(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-515083
(P2010-515083A)
(43)公表日　平成22年5月6日(2010.5.6)

(51)Int.Cl.	F I	テーマコード（参考）
G09C 1/02 (2006.01)	G09C 1/02	5J104

審査請求 有　予備審査請求 未請求　（全 40 頁）

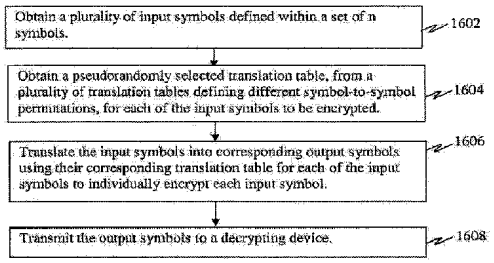
(21)出願番号	特願2009-541607 (P2009-541607)
(86)(22)出願日	平成19年12月14日 (2007.12.14)
(85)翻訳文提出日	平成21年8月7日 (2009.8.7)
(86)国際出願番号	PCT/US2007/087526
(87)国際公開番号	WO2008/076861
(87)国際公開日	平成20年6月26日 (2008.6.26)
(31)優先権主張番号	11/611,827
(32)優先日	平成18年12月15日 (2006.12.15)
(33)優先権主張国	米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】組み合わせコンバイナ暗号化方法

(57)【要約】
別の特徴は、暗号化されたシンボルのセキュリティを保護する効率的な暗号化方法を提供する。各平文シンボルは、別個の擬似ランダムに選択された変換テーブルを使用することにより暗号化される。シンボルのあらゆる可能な順列を変換テーブルとしてあらかじめ記憶することではなくて、変換テーブルは、擬似乱数と、シンボルシャッフリングアルゴリズムとに基づいてオンザフライで効率的に生成されることができる。受信デバイスは、同様に、受信された暗号化シンボルを暗号解読するためにオンザフライで逆変換テーブルを生成することができる。



【特許請求の範囲】
【請求項１】
暗号化デバイス上で動作する方法であって、
複数の入力シンボルを得ることと、
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、擬似ランダムに選択された変換テーブルを得ることと、
各入力シンボルを個別に暗号化するために、前記入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して、前記入力シンボルを対応する出力シンボルへ変換することと、
を備える方法。
【請求項２】
暗号化されるべき前記入力シンボルのおのおのについて前記擬似ランダムに選択された変換テーブルを得ることは、
第１の入力シンボルについての、擬似ランダムに選択された第１の変換テーブルを得ることと、
第２の入力シンボルについての、擬似ランダムに選択された第２の変換テーブルを得ることと、
を含み、
そして、前記入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して前記入力シンボルを対応する出力シンボルへ変換することは、
前記第１の変換テーブルを使用して前記第１の入力シンボルを第１の出力シンボルへ変換することと、
前記第２の変換テーブルを使用して前記第２の入力シンボルを第２の出力シンボルへ変換することと、
を含む、
請求項１に記載の方法。
【請求項３】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義される、但し、Ｎは、正の整数であり、変換テーブルは、前記Ｎ個のシンボルの順列である、請求項１に記載の方法。
【請求項４】
暗号化されるべき前記入力シンボルのおのおのについて、前記擬似ランダムに選択された変換テーブルを得ることは、
暗号化されるべき第１の入力シンボルについての第１の擬似乱数を得ることと、
前記組のＮ個のシンボルの異なる順列を得るために前記組のＮ個のシンボルをシャッフルすること、および前記第１の入力シンボルについての前記変換テーブルとしてその順列を使用することと、
を含む、
請求項３に記載の方法。
【請求項５】
前記第１の擬似乱数は、
前記第１の入力シンボルについての擬似乱数を生成することと、但し、前記擬似乱数はｋビットの長さであり、ｋは正の整数である；
前記擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうかを決定することと、但し、Ｐｍａｘは、最大しきい値2^{k}よりも小さいＮの階乗の最大の倍数である；
前記擬似乱数を、もしそれが前記最大数Ｐｍａｘよりも大きい場合は、捨てることと；
前記最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、前記第１の入力シンボルについての異なる擬似乱数を得ることと；
前記第１の擬似乱数を得るために前記許容可能な擬似乱数のモジュロＮの階乗を除算す

ることと；
によって得られる、
請求項４に記載の方法。
【請求項６】
前記組のＮ個のシンボルをシャッフルすることは、
前記組のＮ個のシンボルのうちのすべてのシンボルを用いて順列ベクトルＰを初期化することと、
前記第１の擬似乱数に基づいて前記順列ベクトルの中の前記シンボルをシャッフルすることと、
を含む、
請求項４に記載の方法。
【請求項７】
前記出力シンボルを暗号解読デバイスに送信すること、
をさらに備える請求項１に記載の方法。
【請求項８】
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の変換テーブルから、第２の擬似ランダムに選択された変換テーブルを得ることと、
各入力シンボルをさらに個別に暗号化するために、前記出力シンボルのおのおのについてそれらの対応する第２の変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへ変換することと、
をさらに備える請求項１に記載の方法。
【請求項９】
複数の入力シンボルを得るための手段と、
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、擬似ランダムに選択された変換テーブルを得るための手段と、
各入力シンボルを個別に暗号化するために、前記入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して、前記入力シンボルを対応する出力シンボルへ変換するための手段と、
を備える暗号化デバイス。
【請求項１０】
第１の入力シンボルについての、擬似ランダムに選択された第１の変換テーブルを得るための手段と、
第２の入力シンボルについての、擬似ランダムに選択された第２の変換テーブルを得るための手段と、
前記第１の変換テーブルを使用して前記第１の入力シンボルを第１の出力シンボルへ変換するための手段と、
前記第２の変換テーブルを使用して前記第２の入力シンボルを第２の出力シンボルへ変換するための手段と、
をさらに備える請求項９に記載のデバイス。
【請求項１１】
暗号化されるべき第１の入力シンボルについての第１の擬似乱数を得るための手段と、
前記組のＮ個のシンボルの異なる順列を得るために前記組のＮ個のシンボルをシャッフルし、そして前記第１の入力シンボルについての前記変換テーブルとしてその順列を使用するための手段と、
をさらに備える請求項９に記載のデバイス。
【請求項１２】
前記第１の入力シンボルについての擬似乱数を生成するための手段と、但し、前記擬似乱数はｋビットの長さであり、ｋは正の整数である；

前記擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうかを決定するための手段と、但し、Ｐｍａｘは、最大しきい値２^{k}よりも小さいＮの階乗の最大の倍数である；
前記擬似乱数を、もしそれが前記最大数Ｐｍａｘよりも大きい場合は、捨てるための手段と；
前記最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、前記第１の入力シンボルについての異なる擬似乱数を得るための手段と；
前記第１の擬似乱数を得るために前記許容可能な擬似乱数のモジュロＮの階乗を除算するための手段と；
をさらに備える請求項１１に記載のデバイス。
【請求項１３】
前記出力シンボルを暗号解読デバイスに送信するための手段、
をさらに備える請求項９に記載のデバイス。
【請求項１４】
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の変換テーブルから、第２の擬似ランダムに選択された変換テーブルを得るための手段と、
各入力シンボルをさらに個別に暗号化するために、前記出力シンボルのおのおのについてそれらの対応する第２の変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへ変換するための手段と、
をさらに備える請求項９に記載のデバイス。
【請求項１５】
入力シンボルストリームを受信するための入力インターフェースと、
前記入力インターフェースに結合された処理回路と、
を備え、
前記処理回路は、
複数の入力シンボルを前記入力インターフェースから取得し、
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、擬似ランダムに選択された変換テーブルを取得し、そして
各入力シンボルを個別に暗号化するために、前記入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して、前記入力シンボルを対応する出力シンボルへ変換する、
ように構成されている、
暗号化デバイス。
【請求項１６】
前記出力シンボルを送信するための、前記処理回路に結合された出力インターフェース、
をさらに備える請求項１５に記載のデバイス。
【請求項１７】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義されている、但し、Ｎは正の整数であり、変換テーブルは、前記Ｎ個のシンボルの順列である、請求項１５に記載のデバイス。
【請求項１８】
前記処理回路に結合されたキーストリームジェネレータと、なお、前記キーストリームジェネレータは、暗号化されるべき第１の入力シンボルについて前記キーストリームジェネレータから第１の擬似乱数を取得するように構成されている；
前記処理回路に結合された変換テーブルジェネレータと、なお、前記変換テーブルジェネレータは、前記組のＮ個のシンボルの異なる順列を取得するために、前記組のＮ個のシンボルをシャッフルするように構成され、そして前記第１の入力シンボルについての前記変換テーブルとしてその順列を使用する；

をさらに備える請求項１７に記載のデバイス。
【請求項１９】
前記処理回路は、さらに、
前記第１の入力シンボルについての擬似乱数を生成し、なお、前記擬似乱数はｋビットの長さであり、ｋは正の整数である；
前記擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうかを決定し、但し、Ｐｍａｘは、最大しきい値2^{k}よりも小さいＮの階乗の最大の倍数である；
前記擬似乱数を、もしそれが前記最大数Ｐｍａｘよりも大きい場合は、捨て；
前記最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、前記第１の入力シンボルについての異なる擬似乱数を取得し；そして
前記第１の擬似乱数を取得するために前記許容可能な擬似乱数のモジュロＮの階乗を除算する；
ように構成されている、
請求項１７に記載のデバイス。
【請求項２０】
前記処理回路は、さらに、
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の変換テーブルから、第２の擬似ランダムに選択された変換テーブルを取得し、そして
各入力シンボルをさらに個別に暗号化するために、前記出力シンボルのおのおのについてそれらの対応する第２の変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへ変換する、
ように構成されている、
請求項１７に記載のデバイス。
【請求項２１】
プロセッサによって実行されるときに、前記プロセッサに、
複数の入力シンボルを取得させ、
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、擬似ランダムに選択された変換テーブルを取得させ、そして
各入力シンボルを個別に暗号化するために、前記入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して、前記入力シンボルを対応する出力シンボルへ変換させる、
シンボルを暗号化するために動作可能な１つまたは複数の命令、を有する機械可読媒体。
【請求項２２】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義される、但し、Ｎは正の整数であり、変換テーブルは、前記Ｎ個のシンボルの順列である、請求項２１に記載の機械可読媒体。
【請求項２３】
プロセッサによって実行されるときに、前記プロセッサに、さらに、
暗号化されるべき第１の入力シンボルについての第１の擬似乱数を取得させ、そして
前記組のＮ個のシンボルの異なる順列を取得するために、前記組のＮ個のシンボルをシャッフルさせ、そして前記第１の入力シンボルについての前記変換テーブルとしてその順列を使用させる、
１つまたは複数の命令、を有する請求項２２に記載の機械可読媒体。
【請求項２４】
プロセッサによって実行されるときに、前記プロセッサに、さらに、
前記第１の入力シンボルについての擬似乱数を生成させ、なお、前記擬似乱数はｋビットの長さであり、ｋは正の整数である；

前記擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうかを決定させ、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数である；
前記擬似乱数を、もしそれが前記最大数Ｐｍａｘよりも大きい場合は、捨てさせ、；
前記最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、前記第１の入力シンボルについての異なる擬似乱数を取得させ；そして
前記第１の擬似乱数を取得するために前記許容可能な擬似乱数のモジュロＮの階乗を除算させる、
１つまたは複数の命令、を有する請求項２２に記載の機械可読媒体。
【請求項２５】
プロセッサによって実行されるときに、前記プロセッサに、さらに、
暗号化されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の変換テーブルから、第２の擬似ランダムに選択された変換テーブルを取得させ、そして
各入力シンボルをさらに個別に暗号化するために、前記出力シンボルのおのおのについてそれらの対応する第２の変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへ変換させる、
１つまたは複数の命令、を有する請求項２１に記載の機械可読媒体。
【請求項２６】
シンボルを暗号解読するための方法であって、
１組のｎ個のシンボル内で定義される複数の入力シンボルを得ることと、
暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、擬似ランダムに選択された逆変換テーブルを得ることと、
各入力シンボルを個別に暗号解読するために、前記入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して、前記入力シンボルを対応する出力シンボルへ変換することと、
を備える方法。
【請求項２７】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義され、但し、Ｎは正の整数であり、逆変換テーブルは前記Ｎ個のシンボルの順列であり、
さらに前記方法は、
暗号解読されるべき第１の入力シンボルについての第１の擬似乱数を得ることと、
前記組のＮ個のシンボルの異なる順列を得るために前記組のＮ個のシンボルをシャッフルすること、および前記第１の入力シンボルについての前記逆変換テーブルとしてその順列を使用することと、
をさらに備える、
請求項２６に記載の方法。
【請求項２８】
前記第１の擬似乱数は、
前記第１の入力シンボルについての擬似乱数を生成することと、なお、前記擬似乱数はｋビットの長さであり、ｋは正の整数である；
前記擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうかを決定することと、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数である；
前記擬似乱数を、もしそれが前記最大数Ｐｍａｘよりも大きい場合は、捨てることと；
前記最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、前記第１の入力シンボルについての異なる擬似乱数を得ることと；
前記第１の擬似乱数を得るために前記許容可能な擬似乱数のモジュロＮの階乗を除算することと；
によって得られる、請求項２７に記載の方法。
【請求項２９】

暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の逆変換テーブルから、第２の擬似ランダムに選択された逆変換テーブルを得ることと、
各入力シンボルをさらに個別に暗号解読するために、前記出力シンボルのおのおのについてそれらの対応する第２の逆変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへ変換することと、
をさらに備える請求項２６に記載の方法。
【請求項３０】
１組のｎ個のシンボル内で定義される複数の入力シンボルを得るための手段と、
暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、擬似ランダムに選択された逆変換テーブルを得るための手段と、
各入力シンボルを個別に暗号解読するために前記入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して前記入力シンボルを対応する出力シンボルへと変換するための手段と、
を備える暗号解読デバイス。
【請求項３１】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義され、但し、Ｎは正の整数であり、逆変換テーブルは前記Ｎ個のシンボルの順列であり、
前記デバイスはさらに、
暗号解読されるべき第１の入力シンボルについての第１の擬似乱数を得るための手段と、
前記組のＮ個のシンボルの異なる順列を得るために、前記組のＮ個のシンボルをシャッフルし、そして前記第１の入力シンボルについての前記逆変換テーブルとしてその順列を使用するための手段と、
を備える、
請求項３０に記載のデバイス。
【請求項３２】
前記第１の擬似乱数は、
前記第１の入力シンボルについての擬似乱数を生成するための手段と、なお、前記擬似乱数はｋビットの長さであり、ｋは正の整数である；
前記擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうかを、決定するための手段と、但し、Ｐｍａｘは、最大しきい値2^{k}よりも小さいＮの階乗の最大の倍数である；
前記擬似乱数を、もしそれが前記最大数Ｐｍａｘよりも大きい場合は、捨てるための手段と；
前記最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、前記第１の入力シンボルについての異なる擬似乱数を得るための手段と；
前記第１の擬似乱数を得るために前記許容可能な擬似乱数のモジュロＮの階乗を除算するための手段と；
によって得られる、
請求項３１に記載のデバイス。
【請求項３３】
暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の逆変換テーブルから、第２の擬似ランダムに選択された逆変換テーブルを得るための手段と、
各入力シンボルをさらに個別に暗号解読するために、前記出力シンボルのおのおのについてそれらの対応する第２の逆変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへと変換するための手段と、
をさらに備える請求項３０に記載のデバイス。
【請求項３４】

