(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6619455号
(P6619455)

(45)発行日　令和1年12月11日(2019.12.11)　(24)登録日　令和1年11月22日(2019.11.22)

(51)Int.Cl.			F I		
H04L	9/12	(2006.01)	H04L	9/00	631
H04L	9/32	(2006.01)	H04L	9/00	675A

請求項の数 43　(全 30 頁)

(21)出願番号	特願2017-560880 (P2017-560880)
(86)(22)出願日	平成28年2月5日 (2016.2.5)
(65)公表番号	特表2018-509117 (P2018-509117A)
(43)公表日	平成30年3月29日 (2018.3.29)
(86)国際出願番号	PCT/US2016/016740
(87)国際公開番号	WO2016/133724
(87)国際公開日	平成28年8月25日 (2016.8.25)
審査請求日	平成31年1月24日 (2019.1.24)
(31)優先権主張番号	201510084941.2
(32)優先日	平成27年2月16日 (2015.2.16)
(33)優先権主張国・地域又は機関	中国 (CN)

(73)特許権者　511050697
アリババ　グループ　ホウルディング　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ジョージ　タウン　ピーオーボックス　８４７　ワン　キャピタル　プレイス　フォース　フロア
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦

最終頁に続く

(54)【発明の名称】アイデンティティ認証のための方法、装置、及びシステム

(57)【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１

６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。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本出願は、２０１５年２月１６日に出願された中国特許出願公開第２０１５１００８４９４１．２号に対する優先権の利益を主張するものであり、その全内容が参照により本明細書に援用される。

【０００２】

技術分野

本出願は、アイデンティティ認証のための方法、装置、及びシステムに関する。

【背景技術】

【０００３】

背景

量子暗号技術は、量子力学と暗号学との異種間生成物として機能し、その安全性は、量子力学の基本原理によって裏付けられ、攻撃者の演算能力及び記憶容量の影響を受けず、従って、無条件安全性及び盗聴者の検出能力を有することが証明されている。最初に提案された量子鍵配送プロトコル（BB84等）は、盗聴者による鍵を盗む動作を検出することが可能であるが、これらのプロトコルは効果的なアイデンティティ認証機構を何ら提供しない。

【０００４】

アイデンティティ認証は、ネットワークの安全性にとって重要なリンクである。不正パーティが、情報を偽造及び変更する並びに通信を遅らせるなど、情報通信を攻撃することを防止するために、両方の通信パーティの真正性、メッセージのインテグリティ、及びソースの信頼性が認証によって検証され得る。従来の量子鍵配送プロトコルは、効果的なアイデンティティ認証機構を何ら有さないため、これらのプロトコルは、量子鍵配送プロセスにおいて中間者攻撃又は分散型サービス妨害（ＤＤｏＳ）攻撃を受ける可能性が高い。

【０００５】

上記の問題に関して、

（ｉ）M. Dusekらは、通信プロセスにおいて全ての従来の情報を認証する必要はなく、量子状態の誤り率の正しい判断に影響を与える従来の情報のみを認証する必要があるが、他の従来の情報を認証する必要はなく、従来の情報が変更されたとしても安全性は影響を受けないと考える。従って、M. Dusekは、従来のメッセージ認証アルゴリズムと組み合わせた量子アイデンティティ認証プロトコルを提案し、その最重要点は、従来の認証アルゴリズムを用いて可能な限り少なく従来のメッセージを認証することである。

【０００６】

（ｉｉ）アイデンティティ認証を備えたBB84プロトコルが使用される。このプロトコルと、オリジナルのBB84プロトコルとの主な違いは、ランダムに送信された量子ビットストリングの一部のビットが特定の認証鍵ビットとして設定され（例えば、量子ビットストリングにおける４ビットにつき１つが特定の認証鍵ビットとなる）、その特定の位置が認証鍵によって決定される。両方の通信パーティのアイデンティティ認証は、認証ビットのビット及び光量子の偏光状態によって表される測定基底ベクトルによって達成され、認証ビットの量子状態情報は、ランダムに送信されることは不可能であるが、特定の規則に従って両方のパーティによって共有される認証鍵によって決定されるべきであり、同時に、量子力学の基本原理が安全な鍵配送の役割を果たす。

【０００７】

上記２つの提案は、以下の問題点を有する。

【０００８】

（ｉ）M. Dusekの解決策に関して、事前に両方の通信パーティによって共有される認証鍵の数は限られており、従って、この解決策は、中間者攻撃及びＤＤｏＳ攻撃を受けやす

く、更に、この解決策は、量子の優位性を十分に活用せず、従来の認証技術を依然として使用しているため、解読される危険性がある。

【０００９】

（ｉｉ）アイデンティティ認証を備えたBB84プロトコルは、量子状態の形式で共有認識鍵情報を送信し、これは、この技術的解決策において送信側の認証鍵の全量子状態を受信側に送信できると想定されているため、鍵配送の安全性を向上させるが、受信側は、予め設定された認証鍵に従って検出のための対応する測定基底を選択することができる。検出結果が整合すれば、この技術的解決策はパスされ、そうでない場合には他方のパーティが不正であると見なされ、量子鍵配送プロセスが終了される。この解決策は、実際の送信プロセスにおける光子の減衰を考慮しておらず（すなわち、光子が必ずしも他方のパーティに送信されるとは限らず、必然的に量子状態の整合性を保証することができない）、すなわち、この技術的解決策は、チャネル減衰に対するフォールトトレランスを提供せず、アイデンティティ認識率及び量子鍵配送の量の低下をもたらす。

【発明の概要】

【課題を解決するための手段】

【００１０】

本開示のある態様は、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に向けられ、送信機及び受信機の量子通信デバイスによって実施することができる。本方法は、送信機により、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの準備基底を選択することと、送信機により、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送信することであって、アイデンティティ認証ビットストリングが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、受信機により、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量子状態情報における受信された量子状態を測定して、アイデンティティ認証ビットストリングの測定からアイデンティティ認証情報を取得することと、受信機により、測定を通して取得されたアイデンティティ認証情報が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を含む。決定の結果が肯定であるの場合、本方法は、受信機により、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、受信機により、測定を通して取得されたアイデンティティ認証情報における受信機認証鍵の位置情報、及び受信機認証鍵で暗号化された予め設定された共有鍵を送信することと、送信機により、受信された位置情報及びアイデンティティ認証ビットストリングに従って、対応する送信機認証鍵を選択することと、送信機により、対応する送信機認証鍵による復号によって取得された予め設定された共有鍵が予め設定されたローカル共有鍵と一致するかどうかを決定することと、復号によって取得された予め設定された共有鍵が予め設定されたローカル共有鍵と一致しない場合に、量子鍵配送プロセスを終了することとを更に含む。

【００１１】

本開示の別の態様は、量子通信送信機デバイスによって実施される、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に向けられる。本方法は、予め設定された異なる波長を使用することにより、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、量子鍵配送プロセスに関与するピアデバイスに送信することを含み、アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置にインタリーブされる。アイデンティティ認証ビットストリングは、ランダムな長さを有してもよい。本開示の別の実施形態によれば、アイデンティティ認証方法は、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの準備基底を選択することを更に含んでもよい。予め設定された基底ベクトル選択規則は、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（例えば、あるビットの位置に従って基底を選択すること）を含んでもよい。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準備

基底を選択することは、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、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んでもよい。

【００１２】

一部の実施形態によれば、上記のアイデンティティ認証方法は、ピアデバイスから認証鍵位置情報を受信することと、認証鍵位置情報に従って量子状態情報における量子状態から認証鍵を選択することとを更に含んでもよい。一部の他の実施形態によれば、本方法は、ピアデバイスから、予め設定された共有鍵を含む暗号化情報を受信することと、受信された暗号化情報を認証鍵で復号することと、復号された予め設定された共有鍵が予め設定されたローカル共有鍵と一致するかどうかを決定することと、復号された予め設定された共有鍵が予め設定されたローカル共有鍵と一致しない場合に量子鍵配送プロセスを終了することとを更に含んでもよい。一部の更に他の実施形態によれば、アイデンティティ認証方法は、アイデンティティ認証ビットストリング及びランダム生成鍵ビットストリングの量子状態情報を送信する前に、ピアデバイスからアカウント情報を受信することと、受信されたアカウント情報に従ってピアデバイスのアイデンティティを検証することと、検証が失敗する場合に量子鍵配送プロセスを終了することとを更に含んでもよい。

【００１３】

本開示の更なる態様は、量子通信送信機デバイスに実装される、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に向けられる。アイデンティティ認証デバイスは、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの準備基底を選択し、予め設定された異なる波長を使用することにより、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、量子鍵配送プロセスに関与するピアデバイスに送信するように構成された量子状態送信ユニットを含み、アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置にインタリーブされる。アイデンティティ認証ビットストリングは、ランダムな長さを有してもよい。予め設定された基底ベクトル選択規則は、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準備基底を選択することを含んでもよい。一部の実施形態によれば、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対応する準備基底を選択することは、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んでもよい。一部の実施形態によれば、アイデンティティ認証デバイスは、ピアデバイスから認証鍵位置情報を受信するように構成された情報受信ユニットと、位置情報及びその量子状態情報に従って認証鍵を選択するように構成された情報復号ユニットとを更に含んでもよい。

【００１４】

本開示の更に別の態様は、量子通信受信機デバイスによって実施される、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に向けられる。本方法は、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、アイデンティティ認証ビットストリング及び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、異なる波長に基づいてアイデンティティ認証ビットストリングと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、受信された量子状態を測定して、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、取得されたアイデンティティ認証情報が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を含む。アイデンティティ認証ビットストリングは、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てもよい。アイデンティティ認証ビットストリングは、ランダムな長さを有してもよい。予め設定された基底ベクトル選択規則は、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んでもよい。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

