(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3642246号
(P3642246)
(45)発行日　平成17年4月27日(2005.4.27)　(24)登録日　平成17年2月4日(2005.2.4)

| (51)Int.Cl.[7] | | F I | | |
|---|---|---|---|---|
| G09C | 1/00 | G09C | 1/00 | 650Z |
| H03M | 7/30 | G09C | 1/00 | 610B |
| H04L | 9/08 | H03M | 7/30 | Z |
| | | H04L | 9/00 | 601A |
| | | H04L | 9/00 | 601E |

請求項の数 8　(全 13 頁)

(21)出願番号　特願2000-12734(P2000-12734)
(22)出願日　平成12年1月21日(2000.1.21)
(65)公開番号　特開2001-202018(P2001-202018A)
(43)公開日　平成13年7月27日(2001.7.27)
審査請求日　平成14年9月27日(2002.9.27)

(73)特許権者　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目１２番地
(72)発明者　猪羽　渉
神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内
(72)発明者　菅原　隆幸
神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内
(72)発明者　黒岩　俊夫
神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

最終頁に続く

(54)【発明の名称】鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情

(57)【特許請求の範囲】

【請求項１】

コンテンツ情報暗号化装置によってコンテンツ情報を暗号化し、又はコンテンツ情報復号化装置によって前記暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵情報生成装置が有する論演算部及びＳ－Ｂｏｘによって鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法であって、

前記鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに前記論理演算部によって論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力する第１ステップと、

前記Ｓ－Ｂｏｘによって、前記第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力する第２ステップとを有する鍵情報生成方法。

【請求項２】

コンテンツ情報暗号化装置によってコンテンツ情報を暗号化し、又はコンテンツ情報復号化装置によって前記暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、

論理演算部及びＳ－Ｂｏｘによって鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置であって、

前記論理演算部は、前記鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力するように論理演算し、

前記Ｓ－Ｂｏｘは、前記論理演算部から出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力するように構成した鍵情報生成装置。

【請求項３】

コンテンツ情報暗号化装置によって、第１鍵のもとになる情報を第２鍵で暗号化すると共に、論理演算部及びＳ－Ｂｏｘで前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、

前記第１鍵を生成するにあたって、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに前記論理演算部によって論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力する第１ステップと、

前記Ｓ－Ｂｏｘによって、前記第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力する第２ステップとを有するコンテンツ情報暗号化方法。

【請求項４】

第１鍵のもとになる情報を第２鍵で暗号化すると共に、論理演算部及びＳ－Ｂｏｘで前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化装置であって、

前記第１鍵を生成するにあたって、前記論理演算部は、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力するように論理演算し、

前記Ｓ－Ｂｏｘは、前記論理演算部から出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力するように構成したコンテンツ情報暗号化装置。

【請求項５】

コンテンツ情報復号化装置によって、暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、論理演算部及びＳ－Ｂｏｘで復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復

号化するコンテンツ情報復号化方法であって、
前記第１鍵を生成するにあたって、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに前記論理演算部によって論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力する第１ステップと、
前記Ｓ－Ｂｏｘによって、前記第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力する第２ステップとを有するコンテンツ情報復号化方法。
【請求項６】
暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、論理演算部及びＳ－Ｂｏｘで復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、
前記第１鍵を生成するにあたって、前記論理演算部は、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力するように論理演算し、
前記Ｓ－Ｂｏｘは、前記論理演算部から出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力するように構成したコンテンツ情報復号化装置。
【請求項７】
請求項３記載のコンテンツ情報暗号化方法、もしくは、請求項４記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第１鍵のもとになる情報とを記録媒体にそれぞれ記録したことを特徴とするコンテンツ情報記録媒体。
【請求項８】
請求項３記載のコンテンツ情報暗号化方法、もしくは、請求項４記載のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第１鍵のもとになる情報とを伝送路を介してそれぞれ送信することを特徴とするコンテンツ情報伝送方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、コンテンツ情報を暗号化したり、暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵のもとになる情報から一方向性関数を用いて生成する、鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法に関するものである。
【０００２】
【従来の技術】
近年、ディジタル化が進み、ディジタル化された映像信号や音声情報などのコンテンツ情報を記録媒体に記録して再生したり、あるいは、ソフトウェアやデータなどのコンテンツ

