(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5468898号
(P5468898)
(45)発行日　平成26年4月9日(2014.4.9)　(24)登録日　平成26年2月7日(2014.2.7)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601A

請求項の数 16 (全 19 頁)

(21)出願番号	特願2009-517566 (P2009-517566)
(86)(22)出願日	平成19年6月29日 (2007.6.29)
(65)公表番号	特表2009-543415 (P2009-543415A)
(43)公表日	平成21年12月3日 (2009.12.3)
(86)国際出願番号	PCT/IB2007/052530
(87)国際公開番号	WO2008/001327
(87)国際公開日	平成20年1月3日 (2008.1.3)
審査請求日	平成22年6月25日 (2010.6.25)
(31)優先権主張番号	06116450.5
(32)優先日	平成18年6月30日 (2006.6.30)
(33)優先権主張国	欧州特許庁 (EP)

(73)特許権者　590000248
コーニンクレッカ　フィリップス　エヌヴェ
オランダ国　５６５６　アーエー　アインドーフェン　ハイテック　キャンパス　５
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介
(74)代理人　100107766
弁理士　伊東　忠重
(72)発明者　ジェリク，メフメト　ウー
オランダ国，５６５６　アーエー　アインドーフェン，ハイ・テク・キャンパス　４４

最終頁に続く

(54)【発明の名称】データを暗号化／復号する方法及び装置

(57)【特許請求の範囲】

【請求項１】

装置を使用してデータを暗号化する方法であって、前記データは、少なくとも部分的に第１の鍵に基づいて複数の暗号化鍵を使用して暗号化され、

前記第１の鍵は、識別情報の雑音のあるソースからの情報を含み、それにより、識別情報ベースの暗号化を提供し、

前記複数の暗号化鍵のうちの少なくとも１つは、前記複数の暗号化鍵のうちのその他のそれぞれの暗号化鍵に存在していない鍵情報を含み、

前記データを冗長表現に符号化器によって符号化する工程であって、前記符号化する工程は、いくつかの群の間で前記データの情報内容を分散させる工程を含み、各群は、前記複数の暗号化鍵のうちの個別の暗号化鍵に関連付けられ、各暗号化鍵は少なくとも一群と関連付けられ、前記冗長表現は、少なくとも、前記複数の暗号化鍵のうちの少なくとも１つに関連付けられた群がない状態で前記冗長表現からの前記データの回復を可能にする工程と、

前記個別の関連付けられた暗号化鍵により、各群を暗号化器によって暗号化する工程とを含む方法。

【請求項２】

請求項１記載の方法であって、前記冗長表現は、少なくとも、前記複数の暗号化鍵の何れかの単一の１つに関連付けられた群がない状態で前記冗長表現から前記データを回復することを可能にする方法。

【請求項３】
請求項１記載の方法であって、前記データは、少なくとも３つの暗号化鍵を使用することによって暗号化され、前記データの情報内容は前記いくつかの群にわたって分散される方法。
【請求項４】
請求項１記載の方法であって、前記それぞれの暗号化鍵を形成するために使用される鍵情報は分離性を有する方法。
【請求項５】
請求項１記載の方法であって、前記複数の暗号化鍵のうちのそれぞれを形成するために使用される鍵情報は、
雑音のある識別情報、及び
雑音のない識別情報を含む方法。
【請求項６】
請求項１記載の方法であって、前記複数の暗号化鍵のうちの個別の暗号化鍵それぞれを形成するために使用される鍵情報は、
雑音のある情報と、
前記雑音のある情報の、鍵情報の１つ又は複数のソースとの関係を識別する記述子とを含む方法。
【請求項７】
請求項１記載の方法であって、前記符号化する工程は、
群の間で共有資源が分散される秘密共有手法を施す工程、及び
前記群に誤り検出符号を組み入れる工程
の少なくとも一方を更に含み、前記誤り検出符号は、少なくとも、前記群に含まれるデータの情報内容を包含する方法。
【請求項８】
請求項１記載の方法であって、前記符号化する工程は、誤り訂正符号を前記冗長表現に組み入れる工程を更に含む方法。
【請求項９】
請求項８記載の方法であって、各群は複数のシンボルを含み、各群の複数のシンボルそれぞれは誤り訂正符号の符号語の一部であり、各符号語は最大、個別の群の一シンボルを含む方法。
【請求項１０】
第２の鍵によって装置を使用して暗号化データを復号する方法であって、前記暗号化データは請求項１記載の方法によって形成され、前記第１の鍵及び前記第２の鍵は暗号化／復号鍵対の推定を形成し、
前記暗号化データは、前記第２の鍵に少なくとも部分的に基づいて複数の復号鍵を使用することによって復号され、
前記暗号化鍵の少なくとも１つは、その他のそれぞれの暗号化鍵に存在していない鍵情報を含み、
前記複数の復号鍵それぞれは、前記複数の暗号化鍵の個別の暗号化鍵に関連付けられ、
前記方法は、
前記群を暗号化するために使用される前記暗号化鍵に関連付けられた個別の復号鍵により、少なくとも１つ又は複数の暗号化群を復号器によって復号する工程と、
正しく復号された少なくとも１つ又は複数の群から前記データに関する情報内容を抽出することにより、前記少なくとも１つ又は複数の復号群から前記データを復号化器によって復号化する工程とを含む方法。
【請求項１１】
請求項１０記載の方法であって、前記第２の鍵は、鍵情報の雑音のあるソースからのデータを含む方法。
【請求項１２】

請求項１０記載の方法であって、前記少なくとも１つ又は複数の復号群から前記データを復号化する工程は、正しく復号された複数の群から前記データに関する情報内容を抽出する工程を含む方法。

【請求項１３】

請求項１２記載の方法であって、前記データを復号化する工程は、

複数の復号群に含まれる共有資源に対して秘密共有手法を使用する工程、及び

前記復号群に組み入れられた誤り検出符号を検証することにより、群の有効性を検証する工程の少なくとも一方を含む方法。

【請求項１４】

請求項１０記載の方法であって、前記データを復号化する工程は、

誤り訂正符号により、少なくとも１つ又は複数の復号群を誤り訂正する工程と、

前記誤り訂正された復号群から前記データに関する前記情報内容を抽出する工程とを含む方法。

【請求項１５】

少なくとも部分的に第１の鍵に基づいて複数の暗号化鍵を使用してデータを暗号化する装置であって、

前記第１の鍵は、識別情報の雑音のあるソースからの情報を含み、それにより、識別情報ベースの暗号化を提供し、

前記複数の暗号化鍵の少なくとも１つは、前記複数の暗号化鍵のうちのその他のそれぞれの暗号化鍵に存在していない鍵情報を含み、

前記装置は、

前記データを冗長表現に符号化するよう構成された符号化手段であって、前記符号化手段は、いくつかの群の間で前記データの情報内容を分散させる手段を含み、各群は、前記複数の暗号化鍵のうちの個別の暗号化鍵と関連付けられ、各暗号化鍵は少なくとも一群と関連付けられ、前記冗長表現は少なくとも、その他のそれぞれの暗号化鍵に存在していない鍵情報を含む暗号化鍵と関連付けられた群がない状態で前記冗長表現からの前記データの回復を可能にする符号化手段と、

前記個別の関連付けられた暗号化鍵により、各群を暗号化するよう構成された暗号化手段とを含む装置。

【請求項１６】

第２の鍵により、暗号化データを復号する装置であって、

前記暗号化データは請求項１記載の方法によって形成され、前記第１の鍵及び前記第２の鍵は暗号化／復号鍵対の推定を形成し、

前記暗号化データは、前記第２の鍵に少なくとも部分的に基づいて複数の復号鍵を使用することによって復号され、

前記暗号化鍵の少なくとも１つは、その他のそれぞれの暗号化鍵に存在していない鍵情報を含み、

前記複数の復号鍵それぞれは、前記複数の暗号化鍵のそれぞれの暗号化鍵と関連付けられ、前記装置は、

前記群を暗号化するために使用される前記暗号化鍵と関連付けられた個別の復号鍵により、前記少なくとも１つ又は複数の暗号化群を復号することにより、少なくとも１つ又は複数の暗号化群を復号するよう構成された復号手段と、

