(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3592118号
(P3592118)
(45)発行日　平成16年11月24日(2004.11.24)　(24)登録日　平成16年9月3日(2004.9.3)

(51)Int.Cl.[7]		F I		
G09C	1/00	G09C	1/00	620Z
H04L	9/30	H04L	9/00	663Z

請求項の数 8　(全 15 頁)

(21)出願番号　特願平11-14866
(22)出願日　平成11年1月22日(1999.1.22)
(65)公開番号　特開2000-214772(P2000-214772A)
(43)公開日　平成12年8月4日(2000.8.4)
審査請求日　平成12年7月21日(2000.7.21)

(73)特許権者　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(73)特許権者　597008636
笠原　正雄
大阪府箕面市粟生外院４丁目１５番３号
(74)代理人　100078868
弁理士　河野　登夫
(72)発明者　笠原　正雄
大阪府箕面市粟生外院４丁目１５番３号
(72)発明者　村上　恭通
京都府京都市伏見区竹田向代町１３６番地
村田機械株式会社　本社工場内

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】暗号化装置，暗号通信方法，暗号通信システム及び記録媒体

(57)【特許請求の範囲】

【請求項１】

平文から積和型の暗号文を作成する暗号化装置において、ビット数の分布を設定する手段と、設定したビット数の分布に従って、その各成分のビット数が不均一である平文ベクトルに前記平文を分割する手段と、分割した平文ベクトルと公開鍵ベクトルとを用いて前記暗号文を作成する暗号文作成手段とを備えることを特徴とする暗号化装置。

【請求項２】

前記暗号文作成手段は、前記平文ベクトルにおける各成分のビット数を表す情報を組み込んで前記暗号文を作成するようにしたことを特徴とする請求項１記載の暗号化装置。

【請求項３】

各成分のビット数を表す情報を、該各成分に付加するようにしたことを特徴とする請求項２記載の暗号化装置。

【請求項４】

各成分のビット数を表す情報を、平文ベクトルの先頭の成分として設定するようにしたことを特徴とする請求項２記載の暗号化装置。

【請求項５】

前記分割した平文ベクトルの成分に、前記平文とは無関係なダミーデータを付加するようにしたことを特徴とする請求項１乃至４のいずれかに記載の暗号化装置。

【請求項６】

一方のエンティティ装置が平文を分割した平文ベクトルと公開鍵ベクトルとを用いて積和

型の暗号文を作成して他方のエンティティ装置へ送信し、該他方のエンティティ装置が送信された暗号文を元の平文に復号することにより、エンティティ装置間で情報の通信を行う暗号通信方法において、前記平文ベクトルにおける各成分のビット数が不均一であり、前記一方のエンティティ装置にて、前記平文ベクトルにおける不均一な各成分のビット数を設定することを特徴とする暗号通信方法。

【請求項７】

平文を分割した平文ベクトルを利用して前記平文を積和型の暗号文に暗号化する暗号化処理、及び、前記暗号文を元の平文に復号する復号処理を、複数のエンティティ装置間で相互に行う暗号通信システムにおいて、前記平文ベクトルにおける各成分のビット数を設定する手段と、設定された各成分のビット数に従って前記平文を平文ベクトルに分割する手段と、分割した平文ベクトルと公開鍵ベクトルとを用いて前記暗号文を作成する手段とを、送信側のエンティティ装置に備えたことを特徴とする暗号通信システム。

【請求項８】

コンピュータを請求項１記載の暗号化装置として機能させるためのコンピュータプログラムを記録してあることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、平文を積和型の暗号文に変換するための暗号化装置、この暗号化装置の手法を利用した暗号通信方法及び暗号通信システム、並びにこの暗号化装置の手法を実施するためのプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】
このような公開鍵暗号系の１つの方式として、積和型暗号方式が知られている。これは、送信者側で平文をＫ分割した平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）と公開鍵である基数ベクトルｃ＝（c_0，c_1，…，c_{K-1}）とを用いて暗号文Ｃ＝$m_0 c_0 + m_1 c_1 + \cdots + m_{K-1} c_{K-1}$を作成し、その暗号文Ｃを受信者側で秘密鍵を用いて平文ベクトルｍに復号して元の平文を得る暗号化形式である。この積和型暗号方式では、通信効率を高めるために、平文ベクトルｍの各成分におけるビット数の分布は一定としている。

【０００７】
【発明が解決しようとする課題】
従来の積和型暗号方式では、平文ベクトルｍの各成分のビット数分布が一定であるので、Ａ．Ｋ．Ｌｅｎｓｔｒａ，　Ｈ．Ｗ．Ｌｅｎｓｔｒａ，　Ｌ．Ｌｏｖａｓｚが提案した数学的なＬＬＬ法によって、公開されている基数ベクトルｃ＝（c_0，c_1，…，c_{K-1}）から平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）が解読されてしまうという問題がある。

【０００８】
本発明は斯かる事情に鑑みてなされたものであり、平文ベクトルの各成分のビット数分布を不均一とすることにより、ＬＬＬ法に対して強い積和型の暗号文を作成する暗号化装置と、この暗号化装置の手法を利用した暗号通信方法及び暗号通信システムと、この暗号化装置の手法を実施するためのプログラムを記録した記録媒体とを提供することを目的とする。

