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 ２０ 日現在

機関番号：１０１０１
研究種目：基盤研究(S)
研究期間：2018～2022
課題番号：１８Ｈ０５２３７

研究課題名（和文）百年以上の超長期秘匿性を保証する情報通信ネットワーク基盤技術

研究課題名（英文）Information communication technology ensuring the long term security over a century

研究代表者
富田　章久（TOMITA, Akihisa）

北海道大学・情報科学研究院・教授

研究者番号：６０５０１４３４

交付決定額（研究期間全体）：（直接経費）　 148,200,000円

研究成果の概要（和文）：本研究は情報理論的に安全な暗号技術と量子暗号技術の融合によって超長期安全性を保証する情報通信ネットワーク基盤を構築することを目的とした．そのために，ネットワーク制御技術，データの統計処理技術，および必要な量子暗号鍵配送（QKD）技術の高度化を行い，情報理論的に安全なデータの中継と保存，処理（秘匿計算）・復元を行うネットワークの研究開発を行った．秘密分散とQKDを応用した中継ネットワークの実現，長距離化に向けた基盤技術の開発，連続量QKDの高度化と光通信との共存実証，および安全性理論の拡張といった研究成果をあげ，次世代セキュアネットワーク技術を確立した．

研究成果の学術的意義や社会的意義
ヒトゲノム情報など長期間にわたって秘匿性を保証する必要がある情報について，これまで数十年から百年以上安全に伝送，保管，処理する技術は知られていなかった．本プロジェクトは情報理論的安全なプロトコルを活用し，これと量子暗号鍵配送によって共有される乱数鍵を組み合わせることによって長期間の安全性を保証する量子セキュアネットワークを実現する技術を開発した．同時に，量子暗号鍵配送をネットワークの要求に応えるために高度化する技術も開発し，長距離化，高速化するための学理と技術を明らかにした．さらに，より現実的な状況でも安全性を解析できる安全性証明の理論的な拡張にも成功した．

研究成果の概要（英文）：This project aims to establish technological fundation of the communication network, where the long-term security is guranteed by integrating integrating information theoretically secure cryptography technology and quantum cryptography. To this end, we conducted research and development of networks for relaying, storing, processing (secure computation), and restoring data in the information theoretically secure manners. We improved the network control technology, data statistical processing technology, as well as quantum key distribution (QKD) technology. We have demonstrated secure data relay on the Tokyo-QKD-Network, by applying secret sharing and QKD. We also established technologies to extend the link distance, to improve key generating speed for continuous-wave QKD, and to realize co-existance with lightwave communication. We also expand security theory on QKD to consider more practical situations. The project has established a next-generation secure network technology.

研究分野：量子情報

キーワード：量子暗号　秘密分散　情報通信ネットワーク

１．研究開始当初の背景

近年，ゲノムデータや製薬情報など長期間秘匿性を担保する必要のある情報を電子的に伝送，保管，処理することが進められている．しかし，電子的データの利用が社会的な合意を得るためにはデータの安全性の保証が必要である．例えばゲノムデータはヒトの寿命を考えれば少なくとも百年は安全に保管されるべきである．ところが，暗号の世代交代がこれまで繰り返されてきたことを考えると，現在の技術で暗号化された情報が百年以上たった後も安全であるとは考えにくい．

そこで，いかなる技術的な進歩に対しても安全性が保証できる情報理論的安全な暗号技術を導入する．情報理論的安全な暗号プロトコルの代表的なものとして秘密分散がある．秘密分散においては，初期乱数（暗号鍵）を共有することができれば，これを用いて完全秘匿通信やデータ認証が可能なことが知られている．一方，量子鍵配送（QKD）は離れた二者間が情報理論的に安全な暗号鍵を共有することを可能にする．その安全性は物理的な原理に基づいているため，技術の進歩による危胎化のおそれはない．QKD システムの開発は各国で進められ，都市圏内や都市間ネットワークの構築も進められているが，ネットワークに期待される様々な機能の実現はなされていない．また，伝送距離の制限や擾乱に対する脆弱性といった量子情報技術の実用上の問題点の解決も不十分である．

そこで，我々は秘密分散に代表される情報理論的安全な暗号技術と QKD による鍵共有を融合させ，お互いの長所を生かしつつ欠点を補いあうことを考えた．これはある意味必然的な発展ではあるが，融合システムの実現に必要な QKD 技術の開発と現実的に意味のある融合システムの構築技術はこれまで検討されていなかった．

２．研究の目的

本研究では情報理論的に安全な暗号技術と量子暗号技術の融合システムを構築する．具体的には秘密分散と QKD の融合により**超長期安全性を保証する情報通信ネットワーク基盤**を構築することを目的とする．

このようなネットワーク基盤には現代暗号技術と量子情報技術の有機的な結合を前提としたシステム設計が必要である．そのために，ネットワーク制御技術，データの統計処理技術，および必要な QKD 技術の高度化を行い，情報理論的に安全なデータの中継と保存，処理（秘匿計算）・復元を行うネットワークを研究開発する．QKD 技術の高度化として，具体的には，損失や雑音に対する耐性を高め，従来の到達距離を超える伝送や既設の光通信とのファイバ共有を実現する．同時に，現実の装置の特性が従来の安全性証明で仮定されている理想的なものから外れることを考慮した，実装安全性保証に関する理論研究を行う．

３．研究の方法

秘匿情報通信ネットワークは秘密分散サーバを QKD リンクで結ぶことによって構成される．秘密分散とネットワーク制御を合わせてネットワーク構築が可能となる．QKD リンクは離れたユーザ間の秘密共有を可能にするための長距離リンクとユーザ-サーバ間，サーバクラスター内の通信を行う近距離高速リンクの 2 種類が必要になる．また，秘匿情報通信ネットワークにおいては実装安全性の保証が重要である．実験を担当する北海道大学・学習院大学・NICT と理論担当の富山大学が密接に連携して安全性保証技術を確立する．

