(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7367860号
(P7367860)

(45)発行日　令和5年10月24日(2023.10.24)

(24)登録日　令和5年10月16日(2023.10.16)

(51)国際特許分類

		FI		
G09C	*1/00 (2006.01)*	G09C	1/00	610A
H04L	*9/32 (2006.01)*	H04L	9/32	200A

請求項の数　25　（全32頁）

(21)出願番号　特願2022-516562(P2022-516562)
(86)(22)出願日　令和2年4月23日(2020.4.23)
(86)国際出願番号　PCT/JP2020/017422
(87)国際公開番号　WO2021/214923
(87)国際公開日　令和3年10月28日(2021.10.28)
審査請求日　令和4年10月19日(2022.10.19)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103894
弁理士　家入 健
(72)発明者　峯松 一彦
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　向井 明子
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　本間 尚文
宮城県仙台市青葉区片平二丁目１番１号 国立大学法人東北大学内
(72)発明者　上野 嶺

最終頁に続く

(54)【発明の名称】　認証暗号化装置、認証復号装置、認証暗号システム、方法及びプログラム

(57)【特許請求の範囲】

【請求項１】

平文の入力を受け付ける入力手段と、

過去に生成された値とは異なるナンスを生成するナンス生成手段と、

前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成する平文暗号化手段と、

前記平文を用いてチェックサムを生成するチェックサム生成手段と、

ハッシュ値を取得するハッシュ手段と、

前記ナンスを暗号化して暗号化ナンスを取得するナンス暗号化手段と、

前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成する認証タグ生成手段と、

前記暗号文及び前記認証タグを出力するための制御を行う出力手段と、

を有する認証暗号化装置。

【請求項２】

前記認証タグ生成手段は、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとの和に基づいて、前記認証タグを生成する、

請求項１に記載の認証暗号化装置。

【請求項３】

前記認証タグ生成手段は、前記和を短縮することによって、前記認証タグを生成する、

請求項２に記載の認証暗号化装置。

【請求項４】
前記ナンス暗号化手段は、前記チェックサムと同じ長さの前記暗号化ナンスを取得する、
請求項１から３のいずれか１項に記載の認証暗号化装置。
【請求項５】
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダとハッシュ関数とを用いて、前記ハッシュ値を取得する、
請求項１から４のいずれか１項に記載の認証暗号化装置。
【請求項６】
前記平文暗号化手段は、前記平文を所定長のブロックに分割した際のブロックのｉ番目の平文ブロックに対して、前記ナンスと前記平文ブロックのインデックスｉとを含めた前記補助変数であるＴｗｅａｋを用いて、前記平文を前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化する、
請求項１から５のいずれか１項に記載の認証暗号化装置。
【請求項７】
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダを所定長のブロックに分割した際のブロックのｉ番目のヘッダブロックに対して、前記ヘッダブロックのインデックスｉを含めた前記補助変数であるＴｗｅａｋを用いて、前記ヘッダを前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化することで、前記ハッシュ値を取得する、
請求項６に記載の認証暗号化装置。
【請求項８】
前記ハッシュ手段は、前記ヘッダを暗号化したブロックを加算することで、前記ハッシュ値を取得する、
請求項７に記載の認証暗号化装置。
【請求項９】
前記ナンス暗号化手段は、前記ナンスを含めた前記補助変数であるＴｗｅａｋを用いて、Ｔｗｅａｋａｂｌｅブロック暗号で暗号化を行うことによって、前記暗号化ナンスを取得する、
請求項６から８のいずれか１項に記載の認証暗号化装置。
【請求項１０】
前記Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードである、
請求項６から９のいずれか１項に記載の認証暗号化装置。
【請求項１１】
暗号文、認証タグ及びナンスの入力を受け付ける入力手段と、
前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成する平文復号手段と、
前記平文を用いてチェックサムを生成するチェックサム生成手段と、
ハッシュ値を取得するハッシュ手段と、
前記ナンスを暗号化して暗号化ナンスを取得するナンス暗号化手段と、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成する検証用タグ生成手段と、
前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う検証手段と、
を有する認証復号装置。
【請求項１２】
前記検証用タグ生成手段は、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとの和に基づいて、前記検証用タグを生成する、
請求項１１に記載の認証復号装置。
【請求項１３】

前記検証用タグ生成手段は、前記和を短縮することによって、前記検証用タグを生成する、
請求項１２に記載の認証復号装置。
【請求項１４】
前記ナンス暗号化手段は、前記チェックサムと同じ長さの前記暗号化ナンスを取得する、
請求項１１から１３のいずれか１項に記載の認証復号装置。
【請求項１５】
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダとハッシュ関数とを用いて、前記ハッシュ値を取得する、
請求項１１から１４のいずれか１項に記載の認証復号装置。
【請求項１６】
前記平文復号手段は、前記暗号文を所定長のブロックに分割した際のブロックのｉ番目の暗号文ブロックに対して、前記ナンスと前記暗号文ブロックのインデックスｉとを含めた前記補助変数であるＴｗｅａｋを用いて、前記暗号文を前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で復号する、
請求項１１から１５のいずれか１項に記載の認証復号装置。
【請求項１７】
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダを所定長のブロックに分割した際のブロックのｉ番目のヘッダブロックに対して、前記ヘッダブロックのインデックスｉを含めた前記補助変数であるＴｗｅａｋを用いて、前記ヘッダを前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化することで、前記ハッシュ値を取得する、
請求項１６に記載の認証復号装置。
【請求項１８】
前記ハッシュ手段は、前記ヘッダを暗号化したブロックを加算することで、前記ハッシュ値を取得する、
請求項１７に記載の認証復号装置。
【請求項１９】
前記ナンス暗号化手段は、前記ナンスを含めた前記補助変数であるＴｗｅａｋを用いて、Ｔｗｅａｋａｂｌｅブロック暗号で暗号化を行うことによって、前記暗号化ナンスを取得する、
請求項１６から１８のいずれか１項に記載の認証復号装置。
【請求項２０】
前記Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードである、
請求項１６から１９のいずれか１項に記載の認証復号装置。
【請求項２１】
認証暗号化装置と、
前記認証暗号化装置との間で通信を行う認証復号装置と、
を有し、
前記認証暗号化装置は、
平文の入力を受け付ける第１の入力手段と、
過去に生成された値とは異なるナンスを生成するナンス生成手段と、
前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成する平文暗号化手段と、
前記平文を用いてチェックサムを生成する第１のチェックサム生成手段と、
ハッシュ値を取得する第１のハッシュ手段と、
前記ナンスを暗号化して暗号化ナンスを取得する第１のナンス暗号化手段と、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成する認証タグ生成手段と、

前記暗号文及び前記認証タグを出力するための制御を行う出力手段と、
を有し、
前記認証復号装置は、
暗号文、認証タグ及びナンスの入力を受け付ける第２の入力手段と、
前記第２の入力手段によって入力された前記暗号文を分割したブロックごとに、前記第２の入力手段によって入力された前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成する平文復号手段と、
前記平文復号手段によって生成された前記平文を用いてチェックサムを生成する第２のチェックサム生成手段と、
ハッシュ値を取得する第２のハッシュ手段と、
前記第２の入力手段によって入力された前記ナンスを暗号化して暗号化ナンスを取得する第２のナンス暗号化手段と、
前記第２のチェックサム生成手段によって生成された前記チェックサムと、前記第２のハッシュ手段によって取得された前記ハッシュ値と、前記第２のナンス暗号化手段によって取得された前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成する検証用タグ生成手段と、
前記認証タグ生成手段によって生成された前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う検証手段と、
を有する、
認証暗号システム。
【請求項２２】
平文の入力を受け付け、
過去に生成された値とは異なるナンスを生成し、
前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成し、
前記平文を用いてチェックサムを生成し、
ハッシュ値を取得し、
前記ナンスを暗号化して暗号化ナンスを取得し、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成し、
前記暗号文及び前記認証タグを出力するための制御を行う、
認証暗号化方法。
【請求項２３】
暗号文、認証タグ及びナンスの入力を受け付け、
前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成し、
前記平文を用いてチェックサムを生成し、
ハッシュ値を取得し、
前記ナンスを暗号化して暗号化ナンスを取得し、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成し、
前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う、
認証復号方法。
【請求項２４】
平文の入力を受け付けるステップと、
過去に生成された値とは異なるナンスを生成するステップと、
前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成するステップと、
前記平文を用いてチェックサムを生成するステップと、
ハッシュ値を取得するステップと、

前記ナンスを暗号化して暗号化ナンスを取得するステップと、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成し、
前記暗号文及び前記認証タグを出力するための制御を行うステップと、
をコンピュータに実行させるプログラム。
【請求項２５】
暗号文、認証タグ及びナンスの入力を受け付けるステップと、
前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成するステップと、
前記平文を用いてチェックサムを生成するステップと、
ハッシュ値を取得するステップと、
前記ナンスを暗号化して暗号化ナンスを取得するステップと、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成するステップと、
前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行うステップと、
をコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証暗号化装置、認証復号装置、認証暗号システム、方法及びプログラムに関する。
【背景技術】
【０００２】
事前に共有された秘密鍵を用いて、平文メッセージに対して暗号化と改ざん検知用の認証タグ計算とを同時に適用する認証暗号（Authenticated Encryption；ＡＥ）という技術が知られている。通信路に認証暗号ＡＥを適用することにより、盗聴に対する内容の秘匿と、不正な改ざんに対する検知とが可能となり、結果として通信内容に対する強力な保護が実現される。認証暗号技術としては、例えば、非特許文献１に開示された技術が知られている。
【０００３】
また、このような認証暗号を効率的に行う技術の１つとして、例えば、特許文献１及び非特許文献２に示すようなＯＣＢ（Offset Code Book）モードと呼ばれる認証暗号方式が知られている。ＯＣＢモードは、暗号化と復号の際に、Ｔｗｅａｋ（トウィーク）と呼ばれる補助変数（調整値）を導入するＴｗｅａｋａｂｌｅブロック暗号と呼ばれるブロック暗号を拡張したものである。具体的には、ＯＣＢモードでは、非特許文献２に記載されているＸＥＸモードによる暗号化を行うことで、Ｔｗｅａｋを用いた暗号化を行っている。また、ＯＣＢモードでは、平文を分割した各ブロックの排他的論理和に上記暗号化を行う際と同様の処理を行うことでタグを生成している。
【０００４】
また、非特許文献３は、非特許文献２に記載されたバージョンのＯＣＢへ修正を施したバージョンであるＯＣＢ２ｆに関する方式を開示している。また、非特許文献４は、ブロック暗号の拡張であるＴｗｅａｋａｂｌｅブロック暗号（Tweakable block cipher；ＴＢＣ；可撚ブロック暗号）をプリミティブとして用いてＯＣＢを抽象化したΘＣＢ３（以下ＴｈｅｔａＣＢ３）方式を開示している。
【先行技術文献】
【特許文献】
【０００５】
【文献】米国特許第８３２１６７５号明細書
【非特許文献】
【０００６】

【文献】NIST Special Publication 800-38D、"Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC"、http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
"Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC"、Phillip Rogaway、ASIACRYPT 2004、http://web.cs.ucdavis.edu/~rogaway/papers/offsets.pdf
【文献】Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, Bertram Poettering、"Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality"、IACR Cryptology ePrint Archive 2019: 311 (2019)
Ted Krovetz, Phillip Rogaway、"The Software Performance of Authenticated-Encryption Modes"、FSE 2011: 306-327
Christof Beierle, Jeremy Jean, Stefan Kolbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, Siang Meng Sim、"The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS"、CRYPTO (2) 2016: 123-153
Daniel J. Bernstein、"The Poly1305-AES Message-Authentication Code"、FSE 2005: 32-49

【発明の概要】
【発明が解決しようとする課題】
【０００７】
認証暗号を含む一般の暗号化方式について、遅延という評価指標がある。これは処理を開始してから最初の出力結果が出るまでの時間を指すものであり、小さいほうが望ましい。一方、上述した特許文献及び非特許文献にかかる技術では、暗号化及び復号における遅延を抑制することは困難である。
【０００８】
本開示の目的は、このような課題を解決するためになされたものであり、暗号化及び復号における遅延を抑制することが可能な認証暗号化装置、認証復号装置、認証暗号システム、方法及びプログラムを提供することにある。
【課題を解決するための手段】
【０００９】
本開示にかかる認証暗号化装置は、平文の入力を受け付ける入力手段と、過去に生成された値とは異なるナンスを生成するナンス生成手段と、前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成する平文暗号化手段と、前記平文を用いてチェックサムを生成するチェックサム生成手段と、ハッシュ値を取得するハッシュ手段と、前記ナンスを暗号化して暗号化ナンスを取得するナンス暗号化手段と、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成する認証タグ生成手段と、前記暗号文及び前記認証タグを出力するための制御を行う出力手段と、有する。
【００１０】
また、本開示にかかる認証復号装置は、暗号文、認証タグ及びナンスの入力を受け付ける入力手段と、前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成する平文復号手段と、前記平文を用いてチェックサムを生成するチェックサム生成手段と、ハッシュ値を取得するハッシュ手段と、前記ナンスを暗号化して暗号化ナンスを取得するナンス暗号化手段と、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成する検証用タグ生成手段と、前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う検証手段と、を有する。
【００１１】
また、本開示にかかる認証暗号システムは、認証暗号化装置と、前記認証暗号化装置と

