(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年3月10日(10.03.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/049655 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/06* (2006.01)

(21) 国際出願番号： PCT/JP2020/033183

(22) 国際出願日： 2020年9月2日(02.09.2020)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電気株式会社(**NEC CORPORATION**) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP). 公立大学法人兵庫県立大学(**UNIVERSITY OF HYOGO**) [JP/JP]; 〒6512197 兵庫県神戸市西区学園西町８－２－１ Hyogo (JP).

(72) 発明者: 峯松 一彦(**MINEMATSU Kazuhiko**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 五十部 孝典(**ISOBE Takanori**); 〒6512197 兵庫県神戸市西区学園西町８－２－１ 公立大学法人兵庫県立大学内 Hyogo (JP). 阪本 光星(**SAKAMOTO Kosei**); 〒6512197 兵庫県神戸市西区学園西町８－２－１ 公立大学法人兵庫県立大学内 Hyogo (JP).

(74) 代理人: 家入 健(**IEIRI Takeshi**); 〒2210835 神奈川県横浜市神奈川区鶴屋町三丁目３３番８ アサヒビルヂング５階 響国際特許事務所 Kanagawa (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ,

(54) **Title:** INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND NON-TRANSITORY COMPUTER-READABLE MEDIUM IN WHICH PROGRAM IS STORED

(54) 発明の名称: 情報処理装置、情報処理方法、及びプログラムが格納された非一時的なコンピュータ可読媒体

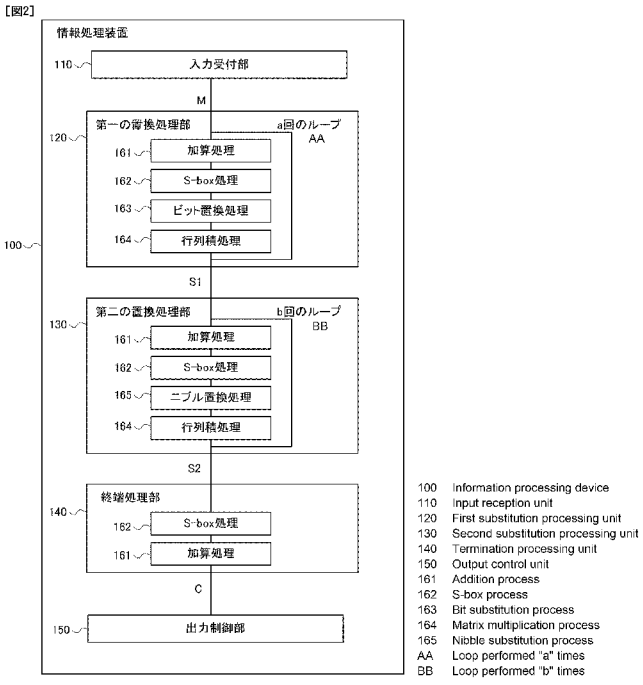

Fig. 2

(57) **Abstract:** The present invention achieves encryption with low latency and a large input width. An information processing device (10) has: an input reception unit (11); a first substitution processing unit (12) that repeats a first substitution process "a" times to output first intermediate text; a second substitution processing unit (13) that repeats a second

WO 2022/049655 A1

[続葉有]

BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

一　国際調査報告（条約第21条(3)）

substitution process "b" times to output second intermediate text; and a termination processing unit (14) that performs a termination process in which the second intermediate text is used as input and ciphertext is output. In the first substitution process, an addition process, an S-box process, a bit substitution process, and a matrix multiplication process are performed in order. In the second substitution process, the addition process, the S-box process, a nibble substitution process, and the matrix multiplication process are performed in order. The termination process is a substitution process in which the S-box process and the addition process are performed in order.

(57) 要約：低遅延かつ大きい入力幅を持つ暗号化処理を実現する。情報処理装置（１０）は、入力受付部（１１）と、第一の置換処理をa回繰り返して、第一の中間文を出力する第一の置換処理部（１２）と、第二の置換処理をb回繰り返して、第二の中間文を出力する第二の置換処理部（１３）と、前記第二の中間文を入力として暗号文を出力する終端処理を行う終端処理部（１４）とを有する。前記第一の置換処理は、加算処理と、S-box処理と、ビット置換処理と、行列積処理とを順番に行う置換処理である。前記第二の置換処理は、前記加算処理と、前記S-box処理と、ニブル置換処理と、前記行列積処理とを順番に行う置換処理である。前記終端処理は、前記S-box処理と、前記加算処理とを順番に行う置換処理である。

明　細　書

発明の名称 ：

情報処理装置、情報処理方法、及びプログラムが格納された非一時的なコンピュータ可読媒体

技術分野

[0001] 本開示は、情報処理装置、情報処理方法、及びプログラムが格納された非一時的なコンピュータ可読媒体に関する。

背景技術

[0002] 一般の共通鍵暗号化方式について、遅延（レイテンシ、latency）という評価指標がある。これは処理を開始してから最初の出力結果が出るまでの時間を指すものであり、小さいほうが望ましい。例えばコンピュータ内部のメモリバスの保護や、リアルタイム処理が求められる通信、例えばオンラインゲームや無人機の制御など、では特に遅延が問題となるため、低遅延であることが望ましい。これらのアプリケーションの中でも、メモリの保護は特に普及が進んでおり、例えば近年のCPU（Central Processing Unit）では、非特許文献１に代表されるように、メモリの暗号化と改ざん検知機能を有するものがある。

[0003] 暗号化の場合、遅延は、複数ブロックからなる平文を入力した際に、最初の暗号文ブロックが出るまでの時間ないし処理量のことを指す。暗号化処理の時間当たりの処理量（スループット）は、ハードウェアでの処理の並列化などにより向上可能である。一方、遅延を下げるためには並列化は有効でない。遅延を下げるためには、暗号化処理内部のループ処理を展開した、フルアンロールド（full unrolled）実装が一般的である。このとき、遅延はフルアンロールド実装の回路のクリティカルパスの長さによって決まる。

[0004] 低遅延を目的とした暗号化処理の例として、非特許文献２のブロック暗号PRINCEがある。PRINCEは、64-bitブロックの軽量ブロック暗号の一種である。しかし、通常の軽量ブロック暗号が比較的シンプルなラウンド関数を数多く

繰り返すのに対して、PRINCEは、比較的処理の多いラウンド関数を用い、かつ暗号化処理の中盤で鍵なしの置換層の処理を入れるなどの工夫がされている。これにより、少ないラウンド数で安全性を確保し、結果的に遅延を少なくすることに成功している。

[0005] また、非特許文献３の軽量ブロック暗号Midoriは、64-bitブロックと128-bitブロックのバージョンを持つブロック暗号であり、もともとは省エネルギーを目的とした設計であるが、ラウンド数が比較的少なく低遅延暗号としてもすぐれている。

[0006] また、非特許文献４のQARMAは軽量な可撚ブロック暗号（tweakable block cipher）であり、メモリの暗号化を目的として開発された低遅延暗号である。

[0007] その他の関連する技術として、非特許文献５は、ブロック暗号の暗号利用モードであるGCMモードについて開示してる。また、非特許文献６は、高い安全性を持つ疑似ランダム関数（Pseudorandom Function, PRF）について開示している。

先行技術文献

非特許文献

[0008] 非特許文献1：S. Gueron, “A Memory Encryption Engine Suitable for General Purpose Processors”, Cryptology ePrint Archive: Report 2016/204, February 2016.

非特許文献2：J. Borghoff et al., “PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications”(Full version), Cryptology ePrint Archive: Report 2012/529, September 2012.

非特許文献3：S. Banik et al., “Midori: A Block Cipher for Low Energy”(Extended Version), Cryptology ePrint Archive: Report 2015/1142, November 2015.

非特許文献4：R. Avanzi, “The QARMA Block Cipher Family: Almost MDS Matrices Over Rings With Zero Divisors, Nearly Symmetric Even-Mansour

Constructions With Non-Involutory Central Rounds, and Search Heuristics for Low-Latency S-Boxes”, Cryptology ePrint Archive: Report 2016/444, May 2016.

非特許文献5：M. Dworkin, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”,NIST Special Publication 800-38D, November 2007.

非特許文献6：W. Dai et al., “Information-theoretic Indistinguishability via the Chi-squared Method”, Cryptology ePrint Archive: Report 2017/537, June 2017.

発明の概要

発明が解決しようとする課題

[0009] PRINCEは64-bitブロック暗号であるため入力幅が64 bitであり、一般的な暗号利用モードの下では、いわゆるバースデー攻撃を避けるために、おおよそO(2^32)ブロックを処理した段階で鍵を更新する必要がある。これはメモリの保護などといった、高速に大量のデータを処理するアプリケーションでは実用上の困難をもたらす。

[0010] Midoriの128-bit入力幅のバージョン（Midori-128）や、QARMAの128-bit入力幅のバージョンは低遅延であるものの、ブロックサイズが大きいこともあり、低遅延についてPRINCEには及ばない。

[0011] そこで、128ビットの入力幅を持ち、低遅延性に優れた暗号プリミティブが重要となる。128-bitブロック暗号であれば上述のバースデー攻撃に必要なデータ量はO(2^64) ブロックになり大幅に安全性があがる。

[0012] 本開示はこのような問題点を解決するためになされたものであり、低遅延かつ大きい入力幅を持つ暗号化処理を実現できる情報処理装置、情報処理方法、及びプログラムを提供することを目的とする。

課題を解決するための手段

[0013] 本開示の第１の態様にかかる情報処理装置は、

128ビットを1ブロックの単位として平文の入力を受付ける入力受付手段と

、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力する第一の置換処理手段と、

前記第一の中間文を最初の入力として、第二の置換処理をb回（ただし、bは所定の整数）繰り返して、第二の中間文を出力する第二の置換処理手段と、

前記第二の中間文を入力として暗号文を出力する終端処理を行う終端処理手段と

を有し、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である。

[0014] 本開示の第２の態様にかかる情報処理方法では、

128ビットを1ブロックの単位として平文の入力を受付け、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力し、

前記第一の中間文を最初の入力として、第二の置換処理をb回（ただし、bは所定の整数）繰り返して、第二の中間文を出力し、

前記第二の中間文を入力として暗号文を出力する終端処理を行い、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である。

[0015] 本開示の第３の態様にかかるプログラムは、

128ビットを1ブロックの単位として平文の入力を受付ける入力受付ステップと、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力する第一の置換処理ステップと、

前記第一の中間文を最初の入力として、第二の置換処理をb回（ただし、bは所定の整数）繰り返して、第二の中間文を出力する第二の置換処理ステップと、

前記第二の中間文を入力として暗号文を出力する終端処理を行う終端処理ステップと

をコンピュータに実行させ、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である。

発明の効果

[0016] 本開示によれば、低遅延かつ大きい入力幅を持つ暗号化処理を実現できる情報処理装置、情報処理方法、及びプログラムを提供できる。

図面の簡単な説明

[0017] [図1]実施形態の概要にかかる情報処理装置の構成の一例を示すブロック図である。

[図2]実施の形態１にかかる情報処理装置の構成の一例を示す模式図である。

[図3]第一の条件について説明する模式図である。

[図4]第二の条件について説明する模式図である。

[図5]実施の形態１にかかる情報処理装置の動作の流れの一例を示すフローチャートである。

[図6]第一の置換処理のラウンド関数（ただし、入力に対するラウンド鍵とラウンド定数の加算処理を除く）を示す模式図である。

[図7]第二の置換処理のラウンド関数（ただし、入力に対するラウンド鍵とラウンド定数の加算処理を除く）を示す模式図である。

[図8]比較例のラウンド関数（ただし、入力に対するラウンド鍵とラウンド定数の加算処理を除く）を示す模式図である。

[図9]実施の形態２にかかる情報処理装置の構成の一例を示す模式図である。

[図10]実施の形態２にかかる情報処理装置の動作の流れの一例を示すフローチャートである。

[図11]コンピュータの構成の一例を示すブロック図である。

発明を実施するための形態

[0018] ＜実施の形態の概要＞

実施形態の詳細を説明する前に、まず、実施形態の概要について説明する。図１は、実施形態の概要にかかる情報処理装置１０の構成の一例を示すブロック図である。図１に示すように、情報処理装置１０は、入力受付部１１と、第一の置換処理部１２と、第二の置換処理部１３と、終端処理部１４とを有する。

