(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5704159号
(P5704159)
(45)発行日　平成27年4月22日(2015.4.22)　(24)登録日　平成27年3月6日(2015.3.6)

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

請求項の数 12 (全 18 頁)

(21)出願番号　特願2012-501785(P2012-501785)
(86)(22)出願日　平成23年2月22日(2011.2.22)
(86)国際出願番号　PCT/JP2011/053832
(87)国際公開番号　WO2011/105367
(87)国際公開日　平成23年9月1日(2011.9.1)
審査請求日　平成26年1月9日(2014.1.9)
(31)優先権主張番号　特願2010-38975(P2010-38975)
(32)優先日　平成22年2月24日(2010.2.24)
(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　100080816
弁理士　加藤　朝道
(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　青木　重徳

最終頁に続く

(54)【発明の名称】ブロック暗号化装置、ブロック復号装置、ブロック暗号化方法、ブロック復号方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する鍵付きハッシュ部と、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する調整値依存鍵導出部と、
前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成するマスク付きブロック暗号化部と、を備えていることを特徴とするブロック暗号化装置。
【請求項２】
前記鍵付きハッシュ関数Ｈは、任意の異なる２つの調整値ＴとＴ’に対応するマスク値、中間値のペアをそれぞれ（Ｓ，Ｖ）と（Ｓ’，Ｖ’）とし、Ｓ＋Ｓ’をＳとＳ’のビット単位の排他的論理和とし、ｅを２－（ｎ＋ｍ）に十分近い値とした場合に、確率
Ｐｒ［Ｓ＋Ｓ’＝ｃ，Ｖ＝Ｖ’］≦ｅ
が任意のＴ，Ｔ’，ｃについて成立する関数であることを特徴とする、請求項１に記載のブロック暗号化装置。
【請求項３】

前記調整値依存鍵導出部は、前記中間値Ｖの後ろに、ｎ－ｍビットの０をパディングすることを特徴とする、請求項１又は２に記載のブロック暗号化装置。
【請求項４】
前記調整値Ｔ及び前記平文Ｍを入力とする入力部をさらに備えていることを特徴とする、請求項１乃至３のいずれか１項に記載のブロック暗号化装置。
【請求項５】
前記暗号文Ｃを出力する出力部をさらに備えていることを特徴とする、請求項１乃至４のいずれか１項に記載のブロック暗号化装置。
【請求項６】
ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する鍵付きハッシュ部と、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する調整値依存鍵導出部と、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成するマスク付きブロック復号部と、を備えていることを特徴とするブロック復号装置。
【請求項７】
前記鍵付きハッシュ関数Ｈは、任意の異なる２つの調整値ＴとＴ’に対応するマスク値、中間値のペアをそれぞれ（Ｓ，Ｖ）と（Ｓ’，Ｖ’）とし、Ｓ＋Ｓ’をＳとＳ’のビット単位の排他的論理和とし、ｅを２－（ｎ＋ｍ）に十分近い値とした場合に、確率
Ｐｒ［Ｓ＋Ｓ’＝ｃ，Ｖ＝Ｖ’］≦ｅ
が任意のＴ，Ｔ’，ｃについて成立する関数であることを特徴とする、請求項６に記載のブロック復号装置。
【請求項８】
前記調整値依存鍵導出部は、前記中間値Ｖの後ろに、ｎ－ｍビットの０をパディングすることを特徴とする、請求項６又は７に記載のブロック復号装置。
【請求項９】
コンピュータがプログラムを読み込むことにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および、
前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成する前記少なくとも１とのハードウェア手段として機能する、ことを特徴とするブロック暗号化方法。
【請求項１０】
コンピュータがプログラムを読み込むことにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成す

る前記少なくとも１つのハードウェア手段として機能する、ことを特徴とするブロック復号方法。

【請求項１１】

コンピュータに読み込まれることにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、

前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および、

前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成する前記少なくとも１つのハードウェア手段として、前記コンピュータを機能させることを特徴とするプログラム。

【請求項１２】

コンピュータに読み込まれることにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、

前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および、

前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成する前記少なくとも１つのハードウェア手段として、前記コンピュータを機能させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

［関連出願についての記載］

本発明は、日本国特許出願：特願２０１０－０３８９７５号（２０１０年２月２４日出願）の優先権主張に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。

本発明は、ブロック暗号化装置、ブロック復号装置、ブロック暗号化方法、ブロック復号方法及びプログラムに関し、特に、ｎビットブロック暗号による調整値付きのブロック暗号化装置、ブロック復号装置、ブロック暗号化方法、ブロック復号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る。置換への入力が平文に相当し、置換からの出力が暗号文に相当する。平文と暗号文の長さをブロックサイズという。一般に、ブロックサイズがｎビットのブロック暗号を、ｎビットブロック暗号という。

【０００３】

調整値付きブロック暗号とは、通常のブロック暗号が入出力として有する（平文、暗号文、鍵）以外に、ｔｗｅａｋと呼ばれる調整値を有するブロック暗号をいう。調整値付きブロック暗号は、ｔｗｅａｋａｂｌｅブロック暗号とも呼ばれる。調整値付きブロック暗号においては、調整値と鍵とが定まれば、平文と暗号文とが１対１に対応することが条件とされる。すなわち、任意の調整値付きブロック暗号に対する暗号化関数ＴＷＥＮＣと、これに対応する復号関数ＴＷＤＥＣは、平文Ｍ、暗号文Ｃ、鍵Ｋ、調整値Ｔについて、

