(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2009-253967
(P2009-253967A)
(43)公開日　平成21年10月29日(2009.10.29)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601C	5J104
H04L	9/10	(2006.01)	H04L	9/00	621A	5K201
G09C	1/00	(2006.01)	G09C	1/00	660F	
H04M	7/00	(2006.01)	G09C	1/00	660G	
			H04M	7/00	A	

審査請求 未請求　請求項の数 5　書面　（全 8 頁）

(21)出願番号　特願2008-123976 (P2008-123976)
(22)出願日　平成20年4月10日 (2008.4.10)

(71)出願人　307006321
竜沢　剣
東京都墨田区文花３－１７－１６－８０８
(71)出願人　508005288
竜沢　前恵
東京都墨田区文花３－１７－１６－８０８
(72)発明者　竜沢　剣
東京都墨田区文花３－１７－１６－８０８
(72)発明者　竜沢　前恵
東京都墨田区文花３－１７－１６－８０８

Fターム(参考)　5J104 AA01 AA16 AA32 DA03 EA04
EA08 EA16 EA17 EA18 EA19
JA03 JA21 NA02 NA03 NA36
NA37 PA02
5K201 AA08 BB07 BD06 CA01

(54)【発明の名称】共通キー暗号と公開キー暗号と認証との組み合わせにより電話機種に縛られない・設定の必要がない・つけるだけですぐに使える電話音声セキュリティ保護を実現する電話音声セキュリティ保

(57)【要約】
【課題】優れた効率と高安全性電話音声セキュリティ保護装置及び実施方法を提供する。
【解決手段】本発明は、各種の電話機種と形態の制限に縛られず、電話機とは別の独立とした電話音声セキュリティ保護装置を電話に付けるだけですぐに装置を付けた通話の両者あるいは複数の通話者のお互いの音声を保護する装置と方法を提供する。公開キー暗号と、秘密キー暗号と、認証の組み合わせにより効率の高い高セキュリティ音声保護機能を提供する。装置は設定の必要がなく、付けるだけですぐに使えるという面倒のいらない装置で、通話者の音声を自動的に暗号化と復号化するプロセスにより、通話者の音声情報を保護し、盗聴を不可能にする。また、通話者の音声セキュリティ強度を保証するために、不定期的に秘密キーが更新される。
【選択図】図１

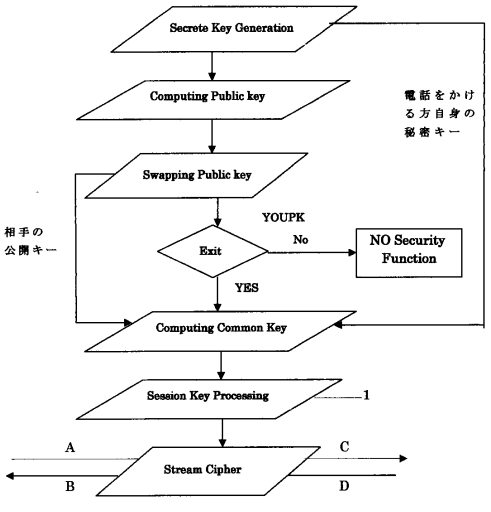

図 1. 本発明の電話音声セキュリティ保護装置の仕組みと方法の全体流れ図。
1. Session キーの生成及び暗号化及び配送
A. 暗号化する前の音声情報
B. 復号化した音声情報を受信
C. 暗号化した音声情報を通話先に送信
D. 暗号化した音声情報を受信