入力シンボルストリームを受信するための入力インターフェースと、
前記入力インターフェースに結合された処理回路と、
を備え、
前記処理回路は、
１組のｎ個のシンボル内で定義される複数の入力シンボルを取得し、
暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、擬似ランダムに選択された逆変換テーブルを取得し、そして
各入力シンボルを個別に暗号解読するために、前記入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して、前記入力シンボルを対応する出力シンボルへ変換する、
ように構成されている、
暗号解読デバイス。
【請求項３５】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義され、但し、Ｎは正の整数であり、逆変換テーブルは前記Ｎ個のシンボルの順列であり、
前記デバイスはさらに、
前記処理回路に結合されたキーストリームジェネレータと、なお、前記キーストリームジェネレータは、暗号解読されるべき第１の入力シンボルについて前記キーストリームジェネレータから第１の擬似乱数を取得するように構成されている；
前記処理回路に結合された逆変換テーブルジェネレータと、なお、前記逆変換テーブルジェネレータは、前記組のＮ個のシンボルの異なる順列を取得するために、前記組のＮ個のシンボルをシャッフルするように構成され、そして前記第１の入力シンボルについての前記逆変換テーブルとしてその順列を使用する；
を備える請求項３４に記載のデバイス。
【請求項３６】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義され、但し、Ｎは正の整数であり、逆変換テーブルは前記Ｎ個のシンボルの順列であり、
前記処理回路は、さらに、
前記第１の入力シンボルについての擬似乱数を生成し、なお、前記擬似乱数はｋビットの長さであり、ｋは正の整数である；
前記擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうかを、決定し、但し、Ｐｍａｘは、最大しきい値2^{k}よりも小さいＮの階乗の最大の倍数である；
前記擬似乱数を、もしそれが前記最大数Ｐｍａｘよりも大きい場合は、捨て；
前記最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、前記第１の入力シンボルについての異なる擬似乱数を取得し；そして
前記第１の擬似乱数を得るために前記許容可能な擬似乱数のモジュロＮの階乗を除算する；
ように構成されている、
請求項３４に記載のデバイス。
【請求項３７】
前記処理回路は、さらに、
暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の逆変換テーブルから、第２の擬似ランダムに選択された逆変換テーブルを取得し、そして
各入力シンボルをさらに個別に暗号解読するために、前記出力シンボルのおのおのについてそれらの対応する第２の逆変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへと変換する、
ように構成されている、
請求項３４に記載のデバイス。

【請求項３８】
プロセッサによって実行されるときに、前記プロセッサに、
１組のｎ個のシンボル内で定義される複数の入力シンボルを取得させ、
暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、擬似ランダムに選択された逆変換テーブルを取得させ、そして
各入力シンボルを個別に暗号解読するために、前記入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して、前記入力シンボルを対応する出力シンボルへと変換させる、
シンボルを暗号解読するための１つまたは複数の命令、を有する機械可読媒体。
【請求項３９】
前記複数の入力シンボルは、１組のＮ個のシンボルによって定義され、但し、Ｎは正の整数であり、逆変換テーブルは前記Ｎ個のシンボルの順列であり、
そして前記機械可読媒体は、
プロセッサによって実行されるときに、前記プロセッサに、さらに、
暗号解読されるべき第１の入力シンボルについての第１の擬似乱数を取得させ、そして
前記組のＮ個のシンボルの異なる順列を取得するために、前記組のＮ個のシンボルをシャッフルさせ、そして前記第１の入力シンボルについての前記逆変換テーブルとしてその順列を使用させる、
１つまたは複数の命令、をさらに備える、
請求項３８に記載の機械可読媒体。
【請求項４０】
プロセッサによって実行されるときに、前記プロセッサに、さらに、
暗号解読されるべき前記入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する前記複数の逆変換テーブルから、第２の擬似ランダムに選択された逆変換テーブルを取得させ、そして
各入力シンボルをさらに個別に暗号解読するために、前記出力シンボルのおのおのについてそれらの対応する第２の逆変換テーブルを使用して、前記出力シンボルを対応する第２の出力シンボルへと変換させる、
１つまたは複数の命令、を有する請求項３８に記載の機械可読媒体。
【発明の詳細な説明】
【背景】
【０００１】
［分野］
様々な例は、一般にセキュリティ保護された通信(secure communications)に関し、より詳細には、変換テーブル(translation tables)を効率的に生成することにより、シンボル(symbols)をセキュリティ保護する(secures)ストリーム暗号化(stream encryption)のための方法に関する。
【０００２】
［背景］
ストリーム暗号化は、通常、暗号化された出力または暗号文を生成するために、擬似乱数(pseudo-random numbers)のキーストリーム(keystream)を生成することと、それらを平文シンボル(plaintext symbols)と組み合わせることと、によって進む。普通は、２進キーストリームシンボルと２進平文シンボルは、排他的論理和(Exclusive-OR)（ＸＯＲ）演算を使用してビット毎に組み合わせられる、というのは、それは自己反転型(self-inversive)であるからである。しかしながら、平文シンボル上でビット毎の暗号化(bit-wise encryption)を実行するのではなくて、全体の平文シンボル(whole plaintext symbol)を暗号化することが、時に望ましいこともある。それ故に、ＸＯＲ演算は、使用されることができない。一般的には、平文シンボルは、暗号文シンボル(ciphertext symbol)を得るために、キーストリームシンボルのモジュロｎ(keystream symbol modulo n)に加算される

。しかし、アクティブな攻撃者(attacker)は、特定のシンボルの位置(position)を知り、送信された暗号文シンボルから減算することにより、そのシンボルを変更することができる可能性がある。例えば、１組の平文ディジット(plaintext digits)（０から９）は、キーストリームのモジュロ１０からの擬似ランダムに(pseudorandomly)生成されたディジット(digit)（０から９）に各ディジットを加算することにより、暗号化されることができる。しかしながら、特定の平文ディジットが、「１」であったが、出力暗号文ディジットは、「７」であったことを知っている攻撃者は、キーストリームディジットが、「６」であったことを決定することができ、そしてそのときには、その特定のシンボル位置のそれらの選択についての他の任意のディジットを正しく暗号化することができる。攻撃者は、平文シンボルと、キーストリームシンボルとがどのようにして組み合わせられているかを決定することができるので、そのような部分的な暗号解読は、暗号化された情報の残りについてのセキュリティを弱める。すなわち、ひとたび暗号文シンボルと、平文シンボルとの間の関係が見出された後に、その情報は、他の暗号文シンボルが、攻撃者によって暗号解読されることを可能にすることができるので、残りの暗号文シンボルのセキュリティは、損なわれる。さらに、簡単な数学的演算（例えば、加算、減算、乗算など）は、速く、そして効率的に平文シンボルと、キーストリームシンボルとを組み合わせるが、より複雑な数学的関数を使用することは、暗号化において注目に値する遅延を引き起こし、あるいはより多くの処理リソースを要求する可能性がある。

【０００３】

したがって、もし、１つの暗号化されたシンボルが見出されるあるいは解読される(discovered or broken)場合は、他のシンボルのセキュリティ(security)を弱めることのない効果的な暗号化方法が必要とされる。

【発明の概要】

【０００４】

データをセキュリティ保護するための、暗号化デバイス(encrypting device)上で動作する方法が、提供される。複数の入力シンボルが、暗号化デバイスによって得られる。擬似ランダムに選択された変換テーブルが、暗号化されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列(different symbol-to-symbol permutations)を定義する複数の変換テーブルから、得られる。入力シンボルは、各入力シンボルを個別に暗号化するために、入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して、対応する出力シンボルへ変換される。出力シンボルは、暗号解読デバイス(decrypting device)に送信されることができる。

【０００５】

さらに、第２の擬似ランダムに選択された変換テーブルが、暗号化されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから得られることができる。出力シンボルは、各入力シンボルをさらに個別に暗号化するために、出力シンボルのおのおのについてそれらの対応する第２の変換テーブルを使用して、対応する第２の出力シンボルへ変換されることができる。

【０００６】

一例においては、暗号化されるべき入力シンボルのおのおのについて擬似ランダムに選択された変換テーブルを得ることは、（ａ）第１の入力シンボルについての、擬似ランダムに選択された第１の変換テーブルを得ることと、（ｂ）第２の入力シンボルについての、擬似ランダムに選択された第２の変換テーブルを得ることと、を含むことができる。入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して入力シンボルを対応する出力シンボルへ変換することは、（ａ）第１の変換テーブルを使用して第１の入力シンボルを第１の出力シンボルへ変換することと、（ｂ）第２の変換テーブルを使用して第２の入力シンボルを第２の出力シンボルへ変換することと、を含むことができる。複数の入力シンボルは、１組のＮ個のシンボル(a set of N symbols)によって定義されることができ、但し、Ｎは、正の整数であり、変換テーブルは、Ｎ個のシンボルの順列である。

【０００７】
別の例においては、暗号化されるべき入力シンボルのおのおのについての、擬似ランダムに選択された変換テーブルを得ることは、（ａ）暗号化されるべき第１の入力シンボルについての第１の擬似乱数を得ることと、（ｂ）該組のＮ個のシンボルの異なる順列を得るために該組のＮ個のシンボルをシャッフルすること(shuffling)、および第１の入力シンボルについての変換テーブルとしてその順列を使用することと、を含むことができる。
【０００８】
１つのコンフィギュレーション(configuration)においては、第１の擬似乱数は、（ａ）第１の入力シンボルについての擬似乱数を生成すること(generating)、但し、擬似乱数は、ｋビットの長さであり、そしてｋは、正の整数である；（ｂ）擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうか、を決定すること(determining)、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数(the largest multiple of N factorial)である；（ｃ）擬似乱数が最大数Ｐｍａｘよりも大きい場合は、擬似乱数を捨てること(discarding)；（ｄ）最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、第１の入力シンボルについての異なる擬似乱数を得ること(obtaining)；および／または（ｅ）第１の擬似乱数を得るために許容可能な擬似乱数のモジュロＮの階乗を除算すること(dividing the acceptable pseudorandom number modulo N factorial)；によって得られることができる。該組のＮ個のシンボルをシャッフルすることは、（ａ）該組のＮ個のシンボルのうちのすべてのシンボルを用いて順列ベクトル(permutation vector)Ｐを初期化することと、（ｂ）第１の擬似乱数に基づいて順列ベクトルの中のシンボルをシャッフルすることと、を含むことができる。
【０００９】
暗号化デバイス(encryption device)もまた、提供され、入力インターフェースと、処理回路と、を備える。入力インターフェースは、入力シンボルストリームを受信する役割を果たすことができる。処理回路は、（ａ）入力インターフェースから複数の入力シンボルを取得し、（ｂ）暗号化されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、擬似ランダムに選択された変換テーブルを取得し、かつ／または（ｃ）各入力シンボルを個別に暗号化するために、入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して、入力シンボルを対応する出力シンボルへ変換する、ように構成されていることができる。暗号化デバイスは、出力シンボルを送信するための、処理回路に結合された出力インターフェースを含むこともできる。
【００１０】
複数の入力シンボルは、１組のＮ個のシンボルによって定義されることができ、但し、Ｎは、正の整数であり、そして変換テーブルは、Ｎ個のシンボルの順列である。暗号化デバイスはまた、（ａ）処理回路に結合されたキーストリームジェネレータと、なお、キーストリームジェネレータは、暗号化されるべき第１の入力シンボルについて第１の擬似乱数をキーストリームジェネレータから得るように構成されている；および／または（ｂ）処理回路に結合された変換テーブルジェネレータと、なお、変換テーブルジェネレータは、該組のＮ個のシンボルの異なる順列を得るために該組のＮ個のシンボルをシャッフルする(shuffle)ように構成され、第１の入力シンボルについての変換テーブルとしてその順列を使用する；も含むことができる。
【００１１】
一例においては、処理回路は、さらに、（ａ）第１の入力シンボルについての擬似乱数を生成し、なお擬似乱数は、ｋビットの長さであり、そしてｋは、正の整数である；（ｂ）擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうか、を決定し、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数である；（ｃ）擬似乱数が、もし最大数Ｐｍａｘよりも大きい場合は、擬似乱数を捨て；（ｄ）最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、第１の入力シンボルについての異なる擬似乱数を取得し；かつ／または（ｅ）第１の擬似乱数を得るために許容可能な擬似乱数ジュロＮの階乗を

除算する（divide the acceptable psedorandom modulo N factorial）；ように構成されることもできる。

【００１２】

１つのコンフィギュレーションにおいては、暗号化デバイスの処理回路はまた、（ａ）暗号化されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、第２の擬似ランダムに選択された変換テーブルを取得し、、かつ／または（ｂ）各入力シンボルをさらに個別に暗号化するために、出力シンボルのおのおのについてそれらの対応する第２の変換テーブルを使用して、出力シンボルを対応する第２の出力シンボルへと変換する、ように構成されることもできる。

【００１３】

その結果として、（ａ）複数の入力シンボルを得るための手段、（ｂ）暗号化されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、擬似ランダムに選択された変換テーブルを得るための手段、（ｃ）各入力シンボルを個別に暗号化するために入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して、入力シンボルを対応する出力シンボルへ変換するための手段、および／または（ｄ）出力シンボルを暗号解読デバイスに送信するための手段、を備える暗号化デバイスが、提供される。暗号化デバイスはまた、（ａ）暗号化されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、第２の擬似ランダムに選択された変換テーブルを得るための手段、および／または（ｂ）各入力シンボルをさらに個別に暗号化するために、出力シンボルのおのおのについてそれらの対応する第２の変換テーブルを使用して、出力シンボルを対応する第２の出力シンボルへ変換するための手段、を含むこともできる。

【００１４】

１つのコンフィギュレーションにおいては、暗号化デバイスは、（ａ）第１の入力シンボルについての擬似ランダムに選択された第１の変換テーブルを得るための手段、（ｂ）第２の入力シンボルについての擬似ランダムに選択された第２の変換テーブルを得るための手段、（ｃ）第１の変換テーブルを使用して第１の入力シンボルを第１の出力シンボルへと変換するための手段、および／または（ｄ）第２の変換テーブルを使用して第２の入力シンボルを第２の出力シンボルへ変換するための手段、を含むことができる。

【００１５】

一例においては、暗号化デバイスはまた、（ａ）暗号化されるべき第１の入力シンボルについて第１の擬似乱数を得るための手段、および／または（ｂ）該組のＮ個のシンボルの異なる順列を得るために該組のＮ個のシンボルをシャッフルし、そして第１の入力シンボルについての変換テーブルとしてその順列を使用するための手段、を含むこともできる。

【００１６】

プロセッサによって実行されるときに、プロセッサに、（ａ）複数の入力シンボルを取得させ、（ｂ）暗号化されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の変換テーブルから、擬似ランダムに選択された変換テーブルを取得させ、かつ／または（ｃ）各入力シンボルを個別に暗号化するために入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して入力シンボルを対応する出力シンボルへ変換させる、シンボルを暗号化するために動作可能な１つまたは複数の命令、を有する機械可読媒体もまた、提供される。複数の入力シンボルは、１組のＮ個のシンボルによって定義されることができる、但し、Ｎは、正の整数であり、そして変換テーブルは、Ｎ個のシンボルの順列である。

