【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成24年3月22日(2012.3.22)

【公表番号】特表2010-514272(P2010-514272A)
【公表日】平成22年4月30日(2010.4.30)
【年通号数】公開・登録公報2010-017
【出願番号】特願2009-541567(P2009-541567)
【国際特許分類】
Ｈ０４Ｍ　11/00　　(2006.01)
Ｈ０４Ｍ　 1/68　　(2006.01)
Ｈ０４Ｋ　 1/00　　(2006.01)
Ｈ０４Ｌ　 9/10　　(2006.01)
【ＦＩ】
Ｈ０４Ｍ　11/00　　３０２
Ｈ０４Ｍ　 1/68
Ｈ０４Ｋ　 1/00　　Ｚ
Ｈ０４Ｌ　 9/00　　６２１Ｚ

【誤訳訂正書】
【提出日】平成24年2月3日(2012.2.3)
【誤訳訂正１】
【訂正対象書類名】明細書
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【発明の詳細な説明】
【発明の名称】安全な電話バンキングのための方法および装置
【技術分野】
【０００１】
［分野］
様々な実施例は、一般に電話機の付属装置、より詳細には電話機からの伝送中にデュアルトーン多重周波数（ＤＴＭＦ；dual tone multifrequency）トーンを保護するための装置および方法に関する。
【背景技術】
【０００２】
［背景］
多くの国で電話によってエレクトロニックバンキングが行われ、顧客は銀行の自動サービス番号を呼び出して、メニュー項目、口座番号、個人の識別番号（ＰＩＮ;private identification number）、額などに関して、録音されたプロンプトに応答するのに電話機のキーパッドを使用する。そのような情報は、電話機から銀行のサーバにデュアルトーン多重周波数（ＤＴＭＦ）信号で伝送されることが多い。インターネットによるそのようなトランザクションはセキュアソケットレイヤ（ＳＳＬ;secure socket layer）を用いて保護することが多いが、電話機からのＤＴＭＦトーンについては相当するセキュリティがない。開発途上国では、銀行が、顧客に対してそのような電話サービスを利用可能にすることが多い。しかし、電話線に侵入して顧客口座番号およびＰＩＮなどの機密情報を発見するかまたは獲得し、次いでその口座から金銭を振り込むのにこの情報を用いる悪意のある一味に対して、そのようなサービスは脆弱である恐れがある。
【０００３】
したがって、電話機からＤＴＭＦトーンの伝送を保護するための方法を提供することが

望ましい。暗号化装置を入手すると、顧客についての認証の第２の要素を同時に形成することができ、セキュリティがさらに強化される。

【発明の概要】

【０００４】

［概要］

伝送中にＤＴＭＦトーンを保護するために、スモールフォームファクタ（small form-factor）の電話セキュリティ装置上で動作する方法が提供される。電話機から第１の通信インターフェースによってデュアルトーン多重周波数（ＤＴＭＦ）トーンが受け取られる。電話機から受け取られたＤＴＭＦトーンが暗号化され、暗号化されたＤＴＭＦトーンは、第２の通信インターフェースによってセキュリティサーバへ送られる。セキュリティ装置から活性化信号が受け取られてよく、結果として、セキュリティ装置を能動動作モードにすることができる。能動動作モードでは、電話機から受け取ったＤＴＭＦトーンを暗号化し、かつ音声信号がセキュリティ装置をそのまま通過することが可能になるようにセキュリティ装置を構成してよい。受動動作モードでは、セキュリティ装置は、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の間で電話機からのＤＴＭＦトーンをそのまま通してよい。

【０００５】

セキュリティ装置は、電話機に近接して、電話機とセキュリティサーバの間に直列で結合して配置されてよく、電話機とセキュリティサーバの間の呼の開始に際して電力供給されてよい。

【０００６】

認証を与えるために、セキュリティサーバから認証チャレンジが受け取られてよい。これに応じて、認証応答が作成されてセキュリティサーバへ送られる。セキュリティサーバがセキュリティ装置を成功裡に認証したことを示す確認が、セキュリティサーバから受け取られ得る。

【０００７】

一実施例では、第１の通信インターフェースによって受け取られた第１のＤＴＭＦトーンが第１の記号に変換される。変換表は、複数の変換表から擬似ランダム的に選択される。選択された変換表を用いて第１の記号が第２の記号に変換され、次に第２の記号が第２のＤＴＭＦトーンに変換される。第２のＤＴＭＦトーンは、暗号化されたＤＴＭＦトーンとして伝送される。一実施例では、セキュリティ装置で発生されたキーストリーム(keystream)から擬似乱数を取得し、この擬似乱数に基づいてベース変換表内で記号をシャッフルして選択された変換表を得ることにより、選択された変換表が発生される。

【０００８】

別の実施例では、第１の通信インターフェースによって受け取られたＤＴＭＦトーンは１組の記号中の関連する記号に変換される。関連する変換表は、受け取られた各ＤＴＭＦトーンに対して、複数の変換表から擬似ランダム的に選択される。次いで、受け取られた各ＤＴＭＦトーンに関連する記号は、その関連する変換表に基づいて暗号化された記号へ変換される。

【０００９】

ある構成では、セキュリティ装置は、電話機によって呼び出された電話番号を検出してよい。電話番号が、関連する安全な団体と認識されると、セキュリティ装置は、電話機から受け取ったＤＴＭＦトーンを暗号化する。そうでなければ、電話機から受け取ったＤＴＭＦトーンを、セキュリティサーバにそのまま渡す。

【００１０】

スモールフォームファクタの電話セキュリティ装置も、第１および第２の通信インターフェースならびに処理回路を含んで提供される。第１の通信インターフェースによってセキュリティ装置が電話機と通信することが可能になり、その上第２の通信インターフェースによってセキュリティ装置がセキュリティサーバと通信することが可能になる。処理回路は、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の間に結合され、（ａ

）電話機からデュアルトーン多重周波数（ＤＴＭＦ）トーンを受け取り、（ｂ）セキュリティ装置から活性化信号を受け取り、（ｃ）一旦活性化信号を受け取るとセキュリティ装置を能動動作モードにし、（ｄ）受け取ったＤＴＭＦトーンを暗号化し、かつ／または（ｅ）セキュリティサーバへ暗号化されたＤＴＭＦトーンを送るように構成されてよい。受動動作モードでは、セキュリティ装置は、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の間でＤＴＭＦトーンをそのまま通す。

【００１１】

セキュリティ装置は、（ａ）第１の通信インターフェースによってＤＴＭＦトーンを受け取ったとき検出するように処理回路に結合されたＤＴＭＦトーン検出器、および／または（ｂ）処理回路が受け取ったＤＴＭＦトーンを暗号化されたＤＴＭＦトーンに変換するのを支援するように処理回路に結合されたＤＴＭＦ暗号化インターフェースも含んでよい。

【００１２】

処理回路は、（ａ）第１の通信インターフェースによって受け取った第１のＤＴＭＦトーンを第１の記号に変換し、（ｂ）複数の変換表から変換表を擬似ランダム的に選択し、（ｃ）選択された変換表を用いることにより第１の記号を第２の記号に変換し、（ｄ）第２の記号を第２のＤＴＭＦトーンに変換し、かつ／または（ｅ）第２のＤＴＭＦトーンを暗号化されたＤＴＭＦトーンとして送るようにさらに構成されてよい。変換表を選択するために、処理回路は、（ａ）セキュリティ装置で発生されたキーストリームから擬似乱数を取得し、かつ／または（ｂ）この擬似乱数に基づいてベース変換表中の記号をシャッフルして、選択された変換表を得るように構成されてよい。

【００１３】

したがって、スモールフォームファクタの電話セキュリティ装置は、（ａ）第１の通信インターフェースによって電話機からデュアルトーン多重周波数（ＤＴＭＦ）トーンを受け取るための手段、（ｂ）セキュリティ装置から活性化信号を受け取るための手段、（ｃ）一旦活性化信号を受け取ると、セキュリティ装置を能動動作モードにするための手段、（ｄ）電話機から受け取ったＤＴＭＦトーンを暗号化するための手段、（ｅ）第２の通信インターフェースによってセキュリティサーバへ暗号化されたＤＴＭＦトーンを送るための手段、および／または（ｆ）受動動作モードでは、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の間でＤＴＭＦトーンをそのまま通すための手段を備えて提供される。

【００１４】

その上、セキュリティ装置は、（ａ）第１の通信インターフェースによって受け取った第１のＤＴＭＦトーンを第１の記号に変換するための手段、（ｂ）複数の変換表から擬似ランダム的に変換表を選択するための手段、（ｃ）選択された変換表を用いて第１の記号を第２の記号に変換するための手段、（ｄ）第２の記号を第２のＤＴＭＦトーンに変換するための手段、および／または（ｅ）第２のＤＴＭＦトーンを暗号化されたＤＴＭＦトーンとして送るための手段を含んでよい。

【００１５】

電話機によって伝送された情報を保護するためのセキュリティ装置上で動作する１つまたは複数の命令を有する機械可読媒体が、プロセッサによって実行されたとき、プロセッサが、（ａ）第１の通信インターフェースによって電話機からデュアルトーン多重周波数（ＤＴＭＦ）トーンを受け取り、（ｂ）電話機から受け取ったＤＴＭＦトーンを暗号化し、かつ／または（ｃ）第２の通信インターフェースによって暗号化されたＤＴＭＦトーンを送るようにする。活性化信号を受け取ると、セキュリティ装置は能動動作モードになってよく、能動モードでは、受け取ったＤＴＭＦトーンを暗号化されたＤＴＭＦトーンに変換する。そうでなければ、セキュリティ装置は、受動動作モードでは、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の間でＤＴＭＦトーンをそのまま通す。セキュリティ装置は、第２の通信インターフェースに結合された受信装置を用いて認証されてもよい。

