(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
2007 年5 月10 日 (10.05.2007)

PCT

(10) 国際公開番号
WO 2007/052477 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G09C 1/00* (2006.01)

(21) 国際出願番号: PCT/JP2006/320826

(22) 国際出願日: 2006 年10 月19 日 (19.10.2006)

(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2005-321234 2005 年11 月4 日 (04.11.2005) JP
特願2006-004812 2006 年1 月12 日 (12.01.2006) JP

(71) 出願人 (米国を除く全ての指定国について): 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; および

(75) 発明者/出願人 (米国についてのみ): 峯松 一彦 (MINEMATSU, Kazuhiko) [JP/JP]; 〒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: 丸山 隆夫 (MARUYAMA, Takao); 〒1700013 東京都豊島区東池袋２－３８－２３ ＳＡＭビル３階 丸山特許事務所 Tokyo (JP).

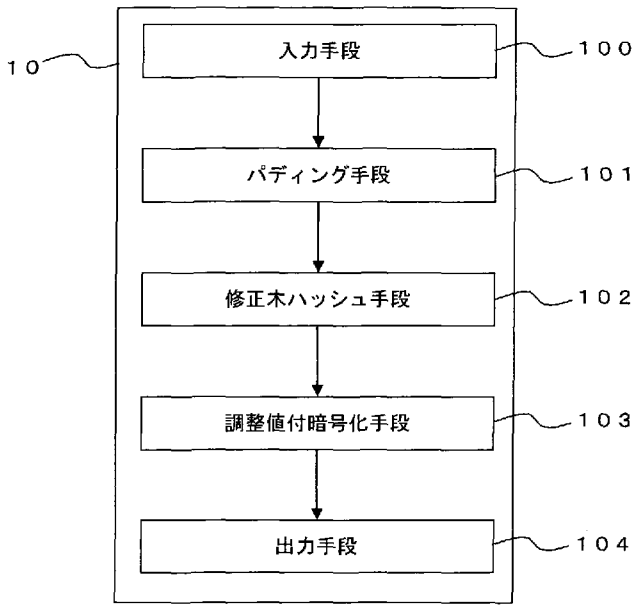
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK,

[続葉有]

WO 2007/052477 A1

(54) Title: MESSAGE AUTHENTICATION DEVICE, MESSAGE AUTHENTICATION METHOD, MESSAGE AUTHENTICATION PROGRAM, AND RECORDING MEDIUM THEREFOR

(54) 発明の名称: メッセージ認証装置、メッセージ認証方法、メッセージ認証プログラムとその記録媒体



100 INPUT MEANS
101 PADDING MEANS
102 CORRECTED TREE HASHING MEANS
103 ADJUSTMENT-VALUED ENCIPHER MEANS
104 OUTPUT MEANS

(57) Abstract: Provided are a message authentication device, a message authentication method, a message authentication program and a recording medium therefor, which combine block ciphers and their partial parts, which are quicker than the authentication mode of the existing block ciphers, which have theoretical safety and which are efficient in the preprocessing and in the used quantity of memory. The message authentication device comprises input means (100) for inputting a message, padding means (101) for padding the message at all times to a constant block length thereby to output it as a padded message, corrected tree hashing means (102) for subjecting the padded message to repeated operations, in which the hash functions of small input/output widths made on the basis of the parts of the block ciphers are arranged for the message, thereby to output the hash value of one block, adjustment-valued encipher means (103) for enciphering the hash value into a tag, and output means (104) for combining the tag and the message thereby to output the combination.

(57) 要約: ブロック暗号とその一部の部品を組合せて、既存のブロック暗号の認証モードより高速で、理論的安全性を有し、事前処理や使用メモリ量の点で効率のよい、メッセージ認証装置、

メッセー

[続葉有]

SL, SM, 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 (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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

ジ認証方法、メッセージ認証プログラムとその記録媒体を提供する。　メッセージを入力する入力手段１００、メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段１０１、パディング済みメッセージをブロック暗号の部品を基に作った小さい入出力幅のハッシュ関数をメッセージ分だけ並べた処理を繰り返し、１ブロックのハッシュ値を出力する修正木ハッシュ手段１０２、ハッシュ値を暗号化してタグとする調整値付暗号化手段１０３、及び、タグとメッセージとを連結して出力する出力手段１０４を備えたメッセージ認証装置とする。

明 細 書

メッセージ認証装置、メッセージ認証方法、メッセージ認証プログラムとその記録媒体

技術分野

[0001] 本発明は、ブロック暗号と、ブロック暗号の一部の処理との組合せにより構築された、汎用的で高速な、メッセージ認証装置、メッセージ認証方法、メッセージ認証プログラムとその記録媒体に関する。

背景技術

[0002] メッセージ認証とは、メッセージに対して秘密鍵を知るものだけが計算できるタグを付与することであり、メッセージが正当であることを保証する技術である。例えば、メッセージ認証を用いれば、秘密鍵を共有した2者の通信において、通信の間に行われた、第3者による改ざんを検知することが可能となる。

[0003] 具体的には、送信者がメッセージとタグを受信者に送ったとき、受信者側では受け取ったメッセージからタグを計算し、受信したタグとの一致をみることで、メッセージが正当な送信者から送られたものかどうかを判断することができる。なお、通常のメッセージ認証方式ではタグの生成方法さえ決まれば受信者側の認証方法は一意に定まるため、タグの生成方法だけを記述すれば十分である。

[0004] メッセージ認証の方法として、ブロック暗号を用いた方式が数多く知られている。これらはブロック暗号のメッセージ認証モードとも呼ばれ、古典的なCBC－MACモードをはじめとして、CBC－MACを改良したEMAC、XCBC、OMACなどが知られている。CBC－MACは可変長ブロックメッセージを受け入れた場合には安全でなく、また、メッセージがブロック長の倍数でない場合の処理が定められていないという欠点が知られている。

[0005] また、EMAC、XCBC、OMACなどの改良されたモードは、CBC－MACとほぼ同等の処理量であり、任意の長さ(ビット)のメッセージについて安全である。CBC－MACを含めたこれらのモードについては、例えば非特許文献1に記載されている。

[0006] ここで、例として、OMACのブロック図を図1に示す。図1に示すように、これらのモ

ードはシンプルであるが、タグの生成においておよそメッセージのブロック数だけブロック暗号を動作させる必要がある。そのため、その速度は常にブロック暗号の速度を超えることはない。

[0007] 一方、ブロック暗号だけを用いるのではなく、ユニバーサルハッシュ関数と呼ばれる鍵つきの関数を組み合わせてメッセージ認証を実現する方法もよく知られている。これはユニバーサルハッシュ関数の提案者の名前を取って、Carter－Wegman認証方式とも呼ばれる。実装環境に応じて最適化されたユニバーサルハッシュ関数は現在よく使われるブロック暗号よりも数倍高速に動作することが報告されている。このようなユニバーサルハッシュ関数は、例えば非特許文献2に記載されている。

[0008] また、小さな入出力幅のユニバーサルハッシュ関数を用いて、入力幅を任意に拡大する(出力幅はそのまま)方法がいくつか知られている。その一つの方式が非特許文献3に記載されている修正木ハッシュである。この修正木ハッシュを、2ブロック入力、1ブロック出力のユニバーサルハッシュ関数Hを用いる場合で以下に説明する。入力Xがmブロック(X＝(X1、X2・・・Xm))であるとし、Hi(但し、i＝1、2・・・)をそれぞれ独立な鍵を用いるHの実現とする。Hによる修正木ハッシュをMTHとすると、以下に示す式(1)で表される。

[0009] $MT_{H(X)}=G[H_S](G[H_{S-1}](\cdots G[H_1](X)\cdots))$・・・式(1)

入力が偶数ブロック数の場合:

$G[H_i](X)=H_i(X_1, X_2) \| H_i(X_3, X_4) \| \cdots \| H_i(X_{m-1}, X_m)$

入力が奇数ブロック数の場合:

$G[H_i](X)=H_i(X_1, X_2) \| H_i(X_3, X_4) \| \cdots \| H_i(X_{m-2}, X_{m-1}) \| X_m$

但し、s＝log(m)(対数の底は2)以上の最小の整数

[0010] MT_Hは、ブロック長の整数倍の長さの任意のメッセージを受け入れ、その出力は常に1ブロックの長さになる。

式(1)が示すように、mブロック平文を処理するのに修正木ハッシュは高々log(m)＋1個のHの鍵を用意すればよい。非特許文献3では、修正木ハッシュを非特許文献2に記載のMMHハッシュを用いて実現している。

[0011] Carter－Wegman認証方式では、タグ生成の速度はユニバーサルハッシュ関数

の速度にほぼ一致するため、一般的にCBC－MACなどのブロック暗号のみの認証モードよりも高速である。しかし、どのような計算機環境でも実装可能で、かつ高速であるユニバーサルハッシュ関数は知られていないため、ユニバーサルハッシュ関数が高速に実装可能な環境でないと使用できないことと、二つの部品を実装するためプログラムのサイズが一般に大きくなることが問題となる。

[0012] これらの問題を解決する一つのアプローチが、ブロック暗号とその部品とを組み合わせることである。非特許文献4において、そのような組合せによるメッセージ認証方式が提案されている。これはブロック暗号の一部の段関数をCBC－MACのように反復処理させることで、ブロック暗号の速度よりも高速なタグ生成処理を実現している。

[0013] しかし、この方式には非特許文献1に記載のブロック暗号認証モードや、ユニバーサルハッシュ関数とブロック暗号を組み合わせる方式が持つ理論的な安全性の保証がないという大きな欠点がある。ここでの理論的安全性とは、認証方式の安全性が常にブロック暗号そのものの安全性に帰着できるという性質を指す。詳しい定義などは非特許文献1に記載されている。理論的安全性を持たない認証方式の場合、使用しているブロック暗号がどんなに強いものであろうとタグの偽造が容易にできてしまう可能性がある。

[0014] また、特許文献1には、メッセージ認証において、XCBCにおける安全性を損なうことなく処理コストを削減する技術が開示されている。本技術は、デジタルデータのデータ長がブロック長の倍数である場合は、最終ブロックに鍵K1及び別の鍵K2のいずれか一方の鍵と排他的論理輪をとって暗号化を行い、デジタルデータのデータ長がブロック長の倍数でない場合は、最終ブロックの末尾に1を付加し、さらにブロック長に収まるよう0を付加したデータを上記鍵K1及び別の鍵K2のいずれか一方の鍵とは異なる別の鍵K2及び鍵K1のいずれか一方の鍵との排他的論理和をとって暗号化を行うものである。

特許文献1:特開2003－333036号公報

非特許文献1:岩田　哲、ブロック暗号利用モードの安全性に関する調査、独立行政法人情報処理推進機構(IPA)暗号技術関連の調査報告、2003年

非特許文献2:S. Halevi and H. Krawczyk, MMH:Software Message Authentication i

n the Gbit/second rates, Fast Software Encryption, 4th International Workshop, FS E '97, Lecture Notes in Computer Science; Vol. 1267, Feb. 1997

非特許文献3:Martin Boesgaard, Ove Scavenius, Thomas Pedersen, Thomas Christe nsen, Erik Zenner, Badger - A Fast and Provably Secure MAC, Applied Cryptograp hy and Network Security (ACNS) 2005

非特許文献4:J. Daemen and V. Rijmen, A New MAC Construction ALRED and a S pecific Instance ALPHA-MAC、Fast Software Encryption, International Workshop, FSE 2005, Lecture Notes in Computer Science; Vol. 3557, Feb. 2005

発明の開示

発明が解決しようとする課題

[0015] しかし、CBC－MACなどの現在知られている安全なブロック暗号の認証モードでは、すべての入力されたメッセージの各ブロック毎にブロック暗号を適用するため、ブロック暗号そのものの速度を超えた速度は達成できないという問題点があった。

