(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
2006 年2 月23 日 (23.02.2006)

PCT

(10) 国際公開番号
WO 2006/019152 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *H04L 9/26* (2006.01)

(21) 国際出願番号: PCT/JP2005/015124

(22) 国際出願日: 2005 年8 月19 日 (19.08.2005)

(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2004-239359 2004 年8 月19 日 (19.08.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社日立製作所 (HITACHI, LTD.) [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目６番６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): 渡辺 大 (WATANABE, Dai) [JP/JP]; 〒2150013 神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 古屋 聡一 (FURUYA, Soichi) [JP/JP]; 〒2150013 神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 吉田 博隆 (YOSHIDA, Hirotaka) [JP/JP]; 〒2150013 神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 宝木 和夫 (TAKARAGI, Kazuo) [JP/JP]; 〒2150013 神奈川県川崎市麻生区王禅寺１０９９番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP).

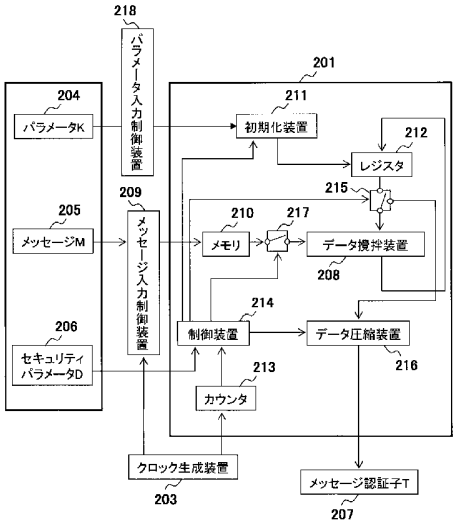
(74) 代理人: 特許業務法人 湘洋内外特許事務所 (THE PATENT CORPORATE BODY SHOWYOU INTERNATIONAL); 〒2200004 神奈川県横浜市西区北幸二丁目９－１０ 横浜ＨＳビル７階 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, 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, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,

[続葉有]

(54) **Title:** MESSAGE AUTHENTICATION CODE GENERATION DEVICE, MESSAGE AUTHENTICATION CODE VERIFICATION DEVICE, AND MESSAGE AUTHENTICATION CODE GENERATION METHOD

(54) 発明の名称: メッセージ認証装置及び認証暗号装置



204 PARAMETER K
205 MESSAGE M
206 SECURITY PARAMETER D
218 PARAMETER INPUT CONTROL DEVICE
209 MESSAGE INPUT CONTROL DEVICE
211 INITIALIZATION DEVICE
212 REGISTER
210 MEMORY
208 DATA MIXING DEVICE
214 CONTROL DEVICE
216 DATA COMPRESSION DEVICE
213 COUNTER
203 CLOCK GENERATION DEVICE
207 MESSAGE AUTHENTICATION CODE T

(57) Abstract: There is provided a high-speed and highly-safe MAC generation and authentication encryption technique which overcomes the conventional weak point that an output difference can be completely controlled by a message difference and which can be operated at an arbitrary platform. By employing a mixing device having non-linear conversion unit in which the size of the input message is 1/2 of the output length or below, it becomes unable to control the output difference value. The MAC generation device enables the mixing device to be employed not only for message mixing but also for initialization and data compression.

(57) 要約: 従来技術の弱点である、出力差分をメッセージ差分で完全にコントロールできる性質を克服し、任意のプラットフォームで動作可能な、高速で安全性の高いＭＡＣ生成および認証暗号技術を提供する。 入力するメッセージのサイズが出力長の１／２以下となる非線形変換部を備える攪拌装置を採用することにより、出力差分値のコントロール不可能にする。本発明のＭＡＣ生成装置は、上記攪拌装置をメッセージの攪拌処理だけでなく、初期化処理、データ圧縮処理にも採用可能である。

WO 2006/019152 A1

MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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
— 請求の範囲の補正の期限前の公開であり、補正書受領 の際には再公開される.

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。

明 細 書

メッセージ認証装置及び認証暗号装置

参照による取り込み

[0001] 本発明は2004年8月19日に出願された日本特願2004－239359の優先権を主張し、文献の参照による織りみ込みが認められる指定国については、上記出願の開示内容および特開2003－37482号公報の開示内容は参照により本出願に織り込まれる。

技術分野

[0002] 本発明は、任意長のメッセージ認証子を高速に生成する技術に関する。

背景技術

[0003] 現在、インターネットを代表とする公開通信路を用いた通信は増加の一途をたどっている。このような通信路では、通信路上で、送信されたメッセージが悪意ある第三者によって改ざんされる可能性があり、受信したメッセージの真贋を確認する方法が必要となる。

[0004] メッセージの真贋を確認する方法として、共通鍵暗号技術を用いたメッセージ認証子(Message Authentication Code: 以下MACと呼ぶ。)を用いるものと、公開鍵暗号技術による電子署名を用いるものとがある。電子署名を用いる方法は、MACを用いるものに比べて処理に時間を要する。従って、小さなパケットを大量に送受信するIP通信などでは、一般的に電子署名による方法よりもMACによる方法が用いられている。

[0005] MACを用いる方法は、送信データに所定の処理を施して生成されるMACを比較することにより、メッセージの改ざんの有無を確認するものである。

[0006] 一般に、MACによる受信メッセージへの改ざんの有無の検証は、以下のように行われる。

[0007] メッセージ送信側とメッセージ受信側とが、同じMAC生成機能を有する。送信側では、送信するメッセージからMAC(第1のMAC)を生成し、メッセージと共に送信す

る。受信側では、受信したメッセージから同様にMAC(第2のMAC)を生成し、上記メッセージと共に受信した第1のMACと第2のMACとを比較する。両者が合致すれば、メッセージの改ざんはないものと検証される。

[0008] このMACを生成する方法としては、ブロック暗号を用いたOMAC、ハッシュ関数を用いたHMAC、擬似乱数生成器を転用したHelix、SOBER－128(非特許文献1参照。)などが知られている。また、MACを生成する専用アルゴリズムとして、UMACなどが知られている。また、前記SOBER－128やHelixはMACの生成とデータの暗号化を同時に行うことができる方式である。MACの生成とデータの暗号化を同時に行う暗号化方式を認証暗号と呼ぶ。

[0009] 非特許文献1:P. Hawkes and G. Rose, Primitive Specification for SOBER-128,'' IACR ePrint Archive, http://eprint.iacr.org/2003/81/, 2003.

発明の開示

発明が解決しようとする課題

[0010] 上記の各方法は、それぞれ問題がある。例えば、ブロック暗号、ハッシュ関数を用いてMACを生成する方法は、処理速度に問題がある。

[0011] 擬似乱数生成器を用いたSOBER－128は、安全性に懸念があることが報告されている。具体的には、SOBER－128では、内部に、非線形変換部を有し、その非線形変換部からの出力長と、非線形変換部に対して入力されるメッセージの長さとが同じである。これは、出力差分をメッセージ差分で完全にコントロールできることを意味する。

[0012] また、Helixや専用アルゴリズムであるUMACは、特定のプラットフォームでは高速だが、ハードウェア実装には向かないなど、汎用性に欠ける。さらに、Helixは、出力長が160ビットであり、将来的に高い安全性を保証できるMAC生成アルゴリズムとは言い難い。

課題を解決するための手段

[0013] 本発明は、このような事情に鑑みてなされたもので、小さなデータを大量に送受信するIP通信などを行う任意のプラットフォームに適用可能な、実用に耐え得る性能と安全性とを備えた、MAC生成の技術を提供する。また、このMAC生成装置を備え、

MAC生成とデータの暗号化を同時に行う技術を提供する。

[0014] 本発明は、このMAC生成機能であって、SOBER－128の弱点を克服するものを提供する。

[0015] 本発明では、上記弱点を克服するために、以下の構成をとる。

(1)非線形変換部に入力されるメッセージのサイズを出力長の1／2以下とする。

(2)非線形変換部からの出力をバッファにフィードバックする。

[0016] 具体的には、送受信するメッセージデータの完全性を検証するためのメッセージ認証子を当該メッセージデータから生成するメッセージ認証子生成装置であって、第1のパラメータに初期化処理を施し、一定長のランダムなビット列からなるデータを出力する初期化装置と、前記初期化装置の出力したデータを格納するレジスタと、入力される前記メッセージデータを一定長に分割した後、一定長のメッセージデータ毎に、当該一定長のメッセージデータと前記レジスタに格納されているデータとを攪拌し、攪拌後のデータを前記レジスタに格納するデータ攪拌装置と、前記レジスタに格納されているデータであって、前記データ攪拌装置において攪拌後のデータを、所定のデータ長に圧縮し、メッセージ認証子として出力する圧縮処理を行うデータ圧縮装置と、を備え、前記データ攪拌装置は、前記一定長のメッセージデータの2倍以上のサイズの出力を有する非線形変換装置を備えることを特徴とするメッセージ認証子生成装置を提供する。

[0017] また、このメッセージ認証子生成装置を備え、メッセージ認証子生成とデータの暗号化とを同時に行う技術を提供するものである。

[0018] 上記態様の、非線形変換部に入力されるメッセージのサイズを出力長の1／2以下とする構成により、出力差分値のコントロールを困難にする。また、本発明の非線形変換部からの出力をバッファにフィードバックする構成により、バッファの状態更新を非線形にすることができ、結果として、暗号学的な強度が増すことが期待できる。

[0019] また、上記態様によれば、バッファ部と非線形変換部のデータの相関が小さくなることが期待できる。このため、任意のプラットフォームで高速に動作するMAC生成装置、およびMAC検証装置を提供することができる。

[0020] 本発明は、特に、特開2003－37482号公報に開示する擬似乱数生成器(以下、

MUGIと称す)に、低コストで適用することが可能である。すなわち、本発明は、MUGIに、MACを生成する機能を安価に提供することができる。また、本発明は、MUGIに認証暗号の機能を提供することができる。

発明の効果

[0021] 本発明によれば、任意のプラットフォームに適用可能な、実用に耐え得る性能と安全性とを備えたMAC生成および認証暗号の技術を提供できる。

図面の簡単な説明

[0022] [図1]本実施形態のMAC生成装置の概略構成を例示する図である。

[図2]本実施形態のMAC生成装置の動作を例示するフローチャートである。

[図3]本実施形態の攪拌装置の概略構成を例示する図である。

[図4]本実施形態の攪拌装置の動作を例示するフローチャートである。

[図5]本実施形態の非線形変換装置の構成を例示する図である。

[図6]本実施形態の非線形置換の構成を例示する図である。

[図7]本実施形態の線形変換装置の構成を例示する図である。

[図8]本実施形態のデータ攪拌装置の構成を例示する図である。

[図9]本実施形態の初期化装置の構成を例示する図である。

[図10]本実施形態の初期化装置の処理を例示するフローチャートである。

[図11]本実施形態のデータ圧縮装置の構成を例示する図である。

[図12]本実施形態のデータ圧縮装置の処理を例示するフローチャートである。

[図13]本実施形態のMAC検証装置の概略構成を例示する図である。

[図14]本実施形態のMAC検証装置の動作を例示するフローチャートである。

[図15]本実施形態のメッセージ認証方式を用いた通信システムの構成を例示する図である。

[図16]本実施形態の認証暗号装置の概略構成を例示する図である。

[図17]本実施形態の認証暗号装置の動作を例示するフローチャートである。

[図18]本実施形態の認証復号装置の概略構成を例示する図である。

[図19]本実施形態の認証復号装置の動作を例示するフローチャートである。

[図20]本実施形態の認証暗号技術を用いた通信システムの構成を例示する図であ

る。

[図21]本実施形態の非線形変換装置の他の構成を例示する図である。

発明を実施するための最良の形態

[0023] 以下に、本発明を適用する実施形態を説明する。

[0024] ここでは、本発明を認証暗号装置に適用した場合を実施形態として説明する。本実施形態の認証暗号装置は、レジスタを持つメッセージ認証子生成装置を利用する。そこでまず、本実施形態の認証暗号装置に最適なメッセージ認証子生成装置を説明する。

[0025] 図1は、本実施形態の認証暗号装置に最適なメッセージ認証子(MAC)生成装置のイメージ図である。本図に示すように、本実施形態のMAC生成装置201は、メッセージ入力制御装置209を介して入力されたメッセージM205に、クロック生成装置203から入力されるクロック信号に従って処理を施し、メッセージ認証子T207を生成する。

[0026] 本実施形態のMAC生成装置201への外部からの入力は、メッセージ入力制御装置209を介して入力されるメッセージM205の他に、パラメータ入力制御装置218を介して入力されるパラメータK204と、セキュリティパラメータD206と、クロック生成装置203の生成するクロック信号とがある。

[0027] メッセージ入力制御装置209は、任意のサイズのメッセージM205を、MAC生成装置201の内部での処理単位に分割して、MAC生成装置201に入力する。

[0028] パラメータ入力制御装置218は、任意のサイズのパラメータK204を、MAC生成装置210の内部での処理単位に分割して、MAC生成装置201に入力する。

[0029] クロック生成装置203は、クロック信号を生成し、MAC生成装置201およびメッセージ入力制御装置209に入力する。

[0030] MAC生成装置201は、初期化装置211、レジスタ212、メモリ210、スイッチ215、217、データ攪拌装置208、制御装置214、データ圧縮装置216、カウンタ213とを備える。

[0031] 初期化装置211は、パラメータ入力制御装置218を介して入力されたパラメータK204をレジスタ212長毎に切り出して、レジスタ212に出力する。

[0032] レジスタ212は、パラメータK204またはデータ攪拌装置208からの出力を一時的に保持する。

[0033] メモリ210は、メッセージ入力制御装置209を介して入力されたメッセージM205を一時的に保持する。

[0034] スイッチ215は、制御装置214の指示に従って、レジスタ212に保持されているデータを、データ攪拌装置208およびデータ圧縮装置216のいずれかに入力するよう切り替える。

[0035] スイッチ217は、制御装置214の指示に従って、メモリ210に保持されているデータを、データ攪拌装置208に入力するか否かを切り替える。

[0036] 制御装置214は、セキュリティパラメータD206、カウンタ213に従って、スイッチ215およびスイッチ217を制御する。

[0037] カウンタ213は、クロック生成装置203からの入力回数をカウントするもので、クロック生成装置203からクロック信号が入力される毎に、保持する値が1ずつ増加するよう更新される。

[0038] データ攪拌装置208は、データ攪拌装置208に入力されたデータを攪拌して出力する。

[0039] データ圧縮装置216は、データ圧縮装置216に入力されたデータに所定の処理を施し、メッセージ認証子T207を生成し、出力する。

[0040] 初期化装置211、データ攪拌装置208、データ圧縮装置216の詳細については、後述する。

[0041] また、入力されるパラメータK204は、基本的には、秘密鍵といった秘密情報である。しかし、その一部をカウンタのような公開値としてもよい。

[0042] セキュリティパラメータD206は、MAC生成装置201の暗号方式の安全性を表す指標であり、鍵長などをセキュリティパラメータD206としてもよい。セキュリティパラメータD206は、初期化装置211、データ圧縮装置216等のMAC生成装置201内の各機能において行われる、後述する攪拌回数を決定する基礎となるパラメータである。セキュリティパラメータD206に基づいて、所定の算出方法に従って決定された各機能での攪拌回数に従って、制御装置214は、各機能での攪拌回数を制御する。

[0043] 本実施形態では、データ攪拌装置208および初期化装置211は、予め定められたデータ長(以後、Lとする)のデータを受け入れ、処理を行う。上記のメッセージ入力制御装置209およびパラメータ入力制御装置218は、任意サイズのメッセージM205およびパラメータK204を、本実施形態のデータ攪拌装置208および初期化装置211でそれぞれ処理するために設けられている。

[0044] メッセージ入力制御装置209を代表として説明すると、メッセージ入力制御装置209は、クロック生成装置203からクロックを受信する毎に、メッセージM205からLビット切り出し、メモリ210に格納する。メッセージM205がLの整数倍でない場合は、予めビット列100…0などを用いてデータパディングを行い、Lの整数倍となるようにする。本実施形態では、メッセージM205は、メッセージ入力制御装置209において、各メッセージブロックM1、M2、…MNに分割される(各メッセージブロックM1、M2…MNのサイズはLである。また、Nは、パディング後のメッセージM205をLで割った場合の商である。)。パラメータ入力制御装置218の動作も基本的に同様であり、パラメータK204は、K1、K2、…Kn…KPに分割される(分割後のパラメータのKnのサイズはLである。また、Pは、パディング後のパラメータK204をLで割った場合の商である。ここで、nは自然数であり、ここでは、P以下の自然数である。)。

[0045] 次に、MAC生成装置201の動作の概要を説明する。図2は、MAC生成装置201の動作概要を説明するためのフローチャートである。

[0046] ステップ301:MAC生成装置201には、パラメータK204とメッセージM205とが入力される。パラメータK204は、パラメータ入力制御装置218を介して初期化装置211に、メッセージM205は、メッセージ入力制御装置209を介してメモリ210に入力される。

[0047] メッセージ入力制御装置209は、メッセージM205を、一定長Lのブロックに分割し、クロック生成装置203からクロック信号が入力されるごとにメモリ210にむけて出力する。パラメータ入力制御装置218も、同様に、パラメータK204を、一定長Lのブロックの分割し、クロック生成装置203からクロック信号が入力されるごとに、初期化装置211にむけて出力する。

[0048] MAC生成装置201は、これらの入力を受けると、クロック生成装置203から入力さ

れるクロック信号に従って、以下の処理を行う。

[0049] ステップ302:メッセージM205を、メッセージブロックMnに分割する。

[0050] ステップ303:パラメータ入力制御装置218を介して入力されたパラメータK204(Kn)を初期化装置211に入力する。初期化装置211に、入力されたパラメータK204(Kn)に後述する初期化処理を施させ、レジスタ212長のデータを出力させる。初期化装置211から出力されたデータは、レジスタ212に格納される。

[0051] ステップ304:カウンタ213の値を初期化する。本実施形態では、全てのビット値を0にセットする。

[0052] ステップ305、306:クロック信号が入力される毎に、メッセージ入力制御装置209を介することにより、メッセージブロックMn(nは、N以下の自然数であり、カウンタ213が現在保持している値となる。)として分割されたメッセージM205が、メモリ210に格納される。データ攪拌装置208に、メモリ210に格納されているメッセージブロックMnとレジスタ212に格納されているデータとを攪拌させ、レジスタ212長のデータを出力させる。出力されたデータは、レジスタ212に格納される。そして、カウンタ213の値を1増加させる。

[0053] ステップ305、306の処理を、全てのメッセージブロックMnを処理し終えるまで、すなわち、nが1からNになるまで繰り返す。

[0054] ステップ307:カウンタ213の値がNになると、制御装置214に、レジスタ212に保持されるデータがデータ圧縮装置216に入力されるようにスイッチ215を切り替えさせる。そして、その時点でレジスタ212に保持されるデータが、データ圧縮装置216に入力される。

[0055] ステップ308:データ圧縮装置216に、入力されたデータの圧縮を行わせ、セキュリティパラメータD205に応じて、レジスタ212のビット長よりも短いデータを生成させる。そして、生成されたデータをメッセージ認証子T207として出力する。

