様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 １４ 日現在

機関番号：８２６３６
研究種目：若手研究
研究期間：2021～2022
課題番号：２１Ｋ１４１６３

研究課題名（和文）物理レイヤ暗号による高秘匿衛星通信技術の確立

研究課題名（英文）Development of high-secure satellite communication schemes based on physical-layer cryptography

研究代表者

遠藤　寛之（Hiroyuki, Endo）

国立研究開発法人情報通信研究機構・量子ICT協創センター・研究マネージャー

研究者番号：５０８０９７０４

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：物理レイヤ暗号は、衛星－地上局間のレーザ通信のように指向性が高く視野が確保でき、盗聴者の盗聴能力に合理的な制約を課すことができる状況下において、高速・長距離な鍵共有を可能とする技術である。衛星による安心・安全なネットワークのグローバル化に資する技術であると期待される一方で、その衛星通信への応用には検討すべき事項が山積している。そこで、本課題では、より一般的な盗聴方法に対しても安全である新しい鍵共有技術の開発、有限の送信パルス数に対する性能評価方法の開拓、地上ビル間量子信号伝送実験から得られたデータに基づく性能検証、開発中の衛星搭載用装置を想定した静止軌道－地上間鍵共有の実現性検討に取り組んだ。

研究成果の学術的意義や社会的意義
本課題から得られた知見から、高速・遠距離かつどのような計算機でも不当に解読できない鍵共有技術の安全性の向上や、実用的な評価が可能となり、さらには静止軌道－地上間での鍵共有の可能性も見出された。これらの成果により、国産技術によるグローバルスケールの安心安全なネットワークの構築がより現実的なものとなった。

研究成果の概要（英文）：Since the channel is highly directional and line-of-sight, it is reasonable to assume that an eavesdropper is hard to fully access a free-space optical link between Alice and Bob without being found. Physical-layer cryptography employs this assumption and hence could achieve much more improved key generation performance. Although, this scheme is expected to construct a global-scale secure network using satellites, there is a lot of issues to be addressed for the implementation of the scheme in the satellite communications. So, we worked on the development of a new key-generation scheme secure against general eavesdropping, the formalization of a practical performance evaluation method with the finite transmission pulses, the performance verification using the data obtained from the long-range quantum signal transmission experiment between the buildings, and the feasibility study of GEO-ground key-generation based on the instruments which is being developed.

研究分野：衛星通信

キーワード：物理レイヤ暗号　量子鍵配送　衛星光通信

１．研究開始当初の背景

人工衛星による情報通信技術は、衛星データビジネスや複数衛星による通信網などといった宇宙産業のキーテクノロジーとなりつつある。人工衛星というシビアな環境下での高速通信を実現するためには、高速・大容量なだけではなく、コンパクトかつ高電力効率な通信技術が必要となる。そのような要求を満足させる通信技術として、レーザなどの光による無線通信である、光空間通信が注目されている。光空間通信の重要な特徴として、広がりの狭いレーザビームにより、送受信者の見通しを確保しながら行われることが挙げられる。この特徴により、悪意ある第三者の実施可能な攻撃を見通し外からの盗聴に限定できるなど、起こり得る盗聴リスクの想定が容易になる。提案者はこれまで、この光空間通信の特徴に着目し、その安全性をいかなる計算機でも不当に解読できないまでに高めることのできる、物理レイヤ暗号と呼ばれる技術を研究してきた。物理レイヤ暗号では、送信者(アリス)は光強度が制限されたパルス信号で鍵の素となる乱数ビットを受信者(ボブ)へと送付する。アリスとボブは公開通信路を通した情報交換を伴う鍵蒸留処理を実施することにより、共有した乱数ビットから最終鍵を作り出す。この流れは量子鍵配送と同様であるが、盗聴者(イブ)の盗聴能力に基づいて送信光強度を適切に調整することにより、盗聴リスクに見合った速度・伝送距離での秘匿通信を実現できる。実際、物理レイヤ暗号によって静止軌道－地上間通信でも現実的な伝送速度の秘匿通信を実現できることを見出してきた。この結果は、物理レイヤ暗号が、高速・大容量な衛星通信ネットワークで今後やり取りされる可能性が高い、重要な情報をサイバー攻撃から守るのに適した技術であることを示している。

