(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
2012 年 10 月 4 日(04.10.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/131856 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2011/057480

(22) 国際出願日: 2011 年 3 月 25 日(25.03.2011)

(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 (米国を除く全ての指定国について): 富士通株式会社(FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 矢嶋 純(YAJIMA, Jun) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP). 伊豆 哲也(IZU, Tetsuya) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP). 武仲 正彦(TAKENAKA, Masahiko) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 酒井 昭徳(SAKAI, Akinori); 〒1006020 東京都千代田区霞が関３丁目２番５号 霞が関ビルディング２０階 酒井総合特許事務所 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, 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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

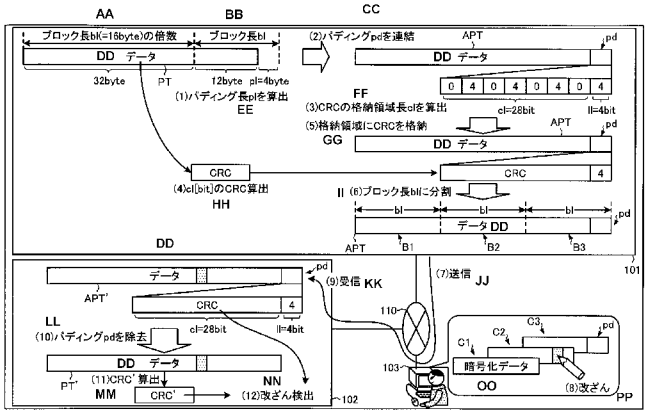
添付公開書類:

— 国際調査報告（条約第 21 条(3)）

(54) **Title**: INFORMATION PROCESSING DEVICE, TAMPERING DETECTION DEVICE, INFORMATION PROCESSING METHOD, TAMPERING DETECTION METHOD, INFORMATION PROCESSING PROGRAM, AND TAMPERING DETECTION PROGRAM

(54) 発明の名称 : 情報処理装置、改ざん検出装置、情報処理方法、改ざん検出方法、情報処理プログラムおよび改ざん検出プログラム

[図1]



AA Block length (bl) (=16 bytes) multiple
BB Block length (bl)
CC Link to padding (pd)
DD Data
EE Compute padding length (pl)
FF Compute CRC storage region length (cl)
GG Store CRC in storage region
HH Compute cl[bit] CRC
II Segment into block length (bl)
JJ Transmit
KK Receive
LL Remove padding (pd)
MM Compute CRC'
NN Detect tampering
OO Encrypted data
PP Tampering

(57) **Abstract**: An information processing device (101) computes a padding length (pl) of padding (pd) which is linked to plaintext (PT) which is to be encrypted. The information processing device (101) stores the padding length (pl) in the padding (pd) within the range of the computed padding length (pl), and stores a CRC in the padding (pd) which is computed from the plaintext (PT), within the range of the computed padding length (pl). The information processing device (101) encrypts the plaintext (PT) which links the padding (pd) which includes the padding length (pl) and the CRC and transmits same to a tampering detection device (102). Conversely, the tampering detection device (102) is capable of carrying out a removal of the padding (pd) and a tampering detection on the basis of the padding length (pl) and the CRC which are included in the plaintext (PT) which is decrypted from the received encrypted block.

(57) 要約:

[続葉有]

WO 2012/131856 A1

情報処理装置（１０１）は、暗号化対象の平文（ＰＴ）に連結するパディング（ｐｄ）のパディング長（ｐｌ）を算出する。情報処理装置（１０１）は、算出したパディング長（ｐｌ）の範囲内でパディング（ｐｄ）にパディング長（ｐｌ）を格納し、また、算出したパディング長（ｐｌ）の範囲内でパディング（ｐｄ）に平文（ＰＴ）から算出するＣＲＣを格納する。情報処理装置（１０１）は、パディング長（ｐｌ）とＣＲＣを含むパディング（ｐｄ）を連結した平文（ＰＴ）を暗号化して改ざん検出装置（１０２）に送信する。一方、改ざん検出装置（１０２）は、受信した暗号化ブロックから復号した平文（ＰＴ）に含まれるパディング長（ｐｌ）とＣＲＣに基づいて、パディング（ｐｄ）の除去と改ざんの検出をおこなうことができる。

明　細　書

発明の名称 ：

情報処理装置、改ざん検出装置、情報処理方法、改ざん検出方法、情報処理プログラムおよび改ざん検出プログラム

技術分野

[0001] 本発明は、ブロック暗号を扱う情報処理装置、改ざん検出装置、情報処理方法、改ざん検出方法、情報処理プログラムおよび改ざん検出プログラムに関する。

背景技術

[0002] 近年、情報化社会において、情報を扱う際の安全性を確保することが重要となっている。情報の安全性を確保するためには、情報を秘匿するための暗号化技術および情報の改ざんを検出する技術が必要となる。

[0003] 暗号化技術には、共通鍵方式の暗号（以下、共通鍵暗号と呼ぶ）や公開鍵方式の暗号（以下、公開鍵暗号と呼ぶ）がある。共通鍵暗号は、公開鍵暗号と比較した場合、処理速度が速くコンパクトに実装できるという利点がある。このため、携帯電話やＩＣカードなどの小型機器に暗号化機能を付加する場合には、共通鍵暗号が使用される。

[0004] 共通鍵暗号の一種であるブロック暗号においては、暗号化の対象となるデータ（以下、「平文」という）をブロック単位に分割して暗号化をおこなう。暗号化がブロック単位でおこなわれるため、平文のデータ長はブロックのデータ長（以下、「ブロック長」という）の倍数である必要がある。

[0005] そのため、平文のデータ長がブロック長の倍数でない場合、パディングを平文に連結して、平文をブロック長の倍数のデータ長に加工する技術がある。連結されるパディングには、復号の際にパディングを除去するために必要な情報が含まれる。例えば、パディングには、パディングのデータ長（以下、「パディング長」という）を示す情報が含まれる。

[0006] また、情報の改ざんを検出する技術としては、例えば、ブロック長ごとに

暗号化された一連のブロック（以下、「暗号化ブロック」という）から復号した平文内のパディングの内容が、パディングの規則に則っているか否かを判定する技術がある。すなわち、暗号化ブロックの改ざんにより、復号した平文内のパディングの内容に変化があった場合には、パディングがパディングの規則を外れるため、改ざんを検出することができる。

[0007] また、情報の改ざんを検出する技術としては、例えば、暗号化の際に、平文を識別するＣＲＣを平文に連結する。ＣＲＣを連結した平文にさらにパディングを連結して、ブロック長の倍数のデータ長に加工して、暗号化をおこなう。そして、復号の際に、復号した平文を識別するＣＲＣと、復号した平文に付与されていたＣＲＣと、を比較する技術がある。すなわち、暗号化ブロックの改ざんにより、平文に変化があった場合には、復号した平文のＣＲＣと、復号した平文に付与されていたＣＲＣが異なるため、改ざんを検出することができる（例えば、下記特許文献１参照）。

先行技術文献

特許文献

[0008] 特許文献1：特開２００６－２２０７４７号公報

発明の概要

発明が解決しようとする課題

[0009] しかしながら、パディングとしての規則に基づいて改ざんを検出する技術では、暗号化ブロックの改ざんにより、パディングを付与するブロック、つまり暗号文の最終ブロック以外を改ざんした場合には、改ざんを検出することができないという問題があった。

[0010] また、上述した特許文献１にかかる技術では、固定の平文データ長のみに使用可能であり、データ長が任意の場合については全く考慮されておらず、仮に任意のデータ長について使用した場合にはＣＲＣをあらたに連結する必要があり、データ量が増えてしまうという問題があった。そのため、リソースが厳しい組み込み環境においては、ＣＲＣを連結する領域を用意できず、

上述した特許文献１にかかる技術を適用することができないという問題があった。

[0011] 本発明は、上述した従来技術による問題点を解消するため、使用リソースの増加なく平文全体の改ざんを検出できる情報処理装置、改ざん検出装置、情報処理方法、改ざん検出方法、情報処理プログラムおよび改ざん検出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

[0012] 本発明の一側面によれば、平文データのデータ長より長く、かつ、所定のブロック長の倍数となるデータ長を特定し、平文データのデータ長と特定されたデータ長との差分のデータ長を算出し、算出された差分のデータ長を示す第１のコードを生成し、平文データに基づいて算出される第２のコードを、算出された差分のデータ長から第１のコードのデータ長を引いた残余のデータ長以内のデータ長で生成し、生成された第２のコードを含み、生成された第１のコードを末尾とするパディングを、差分のデータ長で作成し、作成されたパディングを平文データの末尾に連結させて連結データを生成し、得られた連結データを出力する情報処理装置、情報処理方法および情報処理プログラムが提案される。

[0013] また、本発明の一側面によれば、平文データを所定のブロック長ごとに暗号化した暗号化データを入力し、入力された暗号化データから、暗号化と復号に共通して使用される鍵を用いて復号した復号データを生成し、パディングのデータ長を格納する生成された復号データの末尾となる第１の領域から、第１のコードを抽出し、抽出された第１のコードが示すデータ長に基づいて、平文データから算出されたコードを格納する生成された復号データの第２の領域を決定し、決定された第２の領域から第２のコードを抽出し、抽出された第１のコードが示すデータ長となる生成された復号データの末尾領域を除いた生成された復号データの第３の領域から第３のコードを抽出し、抽出された第３のコードから算出される第４のコードを、第２のコードのデータ長と同一データ長で生成し、生成された第４のコードと第２のコードとの

一致判定をおこない、判定結果を出力する改ざん検出装置、改ざん検出方法および改ざん検出プログラムが提案される。

発明の効果

[0014] 本発明の一側面によれば、使用リソースの増加なく平文全体の改ざんの検出を図ることができるという効果を奏する。

図面の簡単な説明

[0015] [図1]図１は、改ざん検出の内容を示す説明図である。

[図2]図２は、実施の形態にかかる情報処理装置１０１または改ざん検出装置１０２のハードウェア構成例を示すブロック図である。

[図3]図３は、情報処理装置１０１の機能的構成を示すブロック図である。

[図4]図４は、改ざん検出装置１０２の機能的構成を示すブロック図である。

[図5]図５は、連結文ＡＰＴのデータ構造の一例を示す説明図である。

[図6]図６は、情報処理装置１０１による平文ＰＴの暗号化の具体例１を示す説明図である。

[図7]図７は、改ざん検出装置１０２による改ざん検出の具体例１を示す説明図である。

[図8]図８は、情報処理装置１０１による平文ＰＴの暗号化の具体例２を示す説明図である。

[図9]図９は、改ざん検出装置１０２による改ざん検出の具体例２を示す説明図である。

[図10]図１０は、情報処理装置１０１による平文ＰＴの暗号化の具体例３を示す説明図である。

[図11]図１１は、改ざん検出装置１０２による改ざん検出の具体例３を示す説明図である。

[図12]図１２は、情報処理装置１０１がおこなうパディング連結処理の詳細を示すフローチャートである。

[図13]図１３は、改ざん検出装置１０２がおこなう改ざん検出処理の詳細を示すフローチャートである。

発明を実施するための形態

[0016] 以下に添付図面を参照して、この発明にかかる情報処理装置、改ざん検出装置、情報処理方法、改ざん検出方法、情報処理プログラムおよび改ざん検出プログラムの実施の形態を詳細に説明する。以下では、説明の簡単のため、情報処理装置と改ざん検出装置とが別の装置であるとする。しかし、情報処理装置は、改ざん検出装置の機能を併せて持っていてもよく、改ざん検出装置は、情報処理装置の機能を併せて持っていてもよい。

[0017] （改ざん検出の内容）

図１は、改ざん検出の一例を示す説明図である。図１において、平文ＰＴを暗号化して送信する側の装置を情報処理装置１０１とする。暗号化された平文ＰＴを受信して、暗号化された平文ＰＴの改ざんの有無を検出する側の装置を改ざん検出装置１０２とする。

[0018] 情報処理装置１０１と改ざん検出装置１０２とは、ネットワーク１１０に接続されている。また、ネットワーク１１０には、攻撃者のコンピュータ１０３が接続されている。情報処理装置１０１と改ざん検出装置１０２とは、暗号化と復号に共通して使用できる暗号鍵（以下、「共通鍵」という）を有する。

[0019] 情報処理装置１０１は、共通鍵を用いたブロック暗号により平文ＰＴを暗号化する。ブロック暗号では、情報処理装置１０１は、暗号化する平文ＰＴにパディングｐｄを連結することにより、平文ＰＴをブロック単位に分割できるデータ長（すなわち、ブロック長ｂｌの倍数のデータ長）に加工する必要がある。以下では、パディングｐｄが連結された平文ＰＴを「連結文ＡＰＴ」という。

[0020] ここで、平文ＰＴに連結されるパディングｐｄには、改ざん検出装置１０２においてパディングｐｄを除去するために必要なパディングｐｄのデータ長ｐｌ（以下、「パディング長」という）が含まれる。また、平文ＰＴに連結されるパディングｐｄには、改ざん検出装置１０２において改ざんの検出に用いるデータが含まれる。

[0021] 改ざん検出装置１０２は、ネットワーク１１０を介して受信された暗号化ブロックを、共通鍵を用いたブロック暗号により復号する。そして、改ざん検出装置１０２は、復号されたデータに基づいて、改ざんの有無を検出する。

[0022] 以下では、情報処理装置１０１が、データ長が４４［ｂｙｔｅ］の平文ＰＴを暗号化して改ざん検出装置１０２に送信する場合を例に挙げて、改ざん検出装置１０２における改ざんの検出の内容について説明する。ただし、ブロック長ｂｌは、１６［ｂｙｔｅ］であるとする。

[0023] （１）まず、情報処理装置１０１は、送信する平文ＰＴのデータ長を確認して、平文ＰＴに連結するパディングｐｄのパディング長ｐｌを算出する。具体的には、平文ＰＴは、データ長が４４［ｂｙｔｅ］であるから、ブロック長ｂｌ＝１６［ｂｙｔｅ］の３倍のデータ長となる４８［ｂｙｔｅ］に４［ｂｙｔｅ］不足している。よって、情報処理装置１０１は、パディング長ｐｌを４［ｂｙｔｅ］と算出する。

[0024] （２）次に、情報処理装置１０１は、ブロック暗号による暗号化のために、ブロック長ｂｌ＝１６［ｂｙｔｅ］の３倍となる４８［ｂｙｔｅ］のデータ長となる連結文ＡＰＴに平文ＰＴを加工する。具体的には、情報処理装置１０１は、算出したパディング長ｐｌ＝４［ｂｙｔｅ］のパディングｐｄを平文ＰＴの末尾に連結することにより、データ長をブロック長ｂｌの倍数のデータ長とする連結文ＡＰＴを作成する。

[0025] パディングｐｄには、改ざん検出装置１０２がパディングｐｄを除去するために必要なパディングｐｄのパディング長ｐｌの情報がパディングｐｄの末尾となる領域に格納されている。

[0026] ここで、パディング長ｐｌの情報を格納するパディングｐｄの末尾となる領域（以下、「パディング長領域」という）のデータ長ｌｌ（以下、「パディング長領域長ｌｌ」という）は、固定長であり、平文ＰＴに連結されうる最長のパディング長ｐｌを示すことが可能なデータ長である。例えば、ブロック長ｂｌが１６［ｂｙｔｅ］であれば、平文ＰＴに連結されうるパディン

グｐｄは最長でも１６［ｂｙｔｅ］であるから、１６を示すことが可能な４［ｂｉｔ］がパディング長領域長ＬＬである。

[0027] 例えば、ここでのパディングｐｄとしては、ｐｋｃｓ＃７に記載されたパディング方式に基づいて「０４０４０４０４」が採用される。ただし、「０４０４０４０４」は、１６進数表記である。これにより、改ざん検出装置１０２は、パディングｐｄの末尾４［ｂｉｔ］となるパディング長領域が示す４を参照して、パディング長ｐｌが４［ｂｙｔｅ］であると判断できる。

[0028] （３）次に、情報処理装置１０１は、平文ＰＴから算出されるコードを格納するパディングｐｄ内の領域（以下、「格納領域」という）のデータ長ｃｌ（以下、「格納領域長」という）を算出する。平文ＰＴから算出されるコードとしては、例えば、平文ＰＴのＣＲＣを採用できる。

[0029] 具体的には、例えば、情報処理装置１０１は、パディング長領域を除いたパディングｐｄ内の領域をＣＲＣの格納領域とする。よって、格納領域長ｃｌは、パディング長ｐｌ＝４［ｂｙｔｅ］から、パディング長領域長ＬＬ＝４［ｂｉｔ］を除いた２８［ｂｉｔ］である。

[0030] （４）そして、情報処理装置１０１は、算出した格納領域長ｃｌと同一データ長のＣＲＣを平文ＰＴから算出する。すなわち、情報処理装置１０１は、平文ＰＴから２８［ｂｉｔ］のＣＲＣを算出する。

[0031] （５）情報処理装置１０１は、算出した２８［ｂｉｔ］のＣＲＣをパディングｐｄ内の格納領域に格納する。情報処理装置１０１は、結果として、連結文ＡＰＴ内のパディングｐｄを、末尾となるパディング長領域にパディング長ｐｌを含み、格納領域に算出したＣＲＣを含むパディングｐｄに加工する。

[0032] （６）そして、情報処理装置１０１は、連結文ＡＰＴを、ブロック長ｂｌ＝１６［ｂｙｔｅ］ごとに分割する。ここでは、連結文ＡＰＴのデータ長は４８［ｂｙｔｅ］であるから、連結文ＡＰＴは３ブロックに分割される。ここで、分割されたブロックを、先頭からそれぞれブロックＢ１～Ｂ３とする。