[0016] また、あらゆる環境で高速に動作するユニバーサルハッシュ関数は知られていないということ、及び、ブロック暗号とユニバーサルハッシュ関数の両方を実装するためにプログラムサイズが大きくなるという理由から、ブロック暗号モードよりも高速なCarter－Wegman認証は、実装できる環境が限定されるという問題があった。

[0017] 本発明は、上記のような問題点に鑑み、ブロック暗号とその一部の部品を組み合わせて、既存のブロック暗号の認証モードより高速で、理論的安全性を有し、事前処理や使用するメモリ量の点でも効率のよい、メッセージ認証装置、メッセージ認証方法、メッセージ認証プログラムとその記録媒体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

[0018] 請求項1に記載の発明は、メッセージを入力する入力手段と、前記メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段と、前記パディング済みメッセージを、ブロック暗号の部品を基に作った小さい入出力幅のハッシュ関数をメッセージ分だけ並べた処理を繰り返すことで、1ブロックのハッシュ値を出力する修正木ハッシュ手段と、前記ハッシュ値を暗号化してタグとする調整値付暗号化手段と、前記タグと前記メッセージとを連結し

て出力する出力手段とを備えたメッセージ認証装置としたことを特徴とする。

[0019] 請求項2に記載の発明は、メッセージを入力する入力手段と、前記メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段と、ブロック暗号と該ブロック暗号の一部分から導出される置換処理とを、前記パディング済みメッセージを1ブロックずつ足しながら連鎖させて1ブロックのハッシュ値へ圧縮する交替型連鎖手段と、前記ハッシュ値を暗号化してタグとする調整値付暗号化手段と、前記タグと前記メッセージとを連結して出力する出力手段とを備えたメッセージ認証装置としたことを特徴とする。

[0020] 請求項3に記載の発明は、メッセージを入力する入力手段と、前記メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段と、前記パディング済みメッセージを、請求項2記載の交替型連鎖手段の一部の処理を請求項1記載の修正木ハッシュ手段で置き換えた構造により圧縮して1ブロック分のハッシュ値を出力する修正木連鎖ハッシュ手段と、前記ハッシュ値を暗号化してタグとする調整値付暗号化手段と、前記タグと前記メッセージとを連結して出力する出力手段とを備えたメッセージ認証装置としたことを特徴とする。

[0021] 請求項4に記載の発明は、前記修正木ハッシュ手段が、AESの段関数の4回以上の繰り返しを用いて構成され、前記調整値付暗号化手段が、AESを用いて構成される請求項1記載のメッセージ認証装置としたことを特徴とする。

[0022] 請求項5に記載の発明は、前記交替型連鎖手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成される請求項2記載のメッセージ認証装置としたことを特徴とする。

[0023] 請求項6に記載の発明は、前記修正木連鎖ハッシュ手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成される請求項3記載のメッセージ認証装置としたことを特徴とする。

[0024] 請求項7に記載の発明は、ブロック暗号と、該ブロック暗号の段関数を利用した置換処理とを用いる請求項1から3のいずれか1項に記載のメッセージ認証装置としたことを特徴とする。

[0025] 請求項8に記載の発明は、入力手段が、メッセージを入力する第1のステップと、パディング手段が、前記入力されたメッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力する第2のステップと、修正木ハッシュ手段が、前記出力されたパディング済みメッセージを、ブロック暗号の部品を基に作った小さい入出力幅のハッシュ関数をメッセージ分だけ並べた処理を繰り返すことで、1ブロックのハッシュ値を出力する第3のステップと、調整値付暗号化手段が、前記出力されたハッシュ値を暗号化してタグとする第4のステップと、出力手段が、前記暗号化されたタグと前記メッセージとを連結して出力する第5のステップとを有するメッセージ認証方法としたことを特徴とする。

[0026] 請求項9に記載の発明は、入力手段が、メッセージを入力する第1のステップと、パディング手段が、前記入力されたメッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力する第2のステップと、交替型連鎖手段が、ブロック暗号と該ブロック暗号の一部分から導出される置換処理とを、前記出力されたパディング済みメッセージを1ブロックずつ足しながら連鎖させて1ブロックのハッシュ値へ圧縮する第3のステップと、調整値付暗号化手段が、前記ハッシュ値を暗号化してタグとする第4のステップと、出力手段が、前記暗号化されたタグと前記メッセージとを連結して出力する第5のステップとを有するメッセージ認証方法としたことを特徴とする。

[0027] 請求項10に記載の発明は、入力手段が、メッセージを入力する第1のステップと、パディング手段が、前記入力されたメッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力する第2のステップと、修正木連鎖ハッシュ手段が、前記出力されたパディング済みメッセージを、請求項2記載の交替型連鎖手段の一部の処理を請求項1記載の修正木ハッシュ手段で置き換えた構造により圧縮して1ブロック分のハッシュ値を出力する第3のステップと、調整値付暗号化手段が、前記ハッシュ値を暗号化してタグとする第4のステップと、出力手段が、前記暗号化されたタグと前記メッセージとを連結して出力する第5のステップとを有するメッセージ認証方法としたことを特徴とする。

[0028] 請求項11に記載の発明は、前記修正木ハッシュ手段が、AESの段関数の4回以

上の繰り返しを用いて構成され、前記調整値付暗号化手段が、AESを用いて構成される請求項8記載のメッセージ認証方法としたことを特徴とする。

[0029] 請求項12に記載の発明は、前記交替型連鎖手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成される請求項9記載のメッセージ認証方法としたことを特徴とする。

[0030] 請求項13に記載の発明は、前記修正木連鎖ハッシュ手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成される請求項10記載のメッセージ認証方法としたことを特徴とする。

[0031] 請求項14に記載の発明は、ブロック暗号と、該ブロック暗号の段関数を利用した置換処理とを用いる請求項8から10のいずれか1項に記載のメッセージ認証方法としたことを特徴とする。

[0032] 請求項15に記載の発明は、請求項8から10のいずれか1項に記載のメッセージ認証方法を、コンピュータに実行させるためのメッセージ認証プログラムとしたことを特徴とする。

[0033] 請求項16に記載の発明は、請求項15記載のメッセージ認証プログラムを記録した記録媒体としたことを特徴とする。

発明の効果

[0034] 本発明によれば、ブロック暗号とその一部の部品を組み合わせて、既存のブロック暗号の認証モードより高速で、理論的安全性を有し、事前処理や使用するメモリ量の点でも効率のよい、メッセージ認証装置、メッセージ認証方法、メッセージ認証プログラムとその記録媒体を実現することができる。

発明を実施するための最良の形態

[0035] 本発明を実施するための最良の形態は、メッセージを入力する入力手段と、メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段と、パディング済みメッセージをブロック暗号の部品を基に作った小さい入出力幅のハッシュ関数をメッセージ分だけ並べた処理を繰り返すことで、1ブロックのハッシュ値を出力する修正木ハッシュ手段と、ハッシュ値を暗

号化してタグとする調整値付暗号化手段と、タグとメッセージとを連結して出力する出力手段とを備えたメッセージ認証装置とする。

[0036] 以下に、本発明の好適な実施形態を添付図面に基づいて詳細に説明する。尚、以下に述べる実施形態は本発明の好適な具体例であるから、技術的に好ましい種々の限定が付されているが、本発明の範囲は、以下の説明において特に本発明を限定する旨の記載がない限り、これらの実施形態に限られるものではない。

[0037] (実施形態1)

まず、本実施形態のメッセージ認証装置の構成及び各部の機能について添付図面を用いて以下に説明する。図2は、本実施形態のメッセージ認証装置の構成を示すブロック図である。図2に示すように、本実施形態のメッセージ認証装置10は、入力手段100、パディング手段101、修正木ハッシュ手段102、調整値付暗号化手段103、及び、出力手段104を備えている。なお、本実施形態のメッセージ認証装置10は、コンピュータが一般的に備えている、CPU(処理装置)、メモリ(主記憶装置)、及び、ディスク(補助記憶装置)等を用いることにより実現することが可能である。

[0038] 図3は、一般的なコンピュータの構成を示したブロック図である。図3に示すように、一般的なコンピュータは、キーボード、マウス等の入力装置1、処理装置(CPU)2、記憶装置3、ディスプレイやプリンタ等の出力装置4を備えている。処理装置(CPU)2は、制御装置5、演算装置6を備えており、計算などの処理を行う中心となる部分である。記憶装置3は、主記憶装置7(メインメモリ)、補助記憶装置8を備えており、データを一時的又は/及び永久的に記憶する。

[0039] 図2に示す本実施形態のメッセージ認証装置10の備える各手段は、メッセージ認証に必要なプログラムをコンピュータのディスク(図3に示す補助記憶装置8)に格納しておき、このプログラムをCPU(図3に示す処理装置2)上で動作させることにより実現することができる。図2に示す入力手段100は、タグを付与する対象となる平文(メッセージ)を入力する手段である。これは例えばキーボードなどの文字入力装置(図3に示す入力装置1)により実現される。

[0040] パディング手段101は、メッセージ長を常にブロックの倍数に変換する手段である。ブロック長は用いるブロック暗号の入力幅によって決まる。もし1ブロックがnビットで、

平文長をnで割った余りが(n－t)の場合、最初が1で残りがすべて0のtビットを平文に付加することで長さをブロックの倍数にする。既にブロックの倍数である平文については何も処理しない。

[0041] この方式に限らず、パディングの仕方は、メッセージ長がブロック長の倍数でない、異なる長さのメッセージ同士でパディングした結果が常に異なり、メッセージ長がブロック長の倍数であるメッセージについては何もしないという条件さえ守られるならばどのようなパディング方法でもよい。パディング手段101は、パディングされたメッセージと、パディング手段101においてパディングが行われたかどうか、すなわち元のメッセージ長がnの倍数だったかどうかを示すインジケータをd(1ならばnの倍数、2ならばそうでない)として出力する。

[0042] 修正木ハッシュ手段102は、パディング手段101が出力するパディングされたメッセージを、ブロック暗号の部品を基に作った小さい入出力幅のハッシュ関数をメッセージ分だけ並べた処理を繰り返すことで1ブロックに圧縮する手段である。1ブロックをnビットとし、nビットブロック暗号をEとする。また、nビットの決定的置換をfとする。

[0043] 修正木ハッシュ手段102の処理は、以下に示す式(2)から成り立っている。この処理は2nビット入力、nビット出力の鍵付き関数である。鍵はブロック暗号Eの鍵である。

$X=(X_1, X_2)$について、$D_i(X)=X_2+f(E(i)+X_1)$・・・式(2)

但し、i＝2^(n)－1以下の非負整数、式(2)において加算はビット毎の排他的論理和を表す。

[0044] ここで、式(2)で示されるnビット関数fの最大差分確率DP(f)について説明する。nビット関数fの最大差分確率DP(f)とは、aは0以外のnビット値、bは任意のnビット値としたときのPr(f(X)－f(X＋a)＝b)の最小値を指す。ただし、確率はXを一様にランダムなnビット値としたもとで計算される。また、加算も減算も排他的論理和を表す。

[0045] 式(2)で示されるnビット関数fは、上記最大差分確率DP(f)が十分小さい、つまり2^(－n)に十分近いことが要求される。nビット置換の場合、最大差分確率は、理論的に2^(－n＋1)まで小さくできることが知られているが、nが大きい場合に最大差分確率が十分小さい置換を作ることは現実には容易ではない。

[0046] しかし、決定的置換のかわりに鍵つきの置換(いくつかの置換の集合からランダムな鍵がひとつの置換を指定する。)を用いることも可能である。このときは、以下に説明する平均最大差分確率EDP(f_{Kp})が小さいことが求められる。

[0047] nビット鍵付き関数f_{Kp}(ただしK_Pが鍵を表す。)の平均最大差分確率EDP(f_{Kp})とは、aは0以外のnビット値、bは任意のnビット値としたときの$Pr(f_{Kp}(X)-f_{Kp}(X+a)=b)$の最小値を指す。ただし、確率はXを一様にランダムなnビット値とし、さらに鍵をランダムとしたもとで計算される。また、加算も減算も排他的論理和を表す。