[0019] 入力受付部１１は、128ビットを1ブロックの単位として平文の入力を受付

ける。第一の置換処理部１２は、入力受付部１１が受付けた1ブロック分の平文を最初の入力として、第一の置換処理をa回繰り返して、第一の中間文を出力する。なお、aは任意の所定の整数である。第二の置換処理部１３は、第一の置換処理部１２が出力した第一の中間文を最初の入力として、第二の置換処理をb回繰り返して、第二の中間文を出力する。なお、bは任意の所定の整数である。終端処理部１４は、第二の置換処理部１３が出力した第二の中間文を入力として暗号文を出力する終端処理を行う。

[0020] ここで、上述した第一の置換処理は、加算処理、S-box処理、ビット置換処理、及び行列積処理を順番に行う置換処理である。これらの処理は、具体的には次のような処理である。加算処理は、入力に対して、ラウンド鍵とラウンド定数とを加算する処理である。S-box処理は、入力に対して、ニブルごとに、4ビットS-boxを適用する処理である。なお、4ビットS-boxは、4ビットの入力を4ビットの出力に変換する非線形関数である。ビット置換処理は、入力をビット単位で並び替える処理である。行列積処理は、入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する処理である。

[0021] また、上述した第二の置換処理は、加算処理、S-box処理、ニブル置換処理、及び行列積処理を順番に行う置換処理である。第二の置換処理で行われる加算処理、S-box処理、及び行列積処理は、第一の置換処理で行われる処理と同様の処理である。第二の置換処理では、第一の置換処理と異なり、ビット置換処理の代わりに、ニブル置換処理が行われる。ニブル置換処理は、入力をニブル単位で並び替える処理である。

[0022] また、上述した終端処理は、S-box処理及び加算処理を順番に行う置換処理である。終端処理で行われるS-box処理及び加算処理は、第一の置換処理で行われる処理と同様の処理である。

[0023] このような構成を備える情報処理装置１０によれば、低遅延かつ大きい入力幅を持つ暗号化処理を実現できる。

[0024] 次に、実施形態の詳細について説明する。

＜実施の形態１＞

図２は、実施の形態１にかかる情報処理装置１００の構成の一例を示す模式図である。情報処理装置１００は、図２に示すように、入力受付部１１０と、第一の置換処理部１２０と、第二の置換処理部１３０と、終端処理部１４０と、出力制御部１５０とを有する。ここで、入力受付部１１０、第一の置換処理部１２０、第二の置換処理部１３０、終端処理部１４０は、図１に示した入力受付部１１、第一の置換処理部１２、第二の置換処理部１３、終端処理部１４と対応している。本実施の形態にかかる情報処理装置１００は、ブロック暗号化装置とも称される。また、本実施の形態では、1ブロックの長さは128ビットである。したがって、情報処理装置１００は、入力幅が128ビットのブロック暗号化装置である。

[0025] 入力受付部１１０は、情報処理装置１００に対する入力を受付けるハードウェア回路である。入力受付部１１０は、例えばキーボードなどの入力装置を介して入力されたデータを受付ける。本実施の形態において、入力受付部１１０は、平文Mの入力を受付ける。入力受付部１１０は、128ビットを１ブロックの単位として、平文の入力を受付ける。

[0026] 第一の置換処理部１２０は、ブロックを処理単位として、処理を行う。第一の置換処理部１２０は、入力受付部１１０が受付けた１ブロック分の平文を最初の入力として、第一の置換処理をa回繰り返して、第一の中間文S1を出力するハードウェア回路である。繰り返される第一の置換処理における２回目以降では、前回の第一の置換処理の処理結果が第一の置換処理の入力に用いられる。ここで、繰り返し回数を規定するaの値は予め定められている。

[0027] 第一の置換処理部１２０は、第一の置換処理として、具体的には、まず、加算処理１６１を行ない、次に、S-box処理１６２を行ない、次に、ビット置換処理１６３を行ない、最後に行列積処理１６４を行う。

[0028] 加算処理１６１は、入力に対して、ラウンド鍵とラウンド定数とを加算する処理である。ここで、加算処理１６１の入力は128ビットのデータである。以下、加算処理１６１について具体的に説明する。加算処理１６１では、128

ビットの入力Xと、秘密鍵Kと、ループのカウンタiとを用いて、次のような処理が行われる。まず、加算処理１６１では、秘密鍵Kとカウンタiにより決まる値であるラウンド鍵K_iが導出されるとともに、カウンタiより決まる値であるラウンド定数c_iが導出される。秘密鍵Kとカウンタiとから算出されるラウンド鍵K_iと、カウンタiから算出されるラウンド定数c_iの長さは高々128ビットであり、128ビットに満たないビット数である場合には、ゼロパディングにより128ビットとなるよう調整される。秘密鍵Kは、入力受付部１１０により受付けられたものであってもよいし、情報処理装置１００が予め記憶している所定の鍵データが用いられてもよい。秘密鍵Kは、例えば128ビット又は256ビットの任意のビット列であるが、秘密鍵Kのビット数はこれらに限られない。カウンタiは、ループ回数、すなわち処理の繰り返し回数を表すカウンタであり、第一の置換処理として加算処理１６１が行われる場合、例えば、ｉ = 1,2,...,aである。なお、後述する通り、加算処理１６１は、第二の置換処理として行われる場合もあり、この場合、例えば、ｉ = 1,2,...,bである。

[0029] 本実施の形態では、例えば、ラウンド鍵K_iとラウンド定数c_iは次のように導出される。本実施の形態では、秘密鍵Kは128ビットであり、ラウンド鍵K_iは、カウンタiが偶数なら秘密鍵Kの前半64ビットであり、奇数なら後半64ビットである。また、ラウンド定数c_iは円周率（3.14159...）のビット表現から、カウンタiの値に応じて抜き出された4ビットである。ただし、これらは、例に過ぎず、ラウンド鍵K_iとラウンド定数c_iは他の導出方法により導出されてもよい。

[0030] そして、加算処理１６１では、次に、入力Xへラウンド定数c_iとラウンド鍵K_iを加算する処理が行われる。なお、この加算は、例えば、排他的論理和であるが、算術加算などであってもよい。加算処理１６１では、この加算結果として128ビットのデータ列が出力される。

[0031] S-box処理１６２は、入力に対して、4ビットの非線形関数である4ビットS-boxを並列に適用する処理である。本実施の形態では入力は128ビットなので

、S-box処理１６２では32個の4ビットS-boxが並列に適用される。このように、S-box処理１６２では、入力に対して、ニブルごとに、4ビットS-boxが適用される。そして、S-box処理１６２は、128ビットのデータ列を出力する。S-boxは4ビットの範囲で全拡散（full diffusion）することが求められる。すなわち、S-boxの4ビットの入力をxとし、S-boxの4ビットの出力をyとすると、yの各ビットがxの全ビットに依存していることが求められる。換言すると、x[i]をxのi番目ビットとし、y[i]をyのi番目ビットとすると、y[i]がx[1],x[2],x[3],x[4]の全てを用いた論理式で表現されていることが求められる。そのようなS-boxとして、任意のS-boxを用いることが可能であるが、一例として、以下の表のような置換として定義される、MidoriSb_1を用いてもよい。なお、以下の表では、入力xと出力$Sb_1(x)$が16進表記されている。

[0032] [表1]

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$Sb_1(x)$	1	0	5	3	e	2	f	7	d	a	9	b	c	8	4	6

[0033] ビット置換処理１６３は、入力をビット単位で並び替える処理であり、入力された128ビット（すなわち、32ニブル）のデータ列を並び替えて、128ビットのデータ列を出力する。加算処理１６１、S-box処理１６２、ビット置換処理１６３、及び行列積処理１６４からなるループを１ラウンドとすると、ビット置換が拡散性能に関して最適であれば、2.5ラウンドで128ビットのデータが全拡散することが示せる。ここで、2.5ラウンドとは、3ラウンド目の途中まで行うこと、より詳細には、3ラウンド目の加算処理１６１及びS-box処理１６２までを行うことを指す。このため、第一の置換処理の繰り返し回数aの値は3であってもよい。2.5ラウンドでの全拡散を保証するためには、以下の2条件を満たせばよい。ここで、入力32ニブルをX(1), ... ,X(32)とし、出力32ニブルをY(1), ... ,Y(32)とし、さらに出力を4ニブルごとにまとめてW(1) = [Y(1), Y(2), Y(3), Y(4)], W(2) = [Y(5), Y(6), Y(7), Y(8)], ... ,W(8) = [Y(29), Y(30), Y(31), Y(32)]とする。また、入力X(i)の4ビットB

(i,1),B(i,2),B(i,3),B(i,4)がマップされたニブルをそれぞれY(a), Y(b), Y(c), Y(d)とし（ただし、a, b, c, dは、いずれも1以上32以下の整数）とする。そして、これら（すなわち、Y(a), Y(b), Y(c), Y(d)）の4ニブルが所属するW(j)からY(a), Y(b), Y(c), Y(d)を除いた12ニブルをY(j[1]), Y(j[2]), ..., Y(j[12])とする（ただし、j[1], j[2], j[12]は、いずれも1以上32以下の整数）。

[0034] 2.5ラウンドでの全拡散を保証するためのビット置換処理１６３は、以下の第一の条件及び第二の条件を満たす並び替えを行う処理である。

[0035] （第一の条件）

すべてのi=1,...,32について、入力X(i)の4ビットB(i,1),B(i,2),B(i,3),B(i,4)がすべて異なるW(j)（j = 1,...,8)へマップされる。

[0036] （第二の条件）

入力X(1),...,X(32)におけるニブルの位置がY(1),...,Y(32)におけるY(j[1]), Y(j[2]), ..., Y(j[12])の位置と対応している、入力の12ニブルX(j[1]), X(j[2]), ..., X(j[12])のマップによって、W(1),...,W(8)のすべてにおいて2ニブル以上がカバーされる。

すなわち、入力の12ニブルX(j[1]), X(j[2]), ..., X(j[12])をマップしたときに、W(1),...,W(8)のそれぞれにおいて、W(j)（j = 1,...,8)を構成する４つのY(k), Y(k+1), Y(k+2), Y(k+3)（k=1,5,9,13,17, 21, 25, 29)のうちの２つ以上がマップ先として選ばれる。

[0037] 図３は、第一の条件について説明する模式図である。図３では、S-box処理１６２において並列に適用される32個のS-box１７０と、後述する行列積処理１６４において並列に適用される8個の行列１７１が図示されており、ビット置換処理１６３がS-box１７０の出力から行列１７１の入力へ延びる矢印として表されている。ここで、各S-box１７０による合計32ニブルの出力は、ビット置換処理１６３における32ニブルの入力X(1), ... ,X(32)に対応している。また、各行列１７１における合計32ニブルの入力は、ビット置換処理１６３における32ニブルの出力Y(1), ... ,Y(32)に対応している。

[0038] 上述した通り、第一の条件を満たす並び替えでは、各S-box１７０の出力4ビットが異なる行列１７１の入力へマップされる。図３では、図の見やすさを損なわないよう、左端のS-box１７０から出力された4ビット（X(1)）のマップ先だけを示している。この例では、X(1)の1つ目のビットB(1,1)がW(1)を構成するY(1)にマップされ、X(1)の2つ目のビットB(1,2)がW(2)を構成するY(6)にマップされ、X(1)の3つ目のビットB(1,3)がW(4)を構成するY(15)にマップされ、X(1)の4つ目のビットB(1,4)がW(5)を構成するY(18)にマップされている。