【特許請求の範囲】
【請求項１】
電話通話の両者又は複数の通話者の間の音声を保護し、第三者による盗聴を防止する電話音声セキュリティ保護装置において、
通話の両者又は複数の通話者の間の音声を保護する電話機と別に独立とした電話音声セキュリティ保護装置と、
電話音声セキュリティ保護装置の自動的に乱数を生成する乱数生成プロセスと、
前記電話音声セキュリティ保護装置の自動的に乱数を生成するプロセスにより生成された乱数を秘密キーとして、ＤＨ鍵交換アルゴリズムに基づいて公開キーを計算する公開キー計算方法とプロセスと、
認証方法に基づいて通話の両者または複数の通話の方の間の身分を認証し、前記の公開キー計算方法とプロセスで得られた通話の両者または複数の方の公開キーを交換する公開キー交換プロセスと方法と、
前記公開キー交換プロセスにより、通話先の方がこの装置を付けたかどうかを自動的に確認する音声装置確認プロセスと、
話し側の通話者の秘密キーと話し相手の公開キーの使用により、Ｃｏｍｍｏｎキーを計算するＣｏｍｍｏｎキー計算プロセスと、
電話音声セキュリティ保護装置は自動的にＳｅｓｓｉｏｎ　ｋｅｙを生成するＳｅｓｓｉｏｎ　ｋｅｙ生成プロセスと、
Ｓｅｓｓｉｏｎ　ｋｅｙの処理及び配送するＳｅｓｓｉｏｎ　Ｋｅｙ処理及び配送プロセスと、
共通キー暗号により、音声信号を自動的に暗号化と復号化するプロセスと、
音声セキュリティの安全性の強度を保証するために、秘密キーを不定期的に更新する秘密キー更新プロセスと、
通話先が装置を付けていない場合、通話の音声信号受送は影響されず自動に非キュリティ機能に切り換えされるプロセス、
ことを特徴とする公開キー暗号と共通キー暗号と認証との組み合わせにより通話両者または複数の方の間の音声を保護し、第三者による盗聴を防止する電話音声セキュリティ保護装置のアイディアと音声保護実施方法。
【請求項２】
前記に記載された電話音声セキュリティ保護装置において、電話機に付けるだけですぐにセキュリティ化できることと通話者の設定が必要ないことの便利さと面倒がかからない装置のアイディアと音声セキュリティ保護の実施方法と、
【請求項３】
前記に記載された電話音声セキュリティ保護装置は、電話機とは別に独立とした装置であり、各電話の機種と形態と制限に縛られず、装置を付けるだけですぐにどの電話にも使える電話音声セキュリティ保護装置のアイディアと実施方法と、
【請求項４】
音声セキュリティの安全性を保証するには、秘密キーを不定期的に更新する秘密キー更新のアイディアとプロセスと、
【請求項５】
前記請求項１乃至請求項４に記載された方法や装置のアイディアにより公開キー暗号と共通キー暗号と認証の組み合わせで音声を自動的に暗号化と復号化する音声セキュリティ保護装置のアイディアと音声保護実施方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、共通キー暗号と公開キー暗号と認証との組み合わせにより電話音声保護を実現する電話音声セキュリティ保護装置のアイディアと音声保護方法に関する。
【背景技術】

【０００２】
現在の日本と世界で使われている電話、特に固定電話は、音声セキュリティの保護措置がありません。年々増える国内と国外の電話台数は巨大な市場を作っている。同時に、発達している現在の情報社会は情報の保護を必要としている。本発明の電話セキュリティ保護装置は通信データ量を増加せずに、高速的に音声暗号化と復号化を実現し、面倒の欠かせない小型の安全性が高い軽量な音声セキュリティ保護装置のアイディアと実施方法を通話両者または複数の通話の方の間に提供する。本発明は電話機とは別にとした独立の装置で、設定が必要なく、付けるだけですぐに使える簡単な装置である。通話先がもしこの装置をつけていない場合でも、通話のお互いの通信は影響されず装置が自動的な非セキュリティ機能を起動し、通話者は通常の通話を楽しむことができる。セキュリティ性の強度を守り、秘密キーは不定期的に更新される。公開キー暗号と共通キー暗号と認証技術との組み合わせにより、各電話の機種と形態と制限に縛られず自然的に電話音声セキュリティ保護を実現し、情報を現実的に守る方法を提供する。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
前述のように、今に使われている電話、特に固定電話は、音声に関するセキュリティ保護がありません。本発明の電話音声セキュリティ保護装置は徹底的に音声安全性の問題を解決する。本発明の音声セキュリティ保護装置は電話の機種と形態と制限に縛られず、どの電話にも対応する独立とした装置であり、面倒がかからないので、付けるだけですぐに音声セキュリティ保護機能が起動し始める。音声セキュリティ保護装置を通話者の両者または複数の通話者に付けるだけで、音声が保護され、他の人に情報を盗聴されない。
【０００４】
本発明の音声セキュリティ保護装置は、装置を付けた電話と付けていない電話ともに対応する。装置を付けた電話同士で電話をかける時、自動的に両者または複数の通話者のお互いの音声が保護される。また、片方の通話者の電話だけが装置を付けた場合、通話同士のお互いの音声通信の受送信号は影響されなく、装置は自動的に非セキュリティに切り換えられ、通話者同士は通常の通話を楽しむことができる。
【課題を解決するための手段】
【０００５】
前述の課題を解決するために本発明は次の手段を提供する。
【０００６】
（１）各電話の機種と形態と制限に縛られず、どの電話にも使えて、電話機とは別に独立とした音声のセキュリティを保護する電話音声セキュリティ保護装置と、音声装置を付けた電話にも、付けない電話にも対応すると、
音声のセキュリティ保護装置と、設定のいらない、付けるだけですぐに通話両者または複数の通話者の音声を自動的に保護する電話音声セキュリティ保護装置において、
電話音声セキュリティ保護装置は、自動的に乱数を生成し、その乱数生成プロセスで生成された乱数を通話者の秘密キーとする秘密キー生成プロセスと、
前記秘密キー生成プロセスで生成された秘密キーは、ＤＨ鍵交換アルゴリズムによって、公開キーを計算する公開キー計算プロセスと、
前記公開キー計算プロセスより計算された公開キーは、ＤＨ鍵交換アルゴリズムによって、
通話両者または複数の通話者の公開キーをお互いに交換する公開キー交換プロセスと、
前記公開キー交換プロセスにより、通話先がこの音声保護装置を付けたかどうかの自動的に確認する音声装置確認プロセスと、
前記公開キー交換プロセスにより、通話者の秘密キーと話し相手の公開キーをＤＨ鍵交換アルゴリズムに基づいてＣｏｍｍｏｎキーを計算するＣｏｍｍｏｎキー計算プロセスと、
音声セキュリティの安全性を保証するために、秘密キーを不定期的に更新する秘密キー更新プロセスと、