【０００９】
【課題を解決するための手段】
請求項１に係る暗号化装置は、平文から積和型の暗号文を作成する暗号化装置において、ビット数の分布を設定する手段と、設定したビット数の分布に従って、その各成分のビット数が不均一である平文ベクトルに前記平文を分割する手段と、分割した平文ベクトルと公開鍵ベクトルとを用いて前記暗号文を作成する暗号文作成手段とを備えることを特徴とする。
請求項２に係る暗号化装置は、請求項１において、前記暗号文作成手段は、前記平文ベクトルにおける各成分のビット数を表す情報を組み込んで前記暗号文を作成するようにしたことを特徴とする。
請求項３に係る暗号化装置は、請求項２において、各成分のビット数を表す情報を、該各成分に付加するようにしたことを特徴とする。
請求項４に係る暗号化装置は、請求項２において、各成分のビット数を表す情報を、平文ベクトルの先頭の成分として設定するようにしたことを特徴とする。
請求項５に係る暗号化装置は、請求項１乃至４のいずれかにおいて、前記分割した平文ベクトルの成分に、前記平文とは無関係なダミーデータを付加するようにしたことを特徴とする。

【００１０】
請求項６に係る暗号通信方法は、一方のエンティティ装置が平文を分割した平文ベクトルと公開鍵ベクトルとを用いて積和型の暗号文を作成して他方のエンティティ装置へ送信し、該他方のエンティティ装置が送信された暗号文を元の平文に復号することにより、エンティティ装置間で情報の通信を行う暗号通信方法において、前記平文ベクトルにおける各成分のビット数が不均一であり、前記一方のエンティティ装置にて、前記平文ベクトルにおける不均一な各成分のビット数を設定することを特徴とする。

【００１１】
請求項７に係る暗号通信システムは、平文を分割した平文ベクトルを利用して前記平文を積和型の暗号文に暗号化する暗号化処理、及び、前記暗号文を元の平文に復号する復号処理を、複数のエンティティ装置間で相互に行う暗号通信システムにおいて、前記平文ベクトルにおける各成分のビット数を設定する手段と、設定された各成分のビット数に従って

前記平文を平文ベクトルに分割する手段と、分割した平文ベクトルと公開鍵ベクトルとを用いて前記暗号文を作成する手段とを、送信側のエンティティ装置に備えたことを特徴とする。

請求項８に係る記録媒体は、コンピュータを請求項１記載の暗号化装置として機能させるためのコンピュータプログラムを記録してあることを特徴とする。

【００１２】

ＬＬＬ法は、$C=m_0 c_0 +m_1 c_1 +\cdots+m_{K-1} c_{K-1}$ の式において、Ｃ，c_0，c_1，・・・，c_{K-1} を既知数として、未知数m_0，m_1，・・・，m_{K-1} を求める数学的な手法であるが、この場合に未知数m_0，m_1，・・・，m_{K-1} のすべての大きさ（ビット数）が一定であることを前提としてこれらの未知数を求めている。よって、本発明のように未知数m_0，m_1，・・・，m_{K-1} の大きさ（ビット数）を不均一にしておけば、このＬＬＬ法は適応できず、平文ベクトルｍの成分m_0，m_1，…，m_{K-1} は解読できないことになり、ＬＬＬ法に対する強化を図れる。

【００１３】

このような平文ベクトルｍの各成分の大きさを不均一にする、言い換えると、平文ベクトルｍの各成分のビット数分布を不均一にする方式として、次のような２つの方式を本発明では開示する。

【００１４】

本発明の第１の方式（第１発明）では、この各成分の不均一なビット数分布を暗号通信システムの受信側で設定する。即ち、ビット数分布を公開情報として各エンティティに知らせておき、送信側のエンティティは、このビット数分布情報に従って平文を分割した平文ベクトルｍと暗号化鍵である公開鍵ベクトルｃとを用いて暗号文を作成し、受信側のエンティティは、このビット数分布情報に従い秘密の復号鍵を用いて暗号文を復号して元の平文ベクトルｍを求める。ここで、平文ベクトルｍの成分（m_0，m_1，…，m_{K-1}）の大きさ（ビット数）が一定でないので、ＬＬＬ法ではそれらの各成分を求めることができす、ＬＬＬ法に対して強化を図れる。また、公開されているビット数分布に応じた復号を行えるので、データ伝送効率に無駄がない。

【００１５】

本発明の第２の方式（第２発明）では、この各成分の不均一なビット数分布を暗号通信システムの送信側で設定する。即ち、送信側のエンティティは、自身で設定した所望のビット数分布に従って平文を分割した平文ベクトルｍと暗号化鍵である公開鍵ベクトルｃとを用いて暗号文を作成し、受信側のエンティティは、このビット数分布情報に従い秘密の復号鍵を用いて暗号文を復号して元の平文ベクトルｍを求める。なお、送信側で設定するビット数分布は公開されないので、送信側から受信側へその情報を伝送する必要があるが、例えば、その情報は暗号文に組み込ませた形で伝送することが可能である。このように、平文ベクトルｍの成分（m_0，m_1，…，m_{K-1}）の大きさ（ビット数）が一定でなく、しかも、そのビット数分布が公開されていないので、ＬＬＬ法に対して強いことは勿論であって、極めて安全性が高い。

【００１６】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、積和型暗号に基づく暗号通信システムの基本構成を示す模式図であり、図１の例では、一方のエンティティａが、平文ｘを暗号文Ｃに暗号化し、通信路を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂが、その暗号文Ｃを元の平文ｘに復号する場合を示している。

