(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5333450号
(P5333450)
(45)発行日　平成25年11月6日(2013.11.6)　(24)登録日　平成25年8月9日(2013.8.9)

(51)Int.Cl.　F I
G09C 1/00 (2006.01)　G09C 1/00 610A

請求項の数 8　(全 15 頁)

(21)出願番号	特願2010-526597 (P2010-526597)
(86)(22)出願日	平成21年5月22日 (2009.5.22)
(86)国際出願番号	PCT/JP2009/059438
(87)国際公開番号	WO2010/024004
(87)国際公開日	平成22年3月4日 (2010.3.4)
審査請求日	平成24年4月12日 (2012.4.12)
(31)優先権主張番号	特願2008-221657 (P2008-221657)
(32)優先日	平成20年8月29日 (2008.8.29)
(33)優先権主張国	日本国(JP)

(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　100123788
弁理士　宮崎　昭夫
(74)代理人　100106138
弁理士　石橋　政幸
(74)代理人　100127454
弁理士　緒方　雅昭
(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

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】調整値付きブロック暗号化装置、方法及びプログラム並びに復号装置、方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
ｎビットの平文とｎビットの調整値とを入力する入力手段と、
前記調整値をｎビットブロック暗号関数で暗号化し、１より大きくｎ／２未満の値をｍとして、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成する調整値依存鍵導出手段と、
前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号で暗号化し、暗号化した結果に前記マスク値を加算することにより暗号文を生成するマスク付きブロック暗号化手段と、
前記暗号文を出力する出力手段と、
を有する調整値付きブロック暗号化装置。
【請求項２】
前記調整値依存鍵導出手段は、装置の鍵を元にｎビットのブロック暗号の鍵を生成し、生成した前記ブロック暗号の鍵を前記暗号処理において用いることを特徴とする請求項１に記載の調整値付きブロック暗号化装置。
【請求項３】
ｎビットの暗号文とｎビットの調整値とを入力する入力手段と、
前記調整値をｎビットブロック暗号で暗号化し、１より大きくｎ／２未満の値をｍとし

て、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成する調整値依存鍵導出手段と、

前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号に対応する復号関数で復号し、復号した結果に前記マスク値を加算することにより平文を生成するマスク付きブロック復号手段と、

前記平文を出力する平文出力手段と、

を有する調整値付きブロック復号装置。

【請求項４】

前記調整値依存鍵導出手段は、装置の鍵を元にｎビットのブロック暗号の鍵を生成し、生成した前記ブロック暗号の鍵を前記暗号処理において用いることを特徴とする請求項３に記載の調整値付きブロック復号装置。

【請求項５】

プログラムにしたがって処理を実行するＣＰＵを有するコンピュータによる調整値付きブロック暗号化方法であって、

前記ＣＰＵがｎビットの平文とｎビットの調整値とを入力し、

前記ＣＰＵが、前記調整値をｎビットブロック暗号関数で暗号化し、１より大きくｎ／２未満の値をｍとして、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成し、

前記ＣＰＵが、前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号で暗号化し、暗号化した結果に前記マスク値を加算することにより暗号文を生成し、

前記ＣＰＵが前記暗号文を出力する、調整値付きブロック暗号化方法。

【請求項６】

プログラムにしたがって処理を実行するＣＰＵを有するコンピュータによる調整値付きブロック復号方法であって、

前記ＣＰＵがｎビットの暗号文とｎビットの調整値とを入力し、

前記ＣＰＵが、前記調整値をｎビットブロック暗号で暗号化し、１より大きくｎ／２未満の値をｍとして、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成し、

前記ＣＰＵが、前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号に対応する復号関数で復号し、復号した結果に前記マスク値を加算することにより平文を生成し、

前記ＣＰＵが前記平文を出力する、調整値付きブロック復号方法。

【請求項７】

コンピュータを請求項１記載の調整値付きブロック暗号化装置として機能させるためのプログラム。

【請求項８】

コンピュータを請求項３記載の調整値付きブロック復号装置として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ブロック暗号の運用モードに関し、特にｎビットブロック暗号による汎用的で高い安全性を持つ調整値付きブロック暗号化装置、方法及びプログラム並びに復号装置