は、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んでもよい。

【００１５】

本開示の別の態様は、量子通信受信機デバイスに実装される、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に向けられる。本アイデンティティ認証デバイスは、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を含む。アイデンティティ認証ビットストリング及び鍵ビットストリングは、異なる波長を有する。本アイデンティティ認証デバイスは、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、受信された量子状態を測定して、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を更に含んでもよい。本アイデンティティ認証デバイスは、取得されたアイデンティティ認証情報が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ように構成された受信機認証ユニットを更に含んでもよい。

【００１６】

本開示の追加の特徴及び利点は、一部が以下の詳細な説明に記載され、及び一部がその説明から自明となり、又は本開示の実践から学ぶことができる。本開示の特徴及び利点は、添付の特許請求の範囲に具体的に挙げられた要素及び組み合わせにより実現及び達成されるであろう。

【００１７】

上記の概要及び以下の詳細な説明は、例示的及び説明のためのものに過ぎず、特許請求される本発明を限定するものではないことが理解されるものとする。

【００１８】

本明細書の一部を構成する添付の図面は、幾つかの実施形態を図示し、本明細書と共に開示される原理の説明に役立つ。

【図面の簡単な説明】

【００１９】

【図１】ある例示的実施形態によるアイデンティティ認証方法を示すフロー図である。

【図２】別の例示的実施形態によるアイデンティティ認証方法を示すフロー図である。

【図３】別の例示的実施形態によるアイデンティティ認証方法を示すフロー図である。

【図４】ある例示的実施形態によるアイデンティティ認証デバイスを示すブロック図である。

【図５】別の例示的実施形態によるアイデンティティ認証方法を示すフロー図である。

【図６】別の例示的実施形態によるアイデンティティ認証デバイスを示すブロック図である。

【図７】ある例示的実施形態によるアイデンティティ認証システムを示すブロック図である。

【図８】別の例示的実施形態によるアイデンティティ認証方法を示すフロー図である。

【発明を実施するための形態】

【００２０】

詳細な説明

これより、添付の図面に例が示される例示的実施形態を詳細に説明する。以下の説明は、別段の表示がなければ異なる図面の同一の番号が同一又は類似の要素を示す添付の図面を参照する。本発明に従う例示的実施形態の以下の説明に記載される実装形態は、本発明に従う全ての実装形態を示さない。代わりに、それらは、添付の特許請求の範囲に記載される本発明に関連する態様に従うシステム及び方法の例に過ぎない。

【００２１】

図１は、ある例示的実施形態によるアイデンティティ認証方法１００を示すフロー図である。本方法は、量子鍵配送プロセスに関与する送信機及び受信機の量子通信デバイスに

よって実施される。量子鍵配送プロセスは、量子鍵合意プロセスとも称される場合がある。本方法は、複数のステップを含み、それらの幾つかは任意選択的なものである。

【００２２】

一部の実施形態では、配送プロセスに関与する両方のパーティの量子通信デバイスのアイデンティティが量子鍵配送プロセスにおいて動的に検証される。ピアデバイスに量子状態情報を送信するための準備基底を選択するデバイスは、一般的に、アリス（Ａ）側（量子通信送信機デバイスと呼ばれ、略して送信機と呼ばれる）と称され、受信された量子状態情報を測定するための測定基底を選択するデバイスは、一般的に、ボブ（Ｂ）側（量子通信受信機デバイスと呼ばれ、略して受信機と呼ばれる）と称される。送信機及び受信機は、それぞれプロセッサと、実行時に以下に記載のステップを行うようにプロセッサを制御する命令を保存する非一時的メモリとを含み得る。

【００２３】

本開示の一部の実施形態によれば、量子鍵配送プロセス（量子鍵合意プロセスとも称される）のアイデンティティ認証方法は以下のステップを含む。

【００２４】

ステップ１０１：送信機は、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの準備基底を選択する。

【００２５】

ステップ１０２：送信機は、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送信し、アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置及び長さでインタリーブされる。量子状態情報は、アイデンティティ認証ビット及び鍵ビットストリングにおける各ビットの状態を含む。

【００２６】

一部の実施形態では、アイデンティティ認証は、量子鍵配送プロセスにおいて動的に行うことができる。同時に、量子鍵配送プロセスが不正な量子通信デバイス間で実行されることを回避するために、ある実施形態では、送信機が量子鍵配送プロセスを開始する前に、送信機及び受信機の量子通信デバイスが、最初に、標準チャネル（classic channel）を介して他方のパーティのデバイスのアイデンティティを検証することができ、両方のパーティのデバイスが共に検証をパスした場合のみ、後続の量子鍵配送プロセスを継続することができる。

【００２７】

一部の実施形態では、量子鍵合意プロセスのイニシエータ、すなわち、本出願に記載される送信機は、最初に量子鍵合意要求を開始することができ、この要求は、送信機のアカウント情報を含み、アカウント情報は、送信機の識別情報及び署名証明書を含んでもよい。量子鍵合意プロセスに関与するピアデバイス、すなわち、本出願に記載される受信機は、上記のアカウント情報を受信し、受信機は、その中の識別情報を使用することによって署名証明書を検証する。署名証明書が検証をパスした場合、受信機のアカウント情報を含む応答情報が送信機に返され、証明書が検証をパスしなければ量子鍵合意プロセスが終了される。

【００２８】

同じ理由から、受信機からのアカウント情報を受信した後、送信機は、上記と同様に受信機のアイデンティティを検証することができる。受信機のアイデンティティが検証をパスした場合、後続の量子鍵配送プロセスを実行することができ、そうでない場合には量子鍵配送プロセスが終了される。

【００２９】

送信機及び受信機が共に上記のアイデンティティ検証プロセスをパスした場合、後続の量子鍵配送プロセスが継続される。送信機は、基底ベクトル選択規則に従って準備基底を選択し、選択された準備基底を使用してアイデンティティ認証量子状態を準備する。一部の実施形態では、量子鍵配送プロセスにおいてアイデンティティ検証を動的に行うために

、送信機及び受信機は同じ共有鍵を予め設定してもよい。送信機は、鍵ビットストリングの任意の位置にランダムな長さを有するアイデンティティ認証ビットストリングをインタリーブし、予め設定された異なる波長を使用して上記の２種類の情報の量子状態（略して鍵量子状態及びアイデンティティ認証量子状態と呼ばれる）を区別する。鍵ビットストリングは同じ共有鍵又は異なる鍵であり得る。

【００３０】

例えば、送信機は、時点t_1、t_2．．．t_nにおいてｎの長さを有するバイナリビットストリングの量子状態を含む量子状態情報を送信することを意図するものであり、バイナリビットストリングは、一方の部分が鍵ビットストリングとして機能するランダムに生成された従来のバイナリビットストリングであり、他方の部分が予め設定された基底ベクトル選択規則に関連付けられたアイデンティティ認証ビットストリングである、２つの部分である。送信機は、アイデンティティ認証ビットストリングの長さとして機能するｎ未満の乱数ｍを一定のポリシーに従って選択することができ、次に、アイデンティティ認証ビットストリングの前に配置される鍵ビットストリングの長さとして機能する１～ｎ－ｍの自然数から自然数ｉをランダムに選択することができ、すなわち、アイデンティティ認証ビットストリングは、以下に示されるようなバイナリビットストリングを取得するように位置ｉ＋１から挿入され始める。ビットストリングにおいて、x_{i+1}．．．x_{i+m}はアイデンティティ認証ビットストリングであり、残りは鍵ビットストリングの情報である。

x_1、x_2．．．x_i、x_{i+1}．．．x_{i+m}、x_{i+m+1}．．．x_n（$x_i \in \{0、1\}$、ｉ＝１、．．．、ｎ－ｍ）

【００３１】

送信機は、時点t_1、t_2．．．t_nにおいて、上記バイナリビットストリングの符号化量子状態（

【数１】

$$|\varphi_{j_1}^{x_1}\rangle|\varphi_{j_2}^{x_2}\rangle \cdots |\varphi_{j_i}^{x_i}\rangle|\varphi_{j_{i+1}}^{x_{i+1}}\rangle \cdots |\varphi_{j_{i+m}}^{x_{i+m}}\rangle|\varphi_{j_{i+m+1}}^{x_{i+m+1}}\rangle \cdots |\varphi_{j_n}^{x_n}\rangle$$

）を受信機に送信し、j_1、j_2、．．．j_i、j_{i+1}．．．j_{i+m}、j_{i+m+1}、．．．j_nは、送信機によって採用された準備基底シーケンスであり、j_1、j_2、．．．j_i及びj_{i+m+1}、．．．j_nは、鍵ビットストリングに対応するランダム量子状態準備基底であり、j_{i+1}．．．j_{i+m}は、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アイデンティティ認証ビットストリングの量子状態準備基底である。

【００３２】

それに応じて、一部の実施形態では、後続のステップ１０２において、受信機は、測定基底シーケンスk_1、k_2．．．k_i、k_{i+1}．．．k_{i+m}、k_{i+m+1}．．．k_nを使用して、受信された量子状態を測定し、k_1、k_2．．．k_i及びk_{i+m+1}、．．．k_nは、鍵量子状態に対応するランダム量子状態測定基底であり、k_{i+1}．．．k_{i+m}は、アイデンティティ認証量子状態に対応する測定基底である。測定基底k_{i+1}．．．k_{i+m}も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る。

【００３３】

一部の実施形態では、送信機及び受信機のデバイスが従う基底ベクトル選択規則は、異なるポリシーを使用して設定することができる。例えば、送信機によって準備された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、対応する準備基底又は測定基底を選択することが実現可能である。例えば、ある実施形態では、以下の規則が使用される：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選択される。一部の実施形態では、各アイデンティティ認証ビットが準備基底を用いて準備され、異なるアイデンティティ認証ビットは異なる準備基底を有する

