(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 601 19 410 T2** 2006.11.02

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 133 100 B1**
(21) Deutsches Aktenzeichen: **601 19 410.1**
(96) Europäisches Aktenzeichen: **01 302 065.6**
(96) Europäischer Anmeldetag: **06.03.2001**
(97) Erstveröffentlichung durch das EPA: **12.09.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **10.05.2006**
(47) Veröffentlichungstag im Patentblatt: **02.11.2006**

(51) Int Cl.[8]: ***H04L 9/06*** (2006.01)

(30) Unionspriorität:

2000060482	**06.03.2000**	**JP**
2000210484	**11.07.2000**	**JP**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Kabushiki Kaisha Toshiba, Kawasaki, Kanagawa, JP

(74) Vertreter:
HOFFMANN & EITLE, 81925 München

(72) Erfinder:
Kenji, c/o Intellectual Property Division, Ohkuma, Minato-ku, Tokyo 105-8001, JP; Hirofumi, c/o Intellectual Property Div., Muratani, Minato-ku, Tokyo 105-8001, JP; Shinichi, c/o Intellectual Property Div., Kawamura, Minato-ku, Tokyo 105-8001, JP; Fumihiko, Intellectual Property Division, Sano, Minato-ku, Tokyo 105-8001, JP

(54) Bezeichnung: **Vorrichtung und Verfahren zur Blockverschlüsselung und zur Entschlüsselung**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf eine Verschlüsselungsvorrichtung und ein Verfahren, und eine Entschlüsselungsvorrichtung und ein Verfahren basierend auf einem Blockverschlüsselungsschema, und eine Operationseinheit, die in den Verschlüsselungs- und Entschlüsselungsvorrichtungen verwendet wird.

[0002] Typische grundlegende Strukturen eines Verschlüsselungsschemas mit gemeinsamem Schlüsselblock enthalten SPN-Typ und Feistel-Typ. Für beide Strukturen wurde ein Entwurfsverfahren zum Verbessern von Stärkeevaluierung und Beständigkeit gegenüber differenzieller/linearer Kryptoanalyse untersucht (Literaturstelle [1], V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers & E. De Win, "The Cipher SHARK," Fast Software Encryption, LNCS 1039, 1996, Literaturstelle [2] Kazumaro Aoki, Kazuo Ota, "More Strict Evaluation of Maximum Mean Differential Probability and Maximum Mean Linear Probability," SCIS 96-4A, 1996, Literaturstelle [3], Mitsuru Matsui, "Block encryption scheme MISTY," ISEC 96-11, 1996).

[0003] Mit der SPN-Struktur kann, da die Zahl von aktiven S-Boxen garantiert werden kann, die Zahl von Stufen zum Erreichen der eingestellten Stärke leicht bestimmt werden (Literaturstelle [1]). Wenn jedoch die Blockgröße ansteigt, und die Parallelität von S-Boxen hoch wird, wird der Prozess von Diffusionsschichten kompliziert, was zu einer geringen Geschwindigkeit führt.

[0004] SQUARE/Rijndael Cipher kann dieses Problem lösen (Literaturstelle [4] J. Daemen, L.R. Knudsen & V. Rijmen, "The Block encryption scheme Square," Fast Software Encryption, LNCS 1267, 1997, Literaturstelle [5] J. Daemen & V. Rijmen, "AES Proposal: Rijndael, "http://www.east.kuleuven.ac.be/~rijmen/rijdael/rijndaeldocV2.zip).

[0005] Im Code dieses Typs sind 16 parallele S-Boxen in einer Matrix 4 × 4 angeordnet, um lineare Diffusion innerhalb einer einzelnen Spalte zu begrenzen, wobei somit die Verarbeitungslast reduziert wird. Durch Kombinieren einer Neuanordnung von Bytepositionen mit linearer Diffusion wird der Einfluss von einem Byte in einer gegebenen Stufe zu allen Bytes zwei Stufen später diffundiert, und es werden 25 oder mehr aktive S-Boxen in vier Stufen (robust gegenüber differenzieller/linearer Kryptoanalyse) erreicht.

[0006] Da sich jedoch Bytes in einer einzelnen Spalte nicht in der nächsten Stufe mischen, ist ein dedizierter Angriff vorhanden, der SQUARE-Angriff genannt wird (Literaturstelle [1], Literaturstelle [5]). Dies resultiert aus dem Erreichen von sowohl hoher Stärke als auch Effizienz unter der Einschränkung von nur einem Typ von Diffusionsschichten.

[0007] Die SPN-Struktur erlaubt einfache Schätzung der unteren Grenze der Zahl von aktiven S-Boxen, und kann entworfen werden, eine hohe Stärke gegenüber differenzieller/linearer Kryptoanalyse zu garantieren. Wenn jedoch die Parallelität von S-Boxen mit steigender Blockgröße von Klartext/Chiffretxt höher wird, werden die Kalkulationskosten eines koppelnden Abschnitts von Diffusionsschichten hoch. Auch kann einheitliche Datendiffusion abhängig von dem Entwurf von Diffusionsschichten nicht erzielt werden.

[0008] Entsprechend richtet sich die vorliegende Erfindung auf ein Verfahren und eine Vorrichtung, die im wesentlichen eines oder mehr der Probleme wegen Begrenzungen und Nachteilen vom Stand der Technik umgehen.

[0009] In Übereinstimmung mit dem Zweck der Erfindung, wie verkörpert und breit beschrieben, richtet sich die Erfindung auf eine Verschlüsselungsvorrichtung, umfassend Mittel zum Randomisieren eingegebener Daten in Einheiten eines Blocks einer ersten Größe; und Mittel zum Diffundieren von Daten, die von dem Randomisierungsmittel ausgegeben werden mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und das Randomisierungsmittel umfasst erste Randomisierungseinheiten zum Randomisieren der eingegebenen Daten in Einheiten des Blocks der ersten Größe, gekennzeichnet dadurch, dass mindestens eine der ersten Randomisierungseinheiten umfasst zweite Randomisierungseinheiten zum Randomisieren der eingegebenen Daten in Einheiten eines Blocks einer dritten Größe, die kleiner als die erste Größe ist; und eine Diffusionseinheit zum Diffundieren von Daten, die von den zweiten Randomisierungseinheiten ausgegeben werden mit Bezug auf die erste Größe.

[0010] In Übereinstimmung mit der vorliegenden Erfindung wird auch ein Verschlüsselungsverfahren vorgesehen, umfassend einen Schritt zum Randomisieren eingegebener Daten in Einheiten eines Blocks einer ersten Größe; und einen Schritt zum Diffundieren randomisierter Daten mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und der Randomisierungsschritt umfasst einen Teilschritt zum Randomisieren der eingegebenen Daten in Einheiten des Blocks der ersten Größe, gekennzeichnet dadurch, dass der Teilschritt umfasst einen Teilschritt zum Randomisieren der eingegebenen Daten in Einheiten eines Blocks einer dritten Größe, die kleiner als die Daten, die von dem Randomisierungsteilschritt ausgegeben werden mit Bezug auf die erste Größe.

[0011] Gemäß der vorliegenden Erfindung wird eine Entschlüsselungsvorrichtung vorgesehen, umfas-

send: Mittel zum Randomisieren eingegebener verschlüsselter Daten in Einheiten eines Blocks einer ersten Größe; und Mittel zum Diffundieren der Daten, die von dem Randomisierungsmittel ausgegeben werden mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und das Randomisierungsmittel umfasst erste Randomisierungseinheiten zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten des Blocks der ersten Größe; gekennzeichnet dadurch, dass mindestens eine der ersten Randomisierungseinheiten umfasst: zweite Randomisierungseinheiten zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten eines Blocks einer dritten Größe, die kleiner als die erste Größe ist; und eine Diffusionseinheit zum Diffundieren von Daten, die von den zweiten Randomisierungseinheiten ausgegeben werden mit Bezug auf die erste Größe.

[0012] Gemäß der vorliegenden Erfindung wird ein Verfahren zum Entschlüsseln vorgesehen, umfassend: einen Schritt zum Randomisieren eingegebener verschlüsselter Daten in Einheiten eines Blocks einer ersten Größe; und einen Schritt zum Diffundieren der Daten, die von dem Randomisierungsmittel ausgegeben werden mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und der Randomisierungsschritt umfasst einen Teilschritt zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten des Blocks der ersten Größe, gekennzeichnet dadurch, dass der Teilschritt umfasst einen Teilschritt zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten eines Blocks einer dritten Größe, die kleiner als die erste Größe ist; und einen Teilschritt zum Diffundieren von Daten, die von dem Randomisierungsteilschritt ausgegeben werden mit Bezug auf die erste Größe.

[0013] Gemäß der vorliegenden Erfindung wird ein Artikel einer Herstellung vorgesehen, umfassend ein computerverwendbares Medium mit einem computerlesbaren Programmcodemittel, das darin verkörpert ist, das computerlesbare Programmcodemittel umfassend: ein erstes computerlesbares Programmcodemittel zum Veranlassen eines Computers, eingegebene Daten in Einheiten eines Blocks einer ersten Größe zu randomisieren; und ein zweites computerlesbares Programmcodemittel zum Veranlassen eines Computers, randomisierte Daten zu diffundieren mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und das erste computerlesbare Programmcodemittel umfasst ein drittes computerlesbares Programmcodemittel zum Veranlassen eines Computers, die eingegebenen Daten in Einheiten des Blocks der ersten Größe zu randomisieren, gekennzeichnet dadurch, dass das dritte computerlesbare Programmcodemittel umfasst: ein viertes computerlesbares Programmcodemittel zum Veranlassen eines Computers, die eingegebenen Daten in Einheiten eines Blocks einer dritten Größe zu randomisieren, die kleiner als die erste Größe ist; und ein fünftes computerlesbares Programmcodemittel zum Veranlassen eines Computers, Daten zu diffundieren, die von dem vierten computerlesbaren Programmcodemittel ausgegeben werden mit Bezug auf die erste Größe.

[0014] Gemäß der vorliegenden Erfindung erreichen eine Verschlüsselungsvorrichtung und ein Verfahren, und eine Entschlüsselungsvorrichtung und ein Verfahren gleichförmige Diffusion, während Kalkulationskosten niedergehalten werden.

[0015] Gemäß der vorliegenden Erfindung erreichen eine Verschlüsselungsvorrichtung und ein Verfahren, und eine Entschlüsselungsvorrichtung und ein Verfahren gleichförmige Diffusion, während Kalkulationskosten niedergehalten werden.

[0016] Diese Zusammenfassung der Erfindung beschreibt nicht notwendigerweise alle notwendigen Merkmale, sodass die Erfindung auch eine Teilkombination dieser beschriebenen Merkmale sein kann.

[0017] Die Erfindung kann aus der folgenden detaillierten Beschreibung vollständiger verstanden werden, wenn in Verbindung mit den begleitenden Zeichnungen aufgenommen, in denen:

[0018] Fig. 1 eine Ansicht zum Erläutern der Basiskonfiguration von Verschlüsselung gemäß der ersten Ausführungsform der vorliegenden Erfindung ist;

[0019] Fig. 2 eine Ansicht zum Erläutern einer Verschlüsselungsstärke ist;

[0020] Fig. 3 eine Ansicht ist, die ein Beispiel der hierarchischen Struktur eines Datenrandomisierungssteils verschachtelter Verschlüsselung ist;

[0021] Fig. 4 ein Blockdiagramm ist, das ein Beispiel der Anordnung einer Verschlüsselungsvorrichtung zeigt;

[0022] Fig. 5 ein Beispiel einer S-Box zeigt;

[0023] Fig. 6 ein Beispiel der internen Anordnung einer erweiterten S-Box zeigt;

[0024] Fig. 7 ein Beispiel einer MDS unterer Ebene zeigt;

[0025] Fig. 8 ein Beispiel der Struktur einer Stufe des Datenrandomisierungssteils zeigt;

[0026] Fig. 9 ein Beispiel einer MDS höherer Ebene zeigt;

[0027] Fig. 10 ein anderes Beispiel der MDS höherer Ebene zeigt;

[0028] Fig. 11 ein Blockdiagramm ist, das ein Beispiel der Anordnung eines Schlüsselplanungsteils zeigt;

[0029] Fig. 12 ein Blockdiagramm ist, das ein anderes Beispiel der Anordnung des Schlüsselplanungsteils zeigt;

[0030] Fig. 13 ein Blockdiagramm ist, das ein Beispiel der internen Anordnung einer nichtlinearen Transformationsschicht zeigt;

[0031] Fig. 14 ein Blockdiagramm ist, das ein anderes Beispiel der internen Anordnung der nichtlinearen Transformationsschicht zeigt;

[0032] Fig. 15 ein Beispiel einer Additivkonstantentabelle zeigt;

[0033] Fig. 16 ein Blockdiagramm ist, das ein Beispiel der Anordnung eines Galois-Feldmultiplikators zeigt;

[0034] Fig. 17 ein Blockdiagramm ist, das ein Beispiel der Anordnung einer linearen Transformationssektion zeigt;

[0035] Fig. 18 ein Blockdiagramm ist, das ein anderes Beispiel der Anordnung der linearen Transformationssektion zeigt;

[0036] Fig. 19 ein Blockdiagramm ist, das ein Beispiel der Anordnung einer MDS-Matrixgenerierungssektion zeigt;

[0037] Fig. 20 ein Flussdiagramm ist, das ein Beispiel einer MDS-Matrixgenerierungsverarbeitungssequenz zeigt;

[0038] Fig. 21 ein Blockdiagramm ist, das ein anderes Beispiel der Anordnung der MDS-Matrixgenerierungssektion zeigt;

[0039] Fig. 22 ein Flussdiagramm ist, das ein anderes Beispiel der MDS-Matrixgenerierungsverarbeitungssequenz zeigt;

[0040] Fig. 23 ein Flussdiagramm ist, das ein Beispiel einer Verarbeitungssequenz zum Auswählen einer Kombination einer S-Box und MDS unterer Ebene zeigt;

[0041] Fig. 24 ein Blockdiagramm ist, das ein Beispiel der Anordnung einer Entschlüsselungsvorrichtung zeigt;

[0042] Fig. 25 ein Beispiel der internen Anordnung der Umkehrtransformation einer erweiterten S-Box zeigt;

[0043] Fig. 26 ein Beispiel der Struktur einer Stufe der Umkehrtransformation eines Datenrandomisierungssteils zeigt;

[0044] Fig. 27 ein Blockdiagramm ist, das ein Beispiel der Anordnung eines Schlüsselplanungsteils zeigt;

[0045] Fig. 28 eine Ansicht zum Erläutern der Basiskonfiguration von Verschlüsselung gemäß der zweiten Ausführungsform der vorliegenden Erfindung ist;

[0046] Fig. 29 ein Beispiel der Struktur einer Stufe der Umkehrtransformation eines Datenrandomisierungssteils zeigt;

[0047] Fig. 30 ein Beispiel der MDS höherer Ebene zeigt;

[0048] Fig. 31 Leitungsverbindungsausdrücke von Multiplikation über $GF(2^4)$ zeigt;

[0049] Fig. 32 ein anderes Beispiel der MDS höherer Ebene zeigt;

[0050] Fig. 33 eine Ansicht zum Erläutern von erneuter Normalisierung in der MDS höherer Ebene ist;

[0051] Fig. 34 noch ein anderes Beispiel der MDS höherer Ebene zeigt;

[0052] Fig. 35 ein Blockdiagramm ist, das noch ein anderes Beispiel der Anordnung des Schlüsselplanungsteils zeigt;

[0053] Fig. 36 ein Blockdiagramm ist, das noch ein anderes Beispiel der Anordnung des Schlüsselplanungsteils zeigt;

[0054] Fig. 37 ein anderes Beispiel der Additivkonstantentabelle zeigt;

[0055] Fig. 38 ein Blockdiagramm ist, das ein anderes Beispiel der Entschlüsselungsvorrichtung zeigt;

[0056] Fig. 39 ein anderes Beispiel der Struktur einer Stufe der Umkehrtransformation des Datenrandomisierungssteils zeigt;

[0057] Fig. 40 ein Blockdiagramm ist, das noch ein anderes Beispiel der Anordnung des Schlüsselplanungsteils zur Zeit von Entschlüsselung zeigt;

[0058] Fig. 41 ein Blockdiagramm ist, das ein Beispiel eines Systems zeigt, das die Verschlüsselungsvorrichtung der vorliegenden Erfindung verwendet;

[0059] Fig. 42 ein Blockdiagramm ist, das ein anderes Beispiel des Systems zeigt, das die Verschlüsse-

lungsvorrichtung der vorliegenden Erfindung verwendet;

[0060] Fig. 43 ein Blockdiagramm ist, das noch ein anderes Beispiel des Systems zeigt, das die Verschlüsselungsvorrichtung der vorliegenden Erfindung verwendet.

[0061] Es wird nun eine bevorzugte Ausführungsform einer Verschlüsselungsvorrichtung und eines Verfahrens, und einer Entschlüsselungsvorrichtung und eines Verfahrens basierend auf einem Blockverschlüsselungsschema, und einer Operationseinheit, die in den Verschlüsselungs- und Entschlüsselungsvorrichtungen gemäß der vorliegenden Erfindung verwendet wird, mit Bezug auf die begleitenden Zeichnungen beschrieben.

[0062] In der Ausführungsform wird eine verschachtelte (rekursive) SPN-Verschlüsselung als eine Kombination lokaler Randomisierung (Diffusion unterer Ebene) und Diffusion über der Blockbreite (Diffusion höherer Ebene) erläutert. In der folgenden Beschreibung wird hauptsächlich Verschlüsselung erläutert, und Entschlüsselung wird danach erläutert. Es wird vermerkt, dass ein Entschlüsselungsalgorithmus eine Umkehrtransformation (Inverstransformation) eines Verschlüsselungsalgorithmus ist, und ein Schlüssel ein geheimer Schlüssel ist, der Verschlüsselung und Entschlüsselung gemeinsam ist. Das Verschlüsselungssystem dieser Ausführungsform kann durch entweder Hardware oder Software implementiert sein, und ein Anordnungsbeispiel, das nachstehend zu beschreiben ist, kann als ein funktionales Blockdiagramm einer Verschlüsselungsvorrichtung (Entschlüsselungsvorrichtung) oder ein funktionales Moduldiagramm eines Verschlüsselungsalgorithmus (Entschlüsselungsalgorithmus) erreicht werden.

[0063] Fig. 1 zeigt ein Beispiel der Basiskonfiguration verschachtelter SPN-Verschlüsselung (eine Verschlüsselungs- (oder Entschlüsselungs-) Vorrichtung oder ein Verschlüsselungsoder Entschlüsselungs-) Algorithmus, eine Verschlüsselungsverarbeitungsvorrichtung).

[0064] Wie in Fig. 1 gezeigt, führt in der verschachtelten SPN-Struktur jedes aus einer Vielzahl von parallelen nichtlinearen Transformationsmodulen (erweiterte S-Boxen in einem später zu beschreibenden Beispiel) **2** in jeder Stufe lokale Diffusion unterer Ebene aus, ein Diffusionsmodul (eine MDS höherer Ebene in einem später zu beschreibenden Beispiel) **3** führt breite Diffusion höherer Ebene über der Blockbreite aus, die nichtlinearen Transformationsmodule **2** führen lokale Diffusionen unterer Ebene aus, ..., und dieser Prozess wird in einer vorbestimmte Zahl von Stufen wiederholt. Jedes nichtlineare Transformationsmodul **2** ist durch abwechselndes Anordnen nichtlinearer Transformationsmodule (S-Boxen in einem später zu beschreibenden Beispiel) und Diffusionsmodulen (MDS unterer Ebene in einem später zu beschreibenden Beispiel) aufgebaut. Das heißt in der verschachtelten SPN-Struktur dieser Ausführungsform sind SPN-Strukturen unterer Ebene (zwei Stufen von SPN-Strukturen in einem später zu beschreibenden Beispiel) rekursiv in S-Box-Abschnitten der normalen SPN-Struktur eingebettet.

[0065] Gemäß einer derartigen verschachtelten SPN-Struktur kann die Zweigzahl (branch number) hierarchisch garantiert werden (Hierarchie der Zweigzahl), und die untere Grenze der Zahl von aktiven S-Boxen kann auch leicht garantiert werden. In der verschachtelten SPN-Struktur kann Stärkeevaluierung dank ihrer einfachen Struktur leicht durchgeführt werden.

[0066] In Fig. 1 werden lokale Diffusionen unterer Ebene durch vier parallele lineare Transformationsmodule **2** ausgedrückt. Die Zahl von parallelen Modulen ist jedoch nicht auf vier begrenzt, sondern es können andere Zahlen paralleler Module verwendet werden. Auch sind die Zahlen von Bits von vier parallelen nichtlinearen Transformationsmodulen einander gleich. Die vorliegende Erfindung ist jedoch nicht auf eine derartige spezifische Zahl von Bits begrenzt, und es kann eine Vielzahl von nichtlinearen Transformationsmodulen **2** mit unterschiedlichen Zahlen von Bits kombiniert werden. In diesem Fall können alle nichtlinearen Transformationsmodule unterschiedliche Bitlängen haben, oder einige Diffusionen unterer Ebene können die gleiche Bitlänge haben. Auch wird ein Typ von Diffusionsmodul **3** verwendet. Alternativ können zwei oder mehr unterschiedliche Typen von Diffusionsmodulen **3** verwendet werden. Z.B. kann jedes zweite Diffusionsmodul **3** über der Blockbreite durch zwei nichtlineare Transformationsmodule ersetzt werden. Zusätzlich zu dem Verfahren, das die sich wiederholende Struktur identischer Anordnungen annimmt, können des weiteren nur einige Anordnungen ersetzt werden.

[0067] Alle nichtlinearen Transformationsmodule **2** können außerdem die gleiche Anordnung haben oder können unterschiedliche Anordnungen enthalten. Das gleiche trifft auf das Diffusionsmodul, die nichtlinearen Transformationsmodule **4** und Diffusionsmodul **5** zu. Z.B. können die erste Eingangsstufe und die letzte Ausgangsstufe interne Anordnungen haben, die sich von jenen der anderen Zwischenstufen unterscheiden. Diese Ausführungsform nimmt die verschachtelte Struktur von zwei Schichten an, kann aber auch eine verschachtelte Struktur von drei oder mehr Schichten verwenden (im Fall von drei Schichten hat jedes nichtlineare Transformationsmodul **4** ferner eine SPN-Struktur). Z.B. können nichtlineare Transformationsmodule **2** unterschiedliche hierarchische Strukturen haben. Außerdem sind andere Variationen verfügbar.

[0068] Diese Ausführungsform wird nachstehend erläutert, wobei ein 128-Bit-Blockverschlüsselungsschema äquivalent zu AES, das 8-Bit-S-Boxen verwendet, als ein Beispiel genommen wird.

[0069] Stärkeevaluierung eines Blockverschlüsselungsschemas wird nachstehend erläutert.

[0070] Als ein wichtiges Maß zum Schätzen der Verschlüsselungsstärke einer gegebenen Funktion f ist die maximale differenzielle Wahrscheinlichkeit/maximale lineare Wahrscheinlichkeit bekannt.

[0071] Eine maximale differenzielle Wahrscheinlichkeit dp^f und eine maximale lineare Wahrscheinlichkeit lp^f mit Bezug auf eine Funktion f(x) ergeben sich jeweils durch:

$$dp^f = \max_{\Delta x \neq 0, \Delta y} \left| \frac{\#\{x \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n} \right|$$

$$lp^f = \max_{\Gamma x, \Gamma y \neq 0} \left| 2 \frac{\#\{x \mid x \cdot \Gamma x = f(x) \cdot \Gamma y\}}{2^n} - 1 \right|$$

wobei Δx die Differenz von Eingabe x ist, Γx der Maskenwert von x ist und Δy die Differenz von Ausgabe y ist.

[0072] Im allgemeinen ist es schwer, die maximale differenzielle Wahrscheinlichkeit dp^f und die maximale lineare Wahrscheinlichkeit lp^f zu erhalten. Daher wird Sicherheit hier unter Verwendung einer maximalen differenziellen charakteristischen Wahrscheinlichkeit DP^f und einer maximalen linearen charakteristischen Wahrscheinlichkeit LP^f evaluiert, die angenäherte Werte für die maximale differenzielle Wahrscheinlichkeit dp^f und die maximale lineare Wahrscheinlichkeit lp^f sind.

[0073] In dieser Ausführungsform wird die verschachtelte SPN-Struktur als eine Verschlüsselungsfunktion verwendet. Die Charakteristika einer SPS-Struktur als die Basisstruktur der verschachtelten SPN-Struktur wird nachstehend erläutert. Es wird vermerkt, dass SPS eine dreischichtige Struktur einer S-Box und Diffusionsschichten S und P wie S-P-S anzeigt. Die SPS-Struktur wird als die zweistufige SPN-Struktur betrachtet.

[0074] In der SPS-Struktur ist, falls Θ(x) die Ausgabe von der Diffusionsschicht als Reaktion auf Eingabe x darstellt, die Zweigzahl B mit Bezug auf differenzielle Kryptoanalyse durch

$$B \equiv \min_{\Delta x \neq 0} (w(\Delta x) + w(\Theta(\Delta x)))$$

definiert, (siehe Literaturstelle [1], Literaturstelle [6], Hideo Shimizu & Toshinobu Kaneko, "Diffusion Layer of Common Key Cipher," SCIS 99-72, 1999), wobei w ( ) die Hamming-Distanz unter Verwendung der Bitlänge einer S-Box als eine Codelänge ist. Die S-Boxen, die mit Eingabe-/Ausgabedifferenzen ungleich Null verbunden sind, werden als aktive S-Boxen bezeichnet.

[0075] Eine Struktur, die durch Verbinden von S-Boxen mit der Eingabe und Ausgabe einer Diffusionsschicht erhalten wird, wird als eine SPS-Struktur bezeichnet. Falls S-Boxen Bijektionen sind, und mindestens ein Eingabebit zu der SPS-Struktur eine Differenz ungleich Null hat, ist die Zahl von aktiven S-Boxen gleich oder größer der Zweigzahl (d.h. gleich oder größer B) gemäß der Definition der Zweigzahl. Falls p_S die maximale differenzielle Wahrscheinlichkeit von S-Boxen darstellt, überschreitet die maximale differenzielle charakteristische Wahrscheinlichkeit der SPS-Struktur einen oberen Grenzwert p_S^B nicht.

[0076] Wenn M parallele S-Boxen als S-Schichten der SPS-Struktur verwendet werden, ist die Zweigzahl von Diffusionsschichten, die sie koppeln, gleich oder kleiner (M + 1), und eine lineare Transformation, in der die Zweigzahl (M + 1) genügt, wird eine MDS (Maximaldistanztrennbarkeit, Maximum Distance Separable) Matrix genannt.

[0077] Falls die Diffusionsschichten eine MDS-Matrix bilden, überschreitet die maximale differenzielle charakteristische Wahrscheinlichkeit der SPS-Struktur einen oberen Grenzwert p_S^{M+1} nicht [Literaturstelle 1]. Falls q_S die maximale lineare Wahrscheinlichkeit von S-Boxen darstellt, überschreitet die maximale lineare charakteristische Wahrscheinlichkeit der SPS-Struktur gleichermaßen q_S^{M+1} nicht.

[0078] Falls eine zweistufige SPN-Struktur als eine S-Box einer SPN-Struktur höherer Ebene verwendet wird, wird sie eine erweiterte S-Box genannt (Struktur unterer Ebene). Es wird angenommen, dass M_1 parallele S-Boxen verwendet werden, und B_1 die Zweigzahl von Diffusionsschichten in der erweiterten S-Box darstellt. Bei gegebenen M_2 parallelen zweistufigen SPN-Strukturen (Struktur höherer Ebene) für erweiterte S-Boxen, in denen B_2 die Zweigzahl der Diffusionsschichten darstellt, wird die Zahl von aktiven S-Boxen in der Struktur höherer Ebene nicht kleiner als ein unterer Grenzwert $B_1 \times B_2$. Diese Natur wird Hierarchie der Zweigzahl genannt.

[0079] Falls zwei Typen von Diffusionsschichten sowohl höherer Ebene als auch unterer Ebene MDS-Matrizen bilden, wird die Zahl von aktiven S-Boxen nicht kleiner als $(M_1 + 1) \times (M_2 + 1)$. Auf diese Weise können die oberen Grenzen von DP^f und LP^f der verschachtelten SPN-Struktur niedergehalten werden.

[0080] Fig. 2 zeigt ein Beispiel der zweistufigen SPN-Struktur, wenn $M_1 = M_2 = 4$ ist. Bezugszeichen

15 bezeichnet einen Diffusionsteil unter Verwendung einer MDS-Matrix höherer Ebene (später zu beschreiben); **11** bis **14** erweiterte S-Boxen auf der Eingangsseite des Diffusionsteils; und **16** bis **19** erweiterte S-Boxen auf der Ausgangsseite des Diffusionsteils. In jeder erweiterten S-Box bezeichnet Bezugszeichen **20** einen Diffusionsteil unter Verwendung einer MDS unterer Ebene (später zu beschreiben). Die kleinsten Rechtecke **21** und **22** in Fig. 2 zeigen jeweils Eingangs- und Ausgangsseiten-S-Boxen an.

[0081] In Fig. 2 werden aktive S-Boxen durch Schraffierung angezeigt (siehe **21** in Fig. 2), und leere S-Boxen zeigen Null-Differenz an (siehe **22** in Fig. 2). Die erweiterten S-Boxen **11**, **13**, **16**, **17** und **19**, die durch fette Linien angezeigt werden, sind aktive erweiterte S-Boxen, und andere erweiterte S-Boxen **12**, **14** und **18** zeigen Null-Differenz an. Wie aus Fig. 2 gesehen werden kann, ist die Zahl von aktiven S-Boxen in vier Stufen **25** oder mehr.

[0082] Wie oben beschrieben, können im Verschlüsselungsschema dieser Ausführungsform **25** (= 5 × 5) oder mehr aktive S-Boxen durch zwei Stufen garantiert werden. Die maximale differenzielle Wahrscheinlichkeit jeder S-Box ergibt sich durch:

$P_S = 6/256$.

[0083] Die differenzielle charakteristische Wahrscheinlichkeit in zwei Stufen ergibt sich durch:

$p_S\ 25 = 2^{-135,4} \ll 2^{-128}$.

Daher ist differenzielle Kryptoanalyse nicht effektiv.

[0084] Gleichermaßen ergibt sich die lineare charakteristische Wahrscheinlichkeit durch:

$q_S = 22/256$

$q_S^{25} = 2^{-88,5} \ll 2^{-64}$.

[0085] Daher ist lineare Kryptoanalyse nicht effektiv.

[0086] Es wird vermerkt, dass der SQUARE-Angriff, der auf ein konventionelles SQUARE/Rijndael-Verschlüsselungsschema angewendet wird, die Charakteristika ausnutzt, worin, wenn alle 28 unterschiedlichen Muster zu einem Byte in einer Stufe eingegeben werden, während andere Eingaben fixiert sind, alle 28 unterschiedlichen Muster in jeweiligen Ausgabebytes nach zwei Stufen erscheinen. Das Verschlüsselungsschema dieses Beispiels macht jedoch eine einfache Anwendung dieses Angriffs durch Verbessern von Erweiterbarkeit unter S-Boxen über den Weg, den die MDS höherer Ebene (später zu beschreiben) nimmt, schwierig.

