

(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
2009年11月26日(26.11.2009)

PCT

(10) 国際公開番号
WO 2009/142190 A1

- (51) 国際特許分類:
H03M 13/01 (2006.01) H04L 9/10 (2006.01)
G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2009/059167
- (22) 国際出願日: 2009年5月19日(19.05.2009)
- (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 2008-130361 2008年5月19日(19.05.2008) JP
- (71) 出願人 (米国を除く全ての指定国について): 独立行政法人産業技術総合研究所(NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY) [JP/JP]; 〒1008921 東京都千代田区霞が関1丁目3番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 佐藤 証 (SATO Akashi) [JP/JP]; 〒1008921 東京都千代田区霞が関1丁目3番1号 独立行政法人産業技術総合研究所内 Tokyo (JP). 菅原 健(SUG-

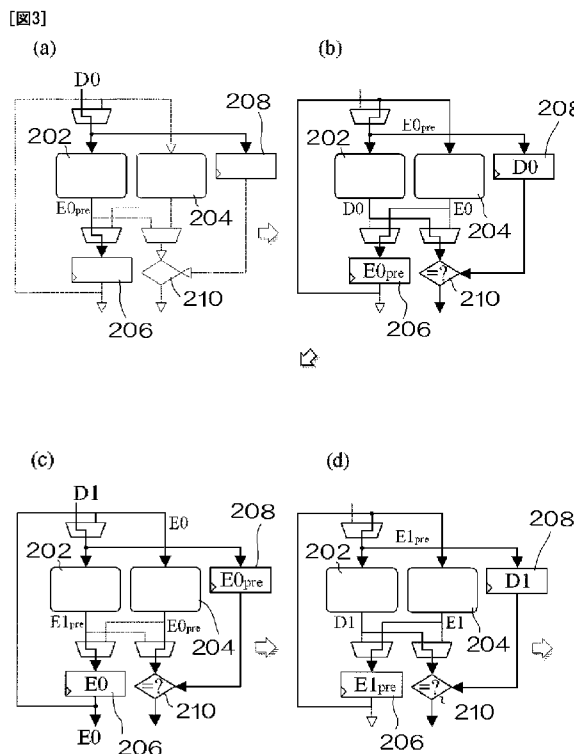
AWARA Takeshi) [JP/JP]; 〒9808577 宮城県仙台市青葉区片平2丁目1番1号 国立大学法人東北大学内 Miyagi (JP). 本間 尚文(HOMMA Naofumi) [JP/JP]; 〒9808577 宮城県仙台市青葉区片平2丁目1番1号 国立大学法人東北大学内 Miyagi (JP). 青木 孝文(AOKI Takafumi) [JP/JP]; 〒9808577 宮城県仙台市青葉区片平2丁目1番1号 国立大学法人東北大学内 Miyagi (JP).

- (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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア

[続葉有]

(54) Title: CODING OR DECODING CIRCUIT STRUCTURE WITH ERROR DETECTING CAPABILITY

(54) 発明の名称: 誤り検出機能を備える符号化又は復号処理のための回路構成



(57) Abstract: Provided are a coding circuit and a decoding circuit that reliably detect errors in operation mode, and reduce penalties to the circuit scale and operational speed. When a coding process is executed at one stage, the coding circuit and decoding circuit execute a decoding process, at a preceding stage, as verification of the coding process in a directly previous cycle in parallel. Decoded data is compared with data to be coded in the previous cycle to check if they match. In the next cycle, data coded earlier at the stage is decoded, and is checked against data before the coding to check if they match. A coding process is performed on the previously coded data at the next stage while new data is input to be subjected to a coding process at the preceding stage in parallel.

(57) 要約: 符号化・復号回路の動作時のエラー検出を確実に、かつ回路規模と動作速度に対するペナルティを軽微なものと符号化回路及び復号回路が提供される。符号化回路及び復号回路は、あるステージにおいて符号化処理が実行されている時、その1つ前段のステージでは、直前のサイクルにおける符号化処理の検証としての復号処理が並行して実行される。復号されたデータは、直前のサイクルにおいて符号化の対象となったデータと比較されて、一致しているかどうか調べられる。その次のサイクルでは、当該ステージにおいて先に符号化されたデータが復号され、符号化される前のデータと一致しているかどうか調べられる。並行して、先に符号化されたデータに対して次段のステージで符号化処理が進められ、前

段のステージには新たなデータが入力されて符号化処理が行われる。



(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ
(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, SE, SI, SK, TR), OAPI (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD,
TG).

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：

誤り検出機能を備える符号化又は復号処理のための回路構成

技術分野

[0001] 本発明は、符号化・復号処理のための回路構成であって、誤り検出能力を有する新規な回路構成に関するものである。

背景技術

[0002] VLSIの高速化・高集積化技術の進歩による情報機器の高性能化と、ブロードバンド・ネットワークの急速な普及にともなって、業務だけでなく日常生活のあらゆる場面で大量のデータをやりとりするようになっている。データバンド幅の拡大や記憶デバイス容量の削減のためにはデータ圧縮技術が用いられ、また誤り検出・訂正符号や暗号技術によって、情報の信頼性と通信の安全性の確保が行われている。データ圧縮技術は音声画像といったデジタルコンテンツへの利用が盛んであるが、このようなデータは多少のエラーが発生しても大きな問題とならず機密性も低い場合が多い。それに対して、サーバーからダウンロードして使用するプログラムや金銭情報やプライバシー情報などは、誤りを生じたり、内容が漏洩したり、すると大きな損害を生じる恐れがある。

[0003] 誤り検出・訂正符号は、主に通信路や記録メディア上で発生したエラーを検出・訂正したり、送信先に再送を求めたりするといった用途で用いられる。従って、その符号化あるいは復号処理の装置自体にエラーが発生した場合には、元々訂正不可能なデータが生成されてしまい、エラーが検出できないといったことが起きる。暗号技術も、送信あるいは記録されるデータの安全性を確保することはできても、暗号装置の故障によるデータの損失や、それを利用した攻撃に対処することはできない。そこで、データを符号化・復号する装置自体の信頼性を確保する技術が必要となる。

[0004] 図1は、符号化の過程で回路に発生するエラーを検出する従来の方式を説

明するための図である。復号処理の時のエラー検出については、図の符号化と復号処理を互いに置き換えて考えればよい。図 1 (a) により説明する方式では、入力されたデータを左側のパスで符号化した後に、その出力のビット幅以下のパリティを生成する。それと同時に期待値回路ではパリティを直接生成し、2つのパリティが一致しているかどうかでエラーの発生を検出する。期待値回路は符号化後にパリティを生成するよりも小さい回路となるが、パリティによる比較なので、エラーの発生を全て検出できるわけではない。

[0005] 図 1 (b) により説明する方式は、同じ符号化回路を 2 つ用意して、両方で同時に同じ演算を行って、その結果を比較する方式である。当然のことながら、回路のコストは 2 倍に増加する。図 1 (c) により説明する方式では、符号化と復号処理が別の回路ブロックでサポートされている。入力データをレジスタ 2 にストアするのと同時に、符号化したデータをレジスタ 1 にストアする。次のサイクルで、新しい入力データの符号化が可能であり、それと並行してレジスタ 1 のデータを復号処理し、レジスタ 2 にストアしたデータと比較してエラー検出を行う。しかし、符号化と復号処理の回路は演算コンポーネントを共有している場合が多く、その場合には適用することができない。また、独立していた場合でも、別のデータに対して符号化と復号処理を同時に行うことはできなくなってしまう。例えばデータの双方向通信を行うときに、符号化と復号処理を同時行うことができないため、結局、回路のコストは 2 倍に増加していることに等しい。

[0006] 図 1 (d) により説明する方式は、一つの符号化回路で同じ処理を 2 回繰り返してその結果を比較するものである。まず、入力データを符号化して結果をレジスタ 1 にストアする。次のサイクルでも同じデータをもう一度符号化して、その結果がレジスタ 1 にストアしたデータと一致するかどうかを検出する。この方式は、電源ノイズなどに起因する一時的なエラーは検出できるものの、トランジスタや配線の欠陥によって常に同じエラーが発生する場合は検出できないという欠点を持つ。また、同じ符号化の処理を 2 回繰り返

すため動作速度は $1/2$ に低下してしまう。

[0007] 図1(e)により説明する方式は、符号化と復号処理が同じ回路ブロックで処理される方式である。入力データをレジスタ2にストアすると同時に、まず、符号化したデータをレジスタ1に保持する。次のサイクルではレジスタ1のデータを復号処理してレジスタ2にストアしているデータと比較する。2サイクルで1つのデータしか処理できないので、エラー検出を行わない場合に対してスループットが $1/2$ になるのは図1(d)の場合と同様である。しかし、同じ演算ブロックを使用しているものの、符号化と復号処理といった異なる処理を行い、元のデータが復元できることを確認しているため、図1(d)のように回路の欠陥によって検出不可能なエラーが起こる可能性は低い。

[0008] 図1(f)により説明する方式は、図1(d)の場合の符号化の回路部を2分割してレジスタを挟み、パイプライン処理する実装である。2つのレジスタの前後で2回結果の比較を行っている。パイプライン化したことで動作周波数が向上し、エラー検出による速度へのペナルティが改善される。しかしながら、図1(d)の場合と同様に、回路の欠陥があった場合にエラーを検出できないという問題は解決されていない。

[0009] 以上のように、従来における回路動作時のエラー検出手法は、エラーの検出率に問題があったり、回路規模が2倍あるいは動作速度が $1/2$ になったりしてしまうといった欠点を持っている。

[0010] 上記のエラー検出方式に準じた暗号回路は、非特許文献1にまとめられている。また特許文献1及び2において、暗号回路の実装方法が開示されているが、これは演算部ではなく、データレジスタに誤りエラー検出・訂正回路を付加する回路構成である。

先行技術文献

非特許文献

[0011] 非特許文献1: T. G. Malkin, et al., "A Comparative Cost/Security Analysis of Fault Attack Countermeasures," FDTG2006, LNCS 4236, pp. 159-

172, Oct. 2006.

