que o seguinte se mantém:

[Equação 34]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} L_{p,q} \geq B_2^L$$

Em outras palavras, o seguinte se mantém:

$$ActL(6) \geq 2B_2{}^L,$$

Foi provado que o número caixas-S ativas lineares incluídas em seis arredondamentos contínuos na estrutura de Feistel estendida do tipo 2, que é mostrado na figura 9 ou na figura 11, é igual ou maior do que $2B_2{}^L$.

[7. Configuração Aperfeiçoada para Implementação com Base em um Plano de Ajuste de Funções-F e Processo de Utilização de Funções-F]

Conforme descrito acima, na presente invenção, pelo menos duas ou mais matrizes diferentes são aplicadas seletivamente aos processos de transformação linear realizados em funções-F em respectivos arredondamentos, isto é, o chamado mecanismo de comutação de matriz de difusão (DSM) é aplicado, na estrutura de Feistel estendida, tendo o número de linhas de dados: d, que é estabelecido em um inteiro que satisfaça $d > 2$, assim, realizando uma configuração em que a resistência à análise linear ou à análise diferencial é acentuada.

Quando uma configuração em que os processos de operação em que uma pluralidade de matrizes diferentes são aplicadas seletivamente a são realizados dessa maneira deve ser realizado com *hardware*, seções de processamento de função-F tendo configurações de *hardware* para realizar operações que corresponde a às respectivas matrizes são necessários. Particularmente, quando uma pluralidade de funções-F devem ser realizadas em paralelo em um arredondamento, uma pluralidade de circuito estará pluralidade de funções-F para realizar processamento paralelo são necessários.

Em outras palavras a estrutura de Feistel estendida do tipo 2,

que foi previamente descrita com referência a figura 9 o asseguram 11, tem uma configuração em que processo de transformação de dados aos quais uma pluralidade de funções-F São aplicadas no mesmo arredondamento o são realizados em paralelo pode quando os processos de acordo com a configuração do tipo 2 devem ser realizados com *hardware*, é necessário implementar ou número de *hardware* de funções-F que corresponde ao número de funções-F que são realizadas em paralelo em um arredondamento. Com relação às funções-F que precisam ser realizadas em paralelo, conforme mencionado acima, uma pluralidade de funções-F tendo a mesma configuração precisam ser proporcionadas mesmo quando elas têm a mesma configuração.

Conforme descrito acima, uma configuração de processo criptográfico da presente invenção é uma configuração em que uma pluralidade de pelo menos duas ou mais matrizes diferentes são aplicadas seletivamente aos processos de transformação linear que são realizados em funções-F em respectivos arredondamentos, pelo que é proporcionada como uma configuração em que a resistência aos vários tipos de ataques é acentuada. Em outras palavras é proporcionada como uma configuração dotada de mecanismo de comutação de matriz de difusão (DSM: Diffusion Switching Mechanism – Mecanismo de Comutação de Difusão).

A fim de satisfazer o mecanismo de comutação de matriz de difusão (DSM), é necessário apenas que uma condição seja satisfeita, por exemplo, em que uma pluralidade de matrizes diferentes, satisfazendo uma condição em que o número mínimo de derivações $[B_k^D]$ para todas as linhas de dados é igual ou maior do que três, são estabelecidas, o número mínimo de derivações $[B_k^D]$ para todas as linhas de dados que estão sendo selecionadas dentre números mínimos de derivações $[B_k^D(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[B_k^D(s(i))]$ correspondendo às linhas de dados que estão sendo calculadas com base nas

matrizes de transformação linear incluídas em k (onde k é um inteiro igual ou maior do que dois) funções-F, que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida. Não há restrição particular das funções-F que são realizadas em paralelo em cada arredondamento.

Um exemplo de uma configuração em que a eficiência da implementação é aperfeiçoada ao mesmo tempo em que mantém a resistência com base no mecanismo de comutação de matrizes de difusão (DSM) em uma estrutura de Feistel estendida com base nessas características será descrito abaixo.

(7-1. Método para Dispor Eficientemente Funções-F em Estrutura de Feistel estendida do Tipo 2)

Primeiro, para começar, uma configuração para dispor eficientemente funções-F Na estrutura de Feistel estendida do tipo 2, que foi descrita com referência à figura 9 ou à figura 11, será descrita. Conforme mencionado no cabeçalho da de seção (5-2. Aplicação de DSM à Estrutura de Feistel estendida do Tipo 2), que foi descrita previamente, a estrutura de Feistel estendida do tipo 2 tem os seguintes parâmetros:

Parâmetros:

(a) O número de divisões para um pedaço de dados: d (onde d é um número par igual ou maior do que quatro).

(b) o comprimento de um pedaço de dados de entrada/saída: dmn bits.

(c) o comprimento de um pedaço de dados divididos: mn bits.

(d) o número de funções-F por arredondamento: d/2.

Em outras palavras, conforme mostrado na figura 9, funções-F são aplicadas às linhas de dados de mn- bits proporcionadas como linhas de dados de números ímpares da extremidade esquerda em cada arredondamento, e os resultados do processo das funções-F saem para as linhas de dados

imediatamente adjacentes e são submetidos a OR-exclusivo. Note que os operadores de OR-exclusivo são omitidos na figura 9.

Uma configuração será descrita abaixo, em que a eficiência de implementação para a estrutura de Feistel estendida do tipo 2, tendo essa configuração é acentuada. Como exemplo, um caso em que o número de linhas de dados (o número de divisões) é ajustado como d = 4 será descrito com referência à figura 12. Na figura 12, duas funções-F, que realizam transformação linear usando duas matrizes diferentes de transformação linear M1 e M2, são denotadas por F1 e F2, respectivamente.

Uma estrutura de Feistel mostrada na figura 12 é a estrutura de Feistel estendida do tipo 2 em que as duas funções-F, isto é, as funções-F F1 e F2, são usadas e em que d = 4 se mantém. Em outras palavras têm uma configuração tendo o seguinte:

(a) O número de divisões para um pedaço de dados: quatro

(b) o comprimento de um pedaço de dados de entrada/saída: 4mn bits.

(c) o comprimento de pedaços de dados divididos: mn bits.

(d) o número de funções-F por arredondamento: 4/2 = 2

Em um caso da configuração mostrada na figura 12, a fim de satisfazer condições para o DSM pelo uso das duas funções-F, algumas disposições podem ser consideradas. Em outras palavras, a fim de satisfazer condições para o DSM, como descrito acima, é necessário apenas que uma condição seja satisfeita, por exemplo, em que uma pluralidade de matrizes diferentes, satisfazendo uma condição em que o número mínimo de derivações $[B_k^D]$ para todas as linhas de dados é igual ou maior do que três, são estabelecidas, o número mínimo de privações $[B_k^D]$ para todas as linhas de dados sendo selecionado dentre os números mínimos de derivações $[B_k^D(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[B_k^D(s(i))]$, correspondendo às linhas de dados que estão sendo

calculadas com base nas matrizes de transformação linear incluídas em k (onde k é um inteiro igual ou maior do que dois) funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida. Não há restrição particular das funções-F que são realizadas em paralelo em cada arredondamento.

Em conseqüência, como maneiras em que as funções-F são estabelecidas, as duas maneiras a seguir podem ser usadas:

(a) ajuste de uma pluralidade de funções-F que devem ser estabelecidas em um arredondamento como as mesmas funções-F;

(b) ajuste de uma pluralidade de funções-F que devem ser estabelecidas em um arredondamento como funções-F diferentes.

Aqui, conforme mostrado na figura 12, uma configuração é proporcionada, em que duas funções-F que existem em um arredondamento são selecionadas de modo que elas são um par de F1 e F2. Uma vantagem dessa configuração aparece, acentuadamente e, quando a implementação de *hardware* (H/W) é realizada com base em processos para um arredondamento.

Em outras palavras, a implementação de *hardware* (H?W) é realizada para ajustar *hardware* tendo uma configuração em que apenas processos para um arredondamento podem ser realizados, isto é, uma configuração em que a função-F F1 e a função-F F2 podem ser realizadas em paralelo, conforme mostrado na figura 13. A figura 13 é um diagrama em blocos mostrando um aparelho de processamento criptográfico 250 tendo uma configuração de *hardware* em que o processo criptográfico de acordo com a estrutura de Feistel estendida mostrada na figura 12 é realizado.

O aparelho de processamento criptográfico 250 inclui um primeiro circuito de processamento dedicado de função-F (F1) 251, que realiza a função-F F1, um segundo circuito de processamento de indicado de função-F (F2) 252, que realiza a função-F F2, um circuito de controle 253 e

um circuito auxiliar 254. O primeiro circuito de processamento dedicado de função-F (F1) 251 e o segundo circuito de processamento dedicado de função-F (F2) 252 são configurados de modo que eles possam operar em paralelo e a transformação de dados com base nas duas funções-F diferentes é realizada através da aplicação desses dois circuitos em cada arredondamento.

O circuito de controle 253 realiza controle de dados de entrada/saída para os respectivos circuitos de processamento dedicados de função-F 251 e 252 e o circuito auxiliar 254. O circuito auxiliar 254 realiza outros processos de operação que não as funções-F ou semelhantes.

Com a aplicação dessa configuração, o primeiro circuito de processamento dedicado de função-F (F1) e o segundo circuito de processamento dedicado de função-F (F2) 252 são aplicados apenas nas vezes que correspondem ao número de arredondamentos requeridos, de modo que as operações de arredondamento podem ser realizadas. Os dois circuitos dedicados de funções-F são operados em paralelo em todos os arredondamentos e implementação em que nenhum circuito sem utilidade é proporcionado pode ser realizada.

Quando o número de funções-F que são realizadas em paralelo em cada arredondamento é dois, conforme mostrado nas figura 12, todas as operações de arredondamento podem ser realizadas usando implementação de *hardware* mostrada na figura 13 com um ajuste em que as funções-F são estabelecidas como funções-F diferentes. Além disso, quando uma configuração em que funções-F que são realizadas em um arredondamento são estabelecidas como as mesmas funções-F, por exemplo, uma configuração em que F1 e F2 são realizadas em paralelo no primeiro arredondamento e F2 e F2 são realizadas no segundo arredondamento, é proporcionada, dois pedaços de cada um de um circuito de realização de F1 e um circuito de realização de F2 precisam ser proporcionados como *hardware*, de modo que uma configuração tendo circuitos cuja escala é maior do que aquela dos circuitos

incluídos na configuração mostrada na figura 13 é requerida.

Conforme mostrado na figura 12, com um ajuste em que todas as combinações das funções-F que são realizadas em respectivas arredondamentos são ajustadas como os pares de F1 e F2, o *hardware* mostrado na figura 13 é aplicado e F1 e F2 podem ser sempre realizados simultaneamente em cada um dos arredondamentos. Um aparelho compacto em que a escala de circuitos é reduzida sem proporcionar qualquer circuito inútil é realizado.

Embora a configuração mostrada na figura 12 corresponda a um caso em que o número de linhas de dados é estabelecido como d = 4, a implementação eficiente pode ser realizada usando um ajuste similar também em um caso em que o número de linhas de dados é ajustado para outro número. Por exemplo, embora quatro funções-F sejam ajustadas em um arredondamento em um caso em que o número de linhas de dados é estabelecido como d = 8, uma configuração é proporcionada em que dois pedaços de cada uma das duas funções-F diferentes F1 e F2 são estabelecidas como essas quatro funções-F.

Em uma configuração de implementação neste caso, dois pedaços de cada uma das funções-F F1 e F2 são proporcionados, pelo que uma configuração em que essas quatro funções-F (F1, F1, F2, F2) podem ser realizadas em paralelo é proporcionada. Com essa configuração, todas as quatro funções-F são realizadas em paralelo em todos os arredondamentos e a implementação sem fornecimento de qualquer circuito inútil pode ser realizada.

Adicionalmente, quando o número de linhas de dados é estabelecido como d = 16, quatro pedaços de cada uma de F1 e F2 são estabelecidas como oito funções-F que existem em um arredondamento. Para generalização adicional, quando o número de linhas de dados é estabelecido como d = 4x , uma configuração em que x pedaços das funções-F F1 e F2 são

utilizados em cada arredondamento. Em um caso em que a implementação de *hardware* é realizada, se uma configuração em que x pedaços de cada uma das funções-F F1 e F2 são estabelecidos é proporcionada, os números de pedaços de F1 e F2 que são requeridos em cada arredondamento são os mesmos. Desse modo, F1 e F2 podem ser realizadas sem excesso ou deficiência e a eficiência de implementação pode ser aperfeiçoada.

Embora o exemplo de processo descrito acima seja um exemplo em que duas funções-F diferentes às quais duas matrizes diferentes de transformação linear são aplicadas são estabelecidas a fim de satisfazer o mecanismo de comutação de matriz de difusão (DSM), uma coisa similar pode ser aplicada também em casos em que três ou mais funções-F são estabelecidas pelo uso de três ou mais matrizes de transformação linear.

Um exemplo de uma disposição para implementar eficientemente três tipos de funções-F é mostrado na figura 14. A figura 14 é um exemplo da estrutura de Feistel estendida do tipo 2, tendo o número de linhas de dados que é estabelecido como d = 6. Uma configuração mostrada na figura 14 é estabelecida para uma configuração em que um pedaço de cada uma das três funções-F F1, F2, F3, que existem em um arredondamento, é utilizado com segurança.

Com essa configuração, quando a implementação de *hardware* (H/W) é realizada, uma configuração em que funções-F podem ser realizadas em paralelo em cada arredondamento pode ser proporcionada usando implementação simples de um pedaço de cada uma de F1, F2 e F3 e uma configuração de circuito que não inclui circuitos sem utilidade em termos de H/W é realizada.

Além disso, quando número de linhas de dados é estabelecido como d = 12, dois pedaços de cada uma de F1, F2 e F3 são estabelecidos como seis funções-F que existem em um arredondamento. Adicionalmente, quando o número de linhas de dados é estabelecido como d = 18, três pedaços

de cada uma de F1, F2 e F3 são estabelecidos como nove funções-F que devem ser estabelecidas em um arredondamento. Em um caso em que os casos mencionados acima são generalizados, quando o número de linhas de dados é estabelecido como d = 6, x pedaços de cada uma de F1, F2 e F3 são proporcionados como funções-F que devem ser estabelecidas em cada arredondamento. Em outras palavras, uma configuração é proporcionada em que funções-F diferentes são igualmente utilizadas.

Com uma configuração em que as funções-F são estabelecidas dessa maneira, os números de pedaços de F1, F2 e F3 que são requeridos em cada arredondamento podem ser ajustados para o mesmo número. Quando a implementação de *hardware* é realizada, circuitos podem ser estabelecidos de modo a serem utilizados sem excesso ou deficiência, de modo que a eficiência de implementação pode ser aperfeiçoada. Em um caso em que *software* é usado, porque utilizando maneiras em que tabelas para obtenção de valores de entrada/e saída são utilizadas em respectivos arredondamento, uma tabela pode ser estabelecida de acordo com uma maneira de utilização sem configurar tabelas para vários casos supostos e ser armazenada em uma memória.

Quando os respectivos exemplos de processos descritos acima são ainda generalizados, o seguinte pode ser dito :

(1) em um caso em que a estrutura de Feistel estendida do tipo 2 em que tipos de funções-F são utilizados é configurada, quando o número de linhas de dados (o número de divisões) é estabelecido como d = 2ax, onde a é um inteiro igual ou maior do que dois e x é um inteiro igual ou maior do que um, uma configuração em que x pedaços de cada um dos tipos de funções-F são igualmente estabelecidos como ax funções-F que devem ser estabelecidas em um arredondamento é usada, de modo que a eficiência de implementação pode ser aperfeiçoada.

Note que, com relação ao ajuste descrito acima de funções-F,

as funções-F que são introduzidas em respectivas linhas de dados são estabelecidas de modo que as condições descritas acima para DSM sejam satisfeitas. Com esse ajuste, a resistência pode ser mantida.

7-2. Associação de Componentes em Estrutura de Feistel e Estrutura de Feistel estendida

Como descrito acima, o mecanismo de DSM é utilizado para qualquer uma das estruturas de Feistel, a estrutura de Feistel estendida do tipo 1, e a estrutura de Feistel estendida do tipo 2, que foram previamente descritas, assim, proporcionando uma vantagem pelo fato de que a resistência aos ataques é acentuada.

Em outras palavras, quando as estruturas de Feistel são amplamente classificadas nos seguintes:

(a) uma estrutura de Feistel tendo o número de linhas de dados (o número de divisões) que é estabelecido como $d = 2$;

(b) uma estrutura de Feistel estendida tendo o número de linhas de dados (o número de divisões) que é estabelecido para qualquer número que satisfaça $d \geq 2$.

Ainda, a estrutura de Feistel estendida pode ser classificada nos seguintes:

(b1) um tipo 1 em que uma função-F é permitida ser realizada em cada arredondamento;

(b2) um tipo 2 em que uma pluralidade de funções-F são permitidas serem realizadas em paralelo em cada arredondamento.

As estruturas de Feistel podem ser classificadas nesses três tipos (a), (b1) e (b2).

A acentuação de resistência é realizada com aplicação do mecanismo de DSM em qualquer um dos três tipos de estruturas de Feistel.

Para aplicação do mecanismo de DSM, é necessário implementar funções-F diferentes que realizam pelo menos duas ou mais

matrizes diferentes de transformação linear. Com uma configuração de implementação tendo essa pluralidade de funções-F diferentes, um aparelho que pode realizar seletivamente a pluralidade mencionada acima de estruturas de Feistel diferentes (a), (b1) e (b2) pode ser realizado. Esse aparelho que realiza um processo de seleção será descrito abaixo.

Uma pluralidade de funções-F diferentes que realizam matrizes de transformação linear satisfazendo mecanismos de comutação de matriz de difusão (DSM) são determinadas e é suposto que o tamanho de dados dos dados de entrada /saída das respectivas funções-F é mn bits. Com a aplicação dessas funções-F, por exemplo, cifra de blocos de 2mn bits é realizada em uma estrutura de Feistel, conforme mostrado na figura 15, tendo o número de linhas de dados que é estabelecido como d = 2.

