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、η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、ξ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、I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* | 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。

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

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。

FIG. 1

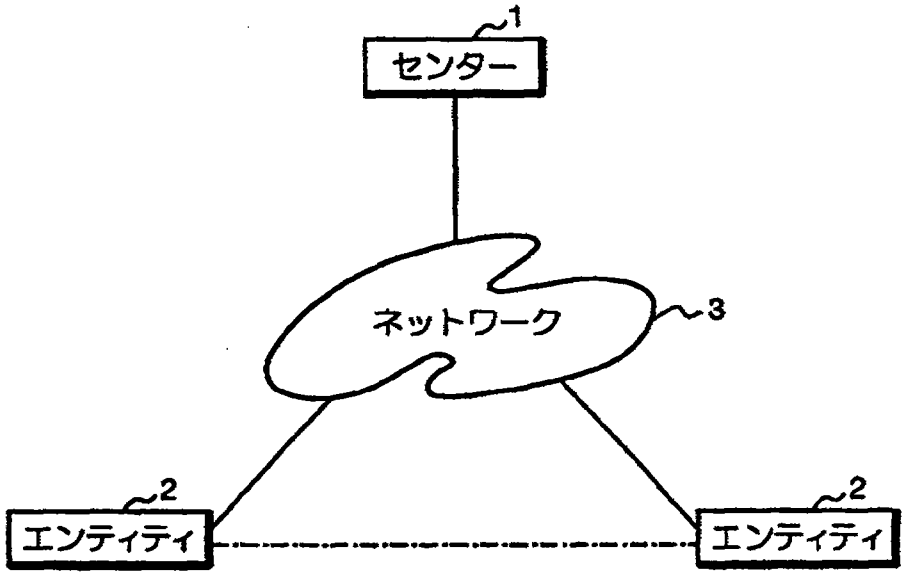


FIG.2

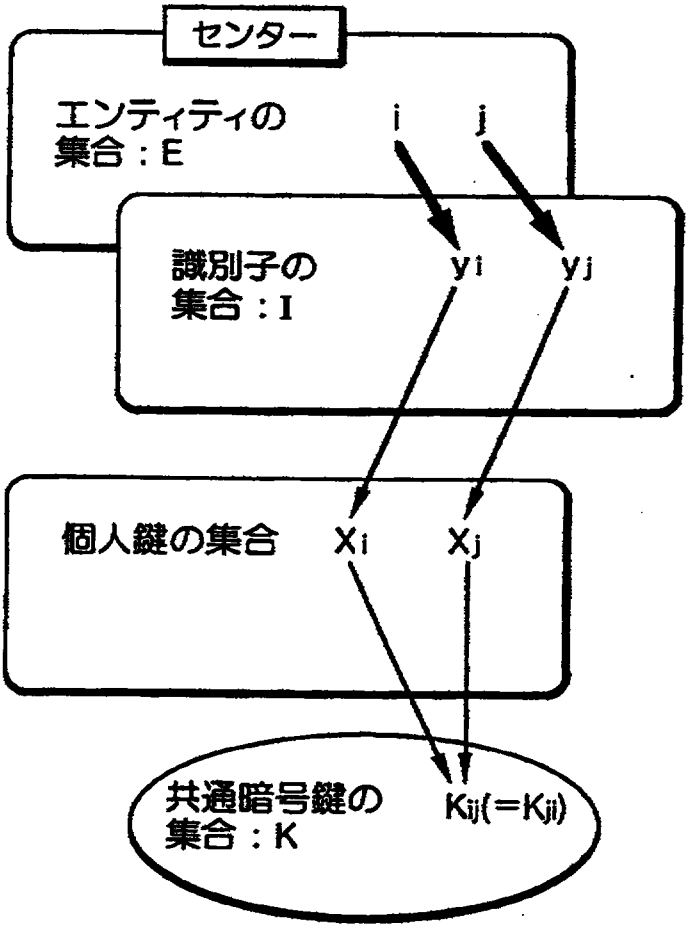

センター
エンティティの
集合：E
i
j
識別子の
集合：I
yi
yj
個人鍵の集合
Xi
Xj
共通暗号鍵の
集合：K
Kij(=Kji)

FIG.3

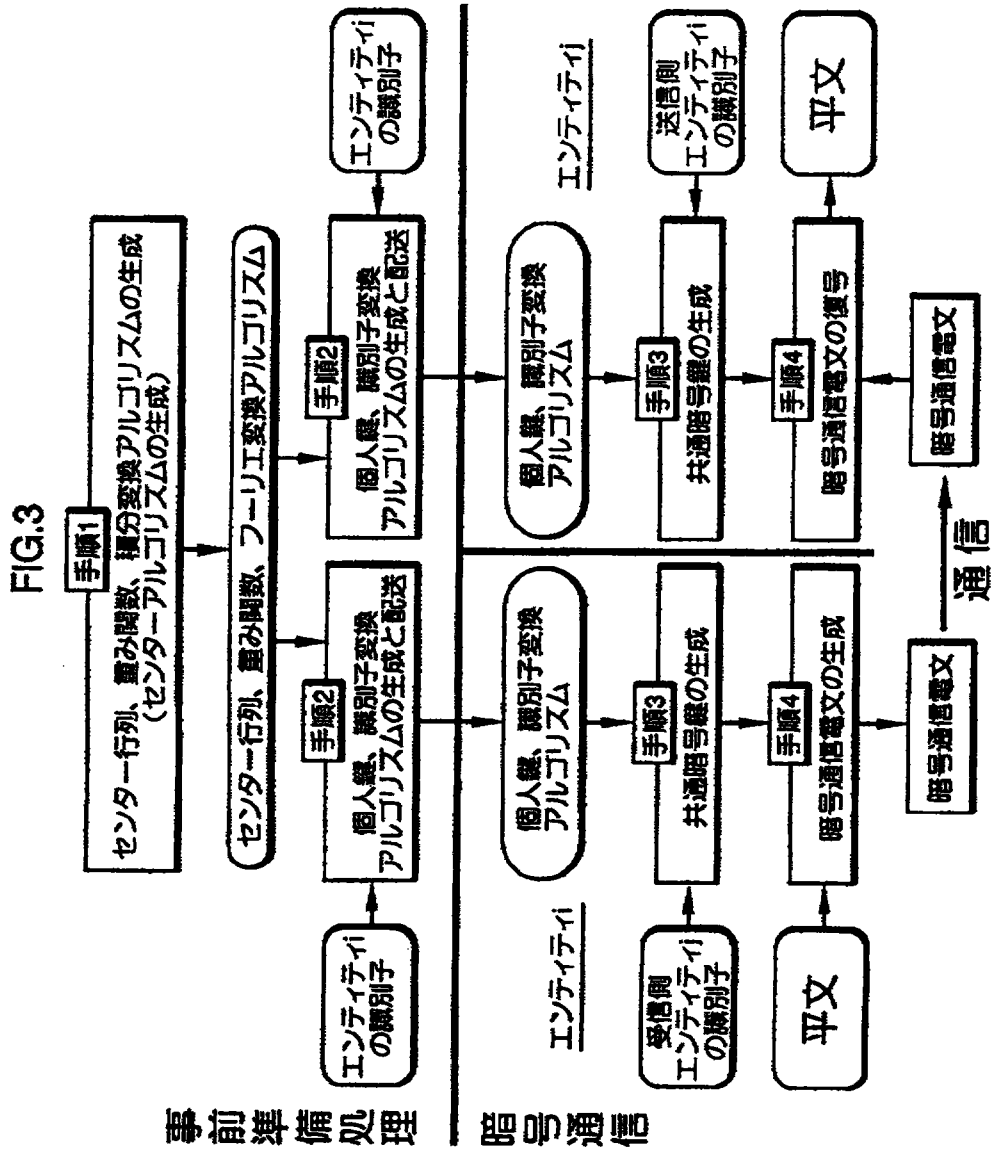

事前準備処理
暗号通信
手順1
センター行列、冪み関数、構分変換アルゴリズムの生成
(センターアルゴリズムの生成)
センター行列、冪み関数、フーリエ変換アルゴリズム
手順2
個人鍵、識別子変換
アルゴリズムの生成と配送
エンティティiの識別子
エンティティj
個人鍵、識別子変換
アルゴリズム
手順3
共通暗号鍵の生成
送信側
エンティティiの識別子
手順4
暗号通信電文の復号
平文
暗号通信電文
通信
手順2
個人鍵、識別子変換
アルゴリズムの生成と配送
エンティティiの識別子
エンティティi
個人鍵、識別子変換
アルゴリズム
手順3
共通暗号鍵の生成
受信側
エンティティiの識別子
手順4
暗号通信電文の生成
平文
暗号通信電文

FIG4

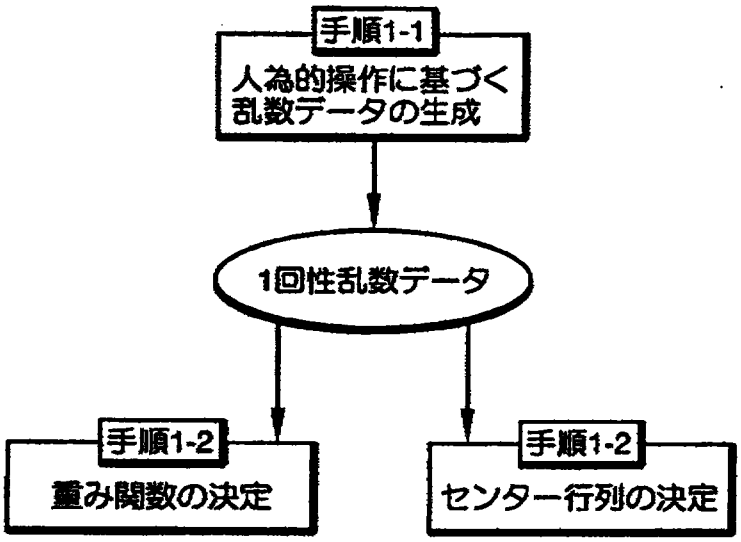

手順1-1
人為的操作に基づく
乱数データの生成
1回性乱数データ
手順1-2
重み関数の決定
手順1-2
センター行列の決定

FIG.5

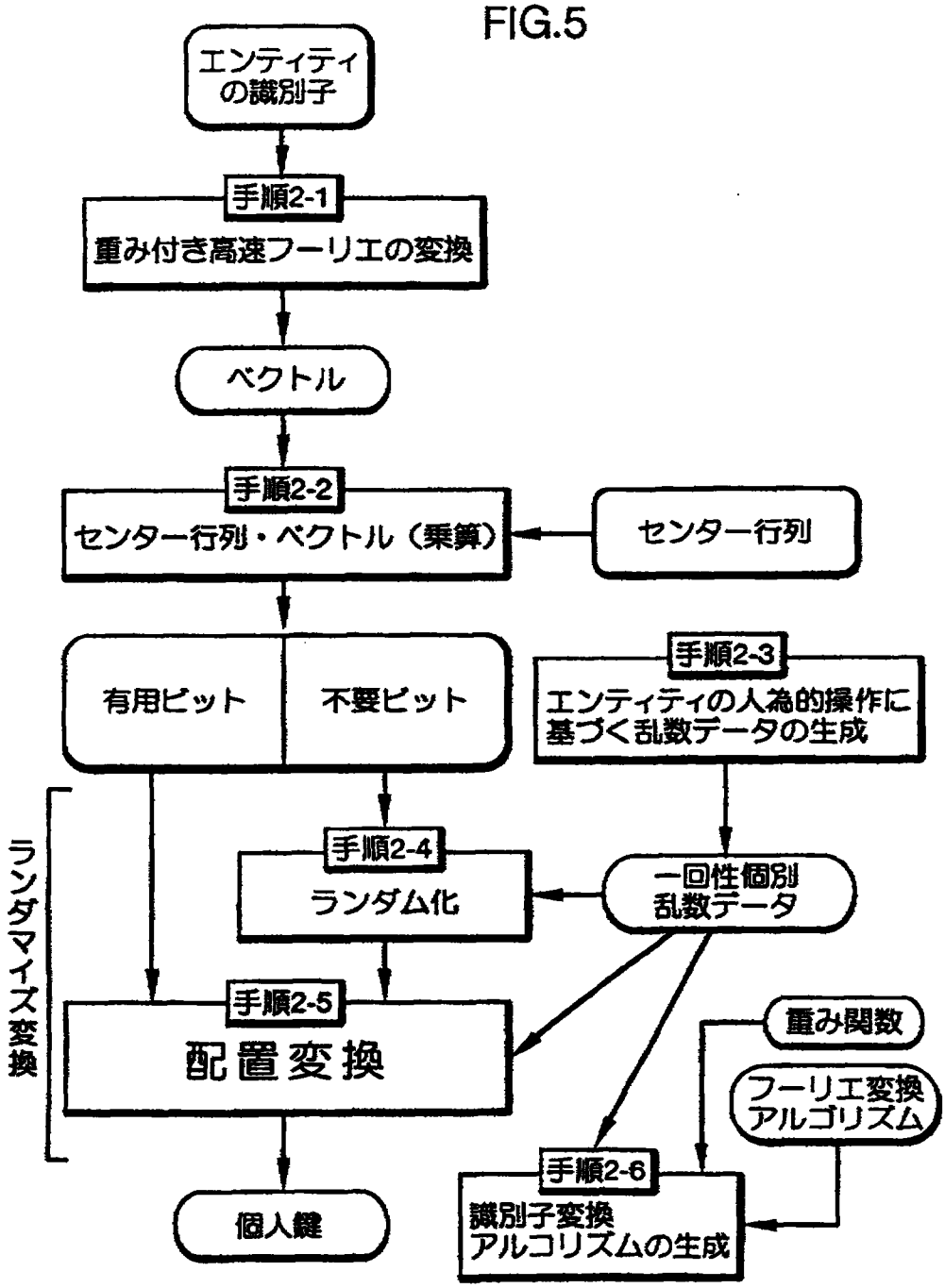

エンティティの識別子
手順2-1
重み付き高速フーリエの変換
ベクトル
手順2-2
センター行列・ベクトル（乗算）
センター行列
有用ビット
不要ビット
手順2-3
エンティティの人為的操作に基づく乱数データの生成
ランダマイズ変換
手順2-4
ランダム化
一回性個別乱数データ
手順2-5
配置変換
重み関数
フーリエ変換アルゴリズム
手順2-6
識別子変換アルゴリズムの生成
個人鍵

