(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
2013 年 12 月 27 日(27.12.2013)

WIPO | PCT

(10) 国際公開番号
WO 2013/190782 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/10* (2006.01)

(21) 国際出願番号: PCT/JP2013/003456

(22) 国際出願日: 2013 年 5 月 31 日(31.05.2013)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2012-141153 2012 年 6 月 22 日(22.06.2012) JP

(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).

(72) 発明者: 山下　哲孝(YAMASHITA, Noritaka); 〒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).

(74) 代理人: 岩壁　冬樹, 外(IWAKABE, Fuyuki et al.); 〒1040031 東京都中央区京橋二丁目８番７号 読売中公ビル６階　サンライズ国際特許事務所 Tokyo (JP).

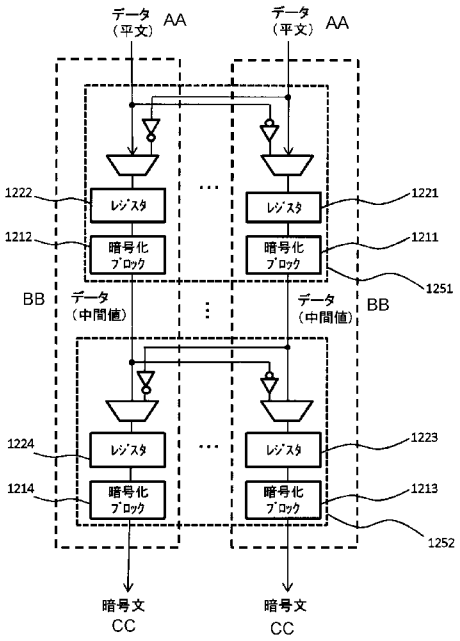
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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).

[続葉有]

(54) **Title**: ENCRYPTION PROCESSING CIRCUIT AND DECRYPTION PROCESSING CIRCUIT

(54) 発明の名称 : 暗号化処理回路および復号処理回路



1221, 1222, 1223, 1224 Register
1211, 1212, 1213, 1214 Encryption block
AA Data (plain text)
BB Data (intermediate value)
CC Encrypted text

(57) **Abstract**: The present invention is provided with a plurality of encryption processors (1251 to 1252) for performing encryption in a plurality of steps using an encryption key. The encryption processors (1251 to 1252) include a plurality of registers (1221 to 1224) for randomly storing and outputting either data or separate inverted data, and a plurality of encryption blocks (1211 to 1214) for encrypting the outputted data and outputting the encrypted data. When the encryption step occurs prior to a final step, an intermediate value encrypted by the encryption block is output to a separate encryption processor, and said separate encryption processor accepts input of the intermediate value as data. When the encryption of the final step has ended, the data encrypted by the encryption blocks is output as encrypted text.

(57) 要約:　暗号鍵を用いて複数ステップの暗号化を行う複数の暗号処理部１２５１～１２５２を備え、暗号処理部１２５１～１２５２は、データ、または反転された別のデータのいずれかをランダムに格納して出力する複数のレジスタ１２２１～１２２４と、出力されたデータを暗号化して出力する複数の暗号化ブロック１２１１～１２１４とを含み、暗号化のステップが最終ステップより前である場合、暗号化ブロックにより暗号化された中間値を、別の暗号処理部に出力し、当該別の暗号処理部は、当該中間値をデータとして入力し、最終ステップの暗号化が終了した場合、暗号化ブロックが暗号化したデータを暗号文として出力する。

WO 2013/190782 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ： 暗号化処理回路および復号処理回路

技術分野

[0001] 本発明は、暗号化処理回路および復号処理回路に関し、特に、サイドチャネル攻撃を困難とする耐タンパー性を有する暗号化処理回路および復号処理回路に関する。

背景技術

[0002] 情報の電子データ化が進む中で、秘匿な通信において、情報の保護のために暗号はかかせない技術となっている。暗号は、その安全性を保つために、鍵等の秘密情報が容易に推測されないようにする必要がある。鍵の全数探索や数学的に解読を行う線形解読や差分解読等といった暗号解析方法が知られているが、処理に時間がかかるため、現実的に一般的なユーザーが利用できる時間での解析は不可能な状況といえる。

[0003] その一方で、携帯端末などの暗号機能を実装した装置（暗号モジュール）において、攻撃者が処理時間や消費電力などのサイドチャネル情報を精密に測定できるとの仮定の下で、サイドチャネル情報から秘密情報の取得を試みるサイドチャネル攻撃とその対策が大きな研究テーマとなっている。

[0004] サイドチャネル攻撃の一つとして、暗号モジュールの消費電力を測定し、消費電力から鍵等の秘密情報を解析する電力解析攻撃がある。電力解析攻撃の中でも、複数の消費電力波形に統計処理を行うことで解析を行う、差分電力解析が特に強力な攻撃法とされている（例えば、非特許文献１参照）。

[0005] 暗号モジュールにおいて、論理ゲートの遷移確率に偏りが生じる場合に、データ列の中で１となるビットの数（ハミング重み）と消費電力とに相関があるとされている（例えば、非特許文献２）。また、あらかじめ規定された暗号化処理を所定回数実行して暗号文を生成する場合、暗号化処理前後でのレジスタのビット遷移（ハミング距離）と消費電力とに相関があるとされている（例えば、非特許文献３参照）。

[0006] そのため、ハミング重みやハミング距離に着目することで、秘密鍵が解析できてしまうという問題点がある。ハミング重みやハミング距離に着目した攻撃への対策手法の例として、Ｗａｖｅ　Ｄｉｆｆｅｒｅｎｔｉａｌ　Ｄｙｎａｍｉｃ　Ｌｏｇｉｃ（ＷＤＤＬ）が提案されている（例えば、非特許文献４参照）。ＷＤＤＬは、プリチャージ動作を行った後、相補回路を用いて演算することで消費電力の均一化を図っている。演算時のビット値の違いによる消費電流の相違をなくすことで、差分電力解析への対策を実現している。ＷＤＤＬにおいては、動作にプリチャージを必要とするが、プリチャージを行う分動作速度が低下する。また、相補回路を必要とするため、回路面積が増大している。その結果、ＷＤＤＬでは性能面積比が低下するという問題点がある。

[0007] 非特許文献５には、複数の暗号化ブロックおよびレジスタを用意して交互に処理に用い、さらに処理の開始タイミングをずらすことによって、ハミング距離に基づく攻撃に関して耐タンパー性を有する暗号処理回路が提案されている。また、パイプライン処理を用いることで性能面積比の改善を図っている。しかしながら、レジスタに書き込まれる中間値に関しては対策をしていないため、ハミング重みに基づく攻撃に関しては対策がなされていない。

[0008] 特許文献１には、２つのラウンド演算回路を直列に接続し、正規のラウンド鍵を適用した正規のラウンド演算と、ダミーラウンド鍵を適用したダミーラウンド演算を交互に切り替えて暗号処理演算を実行する構成を有することにより、ＤＰＡ（Ｄｉｆｆｅｒｅｎｔｉａｌ　Ｐｏｗｅｒ　Ａｎａｌｙｓｉｓ）攻撃に関して耐タンパー性を有する暗号処理装置が開示されている。特許文献１に記載された手法では、ダミーラウンド演算を行う回路を設ける必要があるため、回路規模が２倍となる。その結果、性能面積比が低下するという問題点がある。

[0009] また、特許文献２には、平文を複数のブロックに分割し、各ブロックに対するブロック間で独立した暗号化をする場合において、ブロック毎の暗号化をＣＰＵでパイプライン処理により行う技術が開示されている。

先行技術文献

特許文献

[0010] 特許文献1：特開２００７－１９５１３２号公報

特許文献2：特開２００９－２０５１６１号公報

非特許文献

[0011] 非特許文献1：P. Kocher, J. Jaffe and B. Jun, "Introduction to Differential Power Analysis and Related Attacks,"、Cryptography Research、1998.

非特許文献2：佐々木明彦、阿部公輝、“暗号回路への電力差分解析攻撃に対するアルゴリズムレベルでの耐性評価”電学論Ｃ、１２６巻１０号、２００６．

非特許文献3：E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," CHES 2004 ,LNCS 3156 ,pp.16－29 ,2004.

非特許文献4：Kris Tiri, Ingrid Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", Proceedings of the Design, Automation and Test in Europe Conference and Exhibition ,1530－1591 ,2004.

非特許文献5：山下哲孝　他、“ハミング距離モデルに基づく電力解析攻撃に対するパイプライン処理を用いた耐タンパー手法”、SCIS 2012.

発明の概要

発明が解決しようとする課題

[0012] 非特許文献４に記載された技術では、回路規模が２倍となり、処理速度もプリチャージにより半減してしまう。したがって、当該技術を用いない回路と比べて性能面積比は約１／４に落ちてしまう。

[0013] 非特許文献５に記載された技術では、回路規模の増加や処理速度の低下、および性能面積比の低下は発生しないが、ハミング重みに基づく攻撃に耐性

がない。

[0014] 特許文献１に記載された発明では、スループットは落ちないが、回路規模が約２倍となり、したがって、性能面積比が約１／２に落ちてしまう。

[0015] 特許文献２に記載された発明のようなパイプライン処理は、後述するようにサイドチャネル攻撃に対する耐タンパー性が弱い。

[0016] そこで、本発明は、性能面積比の増大を抑制しつつ、ハミング距離やハミング重みを用いた方法による秘密情報の漏洩を抑制できる、暗号化処理回路および復号処理回路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

[0017] 本発明による暗号化処理回路は、平文または当該平文の暗号化における中間値である複数のデータを入力し、暗号鍵を用いて複数ステップの暗号化を行う複数の暗号処理部を備え、前記暗号処理部は、前記データ、または反転された別の前記データのいずれかをランダムに格納して出力する複数のレジスタと、対となる前記レジスタから出力されたデータを暗号化して出力する複数の暗号化ブロックとを含み、暗号化のステップが最終ステップより前である場合、前記暗号化ブロックにより暗号化された前記中間値を、別の前記暗号処理部に出力し、当該別の前記暗号処理部は、当該中間値を前記データとして入力し、最終ステップの暗号化が終了した場合、前記暗号化ブロックが暗号化したデータを暗号文として出力することを特徴とする。

[0018] 本発明による復号処理回路は、暗号文または当該暗号文の復号における中間値である複数のデータを入力し、暗号鍵を用いて複数ステップの復号を行う複数の復号処理部を備え、前記復号処理部は、前記データ、または反転された別の前記データのいずれかをランダムに格納して出力する複数のレジスタと、対となる前記レジスタから出力されたデータを復号して出力する複数の復号ブロックとを含み、復号のステップが最終ステップより前である場合、前記復号ブロックにより復号された前記中間値を、別の前記復号処理部に出力し、当該別の前記復号処理部は、当該中間値を前記データとして入力し、最終ステップの復号が終了した場合、前記復号ブロックが復号したデータ

を平文として出力することを特徴とする。

発明の効果

[0019] 本発明によれば、性能面積比の増大を抑制しつつ、ハミング重みやハミング距離から秘密情報の漏洩することを抑制できる。

図面の簡単な説明

[0020] [図1]本発明による暗号化処理回路の実施形態の構成を示すブロック図である。

[図2]暗号化処理回路のループ処理部の構成を示すブロック図である。

[図3]出力選択を行うループ処理部の構成を示すブロック図である。

[図4]後処理部が連結された暗号化処理回路の構成を示すブロック図である。

[図5]本発明による実施形態の暗号化処理回路の動作を示すフローチャートである。

[図6]本発明による実施形態の暗号化処理回路の動作を示すタイミングチャートである。

[図7]本発明による暗号化処理回路の実施形態の別の構成を示すブロック図である。

[図8]本発明による暗号化処理回路の実施形態のさらに別の構成を示すブロック図である。

[図9]入力タイミングをずらした場合の暗号化処理回路の動作を示すタイミングチャートである。

[図10]実施例における、ＡＥＳ暗号化処理回路の構成を示すブロック図である。

[図11]実施例における、ＡＥＳの正規値に対するＳｕｂＢｙｔｅのテーブルを示す説明図である。

[図12]実施例における、ＡＥＳの相補値に対するＳｕｂＢｙｔｅのテーブルを示す説明図である。

[図13]実施例における、１２８ビットＡＥＳ暗号化処理回路の動作を示すタイミングチャートである。

[図14]本発明による復号処理回路の実施形態の構成を示すブロック図である。

[図15]本発明による暗号化処理回路の主要部の構成を示すブロック図である。

[図16]順次処理を行う一般的な暗号化処理回路の構成を示すブロック図である。

[図17]順次処理を行う一般的な暗号化処理回路の動作を示すタイミングチャートである。

[図18]データを記憶するレジスタを１ステップごとに入れ替えて処理を行う、一般的な暗号化処理回路の構成を示すブロック図である。

[図19]一般的なパイプライン型の暗号化処理回路の構成を示すブロック図である。

[図20]一般的なパイプライン型の暗号化処理回路の動作を示すタイミングチャートである。

発明を実施するための形態

[0021] 以下、図面を参照して本発明を実施するための形態を詳細に説明する。

[0022] 図１は、本発明による暗号化処理回路の実施形態の構成を示すブロック図である。本実施形態の暗号化処理回路は、暗号化部１００と、鍵生成部２００とを含む。

[0023] また、図１に示すように、暗号化処理回路の前段に、平文の入力タイミングを調節するタイミング調整回路１６０が設けられていてもよい。なお、タイミング調整回路１６０は、暗号化処理回路内に含まれていてもよい。その場合、タイミング調整回路１６０は、例えば入力レジスタ１４１、１４２と前処理部１１１、１１２との間に設けられる。

[0024] 暗号化部１００は、前処理部１１１、１１２と、ループ処理部１２０と、後処理部１３１、１３２と、入力レジスタ１４１、１４２と、出力レジスタ１４３、１４４とを含む。暗号化部１００は、入力されたデータと鍵生成部２００から受け取る暗号鍵をもとに、データを暗号化し、暗号文を出力する

。

[0025] 前処理部１１１、１１２は、暗号化処理において、後段の暗号化ブロックで行なわれるループ処理の前段の処理を実施する。例えば、前処理部１１１、１１２は、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）が用いられる場合、ラウンド処理の前に秘密鍵と平文との排他的論理和を得る処理を実施する。また、前処理部１１１、１１２は、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）が用いられる場合、ＩＰ処理の機能を持つように構成される。また、前処理部１１１、１１２は、平文が分割して入力される場合に、入力された平文データを蓄積してもよい。その場合、前処理部１１１、１１２は、一定量のデータが蓄積された場合、後段の暗号化ブロックにデータを送る。なお、本実施形態の暗号化処理回路は、前処理部１１１、１１２を含まない構成とすることも可能である。

[0026] ループ処理部１２０は、前段の前処理部１１１、１１２からデータを受け取り、データに対して暗号化処理を行い、後段の後処理部１３１、１３２にデータを出力する。図２は、暗号化処理回路のループ処理部の構成を示すブロック図である。ループ処理部１２０は、暗号化ブロック１２１１～１２１４、レジスタ１２２１～１２２４、セレクタ１２３１～１２３６、および乱数生成部１２４０を含む。

[0027] 暗号化ブロック１２１１～１２１４は、直前のレジスタからデータを受け取り、暗号化処理を１ステップ分行い、後段のレジスタに出力する。例えば、ＡＥＳにおいては、暗号化ブロック１２１１～１２１４は、ＳｕｂＢｙｔｅ、ＳｈｉｆｔＲｏｗ、ＭｉｘＣｏｌｕｍｎ、ＡｄｄＲｏｕｎｄＫｅｙのラウンド処理を１ステップ分の処理とみなす。また、暗号化ブロック１２１１または対の暗号化ブロック１２１２が１ステップとして処理され、次の段の暗号化ブロック１２１３または対の暗号化ブロック１２１４が１ステップとして処理される。各ステップにおいて、対となる暗号化ブロックが交互に処理を行なう。

[0028] なお、暗号化ブロック１２１１と暗号化ブロック１２１２とが対をなして

おり、暗号化ブロック１２１１の入出力値と暗号化ブロック１２１２の入出力値は相補の関係になる。暗号化ブロック１２１１に入力された値と相補の関係にある値を暗号化ブロック１２１２に入力した場合、後述する反転処理により、暗号化ブロック１２１１の出力値と相補の関係にある値が、暗号化ブロック１２１２の出力値となる。

[0029] 例えば、暗号化ブロック１２１１への入力値が１０１１１１００であり、その出力値が００１００１１１となる場合、暗号化ブロック１２１２に０１０００００１１が入力された場合には、１１０１１０００が出力される。ＡＥＳを用いてこの機能を実現するには、まずＳｕｂＢｙｔｅでは入出力関係を相補にしたものを用意する。ＳｈｉｆｔＲｏｗ、ＭｉｘＣｏｌｕｍｎでは通常の処理と同じ処理を行う。最後に、ＡｄｄＲｏｕｎｄＫｅｙでは部分鍵を反転したものをＭｉｘＣｏｌｕｍｎの結果に加算すればよい。

[0030] 暗号化ブロック１２１１および暗号化ブロック１２１２と同様に、暗号化ブロック１２１３および暗号化ブロック１２１４は、対をなしている。

[0031] レジスタ１２２１～１２２６は、入力された平文や暗号化ブロックからの出力値を保存し、後段の暗号化ブロックへ出力する機能を持つ。

[0032] セレクタ１２３１は、後段のセレクタ１２３３およびセレクタ１２３４に対して、平文または暗号化ブロック１２１３の出力値のどちらの値を渡すかを選択する。セレクタ１２３１は、暗号化ブロック１２１３の処理でループが終了したかに応じてこの選択を行い、ループが終了していたら平文を、終了していなければ暗号化ブロック１２１３の出力値を選択する。