O tamanho dos dados de entrada/e saída das respectivas funções-F F1 e F2, na estrutura de Feistel tendo número de linhas de dados que é estabelecido como d = 2, que é mostrado na figura 15, é mn bits. A estrutura de Feistel tendo o número de linhas de dados que é estabelecido como d = 2 realiza um processo de transformação de texto normal de 2mn bits em texto cifrado de 2mn bits ou um processo de descriptografia que é o inverso do processo, assim, realizando cifra de bloco de 2mn bits.

Adicionalmente, pela utilização das funções-F F1 e F2 cujo tamanho de dados de entrada/saída é mn bits, que são mostrados na figura 15, uma estrutura de Feistel estendida que satisfaz o mecanismo de comutação de matriz de difusão (DSM) e que tenha o número de linhas de dados que é estabelecido como d = 4 pode ser configurada. Uma configuração da estrutura de Feistel estendida é mostrada na figura 16.

O tamanho dos dados de entrada/saída de respectivas funções-F F1 e F2 na estrutura de Feistel tendo o número de linhas de dados que é estabelecido como d = 4, que é mostrado na figura 16, é mn bits e as funções-F F1 e F2 mostradas na figura 15 são aplicadas como são. A estrutura de

Feistel tendo o número de linhas de dados que é estabelecido como d = 4 realiza um processo de transformação de texto normal de 4mn bits em texto cifrado de 4mn bits ou um processo de descriptografia que é o inverso do processo, assim, realizando cifra de blocos de 4mn bits.

Além disso, para generalização, quando o número de linhas de dados é estabelecido como d = x, onde x é um inteiro igual ou maior do que dois, uma configuração de cifra de blocos em que um processo de criptografia ou descriptografia de xmn bits é realizado pode ser estruturada usando a mesma configuração para realização de funções-F.

Por exemplo, um aparelho capaz de realizar, seletivamente, um processo de cifra de blocos de 128 bits de entrada/saída e um processo de cifra de blocos de 256 bits em que o mecanismo de DSM é realizado pelo uso apenas de funções-F diferentes F1 e F2, cujos bits de entrada/saída são 64 bits.

Em outras palavras, as duas funções-F diferentes F1 e F2, cujos bits de entrada/saída são 64 bits são implementadas como funções-F e uma maneira para utilização das funções-F F1 e F2 é controlada. Por exemplo, quando um processo criptográfico baseado em estrutura de Feistel tendo o número de linhas de dados que é estabelecido como d = 2 (figura 15) deve ser realizado, uma configuração é proporcionada em que uma das respectivas funções-F F1 e F2 é realizada em cada arredondamento. Em contraste, quando um processo criptográfico baseado na estrutura de Feistel tendo o número de linhas de dados que é estabelecido como d-4 (figura 16) deve ser realizada, uma configuração é proporcionada, em que as respectivas funções-F F1 e F2 são realizadas em paralelo em cada arredondamento. Dessa maneira, através da instalação dos dois tipos de funções-F, um aparelho capaz de realizar, seletivamente, cifra de blocos de 128 bits e cifra de blocos de 256 bits de entrada/saída é realizado. Em outras palavras, embora as mesmas funções-F sejam usadas, o método de conexão é mudado, pelo que a cifra de

blocos, tendo os números de bits diferentes pode ser realizada, de modo que pode ser esperado que a eficiência de implementação será aperfeiçoada pela associação de circuitos e/ou códigos ou semelhant4es em ambos, S/W e H/W.

Um exemplo de configuração de um aparelho de processamento criptográfico 270, que é mostrado na figura 17. Um aparelho de processamento criptográfico 270, que é mostrado na figura 17 inclui um primeiro circuito de processamento dedicado de função-F (F1) 271 que realiza a função-F F1, um segundo circuito de processamento dedicado de função-F (F2) 272, que realiza a função-F F2, um circuito de controle 273 e um circuito auxiliar 274.

O primeiro circuito de processamento dedicado de função-F (F1) e o segundo circuito de processamento dedicado de função-F (F2) 272 são configurados de modo que possam operar em paralelo. O circuito de controle 273 realiza o controle dos dados de entrada/saída para as respectivas unidades de processamento e realiza um processo de seleção de uma estrutura de Feistel. O circuito auxiliar 274 realiza outros processos de operação que não as funções-F ou semelhantes.

O circuito de controle 273 realiza o processo de seleção de uma estrutura de Feistel, isto é, seleciona qualquer uma das seguintes estruturas a fim de realizar um processo criptográfico com base na estrutura:

(a) uma estrutura de Feistel tendo o número de linhas de dados (o número de divisões) que é estabelecido como d = 2.

(b1) uma estrutura de Feistel estendida de um tipo 1, que tem o número de linhas de dados (o número de divisões) que é estabelecido como qualquer número que satisfaça $d \geq 2$ e em que uma função-F é permitida ser realizada em cada arredondamento.

(b2) uma estrutura de Feistel estendida de um tipo 2 que tem o número de linhas de dados (o número de divisões) que é estabelecido como qualquer número que satisfaça $d \geq 2$ e em que uma pluralidade de funções-F é

permitida ser realizada em cada arredondamento.

Note que, a informação de ajuste é introduzida, por exemplo, do lado de fora. Alternativamente, uma configuração pode ser proporcionada, em que um modo de processamento deve ser realizado é selecionada de acordo com o comprimento de bits de dados que deve ser submetido a um processo de criptografia ou de descriptografia. O circuito de controle 273 realiza controle de mudança de uma seqüência de aplicação dos respectivos circuito dedicados de função-F de acordo com a seleção e controle de realização de funções de arredondamento de acordo com as respectivas estruturas de Feistel.

Com a aplicação dessa configuração, o primeiro circuito de processamento dedicado de função-F (F1) 251 e o segundo circuito de processamento dedicado de função-F (F2) 252 são aplicados de modo que processos criptográficos aos quais várias estruturas de Feistel são aplicadas podem ser realizadas. Processos criptográficos que suportam vários bits, em que bits a serem processados em um processo DE criptografia ou a um processo de descriptografia são diferentes, podem ser realizados.

Adicionalmente, embora um exemplo em que duas funções-F são usadas seja mostrado na figura 17, a configuração não está limitada àquela proporcionada no exemplo em que duas funções-F são usadas, e um resultado similar pode ser esperado também com uma configuração em que qualquer número de funções-F é usado. Por exemplo, a estrutura de Feistel estendida que foi previamente descrita com referência à figura 14 é configurada como uma estrutura de Feistel estendida que satisfaz o mecanismo de comutação de matriz de difusão (DSM) e que tem o número de linhas de dados d = 6 com aplicação das três funções-F diferentes F1, F2 e F3. Uma configuração de processo criptográfico tendo uma estrutura de Feistel tendo o número de linhas de dados que é estabelecido como d = 2, que é mostrado na figura 18, pode ser construída com a aplicação dos mesmos três

tipos de funções-F, isto é, as funções-F F1, F2 e F3. Também na configuração em que o número de linhas de dados é estabelecido como d = 2, as respectivas matrizes F1, F2 e F3 são dispostas com um ajuste em que satisfazem o mecanismo de DSM.

Um exemplo de uma configuração de um aparelho de processamento criptográfico que realiza os três tipos de funções-F, isto é, F1, F2 e F3, é mostrado na figura 19. Um aparelho de processamento criptográfico 280, que é mostrado na figura 19 inclui um primeiro circuito de processamento dedicado de função-F (F1) 281 que realiza a função-F F1, um segundo circuito de processamento dedicado de função-F (F2) 282 que realiza a função-F F2, um terceiro circuito de processamento dedicado de função-F (F3) 283 que realiza a função-F F3, um circuito de controle 274 e um circuito auxiliar 275. O primeiro circuito de processamento dedicado de função-F (F1) 281, o segundo circuito de processamento dedicado de função-F (F2) 282 e o terceiro circuito de processamento dedicado de função-F (F3) 283 são configurados de modo que podem operar em paralelo. O circuito de controle 284 realiza controle de dados de entrada/saída para as respectivas unidades de processamento e realiza um processo de seleção de uma estrutura de Feistel. O circuito auxiliar 285 realiza outros processos de operação que não as funções-F ou semelhantes.

O circuito de controle 284 realiza o processo de seleção de uma estrutura de Feistel, isto é, seleciona qualquer uma das estruturas seguintes para realizar um processo criptográfico com base na estrutura:

(a) uma estrutura de Feistel tendo o número de linhas de dados (o número de divisões) que é estabelecido como d = 2.

(b1) uma estrutura de Feistel estendida de um tipo 1, que tem o número de linhas de dados (o número de divisões) que é estabelecido como qualquer número que satisfaça $d \geq 2$ e em que uma função-F é permitida ser realizada em cada arredondamento.

(b2) uma estrutura de Feistel estendida de um tipo 2 que tem o número de linhas de dados (o número de divisões) que é estabelecido como qualquer número que satisfaça $d \geq 2$ e em que uma pluralidade de funções-F é permitida ser realizada em cada arredondamento.

Note que, a informação de ajuste é introduzida, por exemplo, do lado de fora. O circuito de controle 284 realiza controle de mudança de uma seqüência de aplicação dos respectivos circuitos dedicados de função-F de acordo com o ajuste e controle de realização de funções de arredondamento de acordo com as respectivas estruturas de Feistel.

Com a aplicação dessa configuração, o primeiro circuito de processamento dedicado de função-F (F1) 281 ao terceiro circuito de processamento dedicado de função-F (F3) 283 são aplicados de modo que processos criptográficos aos quais várias estruturas de Feistel são aplicadas podem ser realizadas. Processos criptográficos que suportam vários bits, em que bits a serem processados em um processo de criptografia ou a um processo de descriptografia são diferentes, podem ser realizados. Note que uma configuração tendo quatro ou mais seções de realização de função-F pode ser proporcionada.

Conforme descrito acima, uma pluralidade de funções-F diferentes que realizam matrizes de transformação linear que satisfazem o mecanismo de comutação de matriz de difusão (DSM) são determinadas e as respectivas funções-F são implementadas. Uma seqüência de processos aos quais as funções-F são aplicadas é mudada, assim, realizando uma configuração em que um processo criptográfico com base em qualquer uma das estruturas seguintes é realizado, seletivamente:

(a) uma estrutura de Feistel tendo o número de linhas de dados (o número de divisões) que é estabelecido como $d = 2$.

(b1) uma estrutura de Feistel estendida de um tipo 1, que tem o número de linhas de dados (o número de divisões) que é estabelecido como

qualquer número que satisfaça d ≥ 2 e em que uma função-F é permitida ser realizada em cada arredondamento.

(b2) uma estrutura de Feistel estendida de um tipo 2 que tem o número de linhas de dados (o número de divisões) que é estabelecido como qualquer número que satisfaça d ≥ 2 e em que uma pluralidade de funções-F é permitida ser realizada em cada arredondamento.

Um aparelho capaz de mudar o número de bits a serem processados em um processo de criptografia ou um processo de descriptografia.

Por exemplo, processos criptográficos com uma alta resistência podem se realizados usando uma configuração de processo em que a (a é um inteiro igual ou maior do que dois) tipos de funções-F são configurados em que processos criptográficos com base nos três tipos de estruturas de Feistel mencionados acima são realizados e em que o mecanismo de comutação de matriz de difusão (DSM) é satisfeito.

[8. Sumário de Processos Criptográficos e Processos de Construção de Algoritmos Criptográficos da Presente Invenção]

Finalmente, os processos criptográficos e os processos de construção de algoritmos criptográficos da presente invenção, que foram descritos acima, serão descritos juntos.

Conforme descrito com referência às figuras 1 e 2, o aparelho de processamento criptográfico da presente invenção tem a seção de processamento criptográfico que realiza um processo de cifra de blocos de chave comum do tipo Feistel de repetição de uma função-F do tipo SP, que realiza um processo de transformação de dados incluindo um processo de transformação não linear e um processo de transformação linear, em uma pluralidade de arredondamentos.

Além disso, a conforme descrito com referência à figura 5 e seguintes, a seção de processamento criptográfico é configurada para realizar

um processo criptográfico ao qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d, que é ajustada a um inteiro que satisfaça d $\geq$ 2 é aplicada e configurada para aplicar seletivamente a uma pluralidade de pelo menos duas ou mais matrizes diferentes aos processos de transformação linear que são realizados nas funções-F em respectivos arredondamentos.

A pluralidade de pelo menos duas ou mais matrizes diferentes é estabelecida de modo a realizar o mecanismo de comutação de matriz de difusão (DSM - Diffusion Switching Mechanism – Mecanismo de Comutação de Difusão), e o processo criptográfico em que a resistência aos ataques diferenciais ou aos ataques lineares é acentuada é realizado pelo uso do DSM. A fim de realizar a acentuação da resistência pelo uso do DSM, seleção e disposição das matrizes são realizadas de acordo com condições específicas.

Em outras palavras, uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado são ajustadas como a pluralidade de matrizes que são aplicadas aos processos de transformação linear que são realizados nas funções-F, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações que correspondem às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseadas em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida. A pluralidade de matrizes diferentes são dispostas repetidamente nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

Mais especificamente, a pluralidade de matrizes diferentes que são utilizadas na seção de processamento criptográfico são uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_k^D]$ é igual ou maior do que três, o número mínimo de

derivações $[B_k^D]$ para todas as linhas de dados sendo selecionados dentre números mínimos de derivações $[B_k^D(s(i))]$ correspondentes às linhas de dados, cada um dos números mínimos de derivações $[B_k^D(s(i))]$ correspondendo à linhas de dados que estão sendo calculadas com base nas matrizes de transformação linear incluídas em k (onde k é um inteiro igual ou maior do que dois) as funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

Alternativamente, a pluralidade de matrizes diferentes que são utilizadas na seção de processamento criptográfico são uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2^L]$ para todas as linhas de dados é igual ou maior do que três, o número mínimo de derivações $[B_2^L]$ para todas as linhas de dados sendo selecionado entre números mínimos de derivações $[B_2^L(s(i))]$ correspondentes à de linhas de dados, cada um dos números mínimos de derivações $[B_2^L(s(i))]$ correspondendo às linhas de dados que estão sendo calculadas com base nas matrizes de transformação linear incluídas em duas funções-F contínuas que são introduzidas em uma linha de dados correspondendo a s(i) na estrutura de Feistel estendida.

Quando a pluralidade de matrizes diferentes são denotadas por n (onde n é um inteiro igual ou maior do que dois) matrizes diferentes, isto é, M_0, M_1, ...M_{n-1}, a seção de processamento criptográfico do aparelho de processamento criptográfico da presente invenção é configurada de modo que as matrizes diferentes M_0, M_1, ...M_{n-1}, são dispostas repetidamente em uma ordem nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida. Como exemplo de uma estrutura de Feistel estendida específica, por exemplo, a estrutura de Feistel estendida do tipo 1 que realiza apenas uma função-F em um arredondamento, que foi descrita com referência às figuras 8 e 10, e a estrutura de Feistel estendida que realiza uma pluralidade de funções-F em paralelo em um arredondamento são

proporcionadas.

Note que a presente invenção inclui o aparelho de processamento criptográfico e um método que realiza o processamento criptográfico ao qual a estrutura de Feistel estendida descrita acima é aplicada e um programa de computador que realiza o processo criptográfico e ainda inclui um aparelho de processamento de informação e método que constrói um algoritmo de processamento criptográfico para realizar o processo criptográfico ao qual a estrutura de Feistel estendida descrita acima é aplicada e um programa de computador.

Um aparelho de processamento de informação, tal como um PC geral, pode ser aplicado como o aparelho de processamento de informação que constrói um algoritmo de processamento criptográfico e o aparelho de processamento de informação tem uma unidade de controle que pode realizar as seguintes etapas de processamento. Em outras palavras, as etapas são:

Uma etapa de determinação de matriz, em uma configuração de algoritmo de processamento criptográfico ao qual uma estrutura de Feistel estendida, tendo o número de linhas de dados: d que é ajustado para um inteiro que satisfaça $d \geq 2$ é aplicada, determinando uma pluralidade de pelo menos duas ou mais matrizes diferentes que devem ser aplicadas aos processos de transformação linear, que são realizados em funções-F, em respectivos arredondamentos; e uma etapa de ajuste de matriz de disposição, repetidamente, na pluralidade de matrizes diferentes, que são determinadas na etapa de determinação de matriz, nas funções-F que são introduzidas nas suas expectativas linhas de dados na estrutura de Feistel estendida.

A etapa de determinação de matriz é realizada como uma etapa de realização de um processo de determinação, como a pluralidade de duas ou mais matrizes diferentes, como matrizes a serem aplicadas, uma pluralidade de matrizes diferentes satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor

predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de dados de verificação de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo as linhas de dados que estão sendo baseadas em matrizes de transformação limiar incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida.

O mecanismo de comutação de matriz de difusão (DSM: Diffusion Switching Mechanism – Mecanismo de Comutação de Difusão) é realizado no processo criptográfico ao qual a estrutura de Feistel estendida que é estabelecida usando esse algoritmo de processamento é aplicada, pelo que o processo criptográfico em que a resistência aos ataques diferenciais ou ataques lineares é acentuada é realizado.

9. Exemplo de Configuração de Aparelho de Processamento Criptográfico

Finalmente, a figura 20 mostra um exemplo de uma configuração de um módulo de CI 300, servindo como o aparelho de processamento criptográfico que realiza o processo criptográfico de acordo com a modalidade descrita acima. O processo descrito acima pode ser realizado, por exemplo, em PCs, cartões de CI, leitoras/impressoras ou vários outros aparelhos de processamento de informação. O módulo de CI 300, mostrado nas figura 20, pode ser configurado nesses vários dispositivos.

Uma CPU (Central Processing Unit - Unidade Central de Processamento) 301, mostrada na figura 20, é um processador que realiza controle de início ou final do processo criptográfico, que realiza controle de transmissão e recepção de dados, que realiza controle de transferência de dados entre respectivas unidades constituintes e que executa outros vários tipos de programas. Uma memória 302 inclui uma ROM (Read Only Memory- Memória Somente para Leitura) que armazena um programa

executado pela CPU 301 ou dados fixos, tais como parâmetros de operação, uma RAM (Random Access Memory - Memória de Acesso Randômico), usada como uma área de armazenamento ou áreas de trabalho para um programa executado em um processo realizado pela CPU 301 e parâmetros que mudam, apropriadamente, no processamento do programa e assim por diante. A memória 302 também pode ser usada como uma área de armazenamento para dados chave necessários para o processo criptográfico, na tabela de transformação (tabela de permutação) aplicada ao processo criptográfico, dados aplicados às matrizes de transformação ou semelhantes. Note que é preferível que a área de armazenamento de dados seja configurada como uma memória tendo uma estrutura resistente à violação.