[0033] （７）情報処理装置１０１は、分割したブロックＢ１～Ｂ３を、ブロック暗号により暗号化して、改ざん検出装置１０２に送信する。ここで、ブロック暗号により暗号化されたブロックＢ１～Ｂ３を、それぞれ暗号化ブロックＣ１～Ｃ３とする。

[0034] （８）ここで、情報処理装置１０１により送信された暗号化ブロックＣ１～Ｃ３が、攻撃者のコンピュータ１０３でキャプチャされ、暗号化ブロックＣ２の一部が改ざんされたとする。

[0035] （９）改ざん検出装置１０２は、暗号化ブロックＣ１～Ｃ３を受信する。そして、改ざん検出装置１０２は、受信した暗号化ブロックＣ１～Ｃ３から、ブロックを復号する。そして、改ざん検出装置１０２は、復号したブロックを連結させて連結文ＡＰＴ’を作成する。

[0036] しかしながら、暗号化ブロックＣ２が改ざんされているため、改ざん検出装置１０２が暗号化ブロックＣ２に基づいて作成した連結文ＡＰＴ’は、情報処理装置１０１での連結文ＡＰＴとは異なるデータになっている。

[0037] （１０）改ざん検出装置１０２は、連結文ＡＰＴ’の末尾のパディング長領域が示す４を参照して、パディング長ｐｌが４［ｂｙｔｅ］であると特定し、連結文ＡＰＴ’の末尾から４［ｂｙｔｅ］のパディングｐｄを除去して平文ＰＴ’を作成する。しかしながら、暗号化ブロックＣ２の改ざんの影響により、改ざん検出装置１０２が作成した平文ＰＴ’は、情報処理装置１０１での平文ＰＴとは異なるデータになっている。

[0038] （１１）次に、改ざん検出装置１０２は、平文ＰＴ’から算出されるコードを、格納領域長ｃｌと同一データ長で算出する。具体的には、改ざん検出装置１０２は、パディング長ｐｌ＝４［ｂｙｔｅ］とパディング長領域長ｌｌ＝４［ｂｉｔ］より、格納領域長ｃｌは２８［ｂｉｔ］であると特定する。そして、改ざん検出装置１０２は、平文ＰＴ’から２８［ｂｉｔ］のＣＲＣ’を算出する。ここで、平文ＰＴ’は平文ＰＴとは異なるデータになっているため、算出されるＣＲＣ’は、情報処理装置１０１でのＣＲＣとは異なるデータになる。

[0039] （１２）改ざん検出装置１０２は、特定された２８［ｂｉｔ］の格納領域から、平文ＰＴのＣＲＣを抽出する。そして、改ざん検出装置１０２は、算出したＣＲＣ’と、パディングｐｄから抽出したＣＲＣとの一致判定をおこなう。そして、改ざん検出装置１０２は、判定結果を出力する。

[0040] 具体的には、ＣＲＣ’とＣＲＣとが異なるデータであれば、改ざん検出装置１０２は、平文ＰＴ’は情報処理装置１０１での平文ＰＴとは異なるデータであると判定でき、改ざんがあったことを出力する。また、ＣＲＣ’とＣＲＣとが同一のデータであれば、改ざん検出装置１０２は、平文ＰＴ’は情報処理装置１０１での平文ＰＴのままであると判定でき、改ざんされていないことを出力する。

[0041] 以上のように、情報処理装置１０１は、パディングｐｄに平文ＰＴから算出されるコードを格納しておく。そして、改ざん検出装置１０２は、復号した平文ＰＴ’全体から算出されるコードとパディングｐｄに格納された平文ＰＴから算出されたコードとの一致判定をおこなう。これにより、改ざん検出装置１０２は、改ざんにより平文ＰＴのどの部分が変化した場合であっても改ざんを検出することができる。

[0042] また、情報処理装置１０１は、平文ＰＴに連結するパディングのパディング長ｐｌを算出してから、算出したパディング長ｐｌの範囲内で平文ＰＴから算出するコードの格納領域長ｃｌを算出する。そして、情報処理装置１０１は、算出した格納領域長ｃｌと同一データ長以下の長さで平文ＰＴから算出するコードを生成し、格納領域に格納する。これにより、連結文ＡＰＴのデータ長の増加を防止し、リソースの使用量の削減をおこなうことができる。

[0043] また、情報処理装置１０１は、格納領域を算出する際に、パディング長領域を確保しておく。これにより、改ざん検出装置１０２は、末尾のパディング長領域のコードが示すデータ長に基づいて、改ざんが検出されなかった連結文ＡＰＴから、パディングｐｄを除去して、情報処理装置１０１での平文ＰＴと同一の平文ＰＴを得ることができる。

[0044] （情報処理装置１０１または改ざん検出装置１０２のハードウェア構成例）

図２は、実施の形態にかかる情報処理装置１０１または改ざん検出装置１０２のハードウェア構成例を示すブロック図である。実施の形態では、情報処理装置１０１と改ざん検出装置１０２とは、同一のハードウェア構成であるとする。

[0045] 図２において、情報処理装置１０１または改ざん検出装置１０２は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）２０１と、ＲＯＭ（Ｒｅａｄ-Ｏｎｌｙ Ｍｅｍｏｒｙ）２０２と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２０３と、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）２０４と、暗号化回路２０５と、Ｉ／Ｆ（Ｉｎｔｅｒｆａｃｅ）２０６と、ディスプレイ２０７と、キーボード２０８と、を備えている。また、各構成部はバス２００によってそれぞれ接続されている。

[0046] ここで、ＣＰＵ２０１は、情報処理装置１０１または改ざん検出装置１０２の全体の制御を司る。ＲＯＭ２０２は、ブートプログラムなどのプログラムを記憶している。また、ＲＯＭ２０２は、ＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）を記憶している。ＲＡＭ２０３は、ＣＰＵ２０１のワークエリアとして使用される。ＨＤＤ２０４は、ＣＰＵ２０１の制御にしたがって内蔵するハードディスクに対するデータのリード／ライトを制御する駆動装置である。暗号化回路２０５は、データを暗号化したり、暗号化されたデータを復号する。

[0047] インターフェース（以下、「Ｉ／Ｆ」と略する。）２０６は、通信回線を通じてＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）、インターネットなどのネットワーク１１０に接続され、このネットワーク１１０を介して他の装置に接続される。そして、Ｉ／Ｆ２０６は、ネットワーク１１０と内部のインターフェースを司り、外部装置からのデータの入出力を制御する。Ｉ／Ｆ２０６には、たとえばモデムやＬＡＮアダプタなどを採用することができる。

[0048] ディスプレイ２０７は、カーソル、アイコンあるいはツールボックスをは

じめ、文書、画像、機能情報などのデータを表示する。このディスプレイ２０７は、たとえば、ＣＲＴ、ＴＦＴ液晶ディスプレイ、プラズマディスプレイなどを採用することができる。キーボード２０８は、文字、数字、各種指示などの入力のためのキーを備え、データの入力をおこなう。また、タッチパネル式の入力パッドやテンキーなどであってもよい。

[0049] 次に、図３および図４を用いて、情報処理装置１０１の機能および改ざん検出装置１０２の機能について説明する。ただし、１装置が情報処理装置１０１の機能と改ざん検出装置１０２の機能とを併せて持っていてもよい。

[0050] （情報処理装置１０１の機能的構成例）

まず、図３を用いて、情報処理装置１０１の機能的構成例について説明する。

[0051] 図３は、情報処理装置１０１の機能的構成を示すブロック図である。情報処理装置１０１は、特定部３０１と、算出部３０２と、第１の生成部３０３と、第２の生成部３０４と、作成部３０５と、連結部３０６と、出力部３０７と、暗号化部３０８と、第３の生成部３０９と、を含む構成である。この制御部となる機能（特定部３０１～暗号化部３０８）は、具体的には、例えば、図２に示したＲＯＭ２０２、ＲＡＭ２０３などの記憶装置に記憶されたプログラムをＣＰＵ２０１に実行させることにより、または、Ｉ／Ｆ２０６により、その機能を実現する。なお、各機能部によって処理されたデータは、ＲＡＭ２０３などの記憶領域に記憶される。

[0052] 特定部３０１は、平文データのデータ長より長く、かつ、所定のブロック長ｂｌの倍数となるデータ長を特定する機能を有する。ここで、平文データとは、ブロック暗号による暗号化の対象となるデータであり、上述した平文ＰＴである。所定のブロック長ｂｌとは、ブロック暗号に規定される分割単位となる１ブロックのデータ長であり、例えば、上述したブロック長ｂｌ＝１６［ｂｙｔｅ］である。

[0053] 具体的には、例えば、特定部３０１は、平文データのデータ長より長く、かつ、所定のブロック長ｂｌの倍数となるデータ長群の中において、最も短

いデータ長を特定する。すなわち、特定部３０１は、平文ＰＴを最小で何ブロックに分割すれば暗号化可能かを判断して、暗号化に必要となる最小のブロック数におけるデータ長を算出する。より具体的には、例えば、特定部３０１は、ブロック長ｂｌが１６［ｂｙｔｅ］、平文ＰＴが４４［ｂｙｔｅ］とすると、平文ＰＴは最小３ブロックに分割すれば暗号化可能であるため、ブロック長ｂｌの３倍の４８［ｂｙｔｅ］を特定する。

[0054] これにより、特定部３０１は、平文ＰＴが最小何ブロックに分割すればブロック暗号化できるかに基づいて、連結文ＡＰＴのデータ長となるブロック長ｂｌの倍数のデータ長を特定することができる。ここで、特定部３０１が連結文ＡＰＴのデータ長を特定することにより、作成される連結文ＡＰＴのデータ長を制限することができる。

[0055] 算出部３０２は、平文データのデータ長と特定部３０１によって特定されたデータ長との差分のデータ長を算出する機能を有する。ここで、差分のデータ長とは、パディング長ｐｌとなるデータ長である。具体的には、例えば、算出部３０２は、平文ＰＴが４４［ｂｙｔｅ］、特定部３０１によって特定されたデータ長が４８［ｂｙｔｅ］とすると、パディング長ｐｌとなる差分のデータ長４［ｂｙｔｅ］を算出する。これにより、算出部３０２は、パディング長ｐｌを算出できる。

[0056] 第１の生成部３０３は、算出部３０２によって算出された差分のデータ長を示す第１のコードを生成する機能を有する。ここで、第１のコードとは、差分のデータ長を示す２進数のコードである。

[0057] 具体的には、例えば、第１の生成部３０３は、差分のデータ長を示す第１のコードを、所定のブロック長ｂｌを示すことができる最も短いデータ長で生成する。ここで、所定のブロック長ｂｌを示すことができる最も短いデータ長とは、パディング長ｐｌとなりうる最長のデータ長であるブロック長ｂｌを示すために必要かつ最も短いデータ長である。

[0058] より具体的には、例えば、第１の生成部３０３は、ブロック長ｂｌが１６［ｂｙｔｅ］、差分のデータ長が４［ｂｙｔｅ］であれば、１６を示すこと

ができる最も短いデータ長の４［ｂｉｔ］で、差分のデータ長４［ｂｙｔｅ］を示す第１のコードを生成する。すなわち、第１の生成部３０３は、差分のデータ長４［ｂｙｔｅ］を示すコード４（１６進数表記、なお、２進数表記では「０１００」である）を生成する。

[0059] これにより、第１の生成部３０３は、改ざん検出装置１０２においてパディングｐｄを除去するために必要となるパディング長ｐｌを示すコードを生成することができる。

[0060] 第２の生成部３０４は、平文データに基づいて算出される第２のコードを、差分のデータ長から第１の生成部３０３によって生成された第１のコードのデータ長を引いた残余のデータ長以内のデータ長で生成する機能を有する。ここで、第２のコードとは、平文ＰＴから算出されたコードであり、例えば、平文ＰＴからハッシュ関数により算出したハッシュ値（例えば、ＣＲＣ）、または、平文ＰＴから算出したパリティ符号である。第１のコードのデータ長とは、上述したパディング長領域長ｌｌ以下である。

[0061] 具体的には、例えば、第２の生成部３０４は、平文データから算出する第２のコードを、差分のデータ長から第１のコードのデータ長を引いた残余のデータ長で生成する機能を有する。より具体的には、例えば、パディング長ｐｌを４［ｂｙｔｅ］、パディング長領域長ｌｌを４［ｂｉｔ］とすると、残余のデータ長は２８［ｂｉｔ］となるから、第２の生成部３０４は、平文ＰＴからＣＲＣを２８［ｂｉｔ］で生成する。

[0062] ここで、ＣＲＣの算出には、例えば、ＲＯＭ２０２に記憶されているＡＰＩを用いる。ＲＯＭ２０２に複数のデータ長のＣＲＣのそれぞれを算出する複数のＡＰＩを記憶しておき、算出するＣＲＣのデータ長に応じてＡＰＩを使い分けてＣＲＣを算出してもよい。また、ＲＯＭ２０２には算出しうるＣＲＣのうち、最長のデータ長のＣＲＣを算出するＡＰＩのみを記憶しておき、必要なデータ長に応じて算出したＣＲＣの一部を抜き出してもよい。

[0063] これにより、第２の生成部３０４は、改ざん検出装置１０２における改ざんの検出の指標となる平文ＰＴから算出するコードを、格納領域長ｃｌで生

成することができる。

[0064] 作成部３０５は、第２の生成部３０４によって生成された第２のコードを含み、第１のコードを末尾とするパディングを、差分のデータ長で作成する機能を有する。具体的には、例えば、作成部３０５は、第１のコードを末尾とし、第２のコードを先頭とするパディングを作成する。

[0065] より具体的には、例えば、作成部３０５は、第１のコードを末尾とし、第２のコードを先頭とするパディングを作成する。より具体的には、例えば、作成部３０５は、パディング長ｐｌを示すコードを末尾とし、平文ＰＴから算出するＣＲＣを先頭とするパディングｐｄを、算出されたパディング長ｐｌで作成する。パディング長ｐｌを７［ｂｙｔｅ］とし、ＣＲＣを３２［ｂｉｔ］の「６３３５０３７３」とすると、パディングｐｄは、パディング長ｐｌを示す「７」を末尾とし、「６３３５０３７３」を先頭とする７［ｂｙｔｅ］の「６３３５０３７３０７０７０７」となる。なお、パディングｐｄは、１６進数表記である。

[0066] また、パディング長ｐｌを４［ｂｙｔｅ］とし、ＣＲＣを２８［ｂｉｔ］の「３Ｆ４５９Ａ１」とすると、パディングｐｄは、パディング長ｐｌを示す「４」を末尾とし、「３Ｆ４５９Ａ１」を先頭とするデータ長４［ｂｙｔｅ］の「３Ｆ４５９Ａ１４」となる。なお、パディングｐｄは、１６進数表記である。

[0067] また、具体的には、例えば、作成部３０５は、第１のコードを末尾とし、第２のコードを第１のコードの先頭と隣接させたパディングを、差分のデータ長で作成する。より具体的には、例えば、作成部３０５は、パディング長ｐｌを示すコードを末尾とし、平文ＰＴから算出するＣＲＣをパディング長ｐｌを示すコードの先頭と隣接させたパディングｐｄを、算出されたパディング長ｐｌで作成する。ここで、パディング長ｐｌを７［ｂｙｔｅ］とし、ＣＲＣを３２［ｂｉｔ］の「６３３５０３７３」とする場合を想定する。この場合、パディングｐｄは、パディング長ｐｌを示す「７」を末尾とし、「６３３５０３７３」をパディング長ｐｌを示すコードの先頭と隣接させた７

［ｂｙｔｅ］の「０７０７０６３３５０３７３７」となる。なお、パディングｐｄは、１６進数表記である。

[0068] また、作成部３０５は、第３の生成部３０９によって生成されたパディング長ｐｌに対応するコードを、パディング長領域と格納領域以外の領域に格納してもよい。

[0069] これにより、作成部３０５は、改ざん検出装置１０２において、パディングｐｄの除去に必要となるパディング長と、改ざんの検出の指標となる平文ＰＴから算出するコードと、を含むパディングｐｄを作成することができる。また、第３の生成部３０９によって生成された改ざん検出装置１０２においてパディング長ｐｌが正しいかを判定する指標となるコードをさらに含むパディングを作成することができる。

[0070] 連結部３０６は、作成部３０５によって作成されたパディングを平文データの末尾に連結させて連結データを生成する機能を有する。ここで、連結データとは、上述した連結文ＡＰＴである。具体的には、例えば、連結部３０６は、平文ＰＴの末尾にパディングｐｄを連結させて、データ長がブロック長ｂｌの倍数となる連結文ＡＰＴを生成する。これにより、連結部３０６は、ブロック暗号による暗号化が可能となるデータ長がブロック長ｂｌの倍数となる連結文ＡＰＴを生成することができる。

[0071] 出力部３０７は、連結部３０６によって得られた連結データを出力する機能を有する。具体的には、例えば、出力部３０７は、Ｉ／Ｆ２０６によりネットワーク１１０を介して他の装置に連結文ＡＰＴを送信する。また、出力部３０７は、光ディスクドライブを介して光ディスクに連結文ＡＰＴを出力する。

[0072] 出力部３０７は、暗号化部３０８によって所定のブロック長ｂｌごとに暗号化された暗号化連結データを出力する機能を有する。ここで、暗号化連結データとは、連結文ＡＰＴをブロック長ｂｌごとに暗号化して生成した１暗号化ブロック、または、一連の暗号化ブロックである。

