(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7440108号
(P7440108)

(45)発行日　令和6年2月28日(2024.2.28)

(24)登録日　令和6年2月19日(2024.2.19)

(51)国際特許分類
Ｈ０４Ｌ　9/12 (2006.01)

ＦＩ
Ｈ０４Ｌ　9/12

請求項の数　15　外国語出願　（全32頁）

(21)出願番号　特願2022-9574(P2022-9574)
(22)出願日　令和4年1月25日(2022.1.25)
(65)公開番号　特開2022-115095(P2022-115095A)
(43)公開日　令和4年8月8日(2022.8.8)
審査請求日　令和4年7月11日(2022.7.11)
(31)優先権主張番号　21153846
(32)優先日　令和3年1月27日(2021.1.27)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　521124319
テラ クアンタム アーゲー
ＴＥＲＲＡ ＱＵＡＮＴＵＭ ＡＧ
スイス連邦、ザンクト ガレン、コルン ハウス シュトラーセ ２５
(74)代理人　100109210
弁理士　新居 広守
(72)発明者　クロンバリ・ドミトリー
スイス連邦、９４００ ロールシャハ、ザンクト・ガラーシュトラーセ １６エー、テラ クアンタム アーゲー内
審査官　行田 悦資

最終頁に続く

(54)【発明の名称】　量子鍵配送のための方法及びシステム

(57)【特許請求の範囲】

【請求項１】

量子鍵配送のための方法であって、前記方法が、複数のデータ処理装置を備えるシステムにおいて、

－第１のデータ処理装置（１０）及び第２のデータ処理装置（１１）が初期鍵を取得するステップと、

－前記第２のデータ処理装置（１１）が、複数の量子状態を含む量子信号を取得するステップと、

－前記第２のデータ処理装置（１１）において、複数の量子測定パラメータを求めるステップと、

－前記第２のデータ処理装置（１１）において、前記複数の量子測定パラメータを使用して前記複数の量子状態を量子測定することにより、生信号を求めるステップと、

－前記第２のデータ処理装置（１１）において、前記複数の量子測定パラメータのうちの少なくとも１つを示す暗号化信号を、前記初期鍵を使用して生成し、次いで前記暗号化信号を前記第１のデータ処理装置（１０）に送信するステップと、

－前記第１のデータ処理装置（１０）又は前記第２のデータ処理装置（１１）のうちの少なくとも一方において、前記暗号化信号から照合信号を求めるステップと、

－前記第１のデータ処理装置（１０）又は前記第２のデータ処理装置（１１）のうちの少なくとも一方において、前記照合信号を補正することにより、前記照合信号から共有鍵を特定するステップと、を含み、

前記暗号化信号から前記照合信号を求めるステップは、前記初期鍵を用いて前記暗号化信号を復号して、前記照合信号を求めるステップを含む、
量子鍵配送のための方法。
【請求項２】
－前記第１のデータ処理装置（１０）において、複数の量子生成パラメータを求めるステップと、
－前記第１のデータ処理装置（１０）において、前記複数の量子生成パラメータを使用して第１の生信号から、複数の第１の量子状態を含む第１の量子信号を生成するステップと、
－前記第１のデータ処理装置（１０）から前記第２のデータ処理装置（１１）に前記第１の量子信号を送信することにより、前記複数の量子状態を含む前記量子信号を前記第２のデータ処理装置（１１）が取得するステップと、
－前記第１のデータ処理装置（１０）において、前記複数の量子生成パラメータのうちの少なくとも１つを示す第１の暗号化信号を、前記初期鍵を使用して生成し、次いで前記第１の暗号化信号を前記第２のデータ処理装置（１１）に送信するステップと、
－前記第２のデータ処理装置（１１）において、前記生信号及び前記第１の暗号化信号から前記照合信号を求めるステップと、
－前記第１のデータ処理装置（１）において、前記第１の生信号及び前記暗号化信号から第１の照合信号を求めるステップと、
のうちの少なくとも１つをさらに含む、請求項１に記載の方法。
【請求項３】
前記複数の量子測定パラメータのうちの少なくとも１つ及び／又は前記複数の量子生成パラメータのうちの少なくとも１つが、量子基底設定値を含む、請求項２に記載の方法。
【請求項４】
－前記第２のデータ処理装置（１１）における前記生信号の桁位置がそれぞれ、前記複数の量子測定パラメータのうちの１つと、前記複数の量子状態のうちの１つとに対応しているか、
－前記複数の量子測定パラメータのうちの対応する１つと前記第１の暗号化信号からの前記量子生成パラメータのうちの対応する１つとが一致しない場合、前記生信号における前記桁位置のうちの１つを破棄することにより、前記第２のデータ処理装置（１１）において前記生信号及び前記第１の暗号化信号から前記照合信号が求められるか、
－前記第１のデータ処理装置（１０）における前記第１の生信号の第１の桁位置がそれぞれ、前記複数の量子生成パラメータのうちの１つと、前記複数の第１の量子状態のうちの１つとに対応しているか、又は
－前記暗号化信号からの前記複数の量子測定パラメータのうちの対応する１つと前記量子生成パラメータのうちの対応する１つとが一致しない場合、前記第１の生信号における前記第１の桁位置のうちの１つを破棄することにより、前記第１のデータ処理装置（１０）において前記第１の生信号及び前記暗号化信号から前記第１の照合信号が求められるか、
のうちの少なくとも１つが実現される、請求項２又は３に記載の方法。
【請求項５】
－前記第１のデータ処理装置（１０）において、前記第１の照合信号から第１のパリティデータを生成するステップと、
－前記第１のデータ処理装置（１０）において、前記第１のパリティデータを前記初期鍵で暗号化して、第１の暗号化されたパリティデータにし、次いで前記第１の暗号化されたパリティデータを前記第２のデータ処理装置（１１）に送信するステップと、
－前記第２のデータ処理装置（１１）において、前記照合信号から第２のパリティデータを生成するステップと、
－前記第２のデータ処理装置（１１）において、前記第２のパリティデータを前記初期鍵で暗号化して、第２の暗号化されたパリティデータにし、次いで前記第２の暗号化されたパリティデータを前記第１のデータ処理装置（１０）に送信するステップと、

－前記第１のデータ処理装置（１０）及び前記第２のデータ処理装置（１１）において、前記第１のパリティデータ及び前記第２のパリティデータを使用して前記第１の照合信号と前記照合信号との差分を求めるステップと、
－前記第１のデータ処理装置（１０）において、前記第１の照合信号と前記照合信号との前記差分に対して前記第１の照合信号を補正することにより、前記第１の照合信号から前記共有鍵を特定し、次いで前記第２のデータ処理装置（１１）において、前記照合信号を前記共有鍵として特定するステップと、
のうちの少なくとも１つをさらに含む、請求項２から４の少なくともいずれか一項に記載の方法。
【請求項６】
－前記第１のパリティデータが、前記第１の照合信号における第１のデータブロックの第１のパリティビットを含み、また、前記第２のパリティデータが、前記照合信号における第２のデータブロックの第２のパリティビットを含むか、あるいは
－前記第１のパリティデータが、前記第１の照合信号の第１のシンドロームを含み、また、前記第２のパリティデータが、前記照合信号の第２のシンドロームを含む、請求項５に記載の方法。
【請求項７】
－前記第１のデータ処理装置（１０）において、前記第１の照合信号から第１の誤り情報を生成し、好ましくは、前記第１の誤り情報を前記初期鍵で暗号化して、第１の暗号化された誤り情報にし、さらに好ましくは、前記第１の誤り情報又は前記第１の暗号化された誤り情報を前記第２のデータ処理装置（１１）に送信するステップと、
－前記第２のデータ処理装置（１１）において、前記照合信号から第２の誤り情報を生成し、好ましくは、前記第２の誤り情報を前記初期鍵で暗号化して、第２の暗号化された誤り情報にし、さらに好ましくは、前記第２の誤り情報又は前記第２の暗号化された誤り情報を前記第１のデータ処理装置（１０）に送信するステップと、
－前記第１のデータ処理装置（１０）及び前記第２のデータ処理装置（１１）において、前記第１の誤り情報及び前記第２の誤り情報から、前記第１の照合信号と前記照合信号との誤り推定値を求めるステップと、
－前記第１の誤り情報及び前記第２の誤り情報を使用して、前記第１の照合信号及び前記照合信号の誤り部分を破棄するステップと、
のうちの少なくとも１つをさらに含む、請求項２から６の少なくともいずれか一項に記載の方法。
【請求項８】
－前記第１のデータ処理装置（１０）及び／又は前記第２のデータ処理装置（１１）において、ハッシュデータを前記初期鍵で暗号化して暗号化ハッシュデータにするステップと、
－前記暗号化ハッシュデータを前記第２のデータ処理装置（１１）及び／又は前記第１のデータ処理装置（１０）に送信するステップと、
－前記第１のデータ処理装置（１０）及び前記第２のデータ処理装置（１１）において、前記ハッシュデータを使用してハッシュ方式を適用することにより、前記共有鍵から増幅鍵を特定するステップと、
をさらに含む、請求項５または６の少なくともいずれか一項に記載の方法。
【請求項９】
前記第１のパリティデータ、前記第２のパリティデータ、又は前記ハッシュデータのうちの少なくとも１つが、前記照合信号、前記第１の照合信号、前記共有鍵、又は前記増幅鍵のうちの少なくとも１つと対応付けられている相関データを含む、請求項８に記載の方法。
【請求項１０】
－前記第１のデータ処理装置（１０）において、前記第１の照合信号、前記共有鍵、又は前記増幅鍵のうちの少なくとも１つと対応付けられていない第１の無相関パリティデー

タを生成し、次いで前記第１の無相関パリティデータを前記第２のデータ処理装置（１１）に送信するステップと、
－前記第２のデータ処理装置（１１）において、前記照合信号、前記共有鍵、又は前記増幅鍵のうちの少なくとも１つと対応付けられていない第２の無相関パリティデータを生成し、次いで前記第２の無相関パリティデータを前記第１のデータ処理装置（１０）に送信するステップと、
のうちの少なくとも１つをさらに含む、請求項８又は９に記載の方法。
【請求項１１】
－前記第１のデータ処理装置（１０）及び前記第２のデータ処理装置（１１）が第２の初期鍵を取得するステップと、
－前記第２の初期鍵によって、前記第１のデータ処理装置（１０）及び前記第２のデータ処理装置（１１）が認証するステップと、
をさらに含む、請求項１から１０の少なくともいずれか一項に記載の方法。
【請求項１２】
前記共有鍵が、前記第１のデータ処理装置（１０）及び第３のデータ処理装置においてのみ特定され、前記方法が、
－前記第３のデータ処理装置が初期鍵を取得するステップと、
－前記第３のデータ処理装置において、複数の追加の量子生成パラメータを求めるステップと、
－前記第３のデータ処理装置において、前記複数の追加の量子生成パラメータを使用して、第３の生信号から複数の第３の量子状態を含む第３の量子信号を生成するステップと、
－前記第３の量子信号を前記第３のデータ処理装置から前記第２のデータ処理装置（１１）に送信するステップと、
をさらに含む、請求項１から１１の少なくともいずれか一項に記載の方法。
【請求項１３】
前記複数の量子状態のそれぞれが、前記第１のデータ処理装置（１０）と前記第２のデータ処理装置（１１）との間の複数の共有もつれ量子状態のうちの１つの短縮状態である、請求項１から１２の少なくともいずれか一項に記載の方法。
【請求項１４】
前記初期鍵が、ＲＳＡ方式又はディフィー・ヘルマン方式を用いて供給される、請求項１から１３の少なくともいずれか一項に記載の方法。
【請求項１５】
複数のデータ処理装置を備え、かつ、
－第１のデータ処理装置（１０）及び第２のデータ処理装置（１１）に初期鍵を供給するステップと、
－前記第２のデータ処理装置（１１）に、複数の量子状態を含む量子信号を供給するステップと、
－前記第２のデータ処理装置（１１）において、複数の量子測定パラメータを求めるステップと、
－前記第２のデータ処理装置（１１）において、前記複数の量子測定パラメータを使用して前記複数の量子状態を量子測定することにより、生信号を求めるステップと、
－前記第２のデータ処理装置（１１）において、前記複数の量子測定パラメータのうちの少なくとも１つを示す暗号化信号を、前記初期鍵を使用して生成し、次いで前記暗号化信号を前記第１のデータ処理装置（１０）に送信するステップと、
－前記第１のデータ処理装置（１０）又は前記第２のデータ処理装置（１１）のうちの少なくとも一方において、前記暗号化信号から照合信号を求めるステップと、
－前記第１のデータ処理装置（１０）又は前記第２のデータ処理装置（１１）のうちの少なくとも一方において、前記照合信号を補正することにより、前記照合信号から共有鍵を特定するステップと、を実行するように構成されており、
前記暗号化信号から前記照合信号を求めるステップは、前記初期鍵を用いて前記暗号化

