

(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2010-514272

(P2010-514272A)

(43) 公表日 平成22年4月30日 (2010.4.30)

(51) Int.Cl.		F I		テーマコード (参考)
HO 4 M 11/00	(2006.01)	HO 4 M 11/00	3 O 2	5 J 1 O 4
HO 4 M 1/68	(2006.01)	HO 4 M 1/68		5 K 1 2 7
HO 4 K 1/00	(2006.01)	HO 4 K 1/00	Z	5 K 2 O 1
HO 4 L 9/10	(2006.01)	HO 4 L 9/00	6 2 1 Z	

審査請求 有 予備審査請求 未請求 (全 36 頁)

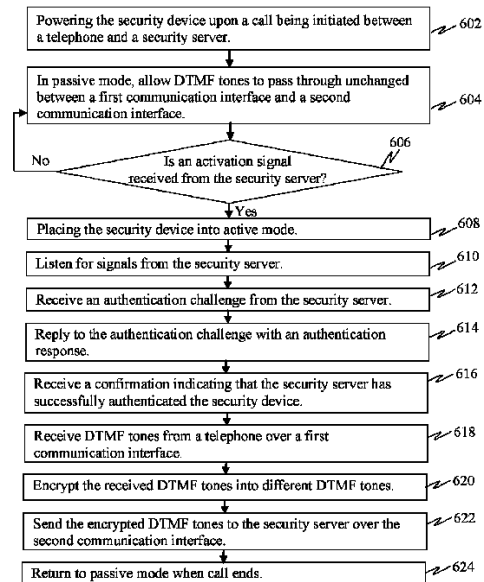
(21) 出願番号	特願2009-541567 (P2009-541567)	(71) 出願人	595020643
(86) (22) 出願日	平成19年12月12日 (2007.12.12)		クアルコム・インコーポレイテッド
(85) 翻訳文提出日	平成21年8月4日 (2009.8.4)		QUALCOMM INCORPORATED
(86) 国際出願番号	PCT/US2007/087312		
(87) 国際公開番号	W02008/076776		アメリカ合衆国、カリフォルニア州 92
(87) 国際公開日	平成20年6月26日 (2008.6.26)		121-1714、サン・ディエゴ、モア
(31) 優先権主張番号	11/611,825		ハウス・ドライブ 5775
(32) 優先日	平成18年12月15日 (2006.12.15)	(74) 代理人	100058479
(33) 優先権主張国	米国 (US)		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】 安全な電話バンキングのための方法および装置

## (57) 【要約】

機密情報の不正な開示を防ぐために、電話機からのデュアルトーン多重周波数 (DTMF) トーンを暗号化するように電話線に直列で挿入され得るスモールフォームファクタのセキュリティ装置が提供される。受信装置は、電話で送られた元の情報を受け取るために暗号化されたDTMFトーンを解読する。セキュリティ装置は、セキュリティ装置を認証する電話サービスのセキュリティサーバを用いた2因子認証方式における第2の因子として働く。



**【特許請求の範囲】****【請求項 1】**

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 ( D T M F ) トーンを受け取ることと、

前記電話機から受け取った前記 D T M F トーンを暗号化することと、

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前記暗号化された D T M F トーンを送ることとを備える、スモールフォームファクタの電話セキュリティ装置上で動作する方法。

**【請求項 2】**

前記セキュリティ装置から活性化信号を受け取ることと、

10

一旦前記活性化信号を受け取ると前記セキュリティ装置を能動動作モードにすることとをさらに備え、能動モードでは、前記セキュリティ装置が、電話機から受け取った D T M F トーンを暗号化し、かつ音声信号が前記セキュリティ装置をそのまま通過することを可能にするように構成される請求項 1 に記載の方法。

**【請求項 3】**

受動動作モードでは、前記第 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前記電話機からの D T M F トーンをそのまま通すことをさらに備える請求項 1 に記載の方法。

**【請求項 4】**

前記電話機と前記セキュリティサーバの間で呼が開始されると、前記セキュリティ装置に直ちに電力を供給することをさらに備える請求項 1 に記載の方法。

20

**【請求項 5】**

前記セキュリティサーバから認証呼掛けを受け取ることと、

前記認証呼掛けに対して認証応答で返答することと、

前記セキュリティサーバが前記セキュリティ装置を成功裡に認証したことを示す確認を受け取ることとをさらに備える請求項 1 に記載の方法。

**【請求項 6】**

前記第 1 の通信インターフェースによって受け取った第 1 の D T M F トーンを第 1 の記号に変換することと、

複数の変換表から擬似ランダム的に変換表を選択することと、

30

前記選択された翻訳表を用いて前記第 1 の記号を第 2 の記号に翻訳することと、

前記第 2 の記号を第 2 の D T M F トーンに変換することと、

前記暗号化された D T M F トーンとして前記第 2 の D T M F トーンを送ることとをさらに備える請求項 1 に記載の方法。

**【請求項 7】**

前記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得ることと、

前記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、前記選択された変換表を得ることとをさらに備える請求項 6 に記載の方法。

**【請求項 8】**

前記第 1 の通信インターフェースによって受け取った D T M F トーンを 1 組の記号中の関連する記号に変換することと、

40

受け取った各 D T M F トーンに対して、複数の変換表から関連する変換表を擬似ランダム的に選択することと、

受け取った各 D T M F トーンに関連する前記記号を、その関連する変換表に基づいて暗号化された記号に変換することとをさらに備える請求項 6 に記載の方法。

**【請求項 9】**

前記セキュリティ装置が、前記電話機に近接して配置され、かつ前記電話機と前記セキュリティサーバの間に直列で結合される請求項 1 に記載の方法。

**【請求項 10】**

前記電話機によって呼び出された電話番号を検出することと、

50

前記電話番号が、関連する安全な機関と認識された場合、前記電話機から受け取った D T M F トーンを暗号化することと、

そうでなければ、前記電話機から受け取った D T M F トーンを前記セキュリティサーバへそのまま渡すこととをさらに備える請求項 1 に記載の方法。

【請求項 1 1】

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 ( D T M F ) トーンを受け取るための手段と、