Ｃ＝ＴＷＥＮＣ（Ｋ，Ｔ，Ｍ）　⇔　Ｍ＝ＴＷＤＥＣ（Ｋ，Ｔ，Ｃ）　　…（１）

を満たす。ここで、矢印（⇔）は左右の命題が等価であることを示す。

【０００４】

非特許文献１に、式（１）を含む調整値付きブロック暗号の形式的な定義と安全性要件が記載されている。安全性要件とは、調整値付きブロック暗号において、調整値と入力が攻撃者に既知であっても、調整値が異なる２つのブロック暗号の出力が攻撃者には互いに独立でランダムな値に見えることをいう。この要件が満たされるとき、調整値付きブロック暗号は安全であるという。

【０００５】

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」と略す）として得られること、すなわち、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ことが示されている。ただし、ここでの理論的安全性とは、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こと、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ことをいう。

【０００６】

さらに、安全性の定義には、攻撃者が選択平文攻撃（ＣＰＡ：Ｃｈｏｓｅｎ－Ｐｌａｉｎｔｅｘｔ　Ａｔｔａｃｋ）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（ＣＣＡ：Ｃｈｏｓｅｎ－Ｃｉｐｈｅｒｔｅｘｔ　Ａｔｔａｃｋ）とを組み合わせて実行可能な場合の安全性の２種類がある。前者をＣＰＡ－ｓｅｃｕｒｉｔｙといい、後者をＣＣＡ－ｓｅｃｕｒｉｔｙという。

【０００７】

安全な調整値付きブロック暗号は、高度な暗号化機能を実現するための鍵となる技術である。例えば、非特許文献２では、ＣＣＡ－ｓｅｃｕｒｉｔｙを有する調整値付きブロック暗号を用いると、効率のよい認証機能付き暗号化を実現しうること、及び、ＣＰＡ－ｓｅｃｕｒｉｔｙを有する調整値付きブロック暗号を用いると効率のよい並列実行可能なメッセージ認証コードを実現しうることが記載されている。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もある。

【０００８】

ここでは、非特許文献１の定理２で提案されたモードをＬＲＷモードと呼ぶ。図７は、非特許文献１に記載された、ｎビットブロック暗号Ｅを用いたＬＲＷモードにおける暗号化と復号を示す図である。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、以下の式（２）によって暗号文Ｃを得る。

Ｃ＝Ｅｎｃ（Ｋ１，Ｍ＋Ｆ（Ｋ２，Ｔ））＋Ｆ（Ｋ２，Ｔ）　　…（２）

【０００９】

一方、暗号文Ｃから平文Ｍへの復号は、以下の式（３）となる。

Ｍ＝Ｄｅｃ（Ｋ１，Ｃ＋Ｆ（Ｋ２，Ｔ））＋Ｆ（Ｋ２，Ｔ）　　…（３）

ここで、Ｋ１はブロック暗号の鍵であり、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）である。ここで、Ｆは、セキュリティパラメータをｅ（ｅは０以上１以下）としたとき、任意のｃ，ｘ，ｘ’（ただしｘとｘ’は異なる）について、以下の式（４）を満たす必要がある。

Ｐｒ［ｆ（Ｋ，ｘ）＋ｆ（Ｋ，ｘ’）＝ｃ］≦ｅ　　…（４）

ここで、＋は排他的論理和をあらわす。

【００１０】

この性質を有するｆ（Ｋ，＊）を、ｅ－ＡＸＵ（ｅ－ａｌｍｏｓｔ　ＸＯＲ　ｕｎｉｖｅｒｓａｌ）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（2^n）上の乗算ｍｕｌを用いて、Ｆ（Ｋ２，Ｔ）＝ｍｕｌ（Ｋ２，Ｔ）とすることが知られている。このとき、Ｆは１／２ｎ－ＡＸ

Uである。
【００１１】
ｅ－ＡＸＵ関数は、有限体ＧＦ（２ｎ）上の乗算ｍｕｌ以外に、非特許文献３で提案されている方式で実現することもできる。これらは、特定の実装環境において、一般的なブロック暗号よりも数倍高速となることが知られている。
【先行技術文献】
【非特許文献】
【００１２】
【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 － ＡＳＩＡＣＲＹＰＴ ２００４，１０ｔｈ 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，Ｆｅｂ．１９９７
【非特許文献４】Ｋ．Ｍｉｎｅｍａｔｓｕ，“Ｂｅｙｏｎｄ－Ｂｉｒｔｈｄａｙ－Ｂｏｕｎｄ Ｓｅｃｕｒｉｔｙ Ｂａｓｅｄ ｏｎ Ｔｗｅａｋａｂｌｅ Ｂｌｏｃｋ Ｃｉｐｈｅｒ，”Ｆａｓｔ Ｓｏｆｔｗａｒｅ Ｅｎｃｒｙｐｔｉｏｎ － ＦＳＥ ２００９，１６ｔｈ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｗｏｒｋｓｈｏｐ，ＦＳＥ ２００９，Ｌｅｕｖｅｎ，Ｂｅｌｇｉｕｍ，Ｆｅｂｒｕａｒｙ ２２－２５，２００９，Ｒｅｖｉｓｅｄ Ｓｅｌｅｃｔｅｄ Ｐａｐｅｒｓ．Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｃｉｅｎｃｅ ５６６５ Ｓｐｒｉｎｇｅｒ ２００９，ｐｐ．３０８－３２６．
【発明の概要】
【発明が解決しようとする課題】
【００１３】
上記非特許文献１－４の全開示内容はその引用をもって本書に繰込み記載する。以下に本発明による分析を与える。
【００１４】
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ＸＥＸモードがある。ＬＲＷ、ＸＥＸモードは、式（２）と式（３）で示される形式を持ち、ＣＣＡ－ｓｅｃｕｒｉｔｙを有する。ＬＲＷとＸＥＸは、構造的にはほぼ同じである。しかし、ＬＲＷモードではＫ２はＫ１