Uma unidade de processamento criptográfico 303 realiza, por exemplo, um processo criptográfico e um processo de descriptografia de acordo com o algoritmo de processamento de cifras de blocos de chave comum do tipo Feistel estendido, descrito acima. Note que, aqui, um exemplo em que o meio de processamento criptográfico é proporcionado como um módulo separado é mostrado. Contudo, uma configuração pode ser proporcionada em que, em lugar de proporcionar esse módulo de processamento criptográfico independente, por exemplo, um programa de processamento criptográfico é armazenado na ROM em que a CPU 301 lê e executa o programa armazenado na ROM.

Um gerador de número randômicos 304 realiza processo de geração de números randômicos necessários para a geração de chaves que são necessárias para o processo criptográfico ou semelhantes.

Uma unidade de transmissão/recepção 305 é uma unidade de processamento de comunicação de dados que realiza comunicação de dados com o exterior. Por exemplo, a unidade de transmissão/recepção 705 realiza comunicação de dados com um módulo de CI e, tal como uma leitora/impressora, etc.

O módulo de CI 300 realiza, por exemplo, o processo criptográfico do tipo Feistel estendido, em que o número de linhas de dados d é estabelecido para um inteiro que satisfaça $d \geq 2$ de acordo com uma modalidade descrita acima. Matrizes diferentes de transformação linear são estabelecidas como matrizes de transformação linear em funções-F em uma estrutura de Feistel estendida em uma maneira de acordo com a modalidade descrita acima, pelo que o mecanismo de comutação de matriz de difusão (DSM: Diffusion Switching Mechanism - – Mecanismo de Comutação de Difusão) é realizado, de modo que a resistência aos ataques diferenciais ou aos ataques lineares pode ser acentuada.

A presente invenção foi descrita em detalhes com referência à modalidade específica. Contudo, é óbvio que uma pessoa habilitada na técnica poderia fazer modificações ou alternativas na modalidade, sem afastamento do escopo da presente invenção. Em outras palavras, a presente invenção foi divulgada em uma forma de ilustração e não será construída restritivamente. A seção de reivindicações será referida a fim de determinar o escopo da presente invenção.

A Série de processos descritos no relatório pode ser realizada por *hardware* ou *software*, ou uma configuração com combinação de ambos, *hardware* e *software*. Em um caso em que os processos são realizados através de *software*, um programa em que uma seqüência de processos é registrada pode ser instalado em uma memória proporcionada em um computador incorporado em *hardware* dedicado e pode ser executado. Alternativamente, o programa pode ser instalado em um computador para fins gerais capaz de realizar vários processos e pode ser executado.

Por exemplo, o programa pode ser gravado, antecipadamente, em um disco rígido ou ROM (Read ONLY memory – memória somente para leitura), servindo como um meio de gravação. Alternativamente, o programa pode ser armazenado (gravado) temporária ou permanentemente em um meio

de gravação removível, tal como um disco flexível, um CD-ROM (Compact Disc Read Only Memory – Memória Somente para Leitura de Disco Compacto), um disco MO (Magneto óptico), um DVD (Digital Versatile Disc - Disco Versátil Digital), um disco magnético ou uma memória de semicondutor. Esse meio de gravação removível pode ser proporcionado como um *software* em pacote.

Note que o programa pode ser instalado a partir de um meio de gravação removível, conforme descrito acima, em um computador. Além disso, o programa pode ser transferido em um modo sem fio de um site de descarregamento para um computador ou ser transferido por fio para um computador via uma rede, tal como uma LAN (Local Area Network - Rede de Área Local) ou a Internet e o computador pode receber o programa transferido dessa maneira e instalá-lo em um meio de gravação embutido, tal como um disco rígido.

Note que vários processos descritos no relatório podem ser realizados em seqüência na ordem descrita ou também podem ser realizados em paralelo ou individualmente, de acordo com capacidade de processamento de um aparelho que realiza os processos ou em uma base conforme necessário. Além disso, um "Sistema" mencionado no relatório é configurado como um conjunto lógico de uma pluralidade de aparelhos e não está limitado a um sistema em que os aparelhos tendo as respectivas configurações estão contidos no mesmo envoltório.

Aplicabilidade industrial

Conforme descrito acima, de acordo com uma configuração em uma modalidade da presente invenção em um processo de cifra de blocos de chave comum do tipo Feistel, em que funções-F do tipo SPN, incluindo seções de transformação não linear e seções de transformação linear, são realizadas repetidamente em uma pluralidade de arredondamentos, sensor de função de arredondamento às quais uma pluralidade de matrizes diferentes de

transformação linear são aplicadas como estabelecido em uma estrutura de Feistel obtida através da expansão de uma estrutura de Feistel tendo duas linhas de dados, isto é, em uma estrutura de Feistel tendo qualquer número de linhas de dados que seja igual ou maior do que dois, tal como três ou quatro, assim, realizando um mecanismo de comutação de matriz de difusão (DSM), de modo que um algoritmo de cifras de blocos de chave comum pode ser construído e um processo criptográfico pode ser realizado com uma alta resistência à análise linear e à análise diferencial.

De acordo com uma configuração em uma modalidade da presente invenção, uma configuração é proporcionada em que um processo criptográfico ao qual uma estrutura de Feistel estendida tendo o número de linhas de dados: d que é estabelecido em um inteiro que satisfaça $d \geq 2$ é aplicada é realizado e a configuração é proporcionada como uma configuração em que uma pluralidade de pelo menos duas ou mais matrizes diferentes são aplicadas, seletivamente, aos processos de transformação linear realizados em funções-F em respectivos arredondamentos. Uma pluralidade de matrizes diferentes satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado são estabelecidas como uma pluralidade de duas ou mais matriz diferentes, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre inúmeros mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida, assim, realizando o mecanismo de comutação de matriz de difusão (DSM) de modo que o algoritmo de cifra de blocos de chave comum pode ser construída e um processo criptográfico pode ser realizado com alta resistência à análise linear e à análise diferencial.

Além disso, de acordo com uma configuração em uma modalidade da presente invenção, uma configuração é proporcionada em que a (a ≥ 2) tipos de funções-F realizam processos de transformação linear usando uma pluralidade de matrizes diferentes, em que uma estrutura de Feistel estendida (x ≥ 1) que utiliza as funções-F e que tem o número de linhas de dados: d que é estabelecido como d = 2ax e em que um processo criptográfico ao qual a estrutura de Feistel estendida é aplicada é realizado. A configuração é proporcionada como uma configuração e em que, igualmente, x pedaços de cada um dos tipos (os a tipos) de funções-F são realizados em um arredondamento, pelo que o aparelho de processamento criptográfico compacto, em que nenhum circuito inútil é proporcionado, é realizado.

Além disso, de acordo com uma configuração em uma modalidade da presente invenção, uma pluralidade de unidades de realização de função-F São configuradas para realizar processos diferentes de transformação linear, ou usando uma pluralidade de matrizes diferentes e uma configuração é proporcionada em que uma seqüência de utilização da pluralidade de unidades de realização de função-F são configuradas para realizar processos diferentes de transformação linear usando uma pluralidade de matrizes diferentes e uma configuração é proporcionada em que uma seqüência de utilização da pluralidade de unidades de realização de função-F é mudada de acordo com um ajuste, pelo que um aparelho de processamento criptográfico é realizado, o qual pode realizar, seletivamente, qualquer um dos processos criptográficos (a), (b1) e (b2), isto é,

a) um processo criptográfico usando uma estrutura de Feistel tendo o número de linhas de dados d que é ajustado como d = 2;

b1) um processo criptográfico usando uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça d ≥ 2 e em que apenas uma função-F é permitida ser realizada em cada arredondamento; ou

b2) um processo criptográfico que usa uma estrutura de Feistel estendida tendo o número de linhas de dados d que é ajustado para qualquer número que satisfaça $d \geq 2$ e em que uma pluralidade de funções-F são permitidas serem realizadas em paralelo em cada arredondamento.

REIVINDICAÇÕES

1. Aparelho de processamento por criptografia, caracterizado pelo fato de compreender uma seção de processamento por criptografia que realiza um processo de cifra de bloco de chave comum do tipo Feistel de repetição de uma função -F do tipo -SP em uma pluralidade de ciclos, a função -F do tipo -SP realizando um processo de transformação de dados e um processo de transformação linear,

em que a seção de processamento por criptografia

é configurada para realizar um processo criptográfico para o qual uma estrutura de Feistel estendida tendo um número de linhas de dados: d que é estabelecido para um inteiro que satisfaça $d \geq 3$ é aplicada, é configurado para aplicar seletivamente uma pluralidade de pelo menos duas ou mais matrizes diferentes para processos de transformação linear que são realizados em funções-F em respectivos ciclos,

a pluralidade de duas ou mais matrizes diferentes sendo uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondentes às linhas de dados sendo baseado em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida

e é configurado de modo que a pluralidade de matrizes diferentes são dispostas, repetidamente, nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

2. Aparelho de processamento por criptografia de acordo com a reivindicação 1, caracterizado pelo fato de a pluralidade de matrizes diferentes, que são utilizadas na seção de processamento por criptografia,

serem uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_K{}^D]$ para todas as linhas é igual ou maior do que três, o número mínimo de derivações $[B_K{}^D]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[Bk^D(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[Bk^D(s(i))]$ correspondendo às linhas de dados sendo calculado com base em matrizes de transformação linear incluídas em k (onde k é um inteiro igual ou maior do que dois) funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

3. Aparelho de processamento por criptografia de acordo com a reivindicação 1, caracterizado pelo fato de:

a pluralidade de matrizes diferentes, que são utilizadas na seção de processamento por criptografia,

serem uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2{}^D]$ para todas as linhas de dados é igual ou maior do que três, o número mínimo de derivações $[B_2{}^D]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_2{}^D(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[B_2{}^D(s(i))]$ correspondendo às linhas de dados sendo calculado com base nas matrizes de transformação linear incluídas em duas funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

4. Aparelho de processamento por criptografia de acordo com a reivindicação 1, caracterizado pelo fato de

a pluralidade de matrizes diferentes, que são utilizadas na seção de processamento por criptografia,

serem uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_K{}^L]$ para todas as

linhas é igual ou maior do que três, o número mínimo de derivações $[B_K{}^L]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[Bk^L(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[Bk^L(s(i))]$ correspondendo às linhas de dados sendo calculado com base em matrizes de transformação linear incluídas em duas funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

5. Aparelho de processamento por criptografia de acordo com a reivindicação 1, caracterizado pelo fato de,

quando a pluralidade de matrizes diferentes é denotada por n (onde n é um inteiro igual a uma ou mais de duas) matrizes diferentes, isto é,

M0, M1, ···Mn-1,

a seção de processamento por criptografia é

configurada de modo que as matrizes diferentes M0, M1, ···Mn-1, são dispostas, repetidamente, em uma ordem nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

6. Aparelho de processamento por criptografia de acordo com qualquer uma das reivindicações de 1 a 5, caracterizado pelo fato de

a seção de processamento por criptografia ser

configurada para realizar um processo criptográfico ao qual uma estrutura de Feistel estendida que realiza apenas uma função-F em um ciclo é aplicada.

7. Aparelho de processamento por criptografia de acordo com qualquer uma das reivindicações de 1 a 5, caracterizado pelo fato de

a seção de processamento por criptografia ser

configurada para realizar um processo criptográfico ao qual uma estrutura de Feistel estendida que realiza um processo criptográfico ao qual uma estrutura de Feistel estendida, que realiza uma pluralidade de funções-F em paralelo em um ciclo, é aplicada.

8. Aparelho de processamento por criptografia de acordo com qualquer uma das reivindicações de 1 a 5, caracterizado pelo fato de

a seção de processamento por criptografia ser

configurada para realizar, quando a é qualquer inteiro que satisfaz a ≥ 2 e x é qualquer inteiro que satisfaz x ≥ 1, um processo criptográfico ao qual uma estrutura de Feistel estendida que utiliza um tipo de funções-F e que tem o número de linhas de dados: d que é estabelecido como d = 2ax é aplicada, o tipo de a de funções-F realizando processos diferentes de transformação linear usando a pluralidade de matrizes diferentes, e

configurada para realizar igualmente x peças de cada um dos tipos (o tipo a) de funções-F em um ciclo.

9. Aparelho de processamento por criptografia de acordo com a reivindicação 8, caracterizado pelo fato de

a seção de processamento por criptografia ser configurada por incluir:

uma unidade de realização de função-F que realiza funções-F de ax que são realizadas em paralelo em um ciclo; e

uma unidade de controle que realiza controle de entrada/saída de dados para a unidade de realização de função-F.

10. Aparelho de processamento por criptografia de acordo com qualquer uma das reivindicações de 1 a 5, caracterizado pelo fato de

a seção de processamento por criptografia incluir:

uma pluralidade de unidades de realização de função-F que realizam diferentes processos de transformação linear, usando a pluralidade de matrizes diferentes; e

uma unidade de controle que muda uma seqüência de utilização da pluralidade de unidades de realização de função-F de acordo com uma configuração;

em que a unidade de controle

é configurada para realizar, seletivamente, qualquer um dos processos criptográficos (a), (b1) e (b2), isto é,:

(a) um processo criptográfico usando uma estrutura de Feistel tendo o número de linhas de dados d que é estabelecido como d = 2;

(b1) um processo criptográfico que usa uma estrutura de Feistel estendida, tendo o número de linhas de dados d que é estabelecido para qualquer número que satisfaça d ≥ 2 e em que é permitido que apenas uma função-F seja realizada em cada ciclo; ou

(b2) um processo criptográfico que usa uma estrutura de Feistel estendida tendo o número de linhas de dados d que é estabelecido para qualquer número que satisfaça d ≥ 2 e em que é permitido que uma pluralidade de funções-F sejam realizadas em paralelo em cada ciclo.

11. Aparelho de processamento por criptografia de acordo com a reivindicação 10, caracterizado pelo fato de

a unidade de controle ser

configurada para selecionar um modo de processamento a ser realizado de acordo com um comprimento de bit de dados que deve ser submetido a um processo de criptografia ou descriptografia.

12. Método de processamento por criptografia para realizar um processo criptográfico em um aparelho de processamento por criptografia, caracterizado pelo fato de compreender

uma etapa de processamento por criptografia de realização de um processo de cifra de bloco de chave comum do tipo Feistel de repetição de uma função-F do tipo-SP em uma pluralidade de ciclos em uma seção de processamento por criptografia, a função-F do tipo-SP realizando um processo de transformação de dados incluindo um processo de transformação não-linear e um processo de transformação linear;

em que a etapa de processamento por criptografia

é uma etapa de realização de um processo criptográfico ao

qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é estabelecido em um inteiro que satisfaça $d \geq 2$ é aplicada e inclui uma etapa de operação de realização de operações em que uma pluralidade de pelo menos duas ou mais matrizes diferentes são aplicadas seletivamente aos processos de transformação linear que são realizados em funções-F em respectivos ciclos;

em que a pluralidade de matrizes diferentes, que são aplicadas na etapa de operação, é uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas linhas de dados sendo selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear incluídas nas funções-F, que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida, e

em que a etapa de operação

é uma etapa de realização de operações de transformação linear com base na pluralidade de matrizes diferentes nas funções-F que são introduzidas em respectivas linhas de dados na estrutura de Feistel estendida.

13. Método de processamento por criptografia de acordo com a reivindicação 12, caracterizado pelo fato de

a pluralidade de matrizes diferentes

ser uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[Bk^D]$ para todas as linhas de dados é igual ou maior do que três, o número mínimo de derivações $[Bk^D]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_k^D(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[B_k^D(s(i))]$ correspondendo às linhas de

dados sendo calculadas com base nas matrizes de transformação linear incluídas em k (onde k é um inteiro igual ou maior do que dois) funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

14. Método de processamento por criptografia de acordo com a reivindicação 12, caracterizado pelo fato de

a pluralidade de matrizes diferentes

serem uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2^D]$ para todas as linhas é igual ou maior do que três, o número mínimo de derivações $[B_2^D]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_2^D(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[B_2^D(s(i))]$ correspondendo às linhas de dados sendo calculado com base em matrizes de transformação linear incluídas em duas funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

15. Método de processamento por criptografia de acordo com a reivindicação 12, caracterizado pelo fato de

a pluralidade de matrizes diferentes

serem uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações $[B_2^L]$ para todas as linhas é igual ou maior do que três, o número mínimo de derivações $[B_2^D]$ para todas as linhas de dados sendo selecionado dentre números mínimos de derivações $[B_2^L(s(i))]$ correspondendo às linhas de dados, cada um dos números mínimos de derivações $[B_2^L(s(i))]$ correspondendo às linhas de dados sendo calculado com base em matrizes de transformação linear incluídas em duas funções-F contínuas que são introduzidas em uma linha de dados correspondente s(i) na estrutura de Feistel estendida.

16. Método de processamento por criptografia de acordo com

a reivindicação 12, caracterizado pelo fato de, quando a pluralidade de matrizes diferentes é denotada por n (onde n é um inteiro igual a uma ou mais de duas matrizes diferentes, isto é, M0, M1, ···Mn-1, a etapa de operação é uma etapa de execução, repetidamente, das matrizes diferentes M0, M1, ···Mn-1 em uma ordem nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

17. Método de processamento por criptografia de acordo com qualquer uma das reivindicações de 12 a 16, caracterizado pelo fato de

a etapa de processamento por criptografia ser

uma etapa de execução de um processo criptográfico ao qual uma estrutura de Feistel estendida, que executa apenas uma função-F em um ciclo é aplicada.