[0033] 同様にセレクタ１２３２は、後段のセレクタ１２３３およびセレクタ１２３４に対して、平文または暗号化ブロック１２１４の出力値のどちらの値を渡すかを選択する。

[0034] セレクタ１２３３は、前段のセレクタ１２３１およびセレクタ１２３２から渡された値のどちらをレジスタ１２２１に渡すかを、乱数生成部１２４０から渡される乱数にしたがって判定する。例えば、乱数が０ならばセレクタ１２３１、乱数が１ならばセレクタ１２３２の値を選択する。

[0035] 同様に、セレクタ１２３４は前段のセレクタ１２３１およびセレクタ１２３２から渡された値のどちらをレジスタ１２２２に渡すかを、乱数生成部１２４０から渡される乱数にしたがって判定する。例えば、乱数が０ならばセレクタ１２３２、乱数が１ならばセレクタ１２３１の値を選択する。

[0036] セレクタ１２３５およびセレクタ１２３６も、セレクタ１２３３およびセレクタ１２３４と同様に暗号化ブロック１２１１および暗号化ブロック１２１２から渡された値を、乱数によって選択し、後段のレジスタ１２２３およびレジスタ１２２４に出力する。

[0037] 相補の関係をつくるため、図２の左側にあるセレクタ１２３２、セレクタ１２３４およびセレクタ１２３６に対して、図２の右側のセレクタや暗号化ブロックの値が渡される場合には、反転した値が渡される。例えば、暗号化ブロック１２１１の出力値がセレクタ１２３６に渡されるときには、反転した値が渡される。

[0038] 同様に、図２の右側にあるセレクタ１２３１、セレクタ１２３３およびセレクタ１２３５に対して、図２の左側のセレクタや暗号化ブロックの値が渡される場合には、反転した値が渡される。例えば、暗号化ブロック１２１２の出力値がセレクタ１２３５に渡されるときには、反転した値が渡される。

[0039] また、セレクタ１２３２に平文を入力するときには、入力された平文を反転する。さらに、暗号化ブロック１２１４の処理結果をループ処理部１２０から出力するさいには、暗号化ブロック１２１４の処理結果を反転したものを暗号文として出力する。

[0040] このように処理することで、左側の暗号化ブロックやレジスタは常に反転した値に対して処理を行うことになり、一方、右側の暗号化ブロックやレジスタでは常に正規の値に対して処理を行うことになる。よって、平文１と平文２とが同一のデータであったとしても、左側と右側とで異なる値に対する処理が行われることとなる。

[0041] なお、ループ処理部１２０は、必ずしも複数回のループ処理を行わなくてもよく、複数ステップの暗号化が終了した時点で、暗号化を終了し暗号文を

出力する構成となっていればよい。

[0042] 乱数生成部１２４０は、乱数を生成する。乱数生成部１２４０に生成された乱数によってループ処理部１２０において、選択する値が切り替わり、各レジスタおよび暗号化ブロックで正規の値を処理するか、反転した値を処理するかが決定される。乱数の生成方法として、線形帰還シフトレジスタ（Ｌｉｎｅａｒ Ｆｅｅｄｂａｃｋ Ｓｈｉｆｔ Ｒｅｇｉｓｔｅｒ：ＬＦＳＲ）を用いる方法や、抵抗の熱雑音など回路素子をノイズ源として乱数を発生させる物理乱数発生器を用いる方法、回路外部から乱数を取り込む方法などが考えられる。出力する乱数のビット長については、１ビットだけとすることも可能であるし、複数ビット出力させて１となったビットの数で値の切り替えを判断することも可能である。

[0043] 図３は、暗号化処理回路の出力選択を行うループ処理部１２０の構成を示すブロック図である。乱数のパターンによっては、平文１の暗号化した結果が暗号文２のほうに出力されることもありえる。例えば、１０回暗号化ブロックで処理を行った場合に、乱数が１となった回数が５回、０となった回数が５回となると、平文１の暗号化した結果が暗号文２のほうに出力される。そのため、本実施形態の暗号化処理回路は、図３に示すようにセレクタ１２３７およびセレクタ１２３８がどちらの暗号化結果を出力するか選択する構成としてもよい。また、ループ処理部１２０が暗号化結果を入れ替える処理を行わず、後段の後処理部１３１、後処理部１３２が暗号化結果を入れ替えてもよい。

[0044] 後処理部１３１および後処理部１３２は、暗号化処理において、前段のループ処理部１２０において行なわれる処理の後段の処理を実施する機能を持つ。例えば、ＤＥＳにおいては、後処理部１３１および後処理部１３２は、ＦＰ（Ｆｉｎａｌ Ｐｅｒｍｕｔａｔｉｏｎ）処理の機能を有する。また、暗号文を一括して出力できない場合、後処理部１３１および後処理部１３２が暗号文を記憶し、１クロックごとに暗号文を分割して出力してもよい。

[0045] 図４は、後処理部が連結された暗号化処理回路の構成を示すブロック図で

ある。図４に示すように、暗号化処理回路は、図１に示す後処理部１３１と後処理部１３２とを連結して後処理部１３０とし、出力されてきた値を入れ替える機能を有する構成であってもよい。なお、暗号化処理回路は、図１における後処理部１３１および後処理部１３２を含まない構成であってもよい。

[0046] 入力レジスタ１４１および入力レジスタ１４２は、入力部から入力された入力データを一時的に記憶する。出力レジスタ１４３および出力レジスタ１４４は、後処理部１３１および後処理部１３２での処理結果を一時的に記憶する。

[0047] 鍵生成部２００は、入力された秘密鍵をもとに、暗号化部１００が使用する鍵を生成する。暗号化部１００では、ループ処理部１２０以外に、前処理部１１１や前処理部１１２、後処理部１３１や後処理部１３２でも鍵を用いることもある。そのため、鍵生成部２００は、各処理にあわせた鍵を複数生成し、生成した鍵を暗号化部１００に出力する。

[0048] 鍵の生成方法については、暗号化部１００での処理の開始前において、使用する鍵をあらかじめすべて生成して保存しておき、暗号化部１００での処理の際に、保存しておいた鍵を出力する方法や、暗号化部１００での処理と並行して鍵を生成し出力する方法が考えられる。なお、本実施形態の暗号化処理回路は、鍵生成部２００を暗号化ブロックの数と同じ数だけ用意し、それぞれの鍵生成部２００が、それに対応する暗号化ブロック用の鍵生成を行う構成であってもよい。

[0049] 次に、本実施形態における暗号化方法の動作を、図５および図６を用いて説明する。図５は、本発明による実施形態の暗号化処理回路の動作を示すフローチャートである。図６は、本発明による実施形態の暗号化処理回路の動作を示すタイミングチャートである。図５は一つのデータに着目した時のフローチャートを示し、図６は暗号化処理回路全体でのタイミングチャートを示している。

[0050] まず、図５を用いて１つの暗号化されるデータ（平文）に着目して説明す

る。暗号化処理が開始されると（ステップＡ１）、平文が暗号化処理回路に入力される（ステップＡ２）。そして、入力レジスタ１４１または入力レジスタ１４２が入力された平文を格納する。

[0051] 前処理部１１１または前処理部１１２は、入力レジスタ１４１または入力レジスタ１４２に格納された平文を入力する。前処理部１１１または前処理部１１２は、平文に対して前処理を行なう（ステップＡ３）。

[0052] 前処理後の平文は、ループ処理部１２０へ入力される。入力された平文はループ処理部１２０における平文１または平文２のどちらかが割り当てられる（ステップＡ４）。入力された平文が平文２に割り当てられた場合、平文２に対して反転処理が行われる（ステップＡ５）。

[0053] セレクタ１２３３およびセレクタ１２３４は、セレクタ１２３１またはセレクタ１２３２を通過したデータを入力する。セレクタ１２３３およびセレクタ１２３４は、乱数値が０か１のどちらであるかを判定する（ステップＡ６－１，Ａ６－２）。このとき、セレクタ１２３３は、乱数が１であれば、セレクタ１２３２から出力されて反転された値を選択してレジスタ１２２１に出力し（ステップＡ７－１）、乱数が０であれば、セレクタ１２３１から出力された値を選択してレジスタ１２２１に出力する（ステップＡ７－３）。セレクタ１２３４は、乱数が１であれば、セレクタ１２３１から出力されて反転された値を選択してレジスタ１２２２に出力し（ステップＡ７－２）、乱数が０であれば、セレクタ１２３２から出力された値を選択してレジスタ１２２２に出力する（ステップＡ７－４）。

[0054] 次に、第１の対の暗号化ブロック１２１１または暗号化ブロック１２１２は、暗号化処理を１ステップ分行う。ここで、暗号化ブロック１２１１は、正規値に対する暗号化処理を行う（ステップＡ８－１）。暗号化ブロック１２１２は、反転値に対する暗号化処理を行う（ステップＡ８－２）。

[0055] 暗号化された結果は、セレクタ１２３５およびセレクタ１２３６へ入力される。セレクタ１２３５およびセレクタ１２３６は、乱数値が０か１のどちらであるかを判定する（ステップＡ９－１，Ａ９－２）。このとき、セレク

タ１２３５は、乱数が１であれば、暗号化ブロック１２１２から出力されて反転された値を選択してレジスタ１２２３に出力し（ステップＡ１０－１）、乱数が０であれば、暗号化ブロック１２１１から出力された値を選択してレジスタ１２２３に出力する（ステップＡ１０－３）。セレクタ１２３６は、乱数が１であれば、暗号化ブロック１２１１から出力されて反転された値を選択してレジスタ１２２４に出力し（ステップＡ１０－２）、乱数が０であれば、暗号化ブロック１２１２から出力された値を選択してレジスタ１２２４に出力する（ステップＡ１０－４）。

[0056] 次に、第２の対の暗号化ブロック１２１３または暗号化ブロック１２１４は、暗号化処理を１ステップ分行う。ここで、暗号化ブロック１２１３は正規値に対する暗号化処理を行う（ステップＡ１１－１）。暗号化ブロック１２１４は、反転値に対する暗号化処理を行う（ステップＡ１１－２）。

[0057] ここで、それまで行なわれた暗号化処理のステップ回数が所定回数を満たしたかどうかの判定が制御部（図示せず。）により行われる（ステップＡ１２－１，Ａ１２－２）。まだ、所定回数を満たしていない場合、ステップＡ６－１またはステップＡ６－２へもどり、処理を繰り返す。

[0058] 所定回数を満たした場合、ループ処理部１２０での処理は終了する。なお、暗号化ブロック１２１４から出力されるデータは、反転しているため、反転処理が行われる（ステップＡ１３）。

[0059] 後処理部１３１および後処理部１３２は、後処理を行い、これにより、暗号文が生成され、出力レジスタ１４３または出力レジスタ１４４へ暗号文が格納される（ステップＡ１４）。最後に、出力レジスタ１４３または出力レジスタ１４４は、暗号文を出力し（ステップＡ１５）、暗号化処理回路に入力された平文に対する暗号化処理は完了する（ステップＡ１６）。なお、暗号化処理の回数が奇数回である場合には、ステップＡ８－１およびステップＡ８－２の後にステップＡ１２－１およびステップＡ１２－２が行われることとなる。

[0060] 次に、図６に示す暗号化処理回路でのタイミングチャートを用い、暗号化

処理回路全体での処理について説明する。図６は、本発明による実施形態の暗号化処理回路の動作を示すタイミングチャートである。図６に示すタイミングチャートは、各クロック時に暗号化処理回路内の各レジスタに格納される値と、乱数の変化とを示している。なお、各前処理部、各暗号化ブロック、後処理部１３１、および後処理部１３２には鍵生成部２００から処理に応じた鍵が送られてくるものとする。また、制御部（図示せず）によって、入出力や暗号化処理のステップ回数が適切に制御されるものとする。

[0061] 図６に示す例では、平文は２つで１組とし、暗号化処理回路は、１組ごとに平文を入力して暗号化処理を行う。暗号化処理にかかるステップ数は、入力に１ステップ、前処理１ステップ、暗号化処理６ステップ、後処理と出力に１ステップの計９ステップとする。ここでは、３ステップごとに次の組の平文を入力している。タイミングチャート内で、（１－１，Ｐ）は１組目のうち１番目のデータの平文を表し、（１－２，Ｐ）は１組目のうち２番目のデータの平文を表し、（ｉ－ｋ，Ｐ）はｉ組目のうちｋ番目のデータの平文を表す。また、（ｉ－ｋ，０）はｉ組目のうちｋ番目のデータの前処理が終わったデータを示す。（ｉ－ｋ，ｎ）は、ｉ組目のうちｋ番目のデータにｎステップ目の暗号化処理が終わったデータを表す。（ｉ－ｋ，Ｃ）は、ｉ組目のうちｋ番目の平文に対して、前処理、繰り返しの暗号化処理、後処理まで終わった暗号文を表す。

[0062] また、所定のクロックで所定の番号の平文が暗号化処理回路に入力されるとしているが、そのためのタイミング調整は、例えば、暗号化処理回路の前段にあるタイミング調整回路１６０により行われる。タイミング調整回路１６０は、例えば、平文が格納されている記憶部から所定クロックおきに平文を１組分ずつ順次読み出し、それらの平文を暗号化処理回路に供給する。

[0063] 暗号化処理回路では、はじめに１組目の平文（１－１，Ｐ）、（１－２，Ｐ）が入力される。次に、前処理部１１１および前処理部１１２が処理を行った後、ループ処理部１２０が６ステップ分の暗号化処理を行う。このループ処理部１２０では、乱数が１となった場合、データの反転が行われ、格納

するレジスタが切り替わる。例えば３クロック目では乱数が１となったことから、格納するレジスタが切り替わり、３クロック目ではレジスタ１２２４に格納されていた１組目の１番目のデータの中間値（１－１，１）は暗号化ブロック１２１４で処理され（１－１，２）と変換されたあと、４クロック目ではレジスタ１２２１に格納される。

[0064] また、ある組の平文が入力されてから３クロック後に次の組の平文が入力され、前に入力された組のデータと並列に暗号化処理が行われる。ループ処理部１２０での処理が終わったのち、後処理部１３１および後処理部１３２で後処理が行われ、出力レジスタ１４１および出力レジスタ１４２に暗号文が格納される。そして、次のクロックで１組の暗号文が出力される。図６のタイミングチャートでは、２９クロック目で出力レジスタ１４１および出力レジスタ１４２に最後の暗号文の組が格納され、３０クロック目で暗号文の組が出力され暗号化処理が終了する。

[0065] 図６に示すタイミングチャートにおいて、不定となっている箇所（×と記載された部分）では、直前の処理結果をそのまま保存する、ランダムな値もしくは固定値のダミーデータを格納する、または、暗号処理を継続しその結果を保存するなどの処理が行われる。ここで、暗号処理を継続するとは、未使用である暗号化ブロックで引き続き何らかのデータに対して暗号化を行い、レジスタに結果を格納することを意味する。

[0066] 例えば、図６において、ＣＬＫ２６以降は、第１の対の暗号化ブロック１２１２、暗号化ブロック１２１３およびレジスタ１２２２、レジスタ１２２１が未使用となるが、次のような処理が行われる。まず、クロックＣＬＫ２６では、レジスタ１２２１およびレジスタ１２２２は、データ（７－１，６）およびデータ（７－２，６）を格納する。次に、クロックＣＬＫ２７では、第１の対の暗号化ブロック１２１１および暗号化ブロック１２１２は、データ（７－１，６）およびデータ（７－２，６）に対して暗号化処理を行う。レジスタ１２２３およびレジスタ１２２４は、その結果（７－１，７）および結果（７－２，７）を格納する。次に、クロックＣＬＫ２８では、第２

の対の暗号化ブロック１２１３および暗号化ブロック１２１４は、第１の対の暗号化ブロックによる暗号化処理の上記の結果をさらに暗号化処理する。レジスタ１２２１およびレジスタ１２２２は、その結果を格納する。

[0067] ここで、本実施形態による暗号化処理回路を、暗号化処理を１つの暗号化ブロックで順次処理した場合のものと比較する。図１６は、順次処理を行う一般的な暗号化処理回路の構成を示すブロック図である。図１６に示す暗号化処理回路と比較すると、図１に示す本実施形態の暗号化処理回路は、レジスタと暗号化ブロック、セレクタなどが追加されている。暗号化ブロックが暗号化処理回路の主な構成要素である場合には、図１に示す本実施形態の暗号化処理回路の規模は図１６に示す暗号化処理回路の規模と比べて約４倍になる。

[0068] 図１７は、順次処理を行う一般的な暗号化処理回路の動作を示すタイミングチャートである。図１６に示す順次処理の回路の処理時間は、１６の平文を順次処理した場合には最大で１４４クロックとなり、１つのデータの入出力ともう１つのデータの暗号処理を同時に処理可能の場合には、図１７に示すように、９８クロックとなる。他方、本実施形態では２つの対の暗号化ブロックが同時に動作し、さらに対の暗号化ブロックで異なるデータの処理に用いられる。結果、同時に４つのデータに対して暗号化処理が実施される。最初と最後では並列処理のデータ数が２となるものの、処理するデータ数が多くなれば図１６に示す順次処理の回路と比べて、図１に示す本実施形態の回路の処理速度は、約４倍となる。

