高速量子鍵配送プロトタイプによる実証運用

Field Test of High-Speed Quantum Key Distribution Prototype

ジェイムズ　ダインズ　　ジュリアン　ユアン　　アンドリュー　シールズ
■James DYNES　■Zhiliang YUAN　■Andrew J. SHIELDS

通信ネットワークの安全性を確保するために，高速ビットレートで連続運用が可能な能動的な安定化法（Active Stabilization法）を適用した量子鍵配送（QKD）を開発した。この鍵配送技術は物理学の法則に基づき，いかなる攻撃からも安全性を保証するものであり，現在及び将来のネットワークにおける情報通信の安全性確保を可能にする。

このQKDシステムは，東京都内に敷設されたロバスト性が必要とされる光ファイバを用いて実証実験が行われた。開発したActive Stabilization法によって，セキュアビットレート値0.3 Mビット/sで24時間，安定に連続運用することができた。この高速かつ安定したセキュアビットレートにより，他に類を見ない帯域での無条件に安全な秘匿通信を実現するドアが開かれたと言える。

Toshiba has developed a high-bit-rate, actively stabilized, and continuously operating quantum key distribution (QKD) system for securing communication networks. This key distribution technology is based on the laws of physics to guarantee security from any attack, and can secure information exchanges in both today's and tomorrow's network infrastructure.

The newly developed QKD system has been robustly field tested on installed fiber in the Tokyo metropolitan area. Other QKD vendors supplied systems to operate over other links in the network. Thanks to an active stabilization technique, the Toshiba QKD system performed stably and continuously with a secure bit rate of 0.3 Mbit/s averaged over a 24-hour period. This high and stable secure bit rate opens the door to the realization of unconditionally secret communications with unparalleled bandwidths.

1　まえがき

量子鍵配送（QKD）では，量子鍵の安全性が量子力学の法則により無条件に保証される。このため，デジタル鍵が秘密裏に交換されるグローバルネットワークの将来の安全性を保障する技術として注目されている。またQKDは，既存の光ファイバを用いて鍵情報を送信できるので，実用的な技術である。

これまで，QKDの多くの検証実験は，研究室内の2点間でのリンク実験に限定されていた。しかしQKDの実現可能性を立証するには，ネットワーク上での実証運用が必要である。また，TV（テレビ）会議の暗号化といった広帯域が要求されるアプリケーションをQKDによって実際に秘匿化できることを示すことが，QKDを商業的に成功させるために不可欠である。

ここでは，クロック周波数1 GHzで動作する高速QKDのプロトタイプを東京都内の市街地エリアネットワーク リンクである，独立行政法人 情報通信研究機構（以下，NICTと呼ぶ）が運用するオープン テストベッド ネットワーク（東京QKDネットワーク，通称JGN-2+）に適用した結果について述べる。

東芝欧州研究所（以下，TRELと記す）は，このネットワークにおいて，24時間以上の無停止連続運用で平均セキュアビットレート値が約304 kビット/sという他に類を見ない高いパフォーマンスを実現した。ワンタイムパッド（OTP）暗号化に十分な速度を確保したことも重要なポイントである。

2　東京QKD ネットワーク

2.1　背景

2008年10月にTRELは，欧州のコンソーシアムであるSECOQC（Secure Communication based on Quantum Cryptography）の一員としてQKDネットワーク実証運用試験に参加した。5台のQKDシステムを使用して行われた実証運用でのセキュアビットレート値は，6 ～ 33 kmの距離範囲の光ファイバネットワーク上において数kビット/sであった。TRELは当時として最長距離33 kmのネットワークで連続セキュアビットレート値3 kビット/sを達成しており，このセキュアビットレート値は電話での会話を実現するのに十分なものであった。しかし，SECOQCで得られた数kビット/sのセキュアビットレート値は，例えばTV会議の安全性確保といった広帯域アプリケーションの暗号化に対しては十分ではなかった。この意味で，より高速のビットレート値でのシステム実証運用が必要であった。

NICTは，50 kmのネットワークでセキュアビットレート値1 Mビット/sでのQKDネットワークの実現を目標として2010年度を最終年度とする国家プロジェクトを統括してきた。このプロジェクトには日本電気（株），三菱電機（株），及び日本電信電話（株）の3企業が参加し，各社の最新量子技術を用いたQKDシステムを個別に構築してきた。このプロジェクトの課題の一つとして，2010年10月に東京QKDネットワークを利用し