。本出願では、両方のシナリオが企図される。本明細書において、準備及び測定基底は単数形で言及される場合があるが、それらは単数形及び複数形の両方を包含するものとする。

【００３４】

バイナリビットストリングを記述する上述の方法を利用して、ｉ＋ｍ＝ｌと仮定して、本実施形態では、アイデンティティ認証量子状態に対応する準備基底及び測定基底は、以下の条件を満たす。

【数２】

$$f(l)=\begin{cases}\text{水平偏光状態 H}, l \bmod 4=0\\ \text{垂直偏光状態 V}, l \bmod 4=1\\ +45^\circ\text{偏光状態}+,\ l \bmod 4=2\\ -45^\circ\text{偏光状態}-,\ l \bmod 4=3\end{cases}$$

【００３５】

上記は、予め設定された基底ベクトル選択規則の一例を提供する。一部の実施形態では、前述の規則と異なる他の基底ベクトル選択規則が送信機及び受信機に対して予め設定されてもよい。例えば、送信機及び受信機が、同じ規則を使用することによってアイデンティティ認証量子状態の準備基底及び測定基底を選択する限り、異なるアルゴリズムを採用することができる。

【００３６】

一部の実施形態では、送信機は、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの量子状態準備基底を選択し、次に、予め設定された異なる波長を使用して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搬送し、量子鍵配送プロセスに関与するピアデバイスに量子状態を送信する。アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置及び長さでインタリーブされ、その結果、アイデンティティ認証情報が盗聴されることを効果的に回避し、並びに量子鍵配送プロセスにおいて中間者攻撃及びＤＤｏＳ攻撃を回避することができる。

【００３７】

ステップ１０３：受信機は、異なる波長及び基底ベクトル選択規則に従って、受信された量子状態を測定し、アイデンティティ認証ビットストリングの測定から、アイデンティティ認証量子状態情報（アイデンティティ認証情報とも称される）を取得する。受信機は、鍵ビットストリングの量子状態も測定し、鍵量子状態情報（鍵情報とも称される）を取得してもよい。

【００３８】

ステップ１０４：受信機は、測定を通して取得されたアイデンティティ認証情報が基底ベクトル選択規則と対応するかどうかを決定する。肯定の場合、本方法は、ステップ１０５に進み、そうでない場合に本方法はステップ１０６に進む。

【００３９】

ステップ１０６：量子鍵配送プロセスが終了する。

【００４０】

ステップ１０５：受信機は、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。

【００４１】

ステップ１０７：受信機は、受信機認証鍵の位置情報と、受信機認証鍵で暗号化された予め設定された共有鍵とを送信する。

【００４２】

一部の実施形態では、送信機が量子状態情報を送信するステップ１０１を実行した後、送信機及び受信機は、インタラクションプロセスにより、アイデンティティ認証量子状態

の測定結果及び両方のパーティによって予め設定された共有鍵の検証に従って、送信機及び受信機のアイデンティティ認証プロセスを完了し、次に、量子鍵配送プロトコルに従って後続の鍵合意プロセスを継続する。鍵配送の実行効率を向上させ、且つインタラクションの回数を減らすために、鍵合意の様々な段階でアイデンティティ認証を行う代替例が提供される。

【００４３】

一部の実施形態では、受信機は、従来の鍵量子状態の測定を完了するだけでなく、アイデンティティ認証量子状態情報の測定結果に従って送信機のアイデンティティも検証する。このプロセスは、サブステップ２０１～２０８を含み、図２を参照して以下に更に説明される。

【００４４】

図２は、ある例示的実施形態による受信機側からのアイデンティティ認証方法２００を示すフロー図である。本方法は、複数のステップを含み、それらの幾つかは任意選択的なものである。

【００４５】

ステップ２０１：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それらの異なる波長に従って区別する。

【００４６】

一部の実施形態では、送信機が異なる波長を使用することによってアイデンティティ認証量子状態及び鍵量子状態を送信するため、受信機は、送信機用の波長設定と同じ波長設定に従って、受信された量子状態情報から上記の２種類の情報を区別することができる。

【００４７】

ステップ２０２：鍵量子状態情報の測定基底をランダムに選択し、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証量子状態情報の測定基底を選択する。

【００４８】

一部の実施形態では、鍵量子状態の部分に関して、量子鍵配送プロトコル（例えば、BB84プロトコル）に従って測定基底をランダムに選択することが可能であり、アイデンティティ認証量子状態の部分に関して、対応する測定基底が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る。これは、上記のステップ１０１に関連して説明されており、ここでは繰り返されない。

【００４９】

ステップ２０３：受信された量子状態情報を測定し、アイデンティティ認証情報を得る。

【００５０】

一部の実施形態では、鍵量子状態が測定され、鍵情報に対するオリジナルの測定結果が得られる。

【００５１】

一部の実施形態では、ステップ２０２において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は、受信されたアイデンティティ認証量子状態情報を測定するために使用され、減衰が量子チャネルに存在し得ることを考慮して、内部に光子が検出されない部分が除去され、測定を通して取得されたアイデンティティ認証情報が得られる。

【００５２】

ステップ２０４：取得されたアイデンティティ認証情報が予め設定された基底ベクトル選択規則と一致するかどうかを決定する。それらが一致すれば、ステップ２０５が実行され、そうでない場合には量子鍵配送プロセスが終了されるステップ２０６が実行される。

【００５３】

量子鍵配送プロセスに関与する送信機及び受信機がアイデンティティ認証情報に関して同じ基底ベクトル選択規則を予め設定するため、送信機は、その規則に従って準備基底を選択し、アイデンティティ認証情報の量子状態を送信し、受信機もその規則に従って対応する量子状態を測定する測定基底を選択し、従って、減衰により検出されない光子が除去

された後、受信機によって測定されたアイデンティティ認証情報は、対応する期待される情報と一致するはずである。

【００５４】

ある実施形態では、受信機にとって、測定により取得されたアイデンティティ認証情報が、対応する期待される情報と一致する場合、アイデンティティ認証情報に関して送信機によって採用された基底ベクトル選択規則が、受信機によって採用されたものと同じであると見なすことができ、正当なアイデンティティを有する送信機のみがその規則を知ることができ、従って、送信機がアイデンティティ認証をパスしたと決定することができる。この状況では、受信機によって測定により取得されたアイデンティティ認証量子状態情報は、基底ベクトル選択規則に対応する又は一致すると見なす又は言うことができる。

【００５５】

一部の実施形態では、量子チャネル送信プロセスにおいて、個々の量子状態の測定結果が雑音障害及び他の要因により期待通りではない結果となる可能性が高い。この場合、送信機がアイデンティティ認証をパスせず、量子鍵配送プロセスが終了されたと見なされる場合、それは、量子鍵配送の量の不必要な低下を生じさせる。上述の状況、並びに中間者攻撃及びＤＤｏＳ攻撃を防ぐことに対する要望に鑑みて、閾値を設定する方法を採用することが実現可能であり、すなわち、受信機によって測定されたアイデンティティ認証情報と、基底ベクトル選択規則に則した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、例えば、測定結果と期待される情報との間の不整合ビットの数が予め設定された上限値未満である場合、受信機は、送信機がアイデンティティ認証をパスしたと見なすことができる。

【００５６】

ステップ２０５：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。

【００５７】

上述のステップ２０４において、受信機は、送信機のアイデンティティを検証済みである。次に、受信機は、送信機に対して自身のアイデンティティの有効性を証明する必要がある。受信機の検証は、送信機により、予め設定された共有鍵を比較することによって実施することができる。受信機は、予め設定されたローカル共有鍵を、量子状態から得られたアイデンティティ認証情報で暗号化し、検証のために送信機に提供することができ、すなわち、アイデンティティ認証情報が受信機認証鍵ＩＤｋｅｙとしてそのまま使用される。

【００５８】

一部の実施形態では、上記の方法に従って、盗まれたアイデンティティ認証情報を使用することにより、悪意のある中間者又は攻撃者が盗まれた共有鍵の暗号化送信を行うことも回避するために、受信機は、ＩＤｋｅｙとしてアイデンティティ認証情報をそのまま使用しなくてもよく、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、受信機認証鍵ＩＤｋｅｙとして、選択されたビットから構成されるビットストリングを使用する。

【００５９】

ステップ２０７：予め設定されたローカル共有鍵を受信機認証鍵で暗号化する。

【００６０】

受信機は、ステップ２０５において選択されたＩＤｋｅｙを使用して、予め設定されたローカル共有鍵を暗号化する。

【００６１】

一部の実施形態では、情報発行者のアイデンティティが量子鍵配送プロセスの他の後続の状態において、例えば正しい測定基底が発行される際になお検証することができるように、及び鍵配送プロセスの安全性が更に保証されるように、受信機によってＩＤｋｅｙで暗号化された情報は、予め設定された共有鍵だけでなく、ローカル生成補助認証情報ｍも含むことができる。

【００６２】

ステップ２０８：標準チャネルを介して、受信機認証鍵の位置情報及び受信機の予め設定されたローカル共有鍵を含む暗号化情報を送信し、鍵量子状態情報の測定基底を公開する。

【００６３】

受信機は、標準チャネルを介して、ステップ２０５において選択されたＩＤｋｅｙに対応する位置情報、及びステップ２０７を実行することによって取得された暗号化情報を送信する。