の間で通信を行う認証復号装置と、を有し、前記認証暗号化装置は、平文の入力を受け付ける第１の入力手段と、過去に生成された値とは異なるナンスを生成するナンス生成手段と、前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成する平文暗号化手段と、前記平文を用いてチェックサムを生成する第１のチェックサム生成手段と、ハッシュ値を取得する第１のハッシュ手段と、前記ナンスを暗号化して暗号化ナンスを取得する第１のナンス暗号化手段と、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成する認証タグ生成手段と、前記暗号文及び前記認証タグを出力するための制御を行う出力手段と、を有し、前記認証復号装置は、暗号文、認証タグ及びナンスの入力を受け付ける第２の入力手段と、前記第２の入力手段によって入力された前記暗号文を分割したブロックごとに、前記第２の入力手段によって入力された前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成する平文復号手段と、前記平文復号手段によって生成された前記平文を用いてチェックサムを生成する第２のチェックサム生成手段と、ハッシュ値を取得する第２のハッシュ手段と、前記第２の入力手段によって入力された前記ナンスを暗号化して暗号化ナンスを取得する第２のナンス暗号化手段と、前記第２のチェックサム生成手段によって生成された前記チェックサムと、前記第２のハッシュ手段によって取得された前記ハッシュ値と、前記第２のナンス暗号化手段によって取得された前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成する検証用タグ生成手段と、前記認証タグ生成手段によって生成された前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う検証手段と、を有する。

【００１２】

また、本開示にかかる認証暗号化方法は、平文の入力を受け付け、過去に生成された値とは異なるナンスを生成し、前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成し、前記平文を用いてチェックサムを生成し、ハッシュ値を取得し、前記ナンスを暗号化して暗号化ナンスを取得し、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成し、前記暗号文及び前記認証タグを出力するための制御を行う。

【００１３】

また、本開示にかかる認証復号方法は、暗号文、認証タグ及びナンスの入力を受け付け、前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成し、前記平文を用いてチェックサムを生成し、ハッシュ値を取得し、前記ナンスを暗号化して暗号化ナンスを取得し、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成し、前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う。

【００１４】

また、本開示にかかるプログラムは、平文の入力を受け付けるステップと、過去に生成された値とは異なるナンスを生成するステップと、前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成するステップと、前記平文を用いてチェックサムを生成するステップと、ハッシュ値を取得するステップと、前記ナンスを暗号化して暗号化ナンスを取得するステップと、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成し、前記暗号文及び前記認証タグを出力するための制御を行うステップと、をコンピュータに実行させる。

【００１５】

また、本開示にかかるプログラムは、暗号文、認証タグ及びナンスの入力を受け付けるステップと、前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成するステップと、前記平文を用いてチェックサムを生成するステップと、ハッシュ値を取得するステップと、前記ナンスを暗号

化して暗号化ナンスを取得するステップと、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成するステップと、前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行うステップと、をコンピュータに実行させる。

【発明の効果】

【００１６】

本開示によれば、暗号化及び復号における遅延を抑制することが可能な認証暗号化装置、認証復号装置、認証暗号システム、方法及びプログラムを提供できる。

【図面の簡単な説明】

【００１７】

【図１】実施の形態１にかかる認証暗号システムの構成を示す図である。

【図２】実施の形態１にかかる認証暗号化装置の構成を示す図である。

【図３】実施の形態１にかかる認証復号装置の構成を示す図である。

【図４】実施の形態１にかかる認証暗号化装置で実行される認証暗号化方法を示すフローチャートである。

【図５】実施の形態１にかかる認証復号装置で実行される認証復号方法を示すフローチャートである。

【図６】非特許文献４に記載された認証暗号方式ＴｈｅｔａＣＢ３方式を用いた暗号化ルーチンを簡略化して示した図である。

【図７】非特許文献４に記載された認証暗号方式ＴｈｅｔａＣＢ３方式を用いた復号ルーチンを簡略化して示した図である。

【図８】実施の形態１にかかる認証暗号化方法をＴｗｅａｋａｂｌｅブロック暗号で実施する場合の暗号化処理を例示する図である。

【図９】実施の形態１にかかる認証暗号化方法をＴｗｅａｋａｂｌｅブロック暗号で実施する場合の復号処理を例示する図である。

【図１０】非特許文献２に記載された暗号化関数及び復号関数を例示する図である。

【図１１】実施の形態２にかかる認証暗号化装置を示す図である。

【図１２】実施の形態２にかかる認証復号装置を示す図である。

【図１３】各実施形態に係る装置およびシステムを実現可能な計算処理装置のハードウェア構成例を概略的に示すブロック図である。

【発明を実施するための形態】

【００１８】

（本開示にかかる実施形態の概要）

本開示の実施の形態の説明に先立って、本開示にかかる実施の形態の概要について説明する。なお、以下、本開示の実施形態を説明するが、以下の実施形態は請求の範囲にかかる発明を限定するものではない。また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【００１９】

認証暗号（ＡＥ）の基本的な入出力について説明する。なお、以下の説明では、秘密鍵Ｋを共有する２者としてＡｌｉｃｅとＢｏｂとの間の通信を考え、ＡｌｉｃｅからＢｏｂへ認証暗号による暗号化を行ったメッセージを通信するものとする。また、以下の説明にかかる方式は、例えば、非特許文献１に記載されたＧＣＭ（Galois/Counter Mode）というアルゴリズムによって実現される。

【００２０】

認証暗号の暗号化関数をＡＥｎｃとし、復号関数をＡＤｅｃとする。また、暗号化したい平文をＭとし、さらにナンス（Ｎｏｎｃｅ（ノンス））と呼ばれる変数Ｎを導入する。また、ヘッダ（ａｓｓｏｃｉａｔｅｄ　ｄａｔａ；ＡＤ）をＡとする。ここで、ヘッダＡは、暗号化は行われないが改ざん検知は行われる値である。

【００２１】

まず、Ａｌｉｃｅ側の暗号化処理について説明する。Ａｌｉｃｅは、ナンスＮを生成後

、（Ｃ，Ｔ）＝ＡＥｎｃ＿Ｋ（Ｎ，Ａ，Ｍ）で表される処理を実行する。ここで、ＡＥｎｃ＿Ｋは、鍵Ｋをパラメータとした暗号化関数であり、Ｃは暗号文である。また、Ｔは、タグ（認証タグ）と呼ばれる、固定長の改ざん検出用の変数である。Ａｌｉｃｅは、ナンスＮ、ヘッダＡ、暗号文Ｃ及びタグＴの組（Ｎ，Ａ，Ｃ，Ｔ）を、Ｂｏｂに送信する。

【００２２】

次に、Ｂｏｂ側の復号処理について説明する。Ｂｏｂが受信した情報を（Ｎ’，Ａ’，Ｃ’，Ｔ’）とする。この場合、Ｂｏｂは、復号処理としてＡＤｅｃ＿Ｋ（Ｎ’，Ａ’，Ｃ’，Ｔ’）を実行する。なお、ＡＤｅｃ＿Ｋは、鍵Ｋをパラメータとした復号関数である。通信の途中で改ざんがあり、（Ｎ’，Ａ’，Ｃ’，Ｔ’）≠（Ｎ，Ａ，Ｃ，Ｔ）である場合、ＡＤｅｃ＿Ｋ（Ｎ’，Ａ’，Ｃ’，Ｔ’）について、改ざんがあったことを示すエラーメッセージ（エラーシンボル）が出力される。つまり、この場合、改ざんが検出される。一方、通信の途中で改ざんがなく、（Ｎ’，Ａ’，Ｃ’，Ｔ’）＝（Ｎ，Ａ，Ｃ，Ｔ）である場合、ＡＤｅｃ＿Ｋ（Ｎ’，Ａ’，Ｃ’，Ｔ’）について、Ａｌｉｃｅが暗号化した平文Ｍが正しく復号される。

【００２３】

また、上記の処理においては、通常、暗号化においてナンスＮが過去の値と偶然一致してしまわないようにすることが重要である。このために、暗号化側では、カウンタなどの何らかの状態変数を用いて、ナンスの一致を防ぐ。すなわち、典型的には、状態変数として直前に使ったＮを記憶しておき、毎回Ｎをインクリメントすることで、ナンスＮが過去の値と重複しないことが、実現される。

【００２４】

ここで、認証暗号を含む一般の暗号化方式について、遅延（レイテンシ；latency）という評価指標がある。これは処理を開始してから最初の出力結果が出るまでの時間を指すものであり、小さいほうが望ましい。例えば、コンピュータ内部のメモリバスの暗号化、又は、例えばオンラインゲームや無人機の制御といったリアルタイム処理が求められる通信の暗号化では、特に遅延の発生が問題となる。したがって、このような場合では、低遅延であることが望ましい。なお、暗号化の場合、遅延は、複数ブロックからなる平文を入力した際に、最初の暗号文ブロックが出力されるまでの時間又は処理量のことを指す。

【００２５】

認証暗号で用いるコアとなる暗号部品のことをプリミティブと称する場合、認証暗号における暗号化の遅延は、最初の暗号文ブロックが出力されるまでに必要なプリミティブのコール回数とするのが一般的である。復号の遅延も同様に定義される。なお、遅延の他の指標として、速度（スループット；throughput）がある。速度は、１プリミティブコールあたりで処理可能なメッセージブロック数とするのが一般的である。この数値はレートとも呼ばれる。ただし、一般に、メッセージによらず発生する定数回の呼び出しは、レートの計算に含まれない。つまり、レートは、メッセージが十分長いときの漸近的速度を反映するものである。一方、遅延は、定義上、上記のような定数回呼び出しを含み得る。

【００２６】

ブロック暗号をプリミティブとする認証暗号方式として、特許文献１及び非特許文献１に記載されたＯＣＢが知られている。ＯＣＢについては、特に、遅延が少ないことが知られている。また、例えば、非特許文献２に記載されたＯＣＢの方式、及び、非特許文献３に記載されたＯＣＢ２ｆでは、暗号化における遅延は、ブロック暗号２回となっている。さらに、非特許文献４に記載されたＴｈｅｔａＣＢ３方式では、暗号化における遅延はＴＢＣ１回となっており、ＴＢＣを用いた方式としては理論的に最良となっている。言い換えると、ＯＣＢ及びＴｈｅｔａＣＢ３においては、暗号化における遅延が小さい。なお、速度については、ＯＣＢ及びＴｈｅｔａＣＢ３のいずれについても、暗号化および復号のレートが１であり、メッセージのブロック単位で並列に実行可能である。したがって、ＯＣＢ及びＴｈｅｔａＣＢ３においては、高速な処理が可能であるといえる。

【００２７】

ここで、ＯＣＢ及びＴｈｅｔａＣＢ３においては、暗号化における遅延は小さいものの、後述するように、復号における遅延は、暗号化における遅延よりも大きくなる。これに

対し、本実施の形態における認証暗号では、以下に説明するように、ＯＣＢ及びＴｈｅｔａＣＢ３と同等の速度（すなわちレート１）を達成しつつ、遅延をさらに小さくすることができる。つまり、本実施の形態においては、高速かつ低遅延な認証暗号を実現することができる。

【００２８】

（実施の形態１）

以下、実施の形態について、図面を参照しながら説明する。説明の明確化のため、以下の記載及び図面は、適宜、省略、及び簡略化がなされている。また、各図面において、同一の要素には同一の符号が付されており、必要に応じて重複説明は省略されている。

【００２９】

図１は、実施の形態１にかかる認証暗号システム１の構成を示す図である。認証暗号システム１は、認証暗号化装置１０と、認証復号装置２０とを有する。認証暗号化装置１０及び認証復号装置２０は、物理的に一体であってもよいし、別個であってもよい。また、図２～図３を用いて後述する各装置の構成要素が、別の装置で実現されてもよい。なお、以下の説明では、特に断りのない限り、平文又は暗号文等を分割して得られた複数のブロックのうちの１ブロックの長さを所定長であるｎビットとする。また、上述したＡｌｉｃｅとＢｏｂとの間の通信の例において、認証暗号化装置１０は、Ａｌｉｃｅに対応し、認証復号装置２０はＢｏｂに対応する。つまり、認証暗号化装置１０及び認証復号装置２０との間で通信が行われる。

【００３０】

なお、本実施の形態においては、平文の長さが常にブロック長ｎの倍数であることが好ましい。仮に、ブロック長ｎの倍数でない平文を扱う場合には、パディングが必要となり、暗号文の長さが増える。しかしながら、平文の長さがブロック長の倍数であるという制限は、多くのアプリケーションでは問題とならない。例えば後述するＡＥＳ（Advanced Encryption Standard）を用いてメモリ、キャッシュ又はハードディスクセクタの暗号化を行うことを考える場合、平文の標準的な長さは、ＡＥＳのブロック長（１６バイト）の倍数である。

【００３１】

図２は、実施の形態１にかかる認証暗号化装置１０の構成を示す図である。図３は、実施の形態１にかかる認証復号装置２０の構成を示す図である。また、図４は、実施の形態１にかかる認証暗号化装置１０で実行される認証暗号化方法を示すフローチャートである。また、図５は、実施の形態１にかかる認証復号装置２０で実行される認証復号方法を示すフローチャートである。また、図６は、非特許文献４に記載された認証暗号方式ＴｈｅｔａＣＢ３方式を用いた暗号化ルーチンを簡略化して示した図である。また、図７は、非特許文献４に記載された認証暗号方式ＴｈｅｔａＣＢ３方式を用いた復号ルーチンを簡略化して示した図である。また、図８は、実施の形態１にかかる認証暗号化方法をＴｗｅａｋａｂｌｅブロック暗号で実施する場合の暗号化処理を例示する図である。また、図９は、実施の形態１にかかる認証暗号化方法をＴｗｅａｋａｂｌｅブロック暗号で実施する場合の復号処理を例示する図である。また、図１０は、非特許文献２に記載された暗号化関数及び復号関数を例示する図である。