特許文献

[0012] 特許文献1：特開2007-174024号公報

特許文献2：特開2007-325219号公報

発明の開示

発明が解決しようとする課題

[0013] 以上のような背景の下、本発明は、符号化・復号処理の回路の動作時のエラー検出を確実にを行い、かつ回路規模と動作速度に対するペナルティを軽微なものとする新たな手法を開発すべくなされたものである。

課題を解決するための手段

[0014] 本発明は、符号化及び復号処理をパイプライン処理で行う方式とする回路構成とし、各パイプライン・ステージは、符号化処理の一部である部分符号化処理だけでなく、その一部処理の逆処理となる部分復号処理を実行する部分符号化・部分復号ブロックを含む回路構成とし、符号化回路及び復号回路を構成する。以下では混乱をきたさない範囲で、部分符号化及び部分復号処理をそれぞれ単純に、符号化及び復号と記す場合がある。

[0015] 本発明の符号化回路における具現化形態では、あるステージにおいて符号化処理が実行されている時、その1つ前段のステージでは、直前のサイクルにおける符号化処理の検証としての復号処理が並行して実行される。復号処理されたデータは、直前のサイクルにおいて符号化の対象となったデータと比較されて、一致しているかどうか調べられる。その次のサイクルでは、前回符号化処理を行った同じステージにおいて、先に符号化されたデータが復号処理され、符号化される前のデータと一致しているかどうか調べられる。並行して、当該先に符号化されたデータに対して、次段のステージで符号化処理が進められ（次段のステージがない場合には回路から出力され）、前段のステージには新たなデータが入力されて符号化処理が行われる。

[0016] 本発明の復号回路における具現化形態では、上記の符号化回路における符

号化と復号処理の順番や役割が逆転する。

- [0017] すなわち、本発明に基づく符号化・復号回路は、複数の符号化・復号ブロックからなるパイプライン処理回路として構成され、各符号化・復号ブロックは、1サイクル毎に、符号化処理と復号処理を切り替える。従って、全体としては、各サイクルにおいてデータの処理が進行するだけでなく、前のサイクルにおける処理の検証も同時に行われる。符号化回路として動作する場合には、復号処理が検証のために行われ、復号回路として動作する場合には、符号化が検証のために行われる。
- [0018] 本発明によれば、符号化及び復号処理を分割して、パイプライン処理すると共に、処理を進めるのと並行して検証処理も行うため、処理の途中でエラー検出を行うことができる。このような能力は、特に、故意にエラーを発生させて情報を盗むような攻撃、例えば、共通鍵暗号に対する故障利用解析攻撃に対する防御に有効であり、エラーを検出した場合に直ちに処理を停止させるなどの目的に利用することができる。
- [0019] また、本発明においては、符号化と復号処理が同じ回路ブロックで処理されるものの、符号化と復号処理といった異なる処理を行い、元のデータが復元できることを確認しているため、回路の欠陥によって検出不可能なエラーが起こる可能性は非常に低い。これらのことから、本発明による誤り検出機能は、非常に強力かつ信頼性の高いものであると言える。
- [0020] 一方、本発明による回路構成では、各符号化・復号ブロックの処理を1サイクル毎に符号化と復号処理とで切り替えるため、データの入力は多くとも2サイクルに1回しか行うことができない。しかしながら、演算ブロックを複数のブロックに分割し、パイプライン処理することで、動作周波数を向上させることができる。このため、処理性能の低下は限定的である。回路規模の点でも、もともと一つであった演算ブロックを複数に分割しただけであるので、回路規模はそれほど増加しない。付加回路も、パイプライン処理用のレジスタとセレクタ、そしてエラー検出用の比較器だけでよい。
- [0021] このため、本発明によれば、強力かつ信頼性の高い誤り検出機能を回路に

持たせつつ、回路規模と動作速度への悪影響を最小限に抑えることができる。

[0022] また、ここで開示される回路構成は、符号化・復号の演算方式に依存した構成ではないため、様々な方式に対して広く適用することが可能である。

[0023] 本発明の実施形態は、次のような符号化回路を含む。この回路は、ステージX及び前記ステージXの次のステージであるステージYを少なくとも含む複数のステージのパイプライン処理によって符号化処理を行う符号化回路であって、

前記複数のステージの各々は、符号化処理の一部である部分符号化処理及び該一部の逆処理となる部分復号処理を実行しうる部分符号化・部分復号ブロックを含み、

或るサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルの1つ前のサイクルにおいて前記ステージXで部分符号化されたデータが部分符号化され、
 - ・ 前記ステージXにおいて、前記1つ前のサイクルにおいて前記ステージXで部分符号化されたデータが部分復号され、
 - ・ 予め記憶されていた、前記1つ前のサイクルにおいて前記ステージXで部分符号化される前のデータと、前記部分復号されたデータとが比較され、
- 前記或るサイクルの次のサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルにおいて前記ステージYで部分符号化されたデータが部分復号され、
 - ・ 予め記憶されていた、前記或るサイクルにおいて前記ステージYで部分符号化される前のデータと、前記ステージYで部分復号されたデータとが比較され、
 - ・ 前記ステージXにおいて、別のデータが部分符号化される、
- 回路として構成される符号化回路である。

[0024] また本発明の実施形態は、次のような復号回路を含む。この回路は、ステージX及び前記ステージXの次のステージであるステージYを少なくとも含

む複数のステージのパイプライン処理によって復号処理を行う復号回路であって、

前記複数のステージの各々は、復号処理の一部である部分復号処理及び該一部の逆処理となる部分符号化処理を実行しうる部分符号化・部分復号ブロックを含み、

或るサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルの1つ前のサイクルにおいて前記ステージXで部分復号されたデータが部分復号され、

- ・ 前記ステージXにおいて、前記1つ前のサイクルにおいて前記ステージXで部分復号されたデータが部分符号化され、

- ・ 予め記憶されていた、前記1つ前のサイクルにおいて前記ステージXで部分復号される前のデータと、前記部分符号化されたデータとが比較され、

前記或るサイクルの次のサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルにおいて前記ステージYで部分復号されたデータが部分符号化され、

- ・ 予め記憶されていた、前記或るサイクルにおいて前記ステージYで部分復号される前のデータと、前記ステージYで部分符号化されたデータとが比較され、

- ・ 前記ステージXにおいて、別のデータが部分復号される、

回路として構成される復号回路である。

[0025] 本発明は、デジタルデータを扱う一般及び業務用の電子情報機器全般に対して有用であり、特に、デジタルコンテンツや暗号技術、情報セキュリティに関係する情報機器に対して有用である。従って本発明の実施形態は、単に、符号化回路や復号回路及びこれらの回路を含む半導体チップを含むだけでなく、これらの回路を含む電子機器、例えば、パーソナルコンピュータや通信機器、デジタルTV・レコーダ、ICカードやネットワーク機器等をも含むものである。また、本明細書に開示される技術思想を具体化した符号化回路や復号回路は、再構成不可能なハードウェアとして実装されうるのみなら

ず、FPGA等の再構成可能なプログラマブルロジックデバイスとしても実装可能なものであり、本発明の実施形態は、本明細書に開示される技術思想をプログラマブルロジックデバイス上に表現するためのプログラムをも含む。

[0026] 本発明の好適な具現化した形態のいくつかの例が、添付の特許請求の範囲に定義されている。また、以下の実施例の説明にも、いくつかの好適な具現化した形態の例が説明されている。しかしながら、本発明の具現化した形態は、特許請求の範囲や実施例の説明に現れる形態に限定されるものではなく、本発明の範囲を逸脱することなく、様々なバリエーションをとることができることには留意されたい。また、本発明の技術的範囲は、特許請求の範囲や明細書、図面に明示的又は黙示的に現れる、全ての新規かつ有用な特徴及びそれらの組合せを包含することを申し述べる。

図面の簡単な説明

[0027] [図1]従来のエラー検出回路の方式を説明するための図である。

[図2]第1実施例として説明する符号化回路200の回路構成の重要な部分を説明するための図である。

[図3]符号化回路200の処理の流れを説明するための図である。

[図4]第2実施例として説明する符号化・復号回路400の回路構成の主要な部分を説明するための図である。

[図5]符号化・復号回路400が復号回路として動作する場合の様子を説明するための図である。

[図6]符号化・復号回路400の変形例を説明するための図である。

[図7]エラー検出機能を有しないAESの暗号化・復号回路の例を説明するための図である。

[図8]本発明の第3実施例として紹介する、AESの暗号化・復号回路を説明するための図である。

[図9]図8のAES回路の動作を説明するための図である。

[図10]図7と図8のAES回路の性能を比較するための図である。

発明を実施するための最良の形態

[0028] 以下、本発明の理解に資するために、添付図面を参照しつつ本発明の実施形態を例示して説明する。前述のように、本発明は、符号化・復号演算のための、誤り検出能力を有する回路構成に関するものであり、この回路構成では、パイプライン処理を利用している。そこでまず、パイプライン処理が2つのステージのみからなる、最も簡単な実施形態の例について説明する。

[0029] 図2は、これから説明する実施形態に係る符号化回路200の回路構成の重要な部分を説明するための図である。符号化回路200は、二つの部分符号化・部分復号ブロック202及び204を有し、これらの二つのブロックによって符号化演算をパイプライン処理によって行う。第1の部分符号化・部分復号ブロック202は、符号化回路200による符号化処理全体の前半部分の演算を担当し、第2の部分符号化・部分復号ブロック204は、当該符号化処理全体の後半部分の演算を担当する。また、部分符号化・部分復号ブロック202及び204は、それぞれの部分符号化演算の逆演算となる部分復号演算を行ないうるように構成される。この場合、復号演算全体の前半部分は符号化演算の後半部分の逆演算となり、復号演算全体の後半部分は符号化演算の前半部分の逆演算となる。したがって、第1の部分符号化・部分復号ブロック202は、復号演算の後半部分进行处理し、第2の部分符号化・部分復号ブロック204は復号演算の前半部分进行处理する。なお、背景技術の項でも説明したように、符号化回路と復号回路は演算コンポーネントを共有して一つの処理回路にまとめられていることが多いので、部分符号化・部分復号ブロック202及び204のように、一つの処理回路で部分符号化及び部分復号の両方の演算进行处理するように構成することは、当業者であれば困難なくできる。

[0030] 符号化回路200には、部分符号化・部分復号ブロック202及び204が演算処理の結果をストアするためのレジスタ206と、部分符号化・部分復号ブロック202及び204への入力データのコピーをストアするためのレジスタ208が設けられる。したがって、レジスタ206及び208は、

部分符号化・部分復号ブロック 202 及び 204 によって共用される。また符号化回路 200 には、比較器 210 が設けられる。比較器 210 も、部分符号化・部分復号ブロック 202 及び 204 で共用されて、演算処理の結果とレジスタ 208 にストアされているデータとの比較を行うために用いられる。レジスタ 206, 208 及び比較器 210 を共用するために、三つのセクタ 212a, 212b, 212c が設けられる。

[0031] 次に、符号化回路 200 の処理の流れを、図 3 に示す演算サイクル (a) ~ (d) と式を追って詳細に説明する。以下の説明においては、部分符号化・部分復号ブロック 202 で符号化が行われるとき、その関数を $ENC_{pre}()$ 、復号が行われるときの関数を $DEC_{post}()$ で表すことにする。また、部分符号化・部分復号ブロック 204 についても、同様に、符号化が行われるときの関数を $ENC_{post}()$ 、復号が行われるときの関数を $DEC_{pre}()$ と表す。