【００６４】

受信機は、量子鍵配送プロトコルに従って、標準チャネルを介して、鍵量子状態を測定するために受信機によって採用された測定基底を公開することもできる。

【００６５】

図１を再び参照すると、ステップ１０８：送信機は、受信された位置情報に従って対応する送信機認証鍵を選択する。送信機は、アイデンティティ認証情報（アイデンティティ認証ビットストリング）を有する。受信された位置情報を用いて、送信機は、対応する送信機認証鍵を識別することができる。

【００６６】

ステップ１０９：送信機は、受信機から受信した暗号化情報を、対応する送信機認証鍵で復号する。受信した情報は、予め設定された共有鍵を含有する。受信した情報を送信機が復号した後、送信機は、予め設定された共有鍵を取得し、それを予め設定されたローカル共有鍵と比較し、それが予め設定されたローカル共有鍵と一致するかどうかを決定する。

【００６７】

ステップ１１０：予め設定された共有鍵を含む受信された情報が予め設定されたローカル共有鍵と一致しない場合、量子鍵配送プロセスが終了する。

【００６８】

一部の実施形態では、送信機は、標準チャネルを介して、受信機によって公開された測定基底、選択されたＩＤｋｅｙの位置情報、及び暗号化情報を受信する。送信機は、位置情報及びステップ１０１において自身によって送信された量子状態情報に従って送信機認証鍵、すなわち、送信機のＩＤｋｅｙを取得し、ＩＤｋｅｙを使用して、受信された暗号化情報を復号し、復号後の予め設定された共有鍵及び補助認証情報を得る。その後、復号後の受信機からの予め設定された共有鍵が、送信機の予め設定されたローカル共有鍵と一致するかどうかが決定される。送信機にとって、受信機によって送信された暗号化情報が自身のＩＤｋｅｙを使用して復号され、取得された予め設定された共有鍵情報が予め設定されたローカル共有鍵と一致する場合、それは、受信機の予め設定された共有鍵が送信機の予め設定されたローカル共有鍵と同じであることを示し、正当なアイデンティティを有する受信機のみが同じ共有鍵を有し得る。一方、それは、受信機が測定基底を選択し、正しいＩＤｋｅｙを使用して暗号化動作を行うために送信機のものと同じ基底ベクトル選択規則に従うことも意味するため、送信機は、予め設定されたローカル共有鍵と一致する予め設定された共有鍵を復号することができる。従って、受信機がアイデンティティ認証をパスしたと決定することができる。逆に、それらが一致しない場合、受信機は、中間者又は攻撃者の可能性があると見なすことができ、従って、量子鍵配送プロセスが終了される。

【００６９】

送信機が、受信機のアイデンティティが正当であると決定した場合、量子鍵配送プロトコルのプロシージャに従って、送信機は、受信機によって公開された測定基底を送信機によって使用された準備基底と比較し、それから正しい測定基底を選択し、正しい測定基底に従ってオリジナルの鍵を選択し、標準チャネルを介して正しい測定基底を受信機に公開することができる。

【００７０】

これまで、ステップ１０１～ステップ１１０を通して、受信機は、アイデンティティ認

証量子状態情報が基底ベクトル選択規則に対応するかどうかを決定することにより、送信機のアイデンティティを検証し、送信機は、予め設定された共有鍵を比較することにより、受信機のアイデンティティを検証する。送信機及び受信機が共に上記の検証をパスした場合、後続の鍵配送プロセスの実行は、量子鍵配送プロトコルのプロシージャに従って継続することができる。

【００７１】

一部の実施形態では、鍵配送プロセスの安全性を更に保証するために、アイデンティティ認証及びデータ暗号化プロシージャが後続の配送プロセスにおいて交互に行われてもよく、このような例が以下に更に説明される。

【００７２】

１）送信機は、補助認証情報のバリアントを暗号化し、補助認証情報のバリアントを含む暗号化情報を送信する。

【００７３】

上記の通り、ステップ１０７～１１０において、送信機は、復号後の補助認証情報を得る。受信機のアイデンティティが有効であることを送信機が検証した後、送信機は、最初に、予め設定されたポリシーを使用することによって復号後の補助認証情報のバリアントを暗号化することができ、次に、鍵量子状態の正しい測定基底が標準チャネルを介して公開されると、暗号化動作が実行された後に暗号化情報を送信することができる。

【００７４】

予め設定されたポリシーは、送信機及び受信機の両方によって予め設定されてもよく、ネゴシエーションによって決定されてもよい。予め設定されたポリシーは、例えば、予め設定された共有鍵で暗号化動作を実行すること、又はＩＤｋｅｙを使用することによって暗号化動作を実行することを含んでもよい。

【００７５】

補助認証情報のバリアントは、補助認証情報に基づいて生成された情報を指す。例えば、バリアントは補助認証情報自体でもよく、又はバリアントは、予め設定された数学的変換方法、例えばｍ＋１（ここで、ｍは、補助認証情報である）を使用することにより、補助認証情報を処理することによって得られる結果である。送信機及び受信機は共に、同じ補助認証情報ｍに関して両方のパーティによって生成されたバリアント情報が一致することを保証するために、同じバリアント生成アルゴリズム又は関数を予め設定することができる。

【００７６】

２）受信機が正しい測定基底及び暗号化情報を受信した後、暗号化情報を復号することにより、送信機のアイデンティティが検証される。

【００７７】

最初に、受信機は、送信機によって採用された予め設定されたポリシーに対応する方法で、受信された暗号化情報を復号する。例えば、送信機がＩＤｋｅｙを使用することによって暗号化動作を実行する場合、受信機もそれ自体のＩＤｋｅｙを使用することによって復号動作を実行し、送信機が予め設定されたローカル共有鍵で暗号化動作を実行する場合、受信機も予め設定されたローカル共有鍵で復号動作を実行する。

【００７８】

次に、復号動作後に取得された情報がローカル生成補助認証情報ｍのバリアントと一致するかどうかが決定される。補助認証情報ｍは、最初に、受信機によってローカルに生成され、標準チャネルを介して暗号化形式で送信機に送信される。補助認証情報が送信機によって復号及び回復された後、補助認証情報のバリアントが予め設定されたポリシーを使用することによって再び暗号化され、受信機に送信される。次に、受信機による復号後の結果が最初に生成されたローカル補助認証情報のバリアントと一致する場合、それは、送信機が補助認証情報ｍを問題なく復号及び回復させることができるだけでなく、送信機によって採用された暗号化方法及びバリアント生成アルゴリズム又は関数が受信機のものと合致することを示し、その結果、受信機は、送信機のアイデンティティを再検証し、それ

は、標準チャネルを介して送信機によって公開された鍵量子状態の正しい測定基底が信頼できることも示す。

【００７９】

従って、判断結果が「肯定」である場合、受信機は、標準チャネルを介して公開された正しい測定基底に従ってオリジナルの鍵を選択することができ、後続のビット誤り率推定を行うために、標準チャネルを介して幾つかの鍵量子状態の測定結果を公開することができ、判断結果が「否定」である場合、それは送信機のアイデンティティが信頼できないことを示し、従って、量子鍵配送プロセスを終了することができる。

【００８０】

受信機が、対応するバリアント計算規則を知っている限り、送信機は、動的変化アルゴリズム又は関数を使用することによって補助認証情報のバリアントを暗号化することもでき、従って、安全性を更に向上させることができる。例えば、送信機は、１回目に以下の方法、補助認証情報＋１でバリアントを計算し、受信機は、復号後の情報を最初に生成されたローカル補助認証情報ｍのバリアントｍ＋１と比較し、送信機は、２回目に以下の方法、補助認証情報＋２でバリアントを計算し、受信機は、復号後の情報を最初に生成されたローカル補助認証情報ｍのバリアントｍ＋２と比較する。

【００８１】

３）送信機がビット誤り率を推定した後、ビット誤り率は、ＩＤｋｅｙを用いて暗号化され、受信機に送信される。

【００８２】

送信機は、受信機によって公開された幾つかの鍵量子状態の測定結果に従ってビット誤り率を推定する。ビット誤り率が特定の閾値範囲内にある場合、誤りが、誤り訂正技術を使用することによって訂正される。次に、通信プロセス及び誤り訂正プロセスにおいて生じる情報漏洩をなくすために、誤り訂正された量子鍵に対してプライバシー増幅を更に行うことができ、最後に無条件安全共有量子鍵が抽出される。ビット誤り率が特定の閾値を超える場合、量子鍵配送プロセスを中止することができる。

【００８３】

ビット誤り率が閾値を超えない場合、送信機が上記の動作を終了した後、両方のパーティが同じ判断を行い、後続のプライバシー増幅及び他の処理動作を同じポリシーに基づいて実行し、その結果、同じ共有量子鍵を得ることを保証するために、ビット誤り率を参照用に受信機に送信することができる。中間者又は攻撃者がビット誤り率情報を盗むことを回避するために、送信機は、ＩＤｋｅｙを用いてビット誤り率を暗号化し、暗号化後の情報を受信機に送信することができる。

【００８４】

４）受信機は、受信された情報を復号し、ビット誤り率を得、対応する処理を実行する。

【００８５】

ビット誤り率の暗号化情報を受信した後、受信機は、ＩＤｋｅｙを用いて情報を復号し、送信機によって推定されたビット誤り率を得る。受信機は、ビット誤り率に従って、送信機によって実行された動作と同じ動作を実行することができ、自身によって推定したビット誤り率を、送信機によって送信されたビット誤り率と比較することもできる。それらの間の差が予め設定された範囲内にある場合、すなわち、ビット誤り率並びに送信機及び受信機の後続の処理ポリシーに基づいた判断結果が同じである場合、受信機は、後続の動作を実行し続けることができ、最終的に送信機のものと同じ無条件安全共有量子鍵を得ることができる。

