世界最高速の無条件に安全な量子暗号鍵配信技術

High-Bit-Rate Unconditionally Secure Quantum Key Distribution

アンドリュー　シールズ　　ジュリアン　ユアン
■ Andrew J. Shields　　■ Zhiliang Yuan

物理法則に基づき鍵配信の無条件安全性が保証される量子暗号鍵配信（QKD：Quantum Key Distribution）技術は，将来のセキュアネットワークを支えるキー技術の一つとして期待されているが，その実用化には，既存のネットワークへの適用と鍵配信の高速化が重要な課題となっている。

東芝は，欧州連合（EU）が主催した世界で初めてのQKDネットワークの実証試験に参加し，ネットワーク上の任意の送受信者間で，完全な秘匿音声通話や秘匿ビデオ通信を実証した。また，高速駆動する新たな単一光子検知器を開発し，無条件に安全な条件下で世界最高速(注1)の鍵配信1 Mビット/sを実現した。

Quantum key distribution (QKD) technology, in which unconditionally secure key distribution is guaranteed based on a physical law, is expected to be a cryptographic primitive in future secure networks. However, it is essential for the technology to be able to be integrated into real communication infrastructures for widespread use.

Toshiba has participated in a field trial of a small-scale QKD network as part of the Secure Communication Based on Quantum Cryptography (SECOQC) Project funded by the European Union, and has successfully demonstrated both secret telephone communications and video distributions between random nodes on a network. Furthermore, using a newly developed single-photon detection device, we have developed a high-bit-rate QKD system that allows key distribution exceeding 1 Mbps under unconditionally secure conditions.

1　まえがき

QKDは，光ファイバで連結される二つの送受信者（アリスとボブ）の間で安全に暗号鍵を配信するための技術である。既存の暗号技術は，ハッカーが使用可能な計算機性能の制約を安全性の基盤としており，計算量的安全性と言われる。

これに対してQKDでは，一つの光子に1ビットの情報をエンコード（符号化）して送信するため，光子に書き込まれた情報を痕跡を残さずに観測することが不可能である。QKDはこの物理法則にその安全性が立脚しており，無条件に安全な鍵配信手段が実現可能である。ただし，実際にこのような最高レベルのセキュリティを実現するためには，十分慎重にシステムを設計して実装する必要がある。

QKDの更なる利用拡大には，ネットワーク対応と鍵配信の高速化に加えて，安全性を定義し，異なるQKDシステムを連結させるための標準の策定が課題である。

東芝は，計算量的安全性に依存しない究極の暗号通信である量子暗号鍵配信の実用化を目指して，高速QKD技術を開発し，そのネットワークへの適用を実証した。

ここでは，この技術と実証試験の概要について述べる。

（注1）　2009年4月現在，当社調べ。

2　QKDを用いた秘匿通信リンクシステム

QKDによる暗号鍵配信と既存の認証・暗号技術を組み合わせることで，安全なセキュア通信を実現することができる。例えば，QKDはVPN（Virtual Private Network）などで利用されている128－256ビットのAES（Advanced Encryption Standard）暗号鍵を配信することができる。後述するように，QKDの鍵配信速度は通信距離20 kmで1 Mビット/sにまで高まっており，QKDは単に安全に鍵を配信するだけでなく，頻

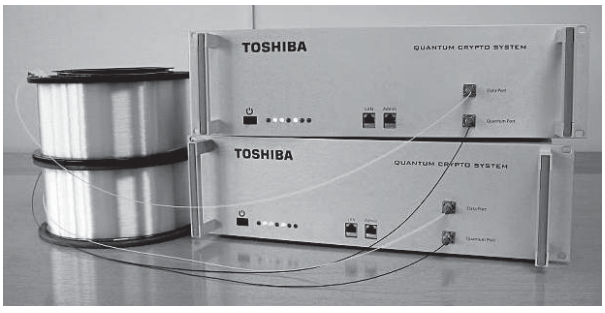


図1. QKDを用いた秘匿リンク通信システム — 送受信器間の暗号鍵配信にQKDを利用することで，安全かつ頻繁な鍵更新を実現している。
Encrypted link combining Advanced Encryption Standard (AES) data encryption and key exchange using QKD

繁な鍵交換を可能とする手段となってきている。更に，QKDとワンタイムパッド暗号(注2)を組み合せることで，計算量的安全性に依存しない無条件に安全な暗号通信を実現できる。