電話音声セキュリティ保護装置が自動的にＳｅｓｓｉｏｎ　ｋｅｙを生成するＳｅｓｓｉｏｎ　ｋｅｙ生成プロセスと、
Ｓｅｓｓｉｏｎ　ｋｅｙの処理及び配送するＳｅｓｓｉｏｎ　ｋｅｙ処理及び配送プロセスと、
前記Ｓｅｓｓｉｏｎキー処理及び配送プロセスで処理及び配送されたＳｅｓｓｉｏｎキーは暗号キーとして、共通キー暗号（ストリーム暗号）の利用を通して自動的に音声の暗号化または復号化の実施を行う音声暗号化と復号化プロセス、
ことを特徴とする自動的な音声セキュリティ暗号化と復号化方法と音声セキュリティ保護装置のアイディア。

【０００７】

（２）前記（１）に記載された方法により音声を自動的に暗号化と復号化をし、公開キー暗号と共通キー暗号と認証との組み合わせを通して自動的に音声を暗号化と復号化する実施方法を特徴とする認証機能付きの音声暗号化セキュリティ保護方法。

【発明の効果】

【０００８】

本発明によれば、効率の高い電話音声セキュリティ保護の自動暗号化と復号化方法と音声セキュリティ保護装置を提供する。本発明の電話音声セキュリティ保護装置は徹底的に音声安全性の問題を解決する。本発明の音声セキュリティ保護装置は電話の機種と形態と制限に縛られず、どの電話にも対応できる独立とした装置であり、面倒がかからない、付けるだけですぐに音声セキュリティ保護機能起動し始める装置である。音声セキュリティ保護装置を通話者の両者または複数の通話者の電話機に付けるだけで、音声保護ができ、他の人に情報が盗聴されない。本発明の音声セキュリティ保護装置は、装置を付けた電話と付けない電話とも対応することができる。装置を付けた電話同士で電話をかける時、自動的に両者または複数の通話者の音声が保護される。また、片方の電話だけが装置を付けた場合、通話同士のお互いの音声通信の受送信号は影響されなく、装置は自動的に非セキュリティに切り換えられ、通話者同士は通常の通話を楽しむことができる。

【発明を実施するための最良の形態】

【０００９】

次に本発明の実施の形態を挙げ、図面を参考し、本発明を一層具体的に説明する。

【００１０】

［概要］

本発明は、電話の音声セキュリティ保護の装置と実施方法に関し、公開キー暗号と共通キー暗号と認証との組み合わせにより通話両者または複数の通話同士の音声を自動的に暗号化・複合化し、効率の高い音声セキュリティ保護を現実的実現する手段を提供する。本発明は、各電話の機種と形態に制限されず、どの電話にも対応できる独立とした音声セキュリティ保護装置である。また、本発明は、通話先が本装置を付けている場合でも、付けていない場合でも対応できる音声セキュリティ保護装置である。