【００８６】

ステップ１０１～１１０を通して、送信機及び受信機に対するアイデンティティ認証が量子鍵配送プロセスによって実施される。一部の実施形態では、鍵情報及びアイデンティティ認証情報は、異なる波長を使用することによって区別され、可変長のアイデンティティ認証情報の量子状態が鍵量子状態においてランダムにインタリーブされ、送信機及び受

信機は共に、準備基底又は測定基底を選択する際にピアデバイスが同じ基底ベクトル選択規則に従うかどうか、及びピアデバイスが同じ予め設定された共有鍵を有するかどうかを検出することにより、アイデンティティ認証プロセスを完了する。本出願の実施形態は、量子の安全性を十分に活用し、量子状態情報によるアイデンティティ認証を行うことにより、アイデンティティ検証を達成する。開示の方法は、中間者攻撃及びＤＤｏＳ攻撃を効果的に防ぎ、量子鍵配送プロセスの安全性を保証することができるだけでなく、量子鍵配送量の低下を生じさせない。

【００８７】

図３は、別の例示的実施形態によるアイデンティティ認証方法３００を示すフロー図である。本方法は、複数のステップを含み、それらの幾つかは任意選択的なものである。本例の幾つかの部分は、上記の第１の例のステップと同じである。これらの部分は繰り返されず、以下の説明はそれらの差異に注目する。本方法は以下のステップを含む。

【００８８】

ステップ３０１：予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの準備基底を選択する。

【００８９】

ステップ３０２：予め設定された異なる波長を使用することにより、アイデンティティ認証ビットストリング及びランダム生成鍵ビットストリングの量子状態情報を、量子鍵配送プロセスに関与する受信機側のピアデバイスに送信し、アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置及び長さでインタリーブされる。

【００９０】

一部の実施形態では、このステップの前に、最初に量子鍵合意要求（この要求は、送信機のアカウント情報を含む）をピアデバイスに送信し、それにより、ピアデバイスが送信機のアイデンティティを検証できるようにすることが実現可能である。ピアデバイスによって送信されたアカウント情報を受信し、アカウント情報に従って相手側のアイデンティティを検証することが実現可能である。上記の検証の何れかが失敗する場合には量子鍵配送プロセスが終了され、検証が成功する場合には量子状態を送信する本ステップを実行することができる。

【００９１】

一部の実施形態では、予め設定された基底ベクトル選択規則は、アイデンティティ認証ビットストリング及び鍵ビットストリングの量子状態情報におけるアイデンティティ検証ビットの位置に従って、対応する準備基底を選択すること、例えば、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検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。

【００９２】

ステップ３０３：ピアデバイスから返された認証鍵位置情報及び認証すべき暗号化情報を受信する。

【００９３】

一部の実施形態では、ピアデバイスから返された情報は、認証鍵位置情報及び認証すべき暗号化情報を含むだけでなく、鍵量子状態の測定に使用される測定基底も含む。暗号化情報は、受信機側の予め設定されたローカル共有鍵を含む。

【００９４】

ステップ３０４：送信機によって送信された位置情報及び量子状態情報に従って認証鍵を選択する。

【００９５】

ステップ３０５：認証すべき受信された暗号化情報を認証鍵で復号する。

【００９６】

ステップ３０６：復号後の情報が送信機側の予め設定されたローカル共有鍵と一致する

かどうかを決定する。

【００９７】

ステップ３０７：復号によって取得された情報が予め設定されたローカル共有鍵と一致しない場合、量子鍵配送プロセスを終了する。

【００９８】

一部の実施形態では、復号によって取得された情報が予め設定されたローカル共有鍵と一致する場合、量子鍵配送プロトコルに従って後続の動作：

鍵量子状態の正しい測定基底を決定し、オリジナルの鍵を選択すること、

標準チャネルを介して鍵量子状態の正しい測定基底を公開すること、及び

ビット誤り率推定、誤り訂正及びプライバシー増幅プロセスによって最終共有量子鍵を得ること

の実行を継続することができる。

【００９９】

一部の実施形態では、受信機によって送信された補助認証情報もステップ３０３において受信される場合、ステップ３０６の決定結果が「肯定」であれば、補助認証情報のバリアントを暗号化し、正しい測定基底が公開されている間に補助認証情報のバリアントの暗号化情報を送信し、それにより、受信機が更なる検証を行うことができるようにすることも実現可能である。加えて、ビット誤り率の推定後、ステップ３０４～３０５で選択された認証鍵でビット誤り率を暗号化し、暗号化されたビット誤り率を受信機に送信することも実現可能である。

【０１００】

図４は、ある例示的実施形態によるアイデンティティ認証デバイス４００を示すブロック図である。本デバイスは、量子鍵配送プロセスに関与する量子通信送信機デバイスに配置されてもよい。本装置は、上記の方法を実施するために使用することができる。換言すれば、上記の方法は、本装置の例示的機能と見なすことができる。従って、以下の装置の機能の説明は、比較的シンプルであり、方法ステップの対応する説明を参照することができる。

【０１０１】

一部の実施形態では、量子鍵配送プロセスのためのアイデンティティ認証装置は、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの準備基底を選択し、予め設定された異なる波長を使用することにより、アイデンティティ認証ビットストリング及びランダム生成鍵ビットストリングの量子状態情報を、量子鍵配送プロセスに関与する受信機側のピアデバイスに送信するように構成された量子状態送信ユニット４０１であって、アイデンティティ認証ビットストリングが鍵ビットストリングにおいてランダムな位置及び長さでインタリーブされる、量子状態送信ユニット４０１と、ピアデバイスによって返された認証鍵位置情報及び認証すべき暗号化情報を受信するように構成された応答情報受信ユニット４０２と、送信された位置情報及び量子状態情報に従って認証鍵を選択し、認証すべき受信された暗号化情報を認証鍵で復号するように構成された情報復号ユニット４０３と、復号によって取得された情報が予め設定されたローカル共有鍵と一致するかどうかを決定し、否定の場合、量子鍵配送プロセスを終了するように構成された送信機認証判断ユニット４０４とを含む。

【０１０２】

一部の実施形態では、応答情報受信ユニット４０２によって受信される情報は、認証鍵位置情報及び認証すべき暗号化情報を含むだけでなく、鍵量子状態の測定に使用される測定基底も含む。

【０１０３】

本装置は、

認証判断ユニットの出力結果が肯定である場合に、鍵量子状態の正しい測定基底を決定し、オリジナルの鍵を選択するように構成されたオリジナル鍵選択ユニットと、

標準チャネルを介して鍵量子状態の正しい測定基底を公開するように構成された正しい

測定基底公開ユニットと、
ビット誤り率推定、誤り訂正及びプライバシー増幅プロセスによって最終共有量子鍵を得るように構成された送信機量子鍵取得ユニットと
を更に含んでもよい。
【０１０４】
一部の実施形態では、本装置は、
量子鍵合意要求をピアデバイスに送信するように構成された合意要求送信ユニットであって、この要求が送信機のアカウント情報を含む、合意要求送信ユニットと、
ピアデバイスによって送信されたアカウント情報を受信するように構成されたアカウント情報受信ユニットと、
アカウント情報に従ってピアデバイスのアイデンティティを検証し、検証が失敗する場合に量子鍵配送プロセスを終了するように構成された第１のアイデンティティ認証ユニットと
を更に含んでもよい。
【０１０５】
一部の実施形態では、量子状態送信ユニットによって採用された予め設定された基底ベクトル選択規則は、量子状態情報におけるアイデンティティ検証ビットの位置に従って、対応する準備基底を選択することを含む。
【０１０６】
一部の実施形態では、量子状態送信ユニットによって採用された予め設定された基底ベクトル選択規則は、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検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指す。
【０１０７】
図５は、別の例示的実施形態によるアイデンティティ認証方法５００を示すフロー図である。本方法は、量子鍵配送プロセスに関与する量子通信受信機デバイスに対して実施されてもよい。上記の第１の例のステップと同じ本例の部分は繰り返されず、以下はそれらの差異に注目する。本方法は以下のステップを含む。
【０１０８】
ステップ５０１：量子鍵配送プロセスに関与する送信機側のピアデバイスによって送信された量子状態情報を受信する。
【０１０９】
一部の実施形態では、このステップの前に、ピアデバイスによって送信された鍵合意要求を受信し、要求内に含まれたアカウント情報に従って相手側のアイデンティティを検証することが実現可能である。検証が失敗する場合には量子鍵配送プロセスが終了され、検証が成功する場合には受信機のアカウント情報がピアデバイスに送信され、ピアデバイスによって送信された量子状態情報を受信するステップを実行することができる。
【０１１０】
ステップ５０２：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、受信された量子状態情報における量子状態を測定し、測定結果に従ってアイデンティティ認証情報を得る。
【０１１１】
一部の実施形態では、予め設定された基底ベクトル選択規則は、量子状態情報のアイデンティティ検証ビットの位置に従って、対応する測定基底を選択すること、例えば、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検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。
【０１１２】
一部の実施形態では、このステップは、以下のサブステップ：予め設定された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、予

め設定された基底ベクトル選択規則に従ってアイデンティティ認証量子状態情報の測定基底を選択することと、選択された測定基底を使用することによってアイデンティティ認証量子状態情報を測定して、内部に光子が検出されない部分を除去することにより、アイデンティティ認証情報を得ることとを含んでもよい。

【０１１３】

ステップ５０３：アイデンティティ認証情報が基底ベクトル選択規則と対応するかどうかを決定する。肯定の場合にはステップ５０４を実行し、そうでない場合には量子鍵配送プロセスが終了されるステップ５０５を実行する。