、方法及びプログラムに関する。
【背景技術】
【０００２】
ブロック暗号とは、鍵により一意に定まる置換の集合であり、置換への入力が平文、出力が暗号文にそれぞれ相当する。平文や暗号文の長さをブロックサイズという。ブロックサイズがｎビットのブロック暗号を、一般的にｎビットブロック暗号という。ブロック暗号化・復号に関連する技術としては、特許文献１に開示される「暗号化方法および装置」がある。
【０００３】
調整値付きブロック暗号とは、通常のブロック暗号が持つ入出力である（平文、暗号文、鍵）以外にtweakと呼ばれる調整値を持つブロック暗号のことであり、tweakableブロック暗号とも呼ばれる。調整値と鍵とが定まれば、平文と暗号文とが一対一に対応することが条件である。すなわち、任意の調整値付きブロック暗号の暗号化関数TWENCと、対応する復号関数TWDECとは、平文M、暗号文C、鍵K、調整値Tについて、常に下記式（１）を満たす。
【０００４】
【数１】

$$C = TWENC(K,T,M) \leftrightarrow M = TWDEC(K,T,C) \quad \cdots (1)$$

【０００５】
式（１）を含めた調整値付きブロック暗号の形式的な定義と安全性要件とは、非特許文献１に開示されている。安全性要件について簡単に言えば、調整値付きブロック暗号においては、調整値が異なる二つのブロック暗号の出力が、調整値と入力が攻撃者に既知であっても、その攻撃者には互いに独立でランダムな値に見えることが要求される。この性質が満たされるとき、調整値付きブロック暗号は安全であるという。
【０００６】
また、非特許文献１において、理論的に安全な調整値付きブロック暗号が通常のブロック暗号の運用モード（以下、モードという）として得られる、換言すると、ブロック暗号をブラックボックスとして用いた変換として得られるということが示されている。ただし、ここでいう理論的安全性とは、あるブロック暗号のモードとして得られる調整値付きブロック暗号の安全性が、元となるブロック暗号の安全性に帰着できる、すなわち安全なブロック暗号を用いる限り、得られる調整値付きブロック暗号も安全であると言うことを示す。
【０００７】
さらに、安全性の定義には、攻撃者が選択平文攻撃（chosen-plaintext attack, CPA）のみ可能な場合の安全性と、選択平文攻撃と選択暗号文攻撃（chosen-ciphertext attack, CCA）とを組み合わせて実行可能な場合の安全性との２種類があり、前者をCPA-security、後者をCCA-securityと呼ぶ。
【０００８】
安全な調整値付きブロック暗号は、高度な暗号化機能の実現のための鍵となる技術であることが知られている。例えば、非特許文献２には、CCA-securityを有する調整値付きブロック暗号を用いると大変効率の良い認証機能付き暗号が実現できることや、CCA-securityを有する調整値付きブロック暗号を用いると、効率の良い、並列実行可能なメッセージ認証コードを実現できることが指摘されている。また、CCA-securityを有する調整値付きブロック暗号は、ディスクセクタ暗号化などのストレージ暗号化のための必須の技術であることも知られている。
【０００９】
ここで、非特許文献１で提案されたモードをLRWモードと称することとする。また、ｎビットブロック暗号Eを用いたLRWモードを図９（ａ）、（ｂ）に示す。ｎビットブロック暗号（暗号化関数をEnc、復号関数をDecとする）を用いたLRWモードは、一般に、鍵K、調

整値T、平文Mが与えられたとき、下記式（２）によって暗号文Cを得る。
【００１０】
【数２】

$$C = Enc(K1,M+F(K2,T))+F(K2,T) \quad \cdots(2)$$

【００１１】
暗号文Cから平文Mへの復号は、下記式（３）となる。
【００１２】
【数３】

$$M = Dec(K1,C+F(K2,T))+F(K2,T) \quad \cdots(3)$$

【００１３】
K1はブロック暗号の鍵、K2はブロック暗号の処理の前後に足される鍵付き関数F（オフセット関数と呼ばれる）。ここで、Fは、セキュリティパラメータをｅ（０≦ｅ≦１）としたとき、任意のｃ、ｘ、ｘ’（ｘ≠ｘ’）について、下記式（４）を満たす性質を持つ必要がある。ただし、＋は排他的論理和（ＸＯＲ）を表す。
【００１４】
【数４】

$$Pr[f(K,x) + f(K,x')= c] < e \quad \cdots(4)$$

【００１５】
この性質を持つとき、f(K,*)はe-almost XOR universal (e-AXU)であるという。e-AXU関数はユニバーサルハッシュ関数の一種である。これを実現するには、例えば有限体GF(2n)上の乗算mulを用いて、F(K2,T) = mul(K2,T)とすることがよく知られている。このときは、Fは1/2n-AXUである。
【００１６】
e-AXU関数はmul以外にも、非特許文献３などで提案されている方式で実現可能である。これらは特定の実装環境においては一般的なブロック暗号より数倍高速となることが知られている。
【００１７】
ｎビットブロック暗号を用いた調整値付きブロック暗号の構成方法としては、非特許文献１のLRWモードと、その変種である非特許文献２のXE、XEXモードがある。LRWモードやXEXモードは、上記式（２）、（３）で示される形式を持ち、CCA-securityを有する。
【００１８】
一方、XEモードは、外側のオフセットを省略した下記式（５）という形式をしており、CPA-securityを有している。
【００１９】
【数５】

$$C = Enc(K1,M+F(K2,T)) \quad \cdots(5)$$

【００２０】
LRWモードではK2はK1と独立であるのに対して、XEモード、XEXモードではK2は固定平文（例えばnビットの全ゼロ値）をEnc(K1,*)で暗号化した結果を用いることで、鍵サイズの効率化を図っている。重要なのは、いずれにおいても、その安全性保証は、一つの鍵で処理する暗号化回数qが2n/2よりも十分に小さい（これをq≪2n/2と表す）場合に限られていることである。2n/2はバースデーバウンドと呼ばれ、バースデーバウンド程度の回数の暗号化の結果を用いた攻撃は一般にバースデー攻撃と呼ばれる。このような攻撃は、64ビットブロック暗号を用いた場合には現実的な脅威となり、また128ビットブロック暗号を用