【００１７】

機械可読媒体は、プロセッサによって実行されるときに、プロセッサに、さらに、（ａ）暗号化されるべき第１の入力シンボルについての第１の乱数を取得させ、かつ／または（ｂ）該組のＮ個のシンボルの異なる順列を取得するために該組のＮ個のシンボルをシャッフルし、そして第１の入力シンボルについての変換テーブルとしてその順列を使用させ

る１つまたは複数の命令、を含むこともできる。

【００１８】

１つのコンフィギュレーションにおいては、機械可読媒体は、プロセッサによって実行されるときに、プロセッサに、さらに、（ａ）第１の入力シンボルについての擬似乱数を生成させ、なお、擬似乱数は、ｋビットの長さであり、そしてｋは、正の整数である；（ｂ）擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうか、を決定させ、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数である；（ｃ）擬似乱数が、もし最大数Ｐｍａｘよりも大きい場合は、擬似乱数を捨てさせ；（ｄ）最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、第１の入力シンボルについての異なる擬似乱数を取得させ；かつ／または（ｅ）第１の擬似乱数を得るために許容可能な擬似乱数のモジュロＮの階乗を除算させる、１つまたは複数の命令、を含むこともできる。

【００１９】

シンボルを暗号解読するための方法もまた提供される。１組のｎ個のシンボル内で(within a set of n symbols)定義される複数の入力シンボルが、得られる。擬似ランダムに選択された逆変換テーブル(reverse translation table)が、暗号解読されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、選択される。次いで、入力シンボルは、各入力シンボルを個別に暗号解読するために、入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して、対応する出力シンボルへ変換される。複数の入力シンボルは、１組のＮ個のシンボルによって定義されることができ、但し、Ｎは、正の整数であり、逆変換テーブルは、Ｎ個のシンボルの順列である。本方法は、（ａ）暗号解読されるべき第１の入力シンボルについての第１の擬似乱数を得ること、および／または（ｂ）該組のＮ個のシンボルの異なる順列を得るために該組のＮ個のシンボルをシャッフルし、そして第１の入力シンボルについての逆変換テーブルとしてその順列を使用すること、をさらに含むことができる。

【００２０】

一例においては、第１の擬似乱数は、（ａ）第１の入力シンボルについての擬似乱数を生成すること、なお擬似乱数は、ｋビットの長さであり、そしてｋは、正の整数である；（ｂ）擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうか、を決定すること、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数である；（ｃ）擬似乱数が、もし最大数Ｐｍａｘよりも大きい場合は、擬似乱数を捨てること；（ｄ）最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、第１の入力シンボルについての異なる擬似乱数を得ること；および／または（ｅ）第１の擬似乱数を得るために許容可能な擬似乱数のモジュロＮの階乗を除算すること；によって得られることができる。

【００２１】

別のコンフィギュレーションにおいては、本方法は、（ａ）暗号解読されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、第２の擬似ランダムに選択された逆変換テーブルを得ること、および／または（ｂ）各入力シンボルをさらに個別に暗号解読するために、出力シンボルのおのおのについてそれらの対応する第２の逆変換テーブルを使用して、出力シンボルを対応する第２の出力シンボルへ変換すること、をさらに含むことができる。

【００２２】

入力インターフェースと処理回路とを備える暗号解読デバイスが提供される。入力インターフェースは、入力シンボルストリームを受信することができる。処理回路は、（ａ）１組のｎ個のシンボル内で定義される複数の入力シンボルを取得し、（ｂ）暗号解読されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、擬似ランダムに選択された逆変換テーブルを取得し、かつ／または（ｃ）各入力シンボルを個別に暗号解読するために入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して入力シンボルを対応する出力シンボルへ変換する、ように構成されることができる。

【００２３】

複数の入力シンボルは、１組のＮ個のシンボルによって定義されることができる、但し、Ｎは、正の整数であり、そして逆変換テーブルは、Ｎ個のシンボルの順列である。暗号解読デバイスはまた、（ａ）処理回路に結合されたキーストリームジェネレータと、なお、キーストリームジェネレータは、暗号解読されるべき第１の入力シンボルについてキーストリームジェネレータから第１の擬似乱数を得るように構成されている；および／または（ｂ）処理回路に結合された逆変換テーブルジェネレータと、なお、逆変換テーブルジェネレータは、該組のＮ個のシンボルの異なる順列を得るために該組のＮ個のシンボルをシャッフルするように構成され、そして第１の入力シンボルについての逆変換テーブルとしてその順列を使用する；を含むこともできる。

【００２４】

複数の入力シンボルは、１組のＮ個のシンボルによって定義されることができる、但し、Ｎは、正の整数であり、そして逆変換テーブルは、Ｎ個のシンボルの順列である。処理回路は、さらに、（ａ）第１の入力シンボルについての擬似乱数を生成し、なお擬似乱数は、ｋビットの長さであり、そしてｋは、正の整数である；（ｂ）擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうか、を決定し、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数である；（ｃ）擬似乱数が、もし最大数Ｐｍａｘよりも大きい場合は、擬似乱数を捨て；（ｄ）最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、第１の入力シンボルについての異なる擬似乱数を取得し；かつ／または（ｅ）第１の擬似乱数を得るために許容可能な擬似乱数のモジュロＮの階乗を除算する、ように構成されることもできる。

【００２５】

別の例においては、処理回路は、さらに、（ａ）暗号解読されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、第２の擬似ランダムに選択された逆変換テーブルを取得し、かつ／または（ｂ）各入力シンボルをさらに個別に暗号解読するために出力シンボルのおのおのについてそれらの対応する第２の逆変換テーブルを使用して、出力シンボルを対応する第２の出力シンボルへ変換する、ように構成されることができる。

【００２６】

その結果として、（ａ）１組のｎ個のシンボル内で定義される複数の入力シンボルを得るための手段、（ｂ）暗号解読されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、擬似ランダムに選択された逆変換テーブルを得るための手段、および／または（ｃ）各入力シンボルを個別に暗号解読するために入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して入力シンボルを対応する出力シンボルへと変換するための手段、を備える暗号解読デバイスもまた、提供される。複数の入力シンボルは、１組のＮ個のシンボルによって定義されることができる、但し、Ｎは、正の整数であり、そして逆変換テーブルは、Ｎ個のシンボルの順列である。暗号解読デバイスは、（ａ）暗号解読されるべき第１の入力シンボルについて第１の擬似乱数を得るための手段、および／または（ｂ）該組のＮ個のシンボルの異なる順列を得るために該組のＮ個のシンボルをシャッフルし、そして第１の入力シンボルについての逆変換テーブルとしてその順列を使用するための手段、をさらに含むこともできる。第１の擬似乱数は、（ａ）第１の入力シンボルについての擬似乱数を生成するための手段、なお擬似乱数は、ｋビットの長さであり、そしてｋは、正の整数である；（ｂ）擬似乱数が最大数Ｐｍａｘの範囲内にあるかどうか、を決定するための手段、但し、Ｐｍａｘは、最大しきい値2^kよりも小さいＮの階乗の最大の倍数である；（ｃ）擬似乱数が、もし最大数Ｐｍａｘよりも大きい場合は、擬似乱数を捨てるための手段；（ｄ）最大数Ｐｍａｘ以下である許容可能な擬似乱数が得られるまで、第１の入力シンボルについての異なる擬似乱数を得るための手段；および／または（ｅ）第１の擬似乱数を得るために許容可能な擬似乱数のモジュロＮの階乗を除算するための手段；によって得られる。

【００２７】

プロセッサによって実行されるときに、プロセッサに、（ａ）１組のｎ個のシンボル内

で定義される複数の入力シンボルを取得させ、（ｂ）暗号解読されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、擬似ランダムに選択された逆変換テーブルを取得させ、かつ／または（ｃ）各入力シンボルを個別に暗号解読するために、入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して、入力シンボルを対応する出力シンボルへ変換させる、シンボルを暗号解読するための１つまたは複数の命令、を有する機械可読媒体もまた、提供される。複数の入力シンボルは、１組のＮ個のシンボルによって定義される、但し、Ｎは、正の整数であり、そして逆変換テーブルは、Ｎ個のシンボルの順列である。

【００２８】

機械可読媒体はまた、プロセッサによって実行されるときに、プロセッサに、さらに、（ａ）暗号解読されるべき第１の入力シンボルについての第１の擬似乱数を取得させ、かつ／または（ｂ）該組のＮ個のシンボルの異なる順列を得るために該組のＮ個のシンボルをシャッフルし、そして第１の入力シンボルについての逆変換テーブルとしてその順列を使用させる、１つまたは複数の命令、を備えることもできる。

【００２９】

別の例においては、機械可読媒体はまた、プロセッサによって実行されるときに、プロセッサに、さらに、（ａ）暗号解読されるべき入力シンボルのおのおのについて、異なるシンボルごとの順列を定義する複数の逆変換テーブルから、第２の擬似ランダムに選択された逆変換テーブルを取得させ、かつ／または（ｂ）各入力シンボルをさらに個別に暗号解読するために、出力シンボルのおのおのについてそれらの対応する第２の逆変換テーブルを使用して、出力シンボルを対応する第２の出力シンボルへ変換させる、１つまたは複数の命令、を備えることもできる。

【図面の簡単な説明】

【００３０】

【図１】図１は、セキュリティデバイスが、電話とセキュリティ保護されたサーバとの間のある種の通信を、セキュリティ保護するために、通信回線に沿って電話に結合されることができるシステムを示す。

【図２】図２は、図１の電話と発行機関(issuing institution)に属するセキュリティサーバとの間のある種の通信を、セキュリティ保護するための一方法を示す流れ図である。

【図３】図３は、送信中にＤＴＭＦトーンをセキュリティ保護することを可能にすることができるテレサービスセキュリティサーバ(tele-services security server)の一例のブロック図を示す。

【図４】図４は、電話デバイスからのＤＴＭＦトーンをセキュリティ保護するための、セキュリティサーバ上で動作する一方法を示す。

【図５】図５は、送信中にＤＴＭＦトーンを保護するように構成されることができるセキュリティデバイスの一例のブロック図を示す。

【図６】図６は、電話デバイスからのＤＴＭＦトーンをセキュリティ保護するための、セキュリティデバイス上で動作する一方法を示す。

【図７】図７は、セキュリティサーバを用いてそれ自体を認証するように構成されたモバイル通信デバイスのブロック図である。

【図８】図８は、通信ネットワーク上でテレサービス局に対してモバイル通信デバイスを認証するための一方法を示す流れ図である。

【図９】図９は、暗号化されるべき各シンボルについて変換テーブルを擬似ランダムに選択することにより、平文シンボルをセキュリティ保護するための組み合わせコンバイナのブロック図を示す。

【図１０】図１０は、平文シンボルを暗号化されたシンボルに変換するための、シンボルごとの変換テーブル(a symbol-to-symbol translation table)の一例を示す。

【図１１】図１１は、どのようにして平文シンボルが、暗号化されたシンボルを得るために異なる変換テーブルを使用して暗号化されることができるのかの一例を示す。

【図１２】図１２は、１組のｎ個のシンボルについての複数の可能な順列から変換テーブ

ルを選択するためのアルゴリズムを示しており、ここでｎは、正の整数である。
【図１３】図１３は、単一の平文シンボルを暗号化するために複数の変換テーブルを使用することにより、シンボル認証を達成することができる別の暗号化スキームを示すブロック図である。
【図１４】図１４は、どのようにして複数の変換テーブルが、対応する暗号化されたシンボルを得るために各平文シンボルを暗号化するために使用されることができるのかを示す。
【図１５】図１５は、どのようにして２つの変換テーブルが、平文シンボルを暗号化されたシンボルへ変換または暗号化するために使用されることができるのかの一例を示す。
【図１６】図１６は、一例による、平文暗号化を実行するための一方法を示す。
【図１７】図１７は、どのようにして暗号化されたシンボルが、単一の平文シンボルを得るために１つまたは複数の逆変換テーブルを使用することにより暗号解読されることができるのかを示すブロック図である。
【図１８】図１８は、一例による、平文暗号化を実行するための一方法を示す。
【図１９】図１９は、一例による暗号化モジュールを示すブロック図である。
【図２０】図２０は、一例による暗号解読モジュールを示すブロック図である。
【詳細な説明】
【００３１】
以下の説明においては、具体的な詳細が、例の十分な理解を提供するために与えられる。しかしながら、それらの例は、これらの特定の詳細なしに実行されることができることが、当業者によって理解されるであろう。例えば、回路は、それらの例を不必要に詳細にあいまいにしないようにするために、ブロック図の形で示されなくてもよい。
【００３２】
また、例は、フローチャート、流れ図、構造図、またはブロック図として示されるプロセスとして説明されることができることにも注意すべきである。フローチャートは、逐次的なプロセスとしてオペレーションを説明することができるが、オペレーションの多くは、並列に、あるいは同時に実行されることができる。さらに、オペレーションの順序は、並べ換えられる(re-arranged)ことができる。プロセスは、そのオペレーションが完了されるときに終了される。プロセスは、方法、ファンクション(function)、プロシージャ、サブルーチン、サブプログラムなどに対応することができる。プロセスが、ファンクションに対応するとき、その終了は、呼出しファンクション(calling function)または主要ファンクションに対するファンクションのリターン(return)に対応する。
【００３３】
さらに、ストレージ媒体は、読取り専用メモリ(read-only memory)（ＲＯＭ）、ランダムアクセスメモリ(random access memory)（ＲＡＭ）、磁気ディスクストレージ媒体、光ストレージ媒体、フラッシュメモリデバイス、および／または情報を記憶するための他の機械可読媒体を含めて、データを記憶するための１つまたは複数のデバイスを表すことができる。用語「機械可読媒体」は、それだけには限定されないが、ポータブルストレージデバイスまたは固定ストレージデバイスと、光ストレージデバイスと、ワイヤレスチャネルと、命令（単数または複数）および／またはデータを記憶し、含み、あるいは搬送することができる様々な他の媒体と、を含む。
【００３４】
さらに、様々なコンフィギュレーションは、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、あるいはそれらの組合せによってインプリメントされることができる。ソフトウェア、ファームウェア、ミドルウェア、またはマイクロコードの形でインプリメントされるときには、説明されたタスクを実行するプログラムコードまたはコードセグメントは、ストレージ媒体や他のストレージ手段などの機械可読媒体に記憶されることができる。プロセッサは、定義されたタスクを実行することができる。コードセグメントは、プロシージャ、ファンクション、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、あるいは命令、

データ構造、またはプログラムステートメントの組合せを表すことができる。コードセグメントは、情報、データ、引数(arguments)、パラメータ、またはメモリ内容を渡すこと、および／または受け取ることにより、別のコードセグメントまたはハードウェア回路に結合されることができる。情報、引数、パラメータ、データなどは、とりわけメモリ共有、メッセージパッシング(message passing)、トークンパッシング(token passing)、およびネットワーク送信を含めて適切な手段を経由して、渡され、転送され、または送信されることができる。ここにおいて開示される方法は、ハードウェア、ソフトウェア、またはそれらの両方の形でインプリメントされることができる。