[0039] 図４は、第二の条件について説明する模式図である。図４でも、図３と同様、S-box処理１６２において並列に適用される32個のS-box１７０と、後述する行列積処理１６４において並列に適用される8個の行列１７１が図示されている。そして、ビット置換処理１６３がS-box１７０の出力から行列１７１の入力へ延びる矢印として表されている。

[0040] 上述した通り、第二の条件を満たす並び替えでは、入力の12ニブルX(j[1]), X(j[2]), ..., X(j[12])のマップによって、W(1),...,W(8)のすべてにおいて2ニブル以上がカバーされる。ここで、12ニブルX(j[1]), X(j[2]), ..., X(j[12])は、入力X(1),...,X(32)におけるニブルの位置がY(1),...,Y(32)におけるY(j[1]), Y(j[2]), ..., Y(j[12])の位置と対応しているX(i)である。そして、上述の通り、Y(j[1]), Y(j[2]), ..., Y(j[12])は、入力X(i)の4ビットB(i,1),B(i,2),B(i,3),B(i,4)がマップされたニブルY(a), Y(b), Y(c), Y(d)が所属するW(j)からY(a), Y(b), Y(c), Y(d)を除いた12ニブルである。

[0041] 図４では、入力X(i)の4ビットB(i,1),B(i,2),B(i,3),B(i,4)として、入力X(1)の4ビットB(1,1),B(1,2),B(1,3),B(1,4)を考えた場合の例を示している。図４に示した例では、Y(a), Y(b), Y(c), Y(d)は、破線の矢印で示されるマップ先のニブルであり、具体的には、Y(1)、Y(6)、Y(15)、Y(18)である。そして、Y(j[1]), Y(j[2]), ..., Y(j[12])は、ニブルY(1), Y(6), Y(15), Y(18)が所属するW(j)からY(1), Y(6), Y(15), Y(18)を除いた12ニブルである。

Y(1)はW(1)に所属し、Y(6)はW(2)に所属し、Y(15)はW(4)に所属し、Y(18)はW(5)に所属しているため、Y(j[1]), Y(j[2]), ..., Y(j[12])は、具体的には、Y(2), Y(3), Y(4), Y(5), Y(7), Y(8), Y(13), Y(14), Y(16), Y(17), Y(19), Y(20)である。よって、12ニブルX(j[1]), X(j[2]), ..., X(j[12])は、具体的には、X(2), X(3), X(4), X(5), X(7), X(8), X(13), X(14), X(16), X(17), X(19), X(20)である。

[0042] したがって、第二の条件を満たすためには、図４に示すように、入力の12ニブルX(2), X(3), X(4), X(5), X(7), X(8), X(13), X(14), X(16), X(17), X(19), X(20)のマップによって、W(1),...,W(8)のすべてにおいて2ニブル以上がカバーされる必要がある。なお、図４では、X(2), X(3), X(4), X(5), X(7), X(8), X(13), X(14), X(16), X(17), X(19), X(20)のマップは、太線の矢印で示されているが、図の見やすさを損なわないよう、一部のビットのマップだけを示している。すなわち、例えば、X(2)（左から2番目のS-boxの出力）のマップとして、具体的にはX(2)の4ビットのそれぞれのマップが存在するが、図４ではそのうちの１つのマップのみを図示している。図４に示した例では、X(i)(i=2,3,4,5,7,8,13,14,16,17,19,20)のマップにより、W(1)を構成する４つのY(1), Y(2), Y(3), Y(4)のうちの少なくともY(1)及びY(3)がマップ先として選択されている。すなわち、W(1)を構成する４つのY(1), Y(2), Y(3), Y(4)のうち２つ以上がマップ先として選ばれている。同様に、図４に示すように、W(2), W(3), W(4), W(5), W(6), W(7), W(8)についても、W(j)を構成する４つのY(k), Y(k+1), Y(k+2), Y(k+3)のうち２つ以上がマップ先として選ばれている。

[0043] 行列積処理１６４は、入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用し、合計128ビットのデータ列を出力する処理である。第一の置換処理として行われる行列積処理１６４では、上述したビット置換処理１６３の出力Y(1), ... ,Y(32)を8つに分けたワードW(1),...,W(8)のそれぞれに対して、Almost MDS行列変換が行われる。なお、後述する通り、行列積処理１６４は、第二の置換処理として行われる

場合もあり、この場合、ニブル置換処理１６５の出力を4ニブルごとに8つに分けたワードのそれぞれに対して、Almost MDS行列変換が行われる。

[0044] Almost MDS行列への入力がA = (a_1,a_2,a_3,a_4)（ただし各a_iはニブル）のとき、Almost MDS行列を適用した結果(b_1,b_2,b_3,b_4)（ただし各b_iはニブル）は、Almost MDS行列とAの転置ベクトルとの積で得られる。ここで、Almost MDS行列について説明する。任意の異なる2入力 A = (a_1,a_2,a_3,a_4) と A' = (a'_1,a'_2,a'_3,a'_4)について、その差分 A xor A' （xorは要素ごとの排他的論理和を行うことを示す）をとり、そのハミング重みをd_Aとする。またそれぞれに行列Mbを適用した出力を B = (b_1,b_2,b_3,b_4)と B' = (b'_1,b'_2,b'_3,b'_4) とし、同様に、差分 B xor B' のハミング重みをd_Bとする。このとき、d_A + d_Bが常に4以上となる場合、行列MbをAlmost MDS行列と称す。

[0045] 例えば以下の行列がAlmost MDS行列である。

[0046] [数1]

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

[0047] この行列を用いた場合、入力 A = (a_1,a_2,a_3,a_4)に対応する出力B = (b_1,b_2,b_3,b_4)は、以下のように表される。

b_1 = a_2+a_3+a_4

b_2 = a_1+a_3+a_4

b_3 = a_1+a_2+a_4

b_4 = a_1+a_2+a_3

[0048] 以上、第一の置換処理で行われる各処理について説明した。上述の通り、

第一の置換処理部１２０は、第一の置換処理をa回繰り返して、第一の中間文S1を出力する。１回目の処理では、入力受付部１１０が受付けた１ブロック分の平文に対して加算処理１６１が行われる。そして、加算処理１６１の結果に対してS-box処理１６２が行われ、S-box処理１６２の結果に対してビット置換処理１６３が行われ、ビット置換処理１６３の結果に対して行列積処理１６４が行われる。これにより１回目の第一の置換処理が終了する。そして、１回目の第一の置換処理における行列積処理１６４の結果が、２回目の第一の置換処理における加算処理１６１の入力に用いられる。そして、２回目の第一の置換処理における加算処理１６１の結果に対して、２回目の第一の置換処理におけるS-box処理１６２が行われる。以降、同様に、処理が行われ、第一の置換処理がa回繰り返される。第一の置換処理部１２０は、第一の置換処理をａ回繰り返すと、最終的な処理結果を第一の中間文S1として第二の置換処理部１３０に出力する。

[0049] 次に、第二の置換処理部１３０について説明する。第二の置換処理部１３０は、第一の置換処理部１２０が出力した128ビットのデータ列である第一の中間文S1を最初の入力として、第二の置換処理をb回繰り返して、第二の中間文S2を出力するハードウェア回路である。繰り返される第二の置換処理における２回目以降では、前回の第二の置換処理の処理結果が第二の置換処理の入力に用いられる。ここで、繰り返し回数を規定するbの値は予め定められている。

[0050] 第二の置換処理部１３０は、第二の置換処理として、具体的には、まず、加算処理１６１を行ない、次に、S-box処理１６２を行ない、次に、ニブル置換処理１６５を行ない、最後に行列積処理１６４を行う。第二の置換処理として行われる加算処理１６１、S-box処理１６２、及び行列積処理１６４は、第一の置換処理として行われるこれらの処理と同様なので、説明を省略する。

[0051] ニブル置換処理１６５は、入力をニブル単位で並び替える処理であり、入力された32ニブル（すなわち、128ビット）のデータ列を並び替えて、32ニブ

ル（すなわち、128ビット）のデータ列を出力する。本実施の形態では、ニブル置換処理１６５として、Active S-box数が、少ないラウンド数で所定値に達するような処理を行う。所定値とは、具体的にはS-boxの最大差分確率の指数とActive S-box数との積が-128になる値である。4ビットS-boxの場合、S-boxの最大差分確率が2^-2であるため、この所定値は、具体的には64である。

[0052] ニブル置換処理１６５は、例えば5ラウンドで、64というActive S-box数を保証する。このため、第二の置換処理の繰り返し回数bの値は5であってもよい。例えば、次のようなニブル置換処理１６５は、5ラウンドで、64というActive S-box数を保証する。なお、入力のビット列に対して4ビット毎に順番に0から31までのインデックスを付与して、当該インデックスの並びの変更により、ニブル置換処理１６５の並び替えを表現するものとする。例えば、ニブル置換処理１６５は、入力時のインデックスの並びが(0, 1, ..., 31)であり、出力時のインデックスの並びが(10, 27, 5, 1, 30, 23, 16, 13, 21, 31, 6, 14, 0, 25, 11, 18, 15, 28, 19, 24, 7, 8, 22, 3, 4, 29, 9, 2, 26, 20, 12, 17)である並び替え処理である。また、別の例では、ニブル置換処理１６５は、入力時のインデックスの並びが(0, 1, ..., 31)であり、出力時のインデックスの並びが(26, 13, 7, 11, 29, 0, 17, 21, 23, 5, 18, 25, 12, 10, 28, 2, 14, 19, 24, 22, 1, 8, 4, 31, 15, 6, 27, 9, 16, 30, 20, 3)である並び替え処理である。

[0053] このように、本実施の形態では、ニブル置換処理１６５は、Active S-box数が所定値以上になるために必要とされる当該ニブル置換処理１６５のラウンド数（処理の繰り返し数）が所定条件を満たす処理である。

[0054] 以上、第二の置換処理で行われる処理について説明した。上述の通り、第二の置換処理部１３０は、第二の置換処理をb回繰り返して、第二の中間文S2を出力する。１回目の処理では、第一の置換処理部１２０が出力したデータ列に対して加算処理１６１が行われる。そして、加算処理１６１の結果に対してS-box処理１６２が行われ、S-box処理１６２の結果に対してニブル置換処理１６５が行われ、ニブル置換処理１６５の結果に対して行列積処理１６

４が行われる。これにより１回目の第二の置換処理が終了する。そして、１回目の第二の置換処理における行列積処理１６４の結果が、２回目の第二の置換処理における加算処理１６１の入力に用いられる。そして、２回目の第二の置換処理における加算処理１６１の結果に対して、２回目の第二の置換処理におけるS-box処理１６２が行われる。以降、同様に、処理が行われ、第二の置換処理がb回繰り返される。第二の置換処理部１３０は、第二の置換処理をb回繰り返すと、最終的な処理結果を第二の中間文S2として終端処理部１４０に出力する。

[0055] 次に、終端処理部１４０について説明する。終端処理部１４０は、第二の置換処理部１３０が出力した128ビットのデータ列である第二の中間文S2を入力として、暗号文Cを出力する終端処理を行うハードウェア回路である。

[0056] 終端処理部１４０は、終端処理として、具体的には、まず、S-box処理１６２を行ない、次に、加算処理１６１を行う。すなわち、終端処理部１４０は、第二の置換処理部１３０が出力した第二の中間文S2に対し、まず、S-box処理１６２を行ない、次に、S-box処理１６２の結果に対して、加算処理１６１を行う。そして、終端処理部１４０は、加算処理１６１の結果を暗号文Cとして出力する。

[0057] 出力制御部１５０は、終端処理部１４０の処理結果をディスプレイなどの出力装置に出力するための制御を行うハードウェア回路である。すなわち、出力制御部１５０は、暗号文Cを出力装置に出力するための制御を行う。