正しく復号された少なくとも１つ又は複数の復号群から前記データに関する情報内容を抽出することにより、前記少なくとも１つ又は複数の復号群から前記データを復号化するよう構成された復号化手段とを含む装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、第１の鍵により、データを暗号化する方法及び装置、第２の鍵により、暗号

化データを復号する方法及び装置、第１の鍵によって暗号化されたデータを含む信号、並びに、本発明による方法のうちの１つを行うためにコンピュータ読み取り可能な媒体上に記憶されたプログラム・コード手段を備えるコンピュータ・プログラムに関する。

【背景技術】

【０００２】

現代社会では、情報は主として、ディジタル形式で記憶される。ディジタル・データは、単純なやり方で再生、伝送、及び記憶することが可能であり、よって、高い利便性をもたらす。しかし、前述の利便性は、認可されていない者によるアクセスのかたちでの潜在的なプライバシ上及びセキュリティ上のリスクも伴う。プライバシ及びセキュリティの課題に対処するために、貴重な情報は多くの場合、暗号化される。

【０００３】

暗号化は、効果的に、認可された個人が情報にアクセスすることを可能にする一方で、認可されていない個人による、情報へのアクセスを阻止する障壁を形成する。情報を暗号化する場合、データは一般に、暗号化鍵によって暗号化され、その結果、暗号化データが生成される。セキュリティを備えるために、暗号化データは、元のデータに関する情報を部外者に提供すべきでない。データは、暗号化データから回復するために、暗号化鍵に対応する復号鍵によって復号する必要がある。

【０００４】

大半の暗号化手法は鍵を使用して情報を暗号化し、復号する。データは暗号化鍵によって暗号化され、暗号化データは復号鍵によって復号される。別々の２つのタイプの暗号化（暗号化鍵及び復号鍵が同じである対称暗号化、並びに、暗号化鍵及び復号鍵が異なる非対称暗号化）を区別することが可能である。非対称暗号における暗号化鍵及び復号鍵は、異なるが、一対の鍵（以下、「鍵対」と表す）を形成し、他の鍵を、暗号化鍵又は復号鍵と組合せて使用すると、データが失われてしまう。

【０００５】

比較的新たな傾向には、暗号の鍵情報のソースとしてバイオメトリック・データを使用するということがある。バイオメトリック・データは、好ましくは経時的に安定した個人の好ましくは一意の物理的な特徴から導き出される。アクセス制御に多く使用されるバイオメトリック・モダリティの例には、指紋、掌紋、虹彩画像や、顔の特徴などのモダリティがある。バイオメトリック・データは多くの場合、個々のアクセス制御を設けるために使用される。

【０００６】

個人の物理的な特徴が変わり得るということの他に、前述の物理的な特性から導き出されるバイオメトリックは、測定及び／検知によって取得される。その結果、バイオメトリックには多くの場合、雑音がある。この雑音は、例えば、取得雑音、種々のセンサの使用、種々の環境条件、及び／又は、個人の物理的な特徴における軽微な変動によって生じ得る。雑音を削減し、よりロバストであり、かつより認識できるデータを導き出すために、バイオメトリック測定から特徴ベクトルを導き出す傾向が存在している。しかし、特徴ベクトルは、かなりのばらつきをなお表し、よって、鍵情報として使用するには適切でない。したがって、バイオメトリックにおける、雑音のあるデータからロバストな鍵を導き出すために多くの研究が行われている。

【０００７】

Ａ．Ｓａｈａｉ及びＢ．Ｗａｔｅｒｓによる「Ｆｕｚｚｙ ｉｄｅｎｔｉｔｙ－ｂａｓｅｄ ｅｎｃｒｙｐｔｉｏｎ，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ＥＵＲＯＣＲＹＰＴ，２００５」には、識別情報ベースの暗号システムにおいて、雑音のあるデータを鍵として使用する別の手法が開示されている。前述の特定の手法は、データを暗号化するために使用される、雑音のある暗号化鍵も、暗号化データの復号のために必要である。

【発明の開示】

【発明が解決しようとする課題】

【０００８】

本発明の目的は、第１の鍵によるデータの暗号化を可能にし、第１の鍵及び第２の鍵が暗号化／復号鍵対の十分な推定を形成しているという前提で、第１の鍵を必要とすることなく、第２の鍵により、暗号化データのその後の復号を可能にすることにより、暗号化及び／又は復号における厳密な鍵情報に対する必要性を軽減する解決策を提供することである。

【課題を解決するための手段】

【０００９】

前述の目的は、請求項１記載のデータを暗号化する方法、及び請求項１２記載のデータを復号する方法によって実現される。

【００１０】

暗号化／復号鍵対の推定を併せて構成する、雑音のある暗号化鍵及び／又は雑音のある復号鍵を使用する場合、雑音のある暗号化鍵によって暗号化されたデータを、雑音のある復号鍵で復号することが可能であるかは確かでない。

【００１１】

正しくない暗号化／復号鍵対の使用に関する問題点を軽減することができるために、本発明は、第１の鍵に少なくとも部分的に基づく複数の暗号鍵を使用することにより、データを暗号化する。複数の暗号化鍵の少なくとも１つは、その他のそれぞれの暗号化鍵に存在していない鍵情報を含む。

【００１２】

データは、暗号化する前に、冗長表現に符号化される。前述の符号化処理は、データの情報内容をいくつかの群に分散させる処理を含む。分散は、例えば、群の間でのデータの完全な複製及び／又は部分的な複製を含み得る。各群は暗号化鍵と関連付けられ、各暗号化鍵は、今度は、少なくとも一群と関連付けられる。

【００１３】

冗長表現は、複数の暗号化鍵の少なくとも１つに関連付けられた群がない状態で、冗長な表現からデータを回復することを可能にする。これは、冗長表現のその他の群が、元のデータにある情報内容全てを含んでいなければならないことを示唆している。

【００１４】

データ群は、符号化されると、暗号化することが可能である。冗長表現における各群は、個別の関連付けられた暗号化鍵によって暗号化される。暗号化されると、暗号化データを構成する暗号化群は、更なる使用のために記憶又は伝送することが可能である。

【００１５】

本発明によって暗号化されたデータを復号するために、第２の鍵が使用される。第１の鍵及び第２の鍵は、暗号化／復号鍵対の推定を構成する。復号中、暗号化データは複数の復号鍵を使用することによって復号される。複数の復号鍵は、複数の暗号化鍵を生成するために使用される情報と同様な情報を使用することによって生成される。しかし、復号鍵を生成する場合、第１の鍵の代わりに第２の鍵が使用される。

【００１６】

複数の復号鍵をそれぞれ、複数の暗号化鍵のうちの個別の１つと関連付け、それによって、暗号化鍵及び関連付けられた復号鍵の複数の対を形成する。理想的には、暗号化鍵と、関連付けられた復号鍵との間の不整合がない場合、暗号化鍵及び関連付けられた復号鍵はそれぞれ、正しい暗号化／復号鍵対を構成する。暗号化鍵のうちの個別の１つによって暗号化された群は、関連付けられた復号鍵によって首尾良く復号することが可能である。しかし、雑音が暗号化鍵及び／又は関連付けられた復号鍵を妨げる場合、前述の暗号化鍵によって暗号化された群内のデータの情報内容は、関連付けられた復号鍵によって復号されると歪曲される。

【００１７】

復号に続く復号化処理は、データが符号化されると付加される冗長性を使用する。請求項１の冗長表現における冗長性を使用して、複数の暗号化鍵の少なくとも１つに関連付けられた群における誤りを少なくとも補償することが可能である。雑音が、複数の暗号化鍵