【００３５】

ここにおいて開示される例に関連して説明される様々な例示的な論理的なブロック、モジュール、回路、要素、および／またはコンポーネントは、ここにおいて説明される機能を実行するように設計された汎用プロセッサ、デジタル信号プロセッサ(digital signal processor)（ＤＳＰ）、特定用途向け集積回路(application specific integrated circuit)（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ(field programmable gate array)（ＦＰＧＡ）または他のプログラマブルロジックコンポーネント、個別ゲートまたはトランジスタロジック、個別ハードウェアコンポーネント、あるいはそれらの任意の組合せを用いてインプリメントされ、または実行されることができる。汎用プロセッサは、マイクロプロセッサとすることができるが、代替案においては、プロセッサは、従来の任意のプロセッサ、コントローラ、マイクロコントローラ、または状態機械とすることもできる。プロセッサはまた、コンピューティングコンポーネント(computing component)の組合せとして、例えばＤＳＰとマイクロプロセッサとの組合せ、いくつかのマイクロプロセッサ、ＤＳＰコアと組み合わされた１つまたは複数のマイクロプロセッサ、あるいは他のそのような任意のコンフィギュレーションとしてインプリメントされることもできる。

【００３６】

ここにおいて開示される例と関連して説明される方法またはアルゴリズムは、処理ユニット、プログラミング命令、または他の指示の形態において、ハードウェアの形で、プロセッサにより実行可能なソフトウェアモジュールの形で、あるいは両方の組合せの形で直接に実施されることができ、そして単一のデバイスの中に含まれ、あるいは複数のデバイスを通して分散されることができる。ソフトウェアモジュールは、ＲＡＭメモリ、フラッシュメモリ、ＲＯＭメモリ、ＥＰＲＯＭメモリ、ＥＥＰＲＯＭメモリ、レジスタ、ハードディスク、着脱可能ディスク、ＣＤ－ＲＯＭ、あるいは当技術分野において知られている他の任意の形態のストレージ媒体の中に存在することができる。ストレージ媒体は、プロセッサが、そのストレージ媒体から情報を読み取り、そのストレージ媒体へと情報を書き込むことができるようにプロセッサに結合されることができる。代替案においては、ストレージ媒体は、プロセッサと一体化していてもよい。

【００３７】

１つの特徴は、顧客の電話回線と直列に挿入されることができる小型フォームファクタ(small form-factor)のセキュリティデバイスを提供し、これは、２ファクタの認証スキームにおける第２のファクタとしての役割を果たし、ＤＴＭＦトーンを暗号化し、それによって慎重な扱いを要する情報(sensitive information)の開示を防止する。本デバイスは、電話の通常オペレーションには干渉しない。本デバイスは、それらが関連づけられるバンクおよび支払いのサービスについてブランドの機会(branding opportunity)を提供することもできる小型フォームファクタの容器(enclosure)を含むことができる。本デバイスは、それが結合される電話回線から電力を供給されることができる。１つのコンフィギュレーションにおいては、複数のそのようなデバイスは、複数の異なるパーティ（例えば、銀行）とのセキュリティ保護された通信を提供するために電話回線に沿ってチェーン接続され(chained)、あるいはカスケード接続されることができる。

【００３８】

別の特徴は、暗号化されたシンボルのセキュリティを保護する効率的な暗号化方法を提供する。各平文シンボルは、別個の擬似ランダムに選択された変換テーブルを使用するこ

とにより暗号化される。シンボルのあらゆる可能な順列を変換テーブルとしてあらかじめ記憶するのではなくて、変換テーブルは、擬似乱数と、シンボルシャッフリングアルゴリズム(symbol shuffling algorithm)とに基づいてオンザフライで(on-the-fly)効率的に生成されることができる。受信デバイスは、同様に、受信された暗号化シンボルを暗号解読するために、オンザフライで逆変換テーブルを生成することもできる。

【００３９】

ＤＴＭＦトーンをセキュリティ保護すること(Securing DTMF Tones)

図１は、セキュリティデバイス１０２(security device)が、電話１０４と、セキュアサーバ(secure server)１０８との間のある種の通信をセキュリティ保護するために通信回線に沿って電話１０４に結合されることができるシステムを示している。セキュリティデバイス１０２は、電話１０４と、通信ネットワーク１０６との間の電話回線上でインラインに、あるいは直列に接続されることができる小型フォームファクタのデバイスとすることができる。セキュリティデバイス１０２は、電話１０４の近くの、またはそれに近接した電話回線に結合されることができる。

【００４０】

一例においては、セキュリティデバイス１０２は、アカウントおよび／または発行機関(issuing institution)１０８（例えば、銀行、クレジットカード会社など）に関連づけられることができる。例えば、銀行は、そのようなセキュリティデバイス１０２をその顧客に対して支給することができ、各セキュリティデバイスは、顧客、または顧客のアカウントに一意に関連づけられる。発行機関１０８は、顧客との電話トランザクションを容易にするセキュリティサーバ１１０を有することができる。

【００４１】

図２は、図１の電話１０４と、発行機関１０８に属するセキュリティサーバ１１０との間のある種の通信をセキュリティ保護するための一方法を示す流れ図である。セキュリティデバイス１０２は、アクティブモードのオペレーションと、非アクティブ（パッシブ）モードのオペレーションとを有することができる。セキュリティデバイス１０２が、発行機関１０８（例えば、セキュリティサーバ１１０）以外の誰かを呼び出すために使用されるときには、それは非アクティブであり、そしてその呼出しは、ＤＴＭＦトーンを含めて、不変に、ただセキュリティデバイス１０２を通過する。しかしながら、電話１０４が、発行機関に対して呼出しを開始する２０８ときに、セキュリティサーバ１１０（例えば、セキュリティサーバ１１０）は、セキュリティデバイスをウェイクアップする(wakes up)アクティブ化信号(activation signal)を送信する２１０。アクティブ化信号は、セキュリティデバイス１０２が、一致によってトリガされる可能性が高くないことをかなり確実にするのに、十分に長く、かつ／または一意である（例えば、十分なディジットまたはシンボルを有する）ようにすることができる。一例においては、このアクティブ化信号は、どのような情報も実際には搬送することができず、非アクティブ（パッシブ）モードからアクティブモードへと切り換えるために、ただセキュリティデバイス１０２をトリガし、あるいはアクティブにするだけである。例えば、アクティブ化信号は、セキュリティデバイス１０２によって認識される短い一片の音楽またはトーンとすることができる。セキュリティデバイス１０２は、セキュリティサーバ１１０からのアクティブ化信号（例えば、ＤＴＭＦトーンの一意の組）をリッスンし(listens)、認識し、そしてアクティブモードへと変化する２１２。一例においては、アクティブ化信号を受信するとすぐに、セキュリティデバイス１０２は、電話からセキュリティサーバ１１０へのすべてのＤＴＭＦトーンを暗号化することを開始することができる。

【００４２】

１つのコンフィギュレーションにおいては、チャレンジ－レスポンススキーム(challenge-response scheme)が、セキュリティデバイス１０２と、セキュリティサーバ１１０との間でインプリメントされることができる。アクティブ化信号に加えて、セキュリティサーバ１１０は、ランダムなチャレンジをセキュリティデバイスに対して送信する２１４ことができる。セキュリティデバイス１０２は、チャレンジを受信し、応答（例えば、識別

子、およびチャレンジに対するレスポンス）を生成し２１６、そしてセキュリティサーバ１１０に対してその応答を送信する。応答は、セキュリティデバイス１０２に関連する識別子と、チャレンジに対するレスポンスとを含むことができる。セキュリティデバイス１０２は、電話１０４からセキュリティサーバ１１０への後続のＤＴＭＦトーンを暗号化するために使用されることができるセッションキー(session key)を生成することもできる。

【００４３】

応答は、セキュリティサーバ１１０に、それが、関連するセキュリティデバイスと通信していること、を通知する。セキュリティサーバ１１０は、特定の顧客のアカウントをルックアップする(look-up)２２０ためにその識別子を使用することができ、それによって、顧客が彼ら自体を手動で識別するトラブルを不要にする(saving)（例えば、顧客に、彼らのアカウント番号を入力させることを避ける）。セキュリティサーバ１１０は、ユーザを認証するために、セキュリティデバイス１０２とセキュリティサーバ１１０との両方において用意される、認証キー(an authentication key)とランダムなチャレンジ(random challenge)とに基づいて、レスポンスが正しいことを検証する(verify)２２２こともできる。セキュリティデバイス１０２は、ユーザの電話に近接して（例えば、ユーザのホームの内側に）位置するので、攻撃者は、攻撃を開始するためにはそれを盗まなければならないであろうことに、留意が必要である。

【００４４】

同じチャレンジとレスポンスとを使用することにより、セキュリティサーバ１１０は、セキュリティデバイス１０２が計算する２２４ときに、同じセッションキー(session key)を計算する２２６。セキュリティサーバ１１０が、それがセキュリティデバイス１０２から受信する応答と意見を異にする（あるいはレスポンスを全く受信しない）場合、その呼出しは、より説得力のある識別および／または認証のために代替経路に迂回させられることができる。すなわち、セキュリティデバイス１０２は、受信されたランダムなチャレンジと認証キーとに基づいてそのレスポンスを計算することができる。次いで、セキュリティサーバ１１０は、ローカルなレスポンスを（ランダムなチャレンジと認証キーとに基づいて）計算することにより、受信されたレスポンスを検証し、そしてそれをセキュリティデバイス１０２からの受信されたレスポンスと比較することができる。

【００４５】

チャレンジ－レスポンスが、適切に認証される場合、セキュリティサーバ１１０は、新しく導き出されたセッションキーを使用して、認証される確認(confirmation that is authenticated)を送信する２２８。この確認は、電話１０４からやって来るＤＴＭＦトーンを暗号化することを開始するようにセキュリティデバイス１０２に通知する。セキュリティサーバからの確認に伴う問題が存在する（例えば、それが、ある種の最大時間内にセキュリティデバイス１０２によって受信されない、あるいは確認が、失敗する、などの）場合、セキュリティデバイス１０２は、ユーザに対する警告信号を生成することができる。例えば、チャレンジ－レスポンス認証が失敗する場合、ライトが、フラッシュする（またはＯＮになる）ことができ、あるいはアラームが、鳴ることができる。さらに、ライト（例えば、発光ダイオード－ＬＥＤ）は、セキュリティデバイス１０２が、アクティブであり、かつ／またはチャレンジ－レスポンスが、正常に認証されることを示すように、輝くことができる。

【００４６】

ひとたび、チャレンジ－レスポンスが、正常に認証された後に、一例においては、セッションキーは、電話１０４からセキュリティサーバへの送信を暗号化するためにセキュリティデバイス１０２によって使用されることができる。ひとたび暗号化が開始された後に、セキュリティデバイスは、電話からやって来るＤＴＭＦトーンを遮断し２３２、そしてその代わりに暗号化されたＤＴＭＦトーンを送信する２３４。ＤＴＭＦトーンのそのような暗号化の一例においては、電話１０４からのＤＴＭＦトーンは、異なるＤＴＭＦトーンへと変換されることができ、この異なるＤＴＭＦトーンは、次いでセキュリティサーバ１

１０に対して送信される。別のコンフィギュレーションにおいては、ＤＴＭＦトーンは、セキュリティデバイス１０２によってデジタルシンボルに変換されることができ、これらのデジタルシンボルは、次いで暗号化され、そしてセキュリティサーバ１１０に対して送信される。セキュリティデバイス１０２はまた、他のどんなもの（非ＤＴＭＦトーンまたは信号）でもそれを修正すること、または暗号化することなしに、両方向に渡す。ユーザが要求されることができる第１の物事のうちの１つは、それらのアカウントに関連するＰＩＮ番号を入力することであるので、このＰＩＮ番号に関連するＤＴＭＦトーンは、暗号化され、そして認証のための第２のファクタを形成することができる。同様に、セキュリティサーバ１１０は、電話からセキュリティデバイスを経由して受信されるＤＴＭＦトーンを暗号解読する２３６ためにセッションキーを使用することができる。

【００４７】

代替コンフィギュレーションにおいては、セキュリティデバイス１０２は、特定の発行機関１０８に関連する特定の電話番号（単数または複数）を認識するように構成されていることができる。セキュリティデバイス１０２が、電話が特定の電話番号をダイアルしていることを認識するときに、そのセキュリティデバイスは、アクティブモードに自動的に切り換わり、かつ／または電話からセキュリティサーバ１１０へのすべてのＤＴＭＦトーンを暗号化することができる。

【００４８】

セキュリティデバイス１０２は、呼出しが終了されるまで電話１０４からのＤＴＭＦトーンを暗号化し続けることができ、このポイントにおいて、セキュリティデバイス１０２は、非アクティブモードに切り換わって戻り、ここでセキュリティデバイスは、すべてのＤＴＭＦトーンが、不変に通過することを可能にする。

【００４９】

セキュリティデバイス１０２は、小型フォームファクタを有することができるので、それは、電話回線に容易にプラグインされることができる。ユーザは、ユーザが、異なるロケーション（例えば、ホーム、オフィスなど）からアカウントにセキュリティ上安全にアクセスすることができるようにするために、単一の機関またはアカウントに関連する複数のセキュリティデバイスを有することができる。ユーザはまた、様々な異なる機関および／またはアカウントに関連する複数のセキュリティデバイスを有することもできる。これらの複数のセキュリティデバイスは、電話回線に沿って直列に結合されることができる。チェーンの中の非アクティブなセキュリティデバイスは、ただそのチェーンの中の次のセキュリティデバイスに信号を渡すだけである。チェーンの中のセキュリティデバイスが、セキュリティサーバによってアクティブにされる場合、そのときには、それは、電話からのＤＴＭＦトーンを暗号化する。

【００５０】

別の例においては、セキュリティデバイス１０２は、１つの電話またはロケーションから、複数のユーザにサーブする(serve)ことができる。そのような場合には、セキュリティサーバは、セキュリティデバイスが、複数のユーザまたはアカウントに関連することを識別することができる。各ユーザの間で区別するために、セキュリティサーバは、特定のユーザまたはアカウントを識別するＰＩＮまたは他の識別子を入力するようにユーザに要求する音声プロンプト(voice prompt)を送信することができる。

【００５１】

図３は、送信中にＤＴＭＦトーンをセキュリティ保護することを可能にすることができるテレサービスセキュリティサーバの一例のブロック図を示している。セキュリティサーバ３０２は、小型および／または低パワーのマイクロプロセッサなどの処理回路(processing circuit)３０４を含むことができる。セキュリティサーバ３０２は、セキュリティサーバ３０２を通信ネットワークに結合するために使用される第１の通信モジュール３０６を含むことができる。認証モジュール(authentication module)３０８は、セキュリティサーバ３０２が、それが通信するセキュリティデバイスを認証することを可能にする。ＤＴＭＦ暗号解読モジュール(DTMF decryption module)３０８は、セキュリティサーバ３０