本研究では，研究項目として(1)ネットワーク構築技術，(2)長距離 QKD 技術，(3)近距離高速 QKD 技術，(4) 秘密分散-QKD ネットワーク理論を設定した．

４．研究成果

(1) <u>ネットワーク構築技術</u>

秘密分散と QKD を融合した量子暗号ネットワークについて，安全なデータ中継を量子暗号ネットワーク上で実現する研究開発を進めた．我々は単なる組み合わせにとどまらず，古典的な暗号プロトコルを取り込むことで安全かつ高速な伝送・保管・処理が可能なシステムを構想し，「量子セキュアクラウド」と名付けた．特に，パスワード一つの情報で，図 1 に示すような，情報理論的安全にデータ伝送・保管・中継・認証できるシステムを核としてネットワークで利用する際に必要な機能を，量子暗号以外の暗号に関する研究成果を取り入れて実現したものである．

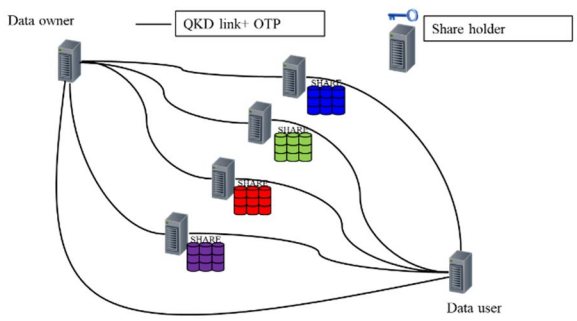

図 1　分散ストレージ＆データ中継構成図

ここでパスワードだけを長距離 QKD で受信者に渡すことができれば，量子セキュアクラウドをもちいて安全なデータ中継を実現することができる．我々は本研究開発により，世紀単位で秘匿性を必要とする情報の中継を可能とするシステムの完成を目指した．なお，研究項目の一つである**ネットワーク制御技術**は以下のデモンストレーションシステムの構築の過程で研究開発が行われた．

マルチユーザ化においては認証機能が重要である．正しい相手にパスワード情報を伝送する認証機能を持つシステムを開発した．その際，パスワードの格納用デバイスとしてスマートフォンを用いている．これにより，個人認証ばかりでなく，機器認証機能も追加することができ，より安全なシステムが構築できた．また，保管されたデータの完全性の担保は現代暗号分野も含め，活発な研究開発が行われている重要な機能である．本研究では量子暗号ネットワーク特有の機能である 安全な乱数供給が可能な機能を用いて，情報理論的安全なデータの完全性保証を第三者により実施できるシステムを開発した．これらの成果は SIP「光・量子を活用した Society5.0 実現化技術」において実施された POC（Proof-of-Concept）にも活用されている．

秘密分散を用いた**秘匿計算**を高速に行うために，信頼できるサーバ上で専用ハードウェア演算を行うシステムを開発した．信頼できる秘匿計算サーバからの出力データに，データの属性・データ閲覧者の権限により閲覧できる範囲を制御できるフィルタリング機能を実装した．秘密を分散したサーバ群と秘匿計算サーバ，秘匿計算サーバからユーザへの通信を QKD とワンタイムパッド(OTP)で行うことにより情報理論的安全かつ高速な伝送を可能にし，専用ハードウェアの高いスループットを損なわない高速秘匿計算システムが構築できた．

秘密分散を用いた**データ中継**は，パスワード１つだけを１リンクの QKD でユーザに伝送できれば実現可能である．現在 QKD ネットワークで利用されている“信頼できる局舎”を利用したネットワークを，信頼できる局舎の安全性に過度に依存しないデータ中継で置き換えることができる．我々は本システムを Tokyo QKD Network 上に実装し，情報理論的安全なデータ中継（リンクの距離の制限から 90km）での情報理論的安全なデータ中継のデモンストレーションに成功した．また実装ソフトウェアの高速化を進め，スループットとして 1Mbps 以上を実現した．

量子鍵配送ネットワーク上での秘密分散におけるシェアの Vernam’s one-time pad(OTP)暗号による高速伝送がスループットの向上のために必要であった．OTP 暗号は数学的処理は単純で高いスループットが期待できるが，一方でデータと同じサイズの鍵を取り扱う必要があり，高速実装は困難であった．我々は図 2 に示すシステム構成で OTP 暗号装置の高速化を通常のサーバを応用して実現し，2Gbps 以上のスループットが実現できた．この高速 OTP 暗号装置は我々が知る限り世界最速である．また本システムを利用し，4K 映像のリアルタイム伝送に成功した．また本システムはゲノムデータの秘匿化にも利用され，その成果は論文化された．

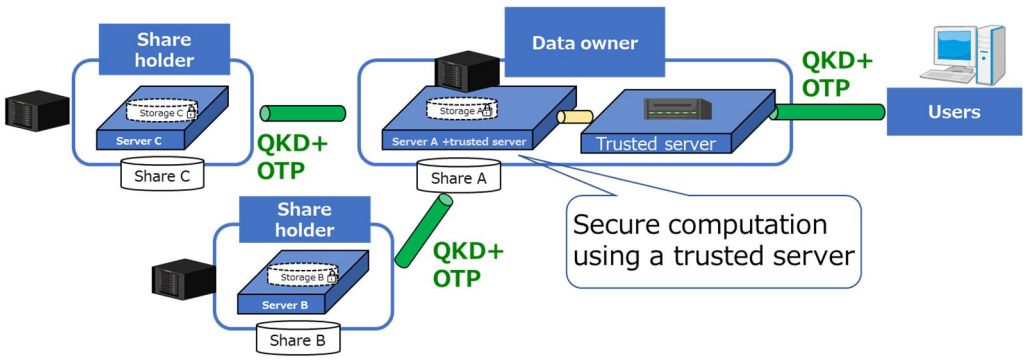

図 2　ゲノム解析データの秘匿伝送，処理概念図

(2)長距離 QKD 技術

まず，DV-QKDの長距離化を阻害する要因を考察した．送信機においては送出される光パルスに含まれる光子数が理想的な単一光子でないことがある．受信機においては光子検出器の暗計数による誤りの増大があげられる．

