【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1年5月23日(2019.5.23)

【公表番号】特表2018-518090(P2018-518090A)
【公表日】平成30年7月5日(2018.7.5)
【年通号数】公開・登録公報2018-025
【出願番号】特願2017-554889(P2017-554889)
【国際特許分類】
Ｈ０４Ｌ　9/12　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/60　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６３１
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｇ０６Ｆ　21/60　３２０

【手続補正書】
【提出日】平成31年4月12日(2019.4.12)
【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】
鍵生成デバイスと、前記鍵生成デバイスと接続された量子鍵配送デバイスとを含む少なくとも１つの鍵インジェクションサブシステムと、
暗号化マシンと、前記暗号化マシンと接続された量子鍵配送デバイスとを含むクラウドベースの暗号化マシンホスティングサブシステムと
を含む、クラウドベースの鍵インジェクションシステムであって、
前記暗号化マシンは、仮想暗号化デバイスを含み、
前記鍵インジェクションサブシステム及び前記暗号化マシンホスティングサブシステムは、それらのそれぞれの量子鍵配送デバイスを通して互いに接続され、
前記鍵生成デバイスは、ルート鍵コンポーネントを生成し、前記量子鍵配送デバイスを介して前記暗号化マシンに前記ルート鍵コンポーネントを送信するように構成され、及び
前記暗号化マシンは、１つ又は複数の鍵生成デバイスからルート鍵コンポーネントを受信し、前記受信されたルート鍵コンポーネントに従って前記仮想暗号化デバイスのルート鍵を生成するように構成される、クラウドベースの鍵インジェクションシステム。
【請求項２】
前記量子鍵配送デバイスは、前記鍵生成デバイスと前記暗号化マシンとの間の共有鍵ペアを取り決めるように構成され、及び
前記少なくとも１つの鍵インジェクションサブシステムの前記量子鍵配送デバイスは、取り決められた共有鍵を用いて、前記暗号化マシンに対する前記ルート鍵コンポーネントの暗号化送信を行うように構成される、請求項１に記載のクラウドベースの鍵インジェクションシステム。
【請求項３】
前記少なくとも１つの鍵インジェクションサブシステムは、１つの鍵インジェクションサブシステムを含み、及び
前記鍵インジェクションサブシステムの前記鍵生成デバイスは、前記仮想暗号化デバイ

スの幾つかのルート鍵コンポーネントを生成し、前記量子鍵配送デバイスを介して前記暗号化マシンに前記ルート鍵コンポーネントを送信するように構成される、請求項１に記載のクラウドベースの鍵インジェクションシステム。
【請求項４】
前記暗号化マシンは、前記仮想暗号化デバイスの１つのルート鍵コンポーネントを生成し、前記少なくとも１つの鍵インジェクションサブシステムと、前記暗号化マシンからの前記受信されたルート鍵コンポーネントとに従って前記仮想暗号化デバイスの前記ルート鍵を生成するようにさらに構成される、請求項１に記載のクラウドベースの鍵インジェクションシステム。
【請求項５】
前記少なくとも１つの鍵インジェクションサブシステムは、クラウドベースの管理サブシステムと、クライアント端末に位置するユーザサブシステムとを含み、
前記管理サブシステムは、量子鍵配送デバイスと、前記鍵生成デバイスを含む管理デバイスとを含み、及び
前記ユーザサブシステムは、量子鍵配送デバイスと、前記鍵生成デバイスを含む端末デバイスとを含む、請求項４に記載のクラウドベースの鍵インジェクションシステム。
【請求項６】
前記ユーザサブシステムの前記端末デバイスは、ユーザマスター鍵を生成し、前記ユーザマスター鍵を前記暗号化マシンに送るようにさらに構成される、請求項５に記載のクラウドベースの鍵インジェクションシステム。
【請求項７】
前記ユーザサブシステムの前記端末デバイスは、ユーザワーク鍵を生成し、前記ユーザワーク鍵を前記暗号化マシンに送るようにさらに構成される、請求項６に記載のクラウドベースの鍵インジェクションシステム。
【請求項８】
前記量子鍵配送デバイスは、データ暗号化及び復号機能を有する量子暗号化マシンを含む、請求項１に記載のクラウドベースの鍵インジェクションシステム。
【請求項９】
前記暗号化マシンは、閾値秘密共有メカニズムに基づく秘密復元アルゴリズムを用いることにより、前記受信されたルート鍵コンポーネントに従って前記仮想暗号化デバイスのルート鍵を生成するように構成される、請求項１に記載のクラウドベースの鍵インジェクションシステム。
【請求項１０】
暗号化マシンのための鍵インジェクション方法であって、
前記暗号化マシンにより、少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することと、
前記暗号化マシンにより、前記少なくとも１つの鍵インジェクションサブシステムからの前記受信されたルート鍵コンポーネントに従ってルート鍵を生成することと
を含む、鍵インジェクション方法。
【請求項１１】
前記暗号化マシンは、仮想暗号化デバイスを含み、
前記ルート鍵は、前記仮想暗号化デバイスのためのものである、請求項１０に記載の鍵インジェクション方法。
【請求項１２】
各ルート鍵コンポーネントは、前記少なくとも１つの鍵インジェクションサブシステムの鍵生成デバイスによって生成される、請求項１０に記載の鍵インジェクション方法。
【請求項１３】
前記暗号化マシンにより、ルート鍵コンポーネントを生成することをさらに含み、前記暗号化マシンにより、前記少なくとも１つの鍵インジェクションサブシステムからの前記受信されたルート鍵コンポーネントに従って前記ルート鍵を生成することは、

