ライセンス情報番号：L2008003649

秘密鍵を交換する必要のない量子暗号通信方法

出　願　人：国立大学法人奈良先端科学技術大学院大学

本発明は、量子暗号を用いた量子暗号通信方法である。量子ビットとして光子を用い、量子ビットの量子状態を変える量子操作として光子の偏向角を変える回転操作を利用する。秘密情報は1個の光子の偏光角で表される。S1：秘密情報に応じた偏光角を持つ1個の光子が入力されると、送信者はこの秘密光子の偏光角をランダムに選定した角度だけ秘密光子に回転操作を施す。この回転操作が送信者による暗号化Aであり、その操作量（回転角）が暗号化Aの秘密鍵である。暗号化した秘密光子を光伝送路で受信者に送信する。S2：受信者は、その偏光角を秘密光子に対しランダムに選定した角度だけ回転操作を施し（暗号化B）、その状態の秘密光子を返信する。S3：送信者は、自らが実行した回転操作を元に戻すように秘密光子を先と逆方向に回転させる操作を行う。この操作は暗号を解く復号化aである。S4：受信者は、再送されてきた暗号化Bの状態の残っている秘密光子に対し、復号化bを行う。これにより、秘密光子の偏光角は元の秘密情報のみを有する状態に戻る。この秘密光子を出力し、例えば量子コンピュータの入力として利用する。これにより1量子ビットの通信が完了する。秘密鍵は、受送信者共に共有する必要がないため、傍受者が秘密鍵から暗号を解くことはできない。また受信者になりすます場合についても、おとりの光子（デゴイ）を秘密光子の前後に付加し、解読を防ぐことができる。

patent review

ユーザー業界	活用アイデア
情報・通信　生活・文化	**金融情報の通信** ○量子コンピュータを用いて、世界各地の気象や経済・収穫状況を各種の予測モデルを駆使しながら計算する。その結果から経済状況を予測し、投資などの金融情報を、傍受されることなく暗号通信する
情報・通信　その他	**軍事情報の通信** ○量子コンピュータを用いて、ミサイル弾道位置や潜水艦などの位置を計算し、その結果を、傍受されることなく時々刻々暗号通信する

market potential

現在開発段階である量子コンピュータが実用化されると、宇宙的・天文学的計算を行えることで、想像もしなかった様な世界を創出できる。人類の叡智を超えたコンピュータになると予想されるが、量子コンピュータは核兵器・遺伝子工学と同じく人類にとって第三のパンドラの箱となる諸刃の剣となる可能性がある。また安全性が保証されている公開鍵暗号方式の一つである「RSA暗号方式」も、このコンピュータでは、計算速度が飛躍的に早くなるため、安全性の保証はなくなる。

本発明による量子暗号通信方法では、「0」または「1」の古典情報と共に量子情報も送信できる。用途としては、主として信頼性が要求される外交・軍事面での利用からスタートすると思われるが、実装が比較的容易な通信方法であるため、金融などの民生面での利用も期待できる。

用　語　解　説

量子コンピュータ
理論上、現在の最速スーパーコンピュータで数千年かかる計算を数十秒で実行可能といわれている

量子
光や電波のような電磁波のように、波としての性質を持つと同時に粒子としての特徴をもつ

暗号
第三者に内容を知られないため、通信を見ても特別な知識なしに読めないように変換する変換アルゴリズム

原稿作成：青山　進　　有限会社青山技術士事務所

図１ 量子暗号通信法の例（基本例）

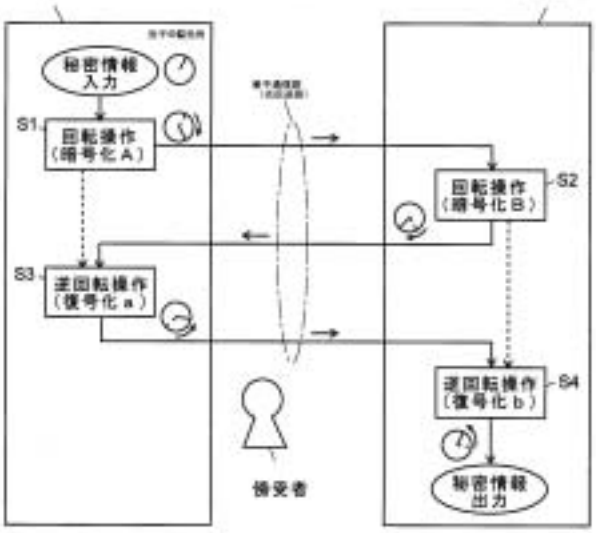
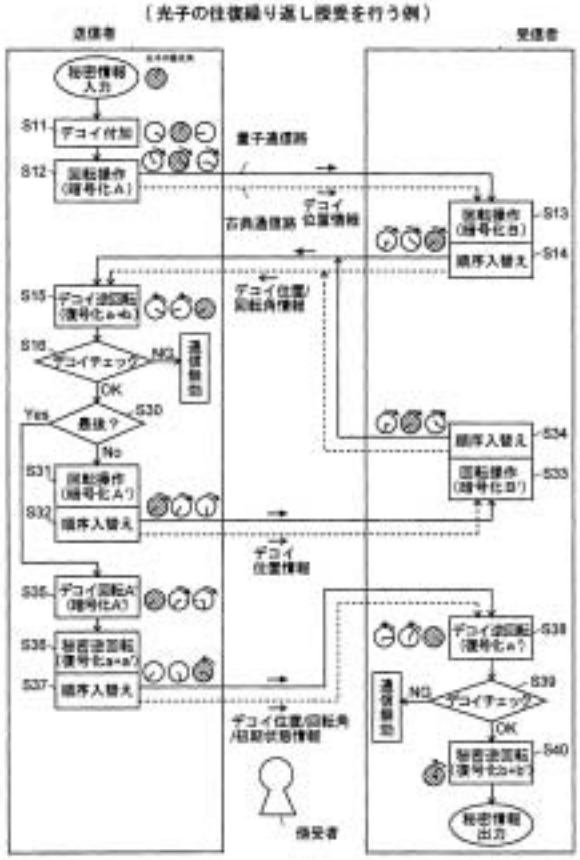


図２ 量子暗号通信法の例
（光子の往復繰り返し授受を行う例）



特　許　情　報

- 権利存続期間：出願中
- 実施段階：実施無し
- 技術導入時の技術指導の有無：応相談
- ノウハウ提供：応相談
- ライセンス制約条件：許諾のみ

○出願番号：PCT/JP2007/000086
○出願日/平19.2.15

○公開番号：WO 2007/105352
○公開日/平19.9.20

○特許番号：出願中
○登録日/出願中

特許流通データベース情報

- タイトル：量子暗号通信方法

- ライセンス番号：L2008003649

http://www.ryutu.inpit.go.jp/db/
からご覧になれます。

参　考　情　報

- 関連特許：なし
- IPC：H04L　9/12
- 参照可能な特許流通支援チャート
  ：17年度　電気31　不正アクセス侵入検知防御技術

皆様からのお問合せを、お待ちしています。

■この特許の問合せ先■

国立大学法人奈良先端科学技術大学院大学
研究協力課　産官学推進室
産官学推進係長
板原　広明
〒630-0101
奈良県生駒市高山町8916－5
TEL:0743-72-5930　FAX:0743-72-5015
E-mail:k-sangaku@ad.naist.jp

もしくはお近くの特許流通アドバイザー（P119をご覧下さい）にご連絡下さい。