【００１７】

このような積和型暗号による暗号通信システムでは、送信側のエンティティａが、伝えるべき情報である平文ｘを以下のように複数（Ｋ個）の成分（m_0，m_1，…，m_{K-1}）からなる平文ベクトルｍに（１）のように分割する。なお、この各成分m_0，m

$_1$ ，…，m_{K-1} のビット数をそれぞれt_0 ，t_1 ，…，t_{K-1} とする。

平文ｘ→平文ベクトルｍ（m_0 ，m_1 ，…，m_{K-1} ） …（１）

【００１８】

そして、この平文ベクトルｍと公開されているＫ個の成分（c_0 ，c_1 ，…，c_{K-1} ）を有する公開鍵ベクトルｃとを用いて、暗号文Ｃを得る。この暗号文Ｃは、通信路を介して、送信側のエンティティａから受信側のエンティティｂへ伝送される。エンティティｂは、送られてきた暗号文Ｃを秘密の復号鍵を用いて復号して平文ベクトルｍを求めて、元の平文ｘを得る。

【００１９】

このような暗号通信システムにおいて、本発明では、平文ベクトルｍの各成分m_0 ，m_1 ，…，m_{K-1} の大きさを一定としていない。つまり、各成分m_0 ，m_1 ，…，m_{K-1} のビット数t_0 ，t_1 ，…，t_{K-1} が一定の数になっていない点に特徴がある。以下、その不均一のビット数分布を公開する方式（第１発明）とその不均一のビット数分布を公開しない方式（第２発明）とについて、具体的に説明する。

【００２０】

まず、平文ベクトルの各成分のビット数分布が予め設定されていて各エンティティに公開されている第１発明（第１実施の形態）について説明する。

【００２１】

〔第１実施の形態〕

図２は、第１発明による第１実施の形態での暗号通信システムの基本構成を示す模式図であり、図２の例では、図１と同様に、エンティティａを送信側、エンティティｂを受信側と設定している。また、エンティティａ，ｂ間には暗号文Ｃを伝送する通信路１０が設けられている。

【００２２】

送信側であるエンティティａには、予め設定されているビット数分布に基づいて、平文ｘを上記（１）のように平文ベクトルｍに分割する平文分割器１１と、この平文ベクトルｍと公開鍵ベクトルｃとを用いて後述するように暗号文Ｃを得る暗号化器１２とが備えられている。

【００２３】

一方、受信側であるエンティティｂには、予め設定されているビット数分布に基づいて、送られてきた暗号文Ｃを平文ベクトルｍに復号する復号器１３が備えられている。

【００２４】

このような第１実施の形態の暗号通信システムにおけるエンティティａ，ｂ間の情報の通信動作について説明する。この第１実施の形態では、平文ｘをＫ個の成分の平文ベクトルｍに分割する際の各成分m_0 ，m_1 ，…，m_{K-1} のビット数の分布（各成分m_0 ，m_1 ，…，m_{K-1} のそれぞれのビット数t_0 ，t_1 ，…，t_{K-1} がいくつであるか）の情報が、公開されていて各エンティティａ，ｂが知っている。

【００２５】

但し、この公開されている所定のビット数分布は一定ではない。つまり、平文ベクトルｍの各成分m_0 ，m_1 ，…，m_{K-1} のビット数t_0 ，t_1 ，…，t_{K-1} が一定ではない。この不均一のビット数分布のパターンとしては、例えば、最初の成分m_0 のみを６４ビット（t_0 ＝６４）として残りの（Ｋ－１）個の各成分m_1 ，…，m_{K-1} は３２ビット（t_1 ，…，t_{K-1} ＝３２）とする、最初と最後との成分m_0 ，m_{K-1} のみを３２ビット（t_0 ，t_{K-1} ＝３２）として残りの（Ｋ－２）個の各成分m_1 ，…，m_{K-2} は６４ビット（t_1 ，…，t_{K-2} ＝６４）とするなど、種々のパターンが可能である。

【００２６】

まず、送信側のエンティティａ側で、各成分のビット数を一定としない、公開されている所定のビット数分布に基づいて、平文分割器１１にて平文ｘがＫ個の成分の平文ベクトルｍに分割される。この結果、平文ベクトルｍの各成分m_0 ，m_1 ，…，m_{K-1} の

各ビット数t_0，t_1，…，t_{K-1}が一定にならない。

【００２７】

そして、暗号化器１２にて、このようにして分割した平文ベクトルｍと公開されているＫ個の成分（c_0，c_1，…，c_{K-1}）を有する公開鍵ベクトルｃとを用い、両ベクトルの内積を式（２）のように求めて暗号文Ｃが作成される。作成された暗号文Ｃは、通信路１０を介して受信側のエンティティｂへ伝送される。

$$C=m_0\ c_0+m_1\ c_1+\cdots+m_{K-1}\ c_{K-1} \quad \cdots(2)$$

【００２８】

通信路１０を伝送された暗号文Ｃは、受信側のエンティティｂの復号器１３へ入力される。そして、復号器１３にて、公開されている所定のビット数分布に基づき秘密の復号鍵を用いて、送られてきた暗号文Ｃが平文ベクトルｍに復号され、元の平文ｘが求められる。