て，128 kビット/sで安全性が確保されたTV会議を含む，いくつかのアプリケーションでQKDの実証運用を示すことがあった。

実証用試験には，TREL，他の欧州のベンダーであるidQuantique（以下，iDQと呼ぶ），及びAll Vienna(注1)も要請されて参加した。iDQは転送速度が数kビット/sのQKDシステムを，All Viennaは量子もつれ光子対を用いた転送速度が数kビット/sのQKDシステムを使用した。一方TRELは，GHzクロックで同期する単一光子検出器を用いて自己制御により調整が不要なQKDシステムを実現していた。このシステムは国家プロジェクトの目標であったセキュアビットレート値1 Mビット/sに対応するものであった。

以下では，このプロジェクトに参加したTREL以外の企業及び機関を，“機関A”～“機関E”と記す。

2.2 物理的リンク設定

東京QKDネットワークでの実験で使用した構成の概要を**図1**に示す。小金井，大手町，白山，及び東京大学本郷キャンパスの4か所のアクセスポイントから構成されている。

各アクセスポイントは市販の光ファイバ束で接続され，光ファイバ束には多数の継ぎ目や接続部があるため，比較的損失が多いことがQKDシステムとして課題となった。例えば，小金井～大手町間の損失は0.3 dB/kmである。

更に，この光ファイバ束は全長の約50 %が電柱を利用して地上に架設されており，周辺環境の変動の影響を受けやすい。また，古典的なトラフィックを転送する他の光ファイバと近接しており，隣接する光ファイバに起因する光子の混入も問題であった。

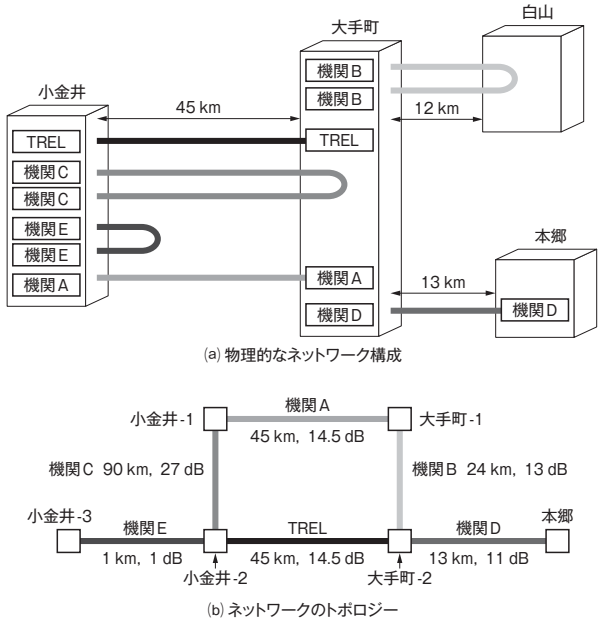


図1. 東京QKDネットワークの概要 — TRELは，小金井～大手町間の45 kmのリンクを担当してQKDシステムを検証した。

Outline of Tokyo QKD Network

2.3 ネットワークの概要

図1(a)で示した物理的構成は，図1(b)で示す6ノードメッシュ対応のアーキテクチャに対応し，合計六つのリンクは1～90 kmの光ファイバで接続された。TRELは小金井～大手町間の45 kmのリンクを担当した（詳細後述）。

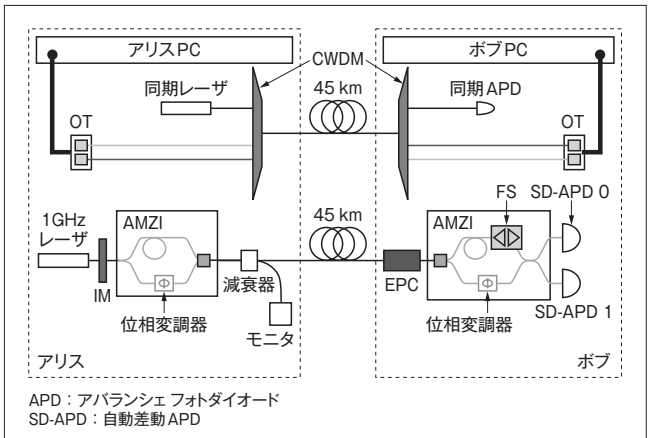
機関Bは大手町～白山～大手町間の24 kmループバック設定でクロック周波数100 MHzのデコイ法によるBB84プロトコルを使用した。機関AとNICTは，小金井～大手町間（45 km，単方向）でクロック周波数1.25 GHzのデコイ法によるBB84プロトコルを採用し，NICTの超伝導単一光子検出器（SSPD）を利用した。機関Cは長さ90 kmのループバックを担当し，独自のSSPDと組み合わせた差分位相シフト（DPS）プロトコルシステムを用いた。機関Eは小金井のNICT構内に敷設された長さ1 kmの光ファイバにBBM92エンタングルQKDシステムを適用した。大手町～東京大学本郷キャンパス間に残ったリンクには機関DのPlug-and-Play型QKDシステム（13 km）を設置した。