FIG.6
（送信側）

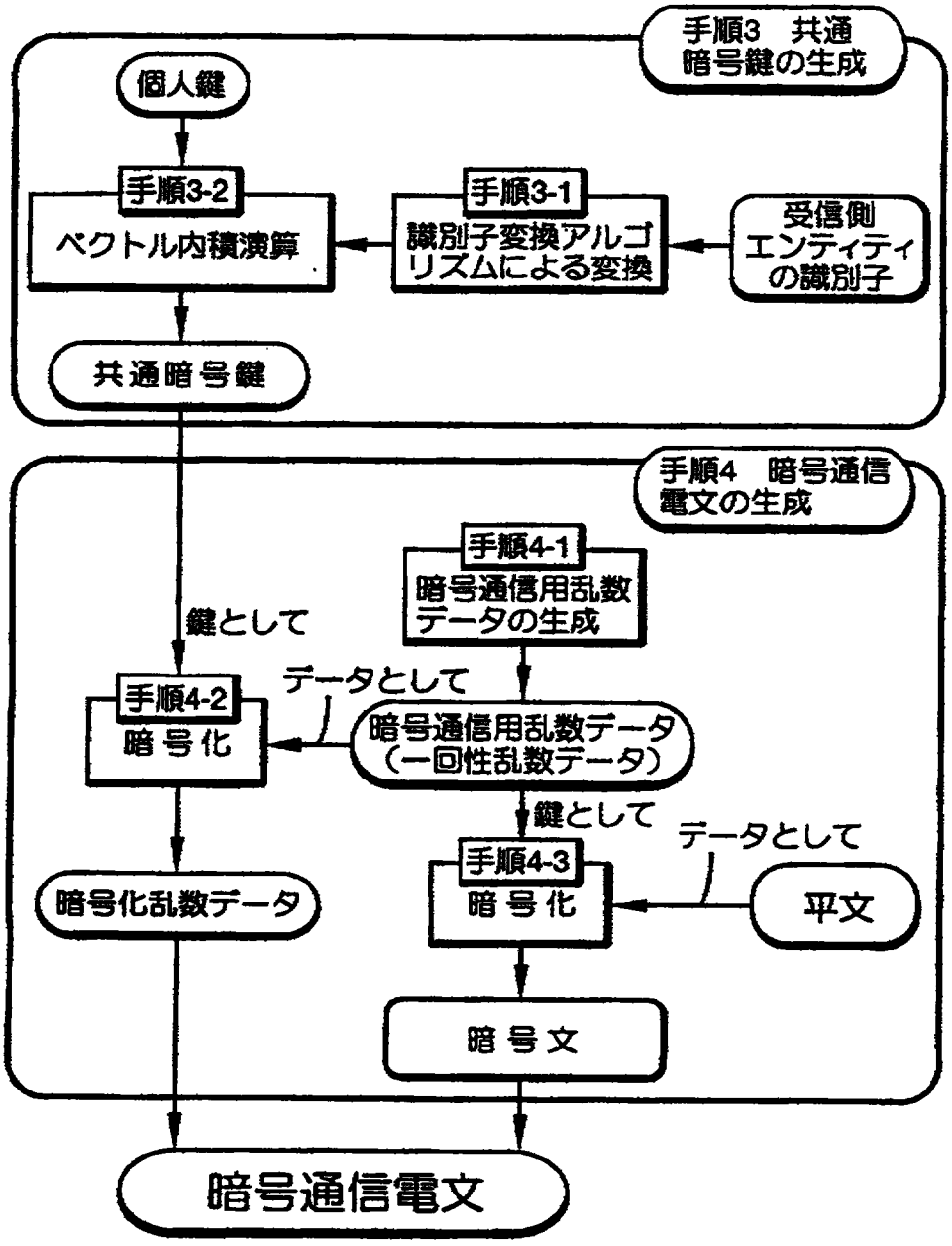

手順3　共通暗号鍵の生成
個人鍵
手順3-2
ベクトル内積演算
手順3-1
識別子変換アルゴリズムによる変換
受信側エンティティの識別子
共通暗号鍵
手順4　暗号通信電文の生成
手順4-1
暗号通信用乱数データの生成
鍵として
データとして
手順4-2
暗号化
暗号通信用乱数データ（一回性乱数データ）
鍵として
データとして
手順4-3
暗号化
平文
暗号化乱数データ
暗号文
暗号通信電文

FIG.7
(受信側)

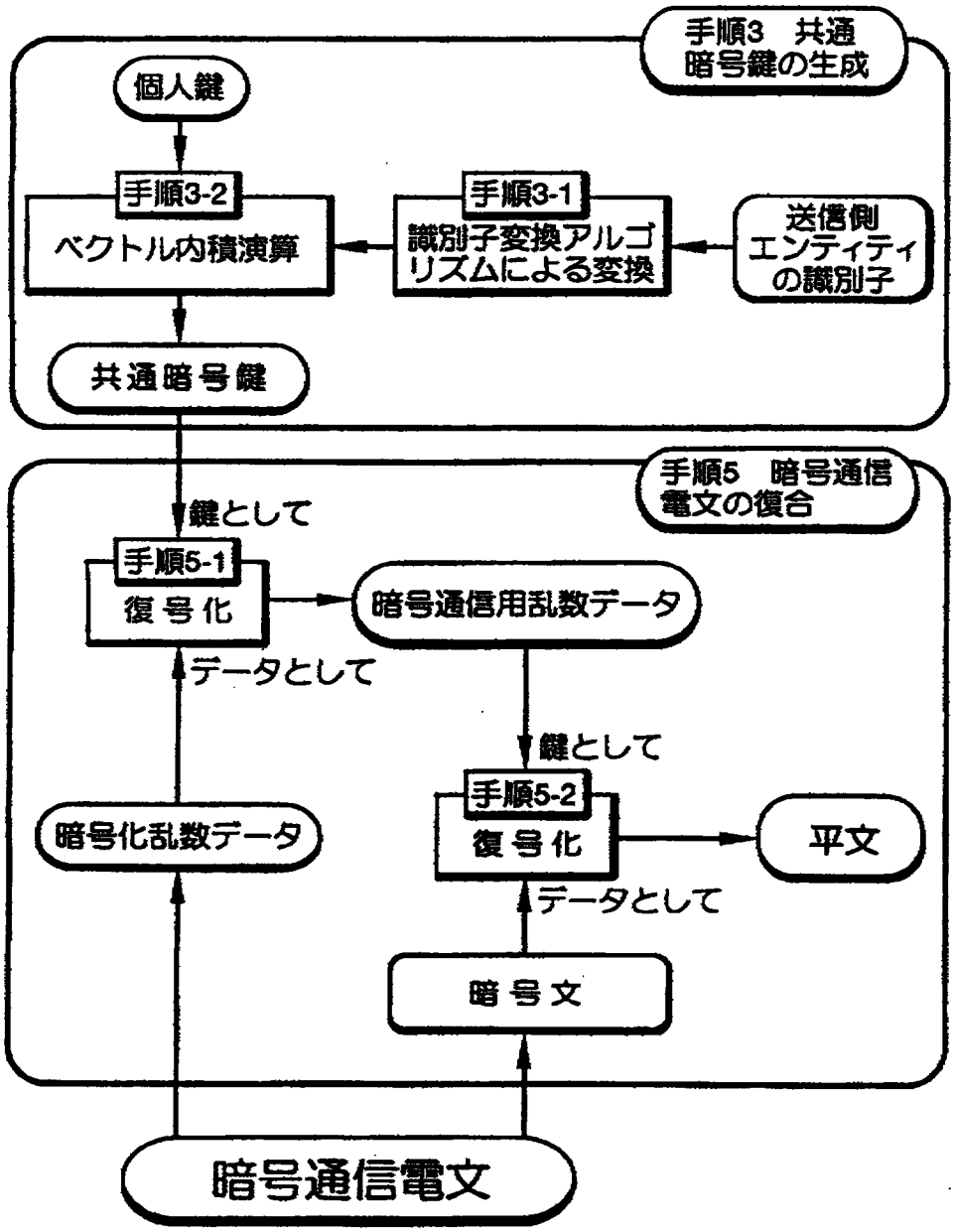
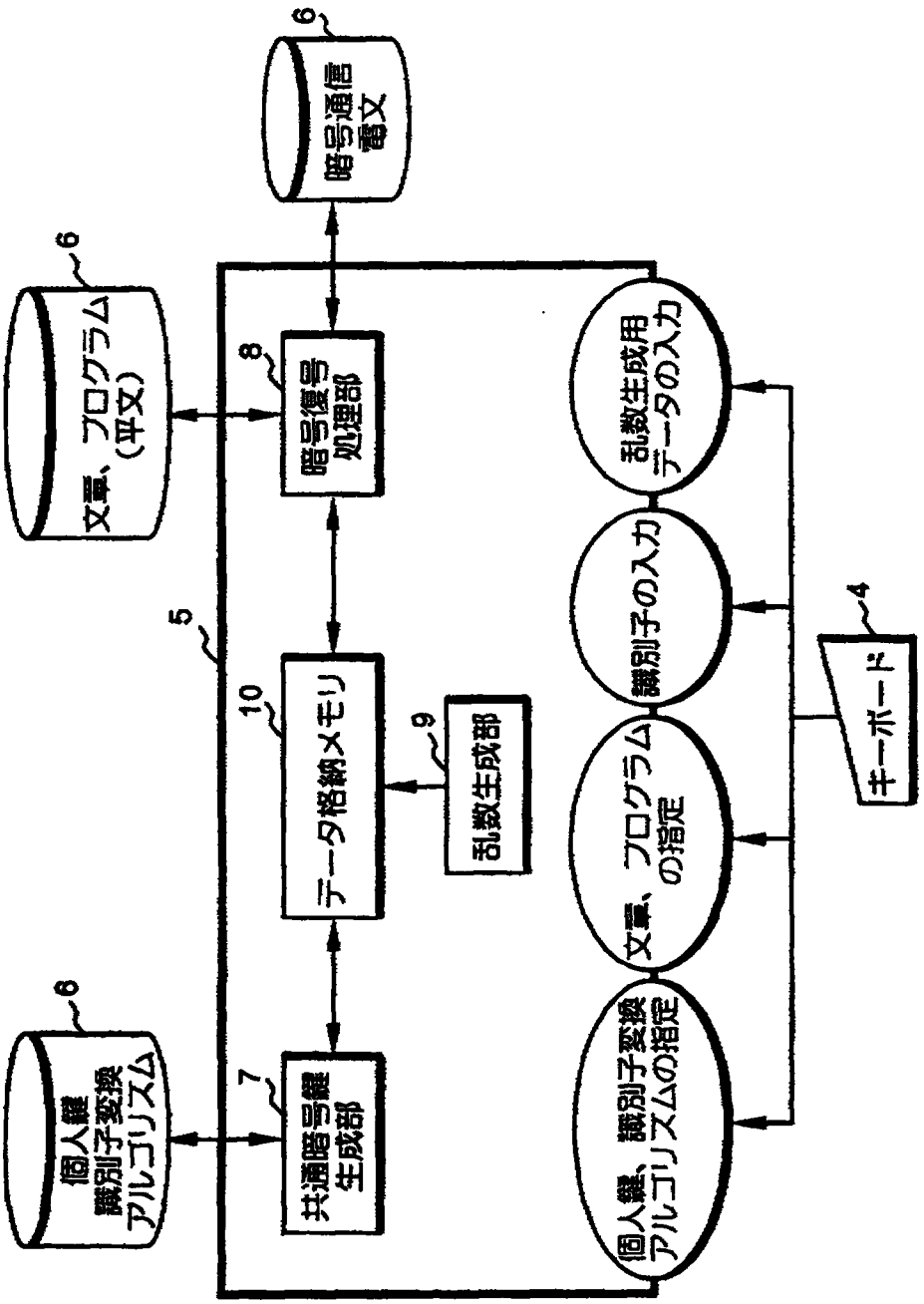

手順3 共通暗号鍵の生成
個人鍵
手順3-2
ベクトル内積演算
手順3-1
識別子変換アルゴリズムによる変換
送信側エンティティの識別子
共通暗号鍵
手順5 暗号通信電文の復合
鍵として
手順5-1
復号化
暗号通信用乱数データ
データとして
鍵として
手順5-2
復号化
平文
暗号化乱数データ
データとして
暗号文
暗号通信電文

FIG. 8


6
暗号通信電文
6
文章、プログラム（平文）
8
暗号復号処理部
5
10
データ格納メモリ
9
乱数生成部
6
個人鍵識別子変換アルゴリズム
7
共通暗号鍵生成部
乱数生成用データの入力
識別子の入力
文章、プログラムの指定
個人鍵、識別子変換アルゴリズムの指定
4
キーボード

Translation of PCT Application

DESCRIPTION

METHOD OF SHARING CRYPTOKEY

TECHNICAL FIELD

The present invention relates to a method of sharing a cryptokey for cryptographic communications between entities on a computer network.

BACKGROUND ART

Recent years have seen a pressing need for ciphertext communication technology to keep communication data secret from third parties for communications on a network such as the Internet.

One well known type of such ciphertext communication technology is a form of public key cryptography known as RSA. Another form of ciphertext communication technology which is generally known in the art is a process of sharing a cryptokey used for communications between entities on a network. According to such a process of sharing a cryptokey, a transmitting entity encrypts communication data of a plaintext using a cryptokey and then transmits the cryptographic communication data to a receiving entity. Then, the receiving entity decrypts the received cryptographic communication data back into the original communication data, using the same cryptokey as the cryptokey used by the transmitting entity. The term "entity" used above sig-

nifies any existing body for carrying out communications, e.g., a device such as a terminal connected to the network, a user of the device, a program for operating the device, a combination thereof, or the like.

Conventional attempts to realize the process of sharing a cryptokey are disclosed in "NON-PUBLIC KEY DISTRIBUTION/Advances in Cryptography: Proceedings of CRYPTO '82 /Plenum Press, 1983, pp. 231 - 236" by Rolf Blom, "An Optimal Class of Symmetric Key Generation Systems/Advances in Cryptology: EUROCRYPT '84/Springer LNCS 209, 1985, pp. 335 - 338" by Rolf Blom, Japanese patent publication No. 5-48980, and U.S. patent No. 5,016,276, for example.

According to the above disclosed proposals, a center or central facility established on the network generates a secret private key for each of entities for generating a common cryptokey and distributes the generated secret privet key to each of entities. When the entities communicate with each other, each of the entities applies its own secret private key to the other entity's identifier (name, address, or the like), generating a common cryptokey shared by the entities.

In the above process, the secret private key for each of entities is generated by transforming the identifier of each entity according to a center algorithm which is held by the center only and common to the entities.

More specifically, if the center algorithm is expressed as a function P(x, y) of variables x, y representing

two arbitrary identifiers, respectively, then the center algorithm is established so that it has a symmetry represented by P(x, y) = P(y, x). A function P(x, i) (hereinafter expressed as "Pi(x)") which is generated when the actual identifier i of each of the entities is substituted in the value of the variable y, for example, of the variables x, y of the function P(x, y) is distributed as a secret private key to each entity. When the entity having the identifier i subsequently communicates with the entity having the identifier j, the entity having the identifier i applies the identifier j of the other entity to its own secret private key Pi(x), i.e., sets the variable x to "j", thus generating a cryptokey Pi(j). Similarly, the entity having the identifier j applies the identifier i of the other entity to its own secret private key Pj(x), thus generating a cryptokey Pj(i). Since the center algorithm has the above symmetry, the cryptokey Pi(j) is equal to the cryptokey Pj(i) (Pi(j) = Pj(i)). Therefore, the entities having the respective identifiers i, j have obtained a common cryptokey.

With the above process of sharing a cryptokey, each entity can obtain a cryptokey common to itself and any other arbitrary entity without involving the center simply by applying the identifier of the arbitrary entity with which to communicate to its own secret private key. Consequently, the above process of sharing a cryptokey is effective to simplify a cryptosystem on a computer network.

According to the above process of sharing a

cryptokey, it is important that the center algorithm should not easily be analyzed in order to keep ciphertexts secret.

While the above process of sharing a cryptokey offers the advantages described above, the secret private keys of respective entities, a cryptokey generated from the secret private keys, and communication data encrypted by the cryptokey thus generated all contain information regarding the center algorithm. Because the center algorithm is common to the entities, it is generally open to attack by a plurality of collaborating entities as described in "Performance of Linear Schemes for the Keypredistribution System /IEICE Technical Report on Information Security, May 20, 1988, pp. 29 - 32" by Matsumoto.