前記電話機から受け取った前記 D T M F トーンを暗号化するための手段と、

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前記暗号化された D T M F トーンを送るための手段とを備えるスモールフォームファクタの電話セキュリティ装置。 10

【請求項 1 2】

前記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と、

一旦前記活性化信号を受け取ると前記セキュリティ装置を能動動作モードにするための手段とをさらに備える請求項 1 1 に記載の装置。

【請求項 1 3】

前記第 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、受動動作モードでは D T M F トーンをそのまま通すための手段をさらに備える請求項 1 1 に記載の方法。

【請求項 1 4】

前記第 1 の通信インターフェースによって受け取った第 1 の D T M F トーンを第 1 の記号に変換するための手段と、 20

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と、

前記選択された変換表を用いて前記第 1 の記号を第 2 の記号に変換するための手段と、

前記第 2 の記号を第 2 の D T M F トーンに変換するための手段と、

前記暗号化された D T M F トーンとして前記第 2 の D T M F トーンを送るための手段とをさらに備える請求項 1 1 に記載の装置。

【請求項 1 5】

前記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得るための手段と、

前記選択された変換表を得るために、前記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するための手段とをさらに備える請求項 1 4 に記載の装置。 30

【請求項 1 6】

電話機と通信するための第 1 の通信インターフェースと、

セキュリティサーバと通信するための第 2 の通信インターフェースと、

前記第 1 の通信インターフェースと前記第 2 の通信インターフェースの間に結合され、

前記電話機からデュアルトーン多重周波数 ( D T M F ) トーンを受け取り、

前記受け取った D T M F トーンを暗号化し、かつ

前記セキュリティサーバへ暗号化された D T M F トーンを送るように構成された処理回路とを備えるスモールフォームファクタの電話セキュリティ装置。

【請求項 1 7】

前記処理回路が、セキュリティ装置から活性化信号を受け取り、かつ 40

一旦前記活性化信号を受け取ると前記セキュリティ装置を能動動作モードにするようにさらに構成される請求項 1 6 に記載の装置。

【請求項 1 8】

前記処理回路が、受動動作モードでは、前記第 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 D T M F トーンをそのまま通すようにさらに構成される請求項 1 6 に記載の装置。

【請求項 1 9】

前記第 1 の通信インターフェースによって D T M F トーンが受け取られたとき検出するように前記処理回路に結合された D T M F トーン検出器と、

前記処理回路が受け取った D T M F トーンを暗号化された D T M F トーンに変換するの 50

を支援するように前記処理回路に結合された D T M F 暗号化モジュールとをさらに備える請求項 16 に記載の装置。

【請求項 20】

前記処理回路が、前記第 1 の通信インターフェースによって受け取った第 1 の D T M F トーンを第 1 の記号に変換し、

複数の変換表から擬似ランダム的に変換表を選択し、

前記選択された変換表を用いることにより前記第 1 の記号を第 2 の記号に変換し、

前記第 2 の記号を第 2 の D T M F トーンに変換し、かつ

前記暗号化された D T M F トーンとして前記第 2 の D T M トーンを送るようにさらに構成される請求項 16 に記載の装置。

10

【請求項 21】

前記処理回路が、前記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

前記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前記選択された変換表を得るようにさらに構成される請求項 20 に記載の装置。

【請求項 22】

機械可読媒体であって、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し、プロセッサによって実行されたとき、前記プロセッサが、

第 1 の通信インターフェースによって前記電話機からデュアルトーン多重周波数 ( D T M F ) トーンを受け取り、

前記電話機から受け取った前記 D T M F トーンを暗号化し、かつ

第 2 の通信インターフェースによって前記暗号化された D T M F トーンを送るようにする機械可読媒体。

20

【請求項 23】

1 つまたは複数の命令を有する機械可読媒体であって、プロセッサによって実行されたとき、前記プロセッサが、さらに、

活性化信号が受け取られた場合、前記セキュリティ装置を、受け取られた D T M F トーンが暗号化された D T M F トーンに変換される能動動作モードにし、かつ

受動動作モードでは、前記第 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 D T M F トーンをそのまま通すようにする請求項 22 に記載の機械可読媒体。

30

【請求項 24】

1 つまたは複数の命令を有する機械可読媒体であって、プロセッサによって実行されたとき、前記プロセッサが、さらに、

前記第 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前記セキュリティ装置を認証するようにする請求項 22 に記載の機械可読媒体。

【請求項 25】

1 つまたは複数の命令を有する機械可読媒体であって、プロセッサによって実行されたとき、前記プロセッサが、さらに、

擬似乱数を発生し、

前記擬似乱数に基づいて複数の変換表から変換表を選択し、かつ

前記電話機から受け取った第 1 の D T M F トーンを前記選択された変換表に基づいて第 2 の D T M F トーンに変換するようにする請求項 22 に記載の機械可読媒体。

40

【請求項 26】

1 つまたは複数の命令を有する機械可読媒体であって、プロセッサによって実行されたとき、前記プロセッサが、さらに、

前記電話機から受け取った後続の D T M F トーン向けに別の擬似乱数を発生し、

前記別の擬似乱数に基づいて受け取った後続の各 D T M F トーン向けに前記複数の変換表から変換表を選択し、かつ

前記電話機から受け取った各 D T M F トーンをそれらの選択された変換表に基づいて別

50

の D T M F トーンに変換するようにする請求項 2 5 に記載の機械可読媒体。

【請求項 2 7】

デュアルトーン多重周波数 ( D T M F ) 対応の電話機から呼を受け取ることと、  
前記 D T M F 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、前記電話機からの D T M F トーンの暗号化を起動することと、  
前記セキュリティ装置から暗号化された D T M F トーンを受け取ることと、  
前記受け取った D T M F トーンを解読して、前記電話機によって送られた情報を得ることとを備える、電話セキュリティサーバ上で動作する方法。