情報をネットワークにより伝送することが盛んに行われている。

【０００３】

そして、著作権を有し且つディジタル化されたコンテンツ情報（以下、ディジタル情報と記す）の不正使用を防止する場合、ディジタル情報に対して所定の暗号化鍵を用いて暗号化し、この暗号化したディジタル情報を磁気テープ，磁気ディスク，光ディスク，カード等の記録媒体に記録したり、あるいは、暗号化したディジタル情報をネットワークを介して伝送したりしている。この後、記録媒体やネットワークを介して提供された暗号化済みのディジタル情報は、暗号化鍵と等価の復号化鍵を用いて復号化されて暗号化前のディジタル情報に戻している。

【０００４】

一方、ＤＥＳ（Data Encryption Standard）暗号化方法は、アメリカ商務省標準局（現在、ＮＩＳＴ：National Institute of Standard Technology ）が決めた暗号標準であり、現在もつとも多く用いられている暗号化方法の一つである。このＤＥＳ暗号化方法では、６４ビット平文入力が６４ビット暗号文出力に変換される。この際、暗号化鍵も平文入力と同じように６４ビット構成であるが、そのうちの８ビットをパリティに使っているので、実質的な暗号化鍵は５６ビット構成となっている。

【０００５】

図４は一般的なＤＥＳ（Data Encryption Standard）暗号化方法に用いられているＳ－Ｂｏｘを示したブロック図である。

【０００６】

図４に示した如く、ＤＥＳ（NIST.FIPS Publication 46-1:Data Encryption Standard.January 22,1988）暗号化方法に用いられているＳ－Ｂｏｘ（Selection －Box ）は、６ビットの入力に対して４ビットを出力する、一方向性関数の一種である。この種の一方向性関数Ｆは、一方向性ハッシュ関数（One-Way Hash Function)、又は単に、ハッシュ関数と呼ばれる、ｘからＦ（ｘ）を計算するのは容易であるが、Ｆ（ｘ）からｘを求めるのは極めて困難な関数Ｆ（ｘ）を用いている。

【０００７】

また、上記したＳ－Ｂｏｘは二次元のテーブルＴを持っていて、４行×１６列のテーブルＴ内に行と列とに対応させて各要素値Ｈが０から１５までの１６進の整数で予め設定されている。そして、入力の６ビットを例えば“ $b_5b_4b_3b_2b_1b_0$ ”とすると、“ $b_5$ ”と“ $b_0$ ”の２ビットでテーブルＴの行を指定し、また“ $b_5$ ”と“ $b_0$ ”の２ビットを除いた“ $b_4b_3b_2b_1$ ”の４ビットでテーブルＴの列を指定し、ここで指定した行列の部位と対応して４ビットからなる一つの要素値Ｈを出力している。

【０００８】

上記した具体例を図４に示すと、Ｓ－Ｂｏｘへの入力６ビットを例えば“１００１００”とした時、“１０”行“００１０”列、すなわち、２行２列の要素値９（＝１００１）を出力している。

【０００９】

【発明が解決しようとする課題】

ところで、公知のＳ－Ｂｏｘを用いて鍵のもとになる情報から、暗号化及び復号化に必要な暗号化鍵及び復号化鍵を生成するために必要な一方向性関数を求めようとする場合、上記したＳ－Ｂｏｘでは入力ビットの“０”と“１”との割合を直接反映しないでテーブルＴから出力を得ることができるので、これを用いて暗号化鍵及び復号化鍵の生成に好適なシステムを実現することが可能である。

【００１０】

しかしながら、暗号化及び復号化に必要な暗号化鍵及び復号化鍵を生成する際に、上記したＳ－Ｂｏｘにより例えば６ビットの入力に対して４ビットを出力するのでは、一定のビット数を減らす一方向性関数しか構成できず、しかも、少ないステップ数で大きなビット数の入力に対して小さなビット数に減らし、かつ任意にその圧縮率を変えられるような一方向性関数を構成することはできないなど問題点が生じている。