If entity names are used as identifiers, then since many similar names tend to occur, the identifiers are not well dispersed, i.e., the distribution of the identifiers is liable to be localized. Many of the secret private keys of the entities which are produced by applying the center algorithm to those identifiers tend to be analogous to each other. As a result, cryptographic communication data are subject to so-called differential attack.

Consequently, there has been a demand for increased security against various forms of attack against the above process of sharing a cryptokey.

It is therefore an object of the present invention to provide a method of sharing a cryptokey for increased security against various forms of attack while simplifying the

generation of a common cryptokey for cryptographic communications and a cryptosystem on a computer network.

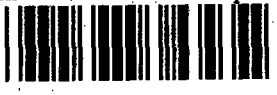
DISCLOSURE OF INVENTION

THIS SHEET HAS BEEN REPLACED

To achieve the above object, there is provided in accordance with a first aspect of the present invention a method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and the integral transformation algorithm to each of the entities, and when the entities communicate with each other, applying, in each of the entities, the integral transformation algorithm and the secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities.

Since the secret private key of each of the entities is generated in the center by transforming the identifier of each of the entities according to the center algorithm including the integral transformation algorithm, the data pro-

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

duced when the integral transformation algorithm is applied to the identifier are made highly dispersive even if the identifiers of the entities are not well dispersed. Consequently, the secret private keys are also made highly dispersive. Therefore, the secret private keys which are less analogous than heretofore are generated for the respective entities by the center, and distributed together with the integral transformation algorithm to the respective entities. For communications between entities, the integral transformation algorithm and the secret private key which are possessed by each of the entities are applied in each of the entities to the identifier of the other entity thereby to generate a common cryptokey. Since the secret private key of each entity contains elements based on the integral transformation algorithm, when not only the secret private key but also the integral transformation algorithm are applied to the identifier of the other entity, the common cryptokey which is common to the entities which are going to communicate with each other is generated by an algorithm portion (which is assumed to be symmetric as described above) of the center algorithm which precludes the integral transformation algorithm.

With the first aspect of the present invention, therefore, as the identifier of each entity is transformed by the center algorithm including the integral transformation algorithm for thereby generating the secret private key peculiar to each entity and used to generate a common

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

cryptokey for communications, the secret private keys of the entities are made highly dispersive, resulting in increased security against differential attack or the like.

For communications, only the identifier of the other entity with which to communicate is applied to the integral transformation algorithm and the secret private key which are owned by each entity for thereby generating a common cryptokey shared by the entities which are going to communicate with each other, without involving the center.

According to the first aspect of the present invention, a cryptosystem on the network is made highly secure against various forms of attack, such as differential attack, while simplifying the generation of a common cryptokey and the arrangement of the cryptosystem, and is also made simple and highly reliable.

The identifier may be the name, address, the mail address or domain name thereof on the network, or their combination of each entity insofar as it is peculiar to each entity and is public to at least to an entity with which to communicate.

The integral transformation algorithm may be a Fourier transformation (including a fast Fourier transformation), a Laplace transformation, a Miller transformation, a Hilbert transformation, or the like. While either one of these transformations may be used, these integral transformations are defined in a analytically infinite interval. Since the identifier to be transformed by the integral

This Sheet Has Been Replaced

THIS SHEET HAS BEEN REPLACED

transformation algorithm according to the first aspect of the present invention is expressed in a finite interval (e.g., a coset on a finite ring), when the data of the identifier is subjected to the integral transformation using a computer or the like, the transformed data tend to suffer anomalous dispersion (aliasing).

According to the first aspect of the present invention, therefore, the integral transformation algorithm preferably comprises a integral transformation algorithm with a weighting function. The aliasing can be prevented by adding such a weighting function when the identifier is subjected to the integral transformation. Since the weighting function may be established arbitrarily insofar as it is capable of preventing aliasing, the secret private key generated when the identifier is transformed by the center algorithm which includes the integral transformation algorithm with the weighting function contains unknown elements based on the weighting function. As a consequence, the security of the cryptosystem to which the first aspect of the present invention is applied is increased.

The weighting function thus added is basically established such that its value approaches "0" at ends of the interval of the data of the identifier. According to the first aspect of the present invention, the weighting function is determined in an unpredictable pattern by random number data generated in the center. More preferably, the random number data comprise one-time pass random number da-

This Sheet Has Been Replaced



ta. The weighting function is determined by the random number data by determining the manner in which the value of the weighting function varies in the interval of the data of the identifier, i.e., the manner in which the weighting function approaches "0" at the ends of the interval of the data of the identifier, using the random number data. The one-time pass random number data are random number data which are not reproducible or hardly reproducible. More specifically, the one-time pass random number data are random number data whose bit values appear at equal frequencies and which are not correlated. Such random number data can be generated based on the timing with which a phrase or a sentence is manually entered into a computer by a human operator.

With the weighting function thus determined in an unpredictable pattern, a person who attacks the cryptosystem finds it difficult to predict the weighting function. Therefore, the security of the cryptosystem to which the first aspect of the present invention is applied is increased. Particularly, if the weighting function is determined by the one-time pass random number data, the security of the cryptosystem is further increased as the reproducibility of the random number data is eliminated.

While the integral transformation algorithm may be of any of various forms, the integral transformation algorithm preferably comprises a Fourier transformation algorithm in the first aspect of the present invention. The Fourier transformation is an integral transformation which

can quickly and easily be carried out by a computer, and data transformed by the Fourier transformation generally tend to be dispersed. If a Fourier transformation algorithm is used as the integral transformation algorithm, then the secret private key can quickly and easily be generated from the identifier, and the secret private keys of the entities are effectively made highly dispersive for thereby increasing the security of the cryptosystem.

According to the first aspect of the present invention, furthermore, the method further comprises the steps of randomizing, in the center, the identifier transformed by the center algorithm, with one-time pass personal random number data which are peculiar and unknown to each of the entities, thereby to generate the secret private key, and distributing, from the center, an identifier transformation algorithm which comprises an algorithm for canceling out the elements of the randomization which are contained in said secret private key and said integral transformation algorithm together with said secret private key, to each of the entities, and when the entities communicate with each other, applying, in each of the entities, the identifier transformation algorithm and the secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate the common cryptokey, so that the entities will possess the common cryptokey shared by the entities.

The randomization or random transformation is carried out by modifying the values of the bits of a sequence

of data representing the identifier transformed by the center algorithm, with the one-time pass personal random number data, or rearranging the sequence of data, or both modifying the values of the bits of the sequence of data and rearranging the sequence of data.

Therefore, the secret private key contains elements due to the random transformation in addition to the center algorithm. Since the random transformation is effected using the one-time pass personal random number data (random number data which are not reproducible or hardly reproducible) which are peculiar and unknown to each entity, the secret private key of each entity contains accidental elements. As a result, the security of the cryptosystem against various forms of attack is further strengthened.

The secret private key to be applied to the identifier of the other entity contains elements due to the random transformation. Therefore, the identifier transformation algorithm which includes the algorithm for canceling out those elements and the integral transformation algorithm is distributed together with the secret private key to each entity. For communications, the identifier transformation algorithm and the secret private key are applied to the identifier of the other entity for thereby generating a common cryptokey shared by the entities which are going to communicate with each other.

The identifier transformed by the center algorithm is randomized by rearranging a sequence of data representing

the identifier transformed by the center algorithm, with the one-time pass personal random number data.

More preferably, the sequence of data contains a plurality of unnecessary bits, and the identifier transformed by the center algorithm is randomized by randomizing the values of the unnecessary bits with the one-time pass personal random number data and further rearranging the sequence of data, including the unnecessary bits, in its entirety.

Because the values of the unnecessary bits of the sequence of data which represents the identifier transformed by the center algorithm are randomized with the one-time pass personal random number data, and the sequence of data, including the unnecessary bits, is rearranged in its entirety, a person who attacks, i.e., attempts to analyze, the cryptosystem is unable to comprehend which part of the acquired data contains the unnecessary bits and which part of the acquired data contains necessary data. The cryptosystem is thus highly secure against such attack.

The one-time pass personal random number data are generated according to a given process of each of the entities, preferably, a manual data entering process, and the one-time pass personal random number data are generated based on the timing of the manual data entering process.

Inasmuch as the random number data are generated based on the timing with which a phrase or a sentence is manually entered into a computer by a human operator, the

generated random number data are not reproducible or hardly reproducible. The one-time pass personal random number data can thus appropriately be generated.

According to a second aspect of the present invention, there is provided a method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities, and then randomizing the transformed identifier with one-time pass personal random number data which are peculiar and unknown to each of the entities, and distributing, from the center, the secret private key and an identifier transformation algorithm which includes an algorithm for canceling out the elements of the randomization which are contained in the secret private key to each of the entities, and when the entities communicate with each other, applying, in each of the entities, the identifier transformation algorithm and the secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities.

Since the secret private key of each of the entities

is generated in the center by randomizing the identifier of each of the entities transformed according to the center algorithm (which contains a portion assumed to be symmetric as described above), with the one-time pass personal random number data (random number data that are not reproducible or hardly reproducible), the secret private key of each entity contains accidental elements. As a result, the cryptosystem to which the second aspect of the present invention is applied is made highly secure against various forms of attack. As with the first aspect of the present invention, the secret private key of each entity contains elements due to the random transformation. Therefore, the identifier transformation algorithm including an algorithm for canceling out those elements and the secret private key are distributed to each entity. For communications between entities, the identifier transformation algorithm and the secret private key are applied in each of the entities to the identifier of the other entity thereby to generate a common cryptokey shared by the entities, without involving the center.

According to the second aspect of the present invention, therefore, a cryptosystem on the network is made highly secure against various forms of attack, such as differential attack, while simplifying the generation of a common cryptokey and the arrangement of the cryptosystem, and is also made simple and highly reliable.

With the second aspect of the present invention, as with the first aspect of the present invention, the identifier

transformed by the center algorithm is randomized by rearranging a sequence of data representing the identifier transformed by the center algorithm, with the one-time pass personal random number data. More preferably, the sequence of data contains a plurality of unnecessary bits, and the identifier transformed by the center algorithm is randomized by randomizing the values of the unnecessary bits with the one-time pass personal random number data and further rearranging the sequence of data, including the unnecessary bits, in its entirety. The security of the cryptosystem to which the second aspect of the present invention is thus increased.

With the second aspect of the present invention, as with the first aspect of the present invention, furthermore, the one-time pass personal random number data are generated according to a given process of each of the entities. More specifically, the given process comprises a manual data entering process, and one-time pass personal random number data are generated based on the timing of the manual data entering process. The one-time pass personal random number data can thus appropriately be generated.

The above and other objects, features, and advantages of the present invention will become apparent from the following description when taken in conjunction with the accompanying drawings which illustrate a preferred embodiment of the present invention by way of example.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a block diagram of a cryptosystem to which a method of sharing a cryptokey according to the present invention is applied;

FIG. 2 is a block diagram showing the concept of a basic structure of the cryptosystem shown in FIG. 1;

FIG. 3 is a flowchart of an operation sequence of the cryptosystem shown in FIG. 1;

FIG. 4 is a flowchart showing details of a step 1 in the operation sequence shown in FIG. 3;

FIG. 5 is a flowchart showing details of a step 2 in the operation sequence shown in FIG. 3;

FIG. 6 is a flowchart showing details of steps 3 and 4 in the operation sequence shown in FIG. 3;

FIG. 7 is a flowchart showing details of steps 3 and 5 in the operation sequence shown in FIG. 3; and

FIG. 8 is a block diagram of a computer for carrying out the steps shown in FIGS. 6 and 7.

BEST MODE FOR CARRYING OUT THE INVENTION

A cryptosystem to which a method of sharing a cryptokey according to the present invention is applied will first be described below with reference to FIGS. 1 and 2.

As shown in FIG. 1, the cryptosystem includes a center or central facility 1, which is a basic main constituent of the system, a plurality of entities 2 which are subscribed to the cryptosystem for communication with each oth-

er, and a network 3 such as the Internet, a personal computer communication network, or the like through which the center 1 and the entities 2 are connected to communicate with each other. The center 1 and the entities 2 include computers such as personal computers for effecting actual communications and data processing and users of those computers.

In the cryptosystem on the network 3, as shown in FIG. 2, the entities 2 (represented by i, j, ・・・ in FIG. 2) have respective peculiar identifiers yi, yj, ・・・ (described in detail later on). If $i \neq j$, then $yi \neq yj$. The entities 2 (i, j, ・・・) have been given, by the center 1, respective secret private keys Xi, Xj, ・・・ (described in detail later on and hereinafter referred to as a "secret private key Xn" if necessary) which are peculiar to the respective entities 2 and generated by the center 1 based on the respective identifiers yi, yj, ・・・ (hereinafter referred to as an "identifier yn" if necessary). For cryptographic communications between any arbitrary entities i, j, a common cryptokey Kij for encrypting communication data (on the transmitting side) and decrypting communication data (on the receiving side) is generated for the entities i, j using the secrete private keys Xi, Xj of the entities i, j. Using the generated common cryptokey Kij, the encrypted communications are carried out between the entities i, j.

Prior to describing the cryptosystem in detail, the identifier yn will first be described below. In this em-

bodiment, the identifier yn of each entity 2 may comprise any attribute which is public and peculiar to each entity 2, e.g., the name, address, mail address or domain name on the network, or their combination of each entity 2. Actually, the center 1 and the computer of each entity 2 handle the identifier yn as vector data which have been encoded by a coset on a finite ring.

The cryptosystem for carrying out the above cryptographic communications will be described below in detail with reference to FIGS. 3 through 8.

As shown in FIG. 3, cryptographic communications are carried out between the entities i, j after the center 1 generates and distributes the secret private key Xn in a preparatory stage.

In the preparatory stage, the center 1 generates a center algorithm which serves as a basis for generating the secret private key Xn of each entity when the center 1 is established or the cryptosystem is updated (step 1).

In this embodiment, the center algorithm comprises a center matrix, a weighting function, and an integral transformation algorithm.

The integral transformation algorithm is an algorithm for producing an integral transform of the data of the identifier yn of each entity 2. In this embodiment, a Fourier transformation (more specifically, a fast Fourier transformation) is used as the integral transformation algorithm. Various Fourier transformations are known in the

art, and one of the Fourier transformations is selected by the center 1 to generate a Fourier transformation algorithm which is used in this embodiment. The Fourier transformation algorithm is actually expressed as a matrix to process the data of the identifier yn.

The weighting function serves to prevent anomalous dispersion (aliasing) in the Fourier transformation of the identifier yn, which is data in a finite interval. The weighting function is a function whose value approaches "0" at ends of the interval of the data of the identifier yn. The center matrix is a symmetric matrix, and more specifically, a nonsingular symmetric matrix.

The weighting function and the center matrix are generated using one-time pass random number data. Specifically, for generating the weighting function and the center matrix, as illustrated in FIG. 4, the center 1 generates random number data based on manual operation of the operator at the computer in the center 1 (step 1-1). More specifically, the operator enters a suitable phrase, sentence, or the like into the computer of the center 1, and the computer sequentially measures the timing of the entered data, i.e., times at which the respective words are entered or time intervals at which the respective words are entered. The computer then generates random number data in a time series based on the measured timing of the entered data. Since the random number data thus generated are based on the timing of the entered data depending on the manual operation which

contains elements of uncertainty, the random number data actually lack reproducibility and are accidental. Therefore, the random number data are one-time pass data.