18. Método de processamento por criptografia de acordo com qualquer uma das reivindicações de 12 a 16, caracterizado pelo fato de

a etapa de processamento por criptografia ser

uma etapa de execução de um processo criptográfico ao qual uma estrutura de Feistel estendida, que executa uma pluralidade de funções-F em um ciclo é aplicada.

19. Método de processamento por criptografia de acordo com qualquer uma das reivindicações de 12 a 16, caracterizado pelo fato de

a etapa de processamento por criptografia ser uma etapa de execução quando a é qualquer inteiro que satisfaça $a \geq 2$ e x é qualquer inteiro que satisfaça $x \geq 1$, um processo criptográfico ao qual uma estrutura de Feistel estendida que utiliza um tipo de funções-F e que tem o número de linhas de dados: d que é estabelecido como $d = 2ax$ é aplicada, o tipo de a de funções-F realizando processos diferentes de transformação linear, usando a pluralidade de matrizes diferentes, e

uma etapa de realização igualmente de x peças de cada um dos tipos (o tipo a) de funções-F em um ciclo.

20. Método de processamento por criptografia de acordo com a reivindicação 19, caracterizado pelo fato de

a etapa de processamento por criptografia ser

uma etapa de realização de um processamento por criptografia, em que uma unidade de execução de função-F que realiza funções-F de ax realizadas em paralelo em um ciclo é aplicada de acordo como o controle realizado por uma unidade de controle que realiza controle de entrada/saída de dados para a unidade de execução de função-F.

21. Método de processamento por criptografia de acordo com qualquer uma das reivindicações de 12 a 16, caracterizado pelo fato de

a etapa de processamento por criptografia ser uma etapa de realização de um processo criptográfico,

usando uma pluralidade de unidades de realização de função-F que realizam diferentes processos de transformação linear, usando a pluralidade de matrizes diferentes, e

pelo uso de uma unidade de controle que muda uma seqüência de utilização da pluralidade de unidades de execução de função-F de acordo com uma configuração,

em que a etapa de processamento por criptografia é uma etapa de acordo com o controle realizado pela unidade de controle, de execução, seletivamente de qualquer um de processos criptográficos (a), (b1) e (b2), isto é,

(a) um processo criptográfico usando uma estrutura de Feistel, tendo o número de linhas distintas d que é estabelecido como $d = 2$;

(b1) um processo criptográfico que usa uma estrutura de Feistel estendida tendo o número de linhas distintas d que é estabelecido para qualquer número que satisfaça $d \geq 2$ e em que é permitido que uma função-F seja realizada em cada ciclo, ou

(b2) um processo criptográfico que usa uma estrutura de

Feistel estendida tendo o número de linhas distintas d que é estabelecido para qualquer número que satisfaça $d \geq 2$ e em que é permitido que uma pluralidade de funções-F seja realizada em paralelo em cada ciclo.

22. Método de processamento por criptografia de acordo com a reivindicação 21, caracterizado pelo fato de a unidade de controle selecionar um modo de processamento a ser realizado de acordo com uma extensão de bit de dados que devem ser submetidos a um processo de criptografia ou descriptografia.

23. Método de construção de algoritmo de processamento por criptografia para construção de um algoritmo de processamento por criptografia em um aparelho de processamento de informação, caracterizado pelo fato de compreender:

uma etapa de determinação de matriz em que, em uma configuração de algoritmo de processamento por criptografia ao qual um estrutura de Feistel estendida, tendo um número de linhas de dados: d que é estabelecido em um inteiro que satisfaça $d \geq 2$ é aplicada, uma unidade de controle proporcionada no aparelho de processamento de informação determina uma pluralidade de pelo menos duas ou mais matrizes diferentes que devem ser aplicadas aos processos de transformação linear realizados em funções-F em respectivos ciclos; e

uma etapa de configuração de matriz em que a unidade de controle dispõe, repetidamente, a pluralidade da matrizes diferentes, que são determinadas na etapa de determinação de matriz, nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida,

em que a etapa de determinação de matriz

é uma etapa de realização de um processo de determinação, como a pluralidade de duas ou mais matrizes diferentes, como matrizes a serem aplicadas, uma pluralidade de matrizes diferentes, satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de

dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações, correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear, incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida.

24. Programa de computador que faz com que o aparelho de processamento por criptografia realize um processamento por criptografia, caracterizado pelo fato de compreender

uma etapa de processamento por criptografia que faz com que uma seção de processamento por criptografia realize um processe de cifra de bloco de chave comum do tipo Feistel de repetição e uma função-F do tipo-SP em uma pluralidade de ciclos, a função-F do tipo-SP realizando um processo de transformação de dados, incluindo um processo de transformação não linear e um processo de transformação linear,

em que a etapa de processamento por criptografia

é uma etapa que faz a seção de processamento por criptografia execute um processo criptográfico ao qual uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é estabelecido em um inteiro que satisfaz $d \geq 2$ é aplicada e inclui uma etapa de operação de realização de operações em que uma pluralidade de pelo menos duas ou mais matrizes diferentes são aplicadas, seletivamente, aos processos de transformação linear que são realizados em funções-F em respectivos ciclos,

em que a pluralidade de matrizes diferentes, que são aplicadas na etapa de operação, é uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números

mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida e em que a etapa de operação é uma etapa de realização de operações de transformação linear com base na pluralidade de matrizes diferentes nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

25. Programa de computador que faz com que o aparelho de processamento de informação construa um algoritmo de processamento por criptografia, caracterizado pelo fato de compreender:

uma etapa de determinação de matriz em que, em uma configuração de algoritmo de processamento por criptografia ao qual um estrutura de Feistel estendida, tendo um número de linhas de dados: d que é estabelecido em um inteiro que satisfaça $d \geq 2$ é aplicada, uma unidade de controle proporcionada no aparelho de processamento de informação determina uma pluralidade de pelo menos duas ou mais matrizes diferentes que devem ser aplicadas aos processos de transformação linear realizados em funções-F em respectivos ciclos; e

uma etapa de configuração de matriz em que a unidade de controle dispõe, repetidamente, a pluralidade da matrizes diferentes, que são determinadas na etapa de determinação de matriz, nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida,

em que a etapa de determinação de matriz

é uma etapa de realização de um processo de determinação, como a pluralidade de duas ou mais matrizes diferentes, como matrizes a serem aplicadas, uma pluralidade de matrizes diferentes, satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de

derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações, correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondendo às linhas de dados sendo baseado em matrizes de transformação linear, incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida.

26. Aparelho de processamento de informação, caracterizado pelo fato de compreender:

uma unidade de memória tangível que armazena dados chave necessários para o processamento criptográfico;

um processador configurado para executar diversos programas e para controlar o início e fim do processamento criptográfico; e

um aparelho de processamento criptográfico configurado para realizar o processamento criptográfico, o aparelho de processamento criptográfico incluindo uma seção de processamento criptográfica que realiza um processo de cifra de bloco de chave comum do tipo Feistel de repetição de uma função -F do tipo -SP em uma pluralidade de ciclos, a função -F do tipo -SP realizando um processo de transformação de dados e um processo de transformação linear, em que a seção de processamento por criptografia:

é configurada para realizar um processo criptográfico para o qual uma estrutura de Feistel estendida tendo um número de linhas de dados d que é estabelecido para um inteiro que satisfaça $d \geq 3$ é aplicada;

é configurada para aplicar seletivamente uma pluralidade de pelo menos duas ou mais matrizes diferentes para processos de transformação linear que são realizados em funções-F em respectivos ciclos, a pluralidade de duas ou mais matrizes diferentes sendo uma pluralidade de matrizes diferentes que satisfazem uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado, o número mínimo de derivações para todas as linhas de dados sendo

selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondentes às linhas de dados sendo baseado em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida;

e é configurada de modo que a pluralidade de matrizes diferentes são dispostas, repetidamente, nas funções-F que são introduzidas nas respectivas linhas de dados na estrutura de Feistel estendida.

FIG. 1

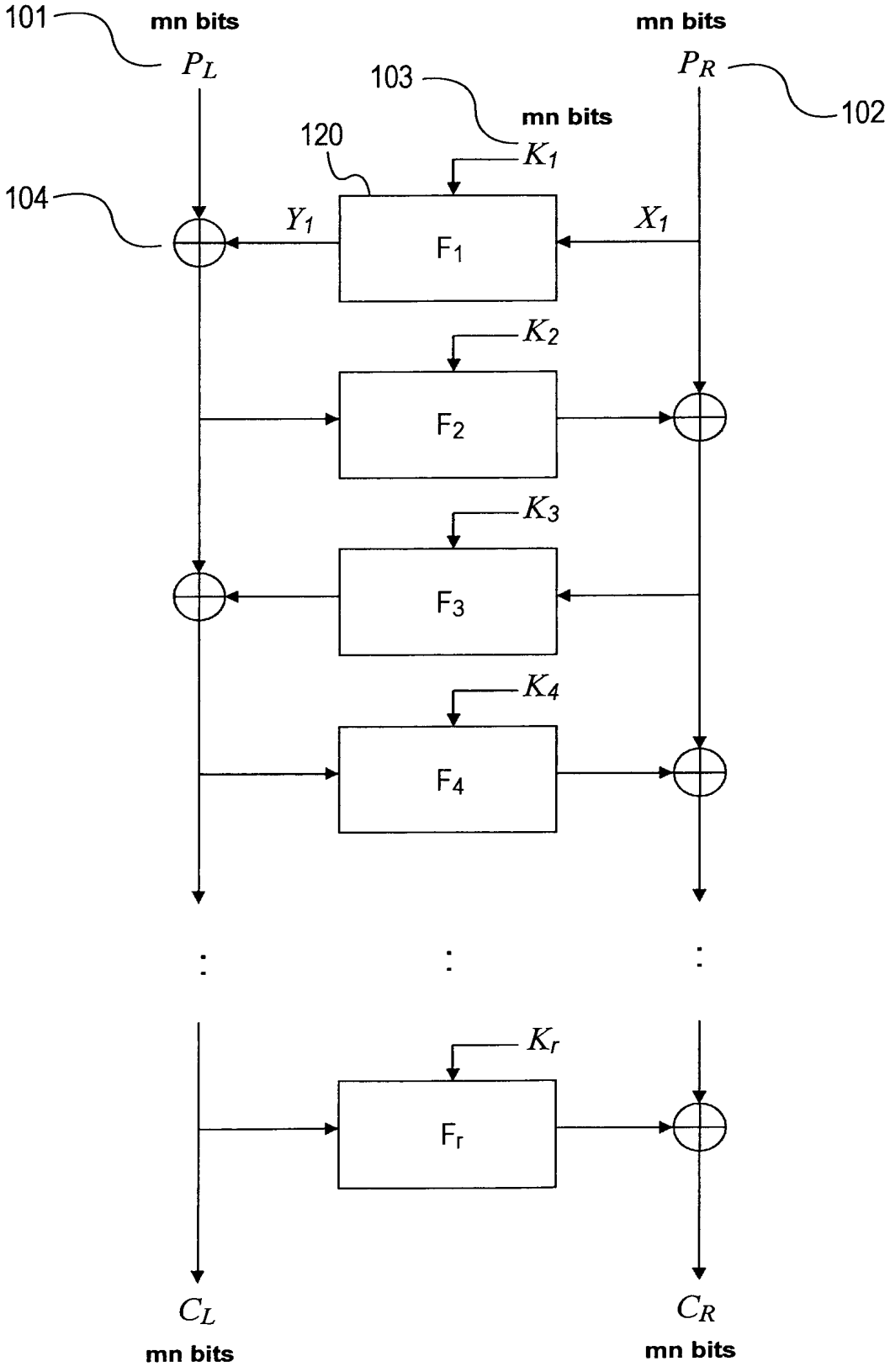

101
mn bits
P_L
103
mn bits
K_1
120
P_R
102
mn bits
104
Y_1
X_1
F_1
K_2
F_2
K_3
F_3
K_4
F_4
K_r
F_r
C_L
mn bits
C_R
mn bits

FIG. 2

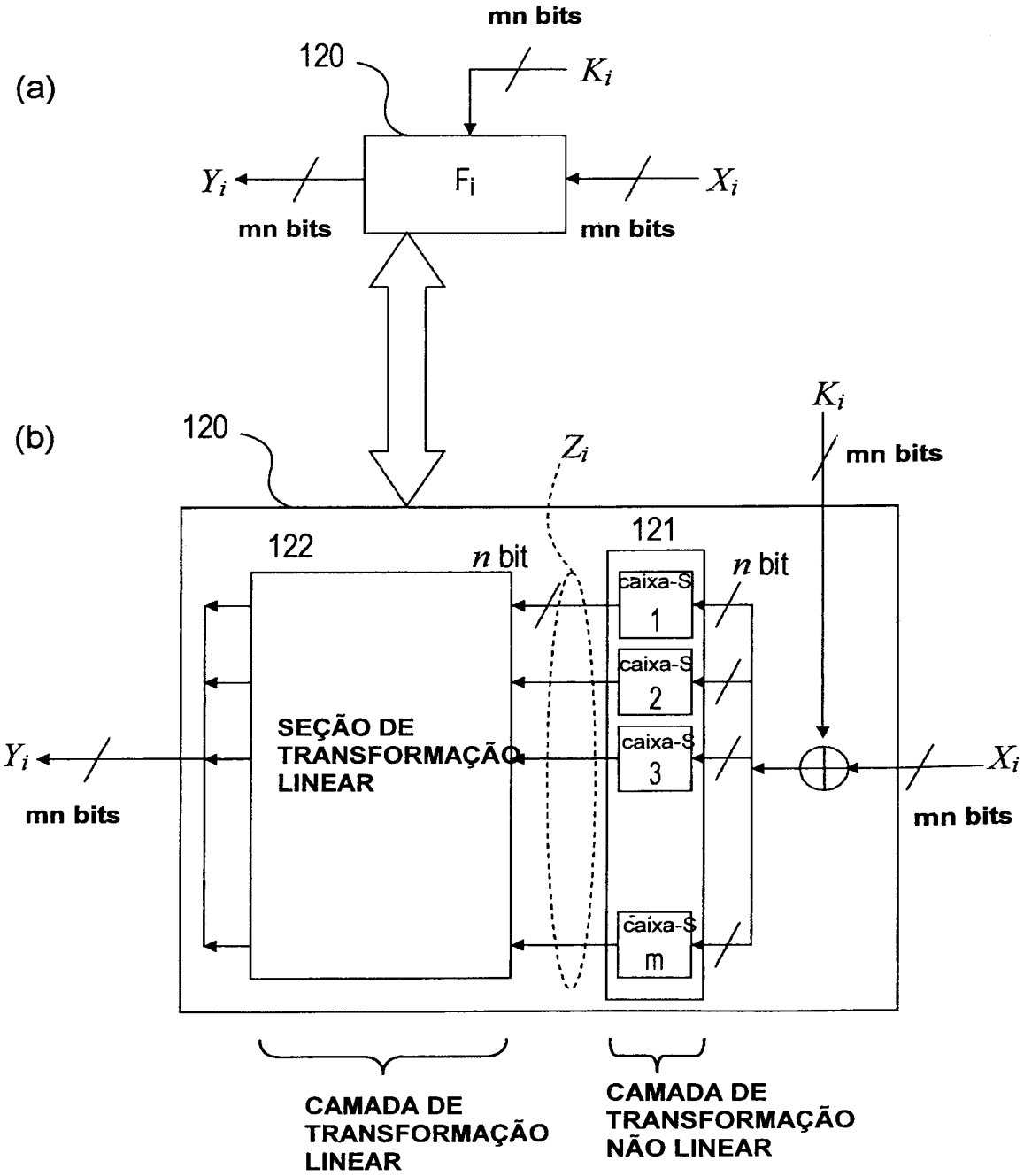

(a)
mn bits
120
K_i
Y_i
Fi
X_i
mn bits
mn bits
(b)
120
Z_i
K_i
mn bits
122
n bit
121
n bit
caixa-S 1
caixa-S 2
caixa-S 3
caixa-S m
SEÇÃO DE TRANSFORMAÇÃO LINEAR
Y_i
mn bits
X_i
mn bits
CAMADA DE TRANSFORMAÇÃO LINEAR
CAMADA DE TRANSFORMAÇÃO NÃO LINEAR

FIG. 3

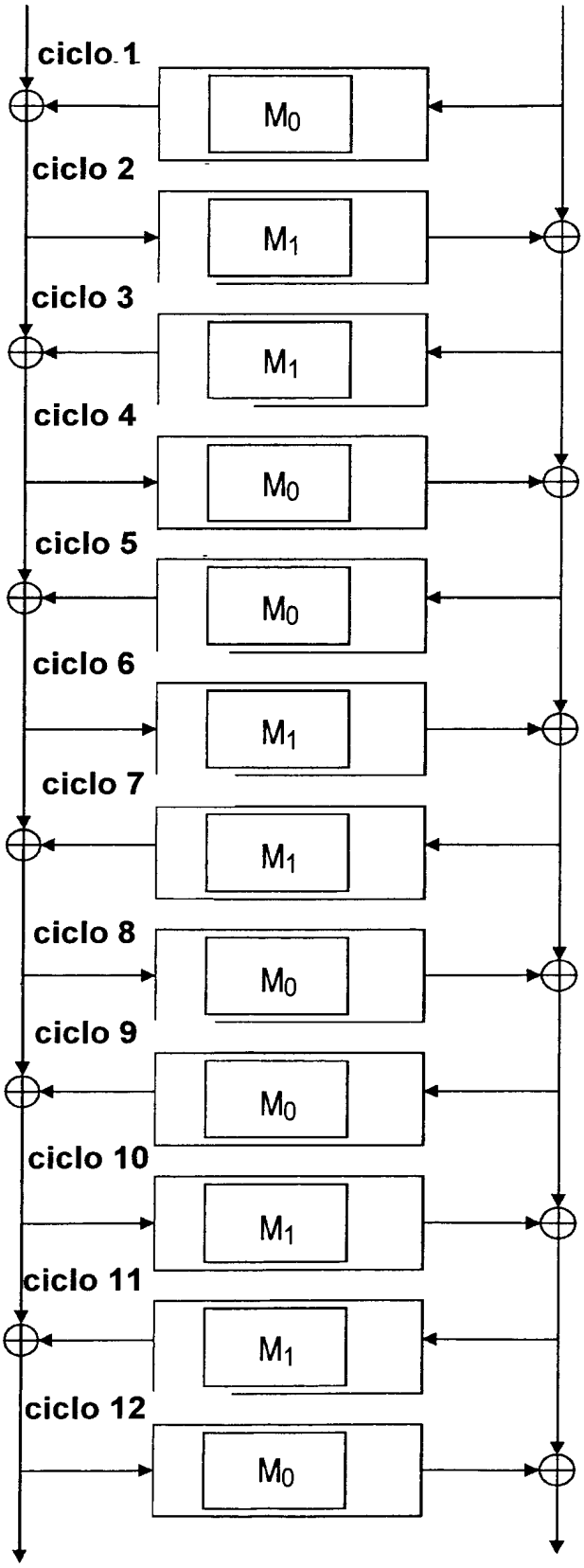

ciclo 1
M0
ciclo 2
M1
ciclo 3
M1
ciclo 4
M0
ciclo 5
M0
ciclo 6
M1
ciclo 7
M1
ciclo 8
M0
ciclo 9
M0
ciclo 10
M1
ciclo 11
M1
ciclo 12
M0