【００３２】

図２に示した認証暗号化装置１０について説明する。認証暗号化装置１０は、入力部１００と、ナンス生成部１０１と、Ｔｗｅａｋ付き暗号化部１０２と、チェックサム生成部１０３と、ヘッダハッシュ部１０４と、ナンス暗号化部１０５と、加算部１０６と、短縮部１０７と、出力部１０８とを有する。認証暗号化装置１０は、例えばコンピュータによって実現可能である。つまり、認証暗号化装置１０は、ＣＰＵ（Central Processing Unit）などの演算装置と、メモリ又はディスクなどの記憶装置とを有している。認証暗号化装置１０は、例えば、記憶装置に格納されたプログラムを演算装置が実行することで、上記の各構成要素を実現する。

【００３３】

入力部１００は、入力手段としての機能を有する。ナンス生成部１０１は、ナンス生成手段としての機能を有する。Ｔｗｅａｋ付き暗号化部１０２は、Ｔｗｅａｋ付き暗号化手段（平文暗号化手段又は暗号文生成手段）としての機能を有する。チェックサム生成部１０３は、チェックサム生成手段としての機能を有する。ヘッダハッシュ部１０４は、ヘッダハッシュ手段（ハッシュ手段）としての機能を有する。ナンス暗号化部１０５は、ナンス暗号化手段としての機能を有する。加算部１０６は、加算手段（加法手段）としての機能を有する。短縮部１０７は、短縮手段（認証タグ生成手段）としての機能を有する。出力部１０８は、出力手段としての機能を有する。

【００３４】

入力部１００は、暗号化の対象となる平文Ｍおよびヘッダ Ａの入力を受け付ける。入力部１００は、例えば、キーボードなどの入力装置により実現されてもよい。入力部１００は、例えば、ネットワークを介して接続された外部装置などから、平文Ｍ及びヘッダ Ａの入力を受け付けてもよい。なお、ヘッダが存在しない場合もあり、この場合は、ヘッダ Ａは入力されない。入力部１００は、平文Ｍを、Ｔｗｅａｋ付き暗号化部１０２及びチェックサム生成部１０３に出力する。また、入力部１００は、ヘッダ Ａを、ヘッダハッシュ部１０４に出力する。

【００３５】

ナンス生成部１０１は、過去の値と重複がないようにナンスＮを生成する。つまり、ナンス生成部１０１は、過去に生成された値とは異なるナンスＮを生成する。具体的には、例えば、ナンス生成部１０１は、最初に任意の固定値を出力する。また、ナンス生成部１０１は、直前に生成したナンスの値を記憶している。そして、ナンス生成部１０１は、２回目以降にナンスＮを生成する際に、記憶された直前の値に１を加えた値を出力する。このように、ナンス生成部１０１は、１つ前に既に出力した値に１を加えた値を出力することで、過去に生成した値とは異なるナンスＮを生成する。なお、ナンス生成部１０１は、過去に生成した値とは異なる値を生成可能ならば、上述した例とは異なる方法でナンスを生成してもよい。ナンス生成部１０１は、生成されたナンスＮを、Ｔｗｅａｋ付き暗号化部１０２及びナンス暗号化部１０５に出力する。また、ナンス生成部１０１は、生成されたナンスＮを、出力部１０８に出力してもよい。

【００３６】

Ｔｗｅａｋ付き暗号化部１０２は、平文Ｍを所定のｎについてｎビットブロックごとに分割し、ナンスＮを補助変数（Ｔｗｅａｋ）として用いて、平文Ｍをブロックごとに並列に暗号化することで、暗号文Ｃを生成する。具体的には、Ｔｗｅａｋ付き暗号化部１０２は、平文Ｍをｎビットブロックごとに（つまり所定長のブロックに）分割することで生成されたｍ個のブロックの系列Ｍ［１］，Ｍ［２］，．．．，Ｍ［ｍ］を得る。そして、Ｔｗｅａｋ付き暗号化部１０２は、ｉ番目のＭ［ｉ］（ｉ＝１，２，．．．，ｍ）それぞれに対して、ナンスＮ及びブロックのインデックスｉをＴｗｅａｋと呼ばれる補助変数に含めて、ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化する。これにより、Ｔｗｅａｋ付き暗号化部１０２は、平文Ｍを分割したｍ個のブロックと同じ長さの暗号文Ｃ＝（Ｃ［１］，Ｃ［２］，．．．，Ｃ［ｍ］）を得る。なお、平文Ｍの分割は、Ｔｗｅａｋ付き暗号化部１０２によって行われる必要はない。入力部１００に平文Ｍが入力されたときに予めｍ個のブロックの系列Ｍ［１］，Ｍ［２］，．．．，Ｍ［ｍ］に分割されていてもよい。あるいは、入力部１００が平文Ｍを分割してもよい。

【００３７】

なお、Ｔｗｅａｋには、処理の種類（暗号化対象が平文かナンスか、などの違い）を表すインデックスｊを含めてもよい。ここで、インデックスｊを１とし、Ｔｗｅａｋａｂｌｅブロック暗号の暗号化関数をＴＥ（Ｔｗｅａｋ，ｍｅｓｓａｇｅ　ｂｌｏｃｋ）とすると、

（式１）

Ｃ［ｉ］＝ＴＥ（（Ｎ，ｉ，ｊ），Ｍ［ｉ］）　ｆｏｒ　ｉ＝１，．．．，ｍ－１

Ｃ［ｍ］＝ＴＥ（（Ｎ，ｍ，ｊ＋１），Ｍ［ｍ］）

と表すことができる。
【００３８】
Ｔｗｅａｋ付き暗号化部１０２は、得られたＣ［１］，．．．，Ｃ［ｍ］を連結して、暗号文Ｃを得る。そして、Ｔｗｅａｋ付き暗号化部１０２は、得られた暗号文Ｃを、出力部１０８に出力する。
【００３９】
なお、式１に示すように、安全性の観点から、最後のブロック（ｉ＝ｍのブロック）のみ、処理の種類を表すインデックスｊを、他のブロックにおけるインデックスｊから変更する必要がある。したがって、Ｃ［ｍ］では、このインデックスをｊ＋１としている。また、平文Ｍの長さがｎの倍数でない場合は、Ｔｗｅａｋ付き暗号化部１０２は、適当な一意の復号可能なパディングを施してから、Ｍ［１］，Ｍ［２］，．．．，Ｍ［ｍ］を得る。
【００４０】
Ｔｗｅａｋ付き暗号化部１０２は、Ｔｗｅａｋａｂｌｅブロック暗号（ＴＢＣ）として、例えば、非特許文献５に記載されているＳＫＩＮＮＹ等の既存のアルゴリズムを用いてもよい。あるいは、Ｔｗｅａｋ付き暗号化部１０２は、Ｔｗｅａｋａｂｌｅブロック暗号（ＴＢＣ）を、ＡＥＳ（Advanced Encryption Standard）などのブロック暗号を用いたブロック暗号利用モード（以下モード）で実現してもよい。この場合、Ｔｗｅａｋ付き暗号化部１０２は、Ｔｗｅａｋａｂｌｅブロック暗号のモードとして、非特許文献２に記載されたＸＥＸ＊モードや、その変種である非特許文献４に記載されているモードを用いることが可能である。つまり、本実施の形態において、Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードであってもよい。
【００４１】
ここで、ブロック暗号の暗号化関数をＥとする。また、Ｔｗｅａｋを（Ｎ，ｉ，ｊ）とし、平文をＭとし、暗号文をＣとする。この場合、ＸＥＸ＊モードの暗号化は、以下の式２で表される。この式は、図１０の上図で表される。
（式２）
Ｃ＝ｇ（Ｎ，ｉ，ｊ）＋Ｅ（Ｍ＋ｇ（Ｎ，ｉ，ｊ）），
ｇ（Ｎ，ｉ，ｊ）＝Ｅ（Ｎ）・２＾ｉ・３＾ｊ
【００４２】
ここで、「・２」は、有限体ＧＦ（２＾ｎ）上の生成元（多項式表現におけるｘ）との乗算を意味し、「・３」は、生成元と単位元の和（多項式で表現するとｘ＋１）との乗算を意味する。また、「Ｅ（Ｎ）・２＾ｉ・３＾ｊ」は、Ｅ（Ｎ）をＧＦ（２＾ｎ）の元とみて、それをｉ回生成元と乗算し、ｊ回生成元と単位元の和との乗算をとることを意味する。なお、これらのＧＦ（２＾ｎ）上の定数乗算は、極めて簡単な処理で実現される。また、上記の方式は、ｎ＝１２８のときに安全性が保証されている。そのほかのｎの場合のブロック暗号の暗号化関数の実現方法は、例えば非特許文献３に記載されている。
【００４３】
なお、Ｔｗｅａｋａｂｌｅブロック暗号を用いて行う処理が上述した暗号化処理でなく、メッセージのハッシュ処理を行う場合などであれば、上記式２における暗号化関数Ｅの外側のｇ（Ｎ，ｉ，ｊ）を省略して、
（式３）
Ｃ＝Ｅ（Ｍ＋ｇ（Ｎ，ｉ，ｊ））
としてもよい。例えば、後述するヘッダハッシュ部１０４で行われる処理がこれに相当する。
【００４４】
チェックサム生成部１０３は、平文Ｍを簡単な計算により圧縮することによって、チェックサムＳを生成する。具体的には、チェックサム生成部１０３は、平文Ｍをｎビットブロックの系列Ｍ［１］，Ｍ［２］，．．．，Ｍ［ｍ］に分割する。そして、チェックサム生成部１０３は、分割されたｎビットブロックの系列Ｍ［１］，Ｍ［２］，．．．，Ｍ［ｍ］に対して簡便な圧縮処理を施すことによって、チェックサムＳを生成する。チェック

サム生成部１０３は、生成されたチェックサムＳを、加算部１０６に出力する。
【００４５】
チェックサム生成部１０３は、例えば、排他的論理和＋を用いる場合は、
（式４）
Ｓ＝Ｍ［１］＋Ｍ［２］＋．．．＋Ｍ［ｍ］
を計算することによって、チェックサムＳを生成する。なお、チェックサム生成部１０３は、排他的論理和に限らず、例えば算術加算など任意の群ないし環演算を用いて、チェックサムＳを生成してもよい。
【００４６】
ヘッダハッシュ部１０４は、ヘッダＡとユニバーサルハッシュ関数とを用いることによって、ヘッダＡのハッシュ値Ｈを取得する。具体的には、ヘッダハッシュ部１０４は、ヘッダＡをｎビットブロックの系列Ａ［１］，Ａ［２］，．．．，Ａ［ａ］に分割する。そして、ヘッダハッシュ部１０４は、分割されたｎビットブロックの系列Ａ［１］，Ａ［２］，．．．，Ａ［ａ］にユニバーサルハッシュ関数を適用することによって、ヘッダのハッシュ値Ｈを取得する。ヘッダハッシュ部１０４は、取得されたヘッダのハッシュ値Ｈを、加算部１０６に出力する。
【００４７】
ここで、ヘッダハッシュ部１０４は、ユニバーサルハッシュ関数として、非特許文献６に記載されたような、乗算を用いた多項式ハッシュ関数（polynomial hash function）を用いてもよい。あるいは、ヘッダハッシュ部１０４は、ブロック暗号又はＴｗｅａｋａｂｌｅブロック暗号を用いた方式によって、ヘッダのハッシュ値Ｈを生成してもよい。ヘッダハッシュ部１０４は、例えば、非特許文献２に記載された方式を用いて、ユニバーサルハッシュ関数として、Ｔｗｅａｋ付き暗号化部１０２で用いられたＴＥ関数を用いると、以下の式５によってハッシュ値Ｈを取得してもよい。
（式５）
Ｈ＝ＴＥ（（ｃｏｎｓｔ，１，ｊ’），Ａ［１］）＋ＴＥ（（ｃｏｎｓｔ，２，ｊ’），Ａ［２］）＋．．．＋ＴＥ（（ｃｏｎｓｔ，ａ，ｊ’），Ａ［ａ］）
【００４８】
ここで、ｃｏｎｓｔは、任意のｎビット定数である。また、ｊ’は、Ｔｗｅａｋ付き暗号化部１０２で用いられたインデックスｊと異なる任意の整数（例えばｊ’＝３）である。また、上述したように、Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードであってもよい。
【００４９】
上記の式５から、ヘッダハッシュ部１０４は、ｉ番目のヘッダブロックＡ［ｉ］に対して、ヘッダのブロックのインデックスｉを含めたＴｗｅａｋを用いて、ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化を行う。そして、ヘッダハッシュ部１０４は、暗号化を行った全てのｉ＝１，．．．，ａについてのブロックの加算を行うことで、ヘッダのハッシュ値Ｈを取得する。
【００５０】
なお、Ａがｎの倍数の長さでない場合は、ヘッダハッシュ部１０４は、適切なパディングを施したのち、ヘッダＡをＡ［１］，Ａ［２］，．．．，Ａ［ａ］に分割する。なお、ヘッダＡが存在しない場合は、ヘッダハッシュ部１０４は、ハッシュ値Ｈを任意の定数（例えばオールゼロ；全てのビット値が０の定数）としてもよい。
【００５１】
ナンス暗号化部１０５は、ナンスＮを暗号化し、チェックサムと同じ長さの暗号化ナンスＶを取得する。具体的には、ナンス暗号化部１０５は、ナンスＮを補助変数（Ｔｗｅａｋ）として用いて任意のｎビット定数を暗号化することで、暗号化ナンスＶを生成する。つまり、ナンス暗号化部１０５は、ナンスＮを含めたＴｗｅａｋを用いて、１ブロックの平文を任意の定数としたＴｗｅａｋａｂｌｅブロック暗号で暗号化を行うことによって、暗号化ナンスＶを生成する。ナンス暗号化部１０５は、生成された暗号化ナンスＶを、加