【００１６】
ＤＴＭＦトーンを暗号化するために擬似乱数が発生され、擬似乱数に基づいて複数の変換表から変換表が選択される。電話機から受け取られた第１のＤＴＭＦトーンは、選択された変換表に基づいて第２のＤＴＭＦトーンに変換される。
【００１７】
伝送中にＤＴＭＦ信号の保護を容易にするために、電話のセキュリティサーバ上で動作する方法も提供される。デュアルトーン多重周波数（ＤＴＭＦ）対応の電話機から呼が受け取られる。電話機からのＤＴＭＦトーンの暗号化を起動するために、ＤＴＭＦ対応の電話機に関連したセキュリティ装置に活性化信号が送られる。セキュリティ装置から暗号化されたＤＴＭＦトーンが受け取られる。次いで、電話機によって送られた情報を得るために、受け取られたＤＴＭＦトーンが解読される。受け取ったＤＴＭＦトーンを解読すると、結果として電話機のユーザによって入力された数の一部を得ることになり得る。
【００１８】
セキュリティ装置は、電話機に近接して配置され、かつ電話機とセキュリティサーバの間に直列で結合されてよい。
【００１９】
セキュリティ装置を認証するために、セキュリティサーバは、セキュリティ装置に認証チャレンジを送ってよい。セキュリティ装置から認証応答が受け取られてよい。認証チャレンジに対して認証応答が有効であれば、次いでセキュリティ装置に確認が送られてよい。セキュリティサーバとセキュリティ装置の間で、記号暗号化アルゴリズムが同期されてよい。
【００２０】
受け取ったＤＴＭＦトーンの解読は、（ａ）第１のＤＴＭＦトーンを第１の記号に変換すること、（ｂ）擬似ランダム的に選択された記号対記号の逆変換表を用いて第１の記号を第２の記号に変換すること、および／または第２の記号を第２のＤＴＭＦトーンに変換することを含んでよい。
【００２１】
電話のセキュリティサーバも、通信モジュール、ＤＴＭＦ解読モジュール、および処理回路を備えて提供される。通信モジュールによって、デュアルトーン多重周波数（ＤＴＭＦ）対応の電話機から電話呼を受け取ることが可能になり得る。ＤＴＭＦ解読モジュールは、暗号化されたＤＴＭＦトーンを解読する働きをしてよい。処理回路は、（ａ）ＤＴＭＦ対応の電話機から呼を受け取り、（ｂ）ＤＴＭＦ対応の電話機に関連したセキュリティ装置に活性化信号を送って、電話機からのＤＴＭＦトーンの暗号化を起動し、（ｃ）ＤＴＭＦ対応の電話機に関連したセキュリティ装置から暗号化されたＤＴＭＦトーンを受け取り、かつ／または（ｄ）受け取ったＤＴＭＦトーンを解読して電話機によって送られた情報を得るように構成されてよい。その上、セキュリティサーバは、セキュリティ装置を認証するように構成された認証モジュールも含んでよい。処理回路は、（ａ）第１のＤＴＭＦトーンを第１の記号に変換し、（ｂ）擬似ランダム的に選択された記号対記号の逆変換表を用いて第１の記号を第２の記号に変換し、かつ／または（ｃ）第２の記号を第２のＤＴＭＦトーンに変換するようにさらに構成されてよい。
【００２２】
したがって、電話のセキュリティサーバは、（ａ）デュアルトーン多重周波数（ＤＴＭＦ）対応の電話機から呼を受け取るための手段、（ｂ）ＤＴＭＦ対応の電話機に関連したセキュリティ装置に活性化信号を送って、電話機からのＤＴＭＦトーンの暗号化を起動するための手段、（ｃ）セキュリティ装置から暗号化されたＤＴＭＦトーンを受け取るための手段、および／または（ｄ）受け取ったＤＴＭＦトーンを解読して電話機によって送られた情報を得るための手段を備えて提供される。セキュリティサーバは、（ａ）セキュリティ装置に認証チャレンジを送るための手段、（ｂ）セキュリティ装置からの認証応答を受け取るための手段、（ｃ）認証チャレンジに対して認証応答が有効である場合、セキュリティ装置に確認を送るための手段、（ｄ）第１のＤＴＭＦトーンを第１の記号に変換す

るための手段、（ｅ）擬似ランダム的に選択された記号対記号の逆変換表を用いて第１の記号を第２の記号に変換するための手段、および／または（ｆ）第２の記号を第２のＤＴＭＦトーンに変換するための手段も含んでよい。

【００２３】

電話機からデュアルトーン多重周波数（ＤＴＭＦ）トーンとして伝送された情報を保護するための、電話のセキュリティサーバ上で動作する１つまたは複数の命令を有する機械可読媒体も提供され、これは、プロセッサによって実行されたとき、プロセッサが、（ａ）電話機から呼を受け取り、（ｂ）電話機に関連したセキュリティ装置に活性化信号を送って電話機からのＤＴＭＦトーンの暗号化を起動し、（ｃ）電話機に関連したセキュリティ装置を認証し、（ｄ）セキュリティ装置から暗号化されたＤＴＭＦトーンを受け取り、かつ／または（ｅ）受け取ったＤＴＭＦトーンを解読して電話機によって送られた情報を得るようにする。その他の命令は、（ａ）暗号化されたＤＴＭＦトーンをディジタル記号に変換し、（ｂ）ディジタル記号のそれぞれに対して記号対記号の逆変換表を取得し、かつ／または（ｃ）逆変換表を用いて各ディジタル記号を変換してよい。

【００２４】

移動体通信装置上で動作する認証方法も提供される。移動体通信装置によってテレサービス局への呼が開始される。テレサービス局から疑似ランダムの認証チャレンジが受け取られる。テレサービス局に認証応答が送られるが、認証応答は、疑似ランダムの認証チャレンジならびに移動体通信装置およびテレサービス局の両方によってあらかじめ準備された認証鍵に基づくものである。テレサービス局から機密情報が要求される。これを受けて、テレサービス局によって認証応答が受諾された場合、要求された機密情報はテレサービス局からのものであり得る。テレサービス局へ、移動体通信装置を認証するのにさらに用いられるユーザ識別子が送られてよい。疑似ランダムの認証チャレンジおよび認証応答に基づいてセッション鍵が発生されてよい。セッション鍵を用いて機密情報を解読することができる。移動体通信装置は携帯電話でよく、テレサービス局は金融機関と関連したものでよい。

【００２５】

テレサービス局での認証向けに構成された移動体通信装置も提供される。移動体通信装置は、通信モジュールおよび処理回路を含んでよい。通信モジュールによって、無線通信網による通信が可能になり得る。処理回路は、通信モジュールに結合され、かつ、（ａ）テレサービス局への呼を開始し、（ｂ）テレサービス局から疑似ランダムの認証チャレンジを受け取り、（ｃ）テレサービス局へ、疑似ランダムの認証チャレンジならびに移動体通信装置およびテレサービス局の両方によってあらかじめ準備された認証鍵に基づく認証応答を送り、（ｄ）疑似ランダムの認証チャレンジおよび認証応答に基づいてセッション鍵を発生し、かつ／または（ｅ）テレサービス局からの機密情報を要求し、かつ／または（ｆ）認証応答がテレサービス局によって受諾された場合、要求した機密情報をテレサービス局から受け取り、セッション鍵を用いて機密情報を解読するように構成されてよい。

【００２６】

したがって、移動体通信装置は、（ａ）テレサービス局に対して呼を開始するための手段、（ｂ）テレサービス局から疑似ランダムの認証チャレンジを受け取るための手段、（ｃ）テレサービス局へ、疑似ランダムの認証チャレンジならびに移動体通信装置およびテレサービス局の両方によってあらかじめ準備された認証鍵に基づく認証応答を送るための手段、（ｄ）疑似ランダムの認証チャレンジおよび認証応答に基づいてセッション鍵を発生するための手段、（ｅ）テレサービス局へ、移動体通信装置を認証するのにさらに用いられるユーザ識別子を送るための手段、（ｆ）テレサービス局に機密情報を要求するための手段、（ｇ）テレサービス局によって認証応答が受諾された場合、要求した機密情報をテレサービス局から受け取るための手段、および／または（ｈ）セッション鍵を用いて機密情報を解読するための手段を備えて提供される。

【００２７】

電話機によって伝送された情報を保護するためのセキュリティ装置上で動作する１つま

たは複数の命令を有する機械可読媒体も提供され、これは、プロセッサによって実行されたとき、プロセッサが、（ａ）テレサービス局に対して呼を開始し、（ｂ）テレサービス局から疑似ランダムの認証チャレンジを受け取り、（ｃ）テレサービス局へ、疑似ランダムの認証チャレンジならびに移動体通信装置およびテレサービス局の両方によってあらかじめ準備された認証鍵に基づく認証応答を送り、（ｄ）疑似ランダムの認証チャレンジおよび認証応答に基づいてセッション鍵を発生し、（ｅ）テレサービス局からの機密情報を要求し、（ｆ）テレサービス局によって認証応答が受諾された場合、要求した機密情報をテレサービス局から受け取り、かつ／または（ｇ）セッション鍵を用いて機密情報を解読する原因となる。