[0087] Diese Ausführungsform wird nachstehend unter Verwendung eines Beispiels eines verschachtelten Verschlüsselungsschemas detailliert beschrieben.

[0088] Es wird ein Beispiel der Anordnung dieser Ausführungsform beschrieben.

[0089] Fig. 3 zeigt ein Beispiel der hierarchischen Struktur des Datenrandomisierungsteils eines verschachtelten Verschlüsselungsschemas dieser Ausführungsform.

[0090] Die Blocklänge nimmt 128 Bits als ein Beispiel (natürlich kann die vorliegende Erfindung für andere Blocklängen praktiziert werden). Die Schlüssellänge nimmt 256 Bits als ein Beispiel (natürlich kann die vorliegende Erfindung für andere Blocklängen praktiziert werden). Ein Fall, worin die Schlüssellänge = 128 Bits oder 192 Bits ist, wenn die Blocklänge = 128 Bits ist, wird später beschrieben.

[0091] Wenn ein Paar aus einer Vielzahl von parallelen erweiterten S-Boxen und einer MDS höherer Ebene (die letzte Stufe enthält keinerlei MDS höherer Ebene, wie später beschrieben wird) als eine Stufe gezählt wird, stellt R die Zahl von Stufen dar, und R = 8 wird in einem Beispiel verwendet. Es wird vermerkt, dass die Zahl von Stufen grundsätzlich nicht besonders begrenzt ist. Die tatsächliche Zahl von Stufen kann in jedoch Anbetracht von Sicherheit, Computerressourcen und dergleichen angemessen eingestellt werden, und es ist effektiver, sechs oder mehr Stufen, und wünschenswerter acht oder mehr Stufen einzustellen.

[0092] Bei Verschlüsselung dieser Ausführungsform entspricht, da eine Stufenfunktion zwei S-Box-Schichten enthält, eine Stufe zwei Stufen in einer normalen Struktur. Bezüglich einer MDS höherer Ebene in der Stufenstruktur werden einige Implementierungen basierend auf unterschiedlichen Galois-Feldern erläutert (es werden Beispiele von Stärkepriorität und Geschwindigkeitspriorität beschrieben).

[0093] Fig. 4 zeigt ein Beispiel der Anordnung einer Verschlüsselungsvorrichtung gemäß dieser Ausführungsform.

[0094] Bezugszeichen **101** bezeichnet eine Verarbeitungseinheit (Stufenfunktion) jeder Stufe; **104** eine Diffusionsschicht einer MDS höherer Ebene; **102** eine erweiterte S-Box-Schicht; und **103** einzelne erweiterte S-Boxen. Bezugszeichen **105** bezeichnet eine EX-OR-Einheit. Bezugszeichen **121** bezeichnet eine Stufe eines Schlüsselplanungsteils (Details werden später beschrieben). Bezugszeichen P bezeichnet 128-Bit-Klartext als eine Eingabe; und C 128-Bit-Chiffretext als eine Ausgabe.

[0095] Die Stufenfunktion **101** hat eine Struktur, in der vier parallele 32-Bit-Verarbeitungsteilblöcke (erweiterte S-Boxen) **103**, jeder bestehend aus einer zweistufigen SPN-Struktur, nebeneinander gestellt sind, und ihre Ausgaben sind durch die MDS-Diffusionsschicht **104** gekoppelt. Die gesamte Basisstruktur wird durch Wiederholungen dieser Stufenfunktion **101** definiert.

[0096] In dem Beispiel von Fig. 4 ist, um symmetrische Verschlüsselungs- und Entschlüsselungsprozesse zu erzielen, die letzte Stufe durch nur eine erweiterte S-Box-Schicht **102** und einen Schlüsseladdierer **105** aufgebaut.

[0097] Da zwei Stufen von SPN-Strukturen in einer Stufe der Stufenfunktion **101** eingebettet sind, und Schlüsseladdition in dem Ende des Prozesses durchgeführt wird, ist die Bitlänge eines erweiterten Schlüssels 2 × 128 × R + 128 = 128 (2R + 1). Wenn R = 8 ist, ist die Bitlänge 128 × 17 Bits.

[0098] Nachstehend wird eine S-Box erläutert.

[0099] Verschlüsselung dieses Beispiels verwendet eine 8-Bit-5-Box, die durch eine Eingabe-/Ausgabetabelle definiert ist.

[0100] Fig. 5 zeigt ein Beispiel der Eingabe-/Ausgabetabelle der 8-Bit-S-Box. In Fig. 5 werden Sequenzelemente durch hexadezimale Schreibweise dargestellt.

[0101] In der Tabelle von Fig. 5 entspricht der oberste linke Wert "72" s[0]; sein rechter benachbarter Wert "AA" s[1]; der rechte Endwert dieser Zeile s[15]; der linke Endwert "69" der nächsten Zeile s[16]; sein rechter benachbarter Wert "6A" s[17]; usw. Der unterste rechte Wert "57" entspricht s[255].

[0102] Die Charakteristika der beispielhaften S-Box in Fig. 5 sind wie folgt.

[0103] Maximale differenzielle Wahrscheinlichkeit: 6/256 (theoretischer Minimalwert = 4/256)

[0104] Maximale lineare Wahrscheinlichkeit: 22/256 (theoretischer Minimalwert = 16/256);

[0105] Algebraische Ordnung: 7. Ordnung (Maximalwert von Bijektionsfunktion).

[0106] Es wird vermerkt, dass die S-Box einen arithmetischen Prozess an Stelle der Eingabe-/Ausgabetabelle verwenden kann.

[0107] Nachstehend wird jede erweiterte S-Box (auch eine Struktur unterer Ebene genannt) erläutert.

[0108] Fig. 6 zeigt ein Beispiel der internen Anordnung der erweiterten S-Box **103**. In diesem Beispiel bilden zwei Mengen von vier parallelen 8-Bit-S-Boxen (siehe Fig. 5) eine zweistufige SPN-Struktur, um eine Diffusionsschicht **113** dazwischen einzulegen. Diese Struktur sollte eine SPS-Struktur genannt werden, wird aber als eine spezielle zweistufige SPN-Struktur betrachtet, aus der die Diffusionsschicht der zweiten Stufe weggelassen wird. Ein Schlüsseladdierer **111** ist unmittelbar vorangehend zu jeder S-Box **112** vorgesehen. Die Diffusionsschicht **113** in der erweiterten S-Box verwendet eine MDS-Matrix, die eine MDS unterer Ebene genannt wird, und wird durch MDS_L ausgedrückt.

[0109] Fig. 7 zeigt ein Beispiel der MDS_L-Matrix, die bei Verschlüsselung dieser Ausführungsform verwendet wird. In Fig. 7 werden Matrixelemente in hexadezimaler Schreibweise ausgedrückt. Es wird vermerkt, dass S-Box-Eingaben und Ausgaben, und Matrixelemente als Elemente eines Galois-Feldes $GF(2^8)$ bei Multiplikation betrachtet werden. Ein primitives Polynom im Fall dieses Beispiels ist $x^8 + x^6 + x^5 + x + 1$.

[0110] Nachstehend wird eine Struktur höherer Ebene als eine Stufenfunktion von Verschlüsselung dieses Beispiels beschrieben.

[0111] Fig. 8 zeigt ein Beispiel der Anordnung eines einstufigen Abschnitts **101** des Randomisierungsteils. Die Struktur höherer Ebene **101** als eine Stufenfunktion von Verschlüsselung dieses Beispiels ist durch Koppeln von vier parallelen 32-Bit erweiterten S-Boxen **103** (siehe Fig. 6) durch eine Diffusionsschicht **104** einer MDS-Matrix aufgebaut. Die Diffusionsschicht **104** in der Struktur höherer Ebene **101** als eine Stufenfunktion verwendet eine MDS-Matrix, die eine MDS höherer Ebene genannt wird und durch MDS_H ausgedrückt ist. Es wird vermerkt, dass die MDS-Matrix in diesem Fall bedeutet, dass die Zweigzahl in Anbetracht der erweiterten S-Box **5** ist.

[0112] Die einfachste Implementierung einer MDS höherer Ebene besteht darin, die 32 Bit breite Ausgabe einer erweiterten S-Box als Elemente von $GF(2^{32})$ zu verwenden. Obwohl diese Technik hohe Stärke leicht rechtfertigt, ist es allgemein schwierig, Verarbeitung hoher Geschwindigkeit zu implementieren oder zu erzielen. In diesem Fall werden vorzugsweise einige Einschränkungen auf die MDS-Matrix höherer Ebene angewendet.

[0113] Die vier parallelen MDS-Matrizen können durch die 4-Bit-Breite ausreichend konfiguriert werden, und können unter Verwendung arithmetischer Operationen über $GF(2^4)$ implementiert werden. Eine zyklische MDS erlaubt effiziente Kalkulationen.

[0114] In der Praxis sind Zwischenkonfigurationen unter Verwendung von $GF(2_8)$ und $GF(2^{16})$ verfügbar.

[0115] Es wird nachstehend eine MDS höherer Ebene unter Verwendung von $GF(2^{32})$ beschrieben.

[0116] In diesem Fall werden die Eingaben und Ausgaben einer erweiterten S-Box als Elemente von $GF(2^{32})$ betrachtet, um eine MDS höherer Ebene zu entwerfen. Dies ist ein natürliches Entwurfsverfahren in der SPN-Struktur. Es ist jedoch mit der 32-Bit-Breite nicht praktisch, unter Verwendung einer Multiplikationstabelle zu implementieren. Auch eine Implementierung mittels Kalkulationen kann Verarbeitung hoher Geschwindigkeit nicht erreichen, da eine normale MDS-Matrix ein großes Kalkulationsvolumen erfordert. Das Kalkulationsvolumen erhöht sich, da der Prozess beim Übertrag aufwärts bei Multiplikation über dem Galois-Feld heftig ist. Um das Kalkulationsvolumen niederzuhalten, ist ein Verfahren zum Konfigurieren einer MDS-Matrix höherer Ebene unter Verwendung von Elementen, in denen "1"en in nur unteren 5 Bits von 32 Bits (Bits mit Ausnahme der unteren 5 Bits sind zu Null fixiert) in einem Bitausdruck erscheinen, verfügbar. Unter Verwendung einer Matrix, die eine derartige Bedingung erfüllt, kann der Prozess zum Schieben nach oben durch Tabellennachschlag verarbeitet werden, der obere 4 Bits als eine Eingabe verwendet.

[0117] Fig. 9 zeigt ein Beispiel der MDS-Matrix höherer Ebene. Ein primitives Polynom im Fall dieses Beispiels ist $x^{32} + x^{28} + x^{27} + x + 1$.

[0118] Es wird eine MDS höherer Ebene unter Verwendung von $GF(2^4)$ erläutert.

[0119] Fig. 10 zeigt ein Beispiel der MDS-Matrix in diesem Fall. Ein primitives Polynom im Fall dieses Beispiels ist $x^4 + x + 1$.

[0120] In diesem Fall bilden 1-Bit-Daten entsprechend Positionen (die signifikantesten Bits werden in Fig. 10 beispielhaft dargestellt) der Ausgaben, d.h. 8-Bit-Daten von vier S-Boxen in einer erweiterten S-Box **103** 4-Bit-Daten pro Menge, und vier Mengen von 4-Bit-Daten von einer erweiterten S-Box **103** werden als Elemente von $GF(2^4)$ betrachtet.

[0121] Eine Diffusionsschicht **104** zwischen zwei Stufen von vier parallelen erweiterten S-Box-Schichten **103** verwendet MDS-Matrizen mit 4 (Zeilen) × 4 (Spalten) (z.B. **104-1** im Fall der signifikantesten Bits in Fig. 10) in entsprechenden Positionen von 8-Bit-Daten.

[0122] Die vier Mengen von 4-Bit-Daten als Ausgaben werden mit entsprechenden Positionen von entsprechenden Quellen-8-Bit-Daten verbunden.

[0123] Es werden 8 MDS-Matrizen (**104-1** bis **104-8**) als MDS-Matrizen höherer Ebene in Entsprechung mit der Bitbreite von S-Boxen vorbereitet.

[0124] Diese MDS-Matrizen mit 4 (Zeilen) × 4 (Spalten) garantieren die Zweigzahl = 5. Da die einzelnen MDS-Matrizen mit unterschiedlichen Bitpositionen in S-Boxen verbunden sind, wird die Zweigzahl = 5 als ein ganzes garantiert.

[0125] Durch Tabellennachschlag in Einheiten von S-Box-Ausgaben in entsprechenden Positionen von erweiterten S-Boxen (auch durch arithmetische Operationen) kann eine effiziente Implementierung durchgeführt werden, die acht MDS-Matrizen gleichzeitig verarbeitet.

[0126] Falls zyklische MDS-Matrizen verwendet werden, kann ein effizienter Prozess, der Verbindung mit EX-OR in Einheiten von 32 Bits und Bitrotationen in Einheiten von 8 Bits kombiniert, durchgeführt werden.

[0127] Basierend auf der gleichen Idee wie oben beschrieben kann eine Verarbeitung in Einheiten von 2 Bits in entsprechenden Positionen von 8-Bit-Daten durchgeführt werden, und vier MDS-Matrizen von 4 (Zeilen) × 4 (Spalten) ($GF(2^8)$) mit 8-Bit-Elementen können als MDS-Matrizen höherer Ebene vorbereitet werden. Andererseits kann eine Verarbeitung in Einheiten von 4 Bits in entsprechenden Positionen von 8-Bit-Daten durchgeführt werden, und es können zwei MDS-Matrizen von 4 (Zeilen) × 4 (Spalten) ($GF(2^{16})$) mit 16-Bit-Elementen als MDS-Matrizen höherer Ebene vorbereitet werden.

[0128] In der obigen Beschreibung werden Bits in entsprechenden Positionen extrahiert und verarbeitet. Alternativ können Bits in unterschiedlichen Positionen (exklusiv) extrahiert und verarbeitet werden. In Fig. 10 werden vier parallele erweiterte S-Boxen **103** verwendet, aber die Zahl von parallelen erweiterten S-Boxen ist nicht auf einen derartigen spezifischen Wert begrenzt. Auch müssen nicht alle erweiterten S-Boxen die gleiche interne Anordnung haben, und einige von ihnen können unterschiedliche Anordnungen haben. Alle MDS-Matrizen höherer Ebene müssen nicht die gleiche interne Anordnung haben, und einige von ihnen können unterschiedliche Anordnungen haben. Das gleiche trifft auf MDS-Matrizen unterer Ebene und die Eingabe-/Ausgabetabellen von S-Boxen zu. Z.B. können die erste Eingangsstufe und die letzte Ausgangsstufe interne Anordnungen haben, die sich von jenen der Zwischenstufen unterscheiden. Außerdem sind verschiedene andere Variationen verfügbar.

[0129] Nachstehend wird der Schlüsselplanungsteil (Schlüsselgenerator) erläutert.

[0130] Fig. 11 zeigt ein Beispiel der Anordnung des Schlüsselplanungsteils. Bezugszeichen **121** bezeichnet einen Abschnitt entsprechend einer Stufe der Stufenfunktion des Datendiffusionsteils; **131** eine li-

neare Diffusionsschicht (in diesem Beispiel eine Diffusionsschicht unter Verwendung einer MDS-Matrix höherer Ebene); **132** eine nichtlineare Transformationsschicht (in diesem Beispiel vier parallele SP-Schichten (S-Box-Schichten/Diffusionsschichten) **133**); **134** eine EX-OR-Einheit; und **135** einen Restaddierer. Obwohl in Fig. 11 nicht gezeigt, wird die Anordnung des Abschnitts **121** in Entsprechung mit der Zahl von Stufen wiederholt. Wenn die Anordnungseinheit, die einen 128-Bit-Schlüssel ausgibt, als eine Stufe des Schlüsselplanungsteils definiert ist, ist die Zahl vom Schlüsselplanungsteil (2R + 1) (= 17, wenn R = 8 ist).

[0131] In dem in Fig. 11 gezeigten Beispiel werden 128 Bits als die linke Hälfte der Ausgabe jeder Stufe eines 256-Bit modifizierten Feistel-Wiederholungsprozesses extrahiert, und es wird eine stufenzahlabhängige Konstante C_i dazu als ein Rest addiert, um einen erweiterten Schlüssel zu erhalten.

[0132] Wenn die Schlüssellänge z.B. 256 Bits ist, werden die oberen 128 Bits zu der linearen Diffusionsschicht **131** der ersten Stufe eingegeben, und die unteren 128 Bits werden zu der nichtlinearen Transformationsschicht **132** eingegeben. Wenn die Schlüssellänge z.B. 128 Bits ist, werden die 128 Bits zu der linearen Diffusionsschicht **131** der ersten Stufe, und auch zu der nichtlinearen Transformationsschicht **132** eingegeben. Wenn die Schlüssellänge z.B. 192 Bits (= 64 Bits × 3) ist, werden 128 Bits, die durch Koppeln der oberen 64 Bits und der zwischenliegenden 64 Bits erhalten werden, zu der linearen Diffusionsschicht **131** der ersten Stufe eingegeben, und 128 Bits, die durch Koppeln der oberen 64 Bits und der unteren 64 Bits erhalten werden, werden zu der nichtlinearen Transformationsschicht **132** eingegeben.

[0133] Es wird vermerkt, dass die Stelle des Restaddierers **136**, der die stufenzahlabhängige Konstante C_i als einen Rest addiert, verschiedene Variationen haben kann, wie in Fig. 12 gezeigt.

[0134] Fig. 13 zeigt ein Beispiel der Anordnung jeder SP-Schicht **133** der nichtlinearen Transformationsschicht **132** in Fig. 11 und Fig. 12. Bezugszeichen **141** bezeichnet S-Boxen; und **142** eine MDS unterer Ebene zum Empfangen der Ausgaben von den vier parallelen S-Boxen.

[0135] Es wird vermerkt, dass diese S-Box entweder die gleiche wie die oder verschieden von der (Fig. 5) für die Verschlüsselungsverarbeitung sein kann, die in Fig. 4 gezeigt wird. Das gleiche trifft auf die MDS unterer Ebene zu. Die S-Boxen und die MDS unterer Ebene können unterschiedliche Anordnungen in Einheiten von Stufen des Schlüsselplanungsteils haben.

[0136] Fig. 14 zeigt ein anderes Beispiel der Anordnung jeder SP-Schicht **133** der nichtlinearen Transformationsschicht **132** in Fig. 11 und Fig. 12. In diesem Beispiel sind EX-OR-Einheiten **143** der in Fig. 13 gezeigten Anordnung hinzugefügt.

[0137] Des weiteren kann eine Konstante, die mit EX-OR mit der Eingabe zu jeder S-Box zu verbinden ist, eine stufenzahlabhängige Konstante in Fig. 14 sein.

[0138] Nachstehend wird ein Beispiel eines Verfahrens zum Generieren unterschiedlicher Konstanten C_i in einzelnen Stufen erläutert.

[0139] Die 128-Bit additiven Konstante C_i des Schlüsselplanungsteils in Fig. 11 und Fig. 12 werden durch eine Kombination von vier Bitkonstanten (H_0, H_1, H_2, H_3) beschrieben. Beispiele von 32-Bitkonstanten H_i sind:

$$H_0 = (5A827999)_H = \lfloor(\sqrt{2}/4 \times 2^{32})\rfloor$$

$$H_1 = (6ED9EBA1)_H = \lfloor(\sqrt{3}/4 \times 2^{32})\rfloor$$

$$H_2 = (8FIBBCDC)_H = \lfloor(\sqrt{5}/4 \times 2^{32})\rfloor$$

$$H_3 = (CA62C1D6)_H = \lfloor(\sqrt{10}/4 \times 2^{32})\rfloor$$

wobei $\lfloor \times \rfloor$ eine Bodenfunktion ist und eine größte ganze Zahl anzeigt, die nicht größer als x ist.

[0140] Eine Kombination von additiven Konstanten C_i wird durch $C_i = (C_{i0}, C_{i1}, C_{i2}, C_{i3},)$ beschrieben. Um eine leichte Generierung von unterschiedlichen 128-Bit-Konstanten C_i in einzelnen Stufen zu erlauben, werden 8-Bit-LFSRs verwendet, um eine Kombination von H_i zu bestimmen, die C_i bilden. Z.B. wird $(1D)_H$ in dem primitiven Polynom von jedem LFSR verwendet, und $(8B)_H$ wird in dem Anfangszustand von jedem LFSR verwendet. Eine Bitsequenz, die unter Verwendung der LFSRs generiert wird, wird in Einheiten von 2 Bits ausgelesen, um eine 32-Bit-Konstante H_i zu bestimmen, die als die Konstante verwendet wird.

[0141] Fig. 15 zeigt ein Beispiel einer Tabelle additiver Konstanten unter Verwendung der LFSRs durch das zuvor erwähnte Verfahren.

[0142] Es wird vermerkt, dass der Anfangszustand von jedem LFSR variabel oder fixiert sein kann. In dem ersteren Fall definiert der Anfangszustand von jedem LFSR den Schlüssel teilweise. In dem letzteren Fall kann nur eine Entschlüsselungsvorrichtung mit dem gleichen Anfangszustand von jedem LFSR wie dem in der Verschlüsselungsvorrichtung den Chiffretext entschlüsseln.

[0143] Gemäß dem zuvor erwähnten Schlüsselplanungsteil können in jeder SP-Schicht **133**, wenn sich

1 Bit der Eingabe geändert hat, die S-Boxen **141** diese Änderung zu 8 Bits ausbreiten, und die MDS unterer Ebene **142** kann die Änderung zu 32 Bits ausbreiten. Da des weiteren in der linearen Diffusionsschicht die MDS höherer Ebene **131** die Ausgabe von der nichtlinearen Transformationsschicht des vorherigen Zustands zum großen Teil diffundiert, wird eine 1-Bit-Differenz zu der 128-Bit-Breite verbreitet.

[0144] Deshalb generieren, d.h. diffundieren, gemäß dem Schlüsselplanungsteil die jeweiligen Stufen leicht zufällige Schlüssel. Da unterschiedliche Konstanten in Einheiten von Stufen verwendet werden, stimmen Schlüssel unter Stufen selten überein (Schlüssel stimmen kaum überein).

[0145] Es wird vermerkt, das der Schlüsselplanungsteil eine andere Anordnung haben kann.

[0146] Nachstehend wird eine effiziente lineare Diffusionseinrichtung, die in dem Diffusionsteil von Blockverschlüsselungsschemendaten mit einer großen Blocklänge verwendet wird, erläutert.

[0147] Fig. 16 zeigt ein Beispiel der Anordnung eines Galois-Feldmultiplikators als eine Basiskomponente der linearen Diffusionseinrichtung dieser Ausführungsform. Diese lineare Diffusionseinrichtung wird verwendet, um das Produkt einer Eingabe und eines Elementes der MDS-Matrix höherer Ebene in der zuvor erwähnten MDS höherer Ebene (siehe **104** in Fig. 9 und Fig. 4, 131 in Fig. 11 und Fig. 12) unter Verwendung von $GF(2^{32})$ oder $GF(2^{16})$ zu kalkulieren.

[0148] Wie in Fig. 16 gezeigt, umfasst der Galois-Feldmultiplikator eine Koeffizientenspeichereinheit **202**, einen Multiplikator **203**, eine Übertragrückgabeeinheit **201** und eine EX-OR-Einheit **204**.

[0149] Die Koeffizientenspeichereinheit **202** speichert einen Koeffizienten, d.h. einen Multiplikator einer Multiplikation (z.B. ein Element der MDS-Matrix höherer Ebene in Fig. 9).

[0150] Der Multiplikator **203** multipliziert das Eingabewort und einen Koeffizienten, wenn sie binäre Werte sind.

[0151] Wenn der Koeffizient der Koeffizientenspeichereinheit **202** eine Potenz von 2 wie 1, 2, 4, ... ist, wird eine Kalkulation unter Verwendung eines normalen Multiplikators durchgeführt. Falls andererseits der Multiplikator ein spezifischer ist, der keinerlei Übertrag verbreitet, wird eine Kalkulation durchgeführt, wenn der Koeffizient der Koeffizientenspeichereinheit **202** ein beliebiger Wert ist.

[0152] Die Übertragrückgabeeinheit **201** sucht nach einem Wert (Rückgabewort), der durch die EX-OR-Einheit **204** zu addieren ist, um einen Übertrag als ein Ergebnis von Multiplikation zu Multiplikation über das Galois-Feld zurückzukoppeln.

[0153] Die EX-OR-Einheit **204** verknüpft die Ausgabe von dem Multiplikator **203** und die Ausgabebits der Übertragrückgabeeinheit **201** über exklusives OR.

[0154] Die Funktion des Galois-Feldmultiplikators **200** besteht darin, ein Produkt von a × b eines Eingabewortes "a" als ein Element eines Erweiterungsfeldes des $GF(2^k)$ eines Galois-Feldes GF(2) und eines Koeffizienten "b" als ein anderes Element dieses Galois-Feldes als ein Ausgabewort zu kalkulieren.

[0155] Das Produkt in dem Galois-Feld wird nachstehend beschrieben.

[0156] In der folgenden Beschreibung reichen i und j bei Kalkulation von Gesamtsummen in $\Sigma a_i x^i$ und $\Sigma b_j x^j$ von 0 bis k – 1, und eine Beschreibung dieser Bereiche wird weggelassen.

[0157] Elemente von $GF(2^k)$ werden als ein Polynom $\Sigma a_i x^i$ (k – 1)-ter Ordnung in einer gegebenen Variablen x durch einen Polynomausdruck ausgedrückt. Element "a" wird häufig durch Anordnen seiner Koeffizienten wie c_{k-1}, c_{k-2}, ..., c_0 ausgedrückt.

[0158] Das Produkt von zwei Elementen "a" = $\Sigma a_i x^i$ und b = $\Sigma b_j x^j$ wird durch:

$$a \times b = (\Sigma a_i x^i a) \times (\Sigma b_i x^i) \bmod p(x)$$

definiert, wobei p(x) ein primitives Polynom von $GF(2^k)$ genannt wird, und ein nicht reduzierbares normiertes Polynom k-ter Ordnung ist. Auch bedeutet "mod", dass z.B. wenn k = 32 und $p(x) = x^{32} + x^{28} + x^{27} + x + 1$ als ein primitives Polynom gewählt wird, falls der Term von x^{32} oder Faktor als ein Produkt des Polynoms erscheint, es als $(x^{28} + x^{27} + x + 1)$ betrachtet wird. Deshalb ist das Produkt auch ein Polynom von Ordnung k oder kleiner.

[0159] Im allgemeinen wird bei Ausführung einer derartigen Operation ein Multiplikator, der eine Multiplikationstabelle verwendet, die nach einem Produkt unter Verwendung eines Multiplikators und eines Multiplikanden als Tags sucht, häufig verwendet, um Verarbeitung hoher Geschwindigkeit zu erzielen. Da jedoch sowohl der Multiplikator als auch der Multiplikand 2^k Werte annehmen können, hat die Multiplikationstabelle 2^{2k} Einträge, jeder mit einer k-Bit-Größe. Wenn k zu einem gewissen Ausmaß groß wird, hat die Multiplikationstabelle aus diesem Grund eine sehr große Größe.

[0160] Diese Ausführungsform ist dem Verfahren, das die Multiplikationstabelle verwendet, grundsätzlich ähnlich, wenn aber Koeffizienten eine gegebene

Einschränkungsbedingung erfüllen, wird eine derartige Tabelle durch eine viel kleinere Speichergröße implementiert.

[0161] In dieser Einschränkungsbedingung ist Koeffizient b eine Konstante, und nur Koeffizienten unterer Ordnung einer gegebenen Ordnung t oder kleiner haben Koeffizienten ungleich Null (Koeffizienten, die die t-te Ordnung überschreiten, sind 0, und Koeffizienten der t-ten Ordnung oder kleiner sind 0 oder 1). Wenn ein gegebenes Element "a" ein beliebiges Element annimmt, wird ein Maximum eines 32-Bit-Übertrags generiert, wenn aber diese Einschränkungsbedingung erfüllt ist, wird höchstens ein t-Bit-Übertrag generiert. Der t-Bit-Übertragwert wird durch das MSB (signifikanteste Bits) innerhalb des oberen t-Bit-Bereichs von Multiplikator "a" bestimmt.

[0162] Die Differenz zwischen Multiplikation über dem Galois-Feld und dem, was als ein normales Polynom betrachtet wird, ist, dass wenn ein Übertrag zu einem Koeffizienten der 32. Ordnung oder höher als ein Produkt von binären Werten generiert wird, ein Beitrag dieses Übertrags zu Koeffizienten von kleiner als der 32. Ordnung durch das primitive Polynom zurückgegeben werden muss, aber die Übertragrückgabeeinheit **201** Worte hat, die in der Form einer Tabelle in dieser Ausführungsform zurückzugeben sind.

[0163] Dieses Rückgabewort wird durch Koeffizienten b von höchstens (t + 1) Bits, obere t Bits von Multiplikand "a" und einem primitiven Polynom bestimmt. D.h. das Rückgabewort ergibt sich durch (a[(k – t) ... (k – 1)] × b)[(t + 1) ... 2t] mod p(x), wobei a[(k – t) ... (k – 1)] Terme von der (k – 1)-ten Ordnung zu der (k – t)-ten Ordnung von "a" extrahiert.

[0164] D.h. der Inhalt der Rückgabeworttabelle der Übertragrückgabeeinheit **201** wird in Entsprechung mit Elementen der entsprechenden MDS-Matrix bestimmt (siehe Fig. 9).

[0165] Die Rückgabeworttabelle der Übertragrückgabeeinheit **201** hat 2^t Einträge, jeder mit einer k-Bit-Größe.

[0166] Die lineare Transformationssektion, die unter Verwendung des zuvor erwähnten Galois-Feldmultiplikators implementiert ist und die linearen Transformationen von Datenblöcken eines Blockverschlüsselungsschemas kalkuliert, wird nachstehend beschrieben.

[0167] Lineare Transformation unter Verwendung einer MDS-Matrix ist als eine Art linearer Transformation bekannt. Die MDS-Matrix ist eine Matrix mit n (Zeilen) × n (Spalten), in der ein Datenblock aus einer Vielzahl von (n) Worten besteht, und wenn jedes Wort eine k-Bit-Länge hat, wird es als ein Element eines Galois-Feldes GF(2^k) betrachtet, und die eine Menge von n Elementen auf eine Menge von n Elementen linear abbildet, und alles kleine Matrizen ungleich Null hat. Lineare Transformation basierend auf der MDS-Matrix kann die untere Grenze der Zahl von Eingabe-/Ausgabeworten ungleich Null garantieren.

[0168] Im allgemeinen enthält jedoch eine Matrixoperation über dem Galois-Feld GF(2^k) mehrere Male von Multiplikation und Addition über dem GF(2^k), was zu hohen Kalkulationskosten führt.