算部１０６に出力する。また、上述したように、Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードであってもよい。

【００５２】

例えば、ナンス暗号化部１０５は、Ｔｗｅａｋ付き暗号化部１０２の処理で用いられたＴＥ関数を用いて、以下のようにして暗号化ナンスＶを生成できる。すなわち、ナンス暗号化部１０５は、処理の種類のインデックスとしてそれまでに使われていない値ｊ’’（例えばｊ’’＝４）を用いて、以下の式６を用いて、暗号化ナンスＶを生成できる。

（式６）

Ｖ＝ＴＥ（（Ｎ，０，ｊ’’），００．．０）

ここで、「００．．０」は、ｎビットのオールゼロを示す。

【００５３】

加算部１０６は、チェックサムＳと暗号化ナンスＶとヘッダのハッシュ値Ｈとの和をとることで、非短縮認証タグＵを生成する。具体的には、加算部１０６は、ヘッダのハッシュ値Ｈとチェックサムと暗号化ナンスＶとを加算する。加算部１０６は、この和を、ｎビットの非短縮認証タグＵとして取得する。なお、加算方法は、排他的論理和であってもよいし、あるいは、任意の群の加法演算であってもよい。加算部１０６は、得られた非短縮認証タグＵを、短縮部１０７に出力する。

【００５４】

短縮部１０７は、所定のｔ（ｔは１以上ｎ以下の整数）について、加算部１０６によって生成された非短縮認証タグＵを任意の方法によってｔビットに短縮して、認証タグＴを生成する。具体的には、短縮部１０７は、任意の方法によって非短縮認証タグＵを短縮して所定のｔビットとすることによって、認証タグＴを生成する。例えば、短縮部１０７は、非短縮認証タグＵの最上位のｔビットを、認証タグＴとしてもよい。

【００５５】

出力部１０８は、暗号文Ｃと認証タグＴとを出力するための制御を行う。このとき、出力部１０８は、暗号文Ｃと認証タグＴとを連結して出力するようにしてもよい。出力部１０８は、例えば、ディスプレイなどの出力装置に暗号文Ｃと認証タグＴとを表示させるための制御を行ってもよい。また、出力部１０８は、例えば、ネットワークを介して接続された外部装置などに対して、暗号文Ｃ及び認証タグＴを出力するように制御を行ってもよい。また、出力部１０８は、ナンスＮ及びヘッダＡを出力するように制御を行ってもよい。

【００５６】

次に、図３に示した認証復号装置２０について説明する。認証復号装置２０は、入力部２００と、Ｔｗｅａｋ付き復号部２０１と、チェックサム生成部２０２と、ナンス暗号化部２０３と、ヘッダハッシュ部２０４と、加算部２０５と、短縮部２０６と、タグ検証部２０７とを有する。認証復号装置２０、例えばコンピュータによって実現可能である。つまり、認証復号装置２０は、ＣＰＵなどの演算装置と、メモリ又はディスクなどの記憶装置とを有している。認証復号装置２０は、例えば、記憶装置に格納されたプログラムを演算装置が実行することで、上記の各構成要素を実現する。

【００５７】

入力部２００は、入力手段としての機能を有する。Ｔｗｅａｋ付き復号部２０１は、Ｔｗｅａｋ付き復号手段（平文復号手段又は平文生成手段）としての機能を有する。チェックサム生成部２０２は、チェックサム生成手段としての機能を有する。ナンス暗号化部２０３は、ナンス暗号化手段としての機能を有する。ヘッダハッシュ部２０４は、ヘッダハッシュ手段（ハッシュ手段）としての機能を有する。加算部２０５は、加算手段（加法手段）としての機能を有する。短縮部２０６は、短縮手段（検証用タグ生成手段）としての機能を有する。タグ検証部２０７は、タグ検証手段（検証手段及び出力手段）としての機能を有する。

【００５８】

入力部２００は、復号の対象となる暗号文Ｃ、ナンスＮ、ヘッダＡ及び認証タグＴの入力を受け付ける。入力部２００は、例えば、キーボードなどの文字入力装置により実現さ

れてもよい。入力部２００は、例えば、キーボードなどの入力装置により実現される。入力部２００は、例えば、ネットワークを介して接続された外部装置などから、暗号文Ｃ、ナンスＮ、ヘッダＡ及び認証タグＴを受け付けてもよい。なお、ヘッダが存在しない場合もあり、この場合は、ヘッダＡは入力されない。入力部２００は、暗号文Ｃを、Ｔｗｅａｋ付き復号部２０１に出力する。また、入力部２００は、ヘッダＡを、ヘッダハッシュ部２０４に出力する。また、入力部２００は、ナンスＮを、Ｔｗｅａｋ付き復号部２０１及びナンス暗号化部２０３に出力する。また、入力部２００は、認証タグＴを、タグ検証部２０７に出力する。

【００５９】

Ｔｗｅａｋ付き復号部２０１は、上述したＴｗｅａｋ付き暗号化部１０２に対応した復号処理を行う。Ｔｗｅａｋ付き復号部２０１は、暗号文Ｃを所定のｎについてｎビットブロックごとに分割し、ナンスＮを補助変数（Ｔｗｅａｋ）として用い、ブロックごとに並列に復号することで、平文Ｍを生成する。具体的には、Ｔｗｅａｋ付き復号部２０１は、暗号文Ｃをｎビットブロックごとに分割することで生成されたｍ個のブロックの系列Ｃ［１］，Ｃ［２］，．．．，Ｃ［ｍ］を得る。そして、Ｔｗｅａｋ付き復号部２０１は、ｉ番目のＣ［ｉ］（ｉ＝１，２，．．．，ｍ）それぞれに対して、ナンスＮ及びブロックのインデックスｉをＴｗｅａｋと呼ばれる補助変数に含めて、ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で復号する。これにより、Ｔｗｅａｋ付き復号部２０１は、暗号文Ｃを分割したｍ個のブロックと同じ長さの平文Ｍ＝（Ｍ［１］，Ｍ［２］，．．．，Ｍ［ｍ］）を得る。なお、暗号文Ｃの分割は、Ｔｗｅａｋ付き復号部２０１によって行われる必要はない。入力部２００に暗号文Ｃが入力されたときに予めｍ個のブロックの系列Ｃ［１］，Ｃ［２］，．．．，Ｃ［ｍ］に分割されていてもよい。あるいは、入力部２００が暗号文Ｃを分割してもよい。

【００６０】

なお、上述したように、Ｔｗｅａｋには、処理の種類（暗号化対象が平文かナンスか、などの違い）を表すインデックスｊを含めてもよい。上述のインデックスｊを１とし、Ｔｗｅａｋａｂｌｅブロック暗号の復号関数をＴＤ（Ｔｗｅａｋ，ｍｅｓｓａｇｅ　ｂｌｏｃｋ）とすると、

（式７）

Ｍ［ｉ］＝ＴＤ（（Ｎ，ｉ，ｊ），Ｃ［ｉ］）　ｆｏｒ　ｉ＝１，．．．，ｍ－１

Ｍ［ｍ］＝ＴＤ（（Ｎ，ｍ，ｊ＋１），Ｃ［ｍ］）

と表すことができる。

【００６１】

Ｔｗｅａｋ付き復号部２０１は、得られたＭ［１］，．．．，Ｍ［ｍ］を連結して、平文Ｍを出力する。そして、Ｔｗｅａｋ付き復号部２０１は、得られた平文Ｍを、タグ検証部２０７及びチェックサム生成部２０２に出力する。なお、式７に示すように、安全性の観点から、最後のブロック（ｉ＝ｍのブロック）のみ、処理の種類を表すインデックスｊを、他のブロックにおけるインデックスｊから変更する必要がある。したがって、Ｍ［ｍ］では、このインデックスをｊ＋１としている。

【００６２】

なお、Ｔｗｅａｋ付き暗号化部１０２と同様に、Ｔｗｅａｋ付き復号部２０１は、Ｔｗｅａｋａｂｌｅブロック暗号（ＴＢＣ）として非特許文献５に記載されているＳＫＩＮＮＹ等の既存のＴｗｅａｋａｂｌｅブロック暗号のアルゴリズムを用いてもよい。あるいは、Ｔｗｅａｋ付き復号部２０１は、Ｔｗｅａｋａｂｌｅブロック暗号（ＴＢＣ）を、ＡＥＳなどのブロック暗号を用いたモードで実現してもよい。この場合、Ｔｗｅａｋ付き復号部２０１は、Ｔｗｅａｋａｂｌｅブロック暗号のモードとして、非特許文献２に記載されたＸＥＸ＊モードや、その変種である非特許文献４に記載されているモードを用いることが可能である。つまり、本実施の形態において、Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードであってもよい。

【００６３】

なお、Ｔｗｅａｋａｂｌｅブロック暗号のモードとして非特許文献２のＸＥＸ＊モードを用いた場合を考える。ブロック暗号の暗号化関数をＥとし、復号関数をＤとする。また、Ｔｗｅａｋを（Ｎ，ｉ，ｊ）とし、平文をＭとし、暗号文をＣとする。この場合、ＸＥＸ＊モードの復号は、以下の式８で表される。この式は、図１０の下図で表される。

（式８）

Ｍ＝ｇ（Ｎ，ｉ，ｊ）＋Ｄ（Ｃ＋ｇ（Ｎ，ｉ，ｊ）），

ｇ（Ｎ，ｉ，ｊ）＝Ｅ（Ｎ）・２＾ｉ・３＾ｊ

【００６４】

なお、関数ｇの定義等については、上述した式２（Ｔｗｅａｋ付き暗号化部１０２）におけるものと実質的に同様である。また、上記の方式は、ｎ＝１２８のときに安全性が保証されている。

【００６５】

チェックサム生成部２０２は、上述したチェックサム生成部１０３と実質的に同様の処理を行う。つまり、チェックサム生成部２０２は、平文Ｍを簡単な計算により圧縮することによって、チェックサムＳを生成する。チェックサム生成部２０２は、生成されたチェックサムＳを、加算部２０５に出力する。

【００６６】

ナンス暗号化部２０３は、上述したナンス暗号化部１０５と実質的に同様の処理を行う。つまり、ナンス暗号化部２０３は、ナンスＮを暗号化し、チェックサムと同じ長さの暗号化ナンスＶを取得する。具体的には、ナンス暗号化部２０３は、ナンスＮを補助変数（Ｔｗｅａｋ）として用いて任意のｎビット定数を暗号化することで、暗号化ナンスＶを生成する。つまり、ナンス暗号化部２０３は、ナンスＮを含めたＴｗｅａｋを用いて、１ブロックの平文を任意の定数としたＴｗｅａｋａｂｌｅブロック暗号で暗号化を行うことによって、暗号化ナンスＶを生成する。ナンス暗号化部２０３は、取得された暗号化ナンスＶを、加算部２０５に出力する。また、上述したように、Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードであってもよい。

【００６７】

ヘッダハッシュ部２０４は、上述したヘッダハッシュ部１０４と実質的に同様の処理を行う。つまり、ヘッダハッシュ部２０４は、ヘッダＡとユニバーサルハッシュ関数とを用いることによって、ヘッダＡのハッシュ値Ｈを取得する。ヘッダハッシュ部２０４は、取得されたハッシュ値Ｈを、加算部２０５に出力する。なお、ヘッダＡが存在しない場合は、ヘッダハッシュ部２０４は、ハッシュ値Ｈを任意の定数（例えばオールゼロ；全てのビット値が０の定数）としてもよい。

【００６８】

具体的には、ヘッダハッシュ部２０４は、ヘッダＡをｎビットブロックの系列Ａ［１］，Ａ［２］，．．．，Ａ［ａ］に分割する。そして、ヘッダハッシュ部２０４は、分割されたｎビットブロックの系列Ａ［１］，Ａ［２］，．．．，Ａ［ａ］にユニバーサルハッシュ関数を適用することによって、ヘッダのハッシュ値Ｈを取得する。そして、上記の式５から、ヘッダハッシュ部２０４は、ｉ番目のヘッダブロックＡ［ｉ］に対して、ヘッダのブロックのインデックスｉを含めたＴｗｅａｋを用いて、ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化を行う。そして、ヘッダハッシュ部２０４は、暗号化を行った全てのｉ＝１，．．．，ａについてのブロックの加算を行うことで、ヘッダのハッシュ値Ｈを取得する。また、上述したように、Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードであってもよい。

【００６９】

加算部２０５は、上述した加算部１０６と実質的に同様の処理を行う。つまり、加算部２０５は、チェックサムＳと暗号化ナンスＶとヘッダのハッシュ値Ｈとの和をとることで、非短縮認証タグＵを生成する。加算部２０５は、生成された非短縮認証タグＵを、短縮部２０６に出力する。

【００７０】

短縮部２０６は、所定のｔ（ｔは１以上ｎ以下の整数）について、加算部２０５によって生成された非短縮認証タグＵを任意の方法によってｔビットに短縮して、推定された認証タグである検証用タグＴ’を生成する。なお、短縮部２０６の具体的な処理は、短縮部１０７の処理と実質的に同様である。短縮部２０６は、生成された検証用タグＴ’を、タグ検証部２０７に出力する。

【００７１】

タグ検証部２０７は、入力部２００によって出力された認証タグＴと、短縮部２０６によって出力された検証用タグＴ’とを比較して、改ざんの有無を検証する。そして、タグ検証部２０７は、検証結果に基づいて、情報を出力するための制御を行う。なお、タグ検証部２０７は、例えば、ディスプレイなどの出力装置に情報を表示させるための制御を行ってもよい。また、タグ検証部２０７は、例えば、ネットワークを介して接続された外部装置などに対して、情報を出力するように制御を行ってもよい。

