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　３ 年　 ６ 月 １４ 日現在

機関番号：８２６３６
研究種目：基盤研究(A)（一般）
研究期間：2017～2020
課題番号：１７Ｈ０１２８１

研究課題名（和文）電波や光など様々な周波数帯で利用可能な高秘匿移動通信ネットワーク技術の研究開発

研究課題名（英文）Research and development of highly secure mobile communications network technologies for various frequency bands including radio-frequency waves and light waves

研究代表者

佐々木　雅英（Sasaki, Masahide）

国立研究開発法人情報通信研究機構・未来ICT研究所・主管研究員

研究者番号：５０３５９０６４

交付決定額（研究期間全体）：（直接経費）　　33,300,000円

研究成果の概要（和文）：移動通信ネットワーク上で超高安全かつ高速の鍵配送の実現に向け、同報型秘密鍵交換の基礎理論を構築するとともに、効率的な鍵蒸留プロトコルを開発し、地上ビル間7.8kmの光空間通信テストベッド（レーザ波長1.5um帯、パルス繰返しレート10MHz）を用いて１対２同報型秘密鍵交換を世界で初めて実証した。最適な大気条件の下で8Mbpsのグループ鍵生成レートを実現するとともに、様々な気象条件の下で実験データを蓄積し、通信路特性に応じて送信電力を適応的に制御する技術や安全性保証技術を開発した。60GHzのミリ波帯においてもフェーズドアレイアンテナを用いた基礎実験を行い、同報型秘密鍵交換の設計指針を導出した。

研究成果の学術的意義や社会的意義
本成果は、どんな計算機でも解読できない鍵配送を1対多のプロトコルにおいて世界で初めて実証したものであり、暗号分野に新たな地平を切り開くものである。また、時々刻々と通信路特性が変動する場合の秘匿容量の導出に成功するなど、新たな理論構築にも成功した。当該技術はレーザ光やミリ波など指向性の強い電磁波を用いる無線通信に適しており、衛星や無人航空機を送受信局、中継局として宇宙から地上網まで網羅する新たな移動通信ネットワークの情報セキュリティを支えてゆくための重要な技術になると期待される。

研究成果の概要（英文）：Toward realizing highly secure and high-speed key distribution in mobile communication networks, we developed a basic theory of multicast secret key agreement, implement an efficient key distillation protocol, and demonstrated 1-to-2 multicast secret key agreement, at the first time, using an optical space communication testbed of 7.8 km terrestrial link (laser wavelength of 1.5um, pulse repetition rate of 10 MHz). We attained the maximum group key rate of 8 Mbps at the optimal atmospheric condition. We accumulated experimental data under various meteorological conditions, and developed adaptive controls of transmission power according to channel characteristics, and security certification technologies. We also conducted basic experiments in the 60 GHz millimeter wave band using a phased array antenna, deriving a design guideline for multicast secret key agreement.

研究分野：量子情報通信

キーワード：暗号　セキュリティ　移動通信ネットワーク

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

衛星や無人航空機を送受信局、中継局として宇宙から地上網まで網羅する新たな移動通信ネットワークが登場しつつある。その発展には、接続性の向上のみならず情報セキュリティの確保が必須である。セキュリティ技術の根幹となる暗号鍵の配送は、現在、公開鍵暗号に基づく鍵交換基盤で行われているが、この基盤は解くのが困難な数学問題に基づいており計算技術の進展とともに安全性がどうしても危殆化する。これに対して、どんな計算機でも解読できない「情報理論的安全性」を持つ鍵配送として、量子鍵配送と秘密鍵交換の２つの方法が知られている。前者は、光の量子効果を使うことで、どんな物理的能力を持つ盗聴者に対しても情報理論的安全性を保証できる。後者は、盗聴者の計算能力に制限は無いが、物理的能力（通信路のタッピング能力）に一定の制限を仮定した上で量子鍵配送よりも長距離・高速で情報理論的に安全な鍵配送を実現できる。両者とも空間光通信路へ適用する研究開発が始まっている。