3 TRELの高速ビットレートQKDシステム

TRELのQKDシステムは，デコイ法を適用して最終的な安全鍵レートを向上させたGHzクロック位相エンコードの高速ビットレートQKDシステムである。

3.1 システムアーキテクチャ

主要コンポーネントの概念を**図2**に示す。送信器（以下，アリスと呼ぶ）では，FPGA（Field Programmable Gate Array）



APD：アバランシェ フォトダイオード
SD-APD：自動差動APD

図2. GHzクロックQKDシステムの概要 — 送・受信器は量子信号と古典的情報の送・受信を行う二つの光ファイバで結合され，システム全体は1 GHzのクロックで制御されている。

Outline of GHz clock QKD system

（注1） オーストリア工学研究所と，量子工学及び量子情報研究所，ウィーン大学の三つの研究機関から成る研究チーム。

ボードがシステムのマスタクロックを供給し，各種のQKD光学系を作動させるための同期パルスのパターンも供給する。パルスレーザは波長1,548 nmで，幅50 p（ピコ：10^{-12}）sのパルスを繰返し率1 GHzで発生させる。これらの光パルスは，信号及び強弱のデコイパルスを発生するために使用される強度変調器（IM）を通して送信される。信号パルスは99％以上の確率で送信されるが，それとは対照的に強いデコイパルスは1/5の強度であり，確率1％以下で送信される。弱いデコイパルスは信号パルスと比較すると，ほぼ1/1,000の強度を持つ。

信号パルスは，平均強度0.5光子/パルスの単一光子レベルまで減衰させる前に非対称マッハ・ツェンダー干渉計（AMZI）を用い，ビット情報を位相にエンコードさせる。光モニタが常時，平均光強度を測定し，減衰器にフィードバック信号を送り光強度を一定に保つ。エンコードされた光子（量子信号）は，大手町～小金井間に敷設された長さ45 kmの専用光ファイバリンクを通って受信機（以下，ボブと呼ぶ）に送信される。

波長1,571 nm及び1,591 nmで作動する2台のGビット/s光トランシーバ（OT）によりアリスとボブが制御されている。ボブとの同期は，波長1,550 nmで作動する粗波長分割多重化（CWDM）レーザにより提供される。これらの古典的な信号はCWMDを使用して波長多重化され，第2の45 km光ファイバリンクを通じて送信される。アリスとボブとの間の古典的なトラフィック（誤り訂正及び秘匿性増強メッセージを含む）は全て，この第2光ファイバを通じて送信され，GHz帯で信頼性を低くする第3者LANを不要とするのが特徴である。

ボブ側ではFPGAボードで光学系の電気信号を駆動する。着信する量子信号は，電子偏光制御装置（EPC）を通過した後，復号AMZIに入力される。2台の自己差分化単一光子検出器が復号された光信号の検出に使用される。自己差分型検出器は小型熱電子冷却器によって-30 ℃に冷却され，暗係数率10 kHz，単一光子効率19％で動作する。

時系列キャプチャボードは光子の到着時刻をサンプリングし各事象に対するクロック数を生成する。これらのクロック数をボブの制御パソコン（PC）に供給し，信号に“篩（ふるい：Sift）”がかけられ，次いで古典的なチャネルを通じてアリスに送信される。アリスは次に，ボブからのクロック数と送信された変調パターンで保存されたクロック数とを比較して“篩をかけた鍵”すなわちシフト鍵（Sifted Key）を発生させる。このシフト鍵は，システムの不完全性に起因するわずかな誤りを除き，アリス側とボブ側の両方で同一になる。これらの誤り頻度を定量化すると，量子ビット誤り率（QBER）は通常約4％である。

