【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31年3月7日(2019.3.7)

【公表番号】特表2018-509117(P2018-509117A)
【公表日】平成30年3月29日(2018.3.29)
【年通号数】公開・登録公報2018-012
【出願番号】特願2017-560880(P2017-560880)
【国際特許分類】
Ｈ０４Ｌ　9/12　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６３１
Ｈ０４Ｌ　9/00　６７５Ａ

【手続補正書】
【提出日】平成31年1月24日(2019.1.24)
【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】
量子鍵配送プロセスのためのアイデンティティ認証方法であって、受信機により実施される前記方法は、
送信機から、アイデンティティ認証ビットストリングの量子状態及びランダム生成鍵ビットストリングの量子状態を含む量子状態情報を、異なる波長を使用することによって受信することであって、前記アイデンティティ認証ビットストリングが前記鍵ビットストリングにおいてランダムな位置で及びランダムな長さでインタリーブされる、送信することと、
前記異なる波長及び予め設定された基底ベクトル選択規則に従って選択された測定基底に従って前記量子状態情報における受信された量子状態を測定して、前記アイデンティティ認証ビットストリングの前記測定からアイデンティティ認証情報を取得することと、
前記測定を通して取得された前記アイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応するかどうかを決定することと、
前記測定を通して取得された前記アイデンティティ認証情報が前記予め設定された基底ベクトル選択規則に対応するとの決定に応じて、
前記アイデンティティ認証情報から受信機認証鍵を選択することと、
前記測定を通して取得された前記アイデンティティ認証情報における前記受信機認証鍵の位置情報、及び前記受信機認証鍵で暗号化された予め設定された共有鍵を前記送信機へ送信することであって、前記位置情報及び前記アイデンティティ認証ビットストリングは、前記送信機により、対応する送信機認証鍵を選択するために使用され、前記受信機認証鍵は、予め設定された新しい共有鍵を取得するために送信機認証鍵で復号される、送信することと、
前記受信機認証鍵を前記送信機認証鍵で復号すること取得された前記予め設定された新しい共有鍵が前記予め設定されたローカル共有鍵と一致しない場合に、前記量子鍵配送プロセスを終了することと
を含む、アイデンティティ認証方法。
【請求項２】

標準チャネルを介して、鍵量子状態を測定するための前記測定基底を公開することを更に含む、請求項１に記載のアイデンティティ認証方法。
【請求項３】
前記送信機が前記アイデンティティ認証ビットストリング及び前記ランダム生成鍵ビットストリングの前記量子状態情報を送信する前に、標準チャネルを介して、予め設定されたアカウント情報を使用することによってアイデンティティ検証を行うことを更に含む、請求項１に記載のアイデンティティ認証方法。
【請求項４】
前記予め設定されたアカウント情報が識別情報及び証明書を含む、請求項３に記載のアイデンティティ認証方法。
【請求項５】
前記予め設定された基底ベクトル選択規則が、前記量子状態情報におけるアイデンティティ認証ビットの位置に従って前記準備基底又は前記測定基底を選択することを含む、請求項１に記載のアイデンティティ認証方法。
【請求項６】
前記量子状態情報における前記アイデンティティ認証ビットの前記位置に従って前記対応する準備基底又は前記測定基底を選択することが、４を法とする量子状態情報における各アイデンティティ認証ビットの位置情報の異なる剰余結果に従って、対応する水平偏光基底、垂直偏光基底、左回り偏光基底、又は右回り偏光基底を選択することを含む、請求項５に記載のアイデンティティ認証方法。
【請求項７】
前記異なる波長及び前記基底ベクトル選択規則に従って選択された前記測定基底に従って前記量子状態情報における前記受信された量子状態を測定することが、
前記異なる波長に従ってアイデンティティ認証量子状態情報及び鍵量子状態情報を区別することと、
