様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　５　月　２０　日現在

機関番号：　１４４０１
研究種目：　基盤研究(C)
研究期間：　2012～2014
課題番号：　２４５６００４５

研究課題名（和文）差動位相シフト量子鍵配送システムの高性能化に関する研究

研究課題名（英文）Study on improving system performance of differential-phase-shift quantum key distribution

研究代表者

井上　恭（Inoue, Kyo）

大阪大学・工学（系）研究科（研究院）・教授

研究者番号：１０３９３７８７

交付決定額（研究期間全体）：（直接経費）　　4,100,000円

研究成果の概要（和文）：量子力学の原理に基づき絶対に安全な暗号通信を実現する量子暗号、特に簡便さを特長とする差動位相シフト（DPS）量子鍵配送(QKD)に関連する技術について研究した。システム性能（伝送距離、データ速度）を向上させる改良版の考案・性能評価、現実の状況に即した状況下でのシステム性能評価、などを行った。また、実用性の高いQKD方式として、通常の光通信システムの装置構成を用いて量子暗号通信を実現する新しいQKD方式を提案・性能評価を行った。

研究成果の概要（英文）：We have studied differential-phase-shift (DPS) quantum-key-distribution (QKD) related technologies. (1) “Intensity-modulated DPS-QKD” and “Measurement-device-independent DPS-QKD” have been proposed, which are modified to improve the system performance. (2) The DPS-QKD system performance considering phase fluctuation, that considering bit-error-rate fluctuation, and the robustness of DPS-QKD systems with power monitoring against blind attacks have been clarified, assuming practical situations. (3) “Intensity-modulation/direct-detection QKD” was proposed and evaluated, which features practicality employing apparatus used in conventional optical communication systems. (4) QKD systems multiplexing a quantum channel and a classical channel over one transmission fiber have been investigated, which is desirable in system implementation, where time-division-multiplexing and wavelength-division-multiplexing are assumed.

研究分野：　光通信

キーワード：　量子暗号通信

１．研究開始当初の背景

量子力学の原理に基づき絶対的に安全な暗号通信を提供する量子暗号（より正確には量子鍵配送：ＱＫＤ）は、1984 年の最初のプロトコル（BB84）の提案以来、新規プロトコルの提案、安全性に関する理論研究、実証実験、などが進められ、本研究開始時には現場環境下でのフィールド実験が行われるまでに至っている。しかしながら、そのシステム性能（秘密鍵生成速度、伝送距離）は実用に供するには不十分であり、また、装置構成が複雑かつ高価なものとなっている。そのため、実用化の可否は不明という状況であった。

２．研究の目的

上記状況を背景に、本研究は実用システムに向けた QKD 技術を研究・開発することを目的とした。

QKD にもいくつかの方式があるが、本研究では、差動位相シフト（DPS）QKD と呼ばれる方式を研究対象とした。QKD 分野では、安全性理論が確立しているという点から、BB84 方式が主流として研究されている。これに対し DPS-QKD 方式は、絶対安全性では劣るものの、装置構成が簡便という特長を有する。実用システム志向という立場から、本研究では DPS-QKD 方式を採り上げ、この QKD 方式のシステム性能を向上させることを目的とした。より具体的には、位相変調 DPS-QKD、強度変調 DPS-QKD、デコイ DPS-QKD、巨視的 DPS-QKD、といった各種改良方式について検討し、そのシステム性能を評価することとした。

加えて、単一光子検出器の性能向上も研究目的とした。QKD では、超微弱な光子状態を用いて秘密鍵情報を伝達する。そのため、単一光子検出器が QKD のシステム性能を決める大きな要因となる。そこで、単一光子検出器の性能向上を目指した。

３．研究の方法

研究リソースに限りがあるため、主として計算機シミュレーションにより研究を進めた。但し、小規模な実験、具体的には、シミュレーション計算に必要な自然ラマン散乱効率の測定[研究成果(4)]、及び APD 単一光子検出器の基本動作検証実験[研究成果(8)]は、研究室保有の実験装置を用いて実施した。

