【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7日(2005.7.7)

【公開番号】特開2002-232418(P2002-232418A)
【公開日】平成14年8月16日(2002.8.16)
【出願番号】特願2001-376564(P2001-376564)
【国際特許分類第７版】
　Ｈ０４Ｌ　9/16
　Ｈ０４Ｑ　7/38
【ＦＩ】
　Ｈ０４Ｌ　9/00　６４３
　Ｈ０４Ｂ　7/26　１０９Ｓ

【手続補正書】
【提出日】平成16年10月26日(2004.10.26)
【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の通信システムのための第１の鍵値（ＫＥＹ１）を第２の通信システムのための第２の鍵値（ＫＥＹ２）に変換する方法であって、
　第１のランダム関数（ｆ）を用いて前記第１の鍵値（ＫＥＹ１）の少なくとも一部から第１の中間値（Ｒ）を生成するステップと、
　第２の値を生成するために、前記第１の中間値（Ｒ）の少なくとも一部を第２のランダム関数（ｈ）に与えるステップと、
　第２の中間値（Ｔ）を生成するために、前記第１の鍵値（ＫＥＹ１）の少なくとも一部と、前記第２の値の少なくとも一部とについての排他的論理和を実行するステップと、
　第３の値を生成するために、前記第２の中間値（Ｔ）の少なくとも一部を第３のランダム関数（ｇ）に与えるステップと、
　前記第３の値の少なくとも一部と、前記第１の中間値（Ｒ）の少なくとも一部とについての排他的論理和を実行することにより、前記第２の鍵値（ＫＥＹ２）の少なくとも第１の部分を生成するステップとを含むことを特徴とする方法。
【請求項２】
　前記第２の鍵値（ＫＥＹ２）の少なくとも第２の部分として、前記第２の中間値（Ｔ）の少なくとも一部を生成することを特徴とする請求項１に記載の方法。
【請求項３】
　前記第１の中間値（Ｒ）を生成する前記ステップは、
　ｎ－ｍビットの前記第１の中間値（Ｒ）を生成するために、ｍビットの前記第１の鍵値（ＫＥＹ１）を第１のランダム関数（ｆ）に与えるステップを含むことを特徴とする請求項１に記載の方法。
【請求項４】
　前記第１の中間値（Ｒ）の少なくとも一部を第２のランダム関数（ｈ）に与える前記ステップと、前記第１の鍵値（ＫＥＹ１）の少なくとも一部と前記第２の値の少なくとも一部とについての排他的論理和を実行する前記ステップとは、
　ｍビットの第２の値を生成するために、前記ｎ－ｍビットの第１の中間値（Ｒ）を第２のランダム関数（ｈ）に与えるステップと、

ｍビットを有する前記第２の中間値（Ｔ）を生成するために、前記ｍビットの第１の鍵値（ＫＥＹ１）と前記ｍビットの第２の値とについての排他的論理和を実行するステップとを含むことを特徴とする請求項３に記載の方法。

【請求項５】

前記第２の中間値（Ｔ）の少なくとも一部を第３のランダム関数（ｇ）に与える前記ステップと、前記第２の鍵値（ＫＥＹ２）の少なくとも第１の部分を生成する前記ステップとは、

ｎ－ｍビットの第３の値を生成するために、前記ｍビットの第２の中間値（Ｔ）を第３のランダム関数（ｇ）に与えるステップと、

前記第２の鍵値（ＫＥＹ２）のｎ－ｍビットの部分（Ｖ）を生成するために、前記ｎ－ｍビットの第３の値と、前記ｎ－ｍビットの第１の中間値（Ｒ）とについての排他的論理和を実行するステップとを含むことを特徴とする請求項４に記載の方法。

【請求項６】

ｎビットを有する前記第２の鍵値（ＫＥＹ２）のｍビットの第２の部分として、前記ｍビットの第２の中間値（Ｔ）を与えるステップを含むことを特徴とする請求項５に記載の方法。

【請求項７】

前記第３の値を生成するために、前記第２の鍵値（ＫＥＹ２）の前記第２の部分（Ｔ）を、前記第３のランダム関数（ｇ）に与えるステップと、

前記第２の鍵値（ＫＥＹ２）の前記第１の部分（Ｖ）と、前記第３の値との排他的論理和をとることにより、前記第１の中間値（Ｒ）を生成するステップとを含むことを特徴とする請求項２に記載の方法。

【請求項８】

前記第１の中間値（Ｒ）から前記第２の値を生成するために、前記第２のランダム関数（ｈ）を用いるステップと、

前記第２の値と、前記第２の鍵値（ＫＥＹ２）の前記第２の部分（Ｔ）との排他的論理和をとることにより、前記第１の鍵値の少なくとも一部を生成するステップとをさらに含むことを特徴とする請求項７に記載の方法。

【請求項９】

第１の通信システムのための第１の鍵値（ＫＥＹ１）を第２の通信システムのための第２の鍵値（ＫＥＹ２）に変換するための鍵変換システムであって、

第１のランダム関数（ｆ）を用いて、前記第１の鍵値（ＫＥＹ１）の少なくとも一部から第１の中間値（Ｒ）を生成するように構成され、前記第１の中間値（Ｒ）の少なくとも一部を第２のランダム関数（ｈ）に与えて第２の値を生成するように構成され、前記第１の鍵値（ＫＥＹ１）の少なくとも一部と前記第２の値の少なくとも一部とについての排他的論理和を実行して第２の中間値（Ｔ）を生成するように構成され、前記第２の中間値（Ｔ）の少なくとも一部を第３のランダム関数（ｇ）に与えて第３の値を生成するように構成され、さらに、前記第３の値の少なくとも一部と前記第１の中間値（Ｒ）の少なくとも一部との排他的論理和をとることにより前記第２の鍵値（ＫＥＹ２）の少なくとも第１の部分を生成するように構成される処理回路を含むことを特徴とする鍵変換システム。

【請求項１０】

前記処理回路はさらに、前記第２の鍵値（ＫＥＹ２）の少なくとも第２の部分として、前記第２の中間値（Ｔ）の少なくとも一部を生成するように構成されることを特徴とする請求項９に記載のシステム。