と独立であるのに対し、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により、鍵サイズの効率化を図っている。重要な点は、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$2^{n/2}$よりも十分に小さい（これをｑ≪$2^{n/2}$と表す）場合に限られていることである。$2^{n/2}$はバースデーバウンドと呼ばれる。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、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、１２８ビットブロック暗号を用いた場合においても将来的には脅威となり得ることから、対策が必要とされる。

【００１５】

かかる対策の一例として、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。特に、非特許文献４で示されているＴＤＲ（Ｔｗｅａｋ－Ｄｅｐｅｎｄｅｎｔ Ｒｅｋｅｙｉｎｇ）は、このアイディアを用いて、調整値の長さがｎ／２ビットよりも十分短い場合に、ブロックサイズのバースデーバウンドを超えた安全性（ＣＣＡ－ｓｅｃｕｒｉｔｙ）を提供する。図８は、ＴＤＲの暗号化と復号を示す図である。ＴＤＲはバースデーバウンドを超えた高い安全性を提供するものの、調整値の長さが制約されている。汎用性を確保するためには、調整値への入力として、任意の長さを許容することが望ましい。

【００１６】

一方、非特許文献１に記載された方式によると、調整値の長さは実質的に任意であるものの、ブロックサイズのバースデーバウンドを超えた安全性が保証されないという問題がある。

【００１７】

上述のように、従来のブロック暗号を用いた調整値付きブロック暗号は、ＬＲＷ、ＸＥＸのように調整値が任意長であるもののバースデー攻撃によって破られる方式、又は、ＴＤＲのようにバースデー攻撃に理論的耐性を有するものの調整値の長さが固定の短い値に限られる方式のいずれかである。

【００１８】

そこで、バースデー攻撃への理論的耐性を有し、調整値が任意長の調整値付きブロック暗号を実現することが課題となる。本発明の目的は、かかる課題を解決するブロック暗号化装置、ブロック復号装置、ブロック暗号化方法、ブロック復号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】

【００１９】

本発明の第１の視点に係るブロック暗号化装置は、

ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する鍵付きハッシュ部と、

前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する調整値依存鍵導出部と、

前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成するマスク付きブロック暗号化部と、を有する。

【００２０】

本発明の第２の視点に係るブロック復号装置は、

ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する鍵付きハッシュ部と、

前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビット

ブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する調整値依存鍵導出部と、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成するマスク付きブロック復号部と、を有する。

【００２１】

本発明の第３の視点に係るブロック暗号化方法は、
コンピュータがプログラムを読み込むことにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および、
前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成する前記少なくとも１つのハードウェア手段として機能する。

【００２２】

本発明の第４の視点に係るブロック復号方法は、
コンピュータがプログラムを読み込むことにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成する前記少なくとも１つのハードウェア手段として機能する。

【００２３】

本発明の第５の視点に係るプログラムは、
コンピュータに読み込まれることにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および
前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成する前記少なくとも１つのハードウェア手段として、前記コンピュータを機能させる。

【００２４】

本発明の第６の視点に係るプログラムは、
コンピュータに読み込まれることにより、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓ及びｍビット（ｍはｎ／２未満の正整数）の中間値Ｖを生成する少なくとも１つのハードウェア手段、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する前記少なくとも１つのハードウェア手段、および、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎ

ビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成する前記少なくとも１つのハードウェア手段として、前記コンピュータを機能させる。

【発明の効果】

【００２５】

本発明に係るブロック暗号化装置、ブロック復号装置、ブロック暗号化方法、ブロック復号方法及びプログラムによると、バースデー攻撃への理論的耐性を有し、調整値が任意長の調整値付きブロック暗号を実現することができる。

【図面の簡単な説明】

【００２６】

【図１】第１の実施形態の構成を示すブロック図である。

【図２】第１の実施形態の構成を概略的に示す図である。

【図３】第１の実施形態の動作を示すフローチャートである。

【図４】第２の実施形態の構成を示すブロック図である。

【図５】第２の実施形態の構成を概略的に示す図である。

【図６】第２の実施形態の動作を示すフローチャートである。

【図７】非特許文献１に記載されたＬＲＷモードにおける暗号化と復号を示す図である。

【図８】非特許文献４に記載されたＴＤＲモードにおける暗号化と復号を示す図である。

【発明を実施するための形態】

【００２７】

（実施形態１）

第１の実施形態に係るブロック暗号化装置について、図面を参照して説明する。図１は、本実施形態の調整値付きのブロック暗号化装置１０の構成を示すブロック図である。一方、図２は、ブロック暗号化装置１０の構成を概略的に示す図である。

【００２８】

図１を参照すると、ブロック暗号化装置１０は、入力部１００、鍵付きハッシュ部１０１、調整値依存鍵導出部１０２、マスク付きブロック暗号化部１０３及び出力部１０４を有する。

【００２９】

ブロック暗号化装置１０は、例えば、ＣＰＵとメモリとディスクにより実現することができる。

【００３０】

ブロック暗号化装置１０の各部は、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って実現することができる。