単一光子に近い光パルスを送出するための手法として，我々は量子もつれ光源を用いた BBM92 プロトコルを改良したプロトコルを提案した．この方法では送信側に量子もつれ光源をおき，ベル測定を行う．ベル測定では複数の光子検出器を用いるため，複数の光子検出器が同時に光子検出したときには高い確率で複数光子対が生成したと結論できる．ま

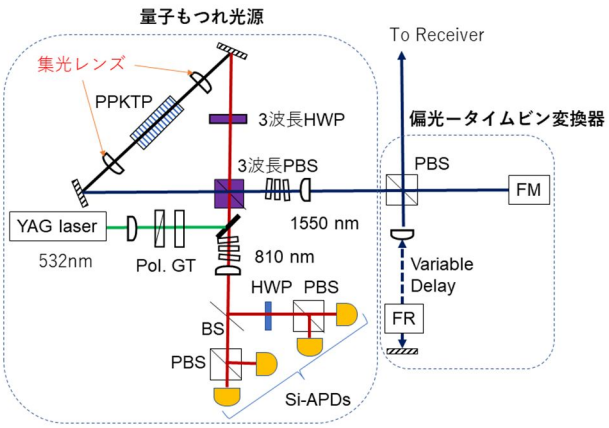

図 3　量子もつれ送信部の構成図

た，光子検出がないときは真空状態が送出されたとする．これにより光子を含まないパルスと多光子を含むパルスを，量子通信の終了後に除去することが可能になり，実効的に単一光子を用いた伝送を高い確率で行うことができる．光子検出器の検出効率が有限であることから生じる複数光子を含むパルスの影響はデコイ法を用いることで抑えることができる．この方法の有効性はシミュレーションで確認され，市販の APD 光子検出器を用いても 200 km 以上の QKD 伝送が行えることを示した．

この結果に基づいて，量子もつれ光源の開発に取り組んだ．検出レートを向上するために送信側の光子検出器は効率が高い Si-APD を用いた．一方，受信側は光ファイバの損失が小さい 1.55μm 帯を用いる．設計・試作した送信部の構成を図 3 に示す．受信機にはこれまでに開発された BB84 プロトコル用のものが使用できる．サニャック干渉計を用いて偏光量子もつれを生成する．サニャック干渉計に必要な 3 波長対応の 1/2 波長板と偏光ビームスプリッタを新規開発した．現在データ補正なしで 95%以上の高い明瞭度が得られている．光ファイバ伝送のために，偏光量子ビットをタイムビン量子ビットに変換する装置も開発した．

光子検出器の暗計数の影響を低減するには 2 つの光子検出器の同時計数を利用することが有効である．我々は受信機に起因するセキュリティループホールがない Measurement Device Independent (MDI)-QKD に着目した．MDI-QKD では離れた場所にある 2 つの光源から光パルスを送り，中間点で同時計数を行う．このとき，2 つの光パルスが識別不能であることが要求される．我々は許容される到達時刻の差を検討した．オリジナルの MDI-QKD プロトコルでは，2 光子干渉の明瞭度が 92%以上必要であるという結果を得た．許容範囲を広げるために中間点での測定法を変えてシミュレーションを行った．その結果ビームスプリッタと偏光ビームスプリッタを用いたベル測定法では誤り率が測定基底によって異なるため，明瞭度が 42%まで低下しても鍵生成が可能なことを見出した．半値幅 100ps のガウス型パルスでは 40ps 程度まで到達時刻の差が許容される．

この程度の精度は高速デテクタと電気的なパルス遅延計測で実現可能である．ただし，光源側に時刻の差をフィードバックするとループが長すぎて安定な制御が行えない．この問題を解決するために中間点で時間差検出と補償を行う方法を提案した．中間点は盗聴者に支配されている可能性があり，従来は中間点での制御は考慮されていなかったが，我々は MDI-QKD の原理に立ち戻り，中間点での操作は安全性に影響しないことに気付いた．さらに，中間点では光が微弱で精度の良い時間差計測が行えない問題を解決するために，レーザーを高速変調して得られる側波帯を利用して周波数的に分離した強い制御光と弱い量子光を時間同期させる方法を考案し，原理実証を行った．この方式はパルスの時間差の補償だけでなく，位相差の補償にも適用できるので，将来さらに長距離化が可能な Twin-Field QKD の実装技術にも応用できる．

また，送信状態の評価にトモグラフィが応用できることを示し，さらに高速 QKD システムにおける量子状態生成には Dual Parallel Modulator が有効であることも提案・実証した．この変調器はコヒーレント光通信における I-Q 変調器として広く使われており，実用性が高い．また，光子の波動関数を直接測定する新手法を提案し，原理実証を行った．

(3) 近距離高速 QKD 技術

近距離高速 QKD 技術では，高速光通信との共存，高速性，コストの点で優位性を有する連続量 QKD(CV-QKD)の研究開発を実施した．研究項目としては，受信側に局部発振光用光源をもつ CV-QKD 受信機の開発と，同一ファイバでの QKD 通信と光通信の共存の２つの項目について研究を実施した．

局部発振光用レーザーを有する CV-QKD 受信機の開発については，通常の光通信と比較して信号光が非常に微弱な CV-QKD において，局部発振光と信号の位相同期をどのように実現するのかということが解決すべき課題であった．本研究では比較的弱いパイロット光を併用するレーザー制御方法として，光注入同期を用いる手法と電気的なフィードバックを用いる手法について研究を行った．