２．研究の目的

本研究開発では、秘密鍵交換に基づき、移動通信ネットワーク上で超高安全かつ高速の鍵配送を実現するために、１対多の同報型秘密鍵交換技術について以下の３つの研究課題に取り組む。
（１）同報型秘密鍵交換のための効率的な鍵蒸留プロトコルと安全性評価理論の開発
（２）光空間通信による１対２同報型秘密鍵交換の実証、盗聴攻撃対策・安全性評価技術の開発
（３）電波による無人航空機間での同報型秘密鍵交換技術と安全性評価技術の開発

３．研究の方法

（１）同報型秘密鍵交換のための効率的な鍵蒸留プロトコルと安全性評価理論の開発

本研究開発では量子鍵配送用に開発した鍵蒸留プロトコルを １ 対多の同報型秘密鍵交換へ適用し、様々な通信条件下における最適な信号・情報処理方法を見出して通信路情報のモデル化を行い、一般化可能な理論体系の構築に取り組む。

（２）光空間通信による１対２同報型秘密鍵交換の実証、盗聴攻撃対策・安全性評価技術の開発

情報通信研究機構（NICT）と電気通信大学のビル間 7.8㎞ を結ぶ光空間テストベッドに１対２の同報型秘密鍵交換システム及び盗聴器に相当する受信システムを構築する。様々なビーミング条件や気象条件下で伝送データを取得し、（１）で開発した理論を用いて盗聴機への漏洩情報量を評価する。

（３）電波による無人航空機間での同報型秘密鍵交換技術と安全性評価技術の開発

種々の電波帯域について、近距離通信を想定した真性乱数の指向性通信による高速秘密鍵交換に適した通信方式設計、装置実装と実現可能性について検討を行う。

４．研究成果

（１）同報型秘密鍵交換のための効率的な鍵蒸留プロトコルと安全性評価理論の開発

A．鍵蒸留プロトコルと安全性評価理論

図１に同報型秘密鍵交換（FSO-GKA）の基本モデルを示す。送信者(アリス)は衛星や航空機など、正規受信者(ボブ)はドローンなどの飛翔体を想定する。ボブらは、盗聴者(イブ)が存在しないことを確認できる監視区域内で鍵交換を行う。イブは、アリスとボブの見通し外や監視エリアの遥か後方など、発見が困難な領域から盗聴を試みる。イブへの漏洩情報量の上限を推定するために、仮想イブ(以下、v-イブ)と呼ばれるプローブ系を監視区域周辺に配置する。

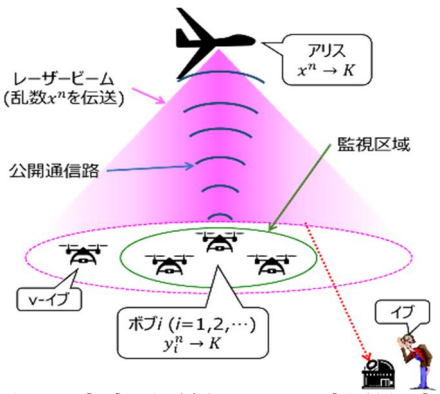

図１　光空間通信による同報型秘密鍵交換（FSO-GKA）の基本モデル

アリスは乱数列x^nに基づいてレーザ光を変調しボブらへ送信する。各ボブは受信信号から乱数ビット列y_i^nを復調する(iは各ボブを識別するインデックス)。アリスとボブは、公開通信路（通常は RF 回線）を通して通信しながら、鍵蒸留処理を行う。

鍵蒸留処理では、送信乱数列x^nと受信乱数列y_i^nの食い違いを訂正するための情報整合(誤り訂正)と、イブへの情報漏洩を防ぐための秘匿性増強が行われる。

情報整合には、アリスからボブへ訂正情報を送信する前方情報整合と、ボブのいずれかがアリスに訂正情報を送信する後方情報整合の２種類があり、グループ鍵生成レートはそれぞれ

$$R_{\mathrm{GKA,D}} = \min_i [I(X;Y_i)] - I(X;\hat{Z})$$

$$R_{\mathrm{GKA,R}} = \max_i \left(\min_j [I(Y_i;Y_j)] - I(Y_i;\hat{Z}) \right)$$