以上のような利点にも関わらず、物理レイヤ暗号の衛星通信への実装可能性は自明ではない。これは、実際の装置に適用可能な評価理論が確立していないことや、大気ゆらぎのような衛星光通信に特有な現象が物理レイヤ暗号の性能に与える影響が明らかになっていないことによる。これらの不確定事項を明確にして、衛星光通信のための物理レイヤ暗号、すなわち衛星光物理レイヤ暗号の実現可能性を示すことが、物理レイヤ暗号実用化に向けた課題として残されている。

２．研究の目的

研究開発当初と比較すると、日本や各国における衛星量子暗号の研究開発がより加速化してきており、日本独自の技術の鍵共有技術である物理レイヤ暗号の研究開発も、より実用的な方向にシフトしていく必要性に迫られてきた。そのためには、提案当初に掲げていた課題に加えて、一般的な盗聴戦略に対しても安全であり、従来の量子暗号とも接続性のある鍵共有技術の開発、実際の衛星量子暗号通信を見込んでより長距離環境での実証試験の実施、などを本課題の目的として再設定した。

具体的には以下の 4 つの課題に取り組むことを目的とした。

(1) **新しい鍵共有技術の開発**：物理レイヤ暗号と同様の、送受信者の見通しが確保されており盗聴者の攻撃を盗聴に制限できるという設定は踏襲しつつも、量子力学の原理に基づく盗聴に対しても安全であり、なおかつ従来の量子暗号とも接続性のある、衛星量子通信向けの鍵共有技術を開発する。

(2) **物理レイヤ暗号の有限長評価法開拓**：実用的な物理レイヤ暗号システムの評価のために、アリスが有限個のパルスをボブに送付した場合の評価方法を確立する。

(3) **長距離伝搬データに基づく評価**：実験室内の模擬データではなく、長距離量子信号伝搬実験から得られた実験データに基づいて、物理レイヤ暗号や(1)で開発する新しい鍵共有技術の性能評価を実施する。

(4) **実際の装置に基づく静止軌道－地上間鍵共有の実現性検証**：本課題で対象とする鍵共有技術により、既存の量子鍵配送技術では実現困難となる、静止軌道－地上間での鍵共有の実現が期待される。その可能性を、実際に開発中の装置や大気ゆらぎのパラメータに基づいた回線計算に基づいて検証する。

３．研究の方法

(1) **新しい鍵共有技術の開発**　盗聴者が送受信者の見通し外でパッシブな盗聴のみを行うとする物理レイヤ暗号の問題設定に、従来の量子暗号の安全性証明手法を適用することにより、新しい情報理論的に安全な鍵共有技術を開発した。量子暗号の安全性証明手法を利用していることから、量子メモリなどを用いるような量子力学の原理に基づく一般的な盗聴に対しても安全性を証明できる。さらに、セキュリティパラメータと呼ばれる、量子暗号の安全性評価と共通した指標で安全性を評価できるため、既存の量子暗号ネットワークとの親和性も高い。この「見通し通信 QKD」と呼ばれる新技術の安全性の証明と、物理レイヤ暗号との性能比較を実施した。

(2) **物理レイヤ暗号の有限長評価法開拓**　物理レイヤ暗号の鍵蒸留処理の内、誤り訂正を担う情報整合と漏えい情報の除去を担う秘匿性増強とのそれぞれについて、復号誤り率と漏えい情報量とを送信光パルス数の指数関数で抑える手法が知られている。それらをまとめて用いること

により、ある所望の復号誤り率と漏えい情報量、そして送信光パルス数が与えられた際の物理レイヤ暗号の鍵生成レートを算出する方法を見出した。

(3) **長距離伝搬データに基づく評価**　大気ゆらぎの効果が物理レイヤ暗号や見通し通信 QKD に及ぼす影響を実伝搬データに基づいて検討し、これらの鍵共有技術の実現に必要な課題を抽出するために、提案者の所属機関が保有する電通大－情報通信研究機構(NICT)間 7.8km の光空間通信テストベッドにて実施された量子信号の伝送実験から得られたデータをこれらの鍵共有技術の立場から解析した。本量子信号伝送実験は、提案者の所属機関も参画機関の一つに名を連ねている総務省からの直轄委託課題「衛星通信における量子暗号技術の研究開発」にて開発した量子送信機と受信機の機能検証試験として、本提案より先だって行われたものである。電通大の 9 階建てビルと NICT の 6 階建てビルの屋上に設置されている全天候ドーム型送信機とコンテナ型受信機のそれぞれに、この量子送信機と受信機を設置した。電通大に設置された量子送信機は、ストレージに内蔵された乱数ビット列に基づいて、1GHz の繰り返し速度で生成される波長 1550nm の光パルスを位相変調する。これらの光パルスはコリメータを通して NICT 側へと照射される。NICT 側に設置されたコンテナ上部のスキャナに入射した光子はシングルモードファイバーへと結合され、ビルの地下 1 階に設置されている超伝導単一光子検出器へと導かれる。この検出器が出力する光子検出データから、量子信号受信確率、量子ビットエラー率、鍵生成レートといった、物理レイヤ暗号や見通し通信 QKD を特徴付ける諸量を評価した。