FIG. 4

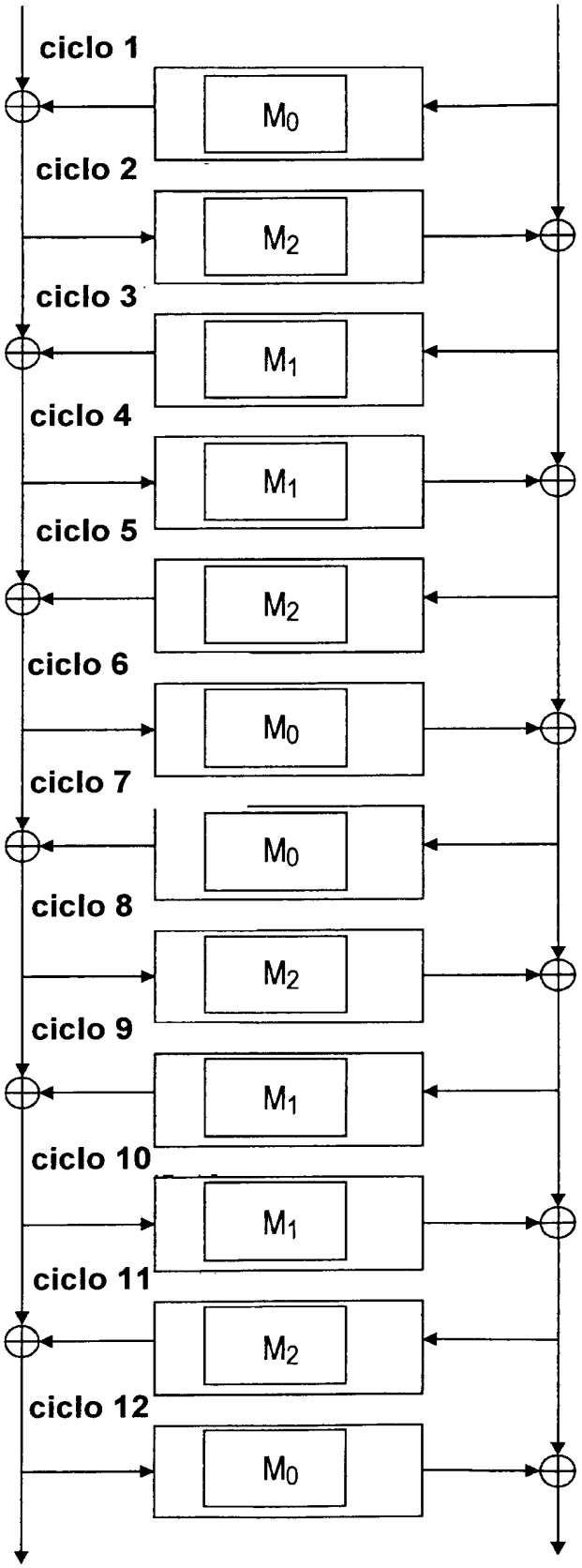

ciclo 1
M0
ciclo 2
M2
ciclo 3
M1
ciclo 4
M1
ciclo 5
M2
ciclo 6
M0
ciclo 7
M0
ciclo 8
M2
ciclo 9
M1
ciclo 10
M1
ciclo 11
M2
ciclo 12
M0

FIG. 5

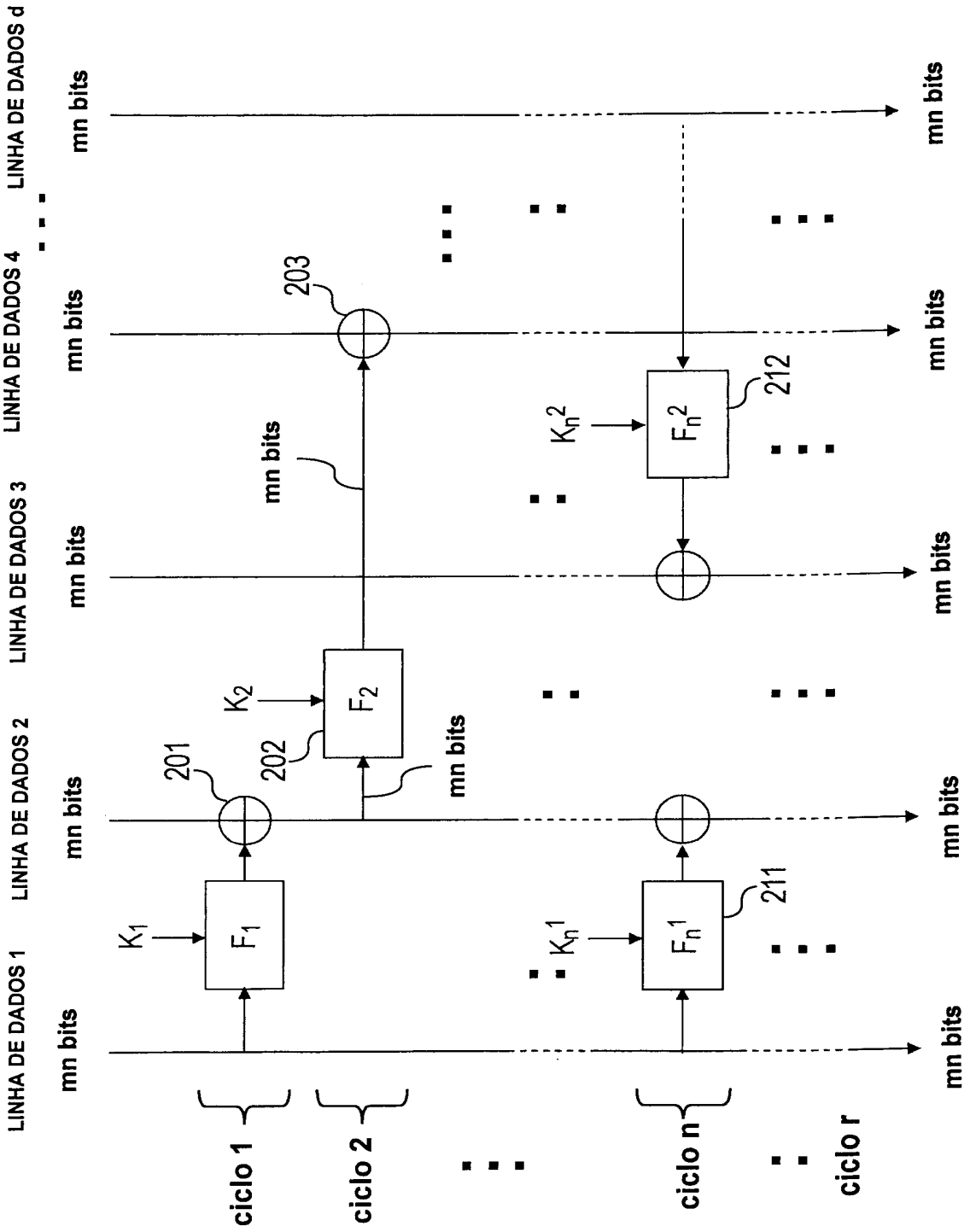

LINHA DE DADOS 1
LINHA DE DADOS 2
LINHA DE DADOS 3
LINHA DE DADOS 4
LINHA DE DADOS d
mn bits
K1
F1
201
K2
202
F2
203
mn bits
Kn1
Fn1
211
Kn2
Fn2
212
ciclo 1
ciclo 2
ciclo n
ciclo r

FIG. 6

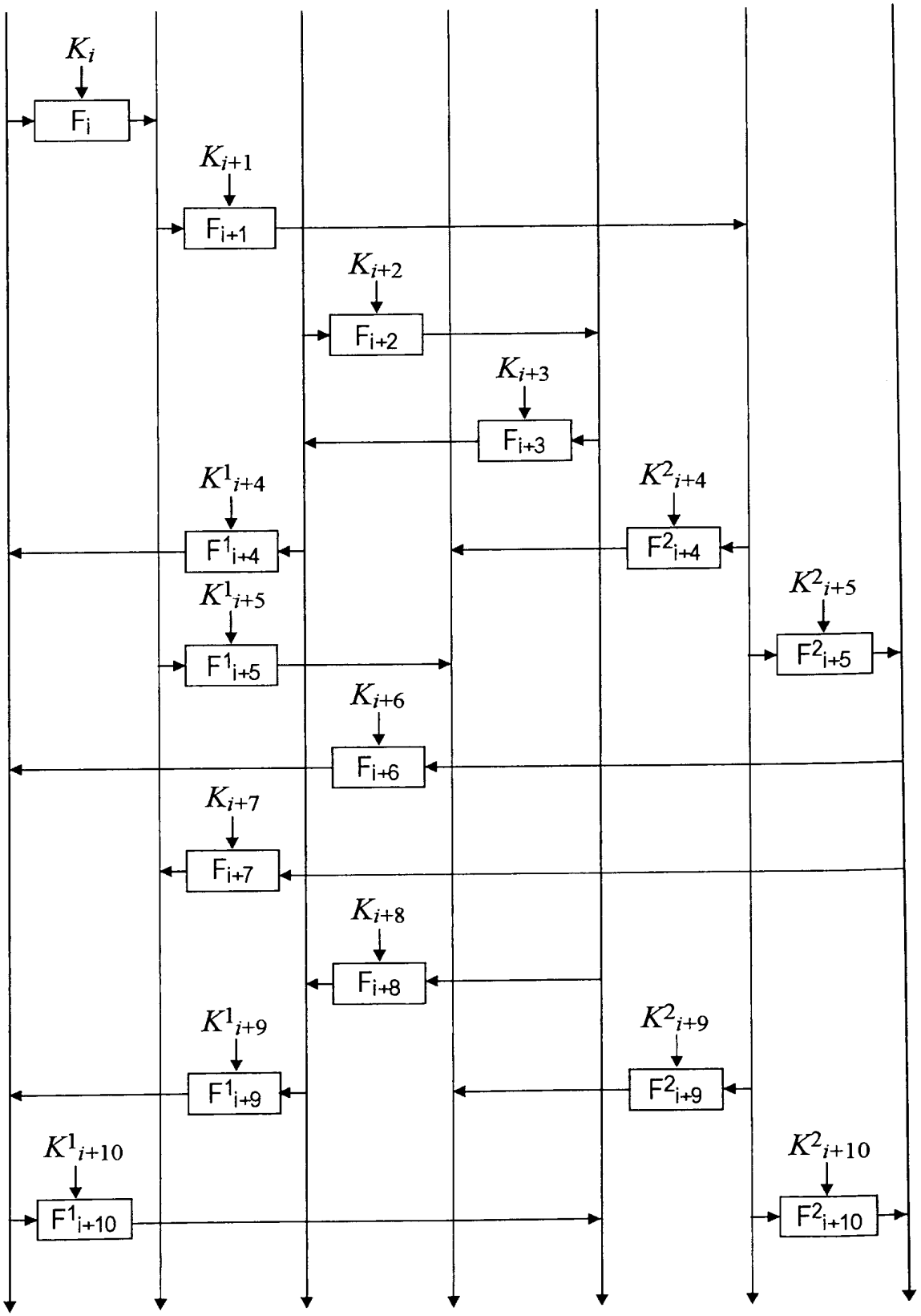

K_i
Fi
K_{i+1}
Fi+1
K_{i+2}
Fi+2
K_{i+3}
Fi+3
K^1_{i+4}
F1i+4
K^2_{i+4}
F2i+4
K^1_{i+5}
F1i+5
K^2_{i+5}
F2i+5
K_{i+6}
Fi+6
K_{i+7}
Fi+7
K_{i+8}
Fi+8
K^1_{i+9}
F1i+9
K^2_{i+9}
F2i+9
K^1_{i+10}
F1i+10
K^2_{i+10}
F2i+10

FIG. 7

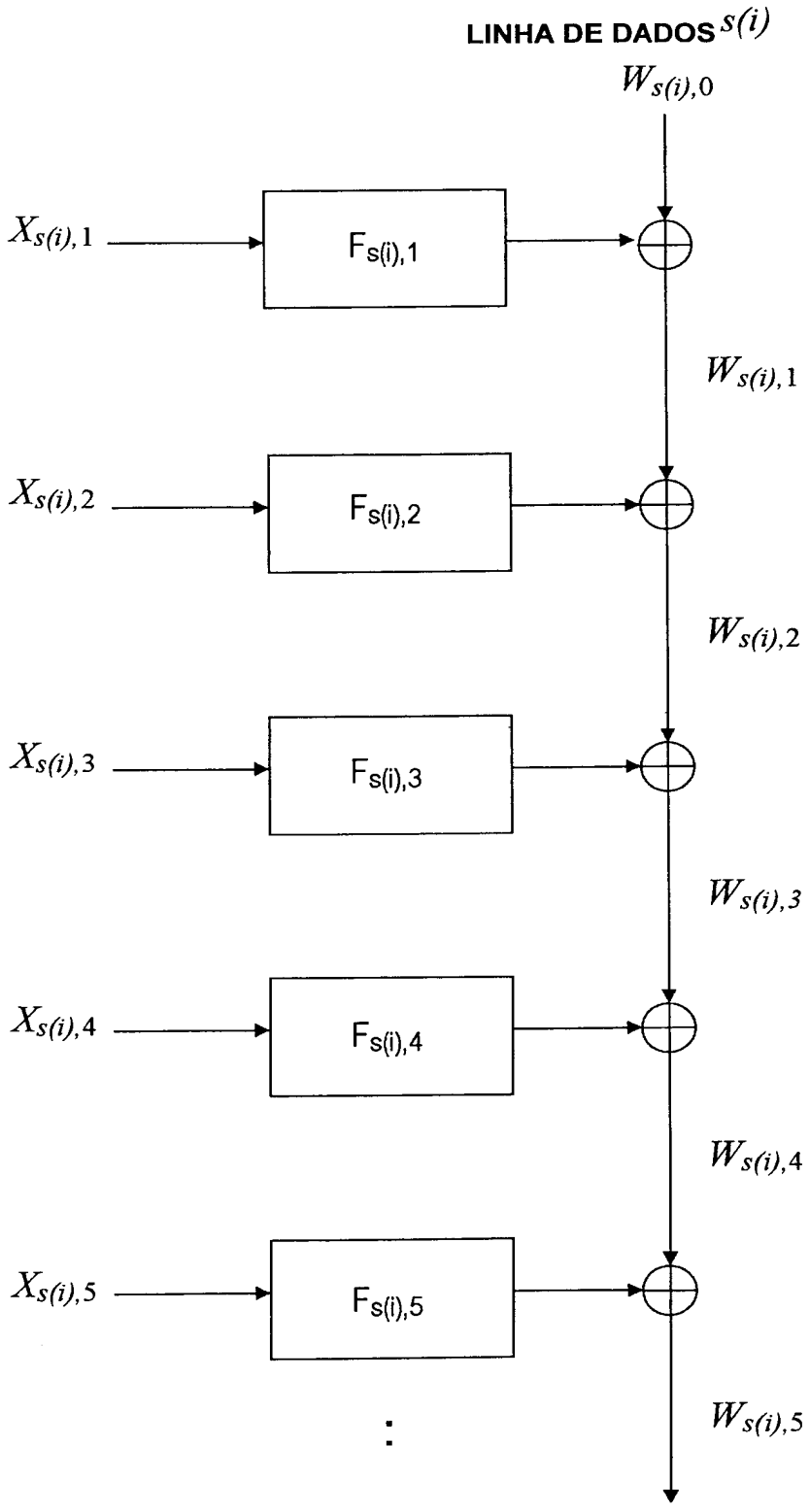

LINHA DE DADOS $s(i)$
$W_{s(i),0}$
$X_{s(i),1}$
$F_{s(i),1}$
$W_{s(i),1}$
$X_{s(i),2}$
$F_{s(i),2}$
$W_{s(i),2}$
$X_{s(i),3}$
$F_{s(i),3}$
$W_{s(i),3}$
$X_{s(i),4}$
$F_{s(i),4}$
$W_{s(i),4}$
$X_{s(i),5}$
$F_{s(i),5}$
$W_{s(i),5}$