２が、セキュリティデバイスから受信される暗号化されたＤＴＭＦトーンを暗号解読する(decrypt encrypted DTMF tones)ことを可能にする。

【００５２】

図４は、電話デバイスからのＤＴＭＦトーンをセキュリティ保護するための、セキュリティサーバ上で動作する一方法を示している。呼出しが、ＤＴＭＦがイネーブルにされた電話(DTMF-enabled telephone)から受信される４０２。アクティブ化信号が、ＤＴＭＦがイネーブルにされた電話に関連するセキュリティデバイスに対して送信される４０４。セキュリティデバイスは、ＤＴＭＦがイネーブルにされた電話に近接して近くに位置することができる。次いで、セキュリティデバイスは、セキュリティサーバによって認証される。例えば、チャレンジ信号が、セキュリティデバイスに対して送信される４０６。セキュリティサーバは、レスポンスが、セキュリティデバイスから受信されるかどうか４０８を決定する。受信されない場合、そのときには、セキュリティデバイスが、電話回線(telephone line)上に存在していない４１０ことが仮定されることができる。そうでない場合には、セキュリティサーバは、受信されたレスポンスが、正常に認証される(successfully authenticated)ことができるのかどうか４１２を決定する。受信されたレスポンスが、正常に認証されることができない場合、そのときには認証は、失敗する４１４。そうでない場合には、セッションキーが、生成される４１６。セッションキーによって認証される確認メッセージが、セキュリティデバイスに送信される４１８。セキュリティサーバは、セキュリティデバイスからの暗号化されたＤＴＭＦトーンを受信する４２０ことができる。次いで、セキュリティサーバは、電話によって送信される情報を得るために受信されたＤＴＭＦトーンを暗号解読する４２２ことができる。そのようなＤＴＭＦトーンは、元のＤＴＭＦトーンを暗号化することにより送信中に盗聴者から保護される機密情報（例えば、アカウント番号、パスワード、ＰＩＮなど）を表すことができる。

【００５３】

図５は、送信中にＤＴＭＦトーンを保護するように構成されていることができるセキュリティデバイスの一例のブロック図を示している。セキュリティデバイス５０２は、小型および／または低パワーのマイクロプロセッサなどの処理回路５０４を含むことができる。セキュリティデバイス５０２は、それが結合される電話回線によって電力を供給されることができる。第１の通信インターフェースＡ５０６は、セキュリティデバイス５０２を電話に結合するために使用されることができる。第２の通信インターフェースＢ５０８は、セキュリティデバイス５０２を通信ネットワークに結合するために使用されることができる。パッシブモードのオペレーションにおいては、セキュリティデバイス５０２は、すべてのＤＴＭＦトーンを不変に通過させる。処理回路５０４は、（例えば、セキュリティサーバからの）アクティブ化信号をリッスンするように構成されていることができる。ＤＴＭＦ検出器５１０は、セキュリティデバイスをアクティブモードのオペレーションに切り換えるＤＴＭＦアクティブ化信号を検出するように構成されていることができる。アクティブモードにおいては、セキュリティデバイス５０２は、セキュリティサーバからの認証チャレンジにレスポンスする(respond)ように構成されていることができる。

【００５４】

アクティブ化モードにおいては、ＤＴＭＦ検出器５１０はまた、通信インターフェースＡ５０６を経由して受信される（例えば、電話からやって来る）ＤＴＭＦトーンを検出するように構成されていることもできる。１つまたは複数のＤＴＭＦトーンが、検出される場合、ＤＴＭＦトーンは、暗号化され、あるいはそうでなければＤＴＭＦ暗号化モジュール(DTMF encryption module)５１２によって修正される。次いで、暗号化されたＤＴＭＦトーンは、通信インターフェースＢ５０８を通してセキュリティサーバに対して送信される。

【００５５】

図６は、電話デバイスからのＤＴＭＦトーンをセキュリティ保護するための、セキュリティデバイス上で動作する一方法を示している。セキュリティデバイスは、呼出しが、電話とセキュリティサーバとの間で開始されるとすぐに電力を供給される６０２。すなわち

、呼出しが行われるときに通信回線はエネルギーが供給されるので、セキュリティデバイスは、通信回線からその電力を引き出すことができる。パッシブモード(passive mode)のオペレーションにおいて、セキュリティデバイスは、ＤＴＭＦトーンが、第１の通信インターフェースと、第２の通信インターフェースとの間を不変に通過する(pass through unchanged)ことを可能にする６０４。例えば、第１の通信インターフェースは、電話に結合されることができ、そして第２の通信インターフェースは、第２の通信インターフェースに結合されることができる。セキュリティデバイスは、（ＤＴＭＦ）アクティブ化信号が、セキュリティサーバから受信されるかどうか６０６を決定するように送信を監視する。セキュリティデバイスは、アクティブ化信号が受信されない限り、パッシブモードで動作することを継続する。ＤＴＭＦアクティブ化信号が、受信される場合、セキュリティデバイスは、アクティブモードのオペレーションへと変化する６０８。セキュリティデバイスはまた、セキュリティサーバからの他の信号をリッスンする６１０こともできる。

【００５６】

セキュリティデバイスは、セキュリティサーバからのチャレンジを受信する６１２ことができる。セキュリティデバイスは、そのチャレンジに対してレスポンスで応答する６１４。そのレスポンスが、有効である場合、セキュリティデバイスは、セキュリティサーバが、セキュリティデバイスを正常に認証していることを示す確認を受信する６１６ことができる。

【００５７】

ひとたびアクティブ化され、そして適切に認証された後に、セキュリティデバイスは、電話からのＤＴＭＦトーンをリッスンする。ＤＴＭＦトーンが、（セキュリティデバイスが結合される）電話から第１の通信インターフェース上で受信される６１８場合、受信されたＤＴＭＦトーンは、異なるＤＴＭＦトーンへと暗号化される６２０。一例においては、電話からのＤＴＭＦトーンは、異なるＤＴＭＦトーンへと変換されることができ、この異なるＤＴＭＦトーンは、次いでセキュリティサーバへと送信される。別のコンフィギュレーションにおいては、ＤＴＭＦトーンは、セキュリティデバイス１０２によってデジタルシンボルへと変換されることができ、このデジタルシンボルは、次いで暗号化され、そしてセキュリティサーバに対して送信される。次いで、暗号化されたＤＴＭＦトーンは、第２の通信インターフェース上でセキュリティサーバへと送信される６２２。セキュリティデバイスは、呼出しが終了するまで、電話からのＤＴＭＦトーンを暗号化し続け、その時に、セキュリティデバイスは、パッシブモードに戻る６２４。セキュリティデバイス１０２は、電話からの暗号化されていないＤＴＭＦトーンが、セキュリティサーバに対して渡らないようにする。一例においては、セキュリティデバイス１０２は、ネットワークがアクティブである間にすべての入力（例えば、送信）を電話から切り離すことができる。この場合においては、例えば、顧客が、代理人(representative)と話す必要がある場合、顧客またはセキュリティサーバのいずれかが、入力を再接続する（例えば、セキュリティデバイス１０２からの送信を可能にする）ための何らかの用意が存在していてもよい。

【００５８】

セルラ電話のセキュリティスキーム(Cellular Phone Security Scheme)

図７は、セキュリティサーバを用いてそれ自体を認証するように構成されたモバイル通信デバイスのブロック図である。モバイル通信デバイス７０２は、通信モジュール７０６と、ユーザ入力インターフェース７０８とに結合される処理回路７０４を含んでいる。通信モジュール７０６は、モバイル通信デバイス７０２が、ワイヤレス通信ネットワーク７１０上で通信することを可能にする。処理回路７０４は、呼出し中に１つまたは複数のセキュリティサーバを用いてそれ自体を認証するように構成されていることができる。例えば、モバイル通信デバイスは、銀行または金融機関が、モバイル通信デバイス７０２のユーザを認証することを可能にする認証キーおよび／またはユーザ識別子を用いて構成されていることができる。認証キーおよび／またはユーザ識別子は、銀行または金融機関によって事前に（例えば、セットアップまたはコンフィギュレーション中に）提供されることができる。さらに、処理回路７０４はまた、認証プロシージャを完了するためにユーザか

らのＰＩＮ、パスワード、および／または他の入力を要求することもできる。

【００５９】

図８は、通信ネットワーク上でテレサービス局８０４に対してモバイル通信デバイス８０２を認証するための一方法を示す流れ図である。モバイル通信デバイス８０２は、モバイル電話とすることができ、そしてテレサービス局８０４は、銀行または金融機関に関連づけられたセキュリティサーバを含むことができる。モバイル通信デバイス８０２とテレサービス局８０４(tele-services station)とは、おのおの同じ認証キーを有することができる。

【００６０】

モバイル通信デバイスは、テレサービス局に関連する発行機関に対して呼出しを開始する８０６ことができる。発行機関は、例えば、銀行または金融機関とすることができる。テレサービス局は、モバイル通信デバイスに対してランダムな認証チャレンジ(random authentication challenge)８０８を送信する。次いで、モバイル通信デバイスは、ランダムなチャレンジと、認証キーとに基づいてレスポンスを生成し８０９、そしてレスポンスと、（もしかすると）ユーザ識別子とをテレサービス局に対して送信する８１０。次いで、テレサービス局は、モバイル通信デバイスからのレスポンスが、正しいかどうかを検証する８１２。その認証キーと、ランダムな認証チャレンジとに基づいて検証値を計算し、そしてそれをモバイル通信デバイスから受信されるレスポンスと比較するテレサービス局によって行われることができる。レスポンスが、正常に認証される場合、認証確認(authentication confirmation)８１４は、モバイル通信デバイスに対して送信されることができる。モバイル通信デバイスは、テレサービス局からの慎重な扱いを要する情報(sensitive information)（例えば、銀行アカウント記録など）を要求する８１６ことができる。モバイル通信デバイスが、正常に認証される場合、そのときには、テレサービス局は、要求された、慎重な扱いを要する情報をモバイル通信デバイスに対して供給する８１８。このようにして、モバイル通信デバイス（例えば、モバイル電話）は、呼出し中に慎重な扱いを要する情報の送信をセキュリティ保護するために、テレサービス局によって認証されることができる。

【００６１】

脅威モデル(Threat Models)

ここにおいて説明されるセキュリティデバイスおよび／または方法によって対処される１タイプの脅威(threat)は、盗聴攻撃である。そのような攻撃においては、攻撃者は、電話上でユーザによって入力される番号に関連するＤＴＭＦトーンをリッスンするために、電話線に対してレコーダを攻撃することができる。これらのＤＴＭＦトーンは、個人および／または機密の情報のうちでもとりわけ、呼び出されている銀行、ユーザの顧客番号および／またはアカウント番号、個人識別番号（ＰＩＮ）、社会保障番号を、識別することができる。次いで、攻撃者は、ユーザのアカウントからの不正なトランザクションを実行するためにこの情報を使用することができる。ここにおいて説明されるセキュリティデバイスは、ＤＴＭＦトーンを暗号化すること、およびさらなる認証を提供することにより、そのような攻撃を打ち負かす(defeat)。ほとんどの機関（例えば、銀行など）は、認証についての２つのファクタ（例えば、セキュリティデバイスの所有と、ＰＩＮの知識と）を使用することができるので、他の慎重な扱いを要する情報を要求する必要があることは、まれであることになる。暗号化されたＤＴＭＦトーンを単に遮断することは、対応するアカウント番号、ＰＩＮなどについて何も明らかにはしない。

【００６２】

攻撃者は、成功するためには、例えば、呼出しが、対象とする(received)レシーバ（例えば、対象とする銀行）へと進まないようにすることにより、呼出しの進行に干渉し、呼出し者にすべての慎重な扱いを要する情報を入力するように要求して、対象とする(intending)レシーバのふりをする必要があることになる。そのような攻撃を打ち負かすためには、セキュリティデバイスは、「暗号化開始(start encrypting)」信号（すなわち、認証された確認）が、受信機関から受信された後に、セキュリティインジケータ（例えば、ラ

イト）をオン(On)にすることができる。呼出し者（例えば、顧客）は、セキュリティデバイスが、任意の慎重な扱いを要する情報または機密情報を入力する前にそのトーンを暗号化していることを確認するために、ただセキュリティインジケータを検査するだけである。

【００６３】

別のタイプの攻撃は、セッションハイジャック攻撃(session hijacking attack)とすることができ、ここでは、攻撃者は、ユーザが、対象とするレシーバ（例えば、銀行）との通信を確立するまで待ち、そのようにして、セキュリティインジケータをアクティブにし、そしてその後に呼出しを乗っ取る。次いで、攻撃者は、呼出しと共に何かが間違ったようなふりをし、そしてユーザに慎重な扱いを要する情報を口頭で提供するように要求することができる。代わりに、攻撃者は、ユーザに、トーン毎の暗号パターンを確立することを試みるために（攻撃者に既に知られている）特定のレスポンスを入力するように要求し、そしてその後に、銀行に対する彼ら自体のレスポンスを暗号化するためにトーン毎の会話を使用することができる。このタイプの攻撃に対処するために、トーン毎の暗号化は、擬似ランダムベース、回転ベース、および／または番号からトーンの関係の発見を禁止する他のベース、に基づいて変更され、あるいは修正されることができる。

【００６４】

メッセージおよびセッションの認証(Message and Session Authentication)

セキュリティデバイスは、例えば、メッセージ認証コード(Message Authentication Code)（ＭＡＣ）ファンクションを使用することにより、メッセージ認証とセッションキー導出とを実行するように構成されていることができる。例えば、セキュリティサーバは、MAC_Kの単一の呼出し（チャレンジ）から出力を分離することにより、呼出し者のセキュリティデバイスを認証することができる。例えば、典型的なＭＡＣファンクションは、１２８ビットの出力を戻すことができ、これは、３２個のＤＴＭＦトーンとして表されることができる。セキュリティサーバと、セキュリティデバイスとが、ＭＡＣを計算した後に、セキュリティサーバは、（ＭＡＣの一部分を表す）第１の１６個のＤＴＭＦトーンをセキュリティデバイスに対して送信することができ、そして、レスポンスの形で、セキュリティデバイスは、（ＭＡＣの他の一部分を表す）他の１６個のＤＴＭＦトーンを返信する。このようにして、セキュリティサーバと、セキュリティデバイスとの両方は、それらが、認可され、あるいは合法的であることを互いに証明することができる。

【００６５】

同様に、セッションキー(session key)は、$Session\ Key = MAC_K$（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｋｅｙ||Ｃｈａｌｌｅｎｇｅ））であるように、おのおのの側について(by each side)計算されることができ、ここで認証キー(authentication key)は、セキュリティデバイスへとあらかじめロードされる。セキュリティデバイスが、そのレスポンスをセキュリティサーバに対して送信するときに、セッションキーが、開示されないようにするために、レスポンスは、追加の情報を含んでいてもよい。例えば、レスポンス(response)は、$Response = MAC_K$（「余分な情報ストリング(extra information string)」||Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｋｅｙ||Ｃｈａｌｌｅｎｇｅ）とすることができる。

【００６６】

ストリーム暗号化(Stream Encryption)