【００１１】
【課題を解決するための手段】
本発明は上記課題に鑑みてなされたものであり、第１の発明は、コンテンツ情報暗号化装置によってコンテンツ情報を暗号化し、又はコンテンツ情報復号化装置によって前記暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、鍵情報生成装置が有する論演算部及びＳ－Ｂｏｘによって鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成方法であって、前記鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに前記論理演算部によって論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力する第１ステップと、前記Ｓ－Ｂｏｘによって、前記第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力する第２ステップとを有する鍵情報生成方法である。
【００１２】
【課題を解決するための手段】
また、第２の発明は、コンテンツ情報暗号化装置によってコンテンツ情報を暗号化し、又はコンテンツ情報復号化装置によって前記暗号化したコンテンツ情報を復号化する際に用いられる鍵情報を、論理演算部及びＳ－Ｂｏｘによって鍵のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置であって、前記論理演算部は、前記鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力するように論理演算し、前記Ｓ－Ｂｏｘは、前記論理演算部から出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記鍵情報として出力するように構成した鍵情報生成装置である。
【００１３】
また、第３の発明は、コンテンツ情報暗号化装置によって、第１鍵のもとになる情報を第２鍵で暗号化すると共に、論理演算部及びＳ－Ｂｏｘで前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化方法であって、前記第１鍵を生成するにあたって、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに前記論理演算部によって論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力する第１ステップと、前記Ｓ－Ｂｏｘによって、前記第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力する第２ステップとを有するコンテンツ情報暗号化方法である。
【００１４】

また、第４の発明は、第１鍵のもとになる情報を第２鍵で暗号化すると共に、論理演算部及びＳ－Ｂｏｘで前記第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いてコンテンツ情報を暗号化するコンテンツ情報暗号化装置であって、前記第１鍵を生成するにあたって、前記論理演算部は、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力するように論理演算し、前記Ｓ－Ｂｏｘは、前記論理演算部から出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力するように構成したコンテンツ情報暗号化装置である。

【００１５】

また、第５の発明は、コンテンツ情報復号化装置によって、暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、論理演算部及びＳ－Ｂｏｘで復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化方法であって、前記第１鍵を生成するにあたって、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに前記論理演算部によって論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力する第１ステップと、前記Ｓ－Ｂｏｘによって、前記第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力する第２ステップとを有するコンテンツ情報復号化方法である。

【００１６】

また、第６の発明は、暗号化した第１鍵のもとになる情報を第２鍵で復号化すると共に、論理演算部及びＳ－Ｂｏｘで復号化後の第１鍵のもとになる情報から一方向性関数を用いて第１鍵を生成し、この第１鍵を用いて暗号化したコンテンツ情報を復号化するコンテンツ情報復号化装置であって、前記第１鍵を生成するにあたって、前記論理演算部は、前記第１鍵のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力するように論理演算し、前記Ｓ－Ｂｏｘは、前記論理演算部から出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記第１鍵として出力するように構成したコンテンツ情報復号化装置である。

【００１７】

また、第７の発明は、上記した第３の発明のコンテンツ情報暗号化方法、もしくは、第４の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第１鍵のもとになる情報とを記録媒体にそれぞれ記録したことを特徴とするコンテ

ンツ情報記録媒体である。

【００１８】

また、第８の発明は、上記した第３の発明のコンテンツ情報暗号化方法、もしくは、第４の発明のコンテンツ情報暗号化装置により暗号化した前記コンテンツ情報と、暗号化した前記第１鍵のもとになる情報とを伝送路を介してそれぞれ送信することを特徴とするコンテンツ情報伝送方法である。

【００１９】

【発明の実施の形態】

以下に本発明に係る鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法の一実施例を図１乃至図３を参照して詳細に説明する。

【００２０】

図１は本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【００２１】

まず、図１を用いて本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法について説明する。

【００２２】

図１において、記録側または送信側とは、著作権を有するコンテンツ情報（以下、ディジタル情報と記す）を暗号化して、暗号化したディジタル情報を磁気テープ，磁気ディスク，光ディスク，カード等の記録媒体（コンテンツ情報記録媒体）に記録する側を示し、または、暗号化したディジタル情報をネットワーク（インターネット，電話回線），電波，光無線などの伝送路に送信する側を示しており、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置と対応する側である。

【００２３】

一方、再生側または受信側とは、記録側で暗号化したコンテンツ情報を記録した記録媒体を再生する側を示し、または、送信側で暗号化したコンテンツ情報を伝送路を介して受信する側を示しており、コンテンツ情報復号化方法、コンテンツ情報復号化装置と対応する側である。