いた場合でも将来的なリスクと考えられるため、対策が必要である。
【００２１】
非特許文献４では、暗号化回数qがq≪2nのときに安全な調整値付きブロック暗号の構成方法が記載されているが、これは、元のブロック暗号が2nビットブロックのFeistel型暗号のときを扱っているため、問題が異なる（ブロック暗号のブロックサイズ(2nビット)のバースデーバウンドまでの安全性のみを保証している）。
【００２２】
非特許文献５など、従来よく行われている方法として、調整値ごとに複数のnビットブロック暗号の鍵を用意する方法がある。この方法は鍵の長さがnビットより十分長い（例えば2nや3nビット）場合か、鍵の長さがnビットであっても調整値の長さがごくわずかである場合は、簡便でバースデーバウンドを超えた安全性を提供する。しかし調整値の長さがある程度あって（例えばn/2ビット）、さらに鍵の長さがnビットである場合は、この方法では一般にバースデーバウンドを超えた安全性は保証できない。
【先行技術文献】
【特許文献】
【００２３】
【特許文献１】特開平９－２３０７８７号公報
【非特許文献】
【００２４】
【非特許文献１】M. Liskov, R. Rivest, D. Wagner, Tweakable Block Ciphers, Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings. Lecture Notes in Computer Science 2442 Springer 2002, pp. 31-46.
【非特許文献２】P. Rogaway: Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. Advances in Cryptology - ASIACRYPT2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings. Lecture Notes in Computer Science 3329 Springer 2004, pp. 16-31
【非特許文献３】S. Halevi and H. Krawczyk, MMH:Software Message Authentication in the Gbit/second rates, Fast Software Encryption, 4th Internatioanl Workshop, FSE '97, Lecture Notes in Computer Science; Vol. 1267, March. 1997
【非特許文献４】D. Goldenberg, S. Hohenberger, M. Liskov, E. C. Schwartz, H.Seyalioglu, On Tweaking Luby-Rackoff Blockciphers, Advances in Cryptology -ASIACRYPT 2007, 13th International Conference on the Theory and Applicationof Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings. Lecture Notes in Computer Science 4833 Springer 2007, pp. 342-356.
【非特許文献５】J. Black, P. Rogaway, CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions, Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings. Lecture Notes in Computer Science 1880 Springer 2000, pp. 197-215.
【発明の概要】
【発明が解決しようとする課題】
【００２５】
このように、ブロック暗号を用いた調整値付きブロック暗号は、バースデー攻撃によって破れる方式しか実現されていなかった。

【００２６】
本発明は係る問題に鑑みてなされたものであり、現実的なブロック暗号を用いて、バースデー攻撃への理論的耐性を持つ調整値付きブロック暗号を形成できる調整値付きブロック暗号化装置、方法及びプログラム並びに復号装置、方法及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【００２７】
上記目的を達成するため、本発明は、第１の態様として、ｎビットの平文とｎビットの調整値とを入力する入力手段と、前記調整値をｎビットブロック暗号関数で暗号化し、１より大きくｎ／２未満の値をｍとして、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成する調整値依存鍵導出手段と、前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号で暗号化し、暗号化した結果に前記マスク値を加算することにより暗号文を生成するマスク付きブロック暗号化手段と、前記暗号文を出力する出力手段と、を有する調整値付きブロック暗号化装置を提供するものである。
【００２８】
また、上記目的を達成するため、本発明は、第２の態様として、ｎビットの暗号文とｎビットの調整値とを入力する入力手段と、前記調整値をｎビットブロック暗号で暗号化し、１より大きくｎ／２未満の値をｍとして、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成する調整値依存鍵導出手段と、前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号に対応する復号関数で復号し、復号した結果に前記マスク値を加算することにより平文を生成するマスク付きブロック復号手段と、前記平文を出力する平文出力手段と、を有する調整値付きブロック復号装置を提供するものである。
【００２９】
上記目的を達成するため、本発明は、第３の態様として、プログラムにしたがって処理を実行するＣＰＵを有するコンピュータによる調整値付きブロック暗号化方法であって、前記ＣＰＵがｎビットの平文とｎビットの調整値とを入力し、前記ＣＰＵが、前記調整値をｎビットブロック暗号関数で暗号化し、１より大きくｎ／２未満の値をｍとして、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成し、前記ＣＰＵが、前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号で暗号化し、暗号化した結果に前記マスク値を加算することにより暗号文を生成し、前記ＣＰＵが前記暗号文を出力する、調整値付きブロック暗号化方法を提供するものである。
【００３０】
また、上記目的を達成するため、本発明は、第４の態様として、プログラムにしたがって処理を実行するＣＰＵを有するコンピュータによる調整値付きブロック復号方法であって、前記ＣＰＵがｎビットの暗号文とｎビットの調整値とを入力し、前記ＣＰＵが、前記調整値をｎビットブロック暗号で暗号化し、１より大きくｎ／２未満の値をｍとして、暗号化した結果のうちの任意のｎ－ｍビットを任意の値に固定し、固定した結果を、ｎビットの入力を持つ暗号処理で暗号化することにより、調整値依存鍵を生成し、前記ＣＰＵが、前記調整値を鍵付き関数へ入力することによりマスク値を生成し、該マスク値を前記平文へ加算し、加算した結果を、前記調整値依存鍵を鍵としたｎビットブロック暗号に対応する復号関数で復号し、復号した結果に前記マスク値を加算することにより平文を生成し、前記ＣＰＵが前記平文を出力する、調整値付きブロック復号方法を提供するものである。