[0169] Fig. 17 zeigt ein Beispiel der Anordnung der linearen Transformationssektion dieser Ausführungsform. Diese lineare Transformationssektion wird in der zuvor erwähnten MDS höherer Ebene (**104** in Fig. 9 und Fig. 4, 131 in Fig. 11 und Fig. 12) unter Verwendung von GF(2^{32}) oder GF(2^{16}) verwendet.

[0170] In der in Fig. 17 gezeigten Anordnung sind die Galois-Feldmultiplikatoren, die in Fig. 16 gezeigt werden, in einem Matrixmuster in Entsprechung mit der MDS-Matrix vorbereitet.

[0171] Falls m = n in Fig. 17 ist, nimmt ein Koeffizient von jedem von n^2 Galois-Feldmultiplikatoren **200** den gleichen Wert wie das entsprechende Element einer MDS-Matrix mit n (Zeilen) × n (Spalten) an. Eine Einrichtung mit einem Koeffizienten a_{ij} empfängt das i-te Eingabewort.

[0172] Die EX-OR-Einheiten **205** entsprechend jeweiligen Ausgabeworten kalkulieren EX-ORs von Ausgabebits von allen der Galois-Feldmultiplikatoren **200** mit Koeffizienten a_{ij} entsprechend einem gegebenen j, und geben sie als die j-ten Ausgabeworte aus.

[0173] Fig. 18 zeigt ein anderes Beispiel der Anordnung der linearen Transformationssektion dieser Ausführungsform. Gemäß der linearen Transformationssektion dieses Beispiels haben, wenn eine MDS-Matrix, die lineare Transformation ausdrückt, durch (a_{ij}) ausgedrückt wird, nur Terme der t-ten Ordnung oder kleiner von jedem Element a_{ij} Koeffizienten ungleich Null. Es wird angenommen, dass i und j eine ganze Zahl annehmen können, die von 0 bis n – 1 reicht. Auch ist t ein positiver Wert kleiner als die Erweiterungsordnung k des Galois-Feldes GF(2^k).

[0174] Auf diese Weise ist die in Fig. 18 gezeigte Multiplikation implementiert.

[0175] Es wird vermerkt, dass der Inhalt der Rückgabeworttabelle der Übertragrückgabeeinheit **201** in Übereinstimmung mit den entsprechenden Elementen der MDS-Matrix bestimmt wird. Deshalb sind in dem Beispiel der MDS-Matrix höherer Ebene, die in Fig. 9 gezeigt wird, nur vier unterschiedliche Rückgabeworttabellen vorbereitet.

[0176] Es wird nachstehend eine MDS-Matrix-Generierungssektion (oder zufälliger Generierungsalgorithmus) zum Generieren einer MDS-Matrix (besonders MDS höherer Ebene) erläutert, die in dem Verschlüsselungssystem der vorliegenden Erfindung verwendet wird.

[0177] Fig. 19 zeigt ein Beispiel der Anordnung der MDS-Matrix-Generierungssektion. Wie in Fig. 19 gezeigt, umfasst die MDS-Matrix-Generierungssektion einen Elementgenerator **231**, eine Kalkulationseinheit einer kleinen Determinante **232** und eine Diskriminationseinheit **233**.

[0178] Fig. 20 zeigt ein Beispiel der Sequenz in diesem Fall.

[0179] Der Elementgenerator **231** generiert zufällig Matrixelemente einer MDS-Matrix mit n (Zeilen) × n (Spalten) (Schritt S1). Wenn dem zuvor erwähnten Galois-Feldmultiplikator erlaubt wird, angewendet werden, wird eine MDS-Matrix generiert, in der nur untere t Bits aus Elementen ungleich Null bestehen (Elemente der t-ten Ordnung oder kleiner) (d.h. in diesem Fall prüft der Elementgenerator **231**, ob nur untere t Bits ungleich Null sind).

[0180] Um Matrixelemente zu generieren, sind verschiedene Verfahren verfügbar, wie etwa ein Verfahren zum Generieren und Verwenden zufälliger Zahlen, ein Verfahren zum Verwenden von Steuerungsvariablenwerten von vielen Schleifen und dergleichen.

[0181] Die Kalkulationseinheit einer kleinen Determinante **232** kalkuliert kleine Determinanten 1. Ordnung der Matrix, die durch den Elementgenerator **231** generiert wird (Schritt S2), und die Diskriminationseinheit **233** prüft, ob die kleine Determinante, die durch die Kalkulationseinheit einer kleinen Determinante **232** kalkuliert wird, ungleich Null ist (Schritt S3). Falls mindestens eine kleine Determinante 1. Ordnung gleich Null gefunden wird, wird die Verarbeitung von Schritt S1 erneut durchgeführt.

[0182] Falls alle kleinen Determinanten 1. Ordnung ungleich Null sind, werden kleine Determinanten 2. Ordnung ähnlich geprüft (Schritte S4 und S5).

[0183] Der zuvor erwähnte Prozess wird bis zu kleinen Determinanten n-ter Ordnung wiederholt (Schritte S6 und S7), und falls bestätigt wird, dass alle kleinen Determinanten von der 1. Ordnung bis zu der n-ten Ordnung ungleich Null sind, wird diese MDS-Matrix ausgegeben (Schritt S8).

[0184] Wenn die in Schritt S8 erhaltene MDS-Matrix bei Verschlüsselung verwendet wird, ergibt sich eine MDS-Matrix, die bei Entschlüsselung verwendet wird, durch eine Umkehrmatrix der MDS-Matrix, die in Schritt S8 erhalten wird (wenn umgekehrt die MDS-Matrix, die in Schritt S8 erhalten wird, bei Entschlüsselung verwendet wird, wird ihre Umkehrmatrix als eine MDS-Matrix verwendet wird, die bei Verschlüsselung verwendet wird).

[0185] Es wird vermerkt, dass selbst wenn alle Elemente der MDS-Matrix, die in Schritt S8 erhalten wird, nur untere t Bits ungleich Null haben, alle Elemente ihre Umkehrmatrix nicht immer nur untere t Bits ungleich Null haben.

[0186] In der in Fig. 20 gezeigten Sequenz werden kleine Determinanten der Reihe nach von der 1. Ordnung bis zu der n-ten Ordnung geprüft, können aber auch in anderen Ordnungen geprüft werden, oder alle oder einige dieser Determinanten können parallel geprüft werden.

[0187] Nachstehend wird ein Verfahren zum Erhalten von MDS-Matrizen erläutert, sodass sowohl die MDS-Matrix, die bei Verschlüsselung verwendet wird, als auch die, die bei Entschlüsselung als die Umkehrmatrix der ersteren Matrix verwendet wird, eine Bedingung erfüllen, dass nur untere t Bits ungleich Null sind.

[0188] Fig. 21 zeigt ein Beispiel der Anordnung der MDS-Matrix-Generierungssektion in diesem Fall. Wie in Fig. 21 gezeigt, umfasst die MDS-Matrix-Generierungssektion den Elementgenerator **231**, die Kalkulationseinheit einer kleinen Determinante **232**, die Diskriminationseinheit **233**, einen Umkehrmatrixgenerator **234** und eine Umkehrmatrix-Diskriminationseinheit **235**. Der Elementgenerator **231**, die Kalkulationseinheit einer kleinen Determinante **232** und die Diskriminationseinheit **233** sind die gleichen wie jene in Fig. 19.

[0189] Fig. 22 zeigt ein Beispiel der Sequenz in diesem Fall.

[0190] Wie in dem obigen Beispiel generieren der Elementgenerator **231**, die Kalkulationseinheit einer kleinen Determinante **232** und die Diskriminationseinheit **233** eine MDS-Matrix, bestehend aus Elementen, von denen nur untere t Bits ungleich Null sind (Schritt S11).

[0191] Der Umkehrmatrixgenerator **234** generiert eine Umkehrmatrix der generierten MDS-Matrix (Schritt S12).

[0192] Die Umkehrmatrix-Diskriminationseinheit **235** prüft, ob nur untere t Bits von jedem Element der erhaltenen Umkehrmatrix ungleich Null sind.

[0193] Falls nur untere t Bits aller Elemente ungleich Null sind (Schritt S13), werden diese MDS-Matrix und Umkehrmatrix ausgegeben (Schritt S14).

[0194] Falls mindestens ein Element gefunden wird, untere t Bits ungleich Null zu haben (Schritt S13), wird die Verarbeitung von Schritt S11 erneut durchgeführt.

[0195] Wenn die in Schritt S11 generierte MDS-Matrix bei Verschlüsselung verwendet wird, wird die in Schritt S12 generierte Umkehrmatrix bei Entschlüsselung verwendet (wenn umgekehrt die in Schritt S11 generierte MDS-Matrix bei Entschlüsselung verwendet wird, wird die in Schritt S12 generierte Umkehrmatrix bei Verschlüsselung verwendet).

[0196] Bei Generieren einer MDS-Matrix kann eine MDS-Matrix, in der Elemente mit identischen Werten in identischen Zeilen nicht vorhanden sind (in einer MDS-Matrix mit n (Zeilen) × n (Spalten) enthalten die (i1)-ten bis (in)-ten Elemente nicht zwei oder mehr Elemente mit identischen Werten), generiert werden. In den Beispielen der Sequenzen, die in Fig. 20 und Fig. 22 gezeigt werden, wird z.B. bei Generieren einer MDS-Matrix bestimmt, ob Elemente mit identischen Werten in einer einzelnen Zeile vorhanden sind, und falls Elemente mit identischen Werten in einer einzelnen Zeile gefunden werden, kann die MDS-Matrix generiert werden. Es wird vermerkt, dass Elemente mit identischen Werten in einer einzelnen Zeile vorhanden sein können.

[0197] Unter Verwendung einer linearen Transformationssektion, die eine MDS-Matrix auswählt, in der Elemente mit identischen Werten in einer einzelnen Zeile nicht vorhanden sind, als eine lineare Transformationssektion von Blockverschlüsselungsschemendaten wird die Wahrscheinlichkeit reduziert, dass differenzielle Werte von Eingabeworten einander aufheben.

[0198] Andererseits kann eine MDS-Matrix, in der die Summe von Elementen in einer einzelnen Zeile nicht 1 oder 0 ist, generiert werden. In diesem Fall wird der gleiche Effekt erhalten.

[0199] Nachstehend wird ein Verfahren zum Verbessern von Sicherheit durch Auswählen (oder Optimieren) der Kombination von S-Box und MDS unterer Ebene, und genauer ein Entwurfsverfahren einer Kombination von S-Box und MDS unterer Ebene, das garantieren kann, dass die maximale differenzielle charakteristische Wahrscheinlichkeit besser als das theoretische schlechteste Beispiel wird, beschrieben.

[0200] Da MDS nur die Zweigzahl B garantiert, falls p die maximale differenzielle Wahrscheinlichkeit von S-Boxen darstellt, ist die maximale differenzielle charakteristische Wahrscheinlichkeit p^B. Z.B. hat eine MDS mit m (Zeilen) × m (Spalten) B = m + 1. Durch Auswählen (Optimieren) der Kombination von S-Box und MDS unterer Ebene wird jedoch eine maximale differenzielle charakteristische Wahrscheinlichkeit von kleiner als p^B durch die Zweigzahl B garantiert. Als ein Ergebnis wird durch Kombinieren einer MDS einer kleineren maximalen differenziellen Wahrscheinlichkeit als eine normale MDS mit S-Boxen ein synergetischer Effekt erwartet, und Sicherheit wird weiter verbessert.

[0201] Als Sicherheitsevaluierungsschemata eines Verschlüsselungsalgorithmus sind differenzielle Kryptoanalyse und lineare Kryptoanalyse bekannt, und sie haben Dualität. Bei Betrachtung differenzieller Kryptoanalyse wird die Sicherheit von S-Boxen durch die Wahrscheinlichkeit spezifiziert, dass die Eingabe und Ausgabe differenzielle Korrelation aufweisen, und mit abnehmender Wahrscheinlichkeit höher ist. In dem Verschlüsselungsalgorithmus wird die Sicherheit verbessert, da eine große Zahl von S-Boxen mit einer kleineren differenziellen Wahrscheinlichkeit kombiniert werden. Als ein effizientes Kopplungsverfahren von S-Boxen wurde konventionell eine lineare Transformationssektion vorgeschlagen. Die lineare Transformationssektion kalkuliert die lineare Transformation von Daten mit einer gegebenen Blocklänge, und wird als eine Komponente einer Verschlüsselungsvorrichtung (und einer Entschlüsselungsvorrichtung) verwendet. Lineare Transformation, die eine MDS-Matrix verwendet, ist als eine Art linearer Transformation bekannt.

[0202] Eine MDS-Matrix definiert lineare Transformation zu n Worten, wenn ein Datenblock aus einer Vielzahl von (n) Worten hergestellt wird, und garantiert (n + 1) oder mehr Eingabe-/Ausgabeworte ungleich Null. Da jedoch eine S-Box eine Vielzahl von Kandidatenwerten, wie etwa 6/256, 4/256, 2/256 und dergleichen als eine differenzielle Wahrscheinlichkeit hat, kann eine MDS, in der jede von (n + 1) Wahrscheinlichkeiten 4/256 ist, eine höhere Sicherheit sicherstellen als eine MDS, in der jede von (n + 1) Wahrscheinlichkeiten 6/256 ist.

[0203] Konventionell werden die Sicherheiten der S-Box und MDS einzeln als alleinige Aufbauelemente evaluiert. In dieser Ausführungsform wird ein Beispiel einer Einrichtung zum Verifizieren des Synergismus der S-Box und MDS beschrieben.

[0204] Fig. 23 zeigt ein Beispiel der Verarbeitungssequenz in diesem Fall. Dieses Beispiel schenkt differenzieller Kryptoanalyse Beachtung, und zeigt einen Prozess zum Bestimmen einer MDS, die Synergismus mit der S-Box erwarten kann. Da differenzielle Kryptoanalyse und lineare Kryptoanalyse Dualität haben, wird der gleiche Effekt für lineare Kryptoanalyse erhalten, wenn dieser Prozess in Anbetracht der linearen Wahrscheinlichkeit durchgeführt wird.

[0205] Es werden eine Vielzahl von S-Box-Kandidaten und eine Vielzahl von MDS-Kandidaten unterer Ebene generiert (Schritte 521 und S22). Es wird ver-

merkt, dass Schritte S21 und S22 in der umgekehrten Reihenfolge ausgeführt werden können, oder parallel ausgeführt werden können.

[0206] Es wird einer der S-Box-Kandidaten ausgewählt (Schritt S23), und es wird einer der MDS-Kandidaten unterer Ebene ausgewählt (Schritt S24). Es wird vermerkt, dass Schritte S23 und S24 in der umgekehrten Reihenfolge ausgeführt werden können, oder parallel ausgeführt werden können.

[0207] Wie später beschrieben wird, wird eine maximale Differenz effektiver (aktiver) S-Boxen kalkuliert (Schritt S25), und es wird bestimmt, ob eine Differenz (z.B. 4/256) kleiner als eine obere Grenze (z.B. 6/256) enthalten ist.

[0208] Falls eine derartige Differenz enthalten ist (Schritt S26), wird eine Kombination der S-Box und der MDS unterer Ebene zu dieser Zeit ausgegeben (Schritt S27).

[0209] Falls andererseits keine derartige Differenz enthalten ist (Schritt S26), wird/werden eine oder beide der S-Box und der MDS unterer Ebene erneut ausgewählt, um den zuvor erwähnten Prozess zu wiederholen.

[0210] In Fig. 23 werden anfangs eine Vielzahl von S-Box-Kandidaten und eine Vielzahl von MDS-Kandidaten unterer Ebene generiert. Alternativ können andere Kandidaten als die erste Menge generiert werden, wenn die Bedingung in Schritt S26 nicht erfüllt ist und eine andere S-Box oder MDS ausgewählt werden muss.

[0211] Die tatsächlichen Prozesse in Schritten S25 und S26 werden wie folgt ausgeführt.

[0212] In dem Beispiel der erweiterten S-Box **103** in Fig. 6 werden die folgenden vier unterschiedlichen Typen von Verifikationen (insgesamt 20 unterschiedliche Verifikationen) für eine Kombination von S-Box und MDS unterer Ebene durchgeführt, und wenn alle Bedingungen erfüllt sind, wird die Menge von S-Boxen und MDS unterer Ebene zu dieser Zeit in Schritt S27 ausgegeben.

(1) Wenn eine S-Box **112** allein auf der Eingangsseite der MDS unterer Ebene **113** aktiviert wird, wird bestimmt, dass diese Verifikation erfolgreich ist, falls alle vier S-Boxen **112** auf der Ausgangsseite der MDS unterer Ebene **113** aktiviert werden und mindestens eine von ihnen eine Differenz hat, die kleiner als die obere Grenze ist. Diese Verifikation wird für jede der vier S-Boxen **112** auf der Eingangsseite durchgeführt (es gibt vier unterschiedliche Muster).

(2) Wenn nur zwei S-Boxen **112** auf der Eingangsseite der MDS unterer Ebene **113** aktiviert werden, wird bestimmt, falls alle vier S-Boxen **112** auf der Ausgangsseite der MDS unterer Ebene **113** aktiviert werden, dass diese Verifikation erfolgreich ist, und falls drei S-Boxen **112** auf der Ausgangsseite der MDS unterer Ebene **113** aktiviert werden, und mindestens eine von ihnen eine Differenz hat, die kleiner als die obere Grenze ist, wird bestimmt, dass diese Verifikation erfolgreich ist. Diese Verifikation wird für jede von Kombinationen von zwei S-Boxen auf der Eingangsseite durchgeführt (es gibt sechs unterschiedliche Muster).

(3) Wenn nur zwei S-Boxen **112** auf der Ausgangsseite der MDS unterer Ebene **113** aktiviert werden, wird bestimmt, falls alle vier S-Boxen auf der Eingangsseite der MDS unterer Ebene **113** aktiviert werden, dass diese Verifikation erfolgreich ist, und falls drei S-Boxen **112** auf der Eingangsseite der MDS unterer Ebene **113** aktiviert werden, und mindestens eine von ihnen eine Differenz hat, die kleiner als die obere Grenze ist, wird bestimmt, dass diese Verifikation erfolgreich ist. Diese Verifikation wird für jede von Kombinationen von zwei S-Boxen auf der Ausgangsseite durchgeführt (es gibt sechs unterschiedliche Muster).

(4) Wenn eine S-Box **112** allein auf der Ausgangsseite der MDS unterer Ebene **113** aktiviert wird, wird bestimmt, dass diese Verifikation erfolgreich ist, falls alle vier S-Boxen **112** auf der Eingangsseite der MDS unterer Ebene **113** aktiviert werden und mindestens eine von ihnen eine Differenz hat, die kleiner als die obere Grenze ist. Diese Verifikation wird für jede der vier S-Boxen **112** auf der Ausgangsseite durchgeführt (es gibt vier unterschiedliche Muster).

[0213] Die Vielzahl von Verifikationsprozessen kann sequenziell durchgeführt werden, oder es können alle oder einige von ihnen parallel durchgeführt werden. Falls einer aus der Vielzahl von Verifikationsprozessen nicht erfolgreich ist, können alle anschließenden Verifikationsprozesse für diese Kombination von S-Box und MDS unterer Ebene aufgehoben werden, und es kann bestimmt werden, dass die Verifikation nicht erfolgreich ist.

[0214] In dem Beispiel der in Fig. 23 gezeigten Sequenz wird der Prozess abgebrochen, wenn die erste Kombination von S-Box und MDS unterer Ebene erhalten wird, die die Bedingungen erfüllt. Alternativ kann eine Vielzahl von Kombinationen von S-Boxen und MDS unterer Ebene erhalten werden, die die Bedingungen erfüllen, und die beste evaluierte von diesen Kombinationen kann ausgewählt werden.

[0215] Es wurde die Verschlüsselungsvorrichtung erläutert. Nachstehend wird eine Entschlüsselungsvorrichtung erläutert.

[0216] Die Entschlüsselungsvorrichtung hat eine

Struktur, die durch Umkehrung der der Verschlüsselungsvorrichtung erhalten wird (es wird der gleiche Schlüssel verwendet).

[0217] Fig. 24 zeigt ein Beispiel der Anordnung einer Entschlüsselungsvorrichtung entsprechend der Verschlüsselungsvorrichtung, die in Fig. 4 gezeigt wird.

[0218] Fig. 25 zeigt ein Beispiel der internen Anordnung der Umkehrtransformation einer erweiterten S-Box entsprechend Fig. 6.

[0219] Fig. 26 zeigt ein Beispiel der Struktur einer Stufe der Umkehrtransformation eines Datenrandomisierungsteils entsprechend **Fig.** B.

[0220] In Fig. 24 hat ein Schlüsselplanungsteil der Entschlüsselungsvorrichtung die gleiche Anordnung wie die der Verschlüsselungsvorrichtung, die in Fig. 4 gezeigt wird.

[0221] Die Eingabe-/Ausgabetabelle jeder S-Box **1112**, eine MDS-Matrix unterer Ebene jeder MDS unterer Ebene **1113** und eine MDS-Matrix höherer Ebene einer MDS höherer Ebene **1104** haben Umkehrfunktionen (Umkehrmatrizen) der Eingabe-/Ausgabetabelle jeder S-Box **112** (z.B. Fig. 5), der MDS-Matrix unterer Ebene jeder MDS unterer Ebene **113** (z.B. Fig. 7) und der MDS-Matrix höherer Ebene der MDS höherer Ebene **104** (z.B. Fig. 9 und Fig. 10) in der Verschlüsselungsvorrichtung.

[0222] In Fig. 24 wird der Schlüssel in der gleichen Reihenfolge wie in Fig. 4 generiert, kann aber in einer Reihenfolge entgegengesetzt zu Fig. 4 generiert werden.

[0223] Fig. 27 zeigt ein Beispiel der Anordnung des Schlüsselplanungsteils in einem derartigen Fall.

[0224] Bezugszeichen **1132** bezeichnet eine Umkehrtransformation der nichtlinearen Transformationsschicht **132** von Fig. 11 (einschließlich vier paralleler Umkehrtransformationen der SP-Schichten **133** (z.B. die Eingaben und Ausgaben in Fig. 13 oder Fig. 14 sind umgekehrt)).

[0225] Die Eingabe-/Ausgabetabelle jeder S-Box, MDS-Matrix unterer Ebene, MDS-Matrix höherer Ebene, die in dem in Fig. 27 gezeigten Schlüsselplanungsteil verwendet werden, haben Umkehrfunktionen (Umkehrmatrizen) von jenen, die in dem Schlüsselplanungsteil in Fig. 11 verwendet werden.

[0226] Es wird angenommen, dass eine Dechiffrierschlüsseleingabe K' in Fig. 27 der Schlüssel ist, der in der letzten Schlüsseladdition in Fig. 4 verwendet wird (für die Verschlüsselungsvorrichtung).

[0227] In diesem Fall sind ebenso verschiedene Variationen der Stellen, wo die stufenzahlabhängigen Konstanten C_i als Reste addiert werden, zusätzlich zu dem gleichen Verfahren wie in Fig. 12 verfügbar.

[0228] Das Beispiel eines 128-Bit-Blockverschlüsselungsschemas äquivalent zu AES, das 8-Bit-S-Boxen verwendet, wurde als ein Anwendungsbeispiel verschachtelter (rekursiver) SPN-Verschlüsselung als eine Kombination lokaler Diffusion (Diffusion unterer Ebene) und Diffusion über der Blockbreite (Diffusion höherer Ebene) beschrieben. Es wird eine andere Ausführungsform beschrieben, die ein Beispiel eines 64-Bit-Blockverschlüsselungsschemas äquivalent zu AES verwendet, das 8-Bit-S-Boxen verwendet (es werden hauptsächlich Abschnitte erläutert, die sich unterscheiden, da 64 Bits an Stelle von 128 Bits verwendet werden).

[0229] Ein Beispiel der Anordnung der zweiten Ausführungsform eines 64-Bit-Blockverschlüsselungsschemas, Verschlüsselungsvorrichtung/Entschlüsselungsvorrichtung oder Verschlüsselungsalgorithmus/Entschlüsselungsalgorithmus, was nachstehend zu beschreiben ist, entspricht einem Fall, worin zwei parallele nichtlineare Transformationsmodule **2** (in dem Beispiel erweiterte S-Boxen) in der in Fig. 1 gezeigten Basisanordnung verwendet werden.

[0230] Wie im oben erwähnten 128-Bit-Blockverschlüsselungsschema kann ein 64-Bit-Blockverschlüsselungsschema Widerstandsfähigkeit gegenüber Angriffen verbessern.

[0231] Ein Beispiel der hierarchischen Struktur des Datendiffusionsteils verschachtelter Verschlüsselung ist das gleiche wie das, das in Fig. 3 gezeigt wird.

[0232] Die Blocklänge ist 64 Bits.

[0233] Die Schlüssellänge ist 128 Bits als ein Beispiel (natürlich kann die vorliegende Erfindung für andere Blocklängen praktiziert werden). Später wird ein Fall beschrieben, worin die Schlüssellänge = 64 Bits oder 96 Bits ist, wenn die Blocklänge = 64 Bits ist.

[0234] Als ein Beispiel der Zahl von Stufen (ein Paar aus einer Vielzahl von parallelen erweiterten S-Boxen und einer MDS höherer Ebene (die letzte Stufe enthält keinerlei MDS höherer Ebene, wie später beschrieben wird) wird als eine Stufe gezählt) wird R = 6 verwendet. Es wird vermerkt, dass die Zahl von Stufen grundsätzlich nicht besonders begrenzt ist. Die tatsächliche Zahl von Stufen wird jedoch in Anbetracht von Sicherheit, Computerressourcen und dergleichen geeignet eingestellt, und es ist effektiver, sechs oder mehr Stufen einzustellen.

[0235] Bei Verschlüsselung dieser Ausführungsform entspricht eine Stufe zwei Stufen in einer nor-

malen Struktur, da eine Stufenfunktion zwei S-Box-Schichten enthält. Bezüglich einer MDS höherer Ebene in der Stufenstruktur werden einige Implementierungsbeispiele basierend auf Galois-Feldern erläutert.

[0236] Fig. 28 zeigt ein Beispiel der Anordnung einer Verschlüsselungsvorrichtung gemäß dieser Ausführungsform.

[0237] Bezugszeichen **2101** bezeichnet jede Stufe; **2104** eine MDS-Diffusionsschicht höherer Ebene; **2102** eine erweiterte S-Box-Schicht; und **2103** einzelne erweiterte S-Boxen. Bezugszeichen **2105** bezeichnet eine EX-OR-Einheit. Bezugszeichen **2121** bis **2124** bezeichnen Komponenten eines Schlüsselplanungsteils (Details werden später beschrieben). Bezugszeichen P bezeichnet einen 64-Bit-Klartext als eine Eingabe; und C einen 64-Bit-Chiffretext als eine Ausgabe. Es wird vermerkt, dass jede erweiterte S-Box **2103** die gleiche wie die erweiterte S-Box **103** in Fig. 4 sein kann.

[0238] Die Stufenfunktion hat eine Struktur, in der zwei parallele 32-Bit-Verarbeitungsteilblöcke (erweiterte S-Boxen) **2103**, jeder bestehend aus einer zweistufigen SPN-Struktur, nebeneinander gestellt sind, und ihre Ausgaben durch die MDS-Diffusionsschicht **2104** gekoppelt sind. Die gesamte Basisstruktur ist durch Wiederholungen dieser Stufenfunktion definiert.

[0239] In dem Beispiel von Fig. 28 ist, um symmetrische Verschlüsselungs- und Entschlüsselungsprozesse zu erzielen, die letzte Stufe durch nur die erweiterte S-Box-Schicht **2102** und einen Schlüsseladdierer **2105** aufgebaut, verbunden mit der Ausgabe der erweiterten S-Box-Schicht **2102**.

[0240] Da zwei Stufen von SPN-Strukturen in einer Stufe einer Stufenfunktion eingebettet sind, und Schlüsseladdition in dem Ende des Prozesses durchgeführt wird, ist die Bitlänge eines erweiterten Schlüssels $2 \times 64 \times R + 64 = 64 (2R + 1)$. Wenn $R = 6$ ist, ist die Bitlänge 128×13 Bits.

[0241] Jede S-Box kann entweder eine Eingabe-/Ausgabetabelle oder einen arithmetischen Prozess verwenden, wie oben beschrieben wird. Ein Beispiel der Eingabe-/Ausgabetabelle der 8-Bit-S-Box ist das gleiche wie das, was in Fig. 5 gezeigt wird.

[0242] Ein Beispiel der internen Anordnung der erweiterten S-Box **2103** ist das gleiche wie das, was in Fig. 6 gezeigt wird. Die Diffusionsschicht **113** in der erweiterten S-Box verwendet ähnlich die MDSL-Matrix, die in Fig. 7 gezeigt wird, und führt Multiplikation durch, während die S-Box-Eingaben und Ausgaben und Matrixelemente als Elemente eines Galois-Feldes $GF(2^8)$ betrachtet werden.

[0243] Die Struktur höherer Ebene als die Stufenfunktion von Verschlüsselung dieses Beispiels wird nachstehend erläutert.

[0244] Fig. 29 zeigt ein Beispiel der Anordnung des Abschnitts für eine Stufe eines Randomisierungsteils. Die Struktur höherer Ebene als eine Stufenfunktion von Verschlüsselung dieses Beispiels ist durch Koppeln von zwei parallelen 32-Bit erweiterten S-Boxen **2103** (siehe Fig. 6) durch eine Diffusionsschicht **2104** einer MDS-Matrix aufgebaut. Die Diffusionsschicht **2104** in der Struktur höherer Ebene als eine Stufenfunktion verwendet auch eine MDS-Matrix.

[0245] Bezüglich der Anordnung der MDS höherer Ebene sind Verfahren wie in der obigen Beschreibung verfügbar, die $GF(2^{32})$, $GF(2^4)$, $GF(2^8)$ und $GF(2^{16})$ verwenden.

[0246] Es wird die MDS höherer Ebene erläutert, die $GF(2^4)$ verwendet.

[0247] Fig. 30 zeigt ein Beispiel einer MDS-Matrix in diesem Fall.

[0248] In diesem Fall bilden 1-Bit-Daten in entsprechenden Positionen (die signifikantesten Bits werden beispielhaft in Fig. 30 dargestellt) der Ausgaben, d.h. 8-Bit-Daten von vier S-Boxen in einer erweiterten S-Box **2103**, 4-Bit-Daten pro Menge, und zwei Mengen von 4-Bit-Daten von einer erweiterten S-Box **2103** werden als Elemente von $GF(2^4)$ betrachtet.

[0249] Eine Diffusionsschicht **2104** zwischen zwei Stufen von zwei parallelen erweiterten S-Box-Schichten **2103** verwendet MDS-Matrizen mit 2 (Zeilen) × 2 (Spalten) (z.B. **2104-1** im Fall der signifikantesten Bits in Fig. 30) in entsprechenden Positionen von 8-Bit-Daten.