信号を復号して、前記照合信号を求めるステップを含む、
量子鍵配送のためのシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、量子鍵配送のための方法に関する。さらに、量子鍵配送のためのシステムが開示される。
【背景技術】
【０００２】
古典相関における量子固定では、第１のデータ処理装置（「アリス」）は、長さｍのメッセージａを第２のデータ処理装置（「ボブ」）に送信する。このメッセージａは、第１のデータ処理装置が長さ｜Ｋ｜の鍵ｋを第２のデータ処理装置にさらに送信するまで、秘密に保たれることになる。メッセージａを依然としてセキュアに暗号化できるようにする一方で、鍵ｋをどれだけ短縮することができるかを判断することが重要である。これら第１及び第２のデータ処理装置が古典的リソースのみを備える場合、鍵ｋは、メッセージａとほぼ同じ長さ、即ち、
【数１】
$$m \approx |K|$$

となる必要がある。典型的な一実装形態は、ワンタイムパッドによって表される。この場合、セキュリティは情報因果律の原理に従うことになり、ｌビットを送信することにより、第１のデータ処理装置と第２のデータ処理装置との相関をｌビットよりも増大させることはできない。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
しかしながら、量子相関の場合、この情報因果律の原理に違反する恐れがあるため、セキュリティ要求度を維持しながら、可能な限り短い鍵長を求めることになる。これとは逆に、鍵長を一定に保つことで、より多くの情報がセキュアに送信され得る。それでもなお、より高度な情報伝送を実現することが望ましい。
【０００４】
本開示の目的は、量子鍵配送を通じてデータを送信するための改良された技法を提供することである。
【課題を解決するための手段】
【０００５】
この課題を解決するために、独立請求項に従って量子鍵配送のための方法及びシステムが提供される。従属請求項には、さらに別の実施形態が開示されている。
【０００６】
一態様によれば、量子鍵配送のための方法が提供され、本方法は、複数のデータ処理装置を備えるシステムにおいて、第１のデータ処理装置及び第２のデータ処理装置に初期鍵を供給するステップと、第２のデータ処理装置に、複数の量子状態を含む量子信号を供給するステップと、第２のデータ処理装置において、複数の量子測定パラメータを求めるステップと、第２のデータ処理装置において、これら複数の量子測定パラメータを使用して複数の量子状態を量子測定することにより、生信号を求めるステップと、第２のデータ処理装置において、複数の量子測定パラメータのうちの少なくとも１つを示す暗号化信号を、初期鍵を使用して生成し、次いでこの暗号化信号を第１のデータ処理装置に送信するステップと、第１のデータ処理装置又は第２のデータ処理装置のうちの少なくとも一方において、この暗号化信号から照合信号を求めるステップと、第１のデータ処理装置又は第２のデータ処理装置のうちの少なくとも一方において、この第１の照合信号を補正することにより、照合信号から共有鍵を特定するステップと、を含む。

【０００７】
別の態様によれば、量子鍵配送のためのシステムが提供され、本システムは複数のデータ処理装置を備え、かつ、第１のデータ処理装置及び第２のデータ処理装置に初期鍵を供給するステップと、第２のデータ処理装置に、複数の量子状態を含む量子信号を供給するステップと、第２のデータ処理装置において、複数の量子測定パラメータを求めるステップと、第２のデータ処理装置において、これら複数の量子測定パラメータを使用して複数の量子状態を量子測定することにより、生信号を求めるステップと、第２のデータ処理装置において、複数の量子測定パラメータのうちの少なくとも１つを示す暗号化信号を、初期鍵を使用して生成し、次いでこの暗号化信号を第１のデータ処理装置に送信するステップと、第１のデータ処理装置又は第２のデータ処理装置のうちの少なくとも一方において、この暗号化信号から照合信号を求めるステップと、第１のデータ処理装置又は第２のデータ処理装置のうちの少なくとも一方において、第１の照合信号を補正することにより、この照合信号から共有鍵を特定するステップと、を実行するように構成されている。
【０００８】
当該生信号を、第２の生信号とすることができる。当該暗号化信号を、第２の暗号化信号とすることができる。当該照合信号を、第２の照合信号とすることができる。複数の量子状態を、複数の第２の量子状態とすることができる。当該量子信号は、第２の量子信号であってもよい。
【０００９】
本方法は、ＢＢ８４（ベネット（Ｂｅｎｎｅｔｔ）とブラサール（Ｂｒａｓｓａｒｄ）が１９８４年に提案）プロトコル、Ｂ９２（ベネットが１９９２年に提案）プロトコル、量子もつれベースの量子鍵配送プロトコル、測定装置に依存しない量子鍵配送プロトコル、又はツインフィールド量子鍵配送プロトコルのうちの少なくとも１つに従ってもよい。当該量子信号は光ファイバを介して送信されてもよく、あるいは無線を介して送信されてもよい。
【００１０】
本方法は、第１のデータ処理装置において、複数の量子生成パラメータを求めるステップと、第１のデータ処理装置において、これら複数の量子生成パラメータを使用して第１の生信号から、複数の第１の量子状態を含む第１の量子信号を生成するステップと、第１のデータ処理装置から第２のデータ処理装置にこの第１の量子信号を送信することにより、複数の量子状態を含む量子信号を第２のデータ処理装置に供給するステップと、第１のデータ処理装置において、複数の量子生成パラメータのうちの少なくとも１つを示す第１の暗号化信号を、初期鍵を使用して生成し、次いでこの第１の暗号化信号を第２のデータ処理装置に送信するステップと、第２のデータ処理装置において、生信号及び第１の暗号化信号から照合信号を求めるステップと、第１のデータ処理装置において、第１の生信号及び暗号化信号から第１の照合信号を求めるステップと、のうちの少なくとも１つをさらに含んでいてもよい。
【００１１】
これら複数の量子状態は、複数の第１の量子状態それぞれをユニタリ発展させることにより、複数の第１の量子状態から取得され得る。暗号化信号、第１の暗号化信号、又は初期鍵で暗号化されたさらに別の信号を送信するステップは、プライベート通信チャネル内での送信を含んでいてもよい。
【００１２】
複数の量子状態それぞれ及び／又は複数の第１の量子状態それぞれは、フォトニック量子状態であってもよい。複数の量子状態それぞれ及び／又は複数の第１の量子状態それぞれは、光子偏光状態であってもよい。
【００１３】
複数の量子測定パラメータのうちの少なくとも１つ及び／又は複数の量子生成パラメータのうちの少なくとも１つは、量子基底設定値を含んでいてもよい。複数の量子測定パラメータのうちの少なくとも１つ及び／又は複数の量子生成パラメータのうちの少なくとも

１つは、例えば不確定結果を示す、ある種の測定結果をさらに含んでいてもよい。
【００１４】
この量子基底設定は、水平偏光基底又は垂直偏光基底で測定するステップ、あるいは反対角偏光基底又は対角偏光基底で測定するステップを含んでいてもよい。
【００１５】
第２のデータ処理装置における生信号の桁位置はそれぞれ、複数の量子測定パラメータのうちの１つ及び／又は複数の量子状態のうちの１つに対応してもよい。複数の量子測定パラメータのうちの対応する１つと第１の暗号化信号の量子生成パラメータのうちの対応する１つとが一致しない場合、生信号の桁位置のうちの１つを破棄することにより、第２のデータ処理装置において生信号及び第１の暗号化信号から照合信号が求められてもよい。第１のデータ処理装置における第１の生信号の第１の桁位置はそれぞれ、複数の量子生成パラメータのうちの１つと、複数の第１の量子状態のうちの１つとに対応してもよい。暗号化信号からの複数の量子測定パラメータのうちの対応する１つと量子生成パラメータのうちの対応する１つとが一致しない場合、第１の生信号の第１の桁位置のうちの１つを破棄することにより、第１のデータ処理装置において第１の生信号及び暗号化信号から第１の照合信号が求められてもよい。
【００１６】
代替的に又は付加的に、量子生成パラメータのうちの対応する１つが破棄フラグを含む場合、生信号の桁位置のうちの１つを破棄することにより、第２のデータ処理装置において生信号及び量子生成パラメータから照合信号が求められてもよい。この破棄フラグは、例えば不確定結果を示すことに相当してもよい。また、第１の暗号化信号からの複数の量子測定パラメータのうちの対応する１つと暗号化信号の量子生成パラメータのうちの対応する１つとが破棄フラグを含む場合、第１の生信号の第１の桁位置のうちの１つを破棄することにより、第１のデータ処理装置において第１の生信号及び暗号化信号から第１の照合信号が求められてもよい。
【００１７】
本方法は、第１のデータ処理装置において、第１の照合信号から第１のパリティデータを生成するステップと、第１のデータ処理装置において、この第１のパリティデータを初期鍵で暗号化して、第１の暗号化されたパリティデータにし、次いでこの第１の暗号化されたパリティデータを第２のデータ処理装置に送信するステップと、第２のデータ処理装置において、照合信号から第２のパリティデータを生成するステップと、第２のデータ処理装置において、この第２のパリティデータを初期鍵で暗号化して、第２の暗号化されたパリティデータにし、次いでこの第２の暗号化されたパリティデータを第１のデータ処理装置に送信するステップと、第１のデータ処理装置及び第２のデータ処理装置において、第１のパリティデータ及び第２のパリティデータを使用して第１の照合信号と照合信号との差分を求めるステップと、第１のデータ処理装置において、第１の照合信号と照合信号との差分に対して第１の照合信号を補正することにより、第１の照合信号から共有鍵を特定し、次いで第２のデータ処理装置において、この照合信号を共有鍵として特定するステップと、のうちの少なくとも１つをさらに含んでいてもよい。
【００１８】
本方法は、第１のデータ処理装置において、第１の照合信号を共有鍵として特定し、次いで第２のデータ処理装置において、第１の照合信号と照合信号との差分に対して照合信号を補正することにより、照合信号から共有鍵を特定するステップをさらに含んでいてもよい。
【００１９】
第１のパリティデータは、第１の照合信号における第１のデータブロックの第１のパリティビットを含んでいてもよく、また、第２のパリティデータは、照合信号における第２のデータブロックの第２のパリティビットを含んでいてもよい。あるいは、第１のパリティデータは、第１の照合信号の第１のシンドロームを含んでいてもよく、また、第２のパリティデータは、照合信号の第２のシンドロームを含んでいてもよい。