[0056] 次に、初期化装置211、データ攪拌装置208、データ圧縮装置216について説明する。

[0057] 初期化装置211、データ攪拌装置208、データ圧縮装置216は、それぞれ独立な関数を用いて構成してもよいが、同じ攪拌関数によっても構成が可能である。実装コ

ストを勘案すれば、同じ攪拌関数を用いる方がよい。以下、一つの攪拌関数を定義し、上記3装置を、この攪拌関数により実現する場合を例にあげ、説明する。

[0058] 図3は、上記3装置に適用可能な攪拌関数の処理を実現する攪拌装置601の概略を説明するための図である。また、図4は、攪拌装置601の動作概要を説明するための図である。

[0059] 図3に示すように、攪拌装置601への入力は、レジスタ602に格納されているデータと、外部入力603に格納されているデータとである。外部入力603のデータは、スイッチ609により、入力の有無を制御される。すなわち、攪拌装置601は、外部入力603のデータ入力ありで、レジスタ602内のデータを攪拌する処理と、外部入力603のデータ入力なしで、レジスタ602内のデータを攪拌する処理とを行うことができる。

[0060] 以下、説明のため、レジスタ602を、2つのレジスタに分割し、それぞれレジスタA604、レジスタB605とする。

[0061] 図3に示すように、本実施形態の攪拌装置601は、非線形変換装置606と、線形変換装置607、および入力フィルタ611とを備える。本実施形態では、線形変換装置607を実現する関数は、非退化なものを用いる。また、線形変換装置606を実現する関数は、レジスタA604からの入力に関して、可逆なものを用いる。それぞれ詳細は、後述する。

[0062] 図3に示すように、攪拌装置601は、スイッチ609と制御装置608とスイッチ610とによって切り替えられるレジスタ602からの入力と外部入力603からの入力とを受けると、以下の処理を行う。

[0063] なお、スイッチ609は、制御装置608からの切り替え指示に従って、入力の切り替えを行う。

[0064] ステップ702:外部入力603に格納されているデータの有無および制御装置608からの信号を確認する。

[0065] ステップ703、704、705:外部入力603にデータが保持されていない場合、すなわち、外部入力603からデータが入力されない場合、もしくは、制御装置608から、外部入力603からのデータを無視する信号を受信した場合には、スイッチ609を、外部入力603が入力フィルタ611に入力しないように切り替える。一方、外部入力603

にデータが保持され、かつ、制御装置608から無視を指示する信号が出力されていない場合には、スイッチ609を、外部入力603が保持しているデータが、入力フィルタ611に入力されるように切り替える。

[0066] ステップ706:スイッチからの入力およびメモリのデータを入力フィルタ610に入力する。入力フィルタ611は入力に応じて、一定長のデータを出力する。

[0067] ここで、入力フィルタ611は、スイッチからの入力とメモリのデータとの排他的論理和をとる処理を行う。また、さらに排他的論理和の結果を後述する非線形置換A801により置換してもよい。

[0068] ステップ707:レジスタA604とレジスタB605とに格納されているデータ、および、スイッチ609を介して受け取る外部入力603が保持しているデータまたはレジスタB605に格納されているデータを、非線形変換装置606に入力し、データを攪拌する。

[0069] ステップ708:非線形装置606の出力およびレジスタB605が保持しているデータを、線形変換装置607に入力する。

[0070] ステップ709:線形変換装置607からの出力を、レジスタA604、レジスタB605に格納する。

[0071] ここで、非線形変換装置606、線形変換装置607の詳細について、説明する。以下において、前記のデータ長Lを64ビットとする。すなわち、外部入力603のサイズを64ビットとする。

[0072] また、レジスタA604、レジスタB605は、それぞれ、3個、16個の64ビット小レジスタから構成されるものとして説明する。また、それぞれの小レジスタを、A0、A1、A2、B0、B1、…B15と表す。

[0073] 図3におけるレジスタA604、レジスタB605からの非線形変換装置606、線形変換装置607への細線は、それぞれ1本の線が64ビットデータの流れを表す。また、各レジスタとも、上位(左)側から、A0、A1、A2、B0、B1、…B15とする。

[0074] また、以下の処理では、各小レジスタが保持するデータは、時刻とともに更新されて行く。時刻tに状態更新がなされた時点でのレジスタA0を、A0(t)と記述する。これは、状態更新を記述する際に、時刻tを明記する必要がある場合のみ採用する。さらに、B1(t+1)←A0(t)+A1(t)との記述は、矢印の右辺のレジスタA0(t)とレジスタA1(t)

とに格納されているデータを結合し、矢印の左辺のレジスタB1(t+1)に代入することを示す。

[0075] 図5は、本実施形態の非線形変換装置606の構成を説明するための図である。本図において、丸に十字の記号は、排他的論理和を表す。また、式中では、排他的論理和は、“XOR”で表す。

[0076] 非線形装置606は、非線形置換A801と非線形置換B802と巡回シフト装置803とを備える。非線形置換A801および非線形置換B802の詳細については、後述する。

[0077] 非線形変換装置606には、レジスタA604に格納されているデータと、レジスタB605のB10に格納されているデータと、スイッチ609により選択される、外部入力603またはレジスタBのB4に格納されているデータと、の3つのデータが入力される。非線形変換装置606は、時刻tにおける、上記3つの入力に処理を施し、その結果を、時刻t+1において、レジスタA604に格納することにより、レジスタA604の状態を更新する。

[0078] 非線形変換装置606によるレジスタA604の状態更新の詳細は、以下の式で与えられる。ここでは、非線形置換A801をF、非線形置換B802をG、スイッチ609からの入力データをP(t)とする。

[0079] A0(t+1)←A1(t)

A1(t+1)←A2(t) XOR G(A1(t) XOR P(t))

A2(t+1)←A0(t) XOR F(A1(t) XOR B10(t) <<< 17)

ここで、上記式中の記号“<<<”は、64ビットレジスタにおけるnビット左巡回シフトを表す。以下、本明細書中、同様である。

[0080] レジスタA604の状態更新の別例を説明する。図21は、本別例の非線形変換装置606の構成を説明するための図である。本図における丸に十字の記号、”XOR”は、図5と同様の意味である。本別例の非線形変換装置606によるレジスタA604の状態更新の詳細は以下の式で与えられる。

[0081] A0(t+1)←A1(t)

A1(t+1)←A2(t) XOR G(A1(t) XOR B4(t))

A2(t+1)←A0(t) XOR F(A1(t) XOR P(t) <<< 17)

以上説明したように、本実施形態および本別例では、非線形変換装置606は、64ビット入力データP(t)から、192(64×3)ビットの出力を得ている。すなわち、入力メッセージのサイズを出力長の1/2以下としている。

[0082] 次に、上記の非線形置換A801、B802について説明する。

[0083] 図6は、非線形置換A801の構成を説明するための図である。非線形置換A801は、入力904に処理を施し、その結果を出力905として出力する。

[0084] 本図において、Si(0＜＝i＜8;iは自然数)(902)は、入力、出力ともに8ビットの変換テーブルであり、非線形変換を行う。また、Li(0＜＝i＜＝1;iは自然数)(903)は、入力、出力ともに32ビットの線形変換を表す。Si、Liとしては、例えば、FIPS197に記述されている8ビットの置換テーブルS－box S、MixColumn()などを用いることができる。

[0085] 本実施形態において、非線形置換A801の処理は、次の式で与えられる。

[0086] x0||x1||...||x7←入力(904)、

yi←Si(xi)、(0<=i<8)、

(z0, z1, z2, z3)←L0(y0, y1, y2, y3),

(z4, z5, z6, z7)←L1(y4, y5, y6, y7),

出力(905)←z4||z5||z2||z3||z0||z1||z6||z7.

ただし、上記式中で、記号"||"はデータの連結を表す。以下、本明細書中、同様である。

[0087] すなわち、64ビットの入力904を、上位ビットから8ビットずつ、それぞれ、S0、S1、…S7に入力し、処理を施し、その結果、S0からS3はL0に、S4からS7はL1に入力される。L0、L1での処理後、L0の上位16ビットとL1の上位16ビットとを入れ替え、出力905とする。

[0088] 非線形置換B802も基本的に上記非線形置換A801と同様の構成で実現することができる。このように、同様の置換処理を用いることにより、実装規模を小さく抑えることができる。ただし、実装に対する制限が少ない場合には、異なる8ビット変換テーブルSi(0＜＝i＜8;iは自然数)(902)や、異なる線形変換Li(0＜＝i＜＝1;iは自然

数)(903)を用いることで、より高い安全性を実現できる。

[0089] 次に、線形変換装置607について説明する。

[0090] 図7は、本実施形態の線形変換装置607の構成を説明するための図である。本図において、1本の線は、64ビットデータの流れを表す。

[0091] 線形変換装置607には、レジスタB605に格納されているデータと、レジスタA604のA0に格納されているデータとの2つの値が入力される。線形変換装置607は、時刻tにおける、上記2つの入力に処理を施し、その結果を、時刻t+1において、レジスタB605に格納することにより、レジスタB605の状態を更新する。

[0092] 線形変換装置607によるレジスタB605の状態更新の詳細は、以下の式で与えられる。

[0093] Bi(t+1)←B(i−1)(t)、(iは、0<i≦15を満たす自然数、ただし、4、10を除く)、

B0(t+1)←B15(t) XOR A0(t)

B4(t+1)←B3(t) XOR B7(t)

B10(t+1)←B9(t) XOR (B13(t) <<< 32)

なお、本線形変換装置607では、レジスタA604に保持されているデータは更新しない。

[0094] 次に、以上説明した攪拌装置601を、本実施形態のMAC生成装置内の、初期化、データ攪拌、データ圧縮の各処理に適用する場合を説明する。

[0095] 図8は、データ攪拌装置208として、攪拌装置601を利用する場合の構成を説明するための図である。

[0096] 本図に示すように、攪拌装置601がデータ攪拌装置208に、レジスタ602がレジスタ212に、外部入力603がメモリ210に、スイッチ610がスイッチ215に、スイッチ609がスイッチ217に対応する。

[0097] 上述のように、本実施形態では、メモリ210にメッセージブロックMn単位で入力されるデータを、クロック生成装置203からのクロック信号に従って動作する制御装置214の指示で、データ攪拌装置208に入力し、攪拌を行う。メモリ210からの入力が完了したら、制御装置214がスイッチ215を操作し、レジスタ212に格納されているデータを、データ圧縮装置216に出力する。

[0098] なお、本実施形態のデータ攪拌装置208は、クロック毎に、メモリ210に格納されたデータの入力と攪拌とを1回行うよう構成されている。しかし、セキュリティパラメータD206に応じて、データ攪拌回数を決定し、全てのメッセージブロックMnの入力終了後、当該データ攪拌回数、スイッチ217の切り替えて外部入力603(メモリ210からの入力)無しに、データを攪拌するよう構成してもよい。

[0099] 次に、上述の攪拌装置601により、初期化装置211を実現する構成を説明する。図9に、初期化装置211を実現する構成を示す。

[0100] 本図に示すように、本実施形態の初期化装置211は、上述の攪拌装置601およびレジスタ602、スイッチ609、スイッチ610、入力フィルタ611により構成される。

[0101] 図3に示す制御装置608は図1に示す制御装置214に対応する。また、外部入力603は、パラメータK204をパラメータ入力制御装置218によりデータ長Lに分割した後のものである。初期化装置211における攪拌の回数は、セキュリティパラメータD206に基づいて定められる。

[0102] 図10は、攪拌装置601により初期化装置211を実現する場合の、MAC生成装置201の処理フローである。

[0103] ステップ1101:入力としてパラメータK204とセキュリティパラメータD206とが与えられる。

[0104] ステップ1102:初期化装置211において、パラメータK204を、攪拌装置601(ここでは、初期化装置211)の入力サイズにあわせて、P個のブロックに分割する。必要に応じてパディング処理を行う。各分割後のパラメータK204を、Knとする(K=K1、K2…Kn…KP;nはP以下の自然数。)。また、入力サイズは、外部入力603のサイズのL、すなわち、本実施形態では、64ビットである。

[0105] ステップ1103:レジスタ602をゼロクリアする。

[0106] ステップ1104:カウンタ213の値を1にセットする(n=1)。

[0107] ステップ1105、1106:nがPより大きくなる(n>P)まで、Knを外部入力603として、クロック信号が入力される毎に、攪拌装置601を動作させ、レジスタ602のデータを攪拌し、nを1増加させることを繰り返す。

[0108] ステップ1107:カウンタ213の値を再度1にセットする(n=1)。

[0109] ステップ1108、1109:nがL(D)より大きくなる(n>L(D))まで、外部入力603無しで、クロック信号が入力される毎に、攪拌装置601を動作させ、レジスタ602のデータを攪拌し、nを1増加させる処理を繰り返す。ここで、L(D)は、初期化処理の攪拌回数を示す値であって、セキュリティパラメータD206に従って定められる。

[0110] ステップ1110:攪拌終了後、この時点でのレジスタ602のデータを出力する。本実施形態では、レジスタ212に出力する。

[0111] 次に、上述の攪拌装置601により、データ圧縮装置216を実現する構成を説明する。図11にデータ圧縮装置216を実現する構成を示す。なお、データ圧縮装置216は、レジスタのデータ以外を入力として持たないため、図中では、入力フィルタ611を省略する。

[0112] 本図に示すように、本実施形態のデータ圧縮装置216は、攪拌装置601およびレジスタ602、スイッチ609、スイッチ610により構成される。

[0113] 図3に示す制御装置608は図1に示す制御装置214に対応する。また、データ圧縮装置216の場合、外部入力603に相当するものは無い。また、メッセージ認証子T207として最終結果を出力する前に、処理結果を一時的に保持するバッファT'216aと、制御装置214からの指示し従って、バッファT'216aのデータを出力するためのスイッチ216bとを備える。

[0114] データ圧縮装置216における攪拌の回数は、セキュリティパラメータD206に従って定められる。

[0115] 図12は、攪拌装置601により、データ圧縮装置216を実現する場合の、MAC生成装置201の処理フローである。

[0116] ステッ1201:入力としてレジスタ212のデータと、セキュリティパラメータD206とが与えられる。レジスタ212のデータは、レジスタ602に保持される。

[0117] ステップ1202:カウンタ213の値を1にセットする(n=1)。

[0118] ステップ1203、1204:nがL'(D)より大きく(n>L'(D)と)なるまで、クロック毎に、外部入力603無しで攪拌装置601を動作させ、レジスタ602のデータを攪拌し、nを1増加させる処理を繰り返す。ここで、L'(D)は、データ圧縮処理の第一の攪拌回数を示す値であって、セキュリティパラメータD206に従って定められる。

[0119] ステップ1205:nがL'(D)より大きくなった時点で、カウンタ213の値を1にセットする(n=1)。また、出力するデータを一時的に格納するバッファT'216aをクリアする。

[0120] ステップ1206、1207、1208:nがL''(D)より大きく(n>L''(D)と)なるまで、クロック信号が入力される毎に、外部入力603無しで、攪拌装置601を動作させ、nを1増加させる処理を繰り返す。ここで、L''(D)は、データ圧縮処理の第二の攪拌回数を示す値であって、セキュリティパラメータD206に従って定められる。そして、各クロック毎、すなわち、攪拌装置601を動作させて攪拌する毎に、以下の操作を行う。

[0121] T'←T'||A2(n)

ステップ1209:nがL''(D)より大きくなった場合、バッファT'216a内のデータをメッセージ認証子T207として出力する。

[0122] これにより、L''(D)の値により、すなわち、第二の攪拌回数により、出力されるメッセージ認証子Tのデータ長を調整できる。従って、本実施形態のMAC生成装置201では、任意長のメッセージ認証子を生成することができる。

[0123] 本実施形態では、上記のように、セキュリティパラメータD206に依存して、攪拌回数が決定されるよう構成されている。しかし、このセキュリティパラメータD206は、固定値であってもよい。

[0124] また、上述のように、本実施形態の攪拌装置601では、外部入力603は、非線形変換装置606への入力とされているが、線形変換装置607に入力されるよう構成してもよい。この場合、レジスタB603の状態更新は、以下の式で表される。

[0125] Bi(t+1)←B(i−1)(t)、(iは、0<i≦15を満たす自然数、ただし、4、10を除く)、

B0(t+1)←B15(t) XOR P(t)、

B4(t+1)←B3(t) XOR B7(t)、

B10(t+1)←B9(t) XOR (B13(t) <<< 32).

