

【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 26 年 12 月 11 日 (2014.12.11)

【公表番号】特表 2014-529261 (P2014-529261A)
 【公表日】平成 26 年 10 月 30 日 (2014.10.30)
 【年通号数】公開・登録公報 2014-060
 【出願番号】特願 2014-529996 (P2014-529996)
 【国際特許分類】

H 0 4 L 9/08 (2006.01)

【F I】

H 0 4 L 9/00 6 0 1 C

H 0 4 L 9/00 6 0 1 E

【手続補正書】

【提出日】平成 26 年 10 月 14 日 (2014.10.14)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

方法であって、

混合通信ネットワークに関連付けられたネットワーク鍵を受信することと、ここで、前記混合通信ネットワークは、第 1 のネットワーク通信プロトコルおよび第 2 のネットワーク通信プロトコルに関連付けられている、

第 1 のデバイスにおいて、前記混合通信ネットワークの前記第 1 のネットワーク通信プロトコルとともに用いられるための第 1 のプロトコル特有鍵を生成することと、ここで、前記第 1 のプロトコル特有鍵は、前記第 1 のネットワーク通信プロトコルに対応する第 1 の識別子および前記ネットワーク鍵に少なくとも一部基づく、

前記第 1 のプロトコル特有鍵を用いて、前記第 1 のネットワーク通信プロトコルで、前記混合通信ネットワークにおける第 2 のデバイスと通信することと、
 を備える方法。

【請求項 2】

前記第 1 のプロトコル特有鍵は、前記第 1 のネットワーク通信プロトコルによる通信の暗号化のために用いられ、

前記第 1 のプロトコル特有鍵は、前記第 1 の識別子および前記ネットワーク鍵を含むハッシュ演算の結果に少なくとも一部基づいて生成される、請求項 1 に記載の方法。

【請求項 3】

前記第 1 のプロトコル特有鍵を生成することは、

前記第 1 のプロトコル特有鍵を生成するために、前記ハッシュ演算の結果を切り捨てること、

前記ハッシュ演算の結果よりも長い第 1 のプロトコル特有鍵を生成するために、前記ハッシュ演算の結果を複製すること、または、

前記第 1 のプロトコル特有鍵を生成するために、前記ハッシュ演算の結果を、さらなる値と組み合わせること、

のうちの 1 つを含む、請求項 2 に記載の方法。

【請求項 4】

前記第 1 のプロトコル特有鍵を生成することは、ハッシュ演算の結果の最下位 n ビット

を含むように、前記第 1 の識別子と前記ネットワーク鍵との間に前記ハッシュ演算の結果を切り詰めることを含む、請求項 1 に記載の方法。

【請求項 5】

前記混合通信ネットワークの第 2 のネットワーク通信プロトコルに関連付けられた第 2 のプロトコル特有鍵を生成することと、ここで、前記第 2 のプロトコル特有鍵は、前記第 2 のネットワーク通信プロトコルに対応する第 2 の識別子および前記ネットワーク鍵に少なくとも一部基づく、

前記第 2 のプロトコル特有鍵を用いて、前記第 2 のネットワーク通信プロトコルによって、第 3 のデバイスと通信することと、ここで、前記第 1 のプロトコル特有鍵は前記第 2 のプロトコル特有鍵と異なる、

をさらに備える請求項 1 に記載の方法。

【請求項 6】

複数のネットワーク通信プロトコルに対応する複数のプロトコル特有鍵を前記第 1 のデバイスにおいて格納することをさらに備え、

前記複数のプロトコル特有鍵は、少なくとも、前記第 1 のプロトコル特有鍵および前記第 2 のプロトコル特有鍵を含む、請求項 5 に記載の方法。

【請求項 7】

前記第 1 のネットワーク通信プロトコルは、イーサネット、マルチメディア・オーバー・コアキシャル (MoCA)、IEEE 1901、送電線通信、または無線ローカル・エリア・ネットワーク (WLAN) のうちの 1 つであり、

前記第 2 のネットワーク通信プロトコルは、前記第 1 のネットワーク通信プロトコルと異なる、請求項 1 に記載の方法。

【請求項 8】

前記第 1 のネットワーク通信プロトコルに対応する前記第 1 の識別子は、前記第 1 のネットワーク通信プロトコルをユニークに識別する英数字ラベルを備える、請求項 1 に記載の方法。