【００２０】
第１のシンドロームは、複数の検査行列のうちの１つを第１の照合信号の第１の部分に乗算することによって求められてもよい。この第２のシンドロームは、複数の検査行列のうちの１つを第２の照合信号の第２の部分に乗算することによって求められてもよい。これら複数の検査行列のうちの少なくとも１つを示す検査行列情報は、第１のデータ処理装置又は第２のデータ処理装置において求められてもよい。この検査行列情報は、自身を暗号化せずに送信されてもよい。複数の検査行列、第１のシンドローム、及び／又は第２のシンドロームのそれぞれは、２値化されていてもよい。
【００２１】
第１の照合信号及び／又は照合信号を補正するステップは、誤り桁位置を特定するステップを含んでいてもよい。この誤り桁位置は、誤りベクトルを使用して特定されてもよい。この誤りベクトルは、複数の検査行列のうちの１つ及び１つの誤りシンドロームから求められてもよい。この誤りシンドロームは、第１のシンドロームと第２のシンドロームとを２進加算することによって求められてもよい。
【００２２】
誤り桁位置は、２分探索によって同様に特定されてもよい。この２分探索は、第１の照合信号と照合信号とをそれぞれ第１のデータブロックと第２のデータブロックとに反復的に分割し、次いで第１のデータブロックの第１のパリティ値と第２のデータブロックの第２のパリティ値とを求めて、これらを比較するステップとを含んでいてもよい。
【００２３】
本方法は、第１のデータ処理装置において、第１の照合信号から第１の誤り情報を生成し、好ましくは、この第１の誤り情報を初期鍵で暗号化して、第１の暗号化された誤り情報にし、さらに好ましくは、第１の誤り情報又は第１の暗号化された誤り情報を第２のデータ処理装置に送信するステップと、第２のデータ処理装置において、照合信号から第２の誤り情報を生成し、好ましくは、この第２の誤り情報を初期鍵で暗号化して、第２の暗号化された誤り情報にし、さらに好ましくは、第２の誤り情報又は第２の暗号化された誤り情報を第１のデータ処理装置に送信するステップと、第１のデータ処理装置及び第２のデータ処理装置において、第１の誤り情報及び第２の誤り情報から、第１の照合信号と照合信号との誤り推定値を求めるステップと、第１の誤り情報及び第２の誤り情報を使用して、第１の照合信号及び照合信号の誤り部分を破棄するステップと、のうちの少なくとも１つをさらに含む。
【００２４】
第１の誤り情報及び第２の誤り情報は、第１の照合信号の第１のパリティビット又はその一部と、第２の照合信号の第２のパリティビット又はその一部とをそれぞれ含んでいてもよい。これら第１の誤り情報及び第２の誤り情報は、第１の照合信号及び第２の照合信号と対応付けられてもよい。
【００２５】
本方法は、第１のデータ処理装置においてハッシュデータを求め、このハッシュデータを初期鍵で暗号化して暗号化ハッシュデータにするステップと、この暗号化ハッシュデータを第２のデータ処理装置に送信するステップと、をさらに含んでいてもよい。本方法は、第２のデータ処理装置においてハッシュデータを求め、このハッシュデータを初期鍵で暗号化して暗号化ハッシュデータにするステップと、この暗号化ハッシュデータを第１のデータ処理装置に送信するステップと、をさらに含んでいてもよい。本方法は、第１のデータ処理装置及び第２のデータ処理装置において、ハッシュデータを使用してハッシュ方式を適用することにより、共有鍵から増幅鍵を特定するステップをさらに含んでいてもよい。
【００２６】
このハッシュデータは、２進テプリッツ行列におけるランダム抽出を示してもよい。
【００２７】
第１のパリティデータ、第２のパリティデータ、又はハッシュデータのうちの少なくと

も１つは、照合信号、第１の照合信号、共有鍵、又は増幅鍵のうちの少なくとも１つと対応付けられている相関データを含んでいてもよい。

【００２８】

本方法は、第１のデータ処理装置において、第１の照合信号、共有鍵、又は増幅鍵のうちの少なくとも１つと対応付けられていない第１の無相関パリティデータを生成し、次いでこの第１の無相関パリティデータを第２のデータ処理装置に送信するステップと、第２のデータ処理装置において、照合信号、共有鍵、又は増幅鍵のうちの少なくとも１つと対応付けられていない第２の無相関パリティデータを生成し、次いでこの第２の無相関パリティデータを第１のデータ処理装置に送信するステップと、のうちの少なくとも１つをさらに含んでいてもよい。

【００２９】

あるいは、第１の無相関パリティデータと第２の無相関パリティデータとを同様に暗号化してから、これらを送信してもよい。

【００３０】

これらの無相関データは、第１及び第２の照合信号を第１のデータブロックと第２のデータブロックとに分割することを示す、データブロック情報を含んでいてもよい。

【００３１】

本方法は、第１のデータ処理装置及び第２のデータ処理装置に第２の初期鍵を供給するステップと、この第２の初期鍵によって、第１のデータ処理装置及び第２のデータ処理装置を認証するステップと、をさらに含んでいてもよい。

【００３２】

この第２の初期鍵は、初期鍵と異なっていてもよい。あるいは、この初期鍵と第２の初期鍵とは同一である。例えば、第２の初期鍵で生成された署名を送信される古典信号それぞれに付加することにより、送信される古典信号を認証することができる。

【００３３】

共有鍵及び／又は増幅鍵は、第１のデータ処理装置及び第３のデータ処理装置においてのみ特定されてもよい。本方法は、第３のデータ処理装置において、複数の追加の量子生成パラメータを求めるステップと、第３のデータ処理装置において、これら複数の追加の量子生成パラメータを使用して、第３の生信号から複数の第３の量子状態を含む第３の量子信号を生成するステップと、この第３の量子信号を第３のデータ処理装置から第２のデータ処理装置に送信するステップと、をさらに含んでいてもよい。

【００３４】

これら複数の量子状態のそれぞれは、第１のデータ処理装置と第２のデータ処理装置との間の複数の共有もつれ量子状態のうちの１つの短縮状態であってもよい。

【００３５】

複数の共有もつれ量子状態のそれぞれは、もつれ光子対を含み得る。

【００３６】

初期鍵は、ＲＳＡ（リベスト・シャミア・エーデルマン（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ））方式又はディフィー・ヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）方式を用いて供給されてもよい。初期鍵はまた、例えば信頼できるクーリエを使用して、異なる方法で配送されてもよい。この初期鍵は、第１のデータ処理装置及び第２のデータ処理装置に供給（配送）されてもよい。また、この初期鍵は、第３のデータ処理装置に供給されてもよい。

【００３７】

共有鍵又は増幅鍵を使用して、追加の古典メッセージが暗号化されてもよい。この暗号化は、ワンタイムパッド方式又は対称鍵方式、好ましくは高度暗号化標準（ａｄｖａｎｃｅｄ ｅｎｃｒｙｐｔｉｏｎ ｓｔａｎｄａｒｄ：ＡＥＳ）を用いて実行されてもよい。

【００３８】

第１のパリティデータ長及び／又は第２のパリティデータ長に共有鍵長が等しくてもよく、具体的には、第１のシンドローム長及び／又は第２のシンドローム長に等しくてもよ

い。あるいは、第１のパリティデータ長及び／又は第２のパリティデータ長に増幅鍵長が等しくてもよく、具体的には、第１のシンドローム長及び／又は第２のシンドローム長に等しくてもよい。

【００３９】

第１の生信号、生信号、第１の暗号化信号、暗号化信号、第１の照合信号、照合信号、共有鍵、又は増幅鍵のうちの少なくとも１つ、好ましくは、それぞれは古典信号であり得る。第１の生信号、生信号、第１の暗号化信号、暗号化信号、第１の照合信号、照合信号、共有鍵、又は増幅鍵のうちの少なくとも１つ、好ましくは、それぞれは２進値で構成され得、具体的には、桁位置ごとに１つの２進値を有し得る。初期鍵及び／又は第２の初期鍵は、第１のデータ処理装置及び第２のデータ処理装置のみ、そして必要に応じて第３のデータ処理装置に供給され得るが、外部データ処理装置には供給されない。

【００４０】

量子鍵配送のための方法に関する前述の実施形態は、量子鍵配送のためのシステムに対応して提供され得る。

【図面の簡単な説明】

【００４１】

以下では、例示として、図面を参照しながら実施形態について説明する。

【図１】量子鍵配送のためのシステム及び外部データ処理装置の配置を示すグラフィカル図である。

【図２】量子鍵配送のための方法を示すグラフィカル図である。

【図３】従来型の量子鍵配送と量子鍵配送のための本方法とを比較した図である。

【図４】従来型の量子鍵配送及び提案している本方法用に設けられた通信チャネル長の関数としてシミュレートされた、鍵レートを示すグラフ図である。

【発明を実施するための形態】

【００４２】

図１は、量子鍵配送のためのシステム及び外部データ処理装置１２の配置を示すグラフィカル図である。本システムは、第１のデータ処理装置１０（「アリス」）と、第２のデータ処理装置１１（「ボブ」）と、を備える。第１のデータ処理装置１０は第１の記憶装置１０ａを含み、第２のデータ処理装置１１は第２の記憶装置１１ａを含む。

【００４３】

第１のデータ処理装置１０と第２のデータ処理装置１１とは、例えば通信チャネル１３を介して古典信号及び／又は量子信号を交換することができる。通信チャネル１３は、量子信号を送るように構成された量子チャネルを含んでいてもよい。例えば、通信チャネル１３は光ファイバを含んでいてもよい。通信チャネル１３はまた、第１のデータ処理装置１０と第２のデータ処理装置１１との間の自由空間であり得る。通信チャネル１３は、古典信号を送信するための古典チャネルをさらに含んでいてもよい。光ファイバは、量子チャネルと古典チャネルとで共用されてもよい。あるいは、量子チャネルと古典チャネルとを離隔させることができる。

【００４４】

本システムは、複数の追加のデータ処理装置、具体的には、第３の記憶装置（図示せず）を有する第３のデータ処理装置を備えていてもよい。この第３のデータ処理装置は、通信チャネル１３に接続されてもよい。付加的に又は代替的に、第３のデータ処理装置は、別の通信チャネルを介して古典信号並びに／又は量子信号を第１のデータ処理装置１０及び／若しくは第２のデータ処理装置１１と交換することができる。

【００４５】

外部記憶装置１２ａを有する外部データ処理装置１２（「イブ」）は本システムの外部にあり、例えば接続部１４を介して通信チャネル１３にアクセスする可能性がある潜在的な盗聴装置を表す。外部データ処理装置１２は、通信チャネル１３を介して送信される古典信号及び／又は量子信号の少なくとも一方若しくはいずれかが外部データ処理装置１２によって受信及び／又は再送信されるように、通信チャネル１３に配置され得る。外部デ

ータ処理装置１２はまた、別の通信チャネルにアクセスする可能性がある。外部データ処理装置１２はまた、複数の追加の外部データ処理装置に接続され得、これら複数の外部データ処理装置はそれぞれ、通信チャネル１３にアクセスする可能性があり、かつ／又はこれら複数の外部データ処理装置はそれぞれ、第１のデータ処理装置１０若しくは第２のデータ処理装置１１の近傍に配置され得る。

【００４６】

第１の記憶装置１０ａ、第２の記憶装置１１ａ、第３の記憶装置及び外部記憶装置１２ａはそれぞれ、量子信号を記憶するように構成された量子メモリと、古典信号を記憶するように構成された古典メモリとを含む。この量子メモリは、光遅延線、制御された可逆な不均一広がり（ｃｏｎｔｒｏｌｌｅｄ ｒｅｖｅｒｓｉｂｌｅ ｉｎｈｏｍｏｇｅｎｅｏｕｓ ｂｒｏａｄｅｎｉｎｇ：ＣＲＩＢ）、Ｄｕａｎ－Ｌｕｋｉｎ－Ｃｉｒａｃ－Ｚｏｌｌｅｒ（ＤＬＣＺ））型方式、エコー抑制による再生（ｒｅｖｉｖａｌ ｏｆ ｓｉｌｅｎｃｅｄ ｅｃｈｏ：ＲＯＳＥ）、及び／又はハイブリッド光子エコーリフェージング（ｈｙｂｒｉｄ ｐｈｏｔｏｎ ｅｃｈｏ ｒｅｐｈａｓｉｎｇ：ＨＹＰＥＲ）を用いて設けられてもよい。