当社が開発したQKDを用いた秘匿通信リンクシステムを**図1**に示す。QKD送受信器が標準的なラックマウント筐体（きょうたい）に実装され，光ファイバで連結されている。秘匿通信リンクはVPNなどに用いられるIPSec(注3)プロトコルを用いた。送受信器間の暗号鍵配信にQKDを利用することで，安全かつ頻繁な鍵更新を実現している。このような秘匿リンクは，オフィス間やオフィスとデータセンター間のような高速秘匿通信リンクなどへの利用が始まっている。

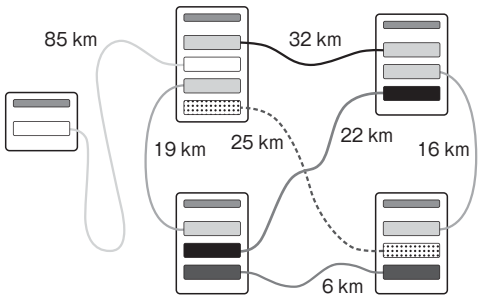
3　QKDネットワーク実証試験

QKDは原理的に1本の光ファイバリンクの両端で暗号鍵を共有する仕組みであり，複数のノードで構成される通信ネットワークへの適用には，複数のリンクを越えて暗号鍵を配信できる仕組みが必要となる。QKDのネットワーク化によって，ユーザーはネットワーク上の任意のエンドポイントに対して安全な秘匿通信を行うことができ，また，QKDの敷設・運用コストをネットワーク上の全ユーザーで負担することができる。更に，QKDにルーティング(注4)機能を持たせることで，特定のリンクが使用できない場合でも，鍵配信や秘匿通信サービスを安定的に継続することができる。

EUのプロジェクトであるSECOQC（Secure Communication based on Quantum Cryptography）は，2008年10月に，オーストリアのウィーンに敷設された商用光ファイバを用いてQKDネットワークの実証試験を行った。当社も，後述するBB84単一方向型QKDで実証試験に参加した。

実証試験では，**図2**に示すウィーンの7本の商用光ファイバで連結された五つのノードの間を，複数種類のQKDリンク装置でメッシュ状に接続した。各ノードに設置されるQKDネットワークシステムは，QKDリンク装置のほか，SECOQCで開発されたルーティング及びリンク管理や鍵管理をつかさどるネットワーク装置で構成される。複数のリンクを挟むノードNとN'間で暗号鍵を配信するときには，まず，各リンクの両端ノード間でQKDによってリンク通信用の暗号鍵を配信し，次に，NとN'間の暗号鍵を，各リンクのQKD暗号鍵でワンタイムパッド暗号を用いて暗号化し配送する。

当社は，無条件に安全性を保証する一方向通信型デコイ(注5)



(a) 五つのノードと7本の商用光ファイバリンク

(b) QKDネットワークでの五つのノード位置

提供：オーストリア リサーチ センター

図2．ウィーンでのQKD実証試験ネットワーク — 2008年10月にEUのプロジェクトであるSECOQCがオーストリアで行った実証試験に東芝もメンバーとして参加した。五つのノードを結ぶ七つの商用光ファイバを用いて，安全なビデオ通信と完全秘匿音声通信を実現した。

QKD network installation in Vienna

QKDシステムを，長さ32 kmの光ファイバに持ち込み実証試験を行った。独自の能動安定制御機構を実装したこのシステムは，商用光ファイバを用いる実環境下でも安定的な鍵配信が可能であることが実証された。

長さの異なる光ファイバの両端に実証試験で利用したQKDシステムを接続し，鍵配信速度とビットエラー率を測定した結果を**図3**に示す。いずれのファイバ長においても，実験した24時間にわたり装置が安定的に鍵を配信できていることがわかる。ファイバ長20 kmと25 kmでの平均的な最終鍵配信速度は，それぞれ10 kビット/sと5.7 kビット/sであった。ファイバ長が長くなると伝送損失が増大するため，ビットエラー率が高くなり最終鍵配信速度が低下する。実証試験条件とほぼ同じ33 kmファイバ長の場合でも，3 kビット/sの最終鍵配信速度が出ることを確認した。

ウィーンでの実証試験では，QKDネットワーク上で二つのアプリケーションのデモンストレーションを行った。まず，ネットワーク上の各ノードと実証試験会場サイト間での秘匿ビデオ通信である。ビデオデータは，QKDネットワークシステムによって配信されたAES鍵によって暗号化される。適切なタイミングで鍵更新を行うことで安全なビデオ通信を実現した。二つ