光注入同期を用いる手法では，当初は音響光学素子により信号光とパイロット光の周波数をずらし，波長分割多重により通信路を伝送させる方式を考案し，実証実験を進めた．実験では，送信者側に平面光回路技術による狭線幅の半導体レーザーを設置し，第1の音響光学素子により約300MHz離調した信号光を生成して元のレーザーをパイロット光として直交する偏光で送信した．受信側では，パイロット光を通常のDFBレーザーに注入してパイロット光に位相同期した強度の強いレーザーを発生し，第2の音響光学素子により約300MHz離調した局部発振光を発生した．２つの音響光学素子の周波数を完全に一致させることはできないので，位相

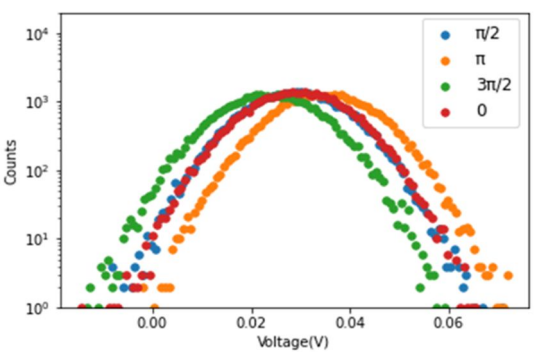

図４　ホモダイン検出の出力電圧の頻度分布

変調器によりずれを補正する手法を開発した．送信側で4値の位相変調を受信側で2値の位相変調を行い，信号光と局部発振光の相対的な位相が0.1秒以上安定に保てることを実証した．

さらに，周波数シフト量を大きくするために，IQ変調器により周波数シフトする方式の実証実験を行った．周波数シフトを大きくすることにより，パイロット光が信号光に漏洩した場合の影響を小さくすることが可能となる．図4は4GHzの周波数シフトをIQ変調器で行ったときのホモダイン検出の出力電圧の頻度分布である．相対位相毎の測定結果はガウス分布によく従っており，通信路過剰雑音は0.34%であった．これは近距離のCV-QKDを行うには十分小さく，安全な鍵を生成可能である．また，パイロット光の漏れに起因する過剰雑音の増加は0.5%程度であった．これにより，高速CV-QKDにおいて局部発振器の独立化を実現することができた．

電気的なフィードバックを用いる手法では，CV-QKDとして4値の位相変調を用いる方式を用いることから，当初はコスタス回路を用いる光位相同期技術に注目し，時分割によりパイロット光を伝送する手法の研究開発を行った．本方式でCVQKDを実現するためには，広帯域低雑音のホモダイン検出技術が必要になるので，光位相同期技術と共に研究を進めた．帯域5Hz，11dBのノイズクリアランスを持つホモダイン検出技術を実証し，このホモダイン検出器の出力をコスタス回路に入力し動作を確認することができた．研究の後半では，光注入同期と同様に，周波数分割多重したパイロット光を用いる方式について研究開発を行った．光源として狭線幅レーザーを用いることにより，位相揺らぎを0.1 rad以内に抑えることに成功し，本光位相同期方式の原理を実証することができた．

CVQKD と光通信との共存については，NICT と学習院大学の共同研究により，100 波のコヒーレント光通信と CVQKD の共存実験を実現することができた．これは，18.3 Tbit/s のデータ通信と CVQKD が共存できることを実証したものであり，CVQKD の高いフィルター効果を明確に示した．CVQKD を既設の光ファイバと多重化することで，低コストに量子鍵配送が可能であることを示した．

(4) 秘密分散-QKD ネットワーク理論

伝送路損失 60dB における長距離 QKD リンク用のデータ処理方法と秘密分散-QKD 融合ネットワークの安全性保証に関して QKD 装置における光源の安全性保証に必要な理論構築，特に実際の装置がもつ不完全性を考慮した安全性理論の構築を行った．研究期間の前半では想定するプロトコルとして Loss tolerant protocol と DPS protocol を取り上げ，DPS protocol については(a)送信状態がテンソル積で記述される，(b)送信する光子数が 1，2，3 以上である確率がそれぞれ抑えられている，(c)真空放出の確率が既知，という 3 つの条件だけで安全性証明を行う方法を考案した．これらの条件は実験でも確かめることが原理的には可能であり，検証可能かつ光源の広範囲な不完全性に対応できる安全性理論である【論文 13】．また，Loss tolerant protocol についてはトロイの木馬攻撃や光源の自発的情報漏れを含む光パルスモードの情報依存性を扱うための一般的な状態記述の方法を考案し，その状態に基づく安全性理論を構築した．

後半は安全性理論の改良と測定装置無依存型量子鍵配送（MDI-QKD）への拡張を行った．安全性理論をより広範囲なプロトコルに使えることを目指した．具体的には，既存の安全性理論ではある特定の確率不等式しか使えなかったが、他の確率不等式を使えるように理論を改良した．

また，MDIQKD で使われるデコイ方式についてのサイドチャンネルについても研究を行い，デコイ方式における強度変調に存在する任意の長さの相関が扱えるようになった【論文 8】．さらに，デコイ法で得られる単一光子部分に存在するほぼ全てのサイドチャネルや不完全性を考慮に入れた安全性理論を構築した．

以上述べてきたように，秘密分散と QKD-OTP ネットワーク，さらに耐量子計算暗号による認証等を組み合わせることによって，安全なデータ伝送・保管・復元を可能とする分散ストレージネットワークを中心とした「量子セキュアクラウド」の実現化技術が開発できた．将来的には，本研究の成果を元に構築される分散ストレージネットワークに，量子コンピュータや AI によるデータ解析機能を備え，ネットワーク内部の通信およびユーザとのインターフェースも QKD と OPT によって情報の秘匿性を担保できる．量子セキュアクラウドの実現によって国家安全保障に関するデータやゲノム情報のような超長期に秘匿化が必要なデータの安全な伝送・保管・復元・二次利用の実現，さらにデータの完全性保証やユーザ認証が行える．