[0069] したがって、図１に示す本実施形態の暗号化処理回路は、図１６に示す順次処理による暗号化処理回路と比較して、回路面積が４倍となるが処理速度も約４倍となるので、性能面積比は、ほぼ同等となる。

[0070] 次に、本実施形態の暗号化処理回路の耐タンパー性について説明する。まず、ビット遷移（または、ハミング距離）に対する耐タンパー性を説明する。図１６に示す回路を用いて順次処理する場合、同一データについての各処理に着目すると、あるクロックにおいて処理前のデータがレジスタ１２２１

に書き込まれ、その次のクロックにおいて処理後のデータが同じレジスタ１２２１に書き込まれる。したがって、暗号化の各ステップの処理前後を比較した場合において、レジスタ１２２１の物理的なビット遷移（または、ハミング距離）と暗号化対象データ自体のビット遷移（または、ハミング距離）に相関が生じる。

[0071] また、レジスタ１２２１の物理的なビット遷移（または、ハミング距離）と、消費電力との間にも相関がある。したがって、暗号化対象データ自体のビット遷移（または、ハミング距離）と消費電力に相関が生じる。そのため、攻撃者が消費電力を解析し、さらに、暗号化対象データ自体のビット遷移（または、ハミング距離）と消費電力との間の相関を利用することにより、暗号化対象データ自体のビット遷移（または、ハミング距離）を推定し、そのビット遷移を基に、秘密鍵を推定することが可能となる。

[0072] 他方、図６に示すタイミングチャートに示されるように、図１に示す本実施形態の暗号化処理回路でレジスタ１２２１に記憶されていたデータに対して暗号化処理が１ステップ行われると、処理後のデータは、レジスタ１２２１ではなく次の対のレジスタ１２２３またはレジスタ１２２４に記憶される。そして、レジスタ１２２１には別のデータの処理結果が記憶される。すなわち、あるデータとそれに処理を施したデータが、時間的に連続して（または、時間的に隣接したクロックで）同一のレジスタに記憶されることを回避することができる。

[0073] また、本実施形態の暗号化処理回路は、ランダムに書き込まれるレジスタが選択されるため、攻撃者が例えばレジスタ１２２３に記憶されていたデータを把握できたとしても、次に記憶されるデータがレジスタ１２２１のデータの処理結果かレジスタ１２２２のデータの処理結果かが確定できない。そのため、攻撃者が物理的なビット遷移（または、ハミング距離）を計算することができなくなる。

[0074] このように、本実施形態の暗号化処理回路によれば、暗号化の各ステップの処理前後を比較した場合において、レジスタ１２２１の物理的なビット遷

移（または、ハミング距離）と暗号化対象データ自体のビット遷移（または、ハミング距離）に相関が生じることを回避することができる。したがって、レジスタ１２２１の物理的なビット遷移（または、ハミング距離）と、消費電力の変化との間にも相関があるとしても、暗号化対象データ自体のビット遷移（または、ハミング距離）と消費電力の変化に相関が生じることを回避することができる。また、暗号化対象データ自体のビット遷移（または、ハミング距離）と消費電力の変化との間の相関がないので、消費電力の変化が解析されたとしても、暗号化対象データ自体のビット遷移（または、ハミング距離）が推定されることを回避することができるので、そのビット遷移を基に、秘密鍵が推定されることも回避できる。

[0075] 次に、１となるビットの数（または、ハミング重み）に対する耐タンパー性を説明する。図１６に示す暗号化処理回路で順次処理する場合において、レジスタ１２２１に記憶されているデータは、暗号化におけるあるステップ後の中間値そのままのデータである。レジスタ１２２１のビットの数（または、ハミング重み）と暗号化対象データ自体のビットの数（または、ハミング重み）に相関が生じる。また、レジスタ１２２１のビットの数（または、ハミング重み）と、消費電力との間にも相関がある。したがって、暗号化対象データ自体のビットの数（または、ハミング重み）と消費電力に相関が生じる。そのため、攻撃者が消費電力を解析し、さらに、暗号化対象データ自体のビットの数（または、ハミング重み）と消費電力との間の相関を利用することにより、暗号化対象データ自体のビットの数（または、ハミング重み）を推定し、そのビットの数を基に、秘密鍵を推定することが可能となる。

[0076] 図１８は、データを記憶するレジスタを１ステップごとに入れ替えて処理を行う、一般的な暗号化処理回路の構成を示すブロック図である。図１８に示す暗号化処理回路を用いた場合、データ自体のビット遷移（または、ハミング距離）と消費電力の変化との間の相関をなくすことは可能であるが、暗号化対象データ自体のビットの数（または、ハミング重み）はそのままである。そのため、暗号化対象データ自体のビットの数（または、ハミング重み

）から秘密鍵を推定することが可能となる。

[0077] また、特許文献２等に開示されているパイプライン型で処理した場合でも、ハミング距離の計算が可能となり秘密鍵の解析をされてしまう場合がある。図１９は、一般的なパイプライン型の暗号化処理回路の構成を示すブロック図である。図２０は、一般的なパイプライン型の暗号化処理回路の動作を示すタイミングチャートである。

[0078] 図２０に示すように、例えばレジスタ１２２２に格納されるデータは、データＩ（１，１）の次はデータＩ（２，１）である。推定した暗号鍵を利用して、後処理と１ステップ分の暗号処理を逆算できるならば、測定した暗号文Ｃ（１）および暗号文Ｃ（２）を基に、それぞれ、データＩ（１，１）およびデータＩ（２，１）を計算することができる。したがって、データＩ（１，１）からデータＩ（２，１）へのビット遷移を算出することができることになる。

[0079] このビット遷移は、レジスタ１２２２の物理的なビット遷移であると共に、暗号化対象データ自体のビット遷移でもある。そして、そのビット遷移とレジスタ１２２２の消費電力の変化の間には相関がある。したがって、推定した多数の暗号鍵のうちの個々の暗号鍵を利用してデータＩ（１，１）からデータＩ（２，１）へのビット遷移を算出することにより、算出したビット遷移とレジスタ１２２２の測定した消費電力との間の相関が求められる。そして、推定したどの暗号鍵を利用した場合にその相関が高いかを調べられることにより、推定したどの暗号鍵が実際に利用されている暗号鍵であるのかが知られてしまう。

[0080] 一方、図２に示す本実施形態の暗号化処理回路では、レジスタ１２２１に記憶されていたデータに対して暗号化処理が１ステップ行われると、処理後のデータは、乱数が１であれば１２２４に記憶される。このとき、レジスタ１２２４に記憶されるデータは本来の暗号化処理１ステップ後のデータそのものではなく、本来の値を反転させた値となる。そのため、レジスタ１２２４のビットの数（または、ハミング重み）と暗号化対象データ自体のビット

の数（または、ハミング重み）との相関が崩れることとなる。したがって、消費電力を解析し、さらに、暗号化対象データ自体のビットの数（または、ハミング重み）と消費電力との間の相関を利用して、秘密鍵を推定することが困難となる。

[0081] なお、本実施形態の暗号化処理回路の構成は、図１に示した構成に限られず、別の構成も考えられる。図７は、本発明による暗号化処理回路の実施形態の別の構成を示すブロック図である。図７は、対となる暗号化ブロックとレジスタを２つずつ、合計４組で１段とした点が図１に示す構成と異なる。

[0082] 図８は、本発明による暗号化処理回路の実施形態のさらに別の構成を示すブロック図である。図１に示す構成は、暗号化ブロックが２段であり各段が交互に用いられる構成である。一方、図８に示す構成は、暗号化ブロックが３段以上であり、各段が順次用いられる。

[0083] 図９は、入力タイミングをずらした場合の暗号化処理回路の動作を示すタイミングチャートである。図６に示すタイミングチャートでは、２つの平文を同時に入力して処理する例を示しているが、２つの平文を同時に入力する必要はない。例えば、図９に示すように、暗号化処理回路は、１番目の平文を入力した１クロック後に２番目の平文を入力し、その１クロック後に３番目の平文を入力し、さらに１クロック後に４番目の平文を入力し、それらを並列に処理してもよい。この場合、一度の入出力に必要なデータ幅は、１つの平文（１つの暗号文）分のデータ幅となる。そのため、図９に示す動作をする暗号化処理回路は、入力レジスタ１４２および出力レジスタ１４４を必要としない。また、入力されたデータは、暗号化ブロック１２１１と暗号化ブロック１２１２のうち、他のデータの処理に使われていない暗号化ブロックにより処理される。

[0084]（実施例）

本実施形態の暗号化処理回路の実施例として、本実施形態（後処理なし）の暗号化処理回路を用いて実装したＡＥＳ暗号化回路の例を示す。

[0085] 図１０は、実施例における、ＡＥＳ暗号化処理回路の構成を示すブロック

図である。前処理部１１１，前処理部１１２により実現される排他的論理和回路（ＸＯＲ）１１１ａ，ＸＯＲ１１２ａは、ＡＥＳの前処理として、平文と秘密鍵との排他的論理和演算を行う。また、本実施例では、後処理部は不要である。

[0086] 本実施例におけるループ処理部１２０の構成は、図２に示した構成と同じである。暗号化ブロック１２１１および暗号化ブロック１２１３は、それぞれ、正規の値に対するＡＥＳのラウンド処理１段分の処理を行うこととし、ＳｕｂＢｙｔｅ、ＳｈｉｆｔＲｏｗ、ＭｉｘＣｏｌｕｍｎ、ＡｄｄＲｏｕｎｄＫｅｙの一連の処理を１ステップ分の処理とする。なお、１０ラウンド目のときにはＭｉｘＣｏｌｕｍｎ処理はスキップするものとする。

[0087] 一方、暗号化ブロック１２１２、暗号化ブロック１２１４は、それぞれ、反転した値に対してＡＥＳのラウンド処理１段分の処理を行うこととし、ＳｕｂＢｙｔｅ、ＳｈｉｆｔＲｏｗ、ＭｉｘＣｏｌｕｍｎ、ＡｄｄＲｏｕｎｄＫｅｙの一連の処理を行い、反転している値を出力することを１ステップ分の処理とする。暗号化ブロック１２１２および暗号化ブロック１２１４は、暗号化ブロック１２１１および暗号化ブロック１２１３と同様に１０ラウンド目のときには、ＭｉｘＣｏｌｕｍｎ処理をスキップする。暗号化ブロック１２１２および暗号化ブロック１２１４は、反転した入力値に対して、反転している出力値を返すため、暗号化ブロック１２１２および暗号化ブロック１２１４の構成要素は以下のような特徴を持つ。

[0088] 図１１は、実施例における、ＡＥＳの正規値に対するＳｕｂＢｙｔｅのテーブルを示す説明図である。図１２は、実施例における、ＡＥＳの相補値に対するＳｕｂＢｙｔｅのテーブルを示す説明図である。なお、図１１および図１２に示す数値は１６進数である。ＳｕｂＢｙｔｅは、入力値と出力値とがそれぞれ正規のＳｕｂＢｙｔｅに対して反転した値となる。例えば、正規の入力値が００である場合、暗号化ブロック１２１１では６３を出力する。他方、暗号化ブロック１２１２では入力値が反転しているため、ＦＦが入力値となる。ＦＦが入力された場合、暗号化ブロック１２１２は９Ｃを出力す

る。このように、暗号化ブロック１２１１と暗号化ブロック１２１２とは、入力値、出力値ともに反転した関係をもつ。

[0089] ＳｈｉｆｔＲｏｗ、ＭｉｘＣｏｌｕｍｎは、どちらも入力値そのものをシフトし、線形和をとるため、暗号化ブロック１２１１でも暗号化ブロック１２１２でも機能は同じである。ＡｄｄＲｏｕｎｄＫｅｙでは、反転している値に対しては、反転した鍵値を加算する必要がある。したがって、ＡｄｄＲｏｕｎｄＫｅｙでは入力された鍵を反転し、反転した鍵とＳｕｂＢｙｔｅ、ＳｈｉｆｔＲｏｗ、ＭｉｘＣｏｌｕｍｎ（１０ラウンド目ではＭｉｘＣｏｌｕｍｎはスキップ）の処理結果を加算し、その結果を１ステップ分の処理結果とする。以上の処理を暗号化ブロック１２１２で行うことで、正規の暗号化ブロックにおける入出力値それぞれを反転した値が、暗号化ブロック１２１２や暗号化ブロック１２１４の入出力値となる。

[0090] 実施例では、１つの平文の処理が開始してから次の平文の処理の開始まで５クロック分間隔を開ける。鍵生成部２００は、秘密鍵および秘密鍵から生成されるラウンド鍵を、前処理部としての排他的論理和回路（ＸＯＲ）１１１ａ、ＸＯＲ１１２ａ、並びにラウンド処理を行う暗号化ブロック１２１１～暗号化ブロック１２１４へ出力する。

[0091] 実施例の動作を説明する。図１３は、実施例における、１２８ビットＡＥＳ暗号化処理回路の動作を示すタイミングチャートである。実施例では、１６個、８組の平文に対してＡＥＳで暗号化が行われる。

[0092] タイミングチャート内の記号は、図６のものと同じく、（１－１，Ｐ）は１組目のうち１番目のデータの平文を示し、（１－２，Ｐ）は１組目のうち２番目のデータの平文を示し、（ｉ－ｋ，Ｐ）はｉ組目のうちｋ番目のデータの平文を示す。次に、（ｉ－ｋ，０）はｉ組目のうちｋ番目のデータの前処理が終わったデータを示す。（ｉ－ｋ，ｎ）は、ｉ組目のうちｋ番目のデータにｎステップ目の暗号化処理が終わったデータを示す。（ｉ－ｋ，Ｃ）は、ｉ組目のうちｋ番目の平文に対して、前処理、繰り返しの暗号化処理、後処理まで終わった暗号文を示す。

[0093] 実施例では、暗号化処理回路は、入力処理に１クロック、前処理に１クロック、ラウンド処理に１０クロック、出力処理に１クロック使用し、計１３クロックで動作する。また、１つの平文の処理を開始してから、次の平文の処理を開始するまでの時間的間隔は、５クロック分の間隔である。

[0094] 実施例では、レジスタにおけるビット遷移と暗号化対象データ自体のビット遷移との間に相関は生じない。そのため、消費電力と暗号化対象データ自体のビット遷移との間にも相関はなく、消費電力を解析することにより秘密鍵を推定することは困難となる。また、ビット値も反転しているため、レジスタにおけるビット値と暗号化対象データ自体のビット値とは、反転時には相関は生じない。そのため、消費電力と暗号化対象データ自体のビット値との間の相関は低くなり、消費電力を解析することにより秘密鍵を推定することは困難となる。

[0095] なお、上記の実施形態および実施例では、暗号化処理回路のみの説明をしたが、本実施形態の暗号化処理回路を適用して、復号処理回路（すなわち、暗号解読処理回路）も暗号化処理回路と同様な構成とすることができる。図１４は、本発明による復号処理回路のループ処理部の構成を示すブロック図である。図１４に示す復号処理回路は、図２に示す暗号化処理回路の構成の「暗号化ブロック」を「復号ブロック」に置き換え、入力するデータを「平文」から「暗号文」に置き換え、出力するデータを「暗号文」から「平文」に置き換えたものである。また、復号処理回路の全体構成は、入出力データ以外は図１に示す暗号化処理回路と同様である。また、復号処理回路の動作に関しては、暗号化処理回路の動作における「暗号化」を「復号」に置き換えればよい。なお、復号処理とは、暗号文を平文に戻す処理のことである。

[0096] なお、上記の暗号化処理回路は、ハードウェア、ソフトウェアまたはこれらの組み合わせにより実現されることができる。また、上記の暗号化処理回路その他の装置等により行なわれる暗号化処理方法も、ハードウェア、ソフトウェアまたはこれらに組み合わせにより実現されることができる。ここで、ソフトウェアによって実現されるとは、コンピュータがプログラムを読み

込んで実行することにより実現されることを意味する。また、ここで、例えば、第１～第ｎのレジスタ１４１～１４Ｎは、ＣＰＵに含まれるレジスタやメインメモリ、キャッシュメモリ等のメモリのエントリなどである。

[0097] 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、コンピュータに実行させることができる。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、および電磁波を含む。一時的なコンピュータ可読媒体は、電線および光ファイバ等の有線通信路、また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。

[0098] 図１５は、本発明による暗号化処理回路の主要部の構成を示すブロック図である。図１５に示すように、本発明による暗号化処理回路は、主要な構成として、平文または当該平文の暗号化における中間値である複数のデータを入力し、暗号鍵を用いて複数ステップの暗号化を行う複数の暗号処理部１２５１～１２５２を備え、暗号処理部１２５１～１２５２は、データ、または反転された別のデータのいずれかをランダムに格納して出力する複数のレジスタ１２２１～１２２４と、対となるレジスタから出力されたデータを暗号化して出力する複数の暗号化ブロック１２１１～１２１４とを含み、暗号化

のステップが最終ステップより前である場合、暗号化ブロックにより暗号化された中間値を、別の暗号処理部に出力し、当該別の暗号処理部は、当該中間値をデータとして入力し、最終ステップの暗号化が終了した場合、暗号化ブロックが暗号化したデータを暗号文として出力する。