【００２９】

第１実施の形態では、平文ベクトルｍの各成分の大きさ（ビット数）が一定ではないので、上記式（２）において公開鍵ベクトルｃの各成分c_0，c_1，…，c_{K-1}及び暗号文Ｃが既知であっても、ＬＬＬ法に従って平文ベクトルｍの各成分m_0，m_1，…，m_{K-1}を求めることは無理である。確かに、ＬＬＬ法により上記式（２）でのＫ個の成分からなる解を求めることは数学的に可能であるが、各成分の大きさ（ビット数）が一定であるということを前提として解を求めているので、得られるベクトルは元の平文ベクトルｍに一致しない。よって、第１実施の形態では、ＬＬＬ法に対して強化されており、従来に比して安全性が向上する。

【００３０】

また、この第１実施の形態では、予め所定のビット数分布が設定されているので、復号側のエンティティｂでは、そのビット数分布パターンにのみ対応できるようにしておけば良く、ビット数分布を不均一にしても、特別に複雑な復号処理が必要ではなく、従来と同様な復号処理で良い。また、従来と同様に、伝送されるすべてのビットを暗号文Ｃ用に用いることができるので、伝送効率が低下することはなく、従来と同様な高い伝送効率を維持できる。

【００３１】

次に、平文ベクトルの各成分のビット数分布を送信側で任意に設定して、そのビット数分布の情報を非公開とする第２発明（第２，第３実施の形態）について説明する。

【００３２】

図３は、第２発明による第２，第３実施の形態での暗号通信システムの基本構成を示す模式図であり、図３の例でも、図１と同様に、エンティティａを送信側、エンティティｂを受信側と設定している。また、エンティティａ，ｂ間には暗号文Ｃを伝送する通信路１０が設けられている。

【００３３】

第２，第３実施の形態では、送信側であるエンティティａには、平文ｘを平文ベクトルｍに分割する際の平文ベクトルｍの各成分のビット数を設定するビット数設定器２１と、設定したビット数に基づいて、平文ｘを平文ベクトルｍに分割する平文分割器２２と、この平文ベクトルｍと公開鍵ベクトルｃとを用いて後述するように暗号文Ｃを得る暗号化器２３とが備えられている。

【００３４】

一方、受信側であるエンティティｂには、暗号文Ｃと共に送られてきたビット数の情報を解析し、そのビット数に基づいて、送られてきた暗号文Ｃを平文ベクトルｍに復号する復号器２４が備えられている。

【００３５】

〔第２実施の形態〕

第２実施の形態の暗号通信システムにおけるエンティティａ，ｂ間の情報の通信動作について説明する。この第２実施の形態では、受信側のエンティティｂは、必要な復号鍵を生成すると共に、受信可能な平文のビット数e_0，e_1，…，e_{K-1}を公開する。

送信側のエンティティａは、一送信毎に、平文ｘをＫ個の成分の平文ベクトルｍに分割する際の各成分m_0，m_1，…，m_{K-1}のビット数t_0，t_1，…，t_{K-1}を任意に設定する。但し、$t_i+1 \leqq e_i$（ｉ＝０，１，…，Ｋ－１）とする。このビット数の情報は公開されず、後述するように暗号文Ｃに組み込んだ形で秘密裏にエンティティｂへ送られる。

【００３６】

このエンティティａが設定するビット数分布は一定ではない。つまり、平文ベクトルｍの各成分m_0，m_1，…，m_{K-1}のビット数t_0，t_1，…，t_{K-1}が一定ではない。この不均一のビット数分布のパターンとしては、例えば、任意のｉ番目（ｉ＝０，１，…，Ｋ－１）の成分m_iのみを６４ビット（$t_i=64$）として残りの（Ｋ－１）個の各成分は３２ビットとする、任意の複数個の成分を６４ビットとして残りの成分はすべて３２ビットとするなど、種々のパターンが可能である。

【００３７】

このように、平文ベクトルｍの各成分のビット数分布を送信側で任意に設定する場合、その設定パターンに応じて受信側の復号処理を変更する必要がある。そこで、このような複雑な復号処理に変更することを防ぐために、後述するように、ビット数を示すデータ及びダミーのデータを平文ベクトルｍの各成分に付け加えて各ブロックを構成し、ブロック毎のビット数を受信可能なビット数に調整して暗号文Ｃを作成するようにする。

【００３８】

まず、送信側のエンティティａ側で、各成分のビット数が一定でない１種のビット数分布をビット数設定器２１にて設定する。そして、設定した不均一のビット数分布に基づいて、平文分割器２２にて平文ｘがＫ個の成分の平文ベクトルｍに分割される。

【００３９】

次いで、暗号化器２３にて、以下のようにして暗号文Ｃが作成される。送りたい情報から、$(t_0+t_1+\cdots+t_{K-1})$ビット分を平文ｘとして取り出し、t_iビット毎（ｉ＝０，１，…，Ｋ－１）に分割したものをm_iとする。このようにＫ分割された平文ベクトルｍの１つの成分m_i（ｉ＝０，１，…，Ｋ－１）に対応する第ｉブロックにおいて、成分m_iの上位ビットにその成分m_iのビット数が分かるように“１”を付け加え、全体のビット長がe_iビットになるように、更にその上位ビットにダミーデータである“０”を必要なビット数だけ付け加えて、成分m_i'を構成する。この成分m_i'の構成例を図４に示す。そして、このようなＫ個の成分m_i'を有する変形平文ベクトルｍ′と公開鍵ベクトルｃとの内積を式（３）のように求めて暗号文Ｃを作成する。