(4) **実際の装置に基づく静止軌道－地上間鍵共有の実現性検証**　提案者の所属機関も参画機関の一つに名を連ねている総務省からの直轄委託課題「グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発」で開発中の装置群を想定し、衛星光通信の分野でも用いられている回線設計の手法によって、静止軌道－地上間の損失の推定を行った。この総務省直轄委託課題では、アリスに相当する搭載用送信装置とボブに相当する可搬型光地上局を開発中である。前者の搭載用送信装置は送信するデータに基づいて変調された光信号を送信アンテナから送出する機能を有する。後者の可搬型光地上局は、天候などの環境条件に縛られないオンデマンドな量子通信の実施を企図してトラック上に構築された可搬型の光受信局であり、量子信号受信用の望遠鏡、環境要因によるビーム方向ずれを補正するための精追尾光学系、受信機への迷光を防ぐためのフィルタ群、そして受信装置からなっている。これらの装置のパラメータや大気による損失の推定値から算出された静止軌道－地上間の損失値に物理レイヤ暗号及び見通し通信 QKD の鍵生成レートの公式を適用することによって、これらの鍵共有技術の静止軌道－地上間における鍵生成速度を算出した。

４．研究成果

(1) **新しい鍵共有技術の開発**　見通し通信 QKD の基本設定は、アリスとボブは見通しが確保されている通信路(見通し通信路)と認証付きの公開通信路とで結ばれており、イブはアリスとボブから発見されないように、ボブの後方からの盗聴や散乱光の窃取など、見通し外から受動的な盗聴を実施するというものである。この受動的な盗聴は、アリスの直前で反射率η_{E}のビームスプリッタでモデル化する。このη_{E}を盗聴者通信路透過率と呼ぶ。アリスとボブは共有した乱数ビット列に対して鍵蒸留処理を実施することで、最終鍵を生成する。この基本設定や光子伝送のシーケンス、そして鍵蒸留処理による最終鍵の生成は物理レイヤ暗号と同様であり、二つの鍵共有技術は同時に実装することができる。しかし、情報整合の方法が制限される、漏洩した情報量の評価が異なるなど、鍵蒸留処理に若干の違いが表れる。情報整合の方法が制限されることは見通し通信 QKD の方が誤り訂正の性能が低いこと意味する。一方で、より一般的な盗聴に対しても安全な見通し通信 QKD の方が、同じη_{E}においても漏洩情報量の評価が厳しめとなる。そのため、鍵生成のパフォーマンスは物理レイヤ暗号の方が高く、二つの鍵共有技術の間にはパフォーマンスと安全性のトレードオフ関係が成立していると考えられる。

図 1 には複数のη_{E}に対して計算した、見通し通信 QKD(赤色)と物理レイヤ暗号(青色)の鍵生成レート理論値を示す。見通し通信路の損失が十分に小さい領域では、両者の鍵生成レートは主通信路の損失の増加に対して単調に減少していく。ただし、共通したη_{E}では、物理レイヤ暗号の鍵生成レートの方が見通し通信 QKD よりも大きい。特に、見通し通信 QKD の鍵生成レートは、見通し通信路の損失が増加して暗計数と受信光子数がほぼ同数になると、急激に 0 へと減少する。これは、上述したような、両者の鍵蒸留処理の違いに起因しており、両者の技術の間のパフォーマンスと安全性のトレードオフ関係を象徴する振る舞いである。図中には、ボブが受信しない光子を全てイブが収集できる場合も示している。こ