[0099] （１）平文または当該平文の暗号化における中間値である複数のデータを入力し、暗号鍵を用いて複数ステップの暗号化を行う複数の暗号処理部（例えば、暗号処理部１２５１，１２５２）を備え、暗号処理部は、データ、または反転された別のデータのいずれかをランダムに格納して出力する複数のレジスタ（例えば、レジスタ１２２１～１２２８）と、対となるレジスタから出力されたデータを暗号化して出力する複数の暗号化ブロック（例えば、暗号化ブロック１２１１～１２１８，１２１Ａ，１２１Ｂ）とを含み、暗号化のステップが最終ステップより前である場合、暗号化ブロックにより暗号化された中間値を、別の暗号処理部に出力し、当該別の暗号処理部は、当該中間値をデータとして入力し、最終ステップの暗号化が終了した場合、暗号化ブロックが暗号化したデータを暗号文として出力する暗号化処理回路。

[0100] （２）暗号化処理回路は、少なくとも１クロックの間に、複数の平文のうちの一つの平文または当該平文の暗号化における中間値と、当該平文とは別の平文または当該別の平文の暗号化における中間値とを同時に暗号化するように構成されていてもよい。このような暗号化処理回路によれば、並列で暗号化処理を行うことで高速に暗号化処理を行うことができる。

[0101] （３）複数の平文のうちの一つの平文または当該平文の暗号化における中間値の暗号化が行われた次のクロックに、当該平文とは別の平文または当該別の平文の暗号化における中間値を暗号化するように構成されていてもよい。このような暗号化処理回路によれば、複数クロックにおいて間を空けずに暗号化処理を行うことで高速に暗号化処理を行うことができる。

[0102] （４）複数の平文を入力するクロックのタイミングを調整するタイミング調整回路（例えば、タイミング調整回路１６０）を備えるように構成されていてもよい。

[0103] この出願は、２０１２年６月２２日に出願された日本出願特願２０１２－１４１１５３を基礎とする優先権を主張し、その開示の全てをここに取り込む。

[0104] 以上、実施形態及び実施例を参照して本願発明を説明したが、本願発明は上記実施形態及び実施例に限定されるものではない。本願発明の構成や詳細には、本願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。

産業上の利用の可能性

[0105] 本発明は、携帯端末等の情報端末の暗号モジュールに適用できる。

符号の説明

[0106] １００　暗号化部

１１１，１１２　前処理部

１２０　ループ処理部

１２１１～１２１８，１２１Ａ，１２１Ｂ　暗号化ブロック

１２２１～１２２８　レジスタ

１２３１～１２３８，１２３Ａ～１２３Ｆ　セレクタ

１２４１～１２４４　復号ブロック

１３０～１３２　後処理部

１４１，１４２　入力レジスタ

１４３，１４４　出力レジスタ

１６０　タイミング調整回路

２００　鍵生成部

請求の範囲

[請求項1] 平文または当該平文の暗号化における中間値である複数のデータを入力し、暗号鍵を用いて複数ステップの暗号化を行う複数の暗号処理部を備え、

前記暗号処理部は、

前記データ、または反転された別の前記データのいずれかをランダムに格納して出力する複数のレジスタと、

対となる前記レジスタから出力されたデータを暗号化して出力する複数の暗号化ブロックとを含み、

暗号化のステップが最終ステップより前である場合、

前記暗号化ブロックにより暗号化された前記中間値を、別の前記暗号処理部に出力し、当該別の前記暗号処理部は、当該中間値を前記データとして入力し、

最終ステップの暗号化が終了した場合、

前記暗号化ブロックが暗号化したデータを暗号文として出力する

ことを特徴とする暗号化処理回路。

[請求項2] 少なくとも１クロックの間に、複数の平文のうちの一つの平文または当該平文の暗号化における中間値と、当該平文とは別の平文または当該別の平文の暗号化における中間値とを同時に暗号化する

請求項１記載の暗号化処理回路。

[請求項3] 複数の平文のうちの一つの平文または当該平文の暗号化における中間値の暗号化が行われた次のクロックに、当該平文とは別の平文または当該別の平文の暗号化における中間値を暗号化する

請求項１または請求項２記載の暗号化処理回路。

[請求項4] 複数の平文を入力するクロックのタイミングを調整するタイミング調整回路を備えた

請求項２または請求項３記載の暗号化処理回路。

[請求項5] 暗号文または当該暗号文の復号における中間値である複数のデータ

を入力し、暗号鍵を用いて複数ステップの復号を行う複数の復号処理部を備え、

前記復号処理部は、

前記データ、または反転された別の前記データのいずれかをランダムに格納して出力する複数のレジスタと、

対となる前記レジスタから出力されたデータを復号して出力する複数の復号ブロックとを含み、

復号のステップが最終ステップより前である場合、

前記復号ブロックにより復号された前記中間値を、別の前記復号処理部に出力し、当該別の前記復号処理部は、当該中間値を前記データとして入力し、

最終ステップの復号が終了した場合、

前記復号ブロックが復号したデータを平文として出力する

ことを特徴とする復号処理回路。

[請求項6] 少なくとも１クロックの間に、複数の暗号文のうちの一つの暗号文または当該暗号文の復号における中間値と、当該暗号文とは別の暗号文または当該別の暗号文の復号における中間値とを同時に復号する

請求項５記載の復号処理回路。

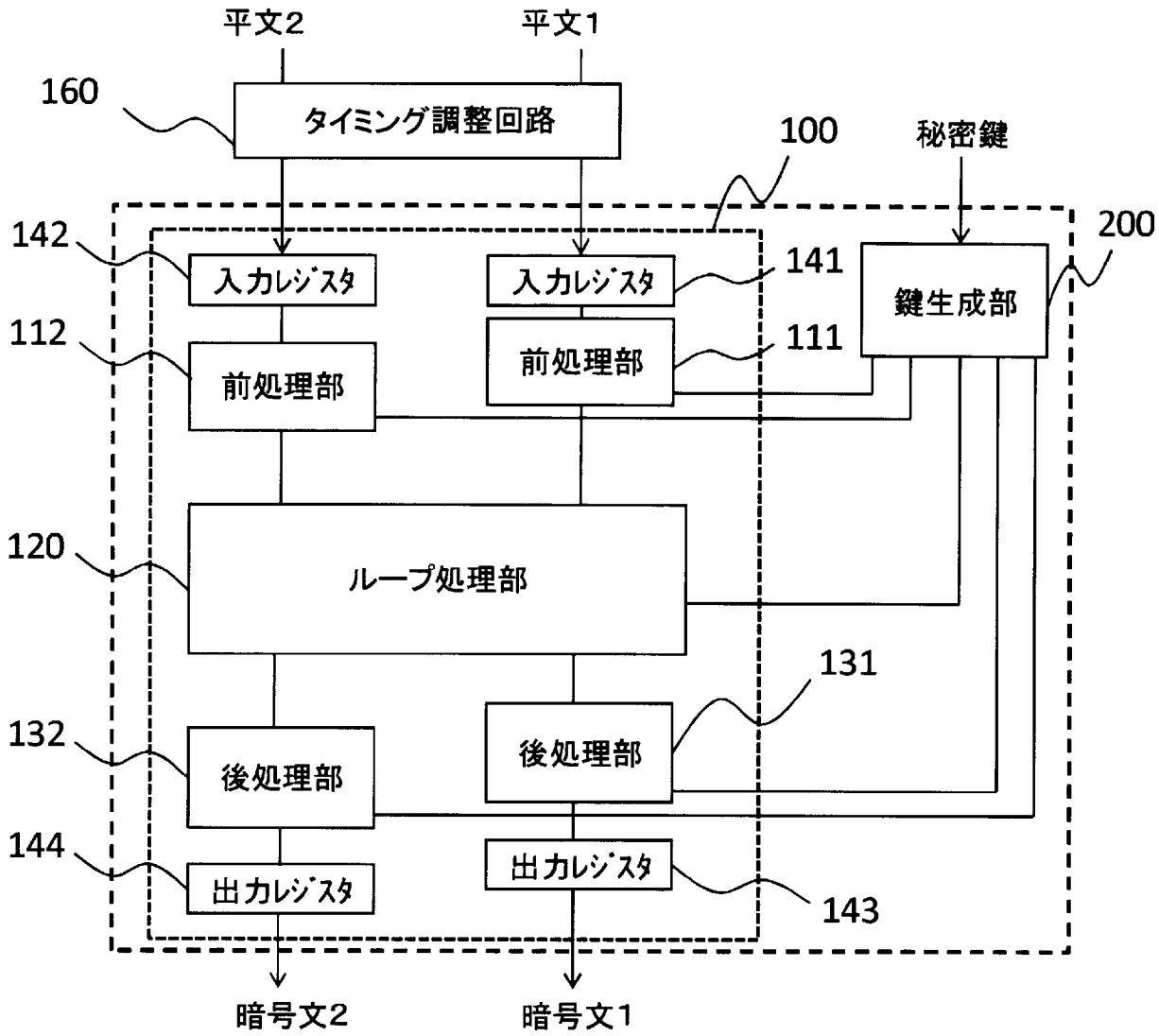
[請求項7] 複数の暗号文のうちの一つの暗号文または当該暗号文の復号における中間値の復号が行われた次のクロックに、当該暗号文とは別の暗号文または当該別の暗号文の復号における中間値を復号する

請求項５または請求項６記載の復号処理回路。

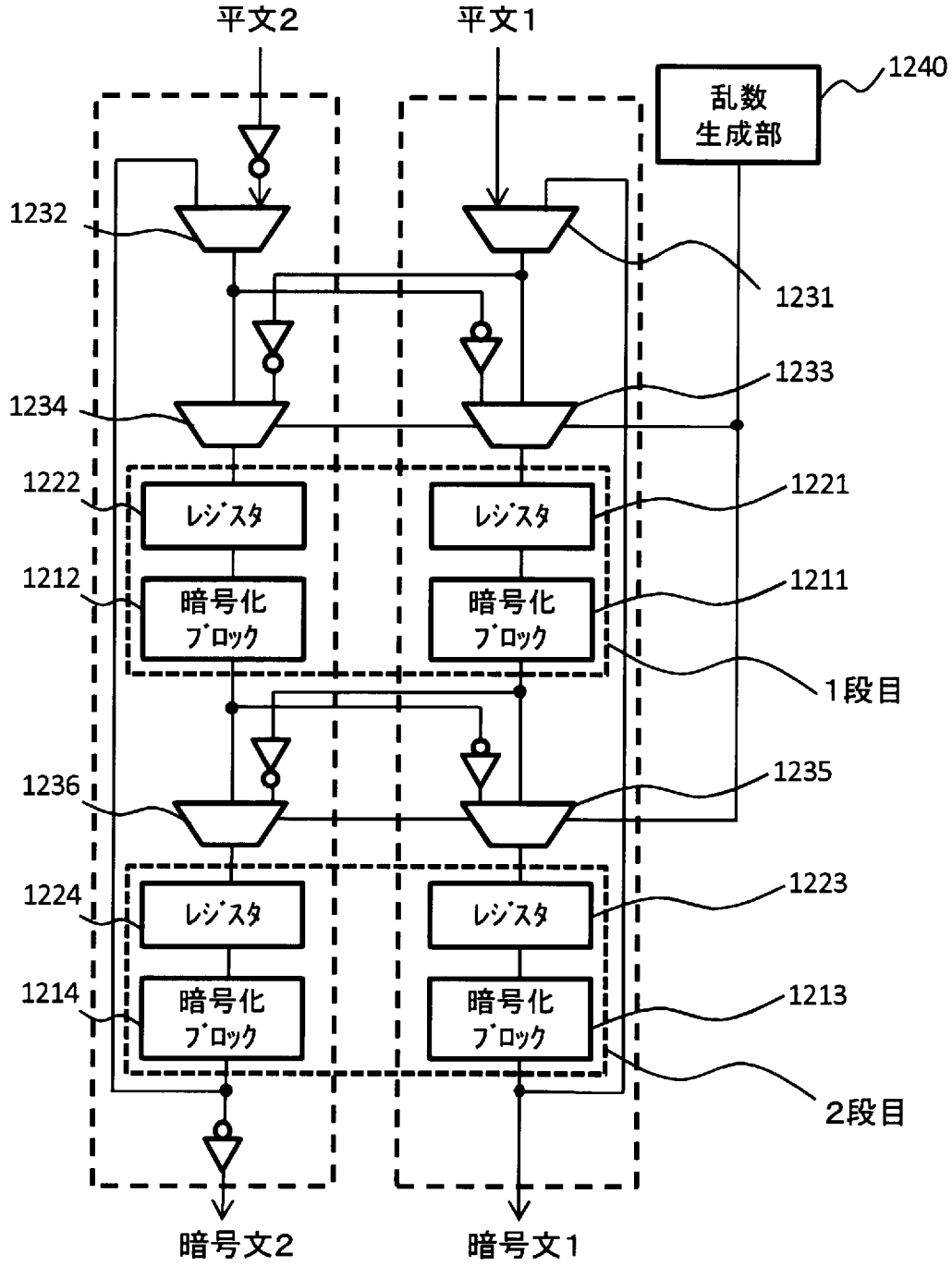
[請求項8] 複数の暗号文を入力するクロックのタイミングを調節するタイミング調節回路を備えた

請求項６または請求項７記載の復号処理回路。

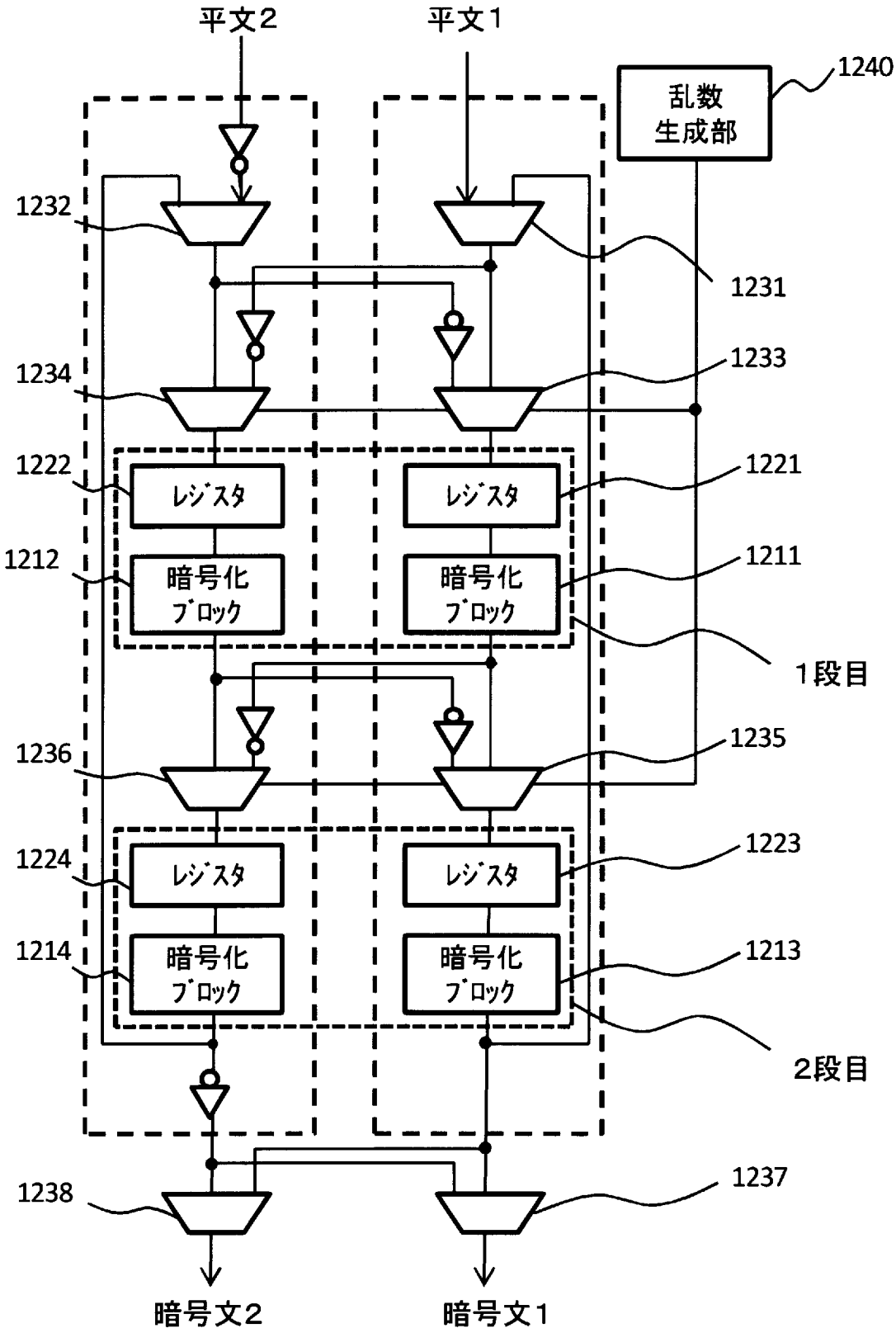
[図1]


平文2
平文1
160
タイミング調整回路
100
秘密鍵
200
142
入力レジスタ
入力レジスタ
141
鍵生成部
112
前処理部
前処理部
111
120
ループ処理部
131
132
後処理部
後処理部
144
出力レジスタ
出力レジスタ
143
暗号文2
暗号文1