【００３１】
上記目的を達成するため、本発明は、第５の態様として、コンピュータを上記本発明の第１の態様の調整値付きブロック暗号化装置として機能させるためのプログラムを提供するものである。
【００３２】
また、上記目的を達成するため、本発明は、第６の態様として、コンピュータを上記本発明の第２の態様の調整値付きブロック復号装置として機能させるためのプログラムを提供するものである。
【発明の効果】
【００３３】
本発明によれば、現実的なブロック暗号を用いて、バースデー攻撃への理論的耐性を持つ調整値付きブロック暗号を形成できる調整値付きブロック暗号化装置、方法及びプログラム並びに復号装置、方法及びプログラムを提供できる。
【図面の簡単な説明】
【００３４】
【図１】本発明を好適に実施した第１の実施形態に係る調整値付きブロック暗号化装置の構成を示す図である。
【図２】調整値依存鍵導出部及びマスク付きブロック暗号化部におけるデータの流れを示す図である。
【図３】暗号文側のマスク値の付加を省略した場合の調整値依存鍵導出部及びマスク付きブロック暗号化部におけるデータの流れを示す図である。
【図４】第１の実施形態に係る調整値付きブロック暗号化装置の動作の流れを示す図である。
【図５】本発明を好適に実施した第２の実施形態に係る調整値付きブロック復号装置の構成を示す図である。
【図６】調整値依存鍵導出部及びマスク付きブロック復号部におけるデータの流れを示す図である。
【図７】暗号文側のマスク値の付加を省略した場合の調整値依存鍵導出部及びマスク付きブロック復号部におけるデータの流れを示す図である。
【図８】第２の実施形態に係る調整値付きブロック復号装置の動作の流れを示す図である。
【図９】ＬＲＷモードにおける暗号化及び復号の動作を示す図である。
【発明を実施するための形態】
【００３５】
本発明は、バースデーバウンドを超えた安全性を保証する効率的な調整値付きブロック暗号を効率よく実現するものである。
【００３６】
本発明においては、部品として用いる（ｎビット鍵、ｎビットブロックの）ブロック暗号Eが理論的に安全で、$m<n/2$をセキュリティパラメータとした場合、攻撃者が用いる平文・暗号文の数が$2(n+m)/2$よりも十分に小さい場合に理論的安全性を持ち、すなわち$2n/2$回の暗号化によるバースデー攻撃に対する理論的耐性を持つためである。耐性の強さはｍでコントロールできる。
【００３７】
また、鍵がｎよりも長い場合にはさらに高い安全性を持つ。これは、調整値ごとに新たなブロック暗号の鍵を導出して暗号化・復号に用いていることによるが、単純に調整値ごとにランダムな鍵を導出するだけでは、攻撃において調整値のバリエーションが$2n/2$程度ある場合、ｎビットの鍵が偶然一致する確率はほぼ１となり、この事実を用いたバースデー攻撃が成立するためである。
【００３８】
これを防ぐため、mpad関数により鍵のバリエーションを高々$2m$個に抑えつつ、調整値に

依存したマスク値加算をブロック暗号の前後に入れることにより、選択暗号文攻撃におけるバースデーバウンドを超えた安全性が保証される。なお、暗号文側のマスク値加算を省略すると、若干処理を簡略化できる代わりに、選択平文攻撃へのバースデーバウンドを超えた安全性のみが保証される。