【００３１】

次に、ブロック暗号化装置１０を構成する各部について説明する。

【００３２】

用いるブロック暗号を、ｎビットブロック、ｎビット鍵とし、調整値の長さを任意の正整数ｂについてｂビットとする。ｍ（１＜ｍ＜ｎ／２）をセキュリティパラメータとすると、この値が安全性を決める。

【００３３】

入力部１００は、暗号化の対象となるｎビットの平文Ｍとｂビットの調整値Ｔを入力する。入力部１００は、例えば、キーボードなどの文字入力装置によって実現することができる。

【００３４】

図１及び図２を参照すると、鍵付きハッシュ部１０１は、入力された調整値Ｔを入力として、鍵Ｋ２を用いた鍵付きハッシュ関数Ｈにより、ｎビットのマスク値Ｓと、ｍビットの中間値Ｖを生成する。

【００３５】

鍵付きハッシュ関数Ｈについては、任意の異なる２つの調整値ＴとＴ’に対応するマスク値、中間値のペアをそれぞれ（Ｓ，Ｖ）と（Ｓ’，Ｖ’）としたとき、確率

Ｐｒ［Ｓ＋Ｓ’＝ｃ，Ｖ＝Ｖ’］≦ｅ　　…（５）
がどのようなＴ，Ｔ’，ｃについても成立するものとする。ただし、Ｓ＋Ｓ’はＳとＳ’のビット単位の排他的論理和を表す。ここで、ｅは$2^{-(n+m)}$に十分近いことが必要とされる。

【００３６】
式（５）の条件は、Ｈがｅ－ＡＸＵ関数と呼ばれる性質を満たせば十分である。このための具体的な構成方法としては、例えば、ｂがｎ＋ｍ以下の場合、鍵Ｋ２をｎ＋ｍビットとし、Ｔに適当なパディングを施しｎ＋ｍビットとした後、パディングされたＴと、Ｋ２との有限体ＧＦ（2^{n+m}）上の乗算ｍｕｌを求め、そこからＳとＶを取り出せばよい。このとき、ｅは$2^{-(n+m)}$となる。

【００３７】
ｅ－ＡＸＵ関数は、有限体ＧＦ（2^{n+m}）上の乗算ｍｕｌ以外に、非特許文献３で提案されている方式で実現することもできる。これらは、特定の実装環境において、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。

【００３８】
調整値依存鍵導出部１０２は、中間値Ｖと鍵Ｋ１を用いて、調整値依存鍵と呼ばれる新たなブロック暗号の鍵Ｌを生成する。

【００３９】
具体的に、調整値依存鍵Ｌは、ブロック暗号の暗号化関数をＥｎｃ（ｘ，ｙ）（ただしｘは鍵、ｙは平文）で表すとすると、
Ｌ＝Ｅｎｃ（Ｋ１，ｐａｄ（Ｖ））　　…（６）
となる（図２参照）。ｐａｄは、ｍビット入力を適当にパディングしてｎビットとするパディング関数である。パディング関数ｐａｄは、例えば、入力されたｍビットの後ろにｎ－ｍビットの０をパディングするようにしてもよい。

【００４０】
図１及び図２を参照すると、マスク付きブロック暗号化部１０３は、調整値依存鍵導出部１０２が出力する調整値依存鍵Ｌと鍵付きハッシュ部１０１が出力するマスク値Ｓを用いて平文Ｍを暗号文Ｃへ暗号化する。

【００４１】
具体的には、暗号文Ｃは
Ｃ＝Ｅｎｃ（Ｌ，Ｍ＋Ｓ）＋Ｓ　　…（７）
となる。

【００４２】
出力部１０４は、マスク付きブロック暗号化部１０３の出力する暗号文Ｃを出力する。出力部１０４は、コンピュータディスプレイ、プリンタ等によって実現することができる。

【００４３】
本発明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、本発明で得られるｎビットブロック、ｂ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。

【００４４】
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（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｄｅ　Ｂｏｏｋ）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、本発明で得られる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ＴＥＮ

Ｃ（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（m_1，m_2，…，m_{32}）、ただし、m_iは１６バイトとする。このとき、m_i（ｉ＝１，…，３２）をＴＥＮＣ（Ｋ，（ＳｅｃＮｕｍ｜｜ｉ），m_i）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。

【００４５】

次に、本実施形態のブロック暗号化装置の全体の動作について、図面を参照して説明する。図３は、本実施形態のブロック暗号化装置の全体の動作を示すフローチャートである。

【００４６】

図３を参照すると、入力部１００は、ｎビットの平文Ｍとｂビットの調整値Ｔを入力とする（ステップＥ１）。

【００４７】

次に、鍵付きハッシュ部１０１は、ｍビット（ただし１＜ｍ＜ｎ／２）の中間値Ｖとｎビットのマスク値Ｓを生成する（ステップＥ２）。

【００４８】

次に、調整値依存鍵導出部１０２は、中間値Ｖをｎビットにパディングして暗号化することで、ｎビットの調整値依存鍵Ｌを求める（ステップＥ３）。

【００４９】

次に、マスク付きブロック暗号化部１０３は、Ｌを鍵、Ｓをマスク値として、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Ｅ４）。