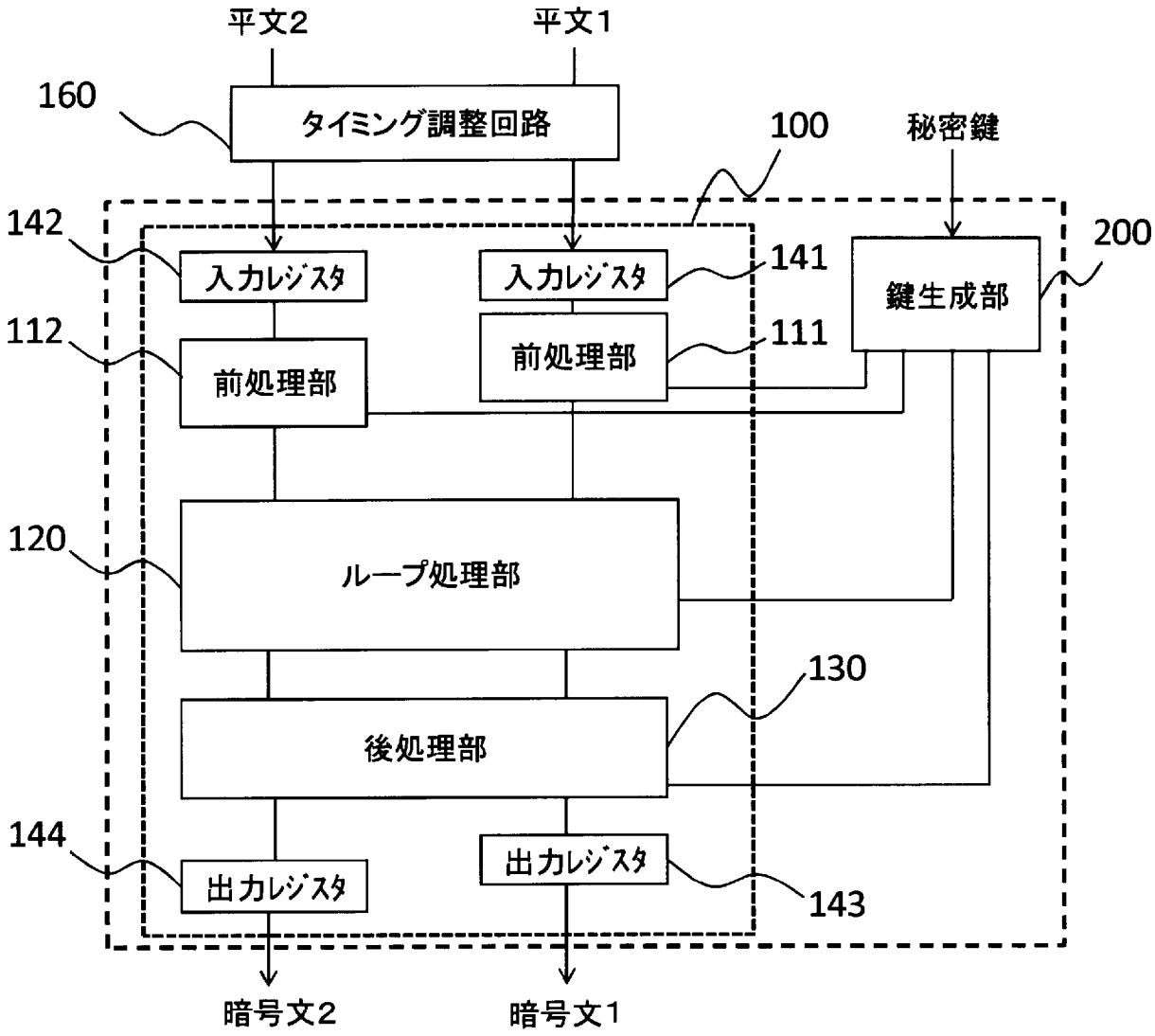
[図2]


平文2
平文1
乱数
生成部
1240
1232
1231
1233
1234
1222
レジスタ
レジスタ
1221
1212
暗号化
ブロック
暗号化
ブロック
1211
1段目
1236
1235
1224
レジスタ
レジスタ
1223
1214
暗号化
ブロック
暗号化
ブロック
1213
2段目
暗号文2
暗号文1

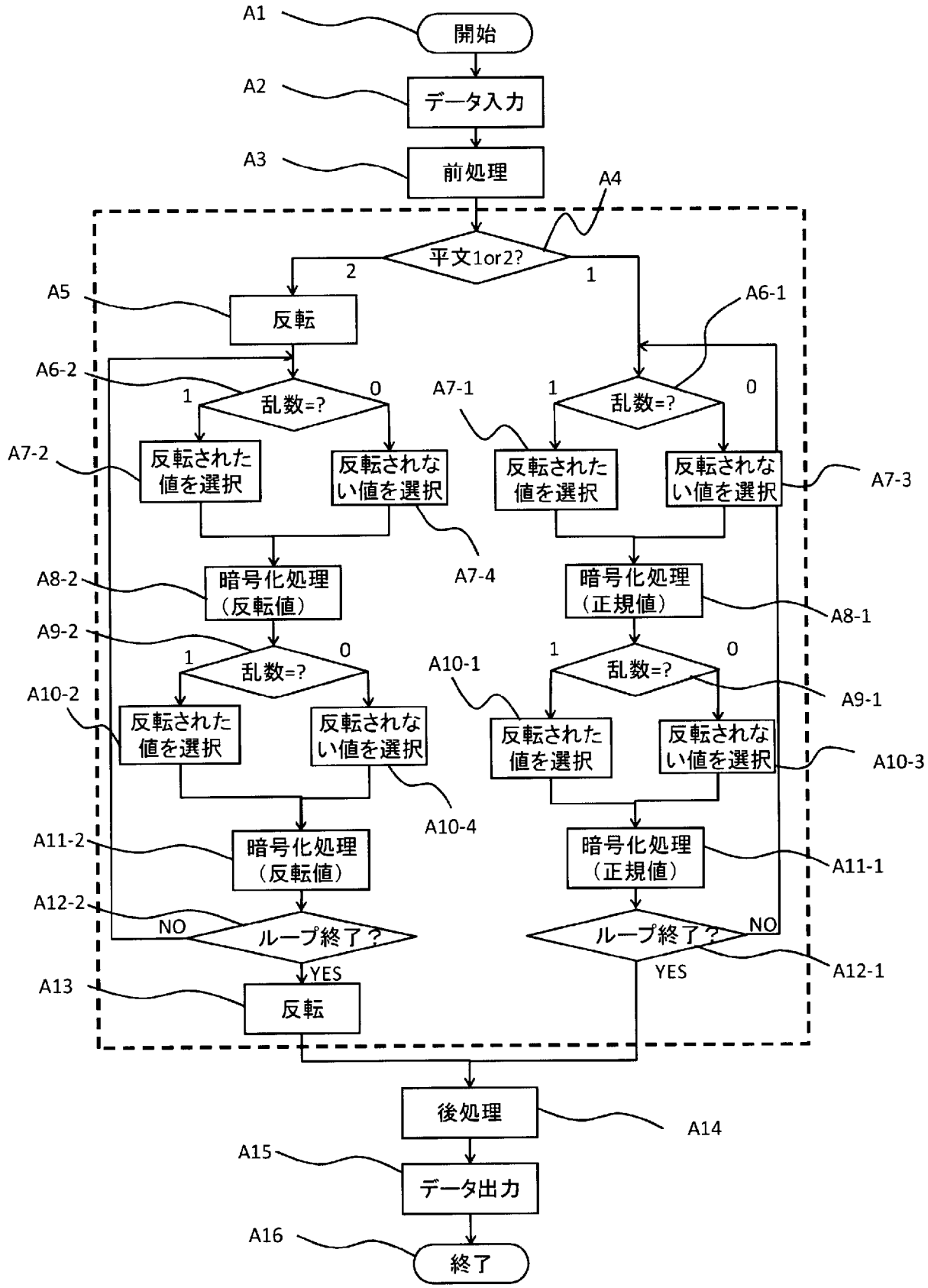
[図3]


平文2
平文1
乱数
生成部
1240
1232
1231
1234
1233
1222
レジスタ
レジスタ
1221
1212
暗号化
ブロック
暗号化
ブロック
1211
1段目
1236
1235
1224
レジスタ
レジスタ
1223
1214
暗号化
ブロック
暗号化
ブロック
1213
2段目
1238
1237
暗号文2
暗号文1

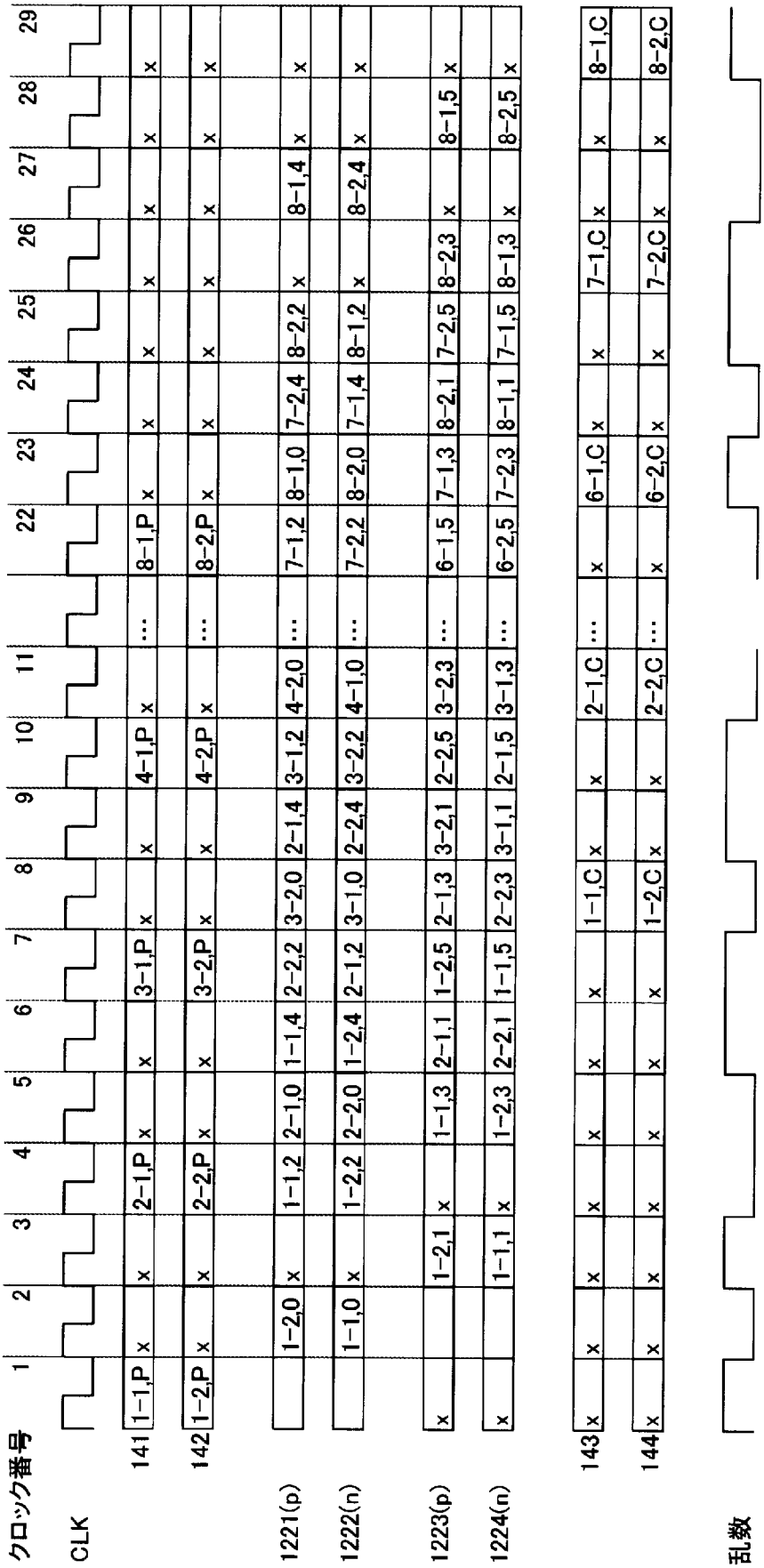
[図4]


平文2
平文1
160
タイミング調整回路
100
秘密鍵
142
入力レジスタ
入力レジスタ
141
200
鍵生成部
112
前処理部
前処理部
111
120
ループ処理部
130
後処理部
144
出力レジスタ
出力レジスタ
143
暗号文2
暗号文1

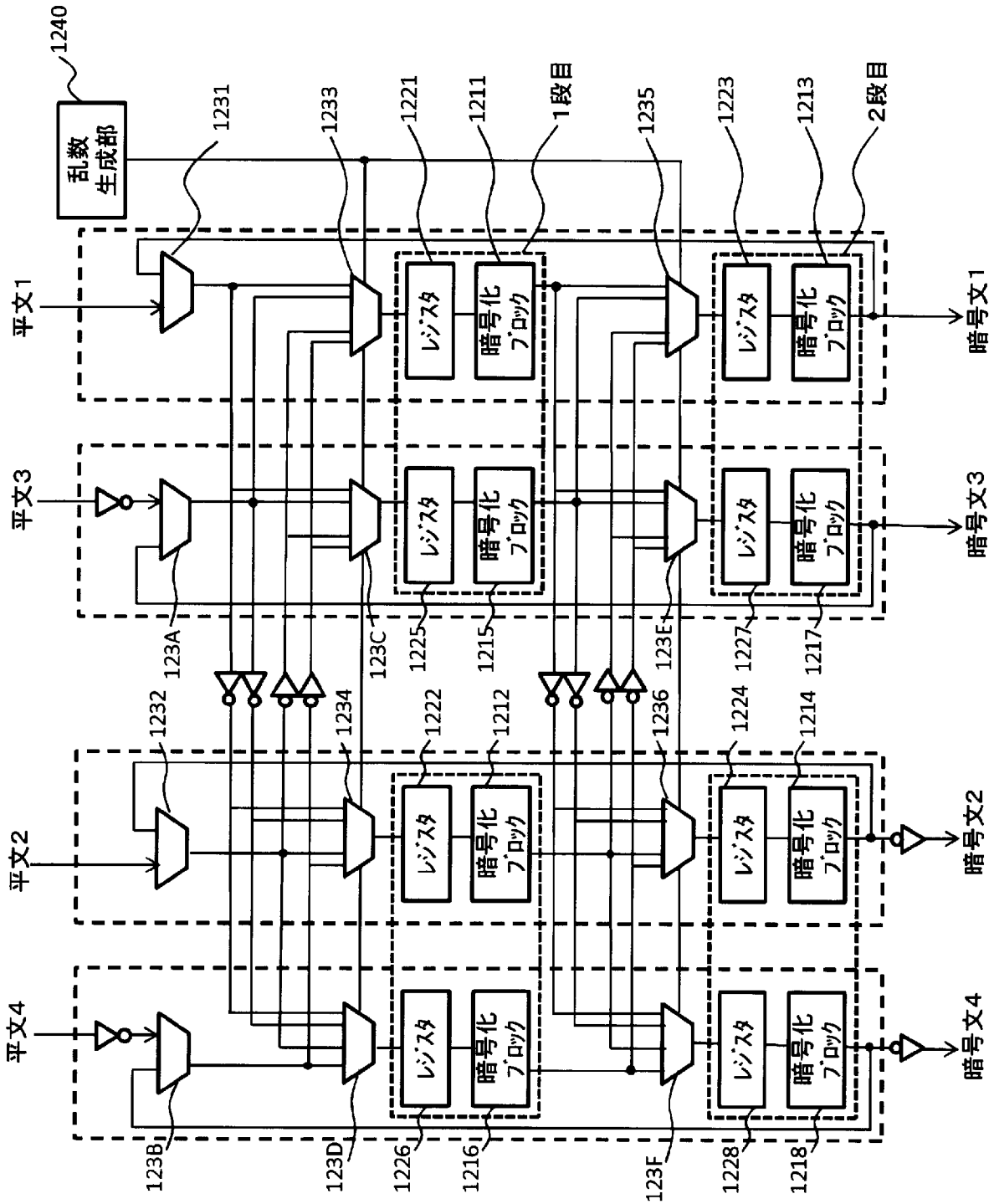
[図5]


A1
開始
A2
データ入力
A3
前処理
A4
平文1or2?
2
1
A5
反転
A6-1
A6-2
乱数=?
1
0
A7-1
乱数=?
1
0
A7-2
反転された値を選択
反転されない値を選択
反転された値を選択
反転されない値を選択
A7-3
A7-4
A8-2
暗号化処理（反転値）
暗号化処理（正規値）
A8-1
A9-2
乱数=?
1
0
A10-1
乱数=?
1
0
A9-1
A10-2
反転された値を選択
反転されない値を選択
反転された値を選択
反転されない値を選択
A10-3
A10-4
A11-2
暗号化処理（反転値）
暗号化処理（正規値）
A11-1
A12-2
NO
ループ終了？
NO
ループ終了？
YES
YES
A12-1
A13
反転
後処理
A14
A15
データ出力
A16
終了

