明 細 書

暗号鍵共有方法

技術分野

本発明は、ネットワーク上のエンティティ間で暗号による通信を行うための暗号鍵を共有する方法に関する。

背景技術

近年、インターネット等のネットワーク上で通信を行う際に、通信データの機密保持等のために暗号文による通信技術が望まれている。

この種の通信技術としては、例えば公開鍵方式としてのＲＳＡが著名であるが、この他に、ネットワークに含まれるエンティティ同士で通信を行う際に、送信側のエンティティが通信データ（平文）を暗号鍵により暗号化して受信側のエンティティに送信し、それを受信側のエンティティが送信側の上記暗号鍵と共通の暗号鍵により元の通信データに復号する暗号鍵共有方法が一般に知られている。尚、ここで、エンティティとは、ネットワークに接続された端末機等の装置、その装置の使用者、その装置のソフトウェア、あるいはそれらの集合等、通信を行う主体を意味するものである。

そして、このような暗号鍵共有方法にあっては、例えばRolf Blom による論文「NON-PUBLIC KEY DISTRIBUTION ／Advances in Cryptology:Proceedings of CRYPTO '82／Plenum Press 1983, pp.231-236」、同じくRolf Blom による論文「An Optimal Class of Symmetric Key Generation Systems／Advances in Cryptology: EUROCRYPT '84 ／Springer LNCS 209, 1985, pp.335-338」、あるいは特公平５－４８９８０号公報もしくは米国特許第５０１６２７６号に見られる技術が知られている。

これらの技術では、ネットワーク上に設立されたセンターにおいて、あらかじめ各エンティティに固有で且つ公開性の識別子（名前、住所等）に、センターだけが秘密に保持するセンターアルゴリズムを施したものが、各エンティティに固

有の個人鍵として各エンティティに配付される。そして、エンティティ同士で通信を行う際には、それらの各エンティティは、互いに通信相手側のエンティティの識別子を自己が保持する個人鍵に作用させることで、エンティティ同士で共通の暗号鍵を生成し、その共通暗号鍵を用いて通信データの暗号化・復号化を行う。

より詳しくは、センターアルゴリズムは、これを例えば任意の二つの識別子を示す変数x，yの関数P（x，y）として表現したとき、P（x，y）＝P（y，x）なる対称性を有するように設定される。そして、この関数P（x，y）の変数x，yのうち、例えば変数yの値を各エンティティの実際の識別子iとした関数P（x，i）（以下、これをPi（x）と表現する）が各エンティティの個人鍵として各エンティティに配付される。その後、識別子iのエンティティが他の識別子jのエンティティと通信を行う場合には、識別子iのエンティティ側では、自己の個人鍵Pi（x）に相手側の識別子jを作用（変数xの値をjとする）させてなるPi（j）が暗号鍵として生成される。同様に、識別子jのエンティティ側では、自己の個人鍵Pj（x）に相手側の識別子iを作用させてなるPj（i）が暗号鍵として生成される。このとき、前記の対称性によって、Pi（j）＝Pj（i）となり、これにより、識別子i，jのエンティティ同士で共通の暗号鍵が得られることとなる。

このような暗号鍵共有方法によれば、各エンティティは、通信相手側の識別子を自己の個人鍵に作用させるだけで、センターの関与を伴うことなく他の任意のエンティティとの間での共通の暗号鍵を得ることができるので、ネットワークにおける暗号通信システムの簡素化を図ることができる。

ところで、このような暗号鍵共有方法では、前記センターアルゴリズムを容易に解読することができないことが暗号通信の機密性を確保する上で重要な課題となる。

しかるに、かかる暗号鍵共有方法では、上記のような利点を有する反面、各エンティティの個人鍵やこれから生成される暗号鍵、あるいはその暗号鍵により暗号化された通信データには、いずれも前記センターアルゴリズムに係わる情報が含まれ、しかも該センターアルゴリズムは各エンティティに対して共通であるため、例えば松本による論文「Performance of Linear Schemes for the Keypredi

stribution System ／IEICE Technical Report on Information Security, May 20, 1988, pp. 29-32」に示されているように、一般に複数のエンティティの結託等よる攻撃に対して弱いものとなり易い。

また、識別子としてエンティティの氏名を用いた場合、類似の氏名が多く現れやすいため、識別子の分散性が悪く（識別子の値の分布の偏りを生じやすい）、ひいてはこの識別子に前記センターアルゴリズムを施してなる各エンティティの個人鍵にも類似のものが多数現れ易い。このため、所謂、差分攻撃を受けやすいものとなっていた。

従って、前述のような暗号鍵共有方法では、種々の攻撃に対する安全性を高めることが望まれていた。

本発明はかかる背景に鑑み、通信に際しての共通の暗号鍵の生成やネットワーク上の暗号通信システムの簡素化を図りつつ、種々の攻撃に対する安全性を高めることができる暗号鍵共有方法を提供することを目的とする。

発明の開示

本発明の暗号鍵共有方法の第１の態様はかかる目的を達成するために、複数のエンティティとセンターとを含むネットワークにおいて、通信を行うエンティティ間で通信データの暗号・復号化を行うための共通の暗号鍵を両エンティティが所有する方法であって、あらかじめ前記センターは、各エンティティに固有で且つ公開性の識別子を、該センターのみが保持する各エンティティに共通で且つ少なくとも積分変換アルゴリズムを含むセンターアルゴリズムにより変換して各エンティティに固有の個人鍵を生成すると共にその個人鍵と前記積分変換アルゴリズムとを各エンティティに配付しておき、前記エンティティ同士が相互に通信を行うとき、互いに通信相手側の識別子に自己が保持する前記積分変換アルゴリズム及び前記個人鍵を作用させることにより該エンティティ同士が共通の暗号鍵を所有することを特徴とする。

かかる本発明の第１の態様によれば、前記各エンティティの個人鍵は、前記センターにおいて、各エンティティの識別子を、前記積分変換アルゴリズムを含むセンターアルゴリズムにより変換して生成されるので、各エンティティの識別子

自体の分散性が悪くても、該識別子に積分変換アルゴリズムが作用することで、その結果に得られるデータの分散性は高まる。従って、前記個人鍵の分散性が高まり、各エンティティ毎に類似性の乏しい個人鍵が前記センターにおいて生成され、これが前記積分変換アルゴリズムと共に各エンティティに配付される。そして、エンティティ同士の通信に際しては、各エンティティにおいて、通信相手側のエンティティの識別子に自己が保持する前記積分変換アルゴリズム及び個人鍵を作用させる。このとき、各エンティティの個人鍵には、前記積分変換アルゴリズムに基づく成分が含まれているので、通信相手側のエンティティの識別子に前記個人鍵だけでなく前記積分変換アルゴリズムをも作用させることで、前記センターアルゴリズムの積分変換アルゴリズムを除くアルゴリズム部分（この部分は前述の対称性を有するものとする）によって、通信を行うエンティティ同士で共通の暗号鍵が生成される。

このように本発明の第1の態様によれば、各エンティティの識別子を、積分変換アルゴリズムを含むセンターアルゴリズムにより変換することで、通信の際の共通の暗号鍵を生成するための各エンティティに固有の個人鍵を生成するので、その個人鍵の分散性が高まり、その結果、差分攻撃等に対する安全性が高まる。そして、通信に際しては、通信相手側の識別子のみを、自己が保持する積分変換アルゴリズム及び個人鍵に作用させるだけで、従来と同様にセンターの関与を伴うことなく通信相手のエンティティとの共通の暗号鍵を生成することができる。

よって、本発明の第1の態様によれば、通信に際しての共通の暗号鍵の生成やネットワーク上の暗号通信システムの簡素化を図りつつ、差分攻撃等の攻撃に対する安全性を高めることができ、ひいては、簡便で信頼性の高い暗号通信システムを提供できる。

尚、前記識別子は、各エンティティの氏名、住所等の他、ネットワーク上のメールアドレス、ドメイン名、あるいはそれらを組み合わせたもの等、各エンティティに対して固定的に用いられ、且つ少なくとも通信相手に対して公開性のあるものであればよい。