前記選択された測定基底を使用することにより、前記アイデンティティ認証量子状態情報を測定することと、
光子が検出されない前記選択された測定基底の部分を除去して、前記測定を通して前記アイデンティティ認証情報を取得することと
を含む、請求項１に記載のアイデンティティ認証方法。
【請求項８】
前記アイデンティティ認証情報と、期待される情報との間の差が予め設定された閾値未満である場合に、前記受信機によって測定された前記アイデンティティ認証情報が前記基底ベクトル選択規則と対応する、請求項７に記載のアイデンティティ認証方法。
【請求項９】
前記アイデンティティ認証情報から前記受信機認証鍵を選択することが、
前記アイデンティティ認証情報を前記受信機認証鍵と見なすこと、又は
前記アイデンティティ認証情報から異なる位置にあるビットをランダムに選択し、及び前記選択されたビットから構成されるビットストリングを前記受信機認証鍵と見なすことを含む、請求項１に記載のアイデンティティ認証方法。
【請求項１０】
前記測定を通して取得された前記アイデンティティ認証情報における前記受信機認証鍵の位置情報、及び前記受信機認証鍵で暗号化された前記予め設定された共有鍵を送信することが、前記測定を通して取得された前記アイデンティティ認証情報における前記受信機認証鍵の位置情報と、予め設定された共有鍵と、前記受信機認証鍵で暗号化された補助認証情報とを送信することを含む、請求項１に記載のアイデンティティ認証方法。
【請求項１１】
標準チャネルを介して暗号化情報を受信することであって、前記暗号化情報は、予め設定されたポリシーを補助認証情報に適用することによって取得された前記補助認証情報のバリアントである、受信することと、

前記予め設定されたポリシーに対応する方法で、前記受信された暗号化情報を復号することと、
前記復号によって取得された情報が前記補助認証情報の前記バリアントと一致するかどうかを決定することと
を更に含む、請求項１０に記載のアイデンティティ認証方法。
【請求項１２】
前記予め設定されたポリシーが、
前記予め設定されたローカル共有鍵を使用することにより、暗号化動作を実行すること、又は
前記対応する送信機認証鍵を使用することにより、暗号化動作を実行すること
を含む、請求項１１に記載のアイデンティティ認証方法。
【請求項１３】
量子鍵配送プロセスのためのアイデンティティ認証方法であって、
ピアデバイスから、鍵ビットストリング内にインタリーブされたアイデンティティ認証ビットストリングの量子状態を含む量子状態情報を受信することであって、前記アイデンティティ認証ビットストリング及び前記鍵ビットストリングが異なる波長を有する、受信することと、
前記異なる波長に基づいて前記アイデンティティ認証ビットストリングと前記鍵ビットストリングとを区別することと、
予め設定された基底ベクトル選択規則に従う測定基底を使用して、前記受信された量子状態を測定して、前記測定を通してアイデンティティ認証情報を取得することと、
前記取得されたアイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応するかどうかを決定することと、
前記取得されたアイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応するとの決定に応じて、前記アイデンティティ認証情報から受信機認証鍵を選択することと
を含む、アイデンティティ認証方法。
【請求項１４】
前記アイデンティティ認証ビットストリングが前記鍵ビットストリング内でランダムな位置にインタリーブされる、請求項１３に記載のアイデンティティ認証方法。
【請求項１５】
前記アイデンティティ認証ビットストリングがランダムな長さを有する、請求項１３に記載のアイデンティティ認証方法。
【請求項１６】
前記予め設定された基底ベクトル選択規則が、前記量子状態情報におけるアイデンティティ認証ビットの位置に従って基底を選択することを含む、請求項１３に記載のアイデンティティ認証方法。
【請求項１７】
前記量子状態情報における前記アイデンティティ認証ビットの前記位置に従って前記基底を選択することが、４を法とする量子状態情報における各アイデンティティ認証ビットの位置情報の異なる剰余結果に従って、対応する水平偏光基底、対応する垂直偏光基底、対応する左回り偏光基底、又は対応する右回り偏光基底を選択することを含む、請求項１６に記載のアイデンティティ認証方法。
【請求項１８】