の少なくとも１つに単独で存在している鍵情報において生じた場合、関連付けられた鍵は全て歪曲されるが、冗長表現はなお、他の群におけるデータに関する情報内容全てを含む。

【００１８】

復号化処理は、正しく復号された少なくとも１つ又は複数の群から上記データに関する情報内容を抽出する処理を含む。正しく復号された２つ以上の群が必要であるか否かは、使用される実際の冗長表現に依存する。したがって、請求項１及び１２により、暗号化及び／又は復号における厳密な鍵情報に対する必要性が少なくとも軽減される。

【００１９】

本発明による暗号化及び復号の方法は、第１の鍵によるデータの暗号化を可能にし、第１の鍵及び第２の鍵が暗号化／復号鍵対の十分な推定を形成しているという前提で、第１の鍵を必要とすることなく、第２の鍵により、暗号化データのその後の復号を可能にする解決策を提供する。

【００２０】

一実施例では、冗長な表現は、複数の暗号化鍵の何れかの単一の１つに関連付けられた群がない状態で、冗長な表現からデータを少なくとも回復することを可能にする。したがって、鍵対の何れが正しくないかはもう適切でない。

【００２１】

更なる実施例では、第１の鍵及び／第２の鍵は、鍵情報の雑音のあるソースからのデータを含む。鍵情報の雑音のあるソースの好適な例には、バイオメトリから導き出された特徴ベクトルがある。更に効果的な実施例では、特徴ベクトルは、複数の暗号化鍵にわたって一様に分散される。結果として生じる暗号化鍵（及び復号鍵）の鍵の誤りの確率はよって、特徴ベクトルの誤りの確率よりもかなり低い。

【００２２】

更なる実施例では、データは少なくとも３つの暗号化鍵を使用することによって暗号化され、データの情報内容は少なくとも３つの群にわたって分散される。ここで、分散されるということは、群内のデータの部分的な複製を示唆しているが、その全体におけるデータの複製を明示的に除外しているということを示唆している。より多数の暗号化鍵を使用することにより、暗号化鍵毎の誤りの確率は低下し得る。更に、多数の群にわたってデータ量を分散させることにより、正しくない暗号化／復号鍵対の使用によって影響を受けるデータの量を削減することが可能である。両方の要因が、データ回復の確率の増加に寄与し得る。

【００２３】

データの分散は、対応する復号方法にも影響を及ぼす。したがって、対応する復号方法は、少なくとも３つの復号鍵を使用する。冗長表現からデータを回復するために、複数の復号化群の情報内容を回復し、合成しなければならない。

【００２４】

更なる実施例では、暗号化鍵を形成するために使用される鍵情報は分離性を有する。複数の暗号化／復号鍵の１つを形成するためにのみ使用される特定の情報における誤りはよって、単一の暗号化／復号鍵にのみ影響を及ぼす。よって、正しくない暗号化／復号鍵対の生起の確率は削減される。その後、暗号化データを復号すると暗号化群が歪曲される確率も削減される。この特定の特性を、上述する実施例と効果的に組み合わせ、暗号化鍵／復号鍵の誤りの確率、及び影響されるデータの量についての前述の誤りの影響を削減することが可能である。

【００２５】

更なる実施例では、使用される暗号化は、ＩＢＥと以下に表す識別情報ベースの暗号化である。本発明は、雑音のある識別情報を使用することにより、データの暗号化を可能にし、復号中に利用可能な、雑音のある、まさにその識別情報を有する必要なく暗号化データのその後の復号を可能にする。そうすることにおいて、本発明は、データを暗号化するために使用される識別情報を露呈させない解決策を提供する。

【００２６】
上記実施例の効果的な第１の変形では、複数の暗号化鍵のうちの個別の１つを形成するために使用される鍵情報は、雑音のある識別情報及び雑音のない識別情報を含む。雑音のない識別情報を使用しながら、複数の復号鍵を生成する者はよって、鍵情報に含まれる者の識別情報が、複数の復号鍵の受領者と同じであるか、又は、前述の受領者によって信頼できるかを検証する。
【００２７】
暗号化がＩＢＥであるこの実施例の効果的な第２の変形では、それぞれの暗号化鍵それぞれを形成するために使用される鍵情報は、雑音のある識別情報と、鍵情報の１つ又は複数のソースとの、雑音のある識別情報の関係を識別する記述子とを含む。よって、複数の復号鍵を生成する者は、復号鍵を生成するために利用可能な方法を有する。
【００２８】
本発明の実施例では、符号化処理は、共有資源が群の間で分散される秘密共有手法を施す処理を更に含む。この特定のタイプの冗長表現は、元のデータに関する情報を得るために、ｋ個の共有資源のうちの少なくともｎ個が必要であるので、セキュリティの向上をもたらす。
【００２９】
更なる実施例では、符号化処理は、一群における誤り検出符号を組み入れる処理を更に含み、誤り検出符号は少なくとも、群に含まれるデータの情報内容を包含する。よって、復号群において存在しているデータが有効であることを、統計的な確信度を有して判定することが可能である。前述の誤り検出符号の複雑度は、必要なロバスト性に応じて選ぶことができる。
【００３０】
本発明の好ましい実施例では、誤り訂正符号の符号語は冗長表現を形成する。符号語を使用して、暗号化／復号鍵対が誤りであった場合に、歪曲された群を補正し、それにより、正しくない暗号化／復号鍵対の使用にもかかわらず、群の回復を可能にすることが可能である。
【００３１】
更に好ましい実施例では、全群が、複数のシンボルを有し、各群のシンボルが誤り訂正符号の符号語の一部である。更に、各符号語は、個別の群から最大一シンボルを含む。よって、正しくない暗号化鍵／復号鍵対の使用により、符号語毎に最大１シンボル誤りが生じる。よって、歪曲された群を補償するために最小量のパリティ・シンボルが必要である。
【００３２】
本願の暗号化方法の各実施例を、対応する復号方法においてミラーリングすることが可能であることを当業者は認識するであろう。前述の暗号化方法及び対応する復号方法は併せて、暗号化のために第１の鍵の推定を使用し、復号のために第２の鍵を使用し、併せて、暗号化／復号鍵対の推定を形成することに関する問題点を軽減する解決策を提供する。更に、これらは、第１の鍵が、復号のために利用可能であることを必要としない。
【００３３】
明らかに、冗長表現が、正しくない暗号化鍵、及び関連付けられた復号鍵に対処することが可能である程度には限度がある。このことは決して驚くべきことでない。セキュリティを備えるために、暗号化データは、第１の鍵が第２の鍵の十分な推定であるという条件下でのみアクセス可能であるべきであるからである。
【００３４】
実際のシステムでは、第１の鍵と第２の鍵との間の許容可能な最大差は送出者によって選択することができ、又は所定の通信システム値でもあり得る。許容可能な最大差は一般に、
冗長表現のタイプの選択、
許容可能な最大オーバヘッド、

利用可能な最大鍵数、
鍵空間のサイズ、及び
鍵空間内の別々のユーザのエイリアシング鍵の確率
などの要因に関係するトレードオフになる。

【００３５】

本発明の目的は、請求項１７記載の、識別情報ベースの暗号化のための装置、及び請求項１８記載の、暗号化データの識別情報ベースの復号のための装置によって更に実現される。

【発明を実施するための最良の形態】

【００３６】

前述及び他の局面は、図面を参照して更に明らかにし、説明する。

【００３７】

図面を通して、同じ参照符号は同じ構成要素、又は同じ機能を行う構成要素を表す。

【実施例】

【００３８】

図１は、本発明による、データの暗号化、及びその後のデータ復号を含む概略図である。

【００３９】

第１の者（アリス）がデータベース１５０にデータ１０５を記憶しようとしている。認可されていない者がデータ１０５にアクセスすることを阻止するために、アリスはデータを暗号化する。大半の暗号化手法（対称及び非対称）は、データを暗号化するための鍵を使用する。ここで、アリスは、対称暗号法を使用するものとする。対称暗号法では、暗号化鍵及び復号鍵は同一の鍵である。プライバシ／セキュリティを保証するためには、暗号化鍵／復号鍵は、秘密に保たれなければならない。

