長期安定運用を可能にする高速量子鍵配送技術

High-Speed Quantum Key Distribution Technology for Realization of Long-Term Stable Operation

アレキサンダー　ディクソン　　ジェイムズ　ダインズ
■Alexander R. DIXON　　■James DYNES

量子鍵配送（QKD：Quantum Key Distribution）は，通信路の盗聴を検出し，情報漏えいを防ぐ唯一の方法を提供する。
東芝は，高速なQKDシステムの試作機を開発した。試作機は，小型で長時間安定して動作させることが可能で，気象条件などの変動があってもQKDを継続できる自動安定化機構を備えている。この試作機を用いて，東京の大手町～小金井間をつなぐ，全長45 kmの標準的な敷設済み通信用光ファイバを利用した実証実験を行った。その結果，34日間の安定稼働と，合計の暗号鍵配送量として世界最大(注1)の878 Gビットを記録し，この間の暗号鍵配送速度は平均301 kビット/sを達成した。

Securing information in communication networks is an important challenge in today's world. Quantum key distribution (QKD) technology can provide unique capabilities toward achieving this security by detecting intrusions and preventing information leakage.

Toshiba has been engaged in the research and development of a high-speed QKD technology. As part of this research, we have conducted a field trial using a high-bit-rate prototype QKD system connected by standard telecommunication fibers over a distance of 45 km from Otemachi to Koganei in central Tokyo that provided a world-record total of 878 Gbit of secure key data over a 34-day period, corresponding to a sustained key rate of around 301 kbit/s. The prototype QKD system is compact, robust, and automatically stabilized, making key distribution possible under diverse weather conditions.

1　まえがき

光ファイバによる情報通信ネットワークは，現代社会の極めて重要な基盤であり，経済や社会活動は地球規模で張り巡らされた光ファイバケーブルに依存していると言っても過言ではない。光ファイバネットワークの重要性が増すとともに，ネットワークを流れる情報の安全性に対するニーズが増大している。利用者は通信相手をお互いに認識し，データ漏えいのない安全な通信ネットワークを望んでいる。

量子鍵配送（QKD：Quantum Key Distribution）は，通信路の盗聴を検知し，安全な情報通信システムを実現する唯一の可能性を提供する技術である。QKDはこれまで実験室での研究が活発に行われており，近年，長期運用を目指した実験や，実際の通信ネットワークを使った実験，複数の異なるQKDシステムの結合など，実用化に向けた研究に焦点が当てられるようになってきた。

実用的なQKDシステムを実現するには，次に述べる様々な課題を克服する必要がある。

(1)　通信に用いる光ファイバの影響　　環境条件の変化や物理的なストレスにより定常的に強い変動が発生し，量子信号（光子）の状態に影響を与える。更に，融着や折曲げなどにより高い損失が発生する。

(注1)　2015年3月にOptics Express[1]で発表，当社調べ。

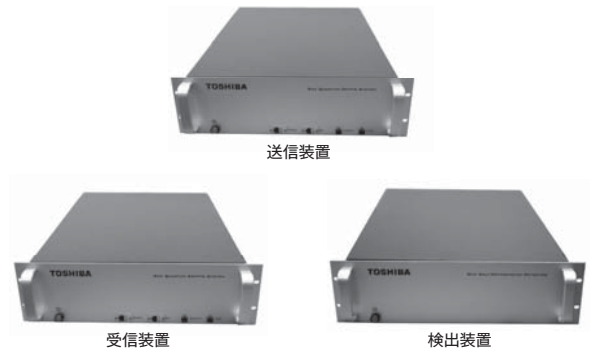


図1．高速QKD装置 — QKDシステムの試作機は送信装置，受信装置，及び検出装置の3台から構成される。
Prototype high-speed QKD system

(2)　QKDシステムを構成するソフトウェア及びハードウェアの要件　　光ファイバでの通信に影響を与える全ての条件に打ち勝つだけでなく，標準的な通信装置として運用できる設計が求められる。

