【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】令和2年1月30日(2020.1.30)

【公表番号】特表2019-507971(P2019-507971A)
【公表日】平成31年3月22日(2019.3.22)
【年通号数】公開・登録公報2019-011
【出願番号】特願2018-531057(P2018-531057)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/31　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
Ｇ０６Ｆ　13/00　(2006.01)
Ｈ０４Ｗ　4/70　(2018.01)
Ｈ０４Ｗ　12/04　(2009.01)
Ｈ０４Ｗ　76/19　(2018.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０６Ｆ　21/31
Ｇ０６Ｆ　21/62
Ｇ０６Ｆ　13/00　３５１Ｚ
Ｈ０４Ｗ　4/70
Ｈ０４Ｗ　12/04
Ｈ０４Ｗ　76/19

【手続補正書】
【提出日】令和1年12月16日(2019.12.16)
【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】
モノのインターネット（ＩｏＴ）デバイスとクライアントデバイスとの間に二次の通信チャネルを確立する方法であって、
一次の鍵のセットを使用して前記ＩｏＴデバイスとＩｏＴサービスとの間に一次の安全な通信チャネルを前記ＩｏＴデバイスによって確立することと、
前記一次の安全な通信チャネルを使用して二次の鍵交換を前記ＩｏＴデバイス実行することであって、前記クライアントデバイス及び前記ＩｏＴデバイスは、それぞれ前記二次の鍵交換の後に二次の鍵のセットを提供される、ことと、
前記クライアントデバイスのアプリケーション（アプリ）からパスコードを前記ＩｏＴデバイスによって受信することであって、前記クライアントデバイスのユーザが前記パスコードを選び、前記パスコードは、前記一次の安全な通信チャネルを介して前記ＩｏＴデバイスに送信される、ことと
前記ＩｏＴデバイスによって、前記ＩｏＴデバイスに前記パスコードを記憶することと、　前記一次の安全な通信チャネルが動作不能であることを検出することと、
それに応じて、前記ＩｏＴデバイス及び／または前記クライアントデバイスによって、前記二次の鍵のセットを使用して、前記クライアントデバイスと前記ＩｏＴデバイスとの間に二次の安全な無線接続を確立することと、

前記ＩｏＴデバイスによって、前記ユーザに前記パスコードを前記クライアントデバイスから入力することを要求することと、
前記ユーザが正しいパスコードを前記クライアントデバイスから入力したときだけ、前記クライアントデバイスに、前記二次の安全な無線接続を介して前記ＩｏＴデバイスによって利用可能にされたデータ及び／又は機能へのアクセスを前記ＩｏＴデバイスによって提供することと、
を含む、方法。
【請求項２】
前記二次の安全な無線接続を介する前記データ及び／又は機能へのアクセスは、前記一次の安全な通信チャネルを介して接続されるときよりも前記データ及び／又は機能へのより限定されたアクセスを含む、請求項１に記載の方法。
【請求項３】
前記二次の安全な無線接続を確立すると、前記ユーザに前記パスコードを入力することを促すために、前記クライアントデバイスの前記アプリを実行することを更に含み、前記パスコードは、前記ＩｏＴデバイスが前記データ及び／又は機能へのアクセスを提供する前に、前記アプリから前記ＩｏＴデバイスに送信される、請求項１に記載の方法。
【請求項４】
前記ＩｏＴデバイスは、無線ドアロックを備え、前記二次の安全な通信チャネルを介してアクセスされるべき少なくとも１つの機能が、前記無線ドアロックをロック解除することを含む、請求項３に記載の方法。
【請求項５】
一次の鍵のセットを使用して、前記ＩｏＴデバイスとＩｏＴサービスとの間に一次の安全な通信チャネルを確立することが、
ＩｏＴハブ又は前記クライアントデバイスを通して前記ＩｏＴサービスと前記ＩｏＴデバイスとの間に通信を確立することと、
サービス公開鍵及びサービス秘密鍵を前記ＩｏＴサービス上の第１の暗号化エンジンの鍵生成ロジックによって生成することと、
デバイス公開鍵及びデバイス秘密鍵を前記ＩｏＴデバイス上の第２の暗号化エンジンの鍵生成ロジックによって生成することと、
前記サービス公開鍵を前記第１の暗号化エンジンから前記第２の暗号化エンジンに送信し、前記デバイス公開鍵を前記第２の暗号化エンジンから前記第１の暗号化エンジンに送信することと、
前記デバイス公開鍵及び前記サービス秘密鍵を使用して秘密を生成することと、
前記サービス公開鍵及び前記デバイス秘密鍵を使用して同一の前記秘密を生成することと、
前記秘密を使用して又は前記秘密から派生したデータ構造を使用して、前記第１の暗号化エンジンと前記第２の暗号化エンジンとの間で送信されるデータパケットを暗号化及び復号することと、
を含む、請求項１に記載の方法。
【請求項６】
前記鍵生成ロジックは、ハードウェアセキュリティモジュール（ＨＳＭ）を備える、請求項５に記載の方法。
【請求項７】
前記秘密から派生した前記データ構造は、前記第１の暗号化エンジンによって生成された第１の鍵ストリームと、前記第２の暗号化エンジンによって生成された第２の鍵ストリームと、を備える、請求項６に記載の方法。
【請求項８】
第１のカウンタは、前記第１の暗号化エンジンと関連し、第２のカウンタは、前記第２の暗号化エンジンと関連し、前記第１の暗号化エンジンは、前記第２の暗号化エンジンに送信される各データパケットに応じる前記第１のカウンタを増加させ、前記第２の暗号化