【００４７】

第１の、第２の、第３の、及び外部データ処理装置（１０、１１、１２）はそれぞれ、量子状態を送信及び／又は受信する手段を備える。

【００４８】

第１の古典データＸ（例えば、第１のデータ処理装置１０の第１の記憶装置１０ａ又は第３のデータ処理装置の第３の記憶装置内の）及び第２の古典データＹ（例えば、第２のデータ処理装置１１の第２の記憶装置１１ａ内の）における第１の古典相互情報量Ｉ（Ｘ：Ｙ）は、以下の（１）の式によって得られ、

$$I_{cl}(X:Y) = H(X) - H(X|Y), \quad (1)$$

【００４９】

その際、第１の古典データＸのシャノンエントロピーＨ（Ｘ）と第１の古典データＸのシャノンエントロピーＨ（Ｘ｜Ｙ）とは、第２の古典データＹを認識していることを条件とする。

【００５０】

第１のデータ処理装置１０と第２のデータ処理装置１１とが共に共有量子状態ρ_{AB}を含む場合、古典相互情報量I_{cl}（Ａ：Ｂ）の一般化が定義され得る。

【００５１】

以下の式（２）で得られる第１のデータＡ（例えば、第１の記憶装置１０ａ内の）及び第２のデータＢ（例えば、第２の記憶装置１１ａ内の）における第１の量子相互情報量Ｉ（Ａ：Ｂ）では、

$$I(A:B) = S(A) - S(A|B), \quad (2)$$

【００５２】

第１のデータＡ及び第２のデータＢのそれぞれは、量子情報量及び古典情報量の両方を含んでいてもよく、この第１の量子相互情報量は、シャノンエントロピーＨの代わりに、（フォン・ノイマン）エントロピーＳによって定義される。量子相関がない場合、第１の量子相互情報量Ｉ（Ａ：Ｂ）は、第１の古典相互情報量I_{cl}（Ａ：Ｂ）と一致する。

【００５３】

以下の式（３）で得られる第１のデータＡ及び第２のデータＢにおけるアクセス可能情報量I_{acc}（Ａ：Ｂ）は、

【数２】

$$I_{\mathrm{acc}}(A:B) = \max_{M_B} I(A:B) = S(\rho_A) - \min_{M_B} \sum_b p_b S(\varrho_{A|b}) \quad (3)$$

【００５４】

第１のデータＡと第２のデータＢとの古典相関の最大値を定量化したものであり、この最大値は、第２のデータ処理装置１１において、量子観測可能量Ｍ＝｛Ｍｂ｝，によって記述される測定を実行することによって求めることができ、ここで、各Ｍｂは非負のエルミート演算子であり、Ｍｂを足し合わせると、次のように恒等演算子になる：Σｂ Ｍｂ＝Ｉ。状態ρＡＢのサブシステムＢに適用すると、共有量子状態ρＡＢを測定する際に、確率

【数３】

$$p_b = \mathrm{Tr}(\varrho_{AB} \cdot I_A \otimes M_b)$$

で測定結果ｂが生じる。（行列）トレースはＴｒで表される。非負のエルミート演算子Ｍｂは、測定結果ｂに対応する。また、Ｂが減少した量子状態は、以下の式によって記述される。

【００５５】

【数４】

$$\varrho_{A|B} = \mathrm{Tr}_B(I_A \otimes \sqrt{M_b} \cdot \varrho_{AB} \cdot I_A \otimes \sqrt{M_b}$$

【００５６】

Ｂに対する部分トレースはＴｒＢで表される。

【００５７】

量子不一致

【数５】

$$D\ (\overleftarrow{AB})$$

は、すべての相関と古典相関との差として定義されている。以下の式（４）で得られる量子不一致Ｄは、第１のデータ処理装置１０と第２のデータ処理装置１１との量子相関のみを定量化している。

【００５８】

【数６】

$$D(\overleftarrow{AB}) = I(A:B) - I_{\mathrm{acc}}(A:B). \quad (4)$$

【００５９】

アクセス可能情報量Ｉａｃｃは、連鎖律、ひいては情報因果律の原理に違反する可能性がある。とりわけ、特定の量子状態について、以下の式が成り立つ。

【００６０】

【数７】

$$I_{\mathrm{acc}}(A,K:B,K) > I_{\mathrm{acc}}(A,K:B) + |K|. \quad (5)$$

【００６１】

ここで、第１のアクセス可能情報量Ｉａｃｃ（Ａ，Ｋ：Ｂ，Ｋ）は、鍵データＫを有する鍵ｋが第１のデータ処理装置１０から第２のデータ処理装置１１に送信された場合のアクセス可能情報量を表し、第２のアクセス可能情報量Ｉａｃｃ（Ａ，Ｋ：Ｂ）は、鍵ｋが第２のデータ処理装置１１に送信されていない場合のアクセス可能情報量を表す。ここで、鍵データＫを使用して測定することにより、鍵データＫを使用せずにその後で鍵ｋのみを取得するよりも、多くの情報がもたらされ得る。

【００６２】

式（５）が成り立つ典型的な状態

【数８】

$\tilde{\varrho}_{AB}$

は、以下の式（６）によって記述され、

【数９】

$$\tilde{\varrho}_{AB}=\frac{1}{2^{m+1}}\sum_{a=0}^{2^{m}-1}\sum_{k=0}^{1}\ |\ a,\ k\rangle\langle a,\ k\ |\ _{A}\otimes\ (U_{k}\ |\ a\rangle\langle a\ |\ U_{k}^{\dagger})\ _{B},\quad(6)$$

【００６３】

ここで、基本状態｜ａ＞及び｜ａ，ｋ＞である場合、ユニタリ行列Ｕｋ、単位行列Ｕ０、及びＵ１｜ａ＞は｜ａ＞と相互にバイアスされない。共役転置は（・）†で表される。

【００６４】

【数１０】

Ａ（テンソル積⊗の左）

でインデックス付けされたＡ量子状態は第１のデータ処理装置１０にあり、

【数１１】

Ｂ（テンソル積⊗の右）

でインデックス付けされたＢ量子状態は第２のデータ処理装置１１にある。典型的な状態

【数１２】

$\tilde{\rho}_{AB}$

では、第１のアクセス可能情報量はＩａｃｃ（Ａ，Ｋ：Ｂ，Ｋ）＝ｍ＋１であり、第２のアクセス可能情報量はＩａｃｃ（Ａ，Ｋ：Ｂ）＝ｍ／２である。したがって、シングルビットのみを含む鍵ｋを使用して取得された、ｍ／２個の付加情報が存在する。量子不一致Ｄは、量子データロッキングの利点を定量化している。

【００６５】

ここでの目的は、第１のデータ処理装置１０と第２のデータ処理装置１１との間の共有データに対する、外部データ処理装置１２のアクセスを制限することである。通常、共有データへのアクセスを最小限に抑えるためには、第２のデータ処理装置１０と外部データ処理装置１２との第２の量子相互情報量Ｉ（Ａ：Ｅ）を測定し、これを最小限に抑える必要がある。

【００６６】

この第２の量子相互情報量Ｉ（Ａ：Ｅ）は、第２のデータ処理装置１１において求められたアクセス・インジケータ・パラメータによって測定され得る。このアクセス・インジケータ・パラメータは、例えば量子ビット誤り率を含んでいてもよい。

【００６７】

続いて、第１のデータ処理装置１０及び第２のデータ処理装置１１において誤り訂正と秘匿性増強とが実行され、以下の（７）の鍵レートを有する鍵ｋが生成される。

【００６８】

【数１３】

$$r_{key}\approx I(A:B)-I(A:E).\quad(7)$$

【００６９】

外部データ処理装置１２に、実質的に無制限のリソースと、量子一括測定を含む任意の

測定形式を実行する機能とが備わっていると仮定すると、第２の量子相互情報量Ｉ（Ａ：Ｅ）はホレボ容量C_χによって、以下の式（８）のように制限される。

【００７０】

【数１４】

$$I(A:E) \leq C_\chi = \max_{p_i^E} \chi(\{p_i^E\},\{\varrho_i^E\}) = \max_{p_i^E}\left[H\left(\sum_i p_i^E \varrho_i^E\right) - \sum_i p_i^E H(\varrho_i^E)\right] \quad (8)$$

【００７１】

ここで、

【数１５】

$$\{\varrho_i^E\}$$

は外部データ処理装置１２内の第３の量子状態のセットであり、この第３の量子状態

【数１６】

$$\varrho_i^E$$

はそれぞれ、第３の確率

【数１７】

$$p_i^E$$

で発生しており、ｘをホレボ値と呼んでいる。本方法のセキュリティを証明するために、求められたアクセス・インジケータ・パラメータに帰結し得る状態のセットが考慮され得、これにより、第２の量子相互情報量Ｉ（Ａ：Ｅ）が制限され得る。

【００７２】

図２は、量子鍵配送のための方法を示すグラフィカル図である。

【００７３】

本方法により、外部データ処理装置１２において、特定可能なデータ量を削減することができる。これに応じて、第２の量子相互情報量Ｉ（Ａ：Ｅ）は、C_χよりも低い値によって制限され得る。このために、鍵ｋに関する古典情報量、又はこれと対応付けられたその後の信号が、外部データ処理装置１２によって特定されてはならない。これは、後処理中に生成され、外部データ処理装置１２によって特定され得る後処理情報を暗号化することによって達成され得る。第２の量子相互情報量Ｉ（Ａ：Ｅ）が減少すると、鍵レートr_{key}は増大する（式（７）を参照のこと）。

【００７４】

第１のステップ２１で、第１のデータ処理装置１０及び第２のデータ処理装置１１に初期秘密鍵が供給される。これは、例えば既知の古典的鍵配送プロトコル若しくは量子鍵配送プロトコル、又は本方法における先行実行から先行する鍵を使用することによって達成され得る。また、第１のデータ処理装置１０及び第２のデータ処理装置１１に、相互認証を行うための第２の初期鍵が供給される。

【００７５】

第２のステップ２２で、確率分布

【数１８】

$$\{p_i^A\}_i$$

を有する乱数発生器を使用することにより、第１のデータ処理装置１０の第１の記憶装置

１０ａで複数の第１の量子状態
【数１９】
$\{\varrho_i^A\}_i$

を含む第１の量子信号が生成される。このために、確率分布
【数２０】
$\{p_i^A\}_i$

を用いて中間古典信号が生成され、次いで第１の記憶装置１０ａの古典メモリに記憶されてもよく、また、第１の量子信号は中間古典信号に従って生成されてもよい。この確率分布
【数２１】
$\{p_i^A\}_i$

は、均一な確率分布とすることができる。第１の量子状態
【数２２】
ϱ_i^A

はそれぞれ、（古典的な）第１の生信号の１桁、例えば１ビットを符号化し、これに対応することができる。第１の量子信号は、通信チャネル１３を介して第１のデータ処理装置１０から第２のデータ処理装置１１に送信される。
【００７６】
複数の第１の量子状態
【数２３】
$\{\rho_i^A\}_i$

が（接続部１４を介して）外部データ処理装置１２において受信され得、また外部データ処理装置１２が量子一括（測定）攻撃を実行することができる場合、複数の第１の量子状態
【数２４】
$\{\varrho_i^A\}$

及びアンシラ
【数２５】
ϱ^E

のそれぞれに対してユニタリ演算
【数２６】
$U_{AE}: H_A \otimes H_E \to H_B \otimes H_E$

（ヒルベルト空間H_A及びH_Eが、サブシステムＡ及びＥにそれぞれ対応している状態で）が実行され、外部データ処理装置１２の外部記憶装置１２ａ内に複数の第３の量子状態
【数２７】
$\{\varrho_i^E\}$

【数２８】

（$\{\mathrm{Tr}_B\,(U_{AE}\cdot\varrho_i^A\otimes\varrho^E\cdot U_{AE}^{\dagger})\}$に対応する）

が生成され、次いで第２のデータ処理装置１１にこれをさらに送信した後、第２のデータ処理装置１１の第２の記憶装置１１ａ内に複数の（第２の）量子状態

【数２９】

$\{\varrho_i^B\}$

【数３０】

（$\{\mathrm{Tr}_E\,(U_{AE}\cdot\varrho_i^A\otimes\varrho^E\cdot U_{AE}^{\dagger})\}$に対応する）