(3)　システム保守の回数削減　　障害が起きても自動的に復旧し，サービス停止が発生しないようにする。

東芝は，このような課題認識のもと，小型で長時間安定した動作が可能な，高速なQKDシステムの試作機を開発した。ここでは，試作機の特長と敷設済みの光ファイバを利用した実証実験の結果について述べる。

2　QKDシステム試作機の概要

開発した試作機は，19インチラックマウント可能な送信装置，受信装置，及び検出装置の3台から構成される（**図1**）。通信プロトコルは，標準的なQKDプロトコルであるBB84[2]の通信速度を最大化し，安全性が証明された[3], [4]効率的BB84プロトコル[5]がベースであり，複数の光子が存在しても安全性が確保されるデコイ状態[6], [7]を持つ一方向通信方式を採用した。

QKDは，送受信者間で安全に暗号鍵（乱数ビット列）を共有する技術であり，最終的に暗号鍵となるビット情報を光子に符号化して送信する。

試作機は，光子を送るための量子チャネルとクロック信号や制御信号など古典信号を送るための古典チャネルを持ち，それぞれのチャネルに光ファイバを接続して通信を行う。極めて微弱な光子は，一般的な光通信で使われる強い信号に埋もれてしまうため，量子チャネルと古典チャネルの光ファイバを分離することでノイズを除去している。今回の試作機は2本の光ファイバを使用する構成であるが，1本の光ファイバに全ての信号を統合する実証試験もこれまでに実施している[8]。

送信装置では，1 GHzでパルス駆動されたレーザが，波長1,550 nm，パルス幅50 p（ピコ：10^{-12}）sの光子パルスを生成する。生成されたパルスは，強度変調器で変調され，信号パルスか，2種類の異なる強度を持つデコイパルスとなる。送信するビット情報は，非対称マッハツェンダー干渉計（AMZI）内の位相変調器によって光子の位相に符号化される。

受信装置では，光ファイバで生じる偏光のずれを補正するために偏光制御器が使用される。受信装置のAMZIには位相変調器及びファイバストレッチャが接続され，それぞれ位相符号化と光路長の補償に使用される。

受信装置のAMZIからの光子は，検出装置に入力される。光子は，ペルチェ素子で冷却され1 GHzでゲート駆動されたInGaAs（インジウム ガリウム ヒ素）アバランシェフォトダイオード（APD）で構成される単一光子検出器で検出される。この高速なゲート動作は，低いアバランシェ電流（低ノイズを実現）と，APDの出力を処理する自己差分技術[9]により実現した。

送信装置と受信装置のFPGA（Field Programmable Gate Array）ボードは，時刻同期のための光子へのタイムスタンプ付加や暗号鍵生成のための初期処理など低レベルプロトコル機能を実現する。また，誤り訂正や秘匿性増強と呼ばれる暗号鍵生成に必要な後処理と最終的な暗号鍵の保存処理を実行するために，鍵データをサーバへ送信する。

試作機の光学系は，これまでの設計[10]をベースとし，制御方式の改良を行った。主な改良点は，市販の電気部品やデバイスをFPGAボードに統合し，制御ソフトウェアの安定性を向上させた点である。これにより，電気系が単純化され予期せぬ異常が減り信頼性の高い運用が可能になるほか，ノイズや消費電力の低減とともに，製造工程を単純化することが可能になる。

3　敷設済み光ファイバによる実証実験

開発した試作機を，**図2**に示す東京の大手町～小金井間の敷設済み通信ネットワークに導入し，実証実験を行った。

大手町に送信装置を設置し，2本の光ファイバで小金井に設置した受信装置と検出装置に接続している。ファイバ長は45 km，損失は14.5 dB（0.33 dB/km）であり，融着や接続点などにより標準的なスプールファイバの損失（0.2 dB/km）よりも大きくなっている。2本の光ファイバの一方は量子チャネルに，他方は古典チャネルに使用している。