で与えられる。ここで、$I(\cdot;\cdot)$は２つの確率変数の間の相互情報量、X、Y_i 、$\hat{Z}$は、それぞれアリス、ボブ i、v-イブの確率変数である。

これら２つの方式について、シミュレーションにより優劣を比較した結果、受信者ごとの受信電力が大きく異なる場合、後方型情報整合の方が有利になることが分かった。しかし、その差はあまり大きくはなく、実際の回線長 7.8㎞ の光空間通信テストベッドで行った実証実験（後述）では、前方情報整合による鍵生成レート$R_{\mathrm{GKA,D}}$が後方情報整合によるものよりもほとんどのケースで大きいことが分かった[1]。

また、光空間通信路では大気揺らぎ等により時々刻々通信路特性が変動（フェーディング）する。そこで、受信信号強度をモニタしながら、信号強度が一定の閾値を下回った際の受信データを敢えて削除したり、複数の受信機の信号強度バランスに応じて情報整合の方式を選択するなどして、鍵交換スループットを最大化する手法（適応的鍵蒸留処理）を開発し、光空間通信テストベッドで蓄積した伝送実験データによる検証で有効性を明らかにした[2]。

B.フェーディングがある場合の秘密鍵交換の理論体系の一般化

時々刻々と特性変動を伴う光空間通信路において、情報理論的に安全な暗号通信の最終的な性能限界や最適な暗号通信方式については未解明な点が多い。実際、これらの問題は、現代情報理論の最先端領域の一つとなっている。具体的には、フェーディング等の通信路の特性変化が通信路状態情報(Channel State Information: CSI)として与えられた際に、秘密鍵交換（レート R_S）や秘匿メッセージ伝送（レート R_M）がどこまで改善され得るのかが主題である。本研究では、CSI が与えられた場合の秘密鍵交換のみならず、秘匿メッセージ伝送、及びこれらを融合した方式（物理レイヤ暗号）を包括的に取り扱う理論体系化に取り組んだ。

これまでの研究のほとんどは通信路状態情報 Sが非因果的な場合に限られていたが、本研究では、実際的・理論的にも重要な因果的な場合まで含めた一般化に取り組み、以下の３つのブレイクスルーを達成した[3,4]。

B１）これまで個別に扱われてきた秘密鍵交換レート R_Sと秘匿メッセージ伝送レート R_Mの問題を、本研究では２つのレートの“トレードオフ”問題ととらえ、レート対(R_M, R_S)の実現可能な領域、いわゆる秘匿容量領域 Cs（２次元領域）を、非因果的場合で“理論的に厳密に”決定した。これを数式で書けば、相互情報量とエントロピーを用いて、

$$R_M \le I(UV;Y|S), \tag{1}$$

$$R_M + R_K \le I(V;Y|SU) - I(V;Z|SU) + H(S|ZU), \tag{2}$$

$$Cs = \cup_{p_{SUV}} R(p_{SUV}). \tag{3}$$

と簡単に書ける。ただし、U、Vは補助変数で、$R(p_{SUV})$は(1)と(2)を満たす(R_M, R_S)の全体を表し、(3)はあらゆる同時分布 p_{SUV}に亘る集合和である。

B２）「差し込み原理(Principle of plugging)」という新しい原理を導入することで、非因果的なシステムで問題が解決していれば、対応する因果的なシステムの問題を解決することが出来ることを示した。その結果、因果的なシステムに関する従来の主要結果の全てを統一的に導出することに成功した。

B3）劣化型物理レイヤ暗号システムの場合に、因果的な秘匿容量領域と非因果的な秘匿容量領域は常に一致するという定理を導出した。これは、実用的な物理レイヤ暗号システムを設計する際の強力な「指導原理」となる。