[0073] 具体的には、例えば、出力部３０７は、Ｉ／Ｆ２０６によりネットワーク

１１０を介して改ざん検出装置１０２に、連結文ＡＰＴをブロック長ｂｌごとに暗号化して生成した暗号化ブロックを送信する。また、暗号化部３０８による暗号化の際に、初期化ベクトルＩＶを使用した場合は、初期化ベクトルＩＶを暗号化ブロックと併せて送信する。なお、初期化ベクトルＩＶは、秘匿された情報である必要はなく、暗号化せずに送信されてもよい。また、出力部３０７は、光ディスクドライブを介して光ディスクに、連結文ＡＰＴをブロック長ｂｌごとに暗号化して生成した暗号化ブロックを出力する。

[0074] 暗号化部３０８は、連結データを、暗号化と復号に共通して使用される鍵を用いて所定のブロック長ｂｌごとに暗号化する機能を有する。暗号化と復号に共通して使用される鍵とは、共通鍵である。具体的には、例えば、暗号化部３０８は、連結文ＡＰＴをブロック長ｂｌごとに分割して、共通鍵を用いたブロック暗号により、暗号化して、暗号化ブロックを生成する。

[0075] より具体的には、例えば、暗号化部３０８は、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）方式やＡＥＳ方式（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）の暗号化回路２０５を用いて暗号化をおこなう。ＤＥＳ方式ではブロック長ｂｌ＝８［ｂｙｔｅ］であり、ＡＥＳ方式ではブロック長ｂｌ＝１６［ｂｙｔｅ］である。また、各暗号化方式には複数の動作モードが規定されており、それらの動作モードに応じて、具体的な暗号化および復号化処理がおこなわれる。

[0076] 動作モードとしては、ＤＥＳ方式、ＡＥＳ方式ともに、ＥＣＢ（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｄｅｂｏｏｋ）モードとＣＢＣ（Ｃｉｐｈｅｒ Ｂｌｏｃｋ Ｃｈａｉｎｉｎｇ）モードとＣＦＢ（Ｃｉｐｈｅｒ Ｆｅｅｄｂａｃｋ）モードとＯＦＢ（Ｏｕｔｐｕｔ Ｆｅｅｄｂａｃｋ）モードとＣＴＲ（Ｃｏｕｎｔｅｒ）モードが利用できる。なお、暗号化に使用される初期化ベクトルＩＶとしては、例えば、暗号化ごとに生成された乱数を採用できる。

[0077] これにより、暗号化部３０８は、共通鍵を用いたブロック暗号により、連結文ＡＰＴをブロック長ｂｌごとに暗号化して、連結文ＡＰＴの秘匿性を確保することができる。

[0078] 第３の生成部３０９は、第１のコードを特定する第３のコードを、差分のデータ長から第１のコードのデータ長と所定のデータ長とを引いた残余のデータ長で生成する機能を有する。ここで、第３のコードとは、パディング長ｐｌに対応するコードである。

[0079] 具体的には、例えば、第３の生成部３０９は、パディング長を示す１ｂｙｔｅコードを連続して並べたコードの先頭から抽出した残余の領域のデータ長分のコードを生成する。これにより、第３の生成部３０９は、改ざん検出装置１０２にて、パディング長ｐｌが正しいかを判定する指標となるコードを生成できる。

[0080] （改ざん検出装置１０２の機能的構成例）

次に、まず、図４を用いて、改ざん検出装置１０２の機能的構成例について説明する。

[0081] 図４は、改ざん検出装置１０２の機能的構成を示すブロック図である。改ざん検出装置１０２は、入力部４０１と、復号部４０２と、第１の抽出部４０３と、決定部４０４と、第２の抽出部４０５と、第３の抽出部４０６と、生成部４０７と、判定部４０８と、出力部４０９と、を含む構成である。この制御部となる機能（入力部４０１～出力部４０９）は、具体的には、たとえば、図２に示したＲＯＭ２０２、ＲＡＭ２０３などの記憶装置に記憶されたプログラムをＣＰＵ２０１に実行させることにより、または、Ｉ／Ｆ２０６により、その機能を実現する。なお、各機能部によって処理されたデータは、ＲＡＭ２０３などの記憶領域に記憶される。

[0082] 入力部４０１は、平文データを所定のブロック長ｂｌごとに暗号化した暗号化データを入力する機能を有する。ここで、平文データとは、上述した平文ＰＴである。暗号化データとは、上述した暗号化ブロックである。

[0083] 具体的には、例えば、入力部４０１は、Ｉ／Ｆ２０６によりネットワーク１１０を介して情報処理装置１０１から、暗号化ブロックを受信する。また、入力部４０１は、光ディスクドライブを介して光ディスクから、暗号化ブロックを読み取る。これにより、入力部４０１は、改ざん検出の対象となる

暗号化ブロックを入力することができる。

[0084] 復号部４０２は、入力部４０１によって入力された暗号化データから、暗号化と復号に共通して使用される鍵を用いて復号した復号データを生成する機能を有する。暗号化と復号に共通して使用される鍵とは、共通鍵である。復号データとは、改ざんされていない暗号化ブロックから復号した場合は、情報処理装置１０１での連結文ＡＰＴである。ただし、復号データとは、改ざんされた暗号化ブロックから復号した場合は、情報処理装置１０１での連結文ＡＰＴとは内容の異なる連結文ＡＰＴ’となる。

[0085] 具体的には、例えば、復号部４０２は、共通鍵を用いたブロック暗号のＣＢＣモードにより、初期化ベクトルＩＶ（Ｉｎｉｔｉａｌ　Ｖｅｃｔｏｒ）と暗号化ブロックから、連結文ＡＰＴまたは、連結文ＡＰＴ’を復号する。なお、初期化ベクトルＩＶは、情報処理装置１０１が暗号化に使用した初期化ベクトルＩＶと同一データである。これにより、復号部４０２は、暗号化ブロックから、連結文を復号できる。

[0086] 第１の抽出部４０３は、パディングｐｄのデータ長を格納する復号データの末尾となる第１の領域から、第１のコードを抽出する機能を有する。ここで、第１の領域とは、上述したパディング長領域である。第１のコードとは、暗号化ブロックの改ざんがなかった場合、または、パディングｐｄに改ざんの影響がなかった場合、パディング長ｐｌである。一方、第１のコードとは、パディングｐｄに改ざんの影響があった場合、無意味なコードである。

[0087] 具体的には、例えば、第１の抽出部４０３は、復号部４０２によって復号された連結文の末尾４［ｂｉｔ］を参照して、パディング長ｐｌと推定される４［ｂｙｔｅ］を抽出する。これにより、第１の抽出部４０３は、パディング長ｐｌと推定されるデータ長を抽出できる。

[0088] 決定部４０４は、第１の抽出部４０３によって抽出された第１のコードが示すデータ長に基づいて、平文データから算出されたコードを格納する復号データの第２の領域を決定する機能を有する。ここで、第２の領域とは、第１の抽出部４０３によって抽出されたパディング長ｐｌから推定される平文

ＰＴから算出されたコードの格納領域である。

[0089] 具体的には、例えば、決定部４０４は、第１の領域の先頭と接する領域であって、第１のコードが示すデータ長から第１の領域のデータ長を引いた残余のデータ長の領域を、第２の領域に決定する。より具体的には、例えば、第１の抽出部４０３は、パディング長ｐｌが４［ｂｙｔｅ］であれば、パディング長領域の先頭と接する２８［ｂｉｔ］の領域を格納領域に決定する。これにより、決定部４０４は、情報処理装置１０１が平文ＰＴから算出したコードを格納した格納領域と推定される領域を決定することができる。

[0090] また、例えば、決定部４０４は、第２の領域の先頭に接する復号データ内の領域であって、第１のコードが示すデータ長から第１のコードのデータ長と所定のデータ長とを引いた残余のデータ長の領域を、第４の領域として決定する。これにより、決定部４０４は、情報処理装置１０１がパディングに対応するコードを格納した領域と推定される領域を決定することができる。

[0091] 第２の抽出部４０５は、決定部４０４によって決定された第２の領域から第２のコードを抽出する機能を有する。ここで、第２のコードとは、暗号化ブロックが改ざんされなかった場合、または、パディングｐｄに改ざんの影響がなかった場合、情報処理装置１０１が格納した平文ＰＴから算出されたコード（例えば、ＣＲＣ）である。一方、第２のコードとは、パディングｐｄに改ざんの影響があった場合、改ざんの影響を受けた無意味なコードである。

[0092] 具体的には、例えば、第２の抽出部４０５は、ＣＲＣの格納領域として推定された領域から、情報処理装置１０１が格納したＣＲＣ、または、改ざんの影響を受けた無意味なコードを抽出する。これにより、第２の抽出部４０５は、改ざんの検出の指標となるコードを抽出することができる。

[0093] 第３の抽出部４０６は、第１のコードが示すデータ長となる復号データの末尾領域を除いた復号データの第３の領域から第３のコードを抽出する機能を有する。ここで、末尾領域とは、復号部４０２によって復号された連結文の末尾となる領域であり、暗号化ブロックが改ざんされなかった場合、また

は、パディングｐｄに改ざんの影響がない場合、パディングｐｄである。一方、末尾領域とは、復号部４０２によって復号された連結文の末尾となる領域であり、パディングｐｄに改ざんの影響があった場合、無意味な領域である。

[0094] 具体的には、例えば、第３の抽出部４０６は、パディングｐｄと推定される末尾データを除いた情報処理装置１０１での平文ＰＴ、または、改ざんされた平文ＰＴ’を抽出する。これにより、第３の抽出部４０６は、改ざんの検出の対象となる平文を抽出することができる。

[0095] 生成部４０７は、第３の抽出部４０６によって抽出された第３のコードを特定する第４のコードを、第２のコードのデータ長と同一データ長で生成する機能を有する。第４のコードとは、第３のコードを特定するコードであり、例えば、第３のコードからハッシュ関数により得られるハッシュ値（例えば、ＣＲＣ）、第３のコードから得られるパリティ符号である。

[0096] 具体的には、例えば、第２のコードが２８［ｂｉｔ］であれば、第３のコードから２８［ｂｉｔ］のＣＲＣを生成する。これにより、生成部４０７は、情報処理装置１０１での平文ＰＴから算出されるコード、または、改ざんされた平文ＰＴ’から算出されるコードを生成することができる。または第２のコードの長さは鍵と同様に事前に共有しておいてもよい。

[0097] 判定部４０８は、生成部４０７によって生成された第４のコードと第２のコードとの一致判定をおこなう機能を有する。具体的には、例えば、判定部４０８は、平文ＰＴから算出したＣＲＣとパディングｐｄに格納されていたＣＲＣとの一致判定をおこなう。

[0098] また、判定部４０８は、暗号化ブロックの改ざんの影響を受けた平文ＰＴ’から算出したＣＲＣ’とパディングｐｄに格納されていたＣＲＣとの一致判定をおこなう。また、判定部４０８は、暗号化ブロックの改ざんの影響を受けた平文ＰＴ’から算出したＣＲＣ’と暗号化ブロックの改ざんの影響を受けたパディングｐｄに格納されていたＣＲＣ’’との一致判定をおこなう。

[0099] これにより、判定部４０８は、第３の抽出部４０６に抽出された平文が改ざんの影響を受けていない場合は、一致判定により一致すると判定され、改ざんなしと判定できる。また、判定部４０８は、第３の抽出部４０６に抽出された平文が改ざんの影響を受けている場合は、一致判定により一致しないと判定され、改ざんありと判定できる。

[0100] また、判定部４０８は、第４の抽出部４１０によって抽出された第５のコードにより特定されるコードと第１のコードとの一致判定をおこなう機能を有する。具体的には、情報処理装置１０１が格納したパディング長ｐｌに対応するコードから、第１の抽出部４０３が抽出したコードが正しいコードか判定する。これにより、判定部４０８は、正しいコードでない場合は、改ざんありと判定できる。

[0101] 出力部４０９は、判定部４０８によって判定された判定結果を出力する機能を有する。具体的には、例えば、出力部４０９は、ディスプレイ２０７に、第４のコードと第２のコードとが一致したこと、すなわち、受信した暗号化ブロックは改ざんされていないことを出力する。また、出力部４０９は、ディスプレイ２０７に、第４のコードと第２のコードとが一致していないこと、すなわち、受信した暗号化ブロックは改ざんされていることを出力する。

[0102] これにより、出力部４０９は、受信した暗号化ブロックの改ざんの有無、すなわち、第３の抽出部４０６によって抽出された平文に改ざんの影響があるか否かを、出力することができる。また復号結果の復号データをディスクに出力する。

[0103] 第４の抽出部４１０は、第１のコードを特定するコードを格納する第４の領域から第５のコードを抽出する機能を有する。具体的には、例えば、第４の抽出部４１０は、決定部４０４によって決定された情報処理装置１０１がパディング長ｐｌに対応するコードを格納したと推定される領域に格納されているコードを抽出する。これにより、第４の抽出部４１０は、パディングｐｄが改ざんの影響を受けていない場合は、情報処理装置１０１が格納した

パディング長ｐｌに対応するコードを抽出できる。

[0104] （連結文ＡＰＴのデータ構造）

次に、図５を用いて、連結文ＡＰＴのデータ構造について説明する。

[0105] 図５は、連結文ＡＰＴのデータ構造の一例を示す説明図である。ここで、平文ＰＴ１～ＰＴ７は、ブロック暗号により暗号化される平文ＰＴである。ここでは、ブロック長ｂｌを１６［ｂｙｔｅ］とする。平文ＰＴに連結されるパディングｐｄは、末尾をパディング長領域とし、ＣＲＣの格納領域を含む。

[0106] ＣＲＣの格納領域は、パディング長領域の先頭に接する領域である。パディング長領域長ｌｌは、ブロック長ｂｌ＝１６［ｂｙｔｅ］を示すために必要な最小限のデータ長となる４［ｂｉｔ］である。ＣＲＣの格納領域長ｃｌは、最大３２［ｂｉｔ］である。パディングｐｄの内容は、１６進数表記とする。ただし、ＣＲＣは、「＄」で示す。

[0107] また、パディングｐｄは、パディング長領域と格納領域とを除いた残余の領域がある場合、パディング長ｐｌに対応するコードを残余の領域に格納する。パディング長ｐｌに対応するコードとは、パディング長を示す１ｂｙｔｅコードを連続して並べたコードの先頭から抽出した残余の領域のデータ長分のコードである。

[0108] 平文ＰＴ１は、ブロック長ｂｌの倍数長より１５［ｂｙｔｅ］長いデータ長のデータである。そのため、平文ＰＴ１を、ブロック暗号により暗号化するためには、１［ｂｙｔｅ］のパディングｐｄが必要となる。パディングｐｄは、末尾４［ｂｉｔ］となるパディング長領域にパディング長ｐｌである１［ｂｙｔｅ］を示す１を含み、パディング長領域の先頭に接する残余の４［ｂｉｔ］となる格納領域に平文ＰＴ１から得られたＣＲＣを含む。

[0109] 平文ＰＴ２は、ブロック長ｂｌの倍数長より１４［ｂｙｔｅ］長いデータ長のデータである。そのため、平文ＰＴ２を、ブロック暗号により暗号化するためには、２［ｂｙｔｅ］のパディングｐｄが必要となる。パディングｐｄは、末尾４［ｂｉｔ］となるパディング長領域にパディング長ｐｌである

２［ｂｙｔｅ］を示す２を含み、パディング長領域の先頭に接する残余の１２［ｂｉｔ］となる格納領域に平文ＰＴ２から得られたＣＲＣを含む。

[0110] 平文ＰＴ３は、ブロック長ｂｌの倍数長より１３［ｂｙｔｅ］長いデータ長のデータである。そのため、平文ＰＴ３を、ブロック暗号により暗号化するためには、３［ｂｙｔｅ］のパディングｐｄが必要となる。パディングｐｄは、末尾４［ｂｉｔ］となるパディング長領域にパディング長ｐｌである３［ｂｙｔｅ］を示す３を含み、パディング長領域の先頭に接する残余の２０［ｂｉｔ］となる格納領域に平文ＰＴ３から得られたＣＲＣを含む。

[0111] 平文ＰＴ４は、ブロック長ｂｌの倍数長より１２［ｂｙｔｅ］長いデータ長のデータである。そのため、平文ＰＴ４を、ブロック暗号により暗号化するためには、４［ｂｙｔｅ］のパディングｐｄが必要となる。パディングｐｄは、末尾４［ｂｉｔ］となるパディング長領域にパディング長ｐｌである４［ｂｙｔｅ］を示す４を含み、パディング長領域の先頭に接する残余の２８［ｂｉｔ］となる格納領域に平文ＰＴ４から得られたＣＲＣを含む。

[0112] 平文ＰＴ５は、ブロック長ｂｌの倍数長より１１［ｂｙｔｅ］長いデータ長のデータである。そのため、平文ＰＴ５を、ブロック暗号により暗号化するためには、５［ｂｙｔｅ］のパディングｐｄが必要となる。パディングｐｄは、末尾４［ｂｉｔ］となるパディング長領域にパディング長ｐｌである５［ｂｙｔｅ］を示す５を含み、パディング長領域の先頭に接する残余の３６［ｂｉｔ］のうちの３２［ｂｉｔ］となる格納領域に平文ＰＴ５から得られたＣＲＣを含む。