3.2　連続運用のためのActive Stabilization法

検出器の計測率を利用したフィードバック信号により，検出器のゲート遅延と光の偏光状態を調整する。光ファイバストレッチャ（FS）はフィードバック信号としてQBERを使用して制御される。セキュアビットレート値を著しく劣化する可能性がある有限鍵のサイズ効果を軽減するためには，能動的な安定化法（Active Stabilization法）が特に有効である。東京QKDネットワークの光ファイバは，光ファイバ束内で並行に敷設された隣接ファイバからの混信がQKDに大きな影響を与えた。通常の強い光信号が，微弱な量子信号に混じりQBERの増大につながる。しかし，自己差分型単一光子検出器は雑音の多い光ファイバで特に威力を発揮する。これらの検出器が有効となる時間は1クロック当たり100 psであることが特徴で，量子信号の幅（50 ps）は，アリスで光子の偏光を規定するBragg格子を設置することで45 kmの光ファイバを通じた送信の後でも保存されている。

したがって，光ファイバ内の浮遊光子の大半は拒絶され，実験用ダークファイバ（未使用の敷設ファイバ）で得られる通常の約4％というQBERが保持できた。また，通常必要であるボブ側でのバンドパスフィルタは不必要であった。バンドパスフィルタは信号の損失を増大させ，最終的なセキュアビットレート値を減少させるので，これを使わないQKDシステムは信号損失に強いと言える。

3.3　誤り訂正，秘匿性増強，及びセキュリティ分析

カスケードプロトコルによる誤り訂正及び秘匿性増強のための演算処理は，複数のスレッドを同時に処理できる2台のPCで行う。試験の結果，シフト鍵のブロックサイズが1 Mビットの場合に5 Mビット/sを上回る誤り訂正速度が得られた。この処理速度は，損失が10 dBを超えるようなチャネルでGHzクロックQKDシステムを運用するのに十分である。

秘匿性増強はテプリッツ行列（対角一定行列）を利用して実現した。誤りが訂正されたシフトビット ベクトル（Sifted Bit Vector）とテプリッツ行列との積により，小さなセキュアビット ベクトルが生成できる。このセキュアビット ベクトルが最終的なセキュア鍵を形成する。送信される信号，デコイ，真空状態及び付随するQBERをリアルタイムで計算し，セキュア鍵の大きさを導き出す。計算は有限なサイズの鍵であることを前提としており，鍵のサイズ効果を含め，無条件に安全性が保証される。これは鍵サイズ効果をしばしば無視してきた以前の実証運用からの著しい改善である。

3.4　敷設光ファイバでのセキュアビットレートの記録

このシステムを24時間連続運用したときのセキュアビットレートの推移を**図3**に示す。(a)は，研究室内のスプール50 kmのシングルモードファイバ（損失10 dB）で得られた1 Mビット/sを超えるセキュアビットレートである。(b)は，大手町～小金井間45 kmに対して得られたセキュアビットレートである。高いチャネル損失14.5 dBが存在する状況でも，24時間運用での平均セキュアビットレート値304 kビット/sが得られた。現時点では，研究室内及び実証運用でのビットレート値のいずれの結果からも安全なOTPビデオ送信が可能になった。