測定を通して取得された前記アイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応する場合に、前記アイデンティティ認証情報から受信機認証鍵を選択することと、
前記受信機認証鍵の位置情報及び前記受信機認証鍵で暗号化された予め設定された共有鍵を前記ピアデバイスに送信することと
を更に含む、請求項１３に記載のアイデンティティ認証方法。

【請求項１９】
前記アイデンティティ認証情報から前記受信機認証鍵を選択することが、
前記アイデンティティ認証情報を前記受信機認証鍵と見なすこと、又は
前記アイデンティティ認証情報から異なる位置にあるビットをランダムに選択し、前記選択されたビットから構成されるビットストリングを前記受信機認証鍵と見なすこと
を含む、請求項１８に記載のアイデンティティ認証方法。
【請求項２０】
前記量子状態情報を受信する前に、
前記ピアデバイスから量子鍵合意要求を受信することと、
受信されたアカウント情報に従って前記ピアデバイスのアイデンティティを検証することと、
前記検証が失敗する場合に前記量子鍵配送プロセスを終了することと、
前記検証が成功する場合に受信機のアカウント情報を前記ピアデバイスに送信することと
を更に含む、請求項１３に記載のアイデンティティ認証方法。
【請求項２１】
前記予め設定された基底ベクトル選択規則に従う前記測定基底を使用して前記量子状態情報における前記受信された量子状態を測定して、前記測定を通して前記アイデンティティ認証情報を取得することが、光子が検出されない前記測定された量子状態の部分を除去して、前記測定を通して前記アイデンティティ認証情報を取得することを更に含む、請求項１３に記載のアイデンティティ認証方法。
【請求項２２】
量子鍵配送プロセスのためのアイデンティティ認証デバイスであって、前記デバイスが、
ピアデバイスから、鍵ビットストリング内にインタリーブされたアイデンティティ認証ビットストリングの量子状態を含む量子状態情報を受信するように構成された量子状態受信ユニットであって、前記アイデンティティ認証ビットストリング及び前記鍵ビットストリングが異なる波長を有する、量子状態受信ユニットと、
前記異なる波長及び予め設定された基底ベクトル選択規則に従って、前記受信された量子状態を測定して、前記測定を通してアイデンティティ認証情報を取得するように構成された量子状態測定ユニットと
を含む、アイデンティティ認証デバイス。
【請求項２３】
命令のセットを格納する非一時的コンピュータ可読媒体であって、前記命令のセットは、受信機に、量子鍵配送プロセスのためのアイデンティティ認証方法を行わせるように、前記受信機の少なくとも一つのプロセッサによって実行可能であり、前記方法が、
送信機から、アイデンティティ認証ビットストリングの量子状態及びランダム生成鍵ビットストリングの量子状態を含む量子状態情報を、異なる波長を使用することによって受信することであって、前記アイデンティティ認証ビットストリングが前記鍵ビットストリングにおいてランダムな位置で及びランダムな長さでインタリーブされる、送信することと、
前記異なる波長及び予め設定された基底ベクトル選択規則に従って選択された測定基底に従って前記量子状態情報における受信された量子状態を測定して、前記アイデンティティ認証ビットストリングの前記測定からアイデンティティ認証情報を取得することと、
前記測定を通して取得された前記アイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応するかどうかを決定することと、
前記測定を通して取得された前記アイデンティティ認証情報が前記予め設定された基底ベクトル選択規則に対応するとの決定に応じて、
前記アイデンティティ認証情報から受信機認証鍵を選択することと、
前記測定を通して取得された前記アイデンティティ認証情報における前記受信機認証

鍵の位置情報、及び前記受信機認証鍵で暗号化された予め設定された共有鍵を前記送信機へ送信することであって、前記位置情報及び前記アイデンティティ認証ビットストリングは、前記送信機により、対応する送信機認証鍵を選択するために使用され、前記受信機認証鍵は、予め設定された新しい共有鍵を取得するために送信機認証鍵で復号される、送信することと、
前記受信機認証鍵を前記送信機認証鍵で復号すること取得された前記予め設定された新しい共有鍵が前記予め設定されたローカル共有鍵と一致しない場合に、前記量子鍵配送プロセスを終了することと