【００７２】

具体的には、認証タグＴと検証用タグＴ’とが一致する場合に、タグ検証部２０７は、Ｔｗｅａｋ付き復号部２０１によって生成された平文Ｍを出力するための制御を行う。なお、平文の長さがｎの倍数でないケースでは、タグ検証部２０７は、所定のパディングを取り除いて、平文Ｍを出力するように制御を行ってもよい。一方、認証タグＴと検証用タグＴ’とが一致しない場合に、タグ検証部２０７は、認証タグＴと検証用タグＴ’とが一致しないことを示すエラーシンボルを出力するように制御を行う。

【００７３】

次に、図４及び図５を用いて、実施の形態１にかかる認証暗号システム１にかかる動作について説明する。図４は、実施の形態１にかかる認証暗号化装置１０で実行される認証暗号化方法を示すフローチャートである。

【００７４】

入力部１００は、平文Ｍ及びヘッダＡを入力する（ステップＳ１００）。具体的には、入力部１００は、上述したように、暗号化の対象となる平文Ｍ＝（Ｍ［１］，Ｍ［２］，．．．，Ｍ［ｍ］）と、ヘッダＡとを入力する。ナンス生成部１０１は、上述したように、ナンスＮを生成する（ステップＳ１０２）。

【００７５】

次に、Ｔｗｅａｋ付き暗号化部１０２は、上述したように、ナンスＮを補助変数Ｔｗｅａｋとして用いて、ブロックごとに平文Ｍを暗号化して、暗号文Ｃを取得する（ステップＳ１０４）。次に、チェックサム生成部１０３は、上述したように、平文Ｍのチェックサムｓを生成する（ステップＳ１０６）。次に、ヘッダハッシュ部１０４は、上述したように、ヘッダＡのハッシュ値Ｈを取得する（ステップＳ１０８）。次に、ナンス暗号化部１０５は、上述したように、ナンスＮを暗号化して、暗号化ナンスＶを取得する（ステップＳ１１０）。

【００７６】

次に、認証暗号化装置１０は、認証タグＴを取得する（ステップＳ１１２）。具体的には、加算部１０６は、上述したように、チェックサムｓと暗号化ナンスＶとヘッダのハッシュ値Ｈとの和をとる。短縮部１０７は、和（非短縮認証タグＵ）を所定のｔビットに短縮することで、認証タグＴを取得する。そして、出力部１０８は、上述したように、暗号文Ｃと認証タグＴとを出力するための制御を行う（ステップＳ１１４）。

【００７７】

図５は、実施の形態１にかかる認証復号装置２０で実行される認証復号方法を示すフローチャートである。入力部２００は、上述したように、復号の対象となる暗号文Ｃ、ナンスＮ、ヘッダＡ及び認証タグＴを入力する（ステップＳ２０２）。次に、ナンス暗号化部２０３は、上述したように、ナンスＮを暗号化し、暗号化ナンスＶを取得する（ステップＳ２０４）。次に、Ｔｗｅａｋ付き復号部２０１は、上述したように、ナンスＮを補助変数Ｔｗｅａｋとして用いて、ブロックごとに暗号文Ｃを復号して、平文Ｍを取得する（ステップＳ２０６）。次に、ヘッダハッシュ部２０４は、上述したように、ヘッダＡのハッ

シュ値Ｈを取得する（ステップＳ２０８）。次に、チェックサム生成部２０２は、上述したように、平文Ｍのチェックサムを生成する（ステップＳ２１０）。

【００７８】

次に、認証復号装置２０は、推定された認証タグＴ’（検証用タグ）を取得する（ステップＳ２１２）。具体的には、加算部２０５は、上述したように、暗号化ナンスＶとヘッダのハッシュ値Ｈとチェックサムとの和をとる。短縮部２０６は、和（非短縮認証タグＵ）を所定のｔビットに短縮することで、推定された認証タグＴ’（検証用タグＴ’）を取得する。

【００７９】

タグ検証部２０７は、認証タグＴと検証用タグＴ’とが一致するか否かを判定する（ステップＳ２１４）。これにより、改ざんの有無が検証される。認証タグＴと検証用タグＴ’とが一致する場合（Ｓ２１４のＹＥＳ）、タグ検証部２０７は、認証が成功したことを示す検証結果として、平文Ｍを出力するための制御を行う（ステップＳ２１６）。一方、認証タグＴと検証用タグＴ’とが一致しない場合（Ｓ２１４のＮＯ）、タグ検証部２０７は、認証が失敗したことを示す検証結果として、エラーシンボルを出力するための制御を行う（ステップＳ２１８）。

【００８０】

次に、実施の形態１にかかる認証暗号システム１の効果を説明する。

上述したように、ＯＣＢ及びＴｈｅｔａＣＢ３においては、暗号化における遅延は小さいものの、復号における遅延は、暗号化における遅延より大きくなる。具体的には、ＯＣＢでは、復号遅延は３であり、ＴｈｅｔａＣＢ３では、復号遅延は２である。このように、復号遅延が暗号化における遅延よりも大きくなる要因は、改ざん検知用の認証タグの計算方法にある。以下、ＴｈｅｔａＣＢ３について説明する。

【００８１】

図６は、非特許文献４に記載された認証暗号方式ＴｈｅｔａＣＢ３方式を用いた暗号化ルーチンを簡略化して示した図である。図６において、「ＴＥ（Ｎ，ｉ，ｊ）」は、Ｔｗｅａｋａｂｌｅブロック暗号の暗号化関数の第一引数にＴｗｅａｋ（Ｎ，ｉ，ｊ）を適用した関数ＴＥ（（Ｎ，ｉ，ｊ），＊）を表す。また、「ｔｒｕｎｃ」は入力の短縮を行う関数である。

【００８２】

また、図７は、非特許文献４に記載された認証暗号方式ＴｈｅｔａＣＢ３方式を用いた復号ルーチンを簡略化して示した図である。図７において、「ＴＤ（Ｎ，ｉ，ｊ）」は、Ｔｗｅａｋａｂｌｅブロック暗号の復号関数の第一引数にＴｗｅａｋ（Ｎ，ｉ，ｊ）を適用した関数ＴＤ（（Ｎ，ｉ，ｊ），＊）を表す。

【００８３】

図６に示すように、認証タグＴは、チェックサムＳと呼ばれる平文ブロックの和（排他的論理和）を、Ｔｗｅａｋａｂｌｅブロック暗号のＴＥ関数（ＴＥ（Ｎ．ｍ．２））で暗号化することにより得られている。また、暗号化は、全てのＴＥ関数について、暗号化に必要な値の入力（ナンスＮ、ヘッダＡ及び平文Ｍ）が決定した段階で、並列に実行され得る。したがって、暗号化における遅延は１である。

【００８４】

一方、図７に示す復号処理では、平文ブロックを得るために、対応する暗号文ブロックをＴｗｅａｋａｂｌｅブロック暗号の復号関数ＴＤで復号する。そして、復号により平文ブロックが得られた後でチェックサムＳを生成し、チェックサムＳをＴＥ関数（ＴＥ（Ｎ．ｍ．２））で暗号化して得られた認証タグＴ’の値と、送信された認証タグＴの値との一致を確認することで、改ざんの有無の検証が行われる。したがって、Ｔｗｅａｋａｂｌｅブロック暗号の復号関数ＴＤと暗号化関数ＴＥ（破線で囲まれたもの）とを直列に呼び出すこととなるため、復号における遅延は２となる。つまり、図７において、破線で囲まれたＴＥ関数は、平文ブロックＭ［１］，．．．，Ｍ［ｍ］が決定されないと実行できない。したがって、この破線で囲まれたＴＥ関数で、遅延が１増加していることになる。

【００８５】
　また、ＯＣＢの場合は、上記の処理に加えて、ＴＥ関数及びＴＤ関数をブロック暗号で実現するために、ブロック暗号によりナンス（暗号化で用いる公開値、カウンタなどで実現）を暗号化することが必要となる。具体的には、非特許文献２及び非特許文献３に記載されたＯＣＢ２又はＯＣＢ２ｆの場合で、暗号化及び復号において、遅延が１増加する。したがって、ＯＣＢの場合、暗号化の遅延が２、復号の遅延が３となる。すなわち、ＯＣＢ及びＴｈｅｔａＣＢ３ともに、復号の遅延は、暗号化の遅延と比べて１増加している。
【００８６】
　また、認証タグによる通信帯域の増加を抑えるために、認証タグの長さは１ブロックよりも短くすることが多い。そして、後述するように、実施の形態１にかかる方法は、上述した技術と比較して、認証タグの長さによらないで、復号遅延を抑制する効果がある。つまり、実施の形態１にかかる方法は、タグの長さによらず、暗号化の遅延及び復号の遅延が、いずれも、Ｔｗｅａｋａｂｌｅブロック暗号の１回となる、という効果を奏する。
【００８７】
　図８は、実施の形態１にかかる認証暗号化方法をＴｗｅａｋａｂｌｅブロック暗号で実施する場合の暗号化処理を例示する図である。また、図９は、実施の形態１にかかる認証暗号化方法をＴｗｅａｋａｂｌｅブロック暗号で実施する場合の復号処理を例示する図である。図８及び図９に示すように、ＴＥ関数及びＴＤ関数の依存関係が、暗号化（図８）でも復号（図９）でも存在せず、ＴＥ関数及びＴＤ関数は、完全に並列となっている。すなわち、暗号化では、図８に示した全てのＴＥ関数を、並列に実行することができる。また、復号では、図９に示した全てのＴＥ関数及びＴＤ関数を、並列に実行することができる。したがって、暗号化の遅延及び復号の遅延が、ともに１となっている。
【００８８】
　上述したように、特に効率のよいＴｗｅａｋａｂｌｅブロック暗号ベースの認証暗号方式であるＴｈｅｔａＣＢ３（図６及び図７）では、暗号化の遅延が１であるのに対して、復号遅延は２となっている。なお、ＴｈｅｔａＣＢ３においても、タグの長さｔをｎビット（つまり短縮を行わない）とすれば、復号手順の変更により復号遅延を１とすることができる。しかしながら、認証タグによる通信帯域の増加を抑えるために、タグの短縮を行うことが一般的である。したがって、タグの長さによらず遅延を抑制できることが望ましい。
【００８９】
　また、タグの長さｔがｎビット未満の場合には、チェックサムの生成及びヘッダのハッシュ値の生成にかかわるＴＥ関数及びＴＤ関数の出力を予めｔビットに短縮しておくことも考えられる。これにより、全体のアルゴリズムを変えることなく、暗号化又は復号に必要なメモリ量を削減することが可能である。一方、ＴｈｅｔａＣＢ３では、チェックサムをＴｗｅａｋａｂｌｅブロック暗号に入力する前に短縮することができないため、このようなメモリ量削減はできない。
【００９０】
　また、Ｔｗｅａｋａｂｌｅブロック暗号を何らかのブロック暗号利用モード（例えば非特許文献２のＯＣＢで用いられるＸＥＸ＊モード）で実現した場合には、ブロック暗号利用モードの部分で計算のオーバーヘッドが生じる。これにより、暗号化と復号の両方の遅延が増加する。具体的にＸＥＸ＊を用いる場合は、ナンスの暗号化による１回が常にオーバーヘッドとして発生する。しかし、これは既存のＯＣＢでも同様であり、Ｔｗｅａｋａｂｌｅブロック暗号を実現する方法が同じであれば、オーバーヘッドは同じであり、結果として、非特許文献に記載された技術に対する、本実施の形態における復号遅延の少なさというメリットは保存されることになる。
【００９１】
　具体的には、非特許文献２及び非特許文献３のＯＣＢ２又はＯＣＢ２ｆでは、ＸＥＸ＊モードを用いており、暗号化遅延が２となり、復号遅延が３となる。これに対し、本実施の形態では、同じＸＥＸ＊モードを用いたときは、暗号化遅延及び復号遅延はともに２と

なる。また、非特許文献４のＯＣＢ３では、ＸＥＸ＊モードの変種（variant）を用いて、ナンスがカウンタの場合に限定されるが、上記の計算オーバーヘッドをほぼなくすことが可能である。この変種を用いた場合には、ＯＣＢ３及び本実施の形態のいずれも、ＸＥＸ＊モードを使ったときと比べ、暗号化遅延と復号遅延の両方が、約１減ることになる。よって、ＯＣＢ３では、暗号化遅延がほぼ１であり、復号遅延がほぼ２となる。これに対し、本実施の形態では、暗号化遅延及び復号遅延の両方が、ほぼ１となる。

【００９２】

また、本実施の形態では、ＴｈｅｔａＣＢ３に対応する方式を採用した場合でも、暗号化及び復号のレートが１であること、並列実行可能、証明可能安全性（provable security）を持つ、などのＴｈｅｔａＣＢ３の利点を保持している。したがって、本実施の形態においては、高速かつ低遅延な認証暗号を実現することができる。

【００９３】

（実施の形態２）

次に、実施の形態２について説明する。実施の形態２は、実施の形態１にかかる構成の概要を示している。

【００９４】

図１１は、実施の形態２にかかる認証暗号化装置３０を示す図である。実施の形態２にかかる認証暗号化装置３０は、実施の形態１にかかる認証暗号化装置１０に対応する。実施の形態２にかかる認証暗号化装置３０は、入力部３１と、ナンス生成部３２と、平文暗号化部３３と、チェックサム生成部３４と、ハッシュ部３５と、ナンス暗号化部３６と、認証タグ生成部３７と、出力部３８とを有する。