【請求項 2 8】

前記セキュリティ装置が、前記電話機に近接して配置され、かつ前記電話機と前記セキュリティサーバの間に直列で結合される請求項 2 7 に記載の方法。

10

【請求項 2 9】

前記セキュリティ装置に認証呼掛けを送ることと、  
前記セキュリティ装置から認証応答を受け取ることと、  
前記認証呼掛けに対して前記認証応答が有効である場合、前記セキュリティ装置に確認を送ることとをさらに備える請求項 2 7 に記載の方法。

【請求項 3 0】

受け取った D T M F トーンを解読することが、結果として前記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る請求項 2 7 に記載の方法。

【請求項 3 1】

前記セキュリティサーバと前記セキュリティ装置の間で記号暗号化アルゴリズムを同期させることをさらに備える請求項 2 7 に記載の方法。

20

【請求項 3 2】

前記受け取った D T M F トーンを解読することが、第 1 の D T M F トーンを第 1 の記号に変換することと、  
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前記第 1 の記号を第 2 の記号に変換することと、  
前記第 2 の記号を第 2 の D T M F トーンに変換することとをさらに備える請求項 2 7 に記載の方法。

【請求項 3 3】

デュアルトーン多重周波数 ( D T M F ) 対応の電話機から呼を受け取るための手段と、  
前記 D T M F 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、前記電話機からの D T M F トーンの暗号化を起動するための手段と、  
前記セキュリティ装置から暗号化された D T M F トーンを受け取るための手段と、  
前記電話機によって送られた情報を得るように前記受け取った D T M F トーンを解読するための手段とを備える電話セキュリティサーバ。

30

【請求項 3 4】

前記セキュリティ装置に認証呼掛けを送るための手段と、  
前記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と、  
前記認証呼掛けに対して前記認証応答が有効である場合、前記セキュリティ装置に確認を送るための手段とをさらに備える請求項 3 3 に記載の電話セキュリティサーバ。

40

【請求項 3 5】

第 1 の D T M F トーンを第 1 の記号に変換するための手段と、  
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前記第 1 の記号を第 2 の記号に変換するための手段と、  
前記第 2 の記号を第 2 の D T M F トーンに変換するための手段とをさらに備える請求項 3 3 に記載の電話セキュリティサーバ。

【請求項 3 6】

デュアルトーン多重周波数 ( D T M F ) 対応の電話機から電話呼を受け取るための通信モジュールと、

50

暗号化された D T M F トーンを解読するための D T M F 解読モジュールと、

前記通信モジュールおよび D T M F 解読モジュールに結合され、D T M F 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 D T M F トーンを受け取るように構成された処理回路とを備え、かつ

前記受け取った D T M F トーンを解読して前記電話機によって送られた情報を得る電話セキュリティサーバ。

【請求項 37】

前記処理回路が、前記 D T M F 対応の電話機から呼を受け取り、かつ

前記 D T M F 対応の電話機に関連した前記セキュリティ装置に活性化信号を送って前記電話機からの D T M F トーンの暗号化を起動するようにさらに構成される請求項 36 に記載のサーバ。

10

【請求項 38】

前記セキュリティ装置を認証する認証モジュールをさらに備える請求項 36 に記載のサーバ。

【請求項 39】

前記処理回路が、第 1 の D T M F トーンを第 1 の記号に変換し、

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前記第 1 の記号を第 2 の記号に変換し、かつ

前記第 2 の記号を第 2 の D T M F トーンに変換するようにさらに構成される請求項 36 に記載のサーバ。

20

【請求項 40】

電話機からデュアルトーン多重周波数 (D T M F) 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であって、プロセッサによって実行されたとき、前記プロセッサが、

前記電話機に関連したセキュリティ装置を認証し、

前記セキュリティ装置から暗号化された D T M F トーンを受け取り、かつ

前記受け取った D T M F トーンを解読して前記電話機によって送られた情報を得るようにする機械可読媒体。

【請求項 41】

1 つまたは複数の命令を有する機械可読媒体であって、プロセッサによって実行されたとき、前記プロセッサが、さらに、

30

前記電話機から呼を受け取り、かつ

前記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前記電話機からの D T M F トーンの暗号化を起動するようにする請求項 40 に記載の機械可読媒体。

【請求項 42】

1 つまたは複数の命令を有する機械可読媒体であって、プロセッサによって実行されたとき、前記プロセッサが、さらに、

前記暗号化された D T M F トーンをデジタル記号に変換し、

前記デ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

前記逆変換表を用いて各デジタル記号を変換するようにする請求項 40 に記載の機械可読媒体。

40

【請求項 43】

移動体通信装置上で動作する方法であって、

テレサービス局に対して呼を開始することと、

前記テレサービス局から疑似ランダムの認証呼掛けを受け取ることと、

前記テレサービス局に対して、前記疑似ランダムの認証呼掛けならびに前記移動体通信装置および前記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ことと、

前記テレサービス局からの機密情報を要求することと、

前記テレサービス局によって前記認証応答が受諾された場合、前記要求した機密情報を

50

前記テレサービス局から受け取ることとを備える方法。

【請求項 4 4】

前記テレサービス局に対して、前記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ことをさらに備える請求項 4 3 に記載の方法。

【請求項 4 5】

前記移動体通信装置が携帯電話であり、前記テレサービス局が金融機関と関連する請求項 4 3 に記載の方法。

【請求項 4 6】

前記疑似ランダム認証呼掛けおよび前記認証応答に基づいてセッション鍵を発生することと、

前記セッション鍵を用いて前記機密情報を解読することとをさらに備える請求項 4 3 に記載の方法。

【請求項 4 7】

テレサービス局に対して呼を開始するための手段と、

前記テレサービス局から疑似ランダム認証呼掛けを受け取るための手段と、

前記テレサービス局に対して、前記疑似ランダム認証呼掛けならびに前記移動体通信装置および前記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と、