Ｃ＝ベクトルｍ′・ベクトルｃ

$$=m_0'c_0+m_1'c_1+\cdots+m_{K-1}'c_{K-1} \quad \cdots(3)$$

但し、

変形平文ベクトルｍ′＝（m_0'，m_1'，…，m_{K-1}'）

成分m_i'のビット数をt_i'とした場合、$t_i'=t_i+1+$（付加するダミーデータのビット数）であり、$t_i'=e_i$を満たす。

【００４０】

このように作成された暗号文Ｃは、通信路１０を介して受信側のエンティティｂへ伝送される。

【００４１】

通信路１０を伝送された暗号文Ｃは、受信側のエンティティｂの復号器２４へ入力される。そして、復号器２４にて、復号鍵を用いて、送られてきた暗号文Ｃを変形平文ベクトルｍ′に復号し、更に逆変換を施して平文ベクトルｍを求めて、元の平文ｘを得る。

【００４２】

第２実施の形態でも、平文ベクトルｍの各成分の大きさ（ビット数）が一定ではないので、上記式（３）において公開鍵ベクトルｃの各成分c_0，c_1，…，c_{K-1}及び暗号文Ｃが既知であっても、ＬＬＬ法に従って平文ベクトルｍの各成分m_0，m_1，

…，m_{K-1} を求めることは無理である。また、第１実施の形態では、各ブロックのビット数を一定と考えて演算を行う改良ＬＬＬ法による攻撃が考えられるが、第２実施の形態では、このような改良ＬＬＬ法の攻撃を受けるような可能性はなく、ＬＬＬ法に対して極めて強い方式であり、従来に比して大幅に安全性が向上する。

【００４３】

第２実施の形態では、分割する平文の大きさを、受信可能な範囲において、送信側のエンティティが任意に設置することができる。しかしながら、ＬＬＬ法に対する安全性を高めるためには、設定ビット数は大きく偏っている必要がある。例えば、t_0 ，t_1 ，…，t_{K-1} の中の半数を６４ビット、残りの半数を３２ビットのように設定のガイドラインを定めておく場合には、弱い暗号文を送信してしまう危険性をなくすことができる。なお、第２実施の形態において攻撃者が平文のサイズを正確に推定できる確率は、$1/{}_KC_{K/2}$ であって極めて低い。更に、いくつかの成分m_i のデータをすべて“０”にして、全く情報を送らないブロックを設定した場合には、ＬＬＬ法に対してより強力な暗号文Ｃを作成できる。

【００４４】

また、第２実施の形態では、暗号文Ｃを作成するための変形平文ベクトルｍ′の各成分のビット数を復号側のエンティティｂでの受信可能な平文のビット数と同じに調整するので、復号側のエンティティｂではそのビット数にのみ対応できるようにしておけば良く、平文ベクトルの各成分のビット数分布を不均一にしても、特別に複雑な復号処理が必要ではなく、従来と同様な復号処理で良い。

【００４５】

第２実施の形態の具体的な数値例について説明する。送信すべき平文ｘは、ｘ＝［００１１１０１００１１１０１１０１０１１１０１０］の２４ビットとする。この場合の各パラメータの設定例を以下に示す。

$e=(9, 9, 9, 9)$

$t=(8, 4, 8, 4)$

ベクトルm＝ (00111010, 0111, 01101011, 1010)

ベクトルm′ ＝ (100111010, 000010111, 101101011, 000011010)

＝ (314, 23, 363, 26)　(10進表記)

【００４６】

〔第３実施の形態〕

第３実施の形態の暗号通信システムにおけるエンティティａ，ｂ間の情報の通信動作について説明する。この第３実施の形態では、受信側のエンティティｂは、必要な復号鍵を生成すると共に、受信可能な平文のビット数e_0 ，e_1 ，…，e_{K-1} を公開する。送信側のエンティティａは、一送信毎に、平文ｘを（Ｋ－１）個の成分の平文ベクトルｍに分割する際の各成分m_1 ，…，m_{K-1} のビット数t_1 ，…，t_{K-1} を任意に設定する。但し、$t_i \leqq e_i$ （ｉ＝１，…，Ｋ－１）とする。このビット数の情報は公開されず、後述するように暗号文Ｃに組み込んだ形で秘密裏にエンティティｂへ送られる。このエンティティａが設定するビット数分布は一定ではない。つまり、平文ベクトルｍの各成分m_1 ，…，m_{K-1} のビット数t_1 ，…，t_{K-1} が一定ではない。

【００４７】

まず、送信側のエンティティａ側で、各成分のビット数が一定でない１種のビット数分布をビット数設定器２１にて設定する。そして、設定した不均一のビット数分布に基づいて、平文分割器２２にて平文ｘが（Ｋ－１）個の成分の平文ベクトルｍに分割される。