情報理論において、厳密な秘匿容量領域を導出できるのは極めて例外的であり、物理レイヤ暗号のフロンティアで得られた本成果は今後大きな意義を持つと期待される。

（２）光空間通信による１対２同報型秘密鍵交換の実証、盗聴攻撃対策・安全性評価技術の開発

FSO-GKA は図１に示すように移動体通信を前提とした同報型秘密鍵交換であるが、その原理は地上固定局間においても未だに実証されていなかった。そこで、本研究では、フィールド環境での初の原理実証と、詳細な性能検証を目的に、地上ビル間水平伝搬リンクで実証実験を行った。図２に用いた光空間通信テストベッドの模式図を示す。

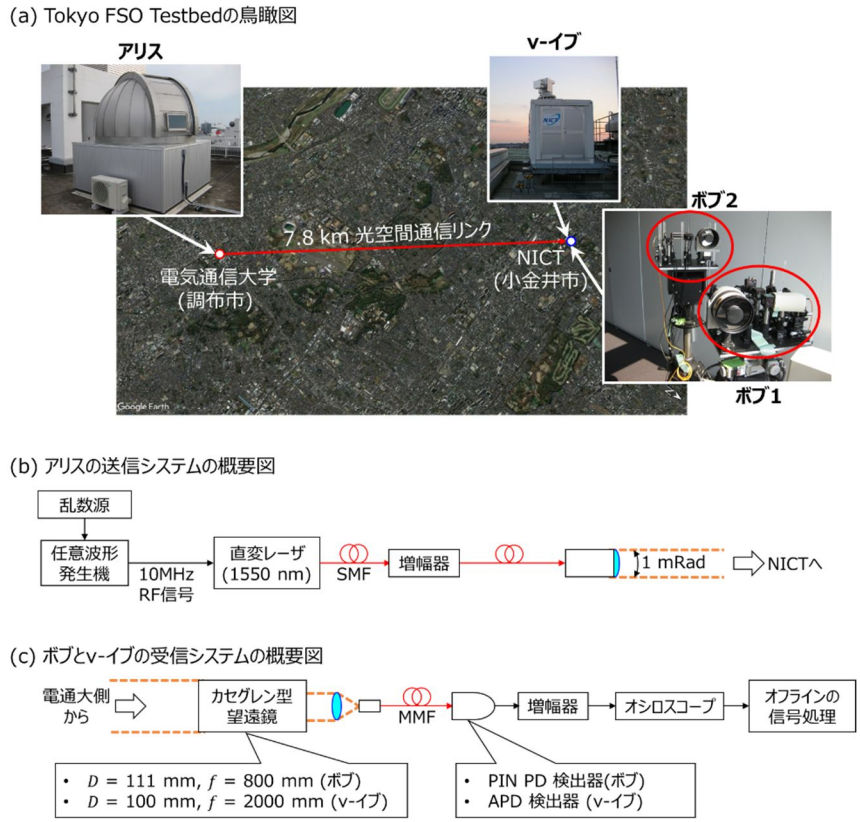

図２　光空間通信テストベッド概要

この光空間通信テストベッドは、電気通信大学に設置された全天候型ドーム内のレーザ送信機(アリス)と、7.8㎞離れた NICT に設置された 3 つの受信機からなっている。受信機の内 2 つは、ボブ 1 とボブ 2 として 6 階建てビルの 6 階窓際に設置されている。もう一つの受信機は v-イブとして同ビルの屋上にコンテナ型受信機として設置されている。v-イブとボブは直線距離にして約 12㎞離れている。光学的な諸元は図２(b)、(c)に示した通りである。

このテストベッドを用いて、何日間に渡る実験キャンペーンを実施した。図３に 10 月 6 日の結果を示す。この実験では、オシロスコープの制約上、10 分に 1 回ごとに測定を実施している。1 回の測定では、1 メガビットの乱数列を含むデータフレームを 10 フレーム分伝送される。