[0032] 最初の演算サイクル (a) では、入力されたデータ D_0 に対して、部分符号化・部分復号ブロック 202 で符号化の前半処理を施し、次式のように、途中結果 $E_{O_{pre}}$ を求める。

$$E_{O_{pre}} = ENC_{pre}(D_0)$$

演算の結果は、次のサイクル (b) において、レジスタ 206 にストアされるべく準備される。また入力データ D_0 も、次のサイクル (b) において、レジスタ 208 にストアされるべく準備される。

[0033] 次のサイクル (b) では、新たなデータの入力が行われませんが、前のサイクルにおける演算結果 $E_{O_{pre}}$ がレジスタ 206 に、前のサイクルにおける入力データ D_0 がレジスタ 208 にストアされる。そして、レジスタ 206 にストアされた演算結果 $E_{O_{pre}}$ に対し、符号化・復号ブロック 204 で符号化の後半処理が行われ、次のように符号化結果 E_O が得られる。

$$E0 = ENC_{post}(E0_{pre})$$

結果E0は、次のサイクルでレジスタ206にストアされるべく準備される。また、部分符号化・部分復号ブロック204への入力データE0_{pre}も、次のサイクルでレジスタ208にストアされるべく準備される。

- [0034] 部分符号化・部分復号ブロック204による処理と同時に、部分符号化・部分復号ブロック202は、レジスタ206にストアされたE0_{pre}に対して復号の後半処理を行い、回路が正しく動作していれば、次のようにD0を得る。

$$D0 = DEC_{post}(E0_{pre}) = DEC_{post}(ENC_{pre}(D0))$$

- [0035] 比較器210では、部分符号化・部分復号ブロック202により復号されたデータD0を、レジスタ208が保持しているD0と比較する。この比較結果が一致すればエラーは存在せず、一致しなければエラーが存在することになり、検証が可能となる。

- [0036] 念のために記しておく、2サイクルで実行される符号化の関数の順番を $ENC_{pre}() \rightarrow ENC_{post}()$ 、復号を $DEC_{pre}() \rightarrow DEC_{post}()$ としたので、 $ENC_{pre}() \rightarrow ENC_{post}() \rightarrow DEC_{pre}() \rightarrow DEC_{post}()$ で元のデータに戻ることになる。従って、 $ENC_{pre}()$ と $DEC_{post}()$ 及び $ENC_{post}()$ と $DEC_{pre}()$ の組が、それぞれ逆関数になっている。

- [0037] 次のサイクル(c)では、レジスタ206に結果E0がストアされると共に、レジスタ208には前のサイクルにおける部分符号化・部分復号ブロック204への入力データE0_{pre}がストアされる。そして、レジスタ206からは符号化結果E0が出力される。同時に、レジスタ206が保持する値E0に対し、部分符号化・部分復号ブロック204によって復号の前半処理が次のように行われ、レジスタ208が保持する値E0_{pre}と一致するかどうか

が比較器 210 でチェックされる。

$$E0_{pre} = DEC_{pre}(E0) = DEC_{pre}(ENC_{post}(E0_{pre}))$$

- [0038] また、これらの処理と同時に新たなデータ D1 が入力され、部分符号化・部分復号ブロック 20 による次の符号化処理によって途中結果 $E0_{pre}$ が計算される。

$$E1_{pre} = ENC_{pre}(D1)$$

$E1_{pre}$ 、D1 は、それぞれ次のサイクルにおいてレジスタ 206、208 にストアされるべく準備される。

- [0039] 次のサイクル (d) では、上述のサイクル (b) と同様に、レジスタ 206 の途中結果 $E1_{pre}$ に次のように符号化の後半処理と、検証処理としての復号処理が行われ、以下、新たなデータ入力がある度に、同様の処理が繰り返されていく。

$$E1 = ENC_{post}(E1_{pre})$$

$$D1 = DEC_{post}(E1_{pre})$$

- [0040] 符号化回路 200 は、符号化と復号が同じ回路ブロックで処理されるものの、符号化と復号といった異なる処理を行い、元のデータが復元できることを確認しているため、回路の欠陥によって検出不可能なエラーが起こる可能性は非常に低い。また、符号化と復号を行って元のデータに戻ることを確認しているため、検出できないエラーのあるパリティ・チェック等に比べて信頼性が高いエラー検出方式であると言える。

- [0041] 一方、符号化回路 200 では、データの入力を 2 サイクルに 1 回しか行う

ことができないので、エラー検出を行わない場合に対して2倍のサイクル数が必要となる。しかしながら、演算ブロックを2分割したことで、動作周波数がおよそ2倍に向上するため、処理性能の低下は限定的である。付加回路もパイプライン処理用のレジスタとセレクタ、そしてエラー検出用の比較器だけでよい。演算ブロックは2つになっているが、もともと1つだったものを分割しただけなので、図1(c)の方式における二重化のように、演算部を丸ごと新たに加えるようなことはなく、回路規模の増加も極めて限定的である。

[0042] すなわち符号化回路200に例示される回路構成は、符号化・復号回路の動作時のエラー検出を確実にし、且つ回路規模と動作速度に対するペナルティを軽微なものとすることを可能とする。さらに、ここで説明された回路構成は、符号化の演算方式に依存した構成ではないため、適用範囲が広いという特長をも有している。

[0043] 以上の説明で理解されるように、符号化処理に係る本発明の実施形態においては、符号化処理が複数のステージに分割され、各サイクルにおいて、符号化の部分演算と、その1サイクル前における符号化部分演算の検証処理としての復号演算が同時に行われる。符号化回路200を用いた例では、簡単のため演算処理を2分割としたか、パイプライン処理が可能な場合は、3、4、5、…と分割数を増やすことで、動作周波数を2分割の場合よりもさらに向上させることが可能である。分割数を増やすほど処理部の遅延時間は短縮されるが、他の部分の固定の遅延時間があるため、動作周波数は次第に向上しなくなる。またその反面、パイプラインレジスタと比較器といった付加回路が増えていくため、処理能力と回路規模のバランスを見ながら、符号化の処理の特性に応じて分割数を選択する必要がある。

[0044] 図2、図3を用いた上述の説明では、回路200を符号化回路として説明したが、部分符号化・部分復号ブロック202と204の使用の順序を入れ替えるだけで、回路200を復号回路として動作させることができる。すなわち、あるステージの復号処理を行いながら、その前ステージの復号処理に

対する逆処理として、符号化処理を並行して行うことで検証を行う回路構成の復号回路が実現できる。本発明の実施形態の多くは、符号化回路としても、復号回路としても動作することができる。そこで次に、分割数を4つとした実施例について、復号処理についても詳しく触れつつ説明する。

[0045] 図4(a)は、第2実施例として説明する符号化・復号回路400の回路構成の主要な部分を説明するための図である。図示するように、この符号化・復号回路400は、符号化演算及び復号演算を、四つのステージ410, 420, 430, 440でパイプライン処理するように構成されている。各ステージは、それぞれ部分符号化・部分復号ブロック(412, 422, 432, 442)を備えており、符号化・復号処理の異なる段階を担当する。ブロック412は符号化処理の1段目と復号処理の4段目を担当し、ブロック422は符号化処理の2段目と復号処理の3段目を担当し、ブロック432は符号化処理の3段目と復号処理の2段目を担当し、ブロック442は符号化処理の4段目と復号処理の1段目を担当する。各部分符号化・部分復号ブロック412~442で処理される符号化処理と復号処理は互いに逆関数の関係になっている。図4(b)に描かれるように、入力データをブロック412, 422, 432, 442の順で処理する場合、符号化・復号回路400は符号化回路として動作し、入力データをブロック442, 432, 422, 412の順で処理する場合は復号回路として動作する。

[0046] 各符号化・復号ブロックには、それぞれ当該ブロックで処理されたデータを保持するための第1レジスタ(413, 423, 433, 443)と、エラー検出のために一つ前のサイクルのデータを保持するための第2レジスタ(414, 424, 434, 444)が設けられる。また、第2レジスタ(414, 424, 434, 444)に保持されたデータと、逆処理を行なって元に戻したデータとの一致・不一致を判定する比較器が、各符号化・復号ブロックに設けられる(415, 425, 435, 445)。このほか符号化・復号回路400は、各符号化・復号ブロック(412, 422, 432, 442)について、それぞれにデータの入力をコントロールするためのセ

レクタ（４１１，４２１，４３１，４４１）が設けられる。

[0047] 符号化・復号回路４００が符号化回路として動作するときであっても復号回路として動作するときであっても、各符号化・復号ブロック（４１２，４２２，４３２，４４２）は、１サイクルごとに、符号化処理と復号処理を切り替える。ある符号化・復号ブロックが符号化処理を行うサイクルにおいて、隣接するブロックは復号処理を行う。符号化・復号回路４００が符号化回路として動作するとき、復号処理はエラー検出のために行われる。反対に、符号化・復号回路４００が復号回路として動作するときは、符号化処理はエラー検出のために行われる。

[0048] 各ステージにおいて部分処理されたデータは第１レジスタ（４１３，４２３，４３３，４４３）に保持され、次のサイクルで符号化ならば右のステージに、復号ならば左のステージに渡されて処理が続けられる。これと同時に、同じステージではエラー検出のための逆処理が行われ、第２レジスタ（４１４，４２４，４３４，４４４）に保持される一つ前のサイクルのデータと逆処理後のデータが一致するかどうか比較器（４１５，４２５，４３５，４４５）でチェックされる。

[0049] 図５は、符号化・復号回路４００が復号回路として動作する場合の様子を描いた図である。上段の（ａ）があるサイクルにおける動作を示し、下段の（ｂ）が（ａ）の次のサイクルにおける動作を示している。また、（ｂ）の次のサイクルにおける符号化・復号回路４００の動作の様子は、また（ａ）に戻る。図の右上から復号すべきデータが入力され、左下に復号されたデータが出力される。

[0050] 図５に描かれるように、各ステージでは、復号と、符号化による検証（エラー検出）が交互に行われる。たとえば、部分符号化・部分復号ブロック４４２は、（ａ）のサイクルでは復号処理を行うが、（ｂ）のサイクルではその復号処理の検証としての符号化処理を行なっている。同様の関係が、いずれの部分符号化・部分復号ブロック４１２，４２２，４３２，４４２についても見ることができる。

[0051] また、復号が行われるステージの隣のステージでは、1サイクル前の復号の結果を検証すべく、符号化が並行的に行われる。たとえば、(b)における部分符号化・部分復号ブロック432と部分符号化・部分復号ブロック442を見ると、部分符号化・部分復号ブロック432が2段目の復号演算を実行しているのに対し、部分符号化・部分復号ブロック442では、1段目の復号演算の逆演算としての4段目の符号化処理を、エラー検出のために実行している。同様の関係が、(a)における部分符号化・部分復号ブロック422と432、(b)における部分符号化・部分復号ブロック412と422にも見ることができる。