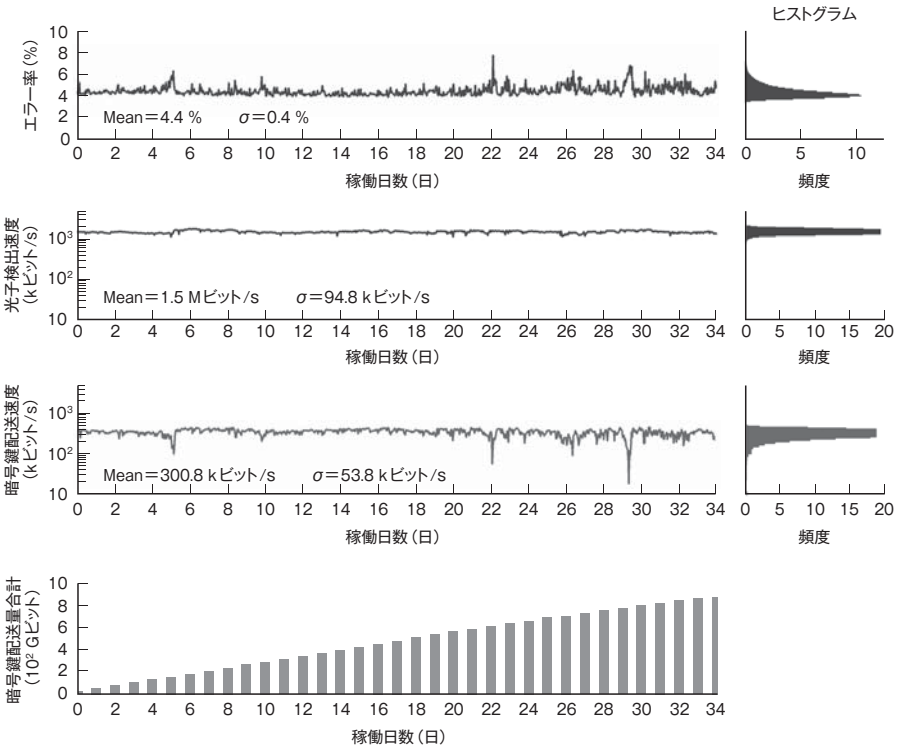
ファイバ全長の約50 %が架空線であることから環境要因に敏感であり，受信した光子の量子状態に影響を与える。環境要因としては，ファイバ長の伸縮の原因となる外気温や直射日光などによる温度変化や，光ファイバの動きの原因となる風や降水などが含まれる。実際に，QKDシステムの性能でもっとも重要な送信時間や複屈折の変動が発生し，光子を送信するための条件を定常的に変化させる。

光子の送信時間の変動による遅延を補正するには，受信装置でのクロック遅延パラメータの安定化が有効である。しかし今回の実証実験では，クロック信号は古典チャネル用光ファイバを通して送信されるが，環境要因の影響は並行する量子チャネル用光ファイバにも同様の変化を生じさせるため，ファイバ長に変化があっても，光子パルスの到着時間はクロック信号に近いものとなり，クロック信号の遅延は小さい。

検出装置での光子検出タイミングと受信装置の他のモジュールはクロック信号に同期しており，ファイバ長の変化による影響はほとんどない。自動安定化機構は，古典信号と量子信号との残りのタイミング差を補償することで，高い光子カウントレートを確実なものとする。

光ファイバで生じる複屈折の変動では，特に明け方や夕方

図2．大手町～小金井間での実証実験 — 45 kmの敷設済み光ファイバ2本で送信装置（大手町に設置）と受信・検出装置（小金井に設置）とを接続している。
Location of field trial of prototype QKD system



Mean：平均　　σ：標準偏差

図3．QKD装置試作機の性能 ― 連続稼働実験での暗号鍵配送量の合計は878 Gビット，暗号鍵配送速度は平均で301 kビット/sとなり，34日間1度も停止することなく安定に動作した。