[0048] ブロック暗号を差分攻撃から守るときには、ブロック暗号の上記平均最大差分確率が小さいことが必要であるため、平均最大差分確率の小さい鍵付き置換はブロック暗号の部品となっていることが多い。例えばブロック暗号AESの場合については4段の段関数が平均最大差分確率の小さい鍵付き置換となることが「S. Park, S. H. Sung, S. Lee, and J. Lim, Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structure and AES, International Workshop, FSE 2003, Lecture Notes in Computer Science; Vol. 2887, Feb. 2003」に記載されている。

[0049] 修正木ハッシュ手段102は、非特許文献3の修正木ハッシュを式(2)に示すD_iを用いて実行することが可能である。すなわち、式(1)に従い、mブロック入力$X=(X_1, X_2\cdots X_m)$について、$MT_{D(X)}=G[D_S](G[D_S-1](\cdots G[D_1](X)\cdots))$(但し、$s=\log(m)$(対数の底は2)以上の最小の整数)を求め、1ブロックの$MT_{D(X)}$を出力する。この$MT_{D(X)}$を修正木ハッシュ値と呼ぶ。

[0050] E(1)、E(2)、・・・、E(s)は、$MT_{D(X)}$を求めるのに用いられ、ハッシュ鍵と呼ばれる。K_Pを鍵とした鍵付き置換f_{Kp}をfの代わりとして用いる場合、式(2)において各D_1、D_2、・・・の鍵K_Pはそれぞれ同一であるか、もしくはそれぞれ異なる独立な値であるかのいずれでもよいが、ランダムに生成されている必要がある。鍵K_Pはブロック暗号Eの鍵と合わせてメッセージ認証装置の秘密鍵とするか、もしくは、ハッシュ鍵がE(1)、E(2)、・・・、E(s)である場合に、E(s+1)、E(s+1)・・・を必要なだけ連結してK_Pとしてもよい。

[0051] 各D_1、D_2、・・・では、ハッシュ鍵E(1)、E(2)、・・・を必要とするが、これはあらかじ

め生成しておいてもよい。非特許文献3においては、異なる長さのメッセージ間でのハッシュ値の衝突を防ぐために、修正木ハッシュ値に長さ情報を付加することが提案されているが、長さ情報を付加しなくとも、異なる長さの入力間での衝突確率は小さいため、非特許文献3に記載の修正木ハッシュを利用して、修正木ハッシュ手段102を実現する場合、長さ情報を付加しなくてよい。

[0052] また、修正木ハッシュを変形して用いることも可能である。例えば、式(1)を変形した、以下に示す式(3)を用いることができる。

$MT_{H(X)}=G[H_S](G[H_{S-1}](\cdots G[H_1](X)\cdots))\cdots$式(3)

入力が偶数ブロック数の場合:

$G[H_1](X)=H_i(X_1, X_2)\|H_i(X_3, X_4)\|\cdots\|H_i(X_{m-1}, X_m)$

入力が奇数ブロック数の場合:

$G[H_1](X)=H_i(X_1, X_2)\|H_i(X_3, X_4)\|\cdots\|H_i(X_{m-2}, X_{m-1})\|H_i(X_m, 000\cdot\cdot0)$

但し、s=log(m)(対数の底は2)以上の最小の整数、000・・0は全てゼロの系列

[0053] これは非特許文献3に記載されている、基本的な木ハッシュの構成である。ただし、この木ハッシュを用いる場合は、異なる長さのメッセージ間でのハッシュ値の衝突を防ぐため、もとのメッセージの長さ情報を最後に連結して、出力としなければならない。

[0054] 調整値付暗号化手段103は、修正木ハッシュ手段102の出力である修正木ハッシュ値を暗号化する手段である。暗号化は、以下に示す式(4)にしたがって行われる。

$TB[E](x, d)=E((L*u_d)+Y)\cdots$式(4)

nビットのu_1とu_2を、互いに異なる、1か0でない任意の定数とする。

任意のnビット値a, bについてa*bを有限体GF(2^(n))上の積とする。

ブロック暗号Eについて、L=E(0)とする(但し、d=1もしくは2)。

[0055] 調整値付暗号化手段103は、修正木ハッシュ手段102の出力をYとすると、TB[E](Y, d)を出力する。ここでdは、パディング手段101が出力するパディングの有無、すなわちメッセージ長がnの倍数だったかを示すインジケータである。dが1ならばメッセージ長がnの倍数、2ならばそうでないとする。L=E(0)、もしくは$L*u_1$と$L*u_2$は事前に計算してメモリに保持しておいてもよい。

[0056] インジケータdにより暗号化の処理内容が変わることから、$L*u_1$と$L*u_2$のことを調整値と呼ぶ。有限体上の積＊は、u_1とu_2が定数であるため、ビットシフトと条件付の定数との排他的論理和という、ごく簡単な演算で実行できる。例えば、$u_1=2$、と$u_2=4$とした場合の計算が、「Tetsu Iwata, Kaoru Kurosawa, OMAC: One-Key CBC MAC、Fast Software Encryption, International Workshop, FSE 2003, Lecture Notes in Computer Science; Vol. 2887, Feb. 2003」に記載されている。

[0057] 出力手段104は、調整値付暗号化手段103が出力したされた暗号文をタグとし、入力手段100に入力されたメッセージと連結してコンピュータディスプレイやプリンタなどへ出力する手段である。例として、mブロック入力でのメッセージ認証装置10の動作例を図4示す。図4は、メッセージがちょうどmブロック分の長さだったとし、入力手段100、パディング手段101、及び、出力手段104は省略してある。図1おいて、Eはブロック暗号、fはある決定的置換もしくは鍵つき置換である。鍵がKでメッセージがXの時の暗号化を$E_{K(X)}$とすれば、ハッシュ鍵は$E_{K(1)}$, $E_{K(2)}$, ・・・, $E_{K(d)}$に相当する。

[0058] 次に、本実施形態のメッセージ認証装置10の動作について図5を用いて以下に詳細に説明する。図5は、本実施形態のメッセージ認証装置10の動作について説明するためのフローチャートである。図5に示すように、まず、修正木ハッシュ手段102と調整値付暗号化手段103が用いるハッシュ鍵と調整値をあらかじめ生成されているかを調べる(ステップ101)。もしすでに生成されているのであればステップ103へ進み、まだであればハッシュ鍵と調整値を生成する(ステップ102)。

[0059] 次にメッセージを入力し(ステップ103)、パディングを実行する(ステップ104)。パディングされたメッセージに対して修正木ハッシュを実行し(ステップ105)、修正木ハッシュの出力に対して調整値付暗号化を適用してタグとする(ステップ106)。最後にタグとメッセージを連結し、出力する(ステップ107)。

[0060] (実施形態2)

まず、本実施形態のメッセージ認証装置の構成及び各部の機能について添付図面を用いて以下に説明する。図6は、本実施形態のメッセージ認証装置の構成を示すブロック図である。図6に示すように、本実施形態のメッセージ認証装置20は、入力手段200、パディング手段201、交替型連鎖手段202、調整値付暗号化手段203

、及び、出力手段204を備えている。なお、本実施形態のメッセージ認証装置20は、コンピュータが一般的に備えている、CPU(処理装置)、メモリ(主記憶装置)、及び、ディスク(補助記憶装置)等を用いることにより実現することが可能である。

[0061] 図3は、一般的なコンピュータの構成を示したブロック図である。図3に示すように、一般的なコンピュータは、キーボード、マウス等の入力装置1、処理装置(CPU)2、記憶装置3、ディスプレイやプリンタ等の出力装置4を備えている。処理装置(CPU)2は、制御装置5、演算装置6を備えており、計算などの処理を行う中心となる部分である。記憶装置3は、主記憶装置7(メインメモリ)、補助記憶装置8を備えており、データを一時的又は/及び永久的に記憶する。

[0062] 図6に示す本実施形態のメッセージ認証装置20の備える各手段は、メッセージ認証に必要なプログラムをコンピュータのディスク(図3に示す補助記憶装置8)に格納しておき、このプログラムをCPU(図3に示す処理装置2)上で動作させることにより実現することができる。図6に示す入力手段200は、タグを付与する対象となる平文(メッセージ)を入力する手段である。これは例えばキーボードなどの文字入力装置(図3に示す入力装置1)により実現される。

[0063] パディング手段201は、メッセージ長を常にブロックの倍数に変換する手段である。ブロック長は用いるブロック暗号の入力幅によって決まる。もし1ブロックがnビットで、平文長をnで割った余りが(n−t)の場合、最初が1で残りがすべて0のtビットを平文に付加することで長さをブロックの倍数にする。既にブロックの倍数である平文については何も処理しない。

[0064] この方式に限らず、パディングの仕方は、メッセージ長がブロック長の倍数でない、異なる長さのメッセージ同士でパディングした結果が常に異なり、メッセージ長がブロック長の倍数であるメッセージについては何もしないという条件さえ守られるならばどのようなパディング方法でもよい。パディング手段201は、パディングされたメッセージと、パディング手段201においてパディングが行われたかどうか、すなわち元のメッセージ長がnの倍数だったかどうかを示すインジケータをd(1ならばnの倍数、2ならばそうでない)として出力する。

[0065] 交替型連鎖手段202は、nビットブロック暗号Eと、Eの一部分から導出されるnビット

置換fとを、メッセージを一ブロックずつ足しながら連鎖させてパディング手段201の出力を1ブロックへ圧縮する手段である。交替型連鎖手段202の処理は、以下に示す式(5)から成り立っている。tをある非負の整数として、この処理はn(t+3)ビット入力、nビット出力の鍵付き関数である。鍵はブロック暗号Eの鍵と補助鍵$KAux_1$, $KAux_2$, ・・・, $KAux_t$である。tが0であっても、つまり補助鍵がなしでもよい。

[0066] ＜処理ACBC＞

$ACBC(X)=(S_{t+1})+X_{t+3}$ ・・・式(5)

$X=(X_1, X_2, \cdots, X_{t+3})$について、$S_1=f(E(X_1)+X_2)$

$1<i<t+2$について、$S_i=f((S_{i-1})+(KAux_{i-1})+X_{i+1})$

[0067] 交替型連鎖手段202は、上記式(5)に記載の処理ACBCを連鎖する。すなわち最初の(t+3)入力ブロックをXとすると、XへACBCを適用し式(5)に従いACBC(X)を求め、ACBC(X)と次の(t+2)入力ブロックとを連結して、再度ACBCへ入力する。この処理を繰り返し、最後の入力ブロックを足した時点でただちに停止し、その結果を出力する。最後の入力ブロックに対応する補助鍵は足してもよいし、足さなくてもよい。

[0068] 補助鍵はブロック暗号の鍵と独立な鍵でもよいが、後述の調整値付暗号化手段203を用いた処理にしたがって生成してもよい。実施形態1における修正木ハッシュ手段102の場合と同様、式(5)のACBCで用いるfが、最大差分確率の小さい置換であることが必要である。さらに、以下に説明するnビット関数fの最大自己差分確率SDP(f)が小さいことも必要となる。

[0069] nビット関数fの最大自己差分確率SDP(f)とは、aは任意のnビット値としたときのPr(X−f(X)＝a)の最小値を指す。但し、確率は、Xを一様にランダムなnビット値としたもとで計算される。また、加算も減算も排他的論理和を表す。

[0070] また、実施形態1における修正木ハッシュ手段102の場合と同様に、ACBCにおいて、Kを鍵とする鍵付きの置換f_{Kp}をfの代わりに使うことが可能である。この場合、Kpは一度設定した後はずっと変更しないか、もしくはt+1個、つまり補助鍵の数+1個、の独立でランダムな値を用意し、メッセージブロックを処理するたびに周期的に変更させてもよい。但し、鍵付きの置換f_{Kp}を用いる場合、f_{Kp}の平均最大差分確率と、以