[0250] Die zwei Mengen von 4-Bit-Daten als Ausgaben sind mit entsprechenden Positionen von entsprechenden Quellen-8-Bit-Daten verbunden.

[0251] Es sind acht MDS-Matrizen (**2104-1** bis **2104-8**) als MDS-Matrizen höherer Ebene in Entsprechung zu der Bitbreite von S-Boxen vorbereitet.

[0252] Durch Tabellennachschlag in Einheiten von S-Box-Ausgaben in entsprechenden Positionen von erweiterten S-Boxen (auch durch arithmetische Operationen) wird eine effiziente Implementierung durchgeführt, die gleichzeitig acht MDS-Matrizen verarbeitet.

[0253] Falls zyklische MDS-Matrizen verwendet werden, werden ein effizienter Prozesses, der Verbindung mit EX-OR in Einheiten von 32 Bits kombiniert und Bitrotation in Einheiten von 8 Bits durchgeführt.

[0254] Es wird vermerkt, dass Fig. 30 als ein Beispiel der MDS-Matrix höherer Ebene für die Verschlüsselungsvorrichtung zeigt:

1. Zeile, 1. Spalte = 5, 1. Zeile, 2. Spalte = 7
2. Zeile, 1. Spalte = A, 2. Zeile, 2. Spalte = 8B

[0255] Eine entsprechende MDS-Matrix höherer Ebene für die Entschlüsselungsvorrichtung wird beschrieben durch:

1. Zeile, 1. Spalte = C, 1. Zeile, 2. Spalte = A
2. Zeile, 1. Spalte = 5, 2. Zeile, 2. Spalte = B

[0256] Es wird vermerkt, dass die erstere Matrix für Entschlüsselung verwendet werden kann, und die letztere für Verschlüsselung verwendet werden kann.

[0257] Auch kann eine Matrix verwendet werden, die durch Ersetzen von Zeilen, Ersetzen von Spalten und beliebiges Austauschen in einer beliebigen MDS-Matrix erhalten wird.

[0258] Des weiteren können andere MDS-Matrizen höherer Ebene verwendet werden.

[0259] Diese MDS-Diffusionsschicht höherer Ebene wird durch Software zum Ausführen von Transformation mittels einer Matrixarithmetikoperation oder Eingabe-/Ausgabe-Transformationstabelle implementiert, kann aber auch durch Hardware implementiert werden (eine tatsächliche Schaltung, die z.B. auf einem Halbleitersubstrat ausgebildet ist).

[0260] Um die MDS höherer Ebene unter Verwendung einer tatsächliche Schaltung zu implementieren, wird ein Leitungsverbindungsmuster äquivalent zu einer MDS-Matrix verwendet.

[0261] Fig. 31 zeigt Leitungsverbindungsausdrücke (Leitungsverbindungsmuster) von Multiplikation über $GF(2^4)$ in Entsprechung mit Elementen l bis F von $GF(2^4)$. Es wird vermerkt, dass ein gekoppelter Abschnitt eine EX-OR kalkuliert.

[0262] Genauer können in jeder der Diffusionsschichten **2104-1** bis **2104-8** in Fig. 30 Leitungsverbindungsausdrücke eines Abschnitts zum Anwenden des 1. Zeilen-, 1. Spaltenelementes der MDS-Matrix auf x_1, eines Abschnitts zum Anwenden des 1. Zeilen-, 2. Spaltenelementes auf x_2, eines Abschnitts zum Anwenden des 2. Zeilen-, 1. Spaltenelementes auf x_1 und eines Abschnitts zum Anwenden des 2. Zeilen-, 2. Spaltenelementes auf x_2 entsprechende Leitungsverbindungsmuster der Matrixelemente in Fig. 31 verwenden.

[0263] Fig. 32 zeigt ein Beispiel einer tatsächlichen Schaltung der MDS höherer Ebene basierend auf der Matrix, die beispielhaft in Fig. 30 dargestellt wird. In Fig. 32 bezeichnet Bezugszeichen **2141** ein Leitungsverbindungsmuster entsprechend dem 1. Zeilen-, 1. Spaltenelement "5"; **2142** ein Leitungsverbindungsmuster entsprechend dem 1. Zeilen-, 2. Spaltenelement "7"; **2143** ein Leitungsverbindungsmuster entsprechend dem 2. Zeilen-, 1. Spaltenelement "A"; und **2144** ein Leitungsverbindungsmuster entsprechend dem 2. Zeilen-, 2. Spaltenelement "B". In einem Abschnitt, wo eine Vielzahl von Bits gekoppelt sind, wird eine EX-OR kalkuliert.

[0264] Nach Kopplungsprozessen durch Verbinden mit EX-OR von Abschnitten entsprechend Produkten der Matrix werden Kopplungsprozesse durch Verbinden mit EX-OR von Abschnitten entsprechend den Summen von Produkten der Matrix durchgeführt. Alternativ können alle derartigen Kopplungsprozesse durch Verbinden mit EX-OR gleichzeitig durchgeführt werden, oder können in einer Vielzahl von Prozessen in Teilung durchgeführt werden.

[0265] Auch kann die folgende Prozedur genommen werden. Das heißt gewünschte Leitungsverbindungsmuster werden aus der in Fig. 31 gezeigten Leitungsverbindungsmustergruppe ausgewählt, um einen Kandidaten einer tatsächlichen Schaltungsanordnung der MDS höherer Ebene für Verschlüsselung zu bilden, und es wird dann verifiziert, ob eine Umkehrmatrix (MDS-Matrix) der entsprechenden MDS-Matrix vorhanden ist. Natürlich kann die Matrix für Entschlüsselung zuerst bestimmt werden.

[0266] Auch können andere Ausdrücke als Leitungsverbindungsausdrücke (Leitungsverbindungsmuster) von Multiplikation über $GF(2^4)$ verwendet werden.

[0267] Dieses Verfahren wird nicht nur auf die zweite Ausführungsform angewendet, sondern auch auf ein 128-Bit-Blockverschlüsselungsschema der oben erwähnten ersten Ausführungsform.

[0268] Nachstehend wird erneute Normalisierung beschrieben.

[0269] Es wird Einfächerung (Fan-in) der MDS-Diffusionsschicht erläutert. In den in Fig. 31 gezeigten Leitungsverbindungsmustern wird die Zahl von Bits (die Zahl von verbundenen Leitungen), die mit einem gegebenen Bit auf der Datenausgangsseite verbunden sind, "Fan-in" genannt. Z.B. haben in einem Leitungsverbindungsmuster entsprechend "1" alle Bits Fan-in = 1. Andererseits ist in einem Leitungsverbindungsmuster entsprechend "5" Fan-in = 2, 3, 3 und 2 der Reihe nach von den linken zu den rechten Bits.

[0270] Eine Gesamtmenge S von Fan-in-Werten von Leitungsverbindungsmustern der MDS-Diffusionsschicht wird nachstehend untersucht. In dem in Fig. 32 gezeigten Beispiel ist die Gesamtmenge S von Fan-in-Werten von 16 Bits, die durch die punktierten Linien **2141** bis **3144** begrenzt sind, 45. Die

Gesamtmenge S von Fan-in-Werten von Leitungsverbindungsmustern der MDS-Diffusionsschicht ist vorzugsweise klein, da sie zu einer Erhöhung in der Zahl von Leitungen (auch einer Erhöhung in EX-OR-Arithmetikoperationen und dergleichen bei Matrixkalkulationen) führt, falls sie groß ist. Im Fall einer MDS mit 2 (Zeilen) × 2 (Spalten) mit Elementen von GF(2^4) als ihre Elemente ist der Minimalwert von S 18.

[0271] Als ein Verfahren zum Reduzieren von S ist ein Schema für erneute Normalisierung (renormalization scheme) bekannt. Diese Schema kann das Schaltungsvolumen (Kalkulationsvolumen beim Durchführen von Matrixkalkulationen) reduzieren.

[0272] Um erneute Normalisierung durchzuführen, sind Vorverarbeitungsschaltungen **2180-1** und **2180-2** für erneute Normalisierung zwischen jeder der MDS-Diffusionsschichten **2104-1** bis **2104-8** und einzelnen S-Boxen auf der Eingangsseite eingefügt, wie in Fig. 33 gezeigt.

[0273] Jede Vorverarbeitungsschaltung **2180** hat eines der in Fig. 31 gezeigten Leitungsverbindungsmuster oder führt einen äquivalenten Kalkulationsprozess durch.

[0274] Fig. 33 zeigt Implementierung durch erneute Normalisierung unter Verwendung eines gemeinsamen Faktors = 5 für beide S-Boxen. Fig. 34 zeigt ein Beispiel der MDS höherer Ebene zu dieser Zeit. In diesem Fall wird die MDS-Matrix höherer Ebene beschrieben durch:

1. Zeile, 1. Spalte = 1, 1. Zeile, 2. Spalte = 4
2. Zeile, 1. Spalte = 2, 2. Zeile, 2. Spalte = 9

[0275] In Fig. 34 bezeichnet Bezugszeichen **2145** ein Leitungsverbindungsmuster entsprechend dem 1. Zeilen-, 1. Spaltenelement "1"; **2146** ein Leitungsverbindungsmuster entsprechend dem 1. Zeilen-, 2. Spaltenelement "4"; **2147** ein Leitungsverbindungsmuster entsprechend dem 2. Zeilen-, 1. Spaltenelement "2"; und **2148** ein Leitungsverbindungsmuster entsprechend dem 2. Zeilen-, 2. Spaltenelement "9". Ein Abschnitt, wo eine Vielzahl von Bits gekoppelt sind, entspricht einer EX-OR, wie oben beschrieben wird. In diesem Fall ist der Wert S 20.

[0276] Diffusion höherer Ebene in Fig. 32 ist der in Fig. 33 oder Fig. 34 äquivalent.

[0277] Als ein Verfahren zum Erhalten eines gemeinsamen Faktors und einer Matrix zu dieser Zeit bei Durchführung erneuter Normalisierung werden z.B. Matrizen, die Diffusion höherer Ebene äquivalent zu der einer Matrix erreichen können, die ohne erneute Normalisierung erhalten wird, unter Verwendung gemeinsamer Faktoren als Parameter erhalten, und ihre Fan-in-Werte werden evaluiert, um eine Matrix auszuwählen, die anzunehmen ist.

[0278] Es wird vermerkt, dass jeweilige S-Boxen eingeschränkt sein können oder nicht, um einen identischen gemeinsamen Faktor aufzuweisen.

[0279] Bei Implementierung durch erneute Normalisierung für jeweilige S-Boxen unter Verwendung eines gemeinsamen Faktors = B in einer Matrix, die beschrieben wird durch:

1. Zeile, 1. Spalte = C, 1. Zeile, 2. Spalte = A
2. Zeile, 1. Spalte = 5, 2. Zeile, 2. Spalte = B

wird eine MDS-Matrix höherer Ebene beschrieben durch:

1. Zeile, 1. Spalte = 9, 1. Zeile, 2. Spalte = 4
2. Zeile, 1. Spalte = 2, 2. Zeile, 2. Spalte = 1

[0280] Natürlich kann dieses Verfahren auch auf ein oben erwähntes 128-Bit-Blockverschlüsselungsschema angewendet werden.

[0281] Es wird vermerkt, dass Verdrahtung und Lay-outs, die oben beispielhaft dargestellt werden, theoretische Beziehungen anzeigen, und tatsächliche Verdrahtung und Lay-outs einen Freiheitsgrad im Entwurf haben. Es können acht Abschnitte **2104-1** bis **2104-8** der MDS-Schicht höherer Ebene montiert sein, oder es können nur einige (z.B. einer, zwei oder vier) der MDS-Abschnitte **2104-1** bis **2104-8** montiert sein und sie können in Zeitteilung gemeinsam verwendet werden.

[0282] Die Verschlüsselungs- und Entschlüsselungsvorrichtungen sind auf die gleiche Weise angeordnet (sie haben nur eine Umkehrtransformationsbeziehung).

[0283] Basierend auf dem gleichen Konzept wie oben beschrieben kann Verarbeitung in Einheiten von 2 Bits in entsprechenden Positionen von 8-Bit-Daten durchgeführt werden, und vier MDS-Matrizen mit 2 (Zeilen) × 2 (Spalten) (GF(2^8)) mit 8-Bit-Elementen können als MDS-Matrizen höherer Ebene vorbereitet werden. Andererseits kann Verarbeitung in Einheiten von 4 Bits in entsprechenden Positionen von 8-Bit-Daten durchgeführt werden, und es können zwei MDS-Matrizen mit 2 (Zeilen) × 2 (Spalten) (GF(2^{16})) mit 16-Bit-Elementen als MDS-Matrizen höherer Ebene vorbereitet werden.

[0284] In der obigen Beschreibung werden Bits in entsprechenden Positionen extrahiert und verarbeitet. Alternativ können Bits in unterschiedlichen Positionen (exklusiv) extrahiert und verarbeitet werden.

[0285] Wie in dem in Fig. 9 gezeigten Beispiel ist auch eine Anordnung basierend auf einer MDS-Matrix höherer Ebene unter Verwendung von GF(2^{32}) möglich.

[0286] Die zuvor erwähnten Anordnungsbeispiele können auch auf ein oben erwähntes 128-Bit-Blockverschlüsselungsschema angewendet werden.

[0287] Wie in der obigen Beschreibung, in Fig. 28, müssen nicht alle erweiterten S-Boxen die gleiche interne Anordnung haben, und einige von ihnen können unterschiedliche Anordnungen haben.

[0288] Es müssen nicht alle MDS-Matrizen höherer Ebene die gleiche interne Anordnung haben, und einige von ihnen können unterschiedliche Anordnungen haben. Das gleiche trifft auf MDS-Matrizen unterer Ebene und die Eingabe-/Ausgabetabellen von S-Boxen zu.

[0289] Z.B. können die erste Eingangsstufe und die letzte Ausgangsstufe interne Anordnungen haben, die sich von jenen der Zwischenstufen unterscheiden.

[0290] Es wird vermerkt, dass auch eine Anordnung zum Ersetzen von Bitpositionen einer Vielzahl von S-Boxen, die zu identischen erweiterten S-Boxen gehören (oder Einfügen einer derartigen Schaltung) auf der Eingangs- und Ausgangsseite jeder MDS höherer Ebene verfügbar ist.

[0291] Außerdem sind verschiedene andere Variationen verfügbar.

[0292] Natürlich wird die so weit beschriebene Anordnung der MDS höherer Ebene auf Verschlüsselungs- und Entschlüsselungsvorrichtungen mit verschiedenen Variationen angewendet.

[0293] Nachstehend wird der Schlüsselplanungsteil (Schlüsselgenerator) erläutert.

[0294] Fig. 35 zeigt ein Beispiel der Anordnung des Schlüsselplanungsteils. Bezugszeichen **2121** bezeichnet einen Abschnitt entsprechend einer Stufe der Stufenfunktion des Datendiffusionsteils; **2131** eine lineare Diffusionsschicht (in diesem Beispiel eine Diffusionsschicht unter Verwendung einer MDS-Matrix höherer Ebene); **2132** eine nichtlineare Transformationsschicht (in diesem Beispiel zwei parallele SP-Schichten (S-Box-Schichten/Diffusionsschichten)); **2134** eine EX-OR-Einheit; und **2135** einen Restaddierer. Obwohl in Fig. 35 nicht gezeigt, wird die Anordnung des Abschnitts **2121** nach Bedarf wiederholt. Wenn die Anordnungseinheit, die einen 64-Bit-Schlüssel ausgibt, als eine Stufe des Schlüsselplanungsteils definiert ist, ist die Zahl vom Schlüsselplanungsteil (2R + 1) (= 13, wenn R = 6 ist).

[0295] In dem in Fig. 35 gezeigten Beispiel werden 64 Bits als die linke Hälfte der Ausgabe jeder Stufe eines 128-Bit modifizierten Feistel-Wiederholungsprozesses extrahiert, und dazu wird eine stufenzahlabhängige Konstante C_i als ein Rest addiert, um einen erweiterten Schlüssel zu erhalten.

[0296] Wenn die Schlüssellänge z.B. 128 Bits ist, werden die oberen 64 Bits zu der linearen Diffusionsschicht **2131** der ersten Stufe eingegeben, und die unteren 64 Bits werden zu der nichtlinearen Transformationsschicht **2132** eingegeben. Wenn die Schlüssellänge z.B. 64 Bits ist, werden die 64 Bits zu der linearen Diffusionsschicht **2131** der ersten Stufe, und auch zu der nichtlinearen Transformationsschicht **2132** eingegeben. Wenn die Schlüssellänge z.B. 96 Bits ist (= 32 Bits × 3), werden die 64 Bits, die durch Koppeln der oberen 32 Bits und der zwischenliegenden 32 Bits erhalten werden, zu der linearen Diffusionsschicht **2131** der ersten Stufe eingegeben, und 64 Bits, die durch Koppeln der oberen 32 Bits und der unteren 32 Bits erhalten werden, werden zu der nichtlinearen Transformationsschicht **2132** eingegeben.

[0297] Es wird vermerkt, dass die Stelle des Restaddierers **136**, der die stufenzahlabhängige Konstante C_i als einen Rest addiert, verschiedene Variationen aufweisen kann, wie in Fig. 36 gezeigt.

[0298] Ein Beispiel der Anordnung jeder nichtlinearen Transformationsschicht **2132** in Fig. 35 und Fig. 36 ist das gleiche wie das in Fig. 13 und Fig. 14 (wie in Fig. 14, kann eine Konstante, die mit der Eingabe zu jeder S-Box mit EX-OR zu verbinden ist, eine stufenzahlabhängige Konstante sein). Auch kann die S-Box entweder die gleiche sein wie die oder verschieden sein von der für die in Fig. 28 gezeigte Verschlüsselungsverarbeitung. Die S-Boxen und MDS unterer Ebene können unterschiedliche Anordnungen in Einheiten von Stufen des Schlüsselplanungsteils haben.

[0299] Ein Beispiel eines Verfahrens zum Generieren unterschiedlicher Konstanten C_i in einzelnen Stufen wird nachstehend erörtert.

[0300] Die 64-Bit additive Konstante C_i des Schlüsselplanungsteils in Fig. 35 und Fig. 36 wird durch eine Kombination von vier Bitkonstanten (H_0, H_1, H_2, H_3) beschrieben. Beispiele von 32-Bit-Konstanten H_i sind:

$$H_0 = (5A827999)_H = \lfloor(\sqrt{2}/4 \times 2^{32})\rfloor$$

$$H_1 = (6ED9EBA1)_H = \lfloor(\sqrt{3}/4 \times 2^{32})\rfloor$$

$$H_2 = (8FIBBCDC)_H = \lfloor(\sqrt{5}/4 \times 2^{32})\rfloor$$

$$H_3 = (CA62C1D6)_H = \lfloor(\sqrt{10}/4 \times 2^{32})\rfloor$$

[0301] Eine Kombination von additiven Konstanten C_i wird durch $C_i = (C_{i0}, C_{i1})$ beschrieben. Um einfache Generierung von unterschiedlichen 64-Bit-Konstanten C_i in einzelnen Stufen zu ermöglichen, wird

8-Bit-LFSR verwendet, um eine Kombination von H_i zu bestimmen, die C_i bilden. Z.B. wird $(1D)_H$ in dem primitiven Polynom von LFSR verwendet, und $(8B)_H$ wird in dem Anfangszustand von LFSR verwendet. Eine Bitsequenz, die unter Verwendung des LFSR verwendet wird, wird in Einheiten von 2 Bits ausgelesen, um eine 32-Bit-Konstante H_i zu bestimmen, die als die Konstante verwendet wird.

[0302] Fig. 37 zeigt ein Beispiel einer Additivkonstantentabelle, die durch unter Verwendung des LFSR durch das zuvor erwähnte Verfahren bestimmt wird.

[0303] Es wird vermerkt, dass die Anfangsstufe von LFSR variabel oder fixiert sein kann. In dem ersteren Fall definiert der Anfangszustand von LFSR teilweise den Schlüssel. In dem letzteren Fall kann nur eine Entschlüsselungsvorrichtung mit dem gleichen Anfangszustand von LFSR wie dem in der Verschlüsselungsvorrichtung den Chiffretext entschlüsseln.

[0304] Gemäß dem zuvor erwähnten Schlüsselplanungsteil können in der nichtlinearen Transformationsschicht, wenn sich 1 Bit der Eingabe geändert hat, die S-Boxen diese Änderung zu 8 Bits ausbreiten, und die MDS unterer Ebene kann die Änderung zu 32 Bits ausbreiten. Des weiteren wird in der linearen Diffusionsschicht, da die MDS höherer Ebene die Ausgabe von der nichtlinearen Transformationsschicht des vorherigen Zustands zum großen Teil diffundiert, eine 1-Bit-Differenz zu der 64-Bit-Breite ausgebreitet.

[0305] Gemäß dem Schlüsselplanungsteil können deshalb die jeweiligen Stufen zufällige Schlüssel leicht generieren, d.h. diffundieren. Da unterschiedliche Konstanten in Einheiten von Stufen verwendet werden, stimmen Schlüssel unter Stufen selten überein (Schlüssel stimmen nahezu nicht überein).

[0306] Es wird vermerkt, dass der Schlüsselplanungsteil eine andere Anordnung aufweisen kann.

[0307] Es wird vermerkt, dass die lineare Diffusionseinrichtung und der Galois-Feldmultiplikator, die mit Bezug auf Fig. 16 bis Fig. 18 erläutert wurden, auch auf diesen Fall angewendet werden können.

[0308] Die MDS-Matrix-Generierungssektion (oder Zufallsgenerierungsalgorithmus), die/der mit Bezug auf Fig. 19 bis Fig. 22 erläutert wurde, kann auch auf diesen Fall angewendet werden.

[0309] Natürlich kann auch das Entwurfsverfahren einer Kombination von S-Box und MDS, das mit Bezug auf Fig. 23 erläutert wurde, auf diesen Fall angewendet werden.

[0310] Nachstehend wird die Entschlüsselungsvorrichtung erläutert.

[0311] Die Entschlüsselungsvorrichtung hat grundsätzlich eine Struktur, die durch Umkehrung der von der Verschlüsselungsvorrichtung erhalten wird (es wird der gleiche Schlüssel verwendet).

[0312] Fig. 38 zeigt ein Beispiel der Anordnung einer Entschlüsselungsvorrichtung entsprechend der in Fig. 28 gezeigten Verschlüsselungsvorrichtung.

[0313] Fig. 39 zeigt ein anderes Beispiel der Struktur einer Stufe der Umkehrtransformation des Datenrandomisierungsteils von Fig. 28, wobei die Stufe der in Fig. 29 gezeigten entspricht.

[0314] Ein Beispiel der Anordnung entsprechend der Struktur unterer Ebene (siehe Fig. 6) in Fig. 28 ist das gleiche wie das, das in Fig. 25 gezeigt wird.

[0315] In Fig. 38 hat ein Schlüsselplanungsteil der Entschlüsselungsvorrichtung die gleiche Anordnung wie die der Verschlüsselungsvorrichtung, die in Fig. 28 gezeigt wird.

[0316] Die Eingabe-/Ausgabetabelle jeder S-Box (siehe **1112** in Fig. 25), eine MDS-Matrix unterer Ebene jeder MDS unterer Ebene (siehe **1113** in Fig. 25) und eine MDS-Matrix höherer Ebene einer MDS höherer Ebene **3104** sind Umkehrfunktionen (Umkehrmatrizen) der Eingabe-Ausgabetabelle jeder S-Box (siehe **1112** in Fig. 6), der MDS-Matrix unterer Ebene jeder MDS unterer Ebene (siehe **113** in Fig. 6) und der MDS-Matrix höherer Ebene der MDS höherer Ebene **3104** in der Verschlüsselungsvorrichtung.

[0317] In Fig. 38 wird der Schlüssel in der gleichen Ordnung wie in Fig. 28 generiert, kann aber in einer Ordnung entgegengesetzt zu Fig. 28 generiert werden.

[0318] Fig. 40 zeigt ein Beispiel der Anordnung des Schlüsselplanungsteils in einem derartigen Fall.

[0319] Bezugszeichen **3132** bezeichnet eine Umkehrtransformation der nichtlinearen Transformationsschicht **2132** von Fig. 35 (einschließlich vier paralleler Umkehrtransformationen von SP-Schichten **2133** (z.B. werden die Eingaben und Ausgaben in Fig. 13 oder Fig. 14 umgekehrt)).

[0320] Die Eingabe-/Ausgabetabelle jeder S-Box, MDS-Matrix unterer Ebene und MDS-Matrix höherer Ebene, die in dem in Fig. 40 gezeigten Schlüsselplanungsteil verwendet werden, sind Umkehrfunktionen (Umkehrmatrizen) jener, die in dem Schlüsselplanungsteil in Fig. 35 verwendet werden.

[0321] Es wird angenommen, dass eine Chiffrierschlüsseleingabe K' in Fig. 40 der Schlüssel ist, der in der letzten Schlüsseladdition in Fig. 28 (für Verschlüsselung) verwendet wird.

[0322] In diesem Fall sind ebenso verschiedene Variationen der Stellen, wo die stufenzahlabhängigen Konstanten C_i als Reste addiert werden, zusätzlich zu dem gleichen Verfahren wie in Fig. 36 verfügbar.

[0323] In der obigen Beschreibung wurden ein 128-Bit-Blockverschlüsselungsschema und ein 64-Bit-Blockverschlüsselungsschema beispielhaft dargestellt, aber die vorliegende Erfindung wird auf ein Blockverschlüsselungsschema anderer Bitlängen angewendet.

[0324] Nachstehend werden die Hardwareanordnung und Softwareanordnung dieser Ausführungsform erläutert.

[0325] Die Verschlüsselungs- und Entschlüsselungsvorrichtungen dieser Ausführungsform sind durch entweder Hardware oder Software implementiert.

[0326] Bei Softwareimplementierung wird diese Ausführungsform auf ein computerlesbares Aufzeichnungsmedium angewendet, das ein Programm aufzeichnet, das die Verschlüsselungs- oder Entschlüsselungsvorrichtung implementiert und einen Computer veranlasst, vorbestimmte Mittel auszuführen (oder einen Computer veranlasst, als ein vorbestimmtes Mittel zu funktionieren, oder einen Computer veranlasst, vorbestimmte Funktionen zu implementieren).

[0327] Bei Hardwareimplementierung werden die Verschlüsselungs- oder Entschlüsselungsvorrichtung als einer Halbleitereinrichtung gebildet.

[0328] Wenn eine Verschlüsselungs- oder Entschlüsselungsvorrichtung aufgebaut wird, auf die die vorliegende Erfindung angewendet wird, oder wenn ein Verschlüsselungs- oder Entschlüsselungsprogramm vorbereitet wird, können alle Blöcke oder Module, die in Fig. 4 und Fig. 24 beispielhaft dargestellt sind, einzeln erstellt werden. Alternativ können einer oder eine geeignete Zahl von Blöcken oder Modulen mit identischer Anordnung vorbereitet werden, und können durch jeweilige Abschnitte des Algorithmus gemeinsam genutzt (gemeinsam verwendet) werden.

[0329] Im Fall von Softwareimplementierung können Multi-Prozessoren verwendet werden, um parallele Prozesse auszuführen, wobei somit Verarbeitung hoher Geschwindigkeit erreicht wird.

[0330] Es wird vermerkt, dass eine Vorrichtung, die eine Verschlüsselungsfunktion, aber keine Entschlüsselungsfunktion hat, eine Vorrichtung, die eine Entschlüsselungsfunktion, aber keine Verschlüsselungsfunktion hat, oder eine Vorrichtung, die sowohl die Verschlüsselungs- als auch Entschlüsselungsfunktionen hat, aufgebaut wird. Gleichermaßen wird ein Programm, das eine Verschlüsselungsfunktion, aber keine Entschlüsselungsfunktion hat, ein Programm, das eine Entschlüsselungsfunktion, aber keine Verschlüsselungsfunktion hat, oder ein Programm, das sowohl die Verschlüsselungs- als auch Entschlüsselungsfunktionen hat, vorbereitet.

[0331] Nachstehend werden Anwendungen dieser Ausführungsform auf Systeme erläutert.

[0332] Das Verschlüsselungssystem dieser Ausführungsform wird grundsätzlich auf jedes System angewendet.

[0333] Wie z.B. in Fig. 41 gezeigt, wird ein Schlüssel zwischen einer Übertragungsvorrichtung **301** und einer Empfangsvorrichtung **303** durch ein vorbestimmtes Verfahren oder Prozedur gemeinsam sicher genutzt. Die Übertragungsvorrichtung **301** verschlüsselt Übertragungsdaten in Einheiten einer Blocklänge durch das Verschlüsselungssystem dieser Ausführungsform, und überträgt verschlüsselte Daten zu der Empfangsvorrichtung **303** über ein Kommunikationsnetz **302** in Übereinstimmung mit einem vorbestimmten Protokoll. Bei Empfang verschlüsselter Daten entschlüsselt die Empfangsvorrichtung **303** die empfangenen verschlüsselten Daten in Einheiten von Blocklängen durch das Verschlüsselungssystem dieser Ausführungsform, um ursprünglichen Klartext zu reproduzieren. Es wird vermerkt, dass wenn diese Vorrichtungen sowohl die Verschlüsselungs- als auch Entschlüsselungsfunktionen aufweisen, sie Zweiweg-Verschlüsselungskommunikationen durchführen können.

[0334] Wie z.B. in Fig. 42 gezeigt, generiert ein Computer **311** einen Schlüssel durch ein vorbestimmtes Verfahren, verschlüsselt Daten, die zu sichern sind, in Einheiten von Blocklängen durch das Verschlüsselungssystem dieser Ausführungsform, und sichert die verschlüsselten Daten in einem Datenserver **313** über ein vorbestimmtes Netz (z.B. ein LAN, Internet oder dergleichen) **314**. Beim Lesen der gesicherten Daten liest der Computer **311** gewünschte verschlüsselte Daten von dem Datenserver **313**, und entschlüsselt die gelesenen Daten in Einheiten von Blocklängen durch das Verschlüsselungssystem dieser Ausführungsform, um ursprünglichen Klartext zu reproduzieren.

[0335] Falls ein anderer Computer **312** diesen Schlüssel kennt, kann er ähnlich entschlüsseln und Klartext reproduzieren. Andere Computer, die den Schlüssel nicht kennen, können jedoch die verschlüsselten Daten nicht entschlüsseln, wobei somit Sicherheitssteuerung von Information erreicht wird.

[0336] Wie z.B. in Fig. 43 gezeigt, verschlüsselt für den Inhaltsanbieter eine Verschlüsselungsvorrich-

tung **321** einen gegebenen Inhalt unter Verwendung eines gegebenen Schlüssels in Einheiten von Blocklängen durch das Verschlüsselungssystem dieser Ausführungsform, zeichnet den verschlüsselten Inhalt auf Aufzeichnungsmedien **322** auf und gibt diese Medien zu Benutzern ab. Der Benutzer, der das Aufzeichnungsmedium **322** erlangt hat, erlangt den Schlüssel durch ein vorbestimmtes Verfahren, und entschlüsselt den Inhalt in Einheiten von Blocklängen durch das Verschlüsselungssystem dieser Ausführungsform unter Verwendung einer Eetschlüsselungsvorrichtung **323**, wobei somit der Inhalt durchgeblättert oder abgespielt wird.