【００５０】

最後に、出力部１０４は、得られた暗号文Ｃを出力する（ステップＥ５）。

【００５１】

本実施形態に係るブロック暗号化装置１０は、ｎビットブロック、ｎビット鍵のブロック暗号について、調整値（ｔｗｅａｋ）に依存してブロック暗号の鍵Ｌとｎビットのマスク値Ｓを導出し、これを用いて平文の暗号化を行う。平文はＬを鍵としたブロック暗号により暗号化されるが、鍵Ｌによる暗号化の前後でＳによる排他的論理和を入れる。具体的には、調整値Ｔをｎ＋ｍビット出力のユニバーサルハッシュ関数へ入力し、ｎビットのＳとｍビットの中間値Ｖを得た後、Ｖをｎビットにパディングしてブロック暗号で暗号化することで、鍵Ｌを得る。上記の方法は、部品としてｎビット鍵、ｎビットブロックの安全なブロック暗号を用い、かつ、セキュリティパラメータｍがｎ／２未満の場合、攻撃者が２ｎ／２回の選択暗号文攻撃を行っても、攻撃が成功する確率を高々２－ｍ／２に抑えることができる。したがって、本実施形態に係る暗号化装置１０は、ブロックサイズｎに対するバースデー攻撃に対する理論的耐性（ＣＣＡ－ｓｅｃｕｒｉｔｙ）を有する。

【００５２】

（実施形態２）

次に、第２の実施形態に係るブロック復号装置について、図面を参照して説明する。図４は、本実施形態の調整値付きのブロック復号装置２０の構成を示すブロック図である。一方、図５は、ブロック復号装置２０の構成を概略的に示す図である。

【００５３】

図４を参照すると、調整値付きのブロック復号装置２０は、入力部２００、鍵付きハッシュ部２０１、調整値依存鍵導出部２０２、マスク付きブロック復号部２０３及び出力部２０４を有する。

【００５４】

ブロック復号装置２０は、ＣＰＵとメモリとディスクによって実現することができる。

【００５５】

ブロック復号装置２０の各部は、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することができる。

【００５６】
次に、ブロック復号装置２０を構成する各部について説明する。
【００５７】
用いるブロック暗号を、ｎビットブロック、ｎビット鍵とし、調整値の長さを任意の正整数ｂについて、ｂビットとする。ｍ（１＜ｍ＜ｎ／２）をセキュリティパラメータとすると、この値が安全性を決定する。
【００５８】
入力部２００は、復号の対象となるｎビットの暗号文Ｃとｂビットの調整値Ｔを入力する。入力部２００は、例えば、キーボードなどの文字入力装置によって実現することができる。
【００５９】
図４及び図５を参照すると、鍵付きハッシュ部２０１及び調整値依存鍵導出部２０２は、それぞれ、第１の発明の実施の形態のブロック暗号化装置１０における鍵付きハッシュ部１０１及び調整値依存鍵導出部１０２（図１、図２）と同様の動作を行う。
【００６０】
図４及び図５を参照すると、マスク付きブロック復号部２０３は、調整値依存鍵導出部２０２が出力する調整値依存鍵Ｌと鍵付きハッシュ部２０１が出力するマスク値Ｓを用いて、暗号文Ｃを平文Ｍへ復号する。
【００６１】
具体的には、復号関数をＤｅｃ（ｘ，ｙ）（ただしｘは鍵、ｙは暗号文）で表すとすると、平文Ｍは

$$M = Dec(L, C+S) + S \qquad \cdots (8)$$

となる。
【００６２】
出力部２０４は、マスク付きブロック復号部２０３の出力する平文Ｍを出力する。出力部２０４は、コンピュータディスプレイ、プリンタ等によって実現することができる。
【００６３】
次に、本実施形態のブロック復号装置２０の全体の動作について、図面を参照して説明する。図６は、本実施形態のブロック復号装置２０の全体の動作を示すフローチャートである。
【００６４】
図６を参照すると、入力部２００は、ｎビットの暗号文Ｃとｂビットの調整値Ｔを入力とする（ステップＤ１）。
【００６５】
次に、鍵付きハッシュ部２０１は、ｍビット（ただし１＜ｍ＜ｎ／２）の中間値Ｖとｎビットのマスク値Ｓを生成する（ステップＤ２）。
【００６６】
次に、調整値依存鍵導出部２０２は、中間値Ｖをｎビットにパディングして暗号化することで、ｎビットの調整値依存鍵Ｌを求める（ステップＤ３）。
【００６７】
次に、マスク付きブロック復号部２０３は、Ｌを鍵、Ｓをマスク値として、式（８）に従ってＣのマスク付き復号を行い、平文Ｍを得る（ステップＤ４）。
【００６８】
最後に、出力部２０４は、得られた平文Ｍを出力する（ステップＤ５）。
【００６９】
上記第１の実施形態に係るブロック暗号化装置１０及び第２の実施形態に係るブロック復号装置２０は、コンピュータとその上で実行されるプログラムによって実現することもできる。
【００７０】
本発明によると、バースデーバウンドを超えた安全性を保証する、調整値が任意長の調

整値付きブロック暗号を効率よく実現することができる。

【００７１】

その理由は、提案方式でｎビットブロックのブロック暗号Ｅを部品として用いる場合、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・暗号文対の数が$2^{(n+m)/2}$より十分小さい場合に理論的安全性を持つ、すなわち、$2^{n/2}$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からである。ここで、ｍは耐性の強さをコントロールするパラメータであり、例えば、非特許文献４に記載されるようにｍ＝ｎ／３に設定することができる。

【００７２】

この安全性の保証は、非特許文献４に記載のＴＤＲをモジュールとして利用することによる。ＴＤＲにおいては、ｍビット調整値をパディングした結果を直接暗号化することで調整値依存の鍵Ｌを導出していたのに対して、本発明では調整値をｎ＋ｍビット出力の鍵付きハッシュ関数へ入力し、この出力のｎビットを非特許文献１のＬＲＷのマスク値として扱い、残りのｍビットをＴＤＲにおける調整値として扱うことにより、バースデーバウンドを越えた理論的安全性がＴＤＲと同様に保証され、ＬＲＷと同様に調整値が任意長であるという特徴も備えている。