かかる本発明の第1の態様では、前記積分変換アルゴリズムとしては、フーリエ変換（高速フーリエ変換を含む）、ラプラス変換、ミラー変換、ヒルベルト変

換等が挙げられ、これらのいずれの積分変換を用いることも可能であるが、これらの積分変換は解析学的な無限区間上で定義されたものである。これに対して、本発明の第1の態様において積分変換アルゴリズムで変換する識別子は、有限区間上で表されるもの（例えば有限環上の剰余類）であるため、コンピュータ等を用いて識別子のデータを積分変換したとき、変換結果の異常分散（エイシアリング）が生じやすい。

そこで、本発明の第1の態様では、好ましくは前記積分変換アルゴリズムは重み関数付きの積分変換アルゴリズムを用いる。このように、識別子に積分変換を施すに際して、重み関数を付加することで、上記の異常分散を防止することができる。さらに、該重み関数は、異常分散を防止できるものであれば任意に設定することができるので、この重み関数を付加した積分変換アルゴリズムを含むセンターアルゴリズムにより識別子を変換して成る前記個人鍵には、該重み関数に基づく未知の成分が付加されることとなる。その結果、本発明の第1の態様を適用した暗号通信システムの安全性をさらに高めることができることとなる。

このように重み関数を付加する場合、該重み関数は、基本的には識別子のデータの区間の端側で、値が「0」に近づくように設定するのであるが、この場合、本発明の第1の態様では、さらに、該重み関数は前記センターにおいて生成された乱数データにより予想のつかないパターンに決定され、より好ましくは、該乱数データとして一回性の乱数データを用いる。ここで、前記乱数データによる重み関数の決定は、前記乱数データによって、識別子のデータの区間における重み関数の値の変化度合い（区間の端側で「0」に近づく形態）を決定することで行われる。また、一回性の乱数データとは、再現性がなく、もしくは再現性に極めて乏しい乱数データであり、さらに詳しくは乱数データを構成する各ビット数値の出現頻度がいずれの数値でも同等で、また乱数データの相関がないものであり、このような乱数データは、例えば人間がある語句もしくは文章をコンピュータに入力する際のタイミングに基づいて生成することが可能である。

このように重み関数を乱数データによって予想のつかないパターンに決定しておくことで、攻撃者にとっては、該重み関数を予測しづらくなり、本発明の第1の態様を適用した暗号通信システムの安全性を高めることができる。特に、一回

性の乱数データにより重み関数を決定したときには、該乱数データの再現性が排除されるので、さらにシステムの安全性が高まる。

前述の如く、前記積分変換アルゴリズムは、各種のものを適用できるが、特に、本発明の第1の態様では該積分変換アルゴリズムとしてフーリエ変換アルゴリズムを用いることが好ましい。すなわち、該フーリエ変換は、コンピュータを用いて迅速且つ容易に行うことができる積分変換であり、また、一般に変換結果のデータの分散化が生じやすい。従って、このようなフーリエ変換アルゴリズムを積分変換アルゴリズムとして用いることで、識別子から前記個人鍵を迅速且つ容易に生成することができるようになると同時に、個人鍵の分散性が効果的に高まって、暗号通信システムの安全性を顕著に高めることができる。

また、本発明の第1の態様では、前記センターは、前記識別子を前記センターアルゴリズムにより変換したものに、さらに各エンティティに固有で且つ各エンティティには不知の一回性の個別乱数データによりランダマイズ変換を施して前記個人鍵を生成すると共に、該個人鍵に含まれる前記ランダマイズ変換の成分を打ち消すためのアルゴリズムと前記積分変換アルゴリズムとからなる識別子変換アルゴリズムを該個人鍵と共に各エンティティに配付しておき、前記エンティティ同士が相互に通信を行うとき、互いに通信相手側の識別子に自己が保持する前記識別子変換アルゴリズム及び前記個人鍵を作用させることにより該エンティティ同士が共通の暗号鍵を所有する。

ここで、前記ランダマイズ変換は、前記識別子を前記センターアルゴリムにより変換したものを表すデータ列の各ビットの値を前記個別乱数データにより変更し、あるいは、該データ列を配置変換し、もしくは、それらを組み合わせて処理することで行われるものである。

これによれば、前記個人鍵には、前記センターアルゴリズムに加えて、前記ランダマイズ変換による成分が含まれることとなる。そして、このとき、該ランダマイズ変換は、その変換を各エンティティに固有で且つ各エンティティには不知の一回性の個別乱数データ（再現性がなく、もしくは再現性に極めて乏しい乱数データ）により行うため、各エンティティの個人鍵毎に、各別の偶然的な成分が含まれることとなる。その結果、暗号通信システムの種々の攻撃に対する安全性

をより一層強固なものとすることができる。

尚、この場合、通信に際して、相手側のエンティティの識別子に作用させる個人鍵には、各エンティティ毎に各別の前記ランダマイズ変換による成分が含まれている。このため、それを打ち消すためのアルゴリズムと前記積分変換アルゴリズムとからなる識別子変換アルゴリズムを前記個人鍵と共に各エンティティに配付しておき、通信に際しては、相手側のエンティティの識別子に該識別子変換アルゴリズム及び個人鍵を作用させることで、通信を行うエンティティ同士で共通の暗号鍵を生成することができる。

このようにランダマイズ変換を行う場合、該ランダマイズ変換は、例えば前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列を前記一回性の個別乱数データにより配置変換することにより行うことができる。

さらに好ましくは、前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列は複数の不要ビットを含み、前記ランダマイズ変換は、該不要ビットの値を前記一回性の個別乱数データによりランダム化し、さらに該不要ビットを含む前記データ列の全体を配置変換することにより行う。

このように各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列の不要ビットの値を前記一回性の個別乱数データによりランダム化し、さらに該不要ビットを含む前記データ列の全体を配置変換することで、攻撃者（暗号通信システムの解読者）にとっては、獲得したデータのどこに不要ビットに対応する部分があり、また、どこに必要なデータがあるかが判らなくなり、暗号通信システムの安全性が高まる。

また、前記ランダマイズ変換を行うための前記一回性の個別乱数データは、前記各エンティティの所定の処理に基づき生成し、より具体的には、前記所定の処理は前記各エンティティの人間による入力操作であり、その入力操作の時間的タイミングに基づき前記一回性の個別乱数データを生成する。

このように、各エンティティの人間による入力操作（例えばある文章や語句を入力する操作）の時間的タイミングに基づき乱数データを生成することで、その乱数データは、再現性がなく、もしくは再現性に極めて乏しいものとなり、前記

一回性の個別乱数データを的確に生成することができる。

次に、本発明の第２の態様は、複数のエンティティとセンターとを含むネットワークにおいて、通信を行うエンティティ間で通信データの暗号・復号化を行うための共通の暗号鍵を両エンティティが所有する方法であって、あらかじめ前記センターは、各エンティティに固有で且つ公開性の識別子を該センターのみが保持する各エンティティに共通のセンターアルゴリズムにより変換したものに、各エンティティに固有で且つ各エンティティには不知の一回性の個別乱数データによりランダマイズ変換を施して各エンティティに固有の個人鍵を生成すると共に、その個人鍵と、該個人鍵に含まれる前記ランダマイズ変換の成分を打ち消すアルゴリズムを含む識別子変換アルゴリズムとを各エンティティに配付しておき、前記エンティティ同士が相互に通信を行うとき、互いに通信相手側の識別子に自己が保持する前記識別子変換アルゴリズム及び個人鍵を作用させることにより該エンティティ同士が共通の暗号鍵を所有することを特徴とする。