[0052] 図5において、ハッチングして示したコンポーネントと破線のバスは、処理が行われていない部分を示しており、各サイクルで、半分のレジスタと比較器が使用されていないことが理解できる。これはすなわち、二つのステージでレジスタと比較器を共有することができることを示している。次に図6で説明する符号化・復号回路600は、このことを利用し、符号化・復号回路400におけるレジスタと比較器を半分にした実施例である。また、図2を用いて説明された符号化回路200において、二つの部分符号化・部分復号ブロック202、204に対してレジスタ(206, 208)が二つ及び比較器(210)が一つしか設けられていなかったのも、同様の理由による。

[0053] 図6に描かれる符号化・復号回路600は、符号化・復号回路400の変形例であり、隣接する符号化・復号ブロックで、レジスタと比較器を共有するように構成したことを特徴とするものである。図6と図4を比較すると分かるように、図4に描かれるレジスタ413と423が、図6においては一つのレジスタ613に置き換えられており、図4におけるレジスタ414と424が、図6ではレジスタ614に置き換えられている。また、図4に描かれる比較器415と425は、図6では一つの比較器615に置き換えられている。図4におけるレジスタ433及び443と図6のレジスタ633、図4におけるレジスタ434及び444と図6のレジスタ634、図4に

おける比較的 4 3 5 及び 4 4 5 と図 6 の比較器 6 3 5 の関係についても同様である。

[0054] 符号化・復号回路 6 0 0 には、レジスタ及び比較器を共有するために、符号化・復号回路 4 0 0 に比べてセクタ 6 1 6, 6 1 7, 6 2 6, 6 2 7 が追加されているが、二つのレジスタ及び一つの比較器が二つのステージで共有されることができるので、全体としての回路規模は、符号化・復号回路 4 0 0 に比べて小さくて済む。

[0055] [A E S への応用例]

次に、本発明の具体的な実施例として、国際標準暗号 A E S (Advanced Encryption Standard) 回路へ適用した例を示す。暗号は、元のデータが 1 ビットでも異なると、まったく異なるデータに変換されるという特性を有する。このため、演算エラーが発生すると、データがまったく復元できなくなるという極めて深刻な問題を生じる結果となる。また、暗号は、I C カードなど金銭に関係するアプリケーションにも使用されるため、秘密の情報を盗み出そうとする悪意の利用者による電源やクロックへの不正なノイズ印加による誤動作にも対応する必要がある。このため、暗号回路は符号化・復号回路の中でも特に高い信頼性が要求され、高性能なエラー検出機構が不可欠である。

[0056] 図 7 は、1 2 8 ビットの秘密鍵を用いた、エラー検出機能を有さない A E S の暗号化・復号回路例の概略図である。1 2 8 ビットのデータにラウンド関数と呼ばれる変換を 1 0 回繰り返して暗号化と復号を行うため、通常は、この図の左側のデータ変換部にあるように、ラウンド関数ブロックを 1 つだけ用意して、それを 1 回の暗号化（または復号）で 1 0 回利用するループアーキテクチャが用いられる。ラウンド関数は大きく 4 つの部分から構成され、暗号化の場合にそれぞれ ShiftRows、SubBytes、MixColumns、AddRoundKey と表される。復号はこれらの逆関数となる処理によって行われ、それぞれ Inv ShiftRows、Inv SubBytes、Inv MixColumns、AddRoundKey と表記される。（なお、図中 MixColumns と Inv MixColumns はそれぞれ MixCol. と Inv MixCol. と表

記されている。)暗号化と復号で対応する関数はそれぞれ回路を共有している。同じ入力データを同じ関数で変換しても、秘密鍵を変えることによってまったく異なるデータが出力される。秘密鍵は右側の鍵スケジューラで簡単な変換が行われながら、ラウンド関数に10回入力される。

[0057] 図7において、データレジスタ712は、ループ処理を行うために、各ループの処理結果を保持するために用いられる。ShiftRows及びその逆関数InvShiftRowsの処理は、ブロック714で行われ、SubBytes及びその逆関数InvSubByteの処理は、ブロック716で行われる。MixColumns及びその逆関数InvMixColumnsの処理は、ブロック718で行われ、AddRoundKeyの処理はブロック720で行われる。

[0058] 図8は、図2を用いて説明した2分割構成を、図7のAES回路に適用した回路構成である。ラウンド関数はShiftRows/InvShiftRowsとSubBytes/InvSubByte、そしてMixColumns/InvMixColumnsとAddRoundKeyをまとめた2ブロックに分割されている。すなわち、図2と図8を比較すると、図2の部分符号化・部分復号ブロック202が、図8におけるShiftRows/InvShiftRowsブロック714及びSubBytes/InvSubByteブロック716に対応し、図2の部分符号化・部分復号ブロック204が、図8におけるMixColumns/InvMixColumnsブロック718及びAddRoundKeyブロック820、821に対応する。また、図2のレジスタ206は図8のレジスタ712に対応し、図2のレジスタ208は図8のレジスタ812に対応する。図2の比較器210に対応するものは、図8では比較器828である。さらに図8のAES回路では、図7のAES回路を2ステージ化するために、図2のセクタ212b、212cに対応するセクタ824、826が設けられている。

[0059] 図2の構成では2サイクルで1回の符号化を行っていた。一方、図7の回路は10サイクルで暗号化(符号化)を行い、図8はその各サイクルのラウンド関数毎に逆変換を行ってエラー検出を行うので、20サイクルで1回の暗号化を行うことになる。しかしながら、1回のラウンド関数変換を1回の符号化と考えれば、図5と基本的に等価である。図8の一致信号1はサイク

ル毎に、半分のラウンド関数処理のエラーチェック結果が出力される。

[0060] 図8のアーキテクチャでは、AddRoundKeyブロックとInvMixColumnsブロックの順序を入れ替えてXORゲートを共有することは行っていない。このため、図7においてはAddRoundKeyブロックが1つ（720）であるのに対し、図8においては2つ（820, 821）となっている。図7のアーキテクチャではXORゲートを共有することでクリティカルパスであるラウンド関数ブロックを短くできるが、その代わりに鍵スケジューラ部においてMixColumnsブロックが必要となる。これに対してラウンド関数を2分割する提案方式の実装では、XORを共有しないで鍵スケジューラ部のMixColumnsブロックを省略したほうが回路規模と動作速度のバランスが良かったためである。ところでラウンド関数ブロックの遅延時間が分割によって短くなると、鍵スケジューラ部がクリティカルパスとなってくる。そこで、鍵スケジューラ部についても1ラウンドを2クロックで処理するようにレジスタを挿入している。

[0061] ラウンド関数は正しく動作していても、鍵スケジューラ部の処理においてエラーが発生したり、または、制御カウンタの故障によって本来10ラウンドの繰り返し処理が1回で終了してしまうといったことも考えられる。これを防ぐために、最終ラウンドの処理が終了したときにオンザフライで生成された鍵を調べ、暗号化であれば復号鍵レジスタと、復号であれば暗号化鍵レジスタとの一致を比較器830で確認している。攻撃者がカウンタの値を飛ばすことができたとしても、値が不明の鍵スケジューラの128ビットまで正しく飛ばすことは不可能である。

[0062] 図9を参照しつつ、図8に示した構成のAES回路の暗号化時の動作例を説明する。矢印の頭部が黒く塗りつぶされている場合は処理の流れがあることを示し、白抜きになっている場合は処理の流れがないことを示す。暗号化用の初期鍵K0は暗号化鍵レジスタ732に入力され、右側の鍵スケジューラ部で復号用の初期鍵（＝暗号化用の最終鍵）K10に変換されて復号鍵レジスタ734に既にセットされているものとする。

[0063] まず（a）では、入力された平文と暗号化用の初期鍵K0がXORされて

データレジスタ 712 に D0 として書き込まれ、暗号化処理の前半の ShiftRows ブロック 714 と SubBytes ブロック 716 のパスを通ったデータが D1X としてフィードバックされる。それと同時にデータ D0 は比較用レジスタ 812 に渡される。また鍵スケジューラでは、オンザフライで初期鍵 K0 から第 1 ラウンドの鍵 K1 が生成される。(b) では、検算のために (a) で暗号化に使用したパスで復号が行われ、データレジスタ 712 に書き込まれたデータ D1X が InvShiftRows ブロック 714 と InvSubBytes ブロック 716 によって逆変換された後、比較器 828 において、比較用レジスタ 812 に保持されている値 D0 と比較される。一方、同じデータ D1X は、別のパスで MixColumns ブロック 718 と AddRoundKey ブロック 820 (ラウンド鍵 K1 との XOR) により D1 に変換される。(c) では、(a) と同じパスでデータレジスタ 712 の値 D1 が D2X に変換されるのと同時に、その右のパスでは InvMixColumns ブロック 718 と AddRoundKey ブロック 821 (ラウンド鍵 K1 との XOR) で D1X に戻されて比較用レジスタ 812 の値と比較される。以下同様に、第 9 ラウンドまで暗号化と検算が繰り返される。

[0064] (d) ではエラー検出のために InvShiftRows ブロックと InvSubBytes ブロックの処理、そして暗号化の最後の処理である最終第 10 ラウンドの鍵 K10 との XOR の処理が行われる。図 3 でも示したように、最終ラウンドでは MixColumns ブロックの処理は行われないので、その処理ブロックはバイパスされる。最終ラウンドなので、オンザフライで生成されたラウンド鍵レジスタの K10 と事前計算による暗号化鍵レジスタ 732 の K10 との比較により、10 ラウンドきちんと処理されたことのチェックが行われる。ここで暗号文 D10 の出力も可能であるが、最後に (e) で D10X に戻ることが確認された後に出力している。この最終チェックが済むまで次の平文は入力されないため、1 ブロックの暗号化に要するクロック数は、20 クロック (= 10 ラウンド × 2 クロック) に (e) の 1 クロック分が加算され、21 クロックとなる。

[0065] 図 7 と図 8 の回路をそれぞれ設計し、90 nm の CMOS スタンダードセ

ル・ライブラリを用いた論理合成で回路規模と動作速度を評価した結果を図 10 の表に示す。なお、図 8 の回路においては、前述のように暗号化が終了してから次のデータを入れるのに 1 サイクルインターバルを入れる設計としているため、サイクル数は 21 となっている。論理合成時の最適化は、回路規模（ゲート）を最小とするものと動作速度（スループット）を最大とする 2 種類の他に、単位ゲートあたりのスループットである回路効率を最大とする実装も行った。論理合成の条件によって回路規模と動作速度は大きく変動し、小型化するほど速度は遅くなり、高速化するほど回路規模は大きくなるので、その値を単純比較しても実装の優劣をつけることは難しい。そこで、回路効率が単純比較の指標としては最適である。図 10 の表からわかるように、回路規模最適化と動作速度最適化の双方において、エラー検出なしと本発明の回路効率は同等である。規模と速度のバランスが最適な実装においても、エラー検出なしの 169.48 kbps/gate に対して本発明はその 85.5% の 145.01 kbps/gate であった。つまり、本発明を適用した AES 回路は、最大でもわずか 15% 程度のオーバーヘッドで、確実なエラー検出が可能である優れた手法であることがわかる。