エンジンは、前記第１の暗号化エンジンに送信される各データパケットに応じる前記第２のカウンタを増加させる、請求項７に記載の方法。
【請求項９】
前記第１の暗号化エンジンは、前記第１のカウンタの現在のカウンタ値及び前記秘密を使用して前記第１の鍵ストリームを生成し、前記第２の暗号化エンジンは、前記第２のカウンタの現在のカウンタ値及び前記秘密を使用して前記第２の鍵ストリームを生成する、請求項８に記載の方法。
【請求項１０】
前記第１の暗号化エンジンは、前記第１のカウンタ値及び前記秘密を使用して前記第１の鍵ストリームを生成するための楕円曲線方法（ＥＣＭ）モジュールを備え、前記第２の暗号化エンジンは、前記第１のカウンタ値及び前記秘密を使用して前記第２の鍵ストリームを生成するためのＥＣＭモジュールを備える、請求項９に記載の方法。
【請求項１１】
前記第１の暗号化エンジンは、前記第１の鍵ストリームを使用して第１のデータパケットを暗号化することにより、第１の暗号化されたデータパケットを生成し、
前記第１の暗号化されたデータパケットを前記第１のカウンタの現在のカウンタ値と共に前記第２の暗号化エンジンに送信する、請求項９に記載の方法。
【請求項１２】
前記第２の暗号化エンジンは、前記第１のカウンタの現在のカウンタ値及び前記秘密を使用して前記第１の鍵ストリームを生成し、前記第１の鍵ストリームを使用して前記第１の暗号化されたデータパケットを復号する、請求項１１に記載の方法。
【請求項１３】
モノのインターネット（ＩｏＴ）ロジックデバイスとクライアントデバイスとの間に二次の通信チャネルを確立するシステムであって、
前記ＩｏＴロジックデバイス、前記クライアントデバイス及び認証回路を備え、
前記ＩｏＴロジックデバイスは、一次の鍵のセットを使用してＩｏＴサービスとの一次の安全な通信チャネルを確立し、
前記ＩｏＴロジックデバイスは、前記一次の安全な通信チャネルを使用して二次の鍵交換を実行し、
前記クライアントデバイス及び前記ＩｏＴロジックデバイスは、前記二次の鍵交換の後に、それぞれ二次の鍵のセットを提供され、
前記認証回路は、前記ＩｏＴロジックデバイスにパスコードを記憶し、前記認証回路が前記ＩｏＴロジックデバイスに前記パスコードを記憶する前に前記クライアントデバイスのアプリケーション（アプリ）から前記パスコードは最初に受信され、前記クライアントデバイスのユーザは前記パスコードを選択し、前記パスコードは前記一次の安全な通信チャネルを介して前記ＩｏＴロジックデバイスへ送信され、
前記認証回路は前記ＩｏＴロジックデバイスに前記パスコードを記憶し、
前記ＩｏＴロジックデバイス及び／又は前記クライアントデバイスは、前記一次の安全な通信チャネルが動作不能であることを検出し、
前記ＩｏＴロジックデバイス及び／又は前記クライアントデバイスは、それに応じて、前記二次の鍵のセットを使用して前記クライアントデバイスと前記ＩｏＴロジックデバイスとの間に二次の安全な無線接続を確立し、
前記認証回路は前記クライアントデバイスから前記パスコードを入力するように前記ユーザを促すためのものであり、
前記ＩｏＴロジックデバイスは、前記ユーザが前記クライアントデバイスから正しいパスコードを入力したときだけ、前記クライアントデバイスに、前記二次の安全な無線接続を介して前記ＩｏＴロジックデバイスによって利用可能にされたデータ及び／又は機能へのアクセスを提供される、システム。
【請求項１４】
前記二次の安全な無線接続を介するデータ及び／又は機能への前記アクセスは、前記一