が生成される。

【００７７】

第３のステップ２３で、第２のデータ処理装置１１において、例えばランダム分布を使用して複数の量子測定パラメータが求められる。さらに、第２のデータ処理装置１１において、複数の量子測定パラメータを使用して複数の第２の量子状態

【数３１】

$\{\rho_i^B\}_i$

が測定され、古典的な（第２の）生信号が生成される。第２の生信号の桁位置はそれぞれ、これら複数の量子測定パラメータのうちの１つ及び複数の第２の量子状態のうちの１つに対応している。

【００７８】

第４のステップ２４で、第１のデータ処理装置１０及び第２のデータ処理装置１１において、通信チャネル１３を使用して基底照合が実行される。

【００７９】

一実施形態では、測定結果のうちの対応する１つが不確定結果である場合、第２の生信号の（第２の）桁位置を破棄することにより、第２のデータ処理装置（１１）において第２の生信号及び測定結果から（第２の）照合信号が求められる。また、第２のデータ処理装置（１１）において、初期鍵を使用して（第２の）暗号化信号が生成され、次いで第１のデータ処理装置（１０）に送信される。この第２の暗号化信号は、不確定結果に対応する測定結果を示す。次に、第１のデータ処理装置（１０）において、第２の暗号化信号が復号される。次いで、測定結果のうちの対応する１つが、１つの不確定結果と一致する場合、第１の生信号の第１の桁位置を破棄することにより、第１のデータ処理装置（１０）において第１の生信号から第１の照合信号が求められる。

【００８０】

別実施形態では、第１のデータ処理装置（１０）において、初期鍵を使用して、複数の量子生成パラメータのうちの少なくとも１つを示す第１の暗号化信号が生成され、次いで第２のデータ処理装置（１１）に送信される。これとは逆に、第２のデータ処理装置（１１）において、複数の量子測定パラメータのうちの少なくとも１つを示す第２の暗号化信号が初期鍵を使用して生成され、次いで第１のデータ処理装置（１０）に送信される。

【００８１】

次いで、第２の暗号化信号からの複数の量子測定パラメータのうちの対応する１つと、量子生成パラメータのうちの対応する１つとが一致しない場合、第１の生信号における第１の桁位置のうちの１つを破棄することにより、第１のデータ処理装置（１０）において第１の生信号及び第２の暗号化信号から第１の照合信号が求められる。

【００８２】

さらに、複数の量子測定パラメータのうちの対応する１つと、量子生成パラメータのうちの対応する１つとが一致しない場合、第２の生信号における桁位置のうちの１つを破棄することにより、第２のデータ処理装置（１１）において第２の生信号及び複数の量子測定パラメータから第２の照合信号が求められる。

【００８３】

既知のプロトコルでは、初期鍵を使用したそのような暗号化は用いられていない。

【００８４】

第５のステップ２５で、第１の照合信号と第２の照合信号との誤り推定値が求められる。このために、第１のデータ処理装置（１０）において、第１の照合信号から第１の誤り情報が生成され、必要に応じて初期鍵で暗号化され、次いで第２のデータ処理装置（１１）に送信される。これとは逆に、第２のデータ処理装置（１１）において、第２の照合信号から第２の誤り情報が生成され、必要に応じて初期鍵で暗号化され、次いで第１のデータ処理装置（１０）に送信される。次いで、第１のデータ処理装置（１０）及び第２のデータ処理装置（１１）において、第１の誤り情報及び第２の誤り情報から誤り推定値が求められる。第１の誤り情報と第２の誤り情報とは、例えば第１の照合信号における第１のパリティビット又はその一部と、第２の照合信号における第２のパリティビット又はその一部とをそれぞれ含み得る。この場合、第１の誤り情報と第２の誤り情報とは、送信前に暗号化される。また、誤り推定値は、第１のパリティビットと第２のパリティビットとを比較することによって求められる。付加的に又は代替的に、この誤り推定値は、視認性及び／又はデコイ状態の統計値をさらに含んでいてもよい。

【００８５】

第１の誤り情報は、第１の照合信号における第１の桁位置の第１のサブセットをさらに含み得、また、第２の誤り情報は、第２の照合信号における第２の桁位置の第２のサブセットを含み得る。この場合、第１の誤り情報と第２の誤り情報とは暗号化されなくてもよい。第１の桁位置の第１のサブセットと第２の桁位置の第２のサブセットとの和集合が、その後、第１及び第２の照合信号から破棄される。

【００８６】

誤り率が閾値を上回る場合、本方法は中止される。そうでない場合、本方法は継続される。誤り推定値は、第２の量子相互情報量Ｉ（Ａ：Ｅ）又は第３の量子相互情報量Ｉ（Ｂ：Ｅ）の推定値をさらにもたらす。第１の照合信号及び第２の照合信号の誤り部分は破棄されてもよい。

【００８７】

第６のステップ２６で、誤り訂正が実行される。このために、第１のデータ処理装置（１０）において、第１の照合信号から第１のパリティデータが生成され、初期鍵で暗号化され、次いで第２のデータ処理装置（１１）に送信されてもよい。付加的に又は代替的に、第２のデータ処理装置（１１）において、第２の照合信号から第２のパリティデータが生成され、初期鍵で暗号化され、次いで第１のデータ処理装置（１０）に送信されてもよい。

【００８８】

続いて、第２のデータ処理装置（１１）において、第１のパリティデータから第１の照合信号と第２の照合信号との差分が求められ得る。付加的に又は代替的に、この差分は、第１のデータ処理装置（１０）において求められ得る。

【００８９】

これにより、種々の実施形態に従って、第１のデータ処理装置（１０）及び第２のデータ処理装置（１１）の両方における共有鍵が特定され得る。

【００９０】

一実施形態によれば、この共有鍵は、第１のデータ処理装置（１０）において、第１の照合信号と第２の照合信号との差分に対して第１の照合信号を補正することにより、第１の照合信号から特定される。第２のデータ処理装置（１１）では、第２の照合信号が共有鍵であると判定される。とりわけ共有鍵は、第１のデータ処理装置（１０）及び第２のデ

ータ処理装置（１１）の両方において同一でさえあればよいが、この共有鍵の具体値は通常、ランダムに決定される。ここでは、第２の照合信号がマスタ信号であると判定され、第１の照合信号が補正される（逆照合）。

【００９１】

別実施形態によれば、この共有鍵は、第２のデータ処理装置（１１）において、第１の照合信号と第２の照合信号との差分に対して第２の照合信号を補正することにより、第２の照合信号から特定される。第１のデータ処理装置（１０）では、第１の照合信号が共有鍵であると判定される。ここでは、第１の照合信号がマスタ信号であると判定され、第２の照合信号が補正される（直接照合）。

【００９２】

第１のパリティデータは、第１の照合信号における第１のデータブロックの第１のパリティビットを含んでいてもよく、また、第２のパリティデータは、第２の照合信号における第２のデータブロックの第２のパリティビットを含んでいてもよい（カスケード方式）。その一方で、第１及び第２の照合信号をデータブロックへと分割することを示すデータブロック情報は、暗号化されずに送信されてもよい。

【００９３】

あるいは、第１のパリティデータは、第１の照合信号の第１のシンドロームを含んでいてもよく、また、第２のパリティデータは、第２の照合信号の第２のシンドロームを含んでいてもよい（線形誤り訂正符号方式又は線形ブロック符号方式）。これら第１のシンドローム及び第２のシンドロームは、複数の検査行列のうちの１つを第１の照合信号及び第２の照合信号の（ベクトル化された）データブロックにそれぞれ乗算することによって求められ得る。とりわけ、各シンドロームビットは、複数の検査行列のうちの１つにおいて対応する行の、１値ビットのパリティビットを構成している。その一方で、複数の検査行列のうちの少なくとも１つを示す検査行列情報は、暗号化されずに送信されてもよい。

【００９４】

第１のパリティデータ及び／若しくは第２のパリティデータから、とりわけ開示しているいくつかのパリティビット並びに／又は第１のシンドローム及び／若しくは第２のシンドロームの長さから、情報漏洩量が特定されてもよい。外部データ処理装置１２において特定され得る部分的な鍵情報が増大すると、情報漏洩が拡大する可能性がある。

【００９５】

第６のステップ２６の目的は、第１及び第２の照合信号に関する古典情報量、ひいては共有鍵の漏洩を防止することである。第６のステップ２６の前に、外部データ処理装置の外部記憶装置１２ａに、第３の確率

【数３２】

$$\{p_i^E\}_i$$

で第３の量子状態

【数３３】

$$\{\varrho_i^E\}_i$$

が供給されていてもよい。外部データ処理装置１２が量子一括攻撃手段を備える場合、第３の確率

【数３４】

$$\{p_i^E\}_i$$

は、共有鍵の桁位置k_1，k_2，．．．，k_Nに依存しておらず、これは$k = k_1 k_2 \ldots k_N$として構築されている。したがって、共有鍵$k = k_1 k_2 \ldots k_N$に対応する、第

３の量子信号
【数３５】

$$\varrho^{E}_{(k)} = \varrho^{E}_{k_1} \otimes \varrho^{E}_{k_2} \otimes \cdots \otimes \varrho^{E}_{k_N}$$

それぞれの結合確率は、以下の式（９）のような積形式を有する。
【００９６】
【数３６】

$$p^{E}_{(k)} = p_{k_1} \cdot p_{k_2} \cdot \cdots \cdot p_{k_N} \quad (9)$$

【００９７】
そのような第３の量子信号（積量子状態としての）及び積確率分布
【数３７】

$$\{p^{E}_{(k)}\}$$

において、量子チャネル容量は加法的となり、個々の測定値は、以下の式（１０）のように最良の結果をもたらす。
【００９８】
【数３８】

$$\max_{M_N} I_N(A^N:E^N) = N \cdot \max_{M_1} I_1(A:E) \quad (10)$$

【００９９】
ここで、左辺は、Ｎ個の量子状態（Ｎ回分の相互情報量I_N）上のすべての観測可能量M_Nに対する最大化を表し、右辺は、単一の量子状態（ワンショットの相互情報量I_1）上の個々の観測可能量M_1に対する個々の最大化を表す。したがって、第６のステップ２６の前に、個々の測定値に対応するワンショットの相互情報量I_1によって、ビットごとの共有鍵に関する情報が制限される。
【０１００】
第６のステップ２６で、第１及び第２のパリティデータが暗号化されない状態で、一部の共有鍵情報が外部データ処理装置１２に漏洩し得る。カスケード方式の場合、こうした情報漏洩は、送信されるデータブロックの第１及び第２のパリティビットに起因している可能性がある。線形誤り訂正符号方式の場合、こうした情報漏洩は、送信される第１及び／又は第２のシンドロームに起因している可能性がある。重要なのは、漏洩したすべてのパリティビットによって、第１のデータ処理装置１０及び第２のデータ処理装置１１の共有鍵において、有効なビットの組み合わせ（符号語）数が半分になるということである。例えば、３ビットのビット文字列の場合、パリティビット値が１であることは、ビット文字列０００、０１１、１０１及び１１０がそれぞれ０の確率を有することを意味している。したがって、８つの組み合わせのうち４つだけが残り、第３の量子信号
【数３９】

$$\varrho^{E}_{(k)}$$

に対する結合確率
【数４０】

$$p^{E}_{(k)}$$

が変化する。

【０１０１】

第１のパリティデータ及び第２のパリティデータを暗号化せずに誤り訂正を行う場合、第１のデータ処理装置１０と外部データ処理装置１２とは、符号化実行時に最終的に古典量子チャネルの状況となる。具体的には、Ｃビットが漏洩した場合、有効な共有鍵のビット組み合わせ数が2^{N}から2^{N-C}に減少する。したがって、第１のデータ処理装置１０及び外部データ処理装置１２に関して、第１のデータ処理装置１０によって符号語のセットが供給されており、この符号語のセットの把握が必要になる量子一括測定が、外部データ処理装置１２によって実行され得るという点で、量子チャネル符号化定理の要件が満たされていると言える。この量子一括測定を用いて桁位置ごとの相互情報を最大化したものは、式（１０）のワンショットの相互情報量I_1よりも大きいホレボ値（式（８）を参照のこと）によってもたらされる。