さらに、外部入力603は、非線形変換装置606および線形変換装置607の両方に入力するよう構成してもよい。この場合は、外部入力603を、線形変換装置607のB0(t)に足しこむように構成する。

[0126] 次に、本実施形態による、メッセージ認証子検証装置について説明する。メッセージ認証子検証装置は、メッセージ生成装置と同様の構成を有し、受信したメッセージ

とMACとの組から、メッセージとMACとをそれぞれ抽出する。そして、抽出したメッセージからMACを生成し、生成したMACと抽出したMACとを比較することにより検証を行う。

[0127] 従って、以下に説明するように、受信したメッセージ認証子の真正性を検証する本実施形態のメッセージ認証子検証装置は、上述のMAC生成装置201と基本的に同様の構造を有するMAC生成処理を行う機能と、受信したMACとメッセージ認証子検証装置で生成したMACとを比較する機能とを備える。

[0128] 図13は、本実施形態のメッセージ認証子(MAC)検証装置401の概要を説明するための図であり、図14は、図13のMAC検証装置による処理フローである。

[0129] 本実施形態のMAC検証装置401は、MAC生成装置201と、データ比較装置402とを備える。MAC検証装置401への入力は、MAC生成装置201への入力である、パラメータK204、メッセージM205、セキュリティパラメータD206と、クロック生成装置404からの入力信号と、データ比較装置402への入力であり、メッセージの真正性を検証するためのタグT405とである。タグT405は、受信したメッセージから抽出したMACである。また、メッセージM205およびパラメータK204は、MAC生成装置201の場合と同様、それぞれメッセージ入力制御装置209およびパラメータ入力制御装置218を介して、所定長Lのブロック単位に分割されて、入力される。

[0130] MAC検証装置401によるメッセージ認証子検証処理について以下に説明する。

[0131] ステップ502:MAC生成装置201に、パラメータK204、メッセージM205、セキュリティパラメータD206を入力し、MAC生成処理を行い、結果を出力する。

[0132] ステップ503:ステップ502の処理結果である出力とタグT405の値とを比較する。

[0133] ステップ504、505:ステップ503の比較において、両者の値が等しければ0を出力し、それ以外の場合は1を出力する。すなわち、メッセージが真正と検証された場合、0を出力し、それ以外の場合1を検証結果406として出力する。

[0134] ステップ506:処理を終了する。

[0135] 次に、本実施形態の認証暗号装置について説明する。

[0136] 図16は、本実施形態の認証暗号装置1601のイメージ図である。本図に示すように、本実施形態の認証暗号装置1601は、図1に示すレジスタ212を持つメッセージ認

証子(MAC)生成装置201、ビット列出力フィルタ1605、レジスタ212から出力フィルタ1605への入力を制御するスイッチ1606、暗号化装置1608、暗号化装置1608へのメッセージ入力を制御するスイッチ1607、暗号化装置1608の出力を蓄えるメモリ1612を備える。それぞれの構成要素の詳細な構成については後述する。

[0137] 次に、上記のメッセージ認証子生成装置201を備えた認証暗号装1601置の処理動作について説明する。

[0138] 本実施形態の認証暗号装置1601は、メッセージ入力制御装置209を介して入力されたメッセージM205に、クロック生成装置203から入力されるクロック信号に従って処理を施し、メッセージM205を暗号化し、暗号文C1609を出力する。また、認証暗号装置1601は、全てのメッセージM205に処理を施した後、メッセージ認証子T207を生成する。

[0139] 本実施形態で認証暗号装置1601への外部からの入力は、メッセージ入力制御装置209を介して入力されるメッセージM205の他に、パラメータ入力制御装置218を介して入力されるパラメータK204と、セキュリティパラメータD206と、暗号化処理をするか否かを決定する暗号化フラグF1610と、クロック生成装置203が生成するクロック信号とがある。

[0140] 次に、認証暗号装置1601の動作の概要を説明する。図17は、認証暗号装置1601の動作概要を説明するためのフローチャートである。

[0141] ステップ1701:認証暗号装置1701には、パラメータK204とメッセージM205とが入力される。パラメータK204は、パラメータ入力制御装置218を介してメッセージ認証子生成装置201に入力され、メッセージ認証子生成装置201の初期化を行う。メッセージM205は、メッセージ入力制御装置209を介してメッセージ認証子生成装置201に、さらに、スイッチ1607を介して暗号化装置1608に入力される。

[0142] メッセージ入力制御装置209は、メッセージM205を、一定長Lのブロックに分割し、クロック生成装置203からクロック信号が入力されるごとにメッセージ認証子生成装置201と暗号化装置1608に向けて出力する。パラメータ入力制御装置218は、図3で説明したメッセージ認証子生成装置201の場合と同様に動作する。

[0143] 認証暗号装置1601は、これらの入力を受けると、クロック生成装置203から入力さ

れるクロック信号に従って、以下の処理を行う。

[0144] ステップ1702:メッセージM205を、ブロック長Lビットのメッセージブロック M1、M2、…、MNに分割する。

[0145] ステップ1703:パラメータ入力制御装置218を介して入力されたパラメータK204(Kn)を順にメッセージ認証子生成装置201に入力し、レジスタ212の初期化を行う。

[0146] ステップ1704:メッセージ認証子生成装置201に含まれているカウンタ(213;図16では不図示)の値を初期化する。本実施形態では、全てのビット値を0にセットする。

[0147] ステップ1705:カウンタ213の値がNになるまでステップ1706、1707の処理を繰り返す。

[0148] ステップ1706:クロック信号が入力されるごとに、メッセージ認証子生成装置201は図3のステップ306に従い処理を行う。

[0149] ステップ1707:レジスタ212の値がスイッチ1606を介して出力フィルタ1605に入力される。出力フィルタ1605は、レジスタ212から入力された値から、一定長のビット列Rn(nはN以下の自然数であり、カウンタが現在保持している値となる)を生成し、暗号化装置1608に向けて出力する。暗号化装置1608は、メッセージ入力制御装置209およびスイッチ1607を介して入力されたメッセージブロックMnと前記のビット列Rnとから暗号文ブロックCnを生成し、メモリ1612に向けて出力する。

[0150] ステップ1708、1709:カウンタ213の値がNになると、メッセージ認証子生成装置201は図3におけるステップ307、308の処理を行い、メッセージ認証子T207を出力する。同時にメモリ1612は暗号文C(暗号文パケット1611)=C1||C2||…||CNを出力する。

[0151] ステップ1710:処理を終了する。

[0152] 以上が認証暗号装置1601の構成と動作のフローである。

[0153] なお、認証暗号装置1601への入力のうち、暗号化フラグF1610はメッセージを暗号化するか否かを決定するフラグである。暗号化フラグF1610が暗号化を指示している場合には、スイッチ1606、1607が接続され、上記の認証暗号装置1601として動作する。一方、暗号化フラグが暗号化を指示していない場合には、スイッチ1606、

1607は切断され、暗号化処理は行われない。この場合には、認証暗号装置1601は前述のメッセージ認証子生成装置201として動作し、メッセージ認証子T207のみを出力する。

[0154] 上記の構成例では、暗号文ブロックCnを一旦メモリ1612に格納し、メッセージ認証子T207と同時に暗号文パケット1611として出力したが、十分なメモリが確保できない場合などには、暗号文ブロックCnは逐次出力しても良い。

[0155] 認証暗号装置1601が備えている出力フィルタ1605は、レジスタA(604)の最下位ブロックA2(t)を出力する。上記の構成例は、最も単純な出力フィルタの例であり、レジスタ212の複数ブロックにさらに非線形変換を施して安全性を高めることも可能である。

[0156] 非線形な出力フィルタの例として、図6に挙げた非線形置換A801を用いる例を以下に説明する。非線形置換A801による変換をFで、出力フィルタ1605をFoutで表すとき、

Fout(A0(t), A1(t), A2(t), B0(t), …, B15(t)) = F(A2(t) XOR Bi(t)) XOR Bj(t)

で定義される出力フィルタは、出力されるビット列とレジスタの値との相関を小さくする働きがあり、結果として、より安全な認証暗号装置を実現することができる。

[0157] 次に、認証暗号装置1601で暗号化されたデータの完全性を検証しつつデータを復号する認証復号装置を説明する。

[0158] 図18は、本実施形態の認証復号装置1801のイメージ図である。認証復号装置1801の構成は、基本的に認証暗号装置1601と同様であるが、暗号化装置1608の代わりに復号装置1806を備え、また、タグT1804とメッセージ認証子生成装置201の出力とを比較するタグ比較装置1808、復号装置1806の出力を保持するメモリ1807を備える。

[0159] 認証復号装置1801への入力は、メッセージM205ではなく暗号文C1803である。暗号文C1803は暗号文入力制御装置1805を介してメッセージ認証子生成装置201と復号装置1806とに入力される。また、付加的な入力として、タグT1804がある。

[0160] 次に、認証復号装置1801の動作の概要を説明する。図19は、認証復号装置1801の動作概要を説明するためのフローチャートである。

[0161] ステップ1901:認証復号装置1801は、パラメータK204と暗号文1803とタグT1804とが入力される。

[0162] メッセージ入力制御装置209は、暗号文C1803を一定長Lのブロックに分割し、クロック生成装置203からクロック信号が入力されるごとにメッセージ認証子生成装置201と復号装置1806とに向けて出力する。

[0163] パラメータ入力制御装置218は、図3で説明したメッセージ認証子生成装置201の場合と同様に動作する。

[0164] 認証復号装置1801は、これらの入力を受けると、クロック生成装置203から入力されるクロック信号に従って、以下の処理を行う。

[0165] ステップ1902:暗号文C1803を、ブロック長Lビットの暗号文ブロックC1、C2、…、CNに分割する。

[0166] ステップ1903:パラメータ入力制御装置218を介して入力されたパラメータK204(Kn)を順にメッセージ認証子生成装置201に入力し、レジスタ212の初期化を行う。

[0167] ステップ1904:メッセージ認証子生成装置201に含まれているカウンタ(213;図18では不図示)の値を初期化する。本実施形態では、全てのビット値を0にセットする。

[0168] ステップ1905:カウンタ213の値がNになるまでステップ1706、1707の処理を繰り返す。

[0169] ステップ1906:クロック信号が入力されるごとに、レジスタ212の値がスイッチ1606を介して出力フィルタ1605に入力される。出力フィルタ1605は、レジスタ212から入力された値から、一定長の乱数列Rn(nはN以下の自然数であり、カウンタが現在保持している値となる。)を生成し、復号装置1806に向けて出力する。復号装置1806は、暗号文入力制御装置1805、スイッチ1607を介して入力された暗号文ブロックCnから復号文Mn'を生成し、出力する。

[0170] ステップ1907:メッセージ認証子生成装置201は図3のステップ306に従い処理を行う。

[0171] ステップ1908、1709:カウンタ213の値がNになると、メッセージ認証子生成装置201は図3におけるステップ307、308の処理を行い、復号文M'に対するメッセージ認証子T'を出力する。

[0172] ステップ1910:ステップ1909で出力されたメッセージ認証子T'とタグT1804の値と比較する。

[0173] ステップ1911、1912:ステップ1910の比較において、両者の値が等しければ復号文M'を出力する。それ以外の場合には、認証が失敗したことを示すエラー信号、たとえば1を出力する。

[0174] ステップ1913:処理を終了する。

[0175] 次に、本実施形態のMAC生成装置201およびMAC検証装置401を用いたメッセージ認証方法について説明する。

[0176] 図15は、本実施形態のMAC生成装置201およびMAC検証装置401によりメッセージ認証を行う通信システムの構成図である。

[0177] ここでは、MAC生成装置201、MAC検証装置401を実現するものとして、例えば、ICカード1301、1309を例にあげて説明する。

[0178] 本実施形態の通信システムは、MAC生成装置201、メッセージ入力制御装置209およびパラメータ入力制御装置218を実現するICカード1301と、MAC検証装置401、メッセージ入力制御装置209およびパラメータ入力制御装置218を実現するICカード1311と、ICカード1301で生成したメッセージ認証子とメッセージとをネットワーク1340を介して相手装置に送信する送信側通信装置1320と、ネットワーク1340を介して送信側通信装置1320から送信されたメッセージ認証子とメッセージとを受信し、ICカード1311に受け渡す受信側通信装置1330とを備える。

[0179] ICカード1301、1311は、本図に示すように、CPU1302、1313、メモリ1303、1313、記憶装置1304、1314、入出力インタフェース1305、1315とをそれぞれ備える。

[0180] また、記憶装置1304、1314には、本図に示すように、秘密鍵1306、1316、メッセージ番号1307、1317、セキュリティパラメータD206、メッセージ認証子生成プログラム1308、メッセージ認証子検証プログラム1318とが、それぞれ格納されている。

[0181] メッセージ認証子生成プログラム1308は、メモリ1303にロードされ、CPU1302にて実行されることにより、上記のMAC生成装置201、メッセージ入力制御装置209およびパラメータ入力制御装置218の機能を実現する。また、秘密鍵1306とメッセ

ージ番号1307との対を、MAC生成装置201のパラメータK204として用いる。

[0182] メッセージ認証子検証プログラム1318は、メモリ1313にロードされ、CPU1312にて実行されることにより、上記のMAC検証装置401、メッセージ入力制御装置209およびパラメータ入力制御装置218の機能を実現する。また、秘密鍵1316とメッセージ番号1317との対を、MAC検証装置401のパラメータK204として用いる。

[0183] なお、クロック信号は、ICカード1301、1311内のクロック生成機能により生成されるものを利用する。

[0184] 以下、本通信システムにおける、メッセージ認証の処理手順について、説明する。

[0185] ステップ1401:データ送信者とデータ受信者は、事前に秘密鍵1306、1316を秘密裏に共有しておく。また、メッセージ番号1307、1317およびセキュリティパラメータD206は、秘密裏である必要はないが、事前に共有しておく。すなわち、ICカード1301の秘密鍵1306とICカード1311の秘密鍵1316、および、メッセージ番号1307と1317とには、それぞれ同じデータが保持される。これらの情報を共有する技術は、例えば、公開鍵暗号技術を用いることで、実現できる。

[0186] ステップ1402:メッセージ送信者は、I/Oインタフェース1305を介して、メッセージM205をICカード1301に入力する。ICカード1301(MAC生成装置201)は、メッセージM205の入力を受け付けると、秘密鍵1306とメッセージ番号1307とからなるパラメータ、および、セキュリティパラメータD206を用いて、入力されたメッセージM205に対するメッセージ認証子T207を生成し、メッセージM205とともに送信側通信装置1320に受け渡す。

[0187] ステップ1403:メッセージM205とメッセージ認証子T207とをICカード1301から受け取ると、送信側通信装置1320は、それらを、ネットワーク1340を介して、受信側通信装置1330に送信する。

[0188] ステップ1404:受信側通信装置1340は、メッセージM205およびメッセージ認証子T207を受信し、I/Oインタフェース1315を介して、ICカード1311(MAC検証装置401)に入力する。

[0189] ステップ1405:ICカード1311は、メッセージM205とメッセージ認証子T207とを受け取ると、共有情報である秘密鍵1316とメッセージ番号1317とからなるパラメータ

、および、セキュリティパラメータD206とを用いて、メッセージ認証子T207を検証し、入力されたメッセージM205の真正性を判断し、真正である場合は0、そうでない場合は1を出力することにより、その結果を出力する。

[0190] 具体的には、受信側でメッセージ認証子T207'を生成し、受け取ったメッセージ認証子T207と比較し、合致すれば、真正、合致しない場合は真正でないものと判断し、上記0、1を出力する。

[0191] 次に、認証暗号装置1601、認証復号装置1801を実現するものとして、ICカード2001、2011を例に挙げて説明する。

[0192] 図20はICカード2001、2011を含む通信システムの構成例である。図20のシステムは、図15で説明したメッセージ認証機能を備えた通信システムとほぼ同様の構成を備える。ただし、ICカード2001は、メッセージ認証子生成プログラム1308の代わりに認証暗号プログラム2002を、そして、ICカード2011は、メッセージ認証子検証装置1318の代わりに、認証復号プログラム2012を格納する。また、暗号処理を行うかどうかを決定する暗号化フラグ2003、2013をそれぞれ格納する。

[0193] 以下、本通信システムにおける、データ処理の手順について説明する。

[0194] ステップ2201:データ送信者とデータ受信者とは、事前に秘密鍵1306、1316を共有しておく。これはメッセージ認証システムのステップ1401と同様であるが、この他に、データ送信者とデータ受信者とは暗号化フラグ2003と2004とを同期させ、データの暗号化を行うか否かを予め決定しておく。ただし、暗号化フラグを暗号文パケット1611に含めることで、データ通信と同時に暗号化フラグの同期を行うこともできる。

[0195] ステップ2202:メッセージ送信者は、I／Oインターフェース1305を介して、メッセージM205をICカード2001に入力する。ICカード2001(認証暗号装置1601)は、メッセージM(205)の入力を受け付けると、秘密鍵1306とメッセージ番号1307とからなるパラメータおよびセキュリティパラメータD206を用い、入力されたメッセージM(205)に対するデータ処理を行う。暗号化フラグ2003が暗号化処理を指示していない場合は、ICカード2001は上記パラメータを用いてメッセージM(205)に対するメッセージ認証子T(207)を生成し、メッセージM(205)と共に送信側通信装置1320に受け渡す。また、暗号化フラグ2003が暗号化処理を指示している場合には、ICカー

ド2001は上記パラメータを用いてメッセージM(205)に暗号化処理を施し、暗号文C(1609)を生成すると同時に、メッセージM(205)に対するメッセージ認証子T(207)を生成し、暗号文C(1609)と共に送信側通信装置1320に受け渡す。

[0196] 暗号化処理を行わない場合のICカード2001、2002の動作は前記のメッセージ認証システムの処理手順と同じなので、以下では記述を省略する。

[0197] ステップ2203:暗号文C(1309)とメッセージ認証子T(207)からなる暗号文パケット(1611)とをICカード2001から受け取ると、送信側通信装置1320は、それらを、ネットワーク1340を介して、受信側通信装置1330に送信する。

[0198] ステップ2204:受信側通信装置1330は、暗号文C(1803)およびタグT(1804)を受信し、I/Oインターフェース1315を介して、ICカード2011(認証復号装置1801)に入力する。

[0199] ステップ2205:ICカード2011は、暗号文C(1803)およびタグT(1804)を受け取ると、共有情報である秘密鍵1316とメッセージ番号1317とからなるパラメータ、およびセキュリティパラメータD206とを用いて、暗号文の復号とタグT(1804)の検証を行う。検証の結果、暗号文の改ざんが検出されなければ(暗号文C1803から計算したメッセージ認証子の値とタグT(1804)の値とが一致すれば)、復号したメッセージM'(1809)を出力する。そうでない場合には、メッセージ認証子の値が一致しなかったことを意味する信号(たとえば0)を出力する。

[0200] 以上説明したように、本実施形態におけるMAC認証装置201およびMAC検証装置401によれば、高速な処理が可能であり、長期間の使用に耐え得る安全なMAC生成装置およびMAC検証装置が提供できる。また、本実施形態における認証暗号装置1601および認証復号装置1801によれば、高速な処理が可能であり、長期間の使用に耐え得る安全な認証暗号装置および認証復号装置が提供できる。さらに、上記各装置で用いられる本実施形態のMAC生成装置201は、攪拌回数を、鍵長などのセキュリティパラメータで決定する構成となっているため、攪拌処理の適用回数の変更が容易である。これは、安全性レベルと処理速度とをフレキシブルに設定できることを意味する。

[0201] インターネットのように、公開通信路を用いた通信では、メッセージの真正性検証は

、信頼できる通信路を確保するために必須の技術である。

[0202] 従来から知られているブロック暗号を利用した方式は、高速な処理が困難である。また、ハッシュ関数を用いた構成では、いずれの方式でも、以下の問題点がある。

(1)処理速度が遅い。

(2)出力長が短い(安全性のレベルが低い)。

[0203] ブロック暗号技術を利用した方式に比べ、ストリーム暗号技術を利用するメッセージ認証は、安価かつ高速に処理を行うことができるため、広い範囲での応用が見込まれる。

[0204] 本実施形態のメッセージ認証は、ストリーム暗号技術を用いたものである。従って、本実施形態によるMAC生成装置、MAC検証装置は、任意のメッセージ認証システムにおけるメッセージ認証子生成機能、および認証子検証機能の、より安価で高速な代替として用いることができる。また、本実施形態のMAC生成装置およびMAC検証装置によれば、上記MAC生成とデータの暗号化とを同時に行う認証暗号の機能を、より安価に提供することができる。

[0205] 本実施形態におけるMAC生成装置およびMAC検証装置によるメッセージの真正性検証機能は、従来方式に比べ、以下の利点を有する。

(1)メッセージの真正性を検証するための実装コストを最小限に抑えられる。

(2)ブロック暗号を用いるものに比べて高速な処理を行うことができ、計算機に対する負荷が少ない。

[0206] 一般的に、組み込み機器や携帯端末では、実装やコストに制約があり、メッセージの真正性検証は軽視されがちである。このような計算機の能力に制限がある環境における暗号処理では、コストパフォーマンスに優れるストリーム暗号を用いる場合が多い。本実施形態のMAC生成装置およびMAC検証装置はこのような環境でのメッセージ検証機能の導入コストを最小限に抑えることができ、今後のユビキタス情報端末での広い応用が期待される。

請求の範囲

[1] 送受信するメッセージデータの完全性を検証するためのメッセージ認証子を当該メッセージデータから生成するメッセージ認証子生成装置であって、

第1のパラメータに初期化処理を施し、一定長のランダムなビット列からなるデータを出力する初期化装置と、

前記初期化装置の出力したデータを格納するレジスタと、

入力される前記メッセージデータを一定長に分割した後、一定長のメッセージデータ毎に、当該一定長のメッセージデータと前記レジスタに格納されているデータとを攪拌し、攪拌後のデータを前記レジスタに格納するデータ攪拌装置と、