【００４０】

鍵は、複数の文字を含む文を完成させるために、数字から文字列にわたる種々の形状を呈し得る。理想的には、鍵は、大きなエントロピを有する。したがって、多くの場合、好適な鍵は、ランダムなデータとしてみえる。しかし、前述のランダムなデータは、人間が使用するためにはあまり適していない。個人の物理的な特徴から導き出されるバイオメトリック・データは、代わりに鍵情報のソースとして使用することができる。指紋又は紅彩走査によって生じるバイオメトリック・データは、鍵情報として使用することが可能なかなりの量の高エントロピ情報を提供する。残念ながら、バイオメトリック・データは、特徴ベクトル抽出を使用する場合にも、雑音を有する傾向にある。

【００４１】

本発明は、雑音のある特徴ベクトル１１５の形式の第１の鍵によるデータ暗号化、及び雑音のある更なる特徴ベクトル１８５の形式の第２の鍵による暗号化データのその後の復号を可能にすることにより、前述の問題点を軽減する解決策を提供する。何れの特徴も事実上、同一の物理的な特徴であるので、対称暗号化手法の場合、暗号化／復号鍵対の推定であるものとして解釈することが可能である。

【００４２】

図１に表すシナリオでは、アリスは、データ暗号化のための装置１２０を使用することにより、データ１０５を暗号化する。データ暗号化のための装置１２０は、データ１０５を暗号化するために複数の暗号化鍵１３５を必要とする。この特定のシナリオでは、複数の暗号化鍵は、２つの鍵情報ソース、すなわち、
アリスの指紋から得られる特徴ベクトル１１５、及び
アリスに知られているパスフレーズ１２５）
を使用しながら形成される。

【００４３】

パスフレーズ１２５及び特徴ベクトル１１５は、必要な複数の暗号化鍵を生成する暗号化鍵生成器１１０によって使用される。この特定の実施例では、暗号化鍵生成器１１０は

、装置１２０に含まれないが、この装置と容易に組み合わせることが可能である。利用可能な鍵ソース１１５、１２５に基づいて、暗号化鍵生成器１１０は、特徴ベクトル１１５の情報内容を含む複数の暗号化鍵１３５を生成する。

【００４４】

この実施例では、個別の暗号化鍵はそれぞれ、パスフレーズの別々のセグメント及び特徴ベクトルの別々のセグメントを含む。パスフレーズの誤りの確率がゼロとすると、複数の暗号化鍵のうちの個別の暗号化鍵それぞれにおける鍵の誤りの確率は、特徴ベクトル１１５における誤りの確率よりも低い。アリスによる不完全な記憶又はタイプミスの結果、パスフレーズの誤りの確率は一般に、ゼロにならない。この特定のシナリオでは、本発明は、前述の誤りも補償する。

【００４５】

データ暗号化のための装置１２０は、符号化手段１２１及び暗号化手段１２３を含む。符号化手段は、データを冗長表現１２２に符号化するよう構成される。符号化処理は、いくつかの群の間でデータ１０５の情報内容を分散させる処理を含む。前述の群はそれぞれ、複数の暗号化鍵の組１３５からの個別の暗号化鍵と関連付けられる。同様に、各暗号化鍵は少なくとも１つの群と関連付けられる。冗長表現１２２は少なくとも、複数の暗号化鍵１３５のうちの何れか３つに関連付けられた群がない状態で、冗長表現１２２からのデータ１０５の回復を可能にする。暗号化手段１２３は、群を暗号化し始め、利用可能になると冗長表現１２２を形成することが可能である。各群は、関連付けられた個別の暗号化鍵によって暗号化される。

【００４６】

アリスは、後に、暗号化データ１２４からのデータ１０５にアクセスしたい場合、複数の復号鍵１６５を得なければならない。複数の復号鍵１６５は、アリスがメッセージを暗号化する前に生成することができるか、又は、あるいは、データが暗号化された後、そうすることができる。更なる特徴ベクトル１８５が、複数の復号鍵を生成するために必要である。

【００４７】

複数の復号鍵それぞれを、複数の暗号化鍵のうちの個別の暗号化鍵と関連付け、事実上、暗号化鍵及び関連付けられた復号鍵の複数の対を形成する。複数の復号鍵１６５は、復号鍵生成器１９０によって生成される。この特定のシナリオは対称暗号法に関係するので、復号鍵生成器１９０は暗号化鍵生成器１１０と同一である。非対称暗号法の場合、同じ入力を同様に使用するが、別々の鍵生成器が必要である。

【００４８】

復号鍵を生成するために、アリスは更なるパスフレーズ１７５を入力し、更なる特徴ベクトル１８５を供給する。このデータを入力として、復号鍵生成器１９０はその後、対応する複数の復号鍵１６５を生成する。復号鍵は、暗号化鍵を生成するために使用されるやり方と同様に生成される。

【００４９】

理想的には、暗号化鍵生成器１１０及び復号鍵生成器１９０の入力が同一である場合、暗号化／復号鍵対は全て正しいものになる。対称暗号手法の場合このことは、各暗号化鍵及び関連付けられた復号鍵が同一であることを示唆している。実際には、少なくとも１つの暗号化／復号鍵対が、取得処理における雑音が理由で、正しくないものになる。

【００５０】

暗号化データを復号する装置１８０は、復号手段１８１及び復号化手段１８３を含む。復号手段１８１は、符号化群を復号するよう構成される。各暗号化群は、群を暗号化するために使用される暗号化鍵と関連付けられた個別の復号鍵によって復号される。復号手段１８１によって出力される復号化群１８２は、正しく復号される群、及び／又は、復号中に歪曲される群を含み得る。

【００５１】

復号化手段１８３は、正しく復号された少なくとも１つ又は複数の群から上記データに

関する情報内容を抽出することにより、復号群１８２からデータを復号化するよう構成される。このシナリオでは、冗長表現は、何れかの３つの暗号化鍵がなくてもデータの再生を可能にし、正しくない暗号化鍵及び関連付けられた復号鍵の最大３つの対を補償することが可能である。

【００５２】

暗号化データ１０５を復号群から試行錯誤手法を使用することによって回復することが可能であるが、誤り検出符号による符号化中に各群に適合させ、それにより、群が正しく復号されたか否かを確認するための単純な機能を提供することが好ましい。

【００５３】

上記例は、本発明を対称暗号システムにおいて使用することができるやり方を示す。しかし、非対称暗号法を使用するシステムにおいて適用して、同様な効果を得ることができる。非対称暗号法における鍵は通常、公開鍵及び秘密鍵として表される。公開及び秘密の語は、意図された鍵の露呈を表す。公開鍵は全員に配布することができる一方、秘密鍵は秘密を保つべきである。公開鍵で暗号化されたメッセージは、対応する秘密鍵で復号することが可能である。逆に、秘密鍵で暗号化されたメッセージは、対応する公開鍵で復号することが可能である。公開鍵及び秘密鍵は対を形成する。ここで、他方の鍵が復号に使用される限り、一方の鍵を暗号化に使用することが可能である。