【０１０２】

第１及び第２のパリティデータを暗号化せずに誤り訂正を行う場合、第１のデータ処理装置１０と外部データ処理装置１２とは、量子データロッキングプロトコルを実行して、外部データ処理装置１２にＣビットの古典情報量を供給していると考えることができる。これにより、潜在的に量子一括測定を実行していることに起因して、外部データ処理装置１２における共有鍵を特定する際の不確実性が、Ｃビットよりも多く低下することになる。

【０１０３】

これに対して、提案している量子鍵配送のための方法を用いることにより、上述したように、外部データ処理装置１２に共有鍵情報を供給することなく、量子データロッキングプロトコルを付与することができる。本方法では、確率の変化を示す情報（結合確率

【数４１】

$$p^{E}{}_{(k)}$$

を変化させる）のいずれも公開してはならない。したがって、この結合確率

【数４２】

$$p^{E}{}_{(k)}$$

は、式（９）のような積形式を有する必要がある。これは、共有鍵と対応付けられたすべての古典信号を暗号化することによって実行され得る。この共有鍵に対応付けられた鍵情報があれば、確率分布

【数４３】

$$\{p^{E}{}_{(k)}\}$$

を変化させるが、これは、そうでなければ、共有鍵に関する情報と漏洩情報との間のその後の相互情報量Ｉ（Ｋ：Ｃ）が０になるためである。

【０１０４】

第６のステップ２６で誤り訂正にカスケード方式を用いる場合、データブロックの第１のパリティビットとデータブロックの第２のパリティビットとは、初期鍵で暗号化される必要がある。その一方で、第１及び第２の照合信号をデータブロックへと分割することを示すデータブロック情報は、共有鍵と対応付けられていないため、公開送信されてもよい。

【０１０５】

線形誤り訂正符号方式を用いる場合、シンドロームを初期鍵で暗号化する必要があるが、複数の検査行列のうちの少なくとも１つを示す検査行列情報が公開送信されてもよい。本方法では、第１のデータ処理装置と第２のデータ処理装置との間で送信されるすべての相関データ、具体的には後処理データが、初期鍵で暗号化される必要がある。

【０１０６】
第７のステップ２７で、情報漏洩を最小限に抑えるために、共有鍵に秘匿性増強が適用され、共有鍵よりも短い増幅鍵が生成される。この秘匿性増強に応じて、増幅鍵に関するその後の盗聴者情報は、０に近似していると判定され得る。
【０１０７】
このために、第１のデータ処理装置（１０）又は第２のデータ処理装置（１１）の一方でハッシュデータが求められ、暗号化され、次いで第１のデータ処理装置（１０）又は第２のデータ処理装置（１１）のもう一方に送信される。このため、第１のデータ処理装置（１０）と第２のデータ処理装置（１１）との間でハッシュデータが分散される。このハッシュデータを命令データとして使用して、第１のデータ処理装置（１０）及び第２のデータ処理装置（１１）の両方で共有鍵にハッシュ方式が適用され、第１のデータ処理装置（１０）及び第２のデータ処理装置（１１）の両方で増幅鍵が生成される。このハッシュデータは、例えば、ベクトルとして共有鍵に乗算される２進テプリッツ行列におけるランダム抽出を示してもよい。
【０１０８】
このように、第１のデータ処理装置１０及び第２のデータ処理装置１１の両方で（同じ）共有鍵、好ましくは（同じ）増幅鍵を配送すると、その後の（古典）メッセージが共有鍵又は増幅鍵で暗号化され得、次いで第１のデータ処理装置１０から第２のデータ処理装置１１へ、かつ／又は第２のデータ処理装置１１から第１のデータ処理装置１０へと送信され得る。
【０１０９】
提案している本方法では、誤り訂正中の情報漏洩量は０になるが、その一方で初期鍵は使い尽くされる。その後のメッセージを暗号化するためにワンタイムパッド方式が用いられる場合、暗号化に必要な量と同量の鍵情報が使い尽くされる。あるいは、例えばその後のメッセージを暗号化するためにＡＥＳが用いられる場合、暗号化に必要な鍵情報のうちで使い尽くされる量が少なくなる。好ましくは、共有鍵長又は増幅鍵長は、シンドローム長又はパリティデータ長に等しい。
【０１１０】
図３は、ａ）初期鍵を使用した暗号化なしの従来型の量子鍵配送と、ｂ）ワンタイムパッドを使用する提案中の本方法とを比較した図である。従来型の量子鍵配送及び提案中の本方法の両方において、第２の初期鍵が認証に使用されている。図３ｂ）に対応する本方法の実施形態では、第２の初期鍵も同様に初期鍵として使用されている。
【０１１１】
従来型の量子鍵配送では、初期鍵データ量３０は従来型の共有鍵データ量３１の分だけ増加し、その後の追加データの暗号化に使用され得る。提案している本方法では、初期鍵データ量３０に加えて、例えば共有鍵と対応付けられた相関データを暗号化するために、相関鍵データ量３２が使用される。ただしここで、その後の追加データの暗号化に使用され得る鍵データ量は、従来型の共有鍵データ量３１の分だけ増加するだけでなく、鍵利得３３の分だけさらに増加する。この鍵利得３３は、第２の量子相互情報量Ｉ（Ａ：Ｅ）の減少、即ち、外部データ処理装置１２に対する情報漏洩量が減少したことに起因するものである。ワンタイムパッドの代わりにＡＥＳ又は別の古典的な暗号化方式が用いられる場合、鍵利得３３を保持しながら、相関鍵データ量３２がより少なくなるようにすることができる。
【０１１２】
提案している本方法は、正規ユーザが鍵レートを増大させるのを補助することができる。盗聴者への潜在的な情報漏洩が大幅に低減される。第１のデータ処理装置１０及び第２のデータ処理装置１１に対するハードウェアの変更は、必要に応じて最小限に留められ得る。本方法は、一方の第１のデータ処理装置１０（及び第２のデータ処理装置１１）内のデータと他方の外部データ処理装置１２内のデータとの間の相関を固定する量子データロッキングプロトコルと考えられ得る。量子測定パラメータなどの追加データが供給されな

い場合、外部データ処理装置で適切な量子測定を実行することができなくなる。この追加データは、確率分布の変化を示すデータと、相関データとを含む。理論上は無制限の量子リソースを利用できる盗聴者に対するセキュリティが、１つの難題となっている。この盗聴者は、使用される符号語や共有鍵又は増幅鍵と対応付けられた他の情報などの新情報をある時点で取得して、しかるべき測定を実行する可能性がある。したがって、ｌビットの初期鍵量の情報漏洩は、盗聴者にｌビットを超える情報を提供する可能性がある。

【０１１３】

ただし、ここで重要なのは、時間制限された量子メモリを有する盗聴者に対して実際に適用できる事例では、提案している本方法が良好に機能するということである。したがって、盗聴者による量子メモリへの保存時間中に、共有鍵又は増幅鍵と対応付けられた情報が情報漏洩しなければよいことになる。初期鍵を用いた暗号化にＡＥＳのような古典的な暗号化方式が用いられる場合、その古典的な暗号化方式は、当該保存時間の間、十分にセキュアであると仮定される。

【０１１４】

本方法は、Ｂ９２様のプロトコル、ＢＢ８４プロトコル、並びに第１のデータ処理装置１０及び第３のデータ処理装置がそれぞれの量子状態を第２のデータ処理装置１１に送信するプロトコル、例えば測定装置に依存しない量子鍵配送又はツインフィールド量子鍵配送などで使用され得る。第１のデータ処理装置１０及び第２のデータ処理装置１１に最初に共有もつれ状態がもたらされるプロトコル、並びに／又は第１のデータ処理装置１０、第２のデータ処理装置１１、及び潜在的盗聴者である外部データ処理装置１２間で共有ｃ‐ｃ‐ｑ状態が発生する別のプロトコルも、同様に使用され得る。

【０１１５】

＜Ｂ９２様のプロトコル＞

以下では、このＢ９２様のプロトコルを使用する、本方法の別実施形態について説明する。外部データ処理装置１２は、ビーム分割攻撃を行うように構成されている。

【０１１６】

第１のステップ２１で、第１のデータ処理装置１０及び第２のデータ処理装置１１に初期鍵が供給される。この初期鍵は、相互認証にも使用される。

【０１１７】

第２のステップ２２で、強度$\mu_A = \alpha^2$（実数値αを有する）｜±α〉の２つのコヒーレント状態｜±α〉を含む量子信号が第１のデータ処理装置１０で生成され、次いで第２のデータ処理装置１１に送信される。ここで生成されるコヒーレント状態のタイプは、第１の生信号における第１の桁位置のうちの１つに対応している。具体的には、ｊ番目に生成されるコヒーレント状態は、第１の生信号におけるｊ番目の第１の桁位置に割り当てられる。例えば、第１のコヒーレント状態｜＋α〉により、第１の生信号における第１の桁位置のうちの対応する１つが０に等しくなる結果がもたらされてもよい一方で、第２のコヒーレント状態｜－α〉により、第１の生信号における第１の桁位置のうちの対応する１つが１に等しくなる結果がもたらされてもよい。共有量子状態は、古典量子状態として、以下の（１１）のように記述される。

【０１１８】

【数４４】

$$\frac{1}{2}\left(|0\rangle\langle 0|_A \otimes |\alpha\rangle\langle\alpha|_B + |1\rangle\langle 1|_A \otimes |-\alpha\rangle\langle -\alpha|_B\right). \quad (11)$$

【０１１９】

ビーム分割攻撃のシナリオでは、コヒーレント状態｜±α〉を外部記憶装置１２ａに部分的に流用することにより、外部データ処理装置１２によってチャネル損失がシミュレートされ得る。このチャネル損失は、光ファイバの減衰係数

【数４５】

$$\delta \approx 0.2\,\mathrm{dB/km}$$

と通信チャネル長ｌとに対して

【数４６】

$$\mu_A \mapsto \mu_A 10^{-\delta\, l/10}$$

の強度低下が生じることによってもたらされる。このため、外部データ処理装置１２には、外部強度がμ$_E$＝μ$_A$（１－１０$^{-δl/10}$）の外部コヒーレント状態が生成され、次いで第２のデータ処理装置１１に対して、強度がμ$_B$＝μ$_A$１０$^{-δl/10}$の第２のコヒーレント状態｜±α$_B$〉を送信する。第１のデータ処理装置１０、第２のデータ処理装置１１、及び外部データ処理装置１２間の全体の共有量子状態は、以下の（１２）によって得られ、

【数４７】

$$\frac{1}{2}\left(|0\rangle\langle 0|_A \otimes |\alpha_B\rangle\langle\alpha_B|_B \otimes |\alpha_E\rangle\langle\alpha_E|_E \;+\; |1\rangle\langle 1|_A \otimes |-\alpha_B\rangle\langle -\alpha_B|_B \otimes |-\alpha_E\rangle\langle -\alpha_E|_E\right), \quad (12)$$

【０１２０】

ここでは

【数４８】

$$\alpha_B^2 = \mu_B,$$

【数４９】

$$\alpha_E^2 = \mu_E$$

であり、外部コヒーレント状態は｜±α$_E$〉である。

【０１２１】

第３のステップ２３で、第２のデータ処理装置１１において、測定パラメータを使用して第２のコヒーレント状態｜±α$_B$〉が測定され、この測定パラメータは、以下の測定演算子（１３）が対応する、Ｂ９２による観測可能量Ｍ$_{B92}$＝｛Ｍ$_0$，Ｍ$_1$，Ｍ$_?$｝を含み、

【数５０】

$$M_0 = \frac{I - |-\alpha_B\rangle\langle -\alpha_B|}{1 + \langle\alpha_B|-\alpha_B\rangle}, \qquad M_1 = \frac{I - |\alpha_B\rangle\langle\alpha_B|}{1 + \langle\alpha_B|-\alpha_B\rangle}, \qquad M_? = I - M_0 - M_1, \quad (13)$$