かかる本発明の第２の態様によれば、前記各エンティティの個人鍵は、前記センターにおいて、各エンティティの識別子を前記センターアルゴリズム（これは前述の対称性を有する部分を含むものとする）により変換したものに、各エンティティに固有で且つ各エンティティには不知の一回性の個別乱数データ（再現性がなく、もしくは再現性に極めて乏しい乱数データ）に基づくランダマイズ変換を施して生成されるので、各エンティティの個人鍵毎に、各別の偶然的な成分が含まれることとなる。その結果、本発明の第２の態様を適用した暗号通信システムの種々の攻撃に対する安全性が高まる。この場合、前記第１の態様で説明した場合と同様に、各エンティティの個人鍵には、各エンティティ毎に各別の前記ランダマイズ変換による成分が含まれているため、それを打ち消すためのアルゴリズムを含む前記識別子変換アルゴリズムを前記個人鍵と共に各エンティティに配付しておく。そして、通信に際しては、相手側のエンティティの識別子に、前記識別子変換アルゴリズム及び個人鍵を作用させることで、前記センターの関与を伴うことなく通信を行うエンティティ同士で共通の暗号鍵を生成することができる。

よって、本発明の第２の態様によっても、通信に際しての共通の暗号鍵の生成

やネットワーク上の暗号通信システムの簡素化を図りつつ、種々の攻撃に対する安全性を高めることができ、ひいては、簡便で信頼性の高い暗号通信システムを提供できる。

かかる本発明の第２の態様では、前記第１の態様で説明した場合と同様に、前記ランダマイズ変換は、前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列を前記一回性の個別乱数データにより配置変換することにより行うことができる。そして、より好ましくは、前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列は複数の不要ビットを含み、前記ランダマイズ変換は、該不要ビットの値を前記一回性の個別乱数データによりランダム化し、さらに該不要ビットを含む前記データ列の全体を配置変換することにより行う。これにより、本発明の第２の態様を適用した暗号通信システムの安全性を高めることができる。

また、本発明の第２の態様では、前記第１の態様で説明した場合と同様に、前記一回性の個別乱数データは、前記各エンティティの所定の処理に基づき生成し、より具体的には、前記所定の処理は前記各エンティティの人間による入力操作であり、その入力操作の時間的タイミングに基づき前記一回性の個別乱数データを生成する。これにより、前記一回性の個別乱数データを的確に生成することができる。

図面の簡単な説明

図１は本発明の暗号鍵共有方法の一実施形態を適用した暗号通信システムの全体構成を示す図、図２は図１のシステムの基本構造を概念的に説明するための図、図３は図１のシステムにおける処理手順の概要を説明するためのフロー図、図４は図３の手順１における処理の詳細を示すフロー図、図５は図３の手順２における処理の詳細を示すフロー図、図６は図３の手順３及び手順４における処理の詳細を示すフロー図、図７は図３の手順３及び手順５における処理の詳細を示すフロー図、図８は図６及び図７の処理を行うためのコンピュータマシンの構成を示すブロック図である。

発明を実施するための最良の実施の形態

本発明の一実施形態を図1乃至図8を参照して説明する。まず、図1及び図2を参照して本実施形態の暗号鍵共有方法を適用した暗号通信システムの概要を説明する。

図1を参照して、本実施形態では暗号通信システムの基本的な構築主体であるセンター1と、その暗号通信システムに加入して相互に暗号通信を行う複数のエンティティ2とがインターネット、パソコン通信網等のネットワーク3を介して相互に通信可能とされている。これらのセンター1及び各エンティティ2は、図示を省略するが、実際の通信やデータ処理を行うためのパソコン等のコンピュータマシンや、該コンピュータマシンの使用者を包含している。

このようなネットワーク3上で構築された本システムでは、図2に示すように、センター1に加入した各エンティティ2（図2では各エンティティ2を参照符号i，j，…により示している）は、それぞれに対応した固有の識別子yi，yj，…（詳細は後述する）を有する。この場合、i≠jならば、yi≠yjである。そして、各エンティティ2（i，j，…）には、それぞれの識別子yi，yj，…（以下、必要に応じて識別子ynと総称する）に基づきセンター1により生成された各エンティティ2に固有の個人鍵Xi，Xj，…（詳細は後述する。以下、必要に応じて個人鍵Xnと総称する）があらかじめセンター1から与えられる。さらに、任意のエンティティi，j同士で暗号通信を行う際には、その通信データの暗号化（送信側）及び復号化（受信側）を行うための共通の暗号鍵Kijがそれぞれのエンティティi，j毎に各別に各エンティティi，jの個人鍵Xi，Xjを用いて生成され、その共通暗号鍵Kijを用いてエンティティi，j間での暗号通信が行われる。

ここで、本実施形態のシステムをさらに詳説する前に、前記識別子ynについて説明しておく。本実施形態では、各エンティティ2の識別子ynは、各エンティティ2の氏名、住所、メールアドレス、ドメイン名、あるいはこれらを組み合わせたもの等、各エンティティ2に固有のものであり、しかも、公開性のあるものを使用する。尚、センター1や各エンティティ2のコンピュータマシンにおける識別子ynの実際の取り扱い上では、各識別子ynは、それを例えば有限環上

の剰余類でコード化してなるベクトルデータとして扱われる。

上記のような暗号通信を行うための本実施形態のシステムを、以下に図3乃至図8を参照して詳説する。

図3を参照して、本実施形態のシステムでは、センター1による前記個人鍵Xn等の生成及び配付等の事前準備処理を経た後、個々のエンティティi，j間での暗号通信が行われる。

前記センター1による事前準備処理では、センター1はその設立時、あるいはシステムの更新時に、まず、各エンティティ2の前記個人鍵Xnを生成するための基本となるセンターアルゴリズムを生成する（手順1）。

このセンターアルゴリズムは、本実施形態ではセンター行列と、重み関数と；積分変換アルゴリズムとにより構成されている。

ここで、前記積分変換アルゴリズムは、各エンティティ2の識別子ynのデータを積分変換するためのアルゴリズムであり、本実施形態では、積分変換アルゴリズムとしてフーリエ変換（詳しくは高速フーリエ変換）を使用する。この種のフーリエ変換としては、複数種のものが知られており、そのうちの一種類をセンター1で選択して、本実施形態で使用するフーリエ変換アルゴリズムを生成する。尚、該フーリエ変換アルゴリズムは、実際上は、識別子ynのデータに作用させる行列として表現される。

また、重み関数は、有限区間のデータである識別子ynをフーリエ変換する際の異常分散（エイシアリング）を防止するためのものであり、識別子ynのデータの区間の端点側で値が「0」に近づくような関数である。さらに、センター行列は、対称行列であり、より詳しくは非特異な対称行列である。

この場合、前記重み関数及びセンター行列は、一回性の乱数データを用いて生成する。すなわち、図4を参照して、重み関数及びセンター行列を生成する際には、センター1はまず、センター1のコンピュータマシンにおけるオペレータの人為的操作に基づき乱数データを生成する（手順1－1）。具体的には、例えばオペレータがセンター1のコンピュータマシンに対して適当な語句や文章等を入力し、この際の入力タイミング（例えば各単語の入力時刻や各単語の入力の時間間隔）をコンピュータマシンで逐次計測する。そして、その計測した入力タイミ

ングに基づき乱数データを時系列で生成する。このようにして生成される乱数データは、あいまいさを有する人為的な入力操作のタイミングに基づいて生成されるため、事実上、再現性の無い偶然的なものとなり、これにより一回性の乱数データが生成される。

そして、このように一回性の乱数データを生成した後、センター1は、その生成した一回性の乱数データに基づき、前記重み関数とセンター行列とを決定する（手順1－2）。この場合、重み関数の決定は、上記の一回性乱数データによって、識別子yn のデータの区間における重み関数の値の変化度合い（区間の端側で「0」に近づく形態）を決定することで行われ、これにより該重み関数が予想のつかないパターンに決定される。尚、該重み関数は、実際上は、対角行列として表現される。また、センター行列の決定は、その対称性及び非特異性を確保しつつ該行列の成分の値を前記一回性の乱数データによって決定することで行われる。

以上のように生成されたセンター行列、重み関数及び積分変換アルゴリズムから成るセンターアルゴリズムは、センター1において秘密裏に保管され、特に、センター行列及び重み関数は、センター1の特定者以外の第三者（各エンティティ2等を含む）が参照することができないように厳重に保管される。尚、これらのセンターアルゴリズムは各エンティティ2に対して共通のものである。

