伝送距離が600 kmを超える光ファイバーによる量子暗号通信

Fiber-Based Quantum Communications beyond Distance of 600 km

ミルコ ピタルガ Mirko PITTALUGA　　アンドリュー シールズ Andrew J. SHIELDS

量子鍵配送（QKD）は，サイバー攻撃する側がどのような計算リソースを使用するかに関わらず，情報通信のための暗号鍵を二者間で安全に共有できる唯一の方法である。QKDでは，物理的な量子状態，すなわち量子ビットを，多くの場合光ファイバーで伝送するが，送信できる量子ビット数は，伝送距離とともに指数関数的に減少するため，QKD回線の最大長には限界がある。

東芝欧州社 ケンブリッジ研究所は，独自のTwin Field QKD（TF-QKD）プロトコルとデュアルバンド安定化と呼ばれる位相安定化技術により，世界最長（注1）となる600 kmを超える伝送距離を達成し，大規模な量子暗号通信網の実現可能性を実証した。

Quantum key distribution (QKD) is the only technique that allows two users to securely share encryption keys for use in digital information systems with guaranteed security regardless of the resources available to an attacker. QKD relies on the transmission of physical quantum states, or qubits, across an optical channel, often an optical fiber. Unfortunately, the number of qubits that reach the end of an optical fiber decreases exponentially with fiber length. This imposes a limit on the maximum length of current QKD links.

The Cambridge Research Laboratory of Toshiba Research Europe Limited overcame this fundamental limitation by introducing a new QKD protocol in 2018 called Twin Field Quantum Key Distribution (TF-QKD). In 2021, we developed an experimental system and a new phase stabilization technique, called dual-band stabilization, which allowed us to set a new distance record for QKD on fiber, surpassing the 600 km distance for the first time and demonstrating the feasibility of quantum communications over national-scale distances.

1. まえがき

暗号化は，秘密を保持して安全な情報の伝送を支える技術であり，非公開のメッセージ送信や，オンラインバンキングの個人認証，パスワード確認などで広く利用されている。現在，多くの暗号化は，攻撃者が使うコンピューターの能力に限界があることを前提とする，公開鍵方式に基づいている。しかし，計算に量子効果を利用する量子コンピューターの発展に伴い，現在の暗号鍵は短時間で解読されるおそれが指摘されており[1]，情報通信の安全性が脅威にさらされている。

一方で，情報通信に量子効果を利用することで，情報理論的に安全に暗号鍵を交換できる。量子の世界では，物理状態の観測が，物理状態そのものに影響を与える。この基本的な仕組みを利用し，量子状態により符号化された情報をやり取りすることにより，2人の正当なユーザー間だけで暗号鍵を共有するQKDで，これを実現できる。暗号鍵が攻撃者に盗聴（観測）されると，鍵そのものが変化して盗聴の検出が可能になる。盗聴を検出した際はその暗号鍵を無効にし，新たな暗号鍵を発行することで，盗聴されていないことが保証された安全な暗号鍵を共有できる。注目すべきことは，攻撃者が使えるリソースが，量子コンピューターを含むどんなに高性能なものであっても，QKDでは安全性が保証された通信が可能であるという点である。

量子暗号通信で広く使用される量子は光の粒子である光子であり，多くの場合，光ファイバーを用いた通信回線で伝送される。しかし光子は，伝播（でんぱ）媒体によって散乱し，回線の端まで到達しない場合があるため，暗号鍵の伝送速度と伝送距離に限界が生じる。理論上，2地点間のQKD回線によって伝送されるセキュアビット数は，ηを通信チャネル伝送確率として，1.44 ηが上限である[2]。この限界は，“repeaterless secret key capacity”，又はPirandola–Laurenza–Ottaviani–Banchi（PLOB）境界と呼ばれ，最近までQKDの限界と考えられていた。2018年に，この限界は，東芝欧州社が提案したTF-QKD[3]により延長された。実用的には，実環境に敷設された光ファイバーの温度変化や振動などの環境変動の影響なども加味され，商用QKDシステムの最大距離は150 km[4]程度，最新の学術論文で

（注1） 2021年6月現在，当社調べ。

も400 km[5]程度である。このように，伝送距離の限界の延長は，QKDの最も大きな課題の一つである。

この論文では，2章でTF-QKDの概要を，3章で光ファイバーの温度変化や振動などの環境変動の影響を補正するデュアルバンド安定化技術について述べる。4章では，これらの技術を用いて達成した，600 kmを超える光ファイバーでの量子暗号通信について述べる。