また，同時に行われた量子セキュアクラウド実現のための QKD 技術の高度化についても優れた成果が得られている．本研究が目標としていた，秘密分散と QKD の融合により超長期安全性を保証する情報通信ネットワークの実現に向けた技術基盤を確立することができたと考える．さらに，本研究で開発された技術は将来，より技術的要求の高い量子通信プロトコルの実装技術として発展させていくことが可能である．高度化された QKD 装置を量子セキュアクラウドに組み込むところまでには至らなかったが，技術的課題は本研究で克服されているので，その実現への道筋は明らかである．

５．主な発表論文等

〔雑誌論文〕　計20件（うち査読付論文　19件／うち国際共著　7件／うちオープンアクセス　15件）

１．著者名 Ge Haobo、Tomita Akihisa、Okamoto Atsushi、Ogawa Kazuhisa	４．巻 4
２．論文標題 Analysis of the Effects of the Two-Photon Temporal Distinguishability on Measurement-Device-Independent Quantum Key Distribution	５．発行年 2023年
３．雑誌名 IEEE Transactions on Quantum Engineering	６．最初と最後の頁 1～8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TQE.2023.3259043	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Amari Jorge、Takai Junnosuke、Hirano Takuya	４．巻 2
２．論文標題 Highly efficient measurement of optical quadrature squeezing using a spatial light modulator controlled by machine learning	５．発行年 2023年
３．雑誌名 Optics Continuum	６．最初と最後の頁 933
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OPTCON.484295	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Huang Anqi、Mizutani Akihiro、Lo Hoi-Kwong、Makarov Vadim、Tamaki Kiyoshi	４．巻 19
２．論文標題 Characterization of State-Preparation Uncertainty in Quantum Key Distribution	５．発行年 2023年
３．雑誌名 Physical Review Applied	６．最初と最後の頁 14048
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevApplied.19.014048	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Fujiwara Mikio、Nojima Ryo、Tsurumaru Toyohiro、Moriai Shiho、Takeoka Masahiro、Sasaki Masahide	４．巻 3
２．論文標題 Long-Term Secure Distributed Storage Using Quantum Key Distribution Network With Third-Party Verification	５．発行年 2022年
３．雑誌名 IEEE Transactions on Quantum Engineering	６．最初と最後の頁 1～11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TQE.2021.3135077	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Fujiwara Mikio、Hashimoto Hiroki、Doi Kazuaki、Kujiraoka Mamiko、Tanizawa Yoshimichi、Ishida Yusuke、Sasaki Masahide、Nagasaki Masao	4．巻 12
2．論文標題 Secure secondary utilization system of genomic data using quantum secure cloud	5．発行年 2022年
3．雑誌名 Scientific Reports	6．最初と最後の頁 18530
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41598-022-22804-x	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Ogawa Kazuhisa、Okazaki Takumi、Kobayashi Hirokazu、Nakanishi Toshihiro、Tomita Akihisa	4．巻 29
2．論文標題 Direct measurement of ultrafast temporal wavefunctions	5．発行年 2021年
3．雑誌名 Optics Express	6．最初と最後の頁 19403～19403
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OE.423969	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Eto Yujiro、Hirano Takuya	4．巻 60
2．論文標題 Effect of cascaded nonlinear phase shift on pulsed second-harmonic generation using periodically poled waveguide: a comparison of experimental and numerical results	5．発行年 2021年
3．雑誌名 Japanese Journal of Applied Physics	6．最初と最後の頁 052001～052001
掲載論文のDOI（デジタルオブジェクト識別子） 10.35848/1347-4065/abf49e	査読の有無 有
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 －

1．著者名 Zapatero Victor、Navarrete Alvaro、Tamaki Kiyoshi、Curty Marcos	4．巻 5
2．論文標題 Security of quantum key distribution with intensity correlations	5．発行年 2021年
3．雑誌名 Quantum	6．最初と最後の頁 602
掲載論文のDOI（デジタルオブジェクト識別子） 10.22331/q-2021-12-07-602	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名	4．巻
Curras-Lorenzo Guillermo、Navarrete Alvaro、Pereira Margarida、Tamaki Kiyoshi	104
2．論文標題	5．発行年
Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory	2021年
3．雑誌名	6．最初と最後の頁
Physical Review A	12406
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1103/PhysRevA.104.012406	有
オープンアクセス	国際共著
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	該当する

1．著者名	4．巻
Zhang Weiyang、Kadosawa Yu、Tomita Akihisa、Ogawa Kazuhisa、Okamoto Atsushi	28
2．論文標題	5．発行年
State preparation robust to modulation signal degradation by use of a dual parallel modulator for high-speed BB84 quantum key distributionsystems	2020年
3．雑誌名	6．最初と最後の頁
Optics Express	13965-13977
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1364/OE.383175	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	－

1．著者名	4．巻
Pereira Margarida、Kato G、Mizutani Akihiro、Curty Marcus、Tamaki Kiyoshi	6
2．論文標題	5．発行年
Quantum key distribution with correlated sources	2020年
3．雑誌名	6．最初と最後の頁
Science Advances	eaaz4487
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1126/sciadv.aaz4487	有
オープンアクセス	国際共著
オープンアクセスとしている（また、その予定である）	該当する

1．著者名	4．巻
Navarrete Alvaro、Pereira Margarida、Curty Marcos、Tamaki Kiyoshi	15
2．論文標題	5．発行年
Practical Quantum Key Distribution That is Secure Against Side Channels	2021年
3．雑誌名	6．最初と最後の頁
Physical Review Applied	34072
掲載論文のDOI（デジタルオブジェクト識別子）	査読の有無
10.1103/PhysRevApplied.15.034072	有
オープンアクセス	国際共著
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	該当する