【００４８】

次いで、暗号化器２３にて、以下のようにして暗号文Ｃが作成される。送りたい情報から

、（t_1 ＋…＋t_{K-1} ）ビット分を平文ｘとして取り出し、t_i ビット毎（ｉ＝１，…，Ｋ－１）に分割したものをm_i とする。また、これらのm_i の大きさ情報（t_1 ，…，t_{K-1} ）をm_0 に格納する。但し、e_0 はこれらの情報を送れるために十分大きな値に設定されているとする。そして、（Ｋ－１）個の成分m_i に成分m_0 を加えた変形平文ベクトルｍ″と公開鍵ベクトルｃとの内積を式（４）のように求めて暗号文Ｃを作成する。

$$C=\text{ベクトル}m'' \cdot \text{ベクトル}c$$
$$=m_0'' c_0+m_1'' c_1+\cdots+m_{K-1}'' c_{K-1} \quad \cdots(4)$$

但し、

$$\text{変形平文ベクトル}m''=(m_0, m_1, \cdots, m_{K-1})$$

【００４９】
このように作成された暗号文Ｃは、通信路１０を介して受信側のエンティティｂへ伝送される。
【００５０】
通信路１０を伝送された暗号文Ｃは、受信側のエンティティｂの復号器２４へ入力される。そして、復号器２４にて、復号鍵を用いて、送られてきた暗号文Ｃを変形平文ベクトルｍ″に復号し、復号したm_0 から各成分m_i の大きさ情報が得られるので、平文ベクトルｍを求めて、元の平文ｘを得ることができる。
【００５１】
第３実施の形態でも、第２実施の形態と同様に、ＬＬＬ法に対して極めて強い方式であり、従来に比して大幅に安全性が向上する。
【００５２】
第３実施の形態においても、例えば、t_0 ，t_1 ，…，t_{K-1} の中の半数を６４ビット、残りの半数を３２ビットのように設定するようにした場合、m_0 をＫビットの２進数で表現したとき、第（ｉ－１）ビットが“１”，“０”であると、それぞれm_i ブロックの大きさが６４ビット、３２ビットというように決めておくこともでき、e_0 を大きな値に設定する必要はない。
【００５３】
また、第３実施の形態では、暗号文Ｃを作成するための変形平文ベクトルｍ″の各成分のビット数を復号側のエンティティｂでの受信可能な平文のビット数と同じに調整するので、復号側のエンティティｂではそのビット数にのみ対応できるようにしておけば良く、平文ベクトルの各成分のビット数分布を不均一にしても、特別に複雑な復号処理が必要ではなく、従来と同様な復号処理で良い。
【００５４】
第３実施の形態の具体的な数値例について説明する。送信すべき平文ｘは、ｘ＝［００１１１０１００１１１０１１０１０１１１０１０］の２４ビットとする。この場合の各パラメータの設定例を以下に示す。

$$e=(4, 8, 8, 8, 8)$$
$$t=(4, 8, 4, 8, 4)$$
$$\text{ベクトル}m=(00111010, 0111, 01101011, 1010)$$
$$\text{ベクトル}m''=(0101, 00111010, 0111, 01101011, 1010)$$
$$=(5, 58, 7, 107, 10) \quad (10\text{進表記})$$

【００５５】
なお、平文ベクトルｍの各成分のビット数分布の情報を暗号文Ｃに組み込ませる２つの例（第２，第３実施の形態）について説明したが、他の例でも良いことは勿論である。

【００５６】
図５は、本発明の記録媒体の実施例の構成を示す図である。ここに例示するプログラムは、第１実施の形態に対応する場合、平文ｘを平文ベクトルｍに分割する処理及び平文ベクトルｍと公開鍵ベクトルｃとの内積計算により暗号文Ｃを作成する処理を含み、第２実施の形態に対応する場合、ビット数分布を設定する処理，平文ｘを平文ベクトルｍに分割する処理，変形平文ベクトルｍ′を構成する処理及び変形平文ベクトルｍ′と公開鍵ベクトルｃとの内積計算により暗号文Ｃを作成する処理を含み、第３実施の形態に対応する場合、ビット数分布を設定する処理，平文ｘを平文ベクトルｍに分割する処理，変形平文ベクトルｍ″を構成する処理及び変形平文ベクトルｍ″と公開鍵ベクトルｃとの内積計算により暗号文Ｃを作成する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、送信側のエンティティに設けられている。
【００５７】
図５において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、コンピュータ４０が暗号文Ｃを作成する。
【００５８】
コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、コンピュータ４０が暗号文Ｃを作成する。
【００５９】
コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピュータ４０を制御することにより、コンピュータ４０が暗号文Ｃを作成する。
【００６０】
次に、本発明を適用した積和型暗号方式の具体例について説明する。以下の実施例では、本発明の第１，第２及び第３実施の形態の何れもが適用可能である。
【００６１】
〔第１実施例〕
平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）を基数Ｂ＝（B_0，B_1，…，B_{K-1}）を用いて、下記式（５）に示すように、整数として表記することができる。なお、ここでは、m_i B_i ＜B_{i+1} が成立するものとする。
$M=m_0\ B_0+m_1\ B_1+\cdots+m_{K-1}\ B_{K-1}$　…（５）
【００６２】
式（５）において、$B_i=2^i$ である場合には平文が通常の２進数で表されていることになり、$B_i=10^i$ である場合には平文が通常の１０進数で表されていることになる。
【００６３】
ここで、上記B_i を下記式（６）のように設定する場合を考える。
$B_i=b_0\ b_1\ \cdots b_i$　…（６）
式（６）において、$b_0=1$，$b_i=2$（$1 \leqq i \leqq K-1$）と設定すると２進数の場合に一致し、$b_0=1$，$b_i=10$（$1 \leqq i \leqq K-1$）と設定すると１０進数の場合に一致する。
【００６４】
第１実施例では、このような多進法を用い、つまり、式（５）及び式（６）を利用して、暗号文Ｃを作成する。