前記テレサービス局からの機密情報を要求するための手段と、

前記テレサービス局によって前記認証応答が受諾された場合、前記要求した機密情報を前記テレサービス局から受け取るための手段とを備える移動体通信装置。

【請求項 4 8】

前記テレサービス局に対して、前記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をさらに備える請求項 4 7 に記載の装置。

【請求項 4 9】

前記疑似ランダム認証呼掛けおよび前記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と、

前記セッション鍵を用いて前記機密情報を解読するための手段とをさらに備える請求項 4 7 に記載の装置。

【請求項 5 0】

無線通信網によって通信するための通信モジュールと、

前記通信モジュールに結合された処理回路であって、

テレサービス局に対して呼を開始し、

前記テレサービス局から疑似ランダム認証呼掛けを受け取り、

前記テレサービス局に対して、前記疑似ランダム認証呼掛けならびに前記移動体通信装置および前記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、

前記テレサービス局からの機密情報を要求し、かつ

前記テレサービス局によって前記認証応答が受諾された場合、前記要求した機密情報を前記テレサービス局から受け取るように構成された処理回路とを備える移動体通信装置。

【請求項 5 1】

前記処理回路が、前記疑似ランダム認証呼掛けおよび前記認証応答に基づいてセッション鍵を発生し、かつ

前記セッション鍵を用いて前記機密情報を解読するようにさらに構成される請求項 5 0 に記載の装置。

【請求項 5 2】

機械可読媒体であって、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し、プロセッサによって実行されたとき、前記プロセッサが、

テレサービス局に対して呼を開始し、

10

20

30

40

50

前記テレサービス局から疑似ランダム認証呼掛けを受け取り、

前記テレサービス局に対して、前記疑似ランダム認証呼掛けならびに前記移動体通信装置および前記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、

前記テレサービス局からの機密情報を要求し、かつ

前記テレサービス局によって前記認証応答が受諾された場合、前記要求した機密情報を前記テレサービス局から受け取るようにする機械可読媒体。

【請求項 5 3】

1 つまたは複数の命令を有する機械可読媒体であって、プロセッサによって実行されたとき、前記プロセッサが、さらに、

前記疑似ランダム認証呼掛けおよび前記認証応答に基づいてセッション鍵を発生し、かつ

前記セッション鍵を用いて前記機密情報を解読するようにする請求項 5 2 に記載の機械可読媒体。

【発明の詳細な説明】

【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回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

10

20

30

40

50



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】

10

20

30

40

50

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】

10

20

30

40

50

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呼掛けを送ってよい。セキュリティ装置から認証応答が受け取られてよい。認証呼掛け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。

10

【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。

20

【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呼掛けを送るための手段、(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)認証呼掛け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。

30

【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トーンをデジタル記号に変換し、(b)デ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ジタル記号を変換してよい。

40

50

## 【 0 0 2 4 】

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な認証呼掛けが受け取られる。テレサービス局に認証応答が送られるが、認証応答は、疑似ランダムな認証呼掛け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。疑似ランダムな認証呼掛け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。

10

## 【 0 0 2 5 】

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な認証呼掛けを受け取り、( c ) テレサービス局へ、疑似ランダムな認証呼掛け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 ) 疑似ランダムな認証呼掛け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。

20

## 【 0 0 2 6 】

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な認証呼掛けを受け取るための手段、( c ) テレサービス局へ、疑似ランダムな認証呼掛け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 ) 疑似ランダムな認証呼掛け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。

30

## 【 0 0 2 7 】

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な認証呼掛けを受け取り、( c ) テレサービス局へ、疑似ランダムな認証呼掛け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 ) 疑似ランダムな認証呼掛け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。

40

## 【 図面の簡単な説明 】

## 【 0 0 2 8 】

【 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。

50

【図 3】伝送中に D T M F 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 D T M F 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 D T M F 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 D T M F 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

10

20

30

40

50

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、EEPROM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

10

20

30

40

50

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、呼掛け-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呼掛けを送ってよい（214）。セキュリティ装置102は、呼掛けを受け取って返答（例えば識別子および呼掛けに対する応答）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呼掛け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、ランダム呼掛け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】

同じ呼掛け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呼掛け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、（ランダム呼掛け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。

10

#### 【0043】

呼掛け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、呼掛け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／または呼掛け応答が成功裡に認証されたことを示してよい。

20

#### 【0044】

一旦呼掛け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）。

30

40

#### 【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

50



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。

10

【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。

20

【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呼掛け信号が送られる(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)。受け取っていないければ、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。

30

40

【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

50

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呼掛け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 A 506 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 B 508 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呼掛けを受け取ってよい（612）。セキュリティ装置は、呼掛け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]

10

20

30

40

50

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。

10

#### 【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呼掛けを送る（808）。次いで、移動体通信装置は、ランダム呼掛け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呼掛け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。

20

30

#### 【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。

40

#### 【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（

50

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。

10

#### 【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、 $MAC_K$ (呼掛け)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。

20

#### 【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、 $Response = MAC_K("extra\ information\ string"\ Authentication\ Key\ Challenge)$ でよい。

30

#### 【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。

40

#### 【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トーンをデジタル値に変換し、各デ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、デジタル値を暗号化する。次いで、暗号化されたデジタル値は、セキュリティサーバ(例えばテレサービス局)へ、デジタル形式で、または暗号化されたデジタル値と関連したDTMFトーンとして、伝送されてよい。

#### 【0066】

50

D T M F トーンは、デジタル記号で表される（あるいはデ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 A E S ( A d v a n c e d E n c r y p t i o n S t a n d a r d )、O F B ( O u t p u t F e e d b a c k )、または C F B ( C i p h e r t e x t F e e d b a c k ) 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、M A C 関数は、C B C - M A C 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 A E S をハードウェアで実施した場合、これは有利であり得る。