【０１１４】

ステップ５０４：アイデンティティ認証情報から認証鍵を選択し、認証鍵の位置情報及び認証鍵で暗号化された予め設定された共有鍵をピアデバイスに送信する。

【０１１５】

一部の実施形態では、アイデンティティ認証情報から認証鍵を選択することは、認証鍵としてアイデンティティ認証情報を選択すること、又は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、選択されたビットから構成されるビットストリングを認証鍵と見なすことを含む。

【０１１６】

一部の実施形態では、認証鍵を使用してローカル生成補助認証情報ｍを暗号化し、位置情報及び暗号化された予め設定された共有鍵と共に暗号化情報をピアデバイスに送信することも実現可能である。

【０１１７】

一部の実施形態では、鍵量子状態の測定に使用される測定基底が標準チャネルを介して受信機デバイスによって公開されてもよい。

【０１１８】

一部の実施形態では、このステップ後、以下の動作も実行することができる。

【０１１９】

１）標準チャネルを介して、ピアデバイスによって送信された鍵量子状態の正しい測定基底を受信する。

【０１２０】

補助認証情報のバリアントの暗号化情報が同時に受信される場合、復号動作が実行され、補助認証情報のバリアントが、最初に生成されたローカル補助認証情報のバリアントと一致するかどうかが検証される。それらが一致する場合、オリジナルの鍵を選択すること等の後続の動作が実行され、そうでない場合には量子鍵配送プロセスが終了される。

【０１２１】

２）オリジナルの鍵を選択し、ビット誤り率の取得、誤り訂正及びプライバシー増幅プロセスによって最終共有量子鍵を得る。

【０１２２】

オリジナルの鍵が選択された後、送信機によって送信されたビット誤り率を含む暗号化情報が受信される場合、復号は、ステップ５０４で選択された認証鍵を使用することによって行うことができ、誤り訂正及びプライバシー増幅等の後続のプロセスは、その結果に従って実行され、それにより、最終共有量子鍵を得る。

【０１２３】

図６は、別の例示的実施形態によるアイデンティティ認証デバイス６００を示すブロック図である。本装置は、量子鍵配送プロセスに関与する量子通信受信機デバイスに配置されてもよい。本装置は、上記の方法を実施するために使用することができる。換言すれば、上記の方法は、本装置の例示的機能と見なすことができる。従って、以下の装置の機能の説明は、比較的シンプルであり、方法の対応する説明を参照することができる。

【０１２４】

本例の量子鍵配送プロセスのアイデンティティ認証装置は、量子鍵配送プロセスに関与する送信機側のピアデバイスによって送信された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６０１と、予め設定された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量子状態情報における受信された量子状態を測定し、測定結果に従ってアイデンティティ認証情報を得るように構成された量子状態測定ユニット６０２と、アイデンティティ認証情報が基底ベクトル選択規則と対応するかどうかを決定し、否定の場合に量子鍵配送プロセスを終了するように構成された受信機認証判断ユニット６０３と、受信機認証判断ユニットの出力が肯定である場合にアイデンティティ認証情報から認証鍵を選択し、認証鍵の位置情報及び認証鍵で暗号化された予め設定された共有鍵をピアデバイスに送信するように構成された情報送信ユニット６０４とを含む。

【０１２５】

一部の実施形態では、本装置は、受信機認証判断ユニットの出力が肯定である場合に、標準チャネルを介して、鍵量子状態の測定に使用される測定基底を公開するように構成された測定基底公開ユニットを更に含んでもよい。

【０１２６】

一部の実施形態では、本装置は、

標準チャネルを介して、ピアデバイスによって送信された鍵量子状態の正しい測定基底を受信するように構成された正しい測定基底受信ユニットと、

オリジナルの鍵を選択し、ビット誤り率の取得、誤り訂正及びプライバシー増幅プロセスによって最終共有量子鍵を得るように構成された受信機量子鍵取得ユニットと

を更に含んでもよい。

【０１２７】

一部の実施形態では、本装置は、

ピアデバイスによって送信された鍵合意要求を受信するように構成された合意要求受信ユニットと、

要求内に含まれたアカウント情報に従ってピアデバイスのアイデンティティを検証するように構成された第２のアイデンティティ認証ユニットと

を更に含む。検証が失敗する場合には量子鍵配送プロセスを終了し、そうでない場合には受信機のアカウント情報をピアデバイスに送信する。

【０１２８】

一部の実施形態では、量子状態測定ユニットによって採用された予め設定された基底ベクトル選択規則は、量子状態情報におけるアイデンティティ検証ビットの位置に従って、対応する基底を選択することを含む。

【０１２９】

一部の実施形態では、量子状態測定ユニットによって採用された予め設定された基底ベクトル選択規則は、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検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指す。

【０１３０】

一部の実施形態では、量子状態測定ユニットは、

予め設定された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ように構成された情報区別サブユニットと、

予め設定された基底ベクトル選択規則に従ってアイデンティティ認証量子状態情報の測定基底を選択するように構成されたアイデンティティ認証測定基底選択サブユニットと、

選択された測定基底を使用することにより、アイデンティティ認証量子状態情報を測定して、内部に光子が検出されない部分を除去することにより、アイデンティティ認証情報を得るように構成されたアイデンティティ認証情報取得サブユニットと

を含む。

【０１３１】

一部の実施形態では、情報送信ユニットは、

アイデンティティ認証情報から認証鍵を選択するように構成された認証鍵選択サブユニットと、

認証鍵の位置情報及び認証鍵で暗号化された予め設定された共有鍵をピアデバイスに送信するように構成された情報送信サブユニットと
を含み、認証鍵選択サブユニットは、
認証鍵としてアイデンティティ認証情報を選択するか、又は
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、選択されたビットから構成されるビットストリングを認証鍵と見なす
ように構成される。

【０１３２】

図７は、ある例示的実施形態によるアイデンティティ認証システム７００を示すブロック図である。本システムは、量子通信送信機デバイスに配置されるアイデンティティ認証装置７０１、量子通信受信機デバイスに配置されるアイデンティティ認証装置７０２を含む。送信機及び受信機の量子通信デバイスに配置されたアイデンティティ認証装置は、同じ基底ベクトル選択規則及び同じ共有鍵を予め設定し、同じ波長設定を使用してアイデンティティ認証情報及び鍵情報を区別する。

【０１３３】

送信機及び受信機の量子通信デバイスにそれぞれ配置されたアイデンティティ認証装置は、本出願において提供されたアイデンティティ認証方法を使用することにより、量子鍵配送プロセスにおいてピアデバイスのアイデンティティに対する動的検証を実現する。

【０１３４】

図８は、別の例示的実施形態によるアイデンティティ認証方法８００を示すフロー図である。量子通信送信機デバイスに配置されたアイデンティティ認証装置はＡ（８１１）と称され、量子通信受信機デバイスに配置されたアイデンティティ認証装置はＢ（８１２）と称される。

【０１３５】

ステップ８０１：Ａは、Ｂに鍵合意要求を送信し、この要求はＡのアカウント情報を有する。

【０１３６】

ステップ８０２：Ｂは、Ａのアイデンティティの有効性を検証し、Ｂのアカウント情報をＡに送信する。

【０１３７】

ステップ８０３：Ａは、受信したアカウント情報に従ってＢのアイデンティティの有効性を検証し、Ａは、予め設定された基底ベクトル選択規則に従ってアイデンティティ認証ビットストリングの準備基底を選択し、異なる波長を使用することによって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送信し、アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置及び長さでインタリーブされる。

【０１３８】

ステップ８０４：Ｂは、異なる波長及び基底ベクトル選択規則に従って、受信した量子状態を測定し、測定を通して取得されたアイデンティティ認証情報が基底ベクトル選択規則と対応する場合、アイデンティティ認証情報から受信機認証鍵ＩＤｋｅｙを選択し、受信機認証鍵の位置情報及び受信機認証鍵で暗号化された予め設定された共有鍵、及びローカル補助認証情報ｍを送信し、鍵量子状態の測定基底を公開し、そうでなければ量子鍵配送プロセスが終了される。

【０１３９】

ステップ８０５：Ａは、受信した位置情報に従って対応する送信機認証鍵（ＩＤｋｅｙ）を選択し、受信した暗号化情報を、対応する送信機認証鍵で復号して予め設定された共有鍵を取得し、予め設定された共有鍵が予め設定されたローカル共有鍵と一致するかどうかを決定し、それらが一致する場合にはオリジナルの鍵を選択し、鍵量子状態の正しい測定基底及び得られた補助認証情報のバリアントの暗号化情報を公開し、それらが一致しない場合には量子鍵配送プロセスが終了される。