1．著者名 富田章久	4．巻 102
2．論文標題 量子暗号通信の最前線	5．発行年 2019年
3．雑誌名 電子情報通信学会誌	6．最初と最後の頁 942-946
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 －

1．著者名 Pereira Margarida、Curty Marcos、Tamaki Kiyoshi	4．巻 5
2．論文標題 Quantum key distribution with flawed and leaky sources	5．発行年 2019年
3．雑誌名 npj Quantum Information	6．最初と最後の頁 62
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41534-019-0180-9	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Tomita Akihisa	4．巻 2
2．論文標題 Implementation Security Certification of Decoy‐BB84 Quantum Key Distribution Systems	5．発行年 2019年
3．雑誌名 Advanced Quantum Technologies	6．最初と最後の頁 1900005～1900005
掲載論文のDOI（デジタルオブジェクト識別子） 10.1002/qute.201900005	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Shinjo Ami、Eto Yujiro、Hirano Takuya	4．巻 27
2．論文標題 Pulse-resolved measurement of continuous-variable Einstein-Podolsky-Rosen entanglement with shaped local oscillators	5．発行年 2019年
3．雑誌名 Optics Express	6．最初と最後の頁 17610～17610
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OE.27.017610	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Mizutani Akihiro、Sasaki Toshihiko、Takeuchi Yuki、Tamaki Kiyoshi、Koashi Masato	4．巻 5
2．論文標題 Quantum key distribution with simply characterized light sources	5．発行年 2019年
3．雑誌名 npj Quantum Information	6．最初と最後の頁 87
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41534-019-0194-3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Eriksson Tobias A.、Hirano Takuya、Puttnam Benjamin J.、Rademacher Georg、Luis Ruben S.、Fujiwara Mikio、Namiki Ryo、Awaji Yoshinari、Takeoka Masahiro、Wada Naoya、Sasaki Masahide	4．巻 2
2．論文標題 Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels	5．発行年 2019年
3．雑誌名 Communications Physics	6．最初と最後の頁 9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s42005-018-0105-5	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Mizutani Akihiro、Kato Go、Azuma Koji、Curty Marcos、Ikuta Rikizo、Yamamoto Takashi、Imoto Nobuyuki、Lo Hoi-Kwong、Tamaki Kiyoshi	4．巻 5
2．論文標題 Quantum key distribution with setting-choice-independently correlated light sources	5．発行年 2019年
3．雑誌名 npj Quantum Information	6．最初と最後の頁 8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41534-018-0122-y	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Namiki Ryo、Kitagawa Akira、Hirano Takuya	4．巻 98
2．論文標題 Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers	5．発行年 2018年
3．雑誌名 Physical Review A	6．最初と最後の頁 42319
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.98.042319	査読の有無 有
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53件（うち招待講演　23件／うち国際学会　31件）

１．発表者名
Tomita Akihisa

２．発表標題
Research and Development Activities for Quantum Secure Cloud in Japan

３．学会等名
The 9th ETSI/IQC Quantum Safe Cryptography Event（招待講演）（国際学会）

４．発表年
2023年

１．発表者名
Tomita Akihisa

２．発表標題
Toward social deployment of Quantum Key Distribution

３．学会等名
22nd Asian Quantum Information Science Conference（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
富田　章久

２．発表標題
量子暗号の基礎と最近の動向

３．学会等名
第3回 量子技術研究会　（招待講演）

４．発表年
2022年

１．発表者名
Fujiwara Mikio

２．発表標題
Information theoretically secure data utilization using "Quantum Secure Cloud,”

３．学会等名
Quantum innovation 2022（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Fujiwara Mikio

２．発表標題
Functions expected of the quantum internet and roadmap in Japan

３．学会等名
European Conference on Optical Communication（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Tomita Akihisa

２．発表標題
Practical Methods for Security Certification of Quantum Key Distribution

３．学会等名
Quantum2.0（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Hirano Takuya

２．発表標題
Introduction to Continuous Variable Quantum Key Distribution

３．学会等名
Optical Fiber Communication Conference（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Hirano Takuya

２．発表標題
Integration of Continuous-Variable Quantum key Distribution and Coherent Optical Communication

３．学会等名
Asia Communications and Photonics Conference（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
富田　章久

２．発表標題
量子暗号通信の最前線

３．学会等名
第12回 光・電波フォーラム（招待講演）

４．発表年
2021年

１．発表者名
富田　章久

２．発表標題
量子鍵配送の高速化に向けた光検出器の研究開発

３．学会等名
第82回 応用物理学会 秋季学術講演会 シンポジウム「グローバル量子暗号通信の展開」（招待講演）

４．発表年
2021年

１．発表者名
平野琢也,

２．発表標題
連続量量子鍵配送の現状と展望

３．学会等名
第82回 応用物理学会 秋季学術講演会 シンポジウム「グローバル量子暗号通信の展開」（招待講演）

４．発表年
2021年

１．発表者名
J. Amari, J. Takai and T. Hirano,

２．発表標題
Improvement of Squeezing using a Spatial Phase Modulator and Machine Learning

３．学会等名
American Physical Society (APS) March Meeting,（国際学会）

４．発表年
2023年

１．発表者名
T. Sato, A. Tomita and A. Okamoto

２．発表標題
The Effect of Optimized Parameters on the Efficiency of QKD Systems

３．学会等名
22nd Asian Quantum Information Science Conference（国際学会）

４．発表年
2022年

１．発表者名
松本遼司，富田章久，岡本淳

２．発表標題
量子鍵配送に向けた自己相関関数による光子数分布評価

３．学会等名
第70回応用物理学会春季学術講演会

４．発表年
2023年

１．発表者名
J. Amari, J. Takai and T. Hirano

２．発表標題
Improvement of Squeezing using a Spatial Light Modulator controlled by Machine Learning