[0113] また、パディングｐｄは、残余の４［ｂｉｔ］に、パディング長ｐｌ＝５［ｂｙｔｅ］に対応するコード「０」を含む。コード「０」とは、パディング長ｐｌを示す１ｂｙｔｅコードを連続して並べた「０５０５０５０５…」の先頭４［ｂｉｔ］である。

[0114] 平文ＰＴ６は、ブロック長ｂｌの倍数長より１０［ｂｙｔｅ］長いデータ長のデータである。そのため、平文ＰＴ６を、ブロック暗号により暗号化するためには、６［ｂｙｔｅ］のパディングｐｄが必要となる。パディングｐ

ｄは、末尾４［ｂｉｔ］となるパディング長領域にパディング長ｐｌである６［ｂｙｔｅ］を示す６を含み、パディング長領域の先頭に接する残余の４４［ｂｉｔ］のうちの３２［ｂｉｔ］となる格納領域に平文ＰＴ６から得られたＣＲＣを含む。

[0115] また、パディングｐｄは、残余の１２［ｂｉｔ］に、パディング長ｐｌ＝６［ｂｙｔｅ］に対応するコード「０６０」を含む。コード「０６０」とは、パディング長ｐｌを示す１ｂｙｔｅコードを連続して並べた「０６０６０６０６…」の先頭１２［ｂｉｔ］である。

[0116] 平文ＰＴ７は、ブロック長ｂｌの倍数長のデータである。しかし、パディングｐｄを連結しない場合、パディングｐｄを連結していないことを示す情報を平文ＰＴ７に連結する必要があり、結果として、平文ＰＴ７は、ブロック長ｂｌの倍数長とならない。すなわち、平文ＰＴ７が、ブロック長ｂｌの倍数長のデータであっても、パディングｐｄを連結する必要がある。

[0117] そのため、平文ＰＴ７を、ブロック暗号により暗号化するためには、１６［ｂｙｔｅ］のパディングｐｄが必要となる。パディングｐｄは、末尾４［ｂｉｔ］となるパディング長領域にパディング長ｐｌである１６［ｂｙｔｅ］を示す「０」を含み、パディング長領域の先頭に接する残余の１２４［ｂｉｔ］のうちの３２［ｂｉｔ］となる格納領域に平文ＰＴ７から得られたＣＲＣを含む。

[0118] また、パディングｐｄは、残余の９２［ｂｉｔ］に、パディング長ｐｌ＝１６［ｂｙｔｅ］に対応するコード「１０１０１０１０１０１０１０１０１０１」を含む。コード「１０１０１０１０１０１０１０１０１０１」とは、パディング長ｐｌを示す１ｂｙｔｅコードを連続して並べた「１０１０１０１０１０１０１０１０１０１０…」の先頭９２［ｂｉｔ］である。

[0119] ここで、格納領域としては、パディングｐｄの先頭となる最大３２［ｂｉｔ］の領域を採用してもよい。また、格納領域として、閾値３２［ｂｉｔ］を設けず、パディングｐｄの残余の全ての領域を採用してもよい。

[0120] 格納領域に格納される平文ＰＴから算出するコードとして、ハッシュ値を採用してもよい。また、格納領域に格納される平文ＰＴから算出するコードとして、パリティを採用してもよい。また、パディング長ｐｌに対応するコードとして、ハッシュ値を採用してもよいし、パリティを採用してもよい。

[0121] 各データ長のＣＲＣを算出する場合は、各データ長に対応するＣＲＣ計算関数によりＣＲＣを算出してもよい。また、パディング長ｐｌに関わらず、所定のデータ長でＣＲＣを算出して、先頭から必要なデータ長のコードを抽出して算出してもよい。例えば、情報処理装置１０１は、パディング長ｐｌが８［ｂｉｔ］の場合に、３２［ｂｉｔ］のＣＲＣを算出し、ＣＲＣの先頭４［ｂｉｔ］を抽出して、格納領域に格納する。

[0122] （改ざん検出の具体例１）

次に、図６および図７を用いて、改ざん検出の具体例１について説明する。ここでは、情報処理装置１０１は、ブロック暗号のＣＢＣモードにより暗号化をおこなう。また、改ざん検出装置１０２は、ブロック暗号のＣＢＣモードにより復号をおこなう。

[0123] 図６は、情報処理装置１０１による平文ＰＴの暗号化の具体例１を示す説明図である。ここで、情報処理装置１０１は、ブロック長ｂｌの倍数長より９［ｂｙｔｅ］長いデータ長となる平文ＰＴを暗号化する。

[0124] よって、情報処理装置１０１は、ブロック暗号による暗号化のために、平文ＰＴに７［ｂｙｔｅ］のパディングｐｄを連結して連結文ＡＰＴを生成する。次に、情報処理装置１０１は、連結文ＡＰＴをブロック長ｂｌごとに分割して、ブロックＢ１～Ｂｎを生成する。そして、情報処理装置１０１は、ブロックＢ１～Ｂｎを、ブロック暗号のＣＢＣモードにより暗号化して、暗号化ブロックＣ１～Ｃｎを生成する。

[0125] 具体的には、情報処理装置１０１は、末尾をパディング長ｐｌ＝７［ｂｙｔｅ］を示す７とし、３２［ｂｉｔ］のＣＲＣ「６３３５０３７３」を含み、残余をパディング長ｐｌ＝７［ｂｙｔｅ］に対応する「０７０７０」とするパディングｐｄを、平文ＰＴに連結する。

[0126] 次に、情報処理装置１０１は、パディングｐｄを連結した連結文ＡＰＴをブロック長ｂｌごとに分割して、ブロックＢ１～Ｂｎを生成する。生成されたブロックＢｎには、パディングｐｄが含まれる。

[0127] そして、情報処理装置１０１は、生成されたブロックＢ１～Ｂｎごとに暗号化して、暗号化ブロックＣ１～Ｃｎを生成する。例えば、情報処理装置１０１は、先頭から１番目のブロックＢ１を暗号化する場合、ブロックＢ１と初期化ベクトルＩＶとの排他的論理和をとり、共通鍵で暗号化して、暗号化ブロックＣ１を生成する。また、情報処理装置１０１は、先頭からｉ番目のブロックＢｉを暗号化する場合、ブロックＢｉと暗号化ブロックＣｉ－１との排他的論理和をとり、共通鍵で暗号化して、暗号化ブロックＣｉを生成する。

[0128] 情報処理装置１０１は、生成した暗号化ブロックＣ１～Ｃｎを改ざん検出装置１０２に送信する。次に、送信された暗号化ブロックＣ１～Ｃｎを受信した改ざん検出装置１０２による改ざんの検出について説明する。

[0129] 図７は、改ざん検出装置１０２による改ざん検出の具体例１を示す説明図である。ここで、情報処理装置１０１により送信された図６に示した暗号化ブロックＣ１～Ｃｎは、改ざんされずに改ざん検出装置１０２に受信されたとする。そして、改ざん検出装置１０２は、受信した暗号化ブロックＣ１～Ｃｎの改ざんの有無を検出する。

[0130] 具体的には、まず、改ざん検出装置１０２は、暗号化ブロックＣ１～Ｃｎからブロック Ｂ１～Ｂｎを復号する。例えば、改ざん検出装置１０２は、先頭から１番目の暗号化ブロックＣ１を復号する場合、暗号化ブロックＣ１を共通鍵で復号して、初期化ベクトルＩＶとの排他的論理和をとって、ブロックＢ１を生成する。また、改ざん検出装置１０２は、先頭からｉ番目の暗号化ブロックＣｉを復号する場合、暗号化ブロックＣｉを共通鍵で復号して、暗号化ブロックＣｉ－１との排他的論理和をとり、ブロックＢｉを生成する。

[0131] 次に、改ざん検出装置１０２は、生成した最終ブロックＢｎの末尾となる

パディング長領域からパディング長ｐｌを抽出する。ここで、改ざん検出装置１０２は、パディングｐｄの末尾７を抽出し、パディング長ｐｌを７［ｂｙｔｅ］と判断する。

[0132] 改ざん検出装置１０２は、抽出したパディング長ｐｌ＝７［ｂｙｔｅ］が正しいか否かを判断するため、パディングｐｄから、パディング長ｐｌに対応するコードを抽出する。パディング長ｐｌに対応するコードとして、「０７０７０」が抽出される。パディング長ｐｌに対応するコードは、「０７０７０」であり、抽出されたコードと同一であるため、改ざん検出装置１０２は、パディング長ｐｌ＝７［ｂｙｔｅ］を正しいと判断する。

[0133] また、改ざん検出装置１０２は、パディングｐｄからＣＲＣを抽出する。改ざん検出装置１０２は、パディング長ｐｌが７［ｂｙｔｅ］であるから、ＣＲＣの格納領域長は、３２［ｂｉｔ］であると判断する。そして、改ざん検出装置１０２は、ＣＲＣの格納領域から、ＣＲＣ「６３３５０３７３」を抽出する。

[0134] 改ざん検出装置１０２は、復号したブロックＢｎの末尾データ７［ｂｙｔｅ］をパディングｐｄと判断して除去し、平文ＰＴを生成する。改ざん検出装置１０２は、パディングｐｄを除去した平文ＰＴから３２［ｂｉｔ］のＣＲＣを生成する。

[0135] ここで、改ざん検出装置１０２は、抽出したＣＲＣと生成したＣＲＣとの一致判定をおこない、改ざんの有無を検出する。改ざん検出装置１０２により生成された平文ＰＴが情報処理装置１０１の平文ＰＴと同一であれば、それぞれの平文ＰＴから生成されるＣＲＣも同一となる。

[0136] ここでは、暗号化ブロックＣ１～Ｃｎの改ざんがなかったので、改ざん検出装置１０２により生成されたＣＲＣと情報処理装置１０１によりパディングｐｄに格納されたＣＲＣとは同一となる。よって、改ざん検出装置１０２は、受信した暗号化ブロックＣ１～Ｃｎの改ざんはなく、改ざん検出装置１０２にてパディングｐｄを除去して得た平文ＰＴは、情報処理装置１０１での平文ＰＴのままであると判断する。

[0137] （改ざん検出の具体例２）

次に、図８および図９を用いて、改ざん検出の具体例２について説明する。ここでは、情報処理装置１０１は、ブロック暗号のＣＢＣモードにより暗号化をおこなう。また、改ざん検出装置１０２は、ブロック暗号のＣＢＣモードにより復号をおこなう。

[0138] 図８は、情報処理装置１０１による平文ＰＴの暗号化の具体例２を示す説明図である。ここで、図６と同様にして、情報処理装置１０１は、ブロック長ｂｌの倍数長より９［ｂｙｔｅ］長いデータ長となる平文ＰＴを暗号化する。そして、暗号化ブロックＣ１～Ｃｎを改ざん検出装置１０２に送信する。

[0139] ただし、送信された暗号化ブロックＣ１～Ｃｎは、送信途中で攻撃者によりキャプチャされたとする。そして、攻撃者により、暗号化ブロックＣｎ－１が改ざんされ、暗号化ブロックＣｎ－１’に変化したとする。

[0140] 図９は、改ざん検出装置１０２による改ざん検出の具体例２を示す説明図である。ここで、図８に示した暗号化ブロックＣ１～Ｃｎ－２，Ｃｎ－１’，Ｃｎは、改ざん検出装置１０２に受信されたとする。そして、改ざん検出装置１０２は、受信した暗号化ブロックＣ１～Ｃｎ－２，Ｃｎ－１’，Ｃｎの改ざんの有無を検出する。

[0141] ここで、改ざん検出装置１０２により復号されたブロックのうち、改ざんされた暗号化ブロックＣｎ－１’に基づいて復号されたブロックは、情報処理装置１０１のブロックＢ１～Ｂｎとは異なるブロックとなる。すなわち、情報処理装置１０１の復号によりブロックＢｎ－１，Ｂｎが生成されるべき暗号化ブロックＣｎ－１’Ｃｎからは、ブロックＢｎ－１，Ｂｎとは異なるブロックＢｎ－１’，Ｂｎ’が生成される。これにより、パディングｐｄの内容が変化することになる。

[0142] ここで、改ざん検出装置１０２は、生成した最終ブロックＢｎ’の末尾となるパディング長領域からパディング長ｐｌを抽出する。ここで、改ざん検出装置１０２は、末尾６を抽出し、パディング長ｐｌを６［ｂｙｔｅ］と判

断する。

[0143] 改ざん検出装置１０２は、抽出したパディング長ｐｌ＝６［ｂｙｔｅ］が正しいか否かを判断するため、パディングｐｄから、パディング長ｐｌに対応するコードを抽出する。パディングｐｄが変化したため、パディング長ｐｌに対応するコードとして「６５１」が抽出される。パディング長ｐｌに対応するコードは、「０６０」であり、抽出されたコードとは異なるため、改ざん検出装置１０２は、パディング長ｐｌ＝６［ｂｙｔｅ］を誤りと判断する。

[0144] これにより、改ざん検出装置１０２は、暗号化ブロックの改ざんにより、パディングｐｄが変化していると判断する。そして、改ざん検出装置１０２は、ＣＲＣの一致判定をおこなわずに、改ざん検出装置１０２にてパディングｐｄを除去して得た平文ＰＴの内容は、暗号化ブロックの改ざんの影響を受けて変化していると判断する。

[0145] なお、ＣＲＣの一致判定によっても改ざんが検出される。改ざん検出装置１０２は、パディングｐｄからＣＲＣを抽出する。改ざん検出装置１０２は、パディング長ｐｌが６［ｂｙｔｅ］であるから、ＣＲＣの格納領域長は、３２［ｂｉｔ］であると判断する。そして、改ざん検出装置１０２は、ＣＲＣの格納領域から、ＣＲＣ’「６５１９８８２４３Ａ」を抽出する。

[0146] 改ざん検出装置１０２は、復号したブロックＢｎ’の末尾データ６［ｂｙｔｅ］をパディングｐｄと判断して除去し、平文を生成する。ブロックＢｎ－１’，Ｂｎ’は改ざんの影響を受けているため、情報処理装置１０１での平文ＰＴとは異なる平文ＰＴ’が生成される。改ざん検出装置１０２は、パディングｐｄを除去した平文ＰＴ’から３２［ｂｉｔ］のＣＲＣ’’を生成する。

[0147] ここで、改ざん検出装置１０２は、抽出したＣＲＣ’と生成したＣＲＣ’’との一致判定をおこない、改ざんの有無を検出する。改ざん検出装置１０２により生成された平文ＰＴ’が情報処理装置１０１の平文ＰＴと同一であれば、それぞれの平文から生成されるＣＲＣも同一となる。

[0148] ここでは、暗号化ブロックＣｎ－１’の改ざんの影響により、格納されたＣＲＣが変化し、ＣＲＣ’となっている。また、暗号化ブロックＣｎ－１’の改ざんの影響により変化した平文ＰＴ’からＣＲＣ’’が生成される。すなわち、パディングｐｄに格納されたＣＲＣ’と改ざん検出装置１０２により生成されたＣＲＣ’’は異なる。よって、改ざん検出装置１０２は、改ざん検出装置１０２にてパディングｐｄを除去して得た平文ＰＴの内容は、暗号化ブロックの改ざんの影響を受けて変化していると判断できる。

[0149] （改ざん検出の具体例３）

次に、図１０および図１１を用いて、改ざん検出の具体例３について説明する。ここでは、情報処理装置１０１は、ブロック暗号のＣＢＣモードにより暗号化をおこなう。また、改ざん検出装置１０２は、ブロック暗号のＣＢＣモードにより復号をおこなう。

[0150] 図１０は、情報処理装置１０１による平文ＰＴの暗号化の具体例３を示す説明図である。ここで、図６と同様にして、情報処理装置１０１は、ブロック長ｂｌの倍数長より９［ｂｙｔｅ］長いデータ長となる平文ＰＴを暗号化する。そして、暗号化ブロックＣ１～Ｃｎを改ざん検出装置１０２に送信する。

[0151] ただし、送信された暗号化ブロックＣ１～Ｃｎは、送信途中で攻撃者によりキャプチャされたとする。そして、攻撃者により、暗号化ブロックＣ２が改ざんされ、暗号化ブロックＣ２’に変化したとする。

[0152] 図１１は、改ざん検出装置１０２による改ざん検出の具体例３を示す説明図である。ここで、図１０に示した暗号化ブロックＣ１，Ｃ２’，Ｃ３～Ｃｎ－１，Ｃｎは、改ざん検出装置１０２に受信されたとする。そして、改ざん検出装置１０２は、受信した暗号化ブロックＣ１，Ｃ２’，Ｃ３～Ｃｎ－１，Ｃｎの改ざんの有無を検出する。

[0153] ここで、改ざん検出装置１０２により復号されたブロックのうち、改ざんされた暗号化ブロックＣ２’に基づいて復号されたブロックは、情報処理装置１０１のブロックＢ１～Ｂｎとは異なるブロックとなる。すなわち、情報

処理装置１０１の復号によりブロックＢ２，Ｂ３が生成されるべき暗号化ブロックＣ２’Ｃ３からは、ブロックＢ２，Ｂ３とは異なるブロックＢ２’，Ｂ３’が生成される。これにより、パディングｐｄの内容は変化しない。

[0154] ここで、改ざん検出装置１０２は、生成した最終ブロックＢｎの末尾となるパディング長領域からパディング長ｐｌを抽出する。ここで、改ざん検出装置１０２は、末尾７を抽出し、パディング長ｐｌを７［ｂｙｔｅ］と判断する。