前記暗号化マシンにより、前記少なくとも１つの鍵インジェクションサブシステムからの前記受信されたルート鍵コンポーネントと、前記暗号化マシンによって生成された前記ルート鍵コンポーネントとに従って前記ルート鍵を生成することを含む、請求項１０に記載の鍵インジェクション方法。
【請求項１４】
前記暗号化マシンにより、前記少なくとも１つの鍵インジェクションサブシステムの各々と共有鍵ペアを取り決めることをさらに含み、前記少なくとも１つの鍵インジェクションサブシステムからの前記ルート鍵コンポーネントは、前記共有鍵ペアの鍵を用いて暗号化される、請求項１０に記載の鍵インジェクション方法。
【請求項１５】
前記暗号化マシンは、量子鍵配送デバイスに接続され、
前記少なくとも１つの鍵インジェクションサブシステムの各々は、量子鍵配送デバイスを含み、
前記暗号化マシンにより、前記少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することは、前記暗号化マシンにより、前記量子鍵配送デバイスを介して前記少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することを含む、請求項１０に記載の鍵インジェクション方法。
【請求項１６】
前記少なくとも１つの鍵インジェクションサブシステムは、クラウドベースの管理サブシステムと、クライアント端末に位置するユーザサブシステムとを含み、前記クラウドベースの管理サブシステムは、鍵生成デバイスを含み、前記ユーザサブシステムは、鍵生成デバイスを含む、請求項１０に記載の鍵インジェクション方法。
【請求項１７】
前記ユーザサブシステムによって生成されたユーザマスター鍵を前記ユーザサブシステムから受信することをさらに含む、請求項１６に記載の鍵インジェクション方法。
【請求項１８】
前記ユーザサブシステムによって生成されたユーザワーク鍵を前記ユーザサブシステムから受信することをさらに含む、請求項１６に記載の鍵インジェクション方法。
【請求項１９】
前記少なくとも１つの鍵インジェクションサブシステムのアイデンティティを検証することをさらに含む、請求項１０に記載の鍵インジェクション方法。
【請求項２０】
前記暗号化マシンにより、前記少なくとも１つの鍵インジェクションサブシステムからの前記受信されたルート鍵コンポーネントに従って前記ルート鍵を生成することは、前記暗号化マシンにより、閾値秘密共有メカニズムに基づく秘密復元アルゴリズムを用いることにより、前記少なくとも１つの鍵インジェクションサブシステムからの前記受信されたルート鍵コンポーネントに従って前記ルート鍵を生成することを含む、請求項１０に記載の鍵インジェクション方法。
【請求項２１】
暗号化マシンのための鍵インジェクション装置であって、
少なくとも１つの鍵インジェクションサブシステムと共有鍵ペアを取り決めるように構成された共有鍵ペア取り決めユニットと、
前記暗号化マシン上の仮想暗号化デバイスのルート鍵コンポーネントを生成するように構成されたルート鍵コンポーネント生成ユニットと、
前記ルート鍵コンポーネント生成ユニットによって生成された前記ルート鍵コンポーネントと、前記少なくとも１つの鍵インジェクションサブシステムから受信されたルート鍵コンポーネントとに従ってルート鍵を生成するルート鍵生成ユニットと
を含む、鍵インジェクション装置。
【請求項２２】
前記少なくとも１つの鍵インジェクションサブシステムから受信された前記ルート鍵コ