FIG. 8

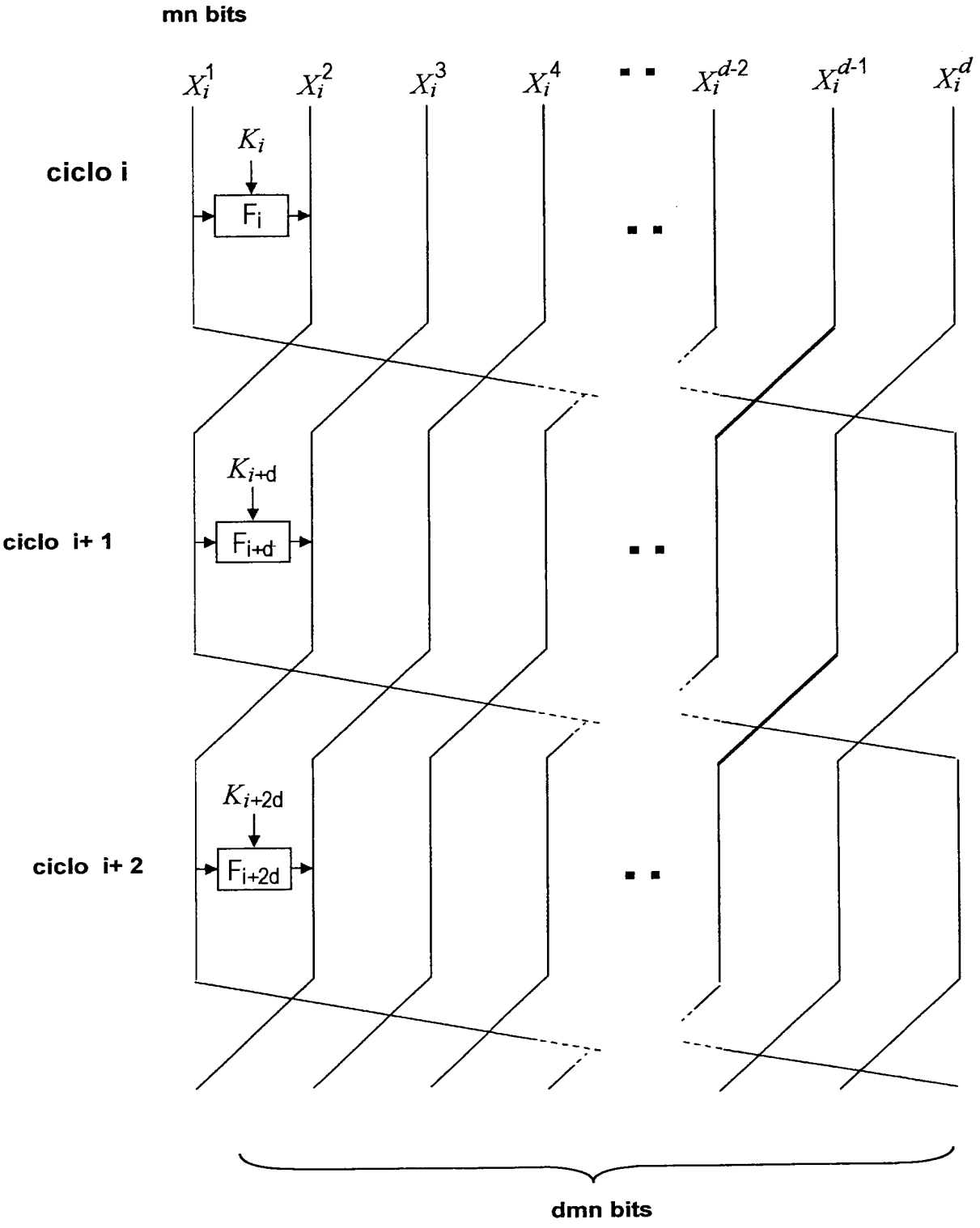

mn bits
X_i^1
X_i^2
X_i^3
X_i^4
X_i^{d-2}
X_i^{d-1}
X_i^d
ciclo i
K_i
F_i
ciclo i+ 1
K_{i+d}
F_{i+d}
ciclo i+ 2
K_{i+2d}
F_{i+2d}
dmn bits

FIG. 9

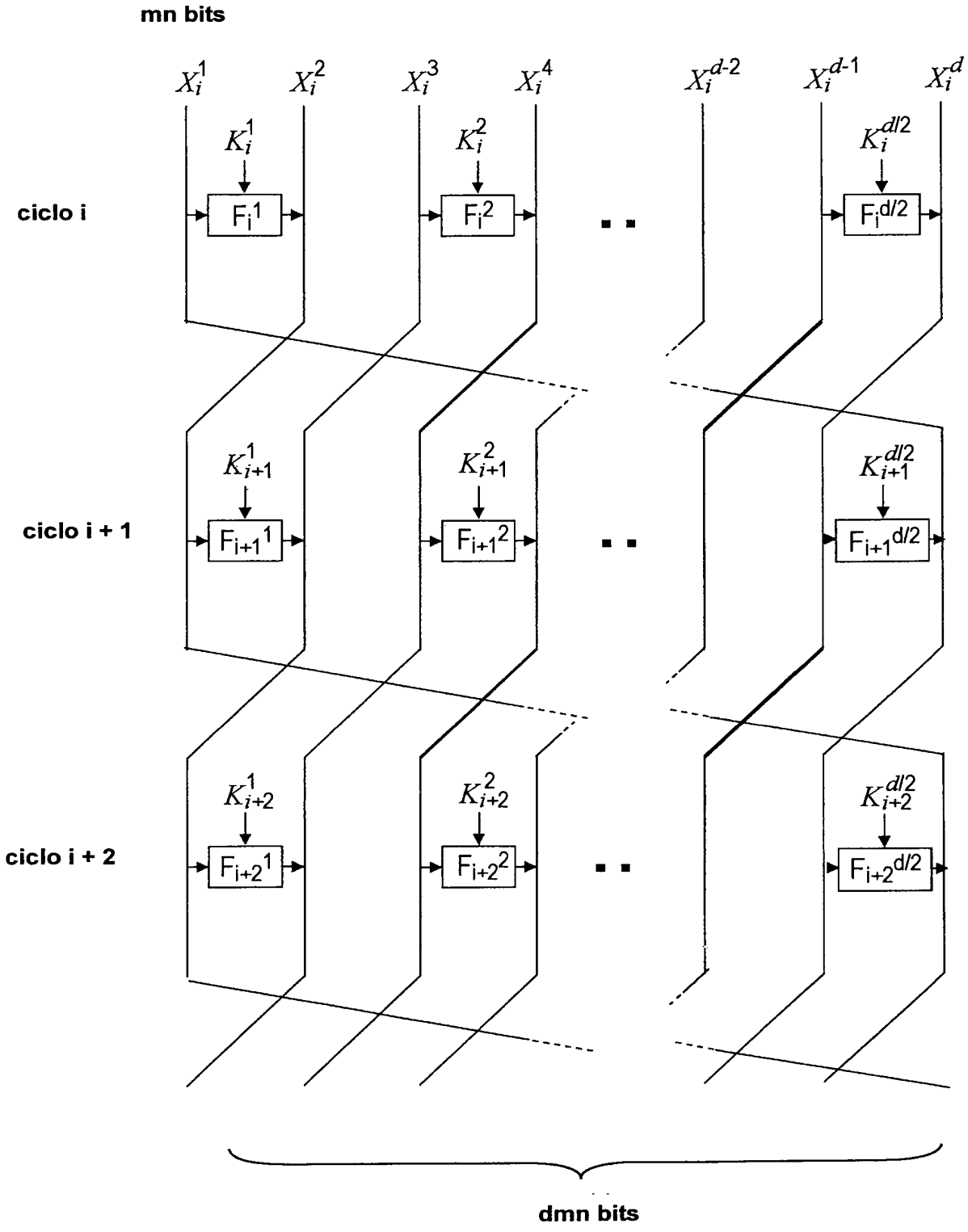

mn bits
X_i^1 X_i^2 X_i^3 X_i^4 X_i^{d-2} X_i^{d-1} X_i^d
K_i^1 K_i^2 K_i^{dl2}
ciclo i
F_i^1 F_i^2 $F_i^{d/2}$
K_{i+1}^1 K_{i+1}^2 K_{i+1}^{dl2}
ciclo i + 1
F_{i+1}^1 F_{i+1}^2 $F_{i+1}^{d/2}$
K_{i+2}^1 K_{i+2}^2 K_{i+2}^{dl2}
ciclo i + 2
F_{i+2}^1 F_{i+2}^2 $F_{i+2}^{d/2}$
dmn bits

FIG. 10

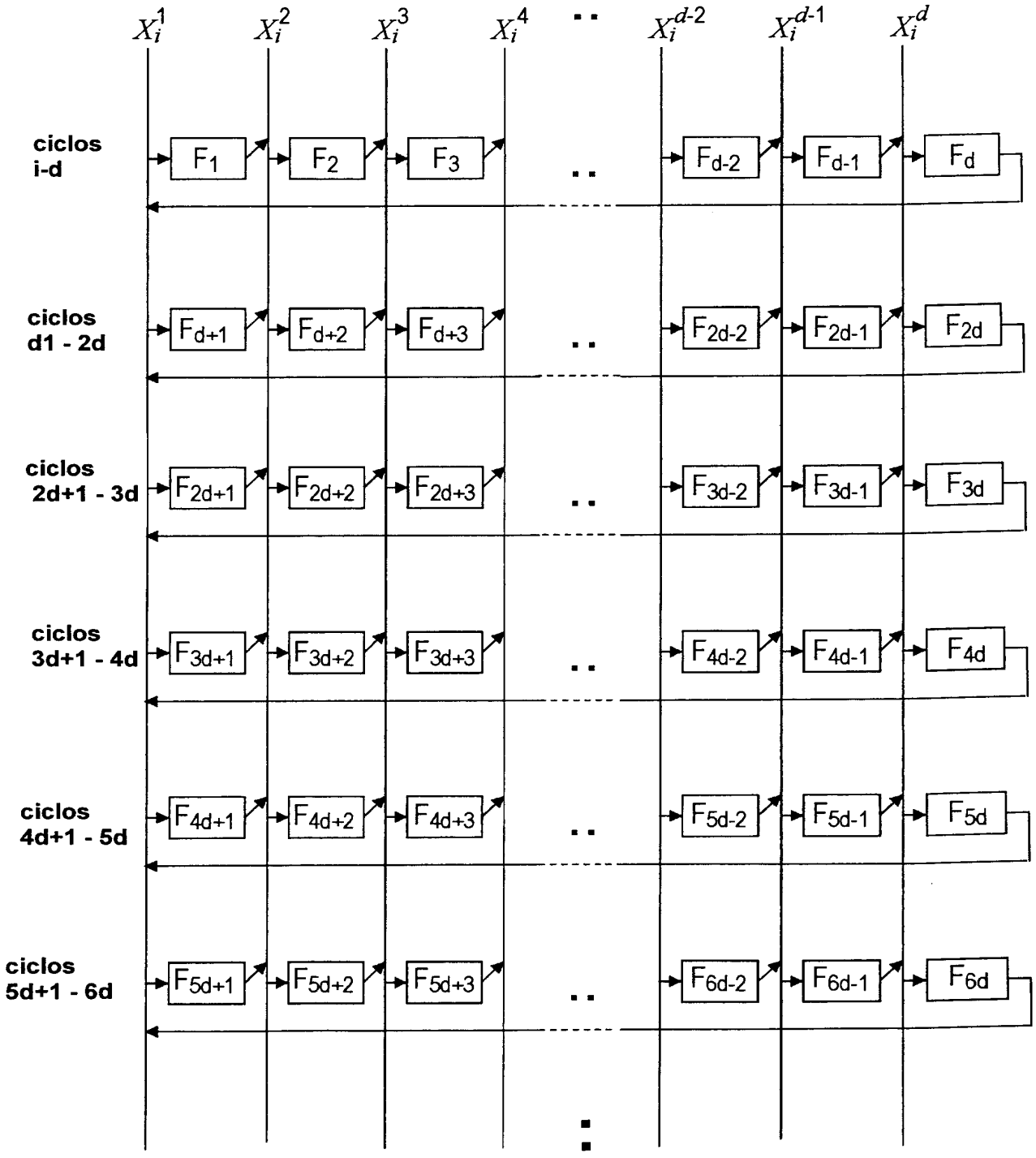

X_i^1
X_i^2
X_i^3
X_i^4
X_i^{d-2}
X_i^{d-1}
X_i^d
ciclos i-d
F1
F2
F3
Fd-2
Fd-1
Fd
ciclos d1 - 2d
Fd+1
Fd+2
Fd+3
F2d-2
F2d-1
F2d
ciclos 2d+1 - 3d
F2d+1
F2d+2
F2d+3
F3d-2
F3d-1
F3d
ciclos 3d+1 - 4d
F3d+1
F3d+2
F3d+3
F4d-2
F4d-1
F4d
ciclos 4d+1 - 5d
F4d+1
F4d+2
F4d+3
F5d-2
F5d-1
F5d
ciclos 5d+1 - 6d
F5d+1
F5d+2
F5d+3
F6d-2
F6d-1
F6d

FIG. 11

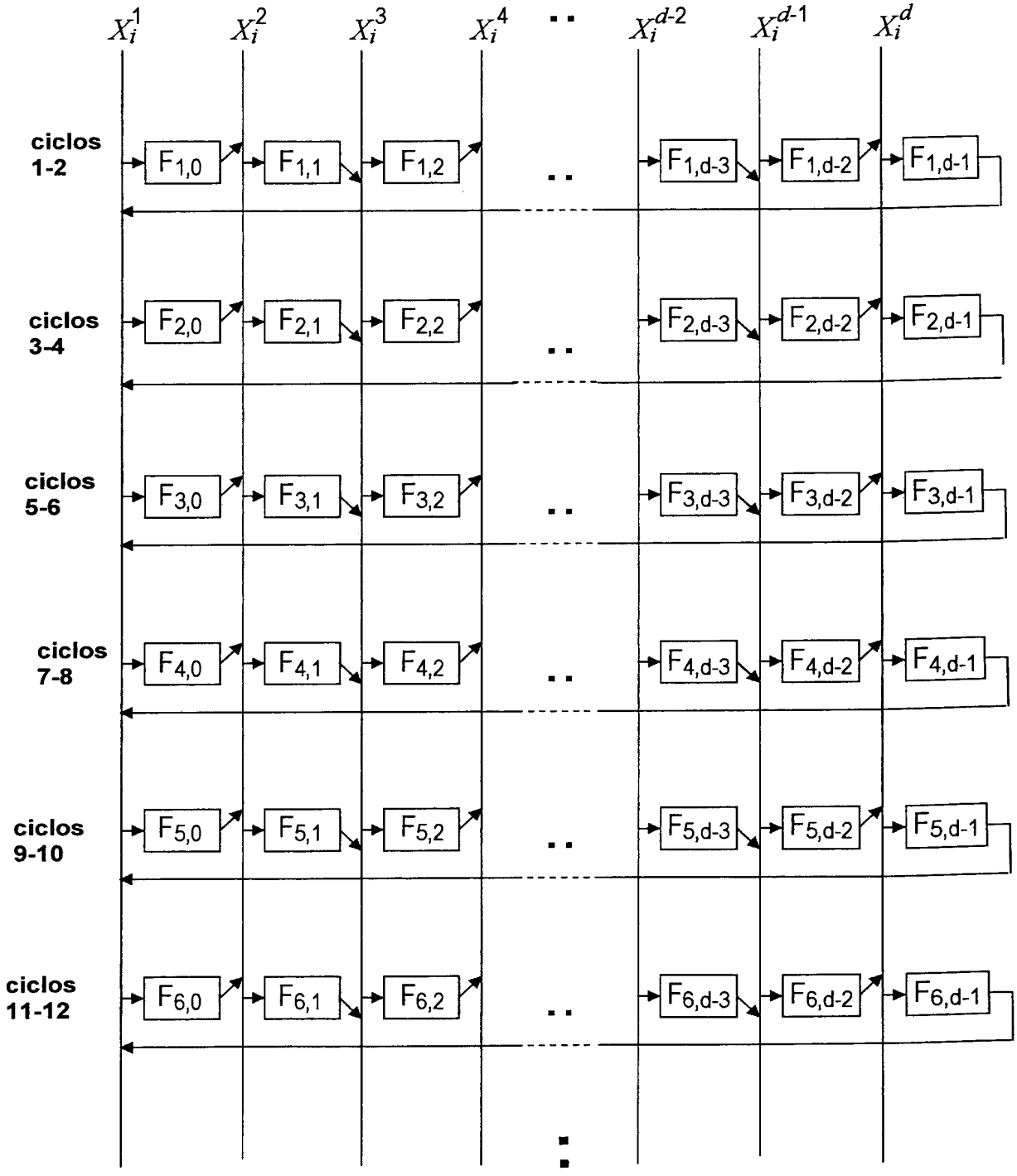

X_i^1
X_i^2
X_i^3
X_i^4
X_i^{d-2}
X_i^{d-1}
X_i^d
ciclos 1-2
ciclos 3-4
ciclos 5-6
ciclos 7-8
ciclos 9-10
ciclos 11-12
F1,0
F1,1
F1,2
F1,d-3
F1,d-2
F1,d-1
F2,0
F2,1
F2,2
F2,d-3
F2,d-2
F2,d-1
F3,0
F3,1
F3,2
F3,d-3
F3,d-2
F3,d-1
F4,0
F4,1
F4,2
F4,d-3
F4,d-2
F4,d-1
F5,0
F5,1
F5,2
F5,d-3
F5,d-2
F5,d-1
F6,0
F6,1
F6,2
F6,d-3
F6,d-2
F6,d-1