【図面の簡単な説明】

【００２８】

【図１】電話機と保護サーバの間の特定の通信を保護するために、電話機への通信回線に沿ってセキュリティ装置が結合され得るシステムを示す図。

【図２】電話機と図１の発行機関に属するセキュリティサーバの間の特定の通信を保護するための方法を示す流れ図。

【図３】伝送中にＤＴＭＦトーンの保護を可能にし得る電話サービスのセキュリティサーバの一実施例を示すブロック図。

【図４】電話装置からのＤＴＭＦトーンを保護するためにセキュリティサーバ上で動作する方法を示す図。

【図５】伝送中にＤＴＭＦトーンを防護するように構成され得るセキュリティ装置の一実施例を示すブロック図。

【図６】電話装置からのＤＴＭＦトーンを保護するためにセキュリティ装置上で動作する方法を示す図。

【図７】セキュリティサーバでそれ自体を認証するように構成された移動体通信装置のブロック図。

【図８】通信網によってテレサービス局に対して移動体通信装置を認証する方法を示す流れ図。

【図９】暗号化されるべき各記号に対して変換表を擬似ランダム的に選択することによりプレーンテキスト記号を保護するための組合せコンバイナのブロック図。

【図１０】プレーンテキスト記号を暗号化された記号に変換するための記号対記号の変換表の一実施例を示す図。

【図１１】暗号化された記号を得るためにプレーンテキスト記号が様々な変換表を用いて暗号化され得る様子を示す一実施例の図。

【図１２】ｎが正整数のとき、ｎ個の記号の組に対して複数の可能な置換から変換表を選択するためのアルゴリズムを示す図。

【図１３】単一のプレーンテキスト記号を暗号化するのに複数の変換表を用いることにより記号認証を実現し得る別の暗号化方式を示すブロック図。

【図１４】各プレーンテキスト記号を暗号化して対応する暗号化された記号を得るために、複数の変換表が用いられ得る様子を示す図。

【図１５】プレーンテキスト記号を暗号化された記号に変換するかまたは暗号化するために、２つの変換表が用いられ得る様子を示す一実施例の図。

【図１６】一実施例に従ってプレーンテキストの暗号化を実行する方法を示す図。

【図１７】単一のプレーンテキスト記号を得るために、１つまたは複数の逆変換表を用いることにより、暗号化された記号が解読され得る様子を示すブロック図。

【図１８】一実施例に従ってプレーンテキストの暗号化を実行する方法を示す図。

【図１９】一実施例による暗号化モジュールを示すブロック図。

【図２０】一実施例による解読モジュールを示すブロック図。

【発明を実施するための形態】

【００２９】

［詳細な説明］

以下の説明では、実施例の十分な理解をもたらすために具体的な詳細が示される。しかし、これらの具体的な詳細なしで実施例が実践され得ることが当業者によって理解されよう。例えば、不必要な細部で実施例が不明瞭にならないように、ブロック図では回路が示されないことがある。

【００３０】

また、実施例が、流れ図、流れ図、構造図またはブロック図として示される処理と記述され得ることが注目される。流れ図が動作を逐次処理として記述することがあるが、動作の多くは、並行して、または同時に実行することができる。さらに、動作の順序は再編成されてよい。処理は、その動作が完成するとき終結する。処理は、方法、関数、手順、サブルーチン、サブプログラムなどに相当してよい。処理が関数に相当するとき、その終結は、呼び出した関数または主関数へその関数が復帰することに相当する。

【００３１】

さらに、記憶媒体は、読取り専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリ素子、および／または情報を保存するための他の機械可読媒体を含む、データを保存するための１つまたは複数の装置を表してよい。用語「機械可読媒体」は、可搬または固定の記憶装置、光学式記憶装置、無線チャネル、ならびに（諸）命令および／またはデータを保存、含有、または保持することができる様々な他の媒体を含むが、これらには限定されない。

【００３２】

その上、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、マイクロコードまたはそれらの組合せによって、様々な構成が実施され得る。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で実施されるとき、記述されたタスクを実行するためのプログラムコードまたはコードセグメントは、記憶媒体または他の記憶手段などの機械可読媒体に保存されてよい。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、手順、関数、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文の組合せを表してよい。コードセグメントは、情報、データ、引数、パラメータまたはメモリ内容を渡しかつ／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てよい。情報、引数、パラメータ、データなどは、メモリ共有、メッセージ引き渡し、トークン引き渡し、およびネットワーク伝送をとりわけ含む適当な手段によって、渡されるか、転送されるか、または伝送されてよい。本明細書に開示された方法は、ハードウェア、ソフトウェアまたは両方で実施されてよい。

【００３３】

本明細書に開示された実施例に関連して説明された様々な例示の論理ブロック、モジュール、回路、エレメント、および／または要素は、汎用プロセッサ、ディジタル信号プロセッサ（ＤＳＰ）、特定用途向けＩＣ（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、あるいは本明細書で説明された関数を実行するように設計された、他のプログラマブル論理要素、個別のゲートまたはトランジスタの論理、個別のハードウェア要素またはそれらの任意の組合せで実施または実行されてよい。汎用プロセッサは、マイクロプロセッサでよいが、代替形態では、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラまたはステートマシンでよい。プロセッサは、コンピュータ要素（例えばＤＳＰとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、ＤＳＰコアと連動する１つまたは複数のマイクロプロセッサ、任意の他のそのような構成）の組合せとして実施されてもよい。

【００３４】

本明細書に開示された実施例に関連して説明された方法またはアルゴリズムは、ハードウェア、プロセッサによって実行可能なソフトウェアモジュール、または両方の組合せで、処理ユニット、プログラム命令または他の指令の形で直接具現されてよく、また、１つの装置に含まれるかあるいは複数の装置にわたって分散してよい。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、ＥＥＰＲＯ

Ｍメモリ、レジスタ、ハードディスク、取外し可能ディスク、ＣＤ－ＲＯＭまたは当技術分野で既知の記憶媒体の任意の他の形式の中に存在してよい。記憶媒体は、プロセッサが情報を読み取りかつ書き込むことができるようにプロセッサに結合されてよい。代替形態では、記憶媒体がプロセッサに一体化されてよい。

【００３５】

１つの特徴に、顧客の電話線に直列で挿入され得て２因子認証方式における第２の因子として働き、かつＤＴＭＦトーンを暗号化し、それによって機密情報の開示を防ぐスモールフォームファクタのセキュリティ装置を提供することがある。この装置は電話機の通常動作に対して干渉しない。この装置は、関連する銀行および支払い業務のために商標を付ける機会も提供するスモールフォームファクタの筐体を含んでよい。電力は、この装置が結合されている電話線から供給され得る。ある構成では、複数のそのような装置が、電話線に沿ってつながれるかまたはカスケード接続されてよく、複数の異なるグループ（例えば銀行）に対して安全な通信を提供する。

【００３６】

別の特徴に、暗号化された記号のセキュリティを守る効率的な暗号化方法を提供することがある。各プレーンテキスト記号は、個別の擬似ランダム的に選択された変換表を用いることにより暗号化される。記号の、可能性のあるあらゆる置換を変換表としてあらかじめ保存するのではなく、変換表は、擬似乱数および記号シャッフリングアルゴリズムに基づいて、進行中に効率的に発生されてよい。同様に、受信装置は、進行中に逆変換表を発生して、受け取った暗号化された記号を解読してよい。

【００３７】

[ＤＴＭＦトーンの保護]

図１は、電話機１０４と保護サーバ１０８の間の特定の通信を保護するために、電話機１０４への通信回線に沿ってセキュリティ装置１０２が結合され得るシステムを示す。セキュリティ装置１０２は、電話機１０４と通信網１０６の間の電話線上で、インラインに、または直列で接続することができるスモールフォームファクタの装置でよい。セキュリティ装置１０２は、電話機１０４の近くに、または隣接して、電話線に結合されてよい。

【００３８】

一実施例では、セキュリティ装置１０２は、口座および／または発行機関１０８（例えば銀行、クレジットカード会社など）と関連づけられてよい。例えば、銀行は、顧客にそのようなセキュリティ装置１０２を発行してよく、各セキュリティ装置は、顧客または顧客の口座と一意に関連づけられている。発行機関１０８は、顧客との電話のトランザクションを容易にするセキュリティサーバ１１０を有してよい。

【００３９】

図２は、電話機１０４と図１の発行機関１０８に属するセキュリティサーバ１１０の間の特定の通信を保護するための方法を示す流れ図である。セキュリティ装置１０２は、能動動作モードおよび不活性の（受動）動作モードを有してよい。セキュリティ装置１０２は、発行機関１０８以外（例えばセキュリティサーバ１１０）の誰かに電話するのに使用されるとき不活性であり、呼はＤＴＭＦトーンを含んでそのままであってセキュリティ装置１０２を単に通過する。しかし、電話機１０４が発行機関に対して呼を開始する（２０８）とき、セキュリティサーバ１１０（例えばセキュリティサーバ１１０）は、セキュリティ装置を起動する活性化信号を送る（２１０）。活性化信号は、セキュリティ装置１０２が一致によって作動することはあり得ないと無理なく確信されるように十分に長くかつ／または一意の（例えば十分な桁または記号を有する）ものでよい。一実施例では、この活性化信号は、実際にはいかなる情報も保持しなくてよく、セキュリティ装置１０２を起動するかまたは活性化して不活性（受動）モードから能動モードへ切り換えるだけである。例えば、活性化信号は、セキュリティ装置１０２によって認識される曲の短い部分またはトーンでよい。セキュリティ装置１０２は、セキュリティサーバ１１０から活性化信号（例えばＤＴＭＦトーンの一意の組）をリッスンし、かつ認識して能動モードへ切り換わる（２１２）。一実施例では、セキュリティ装置１０２は、活性化信号を受け取り次第、