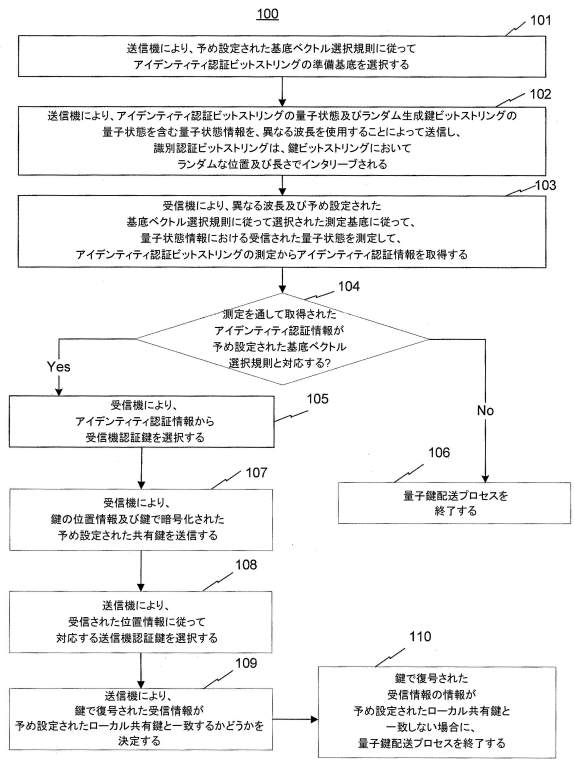
【０１４０】
ステップ８０６：Ｂは、補助認証情報のバリアントの暗号化情報を復号し、復号された暗号化情報が最初に生成されたローカル補助認証情報ｍのバリアントと一致する場合、受信した正しい測定基底に従ってオリジナルの鍵を選択し、幾つかの鍵量子状態の測定結果を公開し、そうでない場合には量子鍵配送プロセスが終了される。
【０１４１】
ステップ８０７：Ａは、幾つかの鍵量子状態の測定結果を受信し、ビット誤り率を計算する。Ａは、ビット誤り率の計算、誤り訂正及びプライバシー増幅によって最終共有量子鍵も得、ＩＤｋｅｙで暗号化されたビット誤り率をＢに送信し、Ｂは、受信したビット誤り率を復号し、ビット誤り率に従って対応する誤り訂正及びプライバシー増幅を実行することにより、最終共有量子鍵を得る。
【０１４２】
上記は、システムの一実装形態を例示し、他の実装形態では異なるインタラクション方法が採用され得ることに留意されたい。例えば、１）及び２）、並びにリンク４）においてＡに対してＢのアイデンティティ認証を行い、且つリンク５）においてＢに対してＡのアイデンティティ認証を行うプロセスにおいて、予め設定されたアカウント情報に基づいてアイデンティティ認証リンクを実行しないことが実現可能である。補助認証情報ｍを使用しないこと、後続のリンクにおいてアイデンティティ認証のためにｍのバリアント情報を使用し続けないこと、並びに暗号化、復号及びビット誤り率に関する他の動作を行うためにＩＤｋｅｙを使用しないことも実現可能である。ＡとＢとの間の相互認証は、アイデンティティ認証量子状態が基底ベクトル選択規則と一致するかどうか、並びにＡ及びＢによって予め設定された共有鍵がリンク３）、４）及び５）において互いに対応するかどうかを検証することによって完了されてもよい。
【０１４３】
本明細書では、アイデンティティ認証のための方法、装置、及びシステムを記載した。例示されたステップは、示された例示的実施形態を説明するために提示されたものであり、現在進行中の技術的発展が、特定の機能が行われる方法を変えるであろうことを認識されたい。従って、これらの例は、本明細書において説明目的のために示されるものであり、限定ではない。例えば、本明細書に開示されたステップ又はプロセスは、記載の順序で行われることに限定されず、任意の順序で行われてよく、開示の実施形態に従う一部のステップは省かれてもよい。更に、機能構成ブロックの境界線は、説明の便宜上、本明細書において任意に定義されている。特定の機能及びそれらの関係性が適切に行われる限り、別の境界線を定義することができる。代替形態（本明細書に記載されたものの均等物、拡張形態、変形形態、逸脱形態等を含む）が本明細書に含有される教示に基づいて関連分野の当業者に明白となるであろう。このような代替形態は、開示の実施形態の範囲及び趣旨の範囲内に入る。
【０１４４】
開示の原理の例及び特徴が本明細書に記載されるが、開示の実施形態の趣旨及び範囲から逸脱することなく、変更形態、適応形態、及び他の実装形態が可能である。また、「含む」、「有する」、「含有する」、及び「包含する」という語及び他の類似の形態が意味的に均等であること、及びこれらの語の何れか１つに続く１つ又は複数のアイテムは、そのような１つ又は複数のアイテムの完全なリストであること、又はリストされた１つ又は複数のアイテムにのみ限定されることを目的としたものではない点でオープンエンド形式であることが意図される。本明細書及び添付の特許請求の範囲において使用される場合、単数形の「１つの（a）」、「１つの（an）」、及び「その（the）」は、文脈が明らかにそうでないことを決定付けない限り、複数参照を含むことも留意される必要がある。
【０１４５】
更に、本開示に従う実施形態を実施する際に、１つ又は複数のコンピュータ可読記憶媒体が利用されてもよい。コンピュータ可読記憶媒体は、プロセッサによる読み出しが可能な情報又はデータを保存することができる任意の種類の物理メモリを指す。従って、コン

ピュータ可読記憶媒体は、１つ又は複数のプロセッサによって実行される命令（本明細書に記載される実施形態に従うステップ又は段階をプロセッサに行わせる命令を含む）を保存してもよい。「コンピュータ可読記憶媒体」という用語は、有形アイテムを含み、並びに搬送波及び過渡信号を除外する、すなわち、非一時的であると理解されるものである。例には、ＲＡＭ、ＲＯＭ、揮発性メモリ、不揮発性メモリ、ハードドライブ、ＣＤ－ＲＯＭ、ＤＶＤ、フラッシュドライブ、ディスク、及び任意のその他の既知の物理記憶媒体が含まれる。

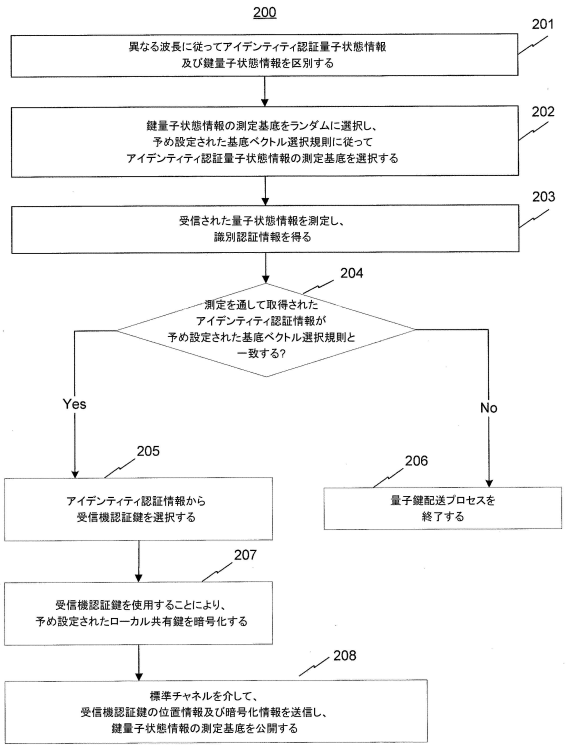
【０１４６】

本発明は、上記に説明された、及び添付の図面に図示された正確な構造に限定されず、並びにその範囲から逸脱することなく、様々な変更形態及び改変形態がなされ得ることが認識されるであろう。本発明の範囲は、添付の特許請求の範囲によってのみ限定されるべきであることが意図される。