FIG. 12

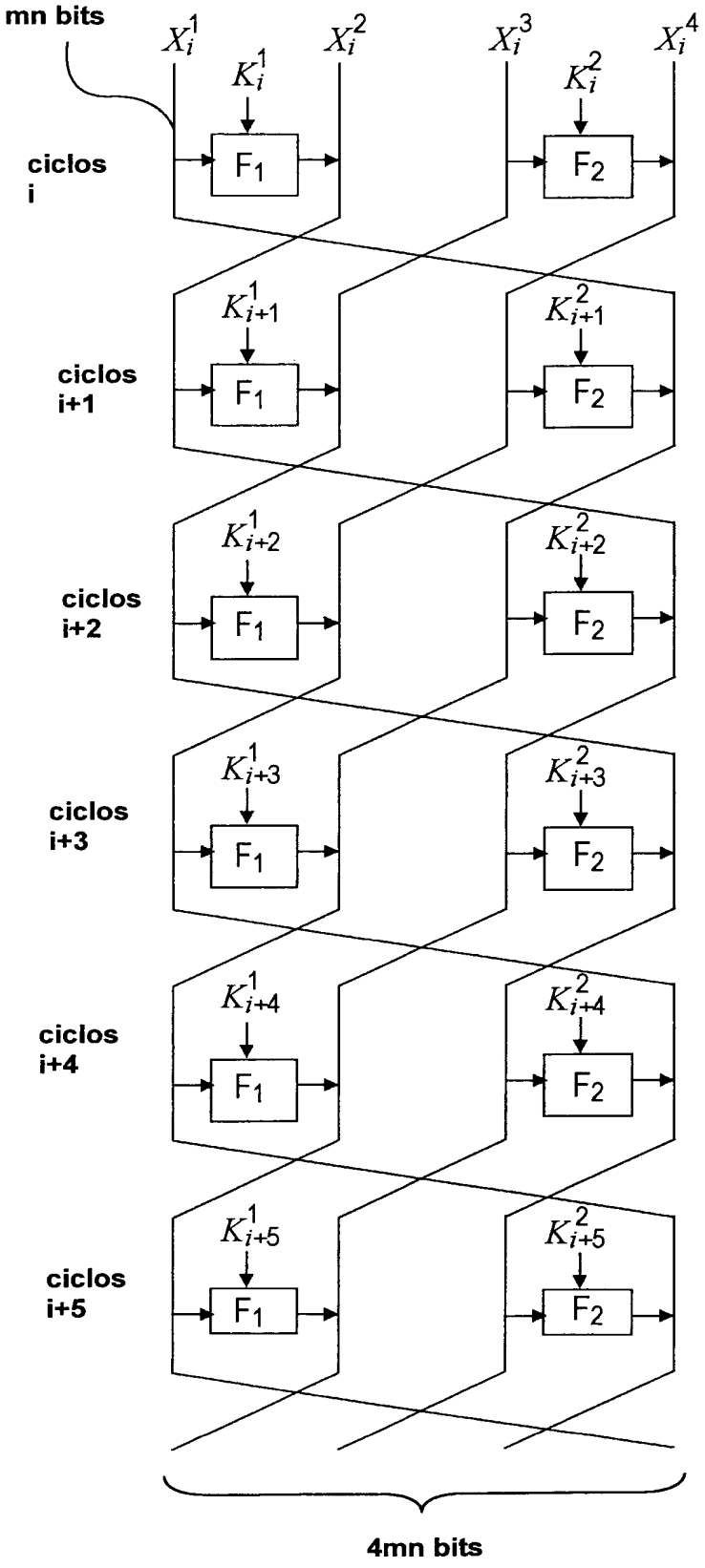

mn bits
X_i^1
X_i^2
X_i^3
X_i^4
K_i^1
K_i^2
ciclos i
F1
F2
K_{i+1}^1
K_{i+1}^2
ciclos i+1
K_{i+2}^1
K_{i+2}^2
ciclos i+2
K_{i+3}^1
K_{i+3}^2
ciclos i+3
K_{i+4}^1
K_{i+4}^2
ciclos i+4
K_{i+5}^1
K_{i+5}^2
ciclos i+5
4mn bits

FIG. 13

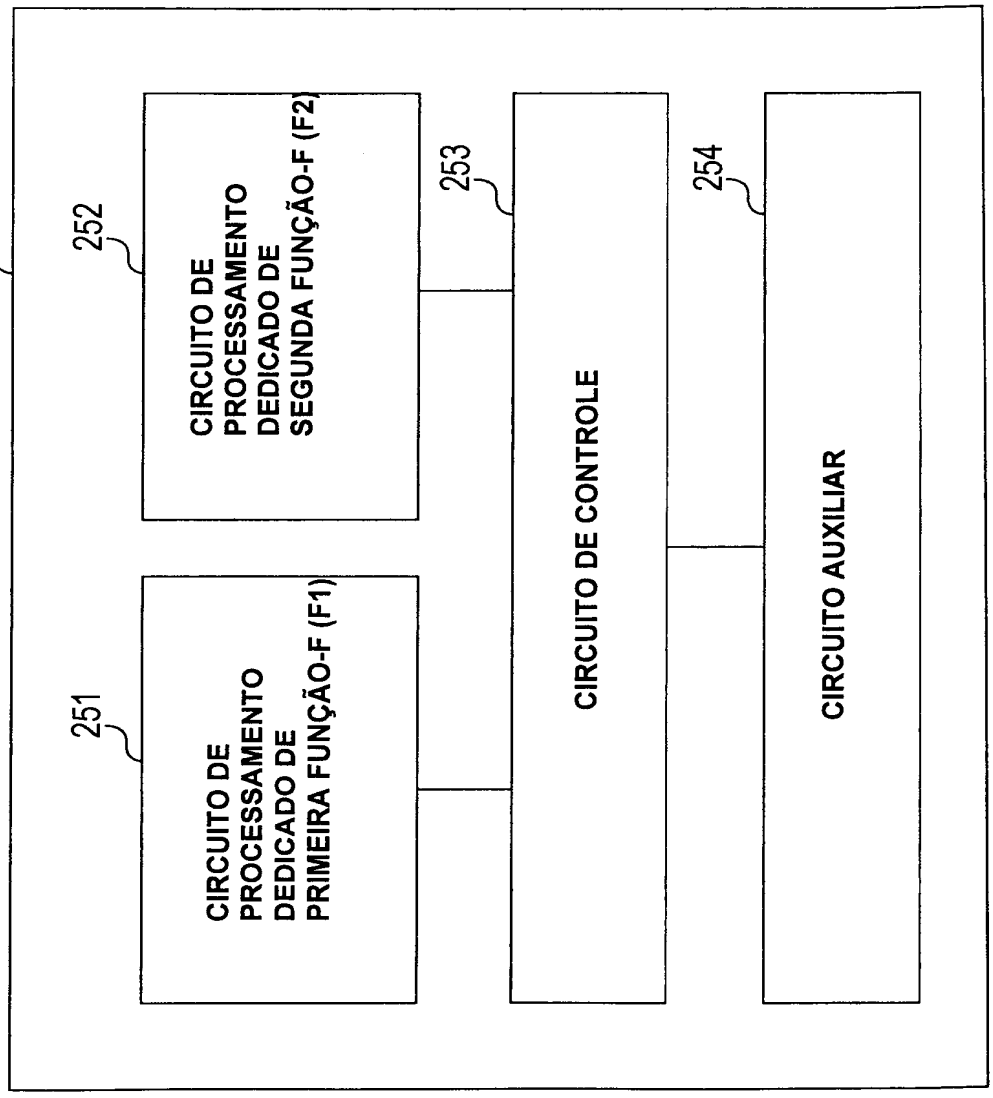

250
251
CIRCUITO DE PROCESSAMENTO DEDICADO DE PRIMEIRA FUNÇÃO-F (F1)
252
CIRCUITO DE PROCESSAMENTO DEDICADO DE SEGUNDA FUNÇÃO-F (F2)
253
CIRCUITO DE CONTROLE
254
CIRCUITO AUXILIAR

FIG. 14

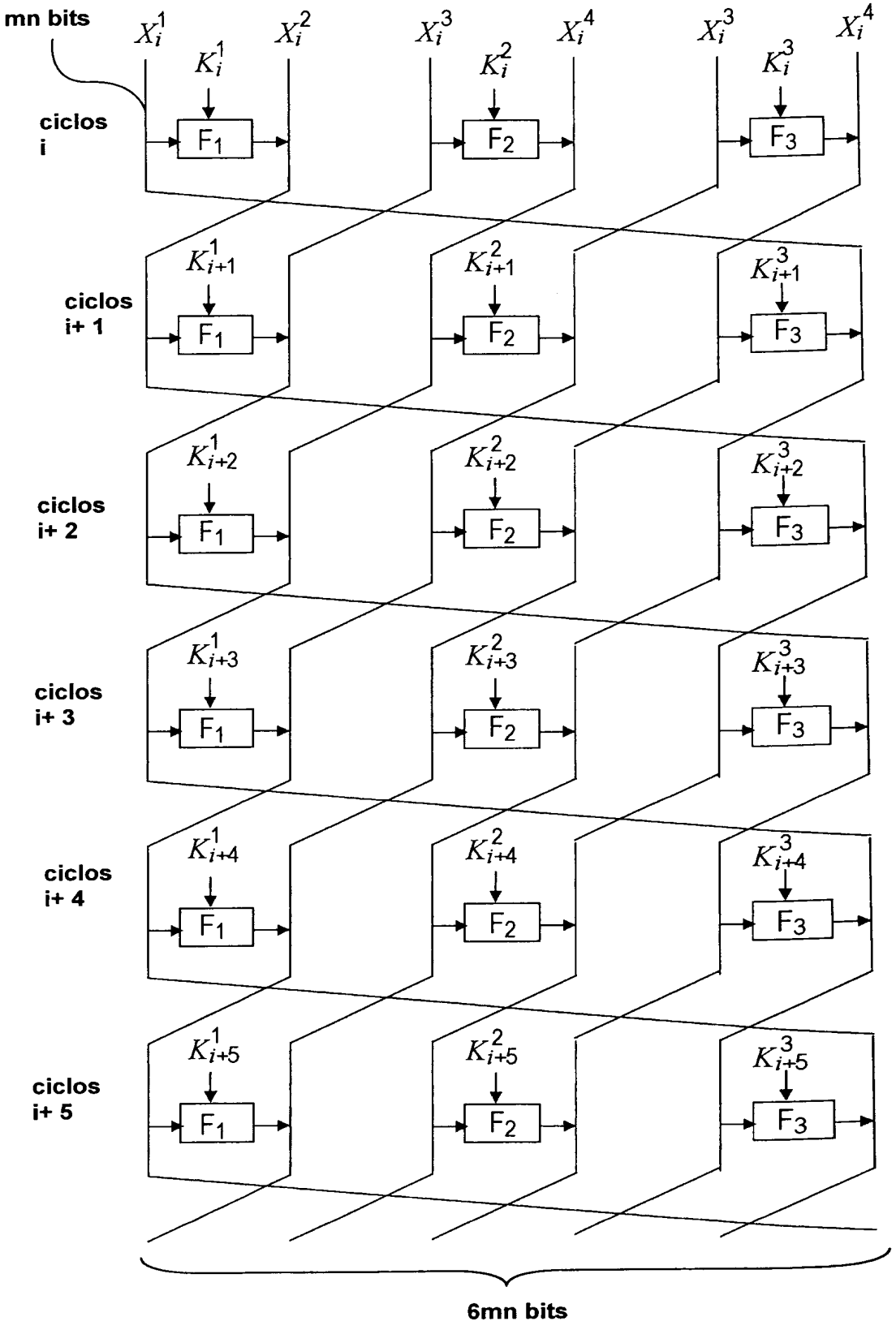

mn bits
X_i^1
X_i^2
X_i^3
X_i^4
X_i^3
X_i^4
K_i^1
K_i^2
K_i^3
ciclos i
ciclos i+ 1
ciclos i+ 2
ciclos i+ 3
ciclos i+ 4
ciclos i+ 5
K_{i+1}^1
K_{i+1}^2
K_{i+1}^3
K_{i+2}^1
K_{i+2}^2
K_{i+2}^3
K_{i+3}^1
K_{i+3}^2
K_{i+3}^3
K_{i+4}^1
K_{i+4}^2
K_{i+4}^3
K_{i+5}^1
K_{i+5}^2
K_{i+5}^3
F1
F2
F3
6mn bits

FIG. 15

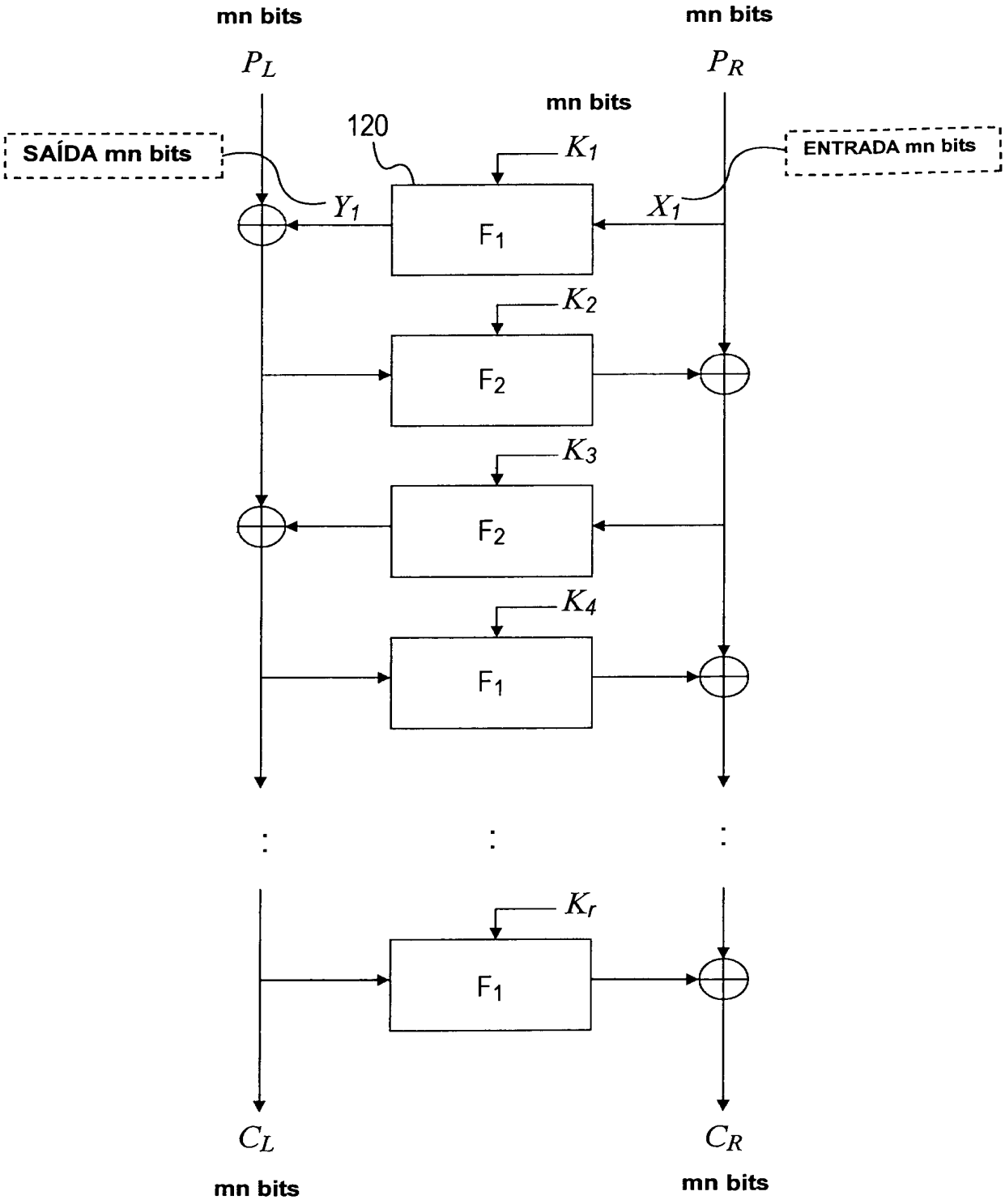

mn bits
P_L
mn bits
P_R
mn bits
120
K_1
SAÍDA mn bits
ENTRADA mn bits
Y_1
X_1
F1
K_2
F2
K_3
F2
K_4
F1
K_r
F1
C_L
mn bits
C_R
mn bits

FIG. 16

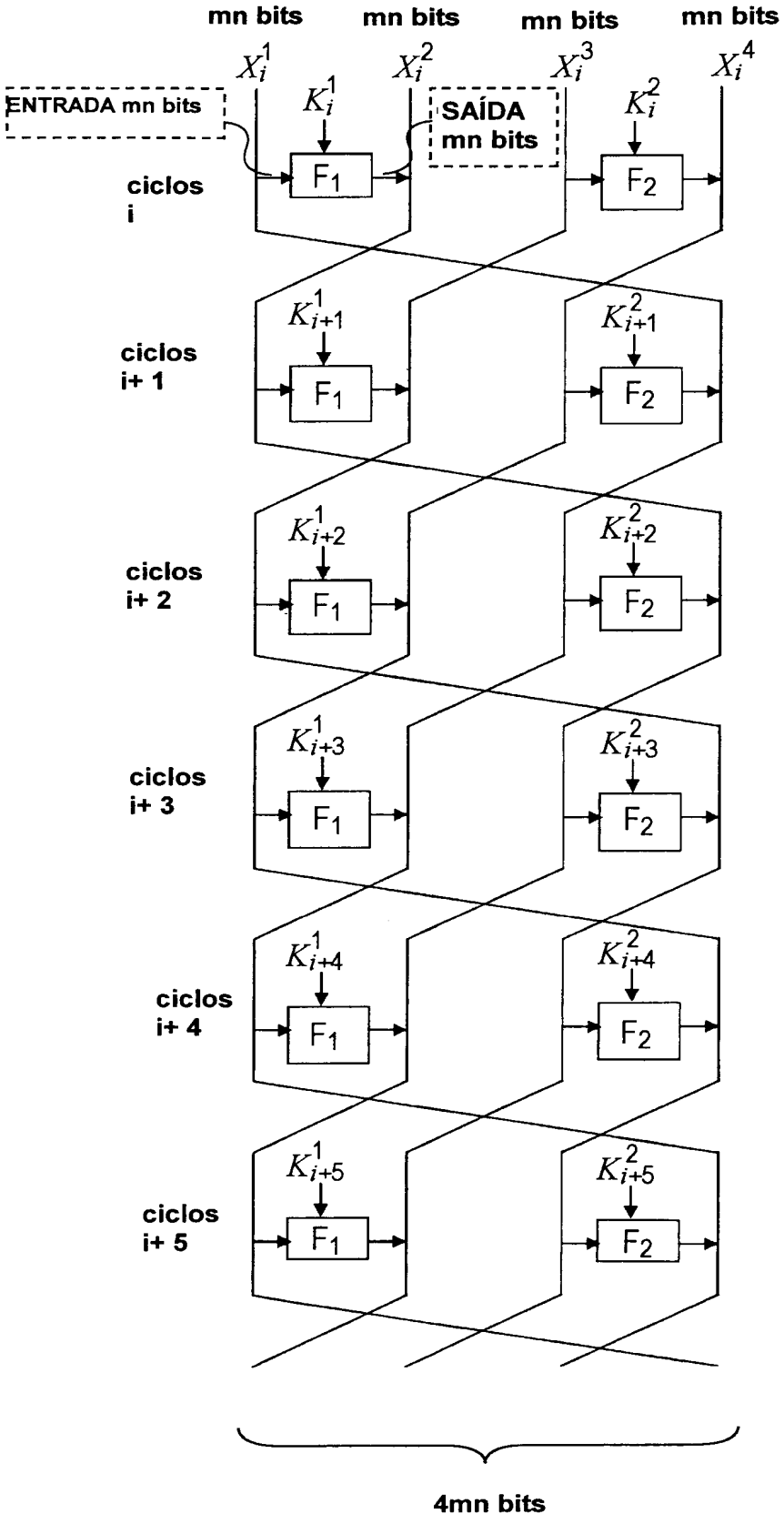

mn bits
mn bits
mn bits
mn bits
X_i^1
X_i^2
X_i^3
X_i^4
ENTRADA mn bits
SAÍDA mn bits
K_i^1
K_i^2
F1
F2
ciclos i
ciclos i+ 1
ciclos i+ 2
ciclos i+ 3
ciclos i+ 4
ciclos i+ 5
K_{i+1}^1
K_{i+1}^2
K_{i+2}^1
K_{i+2}^2
K_{i+3}^1
K_{i+3}^2
K_{i+4}^1
K_{i+4}^2
K_{i+5}^1
K_{i+5}^2
4mn bits