[0155] 改ざん検出装置１０２は、抽出したパディング長ｐｌ＝７［ｂｙｔｅ］が正しいか否かを判断するため、パディングｐｄから、パディング長ｐｌに対応するコードを抽出する。パディングｐｄは変化していないため、パディング長ｐｌに対応するコードとして「０７０７０」が抽出される。パディング長ｐｌに対応するコードは、「０７０７０」であり、抽出されたコードと同一であるため、改ざん検出装置１０２は、パディング長ｐｌ＝７［ｂｙｔｅ］を正しいと判断する。

[0156] 改ざん検出装置１０２は、パディングｐｄからＣＲＣを抽出する。改ざん検出装置１０２は、パディング長ｐｌが７［ｂｙｔｅ］であるから、ＣＲＣの格納領域長は、３２［ｂｉｔ］であると判断する。そして、改ざん検出装置１０２は、ＣＲＣの格納領域から、ＣＲＣ「６３３５０３７３」を抽出する。

[0157] 改ざん検出装置１０２は、復号したブロックＢｎの末尾データ７［ｂｙｔｅ］をパディングｐｄと判断して除去し、平文を生成する。ブロックＢ２’，Ｂ３’は改ざんの影響を受けているため、情報処理装置１０１での平文ＰＴとは異なる平文ＰＴ’が生成される。改ざん検出装置１０２は、パディングｐｄを除去した平文ＰＴ’から３２［ｂｉｔ］のＣＲＣ’を生成する。

[0158] ここで、改ざん検出装置１０２は、抽出したＣＲＣと生成したＣＲＣ’との一致判定をおこない、改ざんの有無を検出する。改ざん検出装置１０２により生成された平文ＰＴ’が情報処理装置１０１の平文ＰＴと同一であれば、それぞれの平文から生成されるＣＲＣも同一となる。

[0159] ここでは、暗号化ブロックＣ２’の改ざんの影響により変化した平文ＰＴ’からＣＲＣ’が生成される。すなわち、パディングｐｄに格納されたＣＲＣと改ざん検出装置１０２により生成されたＣＲＣ’は異なる。よって、改ざん検出装置１０２は、改ざん検出装置１０２にてパディングｐｄを除去して得た平文ＰＴの内容は、暗号化ブロックの改ざんの影響を受けて変化していると判断できる。

[0160] （情報処理装置１０１がおこなうパディング連結処理の詳細）

次に、図１２を用いて、情報処理装置１０１がおこなうパディング連結処理の詳細について説明する。

[0161] 図１２は、情報処理装置１０１がおこなうパディング連結処理の詳細を示すフローチャートである。まず、ＣＰＵ２０１は、平文ＰＴの入力があったか否か判定する（ステップＳ１２０１）。平文ＰＴの入力がない場合（ステップＳ１２０１：Ｎｏ）、ステップＳ１２０１に戻り、ＣＰＵ２０１は、平文ＰＴの入力を待つ。一方、平文ＰＴの入力があった場合（ステップＳ１２０１：Ｙｅｓ）、ステップＳ１２０２に移行する。

[0162] 次に、ＣＰＵ２０１は、入力された平文ＰＴに連結するパディングｐｄのパディング長ｐｌを算出する（ステップＳ１２０２）。そして、ＣＰＵ２０１は、平文ＰＴの末尾に算出したパディング長ｐｌのパディングｐｄを連結する（ステップＳ１２０３）。

[0163] 次に、ＣＰＵ２０１は、算出したパディング長ｐｌに応じたＣＲＣを算出する（ステップＳ１２０４）。そして、ＣＰＵ２０１は、算出したＣＲＣを、パディングｐｄのＣＲＣの格納領域に格納する（ステップＳ１２０５）。

[0164] 次に、ＣＰＵ２０１は、ＣＲＣを格納した連結文ＡＰＴを、ブロック長ｂｌごとに、ブロック暗号のＣＢＣモードにより暗号化する（ステップＳ１２０６）。そして、ＣＰＵ２０１は、暗号化した暗号化ブロックを出力して（ステップＳ１２０７）、パディング連結処理を終了する。

[0165] これにより、情報処理装置１０１は、結果として、パディング長ｐｌを示すコードを末尾に含み、平文ＰＴから算出されるコードを格納領域に含むパ

ディングｐｄを作成できる。また、情報処理装置１０１は、結果として、パディングｐｄにパディング長領域と格納領域とを除いた残余の領域がある場合、パディング長ｐｌに対応するコードを残余の領域に含むパディングｐｄを作成できる。そして、情報処理装置１０１は、入力された平文ＰＴに作成したパディングｐｄを連結して、連結文ＡＰＴを作成することができる。

[0166] （改ざん検出装置１０２がおこなう改ざん検出処理の詳細）

次に、図１３を用いて、改ざん検出装置１０２がおこなう改ざん検出処理の詳細について説明する。

[0167] 図１３は、改ざん検出装置１０２がおこなう改ざん検出処理の詳細を示すフローチャートである。まず、ＣＰＵ２０１は、暗号化ブロックの入力があったか判定する（ステップＳ１３０１）。暗号化ブロックの入力がない場合（ステップＳ１３０１：Ｎｏ）、ステップＳ１３０１に戻り、ＣＰＵ２０１は、暗号化ブロックの入力を待つ。一方、暗号化ブロックの入力があった場合（ステップＳ１３０１：Ｙｅｓ）、ステップＳ１３０２に移行する。

[0168] 次に、ＣＰＵ２０１は、ブロック暗号のＣＢＣモードにより、暗号化ブロックから平文を復号する（ステップＳ１３０２）。そして、ＣＰＵ２０１は、末尾からパディング長ｐｌを抽出し、パディング長ｐｌに基づいてＣＲＣの格納領域長を算出する（ステップＳ１３０３）。次に、ＣＰＵ２０１は、格納領域からＣＲＣを抽出する（ステップＳ１３０４）。

[0169] そして、ＣＰＵ２０１は、パディング長ｐｌが４［ｂｙｔｅ］以下か否かを判定する（ステップＳ１３０５）。パディング長ｐｌが４［ｂｙｔｅ］以下である場合（ステップＳ１３０５：Ｙｅｓ）、ステップＳ１３０８に移行する。

[0170] 一方、パディング長ｐｌが４［ｂｙｔｅ］以下ではない場合（ステップＳ１３０５：Ｎｏ）、ＣＰＵ２０１は、パディング長ｐｌが正しいか否か判定する（ステップＳ１３０６）。パディング長ｐｌが正しい場合（ステップＳ１３０６：Ｙｅｓ）、ステップＳ１３０８に移行する。

[0171] 一方、パディング長ｐｌが誤りである場合（ステップＳ１３０６：Ｎｏ）

、ＣＰＵ２０１は、改ざんありと判断し、判断結果を出力して（ステップＳ１３０７）、改ざん検出処理を終了する。

[0172] ステップＳ１３０８にて、ＣＰＵ２０１は、復号した平文からパディングｐｄを除去する（ステップＳ１３０８）。次に、ＣＰＵ２０１は、パディングを除去した後の平文からＣＲＣを算出する（ステップＳ１３０９）。

[0173] そして、ＣＰＵ２０１は、ステップＳ１３０４にて抽出したＣＲＣとステップＳ１３０９にて算出したＣＲＣとが一致するか否か判定する（ステップＳ１３１０）。一致する場合（ステップＳ１３１０：Ｙｅｓ）、ＣＰＵ２０１は、改ざんされていないと判断して、復号した平文を出力し（ステップＳ１３１１）、改ざん検出処理を終了する。

[0174] 一方、一致しない場合（ステップＳ１３１０：Ｎｏ）、ＣＰＵ２０１は、改ざんありと判断し、判断結果を出力して（ステップＳ１３０７）、改ざん検出処理を終了する。

[0175] これにより、改ざん検出装置１０２は、パディングｐｄにパディング長ｐｌに対応するコードが含まれている場合、パディング長ｐｌが正しいかを判定することにより、暗号化ブロックの改ざんの影響がパディングｐｄに及んでいるか否か判定することができる。

[0176] また、改ざん検出装置１０２は、パディングｐｄに含まれる情報処理装置１０１での平文ＰＴから算出されたコードと改ざん検出装置１０２にて得られた平文から算出されたコードとの一致判定をおこなう。そのため、改ざん検出装置１０２は、暗号化ブロックの改ざんの影響により、改ざん検出装置１０２にて得られた平文が、情報処理装置１０１での平文ＰＴから変化しているか否か判定することができる。

[0177] 以上説明したように、情報処理装置１０１は、平文ＰＴに連結するパディングｐｄのパディング長ｐｌを算出してから、パディング長ｐｌの範囲内で平文ＰＴから算出するコードの格納領域長ｃｌを算出する。これにより、平文ＰＴから算出するコードを、パディングｐｄ内に格納可能なデータ長で生成することができる。これにより、生成した平文ＰＴから算出したコードを

パディングｐｄに格納してもパディングｐｄのデータ長が増加することがないため、連結文ＡＰＴのデータ長の増加を防止し、リソースの使用量の削減をおこなうことができる。

[0178] また、改ざん検出装置１０２は、復号により得た平文から算出されたコードとパディングｐｄに格納された平文ＰＴから算出されたコードとの一致判定をおこなう。これにより、暗号化ブロックの改ざんにより、平文が変化したことを検出することができる。

[0179] また、情報処理装置１０１は、格納領域を算出する際に、パディングｐｄの末尾のパディング長領域を確保しておく。これにより、改ざん検出装置１０２は、末尾のパディング長領域のコードが示すデータ長に基づいて、改ざんが検出されなかった連結文ＡＰＴから、パディングｐｄを除去して、情報処理装置１０１での平文ＰＴと同一の平文ＰＴを得ることができる。

[0180] また、情報処理装置１０１は、パディング長領域長ｌｌをブロック長ｂｌを示すことができる最も短いデータ長で生成する。これにより、必要最小限のデータ長で、パディング長ｐｌを示すコードを格納できる。

[0181] また、情報処理装置１０１は、平文ＰＴを暗号化するために必要最小限のデータ長でパディングｐｄを生成する。これにより、パディングｐｄを連結することによる送信データ量の増加を最小にすることができる。

[0182] なお、本実施の形態で説明した情報処理方法および改ざん検出方法は、予め用意されたプログラムをパーソナル・コンピュータやワークステーション等のコンピュータで実行することにより実現することができる。本情報処理プログラムおよび本改ざん検出プログラムは、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。また本情報処理プログラムおよび本改ざん検出プログラムは、インターネット等のネットワークを介して配布してもよい。

符号の説明

[0183] １０１　情報処理装置

１０２　改ざん検出装置

３０１　特定部

３０２　算出部

３０３　第１の生成部

３０４　第２の生成部

３０５　作成部

３０６　連結部

３０７　出力部

３０８　暗号化部

３０９　第３の生成部

４０１　入力部

４０２　復号部

４０３　第１の抽出部

４０４　決定部

４０５　第２の抽出部

４０６　第３の抽出部

４０７　生成部

４０８　判定部

４０９　出力部

４１０　第４の抽出部

請求の範囲

[請求項1] 平文データのデータ長より長く、かつ、所定のブロック長の倍数となるデータ長を特定する特定手段と、

前記平文データのデータ長と前記特定手段によって特定されたデータ長との差分のデータ長を算出する算出手段と、

前記算出手段によって算出された差分のデータ長を示す第１のコードを生成する第１の生成手段と、

前記平文データから算出される第２のコードを、前記差分のデータ長から前記第１の生成手段によって生成された第１のコードのデータ長を引いた残余のデータ長以内のデータ長で生成する第２の生成手段と、

前記第２の生成手段によって生成された第２のコードを含み、前記第１のコードを末尾とするパディングを、前記差分のデータ長で作成する作成手段と、

前記作成手段によって作成されたパディングを前記平文データの末尾に連結させて連結データを生成する連結手段と、

前記連結手段によって得られた連結データを出力する出力手段と、

を備えることを特徴とする情報処理装置。

[請求項2] 前記連結データを、暗号化と復号に共通して使用される鍵を用いて前記所定のブロック長ごとに暗号化する暗号化手段を備え、

前記出力手段は、

前記暗号化手段によって前記所定のブロック長ごとに暗号化された暗号化連結データを出力することを特徴とする請求項１に記載の情報処理装置。

[請求項3] 前記第１の生成手段は、

前記差分のデータ長を示す第１のコードを、前記所定のブロック長を示すことができる最も短いデータ長で生成することを特徴とする請求項１または２に記載の情報処理装置。

[請求項4] 前記特定手段は、

前記平文データのデータ長より長く、かつ、前記所定のブロック長の倍数となるデータ長群の中において、最も短いデータ長を特定することを特徴とする請求項１～３のいずれか一つに記載の情報処理装置。

[請求項5] 前記第２の生成手段は、

前記平文データから算出される第２のコードを、前記差分のデータ長から前記第１のコードのデータ長を引いた残余のデータ長で生成し、

前記作成手段は、

前記第１のコードを末尾とし、前記第２のコードを先頭とするパディングを作成することを特徴とする請求項１～４のいずれか一つに記載の情報処理装置。

[請求項6] 前記第２の生成手段は、

所定のデータ長が前記差分のデータ長から前記第１のコードのデータ長を引いた残余のデータ長より短い場合、前記平文データから算出する第２のコードを、前記所定のデータ長で生成し、

前記作成手段は、

前記第１のコードを末尾とし、前記第２のコードを前記第１のコードの先頭と隣接させたパディングを、前記差分のデータ長で作成することを特徴とする請求項１～４のいずれか一つに記載の情報処理装置。

[請求項7] 前記第１のコードを特定する第３のコードを、前記差分のデータ長から前記第１のコードのデータ長と前記所定のデータ長とを引いた残余のデータ長で生成する第３の生成手段を備え、

前記作成手段は、

前記第１のコードを末尾とし、前記第２のコードを前記第１のコードの先頭と隣接させ、前記第３のコードを前記第２のコードの先頭と

隣接させたパディングを作成することを特徴とする請求項６に記載の情報処理装置。

[請求項8] 前記第２のコードは、前記平文データから得られたハッシュ値であることを特徴とする請求項１～７のいずれか一つに記載の情報処理装置。

[請求項9] 前記第２のコードは、前記平文データから得られたパリティ符号であることを特徴とする請求項１～７のいずれか一つに記載の情報処理装置。

[請求項10] 平文データを所定のブロック長ごとに暗号化した暗号化データを入力する入力手段と、

前記入力手段によって入力された前記暗号化データから、暗号化と復号に共通して使用される鍵を用いて復号した復号データを生成する復号手段と、

パディングのデータ長を格納する前記復号データの末尾となる第１の領域から、第１のコードを抽出する第１の抽出手段と、

前記第１の抽出手段によって抽出された第１のコードが示すデータ長に基づいて、平文データから算出されたコードを格納する前記復号データの第２の領域を決定する決定手段と、

前記決定手段によって決定された第２の領域から第２のコードを抽出する第２の抽出手段と、

前記第１のコードが示すデータ長となる前記復号データの末尾領域を除いた前記復号データの第３の領域から第３のコードを抽出する第３の抽出手段と、

前記第３の抽出手段によって抽出された第３のコードから算出する第４のコードを、前記第２のコードのデータ長と同一データ長で生成する生成手段と、

前記生成手段によって生成された第４のコードと前記第２のコードとの一致判定をおこなう判定手段と、

前記判定手段によって判定された判定結果を出力する出力手段と、

を備えることを特徴とする改ざん検出装置。

[請求項11] 前記決定手段は、

前記第１の領域の先頭に接する前記復号データ内の領域であって、前記第１のコードが示すデータ長から前記第１の領域のデータ長を引いた残余のデータ長の領域を、前記第２の領域に決定することを特徴とする請求項１０に記載の改ざん検出装置。

[請求項12] 前記決定手段は、

所定のデータ長が前記第１のコードが示すデータ長から前記第１のコードのデータ長を引いた残余のデータ長より短い場合、前記第１の領域の先頭に接する前記復号データ内の領域であって、前記所定のデータ長の領域を、前記第２の領域に決定することを特徴とする請求項１０に記載の改ざん検出装置。

[請求項13] 前記第１のコードを特定するコードを格納する第４の領域から第５のコードを抽出する第４の抽出手段を備え、

前記決定手段は、

前記第２の領域の先頭に接する前記復号データ内の領域であって、前記第１のコードが示すデータ長から前記第１のコードのデータ長と前記所定のデータ長とを引いた残余のデータ長の領域を、前記第４の領域として決定し、

前記第４の抽出手段は、

前記決定手段によって決定された第４の領域から、前記第５のコードを抽出し、

前記判定手段は、

前記第４の抽出手段によって抽出された第５のコードにより特定されるコードと前記第１のコードとの一致判定をおこなうことを特徴とする請求項１２に記載の改ざん検出装置。

[請求項14] 前記第４のコードは前記第３のコードから得られたハッシュ値であ

ることを特徴とする請求項１１～１３のいずれか一つに記載の改ざん検出装置。

[請求項15] 前記第４のコードは前記第３のコードから得られたパリティ符号であることを特徴とする請求項１１～１３のいずれか一つに記載の改ざん検出装置。

[請求項16] コンピュータが、

平文データのデータ長より長く、かつ、所定のブロック長の倍数となるデータ長を特定する特定工程と、

前記平文データのデータ長と前記特定工程によって特定されたデータ長との差分のデータ長を算出する算出工程と、

前記算出工程によって算出された差分のデータ長を示す第１のコードを生成する第１の生成工程と、

前記平文データから算出される第２のコードを、前記差分のデータ長から前記第１の生成工程によって生成された第１のコードのデータ長を引いた残余のデータ長以内のデータ長で生成する第２の生成工程と、