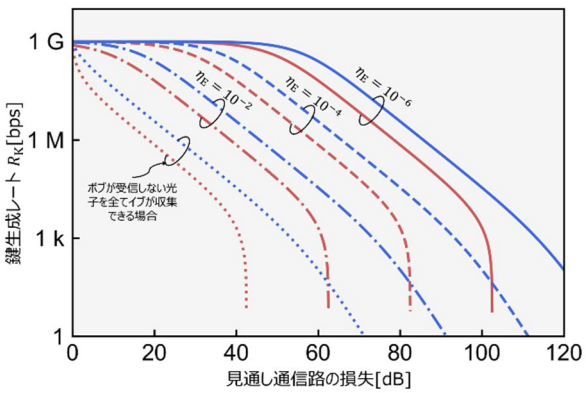

図 1. 物理レイヤ暗号と見通し通信 QKD の鍵生成レートの比較。

れはイブの攻撃方法は盗聴に仮定するものの、その盗聴能力は仮定しないという場合に相当する。このような一般的な場合においても、40dB という低軌道―地上間に相当する損失での鍵生成が可能となっている。

なお、図 1 に示した結果は漸近長解析と呼ばれ、伝送する乱数ビットが無限に長い場合における解析である。これに加えて、伝送する乱数ビットが有限である、より実用的な状況にも利用可能な評価式の導出にも成功している。

(2) **物理レイヤ暗号の有限長評価法開拓**　図 2 に、今回構築した手法により算出した、物理レイヤ暗号の有限長解析の結果を示す。通信路の設定は図 1 と同様であり、図 2 と同様の盗聴者通信路透過率η_Eについて計算している。送信パルス数の長さは、10^9(実線)、10^8(破線)、10^7(点線)、10^6(一点鎖線)とした。また、参考に漸近長解析の結果も示している。なお、復号誤り率と漏えい情報量は共に 10^{-9} と設定している。このパラメータの意味、特に量子暗号で用いられるセキュリティパラメータとの関係性の解明は今後の理論的な課題となる。

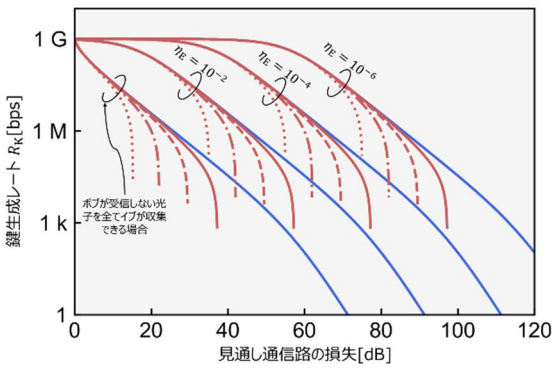

図 2. 物理レイヤ暗号の有限長解析の結果。

図 1 でも見たように、漸近長解析に基づく物理レイヤ暗号の鍵生成レートは見通し通信路の損失の増加に応じて単調的に減少していく。しかし、有限長解析により求められた鍵生成レートはある損失で急激に減少するふるまいを見せる。例えば、$\eta_E = 10^{-2}$の場合、漸近長解析のレートは見通し通信路の損失が-60dB よりも増加しても鍵を作ることができるが、送信パルス数の長さが 10^6 になってしまうと、低軌道衛星―地上間に対応する損失でも鍵を作ることは難しくなる。これらの計算からは、有限長のパルスしか送ることのできない実用的なシステムで漸近長に近いパフォーマンスを得るには、少なくとも 10^9 個のパルスを送らなければならないことが予測される。この量は非常に多いように見えるが、送信レートが 1GHz 程度という現行の量子暗号装置の性能を鑑みると十分に達成できるものである。このように、今回構築した手法により、より現実に即した物理レイヤ暗号の性能検証の議論が可能となった。今後、(1)で導出した見通し通信 QKD の有限長解析の結果とも比較することで、両者のトレードオフ関係についてより実用的な議論も可能となる見通しである。