2. TF-QKDプロトコル

一般的な量子暗号通信では，2人のユーザーが送信者及び受信者として，通信回線を通じて符号化したパルスを直接交換する。この構成を採用しているプロトコルはポイントツーポイント（**図1**(a)）と呼ばれ，1章で述べたPLOB境界[2]による制限を受ける。

TF-QKDプロトコルは，ポイントツーポイントとは異なるトポロジーを採用し，ユーザー1とユーザー2の両方が送信者として符号化したパルスを中央ステーションに送信する。中央ステーションでは，入ってくる光子の1次の光学的干渉を利用することで，実効的に通信距離を2倍に延長し，PLOB境界を超えることも可能となる。図1(b)は，TF-QKDの典型的なトポロジーを示している。これを，多くの送信者が同じ中央ステーションに接続されているスター型ネットワークに発展させることも可能である。この構成では，量子暗号通信ネットワークの展開に必要な資源を共有することができるため，大都市でのネットワーク構成に適している。当社は，2019年に最初の実験的実装を行い，TF-QKDを原理検証した[6]。

3. デュアルバンド安定化技術

量子ビット列の伝送に使用される光ファイバーは，環境の温度変化や振動などで膨張と収縮が発生することは避けられず，これによって位相に符号化された情報が乱される。これは，このプロトコルを実装する際に解決するべき課題である。これに対処するため，デュアルバンド安定化と呼ぶ新たな位相安定化技術を開発した。デュアルバンド安定化技術は，QKD信号に加えて，別の波長の参照信号を導入することで，通信チャネルの位相ノイズの問題を解決する。ほかの研究グループの安定化手法[7, 8]とは異なり，量子信号への影響を最小限に抑えながら，通信チャネルによって生じる数十ラジアン/秒オーダーの高速な位相変動を補正する。その結果，より高い暗号鍵転送速度と長い距離通信を実現できる。

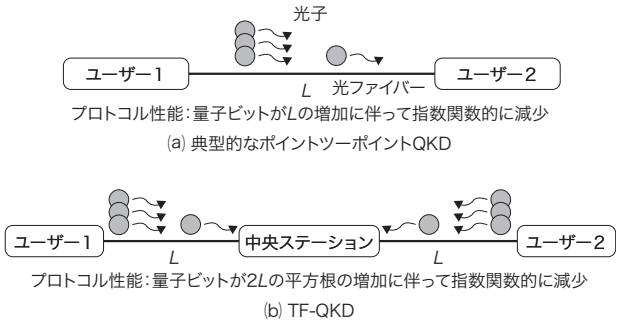

図1. ポイントツーポイントQKD及びTF-QKDのプロトコル
TF-QKDは，中央ステーションを置くことで，実効的に通信距離を2倍に延長できる。
Point-to-point QKD and TF-QKD protocols

デュアルバンド安定化では，二つの異なる，近い波長λ_1，λ_2の光信号を同一通信チャネルに送信する。λ_1は量子情報の符号化に，λ_2は安定化に使用される連続波信号の波長である。λ_2の信号の干渉結果は，長距離の通信チャネル（光ファイバー）で発生する位相ドリフトの検知に使用される。この情報は更に，位相変調器（PM）上で数百キロヘルツの速度で動作する高速フィードバックループを介して，λ_2を完全に安定化させるのに使用される。

λ_1とλ_2は近いため，λ_2に対して通信チャネルが安定化されると，λ_1についてもほぼ安定化される。残るλ_1の低速位相ドリフトは，λ_1だけに作用する第2の低速フィードバックシステムと，アクチュエーターとして数十ヘルツの速度で動作する光ファイバーストレッチャー（FS）とを使用することで，安定化される。この安定化技術は，数百kmの光ファイバーを通って伝播された後でも，量子信号の光学的位相を，波長の数分の一の範囲内で一定に維持できる。

図2に，デュアルバンド安定化技術の性能特性を示す。チャネルノイズ（位相ドリフトの標準偏差）が4桁小さくなっており，安定化後に初めてTF-QKDプロトコルが実行可能となる。

4. 600 kmを超える光ファイバーでの量子暗号通信

図3(a)に示すように，デュアルバンド安定化技術を適用したTF-QKDプロトコルを実装した。実装したシステムは，三つのモジュールで構成されている。伝送路の両端において暗号鍵を生成する伝送ユーザー2か所（ユーザー1とユーザー2）と，鍵生成プロセスにおけるリレーとして働く中央ステーション1か所である。中央ステーションは，モジュール内の二つの連続波長レーザーL1及びL2を使用してλ_1とλ_2を生成する。図3(a)の下方のサービス光ファイバーにより，これらの波長を送信者と受信者に伝送する。送信者と受信者はそれぞれの$L1_A$及び$L1_B$レーザーを，光位相固定ルー