(注2)　通信データと同じ長さの暗号鍵を1回だけ使う暗号で，解読が不可能であることが情報理論的に保証されている。
(注3)　インターネット上のプロトコル名。
(注4)　ネットワークで，目的のホストまでパケットを送信するとき，最適な経路を選択して送信すること。
(注5)　単一光子信号パルスにデコイ（おとり）の光パルスを混ぜて，両者の受信状態を比較することで盗聴者の介入を検知する方法。

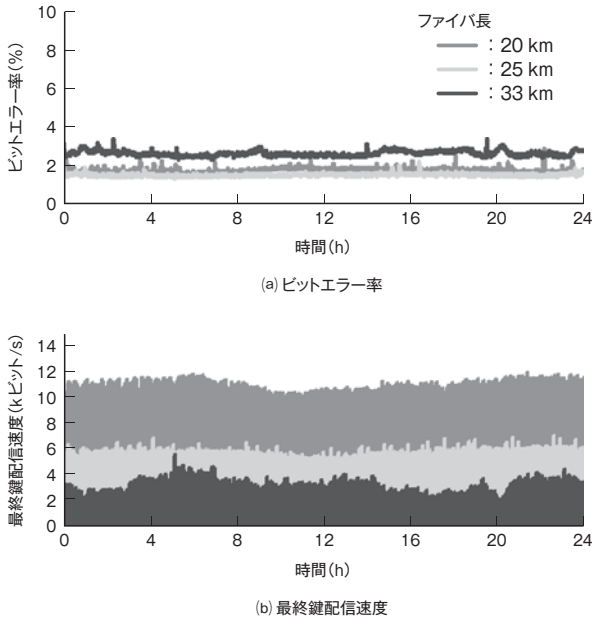


図3. ウィーンQKD実証試験で用いた東芝QKDシステムの特性 ― 光ファイバが長くなるとビットエラー率が高くなるが，33 kmファイバの場合でも，24時間にわたる安定動作と平均3 kビット/sの最終鍵配信速度を確認した。

Secure bit rate and quantum bit error rate (QBER) for fiber lengths of 20, 25, and 33 km

めのアプリケーションは，ワンタイムパッドを用いた完全秘匿音声通信である。ワンタイムパッドは，解読不可能であることが数学的に証明された暗号方式であり，平文と同じ長さの暗号鍵を一度だけ用いて暗号化を行う。QKDと組み合わせることで，無条件に安全なデータ通信を実現することができる。

欧州電気通信標準化機構（ETSI：European Telecommunications Standards Institute）は，この実証試験の成功を受け，QKD標準化グループの設立を決めた。当社も創設メンバーとして参加する。このグループは今後2年間で最初の標準仕様を策定する計画であり，この標準化活動によってQKDのアプリケーションが広がり，QKDのシステムや主要コンポーネントの開発が加速すると期待している。

4　鍵配信の高速化

QKDの応用拡大のために，その鍵配信の高速化が前述のネットワーク対応と並ぶ重要な課題である。現在のQKDは，通信距離20 kmで数百～10 kビット/sの鍵配信ができる。この速度は，一つの通信チャネルの秘匿にはある程度十分であるが，ネットワーク上の複数の通信チャネルへ暗号鍵を配布する場合には十分とは言えない。また，前述のとおり，通信データと同じ長さの暗号鍵を一度かぎり利用するワンタイムパッドとQKDの組合せによって，計算量的安全性に立脚しない安全なデータ通信を実現できる。鍵配信速度の向上によって，無条件に安全というQKDの長所を鍵配信だけでなくデータ通信でも享受できる。

以下に，現在のQKDの鍵配信の制約となっている単一光子検知器の高速化と，新たな高速単一光子検知器を適用した高速QKDの開発について述べる。

4.1　高速単一光子検知器

QKDの鍵配信速度の制約となるのは，光ファイバ中の伝送損失とQKDシステムの単一光子検知器の動作周波数，光子検知効率，ダークカウント(注6)などの性能である。InGaAs/InP（インジウム ガリウム ヒ素／インジウム リン）のAPD（Avalanche Photo Diode）は安価で，比較的高い性能が得られるため，多くのQKDシステムで利用されている。しかし，既存のInGaAs/InP APDは，デバイス内に残留するアバランシェキャリアが原因で，単一光子検知器として動作する周波数に制約があり，10 MHz以上での駆動が極めて難しい。

このような制約を持つAPDに代わる単一光子検知器の開発が試みられている。開発されている単一光子検知器を**表1**に示す。超伝導ナノワイヤ光子検知器や非線形上方置換は光子検知効率が低く，また，液体ヘリウムでの冷却が必要であり，実用的なQKDシステムへの適用には課題が残されている。