【００３９】

以下、本発明の好適な実施の形態について説明する。

【００４０】

〔第１の実施形態〕

本発明を好適に実施した第１の実施形態について説明する。

【００４１】

図１に、本実施形態に係る調整値付きブロック暗号化装置の構成を示す。調整値付きブロック暗号化装置１０は、入力部１００、調整値依存鍵導出部１０１、マスク付きブロック暗号化部１０２、及び出力部１０３を有する。

【００４２】

調整値付きブロック暗号化装置１０はＣＰＵとメモリとディスクにより実現可能である。

【００４３】

調整値付きブロック暗号化装置の各機能部は、プログラムをディスクに格納しておき、このプログラムをＣＰＵ上で動作させることにより実現できる。

【００４４】

用いるブロック暗号を、nビットブロック、ｎ’ビット鍵

【００４５】

【数６】

$$(n' \geq n)$$

とし、調整値の長さをnビットとする。m（1< m<n/2）をセキュリティパラメータとし、これが安全性を決める。

【００４６】

入力部１００は、暗号化の対象となるｎビットの平文Mとｎビットの調整値Tとを入力する。入力部１００は、キーボードなどの文字入力装置として実現される。

【００４７】

図２に、調整値依存鍵導出部１０１及びマスク付きブロック暗号化部１０２における情報の流れを示す。なお、図３に示すように、暗号文側のマスク値加算を省略すると、若干処理を簡略化できる代わりに、選択平文攻撃へのバースデーバウンドを超えた安全性のみが保証される。

【００４８】

調整値依存鍵導出部１０１は、入力された調整値Tと鍵Kとに依存して、調整値依存鍵と呼ばれる新たなブロック暗号の鍵を生成する。

【００４９】

具体的には、ｎ’＝ｎの場合、調整値依存鍵Lは、下記式（６）として実現できる。

【００５０】

【数７】

$$L = Enc(K2, mpad(Enc(K1, T))) \quad \cdots (6)$$

【００５１】

ただし、ブロック暗号の鍵K1、K2は、装置の鍵Kから任意の方法で導出されるものとする（例えば、Kを２ｎビット以上とし最初のｎビットをK1、次のｎビットをK2とすることで実現できる）。また、mpadはｎビットのうち任意のn-mビット（mはセキュリティパラメータ）を任意の値に固定する関数である。例えば、上位n-mビットを全ゼロとすることで

実現できる。

【００５２】

鍵K2による暗号化処理は、ｎビットの入力とｎ’ビットの出力とを持つ任意の暗号関数、例えば鍵付きの一方向性ハッシュ関数などでも実現可能である。特に、ｎ’＝ｎの場合では鍵K2による暗号化処理は、Stefan Lucks, The Sum of PRPs Is a Secure PRF, EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding. Lecture Notes in Computer Science 1807 Springer 2000, pp. 470-484に記載のSUMモードを用いることでも実現でき、また、ｎ’＞ｎの場合は、Tetsu Iwata, New Blockcipher Modes of Operation with Beyond the Birthday Bound Security, Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers. Lecture Notes in Computer Science 4047 Springer 2006, pp. 310-322に記載のCENCモードを用いることでも実現できる。

【００５３】

マスク付きブロック暗号化部１０２は、調整値依存鍵導出部１０１が出力する調整値依存鍵Lと調整値Tとによるマスク値を用いて平文Mを暗号文Cへ暗号化する。

【００５４】

具体的には、攻撃者による選択暗号文攻撃を想定した場合、暗号文Cは、下記式（７）となり、平文選択攻撃のみを想定した場合は、下記式（８）となる。

【００５５】

【数８】

$$C = Enc(L, M+S) + S, \text{ ただし } S = F(K3, T) \quad \cdots(7)$$

$$C = Enc(L, M+S), \text{ ただし } S = F(K3, T) \quad \cdots(8)$$

【００５６】

ここで、K3は、上記式（６）におけるK1、K2と同様に、装置の鍵Kから導出される鍵であり、F(K3,T)は鍵K3を用いる鍵付き関数FへTを入力した結果（ｎビット）である。Fは、異なる二つの調整値TとT'とについて上記式（４）で定義されるe-AUX関数である必要がある。これは、例えば、ｎビットの鍵K3と調整値Tとの有限体GF(2n)上の乗算mul（K3,T）をとることで実現できる。このときFは、下記式（９）で定義され、Fは1/2n-AXU関数である。

【００５７】

【数９】

$$S = F(K3, T) = mul(K3, T) \quad \cdots(9)$$

【００５８】

出力部１０３は、マスク付きブロック暗号部１０２が出力する暗号文Cを出力する。出力部１０３は、コンピュータディスプレイやプリンタなどで実現可能である。

【００５９】

本実施形態に係る調整値付きブロック暗号化装置を具体的に通信やデータストレージにおける暗号化に使用する場合、本実施形態で得られるnビットブロック、nビット調整値のブロック暗号を何らかの暗号モードで使用することが考えられる。例えば、非特許文献１に記載されている、調整値付きブロック暗号のモードであるTweak Block ChainingやTweak Chain Hash, Tweakable Authenticated Encryptionなどで使用することが可能である。