プ（OPLL）を介してL1に固定する。続いて，エンコーダー内にある強度変調器とPMを使用して，送信者と受信者それぞれでローカルに生成した光に対して強度変調・位相変調を掛ける。最後に，λ_1及びλ_2信号を通信チャネル（光ファイバー）上で多重化し，中央ステーションに送信する。中央ステーションは，PMとFSでデュアルバンド安定化を行うことで，通信チャネルに発生した位相ノイズを除去し，ビームスプリッター（BS）で送信者と受信者の信号を干渉させる。検知器D_0とD_1はλ_1における干渉結果を記録し，D_2はλ_2における干渉結果を記録する。

実験では，153.2 ～ 605.2 kmの様々な長さの通信チャネルについてシステムをテストした。図3(b)に，通信チャネルの長さに対する鍵配送速度（SKR：Secure Key Rate）を，シミュレーションした曲線とともに示した。提案したデュアルバンド安定化技術による改善を評価するために，光ファイバーによる従来のTF-QKD[7], [8]及びQKD実証[5]のSKRも同じグラフ内に示した（点線）。デュアルバンド安定化により，長距離QKDの性能が大きく向上したことが分かる。距離については，従来のTF-QKD及びQKD実証に対して100 km以上改善できた。これは，位相安定化のための強い信号による信号光への影響が，ごく僅かであるためと考えられる。SKRについては，これまでの技術で達成できた最大の伝送距離500 kmにおいて，2桁の向上となった。これは，安定化に用いる参照信号を収容するために，符号化のための信号のクロック周波数を下げる必要がなかったことが要因であると考えられる。