[0337] Auch wird die vorliegende Erfindung auf verschiedene andere Systeme angewendet.

[0338] Es wird vermerkt, dass die in dieser Ausführungsform beschriebenen Anordnungen lediglich Beispiele sind, und andere Anordnungen nicht ausschließen, und andere Anordnungen, die durch Ersetzen einiger Komponenten der beispielhaft dargestellten Anordnung durch andere erhalten werden, wobei einige Komponenten der beispielhaft dargestellten Anordnung weggelassen werden, andere Funktionen der beispielhaften Anordnung hinzugefügt werden oder sie kombiniert werden, auch verfügbar sind. Auch sind eine andere Anordnung, die der beispielhaft dargestellten Anordnung theoretisch äquivalent ist, eine andere Anordnung, die Abschnitte enthält, die der beispielhaft dargestellten Anordnung theoretisch äquivalent sind, eine andere Anordnung, die einem prinzipiellen Teil der beispielhaft dargestellten Anordnung theoretisch äquivalent ist und dergleichen verfügbar. Des weiteren sind eine andere Anordnung, die das gleiche oder ähnliche Ziele wie oder zu denen der beispielhaft dargestellten Anordnung erreicht, eine andere Anordnung, die die gleichen oder ähnliche Effekte wie oder zu jenen der beispielhaft dargestellten Anordnung vorsehen kann, und dergleichen verfügbar.

Patentansprüche

1. Eine Verschlüsselungsvorrichtung, umfassend:
Mittel (**102**) zum Randomisieren (zufälligen Anordnen) von Eingangsdaten in Einheiten eines Blocks einer ersten Größe; und
Mittel (**104**) zum Diffundieren von Daten, die von dem Randomisierungsmittel (**102**) ausgegeben werden, mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und
das Randomisierungsmittel (**102**) umfasst erste Randomisierungseinheiten (**103**) zum Randomisieren der Eingangsdaten in Einheiten des Blocks der ersten Größe, gekennzeichnet dadurch, dass mindestens eine der ersten Randomisierungseinheiten (**103**) umfasst:
zweite Randomisierungseinheiten (**112**) zum Randomisieren der Eingangsdaten in Einheiten eines Blocks einer dritten Größe, die kleiner als die erste Größe ist; und
eine Diffusionseinheit (**113**) zum Diffundieren von Daten, ausgegeben von den zweiten Randomisierungseinheiten (**112**) mit Bezug auf die erste Größe.

2. Die Vorrichtung nach Anspruch 1, wobei das Diffusionsmittel (**104**) konfiguriert ist, eine arithmetische Operation unter Verwendung einer Maximalabstands-Trennbarkeitsmatrix (Maximum Distance Separable Matrix) durchzuführen.

3. Die Vorrichtung nach Anspruch 2, wobei das Diffusionsmittel (**104**) konfiguriert ist, eine Maximalabstands-Trennbarkeitsmatrix zu verwenden, von der jedes Element ein Polynom umfasst und Terme von jedem Polynom nicht Null sind, wo die Terme von einer vorbestimmten Ordnung oder weniger sind.

4. Die Vorrichtung nach Anspruch 2, wobei das Diffusionsmittel (**104**) konfiguriert ist, eine Maximalabstands-Trennbarkeitsmatrix zu verwenden, von der alle Elemente auf einer Zeile unterschiedliche Werte haben.

5. Die Vorrichtung nach Anspruch 2, wobei eine Vielzahl der ersten Randomisierungseinheiten (**103**) konfiguriert sind, Eingangsdaten für die Maximalabstands-Trennbarkeitsmatrix vorzusehen, wobei die Eingangsdaten Daten von der gleichen Bitposition in den Blöcken der dritten Größe innerhalb der ersten Randomisierungseinheit (**103**) umfassen.

6. Die Vorrichtung nach Anspruch 1, wobei die Diffusionseinheit (**113**) konfiguriert ist, eine arithmetische Operation unter Verwendung einer Maximalabstands-Trennbarkeitsmatrix durchzuführen.

7. Die Vorrichtung nach Anspruch 1, ferner umfassend:
Schlüsselgenerierungsmittel (**121**) zum Generieren von Schlüsseldaten, das Schlüsselgenerierungsmittel umfassend Schlüsselgeneratoren, die in Reihe verbunden sind, jeder der Schlüsselgeneratoren umfassend eine erste Schaltung (**132**), die konfiguriert ist, eine Ausgabe eines vorangehenden Generators nichtlinear zu transformieren, eine zweite Schaltung (**132**), die konfiguriert ist, eine Ausgabe eines Generators, der dem vorangehenden Generator vorausgeht, nichtlinear zu transformieren, und eine dritte Schaltung (**134**), die konfiguriert ist, EX-OR der ersten und zweiten Schaltungen auszugeben.

8. Eine Verschlüsselungsvorrichtung nach Anspruch 1, ferner umfassend:
eine Vielzahl von Stufensektionen (**101**), die in Reihe verbunden sind, jede Stufensektion umfassend vier erste Randomisierungseinheiten (**103**) und ein Diffusionsmittel (**104**), die vier ersten Randomisierungs-

einheiten (**103**) konfiguriert, 128-Bit-Klartext-Blockdaten in einer ersten Stufe oder 128-Bit-Blockdaten, die durch eine vorangehende Stufe verarbeitet werden, in einer zweiten und nachfolgenden Stufen zu empfangen, und vier Mengen von 32-Bit-Daten zu randomisieren, die 32-Bit-Daten erhalten durch Teilen der 128-Bit-Blockdaten, und das Diffusionsmittel (**104**) konfiguriert, 128-Bit-Blockdaten zu diffundieren, erhalten durch Koppeln von vier Mengen von 32-Bit-Daten, die von den vier ersten Randomisierungseinheiten (**103**) ausgegeben werden, unter Verwendung einer Maximalabstands-Trennbarkeitsmatrix;
weitere vier erste Randomisierungseinheiten (**103**), die mit der letzten Stufe der Stufensektionen (**101**) verbunden sind, und konfiguriert sind, vier Mengen von 32-Bit-Daten zu randomisieren, die durch Teilen von 128-Bit-Blockdaten erhalten werden, die von der letzten Stufensektion ausgegeben werden; und
eine erste Schlüsselhinzufügungssektion (**105**), die mit den weiteren vier ersten Randomisierungseinheiten (**103**) verbunden ist, und konfiguriert ist, 128-Bit-Schlüsseldaten zu 128-Bit-Blockdaten hinzuzufügen, die durch Koppeln von vier Mengen von 32-Bit-Daten erhalten werden, die von den weiteren vier ersten Randomisierungseinheiten (**103**) ausgegeben werden; und
jede der ersten Randomisierungseinheiten (**103**) umfassend: vier zweite Schlüsselhinzufügungssektionen (**111**) zum Hinzufügen von 8-Bit-Schlüsseldaten zu vier Mengen von 8-Bit-Daten, die Mengen von 8-Bit-Daten erhalten durch Teilen einer der vier Mengen von 32-Bit-Daten;
vier zweite Randomisierungseinheiten (**112**) zum Randomisieren von Ausgaben der vier zweiten Schlüsselhinzufügungssektionen unter Verwendung einer 8-Bit-Eingabe-/Ausgabetabelle;
eine Diffusionseinheit (**113**) zum Diffundieren von 32-Bit-Daten, die 32-Bit-Daten erhalten durch Koppeln von vier Mengen von 8-Bit-Daten, die von den vier zweiten Randomisierungseinheiten (**112**) ausgegeben werden unter Verwendung einer Maximalabstands-Trennbarkeitsmatrix; und
vier weitere zweite Schlüsselhinzufügungssektionen (**111**), die mit der Diffusionseinheit (**113**) verbunden sind; und
weitere vier zweite Randomisierungseinheiten (**112**) zum Randomisieren von Ausgaben der vier weiteren zweiten Schlüsselhinzufügungssektionen (**111**) unter Verwendung einer 8-Bit-Eingabe-/Ausgabetabelle.

9. Eine Vorrichtung zum Verschlüsseln von Blockdaten nach Anspruch 1, ferner umfassend:
eine Vielzahl von Stufensektionen (**2101**), die in Reihe verbunden sind, jede Stufensektion umfassend zwei erste Randomisierungseinheiten (**2103**) und ein Diffusionsmittel (**2104**), die zwei ersten Randomisierungseinheiten (**2103**) konfiguriert, eingegebene 64-Bit-Klartext-Blockdaten in einer ersten Stufe oder 64-Bit-Blockdaten, die durch eine vorangehende Stufe verarbeitet werden, in einer zweiten und nachfolgenden Stufen zu empfangen, und zwei Mengen von 32-Bit-Daten zu randomisieren, die durch Teilen der 64-Bit-Blockdaten erhalten werden, und das Diffusionsmittel (**2104**) konfiguriert, 64-Bit-Blockdaten zu diffundieren, die durch Koppeln von zwei Mengen von 32-Bit-Daten erhalten werden, die von den zwei ersten Randomisierungseinheiten (**2103**) ausgegeben werden, unter Verwendung einer Maximalabstands-Trennbarkeitsmatrix;
weitere zwei erste Randomisierungseinheiten (**2103**), die mit der letzten Stufe der Stufensektionen (**2101**) verbunden sind, und konfiguriert sind, zwei Mengen von 32-Bit-Daten zu randomisieren, die durch Teilen von 64-Bit-Blockdaten erhalten werden, die von der letzten Stufe ausgegeben werden; und
eine erste Schlüsselhinzufügungssektion (**2105**), die mit den zwei weiteren ersten Randomisierungseinheiten (**2103**) verbunden ist, und konfiguriert ist, 64-Bit-Schlüsseldaten zu 64-Bit-Blockdaten hinzuzufügen, die durch Koppeln von zwei Mengen von 32-Bit-Daten erhalten werden, die von den zwei weiteren ersten Randomisierungseinheiten (**2103**) ausgegeben werden; und
jede der ersten Randomisierungseinheiten (**2103**) umfassend:
vier zweite Schlüsselhinzufügungssektionen (**111**) zum Hinzufügen von 8-Bit-Schlüsseldaten zu vier Mengen von 8-Bit-Daten, wobei die vier Mengen von 8-Bit-Daten erhalten durch Teilen einer der zwei Mengen von 32-Bit-Daten; vier zweite Randomisierungseinheiten (**112**) zum Randomisieren von Ausgaben der vier zweiten Schlüsselhinzufügungssektionen unter Verwendung einer 8-Bit-Eingabe-/Ausgabetabelle;
eine Diffusionseinheit (**113**) zum Diffundieren von 32-Bit-Daten, die 32-Bit-Daten erhalten durch Koppeln von vier Mengen von 8-Bit-Daten, die von den vier zweiten Randomisierungseinheiten (**112**) ausgegeben werden unter Verwendung einer Maximalabstands-Trennbarkeitsmatrix;
vier weitere zweite Schlüsselhinzufügungssektionen (**111**), die mit der Diffusionseinheit (**113**) verbunden sind; und
weitere vier zweite Randomisierungseinheiten (**112**) zum Randomisieren von Ausgaben der vier weiteren Schlüsselhinzufügungssektionen unter Verwendung einer 8-Bit-Eingabe-/Ausgabetabelle.

10. Artikel einer Herstellung, umfassend ein computerverwendbares Medium mit darauf verkörperten computerlesbaren Programmcodemitteln, die computerlesbaren Programmcodemittel umfassend:
ein erstes computerlesbares Programmcodemittel (**102**) zum Veranlassen eines Computers, Eingangsdaten in Einheiten eines Blocks einer ersten Größe zu randomisieren; und
ein zweites computerlesbares Programmcodemittel (**104**) zum Veranlassen eines Computers, randomisierte Daten mit Bezug auf eine zweite Größe zu dif-

fundieren, die größer als die erste Größe ist, und
das erste computerlesbare Programmcodemittel (**102**) umfasst ein drittes computerlesbares Programmcodemittel (**103**) zum Veranlassen eines Computers, die Eingangsdaten in Einheiten des Blocks der ersten Größe zu randomisieren, gekennzeichnet dadurch, dass das dritte computerlesbare Programmcodemittel (**103**) umfasst:
ein viertes computerlesbares Programmcodemittel (**112**) zum Veranlassen eines Computers, die Eingangsdaten in Einheiten eines Blocks einer dritten Größe zu randomisieren, die kleiner als die erste Größe ist; und
ein fünftes computerlesbares Programmcodemittel (**113**) zum Veranlassen eines Computers, Daten zu diffundieren, die von dem vierten computerlesbaren Programmcodemittel (**112**) ausgegeben werden mit Bezug auf die erste Größe.

11. Ein Verschlüsselungsverfahren, umfassend:
einen Schritt (**102**) zum Randomisieren von Eingangsdaten in Einheiten eines Blocks einer ersten Größe; und
einen Schritt (**104**) zum Diffundieren von randomisierten Daten mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und
der Randomisierungsschritt (**102**) einen Teilschritt (**103**) umfasst zum Randomisieren der Eingangsdaten in Einheiten des Blocks der ersten Größe, gekennzeichnet dadurch, dass der Teilschritt (**103**) umfasst:
einen Teilschritt (**112**) zum Randomisieren der Eingangsdaten in Einheiten eines Blocks einer dritten Größe, die kleiner als die erste Größe ist; und
einen Teilschritt (**113**) zum Diffundieren von Daten, die von dem Randomisierungsteilschritt (**112**) ausgegeben werden, mit Bezug auf die erste Größe.

12. Eine Entschlüsselungsvorrichtung, umfassend:
Mittel (**1102**) zum Randomisieren von eingegebenen verschlüsselten Daten in Einheiten eines Blocks einer ersten Größe; und Mittel (**1104**) zum Diffundieren der Daten, die von dem Randomisierungsmittel (**1102**) ausgegeben werden, mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und
das Randomisierungsmittel (**1102**) umfasst erste Randomisierungseinheiten (**1103**) zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten des Blocks der ersten Größe, gekennzeichnet dadurch, dass
mindestens eine der ersten Randomisierungseinheiten (**1103**) umfasst:
zweite Randomisierungseinheiten (**1112**) zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten eines Blocks einer dritten Größe, die kleiner als die erste Größe ist; und
eine Diffusionseinheit (**1113**) zum Diffundieren von Daten, die von den zweiten Randomisierungseinheiten (**1112**) ausgegeben werden, mit Bezug auf die erste Größe.

13. Ein Verfahren zum Entschlüsseln, umfassend:
einen Schritt (**1102**) zum Randomisieren von eingegebenen verschlüsselten Daten in Einheiten eines Blocks einer ersten Größe; und
einen Schritt (**1104**) zum Diffundieren der Daten, die von dem Randomisierungsschritt (**1102**) ausgegeben werden, mit Bezug auf eine zweite Größe, die größer als die erste Größe ist, und
der Randomisierungsschritt (**1102**) umfasst einen Teilschritt (**1103**) zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten des Blocks der ersten Größe, gekennzeichnet dadurch, dass der Teilschritt umfasst
einen Teilschritt (**1112**) zum Randomisieren der eingegebenen verschlüsselten Daten in Einheiten eines Blocks einer dritten Größe, die kleiner als die erste Größe ist; und
einen Teilschritt (**1113**) zum Diffundieren von Daten, die von dem Randomisierungsteilschritt (**1112**) ausgegeben werden, mit Bezug auf die erste Größe.

Es folgen 23 Blatt Zeichnungen

Anhängende Zeichnungen

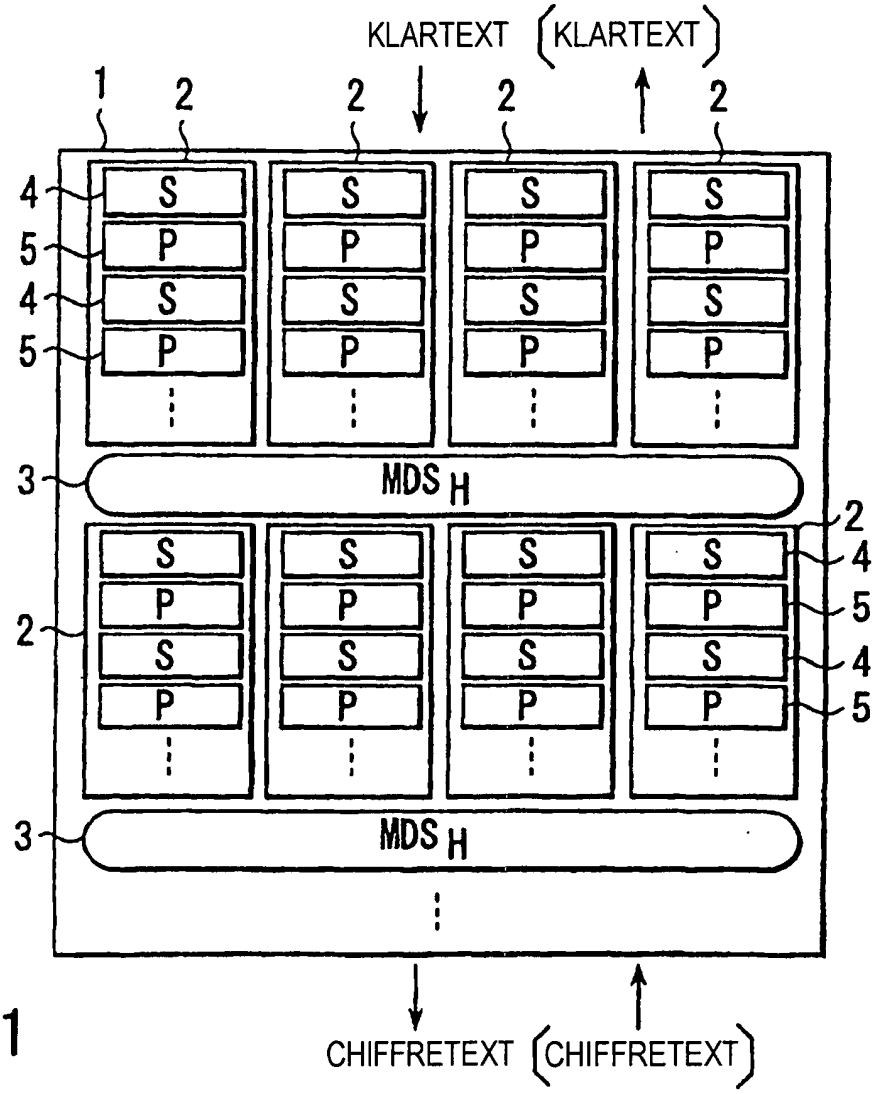


FIG. 1

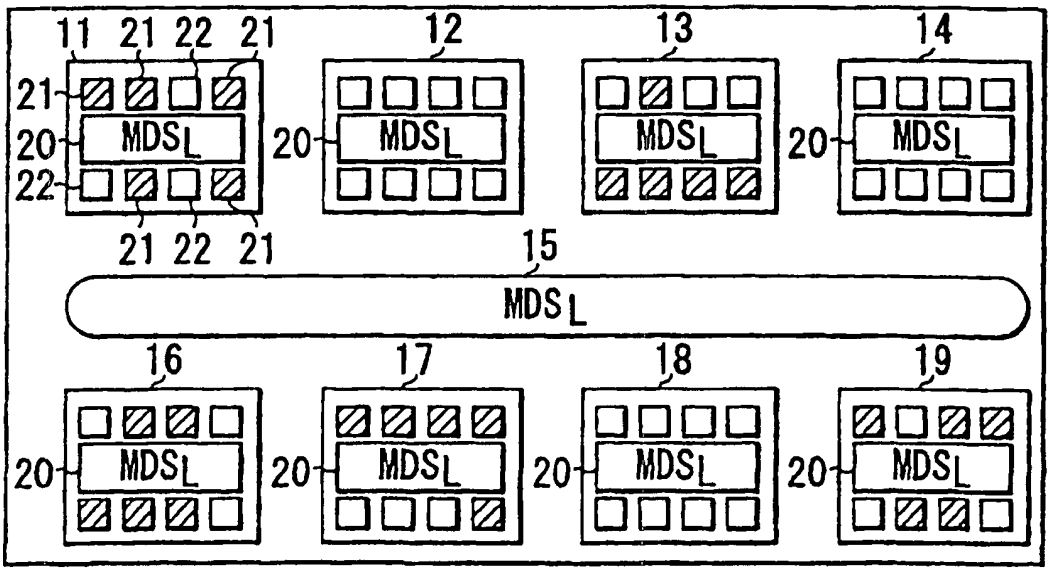


FIG. 2

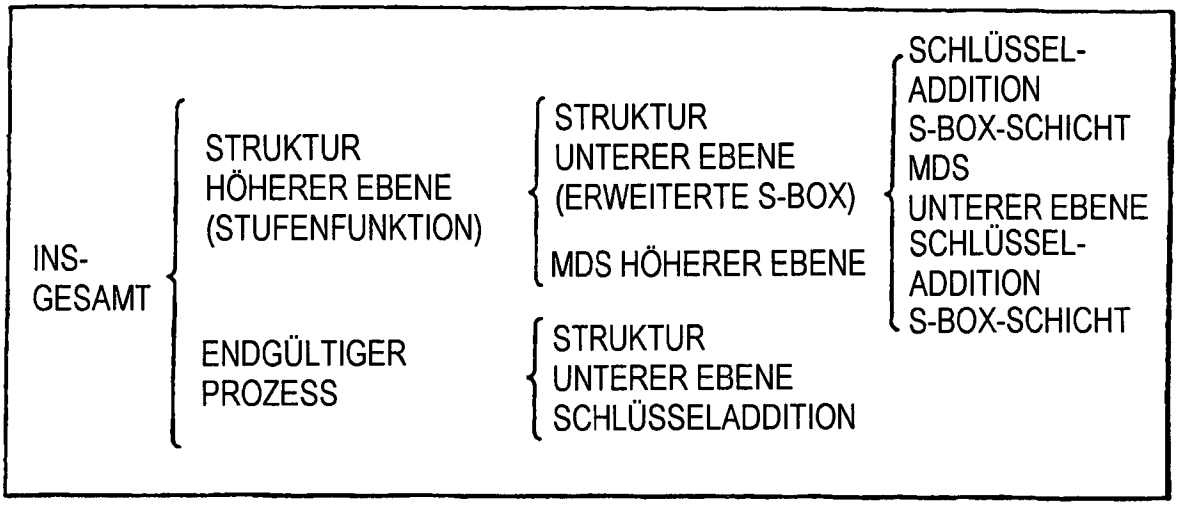

INS-
GESAMT
STRUKTUR
HÖHERER EBENE
(STUFENFUNKTION)
ENDGÜLTIGER
PROZESS
STRUKTUR
UNTERER EBENE
(ERWEITERTE S-BOX)
MDS HÖHERER EBENE
STRUKTUR
UNTERER EBENE
SCHLÜSSELADDITION
SCHLÜSSEL-
ADDITION
S-BOX-SCHICHT
MDS
UNTERER EBENE
SCHLÜSSEL-
ADDITION
S-BOX-SCHICHT

FIG. 3

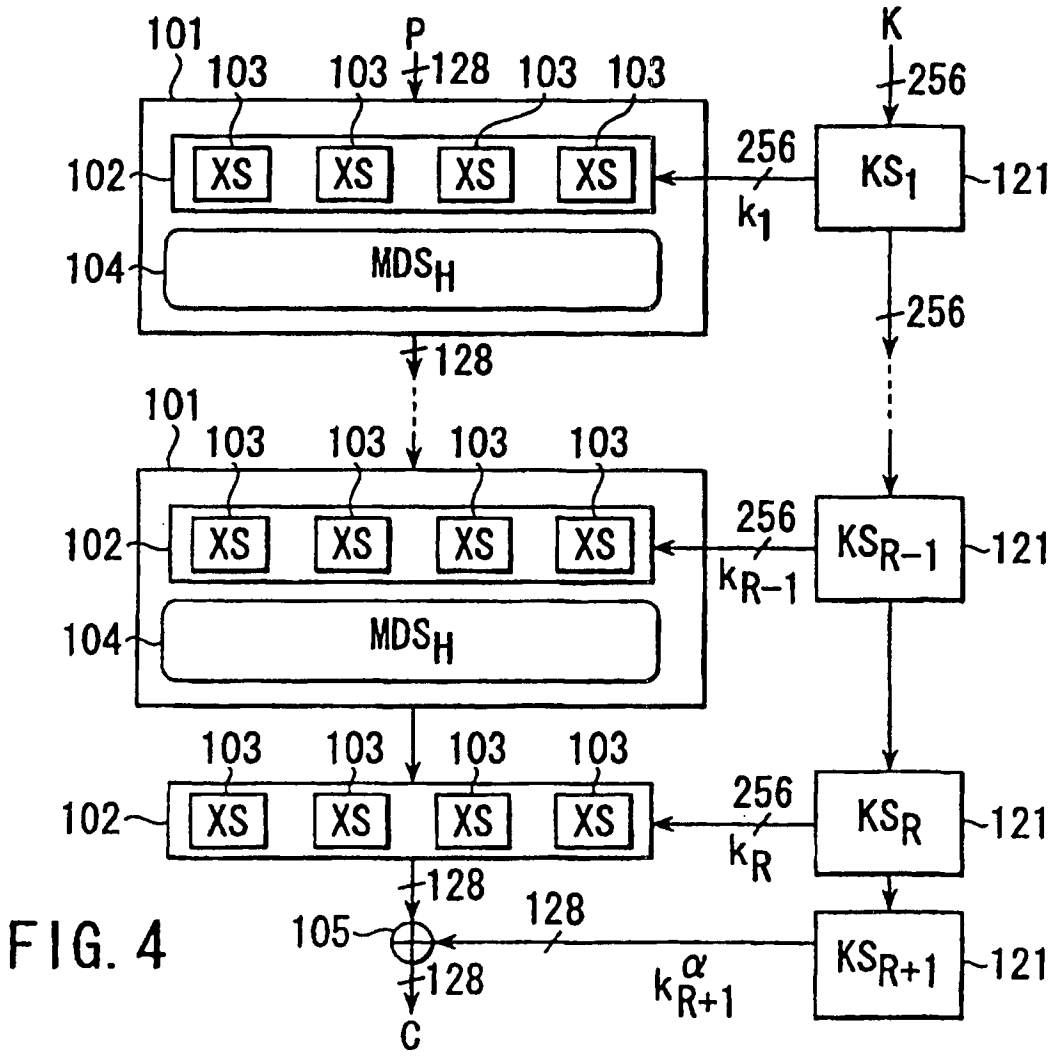

101
P
128
103
K
256
102
XS
104
MDS_H
KS_1
121
k_1
KS_R-1
k_R-1
KS_R
k_R
KS_R+1
k_R+1
105
C

FIG. 4

```
s[256]={
   72 AA 49 16 1E 3A 43 AE 66 BC 00 73 79 3B FB 9F
   69 6A A2 50 6E F5 EF AC 22 02 AD 26 E2 DF 97 F0
   9E BF 17 8B FA 7C F4 71 7F CA F6 52 FD C3 E5 64
   53 8D E0 F3 0F 78 CB 9B 68 3C 0D 1F 89 B6 EB F7
   44 4A 06 A6 56 6B 85 01 30 88 51 31 9C A0 A3 25
   60 5B FF 05 B7 91 15 B3 A9 20 03 2B 61 42 95 4D
   F9 7E 0E E9 D8 F1 46 99 CE BE D9 54 80 B0 D2 4F
   7A E8 35 92 1B 7B 12 D6 4C D5 E7 EE B1 24 DE 21
   04 10 AB 29 9A 81 FE A7 B8 63 28 0A 8A D1 C6 07
   B9 C8 98 82 74 9D 84 47 94 C7 6C 11 D7 BA C1 C9
   DD 77 39 2F 2E C2 67 41 E4 58 34 CD 1C 93 96 7D
   2C F8 B5 70 14 08 DC CC 87 D0 5E 32 C5 C4 59 3E
   CF 55 5C 23 75 2D 2A 86 4B 1D 5F E6 FC B2 4E 09
   27 AF 19 B4 BD 6D 3D 6F ED 62 EA F2 D3 36 38 DB
   BB 83 45 37 A4 EC 8C 5D E1 33 90 A1 40 8E 1A A5
   0B 3F 5A DA 13 76 0C C0 48 E3 65 A8 18 8F D4 57 }
```