図3に戻って、次に、センター1は、各エンティティ2（i，j……）がシステムに加入したとき、前述の如く生成されて保管されたセンターアルゴリズムや各エンティティ2の識別子yn 等を用いて、各エンティティ2に固有の個人鍵Xn と、これと合わせて後述の如く共通暗号鍵Kijを生成するための識別子変換アルゴリズムとを生成して各エンティティ2に配付する（手順2）。

さらに詳細には、図5を参照して、この手順2では、センター1は、エンティティ2の識別子ynのデータ（ベクトルデータ）に前記フーリエ変換アルゴリズム及び重み関数の行列を作用させることで、該識別子yn に重み付き高速フーリエ変換を施す（手順2－1）。さらに、この手順2－1により得られたベクトルデータに前記センター行列を乗算する（手順2－2）。この場合、前記識別子yn のデータに冗長性をもたせておくことで、手順2－2により得られるベクトル

データには、識別子yn のデータとして意味のあるビット列に前記重み関数、積分変換アルゴリズム及びセンタ行列を作用させてなる複数の有用ビットと、それ以外の複数の不要ビットとが現れる。

一方、センター1は、エンティティ2との通信（例えばエンティティ2の加入手続き等の際の通信）によって、該エンティティ2に固有で、しかもエンティティ2には判らないような一回性の個別乱数データを生成する（手順2－3）。具体的には、前述の如く重み関数等を決定する際に一回性の乱数データを生成した場合と同様に、エンティティ2のコンピュータマシン上で、その使用者にある語句もしくは文章を入力させ、それをセンター1側で逐次受信することで、該エンティティ2の人為的な入力操作のタイミングをセンター1のコンピュータマシンにより計測する。そして、その計測した入力操作のタイミングに基づいて前記個別乱数データを生成する。このようにして個別乱数データを生成することで、その個別乱数データは、重み関数等の生成時の乱数データと同様に、再現性のない偶然的なものとなると共に、エンティティ2に固有のものとなり、これにより一回性の個別乱数データが得られる。尚、エンティティ2は、どのような入力操作のタイミングでどのような乱数データが生成されるかは判らず、また、その人為的な入力操作のタイミングを正確にコントロールすることはできないので、前記個別乱数データをエンティティ2が知ることはできない。

次いで、センター1は、前記手順2－2で得られたベクトルデータのうちの前記不要ビットの各ビット値を手順2－3で得られた一回性の個別乱数データによってランダム化する（手順2－4）。さらに、そのランダム化した不要ビットと前記有用ビットとを合わせたベクトルデータを上記一回性の個別乱数データによって、ランダムに配置変換し（ベクトルデータの成分の配列を変更する。手順2－5）、これにより手順2－2で得られたベクトルデータ（識別子yn をセンターアルゴリズムにより変換したもの）をランダマイズ変換する。そして、このランダマイズ変換により得られたベクトルデータをエンティティ2の個人鍵Xn として生成する。尚、上記ランダマイズ変換は、実際上は行列（対称行列とは限らない）で表され、より詳しくは該行列の転置行列と逆行列とが等しくなるような行列で表される。

また、センター１は、前記一回性の個別乱数データと前記フーリエ変換アルゴリズム及び重み関数とから、前記識別子変換アルゴリズムを生成する（手順２－６）。この識別子変換アルゴリズムは、前記個人鍵Xn に反映されている前記ランダマイズ変換の成分を打ち消すためのアルゴリズム（これはランダマイズ変換を表す行列の逆行列により表される）と、前記フーリエ変換アルゴリズム及び重み関数とを合成（それぞれを表す行列同士を乗算）したものである。

このようにしてセンター１によって生成された各エンティティ２に対応する個人鍵Xn と識別子変換アルゴリムとが各エンティティ２に通信等により事前に配付される（図３の手順２を参照）。以上説明した内容がセンター１における事前準備処理の詳細である。

尚、センタ１は前述のように各エンティティ２の個人鍵Xn や識別子変換アルゴリズムを生成した後には、そのエンティティ２に対応する前記一回性の個別乱数データや前記ランダマイズ変換を表す行列は保管せずに消去する。また、自身の個人鍵Xn 及び識別子変換アルゴリムを受け取った各エンティティ２は、それらを自身のコンピュータマシンの適宜の記憶装置に秘密裏に保管する。

図３に戻って、前述のような事前準備処理が行われた後、任意のエンティティ２間で、次のように暗号通信が行われる。尚、ここでは、各エンティティ２のうち、エンティティｉ，ｊ（ｉ≠ｊ）間で、エンティティｉを送信側、エンティティｊを受信側として暗号通信を行うものとする。

この暗号通信では、送信側のエンティティｉは、まず、自身が保持する前記個人鍵Xi 及び識別子変換アルゴリズムと、受信側のエンティティｊの識別子ｙｊとからエンティティｊとの共通暗号鍵Kijを生成する（手順３）。

さらに詳細には、図６を参照して、まず、受信側のエンティティｊの識別子ｙｊに、送信側エンティティｉのコンピュータマシン上で該エンティティｉの識別子変換アルゴリズムを作用させる（識別子ｙｊのベクトルデータに識別子変換アルゴリズムの行列を乗算する。手順３－１）。次いで、この手順３－１により得られるベクトルデータと、送信側エンティティｉの個人鍵Xi （ベクトルデータ）との内積を演算することで、エンティティｊとの共通暗号鍵Kijを生成する（手順３－２）。

同様にして、受信側のエンティティｊは、図７に示すように自身のコンピュータマシン上で自身の識別子変換アルゴリズムを送信側のエンティティｉの識別子ｙｉに作用させ（手順３－１）、さらにその結果に得られるベクトルデータとエンティティｊの個人鍵Ｘｊとの内積を演算する（手順３－２）ことで、エンティティｉとの共通暗号鍵Ｋｊｉを生成する。

このとき、送信側エンティティｉで独自に生成される共通暗号鍵Ｋｉｊと受信側エンティティｊで独自に生成される共通暗号鍵Ｋｊｉとは同一となる。

すなわち、送信側及び受信側の各エンティティｉ，ｊが、それぞれ保持している個人鍵Ｘｉ，Ｘｊは、それぞれ、各エンティティｉ，ｊの識別子ｙｉ，ｙｊに、前述の重み関数付きのフーリエ変換アルゴリズム、センター行列及びランダマイズ変換を作用させてなるベクトルデータであり、また、各エンティティｉ，ｊがそれぞれ共通暗号鍵Ｋｉｊ，Ｋｊｉを生成するに際して、相手側のエンティティｊ，ｉの識別子ｙｊ，ｙｉに作用させる前記識別子変換アルゴリズムは、重み関数付きのフーリエ変換アルゴリズムと、各個人鍵Ｘｉ，Ｘｊに反映されている各エンティティｉ，ｊ毎のランダマイズ変換の成分を打ち消すアルゴリズムとを合成したものである。

このため、前記手順３－２で行う内積演算では、各エンティティｉ，ｊ毎のランダマイズ変換の影響が排除され、該内積演算の結果として得られる各共通暗号鍵Ｋｉｊ，Ｋｊｉは、各エンティティｉ，ｊの識別子ｙｉ，ｙｊに重み関数付きのフーリエ変換アルゴリズムを施したものに、さらにセンター行列を作用させたもの（ベクトルデータ）と、通信相手側のエンティティｊ，ｉの識別子ｙｊ，ｙｉに重み関数付きフーリエ変換アルゴリズムを施したもの（ベクトルデータ）との内積を演算してなる結果に等しい。すなわち、識別子ｙｉ，ｙｊに重み関数付きのフーリエ変換アルゴリズムを施してなるベクトルデータをそれぞれｙｉ′，ｙｊ′（但しｙｉ′，ｙｊ′は縦ベクトルとする）とおき、またセンター行列をＣとすると、Ｋｉｊ＝（ｙｊ′）^{T}・Ｃ・ｙｉ′、Ｋｊｉ＝（ｙｉ′）^{T}・Ｃ・ｙｊ′である（但し、式中の添え字Ｔは転置を意味する）。