[0066] 以上、本発明の実施形態の例を説明してきたが、これらの実施形態は本発明の範囲を限定する意図でなされたものではなく、あくまで本発明の深い理解に資するためのものである。本発明は、その思想の範囲を逸脱することなく、本明細書に説明した実施形態以外にも様々な実施形態を取りうるものである。特許請求の範囲に記載される実施形態は、本発明の好適な実施形態ではあるが、本発明の実施形態はそれに止まるものではなく、本願の出願書類及び技術常識から当業者が感得しうる全ての構成を含むものである。

符号の説明

[0067] 200 符号化回路
200 符号化回路
202, 204 部分符号化・部分復号ブロック
206, 208 レジスタ

208 レジスタ

210 比較器

212 a - 212 c セレクタ

400 符号化・復号回路

410, 420, 430, 440 ステージ

411, 421, 431, 441 セレクタ

412, 422, 432, 442 部分符号化・部分復号ブロック

413, 423, 433, 443 レジスタ

414, 424, 434, 444 レジスタ

415, 425, 435, 445 比較器

600 符号化・復号回路

613 レジスタ

614 レジスタ

615 比較器

616, 617, 626, 627 セレクタ

633 レジスタ

634 レジスタ

635 比較器

請求の範囲

[請求項1]

ステージX及び前記ステージXの次のステージであるステージYを少なくとも含む、複数のステージのパイプライン処理によって符号化処理を行う符号化回路であって、

前記複数のステージの各々は、符号化処理の一部である部分符号化処理及び該一部の逆処理となる部分復号処理を実行しうる部分符号化

- ・ 部分復号ブロックを含み、

或るサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルの1つ前のサイクルにおいて前記ステージXで部分符号化されたデータが部分符号化され、

- ・ 前記ステージXにおいて、前記1つ前のサイクルにおいて前記ステージXで部分符号化されたデータが部分復号され、

- ・ 予め記憶されていた、前記1つ前のサイクルにおいて前記ステージXで部分符号化される前のデータと、前記部分復号されたデータとが比較され、

前記或るサイクルの次のサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルにおいて前記ステージYで部分符号化されたデータが部分復号され、

- ・ 予め記憶されていた、前記或るサイクルにおいて前記ステージYで部分符号化される前のデータと、前記ステージYで部分復号されたデータとが比較され、

- ・ 前記ステージXにおいて、別のデータが部分符号化される回路として構成される符号化回路。

[請求項2]

ステージX及び前記ステージXの次のステージであるステージYを少なくとも含む、複数のステージのパイプライン処理によって復号処理を行う復号回路であって、

前記複数のステージの各々は、復号処理の一部である部分復号処理

及び該一部の逆処理となる部分符号化処理を実行しうる部分符号化・部分復号ブロックを含み、

或るサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルの1つ前のサイクルにおいて前記ステージXで部分復号されたデータが部分復号され、
- ・ 前記ステージXにおいて、前記1つ前のサイクルにおいて前記ステージXで部分復号されたデータが部分符号化され、
- ・ 予め記憶されていた、前記1つ前のサイクルにおいて前記ステージXで部分復号される前のデータと、前記部分符号化されたデータとが比較され、

前記或るサイクルの次のサイクルにおいて、

- ・ 前記ステージYにおいて、前記或るサイクルにおいて前記ステージYで部分復号されたデータが部分符号化され、
- ・ 予め記憶されていた、前記或るサイクルにおいて前記ステージYで部分復号される前のデータと、前記ステージYで部分符号化されたデータとが比較され、
- ・ 前記ステージXにおいて、別のデータが部分復号される回路として構成される復号回路。

[請求項3]

前記ステージXが、暗号化において反復実行されるランダム化関数の一部である部分暗号化処理及び該一部の逆関数となる部分復号処理を実行しうる部分暗号化・部分復号ブロックを含み、前記ステージYが、前記ランダム化関数の残部である部分暗号化処理及び該残部の逆関数である部分復号処理を実行しうる部分暗号化・部分復号処理ブロックを含むことを特徴とする請求項1に記載の符号化回路。

[請求項4]

前記ステージXが、復号において反復実行されるランダム化関数の一部である部分復号処理及び該一部の逆関数となる部分暗号化処理を実行しうる部分復号・部分暗号化ブロックを含み、前記ステージYが、前記ランダム化関数の残部である部分復号処理及び該残部の逆関数で

ある部分暗号化処理を実行しうる部分復号・暗号化処理ブロックを含む

ことを特徴とする請求項 1 に記載の復号回路。

[請求項 5]

(a) 符号化処理を N ステージ (N は 2 以上の整数) のパイプライン処理で行う符号化回路であって、

(b) 各ステージは、符号化処理の一部である部分符号化処理及び該一部の逆処理となる部分復号処理を実行しうる部分符号化・部分復号ブロックを含み、

(c) 前記部分符号化・部分復号ブロックの各々に対し、該部分符号化・部分復号ブロックの部分符号化処理の結果をストアするためのレジスタである第 1 レジスタと、該部分符号化・部分復号ブロックへの入力データのコピーをストアするためのレジスタである第 2 レジスタと、比較器とが割り当てられ、

(d) i 番目 ($2 \leq i \leq N$) の前記部分符号化・部分復号ブロックによる部分符号化処理が行われるサイクルにおいて、

(d-1) $i-1$ 番目の前記部分符号化・部分復号ブロックに関する前記第 1 レジスタにストアされたデータを入力データとして、前記 i 番目の部分符号化・部分復号ブロックによる部分符号化処理が実行され、

(d-2) 前記部分符号化処理を施されたデータが、前記サイクルの次のサイクルにおいて、前記 i 番目の部分符号化・部分復号ブロックに関する前記第 1 レジスタにストアされるように準備され、

(d-3) 前記入力データが、前記次のサイクルにおいて、前記 i 番目の部分符号化・部分復号ブロックに関する前記第 2 レジスタにストアされるように準備され、

(d-4) 前記 $i-1$ 番目の前記部分符号化・部分復号ブロックに関する前記第 1 レジスタにストアされたデータに対し、前記 $i-1$ 番目の部分符号化・部分復号ブロックによる部分復号処理が実行さ

れ、

(d-5) 前記部分復号処理を施されたデータと、前記 $i-1$ 番目の部分符号化・部分復号ブロックに関する前記第2レジスタにストアされたデータとの比較処理が、前記 $i-1$ 番目の部分符号化・部分復号ブロックに関する前記比較器による実行され、

(e) 前記次のサイクルにおいて、

(e-1) 前記 i 番目の部分符号化・部分復号ブロックに関する前記第1及び第2レジスタに対するストア処理が実行され、

(e-2) 前記 i 番目の部分符号化・部分復号ブロックに関する前記第1レジスタにストアされたデータに対し、前記 i 番目の部分符号化・部分復号ブロックによる部分復号処理が実行され、

(e-3) 前記 (e-2) における部分復号処理を施されたデータと、前記 i 番目の部分符号化・部分復号ブロックに関する前記第2レジスタにストアされたデータとの比較処理が、前記 i 番目の部分符号化・部分復号ブロックに関する前記比較器によって実行され、

(e-4) 別のデータに対して前記 $i-1$ 番目の部分符号化・部分復号ブロックによる部分符号化処理が実行される回路として構成される符号化回路。

[請求項6]

(a) 復号処理を N ステージ (N は2以上の整数) のパイプライン処理で行う復号回路であって、

(b) 各ステージは、復号処理の一部である部分復号処理及び該一部の逆処理となる部分符号化処理を実行しうる部分符号化・部分復号ブロックを含み、

(c) 前記部分符号化・部分復号ブロックの各々に対し、該部分符号化・部分復号ブロックの部分復号処理の結果をストアするためのレジスタである第1レジスタと、該部分符号化・部分復号ブロックへの入力データのコピーをストアするためのレジスタである第2レジスタと、比較器とが割り当てられ、

(d) i 番目 ($2 \leq i \leq N$) の前記部分符号化・部分復号ブロックによる部分復号処理が行われるサイクルにおいて、

(d-1) $i-1$ 番目の前記部分符号化・部分復号ブロックに関する前記第 1 レジスタにストアされたデータを入力データとして、前記 i 番目の部分符号化・部分復号ブロックによる部分復号処理が実行され、

(d-2) 前記部分復号処理を施されたデータが、前記サイクルの次のサイクルにおいて前記 i 番目の部分符号化・部分復号ブロックに関する前記第 1 レジスタにストアされるように準備され、

(d-3) 前記入力データが、前記次のサイクルにおいて前記 i 番目の部分符号化・部分復号ブロックに関する前記第 2 レジスタにストアされるように準備され、

(d-4) $i-1$ 番目の前記部分符号化・部分復号ブロックに関する前記第 1 レジスタにストアされたデータに対し、前記 $i-1$ 番目の部分符号化・部分復号ブロックによる部分符号化処理が実行され、

(d-5) 前記部分符号化処理を施されたデータと、前記 $i-1$ 番目の部分符号化・部分復号ブロックに関する前記第 2 レジスタにストアされたデータとの比較処理が、前記 $i-1$ 番目の部分符号化・部分復号ブロックに関する前記比較器によって実行され、

(e) 前記次のサイクルにおいて、

(e-1) 前記 i 番目の部分符号化・部分復号ブロックに関する前記第 1 及び第 2 レジスタに対するストア処理が実行され、

(e-2) 前記 i 番目の部分符号化・部分復号ブロックに関する前記第 1 レジスタにストアされたデータに対し、前記 i 番目の部分符号化・部分復号ブロックによる部分符号化処理が実行され、