【００６５】
秘密鍵と公開鍵とを以下のように準備する。
・秘密鍵：｛b_i｝，Ｐ，ｗ
・公開鍵：｛c_i｝
前記式（６）のように基数を与え、ｗ＜Ｐ（Ｐは大きな素数）を満たす整数ｗをランダムに選び、式（７）を導く。
$c_i \equiv wB_i \pmod{P}$ …（７）
公開鍵ベクトルｃは、式（８）のように与えられる。
$c=(c_0, c_1, \cdots, c_{K-1})$ …（８）
【００６６】
そして、送信側のエンティティで、平文を平文ベクトルｍに分割し、分割した平文ベクトルｍと公開鍵ベクトルｃとを利用して、暗号文Ｃを作成する。この際、平文ベクトルｍの第ｉ成分m_iがt_iビットとなるように平文を区切って送信する。但し、このt_iは式（９）の条件を満たす整数である。
【００６７】
【数１】

$$2^{t_i} \leqq b_{i+1} < 2^{t_i+1} \quad \cdots(9)$$

【００６８】
ここで、第１実施の形態（第１発明）では、この平文ベクトルｍの第ｉ成分m_iのビット数t_iも公開しておく。一方、第２，第３実施の形態（第２発明）では、この平文ベクトルｍの第ｉ成分m_iのビット数t_iは送信側で任意に設定し、そのビット数t_iの情報は暗号文Ｃに組み込んで受信側に秘密裏に送る。
【００６９】
受信側のエンティティでは、以下のようにして復号処理が行われる。
暗号文Ｃに対して、中間復号文Ｍを式（１０）のようにして求める。
$M \equiv w^{-1} C \pmod{P}$ …（１０）
この中間復号文Ｍは、具体的には式（１１）として与えられるので、以下の逐次復号アルゴリズムによって、整数Ｍから平文ベクトルｍ＝（m_0，m_1，…，m_{K-1}）を復号することができる。
$M = m_0 b_0 + m_1 b_0 b_1 + \cdots + m_{K-1} b_0 b_1 \cdots b_{K-1}$ …（１１）
【００７０】
（逐次復号アルゴリズム）
ステップ０
$M_0 = M / b_0$
$m_0 \equiv M_0 \pmod{b_1}$
ステップｉ（ｉ＝１～Ｋ－２）
$M_i = (M_{i-1} - m_{i-1}) / b_i$
$m_i \equiv M_i \pmod{b_{i+1}}$
ステップＫ－１
$m_{K-1} = (M_{K-2} - m_{K-2}) / b_{K-1}$
なお、このアルゴリズムにあっては、$m_j < b_{j+1}$でないと、m_jが一意に復号されない。
【００７１】
〔第２実施例〕

K個の整数を要素とする集合{d_i}を考える。なお、この集合の任意の2つの要素は互いに素である。そして、式（１２）に示すように、これらのK個の要素の積をdとし、基数D_iを式（１３）のように定義する。

$d = d_0 \quad d_1 \quad \cdots d_{K-1}$ …（１２）

$D_i = d / d_i$ …（１３）

【００７２】

そして、平文ベクトルm＝（m_0，m_1，…，m_{K-1}）を、基数D＝（D_0，D_1，…，D_{K-1}）を用いて、下記式（１４）に示すように表記する。

$M = m_0 \quad D_0 + m_1 \quad D_1 + \cdots + m_{K-1} \quad D_{K-1}$ …（１４）

但し、平文ベクトルmの各成分m_iは$m_i < d_i$を満たすように設定する。

【００７３】

第２実施例では、このようにして、つまり、式（１２）～式（１４）を利用して、暗号文Cを作成する。

【００７４】

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：{d_i}，P，w

・公開鍵：{c_i}

前記式（１３）のように基数を与える。この場合、基数ベクトル{D_i}は超増加数列ではなく、ＬＬＬ法攻撃に強い。また、w＜P（Pは大きな素数）を満たす整数wをランダムに選ぶ。また、平文ベクトルmの各成分m_iは$m_i < d_i$を満たすように設定する。整数wを用いてDの成分より、公開鍵ベクトルcを式（１５），（１６）のように導く。

$c_i \equiv w D_i \pmod{P}$ …（１５）

$c = (c_0, c_1, \cdots, c_{K-1})$ …（１６）

【００７５】

そして、送信側のエンティティで、平文を平文ベクトルmに分割し、分割した平文ベクトルmと公開鍵ベクトルcとを利用して、暗号文Cを作成する。この際、平文ベクトルmの第ｉ成分m_iがt_iビットとなるように平文を区切って送信する。但し、このt_iは式（１７）の条件を満たす整数である。

【００７６】

【数２】

$$2^{t_i} \leqq d_i < 2^{t_i+1} \quad \cdots(17)$$

【００７７】

ここで、第１実施の形態（第１発明）では、この平文ベクトルmの第ｉ成分m_iのビット数t_iも公開しておく。一方、第２，第３実施の形態（第２発明）では、この平文ベクトルmの第ｉ成分m_iのビット数t_iは送信側で任意に設定し、そのビット数t_iの情報は暗号文Cに組み込んで受信側に秘密裏に送る。