前記レジスタに格納されているデータであって、前記データ攪拌装置において攪拌後のデータを、所定のデータ長に圧縮し、メッセージ認証子として出力する圧縮処理を行うデータ圧縮装置と、

を備え、前記データ攪拌装置は、前記一定長のメッセージデータの2倍以上のサイズの出力を有する非線形変換装置と、を備えること

を特徴とするメッセージ認証子生成装置。

[2] 請求項1記載のメッセージ認証子生成装置であって、

前記レジスタは、前記初期化装置の出力したデータを分割して格納する第1の小レジスタと第2の小レジスタとを備え、

前記第1の小レジスタのサイズは、前記非線形変換装置の出力データのサイズであり、

前記非線形変換装置は、

前記第1の小レジスタに格納されているデータと前記第2の小レジスタに格納されているデータの一部と前記メッセージデータとを非線形に攪拌し、攪拌後のデータを前記第1の小レジスタに格納し、

前記データ攪拌装置は、

前記第2の小レジスタに格納されているデータと前記第1の小レジスタに格納されているデータの一部とを線形に攪拌し、攪拌後のデータを前記第2の小レジスタに格納する線形変換装置を備えること

を特徴とするメッセージ認証子生成装置。

[3] 請求項2記載のメッセージ認証子生成装置であって、

前記データ攪拌装置は、前記メッセージデータの入力を制御するスイッチをさらに備え、

前記非線形変換装置は、

前記スイッチにより前記メッセージデータの入力が制限されている場合または前記メッセージデータの入力が無い場合は、前記第1の小レジスタに格納されているデータと前記第2の小レジスタに格納されているデータの一部とのみを入力として非線形に攪拌し、攪拌後のデータを前記第1の小レジスタに格納すること

を特徴とするメッセージ認証子生成装置。

[4] 請求項3記載のメッセージ認証子生成装置であって、

前記第1の小レジスタは、nビット(nは、前記一定長のメッセージのサイズを示す数字以上の任意の自然数)サイズのブロック、3ブロック分の容量を備え、

前記第2の小レジスタは、前記ブロック、m(mは任意の自然数)ブロック分の容量を備え、

前記非線形変換装置は、

前記1ブロックのデータを処理して、前記1ブロックのデータを出力する第1の非線形置換および第2の非線形置換を備えること

を特徴とするメッセージ認証子生成装置。

[5] 請求項4記載のメッセージ認証子生成装置であって、

前記非線形変換装置は、前記第1の非線形置換および前記第2の非線形置換とを用いて以下の処理を行い

X0←A1,

X1←A2 XOR G(A1 XOR M),

X2←A0 XOR F(A1 XOR (B10 <<< 17)),

(ただし、前記第1の小レジスタの記憶内容を上位ブロックから順にA0, A1, A2、前記第2の小レジスタの第iブロックをBi(1<=i<=m)、前記第1の非線形置換をF、前記第2の非線形置換をG、前記スイッチを介して入力されるデータをM、レジスタxのブロッ

ク幅での左nビット巡回シフトを(x <<< n)、データの代入を←、前記非線形データ変換装置の出力を上位ブロックからX0, X1, X2と表す。)、

前記X0, X1, X2を、それぞれ、前記小レジスタの上位ブロックから順に格納することを特徴とするメッセージ認証子生成装置。

[6] 請求項5記載のメッセージ認証子生成装置であって、

前記ブロックは64ビットで構成され、

前記第1の非線形置換及び前記第2の非線形置換は、それぞれ、

入力されるブロックを8ビット単位に分けて非線形変換処理を行う変換テーブルと、

32ビット単位で線形変換処理を行う第1の線形変換および第2の線形変換と、をさらに備え、

前記変換テーブルと前記第1の線形変換および第2の線形変換とを用いて、以下の処理を行うこと

p0||p1||...||p7←p,

ti←S[pi] (0 <= i <= 7),

u0||u1||u2||u3←L0(t0, t1, t2, t3),

u4||u5||u6||u7←L1(t4, t5, t6, t7),

c←u4||u5||u2||u3||u0||u1||u6||u7,

(ただし、前記第1および第2の非線形置換への入力をp、前記変換テーブルによる変換をS[x]、32×32行列による前記第1の線形変換をL0、32×32行列による前記第2の線形変換をL1、データxとyとの連結をx||yと表す。)

を特徴とするメッセージ認証子生成装置。

[7] 請求項4記載のメッセージ認証子生成装置であって、

前記第2の小レジスタの容量は64ビットサイズのブロック16ブロック分であり、

前記線形変換装置は、以下の処理を行うこと

Yi←B(i-1), (1<=i<=15, i!= 4, 10)

Y0←B15 XOR A0,

Y4←B3 XOR B7,

Y10←B9 XOR (B13 <<< 32),

(ただし、iは自然数、XORは排他的論理和、前記第1の小レジスタの記憶内容を上位ブロックから順にA0, A1, A2、前記第2の小レジスタの記憶内容を上位ブロックから順にB0, B1, …, B15、線形変換装置の出力データを上位ブロックからY0, Y1, …, Y15、レジスタxのブロック幅での左nビット巡回シフトを(x <<< n)、とする。)

を特徴とするメッセージ認証子生成装置。

[8] 請求項3記載のメッセージ認証子生成装置であって、

前記初期化装置は、前記レジスタと前記データ攪拌装置と前記スイッチとを備え、当該レジスタと当該データ攪拌装置と当該スイッチとにより、前記初期化処理を行い、

前記データ圧縮装置は、前記レジスタと前記データ攪拌装置と前記スイッチとを備え、当該レジスタと当該データ攪拌装置と当該スイッチとにより、前記圧縮処理を行うこと

を特徴とするメッセージ認証子生成装置。

[9] 請求項1記載のメッセージ認証子生成装置であって、

前記データ攪拌装置の攪拌回数を制御する制御装置を備え、

前記制御装置は、予め与えられる前記メッセージ認証子生成装置の安全性の指標である第2のパラメータにより、前記攪拌回数を決定し、制御すること

を特徴とするメッセージ認証子生成装置。

[10] 受信するメッセージデータとともに受信する当該メッセージデータの完全性を検証するためのメッセージ認証子を検証するメッセージ認証子検証装置であって、

請求項1記載のメッセージ認証子生成装置と、

前記メッセージ認証子生成装置を用いて、受信したメッセージデータから、第2のメッセージ認証子を生成し、生成した前記第2のメッセージ認証子と、前記受信したメッセージ認証子とを比較し、比較結果を出力する比較手段と、

を備えることを特徴とするメッセージ認証子検証装置。

[11] 送受信するメッセージデータの完全性を検証するメッセージ検証システムであって、

請求項1記載のメッセージ認証子生成装置を備える送信側通信装置と、

請求項10のメッセージ認証子検証装置を備える受信側通信装置と、

を備えることを特徴とするメッセージ検証システム。

[12] 送受信するメッセージデータの完全性を検証するためのメッセージ認証子を生成するメッセージ認証子生成方法であって、

第1のパラメータに初期化処理を施し、一定長のランダムなビット列からなるデータをレジスタに格納する初期化処理ステップと、

入力される前記メッセージデータを一定長に分割した後、一定長のメッセージデータ毎に、当該一定長のメッセージデータと前記レジスタに格納されているデータとを攪拌し、攪拌後のデータを前記レジスタに格納するデータ攪拌ステップと、

前記データ攪拌ステップにおいて攪拌後のデータであって、前記レジスタに格納されているデータを、所定のデータ長に圧縮し、メッセージ認証子として出力するデータ圧縮ステップと、を備え、

前記攪拌は、前記一定長のメッセージデータの2倍以上のサイズの出力を有する非線形変換装置を有する攪拌装置により行われること、

を特徴とするメッセージ認証子生成方法。

[13] 送受信するメッセージデータを暗号化するとともに完全性を検証するためのメッセージ認証子を当該メッセージデータから生成する認証暗号装置であって、

請求項1記載のメッセージ認証子生成装置と、

前記メッセージ認証子生成装置の備える前記レジスタから一定長のビット列を選択して出力する出力フィルタと、

前記出力フィルタから出力される出力ビット列と前記メッセージ認証子生成装置へ入力される一定長のメッセージデータとの排他的論理和をとり暗号文ブロックを生成する暗号化装置と、を備えること

を特徴とする認証暗号装置。

[14] 一定長の暗号文ブロック単位で受信する暗号化されたメッセージデータを復号するとともに当該メッセージデータの完全性を検証するためのタグを検証する認証復号装置であって、

請求項10に記載のメッセージ認証子検証装置と、

復号した前記メッセージデータである復号文を蓄えるメモリと、

前記メッセージ認証子検証装置が備える前記メッセージ認証子生成装置の前記レジスタから一定長のビット列を選択して出力する出力フィルタと、

前記出力フィルタから出力される出力ビット列と、前記一定長の暗号文ブロック単位のメッセージデータとの排他的論理和をとることにより前記メッセージデータを復号し復号文として、前記メモリに出力する復号装置と、を備え、

前記メッセージ認証子検証装置が完全性を検証した後に、前記メモリに蓄えられた復号文を出力すること

を特徴とする認証復号装置。

[15] 送受信するメッセージを暗号化して送信するとともに前記メッセージの完全性を検証するメッセージ検証システムであって、

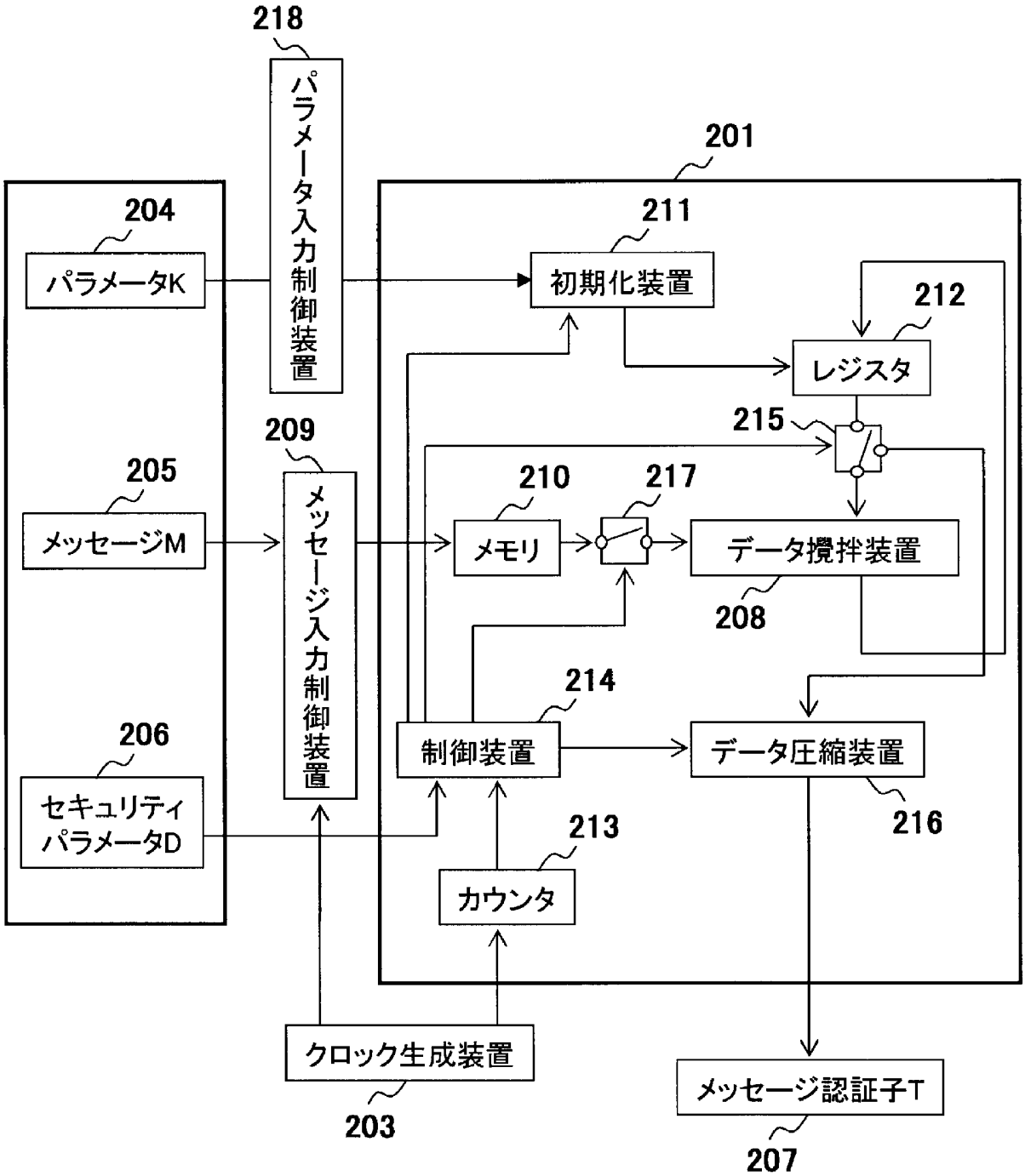
請求項13の認証暗号装置を備える送信側通信装置と、

請求項14の認証復号装置を備える受信側通信装置と、

を備えることを特徴とするメッセージ検証システム。

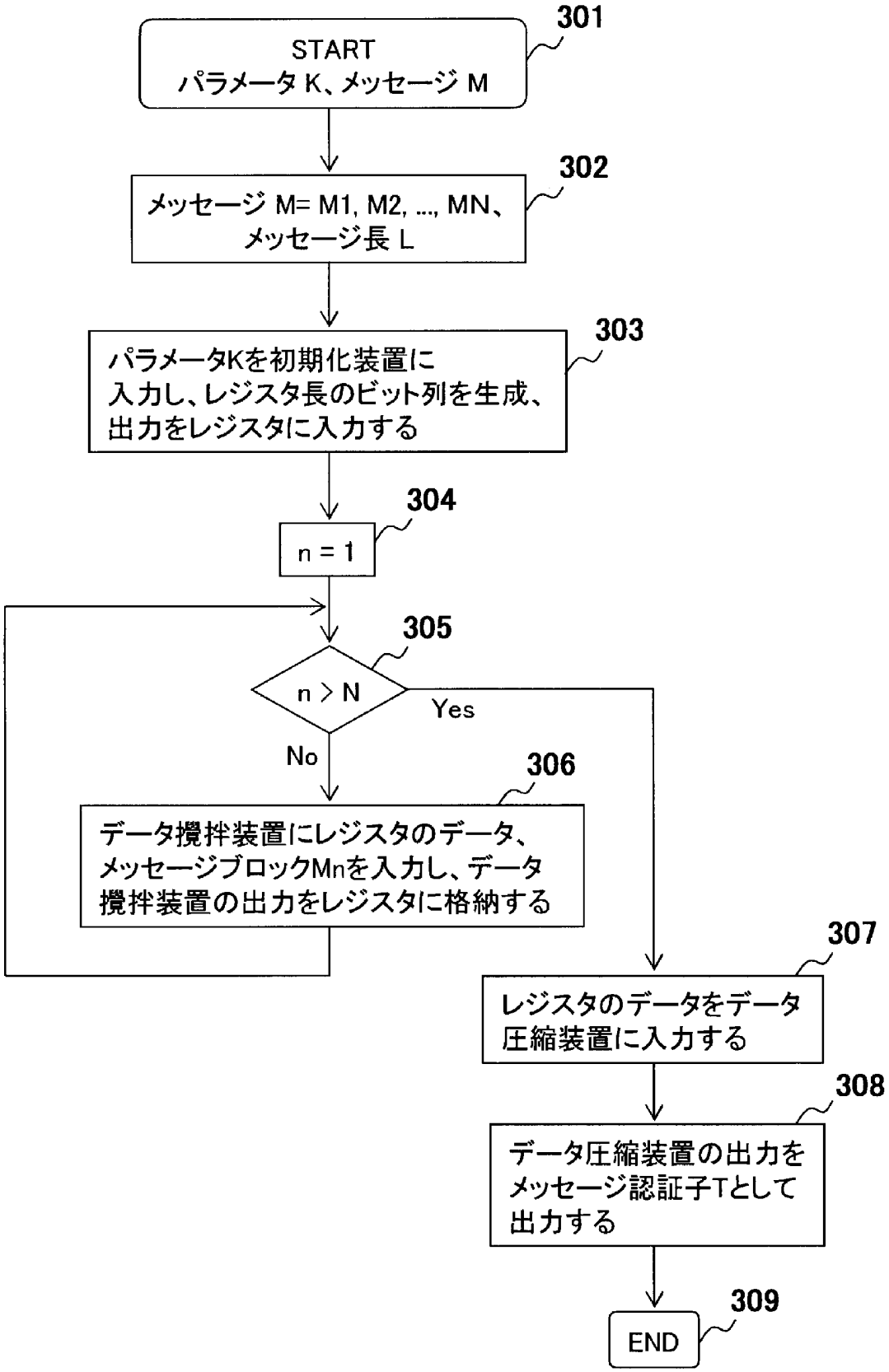
[図1]

図1


218
パラメータ入力制御装置
201
204
パラメータK
211
初期化装置
212
レジスタ
215
209
205
メッセージM
メッセージ入力制御装置
210
メモリ
217
データ撹拌装置
208
214
206
制御装置
データ圧縮装置
セキュリティパラメータD
216
213
カウンタ
クロック生成装置
203
メッセージ認証子T
207