４．研究成果

当初の研究目的は、上記のように主として改良 DPS-QKD 方式の提案・システム性能であったが、それを進める過程で、実システムに即した状況下における QKD 性能を見極めることが重要であることに気付き、その観点からの研究も行った。さらに、研究期間中に、当初目的には無い方式を思いつき、それらについても適宜検討した。以下、得られた研究成果を述べるが、このような事情のため、上記研究目的とは必ずしも合致しないものとなった。

(1)強度変調 DPS-QKD：DPS-QKD では超微弱なコヒーレントパルス列を送受信して秘密鍵を生成する。この信号パルス列を 10-20 パルスごとにフレーム化し、各フレームの強度をランダムに割り当てる改良方式を考案した。このようにすると、盗聴者には各パルスの強度が不明であるため、従来の強度一定 DPS 方式よりも盗聴が困難となる。この強度変調 DPS-QKD 方式の性能評価を行い、従来方式よりも高性能となることを明らかにした。但し、本研究期間内では最終結果を得るまでには至らず、未発表に留まっている。

(2)レーザ光源を用いた DPS-QKD のシステム性能：DPS-QKD システムの伝送距離は、連続クリック攻撃と呼ばれる盗聴法により制限されることが知られている。但しそこでは、理想的なコヒーレント状態を用いた DPS-QKD システムが想定されていた。しかしながら、実際のシステムではスペクトル線幅が有限であるレーザ光が用いられており、理想的なコヒーレント状態ではない信号光により QKD 伝送が行われる。そこで、位相揺らぎのある光源を用いた DPS-QKD システムに対する連続クリック攻撃の盗聴能力を詳細に解析し、これによる伝送距離制限を再検討した。その結果、連続クリック攻撃は DPS-QKD 伝送距離の制限要因とならないことを明らかにした。[雑誌論文①、学会発表④]

(3)DPS-QKD に対するブラインド攻撃対策：DPS-QKD システムに対するサイドチャンネル攻撃として、強いパルス光を単一光子検出器に照射することにより、光子検出動作を外部から任意に操作する盗聴法が知られている。この盗聴法を実行するのに必要な光パワーを詳細に検討し、簡易な光パワーメータを用いて受信装置への入力光パワーをモニターすれば、この盗聴法を検知できることを示した。[学会発表⑤]

(4)量子/古典多重 DPS-QKD システム：QKD システムは、量子状態を転送する量子チャンネルと鍵生成情報や制御情報を転送する古典チャンネルから構成されている。通常、この２チャンネルは、転送される信号パワーレベルが桁違いに異なるため、別々の伝送路上に実装される。これを１本の光ファイバで多重伝送できれば、システムの利便性・経済性向上が期待される。そこで、量子/古典チャンネル多重伝送方式について検討した。多重方法としては、時分割多重方式と波長多重方式を採り上げた。前者では古典信号光のレイリー散乱光が、後者では古典信号光をポンプ光とする自然ラマン散乱光が、量子チャンネルの劣化要因となる。量子チャンネルの劣化が許容範囲に収まるシステム動作条件を検討

し、多重可能な古典チャンネルの伝送容量を明らかにした。特に波長多重方式については、量子/古典チャンネルの波長間隔が狭いときの自然ラマン発生効率を実験的に求め、その結果を基に、十分なデータ速度の古典信号が多重伝送可能であることを示した。[学会発表①③]

(5)誤り率揺らぎを考慮した DPS-QKD システム性能：QKD では、盗聴が行われるとビットエラーが生じることから盗聴を検知するが、もともとのシステムエラーがあると、これに紛れた一部盗聴が可能である。この場合、システムエラーが盗聴エラーに全て置き換えられたとして部分盗聴量を見積もるのが通例であるが、現実的な状況では、これは過大評価となる。そこで、システムエラーの揺らぎに紛れて部分盗聴が行われるという想定下での DPS-QKD 性能を再検討し、従来の想定下よりも伝送距離が長くなることを示した。[学会発表⑨]