112

FIG. 5

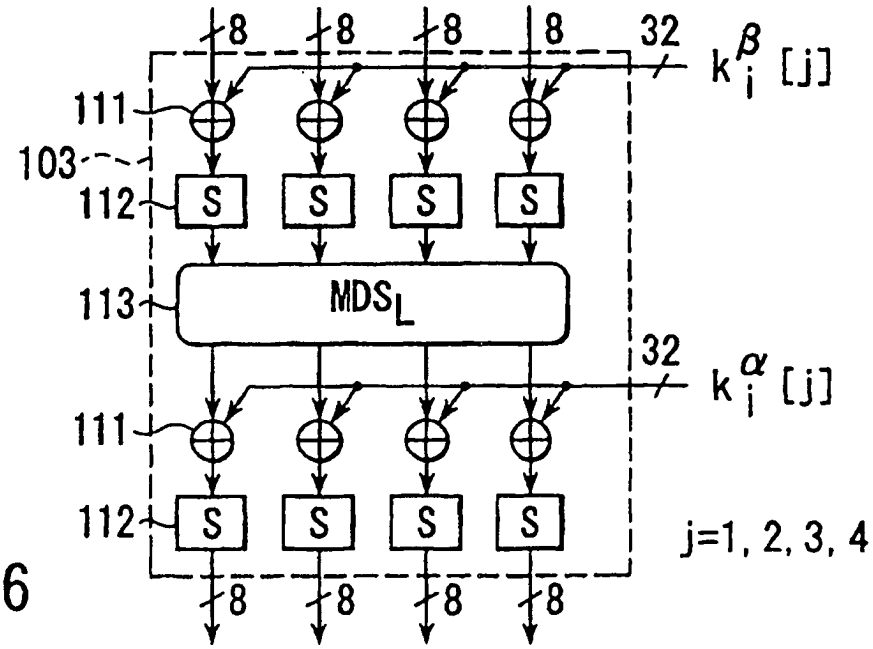


FIG. 6

FIG. 7

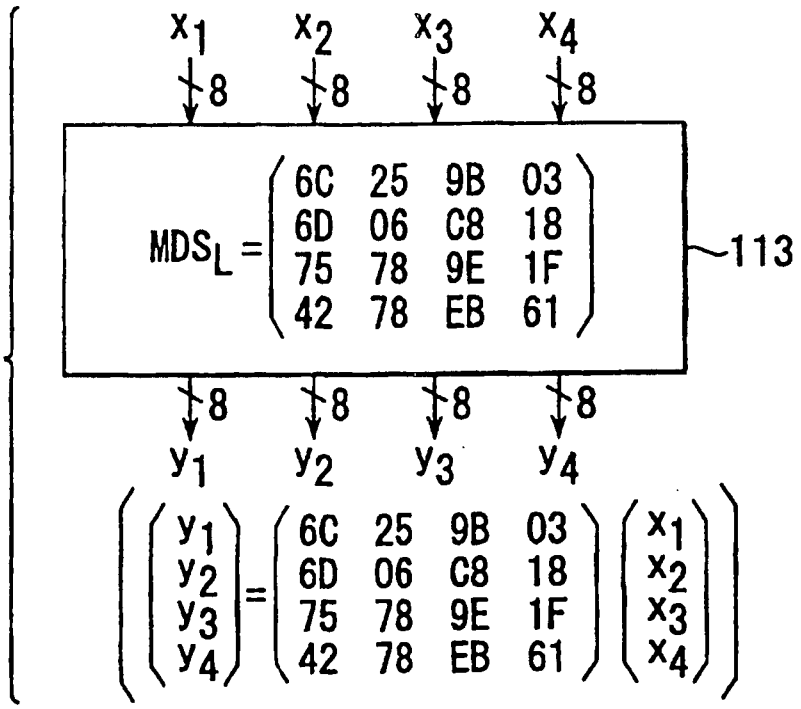


FIG. 8

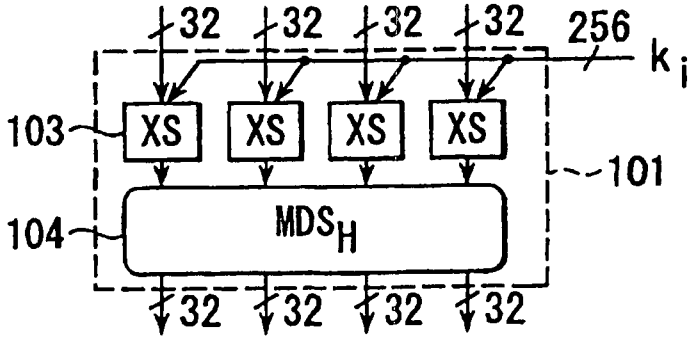
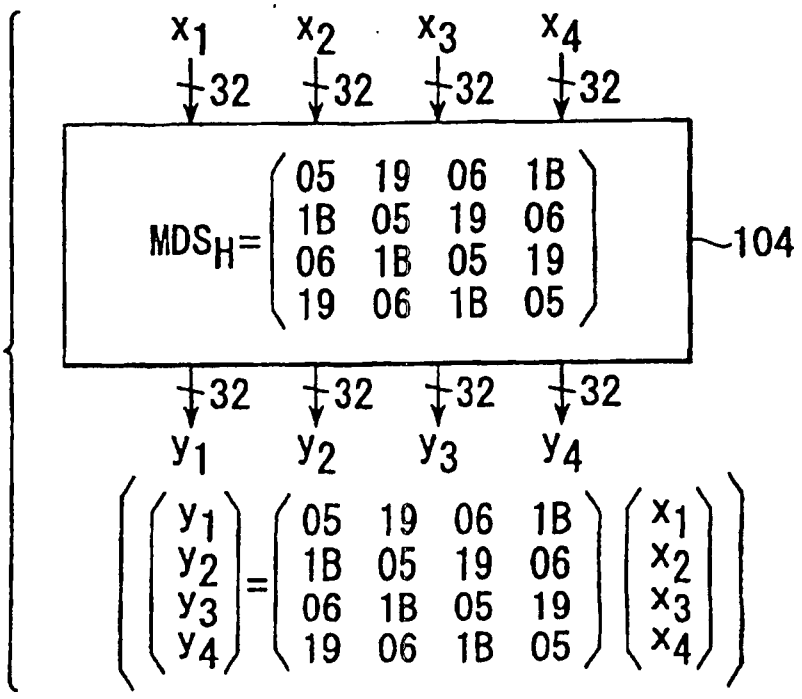
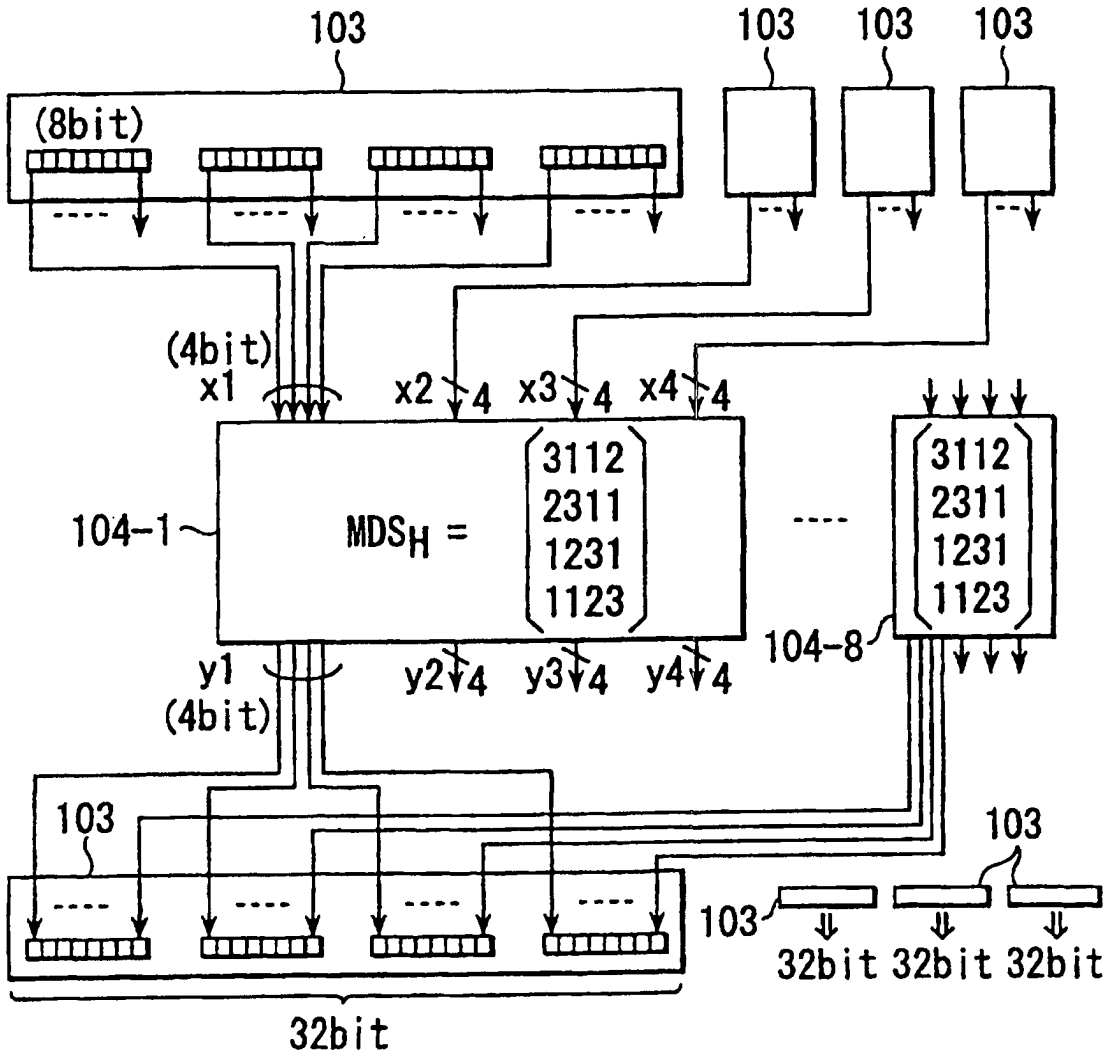


FIG. 9





$$\left(\begin{pmatrix} y1 \\ y2 \\ y3 \\ y4 \end{pmatrix} = \begin{pmatrix} 3112 \\ 2311 \\ 1231 \\ 1123 \end{pmatrix} \begin{pmatrix} x1 \\ x2 \\ x3 \\ x4 \end{pmatrix} \right)$$

FIG. 10

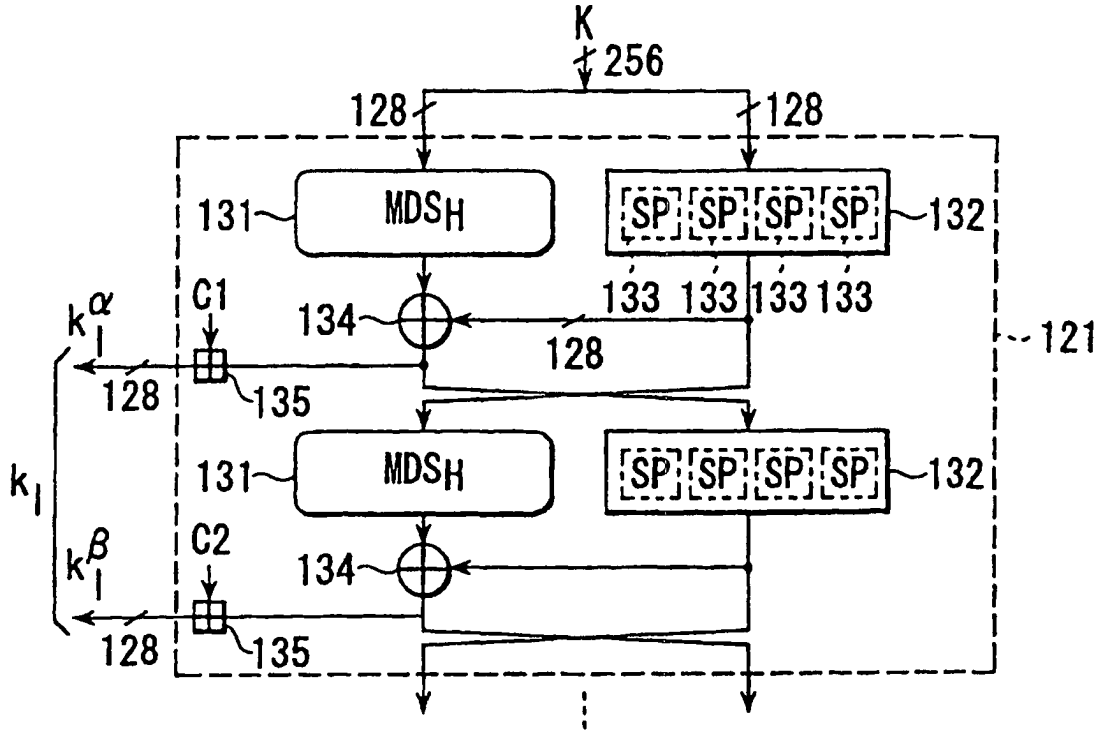

K
256
128
128
131
MDSH
SP SP SP SP
132
133 133 133 133
C1
134
128
121
k_l^{α}
128
135
k_l
131
MDSH
SP SP SP SP
132
C2
134
k_l^{β}
128
135

FIG. 11

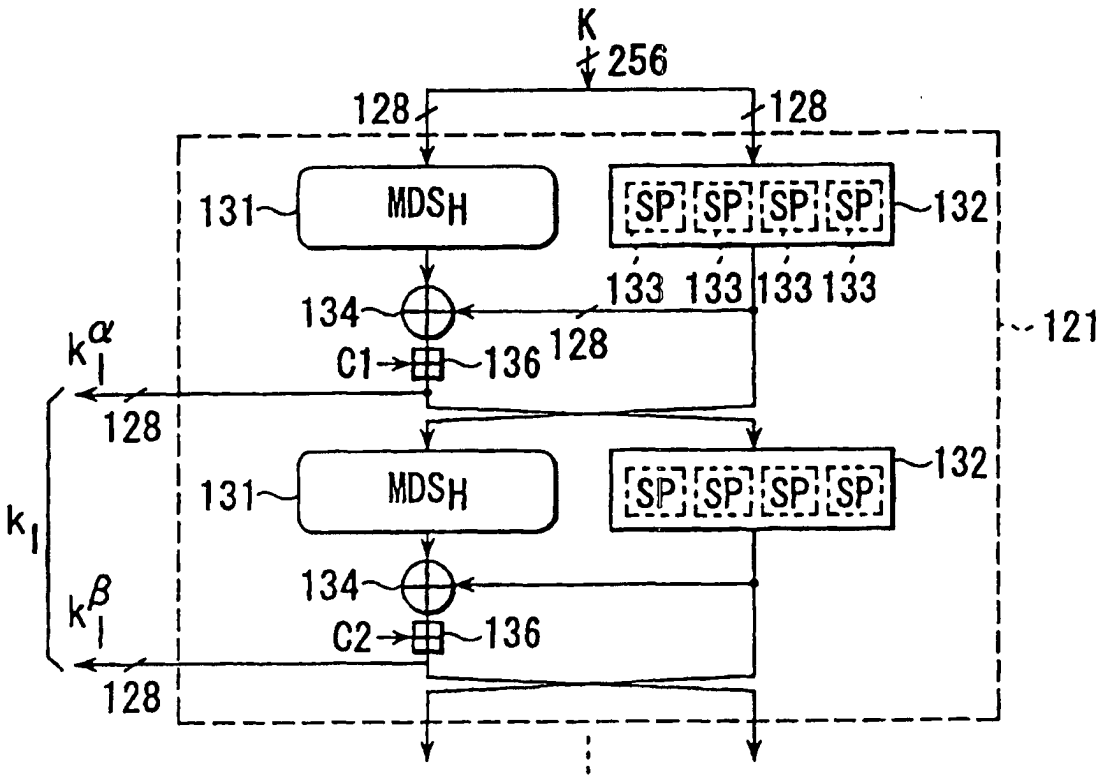

K
256
128
128
131
MDSH
SP SP SP SP
132
133 133 133 133
134
C1
136
128
121
k_l^{α}
128
k_l
131
MDSH
SP SP SP SP
132
134
C2
136
k_l^{β}
128

FIG. 12

FIG. 13

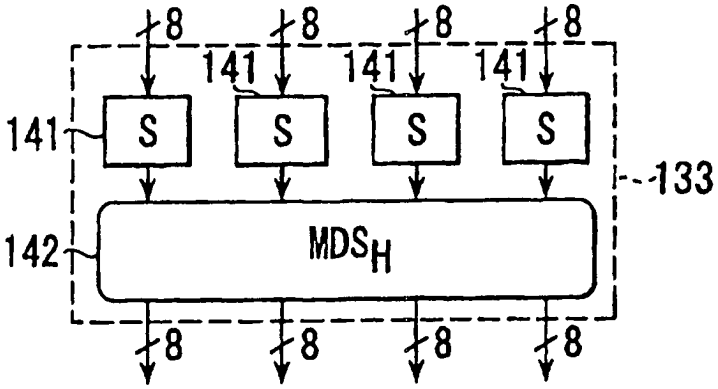


FIG. 14

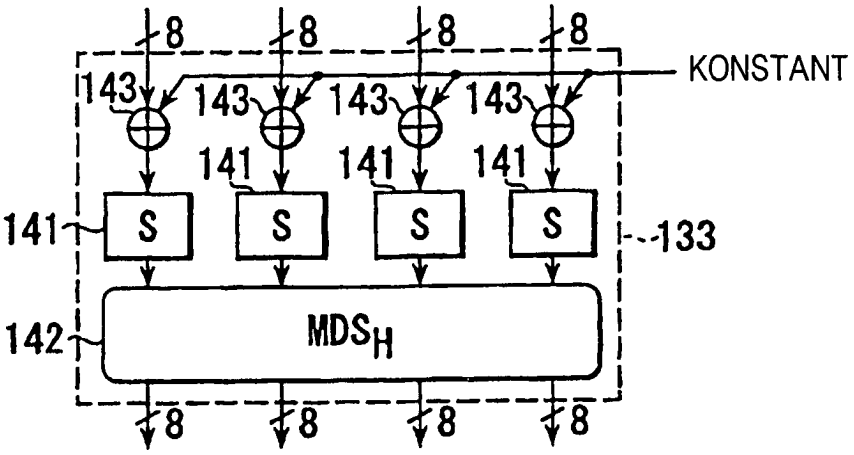


FIG. 15

C1	(H2, H0, H1, H1)
C2	(H3, H2, H0, H3)
C3	(H1, H0, H0, H0)
C4	(H1, H0, H1, H3)
C5	(H0, H1, H0, H2)
C6	(H3, H2, H0, H0)
C7	(H1, H2, H1, H0)
C8	(H2, H1, H2, H3)
C9	(H2, H1, H0, H0)
C10	(H1, H1, H1, H2)
C11	(H3, H1, H1, H2)
C12	(H1, H1, H2, H0)
C13	(H1, H3, H3, H1)
C14	(H2, H3, H3, H1)
C15	(H1, H3, H1, H0)
C16	(H1, H0, H0, H3)
C17	(H1, H2, H0, H3)

WOBEI

$H0 = (5A827999)_H = \lfloor \sqrt{2}/4 \times 2^{32} \rfloor$

$H1 = (6ED9EBA1)_H = \lfloor \sqrt{3}/4 \times 2^{32} \rfloor$

$H2 = (8F1BBCDC)_H = \lfloor \sqrt{5}/4 \times 2^{32} \rfloor$

$H3 = (CA62C1D6)_H = \lfloor \sqrt{10}/4 \times 2^{32} \rfloor$

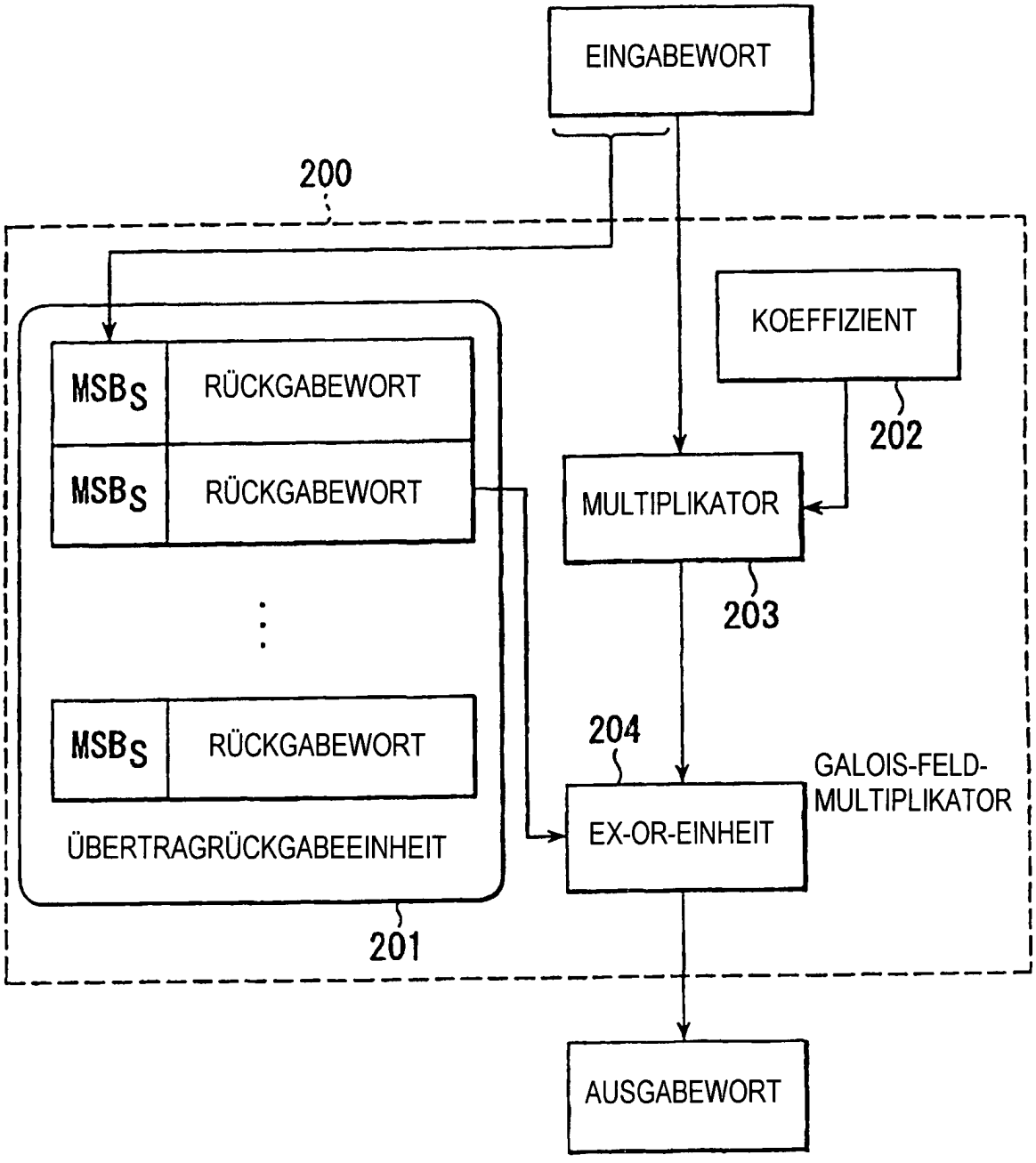

EINGABEWORT
200
KOEFFIZIENT
MSBS
RÜCKGABEWORT
MSBS
RÜCKGABEWORT
202
MULTIPLIKATOR
203
MSBS
RÜCKGABEWORT
204
GALOIS-FELD-
MULTIPLIKATOR
EX-OR-EINHEIT
ÜBERTRAGRÜCKGABEEINHEIT
201
AUSGABEWORT

FIG. 16

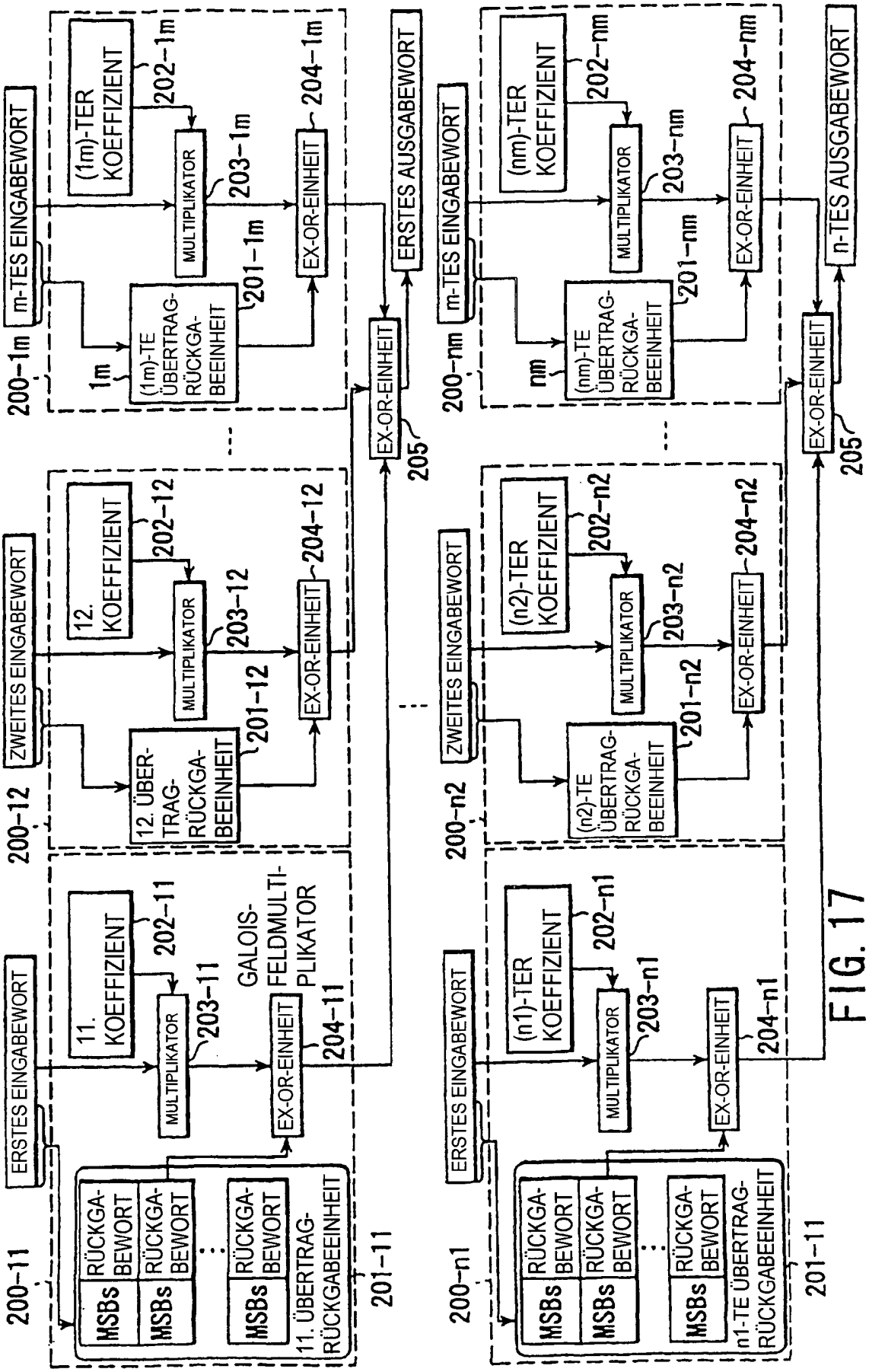

200-11
ERSTES EINGABEWORT
11. KOEFFIZIENT
202-11
MULTIPLIKATOR
203-11
EX-OR-EINHEIT
204-11
GALOIS-FELDMULTI-PLIKATOR
MSBs
RÜCKGA-BEWORT
11. ÜBERTRAG-RÜCKGABEEINHEIT
201-11
200-12
ZWEITES EINGABEWORT
12. KOEFFIZIENT
202-12
MULTIPLIKATOR
203-12
EX-OR-EINHEIT
204-12
12. ÜBER-TRAG-RÜCKGA-BEEINHEIT
201-12
200-1m
m-TES EINGABEWORT
(1m)-TER KOEFFIZIENT
202-1m
MULTIPLIKATOR
203-1m
EX-OR-EINHEIT
204-1m
1m
(1m)-TE ÜBERTRAG-RÜCKGA-BEEINHEIT
201-1m
ERSTES AUSGABEWORT
EX-OR-EINHEIT
205
200-n1
ERSTES EINGABEWORT
(n1)-TER KOEFFIZIENT
202-n1
MULTIPLIKATOR
203-n1
EX-OR-EINHEIT
204-n1
n1-TE ÜBERTRAG-RÜCKGABEEINHEIT
201-11
200-n2
ZWEITES EINGABEWORT
(n2)-TER KOEFFIZIENT
202-n2
MULTIPLIKATOR
203-n2
EX-OR-EINHEIT
204-n2
(n2)-TE ÜBERTRAG-RÜCKGA-BEEINHEIT
201-n2
200-nm
m-TES EINGABEWORT
(nm)-TER KOEFFIZIENT
202-nm
MULTIPLIKATOR
203-nm
EX-OR-EINHEIT
204-nm
nm
(nm)-TE ÜBERTRAG-RÜCKGA-BEEINHEIT
201-nm
n-TES AUSGABEWORT
EX-OR-EINHEIT
205

FIG. 17

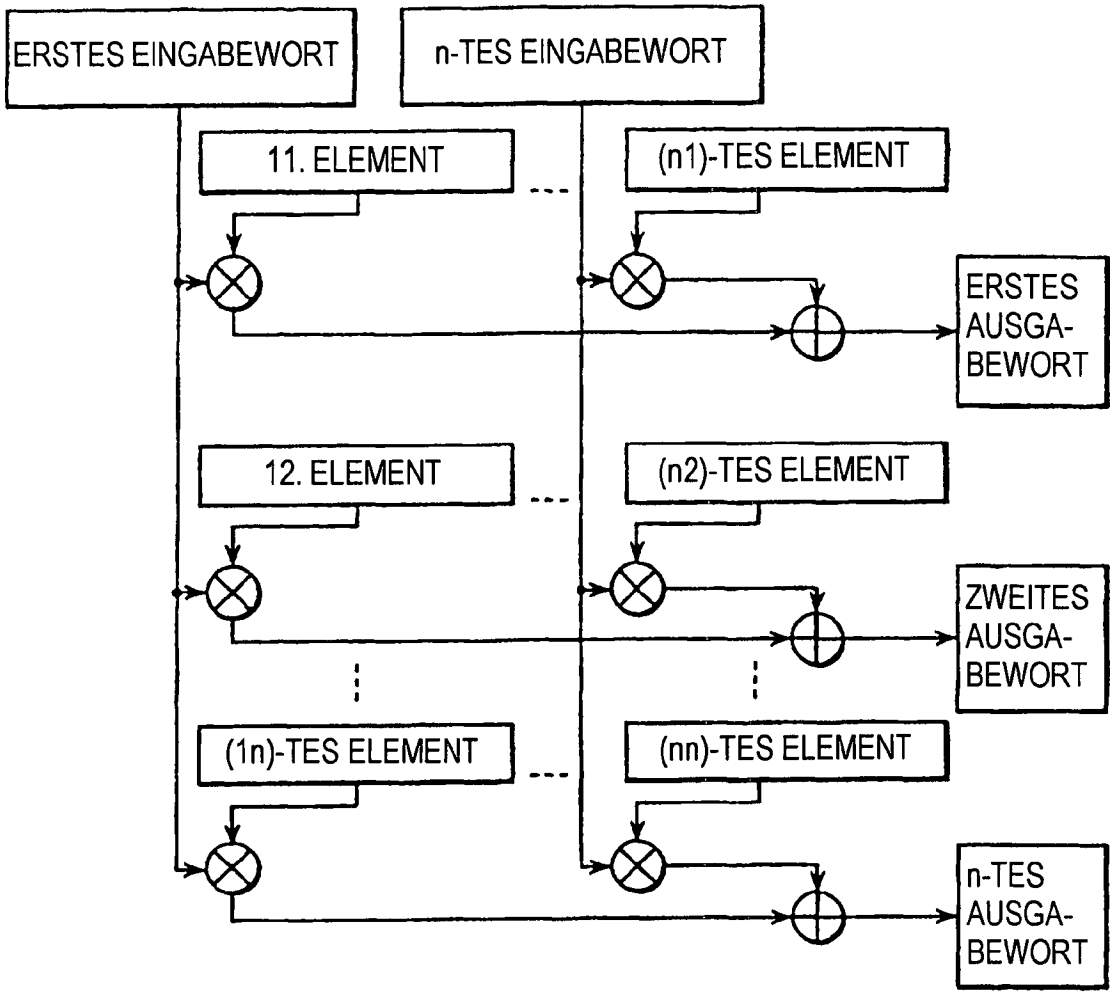

ERSTES EINGABEWORT
n-TES EINGABEWORT
11. ELEMENT
(n1)-TES ELEMENT
ERSTES AUSGA-BEWORT
12. ELEMENT
(n2)-TES ELEMENT
ZWEITES AUSGA-BEWORT
(1n)-TES ELEMENT
(nn)-TES ELEMENT
n-TES AUSGA-BEWORT