#### 【 0 0 6 7 】

これらの関数がソフトウェアで実施されるなら、非線形 S O B E R ( N L S ) 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、M A C 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。

#### 【 0 0 6 8 】

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 D T M F トーンのデジタル表現）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 ( X O R ) 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 D T M F 対応の電話機は 10 個以上のキーを有し、各キーは一意的なトーンを有する。したがって、キーストリームで前記 D T M F トーンを暗号化するのに X O R 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 D T M F トーンは、キーストリームから得られた疑似乱数 / 記号に加算され得る様々なデ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 D T M F 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疑似乱数は「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。

#### 【 0 0 6 9 】

##### [ 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疑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疑似乱数を得て、同じように（例えばモジュロ 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はなく、1つの特徴に、複数の変換表のうちの1つを疑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。

#### 【 0 0 7 0 】

図 9 は、暗号化されるべき各記号に対して変換表を疑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。疑似乱数 / 記号のキーストリーム S i 9 0 4 を発生するのに暗号ジェネレータ 9 0 2 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 P i 9 0 8 向けに、複数の可能な変換表から様々な変換表 9 0 6 を発生するかまたは得るために、キーストリーム 9 0 4 の疑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 9 0 8 を疑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 C i 9 1 0 が

10

20

30

40

50

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 $C_i$ が与えられると、逆置換の表を形成するか、または記号 $C_i$ 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 $P_i$ 908を暗号化されたアウトプット記号 $C_i$ 910（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 $C_i$ 910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疑似ランダム的にシャッフル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

10

20

30

40

50

換表 1 0 0 2 の一実施例を示す。この実施例では、1 6 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 1 6 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、2 5 6 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。

#### 【 0 0 7 7 】

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对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。

#### 【 0 0 7 8 】

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。

#### 【 0 0 7 9 】

図 1 1 は、暗号化された記号 1 1 0 6 を得るために、プレーンテキスト記号 1 1 0 2 が様々な変換表 1 1 0 4 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  $P_0$ 、 $P_1$ 、 $P_2$ 、 $P_3$ 、...、 $P_i$  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 1 1 0 4 を用いて、暗号化された記号  $C_0$ 、 $C_1$ 、 $C_2$ 、 $C_3$ 、...、 $C_i$  を得る。

#### 【 0 0 8 0 】

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 1 2 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 4 7 9 , 0 0 1 , 6 0 0 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、3 2 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 2 5 6 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  $8.5 \times 10^{506}$  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 1 6 8 4 ビットを超過して必要とすることになる。

#### 【 0 0 8 1 】

図 1 2 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、3 2 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な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（1 2 0 2）。 $n!$  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  $P_{max}$  が定義される。擬似乱数  $w$  がこの最大しきい値  $P_{max}$  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  $P_{max}$  以上であると擬似乱数  $w$  は廃棄され、最大しきい値  $P_{max}$  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（1 2 0 4）。

#### 【 0 0 8 2 】

擬似乱数  $w$  は  $n!$  を法として除算され、その結果、 $w = w \bmod n!$  となる（1 2 0 6）。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。

#### 【 0 0 8 3 】

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、 $P = [0, 1, 2, \dots, n-1]$  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  $i \geq 0$  の間、擬似乱数  $w = w / (i+1)$ 、変数  $j = w \bmod (i+1)$  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  $C_i' 1310$  を得るために、プレーンテキストのインプット記号  $P_i 1302$  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  $S_i' 1306$  に基づいて発生されるかまたは選択され得る変換表  $A_1 1304$  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  $C_i' 1310$  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  $S_i 1314$  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  $A_2 1312$  へのインプットとして働き、 $A_2$  は第 2 の暗号化されたアウトプット記号  $C_i 1318$  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  $C_i' 1310$  を認証するのに冗長性が用いられてよい。すなわち、記号  $C_i' 1310$  と  $C_i 1318$  を一緒に用いることにより、記号  $C_i 1318$  が  $C_i' 1310$  を認証する。したがって、例えば、攻撃者が記号  $C_i' 1310$  を変化させることに成功すると、それは記号  $C_i 1318$  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  $P_i$  を 1 対の記号  $C_i' / C_i$  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  $P_n$  を 1 対の記号  $C_n'$  および  $C_n$  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  $P_n = '5'$  に対して、第 1 の変換表  $A_1 1502$  は、第 1 のアウトプット記号  $C_n' = 8$  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  $A_2 1504$  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  $C_n = 7$  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  $C_n'$  に基づいて第 2 のアウトプット記号  $C_n$  が発生されたので、冗長な記号  $C_n$  および  $C_n'$  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  $C_n'$  が  $'8'$  から  $'4'$  へ変更されると、記号  $C_n'$  および  $C_n = '47'$  を受け取る受信者は、 $C_n = '7'$  が  $C_n' = '4'$  でなく  $C_n' = '8'$  を意味するは

10

20

30

40

50



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  $B1 \quad 1506$  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  $B2 \quad 1508$  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。

10

【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。

20

【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。

30

【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  $C_i$  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  $C_i \quad 1702$  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  $S_i \quad 1706$  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  $A1 \quad 1704$  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  $C_i \quad 1710$  を得る。第1の解読されたアウトプット記号  $C_i \quad 1710$  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  $S_i \quad 1714$  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  $A2 \quad 1712$  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  $P_i \quad 1718$  を得るのに用いられる。

40

【0094】

例えば  $C_i = (x, y)$  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  $P_i$  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