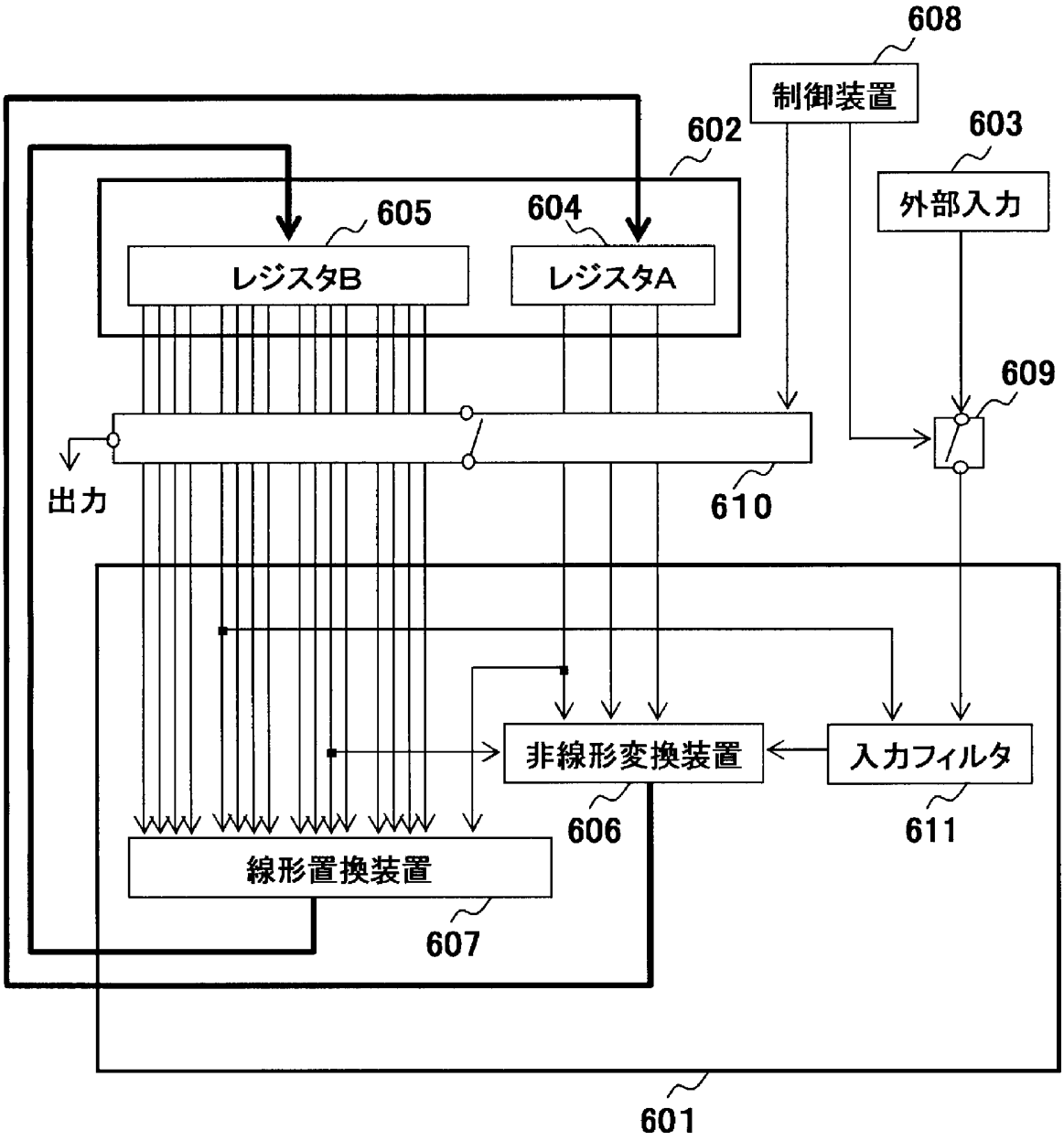
[図2]

図2


301
START
パラメータ K、メッセージ M
302
メッセージ M= M1, M2, ..., MN、
メッセージ長 L
303
パラメータKを初期化装置に
入力し、レジスタ長のビット列を生成、
出力をレジスタに入力する
304
n = 1
305
n > N
Yes
No
306
データ撹拌装置にレジスタのデータ、
メッセージブロックMnを入力し、データ
撹拌装置の出力をレジスタに格納する
307
レジスタのデータをデータ
圧縮装置に入力する
308
データ圧縮装置の出力を
メッセージ認証子Tとして
出力する
309
END

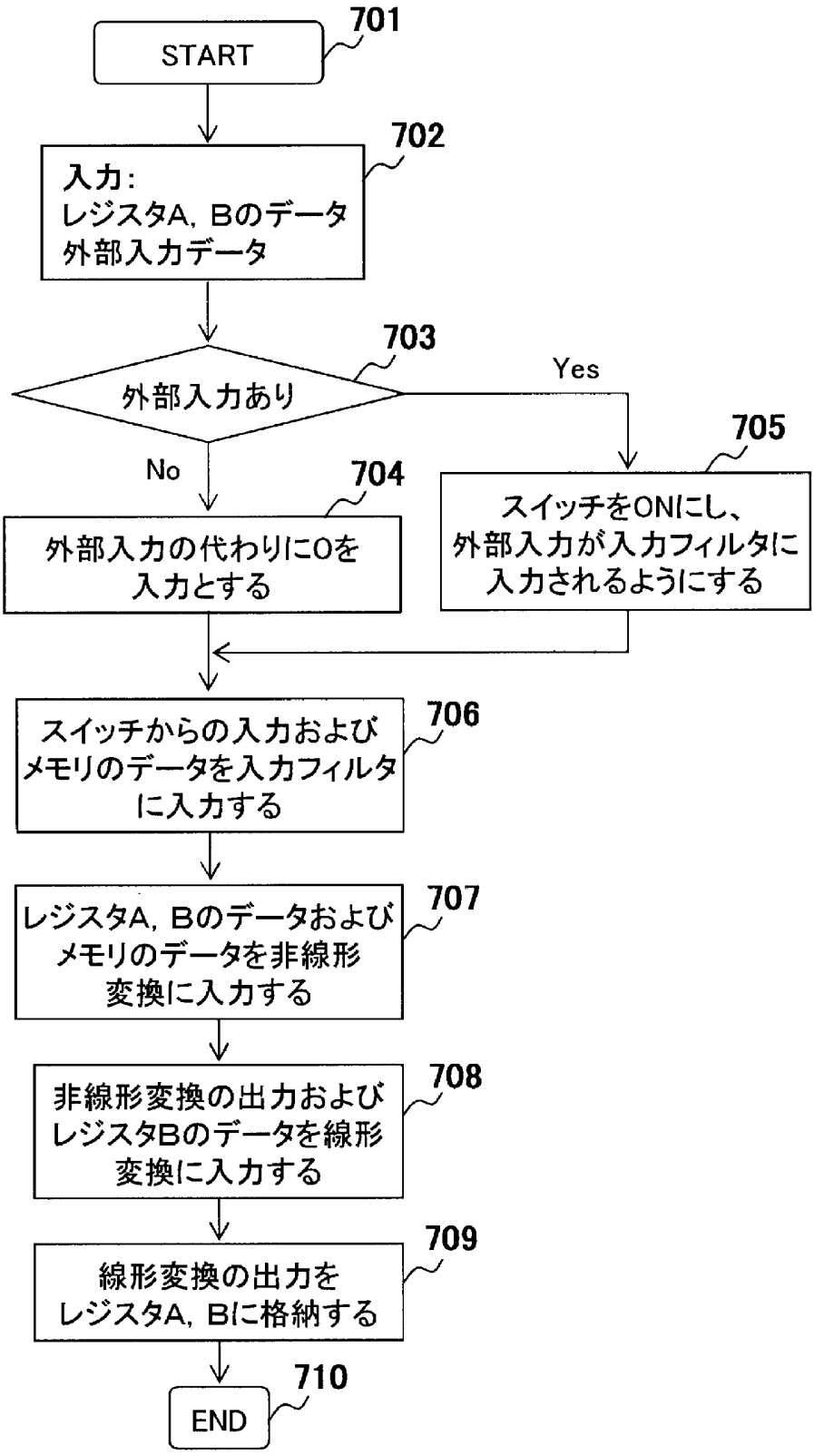
[図3]

図3


608
制御装置
602
603
外部入力
605
604
レジスタB
レジスタA
609
出力
610
非線形変換装置
入力フィルタ
606
611
線形置換装置
607
601

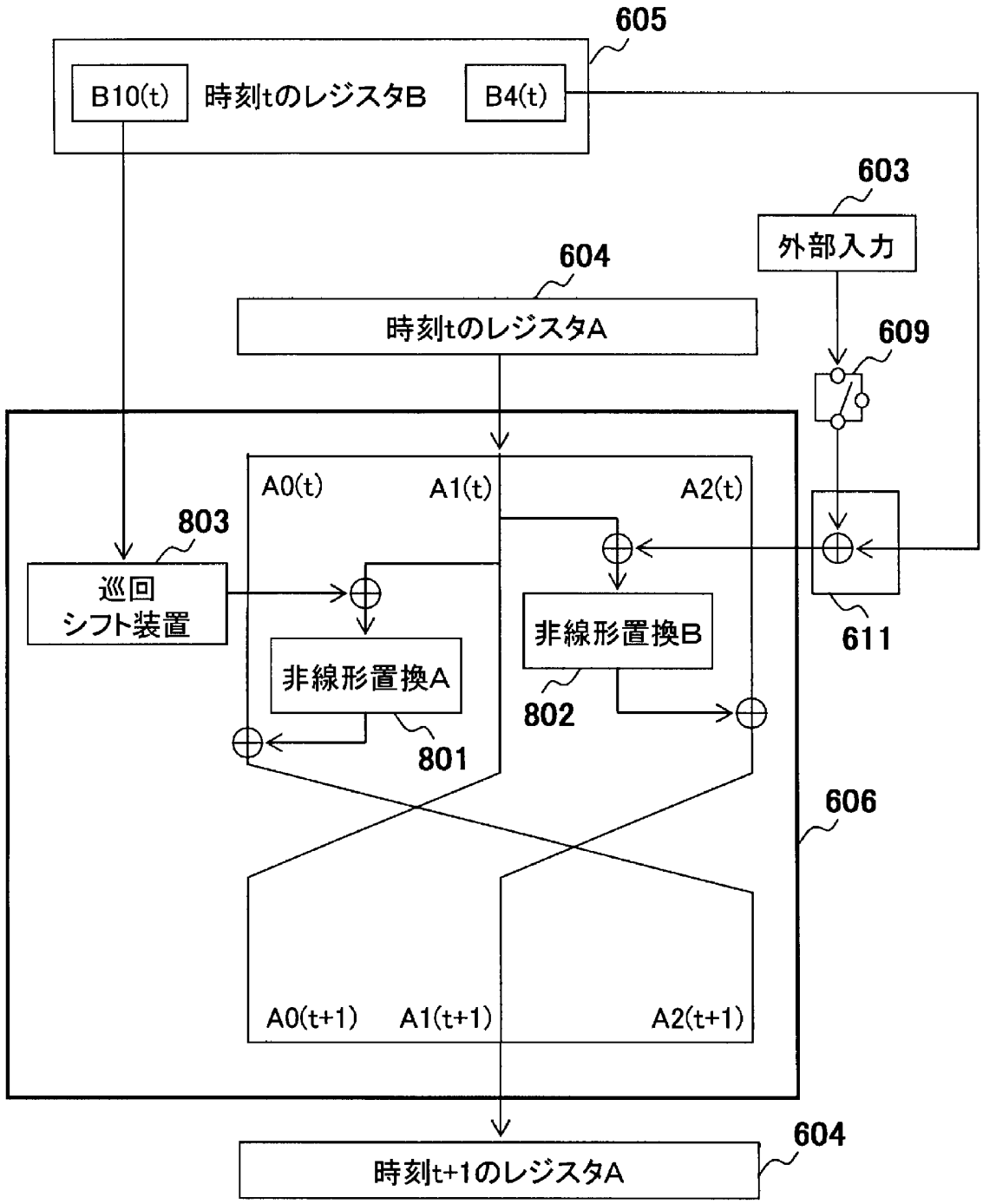
[図4]

図4


701
START
702
入力:
レジスタA, Bのデータ
外部入力データ
703
外部入力あり
Yes
No
705
スイッチをONにし、
外部入力が入力フィルタに
入力されるようにする
704
外部入力の代わりに0を
入力とする
706
スイッチからの入力および
メモリのデータを入力フィルタ
に入力する
707
レジスタA, Bのデータおよび
メモリのデータを非線形
変換に入力する
708
非線形変換の出力および
レジスタBのデータを線形
変換に入力する
709
線形変換の出力を
レジスタA, Bに格納する
710
END

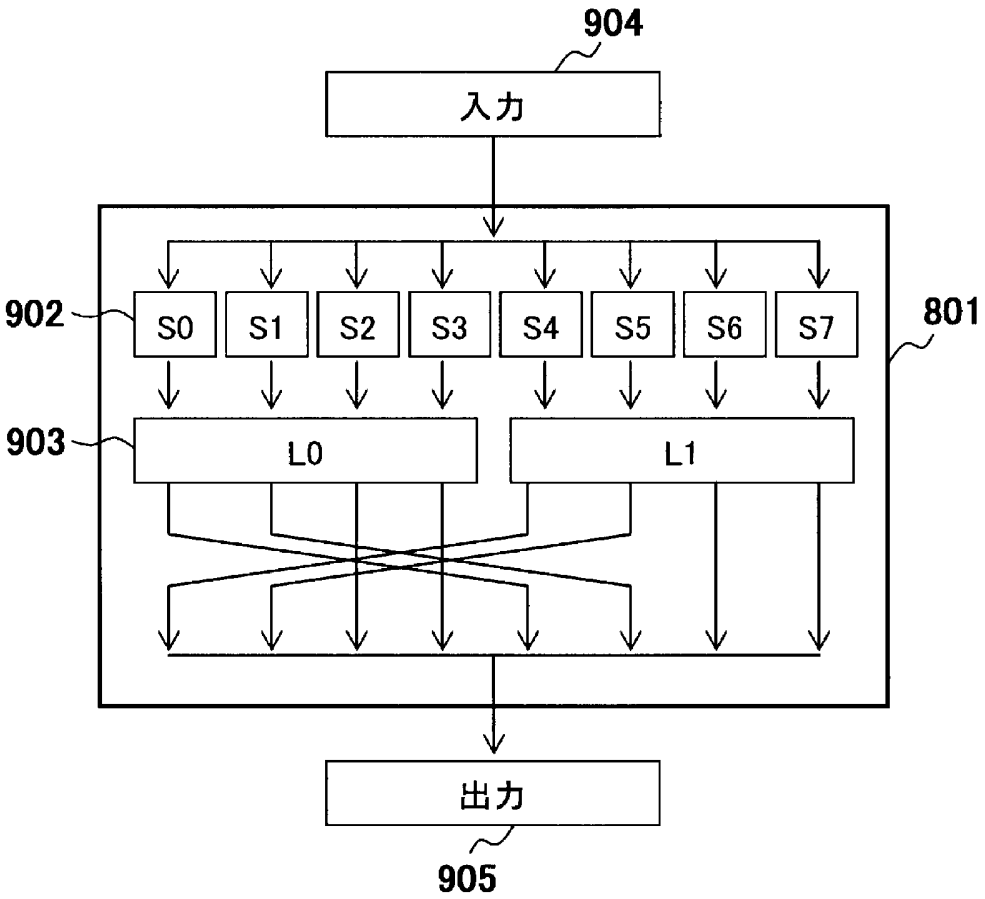
[図5]

図5


605
B10(t)
時刻tのレジスタB
B4(t)
603
外部入力
604
時刻tのレジスタA
609
A0(t)
A1(t)
A2(t)
803
巡回
シフト装置
非線形置換A
801
非線形置換B
802
611
606
A0(t+1)
A1(t+1)
A2(t+1)
604
時刻t+1のレジスタA

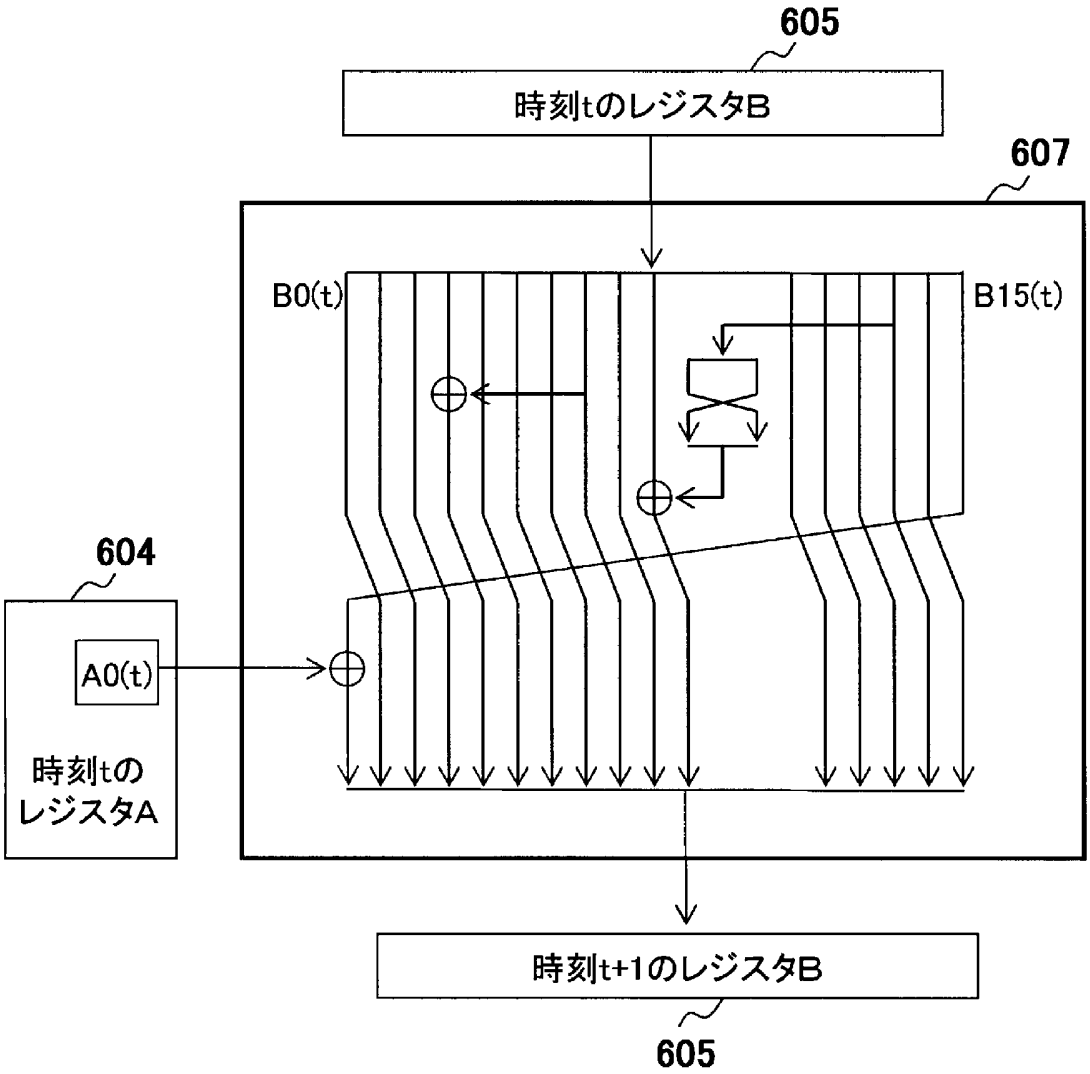
[図6]