FIG. 18

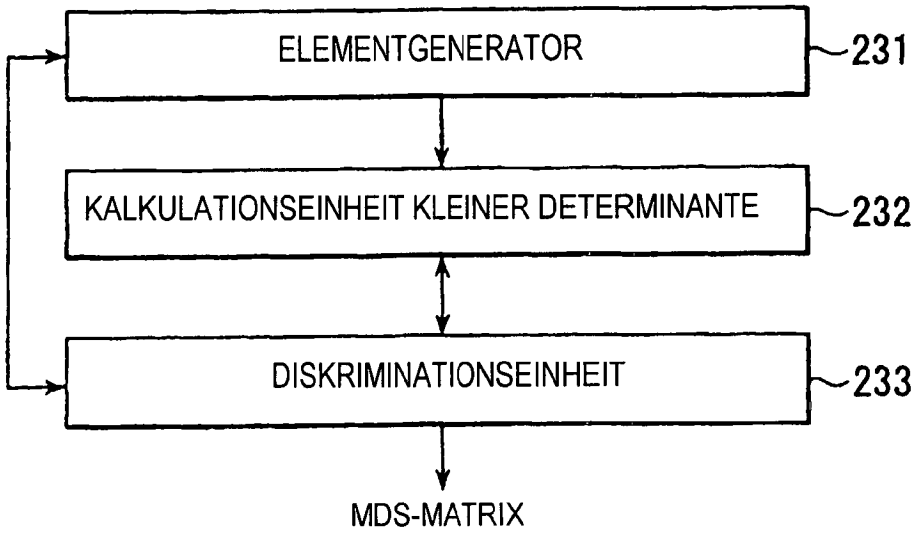

ELEMENTGENERATOR
231
KALKULATIONSEINHEIT KLEINER DETERMINANTE
232
DISKRIMINATIONSEINHEIT
233
MDS-MATRIX

FIG. 19

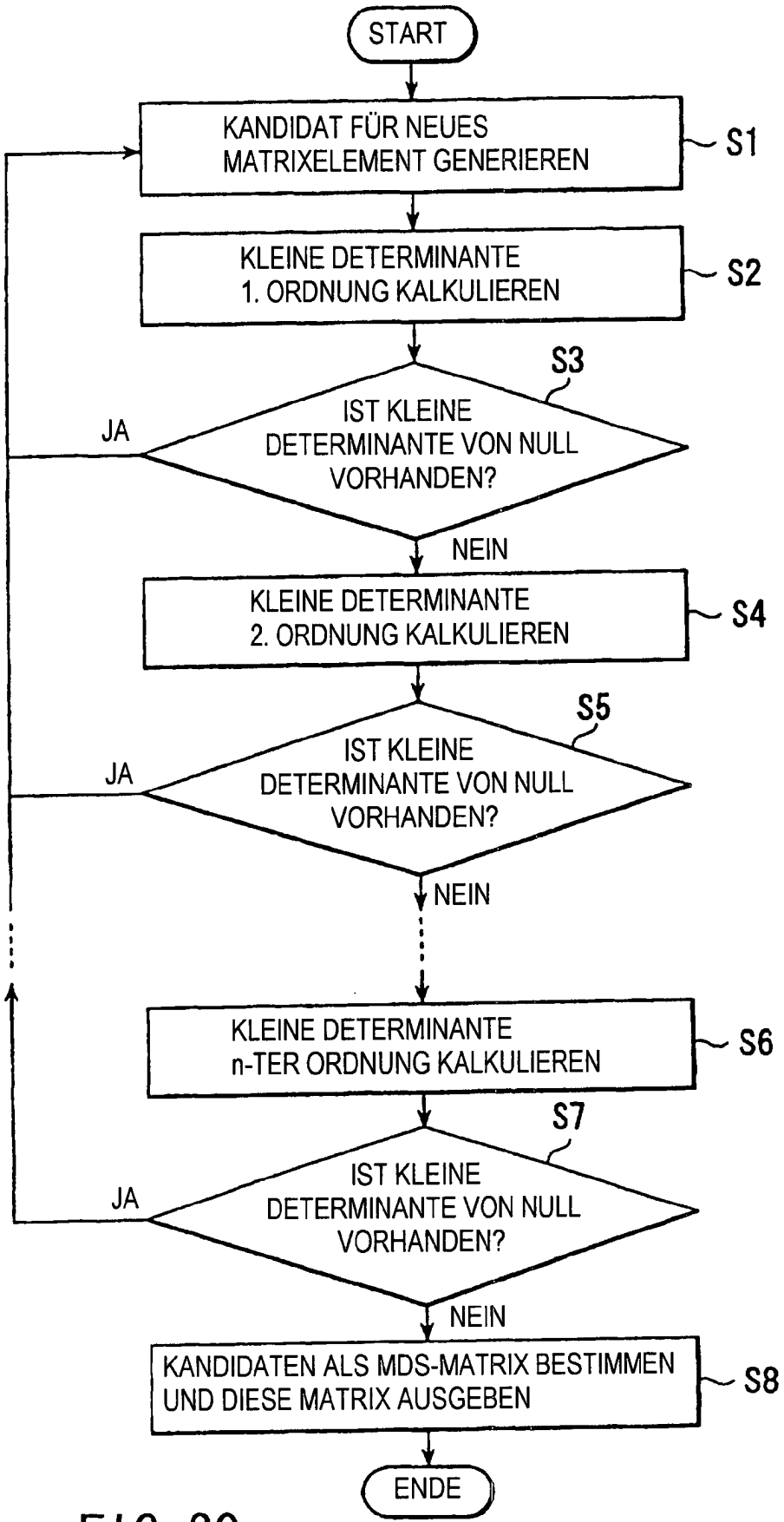

START
KANDIDAT FÜR NEUES MATRIXELEMENT GENERIEREN
S1
KLEINE DETERMINANTE 1. ORDNUNG KALKULIEREN
S2
S3
IST KLEINE DETERMINANTE VON NULL VORHANDEN?
JA
NEIN
KLEINE DETERMINANTE 2. ORDNUNG KALKULIEREN
S4
S5
IST KLEINE DETERMINANTE VON NULL VORHANDEN?
JA
NEIN
KLEINE DETERMINANTE n-TER ORDNUNG KALKULIEREN
S6
S7
IST KLEINE DETERMINANTE VON NULL VORHANDEN?
JA
NEIN
KANDIDATEN ALS MDS-MATRIX BESTIMMEN UND DIESE MATRIX AUSGEBEN
S8
ENDE

FIG. 20

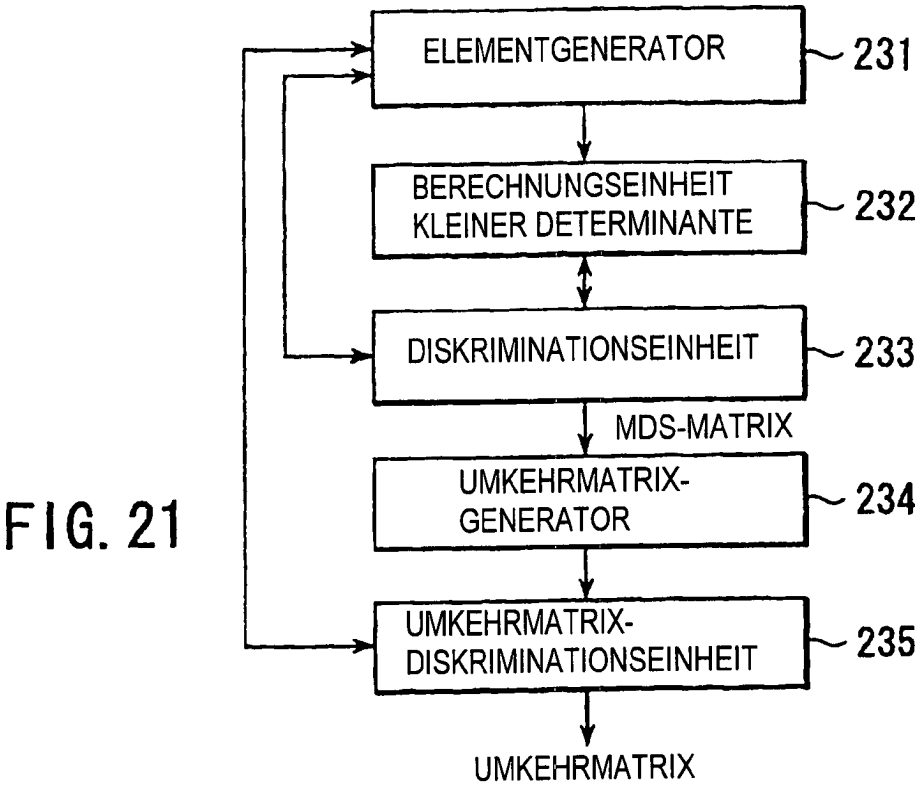

ELEMENTGENERATOR
231
BERECHNUNGSEINHEIT KLEINER DETERMINANTE
232
DISKRIMINATIONSEINHEIT
233
MDS-MATRIX
UMKEHRMATRIX-GENERATOR
234
UMKEHRMATRIX-DISKRIMINATIONSEINHEIT
235
UMKEHRMATRIX

FIG. 21

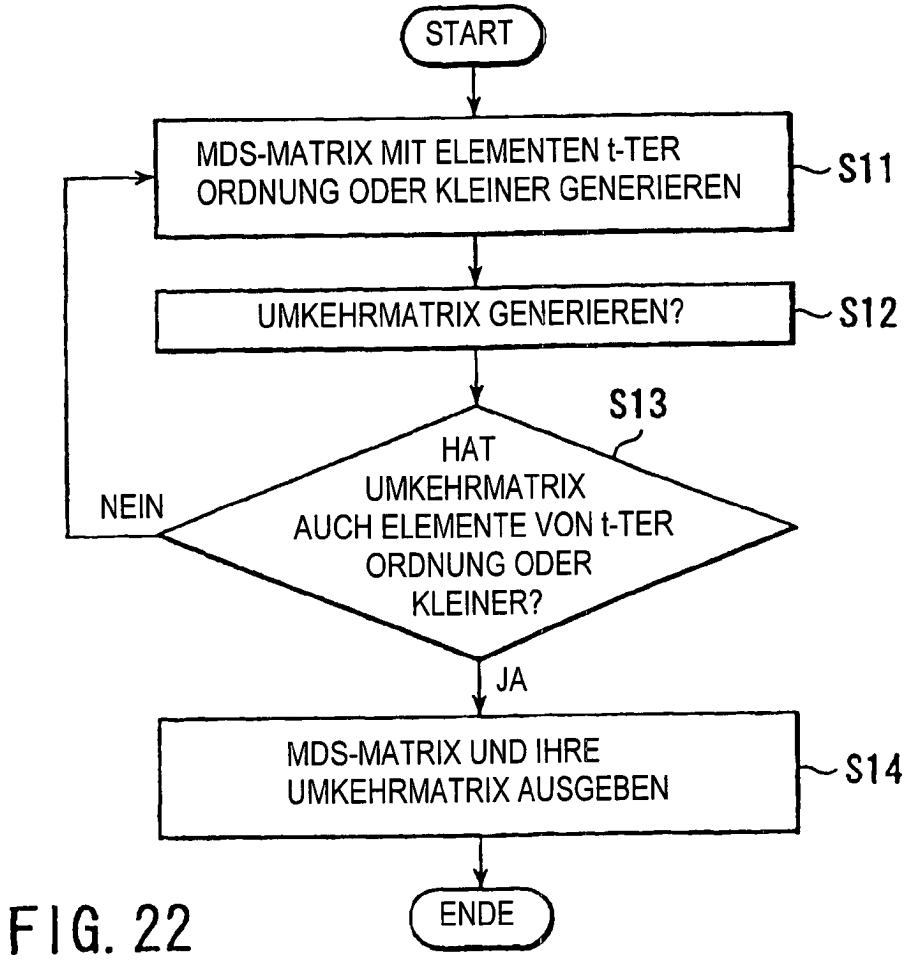

START
MDS-MATRIX MIT ELEMENTEN t-TER ORDNUNG ODER KLEINER GENERIEREN
S11
UMKEHRMATRIX GENERIEREN?
S12
S13
HAT UMKEHRMATRIX AUCH ELEMENTE VON t-TER ORDNUNG ODER KLEINER?
NEIN
JA
MDS-MATRIX UND IHRE UMKEHRMATRIX AUSGEBEN
S14
ENDE

FIG. 22

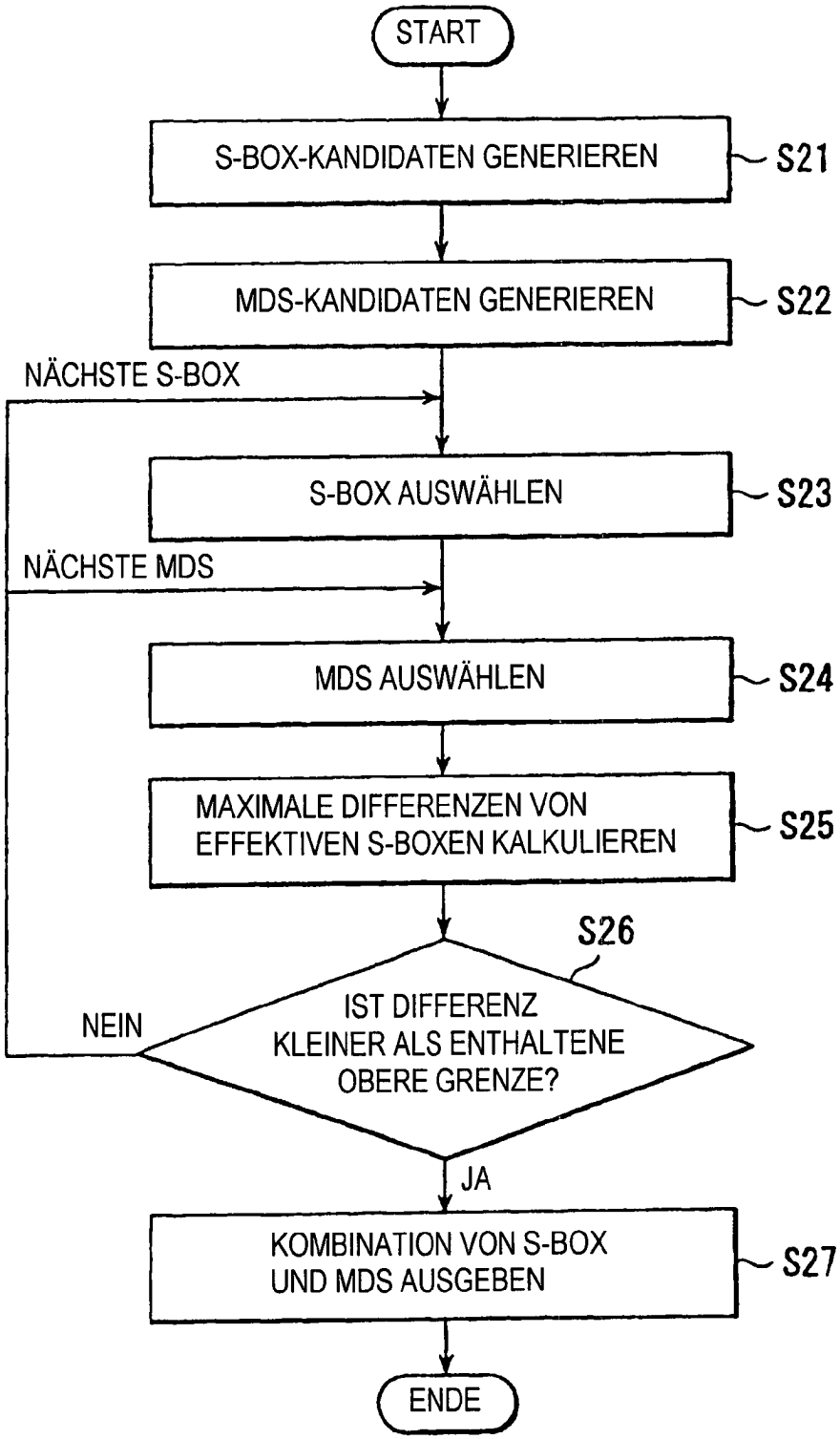

START
S-BOX-KANDIDATEN GENERIEREN
S21
MDS-KANDIDATEN GENERIEREN
S22
NÄCHSTE S-BOX
S-BOX AUSWÄHLEN
S23
NÄCHSTE MDS
MDS AUSWÄHLEN
S24
MAXIMALE DIFFERENZEN VON EFFEKTIVEN S-BOXEN KALKULIEREN
S25
S26
IST DIFFERENZ KLEINER ALS ENTHALTENE OBERE GRENZE?
NEIN
JA
KOMBINATION VON S-BOX UND MDS AUSGEBEN
S27
ENDE

FIG. 23

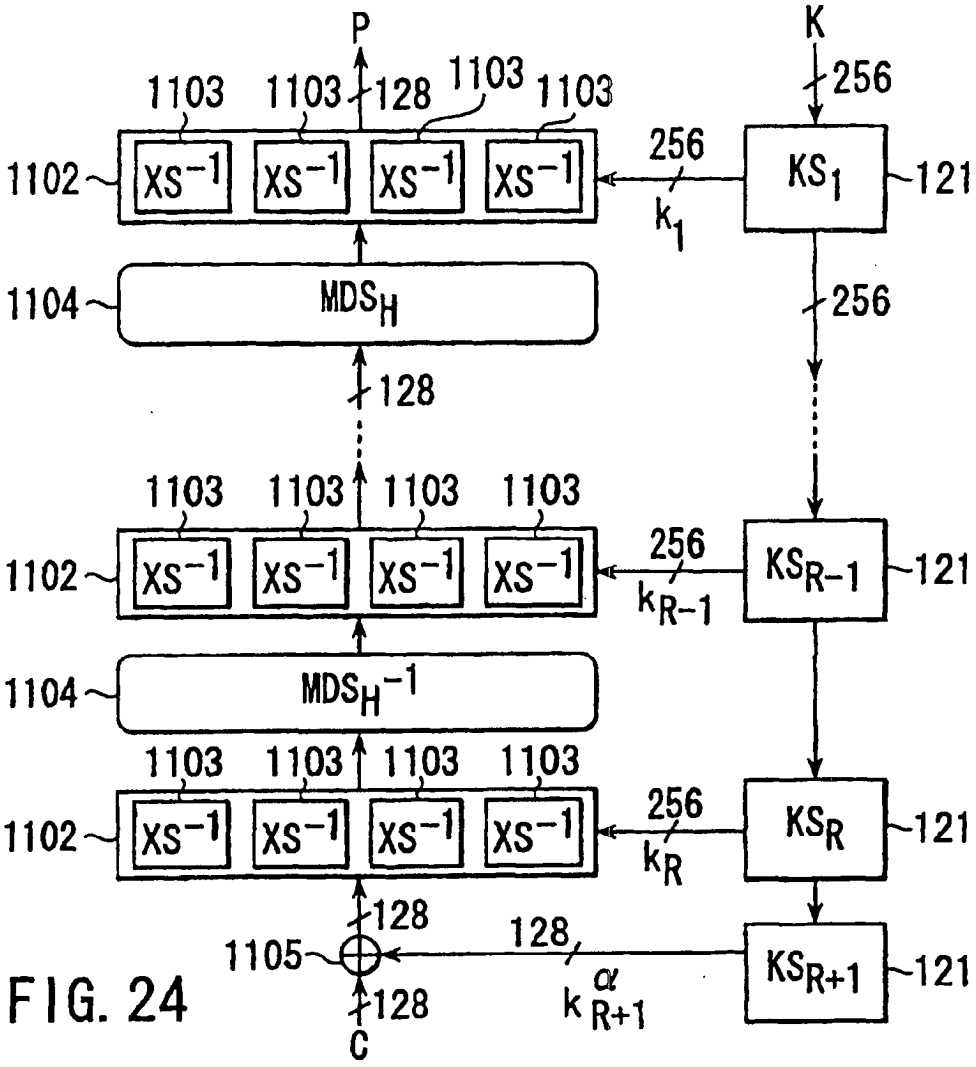

P
K
256
1103
128
1102
XS⁻¹
256
KS1
121
k1
1104
MDSH
MDSH⁻¹
KSR-1
kR-1
KSR
kR
KSR+1
kR+1
1105
C

FIG. 24

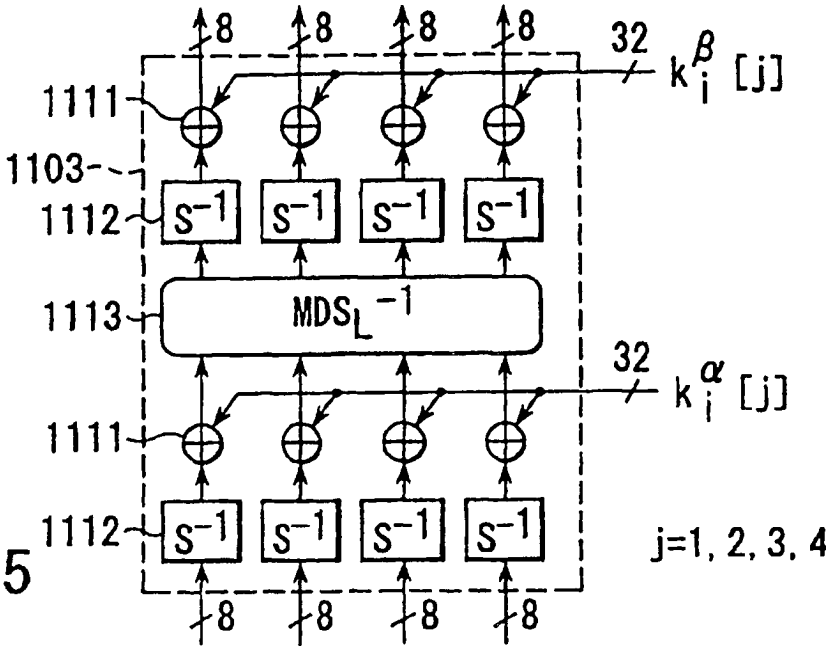

8
32
k i β [j]
1111
1103
1112
S⁻¹
1113
MDSL⁻¹
k i α [j]
j=1, 2, 3, 4

FIG. 25

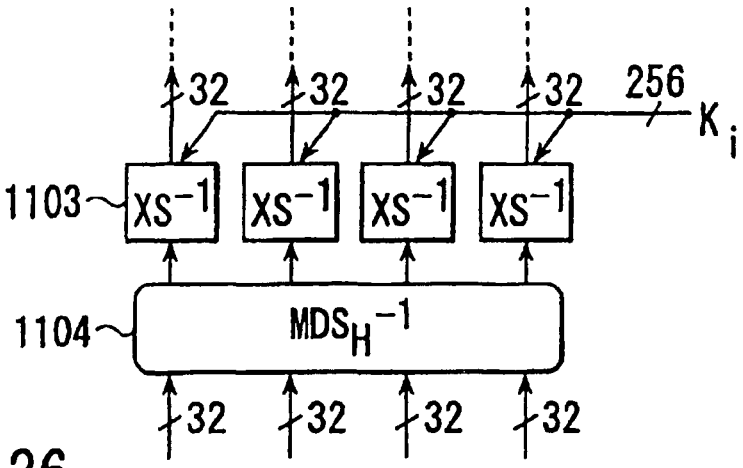

32
32
32
32
256
K_i
1103
XS^{-1}
XS^{-1}
XS^{-1}
XS^{-1}
1104
MDS_H^{-1}
32
32
32
32

FIG. 26

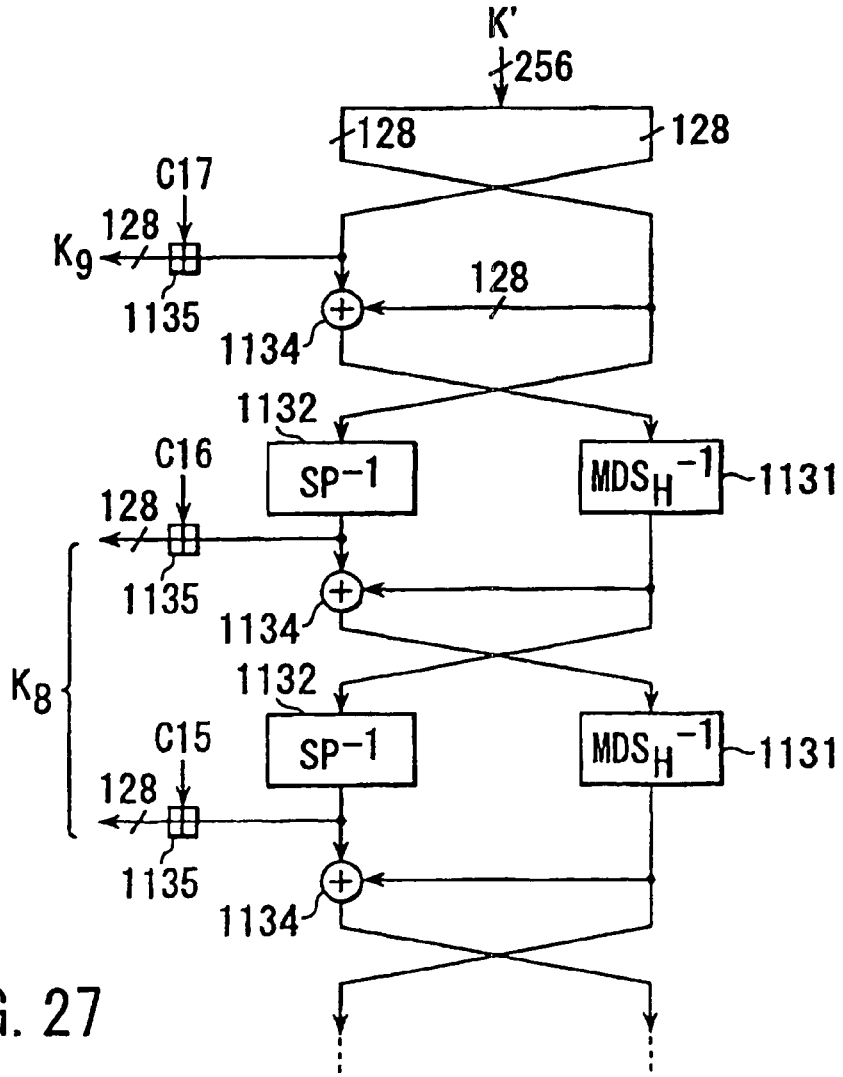

K'
256
128
128
C17
128
K_9
1135
1134
128
1132
C16
SP^{-1}
MDS_H^{-1}
1131
128
1135
1134
K_8
1132
C15
SP^{-1}
MDS_H^{-1}
1131
128
1135
1134

FIG. 27

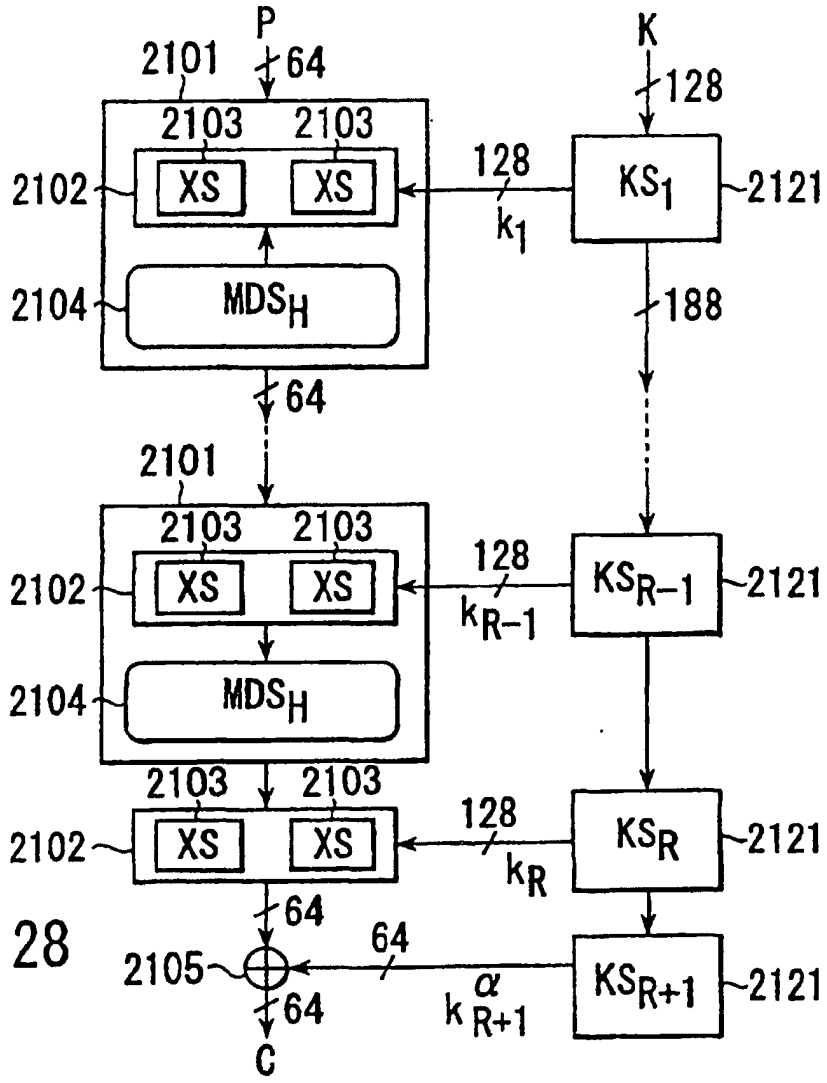

P
K
2101
64
128
2103
2103
2102
XS
XS
128
KS1
2121
k1
2104
MDSH
188
64
2101
2103
2103
2102
XS
XS
128
KSR-1
2121
kR-1
2104
MDSH
2103
2103
2102
XS
XS
128
KSR
2121
kR
64
64
2105
KSR+1
2121
α
k R+1
64
C