[0058] 図５は、情報処理装置１００の動作の流れの一例を示すフローチャートである。以下、図５を参照しつつ、情報処理装置１００の動作の流れについて説明する。

[0059] ステップＳ１０において、入力受付部１１０は、平文Mの入力を受付ける。

[0060] 次に、ステップＳ１１において、第一の置換処理部１２０は、加算処理１６１を行う。

次に、ステップＳ１２において、第一の置換処理部１２０は、S-box処理１６２を行う。

次に、ステップＳ１３において、第一の置換処理部１２０は、ビット置換処理１６３を行う。

次に、ステップＳ１４において、第一の置換処理部１２０は、行列積処理１６４を行う。

[0061] 次に、ステップＳ１５において、第一の置換処理部１２０は、ステップＳ１１からステップＳ１４までの一連の処理をa回繰り返したか否かを判定する。処理がa回繰り返されていない場合、第一の置換処理部１２０は、ステップＳ１１からステップＳ１４までの一連の処理を再度繰り返す。これに対して、処理がa回繰り返された場合、ステップＳ１６が行われる。ここで、例えば、aの値は3である。

[0062] ステップＳ１６において、第二の置換処理部１３０は、加算処理１６１を行う。

次に、ステップＳ１７において、第二の置換処理部１３０は、S-box処理１６２を行う。

次に、ステップＳ１８において、第二の置換処理部１３０は、ニブル置換処理１６５を行う。

次に、ステップＳ１９において、第二の置換処理部１３０は、行列積処理１６４を行う。

[0063] 次に、ステップＳ２０において、第二の置換処理部１３０は、ステップＳ１６からステップＳ１９までの一連の処理をb回繰り返したか否かを判定する。処理がb回繰り返されていない場合、第二の置換処理部１３０は、ステップＳ１６からステップＳ１９までの一連の処理を再度繰り返す。これに対して、処理がb回繰り返された場合、ステップＳ２１が行われる。ここで、例えば、bの値は5である。

[0064] ステップＳ２１において、終端処理部１４０は、S-box処理１６２を行う。

次に、ステップＳ２２において、終端処理部１４０は、加算処理１６１を行う。

[0065] 最後に、ステップＳ２３において、出力制御部１５０は、ステップＳ２２

で得られた128ビットのビット列を暗号文Cとしてディスプレイ等に出力する。なお、上述した例では、繰り返し回数についてa=3, b=5としたが、繰り返し回数はこれらの値に限られない。例えば、より安全性を高めるために、aの値は3より大きくてもよく、bの値は5より大きくてもよい。例えば、a=4, b=7としてもよい。

[0066] 次に、本実施の形態の効果について説明する。本実施の形態によれば、128-bitの入力幅を持つ、低遅延な暗号化処理を実現できる。本実施の形態のラウンド関数はMidoriで導入されたAlmost MDS行列を用いる置換ネットワーク構造（Substitution-Permutation Network, SPN）をベースとしているが、Midoriとは異なり、複数の異なる線形層を用いている。具体的には前半のラウンド（第一の置換処理）でビット置換を用い（図６参照）、後半のラウンド（第二の置換処理）ではニブル置換を用いている（図７参照）。ここで、図６は、第一の置換処理のラウンド関数（ただし、入力に対するラウンド鍵とラウンド定数の加算処理を除く）を示す模式図である。また、図７は、第二の置換処理のラウンド関数（ただし、入力に対するラウンド鍵とラウンド定数の加算処理を除く）を示す模式図である。Midori-128でもビット置換とニブル置換とを用いるが、Midoriでは単一のラウンドにおいて両者を利用する点が本実施の形態とは異なる。また、Midori-128のビット置換は、4ビットS-box二つを並べて、これらを実質的に8ビットS-boxとして機能させるために用いられており、Midori-128のビット置換は8ビット入出力のビット置換を並べることで実現されている（図８参照）。ここで、図８は、Midoriのラウンド関数（ただし、入力に対するラウンド鍵とラウンド定数の加算処理を除く）を示す模式図である。これに対し、本実施の形態のビット置換は128ビット全体を攪拌するためのものである。本実施の形態がビット置換を前半のラウンドで用いる理由は、暗号の安全性評価において重要な全拡散（full diffusion）、すなわち任意の入力データの変化が出力の全体へ波及すること、を少ないラウンド数で担保するためである。ビット置換はニブル置換と比べてデータをより細かく分割するために拡散性能を高めることが可能である。加算処

理１６１、S-box処理１６２、ビット置換処理１６３、及び行列積処理１６４からなる一連の処理を1ラウンドと換算した場合、上述した第一の条件及び第二の条件を満たすビット置換であれば、2.5ラウンドで全拡散が担保される。ここで、2.5ラウンドとは、3ラウンド目の途中まで行うこと、より詳細には、3ラウンド目の加算処理１６１及びS-box処理１６２までを行うことを指す。一方ビット置換でなくニブル置換のみを用いた場合は、全拡散を担保するためには少なくとも4ラウンドが必要となる。Midori-128の場合は上述のようにビット置換とニブル置換を組み合わせているが、ビット置換の変化の波及の幅が小さいため、全拡散には3ラウンドを要している。そして、Active S-boxといった評価条件を満たすために、Midori-128は、最終的に、全体で20ラウンドを必要とする。これに対し、本実施の形態では、例えば、a=4, b=7とした場合、終端処理を1ラウンドとしてカウントしても、合計12（=4+7+1）ラウンドで十分である。したがって、本実施の形態によれば、128-bitの入力幅を持ち、Midori-128と比べて低遅延な暗号化処理が提供される。

[0067] なお、本実施の形態がニブル置換を後半のラウンド（第二の置換処理）で用いる理由は、代表的な安全性評価指標であるActive S-box数における優位性を確保するためである。Active S-box数は重要な暗号解析手法である差分攻撃に対する安全性を反映する。ある暗号において、任意の異なる入力対に対してActive S-box数の最小値が所定値以上となることが示せれば、その暗号は差分攻撃に対して十分な耐性を持つといえる。一般にビット置換は粒度が細かいため、Active S-box数の最小値を精密に導出することが困難になる。結果として、Active S-box数の最小値が所定値以上となることを保証するために必要なラウンド数が大きくなる。したがって、前半のラウンドでビット置換を用い、全拡散したのちはニブル置換に切り替える本実施の形態の構成により、少ないラウンド数で安全性を担保することが可能となる。なお、低遅延暗号の実装は一般的にフルアンロール実装であるため、前半のラウンド（第一の置換処理）と後半のラウンド（第二の置換処理）で構成が変わることはハードウェア実装上問題とならない。

[0068] ＜実施の形態２＞

次に、実施の形態２について説明する。図９は、実施の形態２にかかる情報処理装置２００の構成の一例を示す模式図である。情報処理装置２００は、図９に示すように、入力受付部２１０と、第一のブロック暗号化部２２０と、第二のブロック暗号化部２３０と、加算部２４０と、出力制御部２５０とを有し、実施の形態１で述べた暗号化処理を用いて疑似乱数を生成する。本実施の形態にかかる情報処理装置２００は、疑似ランダム関数装置とも称される。

[0069] 入力受付部２１０は、入力受付部１１０と同様の処理を行うハードウェア回路である。すなわち、入力受付部２１０は、実施の形態１における平文Mに相当する入力を受付ける。入力受付部２１０は、例えばキーボードなどの入力装置を介して情報処理装置２００に入力されたデータを受付ける。

[0070] 第一のブロック暗号化部２２０及び第二のブロック暗号化部２３０は、いずれも実施の形態１で示した暗号化処理を行うハードウェア回路である。すなわち、第一のブロック暗号化部２２０及び第二のブロック暗号化部２３０は、上述した第一の置換処理部１２０、第二の置換処理部１３０、及び終端処理部１４０の処理を順に行い、入力受付部２１０が受付けた128ビットのデータ列を暗号化する。つまり、第一のブロック暗号化部２２０及び第二のブロック暗号化部２３０は、いずれも入力Mに対する暗号文を出力する。ここで、第一のブロック暗号化部２２０及び第二のブロック暗号化部２３０は、入力M（すなわち、同一の平文）に対し、異なる２つの暗号文を出力する。ここでは、第一のブロック暗号化部２２０が、第一の暗号文Xを出力し、第二のブロック暗号化部２３０が、第二の暗号文Yを出力するものとして説明する。なお、第一のブロック暗号化部２２０及び第二のブロック暗号化部２３０は、異なる秘密鍵（ラウンド鍵）を用いることにより、異なる暗号文XとYを出力してもよいし、異なるニブル置換を行うことにより、異なる暗号文XとYを出力してもよい。異なるニブル置換を行う場合、第一のブロック暗号化部２２０及び第二のブロック暗号化部２３０は、同じ秘密鍵（ラウンド鍵）を用い

てもよい。このように、第二の暗号文Yは、第一の暗号文Xの生成に用いられた鍵（ラウンド鍵）とは異なる鍵（ラウンド鍵）を用いることにより得られる暗号文であってもよい。また、第二の暗号文Yは、第一の暗号文Xの生成に用いられたニブル置換処理１６５での並び替えとは異なる並び替えが行われるニブル置換処理１６５を用いることにより得られる暗号文であってもよい。

[0071] ここで、ニブル置換処理１６５における異なる並び替えは、上述した２つの並び替えであってもよい。つまり、入力のビット列に対して4ビット毎に順番に0から31までのインデックスを付与して当該インデックスの並びの変更によりニブル置換処理１６５の並び替えを表現した場合、ニブル置換処理１６５における異なる並び替えは次のようなものであってもよい。第一の並び替えを行うニブル置換処理１６５は、入力時のインデックスの並びが(0, 1, ..., 31)であり、出力時のインデックスの並びが(10, 27, 5, 1, 30, 23, 16, 13, 21, 31, 6, 14, 0, 25, 11, 18, 15, 28, 19, 24, 7, 8, 22, 3, 4, 29, 9, 2, 26, 20, 12, 17)である並び替え処理である。そして、第二の並び替えを行うニブル置換処理１６５は、入力時のインデックスの並びが(0, 1, ..., 31)であり、出力時のインデックスの並びが(26, 13, 7, 11, 29, 0, 17, 21, 23, 5, 18, 25, 12, 10, 28, 2, 14, 19, 24, 22, 1, 8, 4, 31, 15, 6, 27, 9, 16, 30, 20, 3)である並び替え処理である。

このように、第一の暗号文Xは、ニブル置換処理１６５として第一の所定の並び替えを行うことにより得られる暗号文であり、第二の暗号文Yは、ニブル置換処理１６５として第二の所定の並び替えを行うことにより得られる暗号文であってもよい。

[0072] 第一のブロック暗号化部２２０及び第二のブロック暗号化部２３０は、第一の暗号文Xと第二の暗号文Yを加算部２４０に出力する。

加算部２４０は、第一の暗号文Xと第二の暗号文Yを入力として、第一の暗号文Xと第二の暗号文Yを加算して、疑似乱数として出力するハードウェア回路である。すなわち、加算部２４０は、第一の暗号文Xと第二の暗号文Yを加

算することにより疑似乱数Cを生成し、これを出力する。これにより、加算部２４０の処理結果として128ビットの疑似乱数Cが出力される。なお、この加算は、例えば、排他的論理和であるが、算術加算などであってもよい。

[0073] 出力制御部２５０は、加算部２４０の処理結果をディスプレイなどの出力装置に出力するための制御を行うハードウェア回路である。すなわち、出力制御部２５０は、疑似乱数Cを出力装置に出力するための制御を行う。

[0074] 図１０は、情報処理装置２００の動作の流れの一例を示すフローチャートである。以下、図１０を参照しつつ、情報処理装置２００の動作の流れについて説明する。