前記第２の生成工程によって生成された第２のコードを含み、前記第１のコードを末尾とするパディングを、前記差分のデータ長で作成する作成工程と、

前記作成工程によって作成されたパディングを前記平文データの末尾に連結させて連結データを生成する連結工程と、

前記連結工程によって得られた連結データを出力する出力工程と、

を実行することを特徴とする情報処理方法。

[請求項17] コンピュータが、

平文データを所定のブロック長ごとに暗号化した暗号化データを入力する入力工程と、

前記入力工程によって入力された前記暗号化データから、暗号化と復号に共通して使用される鍵を用いて復号した復号データを生成する

復号工程と、

パディングのデータ長を格納する前記復号データの末尾となる第１の領域から、第１のコードを抽出する第１の抽出工程と、

前記第１の抽出工程によって抽出された第１のコードが示すデータ長に基づいて、平文データから算出されたコードを格納する前記復号データの第２の領域を決定する決定工程と、

前記決定工程によって決定された第２の領域から第２のコードを抽出する第２の抽出工程と、

前記第１のコードが示すデータ長となる前記復号データの末尾領域を除いた前記復号データの第３の領域から第３のコードを抽出する第３の抽出工程と、

前記第３の抽出工程によって抽出された第３のコードから算出する第４のコードを、前記第２のコードのデータ長と同一データ長で生成する生成工程と、

前記生成工程によって生成された第４のコードと前記第２のコードとの一致判定をおこなう判定工程と、

前記判定工程によって判定された判定結果を出力する出力工程と、

を実行することを特徴とする改ざん検出方法。

[請求項18] 平文データのデータ長より長く、かつ、所定のブロック長の倍数となるデータ長を特定する特定工程と、

前記平文データのデータ長と前記特定工程によって特定されたデータ長との差分のデータ長を算出する算出工程と、

前記算出工程によって算出された差分のデータ長を示す第１のコードを生成する第１の生成工程と、

前記平文データから算出される第２のコードを、前記差分のデータ長から前記第１の生成工程によって生成された第１のコードのデータ長を引いた残余のデータ長以内のデータ長で生成する第２の生成工程と、

前記第２の生成工程によって生成された第２のコードを含み、前記第１のコードを末尾とするパディングを、前記差分のデータ長で作成する作成工程と、

前記作成工程によって作成されたパディングを前記平文データの末尾に連結させて連結データを生成する連結工程と、

前記連結工程によって得られた連結データを出力する出力工程と、

をコンピュータに実行させることを特徴とする情報処理プログラム。

[請求項19] 平文データを所定のブロック長ごとに暗号化した暗号化データを入力する入力工程と、

前記入力工程によって入力された前記暗号化データから、暗号化と復号に共通して使用される鍵を用いて復号した復号データを生成する復号工程と、

パディングのデータ長を格納する前記復号データの末尾となる第１の領域から、第１のコードを抽出する第１の抽出工程と、

前記第１の抽出工程によって抽出された第１のコードが示すデータ長に基づいて、平文データから算出されたコードを格納する前記復号データの第２の領域を決定する決定工程と、

前記決定工程によって決定された第２の領域から第２のコードを抽出する第２の抽出工程と、

前記第１のコードが示すデータ長となる前記復号データの末尾領域を除いた前記復号データの第３の領域から第３のコードを抽出する第３の抽出工程と、

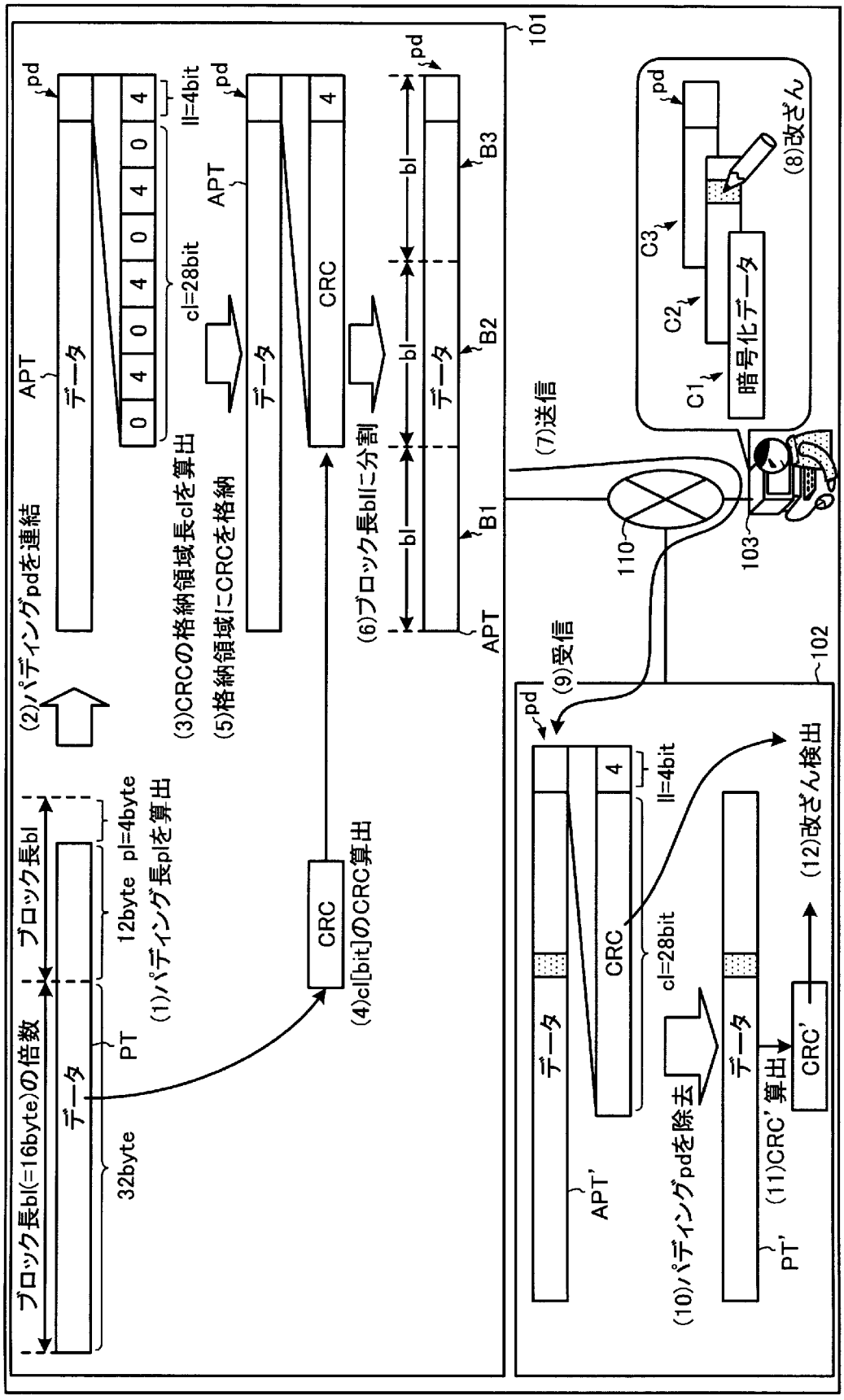
前記第３の抽出工程によって抽出された第３のコードから算出する第４のコードを、前記第２のコードのデータ長と同一データ長で生成する生成工程と、

前記生成工程によって生成された第４のコードと前記第２のコードとの一致判定をおこなう判定工程と、

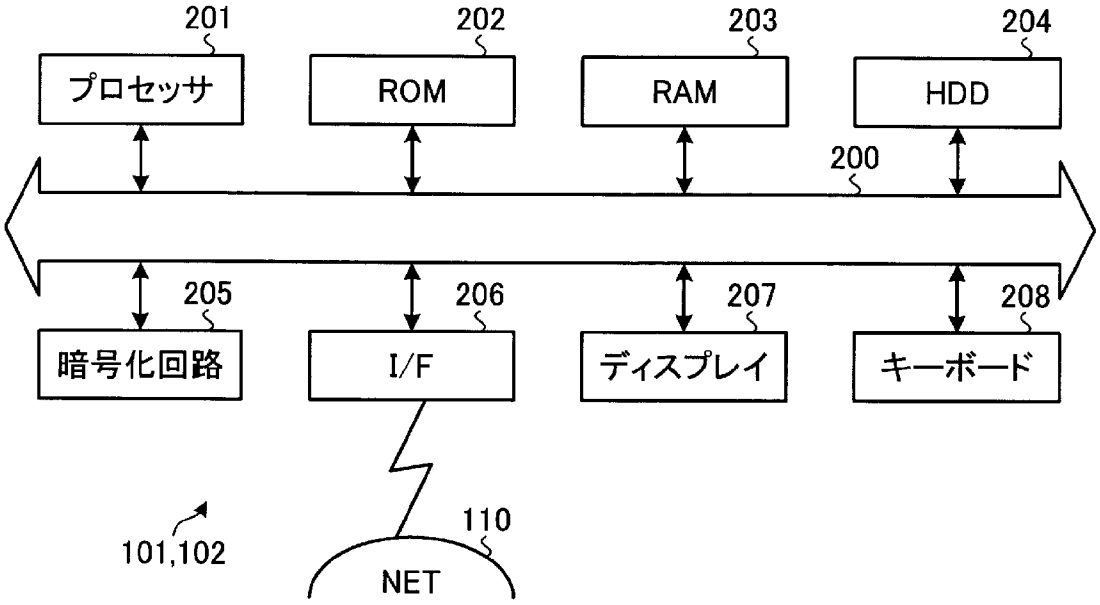
前記判定工程によって判定された判定結果を出力する出力工程と、

をコンピュータに実行させることを特徴とする改ざん検出プログラム。

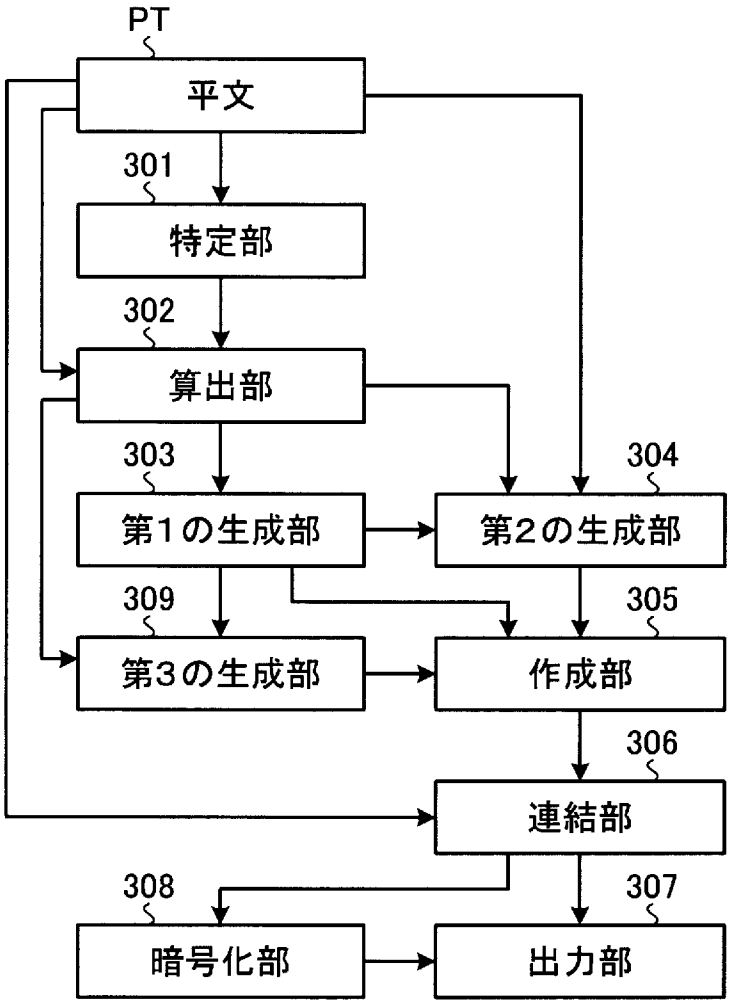
[図1]


ブロック長bl(=16byte)の倍数
ブロック長bl
データ
PT
12byte pl=4byte
(1)パディング長plを算出
32byte
(2)パディングpdを連結
APT
pd
0 4 0 4 0 4 0 4
ll=4bit
(3)CRCの格納領域長clを算出
cl=28bit
(4)cl[bit]のCRC算出
CRC
4
(5)格納領域にCRCを格納
(6)ブロック長blに分割
bl
B1
B2
B3
101
(7)送信
110
103
C1
C2
C3
暗号化データ
(8)改ざん
(9)受信
102
APT'
(10)パディングpdを除去
PT'
(11)CRC'算出
CRC'
(12)改ざん検出

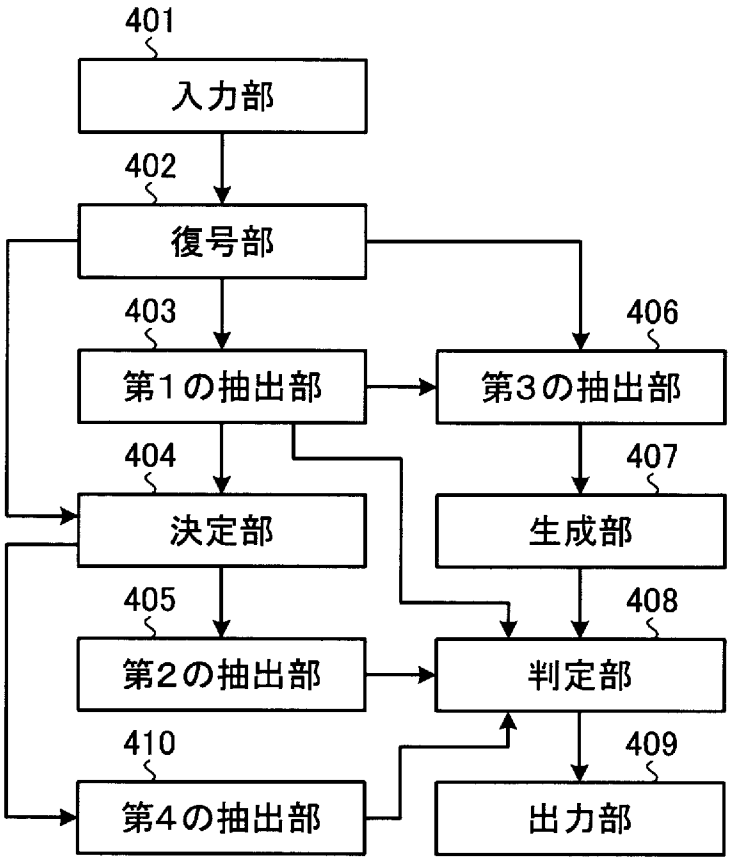
[図2]


201
プロセッサ
202
ROM
203
RAM
204
HDD
200
205
暗号化回路
206
I/F
207
ディスプレイ
208
キーボード
101,102
110
NET

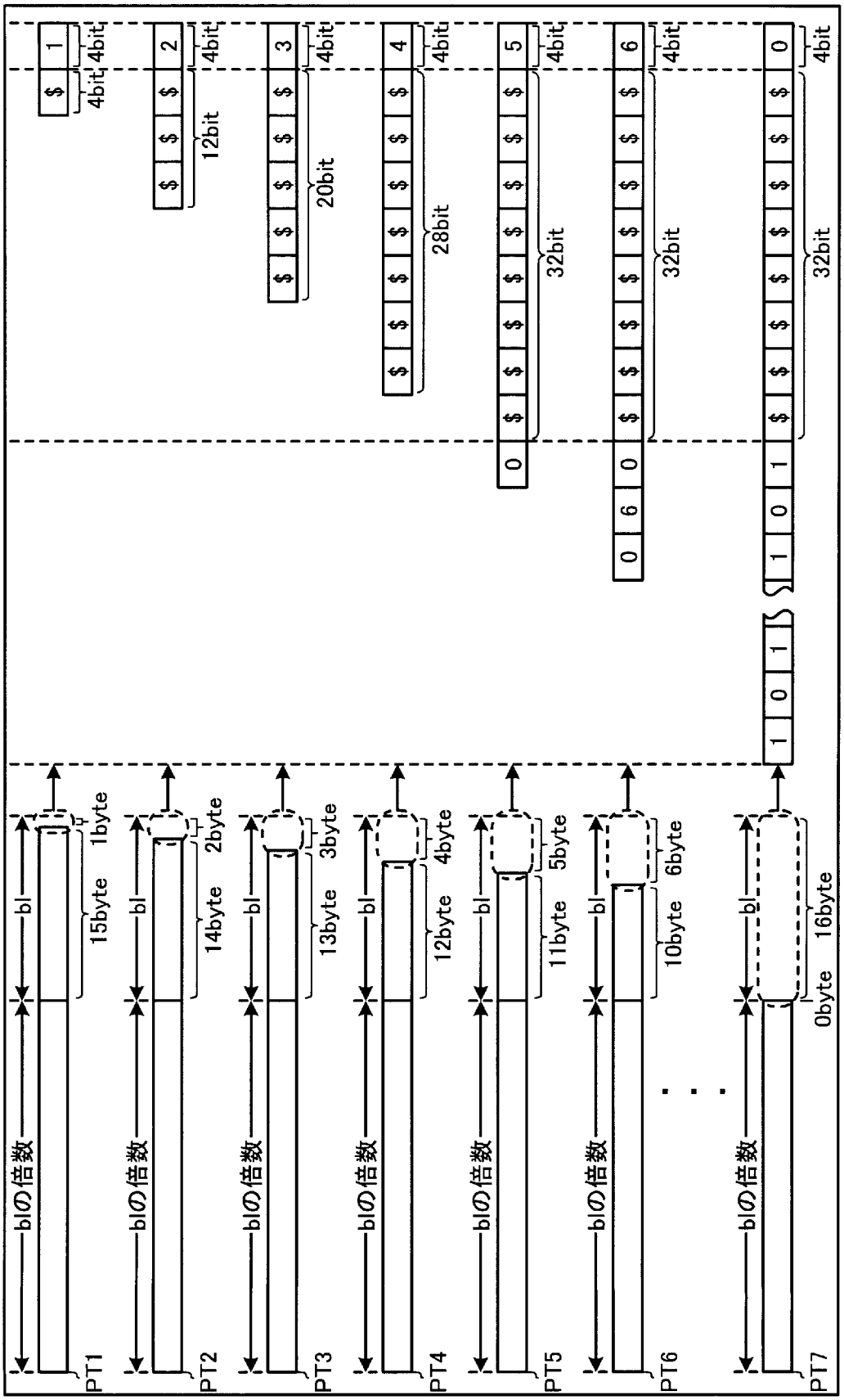
[図3]