【００９５】

入力部３１は、入力手段（第１の入力手段）としての機能を有する。ナンス生成部３２は、ナンス生成手段としての機能を有する。平文暗号化部３３は、平文暗号化手段（Ｔｗｅａｋ付き暗号化手段又は暗号文生成手段）としての機能を有する。チェックサム生成部３４は、チェックサム生成手段（第１のチェックサム生成手段）としての機能を有する。ハッシュ部３５は、ハッシュ手段（第１のハッシュ手段）としての機能を有する。ナンス暗号化部３６は、ナンス暗号化手段（第１のナンス暗号化手段）としての機能を有する。認証タグ生成部３７は、認証タグ生成手段（加算手段及び短縮手段）としての機能を有する。出力部３８は、出力手段としての機能を有する。

【００９６】

入力部３１は、図２に示した入力部１００が有している機能と実質的に同様の機能によって実現できる。入力部３１は、平文の入力を受け付ける。また、入力部３１は、ヘッダの入力を受け付けてもよい。ナンス生成部３２は、図２に示したナンス生成部１０１が有している機能と実質的に同様の機能によって実現できる。ナンス生成部３２は、過去に生成された値とは異なるナンスを生成する。平文暗号化部３３は、図２に示したＴｗｅａｋ付き暗号化部１０２が有している機能と実質的に同様の機能によって実現できる。平文暗号化部３３は、平文を分割したブロックごとに、ナンスを補助変数として用いて暗号化することで、平文に対応する暗号文を生成する。

【００９７】

チェックサム生成部３４は、図２に示したチェックサム生成部１０３が有している機能と実質的に同様の機能によって実現できる。チェックサム生成部３４は、平文を用いてチェックサムを生成する。ハッシュ部３５は、図２に示したヘッダハッシュ部１０４が有している機能と実質的に同様の機能によって実現できる。ハッシュ部３５は、ハッシュ値を取得する。なお、ヘッダが入力される場合、ハッシュ部３５は、ヘッダとハッシュ関数（ユニバーサルハッシュ関数）とを用いてハッシュ値を取得してもよい。ナンス暗号化部３６は、図２に示したナンス暗号化部１０５が有している機能と実質的に同様の機能によって実現できる。ナンス暗号化部３６は、ナンスを暗号化して暗号化ナンスを取得する。

【００９８】

認証タグ生成部３７は、図２に示した加算部１０６及び短縮部１０７が有している機能

と実質的に同様の機能によって実現できる。認証タグ生成部３７は、チェックサムとハッシュ値と暗号化ナンスとを用いて認証タグを生成する。なお、認証タグ生成部３７は、チェックサムとハッシュ値と暗号化ナンスとの和に基づいて、認証タグを生成してもよい。また、認証タグ生成部３７は、この和を短縮することによって、認証タグを生成してもよい。出力部３８は、図２に示した出力部１０８が有している機能と実質的に同様の機能によって実現できる。出力部３８は、暗号文及び認証タグを出力するための制御を行う。

【００９９】

図１２は、実施の形態２にかかる認証復号装置４０を示す図である。実施の形態２にかかる認証復号装置４０は、実施の形態１にかかる認証復号装置２０に対応する。実施の形態２にかかる認証復号装置４０は、入力部４１と、平文復号部４３と、チェックサム生成部４４と、ハッシュ部４５と、ナンス暗号化部４６と、検証用タグ生成部４７と、検証部４８とを有する。

【０１００】

入力部４１は、入力手段（第２の入力手段）としての機能を有する。平文復号部４３は、平文復号手段（Ｔｗｅａｋ付き復号手段又は平文生成手段）としての機能を有する。チェックサム生成部４４は、チェックサム生成手段（第２のチェックサム生成手段）としての機能を有する。ハッシュ部４５は、ハッシュ手段（第２のハッシュ手段）としての機能を有する。ナンス暗号化部４６は、ナンス暗号化手段（第２のナンス暗号化手段）としての機能を有する。検証用タグ生成部４７は、検証用タグ生成手段（加算手段及び短縮手段）としての機能を有する。検証部４８は、検証手段（タグ検証手段及び出力手段）としての機能を有する。

【０１０１】

入力部４１は、図３に示した入力部２００が有している機能と実質的に同様の機能によって実現できる。入力部４１は、暗号文、認証タグ及びナンスの入力を受け付ける。なお、入力部４１は、ヘッダの入力を受け付けてもよい。平文復号部４３は、図３に示したＴｗｅａｋ付き復号部２０１が有している機能と実質的に同様の機能によって実現できる。平文復号部４３は、暗号文を分割したブロックごとに、ナンスを補助変数として用いて復号することで、暗号文に対応する平文を生成する。

【０１０２】

チェックサム生成部４４は、図３に示したチェックサム生成部２０２が有している機能と実質的に同様の機能によって実現できる。チェックサム生成部４４は、平文を用いてチェックサムを生成する。ハッシュ部４５は、図３に示したヘッダハッシュ部２０４が有している機能と実質的に同様の機能によって実現できる。ハッシュ部４５は、ハッシュ値を取得する。なお、ヘッダが入力される場合、ハッシュ部４５は、ヘッダとハッシュ関数（ユニバーサルハッシュ関数）とを用いてハッシュ値を取得してもよい。ナンス暗号化部４６は、図３に示したナンス暗号化部２０３が有している機能と実質的に同様の機能によって実現できる。ナンス暗号化部４６は、ナンスを暗号化して暗号化ナンスを取得する。

【０１０３】

検証用タグ生成部４７は、図３に示した加算部２０５及び短縮部２０６が有している機能と実質的に同様の機能によって実現できる。検証用タグ生成部４７は、チェックサムとハッシュ値と暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成する。なお、検証用タグ生成部４７は、チェックサムとハッシュ値と暗号化ナンスとの和に基づいて、検証用タグを生成してもよい。また、検証用タグ生成部４７は、この和を短縮することによって、検証用タグを生成してもよい。

【０１０４】

検証部４８は、図３に示したタグ検証部２０７が有している機能と実質的に同様の機能によって実現できる。検証部４８は、認証タグと検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う。なお、検証部４８は、認証タグと検証用タグとが一致する場合、検証結果として、平文を出力するための制御を行ってもよい。一方、検証部４８は、認証タグと検証用タグとが一致しない場合、検証結果と

して、エラーシンボルを出力するための制御を行ってもよい。

【０１０５】

実施の形態２にかかる認証暗号化装置３０及び認証復号装置４０は、上述した構成によって、暗号化及び復号における遅延を抑制することが可能である。なお、認証暗号化装置３０及び認証復号装置４０を有する認証暗号システムによっても、暗号化及び復号における遅延を抑制することが可能である。また、認証暗号化装置３０によって実行される認証暗号化方法及び認証暗号化方法を実行するプログラムによっても、暗号化及び復号における遅延を抑制することが可能である。また、認証復号装置４０によって実行される認証復号方法及び認証復号方法を実行するプログラムによっても、暗号化及び復号における遅延を抑制することが可能である。

【０１０６】

（ハードウェア構成例）

上述した各実施形態に係る装置およびシステムを、１つの計算処理装置（情報処理装置、コンピュータ）を用いて実現するハードウェア資源の構成例について説明する。但し、各実施形態に係る装置（認証暗号化装置及び認証復号装置）は、物理的または機能的に少なくとも２つの計算処理装置を用いて実現されてもよい。また、各実施形態に係る装置は、専用の装置として実現されてもよいし、汎用の情報処理装置で実現されてもよい。

【０１０７】

図１３は、各実施形態に係る装置およびシステムを実現可能な計算処理装置のハードウェア構成例を概略的に示すブロック図である。計算処理装置１２０は、ＣＰＵ１２１、揮発性記憶装置１２２、ディスク１２３、不揮発性記録媒体１２４、及び、通信ＩＦ１２７（ＩＦ：Interface）を有する。したがって、各実施形態に係る装置は、ＣＰＵ１２１、揮発性記憶装置１２２、ディスク１２３、不揮発性記録媒体１２４、及び、通信ＩＦ１２７を有しているといえる。計算処理装置１２０は、入力装置１２５及び出力装置１２６に接続可能であってもよい。計算処理装置１２０は、入力装置１２５及び出力装置１２６を備えていてもよい。また、計算処理装置１２０は、通信ＩＦ１２７を介して、他の計算処理装置、及び、通信装置と情報を送受信することができる。

【０１０８】

不揮発性記録媒体１２４は、コンピュータが読み取り可能な、たとえば、コンパクトディスク（Compact Disc)、デジタルバーサタイルディスク（Digital Versatile Disc）である。また、不揮発性記録媒体１２４は、ＵＳＢ（Universal Serial Bus）メモリ、ソリッドステートドライブ（Solid State Drive）等であってもよい。不揮発性記録媒体１２４は、電源を供給しなくても係るプログラムを保持し、持ち運びを可能にする。なお、不揮発性記録媒体１２４は、上述した媒体に限定されない。また、不揮発性記録媒体１２４の代わりに、通信ＩＦ１２７及び通信ネットワークを介して、係るプログラムが供給されてもよい。

【０１０９】

揮発性記憶装置１２２は、コンピュータが読み取り可能であって、一時的にデータを記憶することができる。揮発性記憶装置１２２は、ＤＲＡＭ（dynamic random Access memory）、ＳＲＡＭ（static random Access memory）等のメモリ等である。

【０１１０】

すなわち、ＣＰＵ１２１は、ディスク１２３に格納されているソフトウェアプログラム（コンピュータ・プログラム：以下、単に「プログラム」と称する）を、実行する際に揮発性記憶装置１２２にコピーし、演算処理を実行する。ＣＰＵ１２１は、プログラムの実行に必要なデータを揮発性記憶装置１２２から読み取る。表示が必要な場合、ＣＰＵ１２１は、出力装置１２６に出力結果を表示する。外部からプログラムを入力する場合、ＣＰＵ１２１は、入力装置１２５からプログラムを取得する。ＣＰＵ１２１は、上述した図２，図３，図１１，図１２に示される各構成要素の機能（処理）に対応するプログラムを解釈し実行する。ＣＰＵ１２１は、上述した各実施形態において説明した処理を実行する。言い換えると、上述した図２，図３，図１１，図１２に示される各構成要素の機能は、デ

ィスク１２３又は揮発性記憶装置１２２に格納されたプログラムを、ＣＰＵ１２１が実行することによって実現され得る。

【０１１１】

すなわち、各実施形態は、上述したプログラムによっても成し得ると捉えることができる。さらに、上述したプログラムが記録されたコンピュータが読み取り可能な不揮発性の記録媒体によっても、上述した各実施形態は成し得ると捉えることができる。

【０１１２】

（変形例）

なお、本発明は上記実施形態に限られたものではなく、趣旨を逸脱しない範囲で適宜変更することが可能である。例えば、上述したフローチャートにおいて、各処理（ステップ）の順序は、適宜、変更可能である。また、複数ある処理（ステップ）のうちの１つ以上は、省略されてもよい。

【０１１３】

例えば、図４に示したフローチャートにおいて、Ｓ１０４～Ｓ１１０の処理の順序は、図４に示した順序に限定されない。さらに、Ｓ１０４～Ｓ１１０の処理は、並行して実行され得る。同様に、図５に示したフローチャートにおいて、Ｓ２０４，Ｓ２０６，Ｓ２０８の処理の順序は、図５に示した順序に限定されない。さらに、Ｓ２０４，Ｓ２０６，Ｓ２０８の処理は、並行して実行され得る。

【０１１４】

上述の例において、プログラムは、様々なタイプの非一時的なコンピュータ可読媒体（non-transitory computer readable medium）を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体（tangible storage medium）を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えばフレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば光磁気ディスク）、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、半導体メモリ（例えば、マスクＲＯＭ、ＰＲＯＭ（Programmable ROM）、ＥＰＲＯＭ（Erasable PROM）、フラッシュＲＯＭ、ＲＡＭ）を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体（transitory computer readable medium）によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

【０１１５】

以上、実施の形態を参照して本願発明を説明したが、本願発明は上記によって限定されるものではない。本願発明の構成や詳細には、発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

【０１１６】

上記の実施形態の一部又は全部は、以下の付記のようにも記載されうるが、以下には限られない。

（付記１）

平文の入力を受け付ける入力手段と、

過去に生成された値とは異なるナンスを生成するナンス生成手段と、

前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成する平文暗号化手段と、

前記平文を用いてチェックサムを生成するチェックサム生成手段と、

ハッシュ値を取得するハッシュ手段と、

前記ナンスを暗号化して暗号化ナンスを取得するナンス暗号化手段と、

前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成する認証タグ生成手段と、

前記暗号文及び前記認証タグを出力するための制御を行う出力手段と、

を有する認証暗号化装置。

（付記２）
前記認証タグ生成手段は、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとの和に基づいて、前記認証タグを生成する、
付記１に記載の認証暗号化装置。
（付記３）
前記認証タグ生成手段は、前記和を短縮することによって、前記認証タグを生成する、
付記２に記載の認証暗号化装置。
（付記４）
前記ナンス暗号化手段は、前記チェックサムと同じ長さの前記暗号化ナンスを取得する、
付記１から３のいずれか１項に記載の認証暗号化装置。
（付記５）
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダとハッシュ関数とを用いて、前記ハッシュ値を取得する、
付記１から４のいずれか１項に記載の認証暗号化装置。
（付記６）
前記平文暗号化手段は、前記平文を所定長のブロックに分割した際のブロックのｉ番目の平文ブロックに対して、前記ナンスと前記平文ブロックのインデックスｉとを含めた前記補助変数であるＴｗｅａｋを用いて、前記平文を前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化する、
付記１から５のいずれか１項に記載の認証暗号化装置。
（付記７）
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダを所定長のブロックに分割した際のブロックのｉ番目のヘッダブロックに対して、前記ヘッダブロックのインデックスｉを含めた前記補助変数であるＴｗｅａｋを用いて、前記ヘッダを前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化することで、前記ハッシュ値を取得する、
付記６に記載の認証暗号化装置。
（付記８）
前記ハッシュ手段は、前記ヘッダを暗号化したブロックを加算することで、前記ハッシュ値を取得する、
付記７に記載の認証暗号化装置。
（付記９）
前記ナンス暗号化手段は、前記ナンスを含めた前記補助変数であるＴｗｅａｋを用いて、Ｔｗｅａｋａｂｌｅブロック暗号で暗号化を行うことによって、前記暗号化ナンスを取得する、
付記６から８のいずれか１項に記載の認証暗号化装置。
（付記１０）
前記Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードである、
付記６から９のいずれか１項に記載の認証暗号化装置。
（付記１１）
暗号文、認証タグ及びナンスの入力を受け付ける入力手段と、
前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成する平文復号手段と、
前記平文を用いてチェックサムを生成するチェックサム生成手段と、
ハッシュ値を取得するハッシュ手段と、
前記ナンスを暗号化して暗号化ナンスを取得するナンス暗号化手段と、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成する検証用タグ生成手段と、
前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証