【請求項 9】

前記混合通信ネットワークにおいて用いられる複数のネットワーク通信プロトコルに対応する識別子を、前記第 1 のデバイスのメモリに格納することをさらに備え、

前記複数のネットワーク通信プロトコルは、少なくとも、前記第 1 のネットワーク通信プロトコルおよび前記第 2 のネットワーク通信プロトコルを含む、請求項 1 に記載の方法。

【請求項 10】

新たなネットワーク通信プロトコルに対応する新たな識別子を、前記第 1 のデバイスのメモリに追加することと、

前記新たなネットワーク通信プロトコルのために、前記新たなネットワーク通信プロトコルに対応する前記新たな識別子および前記ネットワーク鍵に少なくとも一部基づいて、新たなプロトコル特有鍵を生成することと、

前記新たなプロトコル特有鍵を用いて、前記新たなネットワーク通信プロトコルによって、他のデバイスと通信することと、
をさらに備える請求項 9 に記載の方法。

【請求項 11】

前記ネットワーク鍵を前記第 1 のデバイスのメモリに格納すること、
をさらに備える請求項 1 に記載の方法。

【請求項 12】

前記ネットワーク鍵は、

前記第 1 のデバイスのユーザ・インタフェース、

前記第 1 のデバイスのセンサ、または、

前記第 1 のネットワーク通信プロトコルとは異なる、異なるネットワーク通信プロトコルのために構成された前記第 1 のデバイスのネットワーク・インタフェース、

のうちの1つによって受信される、請求項1に記載の方法。

【請求項13】

デバイスであって、

混合通信ネットワークに関連付けられたネットワーク鍵を格納するように構成されたメモリと、ここで、前記混合通信ネットワークは、第1のネットワーク通信プロトコルおよび第2のネットワーク通信プロトコルに関連付けられている、

前記第1のネットワーク通信プロトコルとともに用いられるための第1のプロトコル特有鍵を生成するように構成された鍵ジェネレータと、ここで、前記第1のプロトコル特有鍵は、前記第1のネットワーク通信プロトコルに対応する第1の識別子および前記ネットワーク鍵に少なくとも一部基づく、

前記第1のプロトコル特有鍵を用いて、前記第1ネットワーク通信プロトコルによって通信するように構成された第1の通信インタフェースと、
を備えるデバイス。

【請求項14】

前記鍵ジェネレータはさらに、

前記第1の識別子および前記ネットワーク鍵を含む第1のハッシュ演算の結果を切り詰めること、

前記第1のハッシュ演算の結果の複製すること、または、

前記第1のハッシュ演算の結果をさらなる値と組み合わせること、

によって、前記第1のプロトコル特有鍵を生成するように構成された、請求項13に記載のデバイス。

【請求項15】

前記鍵ジェネレータはさらに、前記第1のプロトコル特有鍵が第1のハッシュ演算の結果の最下位nビットを備えるように、前記第1の識別子および前記ネットワーク鍵を含む前記第1のハッシュ演算の結果を切り詰めるように構成された、請求項13に記載のデバイス。

【請求項16】

前記鍵ジェネレータはさらに、前記混合通信ネットワークの第2のネットワーク通信プロトコルに関連付けられた第2のプロトコル特有鍵を生成するように構成され、

前記第2のプロトコル特有鍵は、前記第2のネットワーク通信プロトコルに対応する第2の識別子および前記ネットワーク鍵に少なくとも一部基づいて生成され、

前記デバイスはさらに、前記第2のプロトコル特有鍵を用いて、前記第2のネットワーク通信プロトコルによって、第3のデバイスと通信するように構成された第2の通信インタフェースを備え、

前記第1のプロトコル特有鍵は前記第2のプロトコル特有鍵と異なる、請求項13に記載のデバイス。

【請求項17】

前記メモリはさらに、複数のネットワーク通信プロトコルに対応する複数のプロトコル特有鍵を格納するように構成され、

前記複数のプロトコル特有鍵は、少なくとも、前記第1のプロトコル特有鍵および前記第2のプロトコル特有鍵を含む、請求項16に記載のデバイス。

【請求項18】

前記メモリはさらに、複数のネットワーク通信プロトコルに対応する識別子を格納するように構成され、

前記複数のネットワーク通信プロトコルは、少なくとも、前記第1のネットワーク通信プロトコルおよび前記第2のネットワーク通信プロトコルを含む、請求項13に記載のデバイス。