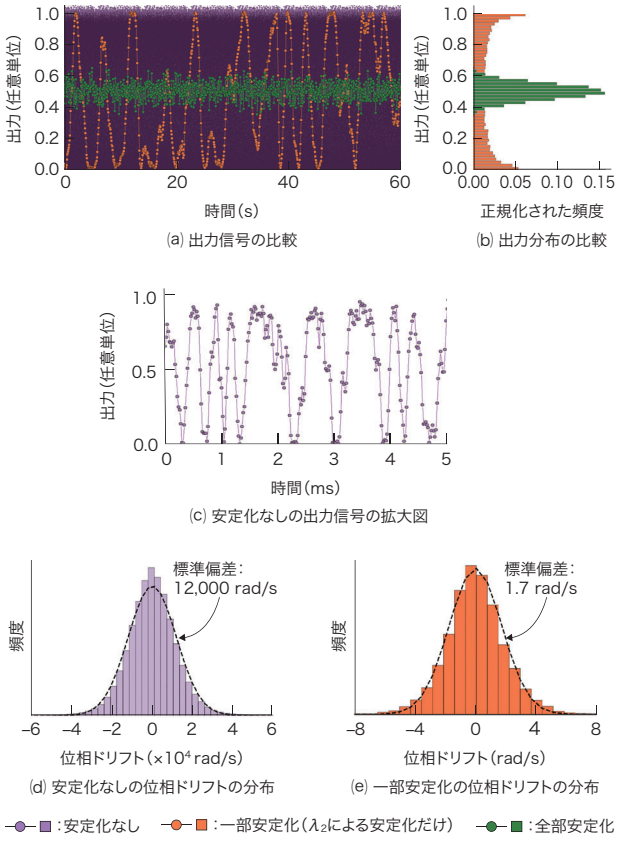

図2.　デュアルバンド安定化技術の性能

デュアルバンド安定化技術の適用で，位相ドリフトの標準偏差が4桁小さくなった。

Performance of dual-band stabilization technique

5.　あとがき

光ファイバーによる安全な量子暗号通信において，伝送距離600 km（損失100 dB）の壁を初めて超えることができ

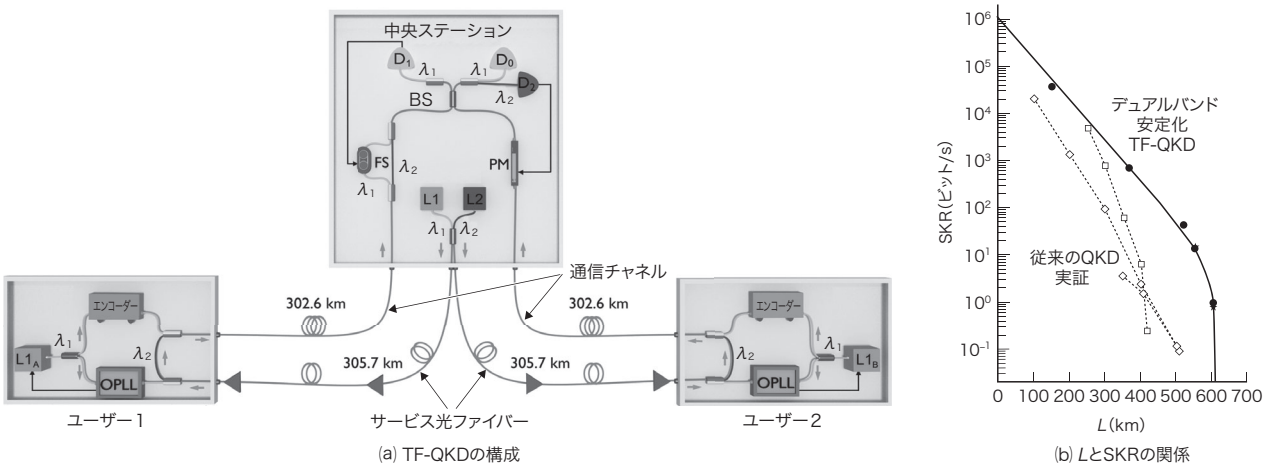

図3.　デュアルバンド安定化技術を用いたTF-QKDの実験設定

ユーザー1とユーザー2が位相で符号化されたパルスをλ_1で中央ステーションに送信する。中央ステーションは，安定化のためにλ_1とλ_2を参照波長として供給する。

Setup of demonstration experiments on TF-QKD using dual-band stabilization technique

た。今回導入したデュアルバンド安定化技術は，TF-QKD以外にも，DLCZ（Duan-Lukin-Cirac-Zoller）タイプの量子リピーター[9]や，長基線望遠鏡[10]，長距離の量子指紋[11]，量子インターネット向けの位相ベースのアーキテクチャー[12]など，ほかの量子通信の用途にも適用できる。量子ネットワーク内でユーザー間の距離を離すことができるため，コストと複雑性を軽減しながら大規模な量子インフラを構築できるというメリットもある。

この研究の一部は，欧州連合のHorizon 2020研究イノベーションプログラムの補助金番号857156「OPENQKD」，マリー・キュリー補助金番号675662，及び英国工学・物理科学研究評議会（EPSRC）による支援を受けた。

文　献

(1) Gidney, C. ; Ekerå, M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum Physics. 2021, **5**, 433.
(2) Pirandola, S. et al. Fundamental limits of repeaterless quantum communications. Nature Communications. 2017, **8**, 15043.
(3) Lucamarini, M. et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature. 2018, **557**, p.400–403.
(4) Wonfor, A. et al. "Quantum networks in the UK". Metro and Data Center Optical Networks and Short-Reach Links IV. Edited by Glick,M. et al. 2021-03, SPIE. 2021, SPIE Proceedings 11712.
(5) Boaron, A. et al. Secure Quantum Key Distribution over 421 km of Optical Fiber. Physical Review Letters. 2018, **121**, 190502.
(6) Minder, M. et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. Nature Photonics. 2019, **13**, p.334–338.
(7) Fang, X.-T. et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. Nature Photonics. 2020, **14**, p.422–425.
(8) Chen, J.-P. et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. Physical Review Letters. 2020, **124**, 070501.
(9) Duan, L.-M. et al. Long-distance quantum communication with atomic ensembles and linear optics. Nature. 2001, **414**, p.413–418.
(10) Gottesman, D. et al. Longer-baseline telescopes using quantum repeaters. Physical Review Letters. 2012, **109**, 070503.
(11) Arrazola, J. M. ; Lütkenhaus, N. Quantum fingerprinting with coherent states and a constant mean number of photons. Physical Review A. 2014, **89**, 062305.
(12) Kimble, H. J. The quantum internet. Nature. 2008, **453**, p.1023–1030.

ミルコ　ピタルガ　Mirko PITTALUGA, Ph.D.
東芝欧州社 ケンブリッジ研究所
博士（工学）
SPIE，Optica 会員
Toshiba Europe Ltd.

アンドリュー　シールズ　Andrew J. SHIELDS, Ph.D.
東芝欧州社 ケンブリッジ研究所
博士（理学）
Royal Academy of Engineering, Institute of Physics 会員
Toshiba Europe Ltd.

和　訳
岡田　隆三　OKADA Ryuzo
東芝欧州社 ケンブリッジ研究所
Toshiba Europe Ltd.