電話機からセキュリティサーバ１１０へのすべてのＤＴＭＦトーンを暗号化し始めてよい。

【００４０】

ある構成では、セキュリティ装置１０２とセキュリティサーバ１１０の間で、チャレンジ－応答方式が実施されてよい。セキュリティサーバ１１０は、セキュリティ装置へ、活性化信号に加えてランダムチャレンジを送ってよい（２１４）。セキュリティ装置１０２は、チャレンジを受け取って返答（例えば識別子およびチャレンジに対する応答）を発生し（２１６）、セキュリティサーバ１１０へこの返答を送る。この返答は、セキュリティ装置１０２に関連した識別子およびチャレンジに対する応答を含んでよい。セキュリティ装置１０２は、電話機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のに用いられ得るセッション鍵も発生してよい。

【００４１】

この返答は、セキュリティサーバ１１０に、セキュリティ装置１０２が関連するセキュリティ装置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、特定の顧客の口座を照合する（２２０）のに識別子を用いてよく、そうすることによって、顧客が自身を手動で同定する（例えば、顧客が自分の口座番号を入力する）手間を省く。セキュリティサーバ１１０は、ユーザを認証するために、ランダムチャレンジならびにセキュリティ装置１０２およびセキュリティサーバ１１０の両方に備わっている認証鍵に基づいて、応答が正確であることを確認してもよい（２２２）。セキュリティ装置１０２がユーザの電話機に近接して（例えばユーザの住居内に）配置されているので、攻撃者は、セキュリティ装置１０２を盗まなければ攻撃を開始することができないはずであることに留意されたい。

【００４２】

同じチャレンジと応答を用いることにより、セキュリティサーバ１１０は、セキュリティ装置１０２が２２４で計算するセッション鍵と同一のセッション鍵を２２６で計算する。セキュリティサーバ１１０がセキュリティ装置１０２から受け取る返答が一致しないと（あるいは応答を全然受け取らないと）、呼は、より厳格な識別および／または認証向けの代替通路へ迂回されてよい。すなわち、セキュリティ装置１０２は、受け取ったランダムチャレンジおよび認証鍵に基づいてその応答を計算してよい。次いで、セキュリティサーバ１１０は、（ランダムチャレンジおよび認証鍵に基づいて）ローカルな応答を計算してそれをセキュリティ装置１０２からの受信応答と比較することにより、受信応答を確認することができる。

【００４３】

チャレンジ応答が適切に認証されると、セキュリティサーバ１１０は、新しく導出されたセッション鍵を用いて、認証された確認を送る（２２８）。この確認は、電話機１０４から来るＤＴＭＦトーンを暗号化し始めることをセキュリティ装置１０２に通知する。セキュリティサーバからの確認に関して問題があると（例えば一定の最大時間内にセキュリティ装置１０２が確認を受け取らない、または確認失敗など）、セキュリティ装置１０２はユーザに警告信号を発生してよい。例えば、チャレンジ応答の認証に失敗すると、光が点滅する（またはオンになる）か、あるいは警報が鳴ってよい。その上、ランプ（例えば発光ダイオード－ＬＥＤ）が光って、セキュリティ装置１０２が活動中であり、かつ／またはチャレンジ応答が成功裡に認証されたことを示してよい。

【００４４】

一旦チャレンジ応答が成功裡に認証されると、一実施例では、電話機１０４からセキュリティサーバへの伝送を暗号化するのに、セキュリティ装置１０２によってセッション鍵が用いられてよい。一旦暗号化が始まると、セキュリティ装置は、電話機から来るＤＴＭＦトーンを遮断し（２３２）、代わりに暗号化されたＤＴＭＦトーンを伝送する（２３４）。ＤＴＭＦトーンのそのような暗号化の一実施例では、電話機１０４からのＤＴＭＦトーンは別のＤＴＭＦトーンに変換されてよく、次いで、これがセキュリティサーバ１１０へ送られる。別の構成では、セキュリティ装置１０２によってＤＴＭＦトーンがディジタ

ル記号に変換されてよく、次いで、これが暗号化されてセキュリティサーバ１１０へ送られる。セキュリティ装置１０２は、任意の他のもの（非ＤＴＭＦトーンまたは信号）も、変更せず、あるいは暗号化せず両方向に通す。ユーザが最初に要求される可能性のあることの１つに、自分の口座と関連したＰＩＮ番号の入力があるので、このＰＩＮ番号と関連したＤＴＭＦトーンは、暗号化されて認証のための第２因子を形成してよい。同様に、セキュリティサーバ１１０は、セキュリティ装置を介して電話機から受け取ったＤＴＭＦトーンを解読するのにセッション鍵を用いることができる（２３６）。

【００４５】

代替構成では、セキュリティ装置１０２は、特定の発行機関１０８に関連した特定の電話番号を認識するように構成されてよい。セキュリティ装置１０２は、電話機が特定の電話番号をダイヤルしたことを認識したとき、自動的に能動モードに切り換わり、かつ／または電話機からセキュリティサーバ１１０へのすべてのＤＴＭＦトーンを暗号化してよい。

【００４６】

セキュリティ装置１０２は、呼が終結するまで電話機１０４からのＤＴＭＦトーンを暗号化し続けてよいが、終結した時点で、セキュリティ装置１０２は不活性モードへ切り換わって戻り、ＤＴＭＦトーンがすべてそのまま通過することが可能になる。

【００４７】

セキュリティ装置１０２は、スモールフォームファクタを有することができるので、電話線に容易にプラグ接続され得る。ユーザは、様々な場所（例えば自宅、会社など）から口座に安全にアクセスすることができるように、１つの機関または口座に関連した複数のセキュリティ装置を有してよい。ユーザは、様々な別々の機関および／または口座に関連した複数のセキュリティ装置を有してもよい。これら複数のセキュリティ装置は、電話線に沿って直列で結合されてよい。チェーン中の不活性のセキュリティ装置は、チェーン中の次のセキュリティ装置へ信号を渡すだけである。チェーン中のセキュリティ装置は、セキュリティサーバによって活性化されると電話機からのＤＴＭＦトーンを暗号化する。

【００４８】

別の実施例では、セキュリティ装置１０２は、１つの電話機または位置からの複数のユーザに対応することができる。そのような場合、セキュリティサーバは、セキュリティ装置が複数のユーザまたは口座に関連づけられていると識別することができる。各ユーザを区別するために、セキュリティサーバは、特定のユーザまたは口座を識別するＰＩＮまたは他の識別子の入力をユーザに要求する音声プロンプトを送ってよい。

【００４９】

図３は、伝送中にＤＴＭＦトーンの保護を可能にし得るテレサービスのセキュリティサーバの一実施例を示すブロック図である。セキュリティサーバ３０２は、小型でかつ／または低電力のマイクロプロセッサなどの処理回路３０４を含んでよい。セキュリティサーバ３０２は、通信網にセキュリティサーバ３０２を結合するのに使用される第１の通信モジュール３０６を含んでよい。認証モジュール３０８によって、セキュリティサーバ３０２が、通信するセキュリティ装置を認証することが可能になる。ＤＴＭＦ解読モジュール３０８によって、セキュリティサーバ３０２は、セキュリティ装置から受け取った暗号化されたＤＴＭＦトーンを解読することが可能になる。

【００５０】

図４は、電話装置からのＤＴＭＦトーンを保護するためにセキュリティサーバ上で動作する方法を示す。呼は、ＤＴＭＦ対応の電話機から受け取られる（４０２）。ＤＴＭＦ対応の電話機に関連したセキュリティ装置に活性化信号が送られる（４０４）。セキュリティ装置は、ＤＴＭＦ対応の電話機に近接して配置されてよい。次いで、セキュリティサーバによってセキュリティ装置が認証される。例えば、セキュリティ装置にチャレンジ信号が送られる（４０６）。セキュリティサーバは、セキュリティ装置から応答を受け取ったかどうか判断する（４０８）。受け取っていなければ、電話線上にセキュリティ装置が存在しないと想定されてよい（４１０）。そうでなければ、セキュリティサーバは、受信応

答が成功裡に認証されたかどうか判断する（４１２）。受信応答を成功裡に認証することができないと認証は失敗する（４１４）。そうでなければ、セッション鍵が発生される（４１６）。セッション鍵によって認証された確認メッセージがセキュリティ装置に送られる（４１８）。セキュリティサーバは、セキュリティ装置から暗号化されたＤＴＭＦトーンを受け取ってよい（４２０）。次いで、セキュリティサーバは、受け取ったＤＴＭＦトーンを解読して、電話機によって送られた情報を得てよい（４２２）。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って伝送中に盗聴者から保護される秘密情報（例えば口座番号、パスワード、ＰＩＮなど）を表すことができる。