50

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。

10

20

30

40

50

## 【 0 1 0 0 】

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。

## 【 0 1 0 1 】

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。

10

## 【 0 1 0 2 】

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。

20

## 【 0 1 0 3 】

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。

【図 1】

図 1

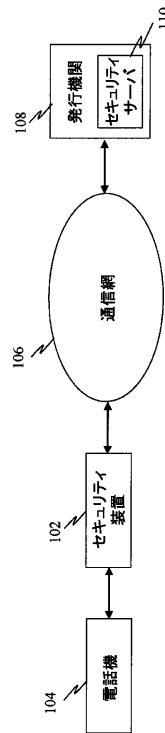


Figure 1

【図 2】

図 2

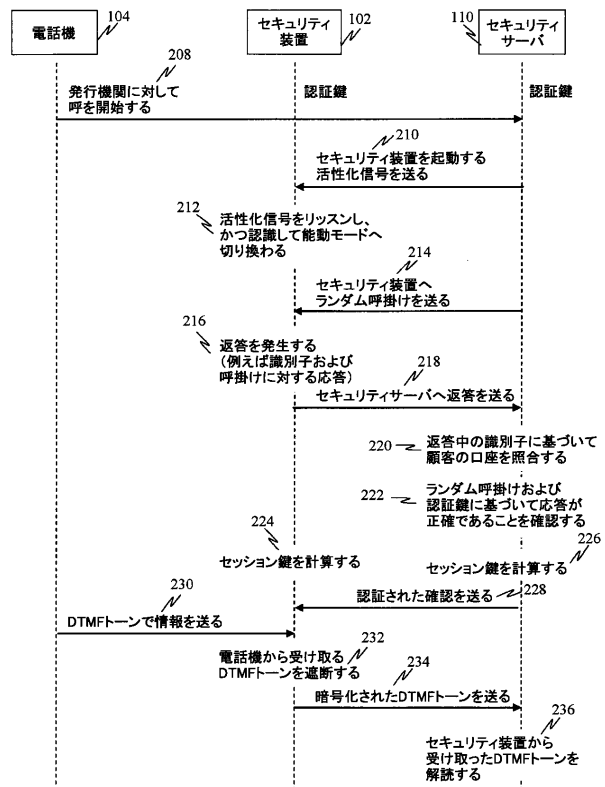


Figure 2

【図 3】

図 3

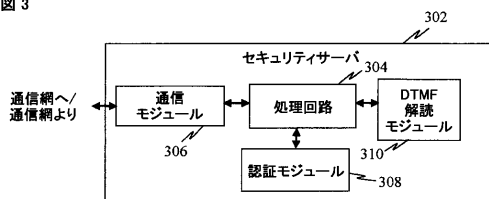


Figure 3

【図 5】

図 5

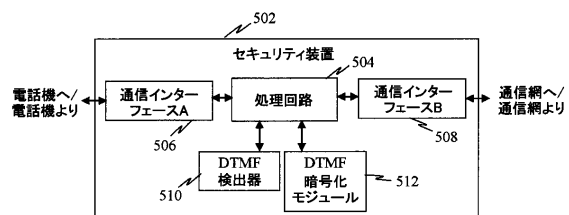


Figure 5

【図 4】

図 4

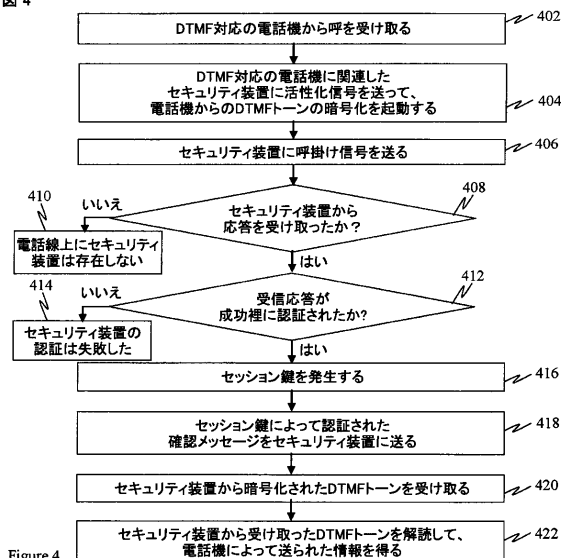


Figure 4

【 図 6 】

図 6

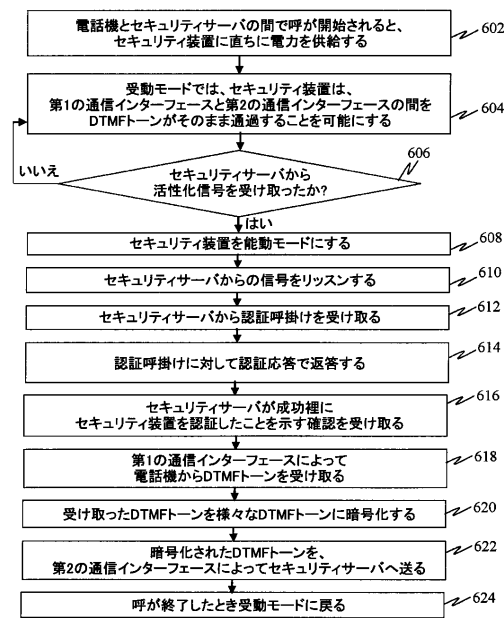


Figure 6

【 図 7 】

図 7

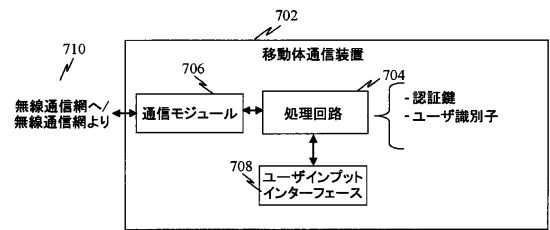


Figure 7

【 図 8 】

図 8

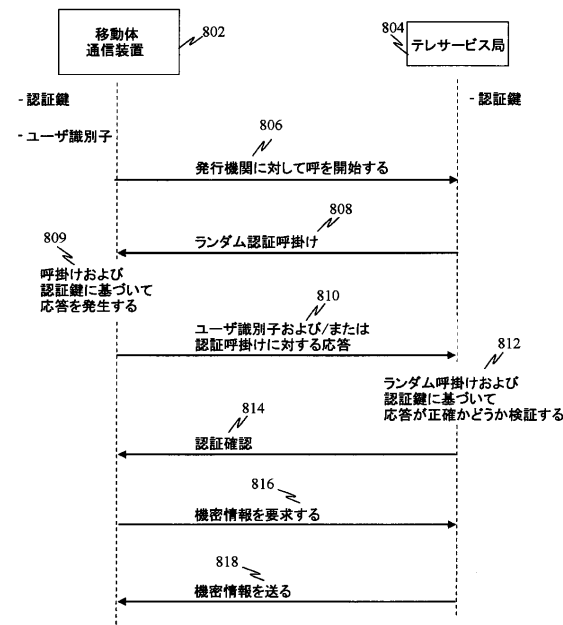


Figure 8

【 図 9 】

図 9

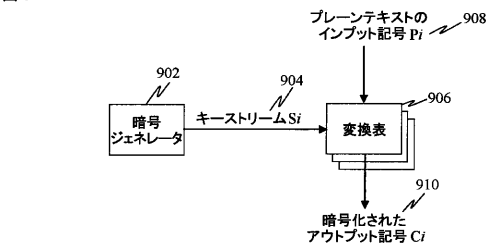


Figure 9

【 図 10 】

図 10

プレーンテキスト記号	プレーンテキスト記号の2進値	暗号化された記号	暗号化された記号の2進値
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