下に説明する平均最大自己差分確率ESDP(f_{Kp})の両方が小さいことが必要となる。

[0071] nビット鍵付き関数f_{Kp}(但し、K_pが鍵を表す。)の平均最大自己差分確率ESDP(f_{Kp})とは、aは任意のnビット値としたときのPr(X－f_{Kp}(X)＝a)の最小値を指す。但し、確率は、Xを一様にランダムなnビット値とし、さらに鍵Kpをランダムとしたもとで計算される。また、加算も減算も排他的論理和を表す。

[0072] ブロック暗号の段関数において、鍵を中間変数へ排他的論理和することは一般的である。このような構造の場合、段関数の平均最大自己差分確率は最小となることが容易に示せる。例えば、AESの段関数では、何段であれ平均最大自己差分確率が最小値2^(－128)となる。交替型連鎖手段202の出力を交替型連鎖ハッシュ値と呼ぶことにする。

[0073] 調整値付暗号化手段203は、以下に示す処理Aにしたがい、交替型連鎖ハッシュ値を暗号化する。

＜処理A＞

nビットのu_1とu_2を、互いに異なる、1か0でない任意の定数とする。任意のnビット値a, bについてa＊bを有限体GF(2^(n))上の積とする。ブロック暗号Eについて、Lをブロック暗号の鍵と独立でランダムなnビット値とする。Lはブロック暗号の鍵と合わせてメッセージ認証装置の鍵となる。dが0, 1, 2のどれかをとるとし、TTB[E, L](Y, d)を、d＝0ならE(L＋Y)と、d＝1ならE((L＊u_1)＋Y)と、d＝2ならE((L＊u_2)＋Y)と、する。

[0074] 調整値付暗号化手段203は、パディング手段201が出力するパディングの有無のインジケータをdとして、交替型連鎖手段202の出力をTTB[E, L]に基づき暗号化する。交替型連鎖手段202の出力をYとすれば、調整値付暗号化手段202の出力は、dが1ならE((L＊u_1)＋Y)、dが2ならE((L＊u_2)＋Y)である。L＊u_1とL＊u_2のことを調整値と呼ぶ。実施形態1における調整値付暗号化手段103同様、u_1とu_2の値をそれぞれ2と4とした場合の計算方法は、「Tetsu Iwata, Kaoru Kurosawa, OMAC: One-Key CBC MAC、Fast Software Encryption, International Workshop, FSE 2003, Lecture Notes in Computer Science; Vol. 2887, Feb. 2003」に記載されている。

[0075] 交替型連鎖手段202における補助鍵がt個ある場合、E(L＋0), E(L＋1), ・・・,

E(L+t−1)を補助鍵$KAux_1$, ・・・, $KAux_t$としてもよい。また、上記処理Aにおけるdの値による場合分けの処理は、任意に入れ替えてもよい。例えば、パディングの有無のインジケータがdで交替型連鎖手段202の出力がYのとき、d=1でE(L+Y)を、d=2でE(L＊u_1+Y)を出力とし、補助鍵がt個ある場合、E((L＊u_2)+0), E((L＊u_2)+1), ・・・, E((L＊u_2)+t−1)を補助鍵としてもよい。

[0076] 出力手段204は、実施形態1におけるメッセージ認証装置10の出力手段104と同様である。例として、ある長さのメッセージに対するメッセージ認証装置20の動作例を図7に示す。メッセージ長がちょうどブロック長の整数倍だったとし、入力手段200、パディング手段201、及び、出力手段204は省略してある。補助鍵がない場合と1個の場合を例として記載している。図7においてEはブロック暗号、fはある決定的置換もしくは鍵つき置換を示す。

[0077] 次に、本実施形態のメッセージ認証装置20の動作について図8を用いて以下に詳細に説明する。図8は、本実施形態のメッセージ認証装置20の動作について説明するためのフローチャートである。図8に示すように、まず、交替型連鎖手段202と調整値付暗号化手段203が用いる補助鍵と調整値をあらかじめ生成されているかを調べる(ステップ201)。もしすでに生成されているのであればステップ203へ進み、まだであれば補助鍵と調整値を生成する(ステップ202)。

[0078] 次にメッセージを入力し(ステップ203)、パディングを実行する(ステップ204)。パディングされたメッセージに対して交替型連鎖手段202を実行し(ステップ205)、交替型連鎖手段202の出力交替型連鎖ハッシュ値に対して調整値付暗号化を適用してタグとする(ステップ206)。最後にタグとメッセージを連結し、出力する(ステップ207)。

[0079] (実施形態3)

まず、本実施形態のメッセージ認証装置の構成及び各部の機能について添付図面を用いて以下に説明する。図9は、本実施形態のメッセージ認証装置の構成を示すブロック図である。図9に示すように、本実施形態のメッセージ認証装置30は、入力手段300、パディング手段301、修正木連鎖ハッシュ手段302、調整値付暗号化手段303、及び、出力手段304を備えている。なお、本実施形態のメッセージ認証装

置30は、コンピュータが一般的に備えている、CPU(処理装置)、メモリ(主記憶装置)、及び、ディスク(補助記憶装置)等を用いることにより実現することが可能である。

[0080] 図3は、一般的なコンピュータの構成を示したブロック図である。図3に示すように、一般的なコンピュータは、キーボード、マウス等の入力装置1、処理装置(CPU)2、記憶装置3、ディスプレイやプリンタ等の出力装置4を備えている。処理装置(CPU)2は、制御装置5、演算装置6を備えており、計算などの処理を行う中心となる部分である。記憶装置3は、主記憶装置7(メインメモリ)、補助記憶装置8を備えており、データを一時的又は/及び永久的に記憶する。

[0081] 図9に示す本実施形態のメッセージ認証装置30の備える各手段は、メッセージ認証に必要なプログラムをコンピュータのディスク(図3に示す補助記憶装置8)に格納しておき、このプログラムをCPU(図3に示す処理装置2)上で動作させることにより実現することができる。図9に示す入力手段300及びパディング手段301は、実施形態1のメッセージ認証装置10の各手段と同様である。調整値付暗号化手段303は、実施形態2のメッセージ認証装置20の調整値付暗号化手段203と同様である。

[0082] 修正木連鎖ハッシュ手段302の処理は、実施形態1の交替型連鎖手段102における一部の処理を、実施形態2の修正木ハッシュ手段202で置き換えたものである。まず1以上の整数tを定める。t個のハッシュ鍵($R_1, R_2, \ldots, R_t$)を用いるものとする。この場合、パディング手段301の出力に対し、最初の1ブロック目をブロック暗号Eで暗号化しY_0を得る。次の2^(t+1)ブロック分の入力を、($R_1, R_2, \ldots, R_t, Y_0$)をハッシュ鍵とした修正木ハッシュを適用する。但し、Y_0は、最後の2ブロックを1ブロックへ圧縮する処理に用いられるものとする。

[0083] この修正木ハッシュの出力をブロック暗号で暗号化し、Y_1を得る。次の2^(t+1)ブロック分の入力を、今度は($R_1, R_2, \ldots, R_t, Y_1$)をハッシュ鍵とした修正木ハッシュで圧縮する。この処理を繰り返す。最後の修正木ハッシュの出力が修正木連鎖ハッシュ手段302の出力となる。但し、最後の修正木ハッシュへの入力が2^(t+1)ブロックより短い場合は、その出力は以下に従う。上記の処理をs回繰り返したとして、ハッシュ鍵を($R_1, R_2, \ldots, R_t, Y_S$)とする。

[0084] 最後の修正木ハッシュへの入力が1ブロックのみのxである場合、(Y_S)+xを出力

する。2ブロック以上の入力の場合、修正木ハッシュにおいて常に最後の2ブロックを1ブロックへ圧縮する処理でY_Sを用いるものとする。つまり修正木ハッシュが式(1)の処理を繰り返して入力を短くしていき、2ブロック(z_1, z_2)を得たとき、$f(z_1+Y_S)+Z_2$が出力となる。

[0085] 修正木ハッシュをある決定的置換fで実現する場合、fは最大差分確率と最大自己差分確率が小さいことが求められる。また、Kpを鍵としたもし鍵付きの置換f_{Kp}で実現する場合には、f_{Kp}は平均最大差分確率と平均最大自己差分確率が小さいことが求められる。t個のハッシュ鍵$(R_1, R_2, \ldots, R_t)$はブロック暗号Eの鍵と独立でもよいし、実施形態2における補助鍵と同様に$E(L+0), E(L+1), \ldots, E(L+t-1)$をそれぞれ$R_1, \ldots, R_t$としてもよい。修正木連鎖ハッシュ手段302の出力を修正木連鎖ハッシュ値と呼ぶことにする。

[0086] 調整値付暗号化手段303は、実施形態2の調整値付暗号化手段203と同様である。出力手段304は、実施形態1の出力手段104と同様である。例として、ある長さのメッセージに対するメッセージ認証装置30の動作例を図10に示す。メッセージ長がちょうどブロック長の整数倍だったとし、入力手段300、パディング手段301、及び、出力手段304は省略してある。図10においてE, f, $g_{R1}, \ldots g_{Rt}$は、図4及び図7と同様である。

[0087] 次に、本実施形態のメッセージ認証装置30の動作について図11を用いて以下に詳細に説明する。図11は、本実施形態のメッセージ認証装置30の動作について説明するためのフローチャートである。図11に示すように、まず、修正木連鎖ハッシュ手段302と調整値付暗号化手段303が用いるハッシュ鍵と調整値をあらかじめ生成されているかを調べる(ステップ301)。もしすでに生成されているのであればステップ301へ進み、まだであればハッシュ鍵と調整値を生成する(ステップ302)。

[0088] 次にメッセージを入力し(ステップ303)、パディングを実行する(ステップ304)。パディングされたメッセージに対して修正木連鎖ハッシュ手段302を実行し(ステップ305)、修正木連鎖ハッシュ手段302の出力に対して調整値付暗号化を適用してタグとする(ステップ306)。最後にタグとメッセージを連結し、出力する(ステップ307)。

[0089] 本発明によれば、第1の効果は、CBC－MACなどのブロック暗号の認証モードよ

りも高速処理なことである。その理由は、ブロック暗号の段関数など、一部分の処理を取り出してメッセージの処理に用いるからである。わずかな事前処理の時間を除けば、任意のメッセージ長においてCBC－MACの処理量よりも少ない処理量で実行可能である。メッセージが1ブロックのときはCBC－MACとほぼ同等となるが、これは明らかに必要不可欠な処理である。

[0090] 例として「J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES submission, 1998.」に記載のブロック暗号AESと、AESの段関数の4回の繰り返し（4段AES）とを用いた場合、AESのCBC－MACよりも約1．3から約2．5倍高速となる。高速化の度合いは実施の形態によって異なり、どの実施の形態が望ましいかは使用可能な動的メモリの量や、許容される事前処理の時間などで決まる。

[0091] 本発明によれば、第2の効果は、CBC－MACなどのブロック暗号の認証モードとほぼ同等のプログラムサイズとなることである。その理由は、ブロック暗号とその一部分のみを用いるためである。その他に必要な演算は排他的論理和などの極めて単純な関数のみである。

[0092] 本発明によれば、第3の効果は、本発明を既知のブロック暗号に適用したとき、CBC－MACなどのブロック暗号の認証モードと同等の理論的安全性を有するように構成できることである。その理由は、本発明で用いるブロック暗号の一部分が差分攻撃に理論的安全性を持つ、すなわち平均最大差分確率が十分小さい場合には、本発明は非特許文献1に記載の理論的安全性の意味で安全な認証方式となるからである。

[0093] ここで、ブロック暗号の段関数の数回の繰り返しが小さい平均最大差分確率を持つことは、十分な安全性を持つブロック暗号の必須条件と言えるため、近年提案されたブロック暗号の多くがこの性質を持つように設計されていることに注意されたい。例えばAESでは、4段AESが十分小さい平均最大差分確率を持つことが「S. Park, S. H. Sung, S. Lee, and J. Lim, Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structure and AES, International Workshop, FSE 2003, Lecture Notes in Computer Science; Vol. 2887, Feb. 2003」に記載されている。