【００１１】

以下、本願発明について、実施の形態を挙げ、説明する。

【００１２】

本発明の電話音声セキュリティ保護装置を付けるだけですぐに音声セキュリティ保護機能が起動し、すぐに自動的に乱数が生成される。生成された乱数は通話者の秘密キーとなる。安全性の強度を保証するために、秘密キーは頻繁的に、自動的に更新される。秘密キーの長さはセキュリティの強度の要求に合わせて自動的に設定される。

【００１３】

前記の秘密キー生成プロセスで生成された秘密キーは、ＤＨ鍵交換アルゴリズムによって、自動的に公開キーを計算する。
$MYPK = g^{MYSK} \bmod P$の式は公開キーを自動的に計算する式である。このときのＭＹＰＫは電話をかける側の通話者自身の公開キーであり、ＭＹＳＫは電話をかける側の通話者自身の秘密キーであり、ｇはＰｒｉｍｉｔｉｖｅ　Ｒｏｏｔで、Ｐは大きな素数

（Ｐｒｉｍｅ）である。
【００１４】
電話をかける側の電話音声セキュリティ保護装置は、ＤＨ鍵交換アルゴリズムにより、前記公開キー計算プロセスで計算された公開キーを通話先側の公開キーと自動的に交換する。
Ｍａｎ－Ｉｎ－Ｔｈｅ－Ｍｉｄｄｌｅ　ａｔｔａｃｋの攻撃を防止するために、認証の技術が使用われる。
【００１５】
前記公開キー交換プロセスにより、通話先がこの音声セキュリティ保護装置を付けたかどうかは電話をかける側の音声装置により自動的に確認する。電話をかける側の音声装置は通話先の公開キーと交換できない場合、通話先が音声装置を付けていないと判断する。
【００１６】
ＤＨ鍵交換アルゴリズムに基づいて、電話をかける側の秘密キーと通話先の公開キーを使用することにより、新Ｃｏｍｍｏｎキーを計算する。
Ｃｏｍｍｏｎキー＝ＹＯＵＰＫ^{ＭＹＳＫ}ｍｏｄ　Ｐの式で、ＹＯＵＰＫは話し相手の公開キーで、Ｃｏｍｍｏｎキーは電話音声セキュリティ保護装置の中でＳｅｓｓｉｏｎ　ｋｅｙを暗号化するための暗号キーである。
【００１７】
電話音声セキュリティ保護装置は自動的にＳｅｓｓｉｏｎ　ｋｅｙを生成する。このＳｅｓｓｉｏｎ　ｋｅｙは毎回の通話に１回だけ使われ、毎回に新しいＳｅｓｓｉｏｎ　ｋｅｙが生成される。
【００１８】
前記生成したＳｅｓｓｉｏｎ　ｋｅｙはＣｏｍｍｏｎキーで、共通キー暗号により暗号化され、通話先に配送する。通話先が暗号化したＳｅｓｓｉｏｎ　ｋｅｙを受信した後、自動的にＣｏｍｍｏｎキーで電話をかけた側と同じ共通キー暗号を復号化する。このプロセス後、通話の両者又は複数の通話者は同じＳｅｓｓｉｏｎ　ｋｅｙが持つことになる。
【００１９】
前記プロセスで生成されたＳｅｓｓｉｏｎ　ｋｅｙは共通キー暗号（ストリーム暗号）の暗号キーとして使われ、電話をかける側の音声情報は通話先に送信する前にまず自動的に暗号化され、その後に、暗号化された情報が電話先に送られ、音声が自動的に本発明の音声保護装置で復号化される。そして、通話先に対しても電話をかける側と同じく、受話した情報は受話者側に届いた後に自動的に復号され、また、通話先も同じく、電話をかける時情報内容はまず暗号化され、そのあとに話し相手側に送り、受話側の装置は自動的に本発明の音声保護装置で暗号化された情報を復号化する。通話の期間では、［００１９］項で記述していた暗号化と復号化プロセスは電話をかける側（送話側）と受話側の両側で繰り返して行い、通話終了まで続く。次回の通話は、項［００１４］乃至項［００１９］のプロセスを繰り返して行う。
【００２０】
安全性の強度を保証するために、電話音声保護装置は自動的に不定期に頻繁的に音声セキュリティ保護装置の秘密キーを更新し、前記［００１２］－［００１９］項目までのプロセスを繰り返して行う。
【００２１】
公開キーを交換する時、通話先の信号反応により通話先が音声セキュリティ保護装置を付けたかどうかを自動的に判断する。もし片方の通話先だけが音声セキュリティ保護装置を付いていない場合、装置の非セキュリティ機能が自動的に起動され、通信信号がそのままに受送信し、通話者同士は普通の電話として楽しむことができる。
【００２２】
本発明では、電話の機種と形態と制限に縛られず、どの電話にも対応する、電話機とは別に独立とした電話音声セキュリティ保護装置である。公開キー暗号と共通キー暗号と認証との組み合わせにより通話両者もしくは複数の話し方とのお互いに音声を自動的に暗号化