【００５４】

識別情報ベースの暗号手法を使用した非対称暗号手法において本発明を使用することは、以下の段落で考察する。

【００５５】

最初の識別情報ベースの暗号システムは、内容を本明細書及び特許請求の範囲に援用する、Ａ．　Ｓｈａｍｉｒによる「Ｉｄｅｎｔｉｔｙ－ｂａｓｅｄ　Ｃｒｙｐｔｏｓｙｓｔｅｍｓ　ａｎｄ　Ｓｉｇｎａｔｕｒｅ　Ｓｃｈｅｍｅｓ，　ｔｈｅ　ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ＣＲＹＰＴＯ　’８４」である。ＳｈａｍｉｒがＩＢＳ手法を開示しているが、最初の識別情報ベース暗号化（ＩＢＥ）の手法は、２者によって互いに独立して開示された、内容を本明細書及び特許請求の範囲に援用するＤ．　Ｂｏｎｅｈ及びＭ．　Ｆｒａｎｋｌｉｎによる「Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　ｆｒｏｍ　ｔｈｅ　Ｗｅｉｌ　Ｐａｉｒｉｎｇ，　ｔｈｅ　Ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ＣＲＹＰＴＯ　２００１」、及びＣ．　Ｃｏｃｋｓによる「Ａｎ　Ｉｄｅｎｔｉｔｙ　Ｂａｓｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｃｈｅｍｅ　Ｂａｓｅｄ　ｏｎ　Ｑｕａｄｒａｔｉｃ　Ｒｅｓｉｄｕｅｓ”，　ｔｈｅ　Ｐｒｏｃｅｅｄｉｎｇｓ　ｏｆ　ＩＭＡ　２００１，　ＬＮＣＳ　２２６０」である。

【００５６】

ＩＢＥ手法は、データを符号化し、復号するために使用することが可能な非対称暗号化手法である。ＩＢＥ手法では、送出者（以下、アリスとして表す）によって送出されたデータは、受領者（以下、ボブとして表す）の識別情報から導き出される公開鍵を使用することによって暗号化される。ボブは、暗号化データをアリスから受信すると、自分の識別情報から導き出された秘密鍵を使用して暗号化データを復号することが可能である。

【００５７】

この手法における公開鍵はボブの識別情報に基づく。前述の識別情報は、アリス及びボブが形式に合意する限り、ボブ自身の名前及び誕生日であり得るか、又は、あるいは、ボブ自身の電子メール・アドレスであり得る。この識別情報をアクセスできる者は何れも、その後、信頼できる権限（以下、ＴＡと表す）からの１つ又は複数の共有公開鍵を使用することにより、ＩＢＥ手法において使用するための公開鍵を生成することが可能である。適切なデータにアクセスできる者は何れも、ボブのためにデータを暗号化するための公開鍵を生成することが可能である。

【００５８】

ＴＡ、又はＴＡによって信頼できる者は対応する秘密鍵を生成する。秘密鍵を生成するために、ＴＡは、ボブの識別情報、及びアリスによって使用されるＴＡのその公開鍵の１

つ又は複数の対応するその秘密鍵の１つ又は複数を使用する。結果として生成される秘密鍵は次いで、ボブに送出される。

【００５９】

受領者の識別データに雑音がある場合のＩＢＥ手法を策定することに対する関心が高まっている。この課題に対処するための手法は、Ｓａｈａｉ ａｎｄ Ｂ．Ｗａｔｅｒｓによる「Ｆｕｚｚｙ ｉｄｅｎｔｉｔｙ－ｂａｓｅｄ ｅｎｃｒｙｐｔｉｏｎ，Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ＥＵＲＯＣＲＹＰＴ，２００５」にみられる。この特定の手法は、暗号化データとともにボブに送出される対象のデータを暗号化するために、アリスによって使用される、雑音がある識別情報を必要とするという欠点を有する。そうすることにおいて、アリスは、ボブの識別情報を盗聴者に、不注意に露呈させてしまう。

【００６０】

対照的に、本発明は、アリスによって使用されるボブの雑音のある識別情報に基づいて複数の暗号化鍵により、データを暗号化することを可能にし、ボブの、雑音のある更なる識別情報に基づいて複数の復号鍵により、データのその後の復号を可能にする。本発明による方法では、暗号化中に使用されたようなボブの雑音のある識別情報を、復号中に利用可能にする必要はない。よって、ボブの識別情報は、盗聴者から隠蔽された状態に留まる。

【００６１】

図２は、本発明による、雑音のある識別情報ベースの暗号化及び復号に関係するシナリオを表す概略図である。アリスとボブは、データを交換したい友人である。ボブは、ボブの指紋のうちの１つから導き出された第１の特徴ベクトル２１５をアリスに供給している。アリスは、ボブ宛のメッセージの暗号化に使用するためにデータベース２２５に第１の特徴ベクトルを記憶している。

【００６２】

アリスは、本発明による、符号化手段１２１及び暗号化手段１２３を有するデータ暗号化装置１２０を使用する。装置は、暗号化鍵生成手段２１０を更に備える。暗号化鍵生成手段２１０は、ＴＡ２９０の１つ又は複数の公開鍵を第１の特徴ベクトル２１５と組み合わせて複数の暗号化鍵１３５を生成する。複数の暗号化鍵１３５をその後、暗号化手段１２３によって使用して、冗長表現１２２を暗号化する。暗号化データ２５０はボブに送出される。

【００６３】

ボブは、暗号化データ２５０を復号するためには、複数の復号鍵の組を得る必要がある。この目的で、ボブはＴＡ２９０に第２の特徴ベクトル２９５を与える。第２の特徴ベクトル２９５は、第１の特徴ベクトル２１５を生成するために使用される指紋の更なる特徴手順から生じる。第２の特徴ベクトル２９５は、第１の特徴ベクトル２１５の推定とみなし得る。

【００６４】

ＴＡ２９０は、第２の特徴ベクトル２９５、及びその秘密鍵のうちの１つ又は複数を使用して複数の復号鍵１６５を生成する。使用する秘密鍵がどれであり、第２の特徴ベクトル２９５とどのようにして合成するかをＴＡ２９０が知っていることが重要である。この知識を使用すれば、かつ、第１の特徴ベクトル２１５及び第２の特徴ベクトル２９５が同一であることを前提とすれば、ＴＡ２９０は、正しい暗号化鍵／復号鍵対を形成する複数の復号鍵１６５を生成することが可能である。しかし、実際には、特徴ベクトルは異なり、１つ又は複数の不一致が、それぞれの複数の暗号化鍵１３５及び関連付けられた復号鍵１６５において生じ得る。

【００６５】

ＴＡ２９０によって生成される復号鍵１６５はボブに送出され、ボブはこれをデータベース２８０に記憶する。ボブは、複数の復号鍵１６５へのアクセスを有する状態になると、暗号化データ１０５を復号する復号処理を開始することが可能である。このために、ボブは装置１８０を使用する。復号処理は、図１中のものと同様であるが、対称復号アルゴ

リズムではなく非対称復号アルゴリズムを伴う。

【００６６】

上記例では、暗号化鍵及び復号鍵は雑音のある鍵の情報のみに基づくが、例えば、ボブの名前や誕生日などの、雑音のない更なる識別情報を、セキュリティに影響を及ぼすことなく付加することができる。雑音のない更なる識別情報は同様に、（秘密）復号鍵が生成される個人の識別情報が、復号鍵を受け取る者に対応するか否かをＴＡ２９０が検証することを可能にする。

【００６７】

更に効果的な実施例では、個別の復号鍵それぞれは、鍵情報、すなわち、

雑音有り識別情報、

雑音なし識別情報、及び

雑音有り識別情報の、鍵情報の１つ又は複数のソースとの関係を識別する記述子

を使用しながら形成される。

【００６８】

ＴＡ２９０はよって、復号鍵の受領者のものと、鍵に関連付けられた識別情報を一致させることが可能であるが、しかし、更に、記述子は、どのようにしてそれぞれの復号鍵を生成するかという方法をＴＡ２９０に与える。

【００６９】

更に好ましくは、雑音のある識別情報は、雑音のある小量の識別情報のみを各暗号化鍵が含むように多数の暗号化鍵にわたって分散される。複数の暗号化鍵のうちの個別の暗号化鍵それぞれの誤りの確率はよって、雑音のある情報全てを使用して単一の鍵を生成する場合よりもかなり低いことがあり得る。

【００７０】

冗長表現の選択が、暗号化データの容量のみならず、暗号化鍵及び関連付けられた復号鍵の正しくない鍵対の使用からの回復の確率にも影響を及ぼすことは上述から明らかである。