そして、前述したようにセンター行列Ｃは対称行列であるから、明らかにＫｉｊ＝Ｋｊｉとなる。従って、各エンティティｉ，ｊでそれぞれ別個に生成される共通

暗号鍵Kij，Kjiは一致し、これにより両エンティティｉ，ｊが共通の暗号鍵を共有することができることとなる。

一方、図３の手順３において前述の如く受信側エンティティｊとの共通暗号鍵Kijを生成した送信側エンティティｉは、その共通暗号鍵Kijや受信側エンティティｊに送信しようとする平文（文章、プログラム等）等から暗号通信電文を生成する（手順４）。この場合、該暗号通信電文の生成に際しては、共通暗号鍵Kijの他、一回性の乱数データも使用する。

さらに詳細には、図６を参照して、暗号通信電文を生成するに際しては、前述したセンター１における事前準備処理の場合と同様にして、送信側エンティティｉは自身のコンピュータマシンにおいて語句や文章等の入力操作の時間的タイミングに基づき一回性の乱数データ（以下、暗号通信用乱数データという）を生成しておき（手順４－１）、この一回性の暗号通信用乱数データを、前記共通暗号鍵Kijを本来の鍵として暗号化する（手順４－２）。この場合、この暗号化は、例えば３段構成のＤＥＳ（Data Encryption Standard）により行われる。

また、手順４－１で生成した一回性の暗号通信用乱数データ（暗号化前のもの）を鍵として平文を暗号化する（手順４－３）。この暗号化は、例えば手順４－２と同様に３段構成のＤＥＳにより行う。

そして、手順４－２により得られた暗号化乱数データと手順４－３により得られた暗号文とを合わせる（１セットにする）ことで、受信側エンティティｊに送信すべき暗号通信電文が生成される。このようにして生成された暗号通信電文はエンティティｉのコンピュータマシンからエンティティｊのコンピュータマシンに送信される。

尚、前記暗号通信用乱数データは、暗号通信を行う都度、生成して更新することが好ましいが、暗号通信を数回行う毎に、該暗号通信用乱数データを更新する（該数回分の暗号通信では同じ暗号通信用乱数データを使用する）ようにしてもよい。

一方、上記暗号通信電文を受信した受信側エンティティｊは、前述の如く生成したエンティティｉとの共通暗号鍵Kji（＝Kij）を用いて暗号通信電文を復号し、最終的に前記平文を得る（手順５）。

すなわち、図7を参照して、まず、エンティティiとの共通暗号鍵Kji（＝Kij）を本来の鍵として使用することで、エンティティiから受信した暗号通信電文のうちの暗号化乱数データを暗号通信用乱数データに復号する（手順5－1）。次いで、その復号化された暗号通信用乱数データを鍵として使用することで、暗号通信電文のうちの暗号文を平文に復号する（手順5－2）。これにより、最終的に受信側エンティティjはエンティティiからの所望の平文の内容を知ることとなり、エンティティi，j間での暗号通信が完結する。

前述のような暗号通信のための処理を行う各エンティティ2のコンピュータマシンは、それを構成的に示すと例えば図8のブロック図に示すように構成されている。

すなわち、各エンティティ2のコンピュータマシンは、キーボード4と、図示しないCPU、RAM、ROM等により構成された本体部5と、前記個人鍵Xn及び識別子変換アルゴリズム、文章、プログラム等の平文、並びに暗号通信電文等を記憶保持するハードディスク等により構成されたデータベース6とを具備する。そして、本体部5には、その機能的構成として、共通暗号鍵を生成する共通鍵生成部7と、通信データの暗号化・復号化処理を行う暗号復号処理部8と、暗号通信用乱数データを生成する乱数生成部9と、暗号通信に際して共通鍵生成部7により生成された共通暗号鍵や乱数生成部9により生成された暗号通信用乱数データ等のデータを格納するデータ格納メモリ10とが備えられている。

このような構成を具備する各エンティティ2のコンピュータマシンは、次のような作動によって、前述のような暗号通信のための処理が行われる。

すなわち、送信側及び受信側のいずれのコンピュータマシンにおいても、共通暗号鍵を生成する際には（前記手順3）、まず、使用する前記個人鍵Xn 及び識別子変換アルゴリズムがキーボード4により本体部5に指定され、その指定された個人鍵Xn 及び識別子変換アルゴリズムが前記データベース6から本体部5の共通鍵生成部7に取り込まれる。さらに、キーボード4により、通信相手側の識別子yn が本体部5に入力される。そして、該本体部5の共通鍵生成部7は、入力された識別子yn のデータに前述の如く識別子変換アルゴリズム及び個人鍵Xn を作用させることで共通暗号鍵を生成し（前記手順3－1，3－2）、その生

成された共通暗号鍵がデータ格納メモリ１０に記憶される。

また、送信側のコンピュータマシンでは、キーボード４により、前記暗号通信用乱数データを生成するためのデータ（語句や文章等の入力操作データ）が本体部５に入力される。そして、該本体部５の乱数生成部９はその入力されたデータに基づき、前述の如く一回性の暗号通信用乱数データを生成し（前記手順４－１）、その生成された暗号通信用乱数データがデータ格納メモリ１０に記憶される。

さらに、送信側のコンピュータマシンでは、データベース６内の送信すべき平文がキーボード４から本体部５に指定され、このとき、指定された平文がデータベース６から暗号復号処理部８に取り込まれる。そして、該暗号復号処理部８は、データ格納メモリ１０に記憶された暗号通信用乱数データを、同じくデータ格納メモリ１０に記憶された共通暗号鍵を使用して暗号化する（前記手順４－２）と共に、その暗号化乱数データを鍵として前記平文を暗号化する（前記手順４－３）。このようにして暗号復号処理部８により暗号化された暗号通信用乱数データ及び平文は、それらを一括して成る暗号通信電文としてデータベース６に保持された後、別途、通信相手側のコンピュータマシンに送信される。

一方、上記暗号通信電文を受信した受信側のコンピュータマシンでは、該暗号通信電文がデータベース６に保持され、それが暗号復号処理部８に取り込まれる。そして、暗号復号処理部８は、データ格納メモリ１０に記憶されている共通暗号鍵を用いて暗号通信電文内の暗号化乱数データを暗号通信用乱数データに復号し（前記手順５－１）、さらにその復号化した暗号通信用乱数データを鍵として、暗号通信電文内の暗号化平文を元の平文に復号する（前記手順５－２）。このようにして暗号復号処理部８により暗号化された平文はデータベース６に保持される。

以上説明したように構築されている本実施形態のシステムでは、センター１で各エンティティ２の個人鍵Ｘｎ を生成する際（事前準備処理）には、各エンティティ２の名前等の識別子ｙｎ に積分変換としてのフーリエ変換のアルゴリズムを作用させるため、識別子ｙｎ 自体に類似のものが多くあっても、それをフーリエ変換してなるデータの分散性が良くなり、ひいてはそのデータにセンター行列等を施して成る個人鍵Ｘｎ の分散性も高めることができる。その結果、所謂、差分

攻撃等によるセンター1のセンター行列等のセンターアルゴリズムの解読を困難なものとすることができる。

この場合、上記の積分変換としては、フーリエ変換の他、ラプラス変換、ミラー変換、ヒルベルト変換等を使用することも可能であるが、本実施形態ではフーリエ変換（くわしくは高速フーリエ変換）を使用しているため、上記のような分散性の向上を顕著に奏することができると同時に、識別子yn にフーリエ変換を施す演算処理をコンピュータマシンを用いて高速で行うことができる。