【００６０】

さらにハードディスクなどデータストレージの暗号化においては、IEEEにおけるストレージ暗号方式標準化で議論されているモードが適用可能である。これは、ハードディスク

のセクタとセクタ中のバイトポジション（1セクタは通常512バイト）に応じてマスク値を足しつつECBモードのように並列に暗号化を行うものである。この方法では、例えばn=128とし、本実施形態で得られる128ビットブロック、128ビット調整値付きブロック暗号の暗号化関数をTENC（鍵K、調整値T、平文Mでの暗号化はTENC(K,T,M)）とすると、まずセクタの内容を128ビット（16バイト）ごとに分割する。分割した結果を（m1,m2,...,m32）、ただしmiは16バイトとする。このとき、mi（i=1,...,32）をTENC(K, (SecNum || i), mi)と暗号化する。ただしSecNumはセクタ番号であり、||はビット系列の連結を表す。すなわち、セクタ番号SecNumの第iブロックを、調整値(SecNum || i)で暗号化するものである。

【００６１】

図４に、本実施形態に係る調整値付きブロック暗号化装置の動作の流れを示す。

【００６２】

まず、入力手段を介してｎビットの平文Mとｎビットの調整値Tとを入力し（ステップＳ１０１）、調整値依存鍵導出部１０１により、上記式（６）に従って調整値依存鍵Ｌを求める（ステップＳ１０２）。次に、ブロック暗号化部１０２により上記式（７）に従ってマスク値Ｓを生成し（ステップＳ１０３）、さらにＬを鍵、Ｓをマスク値として上記式（７）に従ってMのマスク付き暗号化を行い暗号文Cを得る（ステップＳ１０４）。最後に、得られた暗号文Cを出力部１０３によって出力する（ステップＳ１０５）。

【００６３】

このように、本実施形態によれば、現実的なブロック暗号を用いて、バースデー攻撃への理論的耐性を持つ調整値付きブロック暗号を形成できる。

【００６４】

〔第２の実施形態〕

本発明を好適に実施した第２の実施形態について説明する。

【００６５】

図５に、本実施形態に係る調整値付きブロック復号装置の構成を示す。調整値付きブロック復号装置２０は、入力部２００、調整値依存鍵導出部２０１、マスク付きブロック復号部２０２、及び出力部２０３を有する。

【００６６】

調整値付きブロック復号装置２０は、ＣＰＵとメモリとディスクにより実現可能である。

【００６７】

調整値付きブロック復号装置の各機能部は、プログラムをディスクに格納しておき、このプログラムをＣＰＵ上で動作させることにより実現できる。

【００６８】

調整値付きブロック復号装置を構成する各機能部について説明する。

【００６９】

図６に、調整値依存鍵導出部２０１及びマスク付きブロック復号部３０２における情報の流れを示す。なお、図７に示すように、暗号文側のマスク値加算を省略すると、若干処理を簡略化できる代わりに、選択平文攻撃へのバースデーバウンドを超えた安全性のみが保証される。

【００７０】

上記第１の実施形態と同様に、用いるブロック暗号を、ｎビットブロック、ｎ’ビット鍵（ｎ’≧ｎ）とし、セキュリティパラメータをｍ（1<m<n/2）とする。

【００７１】

入力部２００は、復号の対象となるｎビットの暗号文Cとｎビットの調整値Tとを入力する。入力部２００は、キーボードなどの文字入力装置によって実現できる。

【００７２】

調整値依存鍵導出部２０１は、第１の実施形態における調整値依存鍵導出部１０１と同様である。

【００７３】
マスク付きブロック復号部２０２は、調整値依存鍵導出部２０１が出力する調整値依存鍵Lと調整値Tによるマスク値を用いて暗号文Cを平文Mへ復号する。具体的には、ブロック暗号の復号関数をDec（鍵K、暗号文Cの復号はDec(K,C)）、攻撃者による選択暗号文攻撃を想定した場合、平文Mは下記式（１０）とし、選択平文攻撃のみを想定した場合は下記式（１１）となる。
【００７４】
【数１０】

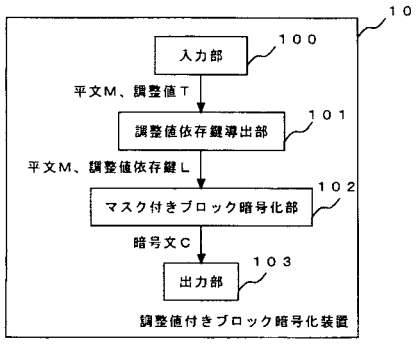
$$M = Dec(L, M+S) + S, \text{ ただし } S = F(K3, T) \quad \cdots(10)$$