【００７１】

広い範囲の冗長表現を本発明と組合せて使用することが可能である。例えば、

１．複製ベースの表現

各群におけるデータの情報内容を複製する

２．分散、又は部分的な複製ベースの表現

各群のデータの情報内容の部分的な複製により、データの情報内容を群にわたって分散させる。

【００７２】

３．秘密共有ベースの表現

共有資源にわたって情報を分散させ、群にわたって共有資源を分散させる

４．誤り訂正符号の符号語ベースの表現

誤り訂正符号の符号語により、群全てが包含される表現を作成する。

【００７３】

冗長表現の上記タイプそれぞれを、個々に、又は組み合わせて使用して、雑音耐性表現を提供することが可能である。

【００７４】

本発明により、データの暗号化及び／又は復号のために使用される鍵情報に雑音がある場合、データに関する情報コンテンツを首尾良く回復する確率が向上する。複数の暗号化／復号鍵の少なくとも１つは、その他の暗号化／復号鍵において使用されない鍵情報を含む。その他の暗号化／復号鍵それぞれにおける誤りの確率はよって、単に、その他の暗号化／復号鍵が、前述の誤りを生じ得る鍵情報全てを含んでいる訳でないため、第１の鍵／第２の鍵の誤りの確率それぞれよりも低くなる。

【００７５】

多数の鍵を使用し、複数の暗号化／復号鍵に、第１／第２の鍵の情報内容を分散させる

ことにより、複数の暗号化／復号鍵のうちの個別の暗号化／復号鍵における誤りの確率を更に削減することが可能である。

【００７６】

更に、いくつかの群を備えた冗長表現を作成し、及び複数の暗号化鍵のうちの別々の暗号化鍵を備えた群を暗号化することにより、首尾良く行う確率は更に向上させることができる。

【００７７】

複製の場合、これは、データを複数の群で複製し、好ましくは、分離性を有する鍵情報を使用することによって形成される別々の暗号化鍵で暗号化することの直接の結果である。その結果、鍵毎の誤りの確率が低くなるのみならず、首尾良く行う確率が、追加された群毎に増加する。個々の群それぞれはデータを回復するだけでよいからである。

【００７８】

部分的な複製の場合、データの回復に必要な群の数が、合計群数よりも小さければ、同様な効果が存在する。よって、データを種々のやり方で回復し、それにより、更なる群毎に、首尾良く行う確率を増加させる。この場合、複製を伴う場合と対照的に、元のデータの一部のみを、更なる鍵毎に複製すればよく、それにより、重複手法よりも、サイズに対する使用鍵数の比がより効率的になるという更なる効果が生じる。

【００７９】

秘密共有手法は、元のメッセージを回復するためにはｋ個の共有資源のうちのｎ個で十分であるという点で、部分的な複製手法の第１の効果を共有する。更に、冗長表現から単一の共有資源を回復することが可能なハッカーは暗号化データについて何も分からないので、秘密共有手法は更なるセキュリティをもたらす。

【００８０】

冗長表現が誤り訂正符号の符号語を有する場合、暗号化／復号鍵対の誤りの確率の削減があてはまるが、更に、符号語は、前述の鍵誤りの場合に、歪曲されたデータへの対処を支援することが可能である。

【００８１】

符号語の間で群を分散させることは、この特定の場合に適切である。それぞれの符号語にわたってそれぞれの群に含まれる情報を（好ましくは均一に）分散させることにより、暗号化／復号鍵対誤りの符号語への影響が削減される。その結果、所定の最大数の暗号化／復号鍵対誤りに対処する必要がある冗長度の量を削減することが可能である。この特定の効果は複数の鍵の使用とも一致する。複数の鍵の使用は、それぞれの群におけるデータに関する情報内容の削減を可能にし、それにより、暗号化／復号鍵対誤りから生じる合計シンボル誤り数が削減される。

【００８２】

図３は、情報の部分的な複製により、分散を施す冗長表現の例を示す。この特定の表現は、３つの暗号化／復号鍵を伴い、単一の暗号化／復号鍵対の不一致が生じても首尾良く回復することを可能にする。

【００８３】

データ３００は、１、２、３で表す等しい大きさの３つの部分に区分される。その後、G_1、G_2及びG_3と呼ばれる３つの群が作成される。前述の群それぞれは、元のデータからの２つの別々の部分を含み、各群はその他の群とは異なる。その後、c_1、c_2及びc_3それぞれの形式の誤り訂正符号が各群に付加される。誤り検出符号は、単一のパリティ・シンボルから、より複雑な符号に及び得る。その後、各群は複数の暗号化鍵Ke_1、Ke_2及びKe_3のうちの１つによって暗号化される。

【００８４】

図３に表す例では、暗号化された群それぞれは、対応する復号鍵Kd_1、Kd_2、Kd_3’によってその後復号され、Kd_3’は、暗号化された第３の群G_3を正しく復号したであろう復号鍵kd_3と異なる。この差の結果、暗号化群G_3は復号中に歪曲される。

【００８５】

復号後、復号群における誤り検出符号が、復号後に得られたデータが有効であるか否かを確かめるために評価される。よって、復号群G_3における誤りを、誤り検出符号の強度に応じた統計的確信度で求めることが可能である。復号誤りが求められると、元のデータ３００は、正しく復号された残りの２つの群に記憶された情報内容を使用することによって回復することができる。

【００８６】

図３は、情報の複製を使用して冗長表現を簡単に生成することができる。更に、部分的な複製を使用することが可能であることを示す。部分的な複製が使用される場合、複数の暗号化／復号鍵毎に、復号する対象のデータ全体を複製することなく、再構成のためにｋ個の部分のうちのｎ個（ｎ＞２）を必要とする種々の表現を構成することができる。しかし、その結果、暗号化／復号鍵対の不一致の場合に、複数の群が、データを回復することを必要とする。

【００８７】

図４は、秘密共有を使用する更なる冗長表現を示す図である。ｋ個の秘密共有手法のうちのｎ個では、データがｋ個の共有資源に符号化される。元のデータを復号化するためには、ｋ個の共有資源のうちのｎ個が必要である（ｎ＞２）。そういうものとしての個々の共有資源はそれぞれ、元のメッセージに関する情報を何ら提供するものでない。

【００８８】

図４は、５つのうちの３つのラグランジュ補間多項式の手法を使用した単純な例を表す。冗長表現を生成するために、ｎ－１次多項式を選択する。ここで、Ｍは符号化する対象のデータである。

【００８９】

$F(x)=(ax^2+bx+M) \bmod p$であり、ここで、ｐは素数であり、ｐ＞ａ、ｐ＞ｂである。

【００９０】

図４中で使用する多項式は、

$F(x)=(8x^2+3x+9) \bmod 11$である。

【００９１】

次の５つの共有資源は、Ｆ（ｘ）の５つの値を算出することによって生成される。

【００９２】

$F(1)=S_1=9$
$F(2)=S_2=3$
$F(3)=S_3=2$
$F(4)=S_4=6$
$F(5)=S_5=4$

各共有資源はその後、複数の暗号化鍵（$K_1,\ldots,K_5$）の１つを使用することにより、暗号化される。５つの暗号化共有資源のうちの２つが、暗号化／復号鍵対の不一致によって失われたとする。S_2、S_3、S_4のみを再構成することが可能であるとすれば、以下の一次方程式の組を解く必要がある。

【００９３】

$a*2^2+b*2+M=3$
$a*3^2+b*3+M=2$
$a*4^2+b*4+M=6$

である。

【００９４】

この方程式の組を解けば、ａ＝８、ｂ＝３及びＭ＝９が得られる。いくつかの群を失うことが有り得る場合でも、元のメッセージを再構成することができる。更に、個々の共有資源は、暗号化データに関する情報を何ら供給しない。