【００２４】

まず、記録側または送信側において、ディジタル化された映像信号や音声情報など著作権を有するディジタル情報０４は、暗号化鍵である第１鍵Ｋ１を用いて第１暗号化装置０５によって暗号化される。この際、第１鍵Ｋ１は、第１鍵のもとになる情報０１から後述する一方向性関数０３を用いて生成される。

【００２５】

また、第１鍵のもとになる情報０１は、システム固有の第２鍵（以下、システム鍵と記す）Ｋ２を用いて暗号化される。このシステム鍵Ｋ２は、システム固有のＩＤなどを用いて生成した暗号化鍵である。

【００２６】

そして、第１鍵Ｋ１を用いて第１暗号化装置０５によって暗号化したディジタル情報０７と、システム鍵Ｋ２を用いて第２暗号化装置０２によって暗号化した第１鍵のもとになる情報０６とが、記録側で磁気テープ，磁気ディスク，光ディスク，カード等の記録媒体に記録されて再生側に提供されるか、または、ネットワーク（インターネット，電話回線），電波，光無線などの伝送路を介して送信されて受信側で受信される。

【００２７】

次に、再生側または受信側において、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化された第１鍵のもとになる情報０６は、第２復号化装置０８でシステム

固有の第２鍵（システム鍵）Ｋ２を用いて第１鍵のもとになる情報０９に復号化される。ここで用いられるシステム鍵Ｋ２も、システム固有のＩＤなどを用いて生成した復号化鍵であり、且つ、記録側または送信側で暗号化時に用いたシステム鍵Ｋ２と等価のものである。

【００２８】

また、記録媒体から読み出すか、または、伝送路を介して受信した、暗号化されたディジタル情報０７は、復号化鍵である第１鍵Ｋ１を用いて第１復号化装置１１で元のディジタル情報（コンテンツ情報）１２に復号化される。この際、第１鍵Ｋ１は、第２復号化装置０８から出力された復号化後の第１鍵のもとになる情報０９から後述する一方向性関数１０を用いて生成され、且つ、記録側または送信側で暗号化時に用いた第１鍵Ｋ１と等価のものである。

【００２９】

上記した暗号化及び復号化において、システム鍵Ｋ２は予め、記録側または送信側と、再生側または受信側で共通になるよう設定しておいても良く、更に、既知の公開鍵暗号方式や鍵配送方式を用いてもかまわない。

【００３０】

次に、本発明の要部をなす上記した第１鍵Ｋ１を生成する鍵情報生成方法及び鍵情報生成装置について、図２乃至図３を用いて説明する。

【００３１】

図２は図１に示した第１鍵を生成する鍵情報生成方法を説明するための具体例を示した図、

図３は第１鍵を生成する鍵情報生成装置の具体例を示したブロック図である。

【００３２】

上記したように、第１鍵Ｋ１は暗号化前のディジタル情報０４への暗号化及び暗号化したディジタル情報０７への復号化に用いられる鍵情報であり、この第１鍵Ｋ１は先に説明した一方向性関数０３，１０を適用しているものの、本発明に係る鍵情報生成方法及び鍵情報生成装置では、本発明で新たに開発した第１ステップと、従来技術で説明したＤＥＳ暗号化方法におけるＳ－Ｂｏｘを適用した第２ステップとを組み合わせて第１鍵Ｋ１を生成することを特徴とするものである。

【００３３】

まず、図２に示した本発明に係る鍵情報生成方法は、一方向性関数を用いて第１鍵Ｋ１を生成するにあたって、第１鍵のもとになる情報０１（又は０９）を入力して、ここで入力した多数のビットからなるビット列を基にして、第１，第２ステップを経て、第１ステップで入力したビット列のビット数より極めて少ないビット数のビット列を生成して、これを第１鍵Ｋ１にすることを示している。

【００３４】

即ち、図２及び図３に示した本発明に係る鍵情報生成方法及び鍵情報生成装置の具体例において、本発明で新たに開発した第１ステップでは、第１鍵のもとになる情報０１（又は０９）は多数のビットで第１ビット列を形成しており、この第１ビット列を鍵情報生成装置２０に設けた論理演算部２１に入力する。

【００３５】

上記した論理演算部２１では、入力した第１ビット列の各ビットを、行列を有する第１マトリックスＭ１内に所定の配列規則に従って配置している。この際、第１マトリックスＭ１内に第１ビット列の各ビットを配置するための所定の配列規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