[0094] 本発明の実施の形態によっては、使用するブロック暗号の一部分に、平均最大差分確率だけでなく、平均最大自己差分確率と呼ばれる値が十分小さいことも要求されるが、これは弱い追加条件である。実際、AESを含めた多くのブロック暗号で、段関数が繰り返し回数に関わらず理論的に最小の平均最大自己差分確率をとることが示せる。

[0095] 本発明は、無線もしくは有線のデータ通信における改ざんを防ぐといった用途や、ストレージ上のデータの改ざん防止といった用途に適用することができる。

図面の簡単な説明

[0096] [図1]OMACを示したブロック図である。

[図2]第1の実施形態におけるメッセージ認証装置の構成を示すブロック図である。

[図3]一般的なコンピュータの構成を示したブロック図である。

[図4]第1の実施形態のメッセージ認証装置における、mブロック入力での動作例を示した図である。

[図5]第1の実施形態のメッセージ認証装置の動作について説明するためのフローチャートである。

[図6]第2の実施形態におけるメッセージ認証装置の構成を示すブロック図である。

[図7]第2の実施形態のメッセージ認証装置における、ある長さのメッセージに対する動作例を示した図である。

[図8]第2の実施形態のメッセージ認証装置の動作について説明するためのフローチャートである。

[図9]第3の実施形態におけるメッセージ認証装置の構成を示すブロック図である。

[図10]第3の実施形態のメッセージ認証装置における、ある長さのメッセージに対する動作例を示した図である。

[図11]第3の実施形態のメッセージ認証装置の動作について説明するためのフローチャートである。

符号の説明

[0097] 1 入力装置

2 処理装置(CPU)

3　記憶装置

4　出力装置

5　制御装置

6　演算装置

7　主記憶装置

8　補助記憶装置

10、20、30　メッセージ認証装置

100、200、300　入力手段

101、201、301　パディング手段

102　修正木ハッシュ手段

103、203、303　調整値付暗号化手段

104、204、304　出力手段

202　交替型連鎖手段

302　修正木連鎖ハッシュ手段

請求の範囲

[1] メッセージを入力する入力手段と、

前記メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段と、

前記パディング済みメッセージを、ブロック暗号の部品を基に作った小さい入出力幅のハッシュ関数をメッセージ分だけ並べた処理を繰り返すことで、1ブロックのハッシュ値を出力する修正木ハッシュ手段と、

前記ハッシュ値を暗号化してタグとする調整値付暗号化手段と、

前記タグと前記メッセージとを連結して出力する出力手段と、

を備えたことを特徴とするメッセージ認証装置。

[2] メッセージを入力する入力手段と、

前記メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段と、

ブロック暗号と該ブロック暗号の一部分から導出される置換処理とを、前記パディング済みメッセージを1ブロックずつ足しながら連鎖させて1ブロックのハッシュ値へ圧縮する交替型連鎖手段と、

前記ハッシュ値を暗号化してタグとする調整値付暗号化手段と、

前記タグと前記メッセージとを連結して出力する出力手段と、

を備えたことを特徴とするメッセージ認証装置。

[3] メッセージを入力する入力手段と、

前記メッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力するパディング手段と、

前記パディング済みメッセージを、請求項2記載の交替型連鎖手段の一部の処理を請求項1記載の修正木ハッシュ手段で置き換えた構造により圧縮して1ブロック分のハッシュ値を出力する修正木連鎖ハッシュ手段と、

前記ハッシュ値を暗号化してタグとする調整値付暗号化手段と、

前記タグと前記メッセージとを連結して出力する出力手段と、

を備えたことを特徴とするメッセージ認証装置。

[4] 前記修正木ハッシュ手段が、AESの段関数の4回以上の繰り返しを用いて構成され、前記調整値付暗号化手段が、AESを用いて構成されることを特徴とする請求項1記載のメッセージ認証装置。

[5] 前記交替型連鎖手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成されることを特徴とする請求項2記載のメッセージ認証装置。

[6] 前記修正木連鎖ハッシュ手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成されることを特徴とする請求項3記載のメッセージ認証装置。

[7] ブロック暗号と、該ブロック暗号の段関数を利用した置換処理とを用いることを特徴とする請求項1から3のいずれか1項に記載のメッセージ認証装置。

[8] 入力手段が、メッセージを入力する第1のステップと、

パディング手段が、前記入力されたメッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力する第2のステップと、

修正木ハッシュ手段が、前記出力されたパディング済みメッセージを、ブロック暗号の部品を基に作った小さい入出力幅のハッシュ関数をメッセージ分だけ並べた処理を繰り返すことで、1ブロックのハッシュ値を出力する第3のステップと、

調整値付暗号化手段が、前記出力されたハッシュ値を暗号化してタグとする第4のステップと、

出力手段が、前記暗号化されたタグと前記メッセージとを連結して出力する第5のステップと、

を有することを特徴とするメッセージ認証方法。

[9] 入力手段が、メッセージを入力する第1のステップと、

パディング手段が、前記入力されたメッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力する第2のステップと、

交替型連鎖手段が、ブロック暗号と該ブロック暗号の一部分から導出される置換処理とを、前記出力されたパディング済みメッセージを1ブロックずつ足しながら連鎖させて1ブロックのハッシュ値へ圧縮する第3のステップと、

調整値付暗号化手段が、前記ハッシュ値を暗号化してタグとする第4のステップと、

出力手段が、前記暗号化されたタグと前記メッセージとを連結して出力する第5のステップと、

を有することを特徴とするメッセージ認証方法。

[10] 入力手段が、メッセージを入力する第1のステップと、

パディング手段が、前記入力されたメッセージをパディングしてその長さを常にブロック長の定数にしてパディング済みメッセージとして出力する第2のステップと、

修正木連鎖ハッシュ手段が、前記出力されたパディング済みメッセージを、請求項2記載の交替型連鎖手段の一部の処理を請求項1記載の修正木ハッシュ手段で置き換えた構造により圧縮して1ブロック分のハッシュ値を出力する第3のステップと、

調整値付暗号化手段が、前記ハッシュ値を暗号化してタグとする第4のステップと、

出力手段が、前記暗号化されたタグと前記メッセージとを連結して出力する第5のステップと、

を有することを特徴とするメッセージ認証方法。

[11] 前記修正木ハッシュ手段が、AESの段関数の4回以上の繰り返しを用いて構成され、前記調整値付暗号化手段が、AESを用いて構成されることを特徴とする請求項8記載のメッセージ認証方法。

[12] 前記交替型連鎖手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成されることを特徴とする請求項9記載のメッセージ認証方法。

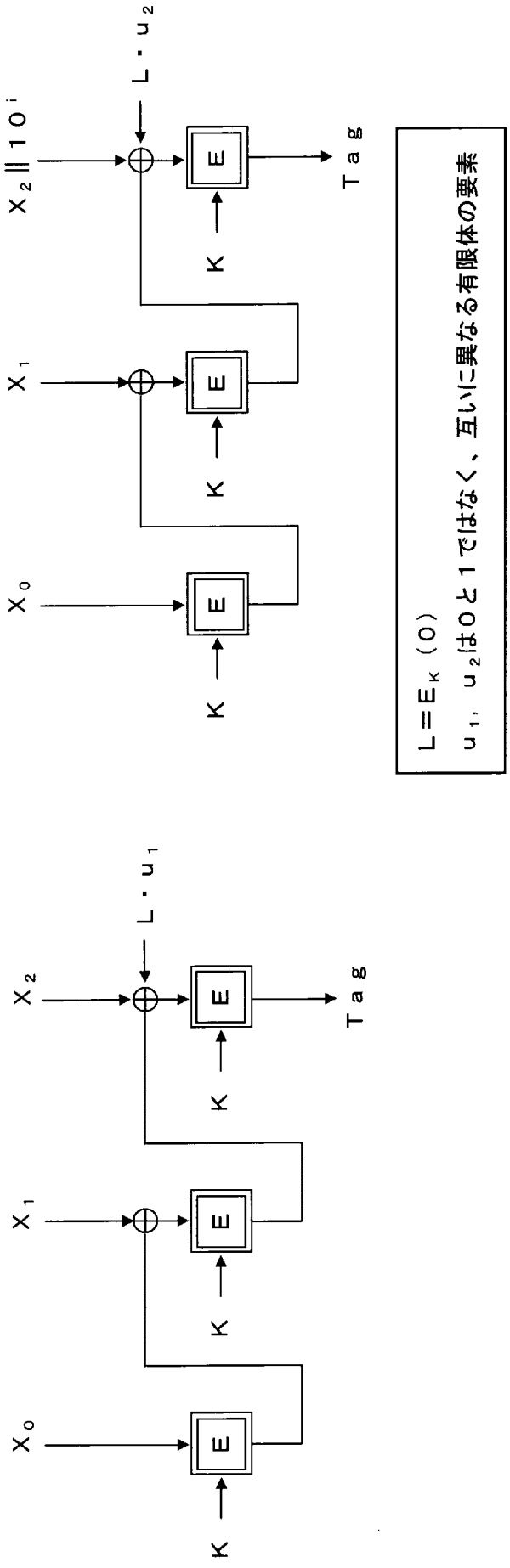
[13] 前記修正木連鎖ハッシュ手段が、AESとAESの段関数の4回以上の繰り返しとを組み合わせて構成され、前記調整値付暗号化手段が、AESを用いて構成されることを特徴とする請求項10記載のメッセージ認証方法。

[14] ブロック暗号と、該ブロック暗号の段関数を利用した置換処理とを用いることを特徴とする請求項8から10のいずれか1項に記載のメッセージ認証方法。

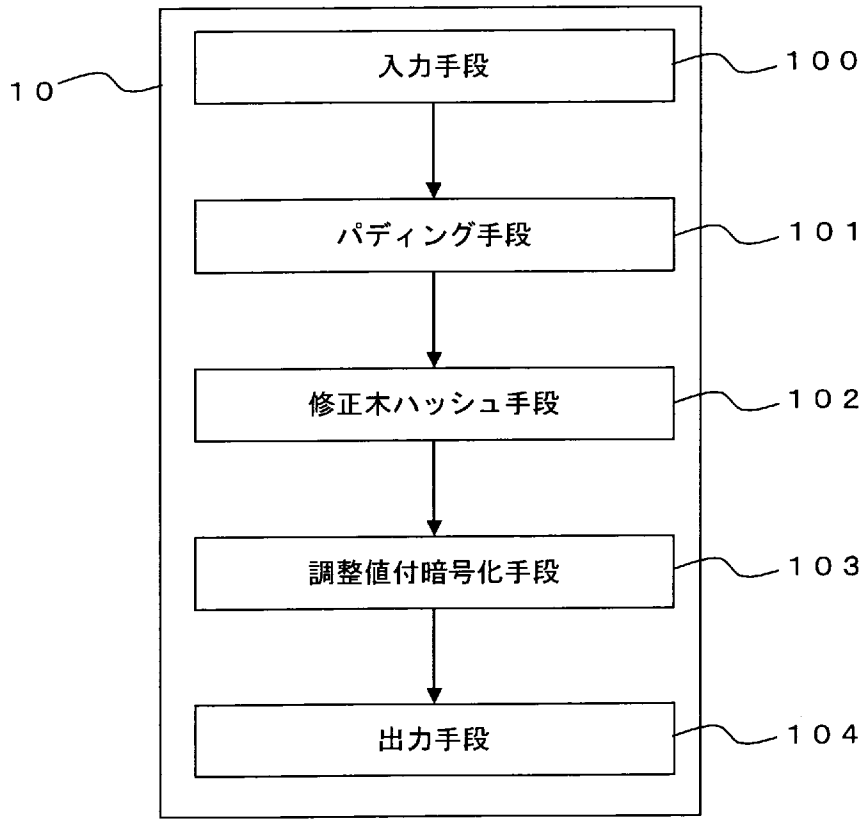
[15] 請求項8から10のいずれか1項に記載のメッセージ認証方法を、コンピュータに実行させるためのメッセージ認証プログラム。