【００７３】

本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態の変更・調整が可能である。また、本発明の請求の範囲の枠内において種々の開示要素の多様な組み合わせないし選択が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。

【００７４】

本発明に係るブロック暗号化装置及びブロック復号装置は、無線又は有線のデータ通信における認証と暗号化、ストレージ上のデータの暗号化と改ざん防止等の用途に適用することができる。

【００７５】

なお、上記実施形態の一部又は全部は、以下の付記として記載することができるものであるが、これらに限定されるものではない。

【００７６】

（付記１）ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓとｍビット（ｍはｎ／２未満の正整数）の中間値Ｖとを生成する鍵付きハッシュ部と、

前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する調整値依存鍵導出部と、

前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成するマスク付きブロック暗号化部と、を備えていることを特徴とするブロック暗号化装置。

【００７７】

（付記２）前記鍵付きハッシュ関数Ｈは、任意の異なる２つの調整値ＴとＴ’に対応するマスク値、中間値のペアをそれぞれ（Ｓ，Ｖ）と（Ｓ’，Ｖ’）とし、Ｓ＋Ｓ’をＳとＳ’のビット単位の排他的論理和とし、ｅを$2^{-(n+m)}$に十分近い値とした場合に、確率

$Pr[S+S'=c, V=V'] \leqq e$

が任意のＴ，Ｔ’，ｃについて成立する関数であることを特徴とする、付記１に記載のブロック暗号化装置。

【００７８】

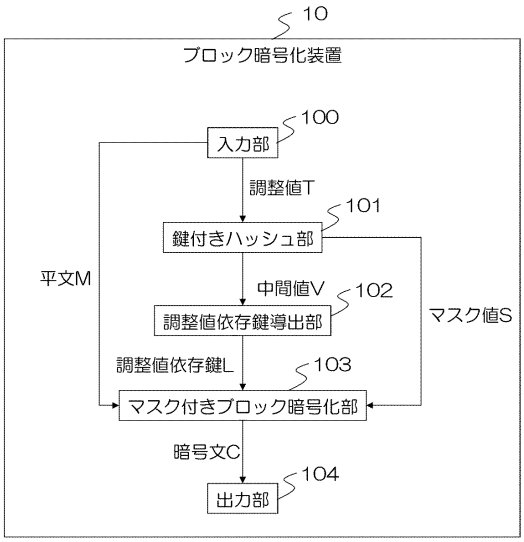
（付記３）前記調整値依存鍵導出部は、前記中間値Ｖの後ろに、ｎ－ｍビットの０をパ

ディングすることを特徴とする、付記１又は２に記載のブロック暗号化装置。
【００７９】
（付記４）前記調整値Ｔ及び前記平文Ｍを入力とする入力部をさらに備えていることを特徴とする、付記１乃至３のいずれか一に記載のブロック暗号化装置。
【００８０】
（付記５）前記暗号文Ｃを出力する出力部をさらに備えていることを特徴とする、付記１乃至４のいずれか一に記載のブロック暗号化装置。
【００８１】
（付記６）ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓとｍビット（ｍはｎ／２未満の正整数）の中間値Ｖとを生成する鍵付きハッシュ部と、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する調整値依存鍵導出部と、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成するマスク付きブロック復号部と、を備えていることを特徴とするブロック復号装置。
【００８２】
（付記７）前記鍵付きハッシュ関数Ｈは、任意の異なる２つの調整値ＴとＴ’に対応するマスク値、中間値のペアをそれぞれ（Ｓ，Ｖ）と（Ｓ’，Ｖ’）とし、Ｓ＋Ｓ’をＳとＳ’のビット単位の排他的論理和とし、ｅを$2^{-(n+m)}$に十分近い値とした場合に、確率
Ｐｒ［Ｓ＋Ｓ’＝ｃ，Ｖ＝Ｖ’］≦ｅ
が任意のＴ，Ｔ’，ｃについて成立する関数であることを特徴とする、付記６に記載のブロック復号装置。
【００８３】
（付記８）前記調整値依存鍵導出部は、前記中間値Ｖの後ろに、ｎ－ｍビットの０をパディングすることを特徴とする、付記６又は７に記載のブロック復号装置。
【００８４】
（付記９）前記調整値Ｔ及び前記暗号文Ｃを入力とする入力部をさらに備えていることを特徴とする、付記６乃至８のいずれか一に記載のブロック復号装置。
【００８５】
（付記１０）前記平文Ｍを出力する出力部をさらに備えていることを特徴とする、付記６乃至９のいずれか一に記載のブロック復号装置。
【００８６】
（付記１１）コンピュータが、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓとｍビット（ｍはｎ／２未満の正整数）の中間値Ｖとを生成する工程と、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する工程と、
前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成する工程と、を含むことを特徴とするブロック暗号化方法。
【００８７】
（付記１２）コンピュータが、入力部を介して、前記調整値Ｔ及び前記平文Ｍを入力とする工程をさらに含むことを特徴とする、付記１１に記載のブロック暗号化方法。
【００８８】
（付記１３）コンピュータが、出力部に対して、前記暗号文Ｃを出力する工程をさらに含むことを特徴とする、付記１１又は１２に記載のブロック暗号化方法。