【００５１】

図５は、伝送中にＤＴＭＦトーンを防護するように構成され得るセキュリティ装置の一実施例を示すブロック図である。セキュリティ装置５０２は、小型でかつ／または低電力のマイクロプロセッサなどの処理回路５０４を含んでよい。セキュリティ装置５０２は、結合されている電話線によって電力供給され得る。電話機にセキュリティ装置５０２を結合するために第１の通信インターフェースＡ５０６が使用されてよい。通信網にセキュリティ装置５０２を結合するために第２の通信インターフェースＢ５０８が使用されてよい。受動動作モードでは、セキュリティ装置５０２は、すべてのＤＴＭＦトーンをそのまま通過させる。処理回路５０４は、活性化信号（例えばセキュリティサーバからのもの）をリッスンするように構成されてよい。ＤＴＭＦ検出器５１０は、ＤＴＭＦ活性化信号を検出してセキュリティ装置を能動動作モードに切り換えるように構成されてよい。能動モードでは、セキュリティ装置５０２は、セキュリティサーバからの認証チャレンジに応答するように構成されてよい。

【００５２】

活性化モードでは、ＤＴＭＦ検出器５１０は、通信インターフェースＡ５０６を介して受け取ったＤＴＭＦトーン（例えば電話機から来るもの）を検出するように構成されてもよい。１つまたは複数のＤＴＭＦトーンが検出された場合、ＤＴＭＦトーンは、ＤＴＭＦ暗号化モジュール５１２によって暗号化されるかそうでなければ変更される。暗号化されたＤＴＭＦトーンは、次いで、通信インターフェースＢ５０８を介してセキュリティサーバに伝送される。

【００５３】

図６は、電話装置からのＤＴＭＦトーンを保護するためにセキュリティ装置上で動作する方法を示す。電話機とセキュリティサーバの間で呼が開始されると、セキュリティ装置に直ちに電力が供給される（６０２）。すなわち、通信回線は呼がなされるときエネルギーを与えられるので、通信回線からセキュリティ装置の電力を引き出すことができる。受動動作モードでは、セキュリティ装置によって、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の間をＤＴＭＦトーンがそのまま通過することが可能になる（６０４）。例えば、第１の通信インターフェースは電話機に結合されてよく、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てよい。セキュリティ装置は、伝送を監視してセキュリティサーバから（ＤＴＭＦ）活性化信号を受け取ったかどうか判断する（６０６）。セキュリティ装置は、活性化信号を受け取らない限り受動モードで動作し続ける。セキュリティ装置は、ＤＴＭＦ活性化信号を受け取ると能動動作モードに切り換わる（６０８）。セキュリティ装置は、セキュリティサーバからの他の信号をリッスンしてもよい（６１０）。

【００５４】

セキュリティ装置は、セキュリティサーバからチャレンジを受け取ってよい（６１２）。セキュリティ装置は、チャレンジに対して応答で返答する（６１４）。応答が有効であると、セキュリティ装置は、セキュリティサーバが成功裡にセキュリティ装置を認証したことを示す確認を受け取ってよい（６１６）。

【００５５】

セキュリティ装置は、一旦活性化されて適切に認証されると、電話機からのＤＴＭＦトーンをリッスンする。第１の通信インターフェース（セキュリティ装置が結合されている

）によって電話機からＤＴＭＦトーンが受け取られると（６１８）、受け取られたＤＴＭＦトーンは様々なＤＴＭＦトーンへ暗号化される（６２０）。一実施例では、電話機からのＤＴＭＦトーンは様々なＤＴＭＦトーンに変換されてよく、次いで、これがセキュリティサーバへ送られる。別の構成では、ＤＴＭＦトーンはセキュリティ装置１０２によってディジタル記号に変換されてよく、次いで、これが暗号化されてセキュリティサーバへ送られる。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によってセキュリティサーバへ送られる（６２２）。セキュリティ装置は、呼が終了するまで電話機からのＤＴＭＦトーンを暗号化し続け、呼が終了したとき受動モードに戻る（６２４）。セキュリティ装置１０２は、電話機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へ通過するのを防止する。一実施例では、セキュリティ装置１０２は、活性状態の間中、電話ネットワークからのすべてのインプット（例えば伝送）を切り離してよい。この場合、例えば顧客が代表と話す必要がある場合、インプットを再接続する（例えばセキュリティ装置１０２からの伝送を可能にする）には、顧客またはセキュリティサーバのいずれかに対して何らかの規定があり得る。

【００５６】

[セルラー電話のセキュリティ方式]

図７は、セキュリティサーバでそれ自体を認証するように構成された移動体通信装置のブロック図である。移動体通信装置７０２は、通信モジュール７０６およびユーザインプットインターフェース７０８に結合された処理回路７０４を含む。通信モジュール７０６により、移動体通信装置７０２が無線通信網７１０によって通信することが可能になる。処理回路７０４は、呼の間中１つまたは複数のセキュリティサーバでそれ自体を認証するように構成されてよい。例えば、移動体通信装置は、銀行または金融機関が移動体通信装置７０２のユーザを認証することを可能にする認証鍵および／またはユーザ識別子を有して構成されてよい。認証鍵および／またはユーザ識別子は、銀行または金融機関によってあらかじめ（例えばセットアップまたは構成中に）供給されてよい。その上、処理回路７０４は、認証手順を完全なものにするために、ユーザからのＰＩＮ、パスワード、および／または他のインプットを要求してよい。

【００５７】

図８は、通信網によってテレサービス局８０４に対して移動体通信装置８０２を認証する方法を示す流れ図である。移動体通信装置８０２は携帯電話でよく、テレサービス局８０４は、銀行または金融機関と関連したセキュリティサーバを含んでよい。移動体通信装置８０２およびテレサービス局８０４は、それぞれ同一の認証鍵を有してよい。

【００５８】

移動体通信装置は、テレサービス局に関連した発行機関に対して呼を開始してよい（８０６）。例えば、発行機関は銀行または金融機関でよい。テレサービス局は、移動体通信装置にランダム認証チャレンジを送る（８０８）。次いで、移動体通信装置は、ランダムチャレンジおよび認証鍵に基づいて応答を発生し（８０９）、テレサービス局に応答および（恐らく）ユーザ識別子を送る（８１０）。次いで、テレサービス局は、移動体通信装置からの応答が正確かどうか検証する（８１２）。これは、テレサービス局が、その認証鍵およびランダム認証チャレンジに基づいて検証値を計算し、それを移動体通信装置から受け取った応答と比較することによって行われてよい。応答が成功裡に認証されると、移動体通信装置に認証確認が送られてよい（８１４）。移動体通信装置は、テレサービス局からの機密情報（例えば銀行口座の記録など）を要求することができる（８１６）。移動体通信装置が成功裡に認証されると、テレサービス局は、移動体通信装置に対して要求された機密情報を提供する（８１８）。このようにして、呼の間中機密情報の伝送を保護するために、移動体通信装置（例えば携帯電話）がテレサービス局によって認証されてよい。

【００５９】

[脅威モデル(Threat Model)]

本明細書に説明されたセキュリティ装置および／または方法によって対処される脅威の

タイプの１つに、盗聴攻撃がある。そのような攻撃では、電話機上でユーザによって入力された数に関連したＤＴＭＦトーンをリッスンするために、攻撃者が電話線に録音装置を付加することがある。これらのＤＴＭＦトーンは、その他の個人情報および／または秘密情報の中で、呼び出されている銀行、ユーザの顧客番号および／または口座番号、個人の識別番号（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、この情報を用いてユーザの口座から不正なトランザクションを行う。本明細書に説明されたセキュリティ装置は、ＤＴＭＦトーンを暗号化し、さらなる認証を与えることにより、そのような攻撃を頓挫させる。ほとんどの機関（例えば銀行など）が２つの因子（例えばセキュリティ装置の所有およびＰＩＮについての知識）を認証に用いることができるので、他の機密情報を求める必要はめったにない。単に暗号化されたＤＴＭＦトーンを傍受するだけでは、対応する口座番号、ＰＩＮ、などについて何も明らかにならない。

【００６０】

攻撃者は、成功するには、例えば呼が意図した受信者（例えば意図した銀行）に行くのを阻止することによって呼の進行を妨げ、意図している受信者を装って、発呼者にすべての機密情報を入力するように要求しなければならない。そのような攻撃を頓挫させるために、セキュリティ装置は、受け側機関から「暗号化開始」信号（すなわち認証された確認）を受け取った後に、セキュリティ表示器（例えばランプ）をオンにしてよい。発呼者（例えば顧客）は、何らかの機密情報または秘密情報を入力する前に、セキュリティ装置がそのトーンを暗号化していることを確かめるためにセキュリティ表示器を検査するだけである。

【００６１】

別のタイプの攻撃にセッションハイジャック攻撃があり得て、攻撃者は、ユーザが意図した受信者（例えば銀行）との通信を確立してセキュリティ表示器を活性化するまで待ち、次いで呼を乗っ取る。次いで、攻撃者は、呼がどこか調子が悪くなったと偽り、口頭で機密情報を提供してくれるようにユーザに要求することがある。あるいは、攻撃者は、特定の応答（攻撃者にとって既知のもの）を入力するようにユーザに依頼してトーン毎の暗号化パターンを確立し、次いで銀行に対する自分の応答を暗号化するのにこのトーン毎の変換を用いようとすることがある。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、擬似ランダム基準、循環基準、および／または数対トーンの関係の発見を阻止する他の基準で、改変されるかまたは変更されてよい。

【００６２】

[メッセージおよびセッションの認証]