[16] 請求項15記載のメッセージ認証プログラムを記録した記録媒体。

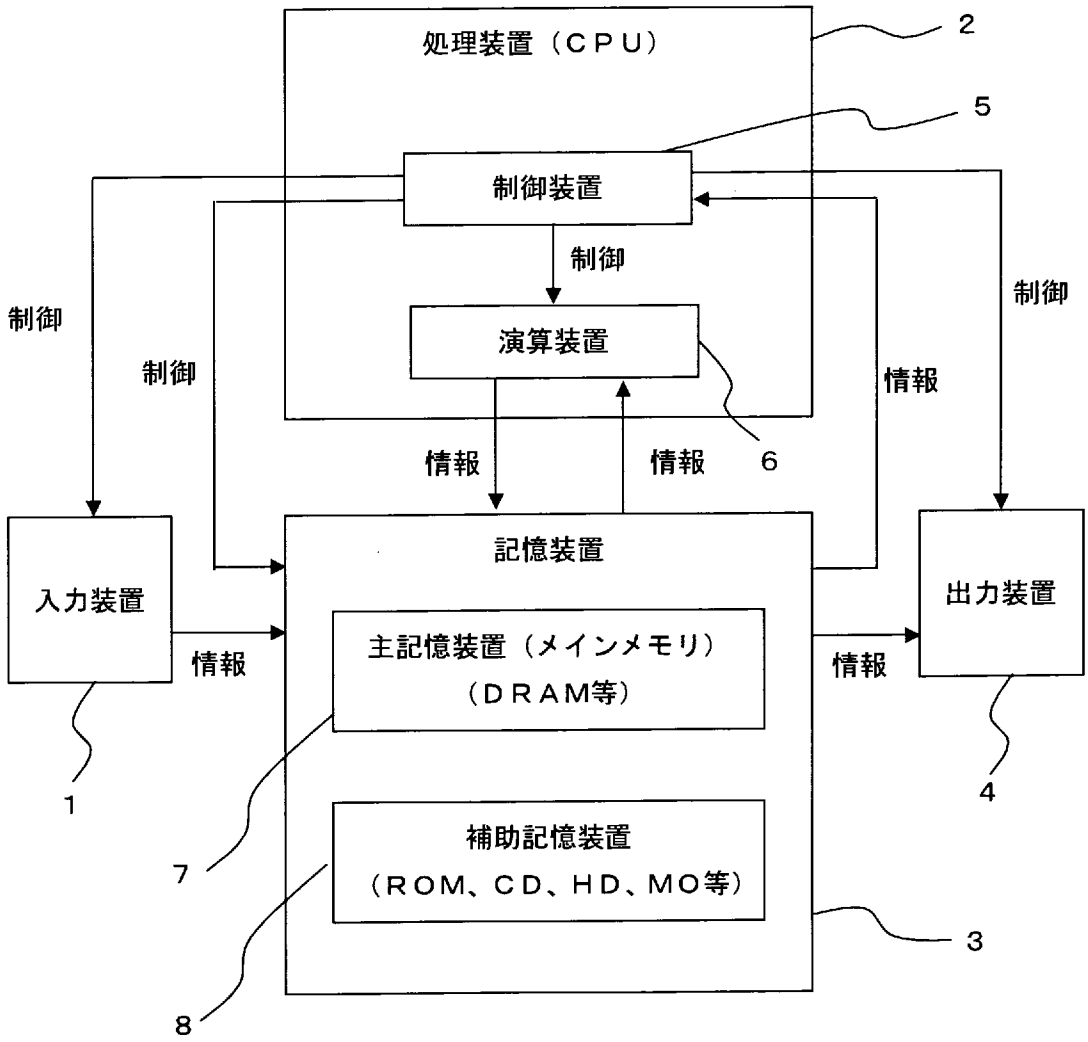
[図1]


L・u2
X2||10i
E
Tag
K
X1
X0
L=EK(0)
u1, u2は0と1ではなく、互いに異なる有限体の要素
L・u1
X2
X1
X0

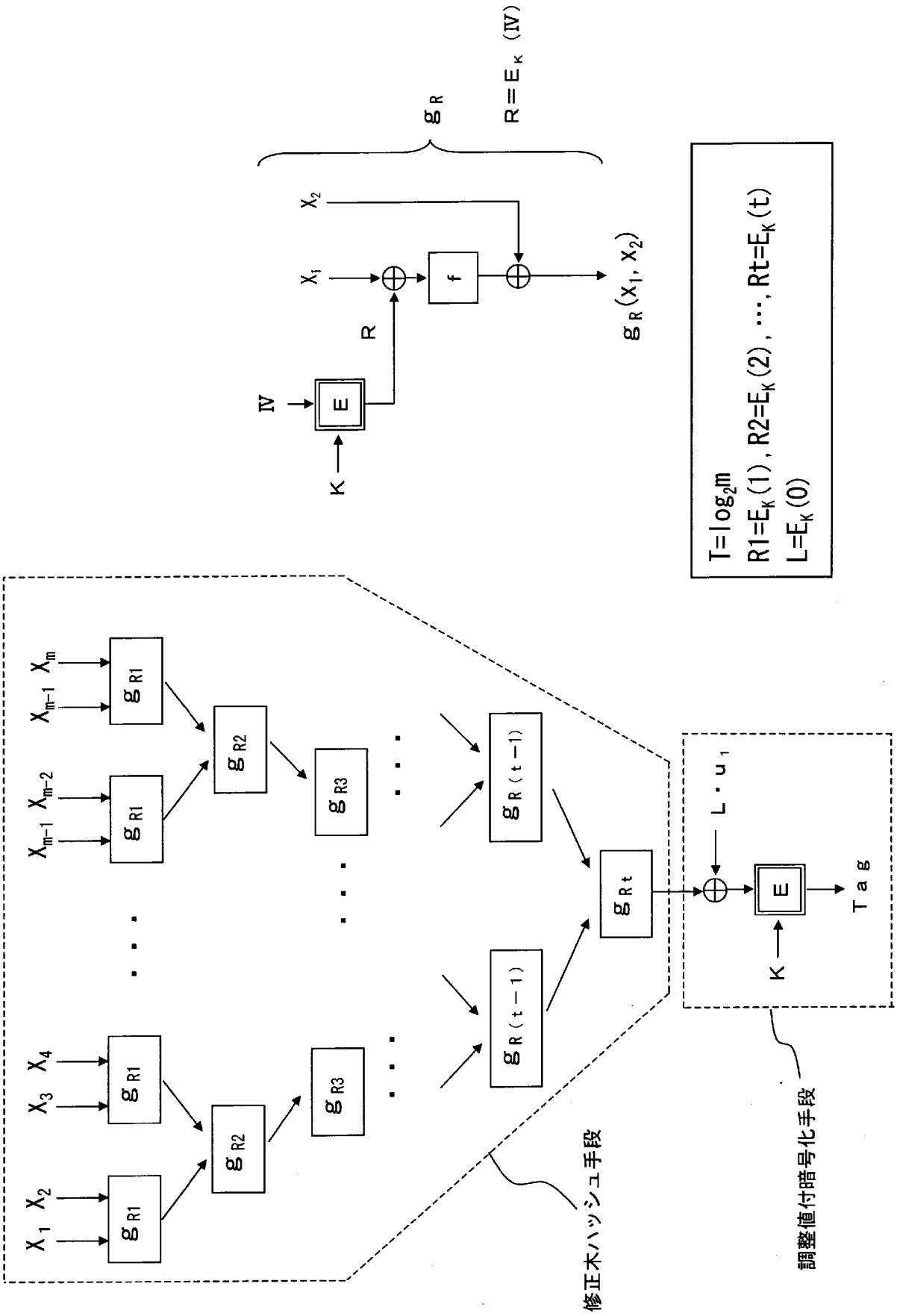
[図2]


１０
入力手段
１００
パディング手段
１０１
修正木ハッシュ手段
１０２
調整値付暗号化手段
１０３
出力手段
１０４

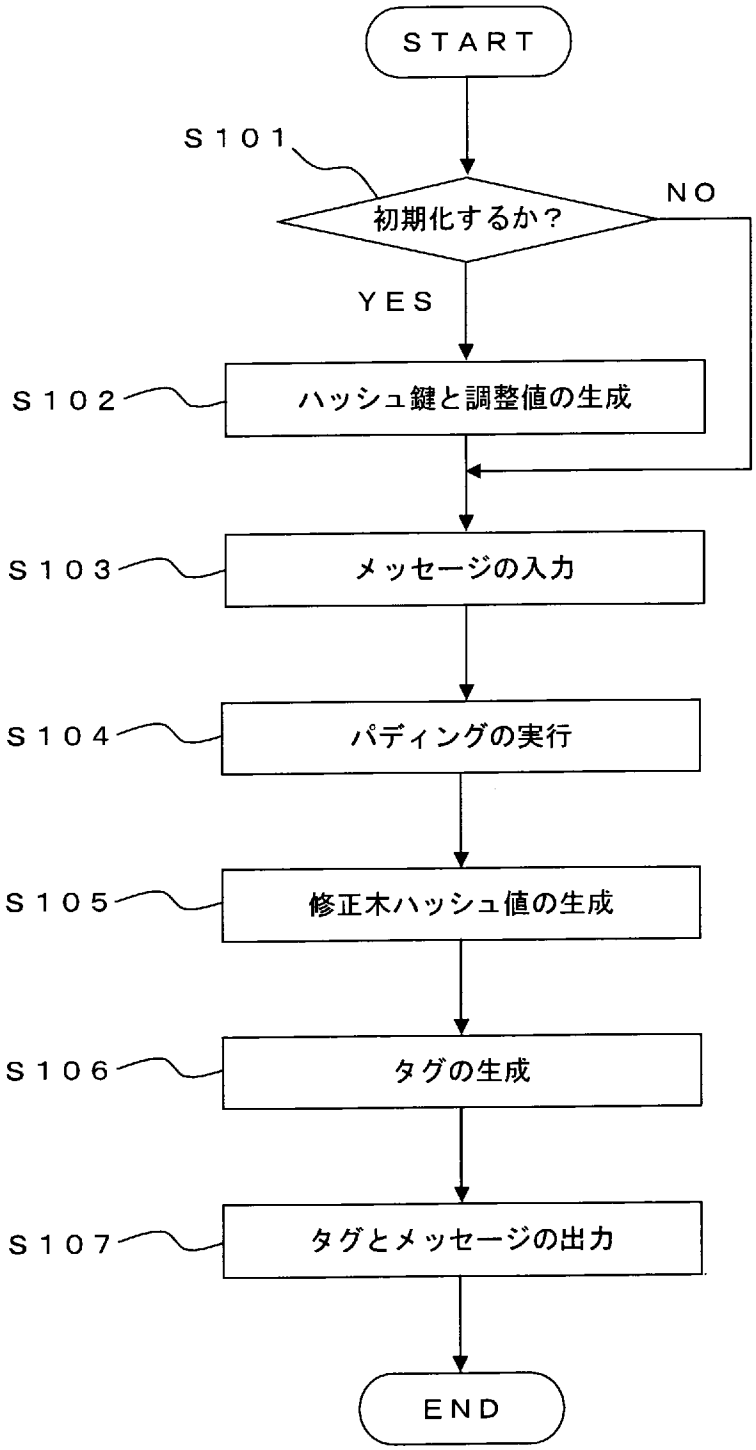
[図3]


処理装置（ＣＰＵ）
2
5
制御装置
制御
演算装置
6
制御
制御
制御
情報
情報
情報
記憶装置
入力装置
情報
主記憶装置（メインメモリ）
（ＤＲＡＭ等）
情報
出力装置
1
4
7
補助記憶装置
（ＲＯＭ、ＣＤ、ＨＤ、ＭＯ等）
3
8