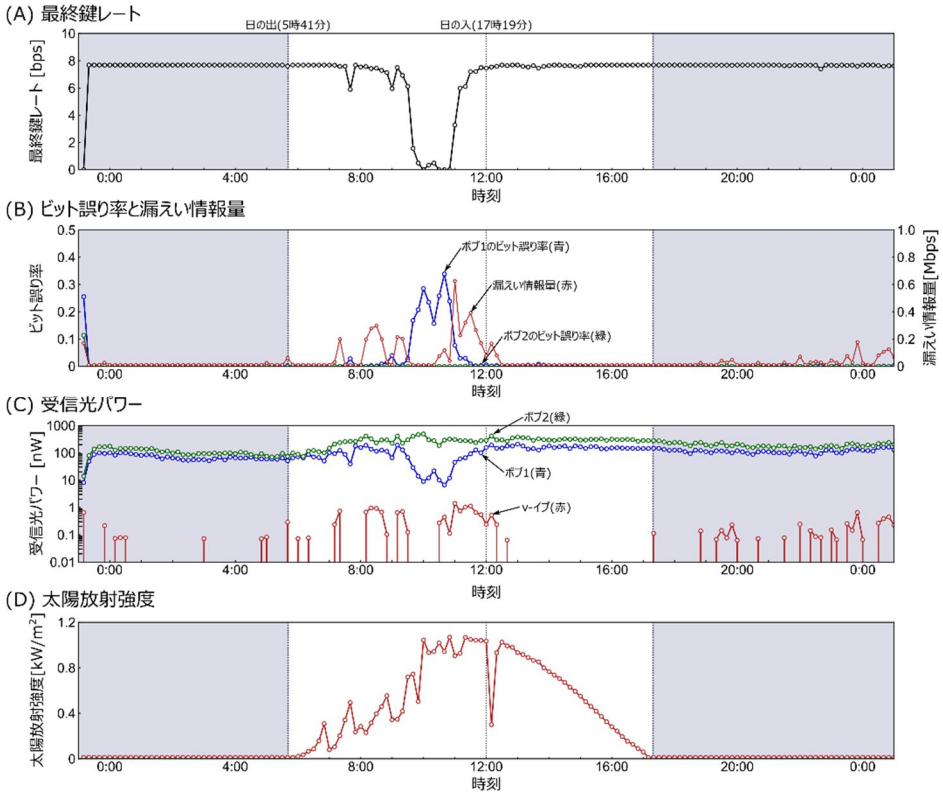

図３　１対２同報型秘密鍵交換の実証実験の結果（2018 年 10 月 6 日）

図 3(A)に示すように、夜間はほぼ 8Mbps でのグループ鍵生成が実現できている。午前 9 時から午前 11 時では、鍵生成レートは大きく減少しており、図 3(B)のように、ボブ 1 のビット誤り率が増加し、漏えい情報量も増加している。日照によるビルや装置のドリフト、大気揺らぎなどの影響によるビーム条件の変動によるものと推定される。変化し v-イブへの情報量が漏洩すると考えられる。これらの成果を OSA Continuum 誌で発表し、レーザ光による世界初の同報型秘密鍵交換の実証として Editor’s pick に選定されるなど高い評価を得た。

その後、さらに鍵交換性能と大気揺らぎの相関データを蓄積し、シンチレーションインデックスの値に応じて、送信電力を適切に設定することで秘密鍵交換の性能を向上させるなどの運用指針を導出し、蓄積データを学習しながらどんどん賢く安全になる秘密鍵交換技術に関する基本コンセプトを確立した。

（3）電波による無人航空機間での同報型秘密鍵交換技術と安全性評価技術の開発

5.7GHz 帯域での検証実験では、ホイップアンテナと平面アンテナを用いた検証を行ったが、アンテナ指向性が低く、見通し通信路における高秘匿な秘密鍵交換の実装は容易でない。この波長帯での通信は鍵蒸留システムの公開通信路としては有効に用いられることを検証した。