After having generated one-time pass random number data, the center 1 determines the weighting function and the center matrix based on the generated one-time pass random number data (step 1-2). Specifically, the center 1 determines the weighting function by determining the manner in which the value of a weigthing function varies in the interval of the data of the identifier yn, i.e., the manner in which a weighting function approaches "0" at the ends of the interval of the data of the identifier yn, using the one-tim e pass random number data. The weighting function is thus determined in a pattern which is unpredictable. In reality, the weighting function is expressed as a diagonal matrix. The center 1 determines the center matrix by determining the values of elements of the matrix using the one-time pass random number data while keeping the matrix symmetric and nonsingular.

The center algorithm which comprises the center matrix, the weighting function, and the integral transformation algorithm thus generated is stored in secrecy in the center 1. Particularly, the center matrix and the weighting function are kept in strictly secure storage such that they cannot be referred to by third parties (including the entities 2) other than those specified by the center 1. The center algorithm is common to the entities 2.

Referring back to FIG. 3, when the entities 2 (i, j, · · ·) are subscribed to the cryptosystem, the center 1 generates a secret private key Xn peculiar to each of the entities 2 and an identifier transformation algorithm for generating a common cryptokey Kij using the center algorithm generated and stored in the center 1 as described above and the identifier yn of each of the entities 2, and distributes the secret private key Xn and the identifier transformation algorithm to each of the entities 2 (step 2).

Specifically, in the step 2, as shown in FIG. 5, the center 1 applies the Fourier transformation algorithm and the matrix of the weighting function to the data (vector data) of the identifier yn of each entity 2, thereby effecting a Fourier transformation with a weighting function on the identifier yn (step 2-1). Then, the center 1 multiplies the vector data produced in the step 2-1 by the center matrix (step 2-2). The data of the identifier yn are made redundant, so that the vector data produced in the step 2-2 contain a plurality of useful bits generated by applying the weighting function, the integral transformation algorithm, and the center matrix to a bit train significant as the data of the identifier yn, and a plurality of other unnecessary bits.

At the time the center 1 communicates with each entity 2, e.g., in a subscription process for the entity 2, the center 1 generates one-time pass personal random number data which are peculiar to the entity 2 and are not known to

the entity 2 (step 2-3). Specifically, in the same manner as when the center 1 has generated one-time pass random number data for determining the weighting function and the center matrix, the operator enters a suitable phrase, sentence, or the like from the computer of the entity 2, and the center 1 sequentially receives the entered data. The computer of the center 1 measures the timing of the entered data. The computer of the center 1 then generates personal random number data based on the measured timing of the entered data. As with the one-time pass random number data generated for determining the weighting function and the center matrix, the one-time pass personal random number data lack reproducibility and are accidental. Therefore, the personal random number data are peculiar to the entity 2 and are one-time pass data. Inasmuch as the timing of the manually entered data cannot accurately be controlled, the entity 2 is unable to know the personal random number data.

Then, the center 1 randomizes the respective values of the unnecessary bits of the vector data produced in the step 2-2, with the one-time pass personal random number data generated in the step 2-3 (step 2-4). Then, the center 1 randomly rearranges vector data, which are composed of the randomized unnecessary bits and the useful bits, i.e., changes the arrangement of the vector data, with the one-tim e pass personal random number data (step 2-5). In this manner, the center 1 randomizes the vector data (transformed

from the identifier yn by the center algorithm) generated in the step 2-2. The center 1 then uses the randomized vector data as the secret private key Xn of each of the entities 2. The above randomization or random transformation is expressed as a matrix (which may not necessarily be a symmetric matrix), and more particularly as a matrix whose transposed matrix and inverse matrix are equal to each other.

The center 1 generates the identifier transformation algorithm from the one-time pass personal random number data, the Fourier transformation algorithm, and the weighting function (step 2-6). The identifier transformation algorithm is generated by combining an algorithm (expressed as the inverse of the matrix which represents the random transformation) for canceling out the elements of the random transformation which are reflected in the secret private key Xn, the Fourier transformation algorithm, and the weighting function, i.e., by multiplying the matrixes representing the algorithm, the Fourier transformation algorithm, and the weighting function.

The secret private key Xn of each entity 2 and the identifier transformation algorithm, which are thus generated by the center 1, are distributed to each entity 2 through communications (see the step 2 in FIG. 3).

The details of the preparatory stage in the center 1 have been described above.

After having generated the secret private key Xn of each entity 2 and the identifier transformation algorithm,

the center 1 does not store, but deletes, the one-time pass personal random number data corresponding to each entity 2 and the matrix representing the random transformation. When each entity 2 receives the secret private key Xn and the identifier transformation algorithm, it stores them secretly in a suitable storage device of its own computer.

After the preparatory stage, a cryptographic communication process is carried out between any arbitrary entities 2 as described below. It is assumed that a cryptographic communication process is carried out between entities i, j ($i \neq j$) with the entity i as the transmitting entity and the entity j as the receiving entity.

In the cryptographic communication process, the transmitting entity i generates a common cryptokey Kij shared by itself and the receiving entity j from the secret private key Xi and the identifier transformation algorithm which are held by the transmitting entity i and the identifier yj of the receiving entity j (step 3).

Specifically, as shown in FIG. 6, the transmitting entity i applies the identifier transformation algorithm of the entity i on the computer of the entity i to the identifier yj of the receiving entity j, i.e., multiplies the vector data of the identifier yj by the matrix of the identifier transformation algorithm (step 3-1). Then, the transmitting entity i calculates an inner product of the vector data generated in the step 3-1 and the secret private key Xi (vector data) of the transmitting entity i (step 3-2), gen-

erating a common cryptokey Kij which is common to the transmitting entity i and the receiving entity j.

Similarly, as shown in FIG. 7, the receiving entity j applies the identifier transformation algorithm of the entity j on the computer of the entity j to the identifier yi of the transmitting entity i (step 3-1), and then calculates an inner product of the vector data generated in the step 3-1 and the secret private key Xj of the receiving entity j (step 3-2), generating a common cryptokey Kji which common to the receiving entity j and the transmitting entity i.

The common cryptokey Kij independently generated by the transmitting entity i and the common cryptokey Kji independently generated by the receiving entity j are the same as each other.

Specifically, the secret private keys Xi, Xj held respectively by the transmitting and receiving entities i, j are vector data produced by applying the Fourier transformation algorithm with a weighting function, the center matrix, and the randomization to the identifiers yi, yj of the respective entities i, j, and the identifier transformation algorithm which is applied to the identifiers yj, yi of the respective other entities j, i for the entities i, j to generate the common cryptokeys Kij, Kji is produced by combining the Fourier transformation algorithm with a weighting function and the algorithm for canceling out the elements of the random transformation for each of the entities i, j, which are reflected in the secret private keys Xi, Xj.

Therefore, when the inner product is calculated in the step 3-2, the effect of the random transformation for each of the entities i, j is eliminated, and the common cryptokeys Kij, Kji obtained as a result of the calculations to produce the inner product are equal to inner products of vector data which are generated by applying the Fourier transformation algorithm with a weighting function and further the center matrix to the identifiers yi, yj of the respective entities i, j and vector data which are generated by applying the Fourier transformation algorithm with a weighting function to the identifiers yj, yi of the respective other entities j, i. Stated otherwise, if it is assumed that the vector data generated by applying the Fourier transformation algorithm with a weighting function to the identifiers yi, yj are represented by yi', yi' (yi', yj' are column vectors) and the center matrix by C, then the common cryptokeys Kij, Kji are expressed respectively by $Kij = (yj')^T \cdot C \cdot yi'$, $Kji = (yi')^T \cdot C \cdot yj'$ where T represents transpose.

Since the center matrix C is a symmetric matrix, the common cryptokeys Kij, Kji are obviously equal to each other (Kij = Kji). Therefore, the common cryptokeys Kij, Kji which are separately generated by the respective entities i, j coincide with each other, so that the entities i, j can share the common cryptokey.

After having generated the common cryptokey Kij which is common to the transmitting and receiving entities

i, j in the step 3 in FIG. 3, the transmitting entity i generates an encrypted communication text from the common cryptokey Kij and a plaintext (sentences, a program, etc.) to be transmitted to the receiving entity j (step 4). For generating the encrypted communication text, the transmitting entity i uses the common cryptokey Kij and one-time pass random number data.

Specifically, for generating a ciphertext, as shown in FIG. 6, the transmitting entity i generates one-time pass random number data (hereinafter referred to as "cryptographic communication random number data") based on the timing of entered data, i.e., times or time intervals at which words of a phrase or sentence are manually entered into the computer of the transmitting entity i, (step 4-1). Then, the transmitting entity i encrypts the one-time pass cryptographic communication random number data using the common cryptokey Kij as an intrinsic key (step 4-2). This encryption process is carried out according to a three-stage DES (Data Encryption Standard), for example.

The transmitting entity i also encrypts a plaintext using the one-time pass cryptographic communication random number data (prior to being encrypted) generated in the step 4-1, as a key (step 4-3). This encryption process is carried out according to a three-stage DES, for example, as is the case with the encryption process in the step 4-2.

The encrypted random number data generated in the step 4-2 and the encrypted plaintext generated in the step

4-3 are combined into one set, thereby generating an encrypted communication text to be transmitted to the receiving entity j. The encrypted communication text thus generated is thereafter transmitted from the computer of the entity i to the computer of the entity j.

The cryptographic communication random number data should preferably be generated and updated each time an cryptographic communication process is carried out. However, the cryptographic communication random number data may be updated each time several cryptographic communication processes are carried out, i.e., the same cryptographic communication random number data are used in the several cryptographic communication processes.

After having received the encrypted communication text, the receiving entity j decrypts the encrypted communication text using the common cryptokey Kji (= Kij) which is common to the entities i, j for finally producing the plaintext (step 5 in FIG. 7).

Specifically, as shown in FIG. 7, the receiving entity j uses the common cryptokey Kji (= Kij) as an intrinsic key to decrypt the encrypted random number data of the received encrypted communication text into encrypted communication random number data (step 5-1). Then, using the decrypted cryptographic communication random number data as a key, the receiving entity j decrypts the ciphertext of the encrypted communication text back into the plaintext (step 5-2). The receiving entity j can finally comprehend the

contents of the plaintext from the transmitting entity i. The cryptographic communication process between the entities i, j is now completed.

The computer of each of the entities 2 for carrying out the above processing for cryptographic communications is shown in block form in FIG. 8.

As shown in FIG. 8, the computer of each of the entities 2 comprises a keyboard 4, a main unit 5 made up of a CPU, a RAM, a ROM, etc., and a data base 6 comprising a hard disk or the like for storing the secret private key Xn, the identifier transformation algorithm, plaintexts such as sentences, programs, etc., and encrypted communication texts. The main unit 5 comprises as its functions a common key generator 7 for generating a common key, an encrypting and decrypting processor 8 for encrypting and decrypting communication data, a random number generator 9 for generating cryptographic communication random number data, and a data storage memory 10 for storing a common cryptokey generated by the common key generator 7 and data such as cryptographic communication random number data generated by the random number generator 9.

The computer of each of the entities 2 operates to carry out the above process of cryptographic communications as follows:

For generating a common cryptokey (the step 3), the secret private key Xn and the identifier transformation algorithm which are to be used are indicated from the keyboard

4 to the main unit 5 of the computer of each of the transmitting and receiving entities. The secret private key Xn and the identifier transformation algorithm which have been indicated are read from the database 6 to the common key generator 7 in the main unit 5. The identifier yn of the other entity with which to communicate is entered from the keyboard 4 into the main unit 5. The common key generator 7 applies the identifier transformation algorithm and the secret private key Xn to the data of the entered identifier yn, generating a common cryptokey (the steps 3-1, 3-2). The generated common cryptokey is then stored in the data storage memory 10.

In the computer of the transmitting entity, data (entered data of a phrase, a sentence, or the like) for generating cryptographic communication random number data are entered from the keyboard 4 into the main unit 5. Based on the entered data, the random number generator 9 generates one-time pass cryptographic communication random number data (the step 4-1) and stores the generated cryptographic communication random number data in the data storage memory 10.

In the computer of the transmitting entity, a plaintext to be transmitted in the database 6 is indicated by the keyboard 4 to the main unit 5, and the indicated plaintext is read from the database 6 to the encrypting and decrypting processor 8. The encrypting and decrypting processor 8 encrypts the cryptographic communication random number data stored in the data storage memory 10 using the

common cryptokey stored in the data storage memory 10 (the step 4-2), and also encrypts the plaintext using the cryptographic communication random number data as a key (the step 4-3). The encrypted random number data and the encrypted plaintext or ciphertext are held as an encrypted communication text in the database 6, and thereafter transmitted to the computer of the receiving entity.

In the computer of the receiving entity, the received encrypted communication text is held in the database 6, and then read to the encrypting and decrypting processor 8. The encrypting and decrypting processor 8 decrypts the encrypted random number data in the encrypted communication text back to the cryptographic communication random number data using the common cryptokey stored in the data storage memory 10 (the step 5-1), and also decrypts the encrypted plaintext in the encrypted communication text back to the original plaintext using the decrypted cryptographic communication random number data as a key (the step 5-2). The plaintext thus decrypted by the encrypting and decrypting processor 8 is held in the database 6.

As described above, in the cryptosystem according to the present invention, when the secret private key Xn of each entity 2 is generated in the preparatory stage by the center 1, the identifier yn, such as a name, of the entity 2 is subjected to a Fourier transformation as the integral transformation. Therefore, even if many of the identifiers yn of the respective entities are analogous each other, data

produced when those identifiers yn are subjected to the Fourier transformation are well dispersed, and hence the secret private keys Xn generated when those data are subjected to the center matrix are also highly dispersed. As a consequence, the center algorithm comprising the center matrix, etc. of the center 1 is made difficult to analyze even under the so-called differential attack.

The integral transformation may be a Laplace transformation, a Miller transformation, a Hilbert transformation, or the like, other than the Fourier transformation. However, the Fourier transformation (more specifically, the fast Fourier transformation) used as the integral transformation in the illustrated embodiment is effective to make the secret private keys Xn highly dispersive, and also to process the identifiers yn at high speed with the computer.

Since the weighting function is added in the center algorithm for generating the secret private key Xn, the data produced when the data of the identifier yn in the finite interval are subjected to the Fourier transformation are prevented from being abnormally dispersed. Furthermore, because the weighting function is added as an unknown algorithm element, in addition to the center matrix and the Fourier transformation algorithm, in the center algorithm for an unauthorized person who attempts to attack the center algorithm, it is highly difficult for such a person to analyze the center algorithm. The center algorithm remains highly difficult to analyze in view of the fact that the

weighting function is generated in an unpredictable form using one-time pass random number data.

For generating the secret private key Xn, the identifier data are subjected to the center algorithm and also the randomization or random transformation based on one-time pass random number data peculiar to each entity 2. Consequently, the secret private key Xn of each entity 2 contains elements peculiar to each entity 2 and based on the random transformation which is not correlated to the random transformation for the other entities 2. Therefore, even when a plurality of entities 2 collaborate with each other in an attempt to analyze the center algorithm from the secret private keys Xn which are possessed by the respective collaborating entities 2, those entities 2 will find it extremely difficult to analyze the center algorithm. In the random transformation, the values of unnecessary bits of the data produced after the data of the identifier yn have been subjected to the Fourier transformation, the weighting function, and the center matrix are randomized by the one-time pass random number data, and then the randomized unnecessary bits and the useful bits are rearranged. It is very difficult for any attacking person to analyze the center algorithm because such a person is unable to recognize which part of the data of the secret private key Xn contains those what corresponding to unnecessary bits. In addition, in order for an unauthorized cryptanalyst to break the cryptosystem completely, the unauthorized cryptanalyst has

to analyze the four algorithms, i.e., the center matrix, the weighting function, the Fourier transformation (integral transformation), and the random transformation, based on the data of the secret private key Xn, etc. Actually, it is impossible to analyze all the four algorithms.