FIG. 28

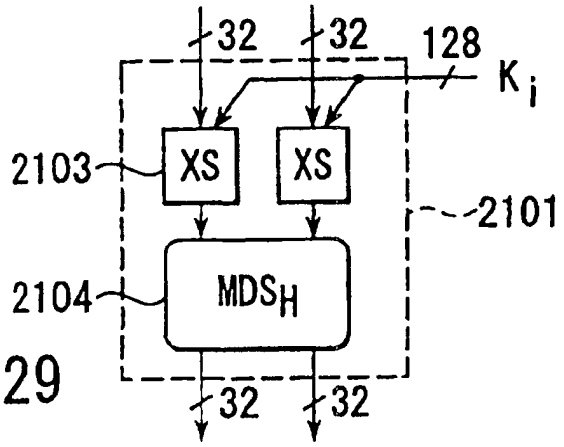
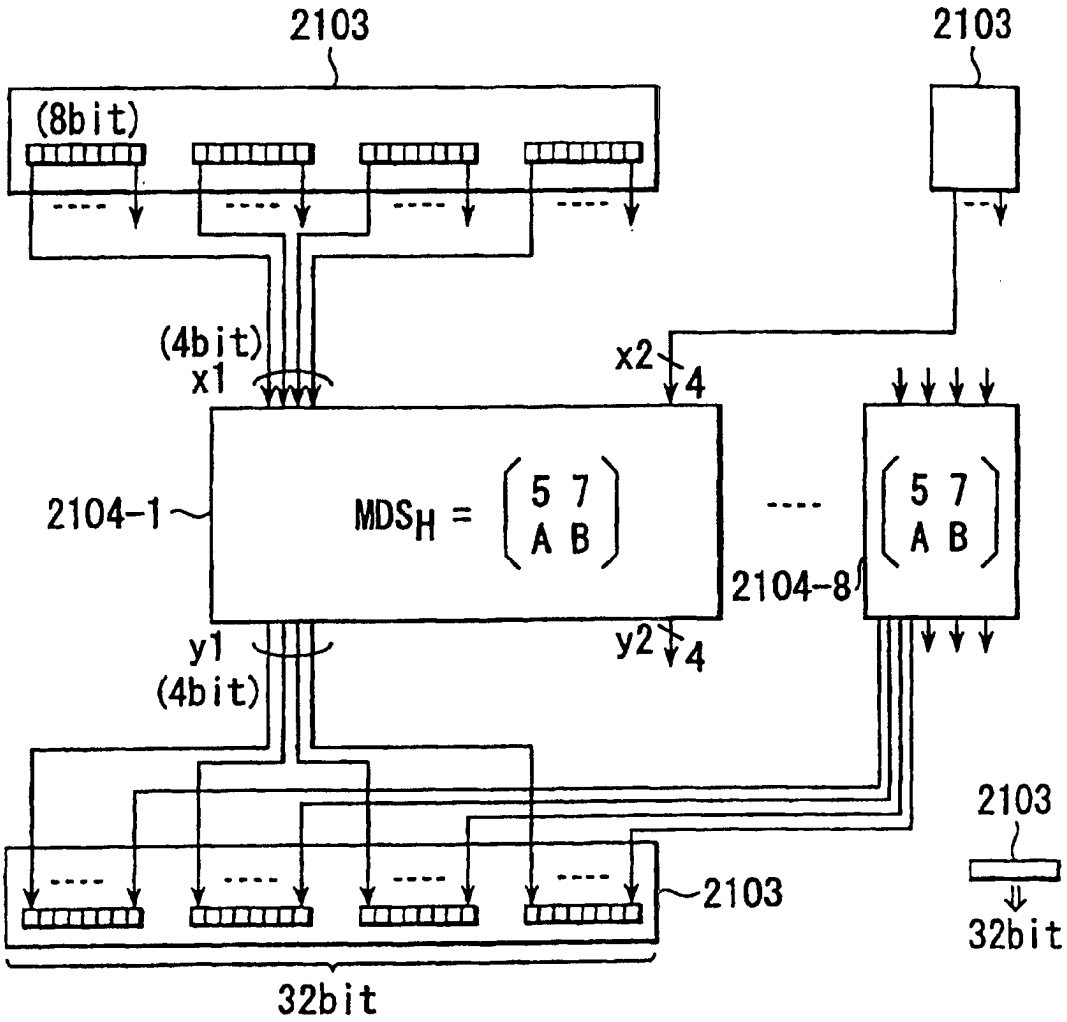

32
32
128
Ki
2103
XS
XS
2101
2104
MDSH
32
32

FIG. 29



$$\left[\begin{pmatrix} y1 \\ y2 \end{pmatrix} = \begin{pmatrix} 5 & 7 \\ A & B \end{pmatrix} \begin{pmatrix} x1 \\ x2 \end{pmatrix}\right]$$

FIG. 30

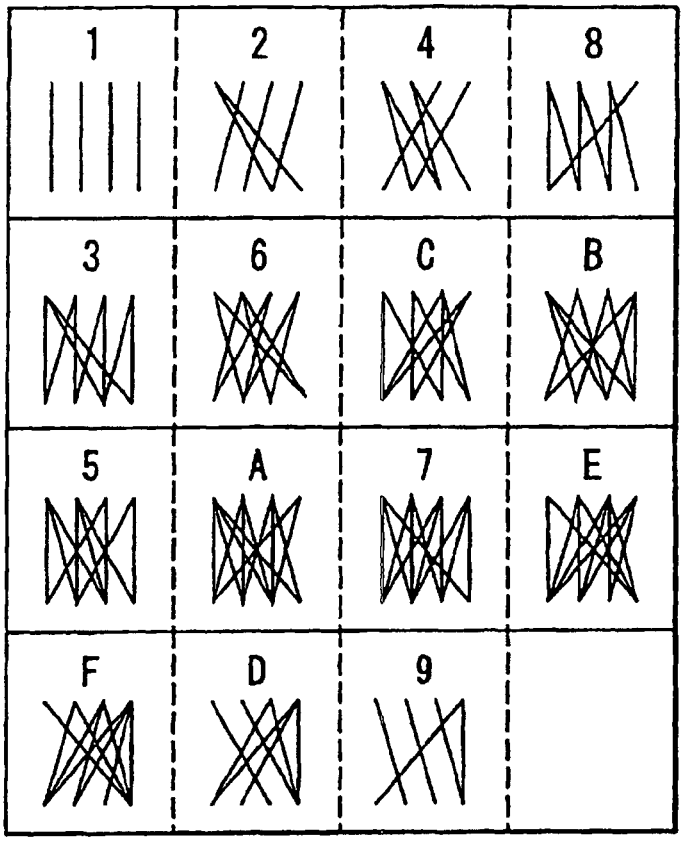


FIG. 31

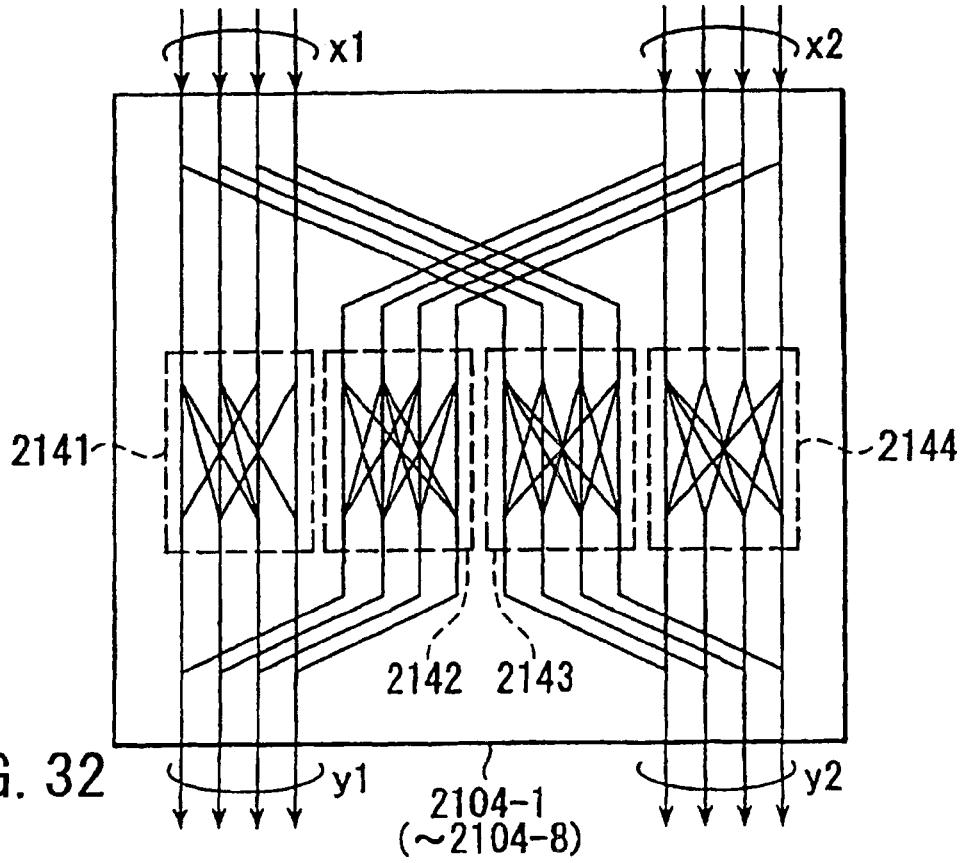


FIG. 32

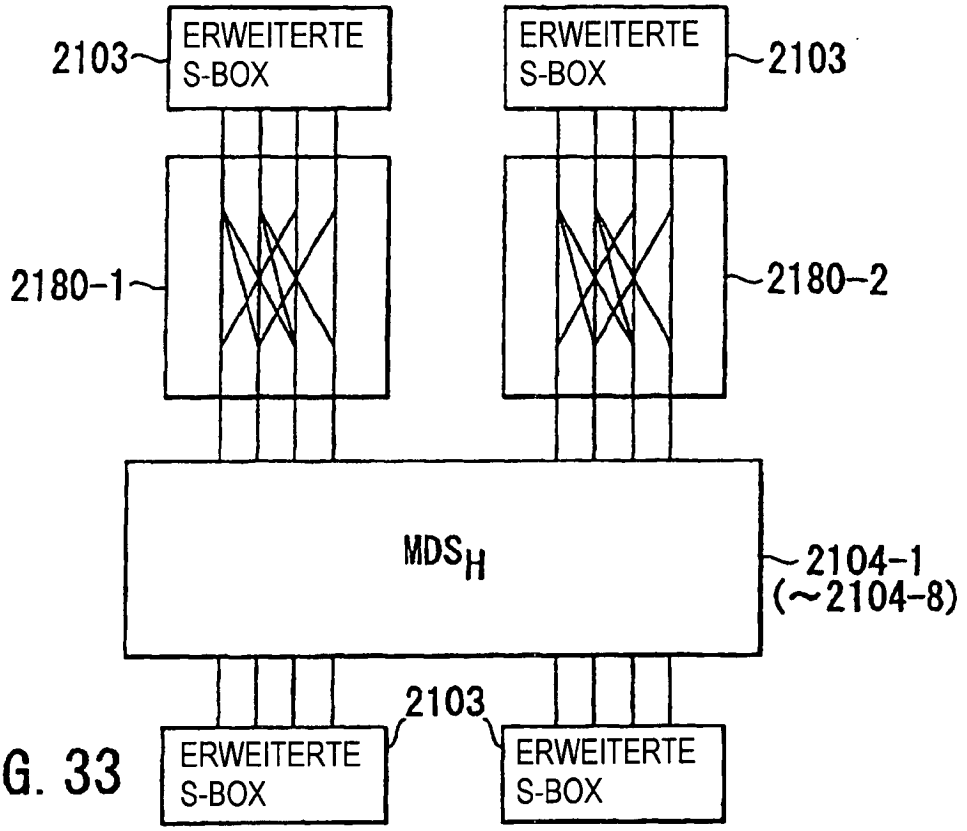

2103
ERWEITERTE S-BOX
ERWEITERTE S-BOX
2103
2180-1
2180-2
MDS$_H$
2104-1
(~2104-8)
2103
ERWEITERTE S-BOX
ERWEITERTE S-BOX

FIG. 33

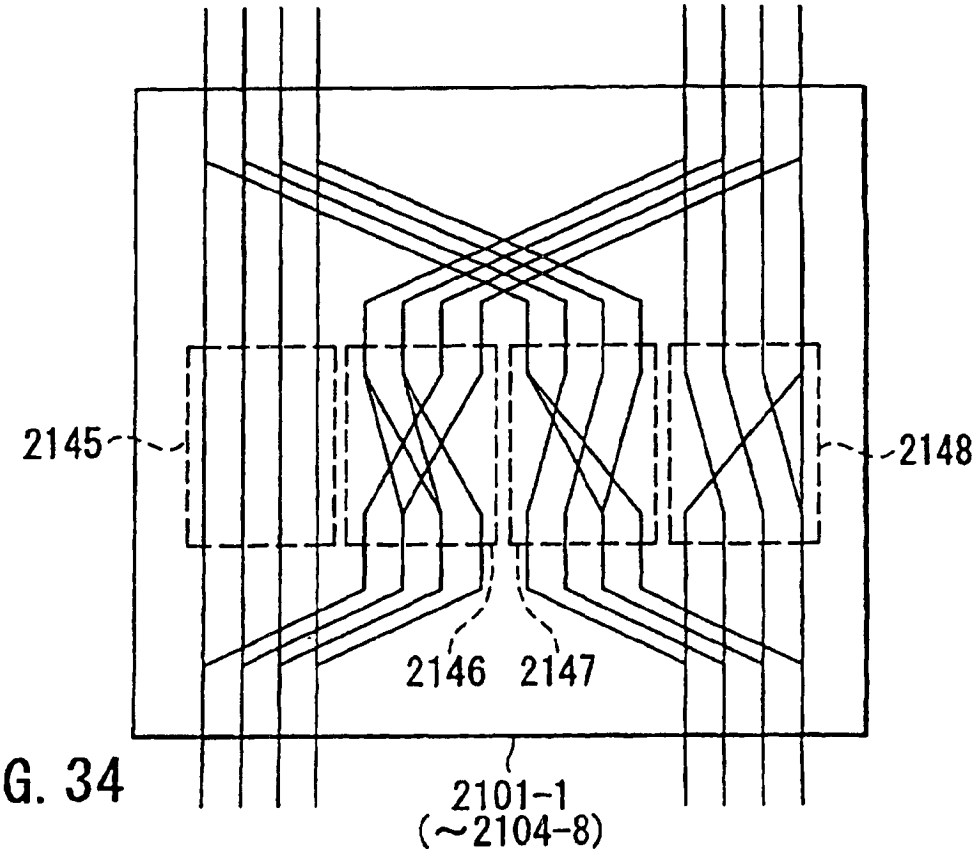

2145
2148
2146
2147
2101-1
(~2104-8)

FIG. 34

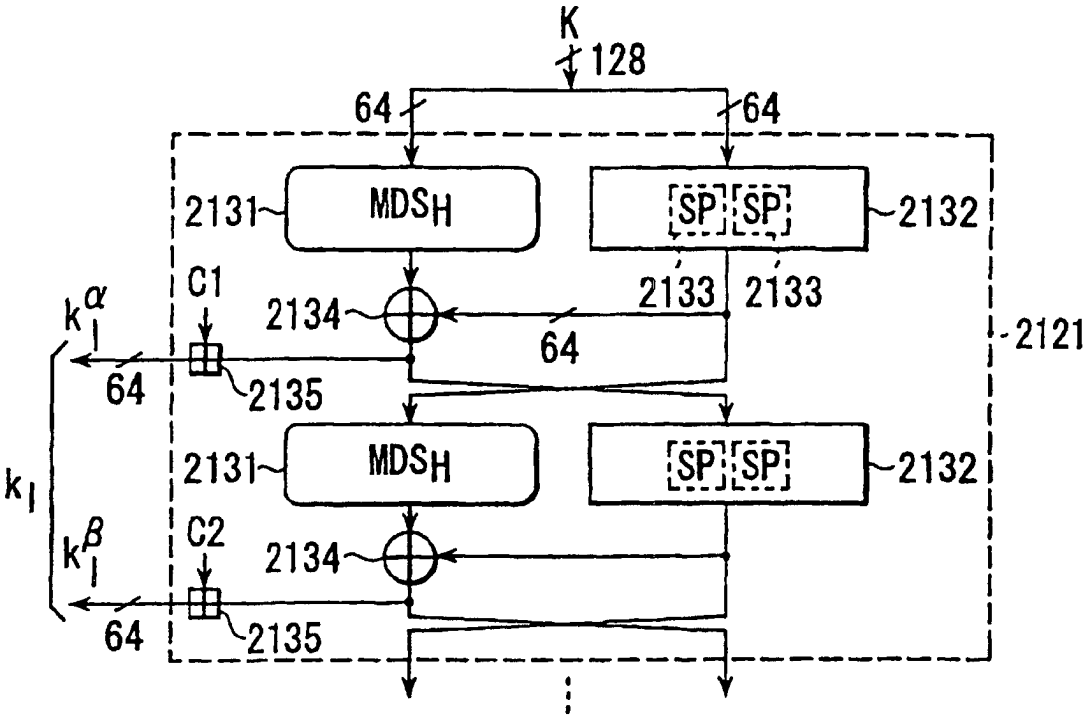

K
128
64
64
2131
MDSH
SP
SP
2132
2133
2133
C1
2134
64
2121
k_l^{α}
64
2135
2131
MDSH
SP
SP
2132
k_l
k_l^{β}
C2
2134
64
2135

FIG. 35

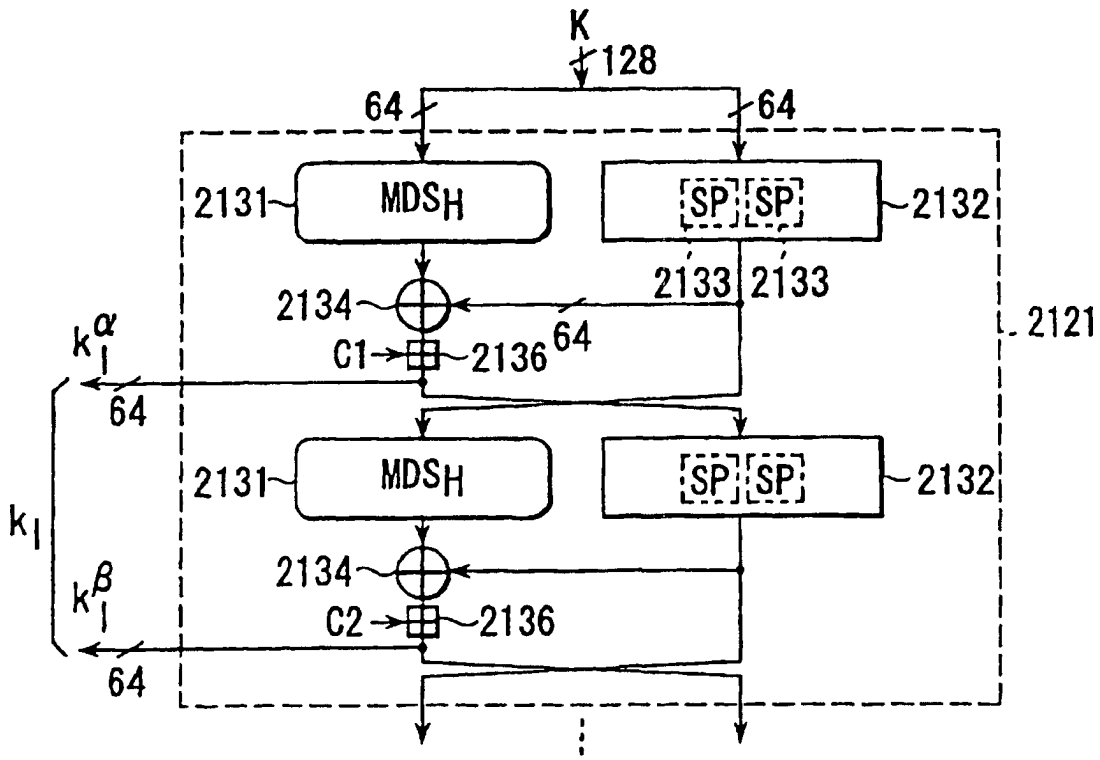

K
128
64
64
2131
MDSH
SP
SP
2132
2133
2133
2134
64
2121
k_l^{α}
C1
2136
64
2131
MDSH
SP
SP
2132
k_l
k_l^{β}
2134
C2
2136
64

FIG. 36

FIG. 37

C1	(H2, H0)
C2	(H1, H1)
C3	(H3, H2)
C4	(H0, H3)
C5	(H1, H0)
C6	(H0, H0)
C7	(H1, H0)
C8	(H1, H3)
C9	(H0, H1)
C10	(H0, H2)
C11	(H3, H2)
C12	(H0, H0)
C13	(H1, H2)

WOBEI

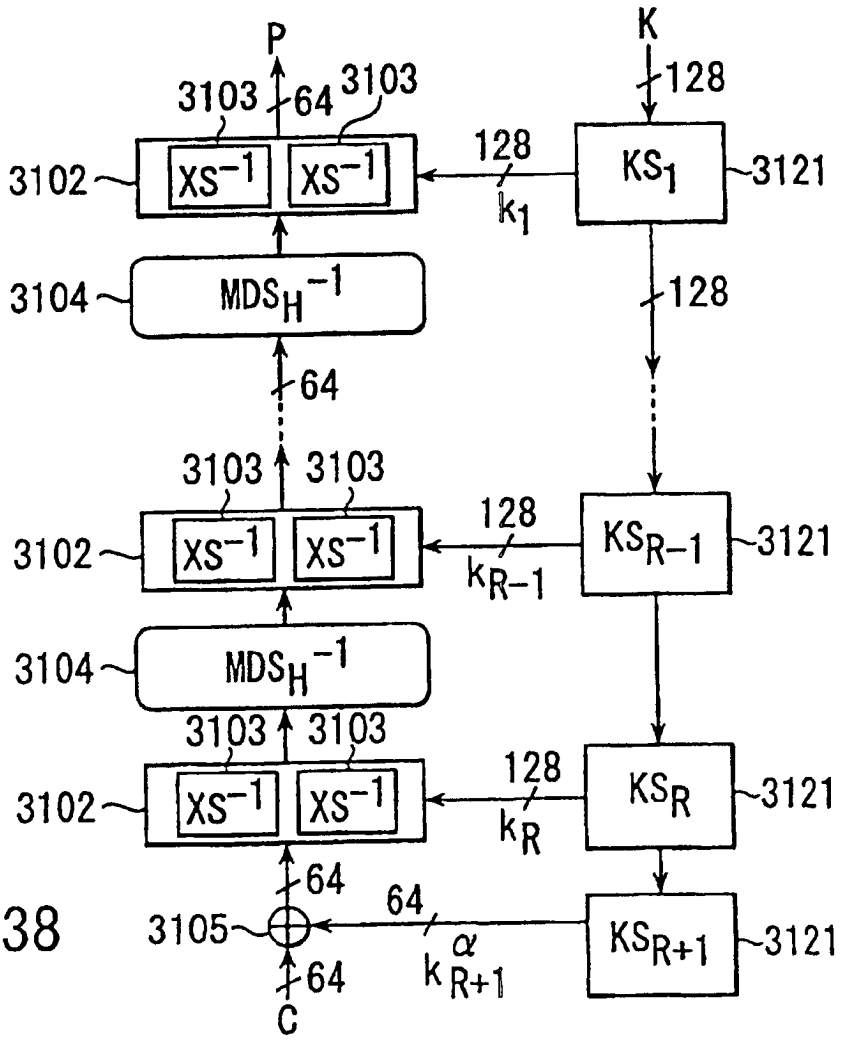
$H0 = (5A827999)_H = \lfloor \sqrt{2}/4 \times 2^{32} \rfloor$

$H1 = (6ED9EBA1)_H = \lfloor \sqrt{3}/4 \times 2^{32} \rfloor$

$H2 = (8F1BBCDC)_H = \lfloor \sqrt{5}/4 \times 2^{32} \rfloor$

$H3 = (CA62C1D6)_H = \lfloor \sqrt{10}/4 \times 2^{32} \rfloor$

FIG. 38



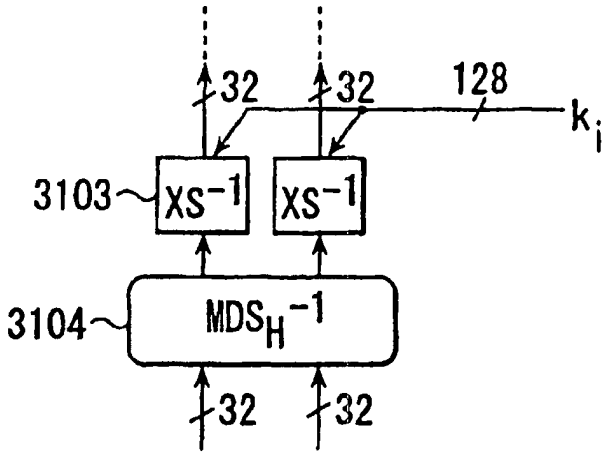

32
32
128
k_i
3103
XS^{-1}
XS^{-1}
3104
MDS_H^{-1}
32
32

FIG. 39

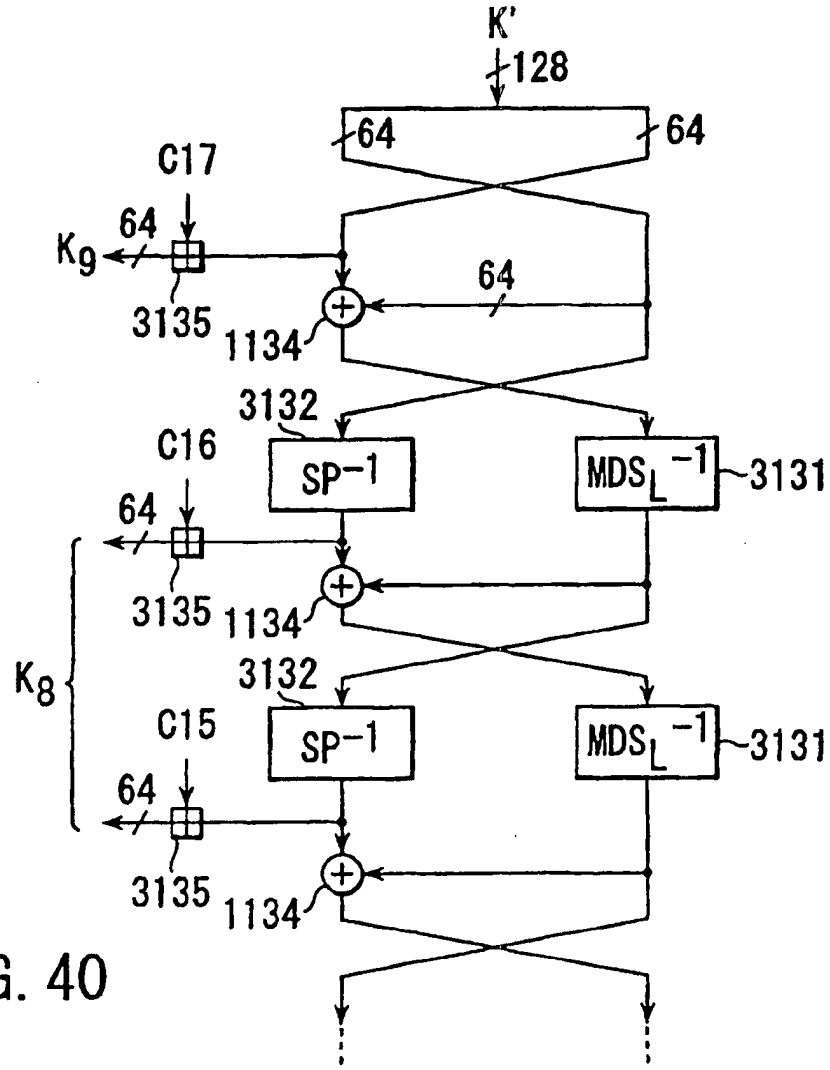

K'
128
64
64
C17
64
K_9
64
3135
1134
3132
C16
SP^{-1}
MDS_L^{-1}
3131
64
3135
1134
K_8
3132
C15
SP^{-1}
MDS_L^{-1}
3131
64
3135
1134

FIG. 40

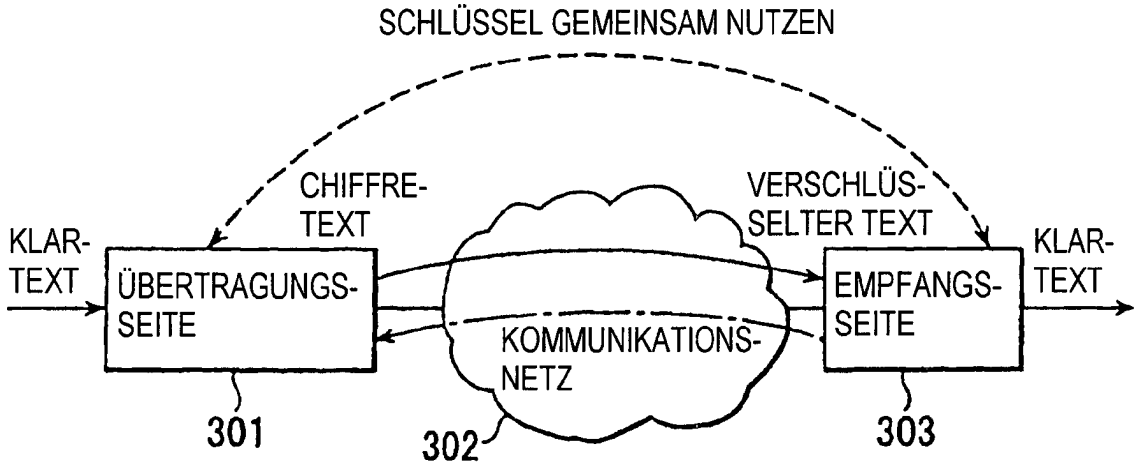


FIG. 41

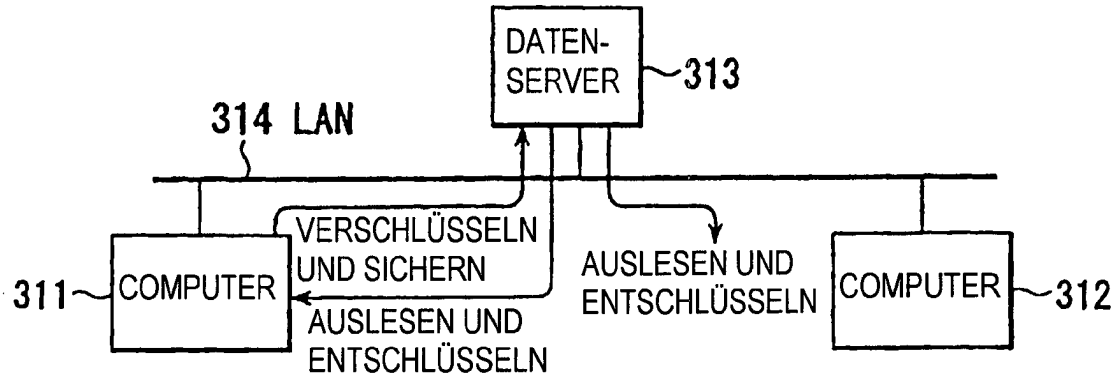


FIG. 42

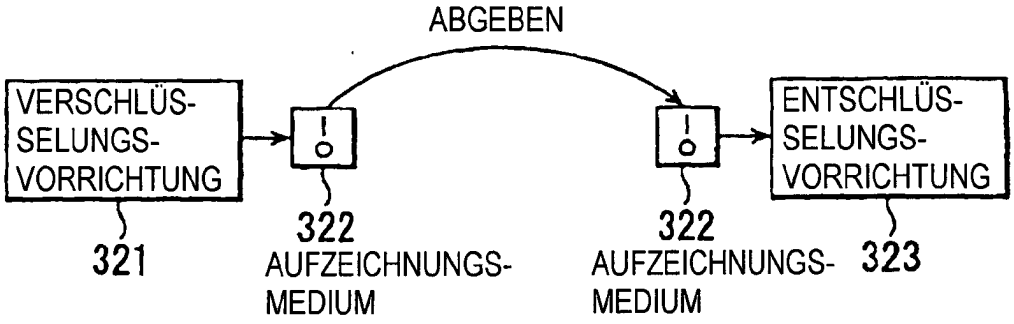


FIG. 43