$$M = Dec(L, M+S), \text{ ただし } S = F(K3, T) \quad \cdots(11)$$

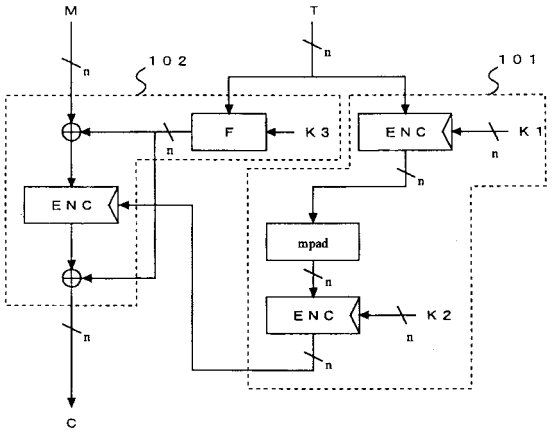
【００７５】
ここで、K3は装置の鍵Kから導出される鍵であり、鍵付き関数Fは第１の実施形態におけるマスク付きブロック暗号化部１０２が用いるものと同様である。
【００７６】
出力部２０３は、マスク付きブロック復号部２０２が出力する平文Mを出力する。出力部２０３は、コンピュータディスプレイやプリンタなどで実現可能である。
【００７７】
図８に、本実施形態に係る調整値付きブロック復号装置の動作の流れを示す。
【００７８】
まず、入力部２００を用いてｎビットの暗号文Cと調整値Tとを入力し（ステップＳ２０１）、調整値依存鍵導出部２０１によって上記式（６）に従って調整値依存鍵Ｌを求める（ステップＳ２０２）。次に、マスク付きブロック復号部２０２によって上記式（１０）に従ってマスク値Sを生成する（ステップＳ２０３）。さらに、Lを鍵、Sをマスク値として上記式（１０）に従って暗号文Cにマスク付き復号を行い平文Mを得る（ステップＳ２０４）。最後に、得られた平文Mを出力部２０３によって出力する（ステップＳ２０５）。
【００７９】
このように、本実施形態によれば、現実的なブロック暗号を用いて形成したバースデー攻撃への理論的耐性を持つ調整値付きブロック暗号を復号できる。
【００８０】
なお、上記各実施形態は本発明の好適な実施の一例であり、本発明はこれらに限定されることはない。
【００８１】
例えば、本発明は、無線又は有線のデータ通信における認証と暗号化といった用途や、ストレージ上のデータの暗号化と改ざん防止といった用途に適用可能である。
【００８２】
このように、本発明は様々な変形が可能である。
【００８３】
この出願は、２００８年８月２９日に出願された日本出願特願２００８－２２１６５７を基礎として優先権の利益を主張するものであり、その開示の全てを引用によってここに取り込む。
【符号の説明】
【００８４】
１０　調整値付きブロック暗号化装置
２０　調整値付きブロック復号装置
１００、２００　入力部
１０１、２０１　調整値依存鍵導出部
１０２　マスク付きブロック暗号化部
１０３、２０３　出力部

