

【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 0 4 L 9/08

H 0 4 Q 7/38

【F I】

H 0 4 L 9/00 6 0 1 C

H 0 4 L 9/00 6 0 1 E

H 0 4 B 7/26 1 0 9 R

【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。