この後、第１マトリックスＭ１内で入力した第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、各ブロック内の複数のビットをブロックごとに順に論理演算する。そして、論理演算して得られた各結果のビットを、第１マトリックスＭ１より行列を小さくした第２マトリックスＭ２内にブロック順に配置して、第２マトリックスＭ２内の各ビットから第１ビット列のビット数より少な

いビット数の第２ビット列を生成して出力している。

【００３６】

即ち、具体例における第１ステップでは、第１鍵のもとになる情報０１（又は０９）を基にして例えば２５ビットごとに順次取り出す。入力した２５ビットの第１ビット列を、最上位から順に$a_{11}a_{12}a_{13}a_{14}a_{15}a_{21}a_{22}a_{23}a_{24}a_{25}\cdots\cdots a_{51}a_{52}a_{53}a_{54}a_{55}$とし、各ビットの値は“０”又は“１”のバイナリデータとする。

【００３７】

そして、入力した２５ビットからなる第１ビット列のうちで例えば$a_{11}a_{12}a_{13}a_{14}a_{15}$を第１マトリックスＭ１内の第１行目に列に沿って配置し、$a_{21}a_{22}a_{23}a_{24}a_{25}$を第２行目に列に沿って配置し、以下同様に順次繰り返して、$a_{51}a_{52}a_{53}a_{54}a_{55}$を第５行目に列に沿って配置することで、入力した各ビットを第１マトリックスＭ１内に５×５のビットマトリックスとして配置している。

【００３８】

この後、第１マトリックスＭ１内で入力した第１ビット列のビット数より少ないビット数で例えば$a_{11}a_{12}a_{21}a_{22}$を第１ブロックとして形成して、$a_{11}$と$a_{12}$と$a_{21}$と$a_{22}$とで排他的論理和を取り、この排他的論理和の結果のビット$b_{11}$を第２マトリックスＭ２内の第１行，第１列目に配置する。次に、第１ブロックに対して列を１列ずらした$a_{12}a_{13}a_{22}a_{23}$を第２ブロックとして形成して、上記と同様に論理演算した結果のビット$b_{12}$を第２マトリックスＭ２内の第１行第２列目に配置する。上記のように、列方向に沿って４ブロックの論理演算処理が終わったら、１行ずらして再び上記処理を順次繰り返し、合計で１６ブロックの論理演算処理が全て終了すると、第２マトリックスＭ２内に４×４のビットマトリックスが形成される。この後、第２マトリックスＭ２内の４×４のビットマトリックスから第２ビット列として１６ビットからなる$b_{11}b_{12}b_{13}b_{14}b_{21}b_{22}b_{23}b_{24}b_{31}b_{32}b_{33}b_{34}b_{41}b_{42}b_{43}b_{44}$を生成して、この第２ビット列を後述するＳ－Ｂｏｘ２２側に出力することで第１ステップを終了する。

【００３９】

この第１ステップでは、入力した２５ビットを第１マトリックスＭ１内でブロックごとの排他的論理和を取ることにより１６ビットまで削減できる。

【００４０】

尚、具体例における第１ステップでは、第１鍵のもとになる情報０１（又は０９）を基にして入力した多数のビットを２５ビットとしたがこれに限ることなく更に大きなビット数でも良い。また、第１マトリックスＭ１内で入力した多数のビット（２５ビット）を第１ビット列の最上位から最下位に向かって順に配置して説明したが、これに限ることなく、所定の配列規則に従って配置しても良い。また、第１マトリックスＭ１内に形成した各ブロックごとの論理演算も排他的論理和（ＥＸ－ＯＲ）に代えて論理和（ＯＲ）又は論理積（ＡＮＤ）で行っても良い。更に、第１鍵のもとになる情報０１（又は０９）により入力した第１ビット列のビット数が大きい場合は第１ステップの形態を複数回繰り返して複数の出力ビットを得れば良い。

【００４１】

次に、具体例の第２ステップは従来技術で説明したＤＥＳ暗号化方法におけるＳ－Ｂｏｘを適用しており、この第２ステップでは、鍵情報生成装置２０に設けたＳ－Ｂｏｘ２２内に二次元のテーブルＴを持ち、このテーブルＴに対して第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従って行と列とを指定している。この際、第２ビット列の複数のビットを用いてテーブルＴの行と列とを指定するための所定の規則は、記録側又は送信側と、再生側又は受信側とが同じになるように決められている。