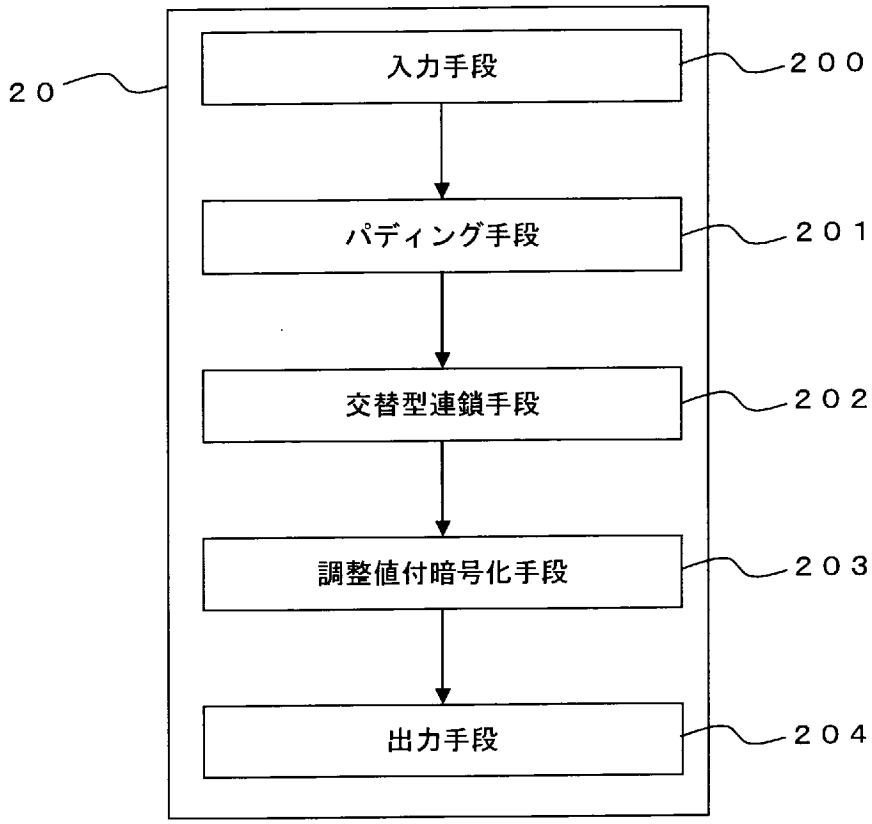
[図4]


T=log2m
R1=EK(1), R2=EK(2), ···, Rt=EK(t)
L=EK(0)
gR
R=EK (IV)
IV
K
E
R
X1
X2
f
gR(X1, X2)
gR1
gR2
gR3
gR(t−1)
gRt
Xm
Xm−1
Xm−2
X4
X3
L・u1
Tag
修正木ハッシュ手段
調整値付暗号化手段

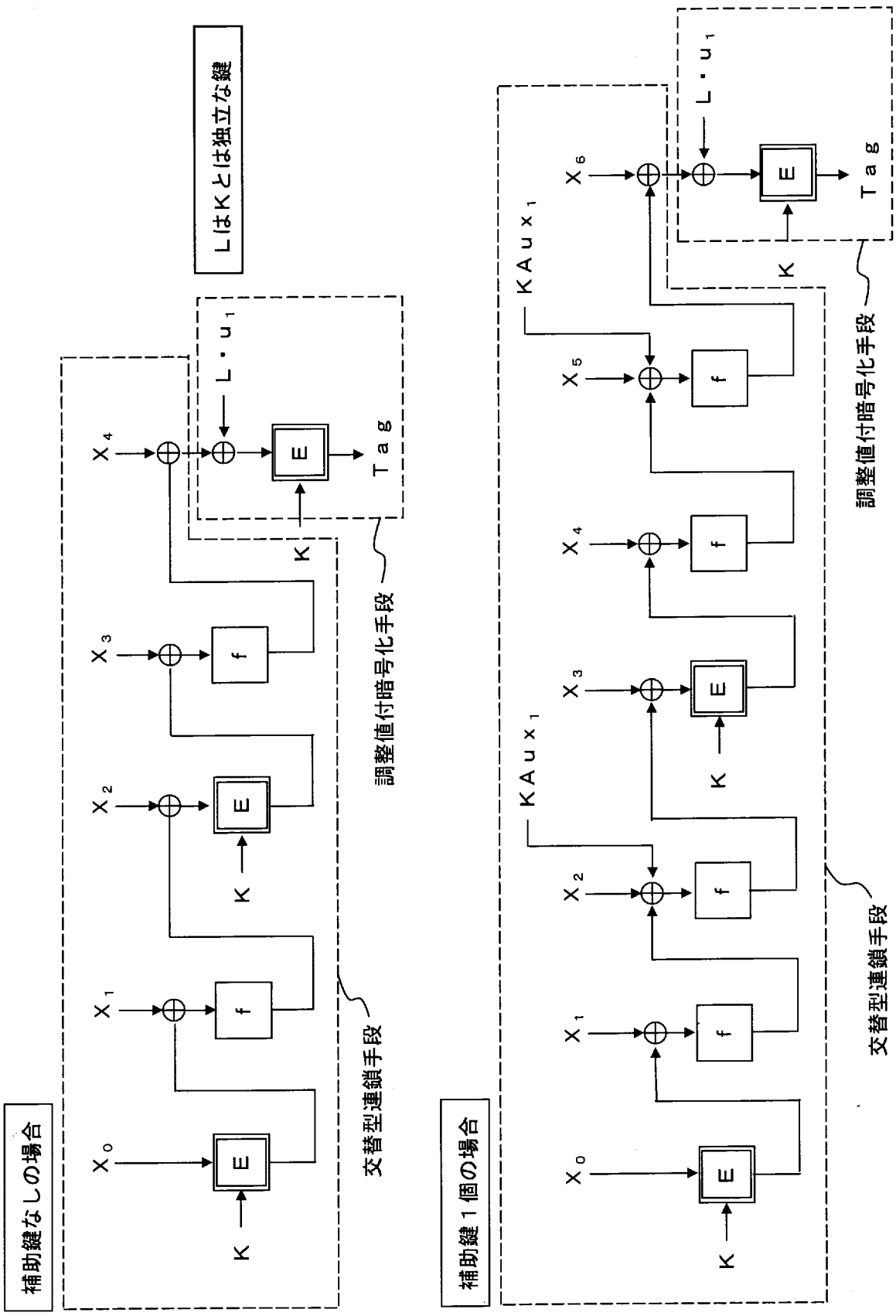
[図5]


START
S101
初期化するか？
NO
YES
S102
ハッシュ鍵と調整値の生成
S103
メッセージの入力
S104
パディングの実行
S105
修正木ハッシュ値の生成
S106
タグの生成
S107
タグとメッセージの出力
END

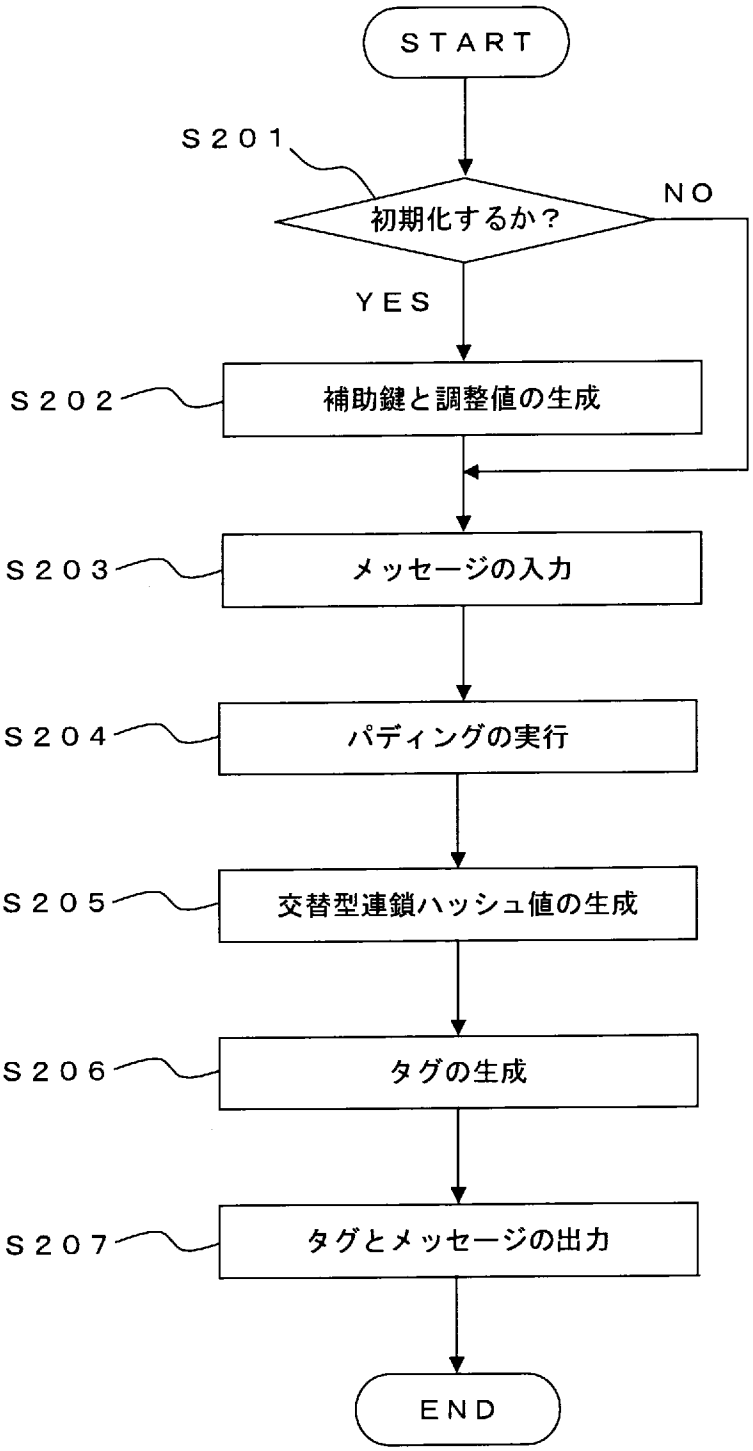
[図6]



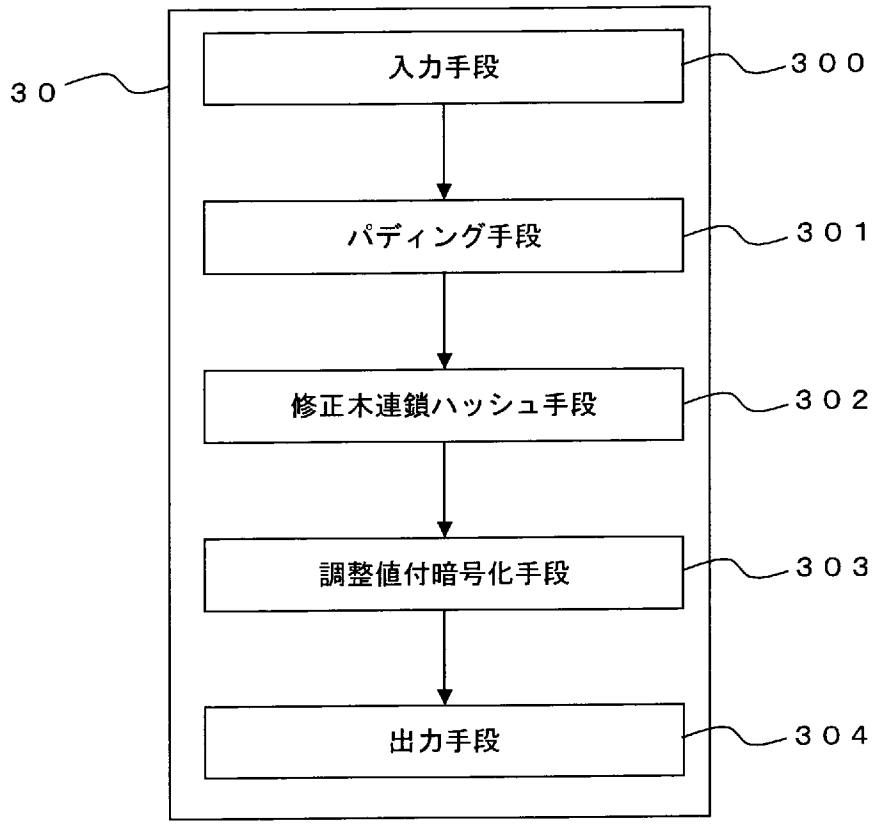
[図7]