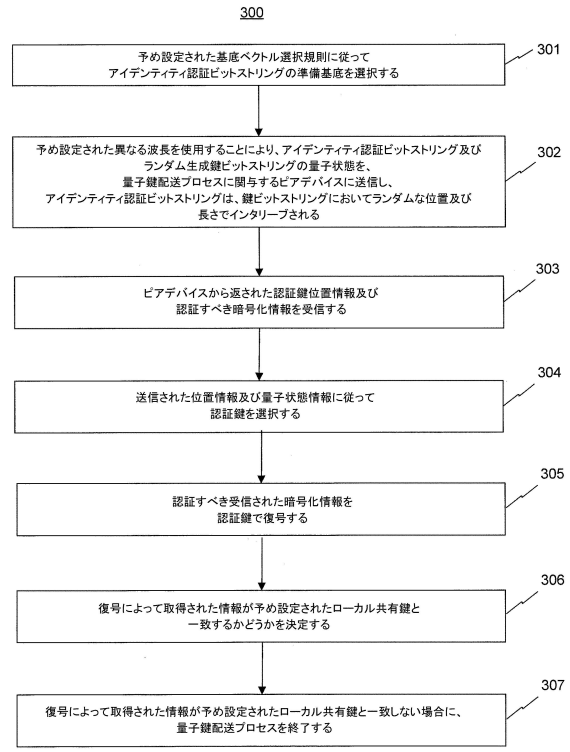
【図１】



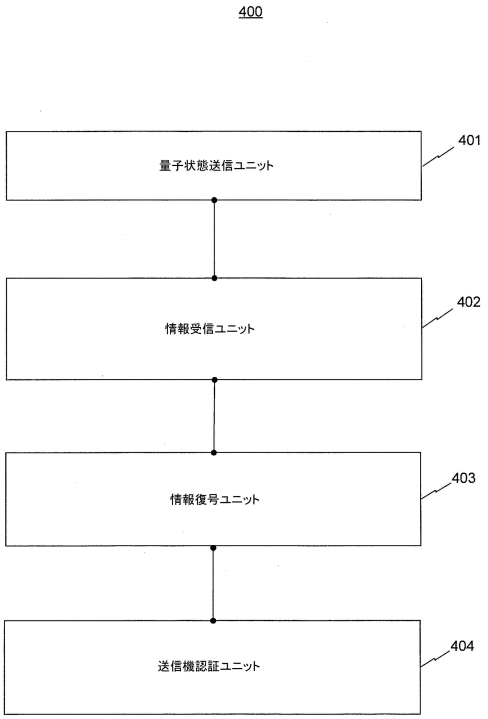
【図２】



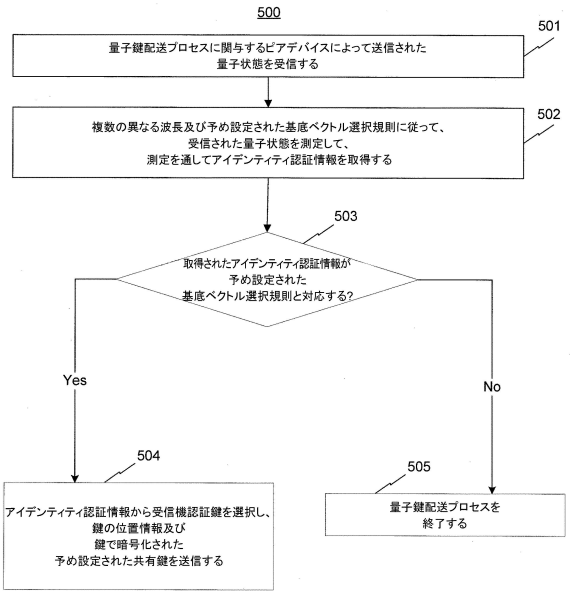
【図３】


300
予め設定された基底ベクトル選択規則に従って
アイデンティティ認証ビットストリングの準備基底を選択する
301
予め設定された異なる波長を使用することにより、アイデンティティ認証ビットストリング及び
ランダム生成鍵ビットストリングの量子状態を、
量子鍵配送プロセスに関与するピアデバイスに送信し、
アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置及び
長さでインタリーブされる
302
ピアデバイスから返された認証鍵位置情報及び
認証すべき暗号化情報を受信する
303
送信された位置情報及び量子状態情報に従って
認証鍵を選択する
304
認証すべき受信された暗号化情報を
認証鍵で復号する
305
復号によって取得された情報が予め設定されたローカル共有鍵と
一致するかどうかを決定する
306
復号によって取得された情報が予め設定されたローカル共有鍵と一致しない場合に、
量子鍵配送プロセスを終了する
307

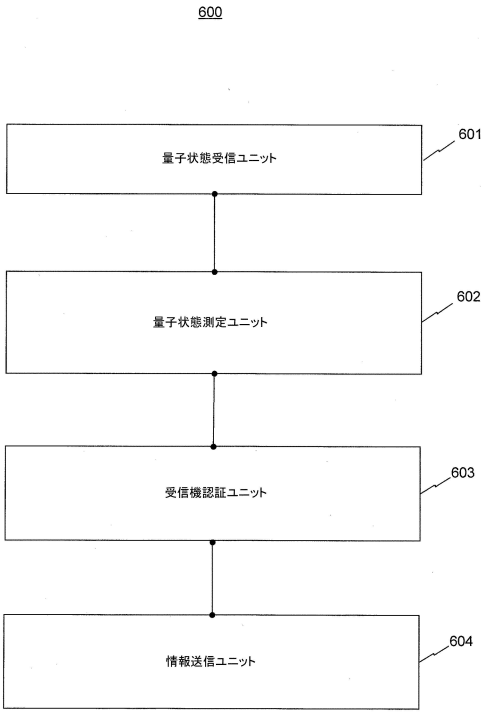
【図４】


400
量子状態送信ユニット
401
情報受信ユニット
402
情報復号ユニット
403
送信機認証ユニット
404

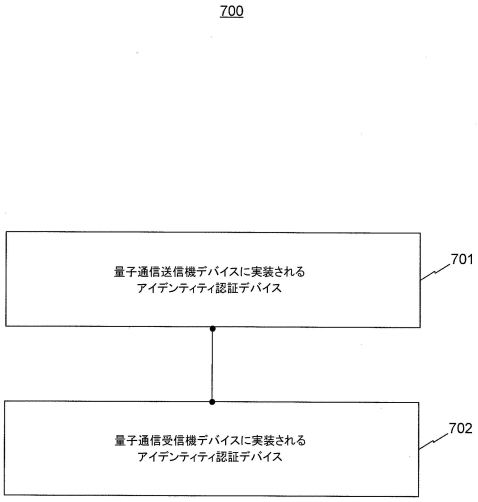
【図５】


500
量子鍵配送プロセスに関与するピアデバイスによって送信された
量子状態を受信する
501
複数の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、
受信された量子状態を測定して、
測定を通してアイデンティティ認証情報を取得する
502
503
取得されたアイデンティティ認証情報が
予め設定された
基底ベクトル選択規則と対応する?
Yes
No
504
アイデンティティ認証情報から受信機認証鍵を選択し、
鍵の位置情報及び
鍵で暗号化された
予め設定された共有鍵を送信する
505
量子鍵配送プロセスを
終了する

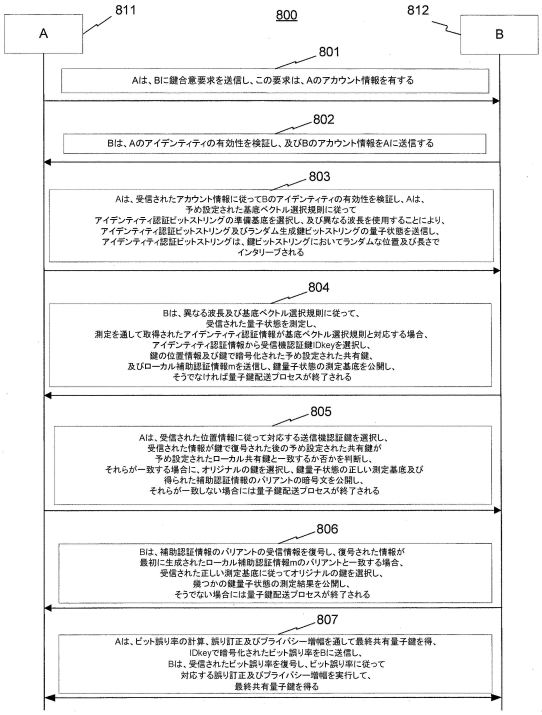
【図６】


600
量子状態受信ユニット
601
量子状態測定ユニット
602
受信機認証ユニット
603
情報送信ユニット
604

【図７】


700
量子通信送信機デバイスに実装される
アイデンティティ認証デバイス
701
量子通信受信機デバイスに実装される
アイデンティティ認証デバイス
702

【図８】


800
A
811
B
812
801
Aは、Bに鍵合意要求を送信し、この要求は、Aのアカウント情報を有する
802
Bは、Aのアイデンティティの有効性を検証し、及びBのアカウント情報をAに送信する
803
Aは、受信されたアカウント情報に従ってBのアイデンティティの有効性を検証し、Aは、
予め設定された基底ベクトル選択規則に従って
アイデンティティ認証ビットストリングの準備基底を選択し、及び異なる波長を使用することにより、
アイデンティティ認証ビットストリング及びランダム生成鍵ビットストリングの量子状態を送信し、
アイデンティティ認証ビットストリングは、鍵ビットストリングにおいてランダムな位置及び長さで
インタリーブされる
804
Bは、異なる波長及び基底ベクトル選択規則に従って、
受信された量子状態を測定し、
測定を通して取得されたアイデンティティ認証情報が基底ベクトル選択規則と対応する場合、
アイデンティティ認証情報から受信機認証鍵IDkeyを選択し、
鍵の位置情報及び鍵で暗号化された予め設定された共有鍵、
及びローカル補助認証情報mを送信し、鍵量子状態の測定基底を公開し、
そうでなければ量子鍵配送プロセスが終了される
805
Aは、受信された位置情報に従って対応する送信機認証鍵を選択し、
受信された情報が鍵で復号された後の予め設定された共有鍵が
予め設定されたローカル共有鍵と一致するか否かを判断し、
それらが一致する場合に、オリジナルの鍵を選択し、鍵量子状態の正しい測定基底及び
得られた補助認証情報のバリアントの暗号文を公開し、
それらが一致しない場合には量子鍵配送プロセスが終了される
806
Bは、補助認証情報のバリアントの受信情報を復号し、復号された情報が
最初に生成されたローカル補助認証情報mのバリアントと一致する場合、
受信された正しい測定基底に従ってオリジナルの鍵を選択し、
幾つかの鍵量子状態の測定結果を公開し、
そうでない場合には量子鍵配送プロセスが終了される
807
Aは、ビット誤り率の計算、誤り訂正及びプライバシー増幅を通して最終共有量子鍵を得、
IDkeyで暗号化されたビット誤り率をBに送信し、
Bは、受信されたビット誤り率を復号し、ビット誤り率に従って
対応する誤り訂正及びプライバシー増幅を実行して、
最終共有量子鍵を得る

フロントページの続き

(72)発明者 フー，インファン
中華人民共和国，３１１１２１，ハンチョウ，ユ ハン ディストリクト，ウェスト ウェン イ ロード ナンバー ９６９，ビルディング ３，５／エフ，アリババ グループ リーガル デパートメント
(72)発明者 リウ，シュアンリン
中華人民共和国，３１１１２１，ハンチョウ，ユ ハン ディストリクト，ウェスト ウェン イ ロード ナンバー ９６９，ビルディング ３，５／エフ，アリババ グループ リーガル デパートメント

審査官 青木 重徳

(56)参考文献 特開２００７－１１６２１６（ＪＰ，Ａ）
特開２０００－２０１１４４（ＪＰ，Ａ）
米国特許出願公開第２０１０／００２７７９４（ＵＳ，Ａ１）
中国特許出願公開第１０２９４６３１３（ＣＮ，Ａ）
韓国公開特許第１０－２０１２－００７１８８３（ＫＲ，Ａ）
Yu Liu et al., A discussion on a quantum key remote distribution scheme not based on the quantum entanglement state, PROCEEDINGS OF SPIE, ［オンライン］，２００４年 ４月１５日，Vol. 5282, p. 889-897, ［検索日 令和１年１０月２９日］、インターネット，ＵＲＬ，<https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5282/0000/A-discussion-on-a-quantum-key-remote-distribution-scheme-not/10.1117/12.523229.full>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／１２
Ｈ０４Ｌ ９／３２
Ｈ０４Ｂ １０／６０