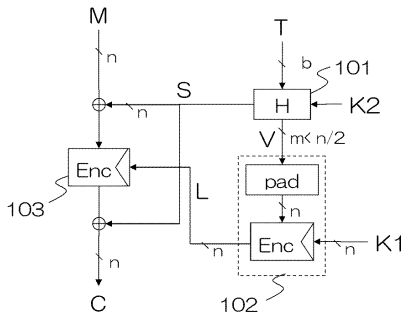
【００８９】
（付記１４）コンピュータが、ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓとｍビット（ｍはｎ／２未満の正整数）の中間値Ｖとを生成する工程と、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する工程と、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成する工程と、を含むことを特徴とするブロック復号方法。
【００９０】
（付記１５）コンピュータが、入力部を介して、前記調整値Ｔ及び前記暗号文Ｃを入力とする工程をさらに含むことを特徴とする、付記１４に記載のブロック復号方法。
【００９１】
（付記１６）コンピュータが、出力部に対して、前記平文Ｍを出力する工程をさらに含むことを特徴とする、付記１４又は１５に記載のブロック復号方法。
【００９２】
（付記１７）ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓとｍビット（ｍはｎ／２未満の正整数）の中間値Ｖとを生成する処理と、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する処理と、
前記マスク値Ｓをｎビットの平文Ｍに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で暗号化し、得られた結果に前記マスク値Ｓを加算して暗号文Ｃを生成する処理と、をコンピュータに実行させることを特徴とするプログラム。
【００９３】
（付記１８）入力部を介して、前記調整値Ｔ及び前記平文Ｍを入力とする処理をさらにコンピュータに実行させることを特徴とする、付記１７に記載のプログラム。
【００９４】
（付記１９）出力部に対して、前記暗号文Ｃを出力する処理をさらにコンピュータに実行させることを特徴とする、付記１７又は１８に記載のプログラム。
【００９５】
（付記２０）ブロック暗号をｎビットブロック、ｎビット鍵とし、調整値の長さをｂビットとしたときに、ｂビットの調整値Ｔを入力とし、鍵Ｋ２を用いた鍵付きハッシュ関数により、ｎビットのマスク値Ｓとｍビット（ｍはｎ／２未満の正整数）の中間値Ｖとを生成する処理と、
前記中間値Ｖをｎビットにパディングした後、鍵Ｋ１を用いて前記中間値Ｖをｎビットブロック暗号で暗号化してｎビットの調整値依存鍵Ｌを生成する処理と、
前記マスク値Ｓをｎビットの暗号文Ｃに加算した後、前記調整値依存鍵Ｌを鍵とするｎビットブロック暗号で復号し、得られた結果に前記マスク値Ｓを加算して平分Ｍを生成する処理と、をコンピュータに実行させることを特徴とするプログラム。
【００９６】
（付記２１）入力部を介して、前記調整値Ｔ及び前記暗号文Ｃを入力とする処理をさらにコンピュータに実行させることを特徴とする、付記２０に記載のプログラム。
【００９７】
（付記２２）出力部に対して、前記平文Ｍを出力する処理をさらにコンピュータに実行させることを特徴とする、付記２０又は２１に記載のプログラム。
【００９８】
（付記２３）付記１７乃至２２のいずれか一に記載のプログラムが記録されていること

を特徴とするコンピュータ読み取り可能な記録媒体。
【符号の説明】
【００９９】
１０　ブロック暗号化装置
２０　ブロック復号装置
１００、２００　入力部
１０１、２０１　鍵付きハッシュ部
１０２、２０２　調整値依存鍵導出部
１０３　マスク付きブロック暗号化部
１０４、２０４　出力部
２０３　マスク付きブロック復号部
Ｃ　暗号文
Ｄｅｃ、ＴＷＤＥＣ　復号関数
Ｅｎｃ、ＴＷＥＮＣ、ＴＥＮＣ　暗号化関数
Ｆ　鍵付き関数
ｆ　ｅ－ＡＸＵ関数
ＧＦ（＊）　有限体
Ｈ　ハッシュ関数
Ｋ１、Ｋ２　鍵
Ｌ　調整値依存鍵
Ｍ　平文
ｍｕｌ　乗算
ｐａｄ　パディング関数
Ｓ、Ｓ’　マスク値
ＳｅｃＮｕｍ　セクタ番号
Ｔ、Ｔ’　調整値
Ｖ、Ｖ’　中間値

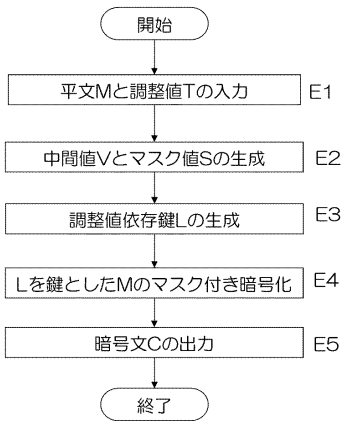
【図１】


10
ブロック暗号化装置
100
入力部
調整値T
101
鍵付きハッシュ部
平文M
中間値V
102
調整値依存鍵導出部
マスク値S
調整値依存鍵L
103
マスク付きブロック暗号化部
暗号文C
104
出力部