図6



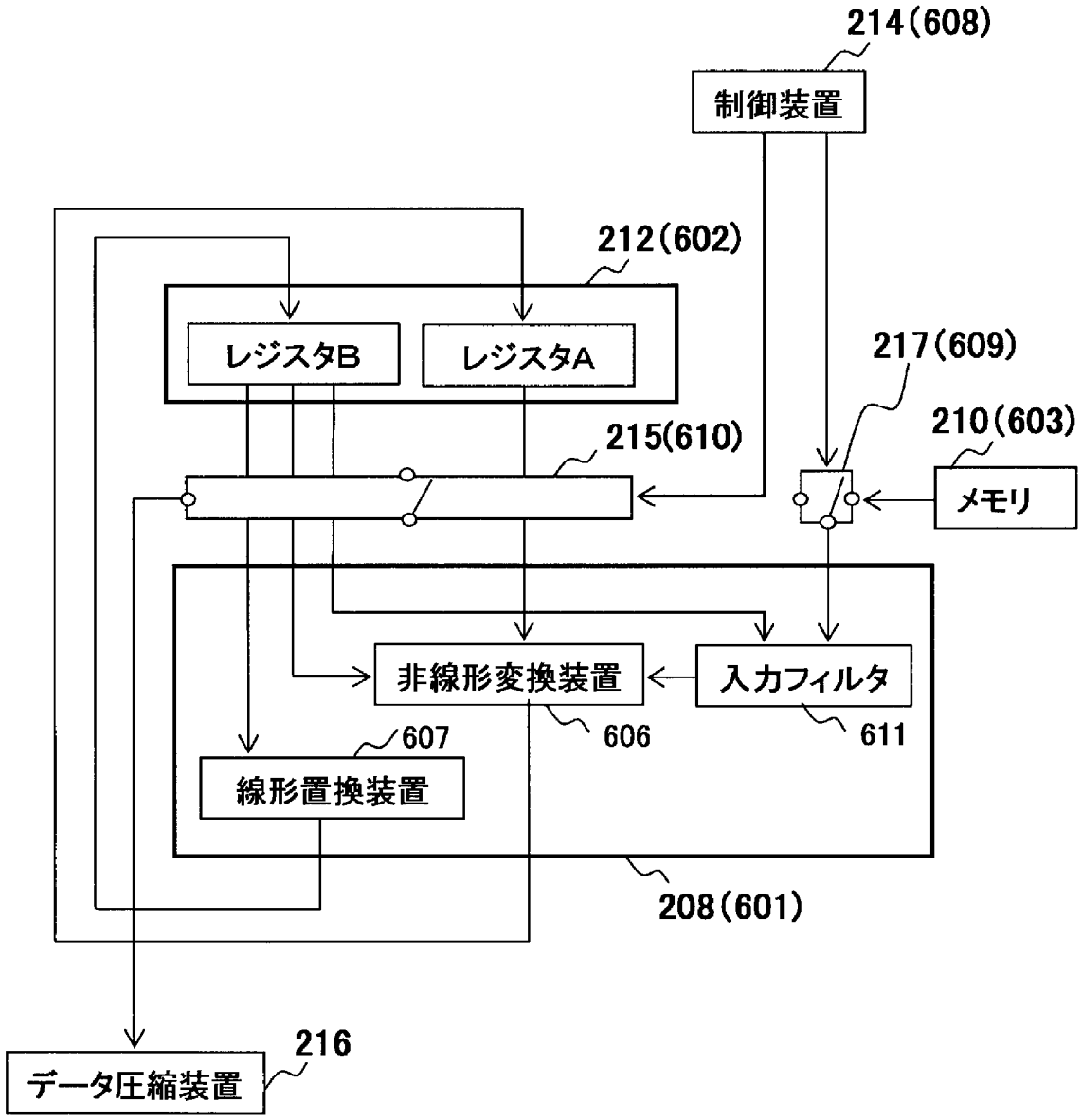
[図7]

図7


605
時刻tのレジスタB
607
B0(t)
B15(t)
604
A0(t)
時刻tの
レジスタA
時刻t+1のレジスタB
605

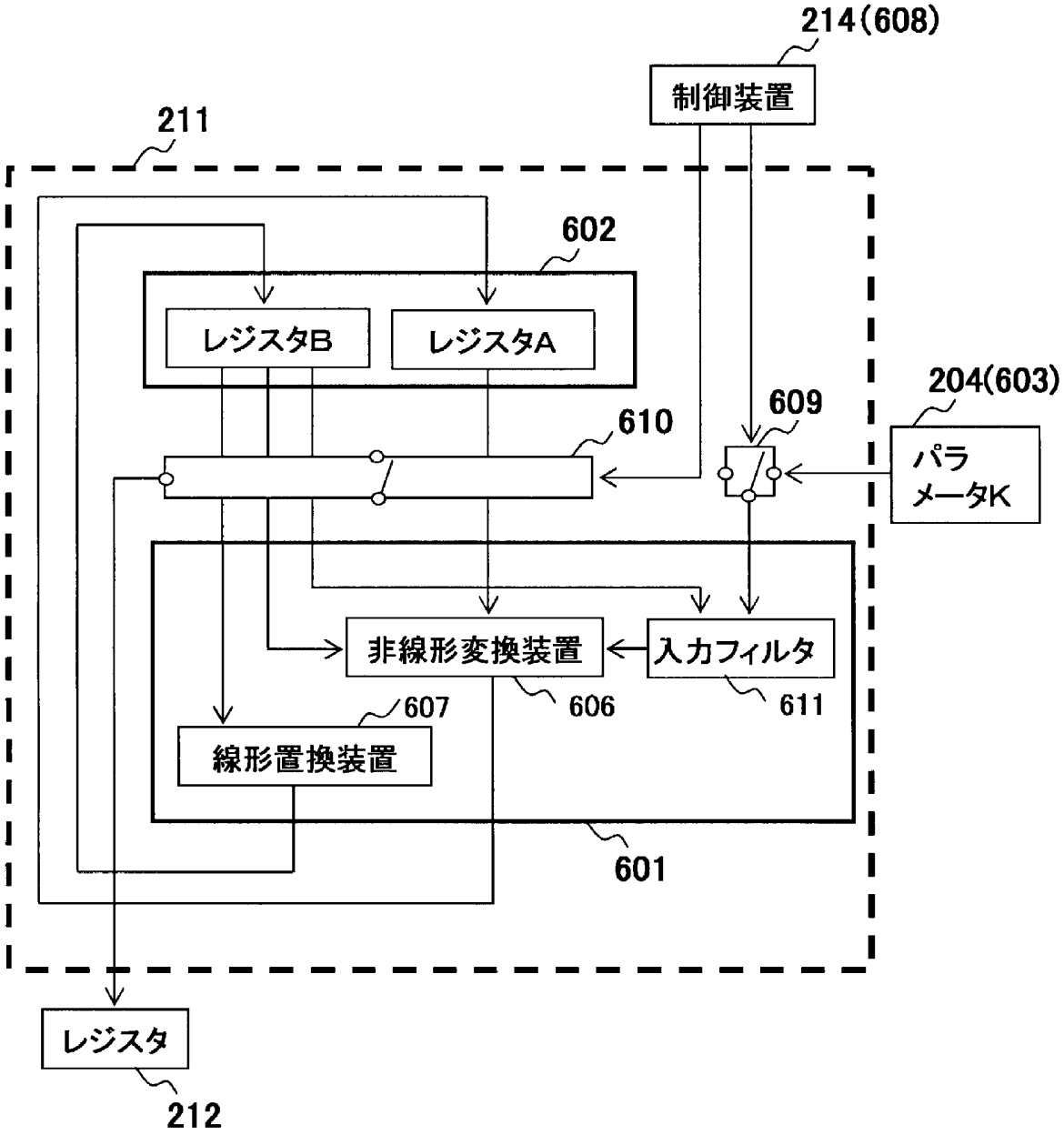
[図8]

図8


214(608)
制御装置
212(602)
レジスタB
レジスタA
217(609)
210(603)
215(610)
メモリ
非線形変換装置
入力フィルタ
606
611
607
線形置換装置
208(601)
216
データ圧縮装置

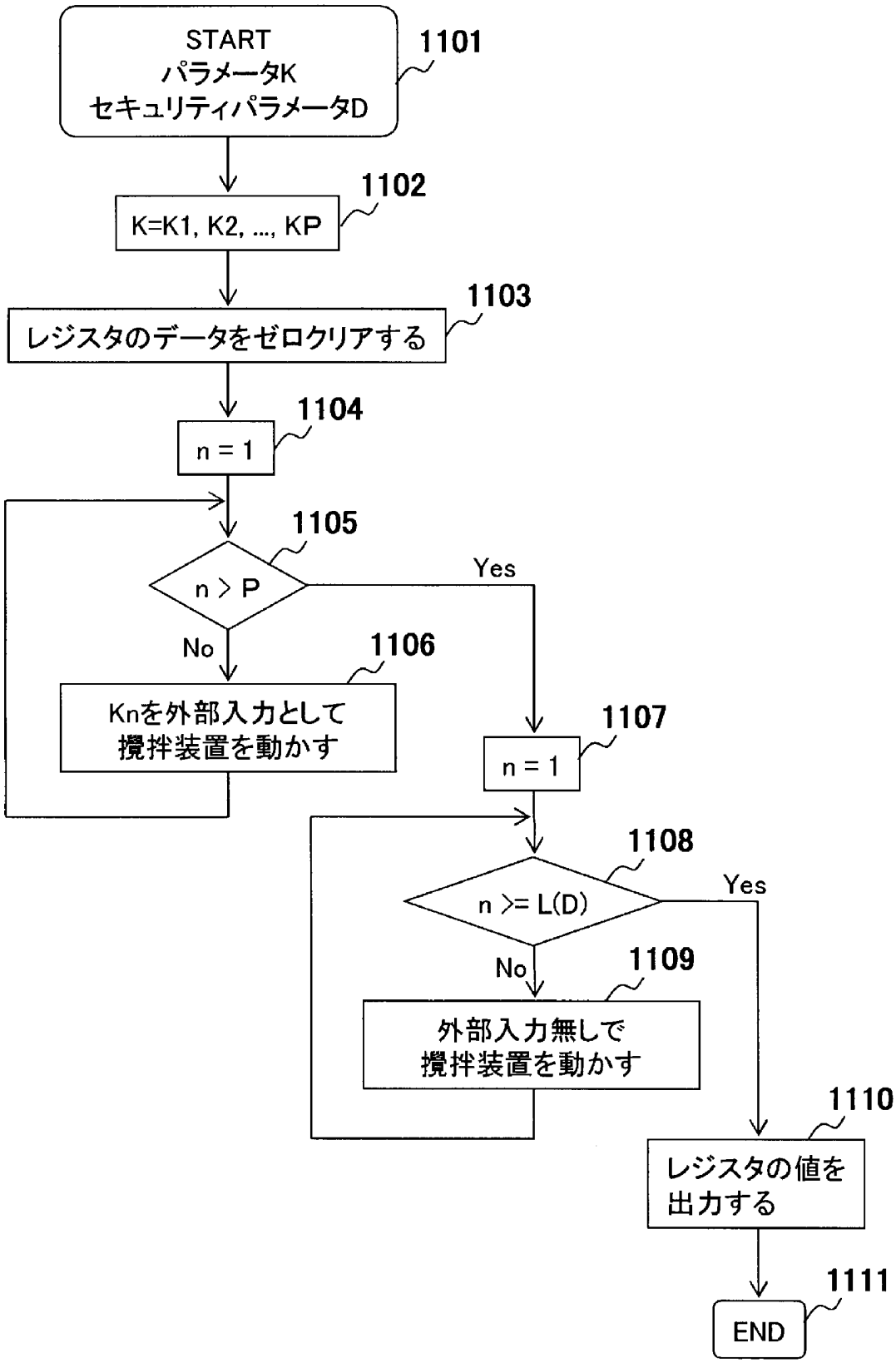
[図9]

図9


214(608)
制御装置
211
602
レジスタB
レジスタA
204(603)
609
610
パラ
メータK
非線形変換装置
入力フィルタ
606
611
607
線形置換装置
601
レジスタ
212

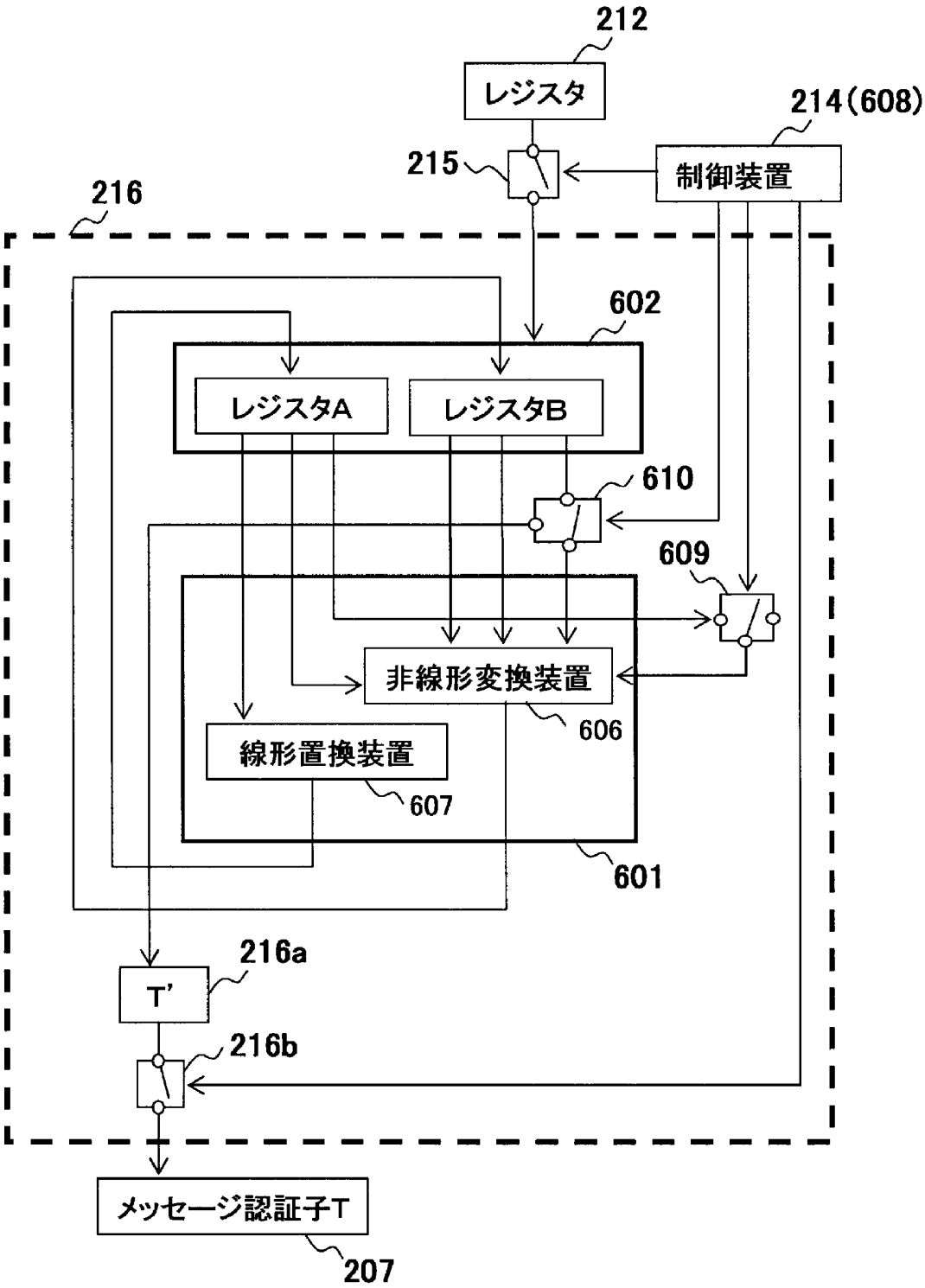
[図10]

図10


START
パラメータK
セキュリティパラメータD
1101
K=K1, K2, ..., KP
1102
レジスタのデータをゼロクリアする
1103
n = 1
1104
n > P
1105
Yes
No
Knを外部入力として
撹拌装置を動かす
1106
n = 1
1107
n >= L(D)
1108
Yes
No
外部入力無しで
撹拌装置を動かす
1109
レジスタの値を
出力する
1110
END
1111

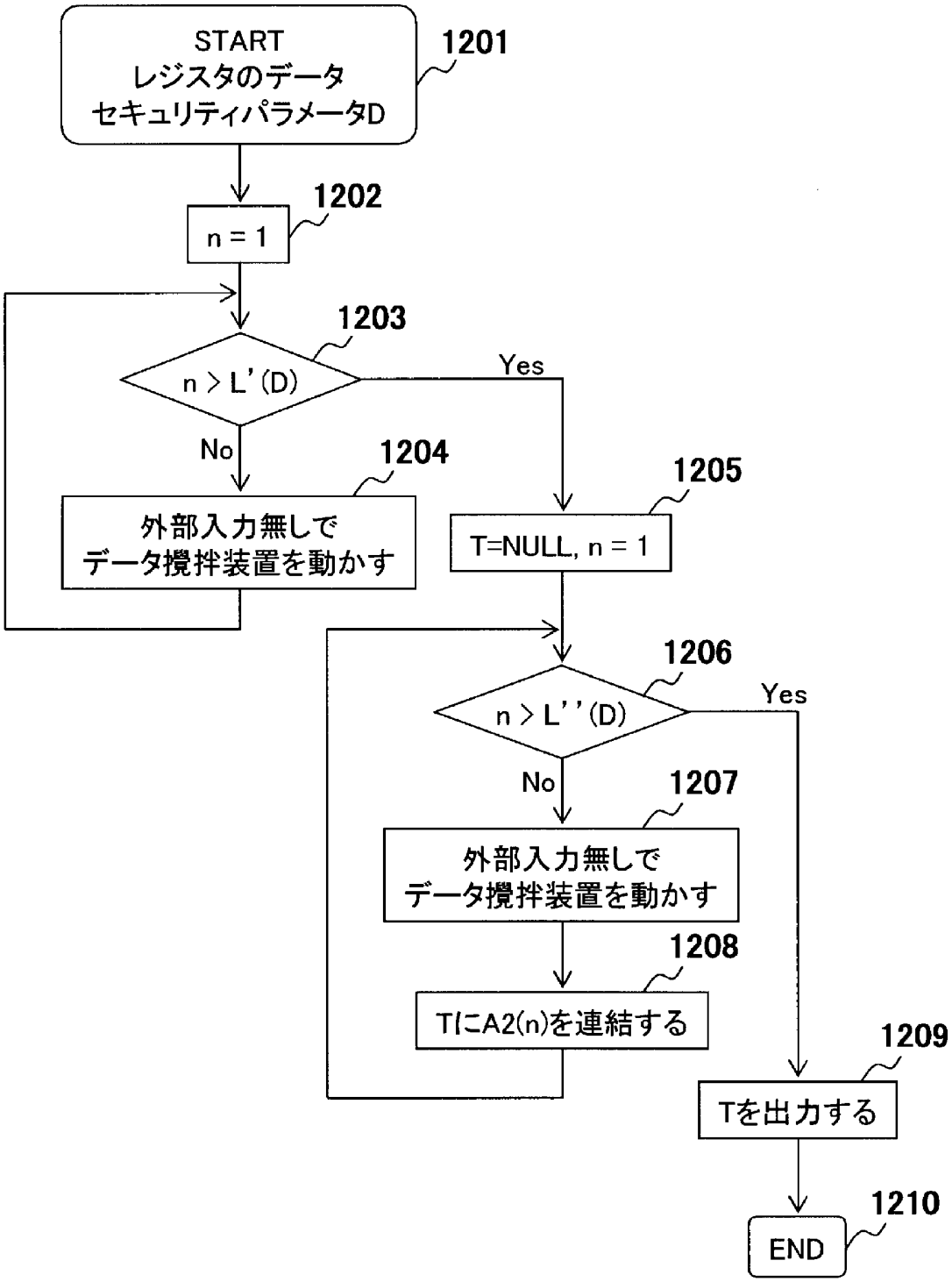
[図11]

図11


212
レジスタ
214(608)
215
制御装置
216
602
レジスタA
レジスタB
610
609
非線形変換装置
606
線形置換装置
607
601
216a
T'
216b
メッセージ認証子T
207