Figure 10

【図 1 1】

図 11

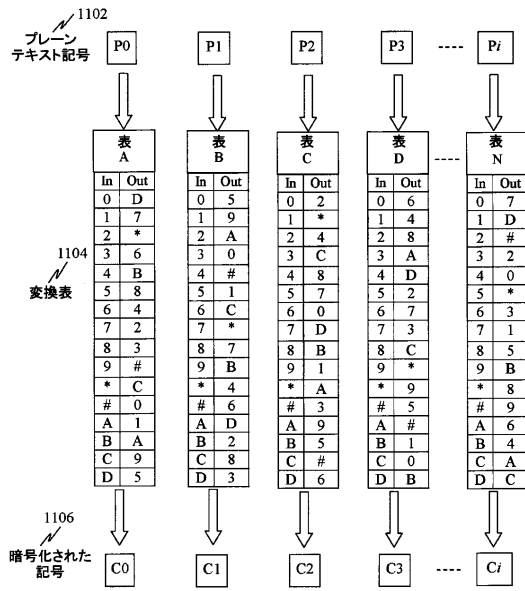


Figure 11

【図 1 2】

図 12

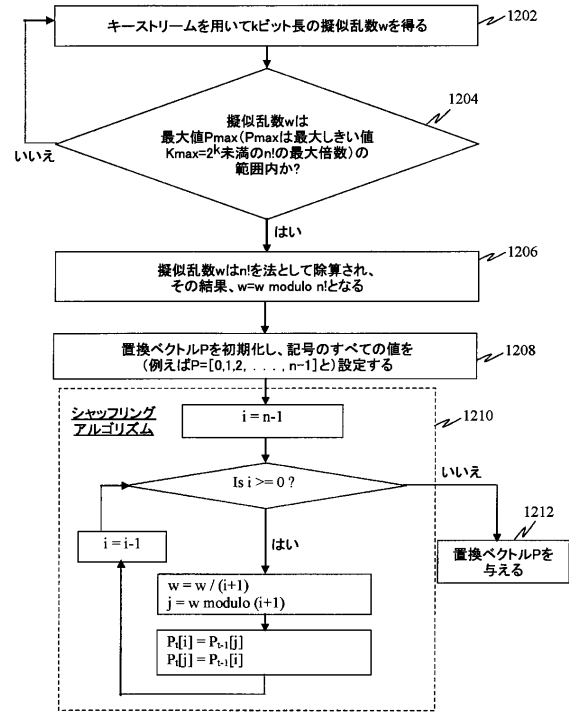


Figure 12

【図 1 3】

図 13

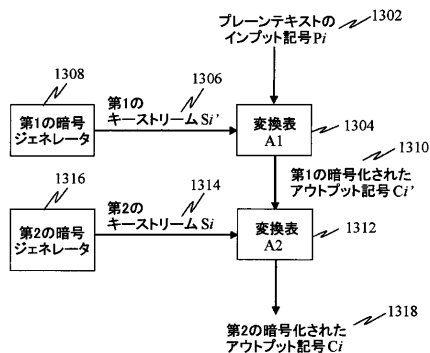


Figure 13

【図 1 5】

図 15

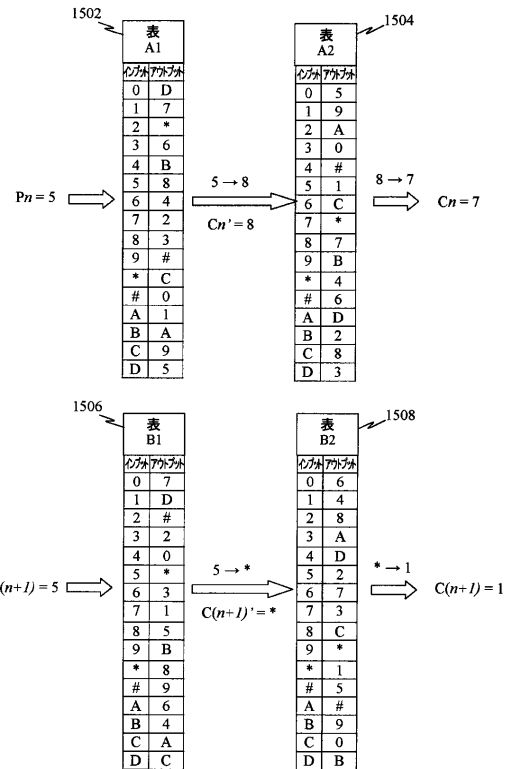


Figure 15

【図 1 4】

図 14

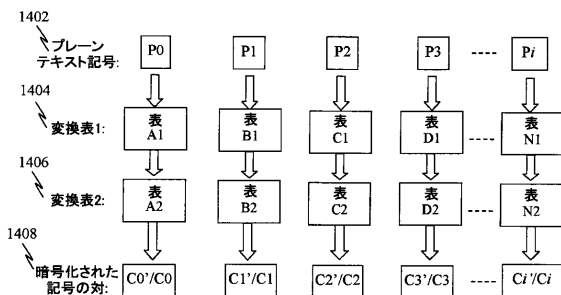


Figure 14

【図 16】

図 16

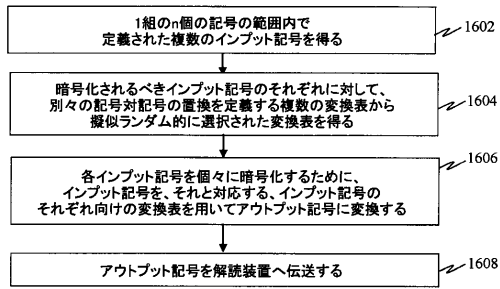


Figure 16

【図 18】

図 18

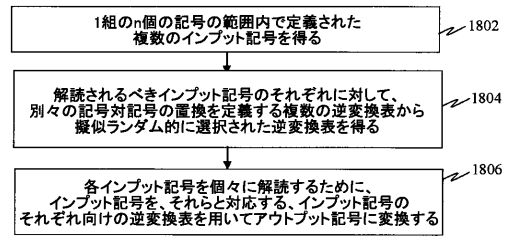


Figure 18

【図 17】

図 17

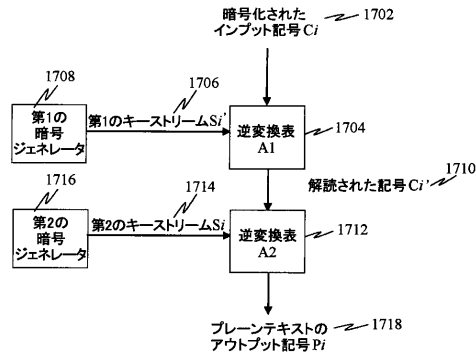


Figure 17

【図 19】

図 19

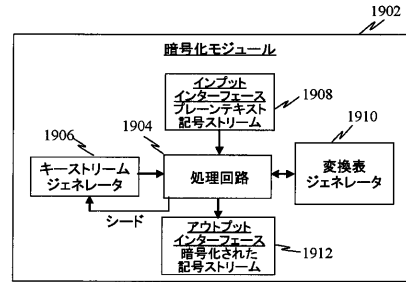


Figure 19

【図 20】

図 20

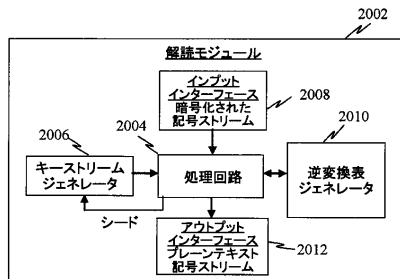


Figure 20

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2007/087312

A. CLASSIFICATION OF SUBJECT MATTER  
INV. H04M3/16 G07F7/00  
ADD. H04M1/215

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)  
H04M G07F

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	DE 43 25 459 A1 (C2S GMBH CRYPTOGRAPHISCHE SICHE [DE]) 9 February 1995 (1995-02-09) abstract column 1, line 1 - column 1, line 37 column 2, line 12 - column 4, line 18 claims 1, 15 figures 1-4	1-53
X	US 6 704 715 B1 (ROSSET FRANCK [FR] ET AL) 9 March 2004 (2004-03-09) abstract figure 1 column 1, line 6 - column 1, line 14 column 1, line 62 - column 4, line 57 column 5, line 3 - column 5, line 52 -/-	1-53

☒ Further documents are listed in the continuation of Box C.

☒ 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.

"G" document member of the same patent family

Date of the actual completion of the international search