また、個人鍵Xn を生成する際には、センターアルゴリズムとして重み関数を付加するため、有限区間上の識別子yn のデータをフーリエ変換してなるデータの異常分散を防止することができると同時に、センターアルゴリズムを解読しようとする攻撃者にとっては、センター行列やフーリエ変換アルゴリズム等の他、重み関数という未知のアルゴリズム要素が増えるため、センターアルゴリズムの解読をさらに困難なものとすることができる。特に、該重み関数が、一回性の乱数データに基づいて予想のつかない形状に生成されているため、上記の解読の困難性をより確実に確保することができる。

さらに、個人鍵Xn を生成する際には、センターアルゴリズムの他、各エンティティ2に固有の一回性の個別乱数データに基づくランダマイズ変換をも付加するため、各エンティティ2の個人鍵Xn には、各エンティティ2毎に各別で、しかも相互に相関性のないランダマイズ変換に基づく成分が含まれることとなる。このため、例えば複数のエンティティ2が結託して、各々が保持する個人鍵Xnからセンターアルゴリズム等を解読しようとしても、その解読を行うことは極めて困難なものとなる。この場合、特に、前記ランダマイズ変換では、識別子ynにフーリエ変換、重み関数及びセンター行列を作用させてなるデータのうちの、不要ビットの値を一回性の個別乱数データによりランダム化した上で、該不要ビットと有用ビットとを合わせて配置変換を行うので、このランダマイズ変換により得られる個人鍵Xn のデータのうちのどの部分に不要ビットに対応するものが含まれているのかが判らず、上記の解読がより一層困難なものとなる。また、その解読者にとっては、本実施形態のシステムを完全に破るためには、個人鍵Xn等のデータから、センター行列、重み関数、フーリエ変換（積分変換）、及びラ

ンダマイズ変換の4種類ものアルゴリズムを解読しなければならないこととなり、このような解読は事実上、不可能なものとなる。

尚、本実施形態のシステムでは、暗号通信の際に共通暗号鍵を生成するためには、個人鍵Xn に反映されている前記ランダマイズ変換による成分を打ち消すためのアルゴリズムを含む前記識別子変換アルゴリズムを個人鍵Xn と共に各エンティティ2に配付しておく必要がある。しかるに、該識別子変換アルゴリズムは、ランダマイズ変換による成分を打ち消すためのアルゴリズムとフーリエ変換アルゴリムと重み関数とを合成したものであるため、該識別子変換アルゴリズムからセンター1のセンターアルゴリズムを構成するランダマイズ変換のアルゴリズムや重み関数、フーリエ変換アルゴリズムを個々に解読することも極めて困難である。

従って、本実施形態のシステムによれば、そのシステムの安全上、最も重要なセンター1のセンターアルゴリズムを各エンティティ2の個人鍵Xn 等から解読することは事実上、不可能である。

また、任意のエンティティi，j間で暗号通信を行う際には、平文そのものを共通暗号鍵Kijを用いて暗号化するのではなく、該平文は偏った特徴性をもたない一回性の暗号通信用乱数データを鍵として暗号化すると共に、その暗号化平文を復号するための鍵としての暗号通信用乱数データを共通暗号鍵Kijを用いて暗号化するようにしたため、暗号化された通信データを第三者が傍受しても、その通信データから共通暗号鍵Kijを解読することは困難である。そして、該共通暗号鍵Kijを解読することが困難であるため、該共通暗号鍵Kijに含まれる各エンティティ2の個人鍵Xn の情報、さらには該個人鍵Xn に含まれるセンターアルゴリズムの情報を第三者が取得することも困難である。また、前記平文にあっては、暗号通信用乱数データを鍵として暗号化されるので、該平文の機密性も確保される。

従って、本実施形態によれば、種々の攻撃に対して安全性の高い暗号通信システムを提供できる。そして、任意のエンティティi，j間での暗号通信に際しては、各エンティティi，jは自己の個人鍵Xi，Xj 及び識別子変換アルゴリズムを、相手側の識別子yj，yi に作用させるだけで、センター1の関与やエン

ティティｉ，ｊ同士での事前連絡等を伴うことなく共通暗号鍵Ｋｉｊを生成して共有することができるので、安全性が高いだけでなく、簡易で汎用性の高い暗号通信システムを提供できる。尚、上記のように共通暗号鍵Ｋｉｊを生成する上で、識別子ｙｎ が重要な役割を演じる点は、A.Shamirによる論文「Identity-Based Cryptosystems and Signature Schemes／Advances in Cryptology:Proceeding of CRYPTO '84 ／Springer LNCS 196,1985,pp.47-53 」に見られる考え方と同様である。

次に、本実施形態のシステムのより理論的な有効性について説明する。

本システムでは、各エンティティ２の個人鍵を演算し、さらに共通暗号鍵を算出する演算は線形変換に基づいて行われ、この線形変換について以下説明する。

まず、Ｘｉｆをｆ人のエンティティ２間で共通暗号鍵を生成する際にエンティティｉの個人鍵とする。このとき、上記の線形変換を構築するための一般的な考え方は、ｆ入力対称変換ｇ（ｆ個の変数の関数で、対称性を有するもの）を任意に選択し、エンティティｉの個人鍵Ｘｉｆを、エンティティｉの識別子ｙｉ に対して $Xif(\xi_1, \cdots\cdots, \xi_{f-1}) = g(yi, \xi_1, \cdots\cdots, \xi_{f-1})$ を満たすようなｆ－１入力変換として決定することである。ここで、添え字付きのξは任意の識別子を示す変数である。この場合、上記線形変換は、ｆ入力対称変換ｇの核が多重線形写像（ｆ重線形写像）に従うように見いだすことができ、この線形変換は、基本的には有限体上の線形空間で定義され、環上の剰余類に一般化される。

本システムはｆ＝２とした場合のものであり、上記の線形変換は次のように定義される。

ここで、以下の説明において、センター１に属するエンティティの集合をＥ、識別子の集合をＩ、共通暗号鍵の集合をＫとする（図１参照）。また、Ｑを単位元をもつ可換環、ＪをＱ上の位数ｍの剰余類、ＫをＱ上の位数ｈの剰余類とし、Ｊ，Ｋの元はそれぞれｍ－縦ベクトル、ｈ－縦ベクトルとする。尚、Ｑが体であるならば、Ｊ，Ｋはそれぞれ次元ｍ，ｈの線形空間となる。また、位数ｍは識別子の総数に等しい。

また、ＲをＩからＪへの写像を構成する線形変換とし、以下、アイデンティティ変換と称する。このアイデンティティ変換は、前述の実施形態のシステムに対

応させると、基本的には識別子のデータに重み関数付きのフーリエ変換（積分変換）を施す変換に相当し、さらには、後述の如く前記ランダマイズ変換をも含む変換に拡張されるものである。

以上のことを前提として、まず、J_2（Jの二つの元の組を要素とする集合）から共通暗号鍵の集合Kへの対称Q階多重線形写像（2入力対称変換）$g : J_2 \rightarrow K$が任意に選択されて決定される。このgは任意の二つの識別子をそれぞれアイデンティティ変換したものからそれらの識別子に対応した共通暗号鍵を生成するための変換に相当する。

また、ある与えられた識別子yi（∈I）に対して、Q上のh行m列の行列xiが$xi \cdot \eta = g(R(yi), \eta)$を満たすように決定される。ここで、$\eta$はQ上の任意のm一縦ベクトルで、Jの元である（以下、同様）。

さらに、ある与えられたyi（∈I）に対して、$Xi(\xi) = xi \cdot R(\xi)$（但し、$\xi$はIの任意の元。以下、同様）となるようにI入力変換Xi（ξ）を構成する。

このXi（ξ）が、エンティティiに対する個人鍵であり、該個人鍵Xi（ξ）は、1入力変換Viを前記行列xiを用いて$Vi(\eta) = xi \cdot \eta$と定義したとき、次式によって表される。

$$Xi(\xi) = Vi(R(\xi))$$

尚、センターが複数存在するとき、$Vi(\eta) = xi \cdot \eta$における「xi」の部分は、各センター毎に上記のように決定される行列xiの総和に置き換えられる。