PT
平文
301
特定部
302
算出部
303
第1の生成部
304
第2の生成部
309
第3の生成部
305
作成部
306
連結部
308
暗号化部
307
出力部

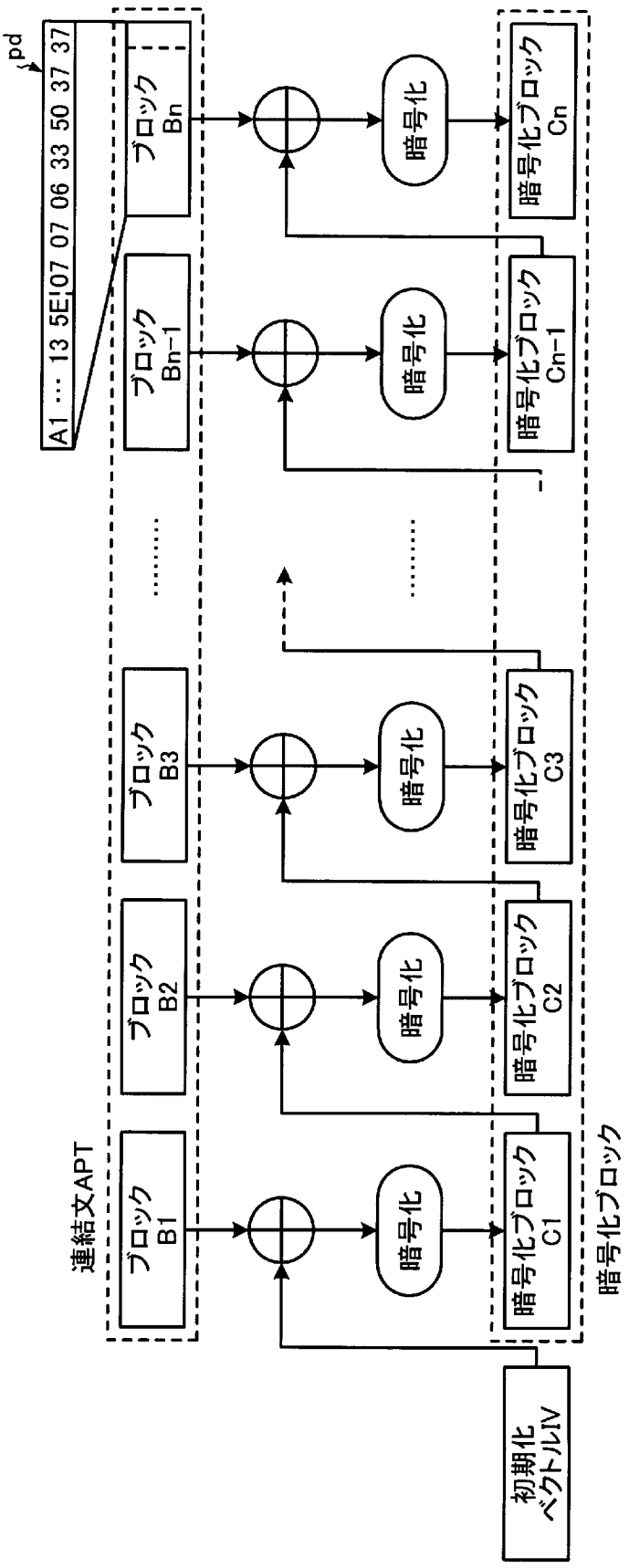
[図4]


401
入力部
402
復号部
403
第1の抽出部
404
決定部
405
第2の抽出部
410
第4の抽出部
406
第3の抽出部
407
生成部
408
判定部
409
出力部

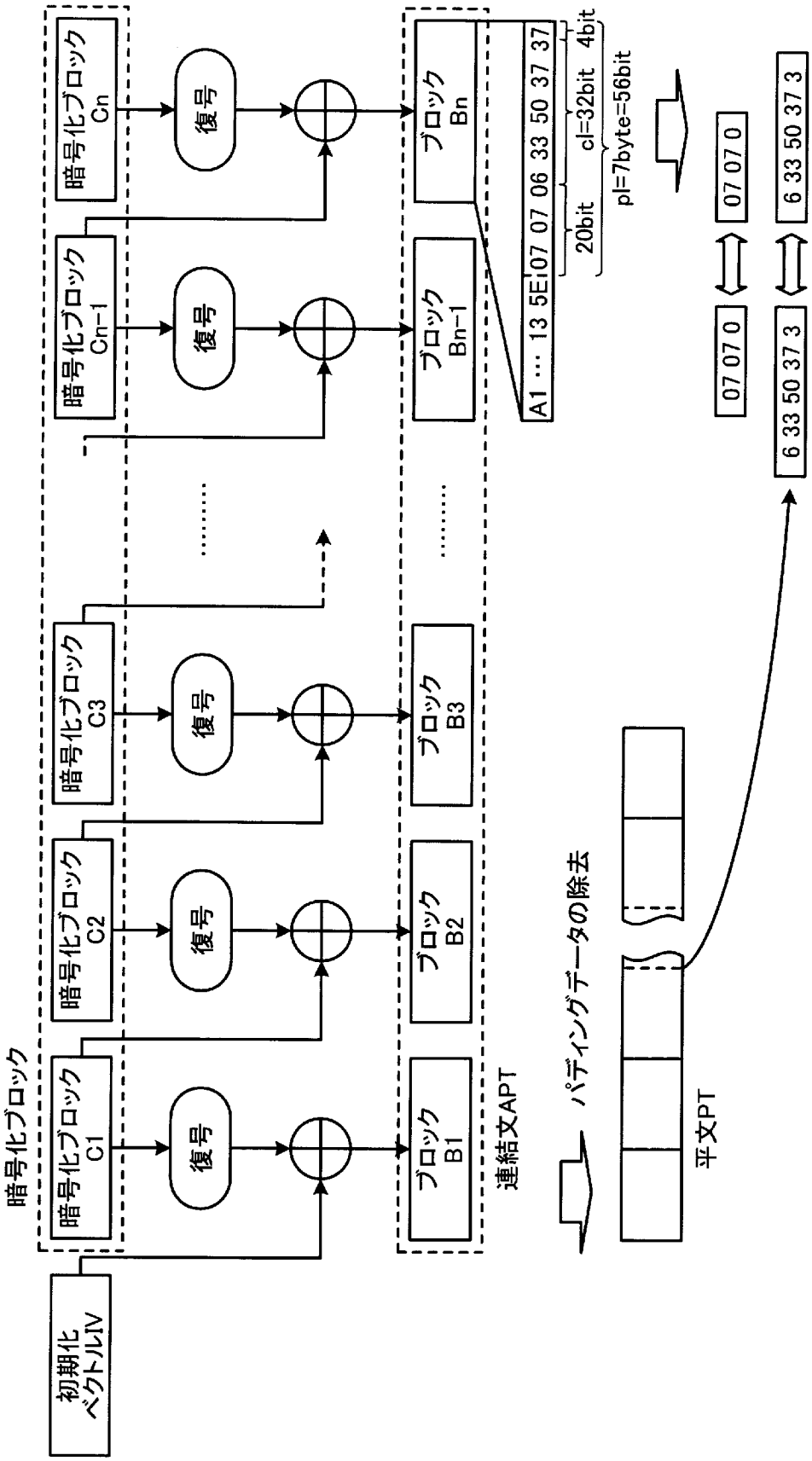
[図5]


PT1
PT2
PT3
PT4
PT5
PT6
PT7
blの倍数
bl
15byte
1byte
14byte
2byte
13byte
3byte
12byte
4byte
11byte
5byte
10byte
6byte
0byte
16byte
4bit
12bit
20bit
28bit
32bit
$
0
1
2
3
4
5
6

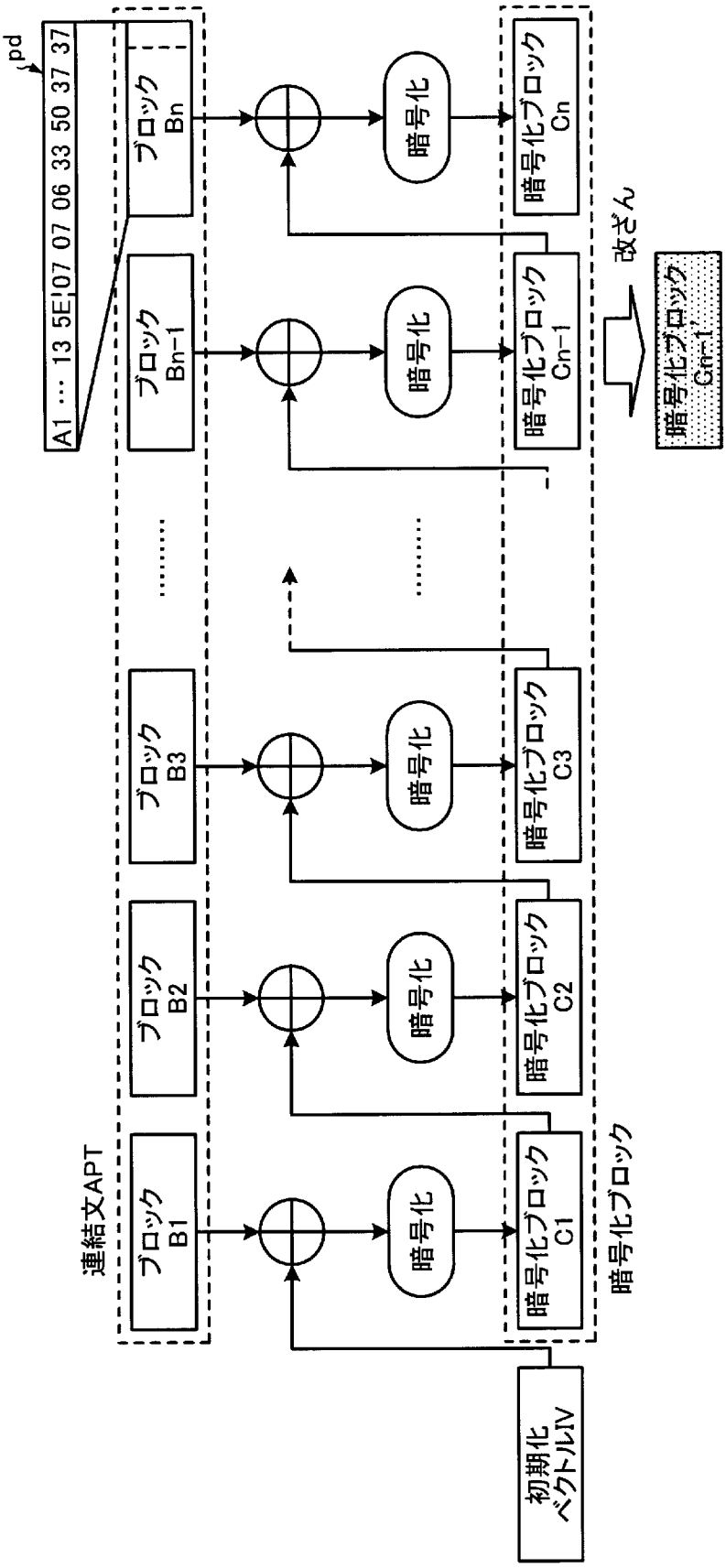
[図6]


pd
A1 ··· 13 5E 07 07 06 33 50 37 37
連結文APT
ブロック B1
ブロック B2
ブロック B3
ブロック Bn-1
ブロック Bn
暗号化
暗号化ブロック C1
暗号化ブロック C2
暗号化ブロック C3
暗号化ブロック Cn-1
暗号化ブロック Cn
暗号化ブロック
初期化ベクトルIV

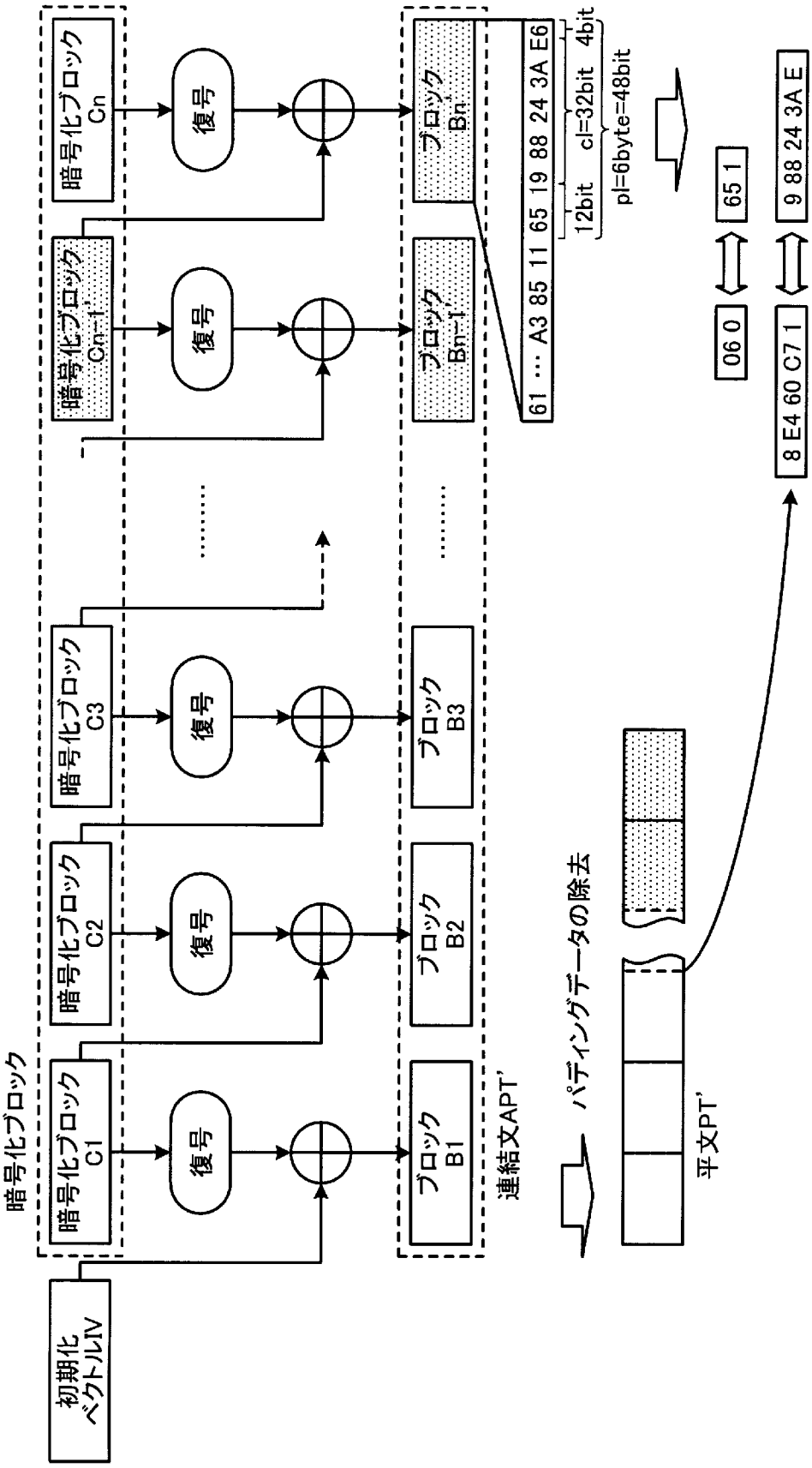
[図7]


暗号化ブロック
初期化ベクトルIV
暗号化ブロック C1
暗号化ブロック C2
暗号化ブロック C3
暗号化ブロック Cn-1
暗号化ブロック Cn
復号
ブロック B1
ブロック B2
ブロック B3
ブロック Bn-1
ブロック Bn
連結文APT
A1 … 13 5E 07 07 06 33 50 37 37
20bit
cl=32bit
4bit
pl=7byte=56bit
パディングデータの除去
平文PT
07 07 0
6 33 50 37 3