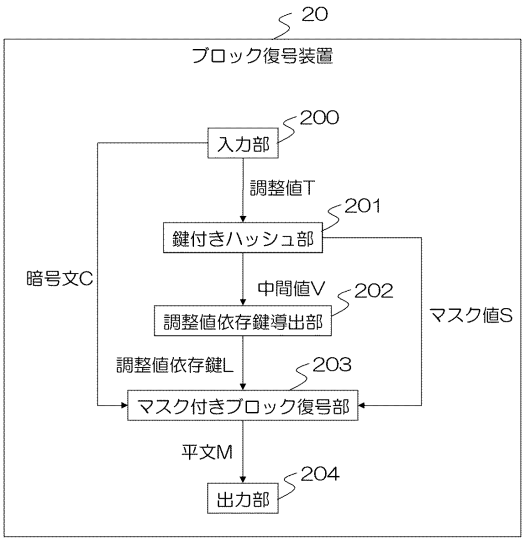
【図２】


M
n
T
b
101
S
n
H
K2
V
m< n/2
Enc
pad
103
L
n
n
Enc
n
K1
n
C
102

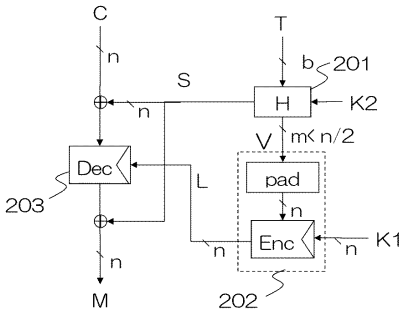
【図３】


開始
平文Mと調整値Tの入力
E1
中間値Vとマスク値Sの生成
E2
調整値依存鍵Lの生成
E3
Lを鍵としたMのマスク付き暗号化
E4
暗号文Cの出力
E5
終了

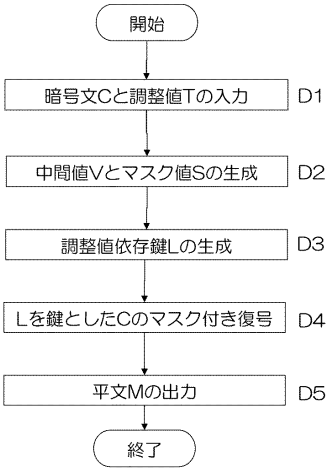
【図４】


20
ブロック復号装置
200
入力部
調整値T
201
鍵付きハッシュ部
暗号文C
中間値V
202
調整値依存鍵導出部
マスク値S
調整値依存鍵L
203
マスク付きブロック復号部
平文M
204
出力部

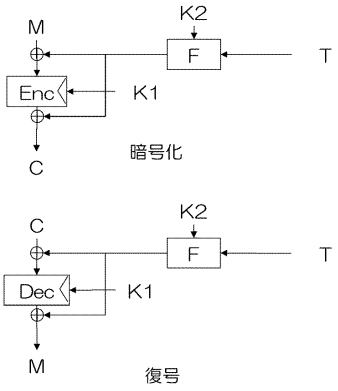
【図５】


C
n
T
b
201
S
n
H
K2
V
m< n/2
Dec
203
L
pad
n
Enc
n
K1
n
M
202

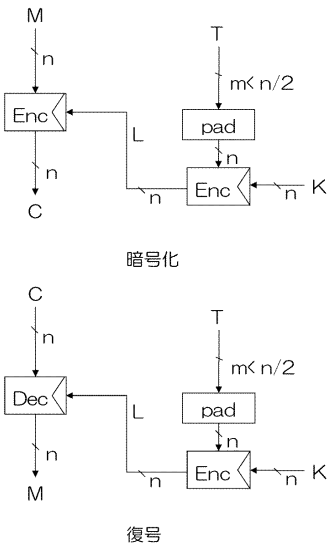
【図６】


開始
暗号文Cと調整値Tの入力
D1
中間値Vとマスク値Sの生成
D2
調整値依存鍵Lの生成
D3
Lを鍵としたCのマスク付き復号
D4
平文Mの出力
D5
終了

【図７】


M
K2
F
T
Enc
K1
C
暗号化
C
K2
F
T
Dec
K1
M
復号

【図８】


M
n
T
m< n/2
Enc
L
pad
n
n
Enc
n
K
C
暗号化
C
n
T
m< n/2
Dec
L
pad
n
n
Enc
n
K
M
復号

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２００９／１２８３７０（WO，Ａ１）
国際公開第２０１０／０２４００４（WO，Ａ１）
米国特許出願公開第２００９／０３１０７７８（ＵＳ，Ａ１）
米国特許第０６２４３４７０（ＵＳ，Ｂ１）
Mohamed Abo El-Fotouch and Klaus Diepold, “A New Narrow Block Mode of Operations for Disk Encryption”, ISIAS'08. Fourth International Conference, IEEE Computer Society, ２００８年 9月, p.126-131
Kazuhiko Minematsu, “Beyond-Birthday-Bound Security Based on Tweakable Block Cipher”, 16th International Workshop, FSE 2009, Springer, ２００９年 1月, p.308-326
Kazuhiko MINEMATSU and Toshiyasu MATSUSHIMA, “Generalization and Extension of XEX* Mode”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, THE ENGINEERING SCIENCE SOCIETY, ２００９年 2月 1日, E92-A(2), p.517-524
Kazuhiko Minematsu, “How to Thwart Birthday Attacks against MACs via Small Randomness”, Fast Software Encryption - FSE 2010, 17th International Workshop, [online], ２０１０年 2月, p.230-249, [retrieved on 2014-08-14]. Retrieved from the Internet, ＵＲＬ, <http://www.iacr.org/archive/fse2010/61470235/61470235.pdf>
Kazuhiko Minematsu, “Improved Security Analysis of XEX and LRW Modes”, LNCS, Selected Areas in Cryptography, ２００６年 8月, Vol.4356, pp.96-113

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ 1／００
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ Ｘｐｌｏｒｅ