For generating a common cryptokey for cryptographic communications in the cryptosystem, the identifier transformation algorithm including an algorithm for canceling out the elements of the random transformation which are reflected in the secret private key Xn has to be distributed, together with the secret private key Xn, to each entity 2. However, since the identifier transformation algorithm is a combination of the algorithm for canceling out the elements of the random transformation, the Fourier transformation algorithm, and the weighting function, it is also difficult to individually analyze the algorithm of the random transformation, the weighting function, and the Fourier transformation algorithm of the center algorithm of the center 1 from the identifier transformation algorithm.

Consequently, it is practically impossible to analyze the center algorithm of the center 1, which is most important for the security of the cryptosystem, from the secret private key Xn, etc. of each entity 2.

For carrying out cryptographic communications between any arbitrary entities i, j, a plaintext is not directly encrypted using the common cryptokey Kij, but is encrypted using, as a key, one-time pass cryptographic commu-

nication random number data having no localized features, and the cryptographic communication random number data as a key for decrypting the encrypted plaintext or a ciphertext are encrypted using the common cryptokey Kij. Therefore, even if a third party intercepts an encrypted communication text, the third party finds it difficult to analyze the common cryptokey Kij based on the encrypted communication text. Inasmuch as it is difficult to analyze the common cryptokey Kij, it is also difficult for the third party to acquire the information of the secret private key Xn of each entity 2 which is contained in the common cryptokey Kij and the information of the center algorithm which is contained in the secret private key Xn. The security of the plaintext is maintained as it is encrypted using the cryptographic communication random number data as a key.

The cryptosystem is therefore highly secure against various forms of attack. In cryptographic communications between any arbitrary entities i, j, the entities i, j can generate and share a common cryptokey Kij simply by applying their own secret private keys Xi, Xj and the identifier transformation algorithm to the other entityls identifiers yj, yi, without involving the center 1 and requiring previous communication between the entities i, j. Accordingly, the cryptosystem is simple and highly versatile as well as highly secure. The idea that the identifier yn plays an important role in generating the common cryptokey Kij as described above is similar to the concept disclosed in "Iden-

tity-Based Cryptosystems and Signature Schemes/Advances in Cryptography: Proceeding of CRYPTO '84/Springer LNCS 196, 1985, pp. 47 - 53" by A. Shamir.

The effectiveness of the cryptosystem to which the method according to the present invention is applied discussed from a more theoretical standpoint will be described below.

In the cryptosystem, the secrete private key of each entity 2 is generated and a common cryptokey is generated according to a linear transformation or scheme. Such a linear transformation will be described below.

It is assumed that Xif represents the secret private key of an entity i for the generation of a common cryptokey shared by f entities 2. According to a general concept for constructing the above linear scheme, an f-input symmetric transformation g (which is a symmetric function having f variables) is arbitrarily selected, and the secret private key Xif of the entity i is determined as an f-1-input transformation which satisfies an equation: $Xif(\xi_1, \cdots, \xi_{f-1}) = g(yi, \xi_1, \cdots, \xi_{f-1})$ with respect to the identifier yi of the entity i where ξ is a variable representing an arbitrary identifier. The linear transformation can be found so that the kernel of the f-input symmetric transformation g is in accord with a multilinear map (an f-linear map), and is basically defined in a vector space on a Galois field and generalized as a cost on a ring.

The cryptosystem is based on the assumption that f =

2, and the above linear transformation is defined as follows:

It is assumed that the set of entities belonging to the center 1 is represented by E, the set of the identifiers of the entities by I, and the set of common cryptokeys by K (see FIG. 1), and that Q represents a commutative ring having a unit element, J a coset of an order m over the commutative ring Q, and K a coset of a higher order h over the commutative ring Q, the cosets J, K having elements as m- and h-column vectors, respectively. If the commutative ring Q is a field, then the cosets J, K are vector spaces having respective dimensions m, h. The order m is equal to the total number of identifiers.

It is also assumed that R represents a linear transformation for injective mapping from the coset I to the coset J, and will hereinafter be referred to as an "identity transformation". The identity transformation basically corresponds to the Fourier transformation with a weighting function (integral transformation) effected on the identifier data, and can further be expanded so as to include the random transformation, as described later on.

Based on the above assumptions, first, a symmetric Qth multilinear mapping (2-input symmetric transformation) $g: J_2 \rightarrow K$ from J_2 (a set of pairs of two elements of the coset J) to the set K of common cryptokeys is arbitrarily selected and determined. The symmetric Qth multilinear mapping g is equivalent to a transformation from any two arbi-

trary identity-transformed identifiers to a common cryptokey corresponding to the two arbitrary identity-transformed identifiers.

For a given identifier yi ($\in$ I), a matrix xi having h rows and m columns over the commutative ring Q is determined to satisfy the equation: $xi \cdot \eta = g(R(yi), \eta)$ where η represents an arbitrary m-column vector and is an element of the coset J.

Moreover, for the given identifier yi ($\in$ I), a 1-input transformation $Xi(\xi)$ is formed to satisfy the equation: $Xi(\xi) = xi \cdot R(\xi)$ where ξ is an arbitrary element of the set I.

The 1-input transformation $Xi(\xi)$ is a secret private key for the entity i, and is expressed by the following equation:

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

where a 1-input transformation Vi is defined as $Vi(\eta) = xi \cdot \eta$ using the above matrix xi.

If there are a plurality of centers, then "xi" in the equation $Vi(\eta) = xi \cdot \eta$ is replaced with the summation of the matrix xi determined as described above for each of the centers.

With the secret private key Xi thus defined, as can easily be seen from the above description, the equation: Xa(yb) = Xb(ya) is satisfied for any arbitrary entities a, b $\in$ E, i.e., a common cryptokey Xa(yb) = Xb(ya) is obtained when the entities a, b enter the otherIs identifiers yb, ya

into their own secret private keys Xa, Xb.

Even if a multivariate polynomial is selected instead of the multilinear mapping g, such a multivariate polynomial is covered by the linear transformation of the present cryptosystem for the reasons that any arbitrary polynomial can be rewritten as a linear polynomial by an appropriate transformation of a set of unknowns and such a transformation can be absorbed in the identity transformation R. Moreover, some transformations are interpreted as a composition of a linear transformation and an operation such as an exponential function.

The performance of the linear transformation of the present cryptosystem and the role of the identity transformation R will be described below.

It is assumed that for an arbitrary transformation A, Cd(A) and Ce(A) represent the complexity of a description of the transformation A and the complexity of an evaluation of the transformation A, respectively. At this time, the above transformations Xi, R, Vi satisfy the following equation and inequality:

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

$$Ce(Xi) \leqq Ce(R) + Ce(Vi).$$

If the input (identifier) of the transformation Xi which represents a secret private key is described by w [bit], then the complexity Cd(Vi) of a description of the transformation Vi is expressed by:

$$Cd(Vi) = h \cdot m \cdot w[bit].$$

The complexity Ce(Vi) of an evaluation of the transformation Vi is expressed by:

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

where $O(h \cdot m)$ [Q-operation] signifies an $h \cdot m$ order on the commutative ring Q and its value can be evaluated substantially by $O(w^2)$ [bit transformation], i.e., a w^2 order. When a small commutative ring Q (e.g., a Galois field GF[2]) is selected, the complexity Ce(Vi) is low in level.

Therefore, the complexity Cd(Xi) of a description of the transformation Xi and the complexity Ce(Xi) of an evaluation of the transformation Xi are largely due to the complexity Cd(R) of a description of the identity transformation R and the complexity Ce(R) of an evaluation of the transformation R.

A case in which one or more entities j attempting to break the cryptosystem use their secret private keys Xj will be described below.

Obviously, to break the cryptosystem completely means to determine the above multilinear mapping $g: J_2 \rightarrow K$. For breaking the cryptosystem completely, it is necessary that the center collaborate with the entity or entities or as many entities as the order of the multilinear mapping g (which is approximately equal to the total number m (= order of J) of identifiers) collaborate with each other. However, such a collaboration is impossible to achieve practically.

The possibility of determining a secret private key Xi of an entity i by some entities j will be discussed be-

low. For this problem, the identity transformation R plays an important role as described below.

First, it can easily be derived that the statement "even if all entities j of a subset B of an entire set E of entities collaborate and the entities $j \in B$ use the whole $\{Xj | j \in B\}$ of their respective secret private keys Xj, they cannot obtain any useful information to determine a secret private key Xi of an arbitrary entity i in the set E - B" is equivalent to the statement "for each entity i in the set E - B, an identity transformation R(yi) is linearly independent of the whole $\{R(yj) | j \in B\}$ of respective identity transformations R(yj) of the entities j in the subset B". Consequently, the security of the linear transformation of the present cryptosystem in terms of the information theory is reduced to the linear dependency of an arbitrary subset U of the set $\{R(yi) | i \in E\}$. Therefore, there is a strong relationship between linear transformations and linear-algebraic combinations. For evaluating the security of a linear transformation, it is important to consider a linear code $LR = \{z \in Q^n | H \cdot z = 0\}$ defined by a parity check matrix $H = (R(y1), \cdots, R(yn))$ with m rows and n columns (n = #E = e: the total number of entities E), i.e., a set of codewords z expressed by an n-column vector over the commutative ring Q, the product of the n-column vector and the parity check matrix H being zero. It can easily be derived that the existence of a codeword z ($\in$ LR) of Hamming weights s is equivalent to the fact that the secret private key Xi of a cer-

tain entity i can be derived by the collaboration of s-1 entities j.

Personalizing the identity transformation R, i.e., making the identity transformation R peculiar to each entity, renders the cryptosystem resistant to attempts to break the cryptosystem even with the collaboration of many entities. Specifically, if the identity transformation R(yi) of an entity i is linearly dependent on the set $\{R(yj) | j \in B\}$ of identity transformations R(yj) of respective entities j ($j \in B$) trying to break the cryptosystem and $R(yi) = \Sigma Cj \cdot R(yj)$ where Cj is a suitable coefficient, then, as can be seen from the above definition of secret private keys, the secret private key Xi of the entity i and the secret private keys Xj of the entities j ($j \in B$) satisfy the equation: $Xi = \Sigma Cj \cdot Xj$. Therefore, the set B of entities j trying to break the cryptosystem can easily know the secret private key Xi of the other entity i. However, when the identity transformation R is personalized, it is made peculiar to each entity, making it difficult for the set B of given entities j to find an entity i having an identifier yi capable of analyzing another secret private key Xi. Stated otherwise, the entities j of the set B are unable to comprehend which entityIs secret private key Xi can be analyzed from the information of the secrete private keys Xj, etc. possessed by those entities j. Conversely, it is also difficult for an entity i having a given identifier yi to find a set B containing an identifier yj capable of analyzing its

secret private key Xi. Therefore, even when an entity i having a secret private key Xi to be analyzed is identified, it is unable to recognize which entities may collaborate with each other to analyze the secret private key Xi. Thus, it is of essential importance to personalize the identity transformation R for the purpose of increasing the complexity and theoretical security of the cryptosystem.

Various linear transformations can be selected for personalization of the identity transformation R. Basically, techniques for personalizing the identity transformation R are roughly classified into two categories.

In one of the categories, an identity transformation R which corresponds to a linear code LR that is a well known algebraic or analytic geometric code is used. In the other class, the identity transformation R is personally randomized for each entity.

According to the former process, if the total number m of identifiers is increased for security, then the amount of necessary data tends to be enormous. For example, it is assumed that Q = GF(q): Galois field with a primitive element of α, h = 1, β is the ξth power of α ($\log\beta = \xi \cdot \log\alpha$), and $R(\xi) = [1, \beta, \beta^2, \cdots \beta^{m-1}]^T$, and I is encoded as {0, 1, 2, · · ·, n-1}. Since this identity transformation R is not unidirectional, it is not a strict linear transformation. However, the identity transformation R corresponds to a linear transformation proposed in the previously mentioned article "An Optimal Class of Symmetric Key

Generation Systems" by R. Blom. The linear code LR corresponds to the Reed-Solomon code. In this category, it is necessary that the total number n of entities in the network be smaller than "q" in the Galois field Q = GF(q). If this category is applied when $n = 10^{12}$, then the minimum Q is GF (2^{40}), requiring a very large amount of data.

The latter process in which the identity transformation R is randomized for each entity is a process which has been realized by the random transformation in the above embodiment. According to this process, even if the total number m of identifiers (which is equal to the total number n of entities in the present cryptosystem), there exist a number of identity transformations R which can be processed at high speed with a small amount of data.

According to a process similar to the process of deriving the well-known asymptotic Varshamov-Gilbert bound, the following relation corresponding to the asymptotic Varshamov-Gilbert bound is obtained:

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

where $r = m \cdot \log_q(q-1)$, Φ is a function defined by

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

In the above inequality, "b" represents the total number (= #B) of entities j attempting to break the cryptosystem.

The above inequality determines a limit for the total number b of entities j required to break the cryptosystem. The number b of entities which does not satisfy the above inequality indicates that the cryptosystem

cannot be broken.

It is derived from the above inequality that with respect to arbitrary numbers m, b, even if at most b entities j collaborate with each other, there exist identity transformations R preventing the entities j from analyzing the secret private key Xi of another entity i. It can also be seen that the personal randomization of the identity transformation R results in a linearly independent structure while satisfying the above condition in many cases.

Therefore, the present cryptosystem is made highly secure by the personal randomization of the identity transformation R. Stated otherwise, the personal randomization of the identity transformation R increases the complexity Cd(R) of a description of the identity transformation R and the complexity Ce(R) of an evaluation of the transformation R, and also the complexity Cd(Xi) of a description of the transformation Xi and the complexity Ce(Xi) of an evaluation of the transformation Xi, thereby keeping the cryptosystem highly secure.

In reality, if Q = GF[2], m = 8192, and h = 64, then Cd(Xi) = 64 [Kbytes]. In this case, it is possible to effect cryptographic communications between two arbitrary entities in the cryptosystem including up to 10120 entities at maximum, using a common cryptokey of 160 bits. If a 32-bit CPU and 640-Kbyte memory are used at a clock of 200 MHz, then each secret private key can be calculated within 20 ms. This cryptosystem cannot be broken completely unless 8192

entities collaborate with each other. Because of personal randomization for each entity, unless at least 256 entities collaborate with each other, any information of the secret private key of another entity cannot be obtained.

In the above embodiment, the center matrix is established in addition to the weighting function and the Fourier transformation algorithm. However, the weighting function itself can be used as the center algorithm.

While the Fourier transformation is used as the integral transformation in the above embodiment, any of various other integral transformations such as a Laplace transformation, a Miller transformation, a Hilbert transformation, or the like may be used.

INDUSTRIAL APPLICABILITY

This invention is useful as a simple and secure ciphertext communication method with the common cryptokey system on a network such as the Internet, a personal computer communication network, etc.