結果を出力するための制御を行う検証手段と、
を有する認証復号装置。
（付記１２）
前記検証用タグ生成手段は、前記チェックサムと前記ハッシュ値と前記暗号化ナンスとの和に基づいて、前記検証用タグを生成する、
付記１１に記載の認証復号装置。
（付記１３）
前記検証用タグ生成手段は、前記和を短縮することによって、前記検証用タグを生成する、
付記１２に記載の認証復号装置。
（付記１４）
前記ナンス暗号化手段は、前記チェックサムと同じ長さの前記暗号化ナンスを取得する、
付記１１から１３のいずれか１項に記載の認証復号装置。
（付記１５）
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダとハッシュ関数とを用いて、前記ハッシュ値を取得する、
付記１１から１４のいずれか１項に記載の認証復号装置。
（付記１６）
前記平文復号手段は、前記暗号文を所定長のブロックに分割した際のブロックのｉ番目の暗号文ブロックに対して、前記ナンスと前記暗号文ブロックのインデックスｉとを含めた前記補助変数であるＴｗｅａｋを用いて、前記暗号文を前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で復号する、
付記１１から１５のいずれか１項に記載の認証復号装置。
（付記１７）
前記入力手段は、ヘッダを受け付け、
前記ハッシュ手段は、前記ヘッダを所定長のブロックに分割した際のブロックのｉ番目のヘッダブロックに対して、前記ヘッダブロックのインデックスｉを含めた前記補助変数であるＴｗｅａｋを用いて、前記ヘッダを前記ブロックごとに並列にＴｗｅａｋａｂｌｅブロック暗号で暗号化することで、前記ハッシュ値を取得する、
付記１６に記載の認証復号装置。
（付記１８）
前記ハッシュ手段は、前記ヘッダを暗号化したブロックを加算することで、前記ハッシュ値を取得する、
付記１７に記載の認証復号装置。
（付記１９）
前記ナンス暗号化手段は、前記ナンスを含めた前記補助変数であるＴｗｅａｋを用いて、Ｔｗｅａｋａｂｌｅブロック暗号で暗号化を行うことによって、前記暗号化ナンスを取得する、
付記１６から１８のいずれか１項に記載の認証復号装置。
（付記２０）
前記Ｔｗｅａｋａｂｌｅブロック暗号は、ブロック暗号を用いたＸＥＸ＊モードである、
付記１６から１９のいずれか１項に記載の認証復号装置。
（付記２１）
認証暗号化装置と、
前記認証暗号化装置との間で通信を行う認証復号装置と、
を有し、
前記認証暗号化装置は、
平文の入力を受け付ける第１の入力手段と、
過去に生成された値とは異なるナンスを生成するナンス生成手段と、

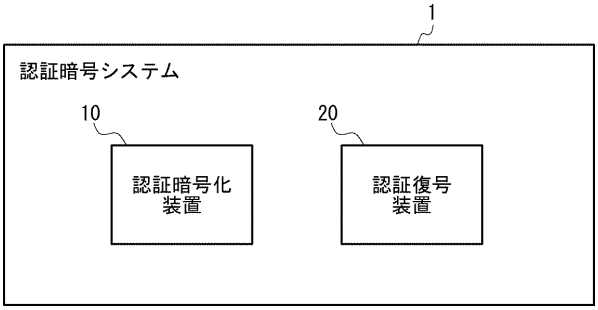
前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成する平文暗号化手段と、
前記平文を用いてチェックサムを生成する第１のチェックサム生成手段と、
ハッシュ値を取得する第１のハッシュ手段と、
前記ナンスを暗号化して暗号化ナンスを取得する第１のナンス暗号化手段と、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成する認証タグ生成手段と、
前記暗号文及び前記認証タグを出力するための制御を行う出力手段と、
を有し、
前記認証復号装置は、
暗号文、認証タグ及びナンスの入力を受け付ける第２の入力手段と、
前記第２の入力手段によって入力された前記暗号文を分割したブロックごとに、前記第２の入力手段によって入力された前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成する平文復号手段と、
前記平文復号手段によって生成された前記平文を用いてチェックサムを生成する第２のチェックサム生成手段と、
ハッシュ値を取得する第２のハッシュ手段と、
前記第２の入力手段によって入力された前記ナンスを暗号化して暗号化ナンスを取得する第２のナンス暗号化手段と、
前記第２のチェックサム生成手段によって生成された前記チェックサムと、前記第２のハッシュ手段によって取得された前記ハッシュ値と、前記第２のナンス暗号化手段によって取得された前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成する検証用タグ生成手段と、
前記認証タグ生成手段によって生成された前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う検証手段と、
を有する、
認証暗号システム。
（付記２２）
平文の入力を受け付け、
過去に生成された値とは異なるナンスを生成し、
前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成し、
前記平文を用いてチェックサムを生成し、
ハッシュ値を取得し、
前記ナンスを暗号化して暗号化ナンスを取得し、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成し、
前記暗号文及び前記認証タグを出力するための制御を行う、
認証暗号化方法。
（付記２３）
暗号文、認証タグ及びナンスの入力を受け付け、
前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成し、
前記平文を用いてチェックサムを生成し、
ハッシュ値を取得し、
前記ナンスを暗号化して暗号化ナンスを取得し、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成し、
前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行う、
認証復号方法。

（付記２４）
平文の入力を受け付けるステップと、
過去に生成された値とは異なるナンスを生成するステップと、
前記平文を分割したブロックごとに、前記ナンスを補助変数として用いて暗号化することで、前記平文に対応する暗号文を生成するステップと、
前記平文を用いてチェックサムを生成するステップと、
ハッシュ値を取得するステップと、
前記ナンスを暗号化して暗号化ナンスを取得するステップと、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて認証タグを生成し、
前記暗号文及び前記認証タグを出力するための制御を行うステップと、
をコンピュータに実行させるプログラムが格納された非一時的なコンピュータ可読媒体。
（付記２５）
暗号文、認証タグ及びナンスの入力を受け付けるステップと、
前記暗号文を分割したブロックごとに、前記ナンスを補助変数として用いて復号することで、前記暗号文に対応する平文を生成するステップと、
前記平文を用いてチェックサムを生成するステップと、
ハッシュ値を取得するステップと、
前記ナンスを暗号化して暗号化ナンスを取得するステップと、
前記チェックサムと前記ハッシュ値と前記暗号化ナンスとを用いて、推定された認証タグである検証用タグを生成するステップと、
前記認証タグと前記検証用タグとを比較することによって改ざんの有無を検証し、検証結果を出力するための制御を行うステップと、
をコンピュータに実行させるプログラムが格納された非一時的なコンピュータ可読媒体。
【符号の説明】
【０１１７】
１　認証暗号システム
１０　認証暗号化装置
１００　入力部
１０１　ナンス生成部
１０２　Ｔｗｅａｋ付き暗号化部
１０３　チェックサム生成部
１０４　ヘッダハッシュ部
１０５　ナンス暗号化部
１０６　加算部
１０７　短縮部
１０８　出力部
２０　認証復号装置
２００　入力部
２０１　Ｔｗｅａｋ付き復号部
２０２　チェックサム生成部
２０３　ナンス暗号化部
２０４　ヘッダハッシュ部
２０５　加算部
２０６　短縮部
２０７　タグ検証部
３０　認証暗号化装置
３１　入力部
３２　ナンス生成部
３３　平文暗号化部
３４　チェックサム生成部

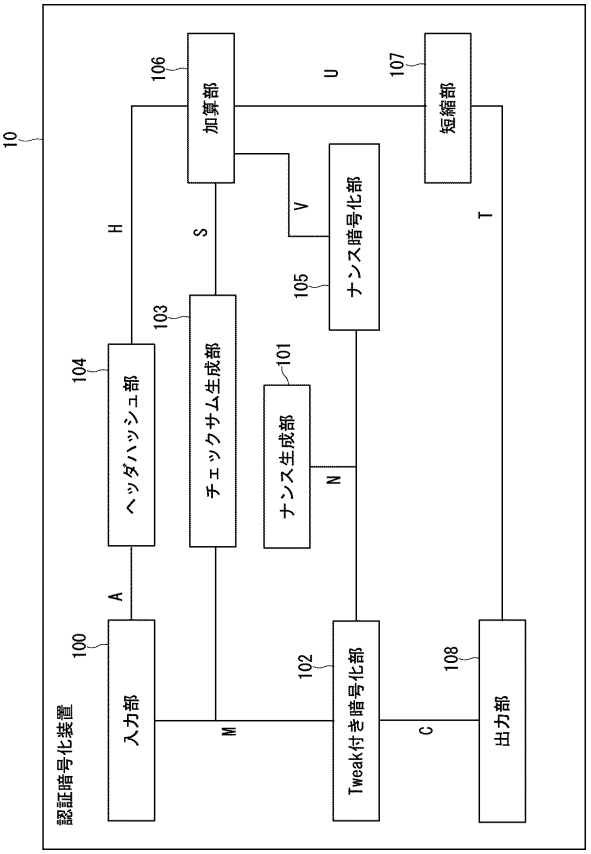
３５　ハッシュ部
３６　ナンス暗号化部
３７　認証タグ生成部
３８　出力部
４０　認証復号装置
４１　入力部
４３　平文復号部
４４　チェックサム生成部
４５　ハッシュ部
４６　ナンス暗号化部
４７　検証用タグ生成部
４８　検証部

【図面】

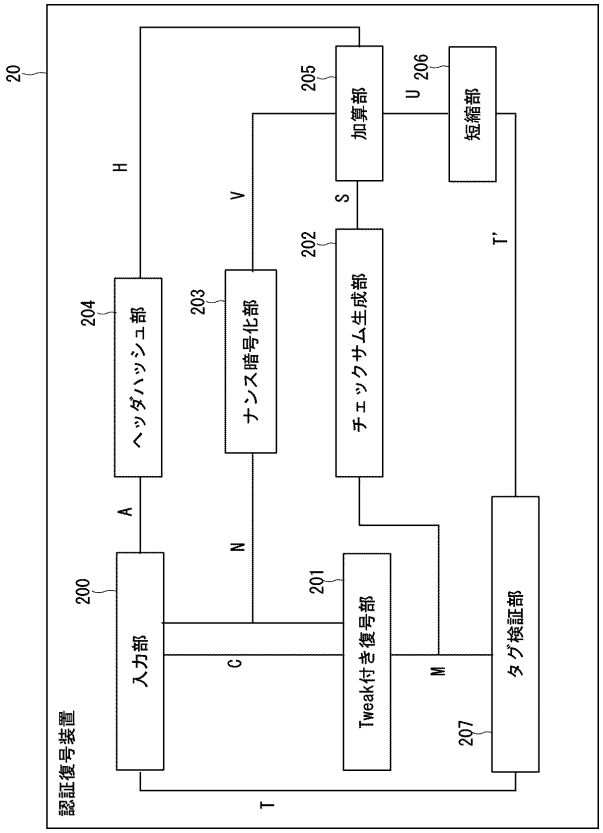
【図１】



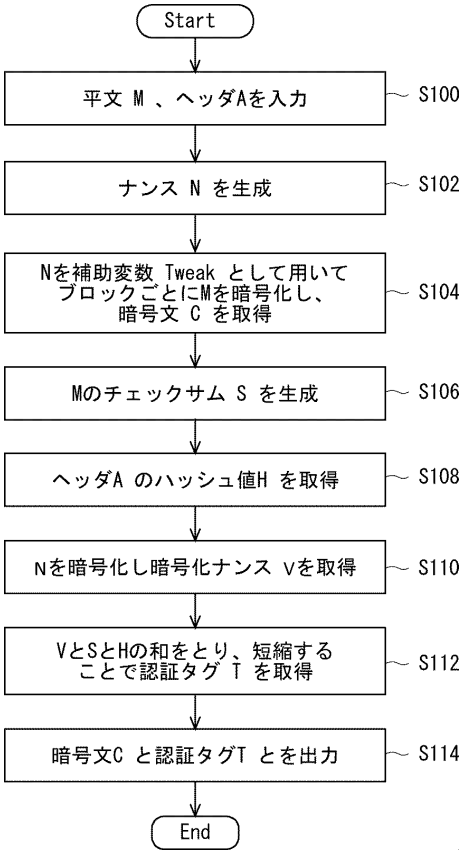
【図２】



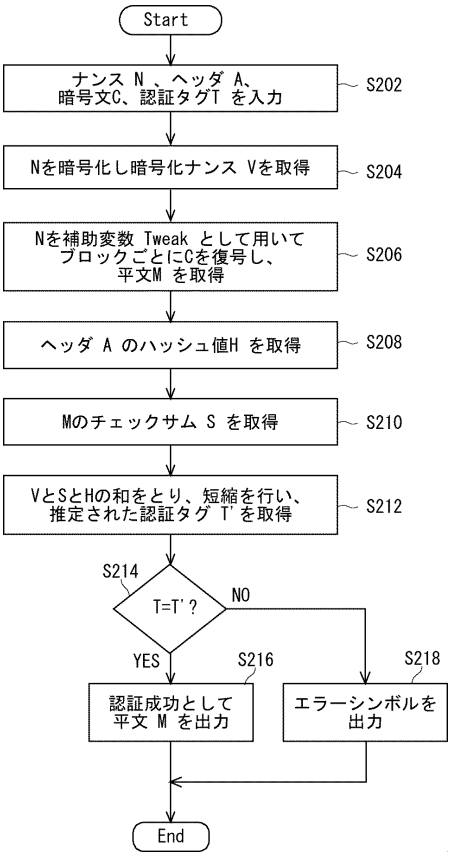
【図３】


20
認証復号装置
200
入力部
201
Tweak付き復号部
202
チェックサム生成部
203
ナンス暗号化部
204
ヘッダハッシュ部
205
加算部
206
短縮部
207
タグ検証部
A
C
H
M
N
S
T
T'
U
V