東京QKDネットワークのTRELシステム及び他のベンダー

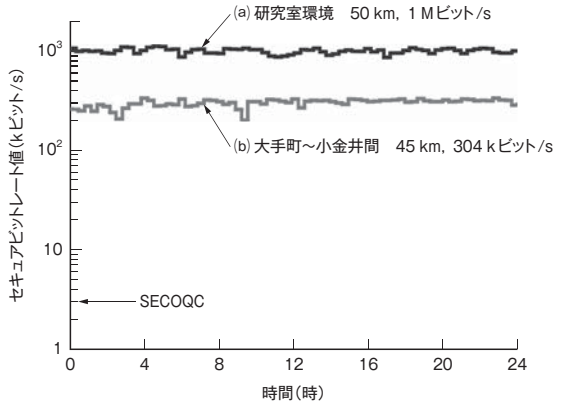


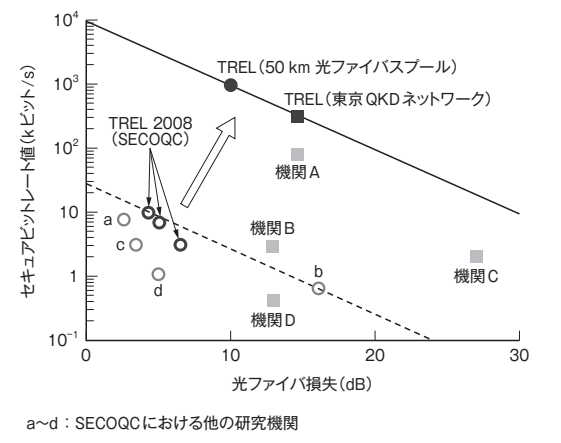
図3．24時間連続運用時のセキュアビットレートの推移 — 研究室環境では50 kmの距離で1 Mビット/s，市中敷設ファイバでは45 kmで304 kビット/sの暗号鍵配信を実現した。

Changes in secure bit rate during 24 hours continuous operation

のセキュアビットレート値，並びに以前のSECOQC実証運用でのセキュアビットレート値を**図4**に示す。TRELシステムのセキュアビットレート値は，他の全てのシステムの値を大きく上回っている。

TREL及び機関Aのシステムは，同じ光ファイバ長45 kmと損失14.5 dBで運用されたものであり，両システムを直接比較できる。TRELシステムのセキュアビットレート値304 kビット/sは機関Aのシステムの値よりも4倍高い。また，今回の実証運用では，機関Aのシステムが約30分間の運用だったのに対し，TRELシステムは24時間連続で運用しており，より堅牢（けんろう）であることも示された。更に，60時間にわたり長時間運用されたにもかかわらず，セキュアビットレート値の劣化はごくわずか，あるいはまったく認められなかった。

TRELシステムのビットレート値304 kビット/sは，2008年10月



a～d：SECOQCにおける他の研究機関

図4．2008年と2010年の実証運用で得られたセキュアビットレートの比較 — TRELは2年間で，セキュアビットレートを2桁以上向上させた。

Comparison of secure bit rates attained by field tests in 2008 and 2010

にSECOQCの協力のもとにTRELで実施した以前のQKD実証運用時の値よりかなり高かった。当時の実証運用では，低いクロック周波数を使用したTRELの古いQKDシステムを採用し，光ファイバ損失はわずか7.5 dBであったにもかかわらずセキュアビットレート値は3 kビット/sであった。今回，東京での実証運用でセキュアビットレート値が少なくとも2桁のオーダーで向上したことは，自己差分型制御技術及び連続運用が実現したことによる単一光子検出技術が進歩した結果である。

4　あとがき

より高いビットレート値のQKDシステムを実現し，市街地光ネットワークで実証運用を行った。Active Stabilization法によりTRELシステムは，全長45 km，セキュアビットレート値304 kビット/sで24時間連続運用を達成した。このシステムからのセキュア鍵により，高速のセキュア鍵リフレッシュ率が要求される広帯域アプリケーションの安全性を確保できる。

文　献

(1) Yuan, Z. L. et al. High speed single photon detection in the near infrared. Appl. Phys. Lett. **91**, 4, 2007, p.041114-1－041114-3.
(2) Dixon, A. R. et al. Continuous operation of a high bit rate quantum key distribution system. Appl. Phys. Lett. **96**, 16, 2010, p.161102-1－161102-3.
(3) Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. Opt. Express. **19**, 11, 2011, p.10387－10409.

ジェイムズ　ダインズ　James DYNES, Ph.D.
東芝欧州研究所 ケンブリッジ研究所 量子情報グループ 研究主務，理博。量子情報半導体デバイス及び量子暗号通信の研究・開発に従事。
Toshiba Research Europe Ltd.

ジュリアン　ユアン　Zhiliang YUAN, Ph.D.
東芝欧州研究所 ケンブリッジ研究所 量子情報グループ 主任研究員，理博。量子情報半導体デバイス及び量子暗号通信の研究・開発に従事。
Toshiba Research Europe Ltd.

アンドリュー　シールズ　Andrew J. SHIELDS, Ph.D.
東芝欧州研究所 ケンブリッジ研究所 量子情報グループ グループリーダー，理博。量子情報半導体デバイス及び量子暗号通信の研究・開発に従事。
Toshiba Research Europe Ltd.

和　訳
内古閑　修一　UCHIKOGA Shuichi
東芝欧州研究所 ケンブリッジ研究所副所長
Toshiba Research Europe Ltd.