【０１２２】

これらの測定演算子はそれぞれ、測定結果のうちの１つに対応している。第２のコヒーレント状態｜±α$_B$〉を測定する際、第１の測定演算子Ｍ$_0$（第１の測定結果に対応している）と第２の測定演算子Ｍ$_1$（第２の測定結果に対応している）とは確定的な信号情報を生成する一方、第３の測定演算子Ｍ$_?$（第３の測定結果に対応している）は不確定的な信号情報を生成する。次いで、第２のコヒーレント状態｜±α$_B$〉を測定して得られた測定結果において判定された測定結果が、（第２の）生信号における桁位置のうちの１つに割り当てられる。具体的には、ｊ回目の繰り返しで第２のコヒーレント状態｜±α$_B$〉を測定して得られた測定結果において、ｊ番目に判定された測定結果が、第２の生信号におけるｊ番目の桁位置に割り当てられる。

【０１２３】

第４のステップ２４で、従来型の量子鍵配送を用いる場合、第２の生信号において第３の測定結果に対応する不確定的な桁位置が、第２のデータ処理装置１１から（例えば、公開チャネルを介して）第１のデータ処理装置１０に公開送信される。提案している本方法では、第２のデータ処理装置１１から第１のデータ処理装置１０に送信される前に、この不確定的な桁位置が初期鍵で暗号化されて、暗号化信号となる。さらに、この不確定的な

桁位置が第２の生信号で破棄され、これによって第２の照合信号が生成される。第１のデータ処理装置１０で暗号化信号を復号した後、この不確定的な桁位置も第１の生信号で破棄され、これによって第１の照合信号が生成される。

【０１２４】

第５のステップ２５で、第１の照合信号と第２の照合信号との誤り推定値が求められる。第１の照合信号における第１の桁位置の第１のサブセットを含む第１の誤り情報と、第２の照合信号における第２の桁位置の第２のサブセットを含む第２の誤り情報とは、第１及び第２のデータ処理装置１０、１１においてそれぞれ求められ、相互に送信され、次いで比較される。第１の桁位置の第１のサブセットと第２の桁位置の第２のサブセットとの和集合が、その後、第１及び第２の照合信号から破棄される。第１の桁位置の第１のサブセットと第２の桁位置の第２のサブセットとは残りの桁位置と対応付けられていないため、第１の桁位置の第１のサブセットと第２の桁位置の第２のサブセットとを初期鍵で暗号化することなく、第１の桁位置の第１のサブセットと第２の桁位置の第２のサブセットとが送信され得る。

【０１２５】

付加的に又は代替的に、第１の誤り情報と第２の誤り情報とは、例えば第１の照合信号における第１のパリティビット又はその一部と、第２の照合信号における第２のパリティビット又はその一部とをそれぞれ含み得る。この場合、これら第１の誤り情報及び第２の誤り情報は、第１の照合信号及び第２の照合信号と対応付けられているため、送信前に暗号化される。

【０１２６】

第５のステップ２５の後、外部データ処理装置１２によってビーム分割攻撃が実行されている場合、外部記憶装置１２ａは外部コヒーレント状態｜±α_E〉を含み得る。

【０１２７】

パリティビットの送信は、誤り率が小さい場合に有用となり得る。例えば、観測された誤り率が約１％である場合、１０００ビットを１０個の誤りで送信すると、不正確な誤り推定値が得られる。例えば、長さ１０の１０００個のデータブロックを選択し、これら１０００個のデータブロックのそれぞれに対するデータブロックのパリティビットを送信すると、より有用となり得る。データブロックのパリティビットが不一致である確率ははるかに高いため、ベイズの定理を用いると、より良好な誤り推定値をもたらすことができる。この場合、桁位置の破棄は好ましいとは言えないが、少なくともその後の秘匿性増強の間、データブロックのパリティビットの漏洩が考慮されるべきである。

【０１２８】

第６のステップ２６で、第１及び第２の照合信号の誤り訂正が実行される。例えば、第１の照合信号が第１の文字列s_A＝（０１１００１０１）を含み、第２の照合信号が第２の文字列s_B＝（０１０００１０１）を含む場合、桁位置３は誤りである。誤り推定値が求められていれば、この場合、１つの誤り桁位置しか存在しないと判定され得る。したがって、その１つの誤り桁位置のみが特定される必要がある。

【０１２９】

カスケード方式を用いる場合、第１の文字列s_Aと第２の文字列s_Bとは、それぞれ第１のデータブロックと第２のデータブロックとにランダムに分割される。第１のデータブロック及び第２のデータブロックのそれぞれにおいて、第１のパリティビット及び第２のパリティビットが特定され、暗号化され、次いで第１のデータ処理装置１０と第２のデータ処理装置１１との間で送信される。誤り桁位置は、２分探索によって特定される。

第１の文字列s_Aはパリティ０を有し、第２の文字列s_Bはパリティ１を有する。第１の文字列s_A及び第２の文字列s_Bの第１の半部（０１１０）と（０１００）とは、それぞれパリティ０とパリティ１とを有する。第１の半部が異なるパリティを有するため、誤り桁位置はこの第１の半部内に位置する。第１の半部をさらに半分にすると、第１の文字列s_A及び第２の文字列s_Bにおける第１の四半部（０１）、（０１）及び第２の四半部（１０），（００）が得られる。第１の文字列s_A及び第２の文字列s_Bにおける第１の四

半部（０１）、（０１）は一致しており、同じパリティを有する。したがって、誤り桁位置は、第１の文字列ｓ$_A$及び第２の文字列ｓ$_B$における第２の四半部（１０），（００）、即ち桁位置３に位置する。

【０１３０】

この誤り桁位置を特定するためには、４つの第１及び第２のパリティビットを第１のデータ処理装置１０と第２のデータ処理装置１１との間で送信する必要があった。

【０１３１】

線形ブロック符号方式を用いる場合、例えば、以下の（１４）などの２値化された検査行列（公開送信され得る）を

【数５１】

$$H=\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \quad (14)$$

使用して、第１のシンドローム

【数５２】

$$z_A = Hs_A^T = (1100)^T$$

及び第２のシンドローム

【数５３】

$$z_B = Hs_B^T = (1010)^T$$

が計算される。

【０１３２】

第１のシンドロームｚ$_A$は暗号化されて、第１のデータ処理装置１０から第２のデータ処理装置１１に送信される。あるいは、第２のシンドロームｚ$_B$は暗号化されて、第２のデータ処理装置１１から第１のデータ処理装置１０に送信される。続いて、第１のデータ処理装置１０及び第２のデータ処理装置１１の双方において、誤りシンドローム

【数５４】

$$z_E = z_A \oplus z_B = (0110)^T$$

が求められる。次いで、誤りシンドロームの連立方程式から求められる誤りベクトルｅは、以下の（１５）の通りである。

【０１３３】

Ｈｅ＝ｚ$_E$（１５）

【０１３４】

この誤りシンドロームの連立方程式が劣決定系であるため、誤りベクトルｅは、例えば、最尤推定又は１ノルム最小化によって求められ得る。ここで、この誤りベクトルｅは、（００１００００）^{T}であると判定される。これにより、誤り桁位置が特定される。

【０１３５】

直接照合の場合、第１の文字列ｓ$_A$が正しいと見なされるため、第２の文字列ｓ$_B$が修正されて、共有鍵（０１１００１０１）が生成される。逆照合の場合、第２の文字列ｓ$_B$が正しいと見なされるため、第１の文字列ｓ$_A$が修正されて、共有鍵（０１０００１０１）が生成される。

【０１３６】

第１及び第２のパリティデータが第１及び第２の照合信号と対応付けられたデータ（カスケード方式を用いた場合の、第１のパリティビット及び第２のパリティビット、又は線形ブロック符号を用いた場合の、第１及び第２のシンドロームなど）を含む場合、第１及

び第２のパリティデータは、セキュリティ要件に応じて、例えばＡＥＳ又はワンタイムパッドのような古典的な暗号化方式を用いて暗号化されるべきである。

【０１３７】

従来型の量子鍵配送では、外部データ処理装置１２に漏洩した第２の量子相互情報量Ｉ（Ａ：Ｅ）は、外部記憶装置１２ａ内の外部コヒーレント状態｜±α_E〉のホレボ値によって、以下の式（１６）のように制限され、

【数５５】

$$I(A:E) \leq \chi(\{|\pm\alpha_E\rangle\}) = h_2\left(\frac{1-e^{-2\mu_A(1-10^{-\frac{\delta l}{10}})}}{2}\right), \quad (16)$$

【０１３８】

ここで、２進シャノンエントロピーは$h_2(x) = -x\log x-(1-x)\log(1-x)$となる。

【０１３９】

これに対して、提案している本方法では、第２の量子相互情報量Ｉ（Ａ：Ｅ）は、量子一括測定ではなく、個別量子測定のみを実行することに相当するワンショット容量C_1によって制限される。外部コヒーレント状態{｜±α_E〉}の最良分解能は、誤り確率

【数５６】

$$q=\frac{1}{2}\left(1-\sqrt{1-e^{-4\mu_A(1-10^{-\delta l/10})}}\right)$$

が計算される。

【０１４０】

したがって、第２の量子相互情報量Ｉ（Ａ：Ｅ）は、以下の式（１７）のように制限される。

【０１４１】

【数５７】

$$I(A:E) \leq C_1 = 1-h_2\left(\frac{1-\sqrt{1-e^{4\mu_A(1-10^{-\frac{\delta l}{10}})}}}{2}\right). \quad (17)$$

【０１４２】

第７のステップ２７で、共有鍵を増幅鍵の長さまで短縮することで、外部データ処理装置１２への情報漏洩を最小限に抑える。このために、以下の（１８）を一例とする、ランダム２進テプリッツ行列Ｔ

【数５８】

$$T=\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \quad (18)$$

が求められ、公開共有される。このテプリッツ行列Ｔは、その第１の行及びその第１の列によって一意に識別可能である。したがって、このテプリッツ行列Ｔを共有するためには

、第１の行及び第１の列のみを含む（暗号化された）ハッシュデータを送信すれば十分である。増幅鍵は、このテプリッツ行列Ｔを共有鍵に乗算する、好ましくは左乗算することによって求められる。テプリッツ行列Ｔの行番号は、第２の量子相互情報量Ｉ（Ａ：Ｅ）の推定に依存するため、推定された情報漏洩が大きいほど、増幅鍵の長さは短くなる。

【０１４３】

暗号化にワンタイムパッド方式が用いられているが、以前にセキュアであった増幅鍵の特定の情報が（暗号化なしで）公開送信されているような状況では、相関データの暗号化はとりわけ有用であり得る。増幅鍵のある桁位置に関する情報漏洩があれば、結合確率

【数５９】

$$p^{E}{}_{(k)}$$

が変化するため、これにより、外部データ処理装置１２で量子一括測定を実行することができるようになる。ここでもやはり、ｌビットの初期鍵量が漏洩すると、盗聴装置にｌビットを超える情報を提供する可能性がある。ただし、相関データを暗号化すると、量子一括測定の実行は不可能になるが、増幅鍵は依然として、提案している本方法に従って配送され得る。

【０１４４】

ワンタイムパッド方式を用いると、比較的大量の鍵データが必要となり、鍵利得が減少する。このため、ＡＥＳなどの暗号化方式が好ましい場合がある。とりわけ、ここでの暗号化方式は、外部コヒーレント状態｜±α$_{E}$〉の保存時間の間に、外部データ処理装置１２によって暗号化が破られることのないようにする必要がある。

【０１４５】

図４は、従来型の量子鍵配送及び提案している本方法の通信チャネル長ｌの関数としてシミュレートされた、鍵レートｒを示すグラフ図である。ここでのチャネル損失は、光ファイバの減衰係数が