Performance data of prototype QKD system obtained by field trial

のように温度変化がある間の影響が大きい。偏光自動安定化システムは，このような高速な変動をリアルタイムで補償することができる。これにより，前述したクロック信号のタイミング安定化とともに，安定した光子カウントレートを実現している。

試作機を用いた連続稼働実験では，34日間1度も停止することなく安定に動作するという結果を得た（**図3**）。この間の暗号鍵配送量は，合計878 Gビットで，平均の鍵配送速度は301 kビット/sであった。光子のカウントレートは平均1.5 Mビット/s，エラー率は平均4.4 %であり，ともに稼働期間中安定していた。また，この間の暗号鍵配送速度は平均301 kビット/sであり，エラー率の上昇による速度低下が数か所見られる。エラー率が上昇した要因の一つとして，環境変動が光ファイバに影響したことが考えられる。例えば，最初の速度低下時には強い風が観測されている。しかしこのような因果関係を実証するには，様々な気象条件の下でのより長期間のデータが必要となる。

34日間の実験終了時点で試作機は正常に動作しており，ここで示した稼働期間は装置の限界値ではなく，更に長期間にわたって動作させることが可能である。

4　他機関による実証実験との比較

QKDシステムの長期稼働を目指した研究は，様々な機関で進められており，それらの報告結果と今回の実証実験結果との比較を**表1**に示す。これらの実証実験では，BB84とは異なるプロトコルが使用されていたり，実装やセキュリティ証明も異なっていたりする。このため，セキュリティレベルや暗号鍵配送速度を今回の結果と直接比較するのは難しいが，**図4**及び**図5**

表1．近年の連続稼働実証実験の報告結果との比較

Comparison of parameters of recent QKD systems in long-term field trials

機関（実施年）	機関A（2011）	機関B（2012）	機関C（2013）	機関D（2014）	機関E（2014）	東芝（2014）
プロトコル	SARG	CV	BB84	DPS	BB84	**BB84**
接続形態	1対1	1対1	ループバック	ループバック	1対1	**1対1**
光ファイバの損失　（dB）	3.3	5.5	12.5	29	18.4	**14.5**
連続稼働期間　（日）	～300	55	30	25	212	**34**
暗号鍵配送速度（kビット/s）	2.5	0.6	110	1	0.8	**301**
暗号鍵配送量合計（Gビット）	64.8	2.85	295	2	14.1	**878**
損失10 dB換算時の暗号鍵配送速度　（kビット/s）	0.44	0.22	200	79	5.3	**848**

CV　：Continuous Variable
DPS：Differential Phase Shift

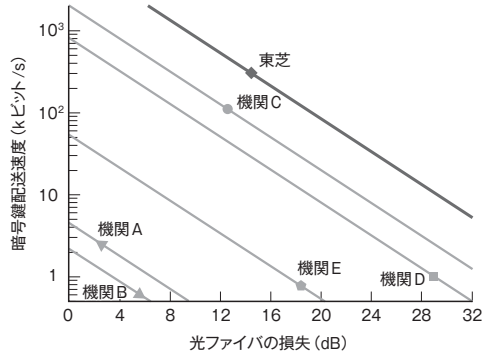


図4．暗号鍵配送速度 ― グラフ上の点は暗号鍵配送速度であり，直線はエラー率に変化がないと仮定したときの光ファイバの損失に対する暗号鍵配送速度の概算値である。光ファイバの損失が大きいと直線からはずれることが想定される。