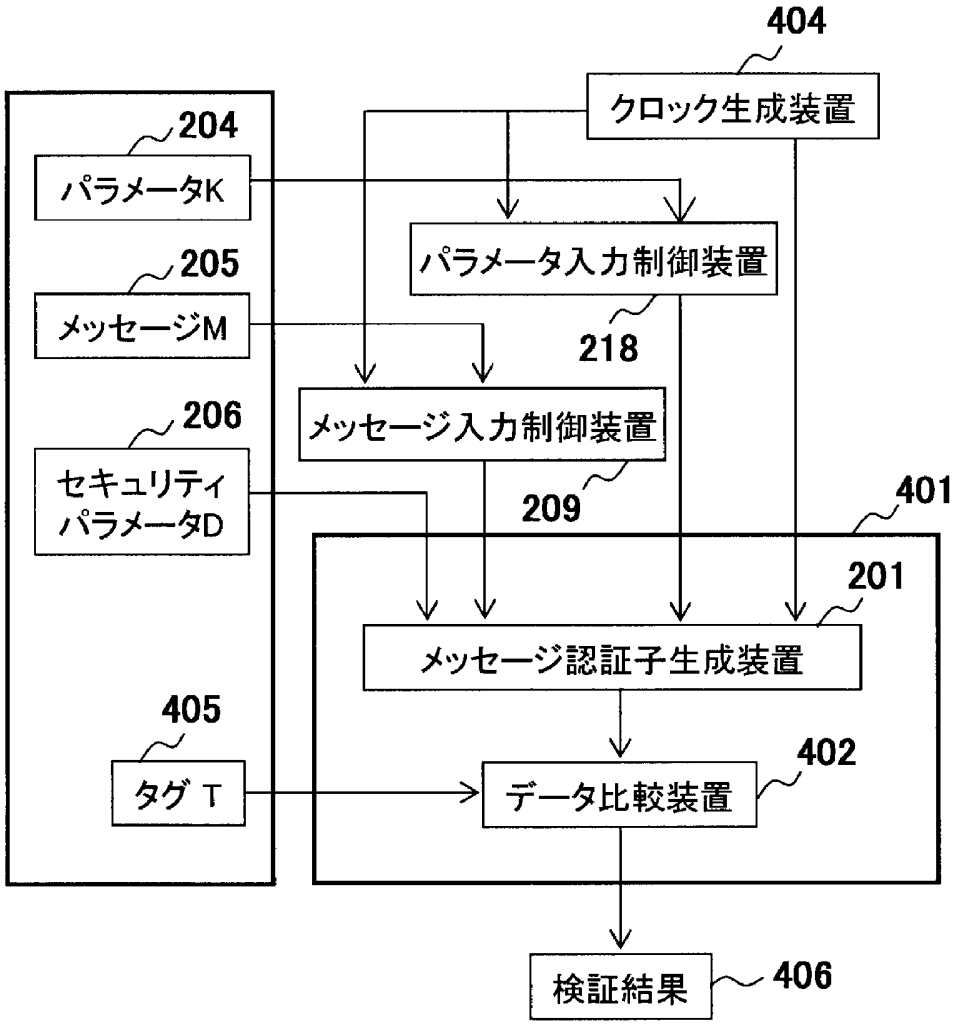
[図12]

図12


START
レジスタのデータ
セキュリティパラメータD
1201
n = 1
1202
n > L'(D)
1203
Yes
No
1204
外部入力無しで
データ撹拌装置を動かす
1205
T=NULL, n = 1
n > L''(D)
1206
Yes
No
1207
外部入力無しで
データ撹拌装置を動かす
1208
TにA2(n)を連結する
1209
Tを出力する
END
1210

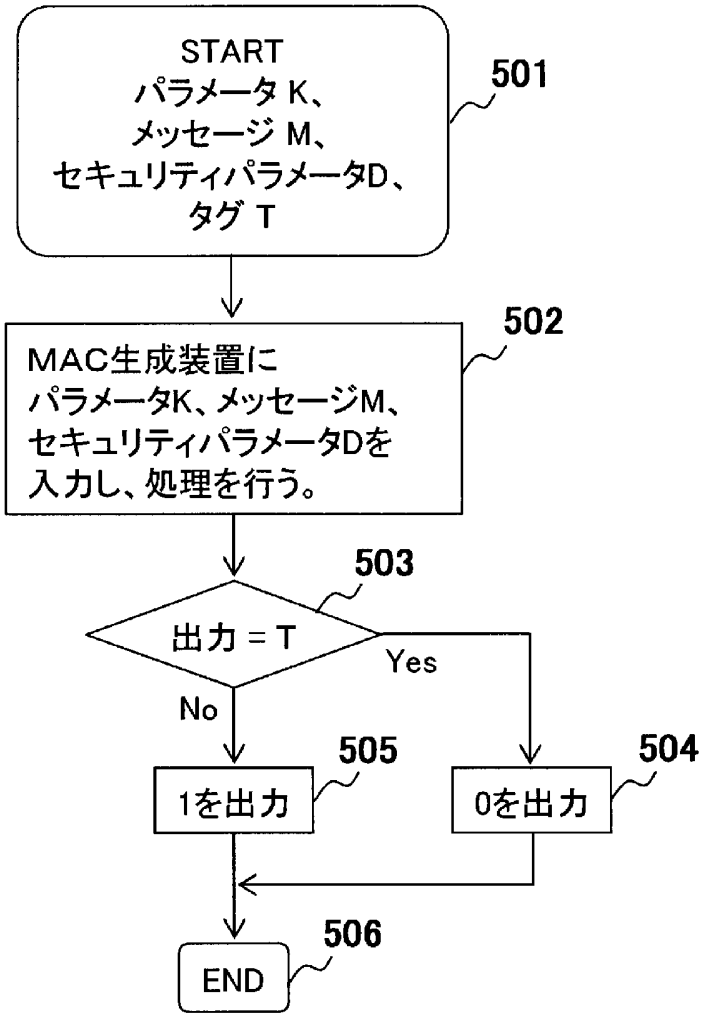
[図13]

図13


404
クロック生成装置
204
パラメータK
205
メッセージM
206
セキュリティ
パラメータD
パラメータ入力制御装置
218
メッセージ入力制御装置
209
401
201
メッセージ認証子生成装置
405
タグ T
402
データ比較装置
検証結果
406

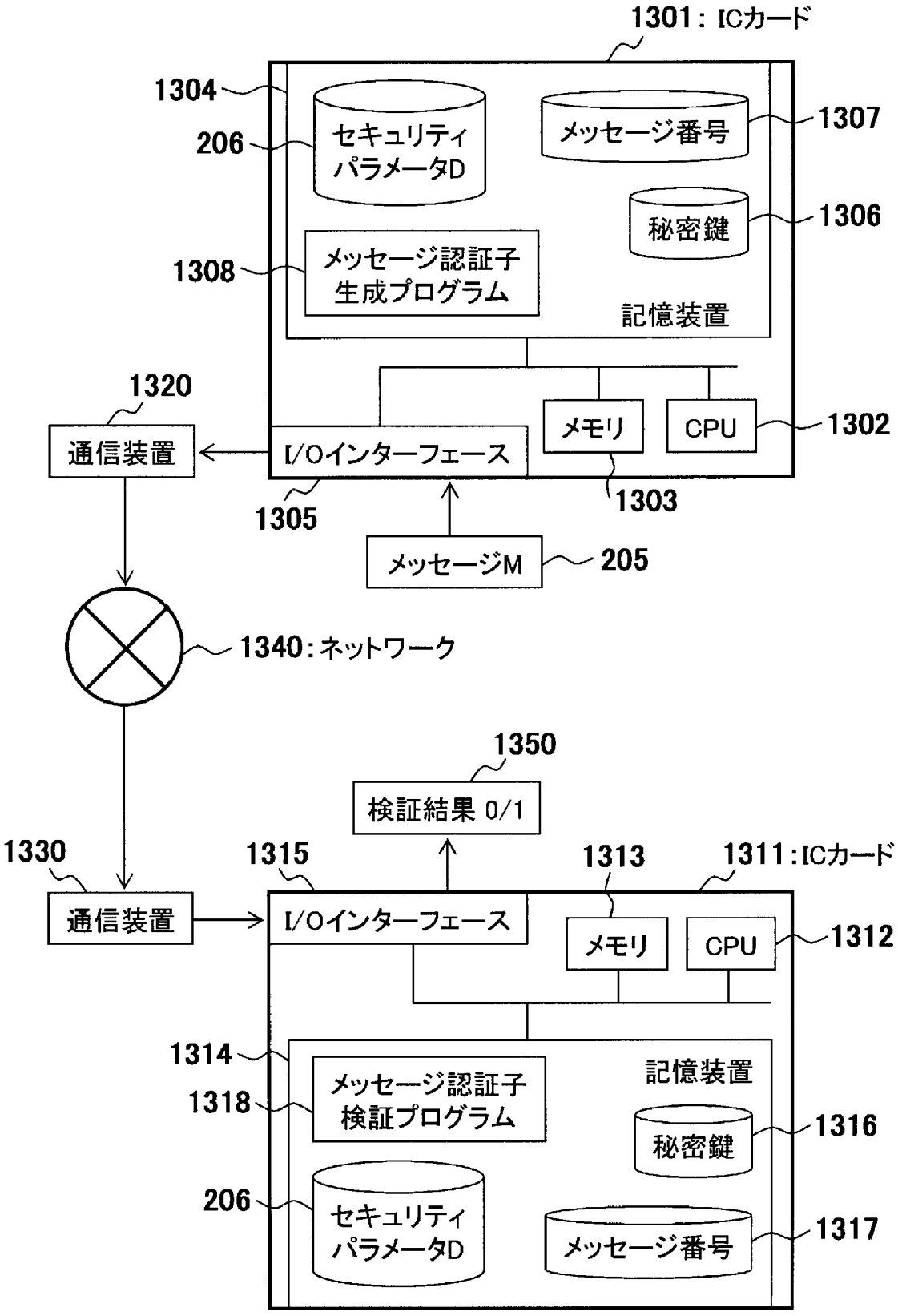
[図14]

図14


START
パラメータ K、
メッセージ M、
セキュリティパラメータD、
タグ T
501
MAC生成装置に
パラメータK、メッセージM、
セキュリティパラメータDを
入力し、処理を行う。
502
出力 = T
503
Yes
No
1を出力
505
0を出力
504
END
506

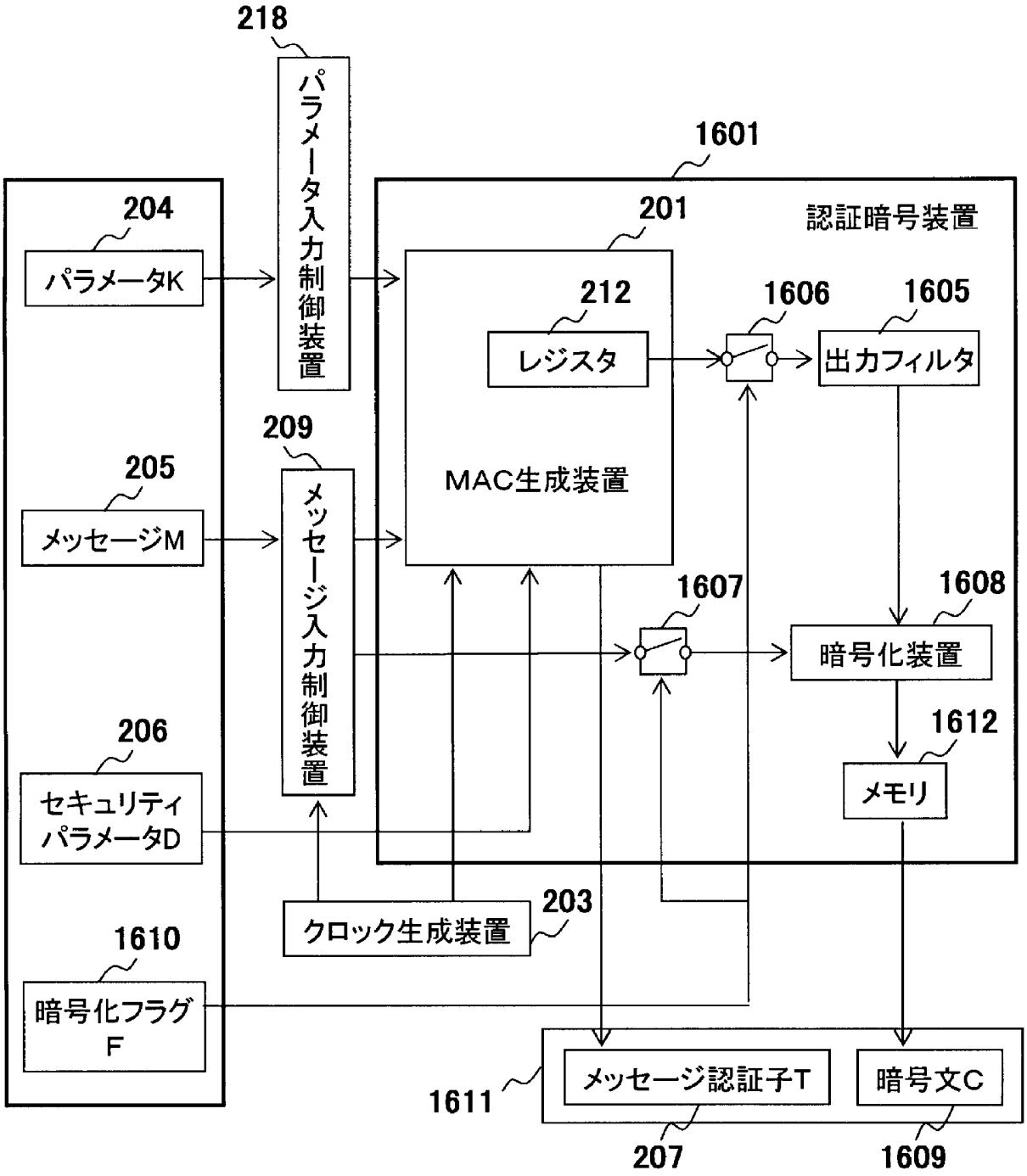
[図15]

図15


1301：ICカード
1304
206
セキュリティ
パラメータD
メッセージ番号
1307
秘密鍵
1306
1308
メッセージ認証子
生成プログラム
記憶装置
1320
通信装置
I/Oインターフェース
メモリ
CPU
1302
1305
1303
メッセージM
205
1340：ネットワーク
1350
検証結果 0/1
1330
1315
1313
1311：ICカード
通信装置
I/Oインターフェース
メモリ
CPU
1312
1314
記憶装置
1318
メッセージ認証子
検証プログラム
秘密鍵
1316
206
セキュリティ
パラメータD
メッセージ番号
1317

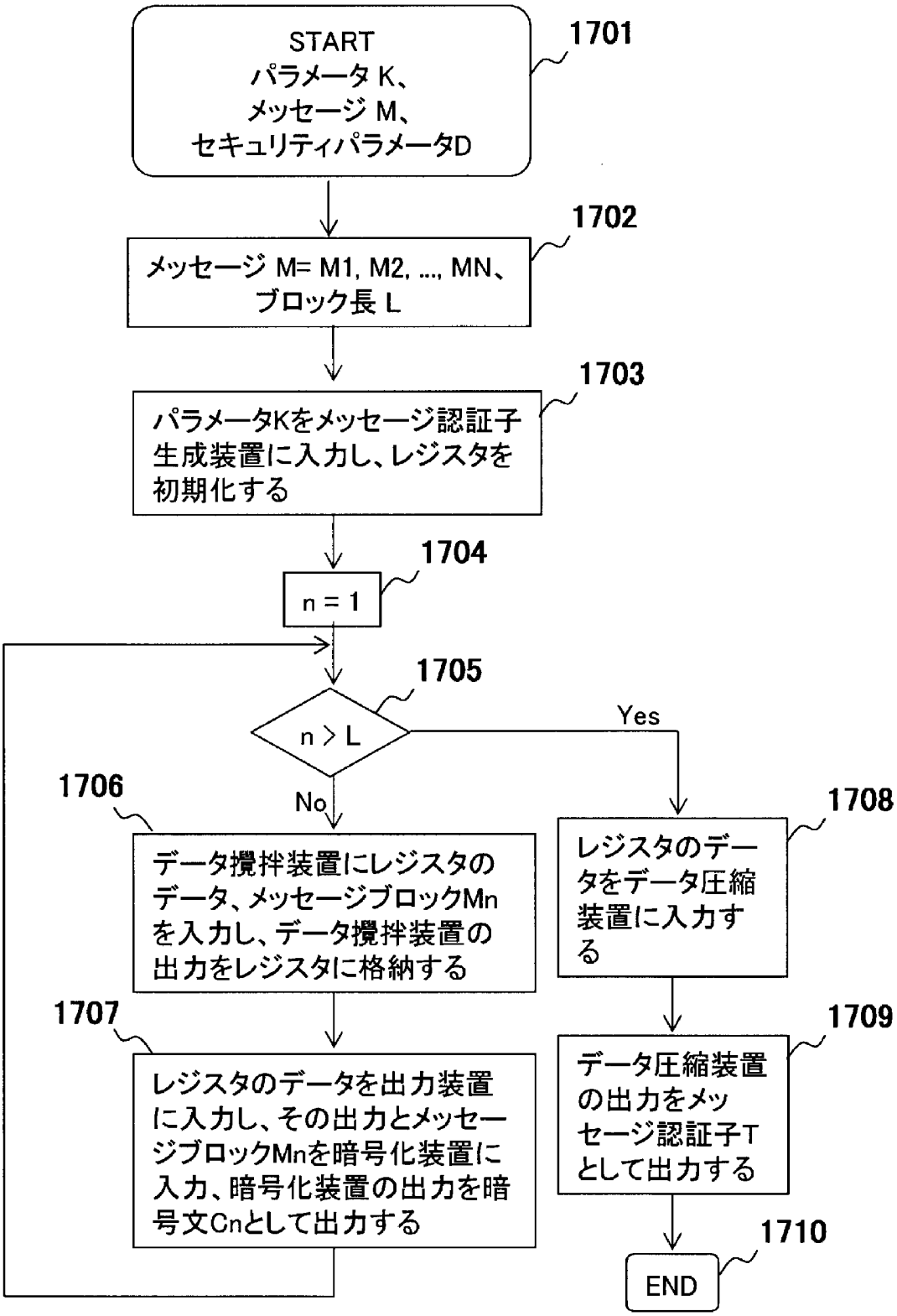
[図16]

図16


218
パラメータ入力制御装置
1601
認証暗号装置
204
パラメータK
201
212
レジスタ
1606
1605
出力フィルタ
MAC生成装置
209
205
メッセージM
メッセージ入力制御装置
1607
1608
暗号化装置
206
セキュリティパラメータD
1612
メモリ
クロック生成装置
203
1610
暗号化フラグF
1611
メッセージ認証子T
暗号文C
207
1609