２０２　　マスク付きブロック復号部

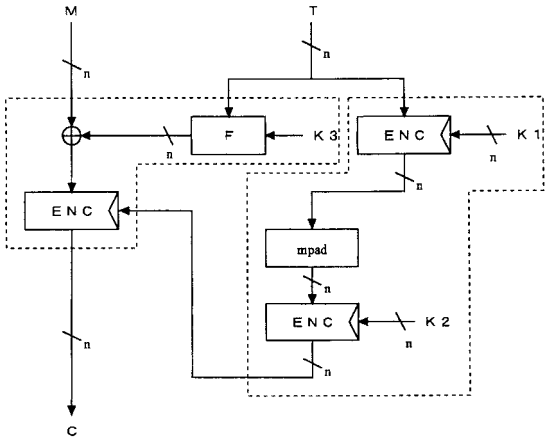
【図１】



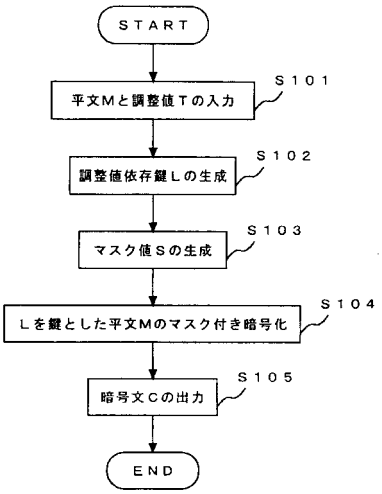
【図２】



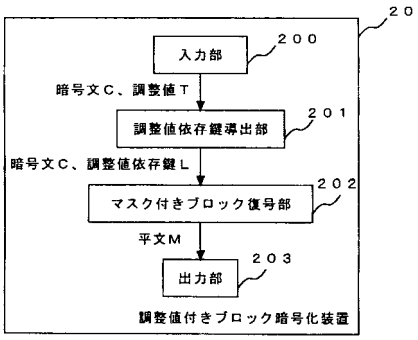
【図３】



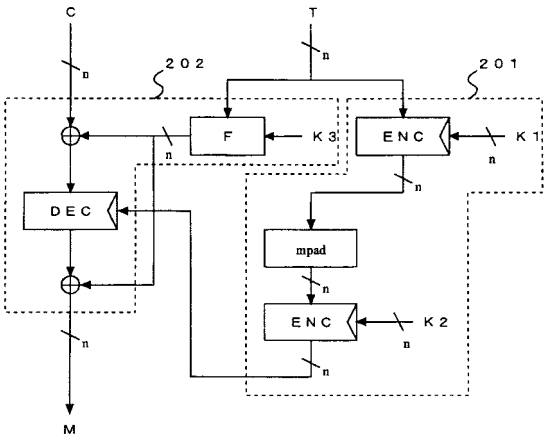
【図４】


START
平文Mと調整値Tの入力
S101
調整値依存鍵Lの生成
S102
マスク値Sの生成
S103
Lを鍵とした平文Mのマスク付き暗号化
S104
暗号文Cの出力
S105
END

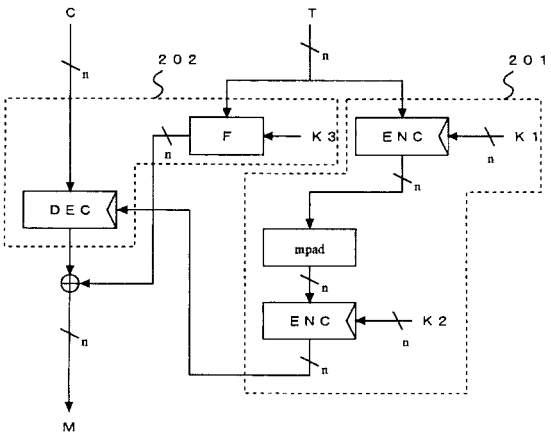
【図５】


20
入力部
200
暗号文C、調整値T
調整値依存鍵導出部
201
暗号文C、調整値依存鍵L
マスク付きブロック復号部
202
平文M
出力部
203
調整値付きブロック暗号化装置

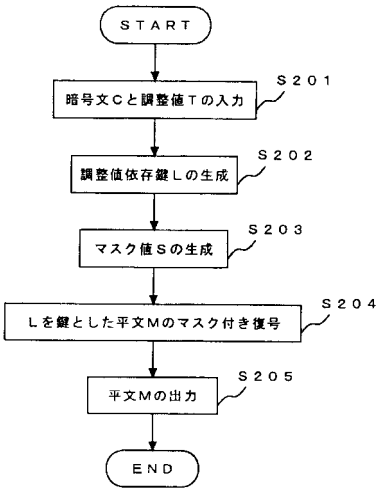
【図６】


C
T
n
202
201
F
K3
ENC
K1
DEC
mpad
ENC
K2
M

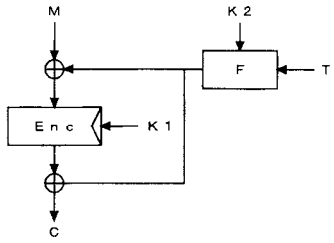
【図７】


C
T
n
202
201
F
K3
ENC
K1
DEC
mpad
ENC
K2
M

【図８】

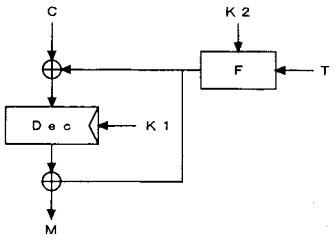

START
暗号文Cと調整値Tの入力
S201
調整値依存鍵Lの生成
S202
マスク値Sの生成
S203
Lを鍵とした平文Mのマスク付き復号
S204
平文Mの出力
S205
END

【図９】



暗号化

（ａ）



復号

（ｂ）

フロントページの続き

(56)参考文献 国際公開第２００８／０１８３０３（WO，Ａ１）
国際公開第２００４／０２３７１５（WO，Ａ１）
M. Liskov et al., Tweakable Block Ciphers, Lecture Notes in Computer Science, Springer, ２００２年, Vol. 2442, pp. 31-46, ［２００９年６月１２日検索］, インターネット, ＵＲＬ, http://www.cs.berkeley.edu/~daw/papers/tweak-crypto02.pdf
Draft Proposal for Tweakable Wide-block Encryption, IEEE, ２００３年 3月２２日, Draft 1.00:00, ［２００９年６月１２日検索］, インターネット, ＵＲＬ, http://siswg.net/docs/EME-AES-03-22-2004.pdf
Draft Proposal for Tweakable Narrow-block Encryption, IEEE, ２００４年 8月 6日, Draft 1.00:00, ［２００９年６月１２日検索］, インターネット, ＵＲＬ, http://siswg.net/docs/LRW-AES-10-19-2004.pdf

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／０６