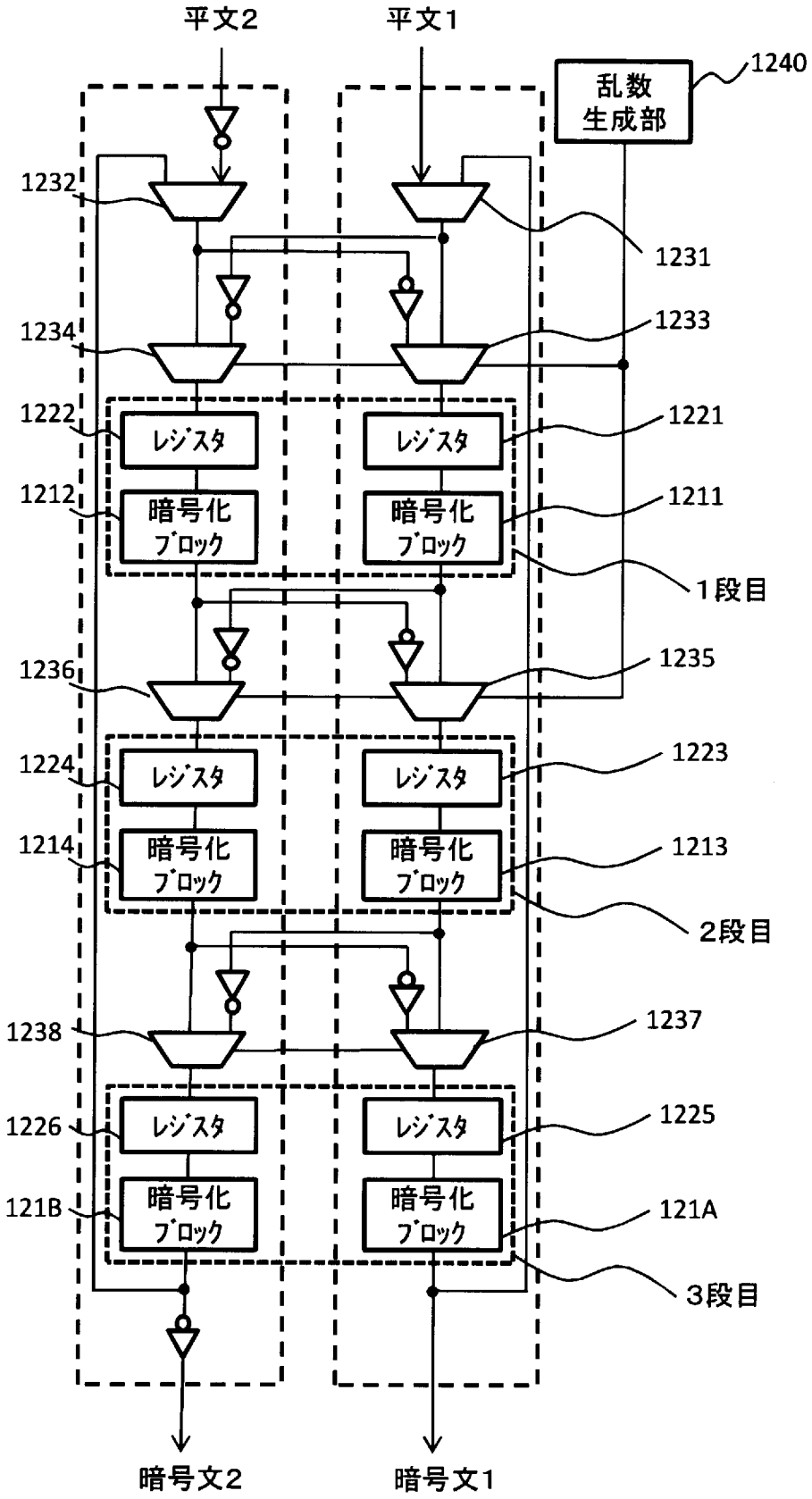
[図6]



[図7]


1240
乱数生成部
1231
1233
1221
1211
1段目
1235
1223
1213
2段目
平文1
平文3
平文2
平文4
暗号文1
暗号文3
暗号文2
暗号文4
レジスタ
暗号化ブロック
123A
123C
123E
123B
123D
123F
1232
1234
1222
1212
1236
1224
1214
1225
1215
1227
1217
1226
1216
1228
1218

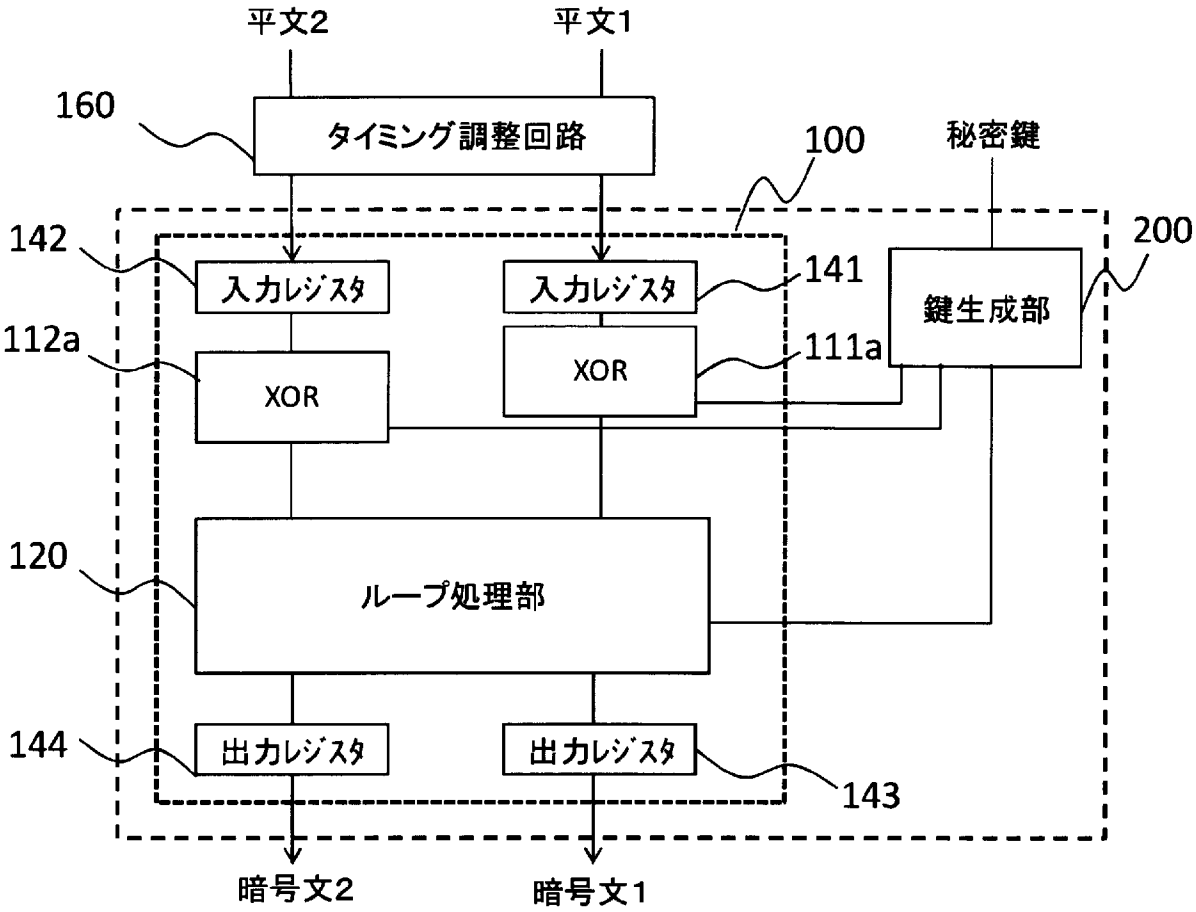
[図8]


平文2
平文1
乱数
生成部
1240
1232
1231
1234
1233
1222
レジスタ
レジスタ
1221
1212
暗号化
ブロック
暗号化
ブロック
1211
1段目
1236
1235
1224
レジスタ
レジスタ
1223
1214
暗号化
ブロック
暗号化
ブロック
1213
2段目
1238
1237
1226
レジスタ
レジスタ
1225
121B
暗号化
ブロック
暗号化
ブロック
121A
3段目
暗号文2
暗号文1

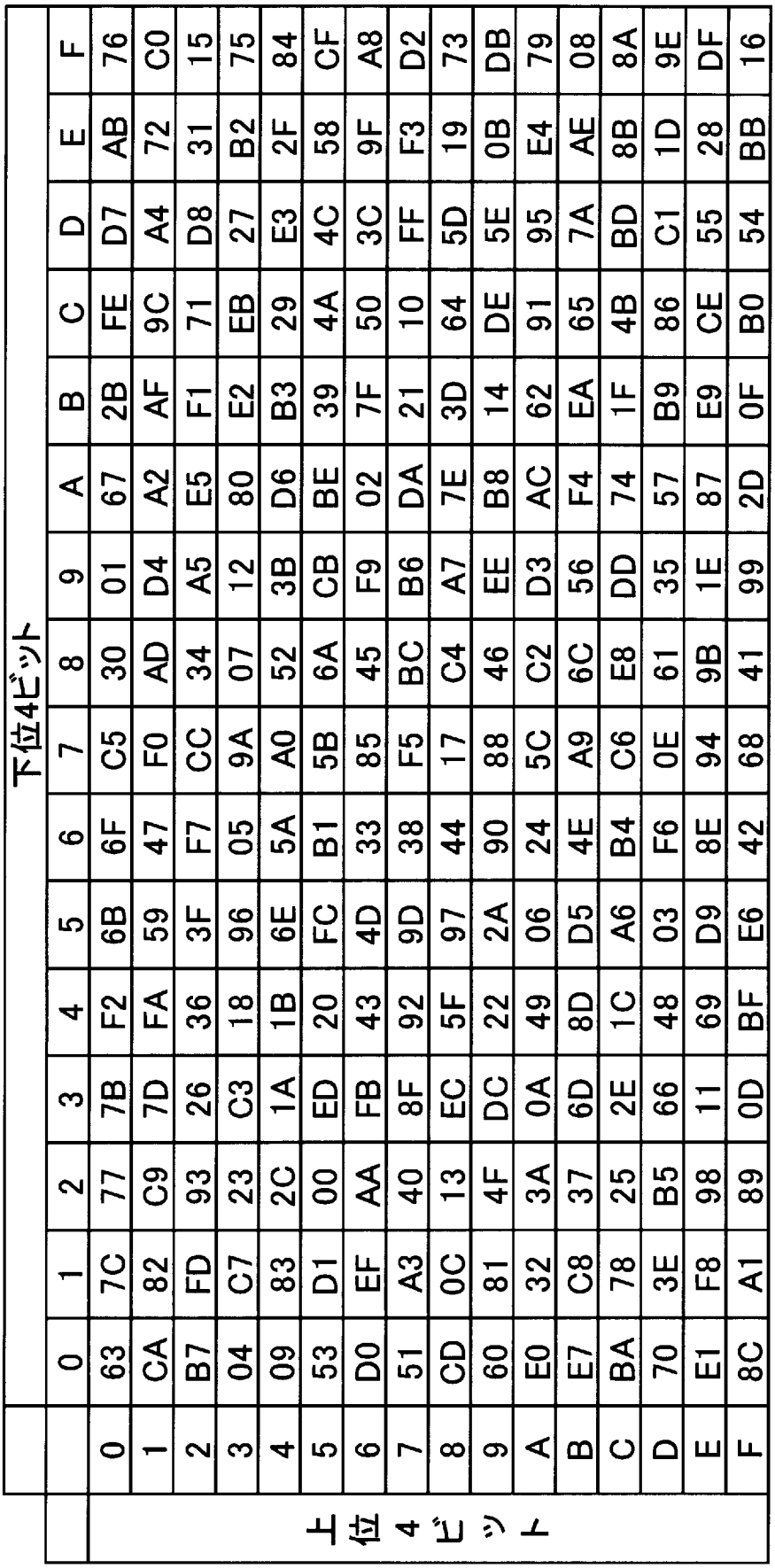
[図9]


クロック番号
1
2
3
4
5
6
7
8
9
CLK
141
1-1,P
1-2,P
2-1,P
2-2,P
x
x
3-1,P
3-2,P
x
1221(p)
x
x
x
1-1,2
1-2,2
1-1,4
2-2,2
3-1,0
3-2,0
1222(n)
x
1-1,0
1-2,0
2-1,0
2-2,0
2-1,2
1-2,4
2-1,4
2-2,4
1223(p)
x
x
x
1-2,1
1-1,3
1-2,3
2-1,3
1-2,5
3-1,1
1224(n)
x
x
1-1,1
x
2-1,1
2-2,1
1-1,5
2-2,3
2-1,5
143
x
x
x
x
x
x
x
1-1,C
1-2,C
乱数

[図10]

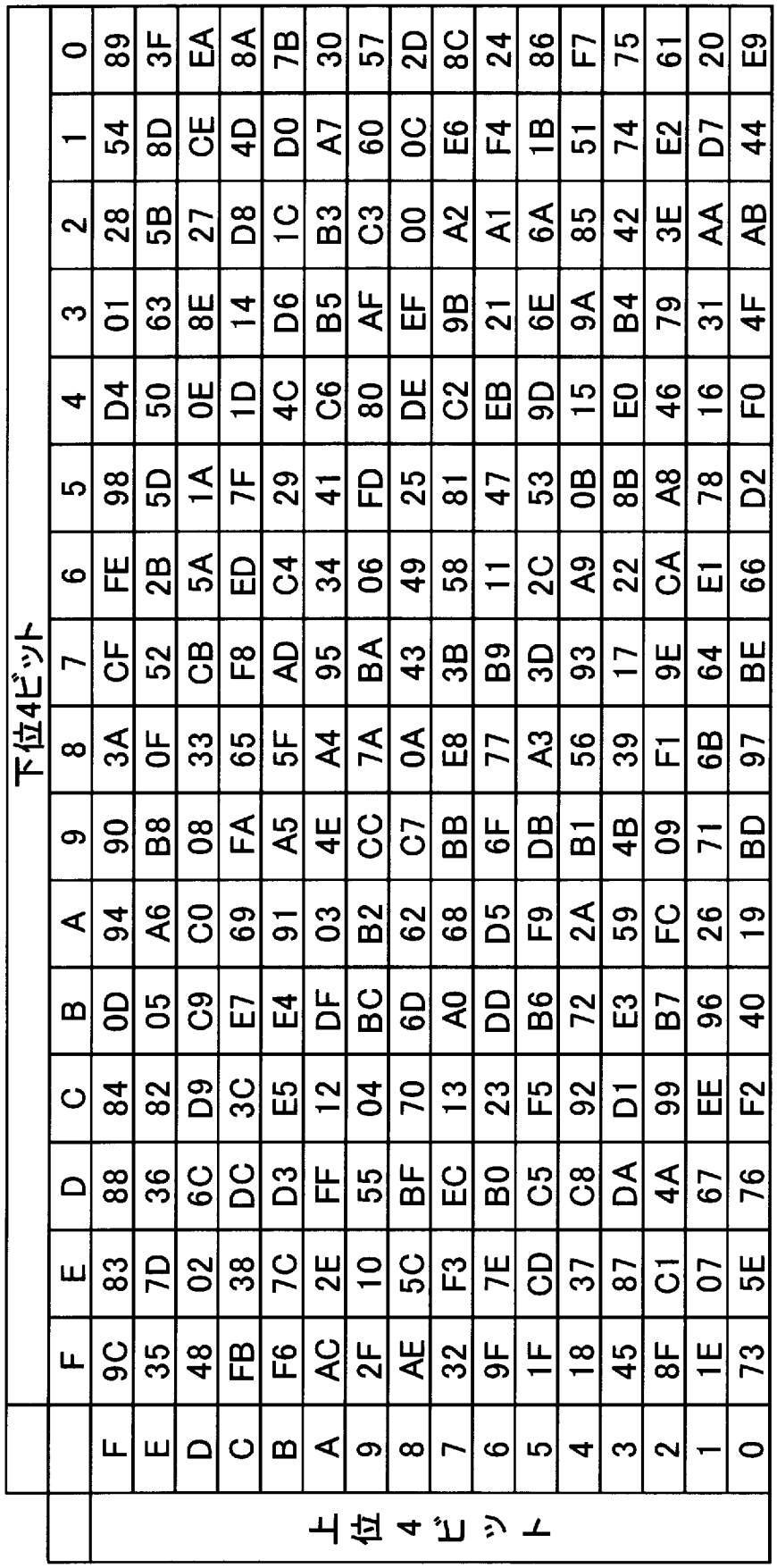

平文2
平文1
160
タイミング調整回路
100
秘密鍵
142
入力レジスタ
入力レジスタ
141
200
鍵生成部
112a
XOR
XOR
111a
120
ループ処理部
144
出力レジスタ
出力レジスタ
143
暗号文2
暗号文1

[図11]