THIS SHEET HAS BEEN REPLACED

This Sheet Has Been Replaced



CLAIMS

1. A method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of:

generating, in said center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by said center only and common to the entities and which includes at least an integral transformation algorithm, and distributing, from the center, the secret private key and said integral transformation algorithm to each of the entities; and

when the entities communicate with each other, applying, in each of the entities, said integral transformation algorithm and said secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities.

2. A method according to claim 1, wherein said integral transformation algorithm comprises an integral transformation algorithm with a weighting function.

3. A method according to claim 2, wherein said



This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED

weighting function is determined in an unpredictable pattern by random number data generated in said center.

4. A method according to claim 3, wherein said random number data comprise one-time pass random number data.

5. A method according to claim 1 or 2, wherein said integral transformation algorithm comprises a Fourier transformation algorithm.

6. A method according to claim 1, further comprising the steps of:

randomizing, in said center, the identifier transformed by said center algorithm, with one-time pass personal random number data which are peculiar and unknown to each of the entities, thereby to generate said secret private key, and distributing, from said center, an identifier transformation algorithm which comprises an algorithm for canceling out the elements of the randomization which are contained in said secret private key and said integral transformation algorithm together with said secret private key, to each of the entities; and

when the entities communicate with each other, applying, in each of the entities, said identifier transformation algorithm and said secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate said common cryptokey, so that



the entities will possess the common cryptokey shared by the entities.

7. A method according to claim 6, wherein said identifier transformed by said center algorithm is randomized by rearranging a sequence of data representing the identifier transformed by said center algorithm, with said one-time pass personal random number data.

8. A method according to claim 7, wherein said sequence of data contains a plurality of unnecessary bits, and said identifier transformed by said center algorithm is randomized by randomizing the values of said unnecessary bits with said one-time pass personal random number data and further rearranging the sequence of data, including said unnecessary bits, in its entirety.

9. A method according to claim 6, wherein said one-time pass personal random number data are generated according to a given process of each of the entities.

10. A method according to claim 9, wherein said given process comprises a manual data entering process, and said one-time pass personal random number data are generated based on the timing of said manual data entering process.

11. A method of sharing a common cryptokey for



encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of:

generating, in said center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by said center only and common to the entities, and then randomizing the transformed identifier with one-time pass personal random number data which are peculiar and unknown to each of the entities, and distributing, from the center, the secret private key and an identifier transformation algorithm which includes an algorithm for canceling out the elements of the randomization which are contained in said secret private key to each of the entities; and

when the entities communicate with each other, applying, in each of the entities, said identifier transformation algorithm and said secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities.

12. A method according to claim 11, wherein said identifier transformed by said center algorithm is randomized by rearranging a sequence of data representing the identifier transformed by said center algorithm, with said



one-time pass personal random number data.

13. A method according to claim 12, wherein said sequence of data contains a plurality of unnecessary bits, and said identifier transformed by said center algorithm is randomized by randomizing the values of said unnecessary bits with said one-time pass personal random number data and further rearranging the sequence of data, including said unnecessary bits, in its entirety.

14. A method according to claim 11, wherein said one-time pass personal random number data are generated according to a given process of each of the entities.

15. A method according to claim 14, wherein said given process comprises a manual data entering process, and said one-time pass personal random number data are generated based on the timing of said manual data entering process.



ABSTRACT

In a center, a Fourier transformation with a weighting function and a center matrix are applied to the identifier of each entity (steps 2-1, 2-2), which is then randomized by one-time pass random number data generated by a manual operation at each entity, thereby generating a secret private key peculiar to each entity (steps 2-3 ~ 2-5). The center also generates an identifier transformation algorithm based on the one-time pass random number data and the Fourier transformation with a weighting function (step 2-6). Thereafter, the center distributes the identifier transformation algorithm and the secret private key to each entity. Each entity applies the identifier transformation algorithm and the secret private key to the identifier of another entity with which to communicate, for thereby generating a common cryptokey for cryptographic communications between the entities.

FIG. 1

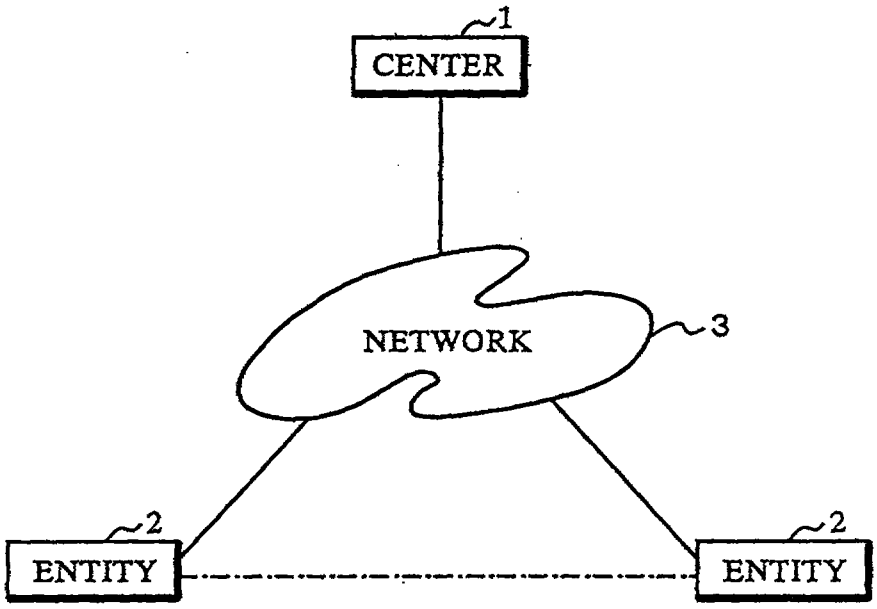


FIG. 2

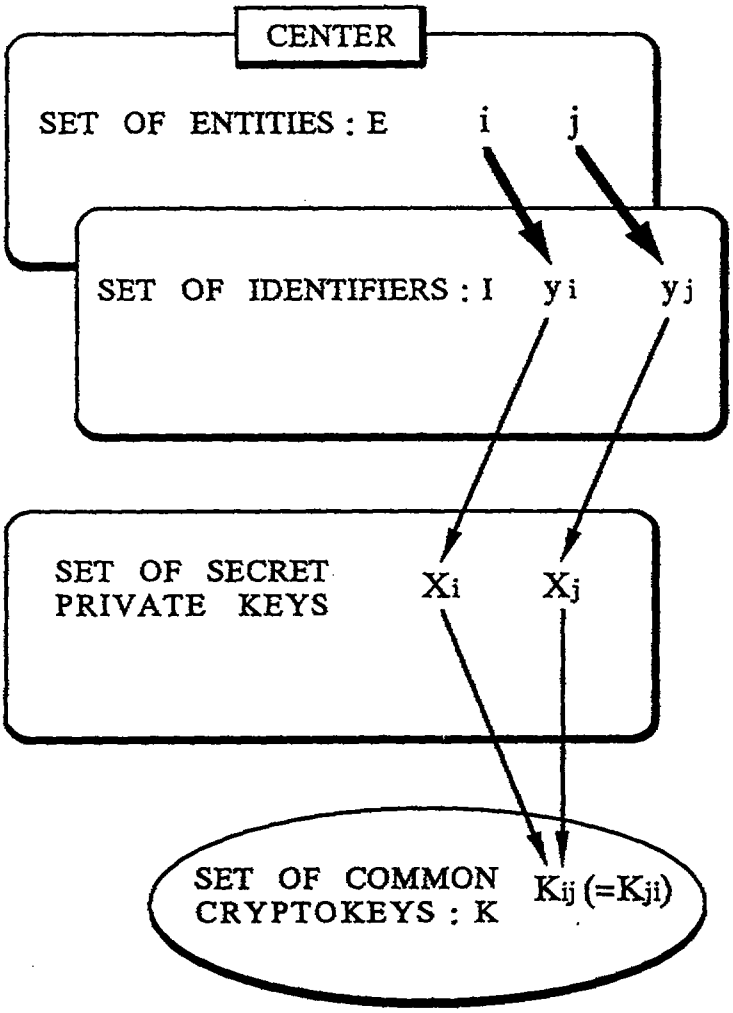

CENTER
SET OF ENTITIES : E
i
j
SET OF IDENTIFIERS : I
yi
yj
SET OF SECRET PRIVATE KEYS
Xi
Xj
SET OF COMMON CRYPTOKEYS : K
Kij (=Kji)

FIG. 3

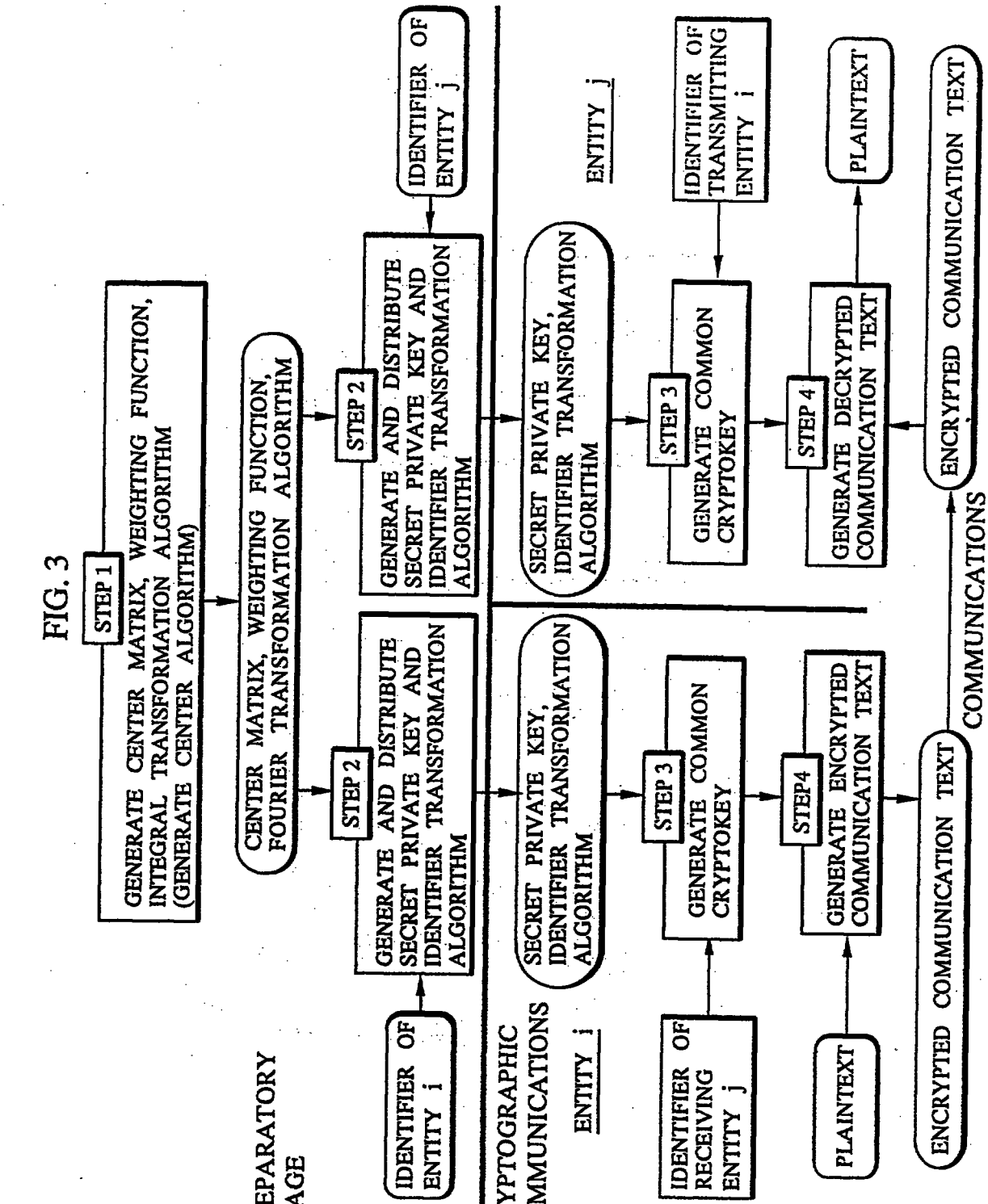

PREPARATORY STAGE
STEP 1
GENERATE CENTER MATRIX, WEIGHTING FUNCTION, INTEGRAL TRANSFORMATION ALGORITHM (GENERATE CENTER ALGORITHM)
CENTER MATRIX, WEIGHTING FUNCTION, FOURIER TRANSFORMATION ALGORITHM
STEP 2
GENERATE AND DISTRIBUTE SECRET PRIVATE KEY AND IDENTIFIER TRANSFORMATION ALGORITHM
IDENTIFIER OF ENTITY j
IDENTIFIER OF ENTITY i
CRYPTOGRAPHIC COMMUNICATIONS
ENTITY i
SECRET PRIVATE KEY, IDENTIFIER TRANSFORMATION ALGORITHM
STEP 3
GENERATE COMMON CRYPTOKEY
IDENTIFIER OF RECEIVING ENTITY j
STEP4
GENERATE ENCRYPTED COMMUNICATION TEXT
PLAINTEXT
ENCRYPTED COMMUNICATION TEXT
COMMUNICATIONS
ENTITY j
SECRET PRIVATE KEY, IDENTIFIER TRANSFORMATION ALGORITHM
STEP 3
GENERATE COMMON CRYPTOKEY
IDENTIFIER OF TRANSMITTING ENTITY i
STEP 4
GENERATE DECRYPTED COMMUNICATION TEXT
PLAINTEXT
ENCRYPTED COMMUNICATION TEXT

FIG. 4

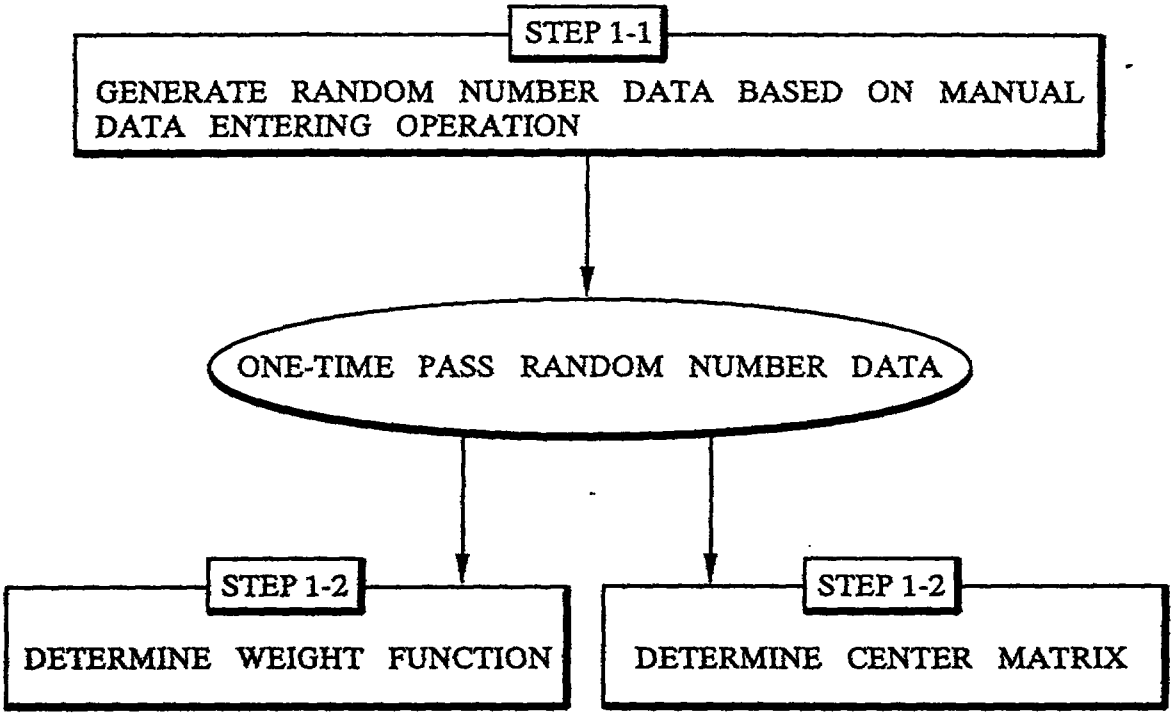

STEP 1-1
GENERATE RANDOM NUMBER DATA BASED ON MANUAL DATA ENTERING OPERATION
ONE-TIME PASS RANDOM NUMBER DATA
STEP 1-2
DETERMINE WEIGHT FUNCTION
STEP 1-2
DETERMINE CENTER MATRIX