[0075] ステップＳ３０において、入力受付部２１０は、入力Mを受付ける。

次に、ステップＳ３１において、第一のブロック暗号化部２２０が第一の暗号文Xを生成し、第二のブロック暗号化部２３０が第二の暗号文Yを生成する。

次に、ステップＳ３２において、加算部２４０が第一の暗号文Xと第二の暗号文Yを加算し、疑似乱数Cを生成する。

最後に、ステップＳ３３において、出力制御部２５０は、ステップＳ２２で得られたビット列を疑似乱数Cとしてディスプレイ等に出力する。

[0076] 情報処理装置２００では、実施の形態１で説明した暗号化処理を二つ並列に並べ、両者の出力を加算することで、高い安全性を持つ疑似ランダム関数を構成している。上述した文献“Information-theoretic Indistinguishability via the Chi-squared Method”に示される疑似ランダム関数は独立な鍵を二つ要するものである。本実施の形態では、それぞれのブロック暗号の中で、異なるニブル置換を用いれば、鍵を複数用意しなくてもよい。特に、それぞれのブロック暗号の中で用いるニブル置換を、Active S-boxの観点で性能のよいものから２種類選択することで安全性を担保することができる。

[0077] 実施の形態１に示したような128-bitブロック暗号であればバースデー攻撃に必要なデータ量はO(2^64) ブロックになり大幅に安全性があがる。しかし、ネットワークなどの高速化・大容量化を考えた場合に、長期的なセキュリ

ティを求める際にはより大量のデータを用いた攻撃にも耐えられることが望ましい。この点において、情報処理装置２００により実現される128ビットの入力幅の疑似ランダム関数は、一般的な暗号化や、認証暗号のモード（例えばカウンターモードやGCMモードなど）で用いられた場合に、攻撃に必要なデータ量がO(2^128)ブロックとなる。このため、長期的にみても十分な安全性を有する暗号化が可能となる。

[0078] なお、上述の説明では、図２又は図９に示す要素についてハードウェアの構成として説明したが、これに限定されるものではない。これらの要素の一部又は全ては、コンピュータのプロセッサがコンピュータプログラムを実行させることにより実現することも可能である。

[0079] 図１１は、図２又は図９に示す要素を実現するコンピュータ３００の構成の一例を示すブロック図である。図１１に示すように、コンピュータ３００は、入出力インタフェース３０１、メモリ３０２、及び、プロセッサ３０３を含む。

[0080] 入出力インタフェース３０１は、他の任意の装置と通信するために使用される。

メモリ３０２は、例えば、揮発性メモリ及び不揮発性メモリの組み合わせによって構成される。メモリ３０２は、プロセッサ３０３により実行される、１以上の命令を含むソフトウェア（コンピュータプログラム）などを格納するために使用される。

[0081] プロセッサ３０３は、メモリ３０２からソフトウェア（コンピュータプログラム）を読み出して実行することで、上述した図２又は図９に示す各構成要素の処理を行う。

[0082] プロセッサ３０３は、例えば、マイクロプロセッサ、ＭＰＵ（Ｍｉｃｒｏ Ｐｒｏｃｅｓｓｏｒ Ｕｎｉｔ）、又はＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）などであってもよい。プロセッサ３０３は、複数のプロセッサを含んでもよい。

[0083] なお、上述したプログラムは、様々なタイプの非一時的なコンピュータ可

読媒体（ｎｏｎ－ｔｒａｎｓｉｔｏｒｙ　ｃｏｍｐｕｔｅｒ　ｒｅａｄａｂｌｅ　ｍｅｄｉｕｍ）を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体（ｔａｎｇｉｂｌｅ　ｓｔｏｒａｇｅ　ｍｅｄｉｕｍ）を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えばフレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば光磁気ディスク）、ＣＤ－ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、半導体メモリ（例えば、マスクＲＯＭ、ＰＲＯＭ（Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）、ＥＰＲＯＭ（Ｅｒａｓａｂｌｅ　ＰＲＯＭ）、フラッシュＲＯＭ、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ））を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体（ｔｒａｎｓｉｔｏｒｙ　ｃｏｍｐｕｔｅｒ　ｒｅａｄａｂｌｅ　ｍｅｄｉｕｍ）によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

[0084] 以上、実施の形態を参照して本願発明を説明したが、本願発明は上記によって限定されるものではない。本願発明の構成や詳細には、発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

[0085] 上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

（付記１）

128ビットを1ブロックの単位として平文の入力を受付ける入力受付手段と、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力する第一の置換処理手段と、

前記第一の中間文を最初の入力として、第二の置換処理をb回（ただし、b

は所定の整数）繰り返して、第二の中間文を出力する第二の置換処理手段と、

前記第二の中間文を入力として暗号文を出力する終端処理を行う終端処理手段と

を有し、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である

情報処理装置。

（付記２）

前記ビット置換処理は、

入力32ニブルをX(1),...,X(32)とし、出力32ニブルをY(1),...,Y(32)とし、出力を4ニブルごとにまとめてW(1)=[Y(1),Y(2),Y(3),Y(4)], W(2)=[Y(5),Y

(6),Y(7),Y(8)], ... ,W(8)=[Y(29),Y(30),Y(31),Y(32)]とし、入力X(i)の4ビットB(i,1),B(i,2),B(i,3),B(i,4)がマップされたニブルをそれぞれY(a), Y(b), Y(c), Y(d)とし（ただし、a, b, c, dは、いずれも1以上32以下の整数）、これらの4ニブルが所属するW(j)からY(a), Y(b), Y(c), Y(d)を除いた12ニブルをY(j[1]), Y(j[2]), ..., Y(j[12])とすると（ただし、j[1], j[2], j[12]は、いずれも1以上32以下の整数）、以下の第一の条件及び第二の条件を満たす並び替えを行う処理である

付記１に記載の情報処理装置。

（第一の条件）

すべてのi=1,...,32について、入力X(i)の4ビットB(i,1),B(i,2),B(i,3),B(i,4)がすべて異なるW(j)（j = 1,...,8)へマップされる。

（第二の条件）

入力X(1),...,X(32)におけるニブルの位置がY(1),...,Y(32)におけるY(j[1]), Y(j[2]), ..., Y(j[12])の位置と対応している、入力の12ニブルX(j[1]), X(j[2]), ..., X(j[12])のマップによって、W(1),...,W(8)のすべてにおいて2ニブル以上がカバーされる。

（付記３）

前記ニブル置換処理は、

Active S-box数が所定値以上になるために必要とされる当該ニブル置換処理のラウンド数が所定条件を満たす処理である

付記１又は２に記載の情報処理装置。

（付記４）

同一の平文に対する異なる前記暗号文である第一の暗号文と第二の暗号文を入力として、前記第一の暗号文と前記第二の暗号文を加算して、疑似乱数として出力する加算手段を

さらに有する

付記１乃至３のいずれか１項に記載の情報処理装置。

（付記５）

前記第一の暗号文は、前記ニブル置換処理として第一の所定の並び替えを行うことにより得られる前記暗号文であり、前記第二の暗号文は、前記ニブル置換処理として第二の所定の並び替えを行うことにより得られる前記暗号文であり、

入力のビット列に対して4ビット毎に順番に0から31までのインデックスを付与して、当該インデックスの並びの変更により前記第一の所定の並び替えを表現した場合、前記第一の所定の並び替えによる前記ニブル置換処理は、入力時のインデックスの並びが(0,1,...,31)であり、出力時のインデックスの並びが(10,27,5,1,30,23,16,13,21,31,6,14,0,25,11,18,15,28,19,24,7,8,22,3,4,29,9,2,26,20,12,17)である処理であり、

入力のビット列に対して4ビット毎に順番に0から31までのインデックスを付与して、当該インデックスの並びの変更により前記第二の所定の並び替えを表現した場合、前記第二の所定の並び替えによる前記ニブル置換処理は、入力時のインデックスの並びが(0,1,...,31)であり、出力時のインデックスの並びが(26,13,7,11,29,0,17,21,23,5,18,25,12,10,28,2,14,19,24,22,1,8,4,31,15,6,27,9,16,30,20,3)である処理である

付記４に記載の情報処理装置。

（付記６）

128ビットを1ブロックの単位として平文の入力を受付け、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力し、

前記第一の中間文を最初の入力として、第二の置換処理をb回（ただし、bは所定の整数）繰り返して、第二の中間文を出力し、

前記第二の中間文を入力として暗号文を出力する終端処理を行い、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である

情報処理方法。

（付記７）

128ビットを1ブロックの単位として平文の入力を受付ける入力受付ステップと、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力する第一の置換処理ステップと、

前記第一の中間文を最初の入力として、第二の置換処理をb回（ただし、bは所定の整数）繰り返して、第二の中間文を出力する第二の置換処理ステップと、

前記第二の中間文を入力として暗号文を出力する終端処理を行う終端処理ステップと

をコンピュータに実行させ、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である

プログラムが格納された非一時的なコンピュータ可読媒体。

符号の説明

[0086] １０　情報処理装置

１１　入力受付部

１２　第一の置換処理部

１３　第二の置換処理部

１４　終端処理部

１００　情報処理装置

１１０　入力受付部

１２０　第一の置換処理部

１３０　第二の置換処理部

１４０　終端処理部

１５０　出力制御部

１６１　加算処理

１６２　S-box処理

１６３　ビット置換処理

１６４　行列積処理

１６５　ニブル置換処理

１７０　S-box

１７１　行列

２００　情報処理装置

２１０　入力受付部

２２０　第一のブロック暗号化部

２３０　第二のブロック暗号化部

２４０　加算部

２５０　出力制御部

３００　コンピュータ

３０１　入出力インタフェース

３０２　メモリ

３０３　プロセッサ

請求の範囲

[請求項1] 128ビットを1ブロックの単位として平文の入力を受付ける入力受付手段と、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力する第一の置換処理手段と、

前記第一の中間文を最初の入力として、第二の置換処理をb回（ただし、bは所定の整数）繰り返して、第二の中間文を出力する第二の置換処理手段と、

前記第二の中間文を入力として暗号文を出力する終端処理を行う終端処理手段と

を有し、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である

情報処理装置。

[請求項2] 前記ビット置換処理は、

入力32ニブルをX(1),...,X(32)とし、出力32ニブルをY(1),...,Y(32)とし、出力を4ニブルごとにまとめてW(1)=[Y(1),Y(2),Y(3),Y(4)], W(2)=[Y(5),Y(6),Y(7),Y(8)], ... ,W(8)=[Y(29),Y(30),Y(31),Y(32)]とし、入力X(i)の4ビットB(i,1),B(i,2),B(i,3),B(i,4)がマップされたニブルをそれぞれY(a), Y(b), Y(c), Y(d)とし（ただし、a, b, c, dは、いずれも1以上32以下の整数）、これらの4ニブルが所属するW(j)からY(a), Y(b), Y(c), Y(d)を除いた12ニブルをY(j[1]), Y(j[2]), ..., Y(j[12])とすると（ただし、j[1], j[2], j[12]は、いずれも1以上32以下の整数）、以下の第一の条件及び第二の条件を満たす並び替えを行う処理である

請求項１に記載の情報処理装置。

（第一の条件）

すべてのi=1,...,32について、入力X(i)の4ビットB(i,1),B(i,2),B(i,3),B(i,4)がすべて異なるW(j) (j = 1,...,8)へマップされる。

（第二の条件）

入力X(1),...,X(32)におけるニブルの位置がY(1),...,Y(32)におけるY(j[1]), Y(j[2]), ..., Y(j[12])の位置と対応している、入力の12ニブルX(j[1]), X(j[2]), ..., X(j[12])のマップによって、W(1),...,W(8)のすべてにおいて2ニブル以上がカバーされる。

[請求項3] 前記ニブル置換処理は、

Active S-box数が所定値以上になるために必要とされる当該ニブル置換処理のラウンド数が所定条件を満たす処理である

請求項１又は２に記載の情報処理装置。

[請求項4] 同一の平文に対する異なる前記暗号文である第一の暗号文と第二の暗号文を入力として、前記第一の暗号文と前記第二の暗号文を加算して、疑似乱数として出力する加算手段を