補助鍵なしの場合
X0
X1
X2
X3
X4
E
f
K
L・u1
Tag
LはKとは独立な鍵
交替型連鎖手段
調整値付暗号化手段
補助鍵1個の場合
X5
X6
KAux1
交替型連鎖手段
調整値付暗号化手段

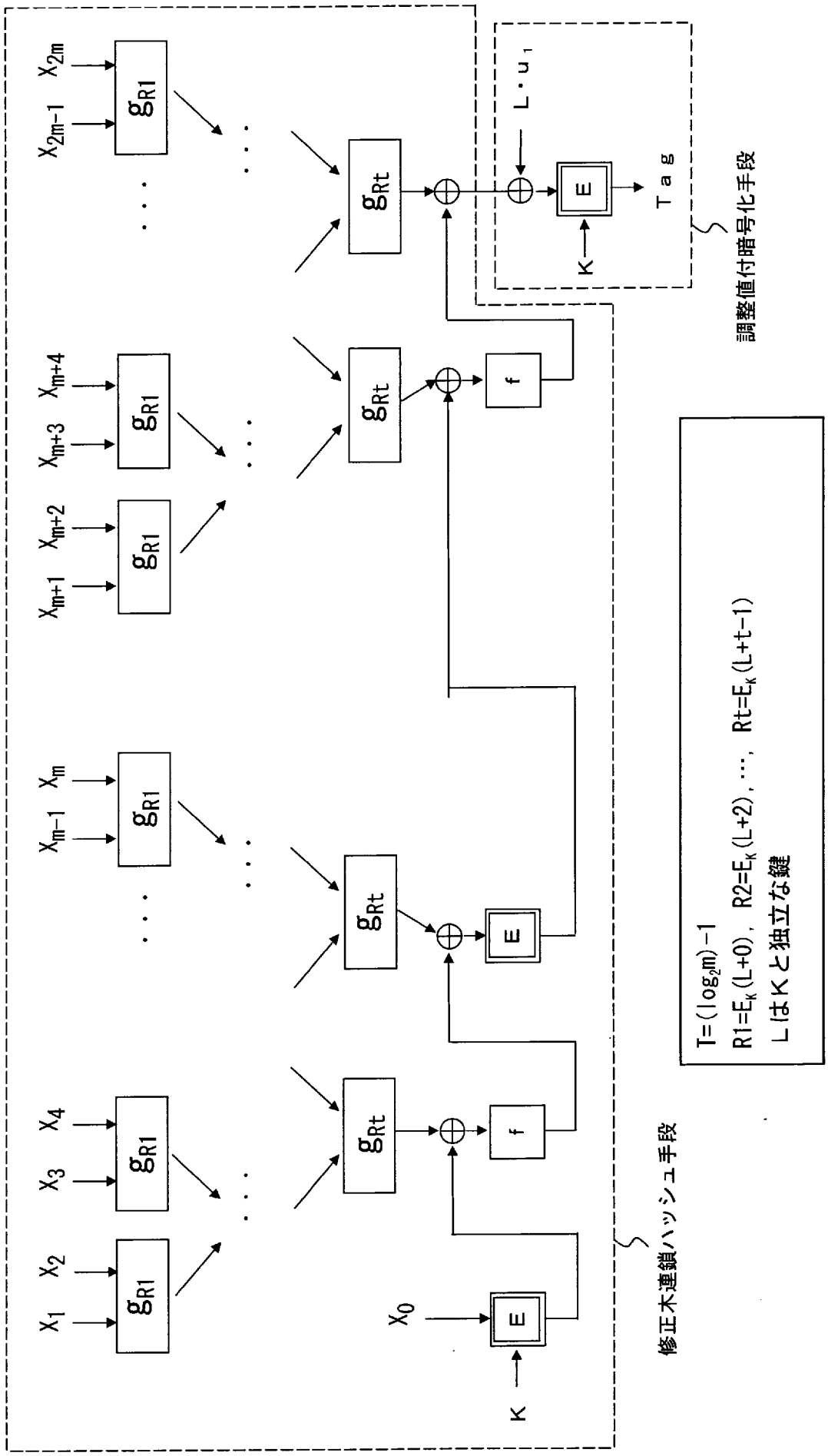
[図8]


START
S201
初期化するか？
NO
YES
S202
補助鍵と調整値の生成
S203
メッセージの入力
S204
パディングの実行
S205
交替型連鎖ハッシュ値の生成
S206
タグの生成
S207
タグとメッセージの出力
END

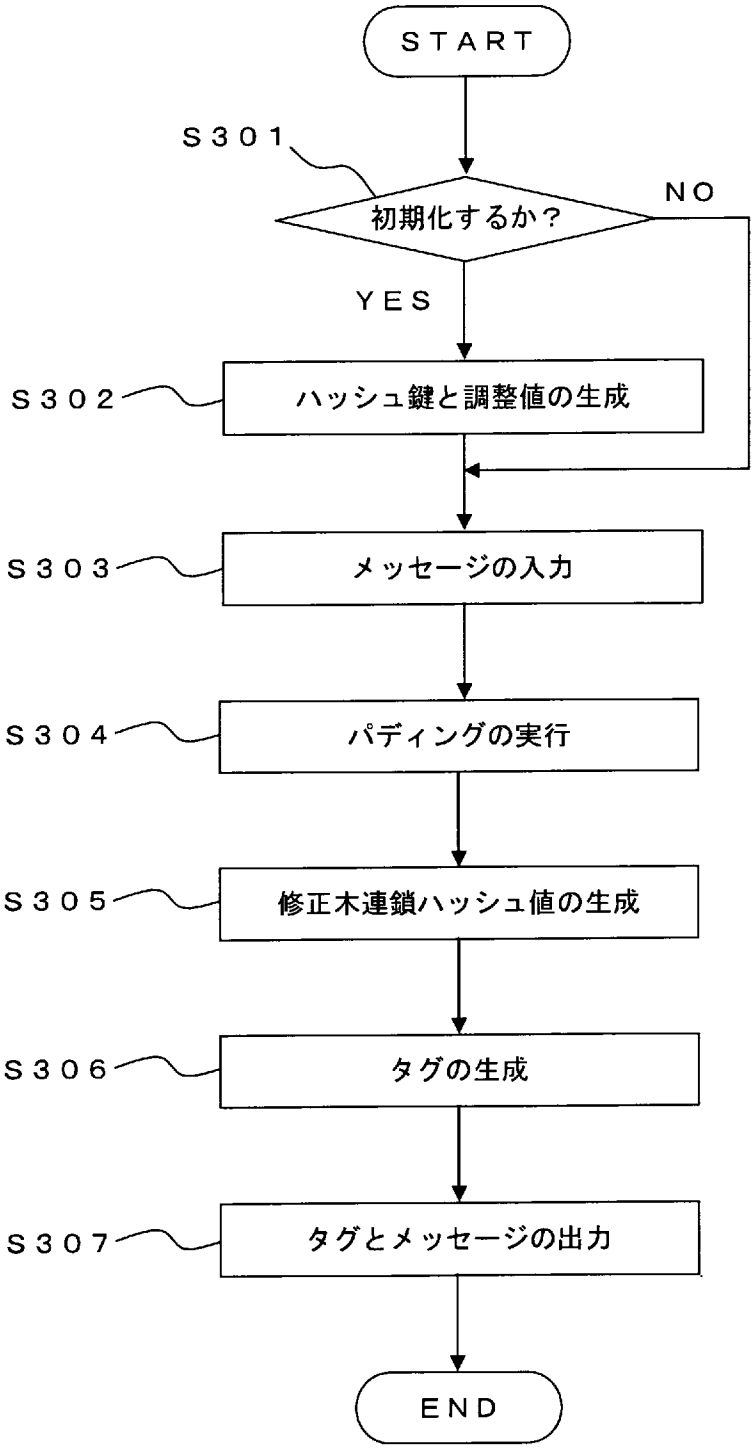
[図9]


３０
入力手段
３００
パディング手段
３０１
修正木連鎖ハッシュ手段
３０２
調整値付暗号化手段
３０３
出力手段
３０４

[図10]


修正木連鎖ハッシュ手段
調整値付暗号化手段
T=(log2m)−1
R1=EK(L+0), R2=EK(L+2), ···, Rt=EK(L+t−1)
Lはkと独立な鍵
gR1
gRt
E
f
K
Tag
L・u1
X0
X1
X2
X3
X4
Xm−1
Xm
Xm+1
Xm+2
Xm+3
Xm+4
X2m−1
X2m

[図11]


START
S301
初期化するか？
NO
YES
S302
ハッシュ鍵と調整値の生成
S303
メッセージの入力
S304
パディングの実行
S305
修正木連鎖ハッシュ値の生成
S306
タグの生成
S307
タグとメッセージの出力
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/320826

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01)i, *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)
H04L9/32, 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 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

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.
Y	JP 63-50223 A (Matsushita Electric Industrial Co., Ltd.), 03 March, 1988 (03.03.88), Figs. 1, 2 (Family: none)	1,4,7,8,11, 14-16
Y	JP 2003-51821 A (Lucent Technologies Inc.), 21 February, 2003 (21.02.03), Figs. 6, 11, 12 & US 2003-41242 A1	1,4,7,8,11, 14-16
A	JP 2004-363739 A (Hitachi, Ltd.), 24 December, 2004 (24.12.04), Full text & US 2004-252836 A1	1-16

☒ 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
05 January, 2007 (05.01.07)	16 January, 2007 (16.01.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/320826

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 2001-519930 A (Sun Microsystems, Inc.), 23 October, 2001 (23.10.01), Full text & EP 972374 A	1-16
A	JP 3-266544 A (NEC Corp.), 27 November, 1991 (27.11.91), Full text (Family: none)	1-16

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３２０８２６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/32(2006.01)i, 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.　H04L9/32, 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	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７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	関連する請求の範囲の番号
Ｙ	ＪＰ　６３－５０２２３　Ａ（松下電器産業株式会社） １９８８．０３．０３，第１，２図　（ファミリーなし）	１，４，７，８，１１，１４－１６
Ｙ	ＪＰ　２００３－５１８２１　Ａ （ルーセント　テクノロジーズ　インコーポレイテッド） ２００３．０２．２１，第６，１１，１２図 ＆ ＵＳ　２００３－４１２４２　Ａ１	１，４，７，８，１１，１４－１６

☑　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 ０５．０１．２００７	国際調査報告の発送日 １６．０１．２００７
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　９４６９ 石田　信行 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	関連する請求の範囲の番号
Ａ	ＪＰ ２００４－３６３７３９ Ａ（株式会社日立製作所） ２００４．１２．２４，全文 ＆ ＵＳ ２００４－２５２８３６ Ａ１	１－１６
Ａ	ＪＰ ２００１－５１９９３０ Ａ （サンマイクロシステムズ　インコーポレーテッド） ２００１．１０．２３，全文 ＆ ＥＰ ９７２３７４ Ａ	１－１６
Ａ	ＪＰ ３－２６６５４４ Ａ（日本電気株式会社） １９９１．１１．２７，全文 （ファミリーなし）	１－１６