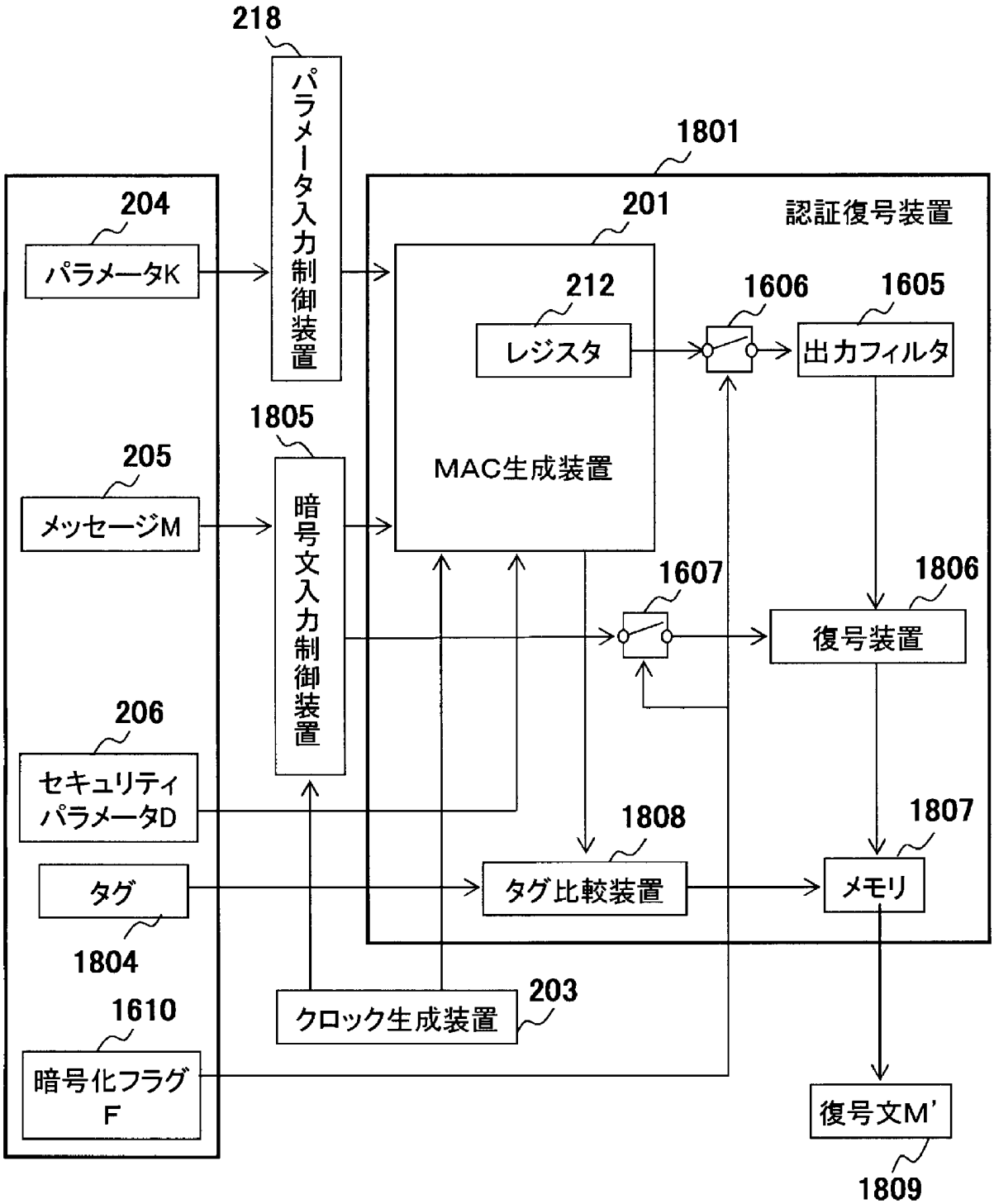
[図17]

図17


START
パラメータ K、
メッセージ M、
セキュリティパラメータD
1701
メッセージ M= M1, M2, ..., MN、
ブロック長 L
1702
パラメータKをメッセージ認証子生成装置に入力し、レジスタを初期化する
1703
n = 1
1704
n > L
1705
Yes
No
1706
データ撹拌装置にレジスタのデータ、メッセージブロックMnを入力し、データ撹拌装置の出力をレジスタに格納する
1707
レジスタのデータを出力装置に入力し、その出力とメッセージブロックMnを暗号化装置に入力、暗号化装置の出力を暗号文Cnとして出力する
1708
レジスタのデータをデータ圧縮装置に入力する
1709
データ圧縮装置の出力をメッセージ認証子Tとして出力する
1710
END

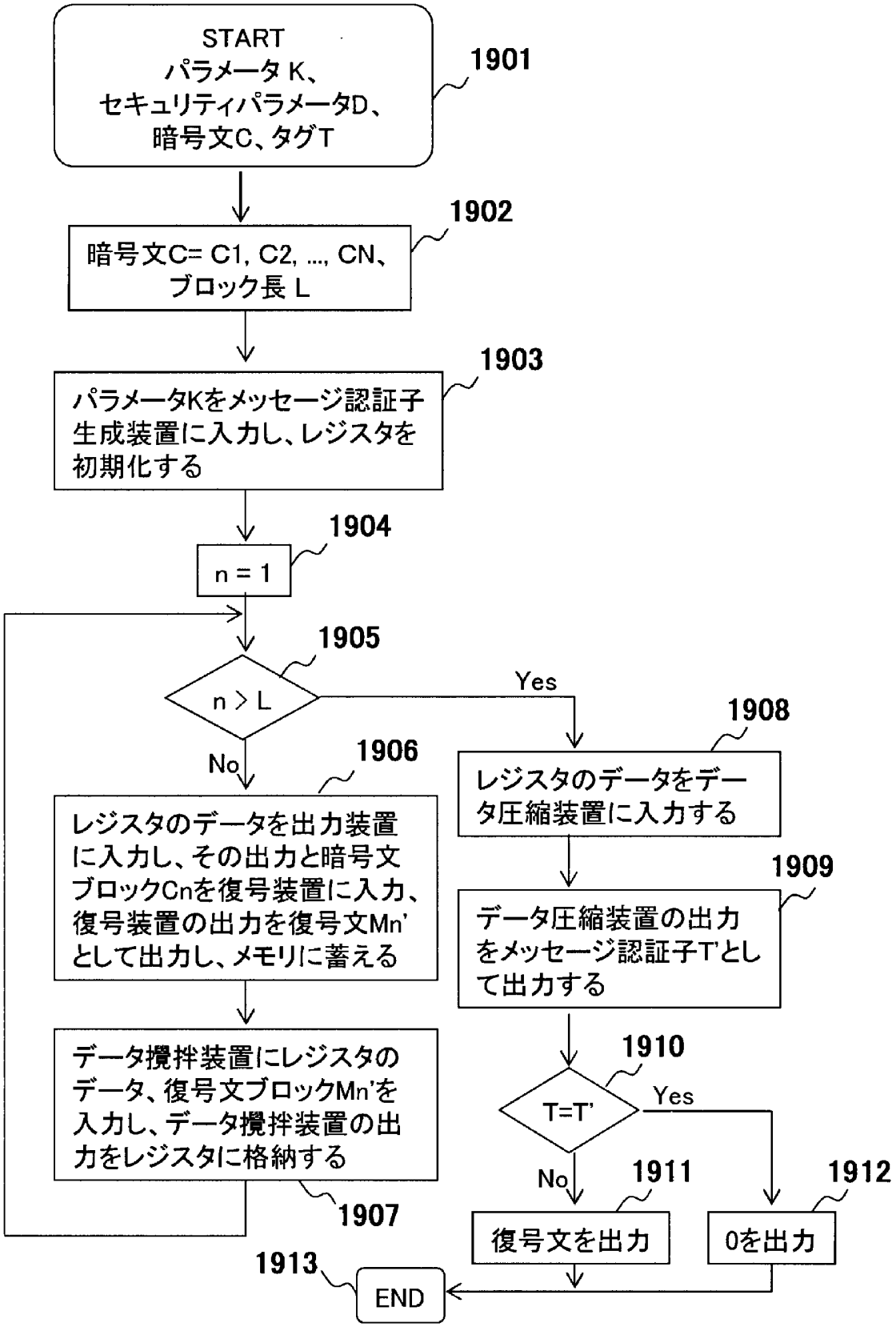
[図18]

図18


218
パラメータ入力制御装置
1801
認証復号装置
204
パラメータK
201
212
レジスタ
1606
1605
出力フィルタ
MAC生成装置
1805
205
メッセージM
暗号文入力制御装置
1607
1806
復号装置
206
セキュリティパラメータD
1808
1807
タグ
タグ比較装置
メモリ
1804
1610
クロック生成装置
203
暗号化フラグF
復号文M'
1809

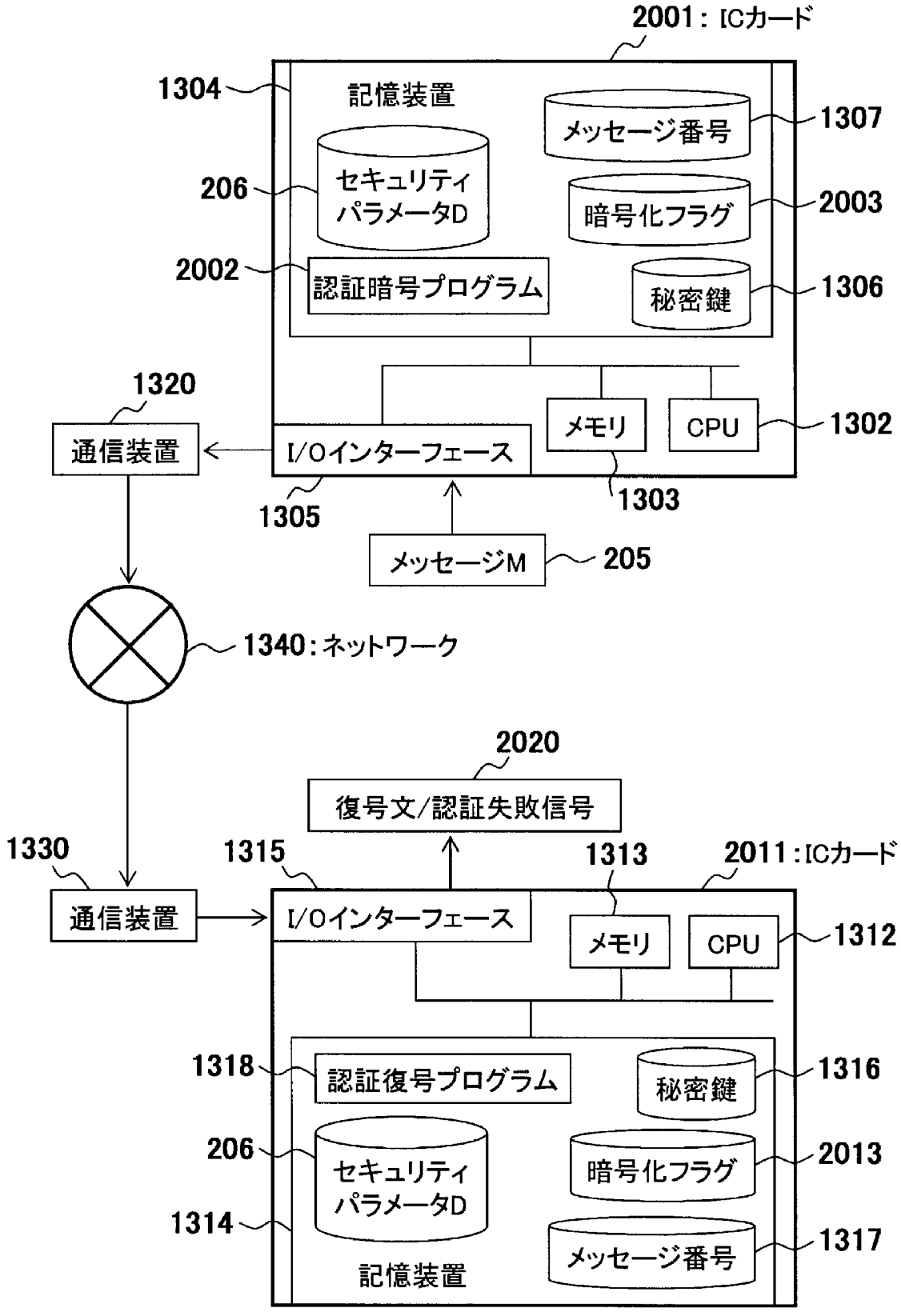
[図19]

図19


START
パラメータK、
セキュリティパラメータD、
暗号文C、タグT
1901
暗号文C= C1, C2, ..., CN、
ブロック長 L
1902
パラメータKをメッセージ認証子生成装置に入力し、レジスタを初期化する
1903
n = 1
1904
n > L
1905
Yes
No
1906
レジスタのデータを出力装置に入力し、その出力と暗号文ブロックCnを復号装置に入力、復号装置の出力を復号文Mn'として出力し、メモリに蓄える
データ攪拌装置にレジスタのデータ、復号文ブロックMn'を入力し、データ攪拌装置の出力をレジスタに格納する
1907
1908
レジスタのデータをデータ圧縮装置に入力する
1909
データ圧縮装置の出力をメッセージ認証子T'として出力する
1910
T=T'
Yes
No
1911
復号文を出力
1912
0を出力
1913
END

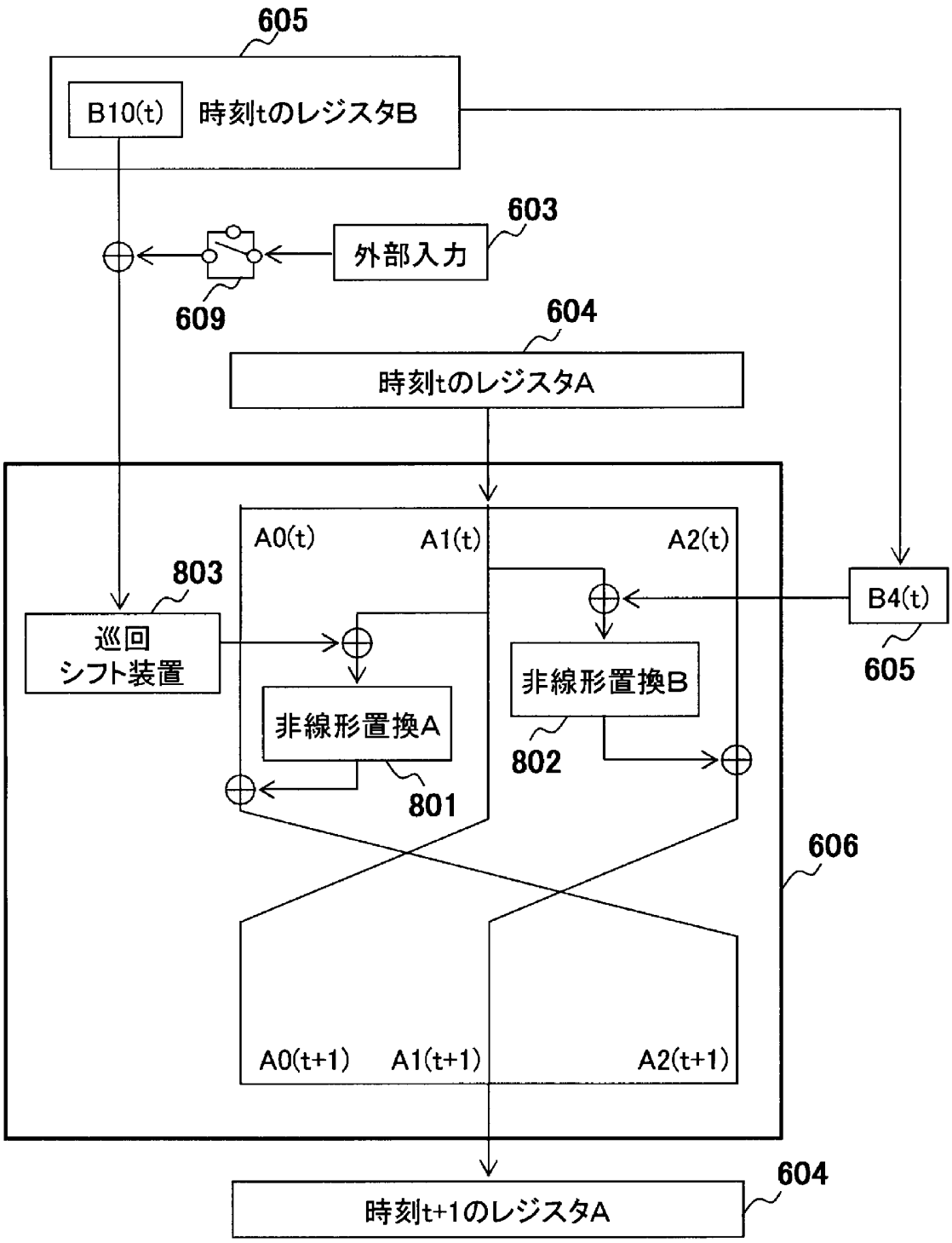
[図20]

図20


2001 : ICカード
1304
記憶装置
メッセージ番号
1307
206
セキュリティ
パラメータD
暗号化フラグ
2003
2002
認証暗号プログラム
秘密鍵
1306
1320
通信装置
I/Oインターフェース
メモリ
CPU
1302
1305
1303
メッセージM
205
1340 : ネットワーク
2020
復号文/認証失敗信号
1330
1315
1313
2011 : ICカード
通信装置
I/Oインターフェース
メモリ
CPU
1312
1318
認証復号プログラム
秘密鍵
1316
206
セキュリティ
パラメータD
暗号化フラグ
2013
1314
メッセージ番号
1317
記憶装置

[図21]

図21


605
B10(t)
時刻tのレジスタB
603
外部入力
609
604
時刻tのレジスタA
A0(t)
A1(t)
A2(t)
803
巡回
シフト装置
非線形置換A
801
非線形置換B
802
B4(t)
605
606
A0(t+1)
A1(t+1)
A2(t+1)
604
時刻t+1のレジスタA

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/015124

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/32(2006.01), ***H04L9/26***(2006.01)

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(2006.01), ***H04L9/26***(2006.01)

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	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JST-PLUS, Stream Cipher

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Helix:Fast Encryption and Authentication in a Single Cryptographic Primitive, Lecture Notes in Computer Science, 2003, Vol.2887, pages 330 to 346, especially 3 Definition of Helix	1,9-15 2-8
Y	A New Keystream Generator MUGI, Lecture Notes in Computer Science, 2002, Vol.2365, pages 179 to 194, especially 3 Specification of MUGI	2-8

☐ 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	Date of mailing of the international search report
13 December, 2005 (13.12.05)	27 December, 2005 (27.12.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０１５１２４

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), ***H04L9/26*** (2006.01)

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*** (2006.01), ***H04L9/26*** (2006.01)

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	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５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）

JST-PLUS
Stream Cipher

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
X	Helix:Fast Encryption and Authentication in a Single Cryptographic Primitive, Lecture Notes in Computer Science, 2003, Vol.2887, p.330-346,	1,9-15
Y	especially 3 Definition of Helix	2-8
Y	A New Keystream Generator MUGI, Lecture Notes in Computer Science, 2002, Vol.2365, p.179-194, especially 3 Specification of MUGI	2-8

☐　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 １３．１２．２００５	国際調査報告の発送日 ２７．１２．２００５
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　９３６４ 中里　裕正 電話番号　０３－３５８１－１１０１　内線　３５４６