３．学会等名
第47回量子情報技術研究会

４．発表年
2022年

１．発表者名
菅原悠生，富田章久，岡本淳

２．発表標題
DPQPSK用変調器を用いた高速QKDの量子状態生成

３．学会等名
第47回量子情報技術研究会

４．発表年
2022年

１．発表者名
清野桜子，平野琢也

２．発表標題
GHz帯域低雑音バランス検出器を用いた量子雑音の測定

３．学会等名
第47回量子情報技術研究会

４．発表年
2022年

１．発表者名
Jorge Amari, Junnosuke Takai and Takuya Hirano,

２．発表標題
Improvement of Squeezing using a Spatial Phase Modulator and Machine Learning

３．学会等名
第83回 応用物理学会 秋季学術講演会

４．発表年
2022年

１．発表者名
井伊 優貴，大森 春輝，武藤 遼，平野 琢也

２．発表標題
光注入同期を用いた連続量量子鍵配送

３．学会等名
第69回応用物理学会春季学術講演会，

４．発表年
2022年

１．発表者名
小川和久，岡崎巧実，小林弘和，中西俊博，富田章久

２．発表標題
時間領域における光子の超短波動関数の直接測定

３．学会等名
第43回 量子情報技術研究会

４．発表年
2020年

１．発表者名
W. Zhang

２．発表標題
A Quantum random number generator integrated into a transmitter of BB84 QKD systems

３．学会等名
The 20th Asian Quantum Information Science Conference (AQIS2020)（国際学会）

４．発表年
2020年

１．発表者名
R. Namiki

２．発表標題
Majorization relations for a set of two-mode squeezed number states

３．学会等名
The 20th Asian Quantum Information Science Conference (AQIS2020)（国際学会）

４．発表年
2020年

１．発表者名
A. Tomita

２．発表標題
Activities on Quantum Information Technology in Japan

３．学会等名
Quantum 2020（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
富田　章久

２．発表標題
光量子情報技術－数学を具現化する技術と実装を救う数学－

３．学会等名
JST-CRDS　数学と科学、工学の協働に関する連続セミナー 第3回（招待講演）

４．発表年
2020年

１．発表者名
藤原　幹生

２．発表標題
量子暗号のユースケース，グローバル量子暗号通信網構築に向けた取り組み

３．学会等名
TTC・量子ICTフォーラム合同オンラインセミナー（招待講演）

４．発表年
2020年

１．発表者名
藤原　幹生

２．発表標題
我が国の量子暗号ネットワーク・グローバル化に向けた取り組み

３．学会等名
電子情報通信学会2021年総合大会（招待講演）

４．発表年
2021年

１．発表者名
Akihisa Tomita

２．発表標題
Implementation Security Certification of Quantum Key Distribution Devices

３．学会等名
Topical Conference on Quantum Communication and Security（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Akihisa Tomita

２．発表標題
Quantum Key Distribution in the Real World

３．学会等名
第80回応用物理学会秋季学術講演会（OSA joint session）（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Akihisa Tomita

２．発表標題
A Long-term Secure Data Transmission and Storage Network Based on Quantum Key Distribution

３．学会等名
Advanced Photonics Congress, Signal Processing in Photonic Communications（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Tobias A. Eriksson, Takuya Hirano, Georg Rademacher, Benjamin J. Puttnam, Ruben S. Luis, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada, and Masahide Sasaki,

２．発表標題
Challenges in Parallel Operation of Quantum Key Distribution and Data Transmission

３．学会等名
Advanced Photonics Congress, Signal Processing in Photonic Communications（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Weiyang Zhang, Akihisa Tomita, Kazuhisa Ogawa, and Atsushi Okamoto

２．発表標題
Phase fluctuation of a gain-switched semiconductor laser for quantum key distribution

３．学会等名
Winter International Symposium on Big-Data, Cybersecurity and IoT,（国際学会）

４．発表年
2019年

１．発表者名
Takumi Matsuura, Liang Min, Kazuhisa Ogawa, Atsushi Okamoto, and Akihisa Tomita

２．発表標題
Numerical analysis of decoy state BBM92 quantum key distribution protocol with multi-photon rejection source

３．学会等名
opical Conference on Quantum Communication and Security,（国際学会）

４．発表年
2019年

１．発表者名
Haobo Ge, Kazuhisa Ogawa, Atsushi Okamoto, and Akihisa Tomita

２．発表標題
Analysis of the effects of the two-photon distinguishability on decoy state measurement-device-independent quantum key distribution

３．学会等名
Topical Conference on Quantum Communication and Security, (国際学会)

４．発表年
2019年

１．発表者名
Takuya Hirano and Ryo Namiki

２．発表標題
Continuous operation of four-states continuous-variable quantum key distribution system

３．学会等名
Topical Conference on Quantum Communication and Security (国際学会)

４．発表年
2019年

１．発表者名
Takumi Matsuura, Liang Min, Kazuhisa Ogawa, Atsushi Okamoto, and Akihisa Tomita

２．発表標題
Numerical analysis of decoy state BBM92 quantum key distribution protocol with multi-photon rejection sourc

３．学会等名
th International Conference on Quantum Cryptography (QCrypt 2019) (国際学会)

４．発表年
2019年

１．発表者名
Weiyang Zhang, Yu Kadosawa, Akihisa Tomita, and Kazuhisa Ogawa

２．発表標題
State preparation robust to the modulation signal defeation by a dual-parallel modulator for high speed BB84 quantum key distribution systems

３．学会等名
ummer International Symposium on Big-Data, Cybersecurity and IoT (国際学会)

４．発表年
2019年

１．発表者名
Tobias A. Eriksson, Takuya Hirano, Georg Rademacher, Benjamin J. Puttnam, Ruben S. Luís, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki

２．発表標題
Joint Propagation of Continuous Variable Quantum Key Distribution and18×24.5Gbaud PM-16QAM Channels