【００９５】

本発明の好ましい実施例では、上記秘密共有手法を誤り検出符号（好ましくは、元のデ

ータに、共有資源を作成する前に付加される誤り検出符号）と組み合わせる。よって、符号化メッセージの復号は、共有資源を復号する工程と、ｎ個の共有資源をその後選択する工程と、データを復号化する工程と、次いで、復号化データが正しいか否かを検証する工程とを含む。

【００９６】

図５は、誤り訂正符号からの符号語が冗長表現を形成する更に効果的な冗長表現である。図５中の冗長表現はリード・ソロモン符号を使用する。リード・ソロモン符号は、データ及びパリティを表すためのシンボルを使用する。この特定の例には、８ビットのシンボルを使用するＲＳ（２５５，２２３）が関係する。ＲＳ（２５５，２２３）の符号語は、原始多項式、この場合、

$$P(x) = 1 + x^2 + x^3 + x^4 + x^8$$

に基づく。

【００９７】

各符号語は、２５５バイト、２２３データ・バイト、及び３２パリティ・バイトを含む。ＲＳ（２５５，２２３）誤り訂正符号は、符号語毎に１６個のシンボル誤りが存在している状態で暗号化データの回復を可能にする。

【００９８】

正しくない暗号化／復号鍵対の使用により、前述の鍵で暗号化／復号された群におけるシンボル全てが歪曲されるので、誤り訂正符号のデータ・バイトの符号語は、単一の群におけるデータ・シンボルと一致しない。好ましい実施例では、各群は、できる限り多くの符号語で包含される。理想的には、符号語内の各シンボルは、別々の群に対応する。誤り耐性は、できる限り多くの符号語にわたり、群のシンボルを分散させることによって向上する。

【００９９】

図５は、m_0乃至m_{891}と番号を付した８９２個のデータ・バイトを４つの符号語にわたって分散させることがどのようにして可能であるかを示す。４つの符号語は垂直に示し、各符号語は２５５個のシンボルを含み、符号語の各シンボルは、２５５個の群のうちの１つの一部である。同様に、各群は４つのシンボルを含み、各符号語に１つのシンボルがある。

【０１００】

２５５個の群は、G_0乃至G_{222}に及ぶデータを含む２２３個の群、及びG_{222}乃至G_{255}に及ぶパリティ・シンボルを含む３２個の群を含む。データもパリティも、群はそれぞれ、K_0乃至K_{255}の２５５個の暗号化鍵のうちの１つを使用することによって暗号化される。

【０１０１】

正しくない暗号化／復号鍵対が使用された場合、前述の特定の鍵で暗号化／復号されたシンボルは全て、歪曲される。これは、図５中で、G_3上の×印で示す。よって、４つの符号語はそれぞれ、正しくない単一のシンボルのみを含む。よって、この特定の冗長な表現は、１６個の暗号化／復号鍵対の不一致を補正することができる。

【０１０２】

図５に示す冗長な表現では、正しくない暗号化／復号鍵は全て、同じ位置における４つの符号語全てに影響を及ぼす。これは、符号語の、群間での分散の直接的な結果である。どのシンボルが群に属するかにかかわらず、群内のシンボルは全て、正しくない暗号化／復号鍵対の結果として歪曲される。どの群に障害が生じたかが分かると、どのシンボルが正しくないかが分かる。

【０１０３】

特定の誤り訂正符号は、既知のシンボル誤りを効率的に処理することに長けている。誤りの場所が与えられれば、上記ＲＳ（２５５，２２３）は、１６個の未知のシンボル誤りではなく、３２個の既知のシンボル誤りを処理することができる。この場合、どの群が歪曲されたかが分かることが重要である。

【０１０４】
既知の誤りの識別をサポートする誤り訂正符号に関係する本発明の好ましい実施例では、各群は、群の完全性を確かめるためのチェックサムを含む。よって、群の完全性の表示を使用して、前述の誤りを警告することができる。
【０１０５】
明らかに、冗長データ表現の上記例は、本発明とともに使用するために利用可能な冗長表現が豊富であることを示す。更に、鍵の数の増加につれ、正しくない暗号化／復号鍵の使用から生じる障害の確率を削減することが可能であることを前述の例は示す。
【０１０６】
本発明の特定の効果的な実施例では、誤り訂正符号を使用した冗長表現をＩＢＥ手法と組み合わせる。本発明によるＩＢＥシナリオを考察する。アリスが暗号化メッセージをボブに送信する。メッセージは、ボブのバイオメトリック識別情報の第１のインスタンス、ボブの名前及び誕生日に基づいた複数の暗号化鍵を使用してアリスによって暗号化される。アリスによって暗号化されたメッセージを復号するために、ボブは、自分のバイオメトリック識別情報の第２のインスタンス、ボブの名前及び誕生日に基づいて複数の復号鍵を得る。ボブの識別情報の第１のインスタンス及び第２のインスタンスは何れも、自分の識別情報の推定ともみすことができる。ＩＢＥ手法を使用するために、アリス及びボブは、普通のＩＢＥを収容することが可能な公開鍵などの公開値の組を有するＴＡを使用する。この実施例における定義
ｖは、固定の一意の識別情報であり、ここで、名前及び誕生日の連結は、名前｜｜誕生日である。
【０１０７】
L_wは、バイオメトリック識別情報の、シンボル単位での長さである。
【０１０８】
Ｚは、シンボルが属するアルファベットであり、
ｗはボブのバイオメトリック識別情報の第１のインスタンスであり、$w \in Z^{L_W}$であり、
ｗ’は、ボブのバイオメトリック識別情報の第２のインスタンスであり、$w' \in Z^{L_W}$であり、$w \neq w'$である。
【０１０９】
アリスがメッセージをボブにセキュアに送出するためには、アリス及びボブは、暗号化鍵及び復号鍵それぞれを得なければならない。暗号化鍵を生成するために、ＴＡには、ボブにより、ｖ及びｗ’が与えられる。ＴＡは、ｖ及びｗ’がともにボブに属することを検証する。ｖ及びｗ’を使用して、ＴＡは、L_w個の復号鍵の組（ボブのバイオメトリック識別情報の第２のインスタンスのシンボル毎に１つの復号鍵$D_v||_i||_{w'}$）を生成する。ここで、w'_iはボブのバイオメトリック識別情報の第２のインスタンスのｉ番目のシンボルである。アリスは同様に、ｖ及びｗを使用して、L_w個の暗号化鍵の組（ボブのバイオメトリック識別情報の第１のインスタンスのシンボル毎に１つの暗号化鍵$E_v||_i||_{w_i}$）を生成する。ここで、w_iはボブのバイオメトリック識別情報の第１のインスタンスのｉ番目の要素である。
【０１１０】
アリスは次いで、ボブに伝達したいメッセージＭを暗号化する。まず、メッセージＭは冗長表現に符号化される。アリスは、ｗとｗ’との間の許容可能な最大差を選択する。この差異は最大d_Δ個の要素である。その後、アリスは、長さ$n = L_w$の系列におけるd_Δ個の誤りを補正することができる適切な誤り訂正符号Ｃ（ｎ；ｋ；d_Δ）を選択する。
【０１１１】
アリスはメッセージＭを行M_rに配置する。各行は長さｋを有する。アリスは各行を独立して符号化し、符号化行Mr^Eが生成される。
【０１１２】
符号化処理の結果、各符号化行は、符号化後、$n = L_w$個の要素を有する。アリスは次

いで、生成された暗号化鍵を使用することにより、暗号化メッセージの各列を暗号化し、その結果、L_w個の暗号化列を含む暗号化メッセージ（$E_{v||i||w_i}, M_C^E$）が生じる。暗号化メッセージはボブに送出される。