セキュリティ装置は、例えばメッセージ認証コード（ＭＡＣ）関数を用いることにより、メッセージ認証およびセッション鍵の導出を行うように構成されてよい。例えば、セキュリティサーバは、MAC_K（チャレンジ）の１つの呼出しからアウトプットを分離することにより、発呼者のセキュリティ装置を認証してよい。例えば、一般的なＭＡＣ関数は１２８ビットのアウトプットを返してよく、これは３２個のＤＴＭＦトーンとして表され得る。セキュリティサーバおよびセキュリティ装置がＭＡＣを計算した後、セキュリティサーバは、セキュリティ装置に最初の１６個のＤＴＭＦトーン（ＭＡＣの一部分を表す）を送ってよく、これを受けて、セキュリティ装置はもう一方の１６個のＤＴＭＦトーン（ＭＡＣのもう一方の部分を表す）を送り返す。このように、セキュリティサーバおよびセキュリティ装置の両方が、認可されたものであるかまたは正当なものであると、互いに立証することができる。

【００６３】

同様に、$Session\ Key = MAC_K(Authentication\ Key \| Challenge)$のように、それぞれの側でセッション鍵を計算してよく、認証鍵はセキュリティ装置に事前ロードされている。セキュリティ装置がセキュリティサーバへその応答を送るときセッション鍵が露呈するのを防ぐために、応答は追加情報を含んでよい。例えば、応答は、$Response = MAC_K(\text{“extra information string”} \| Authentication\ Key \| Challenge)$

でよい。
【００６４】
[ストリーム暗号化]
別の特徴に、暗号化された記号のセキュリティを守る効率的な暗号化の方法を提供することがある。各プレーンテキスト記号は、個別の擬似ランダム的に選択された変換表を用いることにより暗号化される。記号の、可能性のあるあらゆる置換を変換表としてあらかじめ保存するのではなく、変換表は、擬似乱数および記号シャッフリングアルゴリズムに基づいて、進行中に効率的に発生されてよい。同様に、受信装置は、進行中に逆変換表を発生して、受け取った暗号化された記号を解読してよい。
【００６５】
この暗号化の方法は、様々な構成で実施することができる。例えば、電話セキュリティ装置は、ＤＴＭＦトーンをディジタル値に変換し、各ディジタル値に対して擬似ランダム的に選択された変換表を用いることにより、ディジタル値を暗号化する。次いで、暗号化されたディジタル値は、セキュリティサーバ（例えばテレサービス局）へ、ディジタル形式で、または暗号化されたディジタル値と関連したＤＴＭＦトーンとして、伝送されてよい。
【００６６】
ＤＴＭＦトーンは、ディジタル記号で表される（あるいはディジタル記号に関連する）ので、例えばストリーム暗号化によって保護され得る。様々な実施例において、ストリーム暗号化は、カウンタモードにおけるＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）、ＯＦＢ（Ｏｕｔｐｕｔ Ｆｅｅｄｂａｃｋ）、またはＣＦＢ（Ｃｉｐｈｅｒｔｅｘｔ Ｆｅｅｄｂａｃｋ）モードなどのブロック暗号によって発生されたキーストリームを用いてよい。例えば、ＭＡＣ関数は、ＣＢＣ－ＭＡＣモードにおけるブロック暗号で実施されてよい。例えば、セキュリティ装置がＡＥＳをハードウェアで実施した場合、これは有利であり得る。
【００６７】
これらの関数がソフトウェアで実施されるなら、非線形ＳＯＢＥＲ（ＮＬＳ）など専用のストリーム暗号を用いるのが好ましいことであり得る。低効率であるとはいえ、ストリーム暗号は、鍵またはその場限りのインプットとして暗号化されるべきものとしてデータを用い、次いでアウトプットキーストリームを発生することにより、ＭＡＣ関数としても用いられてよい。発生されたキーストリームの長さが望み通りの長さであり得るので、１つの呼で応答鍵およびセッション鍵の両方が発生され得る。
【００６８】
従来のストリーム暗号化は（真のストリーム暗号を用いてもストリームモードでブロック暗号を用いても）、通常、疑似乱数のキーストリームを発生してプレーンテキスト（すなわちＤＴＭＦトーンのディジタル表現）と組み合わせ、暗号化されたアウトプットまたは暗号テキストを形成することにより進行する。通常は、キーストリームとプレーンテキストは排他論理和（ＸＯＲ）演算を用いて組み合わせられる。というのは、この演算が自己反転性であるからである。しかし、従来のＤＴＭＦ対応の電話機は１０個以上のキーを有し、各キーは一意のトーンを有する。したがって、キーストリームで前記ＤＴＭＦトーンを暗号化するのにＸＯＲ演算を用いることができない。その代わりに、電話機キーに関連したＤＴＭＦトーンは、キーストリームから得られた擬似乱数／記号に加算され得る様々なディジタル記号に変換されて（または関連づけられて）、暗号化された記号または暗号テキストを発生してよい。しかし、特定の桁の位置を知っている積極的な攻撃者は、伝送された暗号テキストの数字から引き算をすることにより、その数字を変化させ得ることがある。例えば、特定のＤＴＭＦトーンに関して、インプットが「１」でアウトプットが「７」であったと知っている攻撃者は、このトーンに関して発生された擬似乱数は「６」であると求めることができ、次いで、その特定の桁位置に対して攻撃者が選択するいかなる文字も正確に暗号化することができる。
【００６９】

[組合せコンバイナ]

１つの特徴に、暗号化されるべき各プレーンテキスト記号向けに擬似ランダム的に選択されるかまたは発生される変換表を取得するかまたは発生するために、キーストリームの使用を提供することがある。キーストリームから擬似乱数を得て、同じように（例えばモジューロｎを加算することにより）プレーンテキストを変化させるのでなく、１つの特徴に、複数の変換表のうちの１つを擬似ランダム的に選択することによるインプットストリーム中の各プレーンテキスト記号の変換を提供することがある。変換表は、１組の数または記号の様々な可能な置換をもたらすことができる。これは、本明細書では組合せコンバイナと称される。

【００７０】

図９は、暗号化されるべき各記号に対して変換表を擬似ランダム的に選択することによりプレーンテキスト記号を保護するための組合せコンバイナのブロック図である。擬似乱数／記号のキーストリームＳｉ９０４を発生するのに暗号ジェネレータ９０２が用いられる。インプットストリーム中の各プレーンテキストのインプット記号Ｐｉ９０８向けに、複数の可能な変換表から様々な変換表９０６を発生するかまたは得るために、キーストリーム９０４の擬似乱数が用いられる。プレーンテキストのインプット記号９０８を擬似乱数的アウトプットに変換することによって、暗号化されたアウトプット記号Ｃｉ９１０が発生される。

【００７１】

そのような変換操作は、キーストリーム９０４の管理下でのプレーンテキストのインプット記号９０８の置換を定義する。変換表９０６はｎ個のエレメントのベクトルとして表されてよく、プレーンテキストのインプット記号９０８の変換は、変換表９０６のｐ番目のエレメントを照合することにより行われてよい。暗号化されたアウトプット記号Ｃｉが与えられると、逆置換の表を形成するか、または記号Ｃｉを含むエントリを求めて表を検索し、そのインデックスをｐとして返すことにより、逆変換を行うことができる。

【００７２】

一般に、１組のｎ個のプレーンテキスト記号に対してｎ！（階乗）の可能な置換が存在する。すべてのそのような置換の組から無作為に置換が選択され、変換表９０６として用いられて、プレーンテキストのインプット記号Ｐｉ９０８を暗号化されたアウトプット記号Ｃｉ９１０（暗号テキストとも称される）に変換してよい。インプットストリーム中の各プレーンテキスト記号に対して、擬似ランダム的に選択された変換表が選択される。次いで、暗号化された記号Ｃｉ９１０を見て、それが特定のプレーンテキスト記号に相当することを知っている攻撃者は、他のプレーンテキスト記号と相当する暗号化された記号との間の対応については、依然として何も分からない。すなわち、攻撃者が確認することができる情報は、暗号化された記号を変化させると既知のものとは異なるプレーンテキスト記号をもたらすということがすべてであり、別のどのプレーンテキスト記号になるかということは分からない。したがって、擬似ランダム的に選択された変換表は、プレーンテキストのインプット記号と暗号化されたアウトプット記号（暗号テキスト）の関係を露呈することなく、攻撃者は、暗号テキスト記号変換に対して、どれか１つのプレーンテキスト記号についての知識を利用することはできない。

【００７３】

安全な電話バンキング向けの一実施例では、セキュリティ装置によって電話機から受け取られた各ＤＴＭＦトーンは、ディジタルプレーンテキスト記号に変換される（または関連づけられる）。次いで、プレーンテキスト記号は、暗号化された記号を得るために、変換表（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たもの）によって変換される。暗号化された記号は、次いでセキュリティサーバに伝送され（ディジタル形式にて、あるいは暗号化された記号に対応するＤＴＭＦトーンとして）、そこで逆変換表によって解読される。逆変換表は、セキュリティ装置とセキュリティサーバの両方で同一のキーストリームを発生する同期式暗号ジェネレータを持つことにより、発生するかまたは得ることができる。一実施例では、同一のシード（例えばセッション鍵など）を用い

ることにより、暗号ジェネレータが同期されてよい。

【００７４】

一実施例では、セキュリティ装置および／またはセキュリティサーバによって、複数の変換表が、あらかじめ発生され、かつ／または保存されてよい。進行中に新規の変換表（すなわちインプット記号の置換）を発生するのではなく、変換表は、あらかじめ発生され保存されていてよい。暗号化されるべき各プレーンテキスト記号向けに、あらかじめ発生された変換表のうちの１つを選択するのに、キーストリーム９０４の疑似ランダムの値／記号を用いてよい。あらかじめ発生された変換表が、１組のｎ個のプレーンテキスト記号向けのすべての置換または置換のサブセットを定義してよい。