ンポーネントは、前記少なくとも１つの鍵インジェクションサブシステムと、前記暗号化マシンとにそれぞれ接続された量子鍵配送デバイスを通して受信される、請求項２１に記載の鍵インジェクション装置。
【請求項２３】
前記少なくとも１つの鍵インジェクションサブシステムから受信された前記ルート鍵コンポーネントは、前記共有鍵ペアの鍵を用いて暗号化される、請求項２１に記載の鍵インジェクション装置。
【請求項２４】
前記少なくとも１つの鍵インジェクションサブシステムは、鍵生成デバイスを含むクラウドベースの管理サブシステムと、クライアント端末に位置する鍵生成デバイスを含むユーザサブシステムとを含む、請求項２１に記載の鍵インジェクション装置。
【請求項２５】
閾値秘密共有メカニズムに基づく秘密復元アルゴリズムを用いることにより、前記ルート鍵を生成することをさらに含む、請求項２１に記載の鍵インジェクション装置。
【請求項２６】
命令の組を格納する非一時的なコンピュータ可読媒体であって、前記命令の組は、暗号化マシンに鍵インジェクション方法を行わせるように、前記暗号化マシンの少なくとも１つのプロセッサによって実行可能であり、前記鍵インジェクション方法は、
少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することと、
前記少なくとも１つの鍵インジェクションサブシステムからの前記受信したルート鍵コンポーネントに従ってルート鍵を生成することと、
を含み、
前記暗号化マシンは、量子鍵配送デバイスに接続され、
前記少なくとも１つの鍵インジェクションサブシステムの各々は、量子鍵配送デバイスを含み、
前記少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することは、前記量子鍵配送デバイスを介して前記少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することを含む、非一時的なコンピュータ可読媒体。
【請求項２７】
前記暗号化マシンは、仮想暗号化デバイスを含み、
前記ルート鍵は、前記仮想暗号化デバイスのためのものである、請求項２６に記載のコンピュータ可読媒体。
【請求項２８】
各ルート鍵コンポーネントは、前記少なくとも１つの鍵インジェクションサブシステムの鍵生成デバイスによって生成される、請求項２６に記載のコンピュータ可読媒体。
【請求項２９】
前記鍵インジェクション方法は、前記暗号化マシンにより、ルート鍵コンポーネントを生成することをさらに含み、前記少なくとも１つの鍵インジェクションサブシステムからの前記受信したルート鍵コンポーネントに従って前記ルート鍵を生成することは、
前記少なくとも１つの鍵インジェクションサブシステムからの前記受信したルート鍵コンポーネントと、前記暗号化マシンによって生成された前記ルート鍵コンポーネントとに従って前記ルート鍵を生成することを含む、請求項２６に記載のコンピュータ可読媒体。
【請求項３０】
前記鍵インジェクション方法は、前記少なくとも１つの鍵インジェクションサブシステムの各々と共有鍵ペアを取り決めることをさらに含み、
前記少なくとも１つの鍵インジェクションサブシステムからの前記ルート鍵コンポーネントは、前記共有鍵ペアの鍵を用いて暗号化される、請求項２６に記載のコンピュータ可読媒体。

【請求項３１】
前記暗号化マシンは、量子鍵配送デバイスに接続され、
前記少なくとも１つの鍵インジェクションサブシステムの各々は、量子鍵配送デバイスを含み、
前記少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することは、前記量子鍵配送デバイスを介して前記少なくとも１つの鍵インジェクションサブシステムからルート鍵コンポーネントを受信することを含む、請求項２６に記載のコンピュータ可読媒体。
【請求項３２】
前記少なくとも１つの鍵インジェクションサブシステムは、クラウドベースの管理サブシステムと、クライアント端末に位置するユーザサブシステムとを含み、前記クラウドベースの管理サブシステムは、鍵生成デバイスを含み、前記ユーザサブシステムは、鍵生成デバイスを含む、請求項２６に記載のコンピュータ可読媒体。
【請求項３３】
前記鍵インジェクション方法は、前記ユーザサブシステムによって生成されたユーザマスター鍵を前記ユーザサブシステムから受信することをさらに含む、請求項３２に記載のコンピュータ可読媒体。
【請求項３４】
前記鍵インジェクション方法は、前記ユーザサブシステムによって生成されたユーザワーク鍵を前記ユーザサブシステムから受信することをさらに含む、請求項３２に記載のコンピュータ可読媒体。
【請求項３５】
前記鍵インジェクション方法は、前記少なくとも１つの鍵インジェクションサブシステムのアイデンティティを検証することをさらに含む、請求項２６に記載のコンピュータ可読媒体。
【請求項３６】
前記少なくとも１つの鍵インジェクションサブシステムからの前記受信したルート鍵コンポーネントに従って前記ルート鍵を生成することは、閾値秘密共有メカニズムに基づく秘密復元アルゴリズムを用いることにより、前記少なくとも１つの鍵インジェクションサブシステムからの前記受信したルート鍵コンポーネントに従って前記ルート鍵を生成することを含む、請求項２６に記載のコンピュータ可読媒体。