と復号化を行う装置アイディアと方法である。

【００２３】

本願発明は、具体的に詳しく説明した前述の実施の形態に制限されるものではなく、特許請求の範囲に記載した範囲において各種の変形が可能であることを、ここにあらためて確認する。

【図面の簡単な説明】

【００２４】

【図１】本発明の電話音声セキュリティ保護装置の仕組みと方法の全体流れ図。

【図２】秘密キーの生成するプロセス

【図３】公開キー（Ｐｕｂｌｉｃ　ｋｅｙ）の生成プロセス

【図４】Ｃｏｍｍｏｎキーの生成プロセス

【図５】通話両者もしくは複数の通話者のお互いの音声情報を自動的暗号化・復号化する電話音声セキュリティ保護装置の仕組み。

【図１】

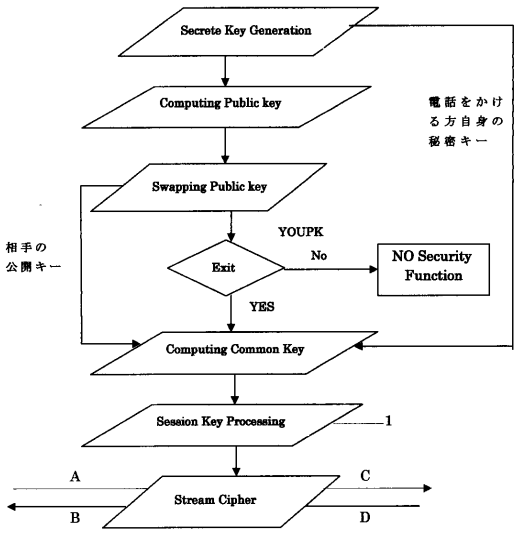

図 1. 本発明の電話音声セキュリティ保護装置の仕組みと方法の全体流れ図。
1． Session キーの生成及び暗号化及び配送
A. 暗号化する前の音声情報
B. 復号化した音声情報を受信
C. 暗号化した音声情報を通話先に送信
D. 暗号化した音声情報を受信

【図２】

図２．秘密キーの生成

【図３】

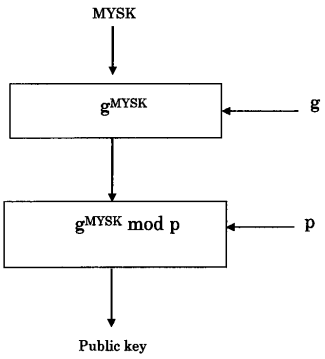

図３．公開キー（Public key）の生成

MYSK　電話をかける側の通話者自身の秘密キー

g　Primitive Root

P　大きな素数（Prime）

【図４】

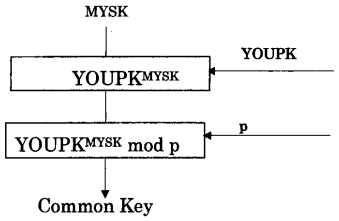

図４．Common キーの生成
MYSK　電話をかける側の通話者自身の秘密キー
YOUPK　電話をかける側の通話者自身の公開キー
P　大きな素数（Prime）

【図５】

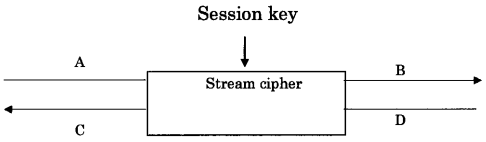

図５．音声情報に対する自動的暗号化・復号化プロセス
A．暗号化する前の音声情報
B．暗号化した音声情報を通話先に送信
C．復号化した音声情報を受信
D．暗号化した音声情報を受話先に送信

フロントページの続き

(54)【発明の名称】共通キー暗号と公開キー暗号と認証との組み合わせにより電話機種に縛られない・設定の必要がない・つけるだけですぐに使える電話音声セキュリティ保護を実現する電話音声セキュリティ保護装置のアイディアと音声保護の方法。