を含む、非一時的コンピュータ可読媒体。
【請求項２４】
前記命令のセットは、
標準チャネルを介して、鍵量子状態を測定するための前記測定基底を公開すること
を前記受信機が更に行うように、前記受信機の前記少なくとも一つのプロセッサによって実行可能である、請求項２３に記載の非一時的コンピュータ可読媒体。
【請求項２５】
前記命令のセットは、
前記送信機が前記アイデンティティ認証ビットストリング及び前記ランダム生成鍵ビットストリングの前記量子状態情報を送信する前に、標準チャネルを介して、予め設定されたアカウント情報を使用することによってアイデンティティ検証を行うこと
を前記受信機が更に行うように、前記受信機の前記少なくとも一つのプロセッサによって実行可能である、請求項２３に記載の非一時的コンピュータ可読媒体。
【請求項２６】
前記予め設定されたアカウント情報が識別情報及び証明書を含む、請求項２５に記載の非一時的コンピュータ可読媒体。
【請求項２７】
前記予め設定された基底ベクトル選択規則が、前記量子状態情報におけるアイデンティティ認証ビットの位置に従って前記準備基底又は前記測定基底を選択することを含む、請求項２３に記載の非一時的コンピュータ可読媒体。
【請求項２８】
前記量子状態情報における前記アイデンティティ認証ビットの前記位置に従って前記対応する準備基底又は前記測定基底を選択することが、４を法とする量子状態情報における各アイデンティティ認証ビットの位置情報の異なる剰余結果に従って、対応する水平偏光基底、垂直偏光基底、左回り偏光基底、又は右回り偏光基底を選択することを含む、請求項２７に記載の非一時的コンピュータ可読媒体。
【請求項２９】
前記異なる波長及び前記基底ベクトル選択規則に従って選択された前記測定基底に従って前記量子状態情報における前記受信された量子状態を測定することが、
前記異なる波長に従ってアイデンティティ認証量子状態情報及び鍵量子状態情報を区別することと、
前記選択された測定基底を使用することにより、前記アイデンティティ認証量子状態情報を測定することと、
光子が検出されない前記選択された測定基底の部分を除去して、前記測定を通して前記アイデンティティ認証情報を取得することと
を含む、請求項２３に記載の非一時的コンピュータ可読媒体。
【請求項３０】
前記アイデンティティ認証情報と、期待される情報との間の差が予め設定された閾値未満である場合に、前記受信機によって測定された前記アイデンティティ認証情報が前記基底ベクトル選択規則と対応する、請求項２９に記載の非一時的コンピュータ可読媒体。
【請求項３１】
前記アイデンティティ認証情報から前記受信機認証鍵を選択することが、

前記アイデンティティ認証情報を前記受信機認証鍵と見なすこと、又は
前記アイデンティティ認証情報から異なる位置にあるビットをランダムに選択し、及び前記選択されたビットから構成されるビットストリングを前記受信機認証鍵と見なすことを含む、請求項２３に記載の非一時的コンピュータ可読媒体。
【請求項３２】
前記測定を通して取得された前記アイデンティティ認証情報における前記受信機認証鍵の位置情報、及び前記受信機認証鍵で暗号化された前記予め設定された共有鍵を送信することが、前記測定を通して取得された前記アイデンティティ認証情報における前記受信機認証鍵の位置情報と、予め設定された共有鍵と、前記受信機認証鍵で暗号化された補助認証情報とを送信することを含む、請求項２３に記載の非一時的コンピュータ可読媒体。
【請求項３３】
前記命令のセットは、
標準チャネルを介して暗号化情報を受信することであって、前記暗号化情報は、予め設定されたポリシーを補助認証情報に適用することによって取得された前記補助認証情報のバリアントである、受信することと、
前記予め設定されたポリシーに対応する方法で、前記受信された暗号化情報を復号することと、
前記復号によって取得された情報が前記補助認証情報の前記バリアントと一致するかどうかを決定することと
を前記受信機が更に行うように、前記受信機の前記少なくとも一つのプロセッサによって実行可能である、請求項３２に記載の非一時的コンピュータ可読媒体。
【請求項３４】
前記予め設定されたポリシーが、
前記予め設定されたローカル共有鍵を使用することにより、暗号化動作を実行すること、又は
前記対応する送信機認証鍵を使用することにより、暗号化動作を実行すること
