

【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17年7月21日(2005.7.21)

【公開番号】特開2003-8565(P2003-8565A)

【公開日】平成15年1月10日(2003.1.10)

【出願番号】特願2002-99963(P2002-99963)

【国際特許分類第7版】

H 04 L 9/08

H 04 Q 7/38

【F I】

H 04 L 9/00 601C

H 04 L 9/00 601E

H 04 B 7/26 109R

【手続補正書】

【提出日】平成16年11月26日(2004.11.26)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

第1のワイヤレスユニットと第2のワイヤレスユニットとの間の安全な通信を提供する方法において、該方法は、

情報を暗号化および/または解読するために、前記第1のワイヤレスユニットによって使用するために前記第1のワイヤレスユニットと、前記第2のワイヤレスユニットとへ共通キー値を、該共通キーを有する、前記第1のワイヤレスユニットおよび第2のワイヤレスユニットの間の少なくとも1つのワイヤレス通信システムを介する安全な通信の間に送るステップからなることを特徴とする方法。

【請求項2】

前記共通キー値を送るステップは、

前記第1のワイヤレスユニットに対応する第1のキー値を生成するステップ、

前記共通キー値を生成するステップと、

前記第1のキー値を使用する前記第1のワイヤレスユニットへ、前記共通キー値を送るステップとを含むことを特徴とする請求項1記載の方法。

【請求項3】

前記第2のワイヤレスユニットに対応する第2のキー値を生成するステップと、

前記第2のキー値を使用する前記第2のワイヤレスユニットへ、前記共通キー値を送るステップとを有する

ことを特徴とする請求項2記載の方法。

【請求項4】

前記第1のキー値を生成するステップは、

前記第1のワイヤレスユニットおよび前記第1のワイヤレスユニットのためのホームワイヤレス通信システムにおいてのみ知られた第1のルートキーの関数として、前記第1のキー値を生成するステップを含むことを特徴とする請求項2記載の方法。

【請求項5】

前記共通キーを送るステップは、

前記第1のキー値を使用して、前記共通キーを暗号化するステップと、

前記第1のキー値で暗号化された前記共通キーを、前記第1のワイヤレスユニットに送信するステップとを含むことを特徴とする請求項2記載の方法。

【請求項6】

前記送るステップは、

前記第1のキー値および前記第2のキー値のうちの少なくとも1つの関数として、前記共通キーを生成するステップを含むことを特徴とする請求項3記載の方法。

【請求項7】

第1のワイヤレスユニットおよび第1のワイヤレスユニットのためのホームワイヤレス通信システムにおいてのみ知られた第1のルートキーの関数として、第1のセッションキー値を生成するステップと、

少なくとも前記第1のセッションキー値の関数であるセッション暗号化キーとして前記共通キーを生成するステップとを有することを特徴とする請求項1記載の方法。

【請求項8】

前記第1のワイヤレスユニットのための第1のワイヤレス通信システムおよび前記第2のワイヤレスユニットのための第2のワイヤレス通信システムにより、前記共通キーを相互に生成するステップをさらに含むことを特徴とする請求項1記載の方法。

【請求項9】

第1のワイヤレスユニットと第2のワイヤレスユニットとの間の安全な通信を提供する方法において、該方法は、

少なくとも1つのワイヤレス通信システムから共通キー値を受信するステップを有し、前記共通キーは、該共通キーを有する、前記第1のワイヤレスユニットおよび前記第2のワイヤレスユニットの間の少なくとも1つのワイヤレス通信システムを介する安全な通信に使用するために、前記第1のワイヤレスユニットによって使用するために前記第1のワイヤレスユニットと、前記第2のワイヤレスユニットによって使用するために前記第2のワイヤレスユニットとにおいて受信されることを特徴とする方法。

【請求項10】

前記第1のワイヤレスユニットに対応する第1のキー値を生成するステップと、

前記第1のキー値を使用する前記第1のワイヤレスユニットにより、前記共通キー値を得るステップとを有することを特徴とする請求項9記載の方法。