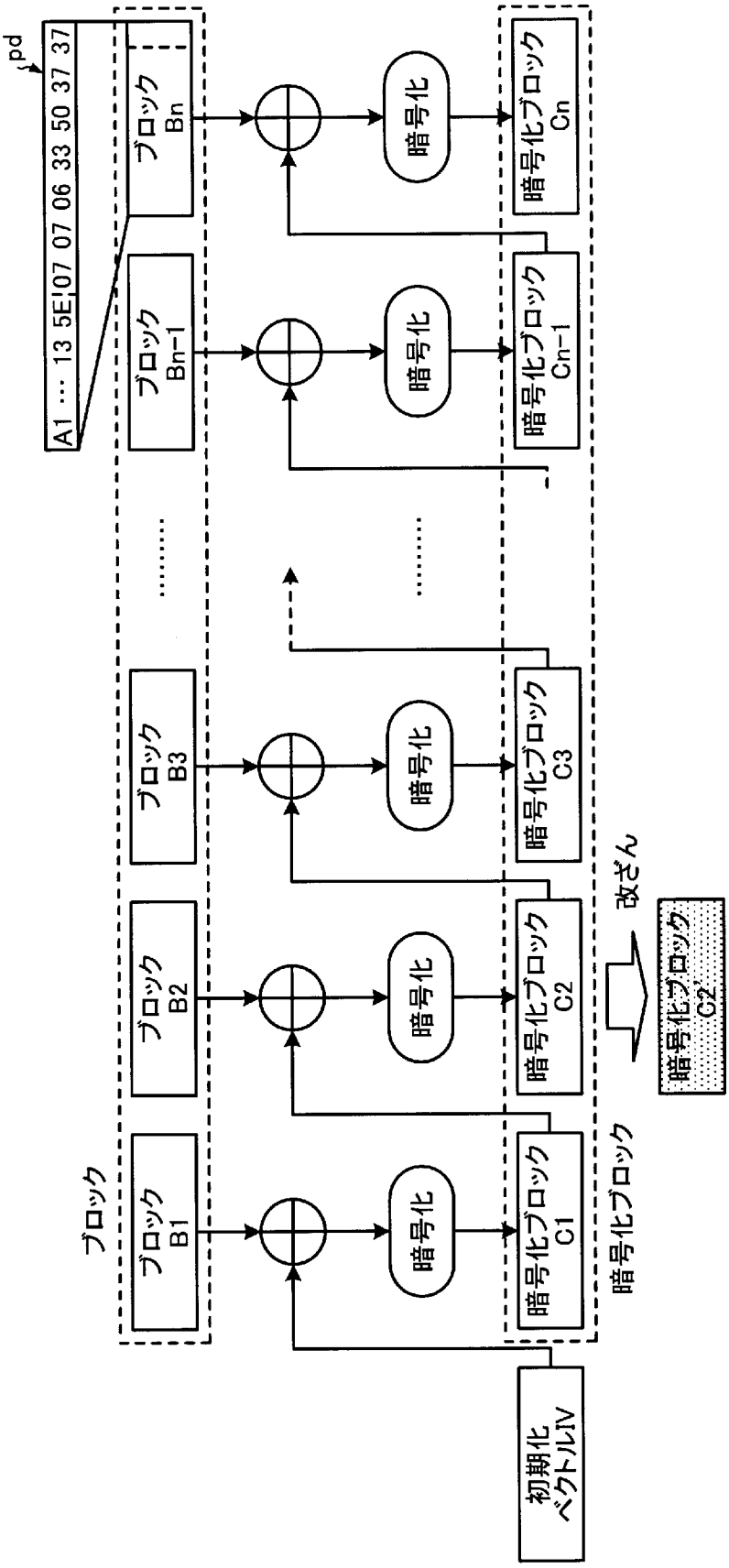
[図8]


pd
A1 … 13 5E 07 07 06 33 50 37 37
連結文APT
ブロック B1
ブロック B2
ブロック B3
ブロック Bn-1
ブロック Bn
暗号化
暗号化ブロック C1
暗号化ブロック C2
暗号化ブロック C3
暗号化ブロック Cn-1
暗号化ブロック Cn
改ざん
暗号化ブロック Cn-1'
初期化ベクトルIV
暗号化ブロック

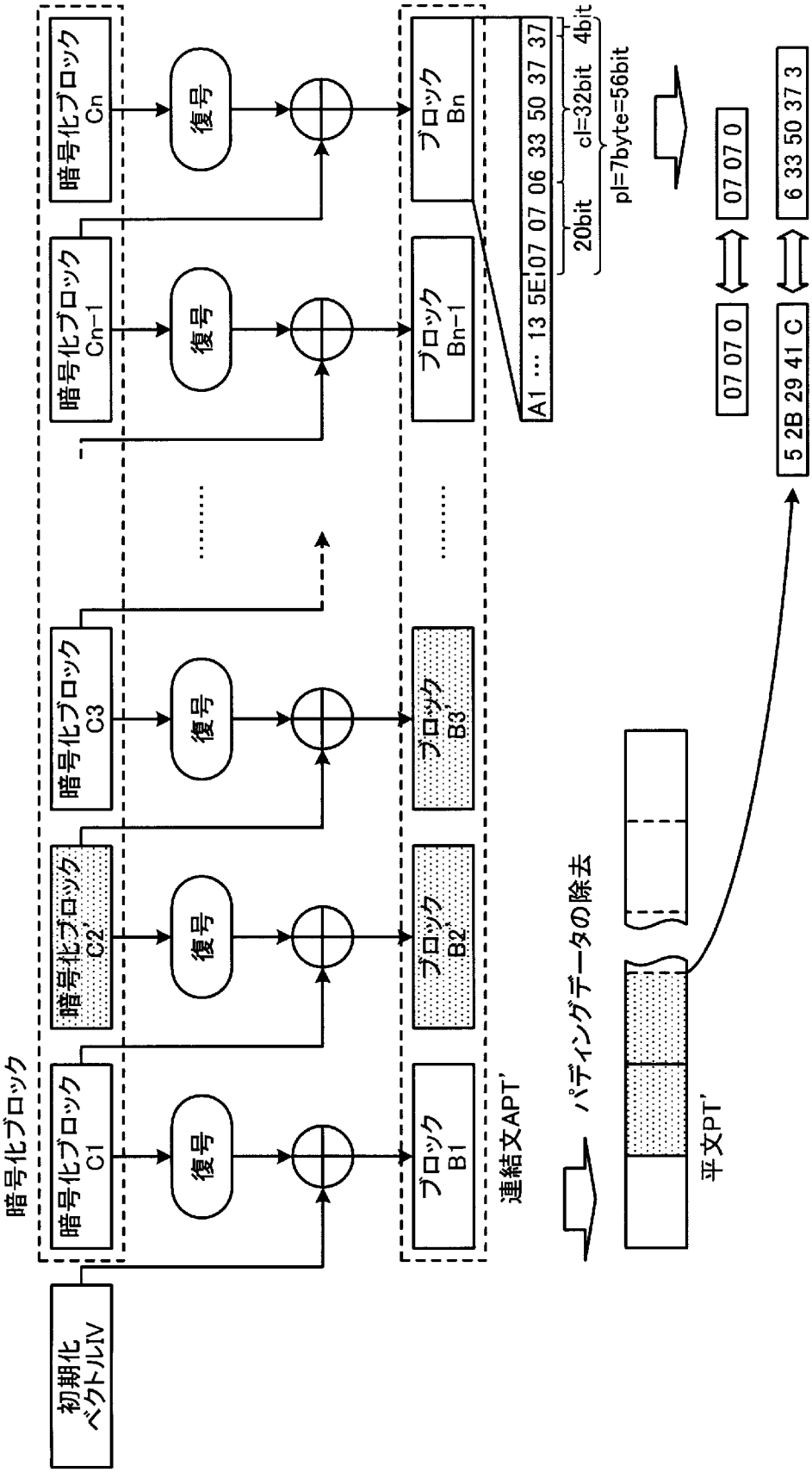
[図9]


暗号化ブロック
初期化ベクトルIV
暗号化ブロック C1
暗号化ブロック C2
暗号化ブロック C3
暗号化ブロック Cn-1'
暗号化ブロック Cn
復号
ブロック B1
ブロック B2
ブロック B3
ブロック Bn-1'
ブロック Bn'
連結文APT'
61 … A3 85 11 65 19 88 24 3A E6
12bit
cl=32bit
4bit
pl=6byte=48bit
パディングデータの除去
平文PT'
06 0
65 1
8 E4 60 C7 1
9 88 24 3A E

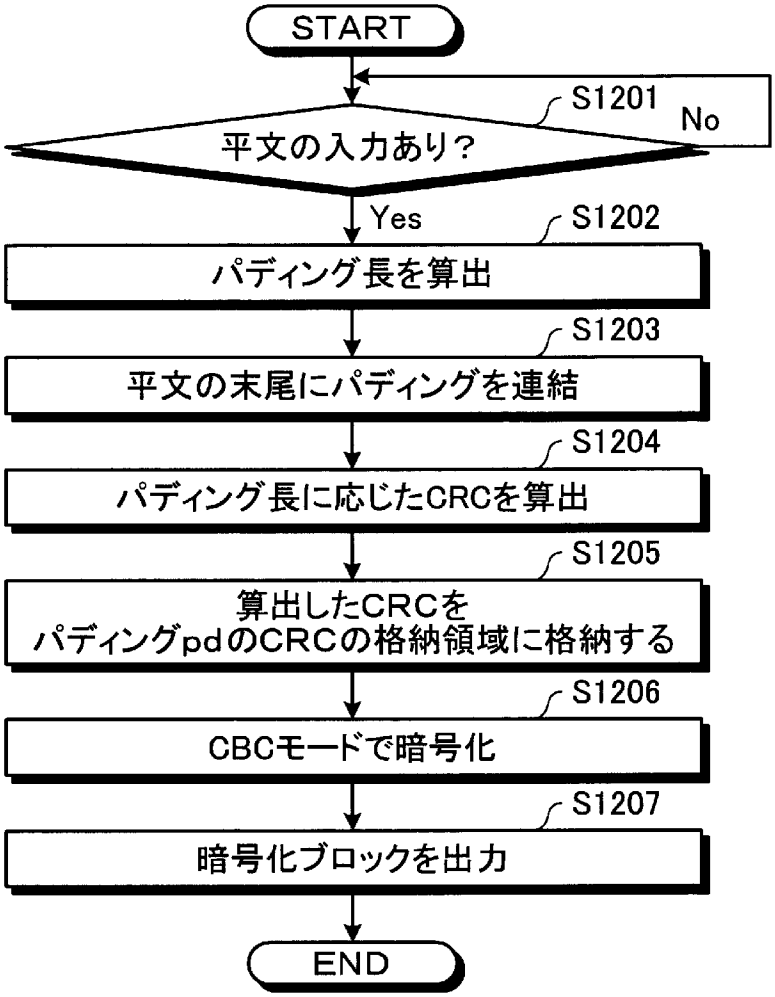
[図10]


pd
A1 … 13 5E 07 07 06 33 50 37 37
ブロック
ブロック B1
ブロック B2
ブロック B3
ブロック Bn-1
ブロック Bn
暗号化
暗号化ブロック C1
暗号化ブロック C2
暗号化ブロック C3
暗号化ブロック Cn-1
暗号化ブロック Cn
暗号化ブロック
改ざん
暗号化ブロック C2'
初期化ベクトルIV

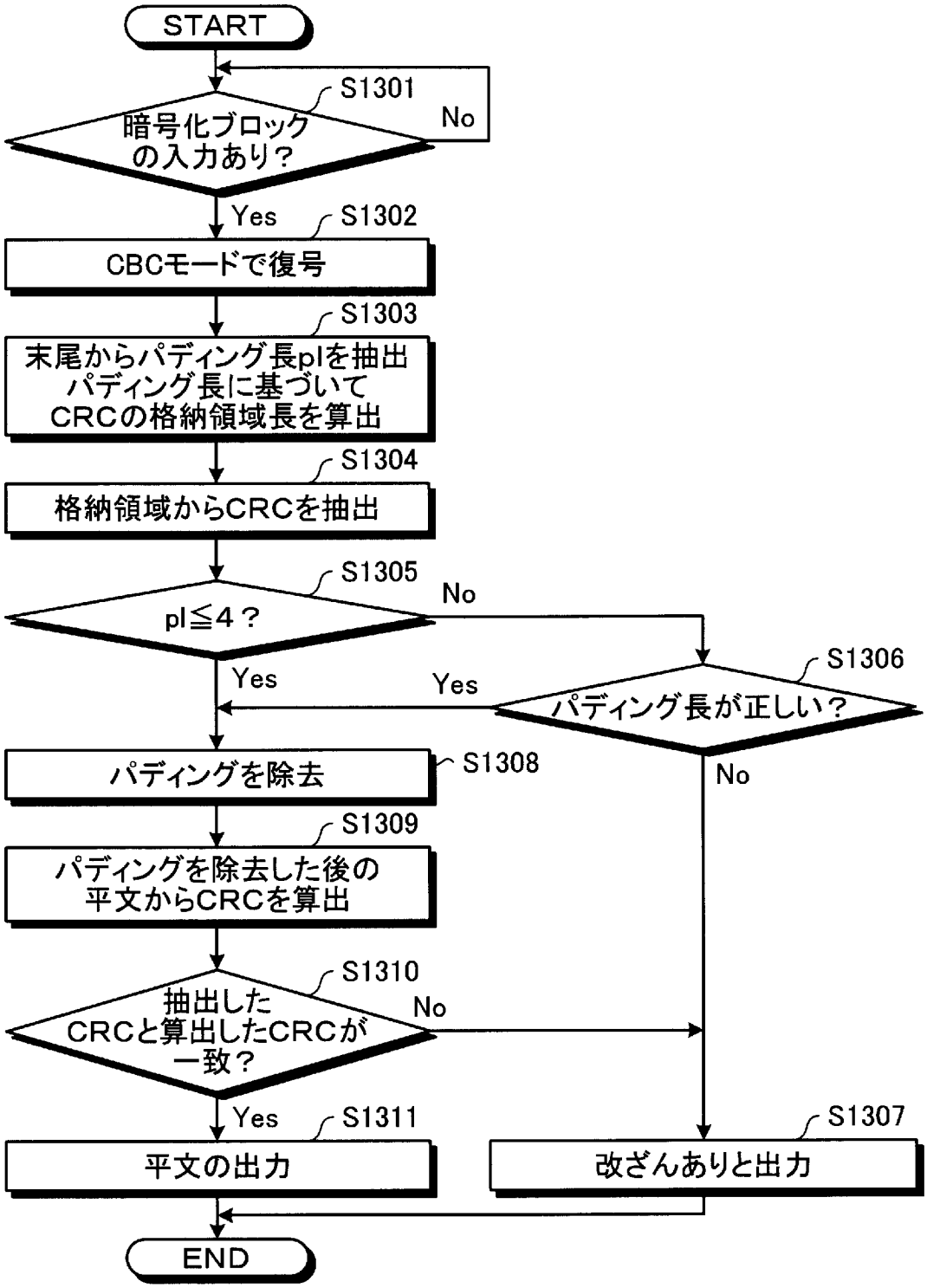
[図11]


暗号化ブロック
初期化ベクトルIV
暗号化ブロック C1
暗号化ブロック C2'
暗号化ブロック C3
暗号化ブロック Cn-1
暗号化ブロック Cn
復号
ブロック B1
ブロック B2'
ブロック B3'
ブロック Bn-1
ブロック Bn
連結文APT'
A1 … 13 5E 07 07 06 33 50 37 37
20bit
cl=32bit
4bit
pl=7byte=56bit
パディングデータの除去
平文PT'
07 07 0
07 07 0
5 2B 29 41 C
6 33 50 37 3

[図12]


START
S1201
No
平文の入力あり？
Yes
S1202
パディング長を算出
S1203
平文の末尾にパディングを連結
S1204
パディング長に応じたCRCを算出
S1205
算出したCRCを
パディングpdのCRCの格納領域に格納する
S1206
CBCモードで暗号化
S1207
暗号化ブロックを出力
END

[図13]


START
S1301
暗号化ブロックの入力あり？
No
Yes
S1302
CBCモードで復号
S1303
末尾からパディング長plを抽出
パディング長に基づいて
CRCの格納領域長を算出
S1304
格納領域からCRCを抽出
S1305
pl≦4？
No
Yes
S1306
Yes
パディング長が正しい？
No
パディングを除去
S1308
S1309
パディングを除去した後の
平文からCRCを算出
S1310
抽出した
CRCと算出したCRCが
一致？
No
Yes
S1311
平文の出力
S1307
改ざんありと出力
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/057480

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(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

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	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

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 2006-220747 A (Toshiba Corp.), 24 August 2006 (24.08.2006), entire text; all drawings & US 2006/0177054 A1 & EP 1724962 A2 & KR 10-2006-0090564 A & CN 1818992 A	1-19
A	JP 2001-318600 A (Mitsubishi Heavy Industries, Ltd.), 16 November 2001 (16.11.2001), entire text; all drawings (Family: none)	1-19
A	JP 2008-219746 A (Fujitsu Ltd.), 18 September 2008 (18.09.2008), entire text; all drawings & US 2008/0219435 A1	1-19

☐ 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
12 April, 2011 (12.04.11)	19 April, 2011 (19.04.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０５７４８０

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

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

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	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１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 2006-220747 A (株式会社東芝) 2006.08.24, 全文、全図 & US 2006/0177054 A1 & EP 1724962 A2 & KR 10-2006-0090564 A & CN 1818992 A	1-19
A	JP 2001-318600 A (三菱重工業株式会社) 2001.11.16, 全文、全図 (ファミリーなし)	1-19

☑　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 １２．０４．２０１１	国際調査報告の発送日 １９．０４．２０１１
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　４１８０ 西田　聡子 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
A	JP 2008-219746 A (富士通株式会社) 2008.09.18, 全文、全図 & US 2008/0219435 A1	1-19