(e-3) 前記 (e-2) における部分符号化処理を施されたデータと、前記 i 番目の部分符号化・部分復号ブロックに関する前記

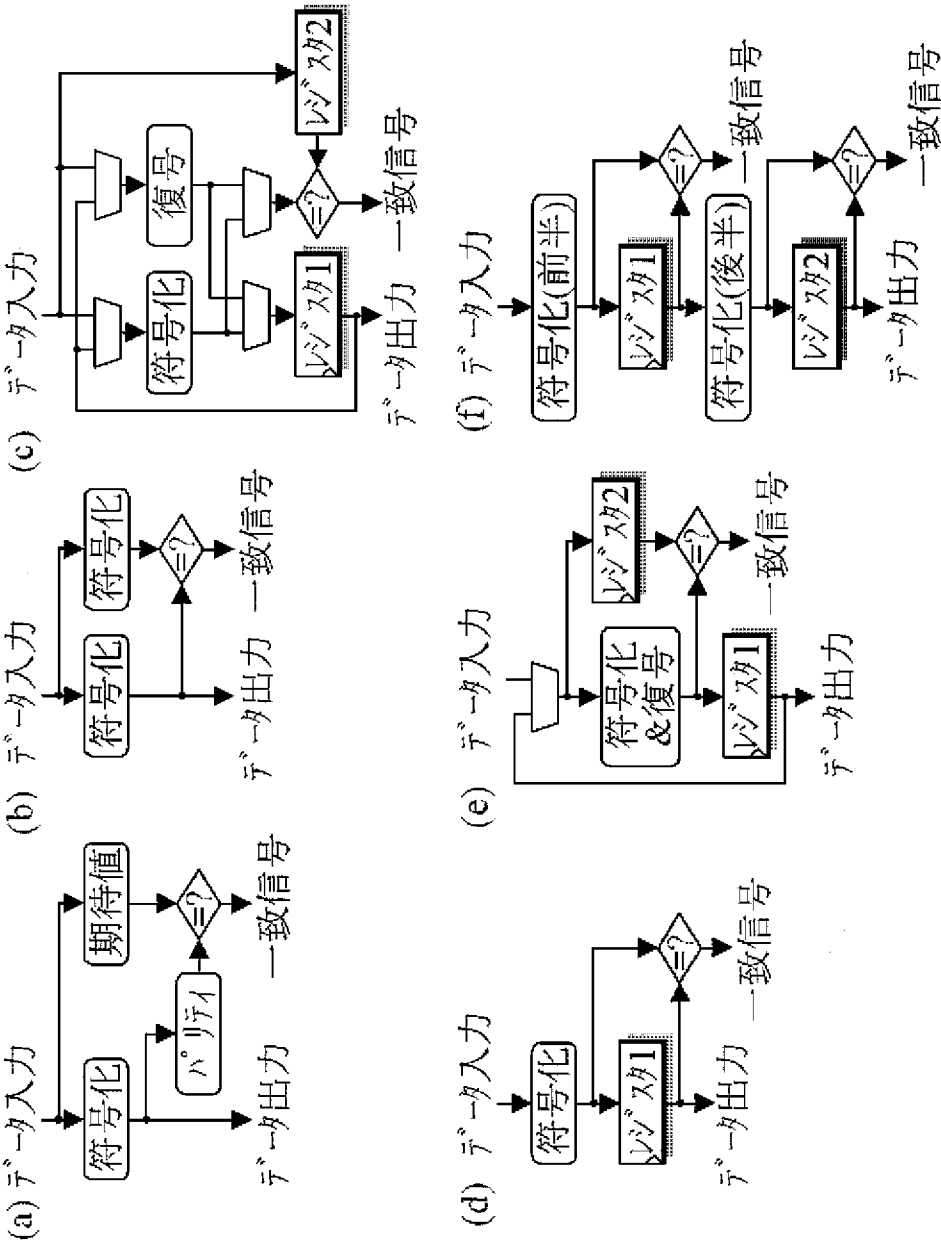
第2レジスタにストアされたデータとの比較処理が、前記i番目の部分符号化・部分復号ブロックに関する前記比較器によって実行され、

(e-4) 別のデータに対して前記i-1番目の部分符号化・部分復号ブロックによる部分復号処理が実行される回路として構成される復号回路。

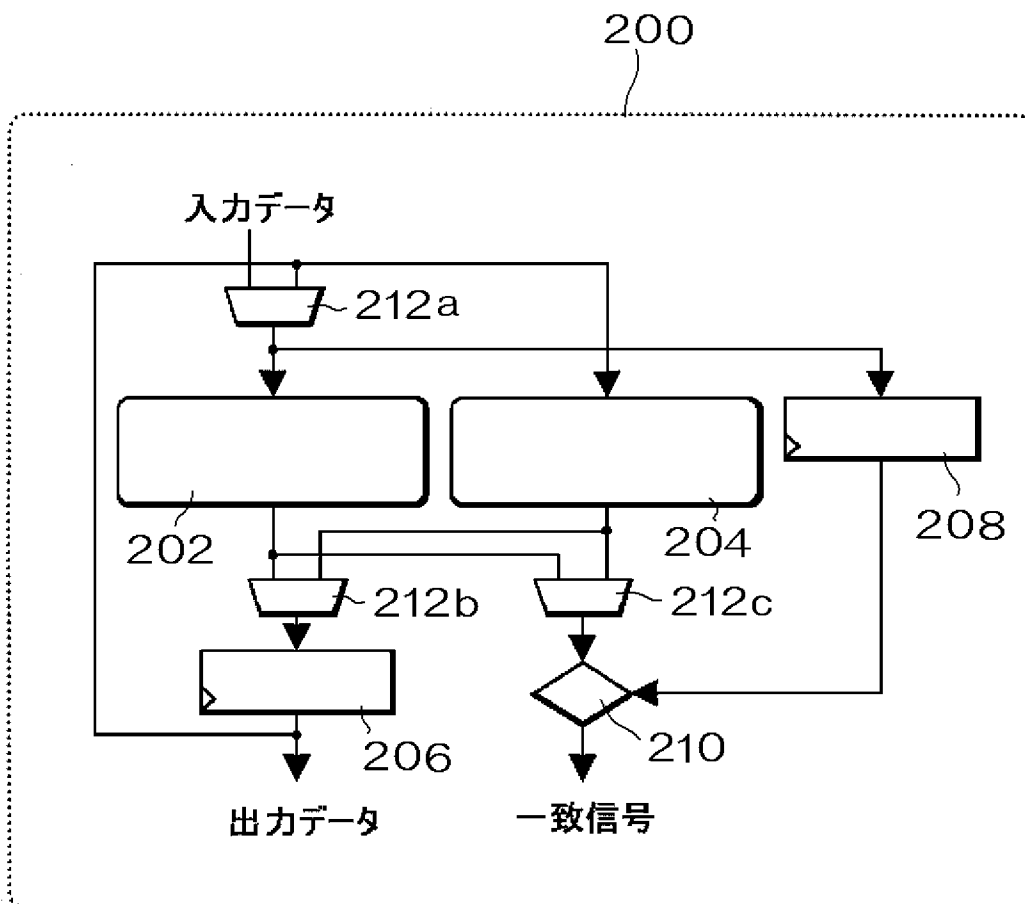
[請求項7] 前記第1レジスタ、前記第2レジスタ、前記比較器の少なくとも1つ以上が、2つの前記部分符号化・部分復号ブロックによって共有される回路として構成される請求項5に記載の符号化回路。

[請求項8] 前記第1レジスタ、前記第2レジスタ、前記比較器の少なくとも1つ以上が、2つの前記部分符号化・部分復号ブロックによって共有される回路として構成される請求項6に記載の復号回路。

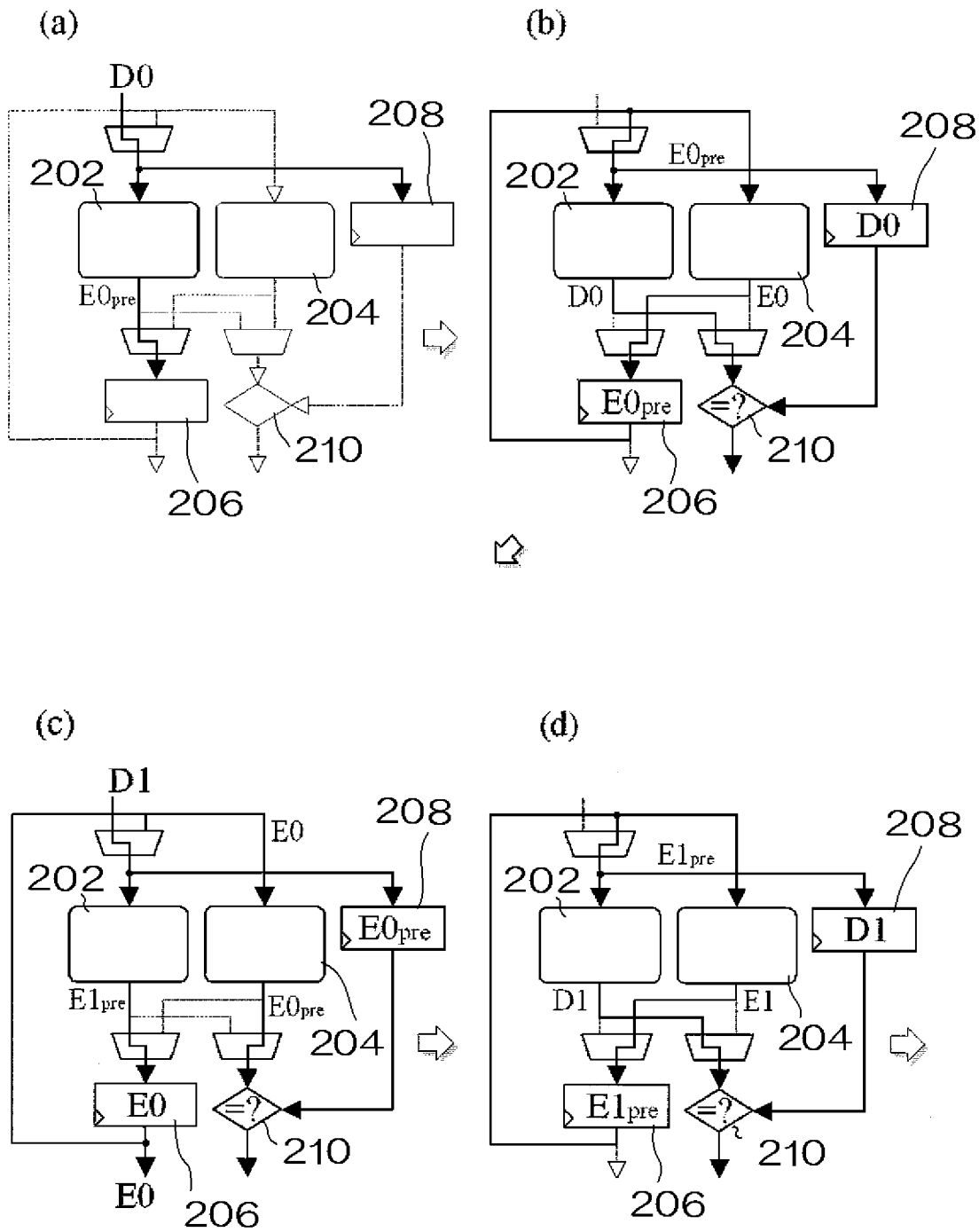
[図1]