次の安全な通信チャネルを介して接続されるときよりも、前記データ及び／又は機能へのより限定されたアクセスを含む、請求項１３に記載のシステム。
【請求項１５】
前記クライアントデバイスで実行される前記アプリが、前記二次の安全な無線接続を確立すると、前記ユーザに前記パスコードを入力することを促すことを更に備え、前記パスコードは、前記ＩｏＴロジックデバイスが前記データ及び／又は機能へのアクセスを提供する前に、前記アプリから前記ＩｏＴロジックデバイスに送信される、請求項１３に記載のシステム。
【請求項１６】
前記ＩｏＴロジックデバイスは、無線ドアロックを備え、前記二次の安全な通信チャネルを介してアクセスされるべき少なくとも１つの機能が、前記無線ドアロックをロック固定又はロック解除することを含む、請求項１５に記載のシステム。
【請求項１７】
一次の鍵のセットを使用して、前記ＩｏＴロジックデバイスと前記ＩｏＴサービスとの間に一次の安全な通信チャネルを確立することが、
前記ＩｏＴロジックデバイスが、ＩｏＴハブ又は前記クライアントデバイスを通して前記ＩｏＴサービスとの通信を確立することと、
サービス公開鍵及びサービス秘密鍵を生成するための鍵生成ロジックを備える、ＩｏＴサービス上の第１の暗号化エンジンと、
デバイス公開鍵及びデバイス秘密鍵を生成するための鍵生成ロジックを備える、ＩｏＴロジックデバイス上の第２の暗号化エンジンと、を備え、
第１の暗号化エンジンは、第２の暗号化エンジンにサービス公開鍵を送信するためのものであって、第２の暗号化エンジンは、第１の暗号化エンジンにデバイス公開鍵を送信するためのものであり、
第１の暗号化エンジンは、デバイス公開鍵及びサービス秘密鍵を使用して秘密を生成するためのものであり、
前記第２の暗号化エンジンは、前記サービス公開鍵及び前記デバイス秘密鍵を使用して同一の前記秘密を生成するためのものであり、
いったん前記秘密が生成されると、前記第１の暗号化エンジン及び前記第２の暗号化エンジンは、前記秘密を使用して又は前記秘密から派生したデータ構造を使用して、前記第１の暗号化エンジンと前記第２の暗号化エンジンとの間で送信されるデータパケットを暗号化及び復号する、請求項１３に記載のシステム。
【請求項１８】
前記鍵生成ロジックは、ハードウェアセキュリティモジュール（ＨＳＭ）を備える、請求項１７に記載のシステム。
【請求項１９】
前記秘密から派生したデータ構造は、前記第１の暗号化エンジンによって生成された第１の鍵ストリームと、前記第２の暗号化エンジンによって生成された第２の鍵ストリームと、を備える、請求項１８に記載のシステム。
【請求項２０】
前記第１の暗号化エンジンと関連する第１のカウンタと、前記第２の暗号化エンジンと関連する第２のカウンタと、を更に備え、前記第１の暗号化エンジンは、前記第２の暗号化エンジンに送信される各データパケットに応じる前記第１のカウンタを増加させ、前記第２の暗号化エンジンは、前記第１の暗号化エンジンに送信される各データパケットに応じる前記第２のカウンタを増加させる、請求項１９に記載のシステム。