また、テーブルＴは、従来例で説明したと同様に、指定した行列の各部位に対応して第２ビット列より少ないビット数の第３ビット列からなる要素値Ｈが予め設定されている。そして、指定された行列に対応した部位から一つの要素値Ｈを第１鍵Ｋ１として出力するか、または、上記した第１，第２ステップを並列処理するか又は第１ステップを並列処理するかもしくは第２ステップを並列処理して、この並列処理で得られた複数の要素値Ｈを合

体させたビット列を第１鍵Ｋ１として出力している。

【００４２】

これにより、第２ステップで得られた第１鍵Ｋ１のビット数は、第１ステップで入力した第１ビット列の多数のビット数に対して極めて少ないビット数に削減されている。

【００４３】

即ち、具体例における第２ステップでは、第１ステップで出力した１６ビットからなる第２ビット列として$b_{11}b_{12}b_{13}b_{14}b_{21}b_{22}b_{23}b_{24}b_{31}b_{32}b_{33}b_{34}b_{41}b_{42}b_{43}b_{44}$のうちから選択した８ビットの$b_{11}b_{12}b_{13}b_{14}b_{21}b_{22}b_{23}b_{24}$を用いて、テーブルＴの行と列とを指定している。尚、$b_{11}b_{12}b_{13}b_{14}b_{21}b_{22}b_{23}b_{24}b_{31}b_{32}b_{33}b_{34}b_{41}b_{42}b_{43}b_{44}$のうちで残りの８ビットの$b_{31}b_{32}b_{33}b_{34}b_{41}b_{42}b_{43}b_{44}$は、同一のテーブルＴで上記と同様に処理するか、または、異なるテーブルで処理している。

【００４４】

ここで、第２ビット列から選択した８ビットの$b_{11}b_{12}b_{13}b_{14}b_{21}b_{22}b_{23}b_{24}$のうちで$b_{11}b_{12}b_{13}b_{14}$の４ビットでテーブルＴの行を指定し、$b_{21}b_{22}b_{23}b_{24}$の４ビットでテーブルＴの列を指定している。

【００４５】

ここで、テーブルＴ内では、指定した行列に対応した部位の要素値Ｈを０から１５までの整数、すなわち１６進数で表せば、０からｆの４ビットの値として予め設定されている。そして、指定した行列に対応した部位の４ビットからなる要素値Ｈを第１鍵Ｋ１としてＳ－Ｂｏｘ２２から出力している。そして、Ｓ－Ｂｏｘ２２から出力され、一方向性関数により生成された第１鍵Ｋ１は、第１暗号化装置０５でディジタル情報０４の暗号化に用いられ、また、第１復号化装置１１で暗号化したディジタル情報０７の復号化に用いられている。

【００４６】

尚、テーブルＴ内の各要素値Ｈを０から１５以外の数とし、４ビット以外の出力としても良い。尚また、実施例では暗号化を２段としたが、第ｎ－１鍵（但し、ｎは３以上の整数）のもとになる情報を第ｎ暗号化装置で暗号化する場合、第ｎ鍵をのもとになる情報から第ｎ鍵を生成するのに、上記の一方向性関数を用いたシステムを構築することも可能である。

【００４７】

【発明の効果】

以上詳述した本発明に係る鍵情報生成方法、コンテンツ情報暗号化方法、コンテンツ情報復号化方法によると、とくに、コンテンツ情報暗号化装置によってコンテンツ情報を暗号化し、又はコンテンツ情報復号化装置によって前記暗号化したコンテンツ情報を復号化する際に用いられる鍵情報（第１鍵）を、鍵情報生成装置が有する論演算部及びＳ－Ｂｏｘによって鍵（第１鍵）のもとになる情報から一方向性関数を用いて生成するにあたって、前記鍵（第１鍵）のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに前記論理演算部によって論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力する第１ステップと、前記Ｓ－Ｂｏｘによって、前記第１ステップで出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記鍵情報（第１鍵）として出力する第２ステップとで行っているので、本発明により容易にシステムに応じた量のビット数を少ないステップ数でかつセキュリティを保持したまま減少させることが可能な一方向性関数を実現することができる。そしてこの一方向性関数は入力ビットの“０”と“１”の割合を出力に直接反映させないため、暗号化鍵及び復号化鍵に利用するのに