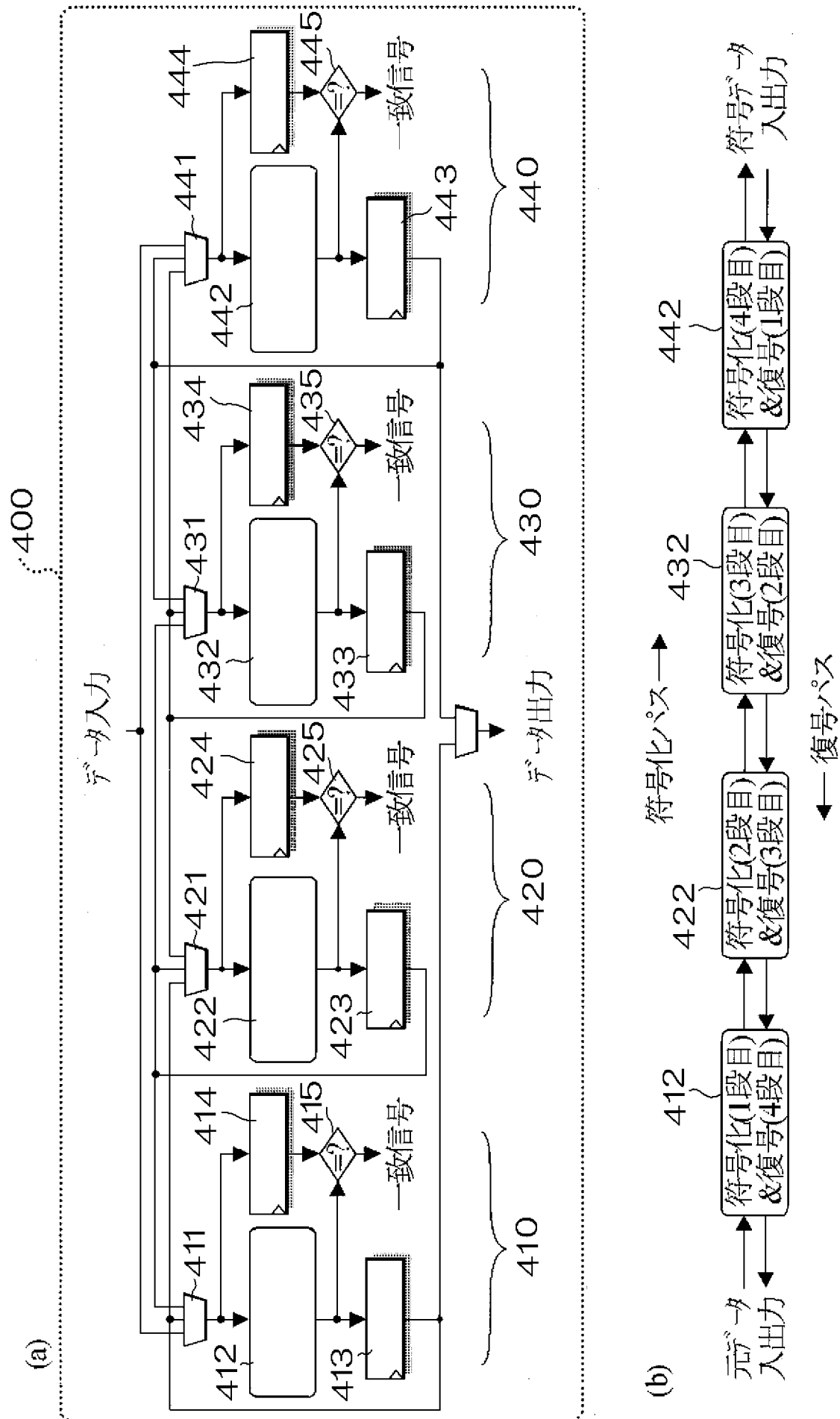
[図2]



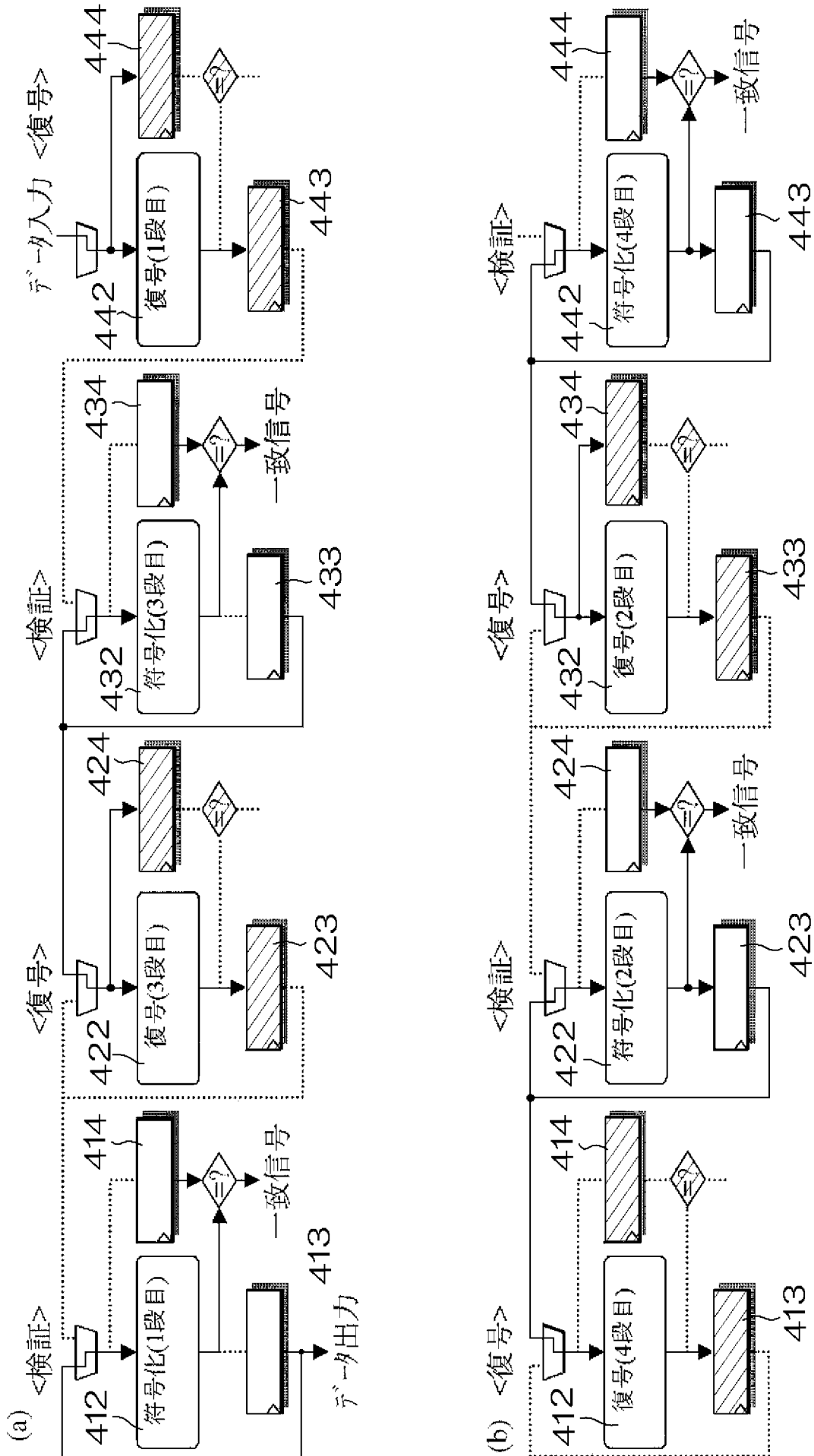
[図3]



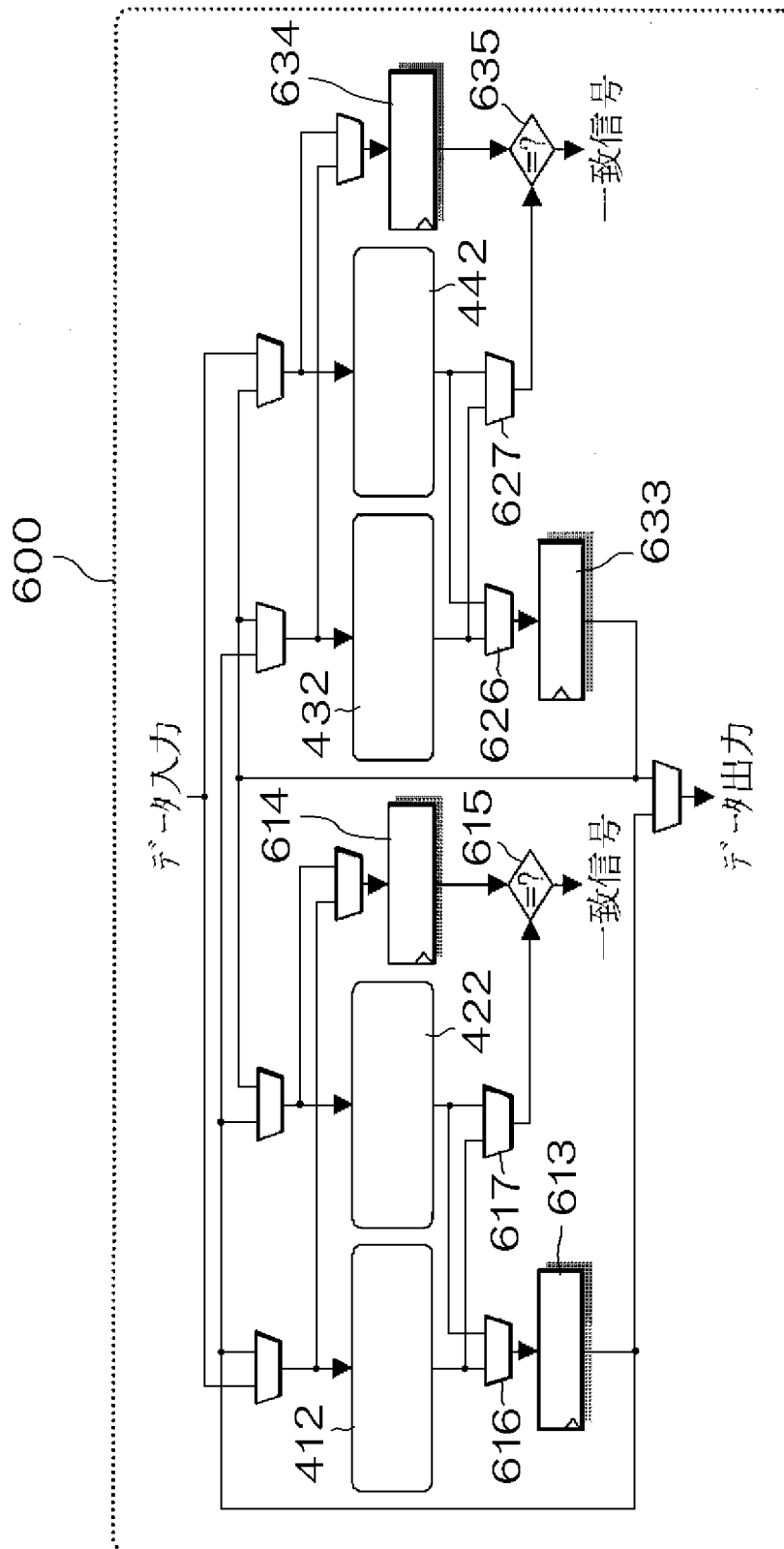
[図4]