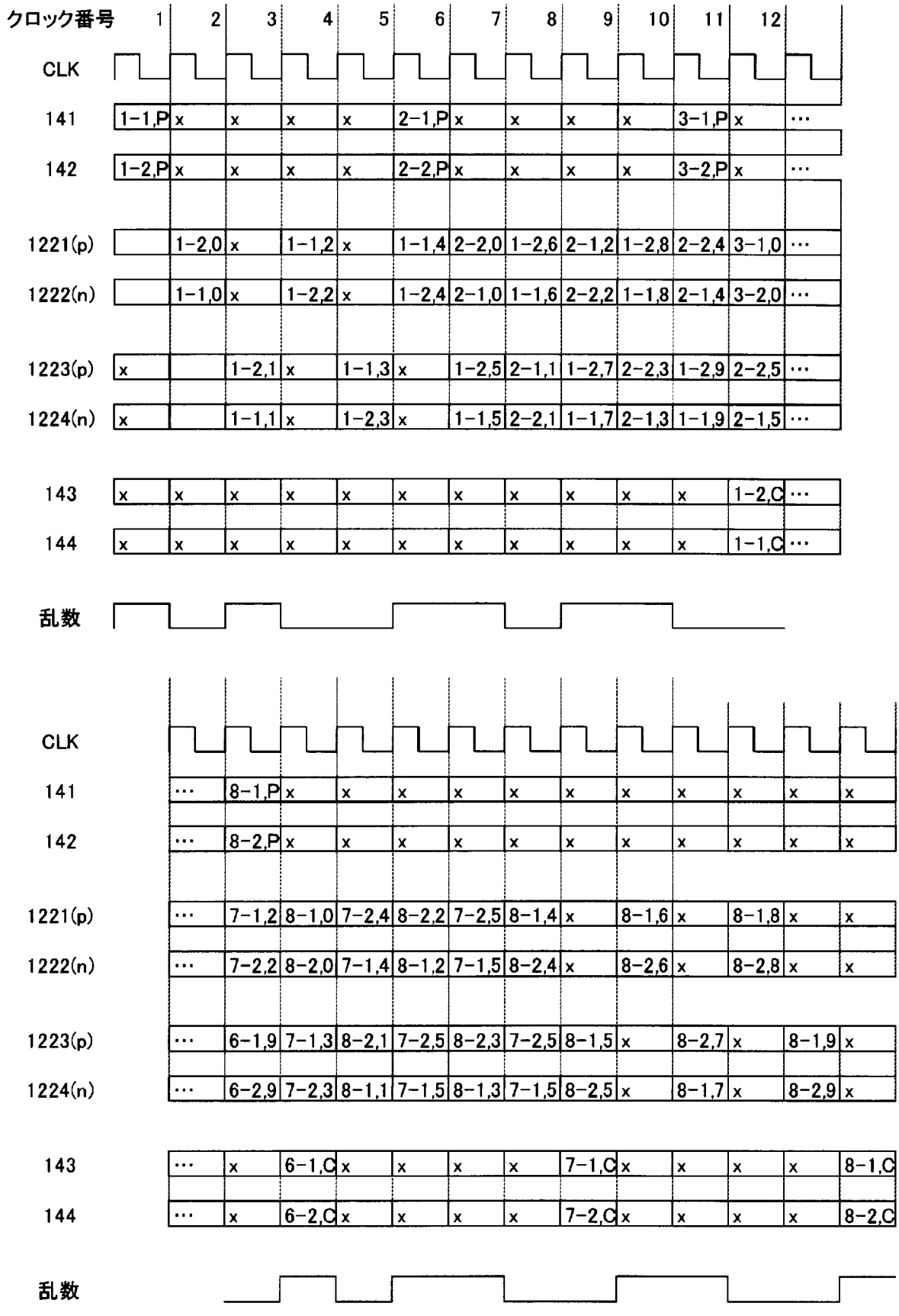
上位4ビット	下位4ビット															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29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

[図12]

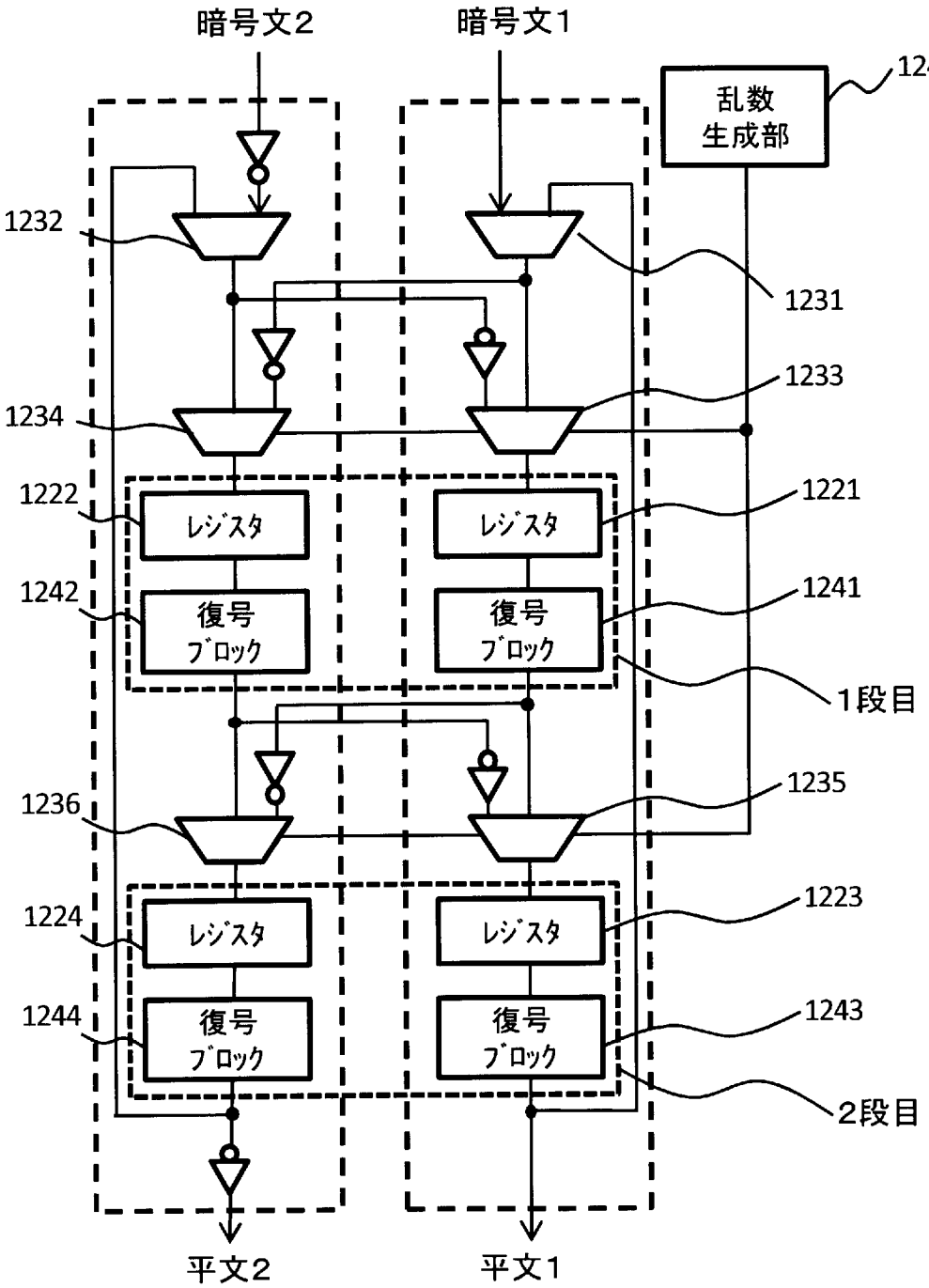


上位4ビット＼下位4ビット	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
F	9C	83	88	84	0D	94	90	3A	CF	FE	98	D4	01	28	54	89
E	35	7D	36	82	05	A6	B8	0F	52	2B	5D	50	63	5B	8D	3F
D	48	02	6C	D9	C9	C0	08	33	CB	5A	1A	0E	8E	27	CE	EA
C	FB	38	DC	3C	E7	69	FA	65	F8	ED	7F	1D	14	D8	4D	8A
B	F6	7C	D3	E5	E4	91	A5	5F	AD	C4	29	4C	D6	1C	D0	7B
A	AC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

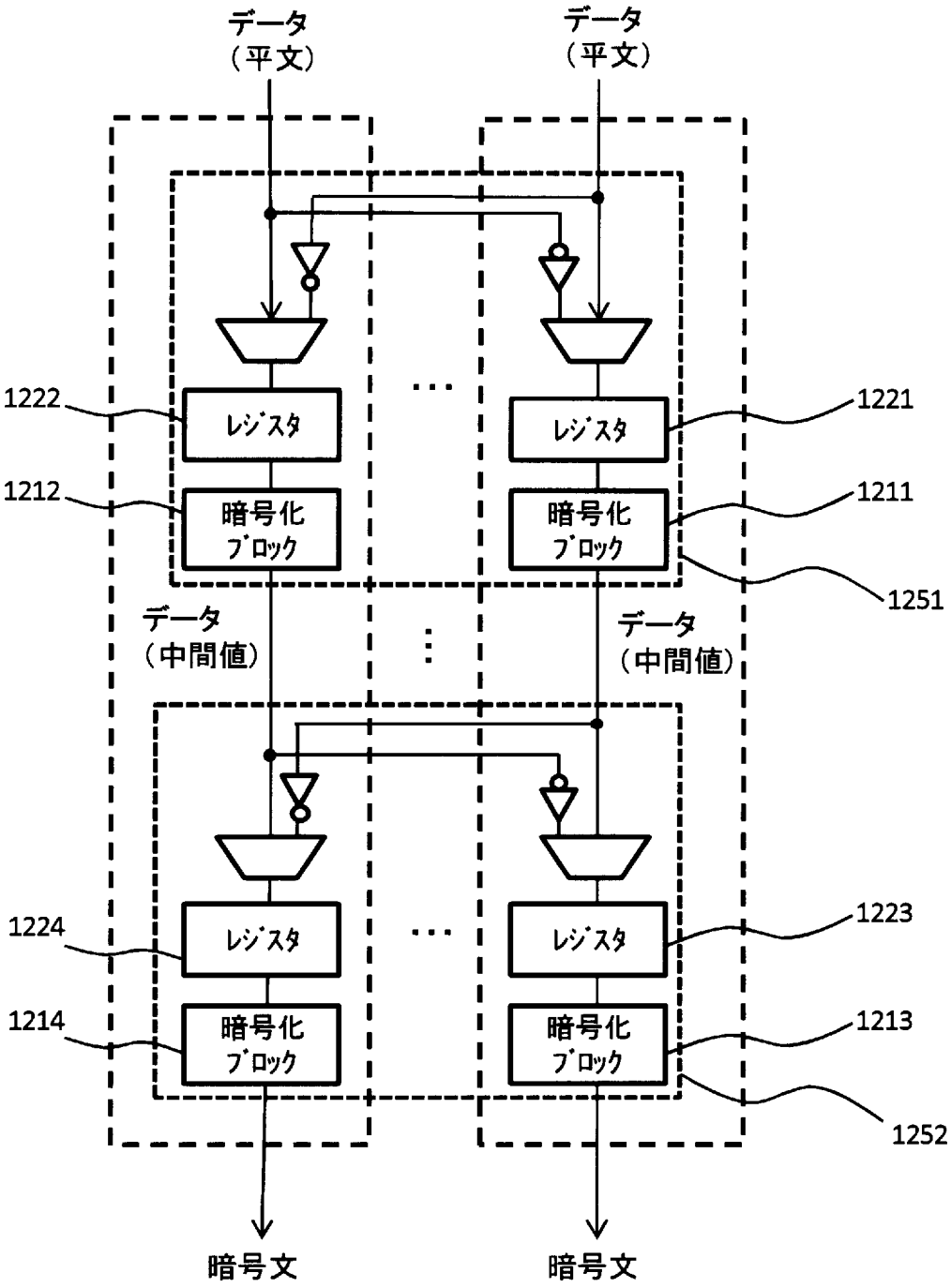
[図13]


クロック番号 1 2 3 4 5 6 7 8 9 10 11 12
CLK
141 1-1,P x x x x 2-1,P x x x x 3-1,P x …
142 1-2,P x x x x 2-2,P x x x x 3-2,P x …
1221(p) 1-2,0 x 1-1,2 x 1-1,4 2-2,0 1-2,6 2-1,2 1-2,8 2-2,4 3-1,0 …
1222(n) 1-1,0 x 1-2,2 x 1-2,4 2-1,0 1-1,6 2-2,2 1-1,8 2-1,4 3-2,0 …
1223(p) x 1-2,1 x 1-1,3 x 1-2,5 2-1,1 1-2,7 2-2,3 1-2,9 2-2,5 …
1224(n) x 1-1,1 x 1-2,3 x 1-1,5 2-2,1 1-1,7 2-1,3 1-1,9 2-1,5 …
143 x x x x x x x x x x x 1-2,C …
144 x x x x x x x x x x x 1-1,C …
乱数
CLK
141 … 8-1,P x x x x x x x x x x x
142 … 8-2,P x x x x x x x x x x x
1221(p) … 7-1,2 8-1,0 7-2,4 8-2,2 7-2,5 8-1,4 x 8-1,6 x 8-1,8 x x
1222(n) … 7-2,2 8-2,0 7-1,4 8-1,2 7-1,5 8-2,4 x 8-2,6 x 8-2,8 x x
1223(p) … 6-1,9 7-1,3 8-2,1 7-2,5 8-2,3 7-2,5 8-1,5 x 8-2,7 x 8-1,9 x
1224(n) … 6-2,9 7-2,3 8-1,1 7-1,5 8-1,3 7-1,5 8-2,5 x 8-1,7 x 8-2,9 x
143 … x 6-1,C x x x x 7-1,C x x x x 8-1,C
144 … x 6-2,C x x x x 7-2,C x x x x 8-2,C
乱数

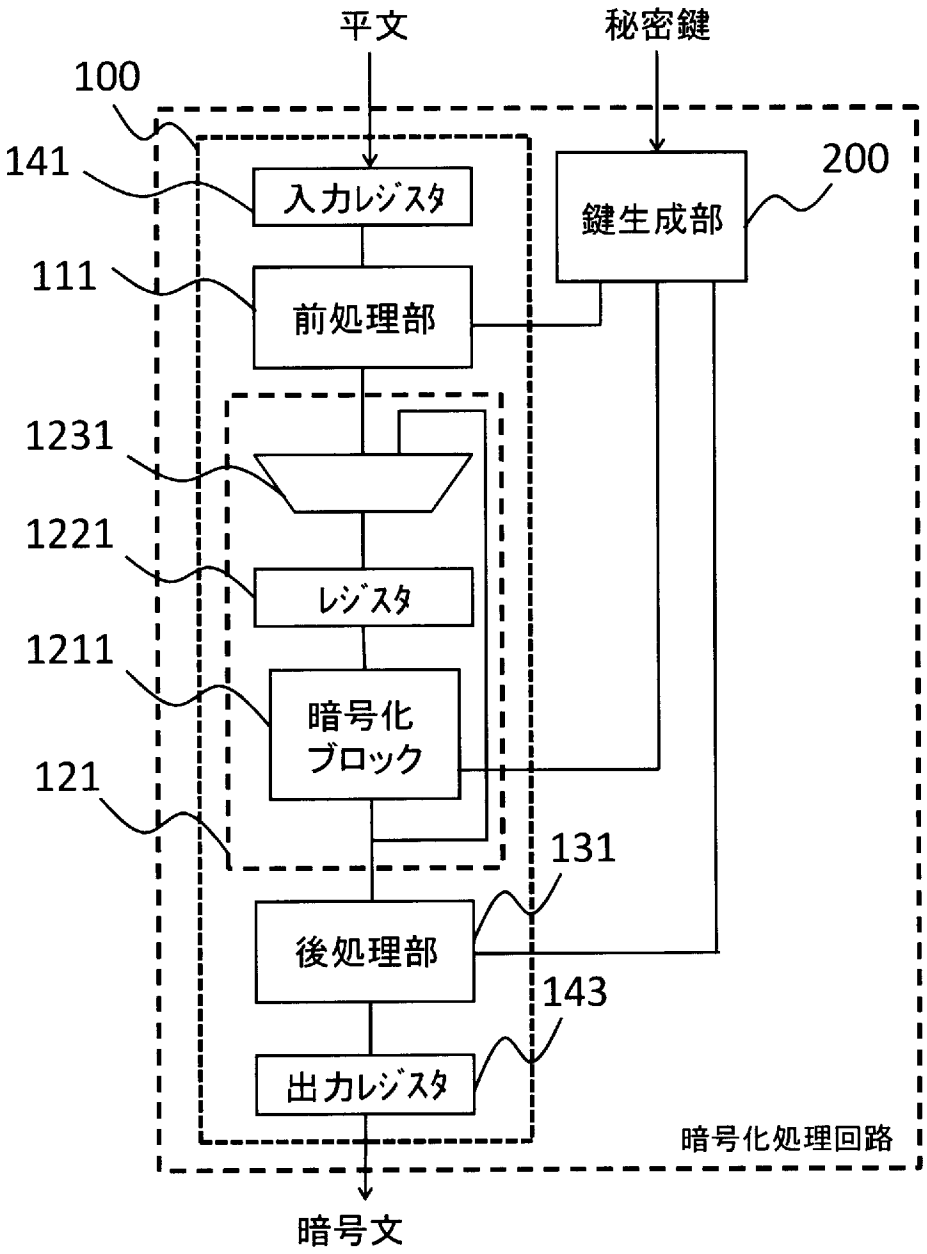
[図14]


暗号文2
暗号文1
乱数
生成部
1240
1232
1231
1233
1234
1222
レジスタ
レジスタ
1221
1242
復号
ブロック
復号
ブロック
1241
1段目
1236
1235
1224
レジスタ
レジスタ
1223
1244
復号
ブロック
復号
ブロック
1243
2段目
平文2
平文1