ミリ波（60GHz）帯無線通信については、32 素子フェーズドアレイアンテナを用いた伝搬実験を行い、見通し 100m 圏では数度以内で良好な高指向通信路を構成できることを確認した。一方、当該アンテナおよび受信装置が小型であり、紙やプラスチック等では電波を遮蔽しきれないため、位置取りによっては信号を傍受できる可能性があることも判明した。

フィールド検証に用いたフェーズドアレイアンテナの放射強度の方向特性（水平方向）から、秘匿容量の推定を行った。図 4 に秘匿容量の空間分布を示す。使用したフェーズドアレイアンテナの放射角強度分布から伝達強度の空間分布を推定し、ガウシアンワイヤータップ通信路を仮定しており、図中白であらわされている部分は秘匿性容量が 0 の区域である。直進性の高い通信搬送波および高指向性のアンテナを用いることで、高秘匿での通信が可能な空間を限定することが可能であることを示している。

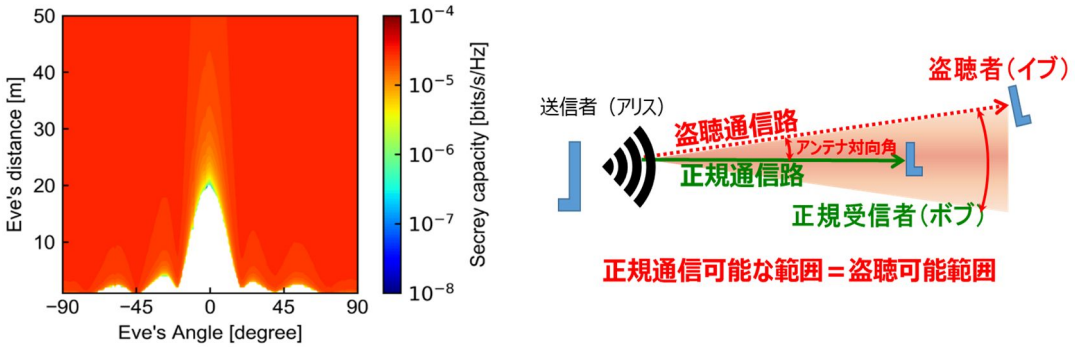

図 4 通信秘匿容量の数値推定（左）。縦軸はアリス・イブ間距離、送受信者間通信路に対するイブの盗聴器角度の開き角（右図の位置関係の模式図を参照）。

これらの研究結果から、ミリ波帯などの高指向性搬送波による秘密鍵交換の基本設計の指針が得られた。秘匿通信性能や詳細な安全性解析などは今後の課題である。

以上により同報型秘密鍵交換に基づく秘匿通信網の構築に必要な諸概念を明確化し、要素技術を開発するとともに設計指針を確立した。

＜引用文献＞

[1]. H. Endo, et al., “Group key agreement over free-space optical links,” OSA Continuum Vol. 3, Issue 9, pp. 2525-2543 (2020).

[2]. H. Endo, et al., “Free-space optical secret key agreement with post-selection based on channel state information,” Environmental Effects on Light Propagation and Adaptive Systems II. 1153 (2019).

[3]. T. S. Han and M. Sasaki, “Wiretap Channels With Causal State Information: Strong Secrecys,” IEEE Trans. IT65(10), pp.6750-6765 (2019).

[4]. T. S. Han and M. Sasaki, submitted to IEEE Trans. IT (2019).