【００７５】

別の実施例では、用いられる変換表は、キーストリームおよび擬似ランダム的にシャッフリング記号を用いて形成することにより、進行中に発生されてよい。ｎ！の表ができることになり、また、これらの表のうちの１つを選択するのに必要とされるキーストリームの量は、そのような表をシャッフルして形成するのに必要とされる量と同一であるという意味で、これらの解決策は同等であることに留意されたい。

【００７６】

図１０は、プレーンテキスト記号を暗号化された記号に変換するための記号対記号の変換表１００２の一実施例を示す。この実施例では、１６個のプレーンテキスト記号が様々な暗号化された記号に変わる。この実施例では、単に、４ビットの暗号化された記号を用いて１６個のプレーンテキスト記号が暗号化され得ることを示すために２進表現が示されている。より多数の（またはより少数の）プレーンテキスト記号が暗号化される他の実施例では、各記号に対して別のビット数が用いられてよい。例えば、２５６個までのプレーンテキスト記号に対しては、各暗号化された記号を発生するためにキーストリームから８ビットが抽出されてよい。

【００７７】

別の特徴に、特定の変換表の範囲内で、プレーンテキスト記号と暗号化された記号の間で一対一の対応を提供することがある。すなわち、特定の変換表の範囲内で、２つのプレーンテキスト記号が同一の暗号化された記号に変換されることはない。これによって、解読装置が、暗号化された記号を元のプレーンテキスト記号へ正確に解読することが可能になる。

【００７８】

解読装置では、暗号化装置の記号対記号の変換を逆転し、それによって受け取った暗号化された記号を解読するために、記号対記号の逆変換表が発生されてよい。

【００７９】

図１１は、暗号化された記号１１０６を得るために、プレーンテキスト記号１１０２が様々な変換表１１０４を用いて暗号化され得る様子を示す一実施例の図である。各プレーンテキスト記号Ｐ０、Ｐ１、Ｐ２、Ｐ３、．．．、Ｐｉに対して、それぞれが記号の別々の置換を有する別々の変換表１１０４を用いて、暗号化された記号Ｃ０、Ｃ１、Ｃ２、Ｃ３、．．．、Ｃｉを得る。

【００８０】

１組の少数の記号については、そのような記号のすべての置換を列挙し（すなわち、あらかじめ発生し）、インデックス（キーストリームからのもの）を用いて諸置換から変換表を選択することが可能であり得る。例えば、１組の１２個の可能な記号については、発生される可能な置換の数は１２！すなわち４７９，００１，６００である。適切に置換を選択するために、偏りのない変換表として１つの置換を選択するのに、３２ビットのキーストリームは十分なものであり得る。しかし、この手法は、組中の記号の数が増加するにつれて非効率になる。例えば、１組の２５６個の可能な記号については、発生される可能な置換の数は２５６！すなわち８．５×10^{506}であり、これは、変換表として諸置換のうちの１つを選択するのに、擬似乱数的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。

【００８１】
図１２は、ｎが正整数のとき、ｎ個の記号の組に対して複数の可能な置換から変換表を選択するためのアルゴリズムを示す。この実施例では、ｋビット長（例えば８ビット長、３２ビット長など）の、０と2^k-1の範囲で一様に分布した擬似ランダムのキーストリーム値をもたらす暗号ジェネレータが用いられてよい。擬似乱数ｗを得るのにキーストリームが用いられる（１２０２）。ｎ！が2^kへ均一に分配され得ないので、偏りを導入せずに擬似乱数ｗを直接用いることはできない。この理由で、2^k未満のｎ！の最大倍数（largest multiple）として、最大しきい値Ｐｍａｘが定義される。擬似乱数ｗがこの最大しきい値Ｐｍａｘ未満であると、偏りを導入せずに擬似乱数ｗを用いることができる。そうでなければ、擬似乱数ｗがこの最大しきい値Ｐｍａｘ以上であると擬似乱数ｗは廃棄され、最大しきい値Ｐｍａｘ未満である擬似乱数ｗが得られるまで、新規の擬似乱数ｗが選択される（１２０４）。
【００８２】
擬似乱数ｗはｎ！を法として除算され、その結果、ｗ＝ｗ　ｍｏｄｕｌｏ（ｎ！）となる（１２０６）。したがって、０からｎ！の範囲で偏りのない擬似乱数ｗが得られ、置換（すなわち変換表）を得るのにこれを用いることができる。
【００８３】
あらかじめ発生された置換を保存し、擬似乱数ｗを用いることによりそのような置換を１つ選択するのではなく、１つの特徴に、変換表を発生するためにベース置換の記号をシャッフルすることにより置換の発生を提供することがある。ベース置換ベクトルＰが初期化され、記号のすべての値が、Ｐ＝［０，１，２，．．．，ｎ－１］のように設定される（１２０８）。次いで、擬似乱数ｗを用いてベース置換ベクトルＰの記号をシャッフルするのに、記号をシャッフルするアルゴリズム１２１０が用いられる。
【００８４】
記号をシャッフルするアルゴリズム１２１０の一実施例は、カウンタｉをｎ－１へ初期化するが、ここでｎは１つの組の記号の数である。カウンタｉ＞＝０の間、擬似乱数ｗ＝ｗ／（ｉ＋１）、変数ｊ＝ｗ　ｍｏｄｕｌｏ（ｉ＋１）であり、置換ベクトルＰの値は、$P_t[i]=P_{t-1}[j]$、かつ$P_t[j]=P_{t-1}[i]$のようにシャッフルされる。ここで開示された特徴から逸脱することなく、記号をシャッフルする他のアルゴリズムが用いられ得ることに留意されたい。
【００８５】
一旦置換ベクトルＰがシャッフルされると、置換ベクトルＰは、例えばインプット記号ストリームを暗号化する変換表としてこれを用いることができるあらゆる用途に供給されてよい（１２１２）。
【００８６】
図１３は、単一のプレーンテキスト記号を暗号化するのに複数の変換表を用いることにより記号認証を実現し得る別の暗号化方式を示すブロック図である。すなわち、第１の暗号化されたアウトプット記号Ｃｉ’１３１０を得るために、プレーンテキストのインプット記号Ｐｉ１３０２は、第１の暗号ジェネレータ１３０８から得られた第１のキーストリームＳｉ’１３０６に基づいて発生されるかまたは選択され得る変換表Ａ１　１３０４によって暗号化される。第１の暗号化されたアウトプット記号Ｃｉ’１３１０は、次いで、第２の暗号ジェネレータ１３１６から得られた第２のキーストリームＳｉ１３１４に基づいて発生されるかまたは選択され得る第２の変換表Ａ２　１３１２へのインプットとして働き、Ａ２は第２の暗号化されたアウトプット記号Ｃｉ１３１８を得るのに用いられる。このように、第１の暗号化されたアウトプット記号Ｃｉ’１３１０を認証するのに冗長性が用いられてよい。すなわち、記号Ｃｉ’１３１０とＣｉ１３１８を一緒に用いることにより、記号Ｃｉ１３１８がＣｉ’１３１０を認証する。したがって、例えば、攻撃者が記号Ｃｉ’１３１０を変化させることに成功すると、それは記号Ｃｉ１３１８によって適切に認証されないことになる。
【００８７】

図１４は、各プレーンテキスト記号１４０２を暗号化して対応する暗号化された記号１４０８の対を得るのに複数の変換表１４０４および１４０６が用いられ得る様子を示す。変換表１４０４および１４０６は、擬似ランダム的に選択され、かつ／または発生されてよく、各プレーンテキスト記号Ｐｉを１対の記号Ｃｉ’／Ｃｉへ暗号化することに留意されたい。

【００８８】

図１５は、プレーンテキスト記号Ｐｎを１対の記号Ｃｎ’およびＣｎに変換するかまたは暗号化するために、２つの変換表が用いられ得る様子を示す一実施例の図である。例えば、第１のプレーンテキスト記号Ｐｎ＝‘５’に対して、第１の変換表Ａ１　１５０２は、第１のアウトプット記号Ｃｎ’＝８をもたらす（すなわち‘５’が‘８’に変わる）。次いで、第１のアウトプット記号‘８’が第２の変換表Ａ２　１５０４に対するインプットとして働いてよく、第２のアウトプット記号Ｃｎ＝７を得る（すなわち‘８’が‘７’に変わる）。第１のアウトプット記号Ｃｎ’に基づいて第２のアウトプット記号Ｃｎが発生されたので、冗長な記号ＣｎおよびＣｎ’が認証用に用いられてよい。どちらか一方または両方の記号が伝送中に攻撃者によって変化されると、認証は失敗する。例えば、攻撃者によってＣｎ’が‘８’から‘４’へ変更されると、記号Ｃｎ’およびＣｎ＝‘４７’を受け取る受信者は、Ｃｎ＝‘７’がＣｎ’＝‘４’でなくＣｎ’＝‘８’を意味するはずであることに気付くことになる。