さらに有する

請求項１乃至３のいずれか１項に記載の情報処理装置。

[請求項5] 前記第一の暗号文は、前記ニブル置換処理として第一の所定の並び替えを行うことにより得られる前記暗号文であり、前記第二の暗号文は、前記ニブル置換処理として第二の所定の並び替えを行うことにより得られる前記暗号文であり、

入力のビット列に対して4ビット毎に順番に0から31までのインデックスを付与して、当該インデックスの並びの変更により前記第一の所定の並び替えを表現した場合、前記第一の所定の並び替えによる前記ニブル置換処理は、入力時のインデックスの並びが(0,1,...,31)であり、出力時のインデックスの並びが(10,27,5,1,30,23,16,13,21,31,6,14,0,25,11,18,15,28,19,24,7,8,22,3,4,29,9,2,26,20,12,17)である処理であり、

入力のビット列に対して4ビット毎に順番に0から31までのインデックスを付与して、当該インデックスの並びの変更により前記第二の所定の並び替えを表現した場合、前記第二の所定の並び替えによる前記ニブル置換処理は、入力時のインデックスの並びが(0,1,...,31)であり、出力時のインデックスの並びが(26,13,7,11,29,0,17,21,23,5,18,25,12,10,28,2,14,19,24,22,1,8,4,31,15,6,27,9,16,30,20,3)である処理である

請求項４に記載の情報処理装置。

[請求項6] 128ビットを1ブロックの単位として平文の入力を受付け、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力し、

前記第一の中間文を最初の入力として、第二の置換処理をb回（た

だし、bは所定の整数）繰り返して、第二の中間文を出力し、

前記第二の中間文を入力として暗号文を出力する終端処理を行い、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である

情報処理方法。

[請求項7] 128ビットを1ブロックの単位として平文の入力を受付ける入力受付ステップと、

1ブロック分の前記平文を最初の入力として、第一の置換処理をa回（ただし、aは所定の整数）繰り返して、第一の中間文を出力する第一の置換処理ステップと、

前記第一の中間文を最初の入力として、第二の置換処理をb回（た

だし、bは所定の整数）繰り返して、第二の中間文を出力する第二の置換処理ステップと、

前記第二の中間文を入力として暗号文を出力する終端処理を行う終端処理ステップと

をコンピュータに実行させ、

前記第一の置換処理は、

入力に対して、ラウンド鍵とラウンド定数とを加算する加算処理と、

入力に対して、ニブルごとに、4ビットの入力を4ビットの出力に変換する非線形関数である4ビットS-boxを適用するS-box処理と、

入力をビット単位で並び替えるビット置換処理と、

入力を4ニブルごとに8つのワードに分けて、各ワードに対して、4行4列のAlmost MDS行列変換を適用する行列積処理と

を順番に行う置換処理であり、

前記第二の置換処理は、

前記加算処理と、

前記S-box処理と、

入力をニブル単位で並び替えるニブル置換処理と、

前記行列積処理と

を順番に行う置換処理であり、

前記終端処理は、

前記S-box処理と、

前記加算処理と

を順番に行う置換処理である

プログラムが格納された非一時的なコンピュータ可読媒体。

[図1]

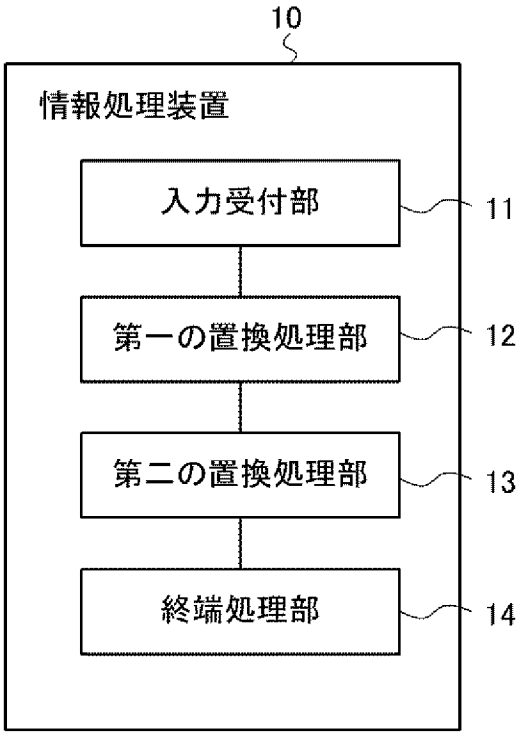

Fig. 1

[図2]

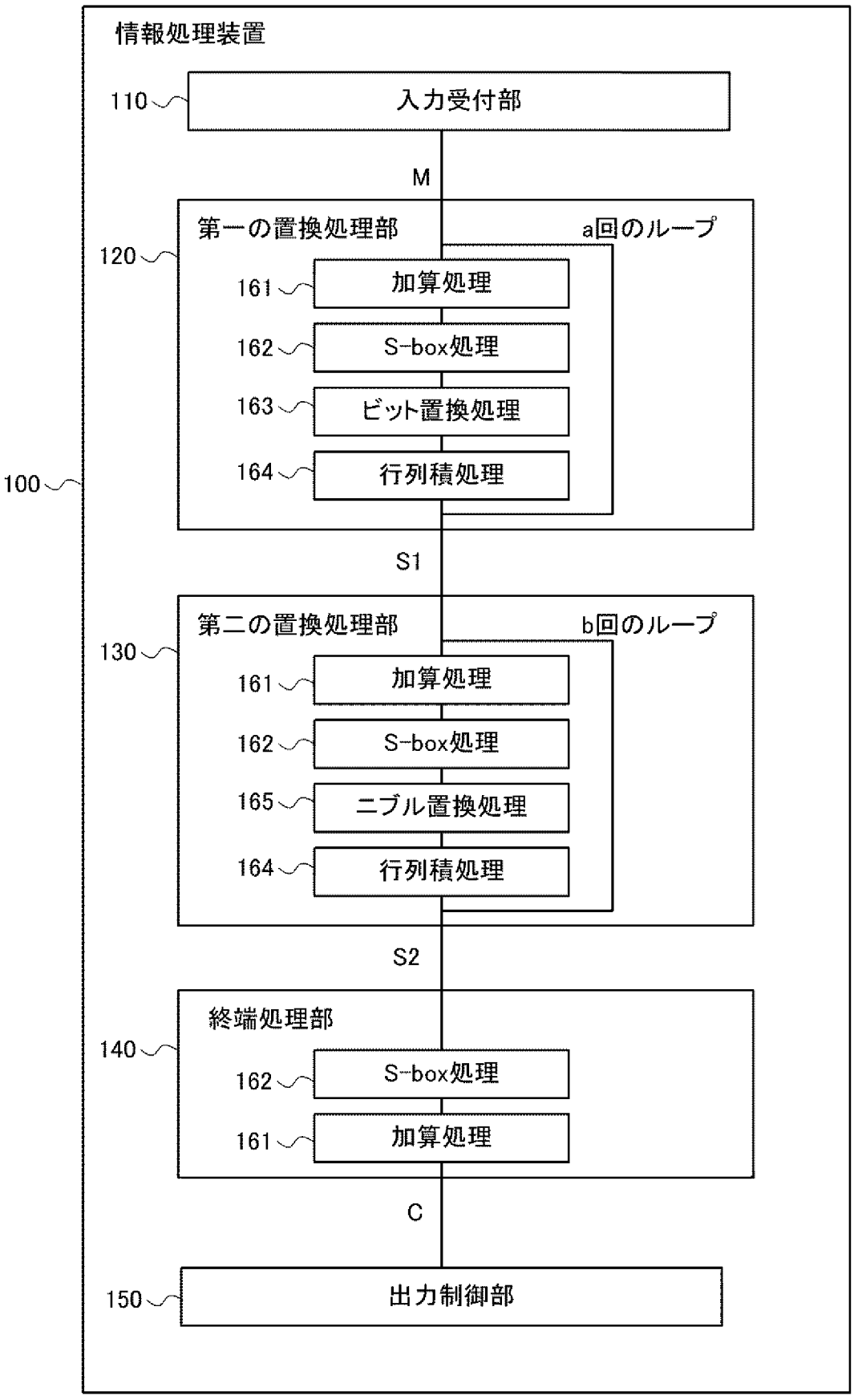
情報処理装置
110
入力受付部
M
第一の置換処理部
a回のループ
120
161
加算処理
162
S-box処理
163
ビット置換処理
164
行列積処理
100
S1
第二の置換処理部
b回のループ
130
161
加算処理
162
S-box処理
165
ニブル置換処理
164
行列積処理
S2
終端処理部
140
162
S-box処理
161
加算処理
C
150
出力制御部

Fig. 2

[図3]

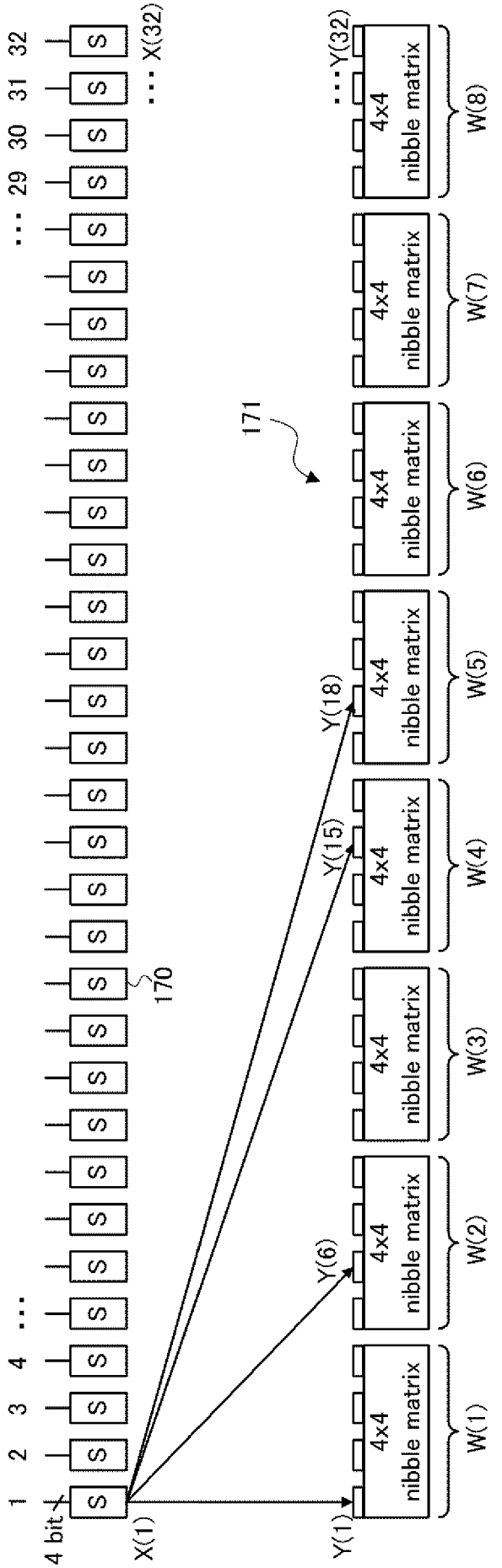
1 2 3 4 ... 29 30 31 32
4 bit
X(1)
X(32)
170
171
Y(1)
Y(6)
Y(15)
Y(18)
Y(32)
4x4 nibble matrix
W(1)
W(2)
W(3)
W(4)
W(5)
W(6)
W(7)
W(8)

Fig. 3

[図4]