３．学会等名
European Conference on Optical Communication (ECOC)（国際学会）

４．発表年
2019年

１．発表者名
葛 皓波, 富田 章久, 小川 和久, 岡本 淳

２．発表標題
デコイ法を用いた測定装置に依存しない量子鍵配送に対する二光子判別可能性の影響

３．学会等名
第41回 量子情報技術研究会（QIT41）

４．発表年
2019年

１．発表者名
松浦 巧, 関 亮, 小川 和久, 岡本 淳, 富田 章久

２．発表標題
デコイ法を用いた多光子パルスを削減できるBBM92量子暗号鍵配付プロトコルの数値解析

３．学会等名
第40回 量子情報技術研究会（QIT40）

４．発表年
2019年

１．発表者名
Akihisa Tomita

２．発表標題
Implementation Security Certification of a Quantum Key Distribution System through Device Characterization

３．学会等名
Optical Fiber Communications Conference and Exhibition（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Weiyang Zhang, Yu Kadosawa, Akihisa Tomita, Kazuhisa Ogawa, Atsushi Okamoto

２．発表標題
State tomographic characterization of BB84 states generated by a Dual-Parallel Modulator

３．学会等名
8th International Conference on Quantum Cryptography（国際学会）

４．発表年
2018年

１．発表者名
Tobias Eriksson, Takuya Hirano, Motoharu Ono, Mikio Fujiwara, Ryo Namiki, Ken-ichiro Yoshino, Akio Tajima, Masahiro Takeoka and Masahide Sasak

２．発表標題
Coexistence of Continuous Variable Quantum Key Distribution and 7 × 12.5 Gbit/s Classical Channels

３．学会等名
IEEE Summer Topicals Meeting Series , Hawaii, USA（国際学会）

４．発表年
2018年

１．発表者名
Ami Shinjjo, Yujiro Eto,and Takuya Hirano

２．発表標題
Time-Domain Measurement of Continuous-Variable Entanglement Using Temporally Shaped Local Oscillator Pulse

３．学会等名
IEEE Summer Topicals Meeting Series , Hawaii, USA（国際学会）

４．発表年
2018年

１．発表者名
Tobias Eriksson, Takuya Hirano, Georg Rademacher, Benjamin Puttnam, Ruben Luis, Mikio Fujiwara, Ryo Namiki, Ken-Ichiro Yoshino, Akio Tajima, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki

２．発表標題
Continuous Variable Quantum Key Distribution Multiplexed with Classical Channels

３．学会等名
8th International Conference on Quantum Cryptography（国際学会）

４．発表年
2018年

１．発表者名
Tobias A. Eriksson, Takuya Hirano, Georg Rademacher, Benjamin J. Puttnam, Ruben S. Luis, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki

２．発表標題
Joint Propagation of Continuous Variable Quantum Key Distribution and18×24.5Gbaud PM-16QAM Channels

３．学会等名
European Conference on Optical Communication（国際学会）

４．発表年
2018年

１．発表者名
Akihisa Tomita

２．発表標題
Characterization and Security Certification of a Practical Quantum Key Distribution System

３．学会等名
Laser Physics Workshop（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
新城亜美，片山拓哉，衞藤雄二郎，平野琢也

２．発表標題
時間幅の短い局部発振光を用いたパルス光連続変数エンタングルメントの時間領域測定II

３．学会等名
日本物理学会 2018年 秋季大会

４．発表年
2018年

１．発表者名
Ami Shinjo、Takuya Katayama、Yujiro Eto、Takuya Hirano

２．発表標題
Pulse-resolved measurement of continuous-variable EPR entanglement with shaped local oscillators

３．学会等名
第79回 応用物理学会 秋季学術講演

４．発表年
2018年

１．発表者名
Ryo Namiki

２．発表標題
Two instances of majorization relations for two-mode squeezed number states

３．学会等名
第39回量子情報技術研究会

４．発表年
2018年

１．発表者名
新城 亜美, 片山 拓哉, 衞藤 雄二郎, 平野 琢也

２．発表標題
波形整形した局部発振光を用いたパルス光連続変数エンタングルメントの時間領域測

３．学会等名
第66回応用物理学会 春季学術講演会

４．発表年
2018年

１．発表者名
Weiyang Zhang・Akihisa Tomita・Yu Kadosawa・Kazuhisa Ogawa

２．発表標題
State tomographic characterization of BB84 states generated by a Dual-Parallel Modulator

３．学会等名
第38回量子情報技術研究会

４．発表年
2018年

１．発表者名
Akihisa Tomita

２．発表標題
Quantum Key Distribution - How do you know it's secure

３．学会等名
Okinawa School in Physics:Coherent Quantum Dynamics 2018（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
富田　章久

２．発表標題
量子暗号鍵配送ー最近の研究開発動向

３．学会等名
物性研短期研究会 量子情報・物性の新潮流（招待講演）

４．発表年
2018年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
受信機、暗号鍵配送システム、受信機の制御方法、及び、制御プログラム	遠山 裕之，吉野 健一郎，飯田 信彦，平野 琢也	日本電気株式会社，学校法人学習院
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2022-154680	2022年	国内

〔取得〕　計0件

〔その他〕

プレスリリース『量子セキュアクラウドによる高速安全なゲノム解析システムの開発に成功』
https://www2.nict.go.jp/qictcc/news/20221117.html

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
研究分担者	平野　琢也 (HIRANO Takuya) (00251330)	学習院大学・理学部・教授 (32606)	
研究分担者	玉木　潔 (TAMAKI Kiyoshi) (20435928)	富山大学・学術研究部工学系・教授 (13201)	

６．研究組織（つづき）

	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
研究分担者	藤原　幹生 (FUJIWARA Mikio) (70359066)	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・研究センター長 (82636)	

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			
スペイン	University of Vigo			
カナダ	University of Toronto	Quantum Bridge Technologies, Inc		
中国	NUDT	USTC	University of Hong Kong	
ロシア連邦	Russian Quantum Center	NUST		