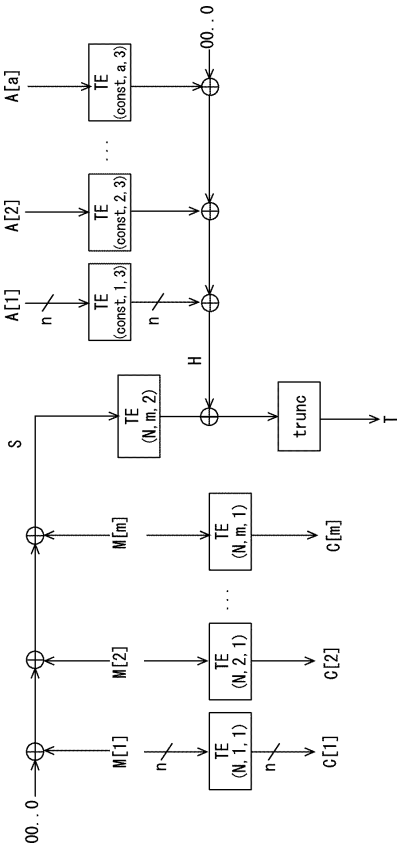
【図４】


Start
平文 M 、ヘッダAを入力
S100
ナンス N を生成
S102
Nを補助変数 Tweak として用いて
ブロックごとにMを暗号化し、
暗号文 C を取得
S104
Mのチェックサム S を生成
S106
ヘッダA のハッシュ値H を取得
S108
Nを暗号化し暗号化ナンス Vを取得
S110
VとSとHの和をとり、短縮する
ことで認証タグ T を取得
S112
暗号文C と認証タグT とを出力
S114
End

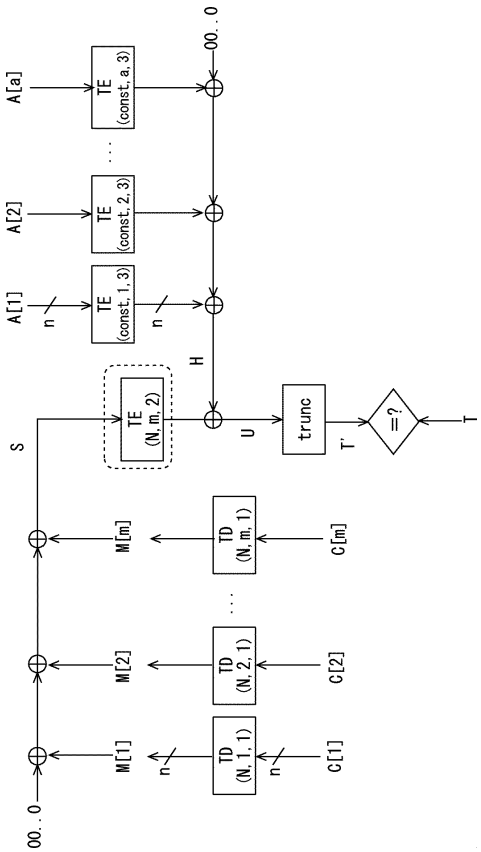
【図５】


Start
ナンス N 、ヘッダ A、
暗号文C、認証タグT を入力
S202
Nを暗号化し暗号化ナンス Vを取得
S204
Nを補助変数 Tweak として用いて
ブロックごとにCを復号し、
平文M を取得
S206
ヘッダ A のハッシュ値H を取得
S208
Mのチェックサム S を取得
S210
VとSとHの和をとり、短縮を行い、
推定された認証タグ T'を取得
S212
S214
T=T'？
NO
YES
S216
認証成功として
平文 M を出力
S218
エラーシンボルを
出力
End

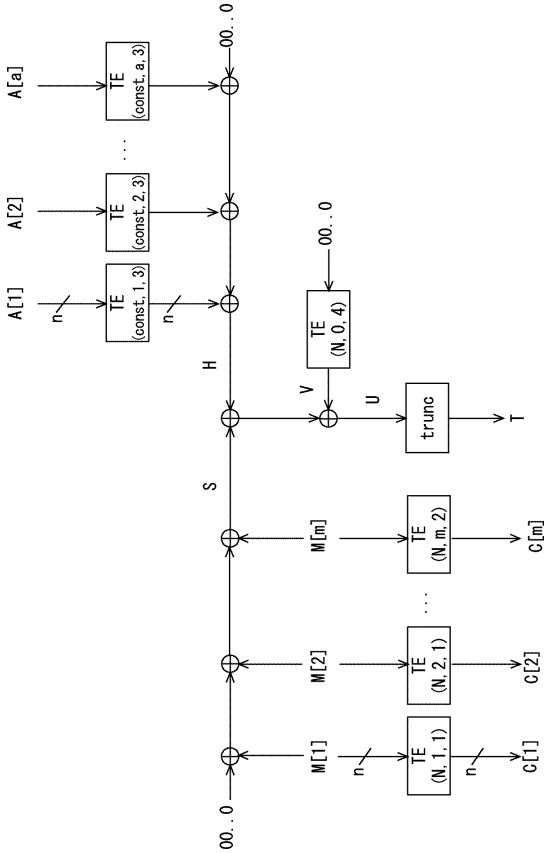
【図６】


00..0
A[a]
TE (const.a,3)
A[2]
TE (const.2,3)
A[1]
TE (const.1,3)
n
H
S
TE (N,m,2)
trunc
T
M[m]
TE (N,m,1)
C[m]
M[2]
TE (N,2,1)
C[2]
M[1]
TE (N,1,1)
C[1]

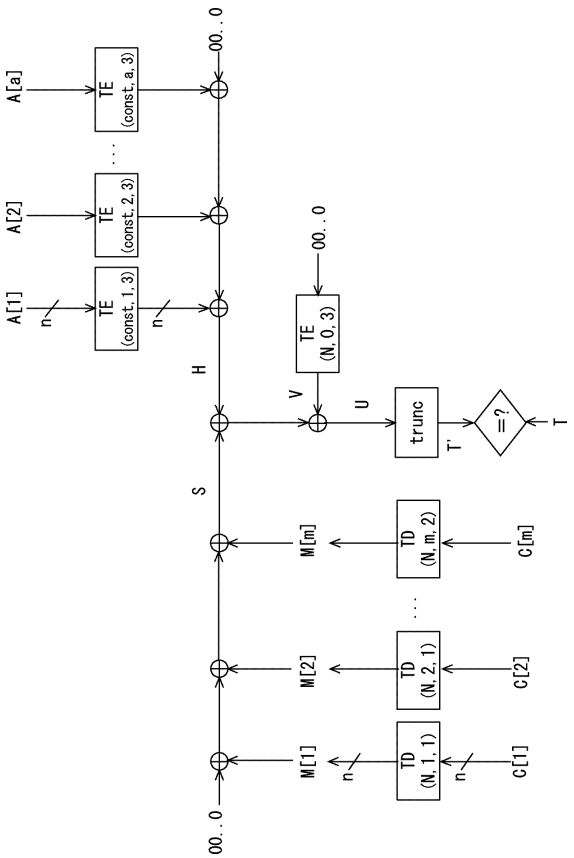
【図７】



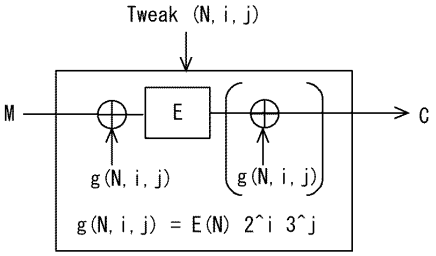
【図８】



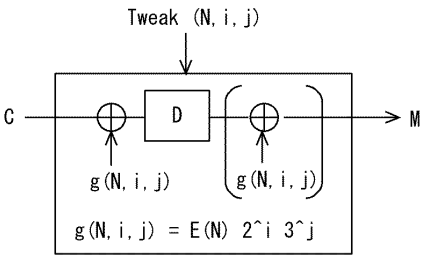
【図９】



【図１０】

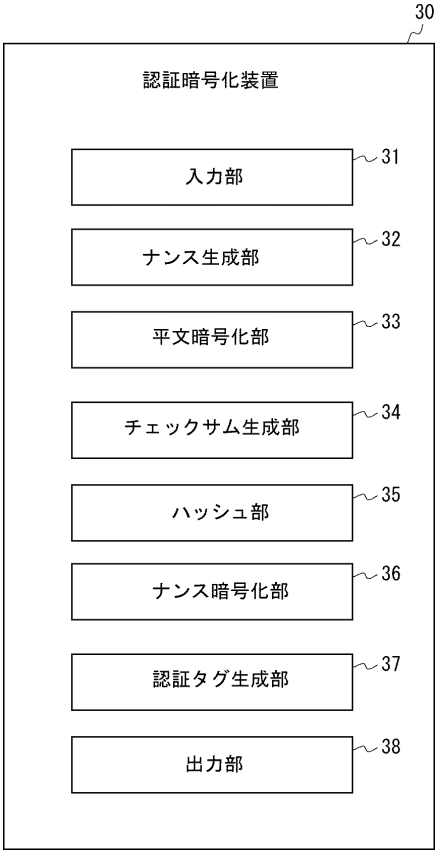


C = TE((N, i, j), M)

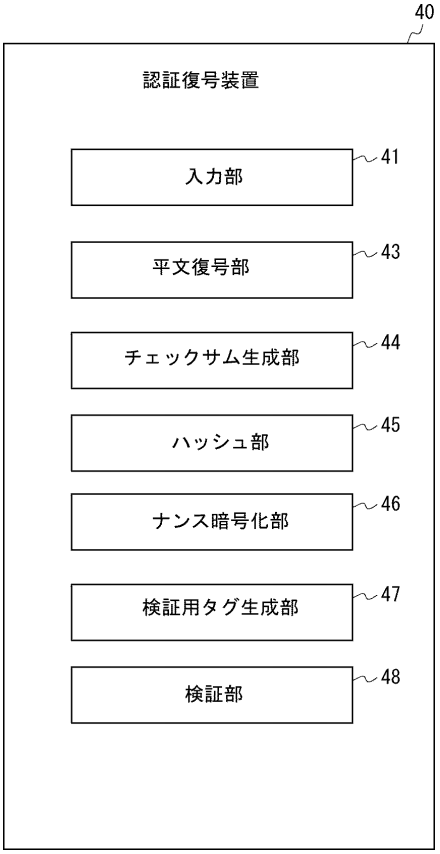


M = TD((N, i, j), M)

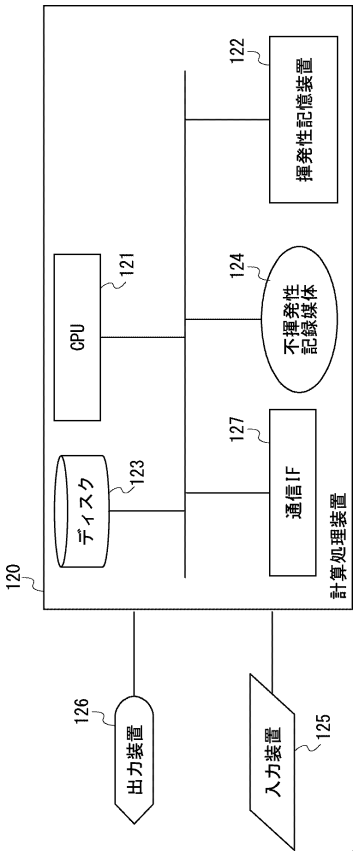
【図１１】


30
認証暗号化装置
入力部
31
ナンス生成部
32
平文暗号化部
33
チェックサム生成部
34
ハッシュ部
35
ナンス暗号化部
36
認証タグ生成部
37
出力部
38

【図１２】


40
認証復号装置
入力部
41
平文復号部
43
チェックサム生成部
44
ハッシュ部
45
ナンス暗号化部
46
検証用タグ生成部
47
検証部
48

【図１３】


120
計算処理装置
CPU
121
揮発性記憶装置
122
ディスク
123
不揮発性記録媒体
124
通信IF
127
出力装置
126
入力装置
125

フロントページの続き

宮城県仙台市青葉区片平二丁目１番１号 国立大学法人東北大学内

審査官　行田 悦資

(56)参考文献　国際公開第２０１５／０１５７０２（WO，Ａ１）
特開２０１６－０７５７６５（ＪＰ，Ａ）
国際公開第２０１９／１６３０３２（WO，Ａ１）
特開２０１９－０１５９１８（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　１／００
Ｈ０４Ｌ　９／３２