FIG. 17

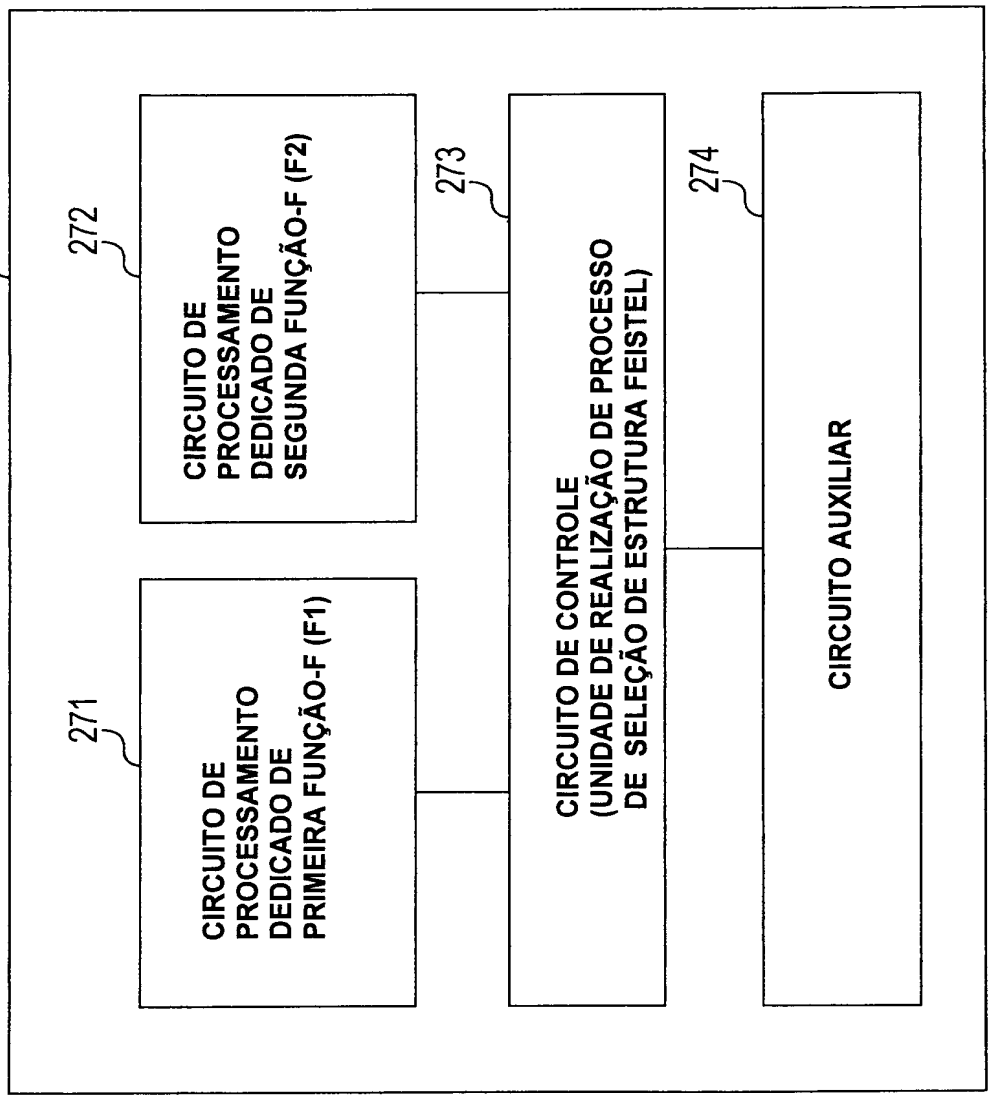

270
271
CIRCUITO DE PROCESSAMENTO DEDICADO DE PRIMEIRA FUNÇÃO-F (F1)
272
CIRCUITO DE PROCESSAMENTO DEDICADO DE SEGUNDA FUNÇÃO-F (F2)
273
CIRCUITO DE CONTROLE (UNIDADE DE REALIZAÇÃO DE PROCESSO DE SELEÇÃO DE ESTRUTURA FEISTEL)
274
CIRCUITO AUXILIAR

FIG. 18

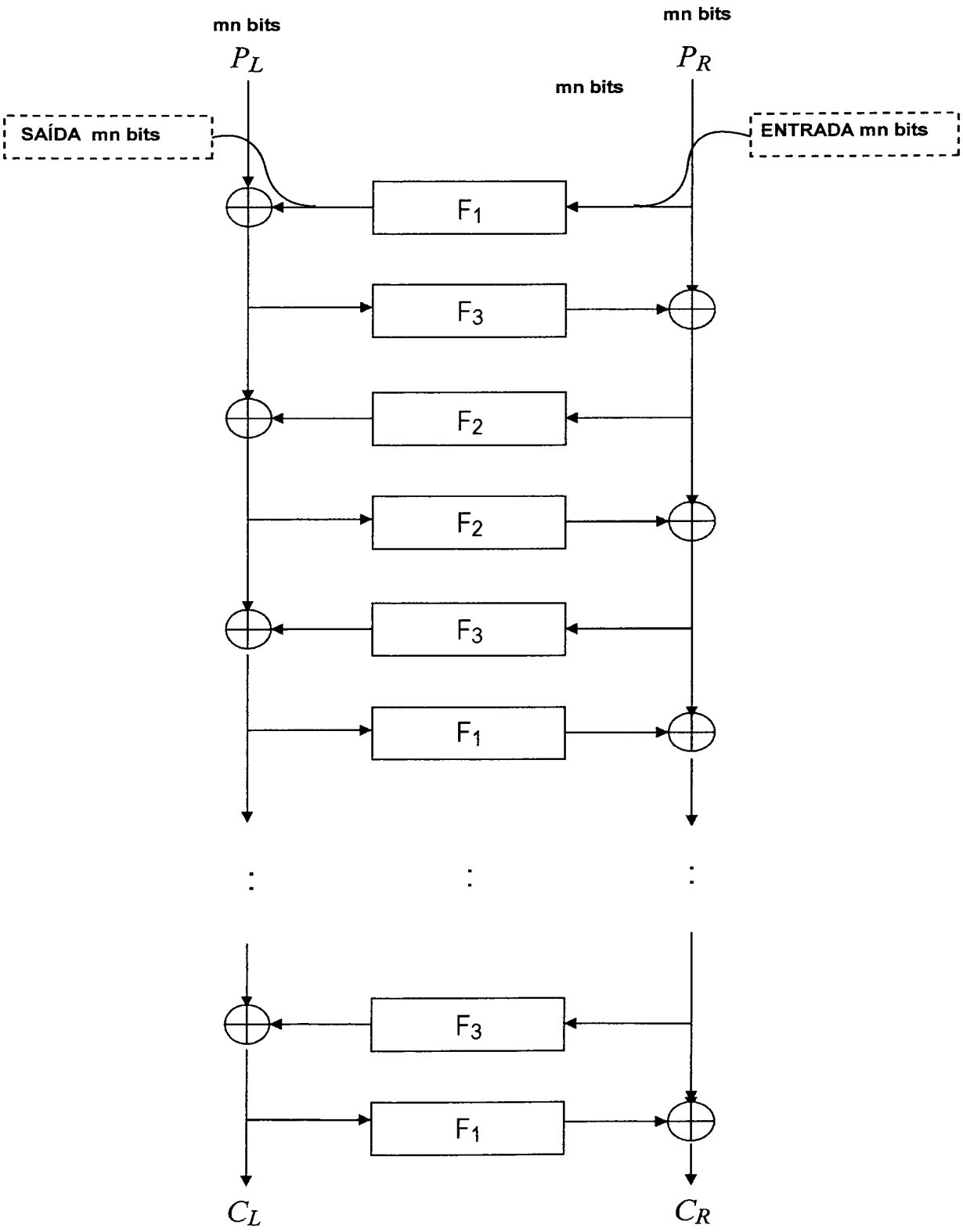

mn bits
P_L
mn bits
P_R
mn bits
SAÍDA mn bits
ENTRADA mn bits
F1
F3
F2
F2
F3
F1
F3
F1
C_L
C_R

FIG. 19

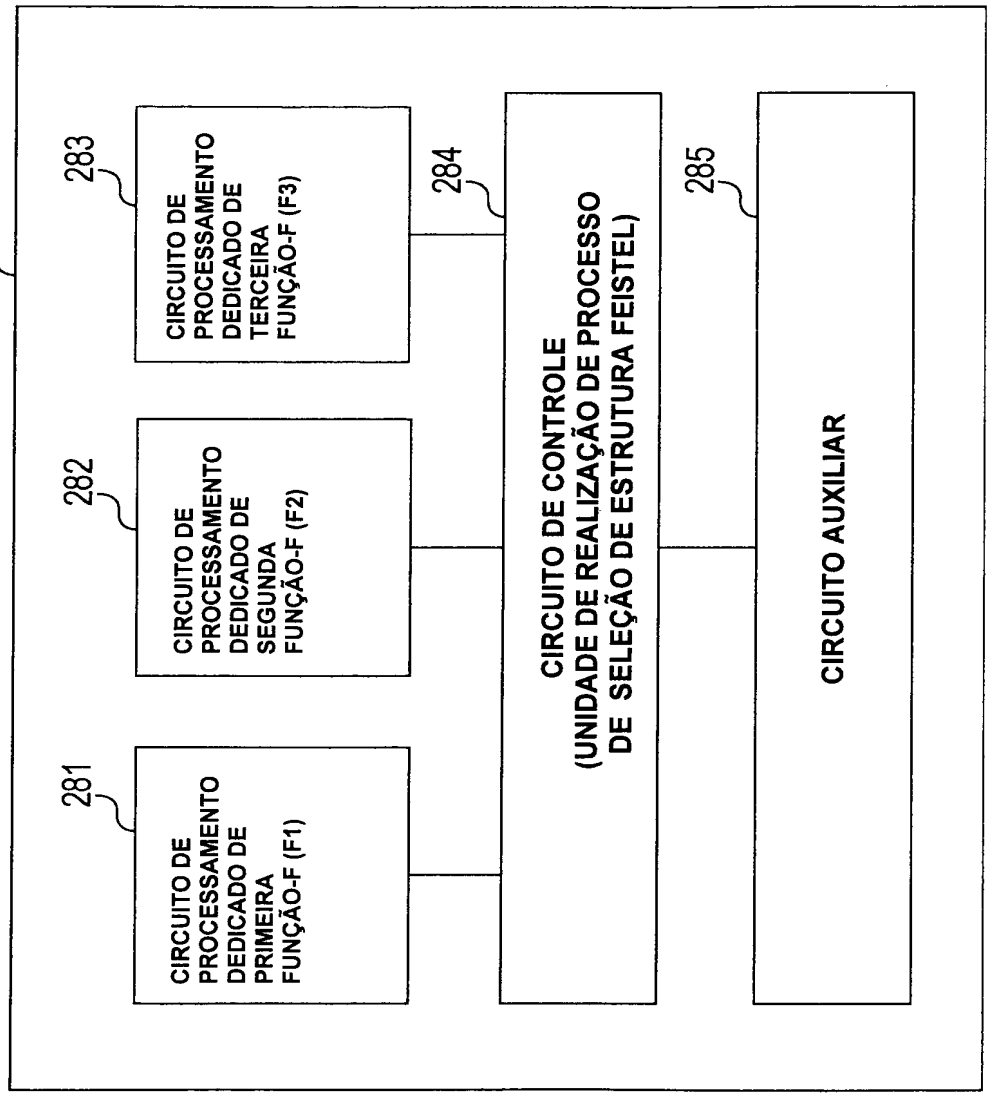
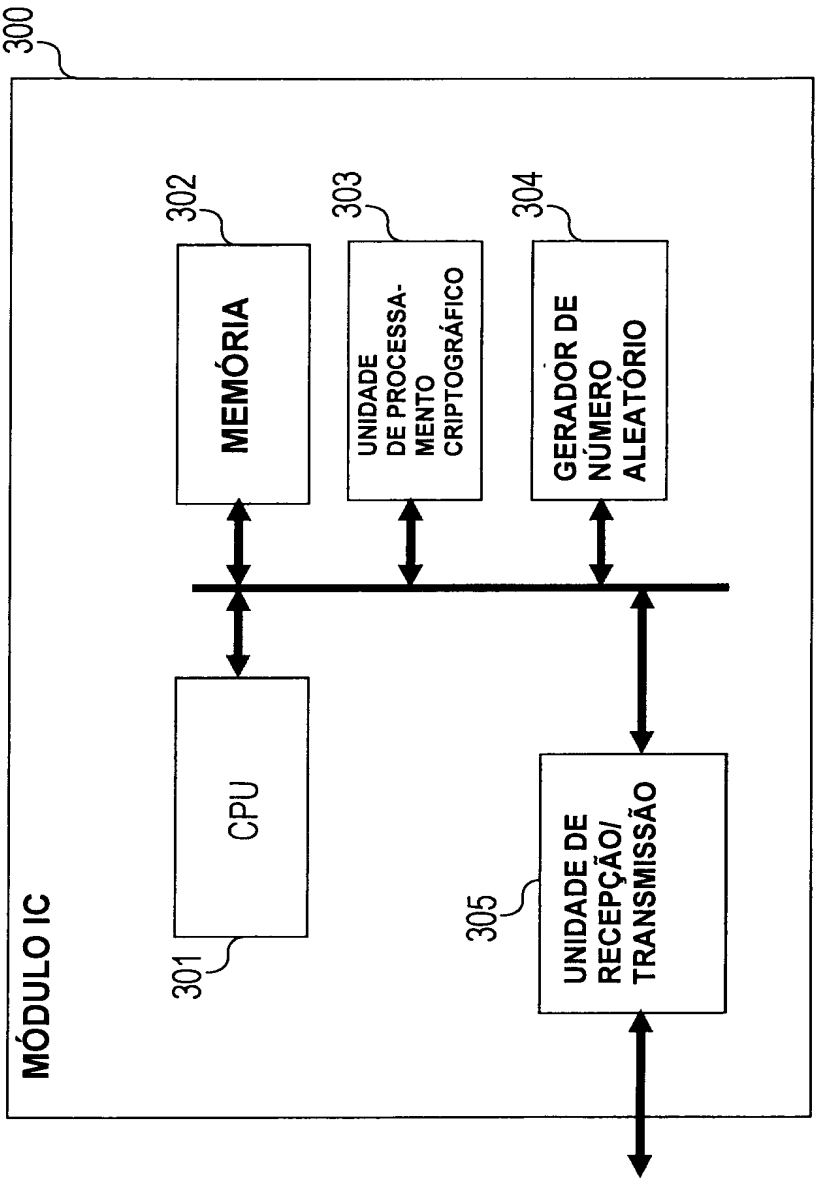

280
281
CIRCUITO DE PROCESSAMENTO DEDICADO DE PRIMEIRA FUNÇÃO-F (F1)
282
CIRCUITO DE PROCESSAMENTO DEDICADO DE SEGUNDA FUNÇÃO-F (F2)
283
CIRCUITO DE PROCESSAMENTO DEDICADO DE TERCEIRA FUNÇÃO-F (F3)
284
CIRCUITO DE CONTROLE (UNIDADE DE REALIZAÇÃO DE PROCESSO DE SELEÇÃO DE ESTRUTURA FEISTEL)
285
CIRCUITO AUXILIAR

FIG. 20


300
MÓDULO IC
302
MEMÓRIA
303
UNIDADE DE PROCESSA-MENTO CRIPTOGRÁFICO
304
GERADOR DE NÚMERO ALEATÓRIO
CPU
301
305
UNIDADE DE RECEPÇÃO/ TRANSMISSÃO

RESUMO

"APARELHO E MÉTODO DE PROCESSAMENTO POR CRIPTOGRAFIA, MÉTODO DE CONSTRUÇÃO DE ALGORITMO DE PROCESSAMENTO POR CRIPTOGRAFIA, E, PROGRAMA DE COMPUTADOR"

Realizar uma configuração de processo de cifra de bloco de chave comum do tipo Feistel estendido para realização de um mecanismo de comutação de matriz de difusão (DSM). Em uma configuração de processo criptográfico em que uma estrutura de Feistel estendida, tendo um número de linhas de dados: d que é estabelecida para um inteiro que satisfaça $d \geq 2$ é aplicada, uma pluralidade de múltiplas matrizes diferentes são aplicadas, seletivamente, a processos de transformação linear realizados em seções de função-F. Uma pluralidade de matrizes diferentes satisfazendo uma condição em que um número mínimo de derivações para todas as linhas de dados é igual ou maior do que um valor predeterminado são selecionadas como as matrizes, o número mínimo de derivações para todas as linhas de dados sendo selecionado dentre números mínimos de derivações correspondendo às linhas de dados, cada um dos números mínimos de derivações correspondentes às linhas de dados sendo baseado em matrizes de transformação linear incluídas em funções-F que são introduzidas em uma linha de dados correspondente na estrutura de Feistel estendida. De acordo com a presente invenção, cifra de bloco de chave comum com base na DSM com uma alta resistência à análise linear e análise diferencial é realizada.