このように個人鍵Xiを定義したとき、前述したことから容易に判るように、任意のエンティティa，b∈Eに対して、Xa（yb）＝Xb（ya）となる。すなわち、エンティティa，bがそれぞれの個人鍵Xa，Xbに相手側の識別子yb，yaを入力すれば、共通の暗号鍵Xa（yb）＝Xb（ya）が得られる。

尚、前記多重線形写像gの代わりに、多変数多項式を選択したとしても、本システムの線形変換の適用範囲に含まれる。この理由は、任意の多項式が未知数の集合の適当な変換によって線形多項式に書き換えられるという事と、そのような変換は前記アイデンティティ変換Rの中に吸収することができるという事とによ

る。更に、いくつかの変換は、線形変換と、指数関数のような演算との合成と見なすことができる。

次に、本システムの線形変換の実行性能とアイデンティティ変換Rの役割とについて述べる。

任意の変換Aに対して、Cd（A）、Ce（A）をそれぞれ変換Aの記述の複雑さ、及び変換Aの評価の複雑さとする。このとき、前述の変換Xi，R，Viに対して、次の関係式が成り立つ。

$$Cd(Xi) = Cd(R) + Cd(Vi)$$

$$Ce(Xi) \leq Ce(R) + Ce(Vi)$$

この場合、個人鍵を示す変換Xi の入力（識別子）がw [bit] で記述されるとすると、変換Vi の記述の複雑さCd（Vi ）については

$$Cd(Vi) = h \cdot m \cdot w \text{ [bit]}$$

が成り立つ。また、変換Vi の記述の複雑さCe（Vi ）については

$$Ce(Vi) = O(h \cdot m) \text{ [Q−演算]}$$

が成り立つ。ここで、O（h・m）[Q−演算] は可換環Q上でのh・mのオーダーを意味し、この値は、概ねO（w^2 ）[bit 変換] 、すなわち、w^2 のオーダーによって評価できる。そして、小さい可換環Q（例えばガロア体GF [2] ）を選んだとき、Ce（Vi ）は低いものとなる。

従って、変換Xi の記述の複雑さCd（Xi ）及び評価の複雑さCe（Xi ）は、アイデンティティ変換Rの記述の複雑さCd（R）及び評価の複雑さCe（R）に負うところが大きい。

ここで、システムを破ろうとする一つもしくは複数のエンティティjが、それぞれの個人鍵Xj を利用する場合について考察する。

明らかに、本システムを完璧に破ることは、前述の多重線形写像g：$J_2 \rightarrow K$ を決定することである。この場合、システムを完全に破るためには、センターが協力するか、あるいは、多重線形写像gの位数と同じ数（これは概ね、識別子の総数m（＝Jの位数）に等しい）のエンティティの協力が必要であり、実際上は、不可能である。

さらに、一部のエンティティjによる、他のエンティティiの個人鍵Xi の決

定の可能性について考察する。この問題については、以下に述べるようにアイデンティティ変換Rが重要な役割を担う。

まず、「エンティティ全体の集合Eの部分集合Bの全てのエンティティjが協力して、それらのエンティティj∈Bがそれぞれの個人鍵Xj の全体{Xj | j∈B}を使ったとしても、集合E－B内の任意のエンティティiの個人鍵Xi を決定するために有用などのような情報も得ることができない」ということは、「E－B内の各エンティティiにとって、アイデンティティ変換R（yi）が、B内のエンティティjのそれぞれのアイデンティティ変換R（yj）の全体{R（yj）| j∈B}から線形独立である」ということと同値であることが容易に導かれる。従って、本システムの線形変換の情報理論的安全性は、集合{R（yi）| i∈E}の任意の部分集合Uが線形独立であることに帰着させられる。よって、線形変換と線形代数学的な順列組み合わせとの間には強い関係があり、線形変換の安全性を評価する上では、特に、m行n列（ここでn＝#E＝eエンティティEの総数である）のパリティチェック行列H＝（R（y1），……，R（yn））によって定義される線形符号LR ＝{z∈Q^n | H・z＝0}、すなわち、パリティチェック行列Hとの積が零ベクトルとなるような可換環Q上のn－縦ベクトルで表される符号語zの集合を考察することが重要である。所謂、ハミング（Hamming）重率sの符号語z（∈LR）が存在するということと、s－1個のエンティティjの協力によって、特定のエンティティiの個人鍵Xi を導くことができるということと同値であることは容易に導かれる。

一方、以下のようにアイデンティティ変換Rを個別化する（アイデンティティ変換Rを各エンティティに固有のものとする）ことによって、多数のエンティティが結託しても、システムを破ることは難しくなる。すなわち、仮にシステムを破ろうとする各エンティティj（j∈B）のアイデンティティ変換R（yj）の集合{R（yj）| j∈B}に対し、他のエンティティiのアイデンティティ変換R（yi）が線形従属で、R（yi）＝ΣCj ・R（yj）（但し、Cj は適当な係数）であるならば、前述した個人鍵の定義から明らかなように、エンティティiの個人鍵Xi 及びエンティティj（j∈B）の個人鍵Xj について、Xi ＝ΣCj ・Xj が成り立つ。このため、システムを破ろうとする各エンティティ

jの集合Bは容易に他のエンティティiの個人鍵Xi を知ることができることとなる。ところが、アイデンティティ変換Rを個別化した場合には、該変換Rは各エンティティに固有のものであるので、与えられたエンティティjの集合Bに対して、他の個人鍵Xi を解読し得るような識別子yi を有するエンティティiを見いだすことは容易なことではない。換言すれば、集合Bのエンティティjは、それらが所持する個人鍵Xj 等の情報からどのエンティティiの個人鍵Xi を解読し得るのかを知ることができない。また、逆に、与えられた識別子yi を有するエンティティiに対し、その個人鍵Xi を解読し得るような識別子yj を含む集合Bを見いだすことも容易ではない。換言すれば、解読しようとする個人鍵Xi を有するエンティティiを特定しても、その個人鍵Xi を解読するためにどのエンティティ同士が結託すればよいのかを知ることができない。このように、アイデンティティ変換Rを個別化することは、システムの複雑さ理論的な安全性を高める上で本質的に重要なことである。

このようにアイデンティティ変換Rを個別化する場合、種々の線形変換を選択することが可能であるが、それらは、基本的には二つの範疇に大別される。

その一つは、対応する線形符号LR がよく知られた代数学的または代数幾何学的な符号になるようなアイデンティティ変換Rを用いる場合であり、他の一つは、アイデンティティ変換Rをエンティティ毎に個別にランダム化する場合である。

この場合、前者の手法では、安全性のために識別子の総数mを大きなものとすると、必要なデータ量が大規模なものとなる傾向がある。例えば、原始要素がαでQ＝GF（q）：ガロア体とし、また、h＝1、βをαのξ乗（$\log\beta=\xi\cdot\log\alpha$）とし、さらにR（$\xi$）＝$[1, \beta, \beta^2, \cdots, \beta^{m-1}]^T$とし、Iが{0，1，2，…，n－1}と符号化されたとする。このアイデンティティ変換Rは一方向性を有さないので、厳密な線形変換ではないが、前述のR. Blomの論文「An Optimal Class of Symmetric Key Generation Systems」中に提案された線形変換に相当し、線形符号LR は所謂、リードーソロモン（Reed-Solomon）符号に相当する。そして、この手法では、ネットワーク内のエンティティの総数nはガロア体Q＝GF（q）におけるqよりも小さいことが必要であり、例えばn＝10^{12}の場合に、この手法を適用すると、最小のQはGF（2^{40}）となって、

極めて大規模なデータ量が必要となる。

これに対して、アイデンティティ変換Rをエンティティ毎に個別にランダム化する後者の手法は、前述の実施形態で、前記ランダマイズ変換によって実現化した手法であり、この手法によれば、識別子の総数m（本システムではこれはエンティティの総数nに等しい）が大きくとも、高速な処理が可能で且つ小規模なデータ量で済む多数のアイデンティティ変換Rが存在する。