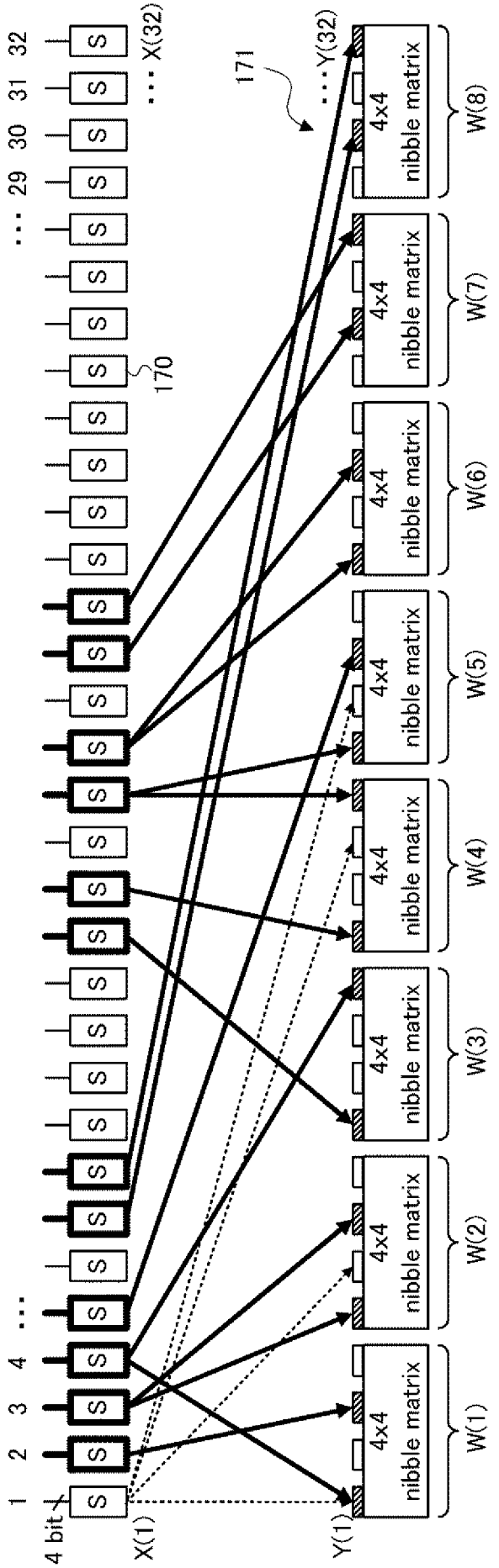
1 2 3 4 ... 29 30 31 32
4 bit
X(1)
X(32)
170
171
Y(1)
Y(32)
4x4 nibble matrix
W(1)
W(2)
W(3)
W(4)
W(5)
W(6)
W(7)
W(8)

Fig. 4

[図5]

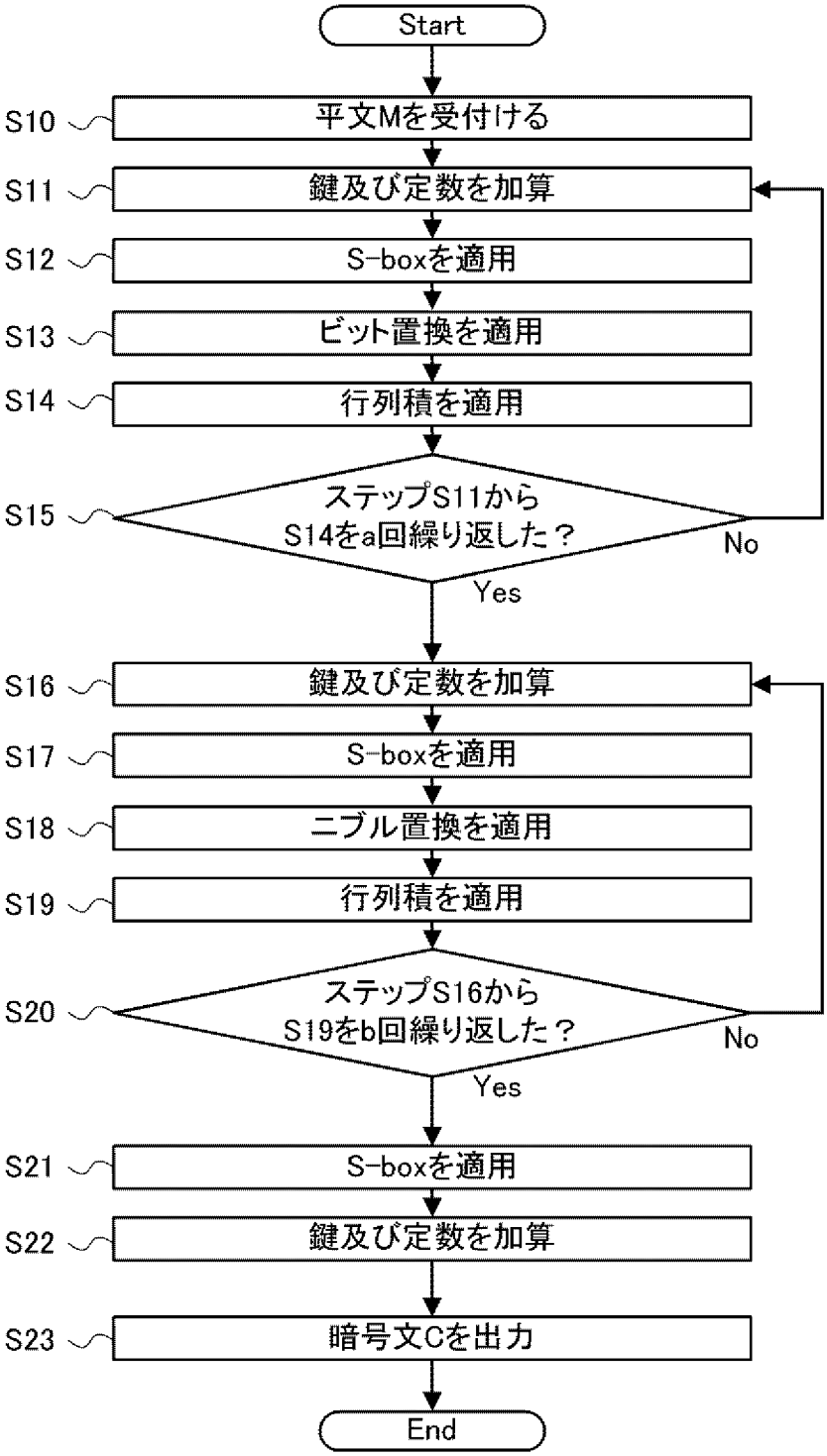
Start
S10
平文Mを受付ける
S11
鍵及び定数を加算
S12
S-boxを適用
S13
ビット置換を適用
S14
行列積を適用
S15
ステップS11から
S14をa回繰り返した？
No
Yes
S16
鍵及び定数を加算
S17
S-boxを適用
S18
ニブル置換を適用
S19
行列積を適用
S20
ステップS16から
S19をb回繰り返した？
No
Yes
S21
S-boxを適用
S22
鍵及び定数を加算
S23
暗号文Cを出力
End

Fig. 5

[図6]

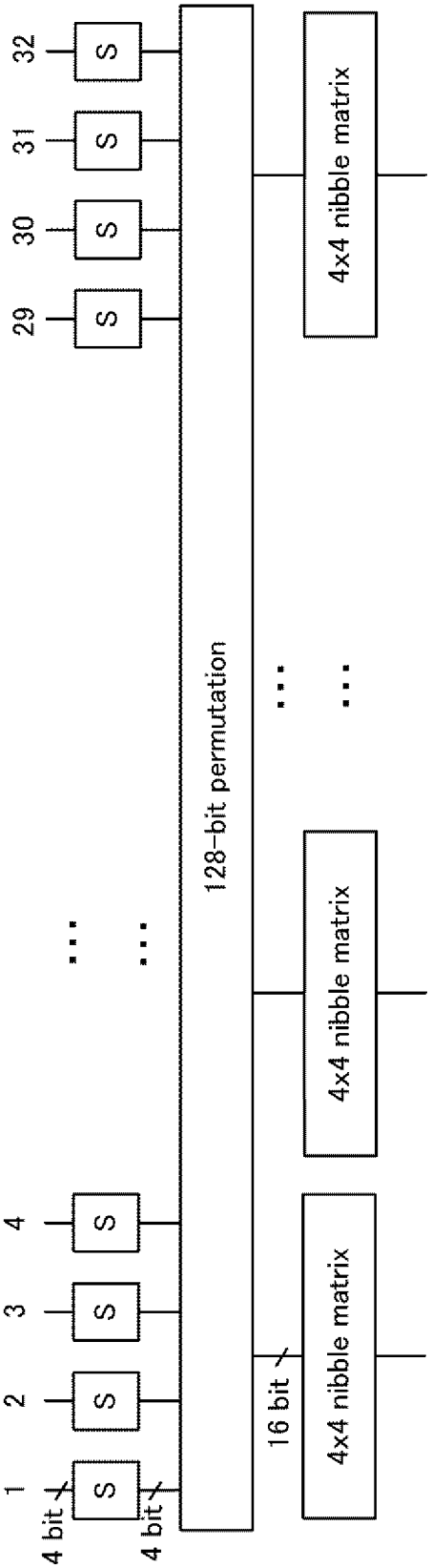
1
2
3
4
29
30
31
32
S
4 bit
4 bit
16 bit
128-bit permutation
4x4 nibble matrix
4x4 nibble matrix
4x4 nibble matrix

Fig. 6

[図7]

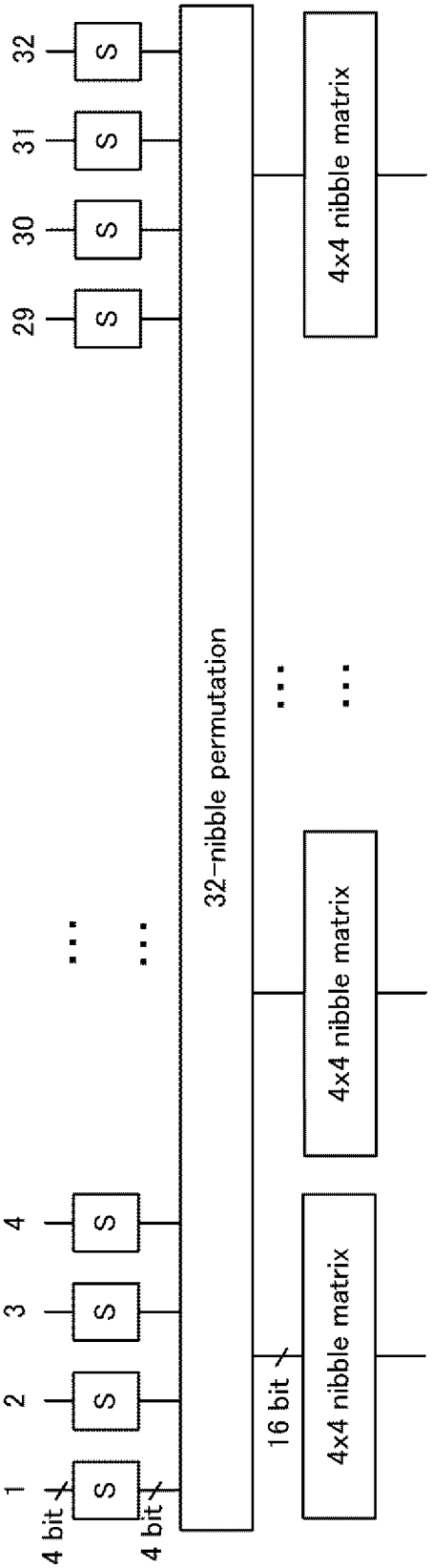
1
2
3
4
29
30
31
32
S
4 bit
4 bit
16 bit
32-nibble permutation
4x4 nibble matrix
4x4 nibble matrix
4x4 nibble matrix

Fig. 7

[図8]