FIG. 5

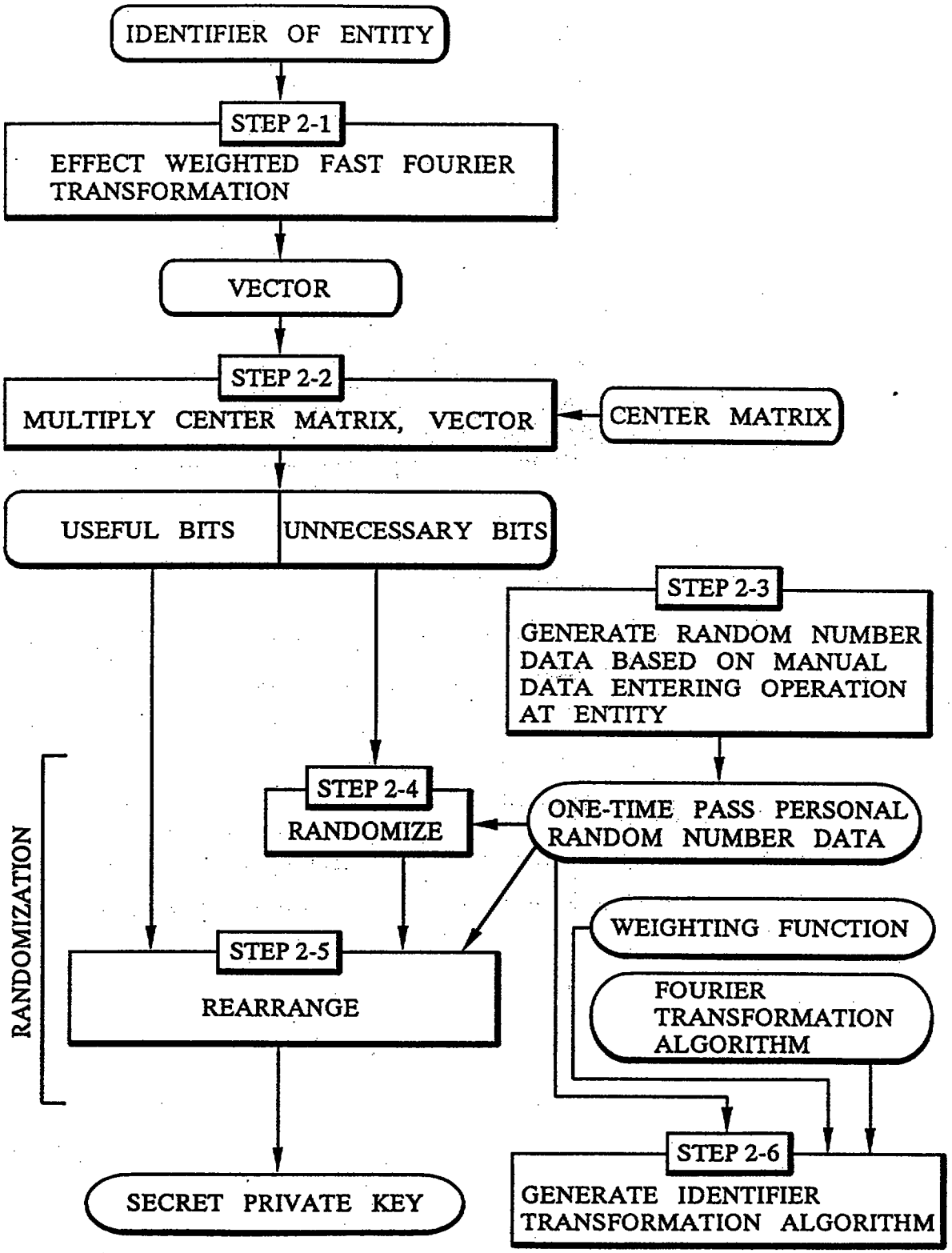

IDENTIFIER OF ENTITY
STEP 2-1
EFFECT WEIGHTED FAST FOURIER TRANSFORMATION
VECTOR
STEP 2-2
MULTIPLY CENTER MATRIX, VECTOR
CENTER MATRIX
USEFUL BITS
UNNECESSARY BITS
STEP 2-3
GENERATE RANDOM NUMBER DATA BASED ON MANUAL DATA ENTERING OPERATION AT ENTITY
STEP 2-4
RANDOMIZE
ONE-TIME PASS PERSONAL RANDOM NUMBER DATA
RANDOMIZATION
STEP 2-5
REARRANGE
WEIGHTING FUNCTION
FOURIER TRANSFORMATION ALGORITHM
SECRET PRIVATE KEY
STEP 2-6
GENERATE IDENTIFIER TRANSFORMATION ALGORITHM

FIG. 6
(TRANSMITTING SIDE)

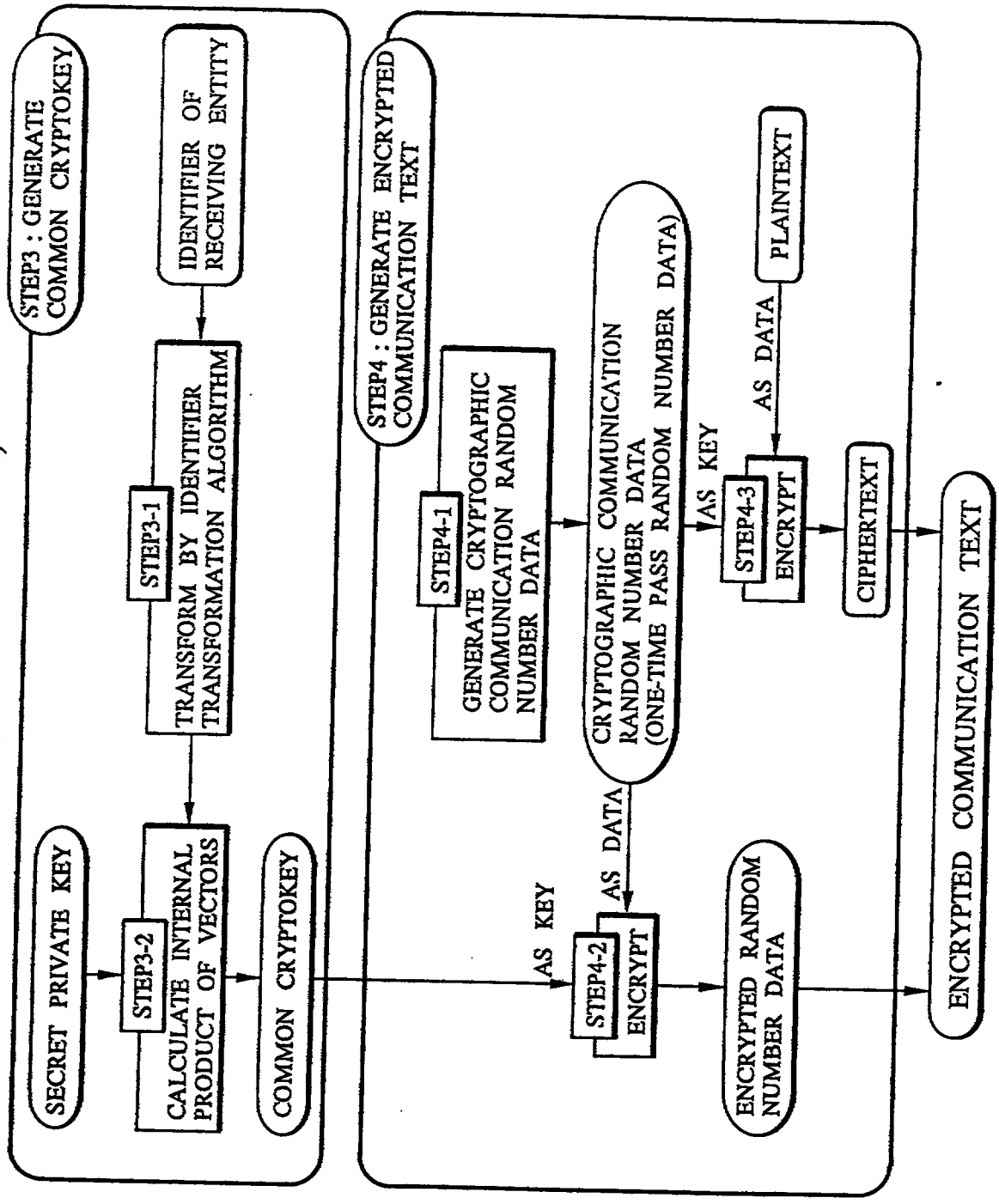


FIG. 7
(RECEIVING SIDE)

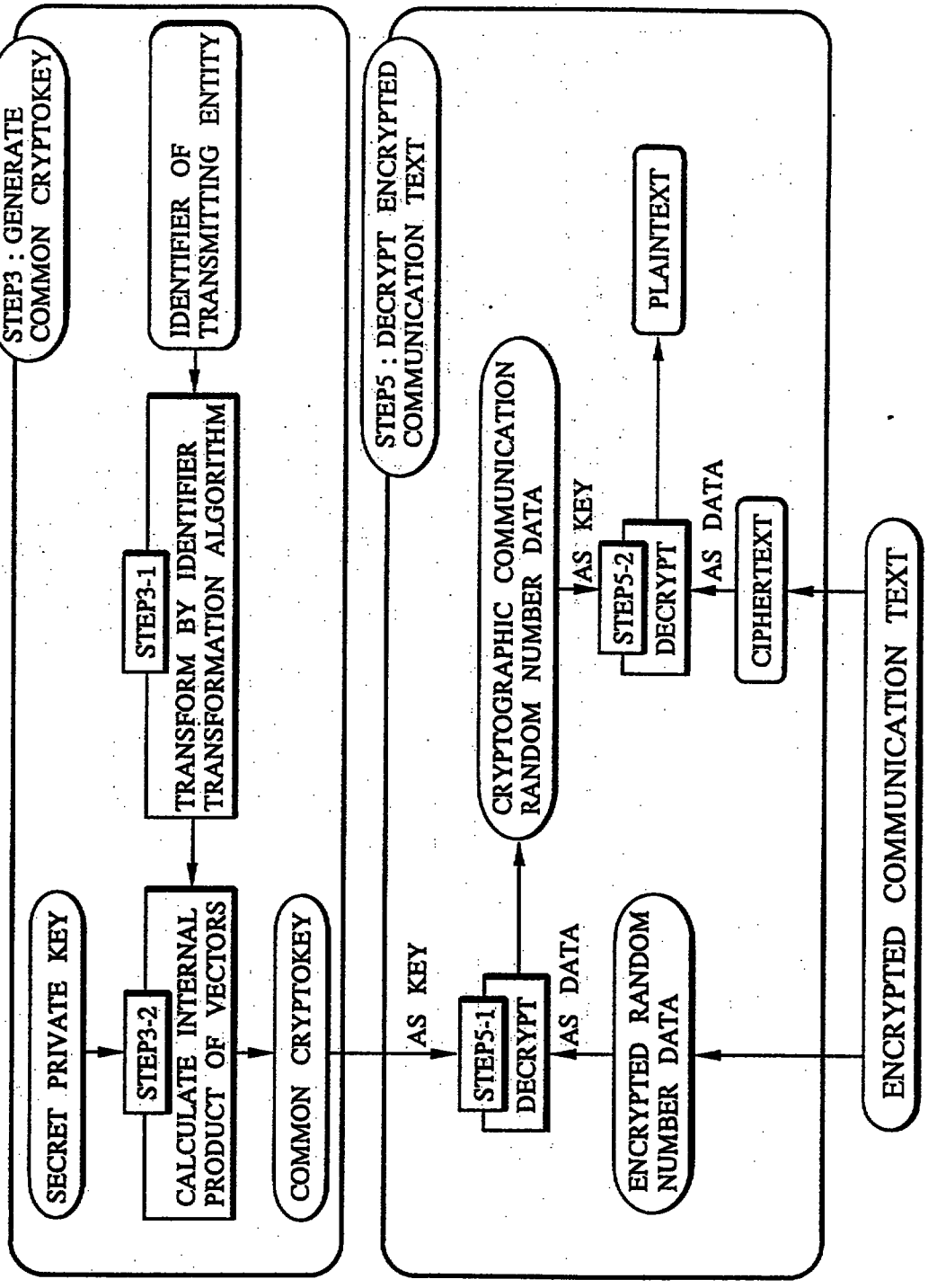
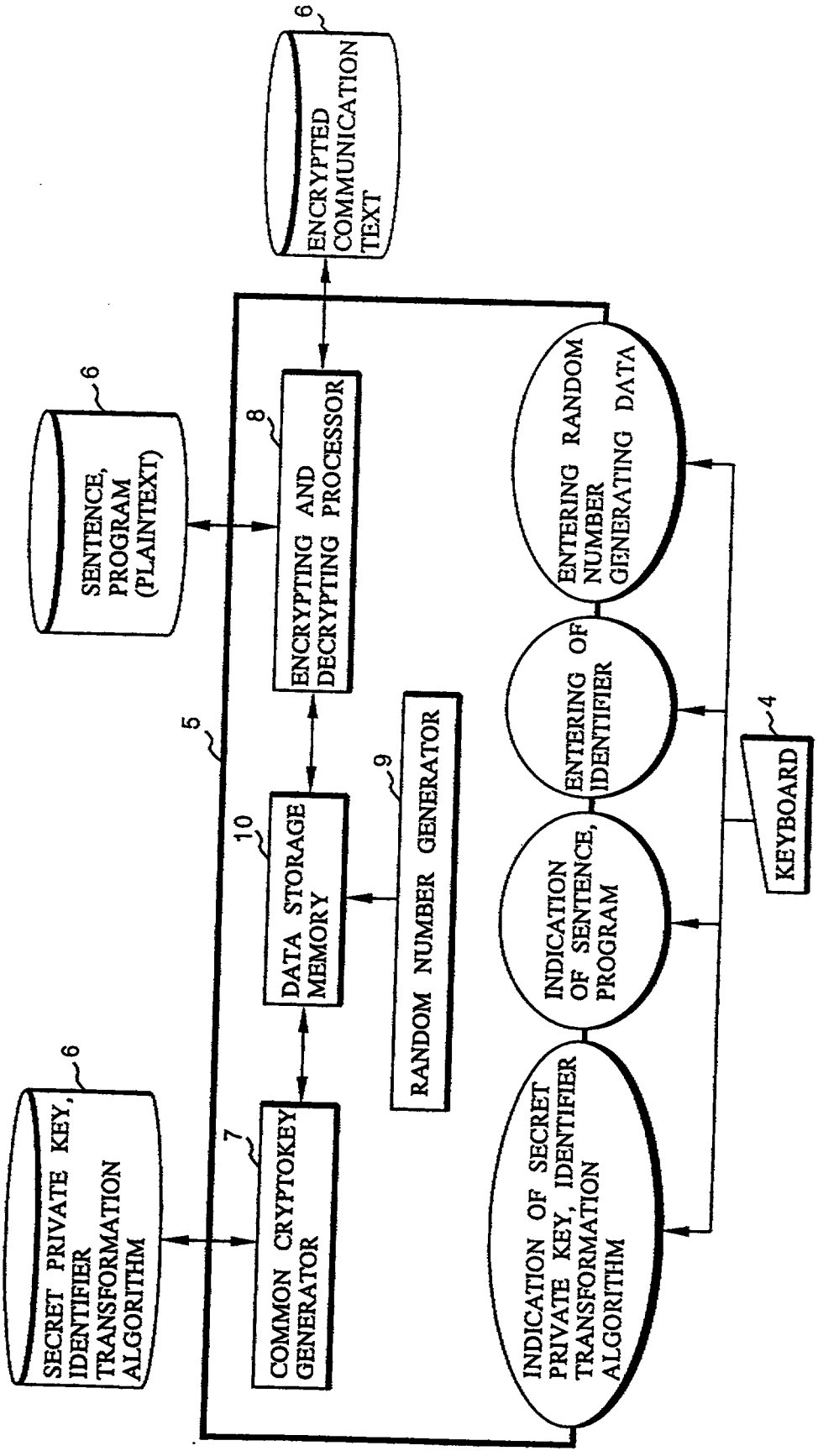