【０１１３】

ボブは、暗号化列を含む暗号化メッセージを受信し、関連付けられた復号鍵$D_{v||i||w_i}$を使用することにより、各列ｉを復号する。ｗ＝ｗ’の場合、列は全て、正しく復号される。ｗ≠ｗ’の場合、１つ又は複数の列が復号中に歪曲される。歪曲されたデータを補償するために、ボブは、誤り訂正符号を使用することにより、各行を復号化する。メッセージを回復するために、ボブは、データを符号化するためにどの誤り訂正符号を使用したかを知らなければならず、そうするために、アリスは適切なパラメータをボブに与えることが可能である。あるいは、誤り訂正符号は標準化することが可能である。

【０１１４】

上記処理では、誤って復号された要素を含み得るｎ個の要素の行は誤り訂正符号の符号語にマッピングされる。ｗ’に対するｗにおける誤りの数が十分少ない場合（すなわち、d_Δよりも少ない場合）、誤り符号はＭを正しく復号化することができる。よって、ボブは、行からメッセージＭを首尾良く回復することが可能である。

【０１１５】

本発明は概括的に、雑音のあるデータに基づいた鍵を参照して説明してきたが、雑音のない鍵マテリアルを使用するが、雑音のある伝送チャネルなどの他の影響により、十分な暗号化／復号鍵対が正しくないという確率がかなりある限り、劣悪な品質の記憶装置又は劣悪な品質のデータ担体が得られるシナリオにおいて適用すると同様の利点を得ることが可能である。本発明は、例えば、物理的にクローン可能でない関数からの応答などの、バイオメトリック以外のソースからの雑音のある鍵マテリアルを伴う場合に容易に適用することも可能である。

【０１１６】

前述の実施例は本発明を限定するよりも例証するものであり、本特許請求の範囲記載の範囲から逸脱しない限り、当業者は多くの別の実施例を設計することができる。

【０１１７】

特許請求の範囲では、括弧内にある参照符号は何れも、請求項を限定するものと解されるべきでない。「ｃｏｍｐｒｉｓｅ」の語、及びその活用を使用していることは、請求項記載のもの以外の構成要素又は構成工程が存在することを排除するものでない。構成要素に先行する冠詞「ａ」又は「ａｎ」を使用していることは、前述の複数の構成要素が存在していることを排除するものでない。

【０１１８】

本発明は、別個のいくつかの構成要素を備えたハードウェアにより、かつ、適切にプログラムされたコンピュータによって実現することが可能である。いくつかの手段を列挙した装置クレームでは、それらの手段のいくつかを同一のハードウェアによって実現することが可能である。単に特定の方策が相互に別々の従属請求項に記載されていることは、前述の方策の組合せを使用して効果を得ることが可能でないことを示すものでない。

【図面の簡単な説明】

【０１１９】

【図１】本発明による、データの暗号化、及びその後の復号を示す概略図である。

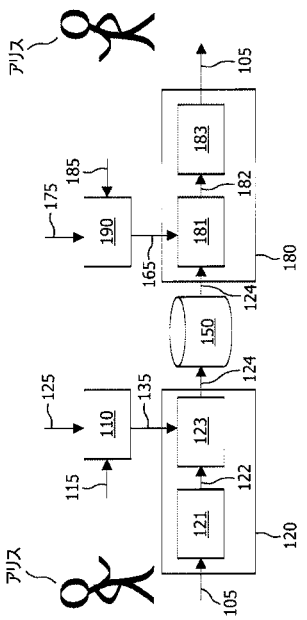
【図２】本発明による識別ベースの暗号化及び復号のシナリオを示す概略図である。

【図３】本発明による方法において使用するためのデータの第１の冗長表現を示す図である。

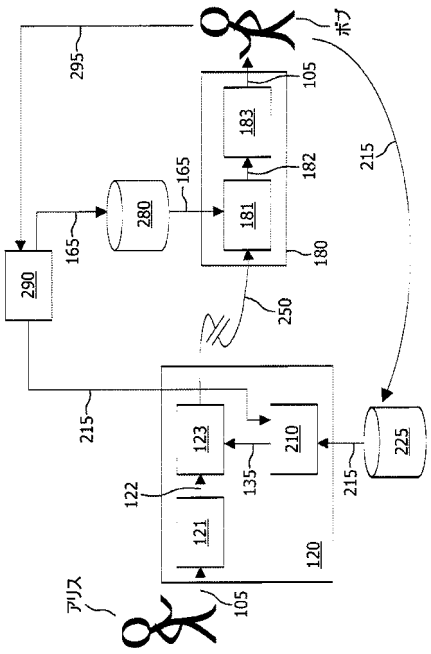
【図４】本発明による方法において使用するためのデータの第２の冗長表現を示す図である。

【図５】本発明による方法において使用するためのデータの第３の冗長表現を示す図である。

【図１】



【図２】



【図３】

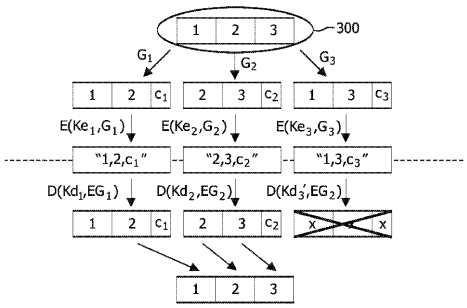


FIG. 3

【図４】

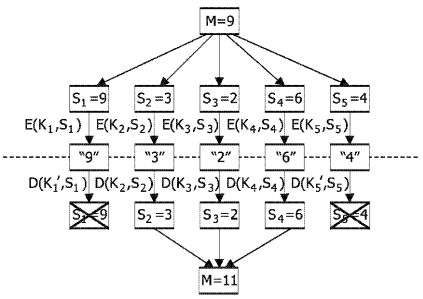


FIG. 4

【図５】

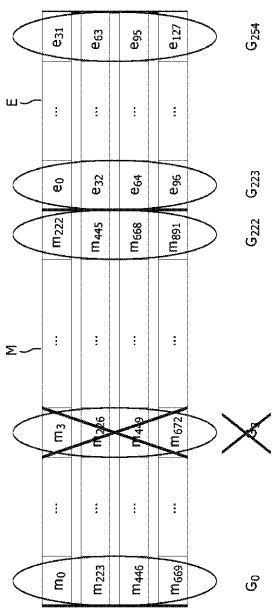


FIG. 5

フロントページの続き

(72)発明者 スコーリク，ボリス
オランダ国，５６５６ アーエー アインドーフェン，ハイ・テク・キャンパス ４４
(72)発明者 タイルス，ピム テー
オランダ国，５６５６ アーエー アインドーフェン，ハイ・テク・キャンパス ４４

審査官 青木 重徳

(56)参考文献 特開２００６－１２１３４２（ＪＰ，Ａ）
特開２００３－０３２３８２（ＪＰ，Ａ）
特開２００２－０７７１３５（ＪＰ，Ａ）
国際公開第２００５／０２５１２２（WO，Ａ１）
米国特許第０６３６３４８５（ＵＳ，Ｂ１）
米国特許出願公開第２００６／００７２７６３（ＵＳ，Ａ１）
笠原正雄，“代数誤り訂正符号とランダム符号化に基づく拡大体上の公開鍵暗号”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会［オンライン］，２００４年１１月 １日，Ｖｏｌ．１０４，Ｎｏ．４２３，ｐ．２１－２６，［平成２４年 ９月２６日検索］，インターネット，ＵＲＬ，<http://ci.nii.ac.jp/els/110003204397.pdf?id=ART0003631922&type=pdf&lang=jp&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1348710557&cp=>
Amit Sahai, Brent Waters, “Fuzzy Identity-Based Encryption”, Cryptology ePrint Archive: Report 2004/086, [online], ２００５年 3月 3日, Version: 20050303:192404, p.1-15, [retrieved on 2012-09-26]. Retrieved from the Internet, ＵＲＬ, <http://eprint.iacr.org/2004/086.pdf>
Yeveniy Dodis, Leonid Reyzin, and Adam Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”, LNCS, Advances in Cryptology - EUROCRYPT 2004, ２００４年 5月, Vol.3027, pp.523-540

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）