(3) **長距離伝搬データに基づく評価**　量子信号伝送実験は 2021 年 2 月 8 日の昼間(10 時 21 分から 15 時 53 分)と夜間(19 時 34 分から 21 時 24 分)の二つのキャンペーンに分けて実施された。図 3 に、この量子信号伝送実験データの解析に基づいて計算された、見通し通信 QKD の鍵生成レートの推定値を、信号パルスの平均光子数μ_Aの関数として示す。この図では、盗聴者通信路透過率η_Eを 10^{-2} と仮定している。同時に、公式に基づいて計算した理論曲線も示している。理論曲線の計算に際して伝搬損失および単一光子検出器の暗計数率を実験データから推算している。昼間では夜間と比較して伝搬損失及び暗計数率が大きくなっているため、昼間の理論曲線の方が夜間のものよりも下方に位置している。夜間のキャンペーンのデータ(三角)は理論曲線とよく整合する一方で、昼間のキャンペーンのデータ(丸)は理論曲線から大きく逸脱する。この結果によると、夜間ではμ_A=10 とすることで 1kbps の情報理論的に安全な鍵を生成できる。しかし、昼はμ_A=30 としても、数 10bps まで鍵生成速度は落ち込む。これは、大気ゆらぎによる時刻同期の失敗によるものである。

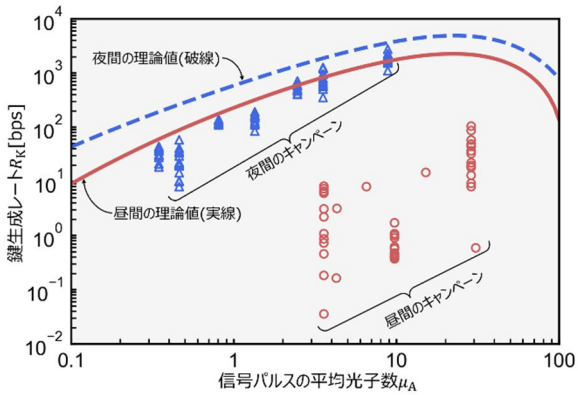

図 3. $\eta_E = 10^{-2}$における鍵生成レートの推定値。実線と破線は公式に基づいて計算された、昼間及び夜間のキャンペーンにおける理論値である。

以上の実験結果からは、損失-60dB という従来の量子鍵配送では鍵生成自体が困難になるような損失においても、見通し通信 QKD による情報理論的に安全な鍵生成の可能性を見出すことができた。特に、昼間においても数 10bps という低速度ながら鍵生成が可能であるという事実は、衛星―地上局間に関わらず、光空間通信による情報理論的に安全な鍵生成技術の発展に大きな意義を持つ。一方で、大気ゆらぎによるフェーディングによって、鍵生成速度が大きく劣化することも確認された。このことは、今回使用した実験装置には備わっていない捕捉追尾機構などによる見通し通信路の安定化の必要性を示唆している。また、安定な時刻同期法の開発も重要な研究開発課題となる。

図 4 には、夜間のキャンペーンについて、物理レイヤ暗号と見通し通信 QKD の鍵生成レート

推定値を同時に評価した結果を示している。盗聴者通信路透過率η_Eは$10^{-1.2}$と仮定している。物理レイヤ暗号(丸)と見通し通信QKD(三角)の鍵生成レートは平均光子数が小さい領域ではほぼ重なっている。しかし，平均光子数の増加につれて両者の乖離が顕著となり，やがては見通し通信QKDでは鍵生成が不可能であるが、物理レイヤ暗号では鍵生成が可能である領域が現れる。

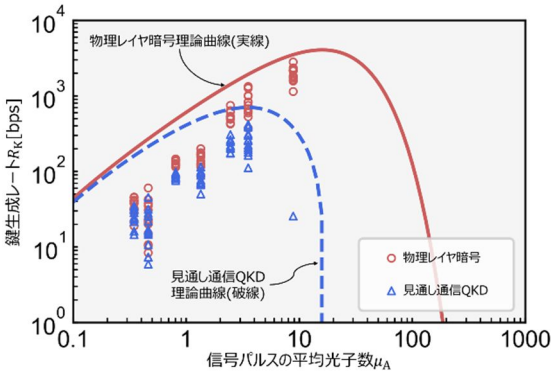

図 4. 実験データに基づく物理レイヤ暗号と見通し通信 QKD の鍵生成レートの比較。夜間のキャンペーンのみ示している。

この結果のように、見通し通信QKDと物理レイヤ暗号の同時実装により、より高い安全性を求める場合には前者を用い、ひとまずは鍵生成の成立を目指す、あるいはより高いスループットを求める場合には後者を用いるといった、幅広いユーザの要求に応える柔軟な運用が可能となる。この性質により、衛星を介したグローバルスケールのQKDネットワークの可用性を大いに高めるられる。ただし、図6にも見たように、見通し通信路の損失に対してη_Eが低い場合には、物理レイヤ暗号は鍵生成ができるものの、見通し通信QKDでは鍵生成ができないというケースも起こり得る。このような領域では安全性を妥協して物理レイヤ暗号を用いるか、あるいは鍵生成そのものを諦めなければならない。