FIG. 8


6
ENCRYPTED COMMUNICATION TEXT
6
SENTENCE, PROGRAM (PLAINTEXT)
8
ENCRYPTING AND DECRYPTING PROCESSOR
5
9
RANDOM NUMBER GENERATOR
10
DATA STORAGE MEMORY
6
SECRET PRIVATE KEY, IDENTIFIER TRANSFORMATION ALGORITHM
7
COMMON CRYPTOKEY GENERATOR
ENTERING RANDOM NUMBER GENERATING DATA
ENTERING OF IDENTIFIER
INDICATION OF SENTENCE, PROGRAM
INDICATION OF SECRET PRIVATE KEY, IDENTIFIER TRANSFORMATION ALGORITHM
4
KEYBOARD

PCT/JP94/00455
Translation of
Annexes to IPER

generation of a common cryptokey for cryptographic communications and a cryptosystem on a computer network.

DISCLOSURE OF INVENTION

To achieve the above object, there is provided in accordance with a first aspect of the present invention a method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of generating, in the center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by the center only and common to the entities and which includes an integral transformation algorithm with a weighting function, and distributing from the center, the secret private key and the integral transformation algorithm with the weighting function to each of the entities, and when the entities communicate with each other, applying, in each of the entities, the integral transformation algorithm with the weighting function and the secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities.

Since the secret private key of each of the entities is generated in the center by transforming the identifier of

each of the entities according to the center algorithm including the integral transformation algorithm (specifically an integral transformation function with a weighting function, however the significance of the weighting function shall be described hereinbelow), the data produced when the integral transformation algorithm is applied to the identifier are made highly dispersive even if the identifiers of the entities are not well dispersed. Consequently, the secret private keys are also made highly dispersive. Therefore, the secret private keys which are less analogous than heretofore are generated for the respective entities by the center, and distributed together with the integral transformation algorithm to the respective entities. For communications between entities, the integral transformation algorithm and the secret private key which are possessed by each of the entities are applied in each of the entities to the identifier of the other entity thereby to generate a common cryptokey. Since the secret private key of each entity contains elements based on the integral transformation algorithm, when not only the secret private key but also the integral transformation algorithm are applied to the identifier of the other entity, the common cryptokey which is common to the entities which are going to communicate with each other is generated by an algorithm portion (which is assumed to be symmetric as described above) of the center algorithm which precludes the integral transformation algorithm.

With the first aspect of the present invention, therefore, as the identifier of each entity is transformed by the center algorithm including the integral transformation algorithm for thereby generating the secret private key peculiar to each entity and used to generate a common cryptokey for communications, the secret private keys of the entities are made highly dispersive, resulting in increased security against differential attack or the like.

For communications, only the identifier of the other entity with which to communicate is applied to the integral transformation algorithm and the secret private key which are owned by each entity for thereby generating a common cryptokey shared by the entities which are going to communicate with each other, without involving the center.

According to the first aspect of the present invention, a cryptosystem on the network is made highly secure against various forms of attack, such as differential attack, while simplifying the generation of a common cryptokey and the arrangement of the cryptosystem, and is also made simple and highly reliable.

The identifier may be the name, address, the mail address or domain name thereof on the network, or their combination of each entity insofar as it is peculiar to each entity and is public to at least to an entity with which to communicate.

The integral transformation algorithm may be a Fourier transformation (including a fast Fourier transforma-

tion), a Laplace transformation, a Miller transformation, a Hilbert transformation, or the like. While either one of these transformations may be used, these integral transformations are defined in a analytically infinite interval. Since the identifier to be transformed by the integral transformation algorithm according to the first aspect of the present invention is expressed in a finite interval (e.g., a coset on a finite ring), simply by subjecting the data of the identifier to the integral transformation using a computer or the like, the transformed data tend to suffer anomalous dispersion (aliasing).

Therefore, according to the first aspect of the present invention, the integral transformation algorithm comprises an integral transformation algorithm with a weighting function. The aliasing can be prevented by adding such a weighting function when the identifier is subjected to the integral transformation. Since the weighting function may be established arbitrarily insofar as it is capable of preventing aliasing, the secret private key generated when the identifier is transformed by the center algorithm which includes the integral transformation algorithm with the weighting function contains unknown elements based on the weighting function. As a consequence, the security of the cryptosystem to which the first aspect of the present invention is applied is increased.

The weighting function thus added is basically established such that its value approaches "0" at ends of

the interval of the data of the identifier. According to the first aspect of the present invention, the weighting function is determined in an unpredictable pattern by random number data generated in the center. More preferably, the random number data comprise one-time pass random number da

CLAIMS

1. (Amended) A method of sharing a common cryptokey for encrypting and decrypting communication data between entities in a network which includes a plurality of entities and a center, comprising the steps of:

generating, in said center, a secret private key peculiar to each of the entities by transforming an identifier which is peculiar to each of the entities and which is public, according to a center algorithm which is held by said center only and common to the entities and which includes an integral transformation algorithm with a weighting function, and distributing, from the center, the secret private key and said integral transformation algorithm with said weighting function to each of the entities; and

when the entities communicate with each other, applying, in each of the entities, said integral transformation algorithm with said weighting function and said secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate a common cryptokey, so that the entities will possess the common cryptokey shared by the entities.

2. (Canceled)

3. (Amended) A method according to claim 1, wherein said weighting function is determined in an unpredictable



pattern by random number data generated in said center.

4. A method according to claim 3, wherein said random number data comprise one-time pass random number data.

5. (Amended) A method according to claim 1, wherein said integral transformation algorithm comprises a Fourier transformation algorithm.

6. A method according to claim 1, further comprising the steps of:

randomizing, in said center, the identifier transformed by said center algorithm, with one-time pass personal random number data which are peculiar and unknown to each of the entities, thereby to generate said secret private key, and distributing, from said center, an identifier transformation algorithm which comprises an algorithm for canceling out the elements of the randomization which are contained in said secret private key and said integral transformation algorithm together with said secret private key, to each of the entities; and

when the entities communicate with each other, applying, in each of the entities, said identifier transformation algorithm and said secret private key which are possessed by each of the entities to the identifier of the other entity thereby to generate said common cryptokey, so that

* C L M S *

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、該センターのみが保持する各エンティティに共通の重み関数付きの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、各エンティティに固有で且つ公開性の識別子を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重み関数付き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重み関数付き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（詳しくは重み関数付きの積分変換アルゴリズムであるが、重み関数の意義については

PCT/JP97/00433
日本国特許庁 14.01.98

後述する）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

日本国特許庁 14.01.98

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単に積分変換しただけでは、変換結果の異常分散（エイシアリング）が生じやすい。

このため、本発明の第１の態様では、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ており、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

請 求 の 範 囲

1．（補正後）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、該センターのみが保持する各エンティティに共通の重み関数付きの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、各エンティティに固有で且つ公開性の識別子を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重み関数付き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重み関数付き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．（削除）

3．（補正後）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1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．（補正後）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、

世界知的所有権機関
国際事務局

PCT 特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 H04L 9/08	A1	(11) 国際公開番号	WO97/31449
		(43) 国際公開日	1997年8月28日(28.08.97)

(21) 国際出願番号 PCT/JP97/00433

(22) 国際出願日 1997年2月19日(19.02.97)

(30) 優先権データ

特願平8/70832	1996年2月21日(21.02.96)	JP
特願平8/70835	1996年2月21日(21.02.96)	JP
特願平8/210376	1996年7月8日(08.07.96)	JP

(81) 指定国 AU, BG, BR, CA, CN, CU, CZ, HU, IL, KR, LT, MX, NO, NZ, PL, RO, RU, SG, SK, TR, UA, VN.

添付公開書類
国際調査報告書

(71) 出願人
カード・コール・サービス株式会社
(CARD CALL SERVICE CO., LTD.)[JP/JP]
〒150 東京都渋谷区道玄坂1丁目22番7号 Tokyo, (JP)
(72) 発明者
馬場芳美(BABA, Yoshimi)
〒273 千葉県船橋市宮本8丁目10番3号 Chiba, (JP)
(74) 代理人
弁理士 佐藤辰彦, 外(SATO, Tatsuhiko et al.)
〒151 東京都渋谷区代々木2丁目1番1号
新宿マインズタワー16階 Tokyo, (JP)

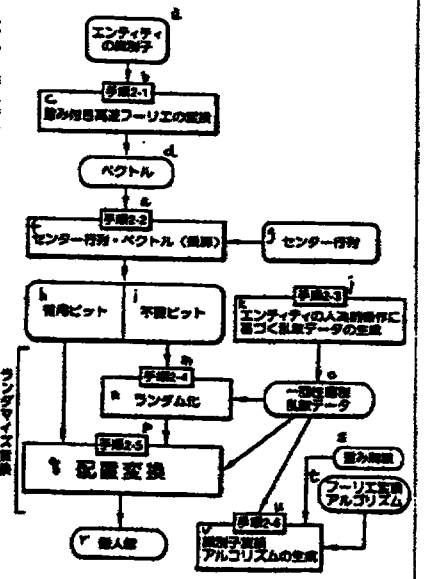
(54)Title: COMMUNICATION METHOD USING COMMON CRYPTOGRAPHIC KEY

(54)発明の名称 暗号鍵共有方法

(57) Abstract

A communication method using a common cryptographic key by which security against various kinds of attacks can be improved while the preparation of a common cryptographic key prepared at the time of performing communication or a cryptographic communication system on a network is simplified. At a center, a personal key peculiar to each entity is prepared by applying Fourier transformation with weight function and center matrix to the identifier of each entity (procedures 2-1 and 2-2) and performing randomized transformation based on one-time random number data prepared by artificial processing of the entities (procedures 2-3 to 2-5) and, at the same time, an identifier converting algorithm is prepared based on the random number data and Fourier transformation with weight function (procedure 2-6) and distributes the algorithm and personal keys to the entities. Each entity prepares a common key used for performing cryptographic communication with a partner by applying the identifier converting algorithm and personal key to the identifier of the partner.

a ... identifier of entity
b ... procedure 2-1
c ... weighted fast Fourier transformation
d ... vector
e ... procedure 2-2
f ... center matrix and vector (multiplication)
g ... center matrix
h ... significant bit
i ... unnecessary bit
j ... procedure 2-3
k ... preparation of random number data based on artificial operation of entity
l ... randomizing conversion
m ... procedure 2-4
n ... randomization
o ... individual one-time random number data
p ... procedure 2-5
q ... rearrangement
r ... personal key
s ... weight function
t ... Fourier transformation algorithm
u ... procedure 2-6
v ... preparation of identifier converting algorithm



（５７）要約

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。センターにおいて、各エンティティの識別子に、重み関数付きフーリエ変換及びセンター行列を作用させ（手順２－１，２－２）、さらにそのエンティティの人為的操作により生成した一回性の乱数データに基づくランダマイズ変換を施すことによって、各エンティティに固有の個人鍵を生成する（手順２－３～５）と共に、上記乱数データ及び重み関数付きフーリエ変換に基づき識別子変換アルゴリムを生成し（手順２－６）、このアルゴリズム及び個人鍵をエンティティに配付する。各エンティティは通信相手側の識別子に識別子変換アルゴリム及び個人鍵を作用させることで通信相手側との暗号通信のための共通鍵を生成する。

情報としての用途のみ
ＰＣＴに基づいて公開される国際出願をパンフレット第一頁にＰＣＴ加盟国を同定するために使用されるコード

AL	アルバニア	ES	エストニア	LR	リベリア	RU	ロシア連邦
AM	アルメニア	FI	フィンランド	LS	レソト	SD	スーダン
AT	オーストリア	FR	フランス	LT	リトアニア	SE	スウェーデン
AU	オーストラリア	GA	ガボン	LU	ルクセンブルグ	SG	シンガポール
AZ	アゼルバイジャン	GB	英国	LV	ラトヴィア	SI	スロヴェニア
BA	ボスニア・ヘルツェゴビナ	GD	グレナダ	MC	モナコ	SK	スロヴァキア共和国
BB	バルバドス	GE	グルジア	MD	モルドバ	SL	シエラレオネ
BE	ベルギー	GH	ガーナ	MG	マダガスカル	SN	セネガル
BF	ブルキナ・ファソ	GN	ギニア	MK	マケドニア旧ユーゴスラヴィア共和国	SZ	スワジランド
BG	ブルガリア	GR	ギリシャ	ML	マリ	TD	チャド
BJ	ベナン	HU	ハンガリー	MN	モンゴル	TG	トーゴ
BR	ブラジル	IE	アイルランド	MR	モーリタニア	TJ	タジキスタン
BY	ベラルーシ	IL	イスラエル	MW	マラウイ	TM	トルクメニスタン
CA	カナダ	IS	アイスランド	MX	メキシコ	TR	トルコ
CF	中央アフリカ共和国	IT	イタリア	NE	ニジェール	TT	トリニダード・トバゴ
CG	コンゴー	JP	日本	NL	オランダ	UA	ウクライナ
CH	スイス	KE	ケニア	NO	ノルウェー	UG	ウガンダ
CI	コート・ジボアール	KG	キルギスタン	NZ	ニュージーランド	US	米国
CM	カメルーン	KP	朝鮮民主主義人民共和国	PL	ポーランド	UZ	ウズベキスタン共和国
CN	中国	KR	大韓民国	PT	ポルトガル	VN	ヴィエトナム
CU	キューバ	KZ	カザフスタン	RO	ルーマニア	YU	ユーゴスラビア
CZ	チェッコ共和国	LC	セントルシア				
DE	ドイツ	LI	リヒテンシュタイン				
DK	デンマーク	LK	スリランカ				