別の特徴は、暗号化されたシンボルのセキュリティを保護する効率的な暗号化方法を提供する。各平文シンボルは、別個の擬似ランダムに選択された変換テーブルを使用することにより暗号化される。シンボルのあらゆる可能な順列をあらかじめ記憶しておくのではなくて、変換テーブルは、擬似乱数と、シンボルシャッフリングアルゴリズムとに基づいてオンザフライで効率的に生成されることができる。受信デバイスは、同様に、受信された暗号化シンボルを暗号解読するために逆変換テーブルをオンザフライで生成することができる。

【００６７】

この暗号化方法は、様々なコンフィギュレーションでインプリメントされることができる。例えば、電話セキュリティデバイスは、ＤＴＭＦトーンをデジタル値へと変換し、各デジタル値について擬似ランダムに選択された変換テーブルを使用することにより、そのデジタル値を暗号化することができる。次いで、暗号化されたデジタル値は、デジタル形式で、または暗号化されたデジタル値に関連するＤＴＭＦトーンとしてのいずれかで、セキュリティサーバ（例えば、テレサービス局）へと送信されることができる。

【００６８】

ＤＴＭＦトーンは、デジタルシンボルによって表され（あるいは、それに関連づけられ）るので、それらは、例えばストリーム暗号化によってセキュリティ保護されることができる。様々な例においては、ストリーム暗号化は、カウンターモード、出力フィードバック(Output Feedback)（ＯＦＢ）モード、または暗号文フィードバック(Ciphertext Feedback)（ＣＦＢ）モードの高度暗号化規格(Advanced Encryption Standard)（ＡＥＳ）などのブロック暗号(block cipher)によって生成されるキーストリームを使用することができる。例えば、ＭＡＣファンクションは、ＣＢＣ－ＭＡＣモードのブロック暗号を用いてインプリメントされることができる。これは、例えば、セキュリティデバイスが、ＡＥＳをハードウェアでインプリメントしている場合に、有利とすることができる。

【００６９】

これらのファンクションが、ソフトウェアでインプリメントされる場合、非線形ＳＯＢＥＲ(Non-linear SOBER)（ＮＬＳ）などの専用化ストリーム暗号を使用することが好ましい可能性がある。ストリーム暗号はまた、キーまたは臨時の入力として暗号化されるべきデータを使用すること、次いで出力キーストリームを生成することにより、低効率ではあるが、ＭＡＣファンクションとして使用されることもできる。生成されるキーストリームの長さは、できるだけ望ましいものとすることができるので、レスポンスと、セッションキーとの両方は、単一の呼出しの中で生成されることができる。

【００７０】

（真のストリーム暗号を使用しようと、ストリーミングモードのブロック暗号を使用しようと）従来のストリーム暗号化は、通常、擬似乱数のキーストリームを生成することと、暗号化された出力または暗号文を形成するためにそれらを平文（すなわち、ＤＴＭＦトーンのデジタル表現）と組み合わせることと、により進行する。普通は、キーストリームと平文とは、それが自己反転であるので、排他的論理和（ＸＯＲ）演算を使用して組み合わされる。しかしながら、従来のＤＴＭＦがイネーブルにされた電話は、各キーが固有のトーンを有する１０個以上のキーを有する。それ故に、ＸＯＲ演算は、キーストリームを用いて前記ＤＴＭＦトーンを暗号化するために使用されることができない。その代わりに、電話キーに関連するＤＴＭＦトーンは、暗号化されたシンボルまたは暗号文を生成するためにキーストリームから得られる擬似ランダムな数／シンボルに追加されることができる異なるデジタルシンボルへと変換される（またはそれに関連づけられる）ことができる。しかし、特定のディジットの位置を知っているアクティブな攻撃者は、送信された暗号文から数を差し引くことによりその数を変更することができる。例えば、特定のＤＴＭＦトーンの場合に、入力が、「１」であったが、出力は「７」であったことを知っている攻撃者は、このトーンについて生成された擬似乱数は、「６」であったことを決定することができ、そしてそのときには、特定のディジット位置についての彼らの選択した任意のキャラクタを正しく暗号化することができる。

【００７１】

組み合わせコンバイナ(Combinational Combiner)

１つの特徴は、暗号化されるべき各平文シンボルについて擬似ランダムに選択され、あるいは生成された変換テーブルを得るために、または生成するためにキーストリームを使用することを提供する。キーストリームから擬似乱数を取ることと、平文を同じように（例えば、モジュロｎを加算することにより）変更することとの代わりに、１つの特徴は、複数の変換テーブルのうちの１つを擬似ランダムに選択することにより、各平文シンボルを入力ストリームに変換することを提供する。変換テーブルは、数またはシンボルの組の

異なる可能な順列を提供することができる。これは、ここにおいて組み合わせコンバイナと称される。

【００７２】

図９は、暗号化されるべき各シンボルについて変換テーブルを擬似ランダムに選択することにより、平文シンボルをセキュリティ保護するための組み合わせコンバイナのブロック図を示している。暗号ジェネレータ９０２は、擬似ランダムな数／シンボル(pseudorandom numbers/symbols)のキーストリーム(keystream)Ｓｉ９０４を生成するために使用される。キーストリーム９０４の擬似乱数は、入力ストリームの中の各平文入力シンボル(plaintext input symbol)Ｐｉ９０８について、複数の可能な変換テーブルから異なる変換テーブル(different translation table)９０６を生成し、または得るために使用される。平文入力シンボル９０８を擬似ランダムな出力へと変換することにより、暗号化された出力シンボル(encrypted output symbol)Ｃｉ９１０が、生成される。

【００７３】

そのような変換オペレーションは、キーストリーム９０４の制御の下で平文入力シンボル９０８の順列を定義する。変換テーブル９０６は、ｎ個の要素のベクトルとして表されることができ、そして平文入力シンボル９０８の変換は、変換テーブル９０６のｐ番目の要素をルックアップすることにより行われることができる。暗号化された出力シンボルＣｉを仮定すると、逆変換は、逆の順列のテーブルを作成することにより、あるいはシンボルＣｉを含む入力を求めてテーブルをサーチすること、およびそのインデックスをｐとして戻すことにより、そのいずれかで行われることができる。

【００７４】

一般的に言って、ｎ個の平文シンボルの組では、ｎ！（階乗）の可能な順列が、存在する。順列は、すべてのそのような順列の組からランダムに選択され、そして平文入力シンボルＰｉ９０８を暗号化された出力シンボルＣｉ９１０（暗号文とも称される）に変換するために変換テーブル９０６として使用されることができる。入力ストリームの中の各平文シンボルについて、擬似ランダムに選択された変換テーブルが、選択される。そのときには、暗号化されたシンボルＣｉ９１０を調べ、そしてそれが、特定の平文シンボルに対応することを知っている攻撃者は、他の平文シンボルと、対応する暗号化されたシンボルとの間の対応について依然として何も知らないままである。すなわち、攻撃者が、確認することができるすべての情報は、暗号化されたシンボルを変更することは、彼らが知っているものとは異なる平文シンボルを与えることになるが、そのようになる他の平文シンボルではないことである。それ故に、擬似ランダムに選択された変換テーブルは、平文入力シンボルと、暗号化された出力シンボル（暗号文）との間の関係を明らかにせず、そして攻撃者は、暗号文シンボル変換に対するどのような単一の平文シンボルの知識も活用することができない。

【００７５】

セキュリティ保護された電話バンキングについての一例においては、電話からセキュリティデバイスによって受信される各ＤＴＭＦトーンは、デジタル平文シンボルへと変換され（またはそれに関連づけられ）る。次いで、平文シンボルは、暗号化されたシンボルを得るために（キーストリームからの１つまたは複数の擬似乱数に基づいて得られる）変換テーブルによって変換される。次いで、暗号化されたシンボルは、（デジタル形式で、または暗号化されたシンボルに対応するＤＴＭＦトーンとしてのいずれかで）セキュリティサーバに送信され、ここでそれは、逆変換テーブルによって暗号解読される。逆変換テーブルは、同じキーストリームを生成するセキュリティデバイスと、セキュリティサーバとの両方において同期化された暗号ジェネレータを有することにより、生成され、または得られることができる。一例においては、暗号ジェネレータは、同じシード(seed)（例えば、セッションキーなど）を使用することにより同期化されることができる。

【００７６】

一例においては、複数の変換テーブルは、あらかじめ生成され、かつ／またはセキュリティデバイスおよび／またはセキュリティサーバによって記憶されることができる。オン

ザフライで新しい変換テーブル（すなわち、入力シンボルの順列）を生成することではなくて、変換テーブルは、あらかじめ生成され、そして記憶されることができる。キーストリーム９０４の擬似ランダムな数／シンボルは、暗号化されるべき各平文シンボルについてのあらかじめ生成された変換テーブルのうちの１つを選択するために使用されることができる。あらかじめ生成された変換テーブルは、ｎ個の平文シンボルの組についてのあらゆる順列、または順列のサブセットを定義することができる。

【００７７】

別の例においては、使用される変換テーブルは、変換テーブルを形成するためにキーストリームを使用することと、擬似ランダムにシンボルをシャッフルすることとにより、オンザフライで生成されることができる。これらのソリューションは、ｎ！個のテーブルが存在することになるという意味で同等であり、そして、これらのテーブルのうちの１つを選択するために必要とされるキーストリームの量は、シャッフルすることによりそのようなテーブルを作成するために必要とされる量と同じであることに注意すべきである。

【００７８】

図１０は、平文シンボル(plaintext symbol)を暗号化されたシンボル(encrypted symbol)に変換するための、シンボルごとの変換テーブル(a symbol-to-symbol translation table)１００２の一例を示している。この例においては、１６個の平文シンボルが、異なる暗号化されたシンボルへと変換される。２進表現は、この例においては、１６個の平文シンボルが、４－ビットの暗号化されたシンボルを使用して、暗号化されることができることを単に示すために示される。より多くの、あるいはより少ない数の平文シンボルが暗号化されるべきであるという他の例においては、異なる数のビットが、各シンボルについて使用されることができる。例えば、２５６個までの平文シンボルの場合には、８ビットが、各暗号化シンボルを生成するためにキーストリームから抽出されることができる。

【００７９】

別の特徴は、特定の変換テーブル内で、平文シンボルと、暗号化されたシンボルとの間の１対１の対応を提供する。すなわち、どの２つの平文シンボルも、特定の変換テーブル内で、同じ暗号化されたシンボルには変換されない。これにより、暗号解読デバイスは、暗号化されたシンボルをその元の平文シンボルへと正確に暗号解読することができるようになる。

【００８０】

暗号解読デバイスにおいては、シンボルごとの逆変換テーブル(a symbol-to-symbol reverse translation table)は、暗号化デバイスのシンボルごとの変換(symbol-to-symbol translation)を逆にし、そしてそれによって受信された暗号化シンボルを暗号解読するように生成されることができる。

【００８１】

図１１は、どのようにして平文シンボル１１０２が、暗号化されたシンボル１１０６を得るために異なる変換テーブル１１０４を使用して暗号化されることができるのかの一例を示している。各平文シンボルＰ０、Ｐ１、Ｐ２、Ｐ３、...Ｐｉについて、おのおのシンボルの異なる順列を有する異なる変換テーブル１１０４が、暗号化されたシンボルＣ０、Ｃ１、Ｃ２、Ｃ３、...Ｃｉを得るために使用される。

【００８２】

組の中のシンボルの数が少ない場合には、そのようなシンボルのすべての順列をリストアップし（すなわち、あらかじめ生成し）、そしてそれらの順列から変換テーブルを選択するために（キーストリームからの）インデックスを使用することを、可能とすることができる。例えば、１２個の可能なシンボルの組の場合には、生成される可能な順列の数は、１２！、すなわち４７９，００１，６００である。順列を適切に選択するためには、３２ビットのキーストリームは、バイアスのない変換テーブルとして１つの順列を選択することで十分とすることができる。しかしながら、このアプローチは、組の中のシンボルの数が、増大するにつれて非効率的になる。例えば、２５６個の可能なシンボルの組の場合には、生成される可能な順列の数は、２５６！、すなわち8.5×10^{506}であり、こ

れは、変換テーブルとして順列のうちの１つを選択するために、擬似ランダムなキーストリームから１６８４ビットを超過して必要とすることになる。

【００８３】

図１２は、１組のｎ個のシンボルについての複数の可能な順列から変換テーブルを選択するためのアルゴリズムを示しており、ここでｎは、正の整数である。この例においては、０と、2^k-1との範囲に一様に分散されたｋビットの長さ（例えば、８ビット、３２ビットなど）の擬似ランダムなキーストリーム値(pseudorandom keystream values)を与える暗号ジェネレータが、使用されることができる。キーストリームは、擬似乱数ｗを得るために使用される１２０２。ｎ！は、2^kに均一に分割することができないので、擬似乱数ｗは、バイアスを導入することなく直接に使用されることができない。この理由のために、最大のしきい値Ｐｍａｘ(maximum threshold Pmax)は、2^kよりも小さいｎ！の最大の倍数(the largest multiple of n! that is less than 2^k)として定義される。もし擬似乱数ｗがこの最大のしきい値Ｐｍａｘよりも小さい場合は、そのときには、それは、バイアスを導入することなく使用されることができる。そうではなくて、もし擬似乱数ｗがこの最大のしきい値Ｐｍａｘ以上である場合は、それは、捨てられ、そして新しい擬似乱数ｗが、最大のしきい値Ｐｍａｘよりも小さい擬似乱数ｗが得られるまで、選択される１２０４。

【００８４】

ｗ＝ｗ　ｍｏｄｕｌｏ（ｎ！）であるように、擬似乱数ｗは（ｎ！）を法として割られる(the pseudorandom number w is divided modulo n! so that w = w modulo (n!))１２０６。それ故に、バイアスされない擬似乱数ｗは、順列（すなわち、変換テーブル）を得るために使用されることができる０からｎ！の範囲の中で得られる。

【００８５】

あらかじめ生成された順列を記憶することと、擬似乱数ｗを使用することにより１つのそのような順列を選択することとではなくて、１つの特徴は、変換テーブルを生成するために基本の順列(base permutation)のシンボルをシャッフルすることにより、順列を生成することを提供する。基本の順列ベクトルＰは、Ｐ＝［０，１，２，...ｎ－１］となるようにシンボルの組のすべての値で初期化される１２０８。次いで、シンボルシャッフリングアルゴリズム１２１０は、擬似乱数ｗを使用して、基本の順列ベクトルＰの中でシンボルをシャッフルするために使用される。

【００８６】

シンボルシャッフリングアルゴリズム１２１０の一例は、カウンタｉからｎ－１を初期化し、ここでｎは、組の中のシンボルの数である。カウンタｉ＞＝０である間に、擬似乱数ｗ＝ｗ／（ｉ＋１）であり、変数ｊ＝ｗ　ｍｏｄｕｌｏ（ｉ＋１）であり、そして順列ベクトルＰの値は、$P_t[i]=P_{t-1}[j]$であり、そして$P_t[j]=P_{t-1}[i]$であるようにシャッフルされる。他のシンボルシャッフリングアルゴリズムも、本開示の特徴を逸脱することなく使用されることができることに注意すべきである。

【００８７】

ひとたび、順列ベクトルＰが、シャッフルされた後に、その順列ベクトルＰは、入力シンボルストリームを暗号化するために、例えば、変換テーブルとしてそれを使用することができる任意のアプリケーションに対して提供される１２１２ことができる。