(4)**実際の装置に基づく静止軌道－地上間鍵共有の実現性検証**　総務省からの直轄委託課題で開発中の装置群のパラメータから計算された静止軌道－地上間の損失値は、－85.28dBであった。ただし、光地上局が可搬型であるという特性を活かして、大気ゆらぎや天候条件は非常に良いものであると仮定して、大気ゆらぎの効果を算出している。図5には、物理レイヤ暗号(実線)と見通し通信QKD(破線)の鍵生成レートを、見通し通信路の損失の関数として、複数の盗聴者通信路透過率η_Eについて示している。また、従来の量子鍵配送の鍵生成レート(一点鎖線)も参考として示している。回線計算により求められた静止軌道－地上間の損失値は図中の点線により示されている。

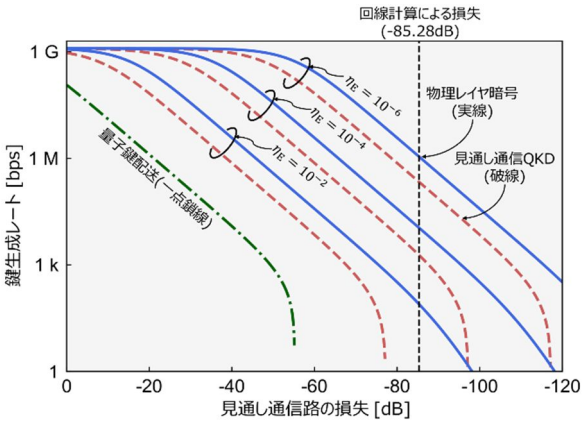

図 5. 鍵生成レート。光パルスの繰り返しレートを1.25GHz、光子検出器の暗計数を100Hz、量子効率を70%と仮定している。

図5中に示したη_Eのほとんどで、物理レイヤ暗号と見通し通信QKDの両者で鍵生成レートが0より大きい。特に、$\eta_E = 10^{-6}$という盗聴者がごく限られた能力しか持たない状況では、物理レイヤ暗号で約1Mbps、見通し通信QKDでも約200kbpsでの鍵生成が可能となっている。従来のQKDの鍵生成レートがおおよそ低軌道衛星の損失に相当する60dB付近の損失で急激に減少している事実と比較するとm非常に高いスループットであると言える。ただし、$\eta_E = 10^{-2}$では、物理レイヤ暗号は鍵生成ができるものの、見通し通信QKDの鍵生成レートは0となっている。上でも述べたように、このような領域では安全性を妥協して物理レイヤ暗号を用いるか、あるいは鍵生成そのものを諦めなければならない。なお、見通し通信QKDにより鍵生成が行えなくなる限界の盗聴者透過率の値を検証したところ、その値は$\eta_E = 10^{-2.82}$であった。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Endo Hiroyuki、Sasaki Toshihiko、Takeoka Masahiro、Fujiwara Mikio、Koashi Masato、Sasaki Masahide	４．巻 24
２．論文標題 Line-of-sight quantum key distribution with differential phase shift keying	５．発行年 2022年
３．雑誌名 New Journal of Physics	６．最初と最後の頁 025008～025008
掲載論文のDOI（デジタルオブジェクト識別子） 10.1088/1367-2630/ac5056	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 遠藤寛之，北村光雄，小澤俊介，清水亮介，藤原幹生，佐々木雅英
２．発表標題 見通し通信QKD実現に向けた量子信号伝送実験
３．学会等名 電子情報通信学会　衛星通信研究会
４．発表年 2023年

１．発表者名 遠藤寛之，佐々木雅英，藤原幹生
２．発表標題 回線計算に基づく静止軌道－地上間の物理レイヤ暗号と見通し通信QKDの実現性検討
３．学会等名 電子情報通信学会　衛星通信研究会
４．発表年 2023年

１．発表者名 遠藤寛之，北村光雄，小澤俊介，清水亮介，藤原幹生，佐々木雅英
２．発表標題 地上ビル間7.8㎞量子信号伝送実験に基づく物理レイヤ暗号と見通し通信QKDの性能比較
３．学会等名 電子情報通信学会　ソサイエティ大会
４．発表年 2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関