を含む、請求項３３に記載の非一時的コンピュータ可読媒体。
【請求項３５】
命令のセットを格納する非一時的コンピュータ可読媒体であって、前記命令のセットは、受信機に、量子鍵配送プロセスのためのアイデンティティ認証方法を行わせるように、前記受信機の少なくとも一つのプロセッサによって実行可能であり、前記方法が、
ピアデバイスから、鍵ビットストリング内にインタリーブされたアイデンティティ認証ビットストリングの量子状態を含む量子状態情報を受信することであって、前記アイデンティティ認証ビットストリング及び前記鍵ビットストリングが異なる波長を有する、受信することと、
前記異なる波長に基づいて前記アイデンティティ認証ビットストリングと前記鍵ビットストリングとを区別することと、
予め設定された基底ベクトル選択規則に従う測定基底を使用して、前記受信された量子状態を測定して、前記測定を通してアイデンティティ認証情報を取得することと、
前記取得されたアイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応するかどうかを決定することと、
前記取得されたアイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応するとの決定に応じて、前記アイデンティティ認証情報から受信機認証鍵を選択することと
を含む、非一時的コンピュータ可読媒体。
【請求項３６】
前記アイデンティティ認証ビットストリングが前記鍵ビットストリング内でランダムな位置にインタリーブされる、請求項３５に記載の非一時的コンピュータ可読媒体。
【請求項３７】
前記アイデンティティ認証ビットストリングがランダムな長さを有する、請求項３５に

記載の非一時的コンピュータ可読媒体。
【請求項３８】
前記予め設定された基底ベクトル選択規則が、前記量子状態情報におけるアイデンティティ認証ビットの位置に従って基底を選択することを含む、請求項３５に記載の非一時的コンピュータ可読媒体。
【請求項３９】
前記量子状態情報における前記アイデンティティ認証ビットの前記位置に従って前記基底を選択することが、４を法とする量子状態情報における各アイデンティティ認証ビットの位置情報の異なる剰余結果に従って、対応する水平偏光基底、対応する垂直偏光基底、対応する左回り偏光基底、又は対応する右回り偏光基底を選択することを含む、請求項３８に記載の非一時的コンピュータ可読媒体。
【請求項４０】
前記命令のセットは、
測定を通して取得された前記アイデンティティ認証情報が前記予め設定された基底ベクトル選択規則と対応する場合に、前記アイデンティティ認証情報から受信機認証鍵を選択することと、
前記受信機認証鍵の位置情報及び前記受信機認証鍵で暗号化された予め設定された共有鍵を前記ピアデバイスに送信することと
を前記受信機が更に行うように、前記受信機の前記少なくとも一つのプロセッサによって実行可能である、請求項３５に記載の非一時的コンピュータ可読媒体。
【請求項４１】
前記アイデンティティ認証情報から前記受信機認証鍵を選択することが、
前記アイデンティティ認証情報を前記受信機認証鍵と見なすこと、又は
前記アイデンティティ認証情報から異なる位置にあるビットをランダムに選択し、前記選択されたビットから構成されるビットストリングを前記受信機認証鍵と見なすこと
を含む、請求項４０に記載の非一時的コンピュータ可読媒体。
【請求項４２】
前記命令のセットは、
前記量子状態情報を受信する前に、
前記ピアデバイスから量子鍵合意要求を受信することと、
受信されたアカウント情報に従って前記ピアデバイスのアイデンティティを検証することと、
前記検証が失敗する場合に前記量子鍵配送プロセスを終了することと、
前記検証が成功する場合に受信機のアカウント情報を前記ピアデバイスに送信することと
を前記受信機が更に行うように、前記受信機の前記少なくとも一つのプロセッサによって実行可能である、請求項３５に記載の非一時的コンピュータ可読媒体。
【請求項４３】
前記予め設定された基底ベクトル選択規則に従う前記測定基底を使用して前記量子状態情報における前記受信された量子状態を測定して、前記測定を通して前記アイデンティティ認証情報を取得することが、光子が検出されない前記測定された量子状態の部分を除去して、前記測定を通して前記アイデンティティ認証情報を取得することを更に含む、請求項３５に記載の非一時的コンピュータ可読媒体。