(6)巨視的 QKD 方式：QKD では、単一光子または超微弱光により秘密鍵情報を伝送する。そのため、実装にあたっては、高度な光検出技術が必須となっている。これに対し、通常の光通信で用いられているパワーレベルで QKD 機能を実現する方式を提案し、そのシステム性能を評価した。その結果、中・短距離であれば、秘密鍵配送が可能であることが明らかとなった。これまでの QKD 方式より性能は劣るものの、 通常光通信システムの装置構成をそのまま用いることを特長としており、実用性の高い方式といえる。[学会発表②⑦]

(7)測定装置無依存 DPS-QKD：最近、QKD 分野では、測定装置の不完全性につけ入る盗聴法を排除するため、測定装置の特性・性能に依らない秘密鍵配送を可能とする測定装置無依存 QKD が話題となっている。そこで、本研究で取り扱っている DPS プロトコルに基づく測定装置無依存 QKD 方式を考案した。但し、現在のところ方式提案をした段階にあり、そのシステム性能評価は現在進行中である。[学会発表⑧]

(8)APD 単一光子検出器：QKD システムのキーデバイスである単一光子検出器の性能向上に関しては、様々な技術が研究・開発されているが、本研究では、APD 光検出器の出力段にローパスフィルタをだけという簡便な構成で動作速度を速める手法を提案し、実験により基本動作を確認した。但し、基本実証実験に留まり、どこまで性能が向上するか示すまでには至らなかった。[学会発表⑥]

５．主な発表論文等

〔雑誌論文〕（計 2 件）

① Toru Oka, Kyo Inoue, Quasi-unambiguous state discrimination with phase fluctuation, Opt. Commun., 査読有、vol. 304, 2013, pp. 136-142 DOI:10.1016/j.optcom.2013.04.067

②Kyo Inoue, Differential-phase-shift quantum key distribution, IEEE J. Sel. Top. Quantum Electron., 査読有、vol. 21、6600207 DOI:10.1109/JSTQE.2014.2360362

〔学会発表〕（計 9 件）

①橘　遼太郎、中谷　俊晴、井上　恭、アイソレータを挿入した DPS-QKD システムにおけるクロック信号の時間多重、第 73 回応用物理学会秋季学術講演会、2012、13a-B1-4

②岡　徹、井上　恭、２値強度変調/直接検波方式による量子鍵配送、第 60 回応用物理学会春季学術講演会、2013、30p-D1-1

③國安　崇行、井上　恭、狭波長間隔量子/古典波長多重量子鍵配送における自然ラマン散乱の影響、第 74 回応用物理学会秋季学術講演会、2013、16p-A14-12

④岡　徹、井上　恭、レーザ光を用いた差動位相シフト量子鍵配送の連続クリック攻撃による距離制限、第 74 回応用物理学会秋季学術講演会、2013、16p-A14-9

⑤永田　恒一、井上　恭、ハンディ光パワーメータを用いる DPS-QKD ブラインド攻撃対策、第 61 回応用物理学会春季学術講演会、2014、17a-D10-7

⑥徐　雪、井上　恭、ローパスフィルタによる APD 単一光子検出器のアフターパルス低減、第 61 回応用物理学会春季学術講演会、2014、18a-F9-3

⑦生田　拓也、井上　恭、過剰雑音及びビットエラー分布を考慮した光プリアンプを用いない IM/DDQKD、応用物理学会学術講演会、第 75 回応用物理学会秋季学術講演会、2014、18p-C2-4

⑧井上　恭、測定装置無依存 DPS 量子鍵配送、第 75 回応用物理学会秋季学術講演会、2014、18p-C2-3

⑨生田　拓也、井上　恭、エラーレート揺らぎを考慮した現実的想定化における DPS-QKD の性能、第 62 回応用物理学会春季学術講演会、2015、11a-A17-6

〔図書〕（計 1 件）

井上　恭、朝倉書店、光科学の世界、2014、pp. 2-14

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
井上研ホームページ：
http://www1b.comm.eng.osaka-u.ac.jp/

６．研究組織
(1)研究代表者
井上　恭（INOUE, Kyo）
大阪大学・大学院工学研究科・教授
研究者番号：1039787

(2)研究分担者
無し

(3)連携研究者
無し