【００８９】

第１のプレーンテキスト記号と第２のプレーンテキスト記号が同一の場合でさえ、第２のプレーンテキスト記号Ｐ（ｎ＋１）は完全に異なる諸変換表を有してよい。例えば、第２のプレーンテキスト記号Ｐ（ｎ＋１）＝‘５’に対して、第１の変換表Ｂ１　１５０６は、第３のアウトプット記号Ｃ（ｎ＋１）’＝‘＊’をもたらす（すなわち‘５’が‘＊’に変わる）。次いで、第３のアウトプット記号Ｃ（ｎ＋１）’＝‘＊’が第２の変換表Ｂ２　１５０８に対するインプットとして働いてよく、第４のアウトプット記号Ｃ（ｎ＋１）’＝‘１’を得る（すなわち‘＊’が‘１’に変わる）。前と同じように、記号対Ｃ（ｎ＋１）’およびＣ（ｎ＋１）の冗長な使用が、認証の形式として働いてよい。

【００９０】

図１６は、一実施例に従ってプレーンテキストの暗号化を実行する方法を示す。１組のｎ個の記号の範囲内で定義された複数のインプット記号が得られる（１６０２）。暗号化されるべきインプット記号のそれぞれに対して、別々の記号対記号の置換を定義する複数の変換表から擬似ランダム的に選択された変換表が得られる（１６０４）。各インプット記号を個々に暗号化するために、インプット記号は、それらと対応する、インプット記号のそれぞれ向けの変換表を用いてアウトプット記号に変換される（１６０６）。次いで、アウトプット記号は解読装置に伝送されてよい（１６０８）。

【００９１】

そのような方法の一実施例では、第１のプレーンテキスト記号が得られ、第１のプレーンテキスト記号は１組のｎ個の記号のうちの１つでよい。ｎ個の記号を、ｎ個の記号の別々の置換に変換する第１の変換表が得られる。ｎ個の記号をシャッフルするのに擬似乱数を用いることにより、第１の変換表が擬似ランダム的に発生されてよい。次いで、この第１の変換表を用いて、第１のプレーンテキスト記号が第１のアウトプット記号に変換される。

【００９２】

第１の変換表よりも、ｎ個の記号をｎ個の記号の別々の置換に変換する第２の変換表が得られてよい。この第２の変換表を用いて、第１のアウトプット記号が第２のアウトプット記号に変換される。次いで、第１のアウトプット記号および／または第２のアウトプット記号に基づいて、暗号化された記号が伝送される。

【００９３】

図１７は、単一のプレーンテキスト記号を得るのに１つまたは複数の逆変換表を用いることにより、暗号化された記号Ｃｉが解読され得る様子を示すブロック図である。すなわ

ち、暗号化されたインプット記号Ｃｉ１７０２は、第１の暗号ジェネレータ１７０８から得られた第１のキーストリームＳｉ’１７０６に基づいて発生されるかまたは選択され得る第１の逆変換表Ａ１　１７０４によって解読されてよく、第１の解読されたアウトプット記号Ｃｉ’１７１０を得る。第１の解読されたアウトプット記号Ｃｉ’１７１０は、次いで、第２の暗号ジェネレータ１７１６から得られた第２のキーストリームＳｉ１７１４に基づいて発生されるかまたは選択され得る第２の逆変換表Ａ２　１７１２へのインプットとして働き、プレーンテキストのアウトプット記号Ｐｉ１７１８を得るのに用いられる。

【００９４】

例えばＣｉ＝（ｘ，ｙ）である代替構成では、暗号化された記号ｘおよびｙは、それらが暗号化された順序と逆順に解読されてよく、プレーンテキストのアウトプット記号Ｐｉを得る。

【００９５】

図１８は、一実施例に従って記号の解読を実行する方法を示す。１組のｎ個の記号の範囲内で定義された複数の（暗号化された）インプット記号が得られる（１８０２）。解読されるべきインプット記号のそれぞれに対して、別々の記号対記号の置換を定義する複数の逆変換表から擬似ランダム的に選択された逆変換表が得られる（１８０４）。各インプット記号を個々に解読するために、インプット記号を、それらと対応する、インプット記号のそれぞれ向けの逆変換表を用いてアウトプット記号に変換する（１８０６）。

【００９６】

そのような方法の一実施例では、第１の暗号化された記号（インプット記号）が得られ、ここで第１の暗号化された記号は１組のｎ個の記号のうちの１つである。ｎ個の記号を、ｎ個の記号の別々の置換に変換する第１の逆変換表も得られる。ｎ個の記号をシャッフルするために、擬似乱数を用いることにより、第１の逆変換表が擬似ランダム的に発生されてよい。この第１の逆変換表を用いて、第１の暗号化された記号が第１のアウトプット記号に変換される。第１の変換表よりも、ｎ個の記号をｎ個の記号の別々の置換に変換する第２の逆変換表が得られる。この第２の逆変換表を用いて、第１のアウトプット記号が第２のアウトプット記号に変換される。次いで、第１のアウトプット記号および／または第２のアウトプット記号に基づいてプレーンテキスト記号が得られてよい。

【００９７】

図１９は、一実施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にシードを供給するように構成された処理回路１９０４を含んでよい。キーストリームジェネレータ１９０６は、処理回路１９０４へ送られる擬似乱数または記号のキーストリームを発生する。処理回路１９０４に結合されたインプットインターフェース１９０８は、プレーンテキスト記号ストリームを受け取ってよい。プレーンテキスト記号ストリームを暗号化するために、処理回路１９０４は、キーストリームから得られた擬似乱数を用いるように構成されてよく、変換表ジェネレータ１９１０から変換表を得る。変換表ジェネレータ１９１０は、例えば擬似ランダム的に偏りのないやり方でベース表の記号をシャッフルしかつ／または組み合わせるのに擬似乱数を用いるように構成されてよく、変換表をもたらす。次いで、処理回路１９０４は、この変換表を１回用いて、最初のプレーンテキスト記号を暗号化された記号ストリームの最初の暗号化された記号に変換する。暗号化された記号ストリームは、処理回路１９０４に結合されたアウトプットインターフェース１９１２を介して伝送されてよい。プレーンテキスト記号ストリーム中の各プレーンテキスト記号に対して、その記号を変換するのに、別々の変換表が発生されかつ用いられてよい。

【００９８】

図２０は、一実施例による解読モジュールを示すブロック図である。解読モジュール２００２は、キーストリームジェネレータ２００６にシードを供給するように構成された処理回路２００４を含んでよい。キーストリームジェネレータ２００６は、処理回路２００４へ送られる擬似乱数または記号のキーストリームを発生する。処理回路２００４に結合

されたインプットインターフェース２００８は、暗号化された記号ストリームを受け取ってよい。暗号化された記号ストリームを解読するために、処理回路２００４は、キーストリームから得られた擬似乱数を用いるように構成されてよく、逆変換表ジェネレータ２０１０から逆変換表を得る。逆変換表ジェネレータ２０１０は、例えば擬似ランダム的に偏りのないやり方でベース表の記号をシャッフルしかつ／または組み合わせるのに擬似乱数を用いるように構成されてよく、変換表をもたらす。次いで、処理回路２００４は、逆変換表を１回用いて、最初の暗号化された記号をプレーンテキスト記号ストリームの最初のプレーンテキスト記号に変換する。プレーンテキスト記号ストリームは、処理回路２００４に結合されたアウトプットインターフェース２０１２を介して伝送されてよい。

【００９９】

暗号化モジュール１９０２および解読モジュール２００２が、それぞれ適切に記号を暗号化し解読するように、これらは、同一のキーストリームジェネレータを有し、かつ相補的な変換表ジェネレータを有してよい。キーストリームジェネレータ１９０６と２００６を同期させるために、（例えば安全な認証方式によって）暗号化モジュールと解読モジュールの間の特定の通信セッション向けに共通のシードが確立されてよい。例えば、キーストリームジェネレータ１９０６および２００６向けのシードとしてセッション鍵が用いられてよい。

【０１００】

本明細書で説明された実施例のうちのいくつかはＤＴＭＦトーンの暗号化に言及しているが、本明細書で説明された暗号化の方法は、伝送される情報を保護するために他の多くのタイプの通信システムで実施され得る。

【０１０１】

１つまたは複数の要素、ステップ、および／または図１～図１８に示された関数は、本発明から逸脱することなく、単一の要素、ステップ、および／または関数へ再配置され、かつ／または組み合わせられるか、あるいは、いくつかの要素、ステップ、および／または関数へ分離され得る。その他のエレメント、要素、ステップ、および／または関数も、本発明から逸脱することなく付加され得る。図の１、２、３、５、７、９、１３、１７、１９および／または２０に示された器具、装置、および／または要素は、図の２、４、６、８、１０、１１、１２、１４、１５、１６および／または１８に説明された方法、特徴またはステップの１つまたは複数を実行するように構成されてよい。

【０１０２】

当業者なら、本明細書に開示された実施例と関連して説明された様々な例示的論理ブロック、モジュール、回路およびアルゴリズムのステップは、電子ハードウェア、コンピュータソフトウェアまたは両方の組合せとして実施され得ることをさらに理解するであろう。上記で、ハードウェアとソフトウェアのこの互換性を明白に示すために、様々な例示の要素、ブロック、モジュール、回路およびステップが、それらの機能に関して全体的に説明されてきた。そのような機能がハードウェアとして実施されるのか、あるいはソフトウェアとして実施されるのかということは、システム全体に課された特定の用途および設計制約条件次第である。

【０１０３】

前述の構成は、単に実施例であって、本発明を限定するものと解釈するべきでないことに留意されたい。これらの実施例の説明は、例示であって、特許請求の範囲を限定することのないように意図されている。そのため、本教示は、容易に他のタイプの装置に適用することができ、また、多くの代替形態、変更形態、および変形形態は当業者には明白であろう。