【００８８】

図１３は、単一の平文シンボルを暗号化するために複数の変換テーブルを使用することにより、シンボル認証を達成することができる別の暗号化スキームを示すブロック図である。すなわち、平文入力シンボルＰｉ１３０２は、第１の暗号化された出力シンボルＣｉ’１３１０を得るために、第１の暗号ジェネレータ１３０８から得られる第１のキーストリームＳｉ’１３０６に基づいて生成され、または選択されることができる変換テーブルＡ１　１３０４によって暗号化される。次いで、第１の暗号化された出力シンボルＣｉ’１３１０は、第２の暗号化された出力シンボルＣｉ１３１８を得るために使用される、第２の暗号ジェネレータ１３１６から得られる第２のキーストリームＳｉ１３１４に基づい

て生成され、または選択されることができる第２の変換テーブルＡ２　１３１２に対する入力としての役割を果たす。このようにして、リダンダンシーが、第１の暗号化された出力シンボルＣｉ’１３１０を認証するために使用されることができる。すなわち、シンボルＣｉ’１３１０とＣｉ１３１８とを一緒に使用することにより、シンボルＣｉ１３１８は、Ｃｉ’１３１０を認証する。それ故に、攻撃者が、例えば、シンボルＣｉ’１３１０を変更する際に成功する場合には、それは、シンボルＣｉ１３１８によって適切に認証されないことになる。

【００８９】

図１４は、どのようにして複数の変換テーブル１４０４および１４０６が、対応する１対の暗号化されたシンボル１４０８を得るために各平文シンボル１４０２を暗号化するために使用されることができるのかを示している。変換テーブル１４０４および１４０６は、各平文シンボルＰｉを１対のシンボルＣｉ’／Ｃｉへと暗号化するために擬似ランダムに選択され、かつ／または生成されることができることに注意すべきである。

【００９０】

図１５は、どのようにして２つの変換テーブルが、平文シンボルＰｎを１対のシンボルＣｎ’およびＣｎへと変換し、または暗号化するために使用されることができるのかの一例を示している。例えば、第１の平文シンボルＰｎ＝「５」の場合には、第１の変換テーブルＡ１　１５０２は、第１の出力シンボルＣｎ’＝８を提供する（すなわち、「５」が、「８」に変換される）。第１の出力シンボル「８」は、そのときには、第２の出力シンボルＣｎ＝７を得るために、第２の変換テーブルＡ２　１５０４に対する入力としての役割を果たすことができる（すなわち、「８」が、「７」に変換される）。第２の出力シンボルＣｎは、第１の出力シンボルＣｎ’に基づいて生成されたので、冗長なシンボルＣｎおよびＣｎ’は、認証のために使用されることができる。いずれかまたは両方のシンボルが、送信中に攻撃者によって変更される場合、そのときには認証は、失敗する。例えば、Ｃｎ’が、「８」から「４」へと攻撃者によって修正される場合、シンボルＣｎ’およびＣｎ＝「４７」を受信する受信者は、Ｃｎ＝「７」が、Ｃｎ’＝「８」であり、「４」ではないことを意味すべきであることを見出すことになる。

【００９１】

第２の平文シンボルＰ（ｎ＋１）は、第１の平文シンボルと、第２の平文シンボルとが、同じである場合でさえ、完全に異なる変換テーブルを有することができる。例えば、第２の平文シンボルＰ（ｎ＋１）＝「５」の場合には、第１の変換テーブルＢ１　１５０６は、第３の出力シンボルＣ（ｎ＋１）’＝「＊」を提供する（すなわち、「５」は、「＊」に変換される）。第３の出力シンボルＣ（ｎ＋１）’＝「＊」は、そのときには第４の出力シンボルＣ（ｎ＋１）＝「１」を得るために第２の変換テーブルＢ２　１５０８に対する入力としての役割を果たすことができる（すなわち、「＊」は、「１」に変換される）。上記のように、シンボル対Ｃ（ｎ＋１）’とＣ（ｎ＋１）との冗長な使用は、認証の一形式としての役割を果たすことができる。

【００９２】

図１６は、一例による、平文暗号化を実行するための一方法を示している。１組のｎ個のシンボル内で定義される複数の入力シンボルが、得られる１６０２。異なるシンボルごとの順列を定義する複数の変換テーブルからの、擬似ランダムに選択された変換テーブルが、暗号化されるべき入力シンボルのおのおのについて得られる１６０４。入力シンボルは、各入力シンボルを個別に暗号化するために入力シンボルのおのおのについてそれらの対応する変換テーブルを使用して対応する出力シンボルへと変換される１６０６。次いで、出力シンボルは、暗号解読デバイスに対して送信される１６０８ことができる。

【００９３】

そのような方法の一例において、第１の平文シンボルが得られ、ここで第１の平文シンボルは、１組の中のｎ個のシンボルのうちの１つとすることができる。ｎ個のシンボルをｎ個のシンボルの異なる順列へと変換する第１の変換テーブルが、得られる。第１の変換テーブルは、ｎ個のシンボルをシャッフルするために擬似乱数を使用することにより擬似

ランダムに生成されることができる。次いで、第１の平文シンボルは、第１の変換テーブルを使用して第１の出力シンボルへと変換される。

【００９４】

ｎ個のシンボルを第１の変換テーブル以外のｎ個のシンボルの異なる順列へと変換する第２の変換テーブルが、得られることができる。第１の出力シンボルは、第２の変換テーブルを使用して第２の出力シンボルへと変換される。次いで、暗号化されたシンボルが、第１および／または第２の出力シンボルに基づいて送信される。

【００９５】

図１７は、どのようにして暗号化されたシンボルＣｉが、単一の平文シンボルを得るために１つまたは複数の逆変換テーブルを使用することにより暗号解読されることができるのかを示すブロック図である。すなわち、暗号化された入力シンボルＣｉ１７０２は、第１の暗号解読された出力シンボルＣｉ’１７１０を得るために、第１の暗号ジェネレータ１７０８から得られる第１のキーストリームＳｉ’１７０６に基づいて生成され、または選択されることができる第１の逆変換テーブルＡ１　１７０４によって暗号解読されることができる。次いで、第１の暗号解読された出力シンボルＣｉ’１７１０は、平文出力シンボルＰｉ１７１８を得るために使用される、第２の暗号ジェネレータ１７１６から得られる第２のキーストリームＳｉ１７１４に基づいて生成され、または選択されることができる第２の逆変換テーブルＡ２　１７１２に対する入力としての役割を果たす。

【００９６】

例えば、Ｃｉ＝（ｘ，ｙ）である代替コンフィギュレーションにおいては、暗号化されたシンボルおよびｙは、平文出力シンボルＰｉを得るために暗号化されたのと逆の順序で暗号解読されることができる。

【００９７】

図１８は、一例による、シンボル暗号解読を実行するための一方法を示している。１組のｎ個のシンボル内で定義される複数の（暗号化された）入力シンボルが、得られる１８０２。異なるシンボルごとの順列を定義する複数の逆変換テーブルからの、擬似ランダムに選択された逆変換テーブルが、暗号解読されるべき入力シンボルのおのおのについて得られる１８０４。各入力シンボルを個別に暗号解読するために入力シンボルのおのおのについてそれらの対応する逆変換テーブルを使用して入力シンボルを対応する出力シンボルへと変換する１８０６。

【００９８】

そのような方法の一例においては、第１の暗号化されたシンボル（入力シンボル）が、得られ、ここでその第１の暗号化されたシンボルは、１組の中のｎ個のシンボルのうちの１つである。ｎ個のシンボルをｎ個のシンボルの異なる順列へと変換する第１の逆変換テーブルも、得られる。第１の逆変換テーブルは、ｎ個のシンボルをシャッフルするために擬似乱数を使用することにより擬似ランダムに生成されることができる。第１の暗号化されたシンボルは、第１の逆変換テーブルを使用して第１の出力シンボルへと変換される。ｎ個のシンボルを第１の変換テーブル以外のｎ個のシンボルの異なる順列へと変換する第２の逆変換テーブルが、得られる。第１の出力シンボルは、第２の逆変換テーブルを使用して第２の出力シンボルへと変換される。次いで、平文シンボルが、第１および／または第２の出力シンボルに基づいて得られることができる。

【００９９】

図１９は、一例による暗号化モジュールを示すブロック図である。暗号化モジュール１９０２は、キーストリームジェネレータ１９０６に対してシードを供給するように構成された処理回路１９０４を含むことができる。キーストリームジェネレータ１９０６は、処理回路１９０４に送られる擬似ランダムな数またはシンボルのキーストリームを生成する。処理回路１９０４に結合された入力インターフェース１９０８は、平文シンボルストリームを受信することができる。平文シンボルストリームを暗号化するために、処理回路１９０４は、変換テーブルジェネレータ１９１０から変換テーブルを得るためにキーストリームから得られる擬似乱数を使用するように構成されていることができる。変換テーブル

ジェネレータ１９１０は、変換テーブルを提供するために擬似ランダムな、バイアスされない方法で、例えば、基本のテーブルのシンボルをシャッフルし、かつ／または組み合わせるために擬似乱数を使用するように構成されていることができる。次いで、処理回路１９０４は、第１の平文シンボルを暗号化されたシンボルストリームの第１の暗号化されたシンボルへと変換するために変換テーブルを一度使用する。暗号化されたシンボルストリームは、処理回路１９０４に結合された出力インターフェース１９１２を介して送信されることができる。平文シンボルストリームの中の各平文シンボルについて、異なる変換テーブルが、そのシンボルを変換するために生成され、そして使用されることができる。

【０１００】

図２０は、一例による暗号解読モジュールを示すブロック図である。暗号解読モジュール２００２は、キーストリームジェネレータ２００６に対してシードを供給するように構成された処理回路２００４を含むことができる。キーストリームジェネレータ２００６は、処理回路２００４に送られる擬似ランダムな数またはシンボルのキーストリームを生成する。処理回路２００４に結合された入力インターフェース２００８は、暗号化されたシンボルストリームを受信することができる。暗号化されたシンボルストリームを暗号解読するために、処理回路２００４は、逆変換テーブルジェネレータ(reverse translation table generator)２０１０から変換テーブルを得るためにキーストリームから得られる擬似乱数を使用するように構成されていることができる。逆変換テーブルジェネレータ２０１０は、変換テーブルを提供するために擬似ランダムな、バイアスされない方法で、例えば、基本のテーブルのシンボルをシャッフルし、かつ／または組み合わせるために擬似乱数を使用するように構成されていることができる。次いで、処理回路２００４は、第１の暗号化されたシンボルを平文シンボルストリームの第１の平文シンボルへと変換するために逆変換テーブルを一度使用する。平文シンボルストリームは、処理回路２００４に結合された出力インターフェース２０１２を介して送信されることができる。

【０１０１】

暗号化モジュール１９０２と、暗号解読モジュール２００２とが、それぞれシンボルを適切に暗号化し、そして暗号解読するために、それらは、同じキーストリームジェネレータを有し、そして相補的な変換テーブルジェネレータを有することができる。キーストリームジェネレータ１９０６と２００６とを同期化するために、共通のシードが、暗号化モジュールと、暗号解読モジュールとの間の特定の通信セッションについて（例えば、セキュリティ保護された認証スキームによって）確立されることができる。例えば、セッションキーは、キーストリームジェネレータ１９０６と２００６とについてのシードとして使用されることができる。

【０１０２】

ここにおいて説明される例のうちのいくつかは、ＤＴＭＦトーンの暗号化について言及しているが、ここにおいて説明される暗号化方法は、送信された情報をセキュリティ保護するために多くの他のタイプの通信システムを用いてインプリメントされることができる。

【０１０３】

図１～１８に示される１つまたは複数のコンポーネント、ステップ、および／またはファンクションは、本発明を逸脱することなく、単一のコンポーネント、ステップ、および／またはファンクションへと並べ換えられ、かつ／または組み合わされ、あるいはいくつかのコンポーネント、ステップ、および／またはファンクションへと分離されることができる。追加の要素、コンポーネント、ステップ、および／またはファンクションもまた、本発明を逸脱することなく、加えられることができる。図１、２、３、５、７、９、１３、１７、１９および／または２０に示される装置、デバイス、および／またはコンポーネントは、図２、４、６、８、１０、１１、１２、１４、１５、１６および／または１８に説明される１つまたは複数の方法、機能、またはステップを実行するように構成されていることができる。

【０１０４】

当業者は、さらに、ここにおいて開示される例に関連して説明される様々な例示の論理ブロック、モジュール、回路、およびアルゴリズムステップが、電子的なハードウェア、コンピュータソフトウェア、またはそれらの両方の組合せとしてインプリメントされることができることを理解するであろう。ハードウェアとソフトウェアとのこの交換可能性を明確に説明するために、様々な例示のコンポーネント、ブロック、モジュール、回路、およびステップは、それらの機能に関して、上記に一般的に説明されている。それらの機能がハードウェアとしてインプリメントされるか、あるいはソフトウェアとしてインプリメントされるかは、特定のアプリケーションと、全体システムに課される設計制約条件と、に依存する。

【０１０５】

上記コンフィギュレーションは、単なる例にすぎず、そして本発明を限定するものとして解釈されるべきでないことに注意すべきである。これらの例の説明は、例示的であり、請求の範囲の範囲を限定すべきでないように意図される。したがって、本教示は、他のタイプの装置、および多数の代替案に対しても容易に適用されることができ、修正、および変形は、当業者にとって明らかであろう。