【００７８】

受信側のエンティティでは、以下のようにして復号処理が行われる。

最初に、暗号文Cに対して、中間復号文Mを式（１８）のようにして導く。

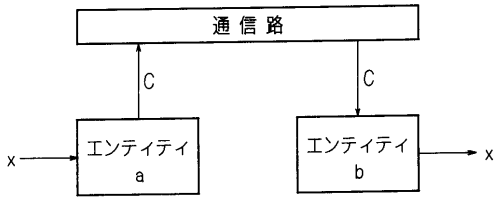
$M \equiv w^{-1} C \pmod{P}$ …（１８）

【００７９】

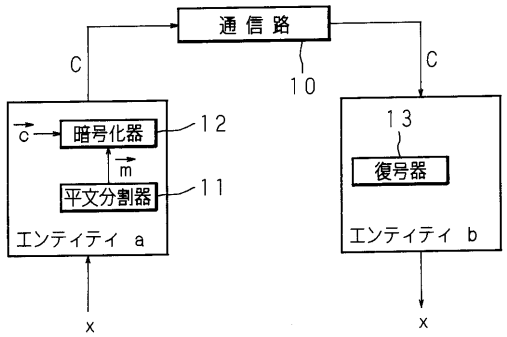
この中間復号文Mは、具体的には前記式（１４）として与えられるので、以下の並列復号アルゴリズムによって、整数Mからメッセージm＝（m_0，m_1，…，m_{K-1}）を復号することができる。

【００８０】
（並列復号アルゴリズム）
ｕｎｉｔ　　ｉ（m_i　の復号）
$m_i \equiv MD_i^{-1}$　（ｍｏｄ　d_i　）
【００８１】
なお、上述した実施例は、本発明を適用できる積和型暗号方式の一例を示しただけであり、すべての積和型暗号方式に本発明を適用できることは言うまでもない。
【００８２】
【発明の効果】
以上のように本発明では、積和型の暗号形式にあって、平文を分割した平文ベクトルの各成分の大きさ（ビット数）を不均一とするようにしたので、ＬＬＬ法による攻撃に対する安全性を向上することができる。
【図面の簡単な説明】
【図１】積和型暗号に基づく暗号通信システムの基本構成図である。
【図２】第１実施の形態（第１発明）での暗号通信システムの基本構成図である。
【図３】第２，３実施の形態（第２発明）での暗号通信システムの基本構成図である。
【図４】変形平文ベクトルｍ′の成分m_i　′のデータ構成を示す図である。
【図５】記録媒体の実施例の構成を示す図である。
【符号の説明】
１０　通信路
１１，２２　平文分割器
１２，２３　暗号化器
１３，２４　復号器
２１　ビット数設定器

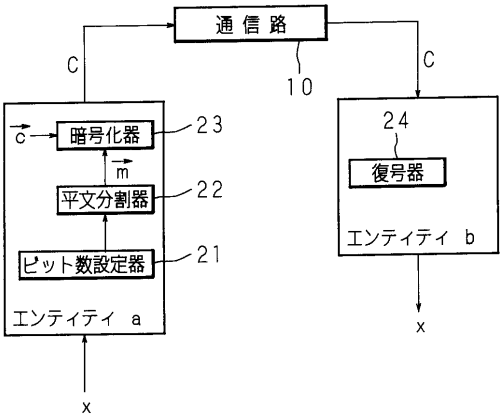
【図１】



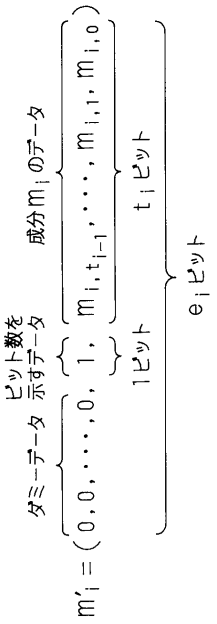
【図２】



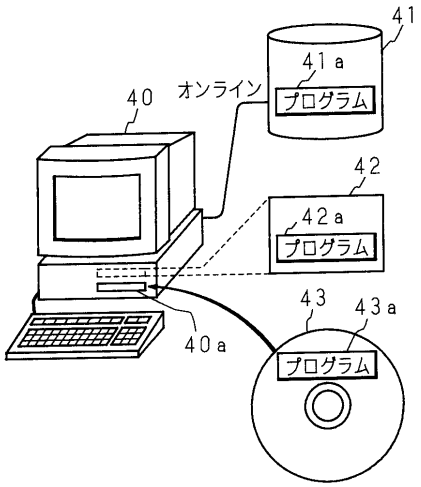
【図３】



【図４】


ダミーデータ
ビット数を示すデータ
成分m_iのデータ
$m'_i = (0,0,\cdots,0,\ 1,\ m_{i,t_{i-1}},\cdots,m_{i,1},m_{i,0})$
1ビット
t_iビット
e_iビット

【図５】


41
41a
プログラム
40
オンライン
42
42a
プログラム
43
43a
プログラム
40a

フロントページの続き

(56)参考文献 公開鍵暗号の二、三の方式, 電子情報通信学会技術研究報告, １９９８年 ９月１７日, Vol.98, No.268, p.33-49

(58)調査した分野(Int.Cl.[7], ＤＢ名)
G09C 1/00 620
H04L 9/30
JICSTファイル(JOIS)