【請求項19】

前記混合通信ネットワークに関連付けられたネットワーク鍵を受信するように構成されたユーザ・インタフェース構成要素、をさらに備える請求項13に記載のデバイス。

【請求項 20】

前記混合通信ネットワークに関連付けられたネットワーク鍵を検出するように構成されたセンサ、をさらに備える請求項 13 に記載のデバイス。

【請求項 21】

前記第 1 の通信インタフェースとは異なる、第 2 の通信インタフェースをさらに備え、前記第 2 の通信インタフェースは、前記混合通信ネットワークに関連付けられたネットワーク鍵を受信するように構成された、請求項 13 に記載のデバイス。

【請求項 22】

前記デバイスは、前記混合通信ネットワークのアクセス・ポイントである、請求項 13 に記載のデバイス。

【請求項 23】

プログラム命令群を格納する非一時的なコンピュータ読取可能な記憶媒体であって、前記プログラム命令群は、第 1 のデバイスのプロセッサによって実行された場合、前記第 1 のデバイスに対して、

混合通信ネットワークに関連付けられたネットワーク鍵を受信することと、ここで、前記混合通信ネットワークは、第 1 のネットワーク通信プロトコルおよび第 2 のネットワーク通信プロトコルに関連付けられている、

前記混合通信ネットワークの第 1 のネットワーク通信プロトコルと用いられるための第 1 のプロトコル特有鍵を、前記第 1 のデバイスにおいて生成することと、ここで、前記第 1 のプロトコル特有鍵は、前記第 1 のネットワーク通信プロトコルに対応する第 1 の識別子および前記ネットワーク鍵に少なくとも一部基づく、

前記第 1 のプロトコル特有鍵を用いて、前記第 1 のネットワーク通信プロトコルで、前記混合通信ネットワークにおける第 2 のデバイスと通信することと
を実行させる、非一時的なコンピュータ読取可能な記憶媒体。

【請求項 24】

前記プログラム命令群は、前記第 1 のデバイスのプロセッサによって実行された場合、前記第 1 のデバイスに対してさらに、前記第 1 のプロトコル特有鍵が第 1 のハッシュ演算の結果の最下位 n ビットを備えるように、前記第 1 の識別子および前記ネットワーク鍵を含む前記第 1 のハッシュ演算の結果を切り詰めることを実行させる、請求項 23 に記載の非一時的なコンピュータ読取可能な記憶媒体。

【請求項 25】

前記プログラム命令群は、前記第 1 のデバイスのプロセッサによって実行された場合、前記第 1 のデバイスに対してさらに、

前記混合通信ネットワークの第 2 のネットワーク通信プロトコルに関連付けられた第 2 のプロトコル特有鍵を生成することと、ここで、前記第 2 のプロトコル特有鍵は、前記第 2 のネットワーク通信プロトコルに対応する第 2 の識別子および前記ネットワーク鍵に少なくとも一部基づく、

前記第 2 のプロトコル特有鍵を用いて、前記第 2 のネットワーク通信プロトコルによって、第 3 のデバイスと通信することと、ここで、前記第 1 のプロトコル特有鍵は前記第 2 のプロトコル特有鍵と異なる、
を実行させる、請求項 23 に記載の非一時的なコンピュータ読取可能な記憶媒体。

【請求項 26】

前記プログラム命令群は、前記第 1 のデバイスのプロセッサによって実行された場合、前記第 1 のデバイスに対してさらに、複数のネットワーク通信プロトコルに対応する複数のプロトコル特有鍵を格納することを実行させ、

前記複数のプロトコル特有鍵は、少なくとも、前記第 1 のプロトコル特有鍵および前記第 2 のプロトコル特有鍵を含む、請求項 25 に記載の非一時的なコンピュータ読取可能な記憶媒体。

【請求項 27】

前記プログラム命令群は、前記第 1 のデバイスのプロセッサによって実行された場合、

前記第 1 のデバイスに対してさらに、

前記混合通信ネットワークにおいて用いられる複数のネットワーク通信プロトコルに対応する識別子を格納することを実行させ、

前記複数のネットワーク通信プロトコルは、少なくとも、前記第 1 のネットワーク通信プロトコルおよび前記第 2 のネットワーク通信プロトコルを含む、請求項 2 3 に記載の非一時的なコンピュータ読取可能な記憶媒体。