【図１】

図 1

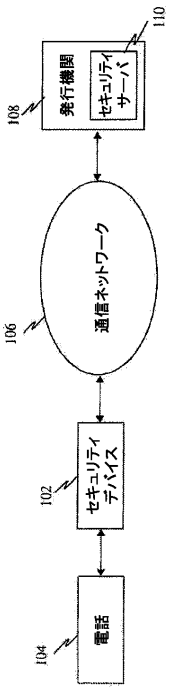


Figure 1

【図２】

図 2

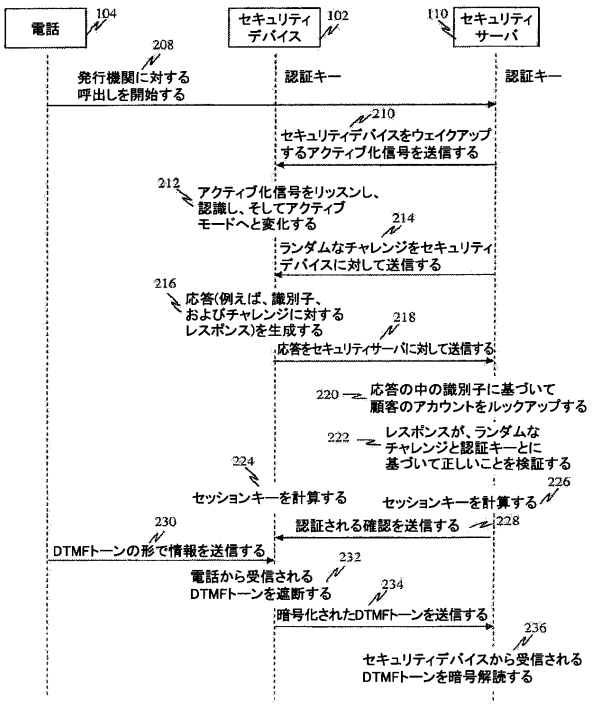


Figure 2

【図３】

図 3

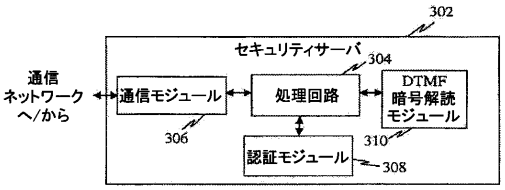


Figure 3

【図４】

図 4

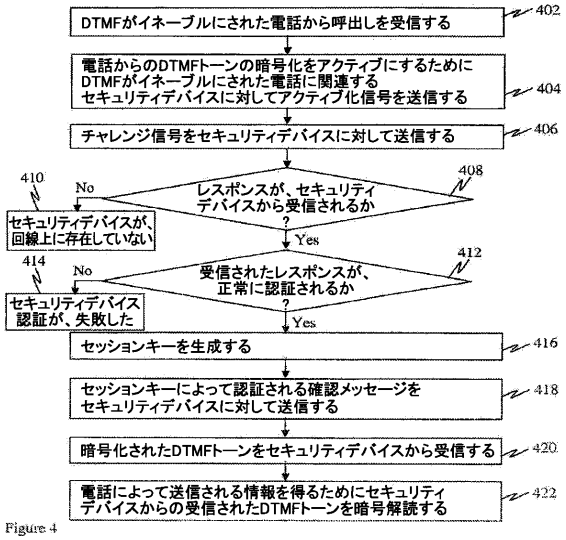


Figure 4

【図５】

図 5

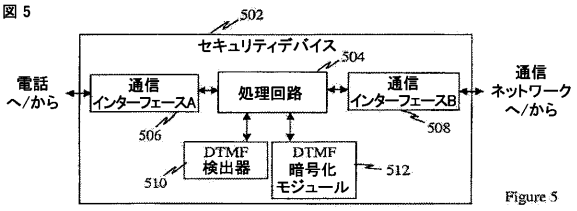


Figure 5

【図６】

図 6

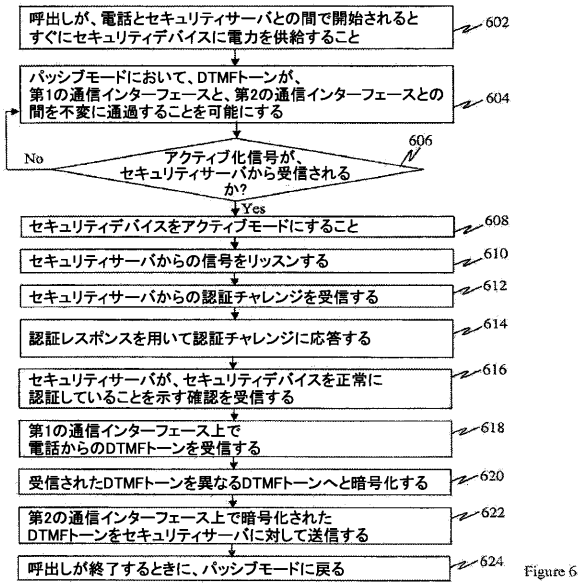


Figure 6

【図７】

図 7

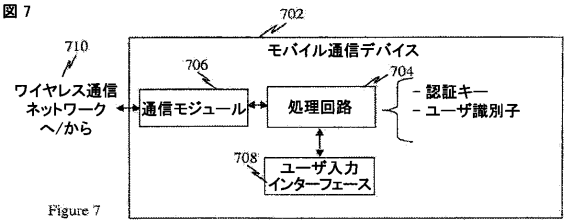


Figure 7

【図８】

図 8

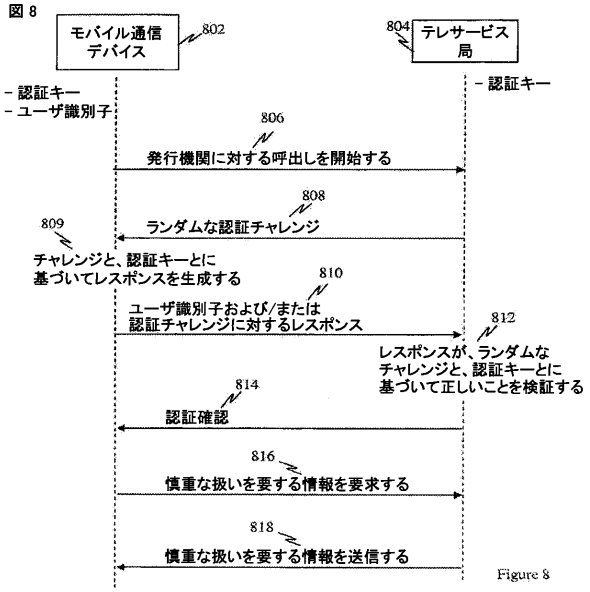


Figure 8

【図９】

図 9

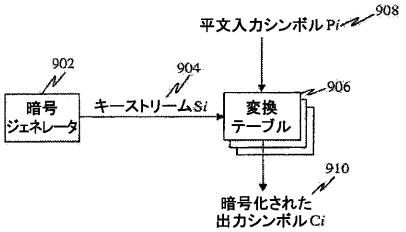


Figure 9

【図１０】

図 10

平文シンボル	平文シンボルの2進数	暗号化されたシンボル	暗号化されたシンボルの2進数
0	0000	5	0101
1	0001	9	1001
2	0010	A	1100
3	0011	0	0000
4	0100	#	1011
5	0101	1	0001
6	0110	C	1110
7	0111	*	1010
8	1000	7	0111
9	1001	B	1101
*	1010	4	0100
#	1011	6	0110
A	1100	D	1111
B	1101	2	0001
C	1110	8	1000
D	1111	3	0011

1002

Figure 10

【図１１】

図 11

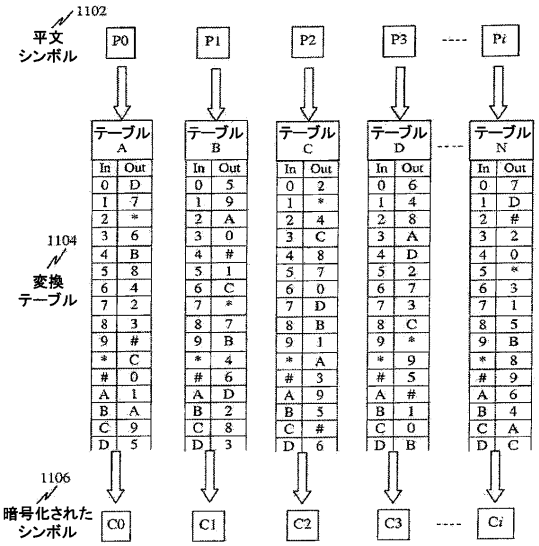


Figure 11

【図１２】

図 12

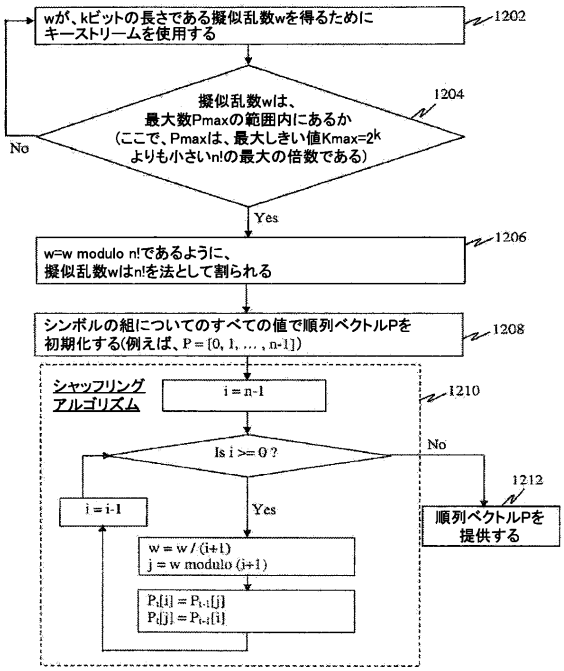


Figure 12

【図１３】

図 13

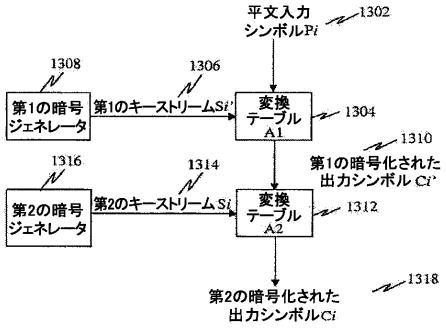


Figure 13

【図１４】

図 14

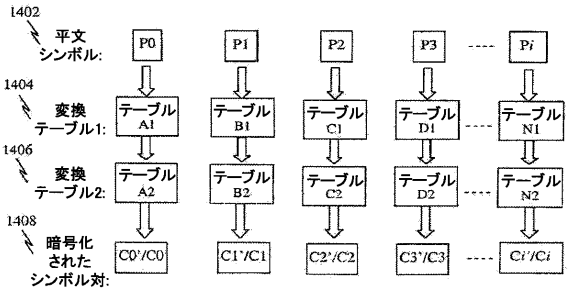


Figure 14

【図１５】

図 15

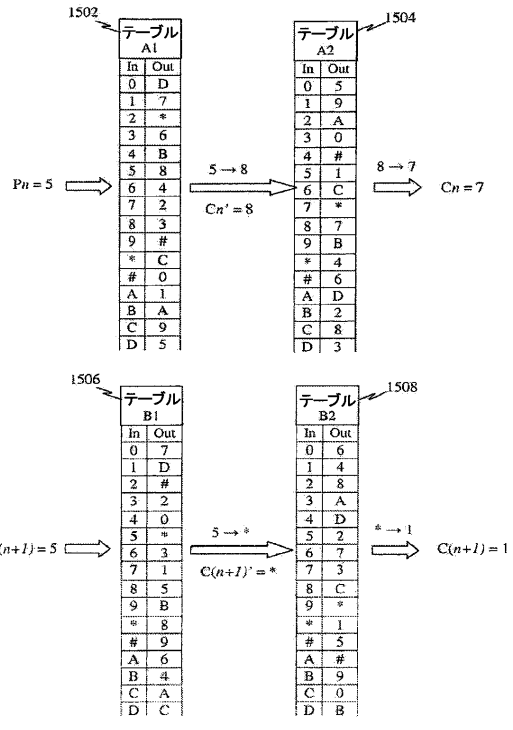


Figure 15

【図１６】

図 16

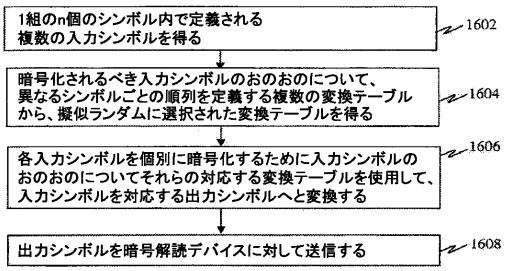


Figure 16

【図１７】

図 17

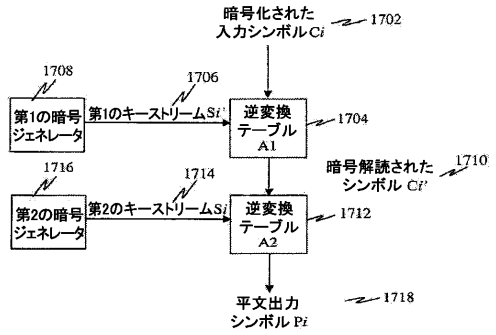


Figure 17

【図１８】

図 18

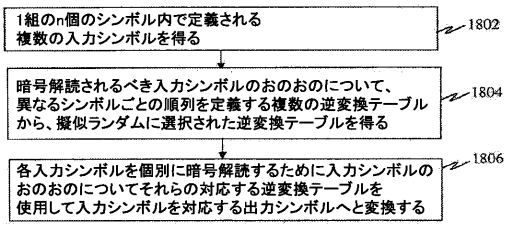


Figure 18

【図１９】

図 19

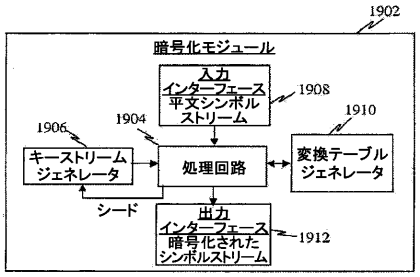


Figure 19

【図２０】

図 20

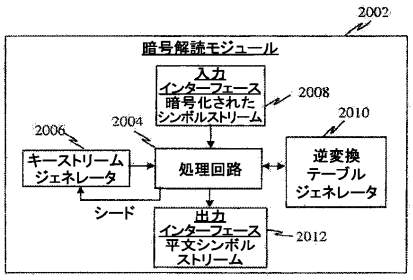


Figure 20

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/087526

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/06 G09C1/00 H04L9/18

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G09C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 979 832 A (RITTER TERRY F [US]) 25 December 1990 (1990-12-25) abstract column 1, line 40 - column 2, line 7 column 8, line 30 - column 11, line 35	1-40
X	US 4 870 683 A (ATALLA MARTIN M [US]) 26 September 1989 (1989-09-26) column 5, line 33 - column 7, line 65 figures 1A,1B,5	1-40
X	US 6 075 859 A (ROSE GREGORY G [AU]) 13 June 2000 (2000-06-13) column 2, line 10 - line 13 column 5, line 21 - column 9, line 5	1-40

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 June 2008	01/07/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Apostolescu, Radu

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/087526

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004/045134 A (TITAN CORP [US]) 27 May 2004 (2004-05-27) page 11, line 20 - page 19, line 19 page 21, line 10 - page 26, line 3	1-40

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/087526

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 4979832	A	25-12-1990	NONE		
US 4870683	A	26-09-1989	AU	594752 B2	15-03-1990
			AU	7060087 A	08-10-1987
			CA	1277421 C	04-12-1990
			EP	0243651 A2	04-11-1987
			JP	2709059 B2	04-02-1998
			JP	62265686 A	18-11-1987
			NZ	219211 A	26-10-1990
US 6075859	A	13-06-2000	AU	6938898 A	29-09-1998
			BR	9808232 A	16-05-2000
			CA	2283304 A1	17-09-1998
			CN	1251232 A	19-04-2000
			EP	0966809 A1	29-12-1999
			FI	991876 A	11-11-1999
			ID	24932 A	31-08-2000
			JP	2001514769 T	11-09-2001
			KR	20060069524 A	21-06-2006
			WO	9840984 A1	17-09-1998
			US	6385316 B1	07-05-2002
			ZA	9802022 A	08-09-1998
WO 2004045134	A	27-05-2004	AU	2002368351 A1	03-06-2004

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 ガントマン、アレクサンダー
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ローズ、グレゴリー・ゴードン
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 チョイ、ジェーヒー

アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　ノーレンバーグ、ジョン・ダブリュ．・ザ・セカンド
アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５

Ｆターム(参考) 5J104 AA01　JA03　NA02　NA10　NA20