好適で、かつ鍵（第１鍵）のもとになる情報は必要な鍵のサイズに関係なく設定することが可能となる。また、一方向性関数内のビット演算の方法や置換によって、より鍵生成のメカニズムのセキュリティを高めることができる。

【００４８】

本発明に係る鍵情報生成装置、コンテンツ情報暗号化装置、コンテンツ情報復号化装置によると、とくに、コンテンツ情報暗号化装置によってコンテンツ情報を暗号化し、又はコンテンツ情報復号化装置によって前記暗号化したコンテンツ情報を復号化する際に用いられる鍵情報（第１鍵）を、論理演算部及びＳ－Ｂｏｘによって鍵（第１鍵）のもとになる情報から一方向性関数を用いて生成する鍵情報生成装置であって、前記論理演算部は、前記鍵（第１鍵）のもとになる情報を入力し、ここで入力した多数のビットからなる第１ビット列の各ビットをマトリックス内に所定の配列規則に従って配置し、且つ、前記マトリックス内で前記第１ビット列のビット数より少ないビット数からなる複数のビットを１単位としたブロックを複数形成し、更に、前記各ブロック内の複数のビットを当該ブロックごとに論理演算して得られた各結果のビットで前記第１ビット列のビット数より少ないビット数の第２ビット列を出力するように論理演算し、前記Ｓ－Ｂｏｘは、前記論理演算部から出力した第２ビット列の複数のビットを用いて所定の規則に従ってテーブルの行と列とを指定すると共に、前記テーブル内に行と列とに対応させて前記第２ビット列より少ないビット数の第３ビット列からなる各要素値を予め設定しておき、前記指定した行列の部位と対応して一つの前記要素値を前記鍵情報（第１鍵）として出力するように構成したので、上記した各方法で述べた効果と同様の効果を得ることができる。

【００４９】

また、本発明に係るコンテンツ情報記録媒体、コンテンツ情報伝送方法によれば、上記した第１鍵を用いて暗号化したコンテンツ情報と、暗号化した第１鍵のもとになる情報とを記録媒体にそれぞれ記録するか、または、伝送路を介してそれぞれ送信しているので、コンテンツ情報のセキュリティを高めることができる。

【図面の簡単な説明】

【図１】本発明に係るコンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法を説明するためのブロック図である。