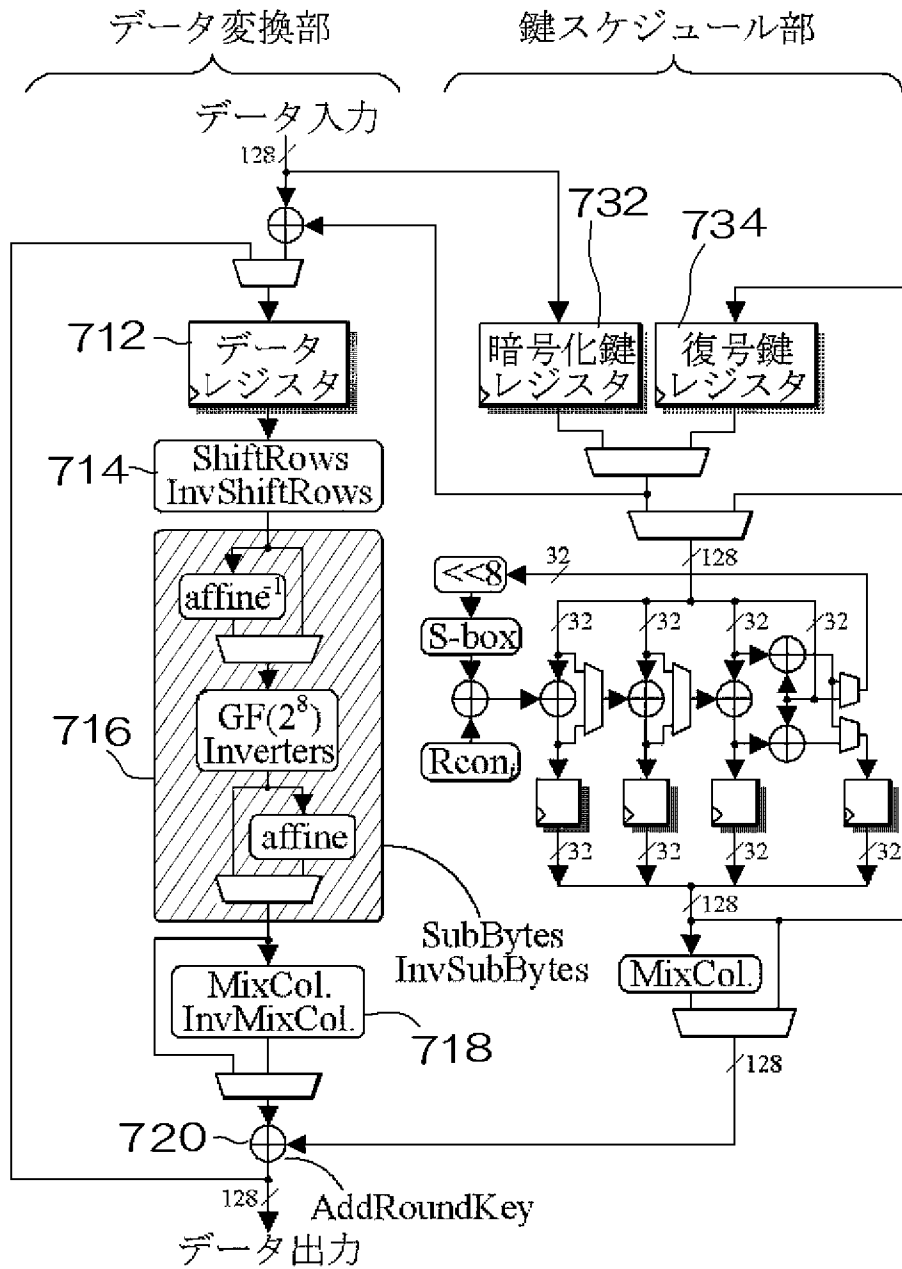
[図5]



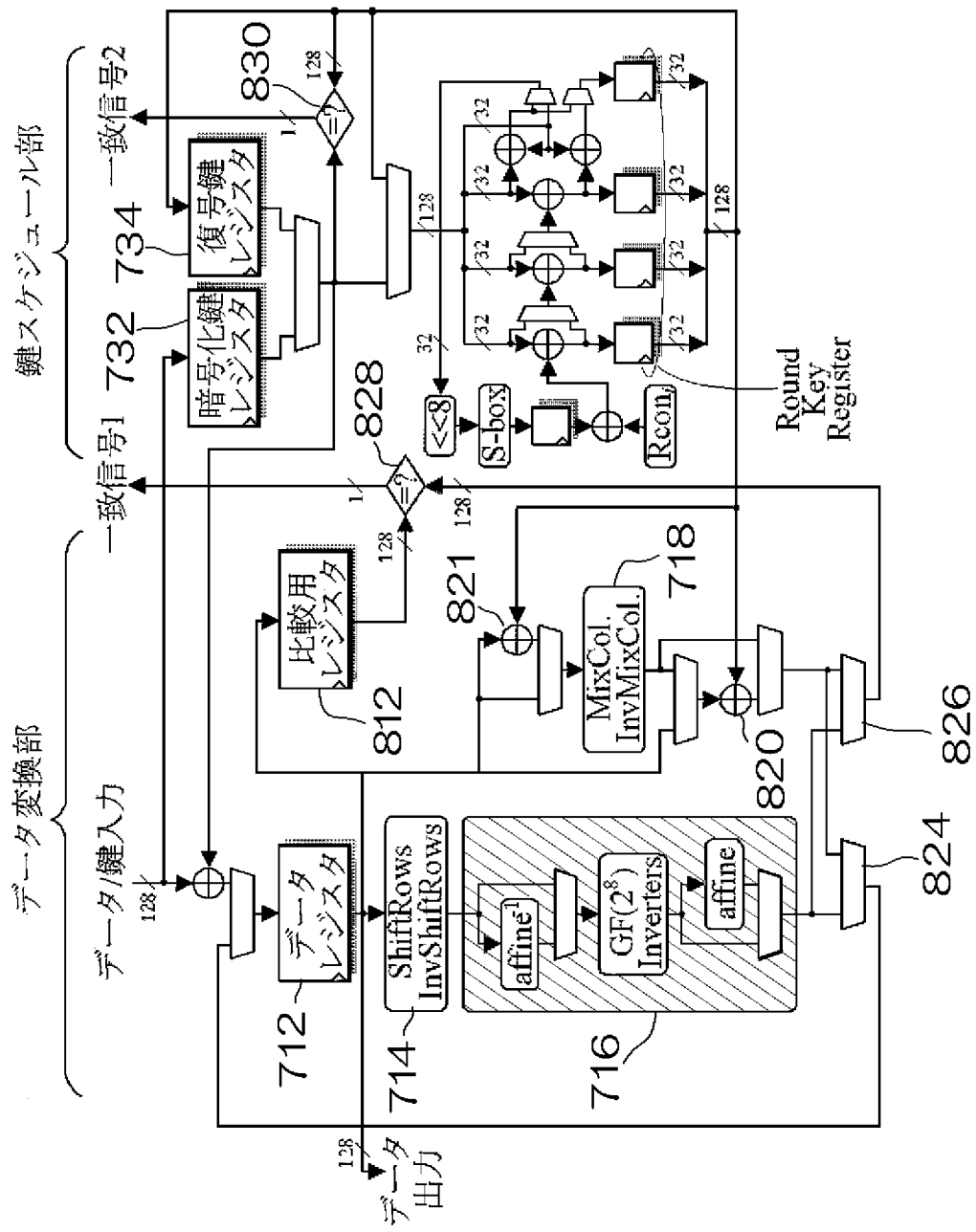
[図6]



[図7]



[図8]



[illegible]

[図10]

表：AES 回路の性能比較

	サイクル数 (Clock)	回路規模 (gates)	最大動作 周波数 (MHz)	スルー プット (Mbps)	回路効率 (Kbps/gate)	最適化
エラー 検出なし (図7)	10	12,949	129.37	1,655.9	127.88	規模
		20,003	265.25	3,395.2	169.48	効率
		30,708	330.03	4,224.4	137.57	速度
本発明 実施例 (図8)	21	16,099	362.32	2,208.4	137.18	規模
		17,087	406.50	2,477.7	145.01	効率
		24,114	526.32	3,208.0	133.04	速度

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/059167

A. CLASSIFICATION OF SUBJECT MATTER

H03M13/01(2006.01) i, 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)

H03M13/01, 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 1996-2009

Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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	JP 2003-298426 A (Sony Corp.), 17 October, 2003 (17.10.03), Full text; all drawings (Family: none)	1-8
A	JP 2005-285270 A (Elpida Memory, Inc.), 13 October, 2005 (13.10.05), Full text; all drawings & US 2005/0229076 A1 & CN 1677563 A	1-8
A	JP 2007-221346 A (Toshiba Corp.), 30 August, 2007 (30.08.07), Full text; all drawings (Family: none)	1-8

☒ 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
08 June, 2009 (08.06.09)Date of mailing of the international search report
16 June, 2009 (16.06.09)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/059167

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 3-177120 A (Fujitsu Ltd.), 01 August, 1991 (01.08.91), Full text; all drawings (Family: none)	1-8

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H03M13/01(2006.01)i, 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（I P C））

Int.Cl. H03M13/01, 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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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	JP 2003-298426 A（ソニー株式会社） 2003.10.17, 全文, 全図（ファミリーなし）	1-8
A	JP 2005-285270 A（エルピーダメモリ株式会社） 2005.10.13, 全文, 全図 & US 2005/0229076 A1 & CN 1677563 A	1-8
A	JP 2007-221346 A（株式会社東芝） 2007.08.30, 全文, 全図（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

0 8 . 0 6 . 2 0 0 9

国際調査報告の発送日

1 6 . 0 6 . 2 0 0 9

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

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）

渡辺 未央子

5 K

3 7 8 9

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 5 6

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
A	JP 3-177120 A (富士通株式会社) 1991.08.01, 全文, 全図 (ファミリーなし)	1-8