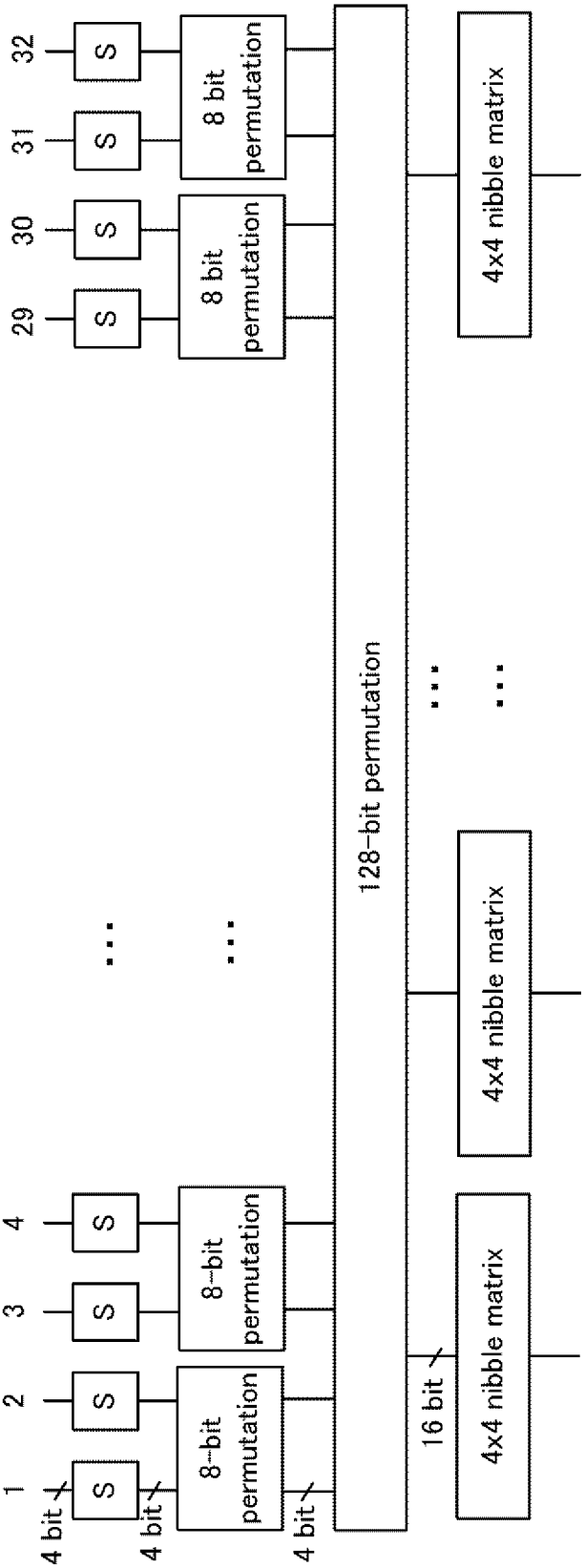
1
2
3
4
29
30
31
32
S
8-bit permutation
8 bit permutation
128-bit permutation
4x4 nibble matrix
4 bit
16 bit

Fig. 8

[図9]

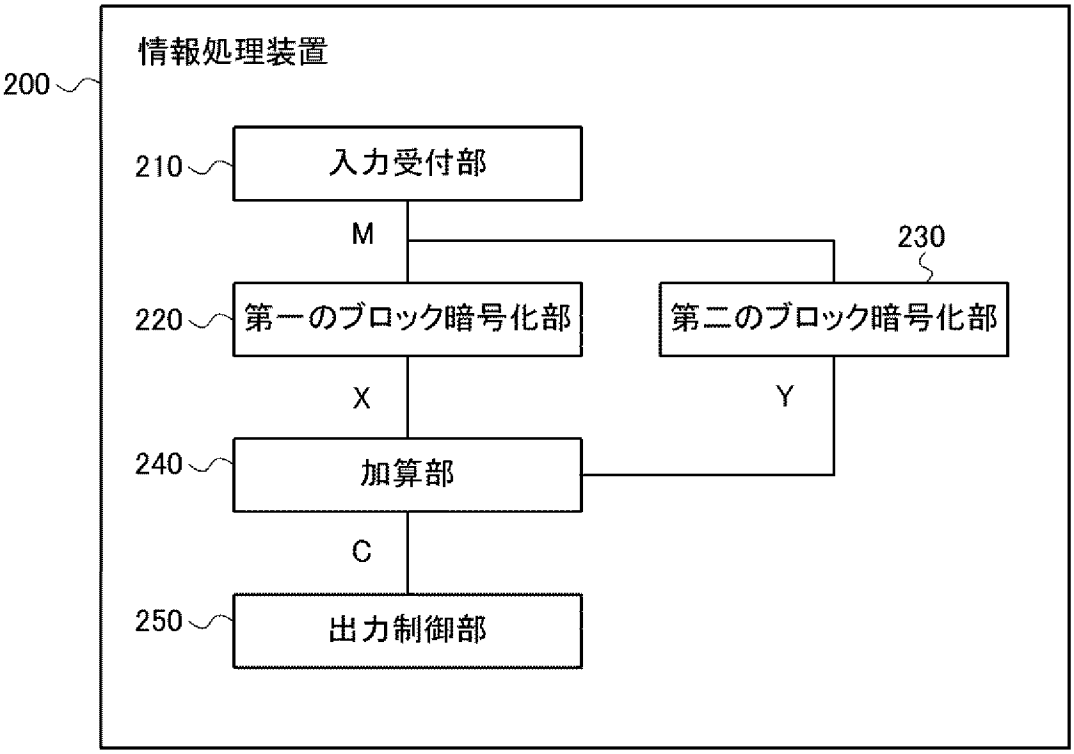

Fig. 9

[図10]

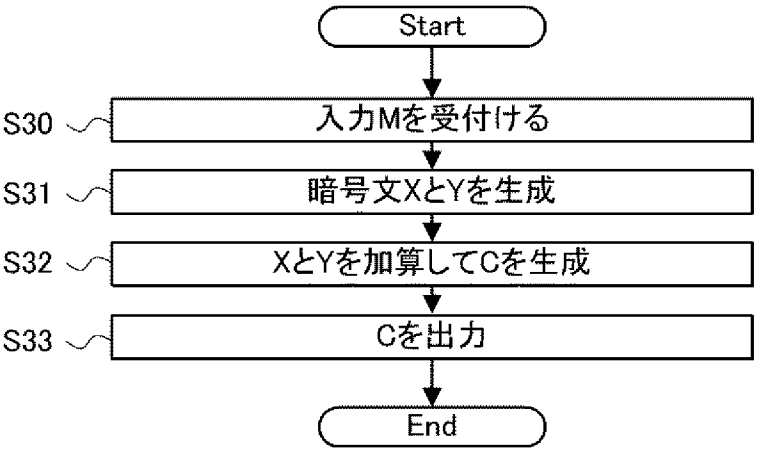

Fig. 10

[図11]

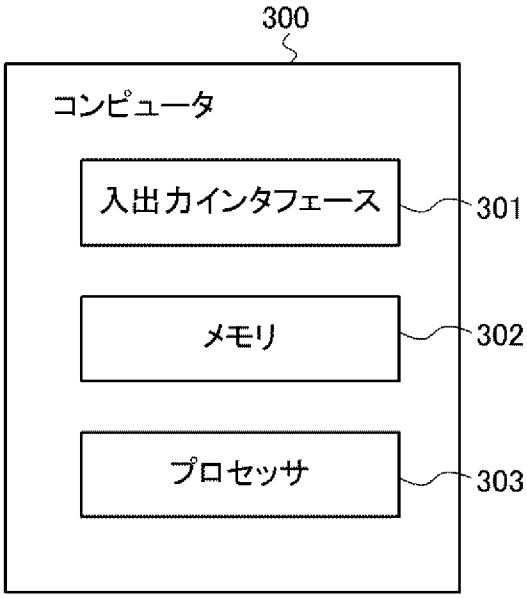

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/033183

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. G09C1/00(2006.01)i, H04L9/06(2006.01)i
FI: G09C1/00 610A, H04L9/00 611Z

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl. G09C1/00, H04L9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2020
Registered utility model specifications of Japan 1996-2020
Published registered utility model applications of Japan 1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2009/087972 A1 (NEC CORP.) 16 July 2009, paragraphs [0077]-[0099], fig. 6-11	1-7
A	WO 2008/026624 A1 (SONY CORP.) 06 March 2008, paragraphs [0028]-[0126], fig. 1-18	1-7
A	WO 2012/132622 A1 (SONY CORP.) 04 October 2012, paragraphs [0028]-[0155], fig. 1-28	1-7

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17.11.2020	24.11.2020
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2020/033183

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	阪本光星他．複数線形層を用いた低遅延ブロック暗号の構成方法．2020年暗号と情報セキュリティシンポジウム予稿集．[online], 21 January 2020, 2B2-2, in particular, "6. Discussion of Active S-box Evaluation Optimal Pn", non-official translation (SAKAMOTO, Kosei et al. The Design of Low-latency Block Cipher Using Multiple Permutations. Proceedings of the 2020 Symposium on Cryptography and Information Security.)	1-7

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/033183

Patent Documents referred to in the Report	Publication Date	Patent Family	Publication Date
WO 2009/087972 A1	16.07.2009	US 2011/0110519 A1 paragraphs [0095]- [0118], fig. 6-13	
WO 2008/026624 A1	06.03.2008	US 2010/0002872 A1 paragraphs [0068]- [0231], fig. 1-18 EP 2058783 A1 CN 101512618 A	
WO 2012/132622 A1	04.10.2012	US 2014/0003603 A1 paragraphs [0066]- [0366], fig. 1-2S EP 2693682 A1 CN 103503362 A	

国際調査報告

国際出願番号
PCT/JP2020/033183

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））
G09C 1/00(2006.01)i; H04L 9/06(2006.01)i
FI: G09C1/00 610A; H04L9/00 611Z

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
G09C1/00; H04L9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	WO 2009/087972 A1 (日本電気株式会社) 16.07.2009 (2009-07-16) 段落［００７７］－［００９９］、［図６］－［図１１］	1-7
A	WO 2008/026624 A1 (ソニー株式会社) 06.03.2008 (2008-03-06) 段落［００２８］－［０１２６］、［図１］－［図１８］	1-7
A	WO 2012/132622 A1 (ソニー株式会社) 04.10.2012 (2012-10-04) 段落［００２８］－［０１５５］、［図１］－［図２８］	1-7
A	阪本 光星 Kosei Sakamoto　他，複数線形層を用いた低遅延ブロック暗号の構成方法 The Design of Low-latency Block Cipher Using Multiple Permutations，２０２０年 暗号と情報セキュリティシンポジウム予稿集 ［ｏｎｌｉｎｅ］ Proceedings of 2020 Symposium on Cryptography and Information Security, 2020.01.21, 2B2-2 特に、「６　Ａｃｔｉｖｅ Ｓ－ｂｏｘ評価における最適なＰｎの検討」	1-7

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
“A” 特に関連のある文献ではなく、一般的技術水準を示すもの
“E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
“L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
“O” 口頭による開示、使用、展示等に言及する文献
“P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
17.11.2020	24.11.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
松平　英 5S 3146

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2020/033183

引用文献	公表日	パテントファミリー文献	公表日
WO 2009/087972 A1	16.07.2009	US 2011/0110519 A1 段落［００９５］－［０１１８］、ＦＩＧ．６－ＦＩＧ．１３	
WO 2008/026624 A1	06.03.2008	US 2010/0002872 A1 段落［００６８］－［０２３１］、ＦＩＧ．１－ＦＩＧ．１８ EP 2058783 A1 CN 101512618 A	
WO 2012/132622 A1	04.10.2012	US 2014/0003603 A1 段落［００６６］－［０３６６］、ＦＩＧ．１－ＦＩＧ．２８ EP 2693682 A1 CN 103503362 A	