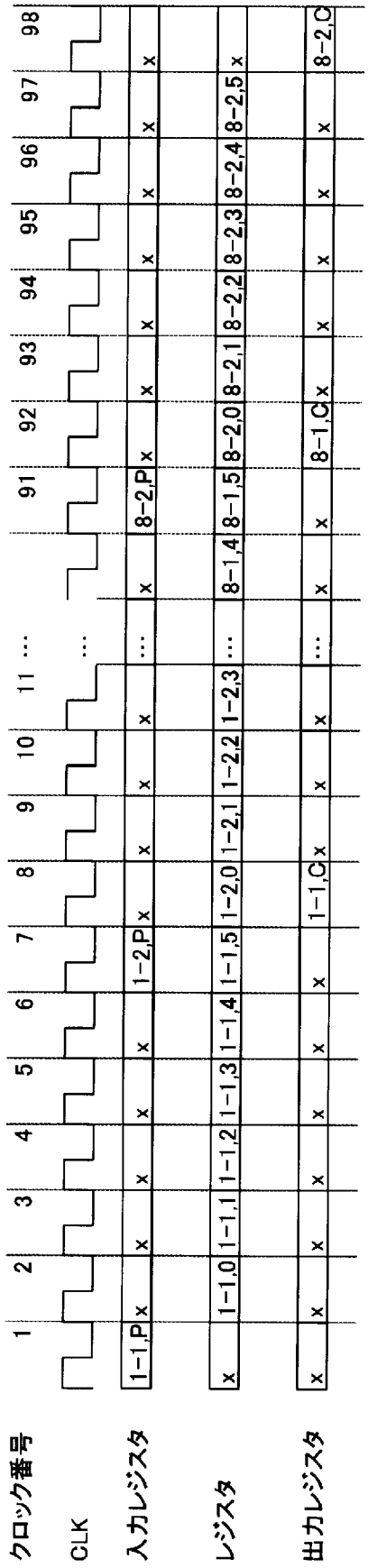
[図15]


データ
（平文）
データ
（平文）
1222
レジスタ
1221
レジスタ
1212
暗号化
ブロック
1211
暗号化
ブロック
1251
データ
（中間値）
データ
（中間値）
1224
レジスタ
1223
レジスタ
1214
暗号化
ブロック
1213
暗号化
ブロック
1252
暗号文
暗号文

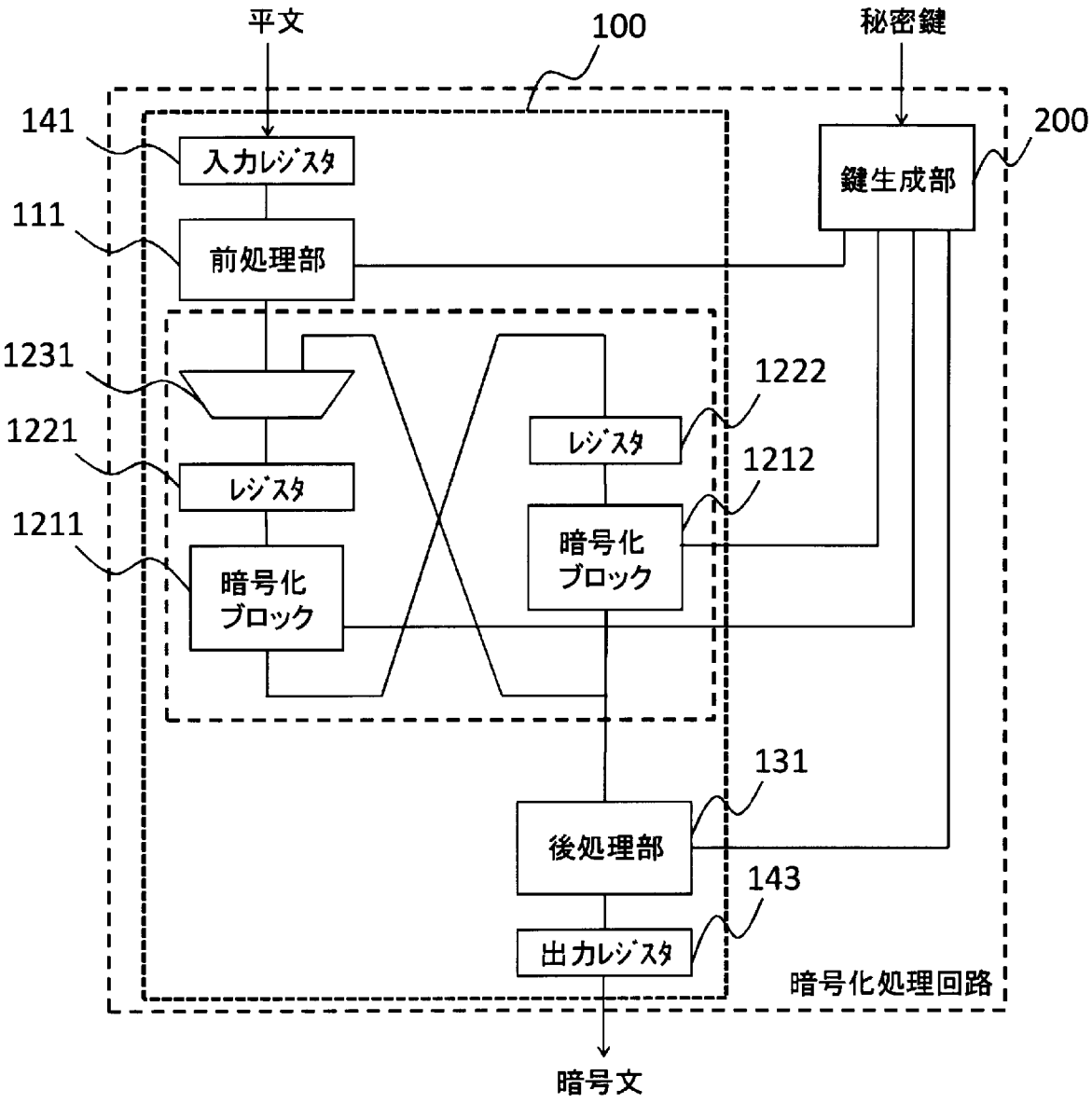
[図16]


平文
秘密鍵
100
141
入力レジスタ
200
鍵生成部
111
前処理部
1231
1221
レジスタ
1211
暗号化
ブロック
121
131
後処理部
143
出力レジスタ
暗号化処理回路
暗号文

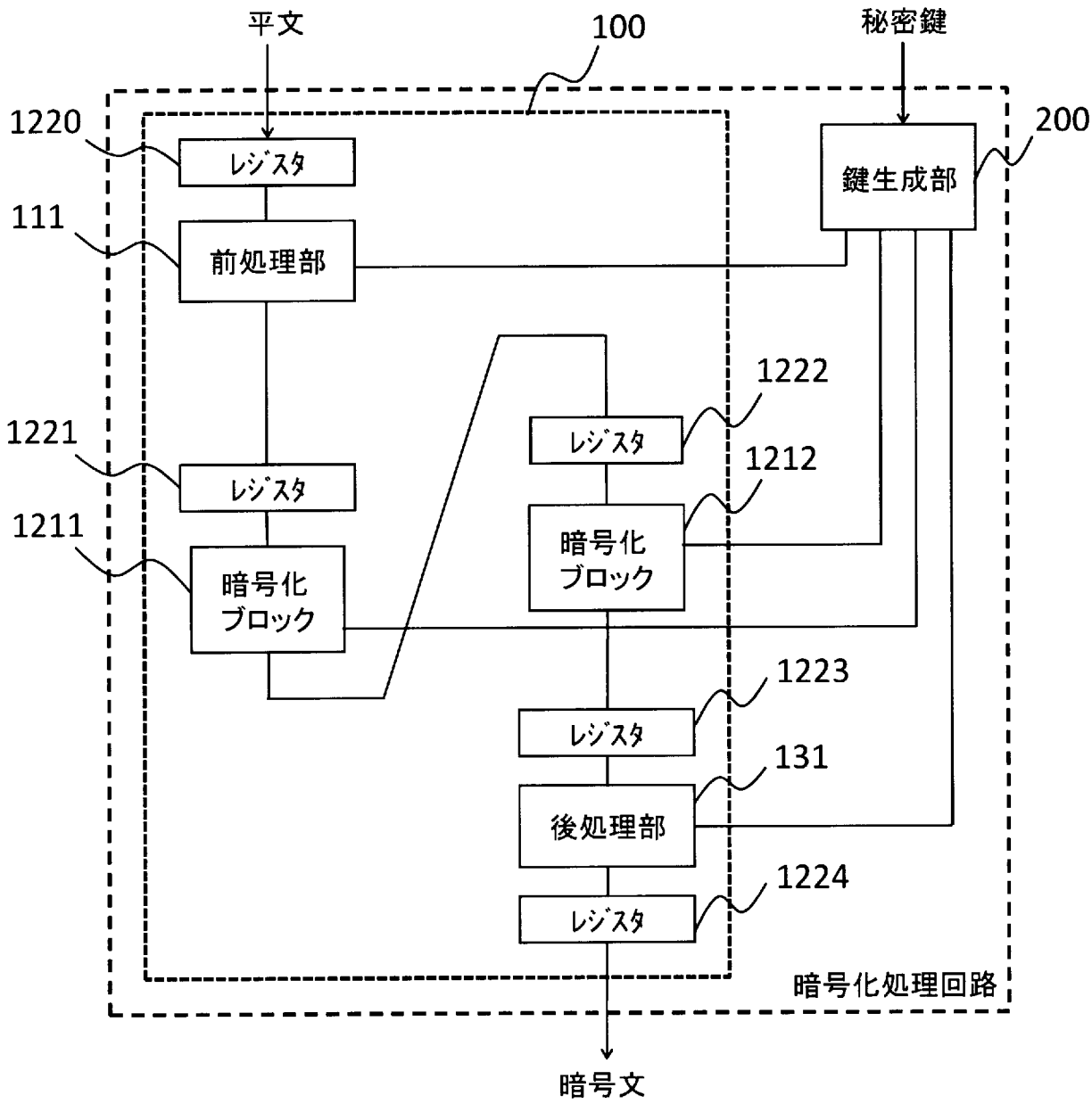
[図17]


クロック番号
CLK
入力レジスタ
レジスタ
出力レジスタ
1
2
3
4
5
6
7
8
9
10
11
…
91
92
93
94
95
96
97
98
1-1,P
1-1,0
1-1,1
1-1,2
1-1,3
1-1,4
1-1,5
1-1,C
1-2,P
1-2,0
1-2,1
1-2,2
1-2,3
8-2,P
8-2,0
8-2,1
8-2,2
8-2,3
8-2,4
8-2,5
8-1,C
8-2,C
x

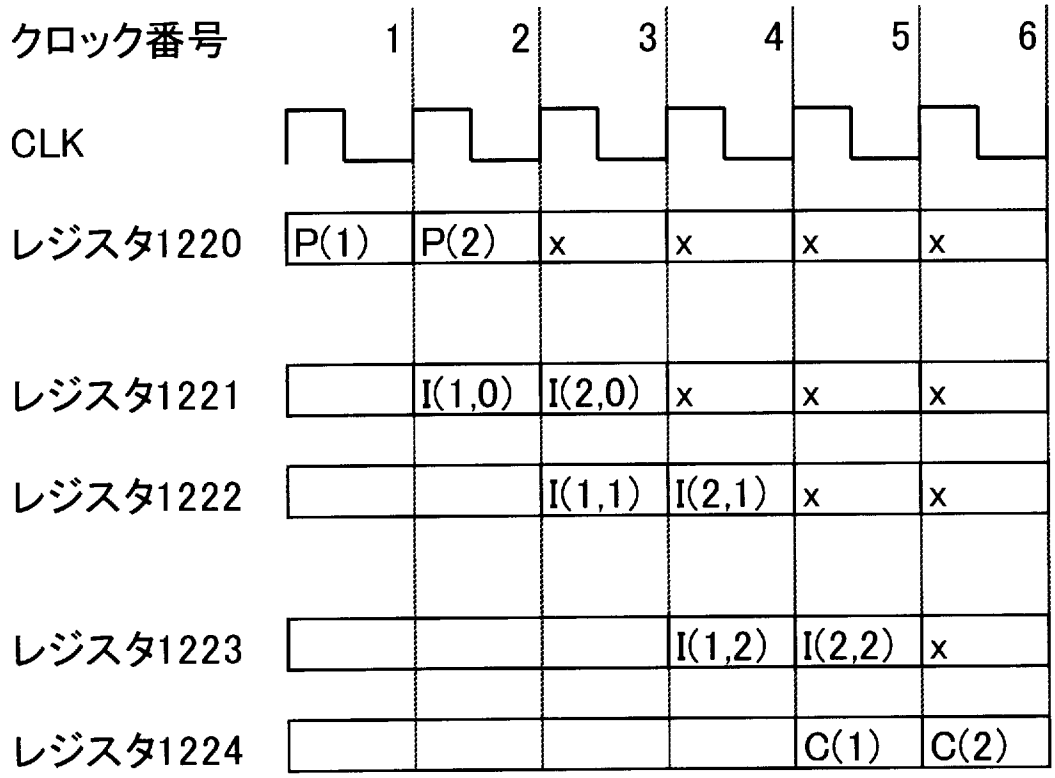
[図18]


平文
100
秘密鍵
141
入力レジスタ
200
鍵生成部
111
前処理部
1231
1222
レジスタ
1221
1212
レジスタ
暗号化
ブロック
1211
暗号化
ブロック
131
後処理部
143
出力レジスタ
暗号化処理回路
暗号文

[図19]


平文
100
秘密鍵
1220
レジスタ
200
鍵生成部
111
前処理部
1222
レジスタ
1221
レジスタ
1212
暗号化
ブロック
1211
暗号化
ブロック
1223
レジスタ
131
後処理部
1224
レジスタ
暗号化処理回路
暗号文

[図20]


クロック番号
1
2
3
4
5
6
CLK
レジスタ1220
P(1)
P(2)
x
x
x
x
レジスタ1221
I(1,0)
I(2,0)
x
x
x
レジスタ1222
I(1,1)
I(2,1)
x
x
レジスタ1223
I(1,2)
I(2,2)
x
レジスタ1224
C(1)
C(2)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/003456

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i, *H04L9/10*(2006.01)i

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)
G09C1/00, H04L9/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII), CiNii

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2005-31471 A (Sony Corp.), 03 February 2005 (03.02.2005), paragraphs [0040] to [0046], [0087] to [0103]; fig. 1 to 3, 7 & US 2005/0055596 A1 & EP 1496641 A2 & KR 10-2005-0006062 A & CN 1601578 A	1-8
Y	WO 2005/027403 A1 (Renesas Technology Corp.), 24 March 2005 (24.03.2005), column 8, line 49 to column 10, line 41; fig. 1, 2 (Family: none)	1-8
Y	JP 2011-2790 A (Sony Corp.), 06 January 2011 (06.01.2011), paragraph [0014] (Family: none)	2,3,6,7

☒ 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
26 June, 2013 (26.06.13)	09 July, 2013 (09.07.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/003456

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Shin'ichi IKENO et al., Gendai Ango Riron, 1st edition, Denshi Tsushin Gakkai, 01 September 1986 (01.09.1986), pages 43 to 46	5-8
A	JP 2002-311826 A (Hitachi, Ltd.), 25 October 2002 (25.10.2002), paragraphs [0010] to [0015], [0022] to [0023]; fig. 1 to 4, 8 & WO 2002/086846 A1	1-8
A	JP 2003-526134 A (Koninklijke Philips Electronics N.V.), 02 September 2003 (02.09.2003), paragraphs [0012] to [0014]; fig. 2 & US 6498404 B1 & EP 1057096 A2 & WO 2000/026746 A2 & CN 1292111 A	1-8
A	JP 2006-25366 A (Sony Corp.), 26 January 2006 (26.01.2006), paragraphs [0084] to [0089]; fig. 11 (Family: none)	1-8

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／００３４５６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i, H04L9/10(2006.01)i

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））

Int.Cl.　G09C1/00, H04L9/10

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	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３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）

JSTPlus/JMEDPlus/JST7580(JDreamIII), CiNii

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
Y	JP 2005-31471 A（ソニー株式会社）2005.02.03, 段落【００４０】－【００４６】,【００８７】－【０１０３】,【図１】－【図３】,【図７】 & US 2005/0055596 A1 & EP 1496641 A2 & KR 10-2005-0006062 A & CN 1601578 A	１－８
Y	WO 2005/027403 A1（株式会社ルネサステクノロジ）2005.03.24, 第８欄第４９行－第１０欄第４１行, [図１], [図２]（ファミリーなし）	１－８

☑　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矛盾するものではなく、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
２６．０６．２０１３	０９．０７．２０１３

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３１４６
松平　英
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　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
Ｙ	JP 2011-2790 A（ソニー株式会社）2011.01.06，段落【００１４】（ファミリーなし）	２，３，６，７
Ｙ	池野　信一　他，現代暗号理論，初版，社団法人電子通信学会，1986.09.01，p.43-46	５－８
Ａ	JP 2002-311826 A（株式会社日立製作所）2002.10.25，段落【００１０】－【００１５】，【００２２】－【００２３】，【図１】－【図４】，【図８】 & WO 2002/086846 A1	１－８
Ａ	JP 2003-526134 A（コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ）2003.09.02，段落【００１２】－【００１４】，【図２】 & US 6498404 B1 & EP 1057096 A2 & WO 2000/026746 A2 & CN 1292111 A	１－８
Ａ	JP 2006-25366 A（ソニー株式会社）2006.01.26，段落【００８４】－【００８９】，【図１１】（ファミリーなし）	１－８