他方、周知の漸近的バルシャモフ・ギルバート（Varshamov-Gilbert ）の限界式を導くのと同様の手法によって、該限界式に対応する次の関係式が得られる。

$$m/n + r \leqq \Phi(b/n)$$

但し、$r = m \cdot \log_q(q-1)$

ここで、Φは

$$\Phi(u) = u \cdot \log_q(q-1) - u \cdot \log_q u - (1-u)\log_q(1-u)$$

によって定義される関数である。また、上記の不等式中のｂはシステムを破ろうとするエンティティｊの総数（＝＃Ｂ）である。

上記の不等式は、システムを破るために必要なエンティティｊの総数ｂの限界を規定するものであり、この不等式が成立しないエンティティ数ｂではシステムを破ることができないことを意味する。

そして、この不等式に基づいて、任意のm及びｂに対して、高々ｂ個のエンティティｊが共謀しても、他のエンティティｉの個人鍵Ｘｉ を解読することができないようなアイデンティティ変換Rが存在することが導かれる。また、アイデンティティ変換Rの個別のランダム化は、多くの場合、上記のような条件を満たしつつ良好な線形独立な構造をもたらすことも判る。

従って、本システムは、アイデンティティ変換Rの個別的なランダム化によって、安全性の高いシステムを提供することができるものである。言い換えれば、本システムは、アイデンティティ変換Rの個別的なランダム化によって、該変換Rの記述の複雑さＣｄ（Ｒ）及び評価の複雑さＣｅ（Ｒ）を高め、ひいては、個人鍵Ｘｉ の記述の複雑さＣｄ（Ｘｉ ）及び評価の複雑さＣｅ（Ｘｉ ）を高めてシステムの安全性を確保したものである。

実際、例えばQ＝GF［2］、m＝8192、h＝64とした場合、Cd（Xi）＝64［Kbyte］となる。この場合、160bitの共通暗号鍵によって、最大で10120個のエンティティまでを含むシステム上の任意の二つのエンティティ間で暗号通信を行うことができる。そして、例えばクロック200MHzで32bitのCPUと640Kbyteのメモリを使用した場合、20ms以内に各個人鍵を算出することができる。さらに、このシステムは8192個のエンティティが結託しなければシステムを完全に破ることはできず、また、各エンティティ毎の個別のランダム化によって、256個以上のエンティティが結託しなければ、他のエンティティの個人鍵に対するいかなる情報も得ることができない。

尚、前述の実施形態では、センターアルゴリズムとして、重み関数及びフーリエ変換アルゴリズムの他、センター行列を設定したが、重み関数自体をセンター行列として用いることも可能である。

また、前記実施形態では、積分変換としてフーリエ変換を用いたが、ラプラス変換、ミラー変換、ヒルベルト変換等、他の形式の積分変換を用いてもよい。

産業上の利用可能性

本発明はインターネット、パソコン通信網等のネットワークにおいて、共通鍵方式による暗号通信を簡便且つ安全に行うことができる手法として有用である。

請 求 の 範 囲

1．複数のエンティティとセンターとを含むネットワークにおいて、通信を行うエンティティ間で通信データの暗号・復号化を行うための共通の暗号鍵を両エンティティが所有する方法であって、

あらかじめ前記センターは、各エンティティに固有で且つ公開性の識別子を、該センターのみが保持する各エンティティに共通で且つ少なくとも積分変換アルゴリズムを含むセンターアルゴリズムにより変換して各エンティティに固有の個人鍵を生成すると共にその個人鍵と前記積分変換アルゴリズムとを各エンティティに配付しておき、

前記エンティティ同士が相互に通信を行うとき、互いに通信相手側の識別子に自己が保持する前記積分変換アルゴリズム及び前記個人鍵を作用させることにより該エンティティ同士が共通の暗号鍵を所有することを特徴とする暗号鍵共有方法。

2．前記積分変換アルゴリズムは重み関数付きの積分変換アルゴリズムであることを特徴とする請求の範囲第1項記載の暗号鍵共有方法。

3．前記重み関数は前記センターにおいて生成された乱数データにより予想のつかないパターンに決定されていることを特徴とする請求の範囲第2項記載の暗号鍵共有方法。

4．前記乱数データは一回性の乱数データであることを特徴とする請求の範囲第3項記載の暗号鍵共有方法。

5．前記積分変換アルゴリズムはフーリエ変換アルゴリズムであることを特徴とする請求の範囲第1項又は第2項記載の暗号鍵共有方法。

6．前記センターは、前記識別子を前記センターアルゴリズムにより変換したものに、さらに各エンティティに固有で且つ各エンティティには不知の一回性の個別乱数データによりランダマイズ変換を施して前記個人鍵を生成すると共に、該個人鍵に含まれる前記ランダマイズ変換の成分を打ち消すためのアルゴリズムと前記積分変換アルゴリズムとからなる識別子変換アルゴリズムを該個人鍵と共に各エンティティに配付しておき、

前記エンティティ同士は相互に通信を行うとき、互いに通信相手側の識別子に自己が保持する前記識別子変換アルゴリズム及び前記個人鍵を作用させることにより該エンティティ同士が共通の暗号鍵を所有することを特徴とする請求の範囲第1項に記載の暗号鍵共有方法。

7．前記ランダマイズ変換は、前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列を前記一回性の個別乱数データにより配置変換することにより行うことを特徴とする請求の範囲第6項記載の暗号鍵共有方法。

8．前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列は複数の不要ビットを含み、前記ランダマイズ変換は、該不要ビットの値を前記一回性の個別乱数データによりランダム化し、さらに該不要ビットを含む前記データ列の全体を配置変換することにより行うことを特徴とする請求の範囲第7項記載の暗号鍵共有方法。

9．前記一回性の個別乱数データは、前記各エンティティの所定の処理に基づき生成することを特徴とする請求の範囲第6項記載の暗号鍵共有方法。

10．前記所定の処理は前記各エンティティの人間による入力操作であり、その入力操作の時間的タイミングに基づき前記一回性の個別乱数データを生成することを特徴とする請求の範囲第9項記載の暗号鍵共有方法。

11．複数のエンティティとセンターとを含むネットワークにおいて、通信を行うエンティティ間で通信データの暗号・復号化を行うための共通の暗号鍵を両エンティティが所有する方法であって、

あらかじめ前記センターは、各エンティティに固有で且つ公開性の識別子を該センターのみが保持する各エンティティに共通のセンターアルゴリズムにより変換したものに、各エンティティに固有で且つ各エンティティには不知の一回性の個別乱数データによりランダマイズ変換を施して各エンティティに固有の個人鍵を生成すると共に、その個人鍵と、該個人鍵に含まれる前記ランダマイズ変換の成分を打ち消すアルゴリズムを含む識別子変換アルゴリズムとを各エンティティに配付しておき、

前記エンティティ同士が相互に通信を行うとき、互いに通信相手側の識別子に

自己が保持する前記識別子変換アルゴリズム及び個人鍵を作用させることにより該エンティティ同士が共通の暗号鍵を所有することを特徴とする暗号鍵共有方法。

１２．前記ランダマイズ変換は、前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列を前記一回性の個別乱数データにより配置変換することにより行うことを特徴とする請求の範囲第１１項記載の暗号鍵共有方法。

１３．前記各エンティティの識別子を前記センターアルゴリズムにより変換したものを表すデータ列は複数の不要ビットを含み、前記ランダマイズ変換は、該不要ビットの値を前記一回性の個別乱数データによりランダム化し、さらに該不要ビットを含む前記データ列の全体を配置変換することにより行うことを特徴とする請求の範囲第１２項記載の暗号鍵共有方法。

１４．前記一回性の個別乱数データは、前記各エンティティの所定の処理に基づき生成することを特徴とする請求の範囲第１１項記載の暗号鍵共有方法。

１５．前記所定の処理は前記各エンティティの人間による入力操作であり、その入力操作の時間的タイミングに基づき前記一回性の個別乱数データを生成することを特徴とする請求の範囲第１４項記載の暗号鍵共有方法。

* C L M S *