【数６０】

$$\delta \approx 0.2\,\mathrm{dB/km}$$

である。

【０１４６】

【数６１】

$$\mu_A \mapsto \mu_A 10^{-\delta\, l/10}$$

によってもたらされる。

【０１４７】

第１の曲線４０は、Ｂ９２様のプロトコルにおいて提案している本方法の鍵レートを表し、第２の曲線４１は、従来型のＢ９２様の量子鍵配送方法における鍵レートを表し、第３の曲線４２は、提案している本方法と従来型の量子鍵配送との間の鍵レート比を表す。第３の曲線４２は長いチャネル長ｌにおいて、鍵利得の７０％超に相当する１．７５に近似する鍵レート値に近付きつつある。第１の曲線４０及び第２の曲線４１については、第２のデータ処理装置１１の確定結果による確率ｐ$_{conc}$が考慮され、以下の式（１９）のようになる。

【０１４８】

【数６２】

$$r = p_{conc}\left(1 - \mathrm{leak}(q) - I(A:E)\right)$$

$$= \left(1 - e^{-2\mu_A 10^{-\delta l/10}}\right) \cdot \left(1 - \mathrm{leak}(q) - I(A:E)\right) \quad (19)$$

【０１４９】

第１のデータ処理装置１０における強度μ$_A$は、チャネル長ごとに最適化されている。式（１９）を単純化するために、チャネル誤り率ｑが０であると仮定している。ただし、任意の実用的な方程式では、チャネル誤り率ｑは正となる。したがって、相関情報の暗号化は、鍵レートｒを増大させるのに有用であり得る。

【０１５０】

＜ＢＢ８４プロトコル＞

以下では、ＢＢ８４プロトコルを使用する本方法の、さらに別の実施形態について説明する。ステップ２１～２７は、Ｂ９２様のプロトコル実施形態に応じて実行されるべきである。ステップ２１～２７におけるＢ９２様のプロトコル実施形態との相違点は、以下の通りである。Ｂ９２様のプロトコルとは対照的に、単一光子型のＢＢ８４プロトコルには、ビーム分割攻撃のような単純な攻撃形式が存在しない。

【０１５１】

第２のステップ２２で、以下の（２０）のような第１のフォトニック量子状態

【数６３】

$$\left\{ |0\rangle, \quad |1\rangle, \quad |+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \right\} \quad (20)$$

が、第１のデータ処理装置１０から第２のデータ処理装置１１に送信される。第１のフォトニック量子状態はそれぞれ、水平偏光状態の光子、垂直偏光状態の光子、対角偏光状態の光子、及び反対角偏光状態の光子に対応してもよい。２つの測定基底＋，×、即ちＨＶ（水平／垂直）基底＋と、ＡＤ（反対角／対角）基底×とが使用されている。桁位置の共有量子状態は、フォトニック古典量子状態として、以下の（２１）のように記述される。

【０１５２】

【数６４】

$$1/4\ \left(|0_+\rangle\langle 0_+|_A \otimes |0\rangle\langle 0|_B \quad + \quad |1_+\rangle\langle 1_+|_A \otimes |1\rangle\langle 1|_B \right.$$
$$\left. + |0_\times\rangle\langle 0_\times|_A \otimes |+\rangle\langle +|_B \quad + \quad |1_\times\rangle\langle 1_\times|_A \otimes |-\rangle\langle -|_B\right). \qquad (21)$$

【０１５３】

量子一括攻撃のシナリオでは、アンシラのフォトニック量子状態が各フォトニック古典量子状態に付加され、次いで外部データ処理装置１２によってユニタリ演算が実行され、結果として生じる状態がもつれていく。第１のデータ処理装置１０、第２のデータ処理装置１１、及び外部データ処理装置１２間の全体の共有状態は、以下の（２２）によって得られる。

【０１５４】

【数６５】

$$\frac{1}{4}\Big(|0_+\rangle\langle 0_+|_A \otimes |\Psi_{0_+}\rangle\langle\Psi_{0_+}|_{BE} + |1_+\rangle\langle 1_+|_A \otimes |\Psi_{1_+}\rangle\langle\Psi_{1_+}|_{BE}$$

$$+ |0_\times\rangle\langle 0_\times|_A \otimes |\Psi_+\rangle\langle\Psi_+|_{BE} + |1_\times\rangle\langle 1_\times|_A \otimes |\Psi_-\rangle\langle\Psi_-|_{BE}\Big). \quad (22)$$

【０１５５】

第３のステップ２３で、以下の（２３）の測定演算子が対応するＢＢ８４による観測可能量Ｍを使用して、第２のデータ処理装置１１において第２のフォトニック量子状態が測定される。

【０１５６】

【数６６】

$$M_0 = \frac{1}{2} | 0 \rangle\langle 0 |, \quad M_1 = \frac{1}{2} | 1 \rangle\langle 1 | \quad M_+ = \frac{1}{2} | + \rangle\langle + | \quad M_- = \frac{1}{2} | - \rangle\langle - | \quad (23)$$

【０１５７】

続いて、外部データ処理装置１２における外部フォトニック量子状態が、以下の（２４）によって記述され、

【０１５８】

【数６７】

$$\rho_0^E = (1-q) \ | \psi_0 \rangle\langle \psi_0 | + q | \theta_0 \rangle\langle \theta_0 |,$$

$$\rho_1^E = (1-q) \ | \psi_1 \rangle\langle \psi_1 | + q | \theta_1 \rangle\langle \theta_1 |,$$

$$\rho_+^E = (1-q) \ | \psi_+ \rangle\langle \psi_+ | + q | \theta_+ \rangle\langle \theta_+ |,$$

$$\rho_-^E = (1-q) \ | \psi_- \rangle\langle \psi_- | + q | \theta_- \rangle\langle \theta_- |, \quad (24)$$

【０１５９】

ここで、第２のデータ処理装置の誤り確率はｑである。

【０１６０】

第４のステップ２４で、第１のフォトニック量子状態の生成に使用される量子生成パラメータ（即ち、第１の量子基底設定値）を示す第１の暗号化信号が、第１のデータ処理装置１０において初期鍵を使用して生成され、次いで第２のデータ処理装置１１に送信される。これとは逆に、第２のフォトニック量子状態の測定に使用される量子測定パラメータ（即ち、第２の量子基底設定値）を示す第２の暗号化信号が、第２のデータ処理装置１１において初期鍵を使用して生成され、次いで第１のデータ処理装置１０に送信される。

【０１６１】

第１の量子基底設定値のうちの対応する１つと第２の量子基底設定値のうちの対応する１つとが一致しない状態の、第１の生信号及び第２の生信号における一致しない桁位置が破棄され、これにより、第１の照合信号及び第２の照合信号がそれぞれ生成される。

【０１６２】

第１又は第２の量子基底設定値を把握せずに０と１とを区別するために、非直交の外部フォトニック量子状態

【数６８】

$$(\rho_0^E + \rho_+^E) \ / \ 2$$

及び

【数６９】

$$(\rho_1^E + \rho_-^E) \ / \ 2$$

が外部データ処理装置１２において識別される必要がある。これは、第３のデータ処理装置１２に第１又は第２の量子基底設定値が設けられる場合、追加の外部フォトニック量子状態

【数７０】

ρ_{O}^{E}

及び

【数７１】

ρ_{I}^{E}（又はρ_{+}^{E}及びρ_{-}^{E}）

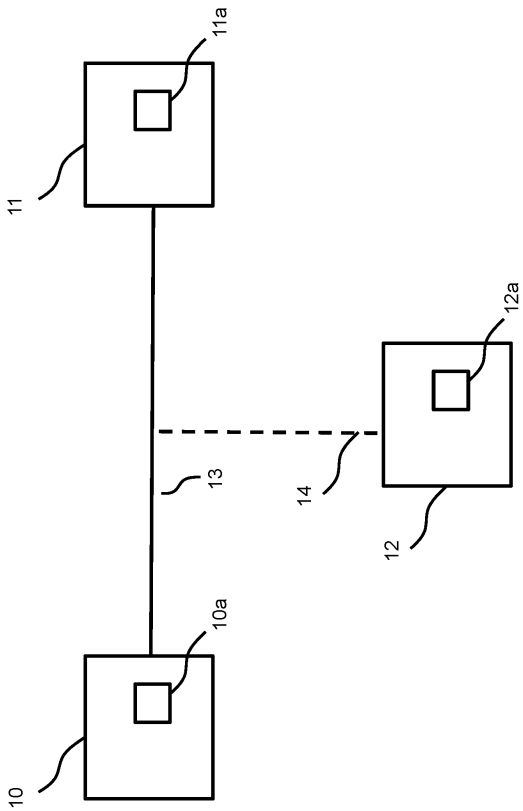
を識別するよりも困難である。したがって、第１又は第２の量子基底設定値は非公開であるとともに、桁位置も一致していなければならない。

【０１６３】

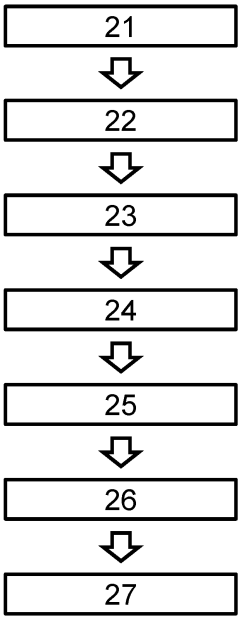
本明細書、図及び／又は特許請求の範囲に開示された特徴は、単独で、又はそれらを様々に組み合わせて取り入れられる、様々な実施形態を実現するための材料であってもよい。

【図面】

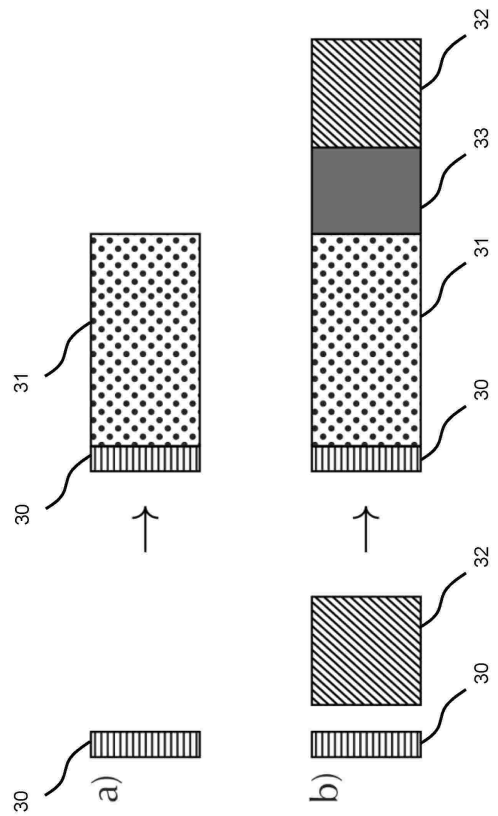
【図１】


11a
11
12a
13
14
12
10a
10

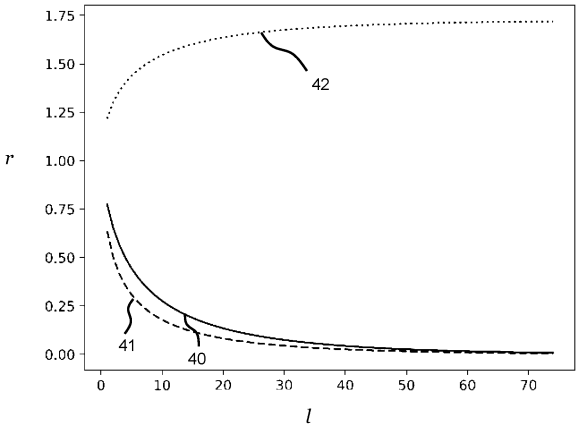
【図２】


21
22
23
24
25
26
27

【図３】


32
33
31
30
31
30
32
30
30
a)
b)

【図４】


1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
r
42
41
40
0
10
20
30
40
50
60
70
l

フロントページの続き

(56)参考文献　特開２０１７－１６９１８７（ＪＰ，Ａ）
特表２００７－５１１９５６（ＪＰ，Ａ）
特表２０１１－５１０５８１（ＪＰ，Ａ）
特開２００５－１１７５１１（ＪＰ，Ａ）
特表２０１９－５１７１８４（ＪＰ，Ａ）
米国特許出願公開第２０１７／０２６４４３３（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／１２