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　1件／うちオープンアクセス　9件）

１．著者名 T. S. Han, and M. Sasaki	４．巻 65
２．論文標題 Wiretap Channels With Causal State Information: Strong Secrecy	５．発行年 2019年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 6750～6765
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2019.2925611	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 H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, R. Shimizu, M. Takeoka, and M. Sasaki	４．巻 1153
２．論文標題 Free-space optical secret key agreement with post-selection based on channel state information	５．発行年 2019年
３．雑誌名 Environmental Effects on Light Propagation and Adaptive Systems II.	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1117/12.2532232	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 H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, T. Ito, R. Shimizu, M. Takeoka, and M. Sasaki	４．巻 26
２．論文標題 Free space optical secret key agreement	５．発行年 2018年
３．雑誌名 Optics Express	６．最初と最後の頁 23305～23332
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OE.26.023305	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 T. Eriksson, Trinh Phuc V., H. Endo, M. Takeoka, and M. Sasaki	４．巻 26
２．論文標題 Secret key rates for intensity-modulated dual-threshold detection key distribution under individual beam splitting attacks	５．発行年 2018年
３．雑誌名 Optics Express	６．最初と最後の頁 20409～20419
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OE.26.020409	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 H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, T. Ito, R. Shimizu, M. Takeoka, and M. Sasaki	4．巻 26
2．論文標題 Free-space optical wiretap channel and experimental secret key agreement in 78 km terrestrial link	5．発行年 2018年
3．雑誌名 Optics Express	6．最初と最後の頁 19513～19523
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OE.26.019513	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 M. Sasaki	4．巻 2
2．論文標題 Quantum networks: where should we be heading?	5．発行年 2017年
3．雑誌名 Quantum Science and Technology	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1088/2058-9565/aa6994	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 M. Sasaki, H. Endo, M. Fujiwara, M. Kitamura, T. Ito, R. Shimizu, and M. Toyoshima	4．巻 375
2．論文標題 Quantum photonic network and physical layer security	5．発行年 2017年
3．雑誌名 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1098/rsta.2016.0243	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 T. S. Han, H. Endo, and M. Sasaki	4．巻 13
2．論文標題 Wiretap Channels With One-Time State Information: Strong Secrecy	5．発行年 2018年
3．雑誌名 IEEE Transactions on Information Forensics and Security	6．最初と最後の頁 224～236
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2017.2746008	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 H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, R. Shimizu, M. Takeoka, and M. Sasaki	4．巻 3
2．論文標題 Group key agreement over free-space optical links	5．発行年 2020年
3．雑誌名 OSA Continuum	6．最初と最後の頁 2525～2543
掲載論文のDOI（デジタルオブジェクト識別子） 10.1364/OSAC.389853	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 －

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　2件）

1．発表者名 H. Endo and M. Sasaki,
2．発表標題 Secret Key Agreement for Satellite Laser Communications
3．学会等名 37th International Communications Satellite Systems Conference (ICSSC).（国際学会）
4．発表年 2019年

1．発表者名 M. Sasaki
2．発表標題 System integration of QKD and post-quantum signatures for a distributed storage system with long-term integrity, authenticity, and confidentiality
3．学会等名 The 6th ETSI/IQC Workshop on Technical Trach（国際学会）
4．発表年 2018年

〔図書〕　計0件

〔出願〕　計3件

産業財産権の名称 秘密鍵共有方法及びシステム	発明者 遠藤 寛之，佐々木 雅英	権利者 同左
産業財産権の種類、番号 特許、特願2019-235286	出願年 2019年	国内・外国の別 国内

産業財産権の名称 秘密鍵共有システム及び秘密鍵共有方法	発明者 遠藤 寛之，佐々木 雅英	権利者 同左
産業財産権の種類、番号 特許、特願2020-012325	出願年 2019年	国内・外国の別 国内

産業財産権の名称 秘密鍵共有システム及び秘密鍵共有方法	発明者 遠藤 寛之，佐々木 雅英	権利者 同左
産業財産権の種類、番号 特許、PCT/JP2021/2129	出願年 2021年	国内・外国の別 外国

〔取得〕　計0件

〔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
研究分担者	松本　隆太郎 (Matsumoto Ryutaroh) (10334517)	東京工業大学・工学院・准教授 (12608)	
研究分担者	清水　亮介 (Shimizu Ryousuke) (50500401)	電気通信大学・大学院情報理工学研究科・准教授 (12612)	

	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
研究協力者	遠藤　寛之 (Endo Hiroyuki)		

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