【図２】図１に示した第１鍵を生成する鍵情報生成方法を説明するための具体例を示した図である。

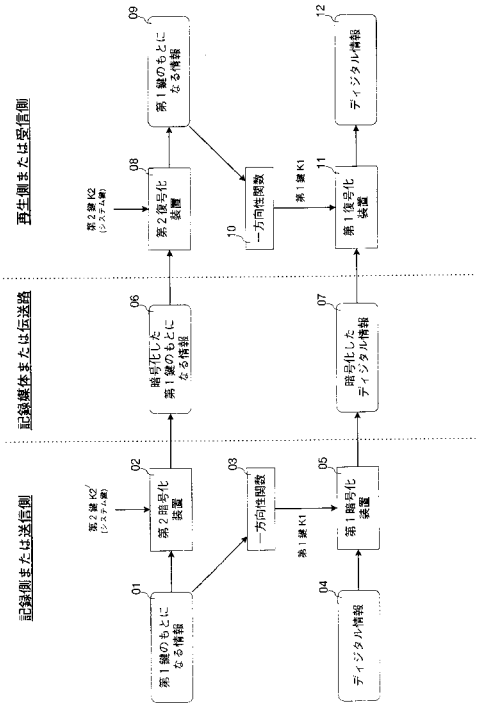
【図３】第１鍵の生成する鍵情報生成装置の具体例を示したブロック図である。

【図４】一般的なＤＥＳ（Data Encryption Standard）暗号化方法に用いられているＳ－Ｂｏｘを示したブロック図である。

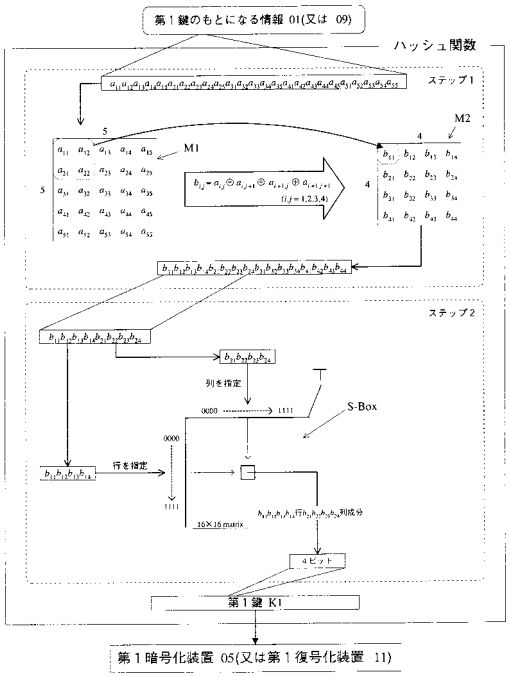
【符号の説明】

０１…第１鍵のもとになる情報、０２…第２暗号化装置、
０３…一方向性関数、０４…コンテンツ情報（ディジタル情報）、
０５…第１暗号化装置、０６…暗号化した第１鍵のもとになる情報、
０７…暗号化したディジタル情報、０８…第２復号化装置、
０９…第１鍵のもとになる情報、１０…一方向性関数、
１１…第１復号化装置、１２…コンテンツ情報（ディジタル情報）、
２０…鍵情報生成装置、２１…論理演算部、
２２…Ｓ－Ｂｏｘ、
Ｋ１…第１鍵、Ｋ２…第２鍵（システム鍵）、
Ｍ１…第１マトリックス、Ｍ２…第２マトリックス、
Ｔ…テーブル。

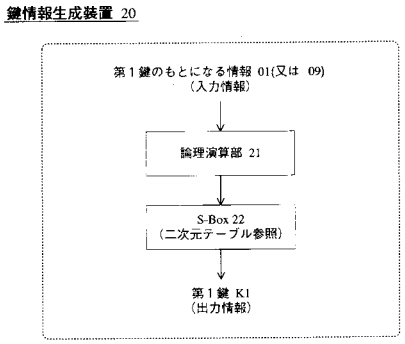
【図１】


再生側または受信側
記録媒体または伝送路
記録側または送信側
第１鍵のもとになる情報
第２復号化装置
一方向性関数
第１復号化装置
ディジタル情報
暗号化した第１鍵のもとになる情報
暗号化したディジタル情報
第２暗号化装置
第１暗号化装置
第２鍵 K2
第１鍵 K1

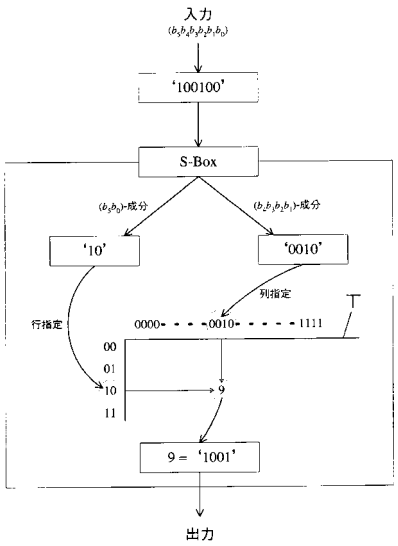
【図２】


第１鍵のもとになる情報 01(又は 09)
ハッシュ関数
ステップ１
M1
M2
ステップ２
列を指定
行を指定
S-Box
16×16 matrix
4ビット
第１鍵 K1
第１暗号化装置 05(又は第１復号化装置 11)

【図３】


鍵情報生成装置 20
第１鍵のもとになる情報 01(又は 09)
（入力情報）
論理演算部 21
S-Box 22
（二次元テーブル参照）
第１鍵 K1
（出力情報）

【図４】


入力
'100100'
S-Box
'10'
'0010'
列指定
行指定
00
01
10
11
9
9 = '1001'
出力

フロントページの続き

(72)発明者　上田　健二朗
神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内
(72)発明者　日暮　誠司
神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

審査官　青木　重徳

(56)参考文献　特開平４－１５０４２８（ＪＰ，Ａ）
特開２００１－２１１１５８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
G09C　1/00　650
G09C　1/00　610
H03M　7/30
H04L　9/08

(54)【発明の名称】鍵情報生成方法、鍵情報生成装置、コンテンツ情報暗号化方法、コンテンツ情報暗号化装置、コンテンツ情報復号化方法、コンテンツ情報復号化装置、コンテンツ情報記録媒体、コンテンツ情報伝送方法