28 May 2008

Date of mailing of the international search report

04/06/2008

Name and mailing address of the ISA/  
European Patent Office, P.B. 5318 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Molinari, Fausto



## INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2007/087312

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/046092 A1 (OSTROFF MAURICE [IL]) 18 April 2002 (2002-04-18) figures 2-6 paragraphs [0082], [0083] paragraphs [0144] - [0151] claims 1,10,15 -----	1-53

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2007/087312

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4325459	A1	09-02-1995	NONE
US 6704715	B1	09-03-2004	AT 316725 T 15-02-2006
		AU 4388897 A 17-04-1998	
		DE 69735166 T2 16-11-2006	
		DK 0950303 T3 29-05-2006	
		EP 0950303 A1 20-10-1999	
		ES 2257781 T3 01-08-2006	
		FR 2753860 A1 27-03-1998	
		WO 9813971 A1 02-04-1998	
		JP 2001508563 T 26-06-2001	
		PT 950303 T 30-06-2006	
US 2002046092	A1	18-04-2002	US 2006190412 A1 24-08-2006

## 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 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5
- (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 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5
- (72)発明者 チョイ、ジェ - ヒー

アメリカ合衆国、カリフォルニア州 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5

(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 9 2 1 2 1、サン・ディエゴ、モアハウス・ドライブ 5 7  
7 5

F ターム(参考) 5J104 AA07 AA16 AA32 EA01 EA17 HA01 KA02 NA06 NA10 PA02

5K127 AA21 BB27 BB32 CA26 EA25 GE04 KA12

5K201 AA08 CD04 EC05