Secure key rates of recent QKD systems obtained in long-term field trials

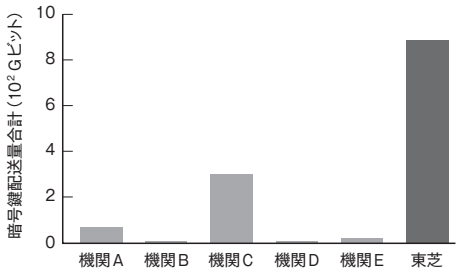


図5．稼働期間内の暗号鍵配送量の合計値 ― 他の実証実験と比較して暗号鍵配送量の合計値は最大となった。

Total volume of continuous secure key data distributed during field trials

に示すように，暗号鍵配送速度と暗号鍵配送量の合計値をそれぞれ比較すると，これまでの最大値を達成したと考えられる。

図4の直線はエラー率に変化がないと仮定したときのファイバ損失に対する暗号鍵配送速度を示している。ファイバ損失が10 dBのとき，暗号鍵配送速度は848 kビット/sとなり，これまでの最大速度であると推定される。

図5からは，稼働期間内の鍵配信量がこれまでの実証実験で最大の878 Gビットであることがわかる。これは1日当たりに換算すると25.8 Gビットであり，例えば1件100 kバイトの電子メールであれば，1日に3万2千件以上を暗号化できる量になる。長期間にわたって安定した高速なQKDを実現することで，大量の暗号鍵を共有することが可能となり，数多くのアプリケーションへ暗号鍵を提供できるようになる。

5　あとがき

FPGAボードをベースに構築した高速なQKDシステムの試作機の概要と，その試作機を用いた実証実験の結果について述べた。試作機は小型かつロバストで標準的な通信環境へ容易に導入することができる。今回，開発した試作機を敷設済みの光ファイバネットワークへ導入し，全長が45 kmの光ファイバ2本を使用した実証環境において連続稼働実験を実施した。34日間の連続稼働を確認し，合計878 Gビットの暗号鍵を301 kビット/sの平均速度で配送した。合計の鍵配送量は，これまで報告された実証実験結果と比べて最大となる。暗号鍵配送速度は安定しており，様々な気象条件下でも停止することなく実験終了まで連続稼働した。

今後も，実用化に向けてQKDシステムの更なる長期安定動作に向けた検証を進めるとともに，暗号鍵配送速度の向上を目指す。

この研究の一部は，国立研究開発法人 情報通信研究機構（NICT）の「セキュアフォトニックネットワーク技術の研究開発」で実施したものである。

文　献

(1) Dixon, A.R. et al. High speed prototype quantum key distribution system and long term field trial. Opt. Express. **23**, 6, 2015, p.7583－7592.
(2) Bennett, C.; Brassard, G. "Quantum cryptography: Public key distribution and coin tossing". Proc. IEEE Int. Conf. Comput. Syst. Signal Process. Bangalore, India, 1984-12, IEEE. 1984, p.175－179.
(3) Scarani, V.; Renner, R. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. Phys. Rev. Lett. **100**, 2008, p.1－4.
(4) Lucamarini, M. et al. Efficient decoy-state quantum key distribution with quantified security. Opt. Express. **21**, 21, 2013, p.24550－24565.
(5) Lo, H-K. et al. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. J. Cryptol. **18**, 2, 2005, p.1－46.
(6) Hwang, W-Y. Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901, 2003.
(7) Lo, H-K. et al. Decoy State Quantum Key Distribution. Phys. Rev. Lett. **94**, 230504, 2005.
(8) Patel, K. et al. Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber. Phys. Rev. X. **2**, 4, 2012.
(9) Yuan, Z. et al. High speed single photon detection in the near infrared. Appl. Phys. Lett. **91**, 041114, 2007.
(10) ジェイムズ ダインズ 他. 高速量子鍵配送プロトタイプによる実証運用. 東芝レビュー. **66**, 11, 2011, p.14－17.

アレキサンダー ディクソン　Alexander R. DIXON, Ph.D.
研究開発統括部 研究開発センター ネットワークシステムラボラトリー，Ph.D.。量子暗号通信の研究・開発に従事。
Network System Lab.

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，Ph.D.。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

佐藤　英昭
研究開発統括部 研究開発センター ネットワークシステムラボラトリー主任研究員。
Network System Lab.