表1. 光通信波長帯の単一光子検知技術の比較

Comparison of detectors of telecom-wavelength single photons

単一光子検知器の種類	最大光子検知数（MHz）	検知効率（%）	ダークカウント	ジッタータイミング（ps）	動作温度（K）	コスト
InGaAs APD	0.1	10～30	10^{-5}	500	250	低
自己差分型APD（提案方式）	497	10～30	2×10^{-6}	50	250	低
非線形上方置換法	15	1	10^{-5}	50～200	250	中
超伝導ナノワイヤ	20	0.9	10^{-7}	68	2.9	高

当社は既存のAPDを用いて，駆動周波数が1 GHz以上，従来比100倍の単一光子検知器の開発に成功した(1)。このブレークスルー（突破）によって，QKDシステムの鍵配信速度を1 Mビット/s以上へ高めることができる。今回開発した単一光子検知器は，表1に示すように高い光子検知性能を示すだけでなく，高信頼で安価，かつ液体ヘリウム冷却が不要という長所を備える実用的な検知器である。

開発した高速単一光子検知器の仕組みを説明するために，まず，一般のAPDが抱える問題を述べる。光子がAPDに吸収されると，デバイス内でキャリア電子が励起され，印加され

(注6)　光子が存在しないときに雑音によって光子をカウントしてしまうこと。

た高電場によって加速し，原子と衝突して2次キャリアを生成する。この2次キャリアが原子との衝突とキャリア発生を雪崩現象のように次々と繰り返し，最後には約10^7個のアバランシェキャリアが生成され，検知可能なアバランシェパルスとなって現れる。アバランシェキャリアは，時にAPD内の結晶欠陥に閉じ込められ，次の光子検知サイクルで開放されて，疑似アバランシェキャリアを発生させる。このアフターパルスと呼ばれる疑似光子検知信号がQKDシステムの誤差となる。

通常，APDを単一光子検知に用いる場合，ゲート電圧の周期的印加によって現れるキャパシティブノイズよりもアバランシェパルスを大きくとる必要がある。デバイス内のアバランシェキャリア密度が高くなると，キャリアが結晶欠陥にトラップされる確率が高まり，高駆動周波数条件では，トラップされたキャリアが次の光子検知サイクルでアフターパルスを引き起こす。アフターパルスの発生を抑制するためには，次の光子検知サイクルのゲート電圧印加の前に，トラップされたキャリアが十分に解放されるように駆動周波数を10 MHz以下に落とす必要があった。

当社は，APDの駆動周波数を高めるために，アフターパルスをほとんど起こさない条件でアバランシェパルスを検知できる，自己差分方式と呼ばれる新たな手法を開発した。この手法の回路を**図4**に示す。この回路は，APD出力を分離するスプリッタ，動作周波数1サイクル分に相当する遅延ループ，及び差分器で構成され，連続する検知サイクルの出力信号を比較することで，周期的なキャパシティブノイズの影響を除去し，単一光子検知に対応するアバランシェパルスだけを出力する。従来は，キャパシティブノイズよりもアバランシェパルスのピークを大きくするためにゲート電圧を高める必要があったが，自己差分回路を連結することで微弱なアバランシェパルスを検知することが可能となり，アフターパルスを誘起するゲート電圧を下げることができるようになった。

表1に示すように，今回開発した自己差分型APDは高い検知効率を備え，同時に，低ジッタ及び低ダークカウントレートで非常に高い最大光子検知レートを示す。したがって，自己差分型APDはQKD利用にもっとも適した単一光子検知器と言える。

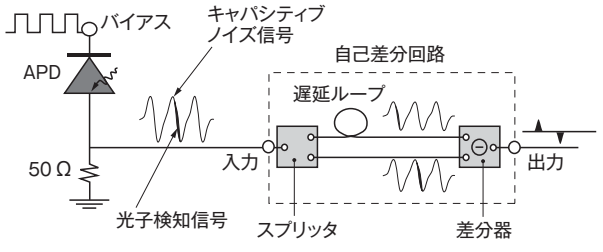
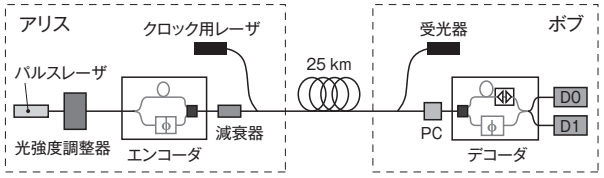


図4. 自己差分型APD — 従来は，容量性ノイズよりもアバランシェパルスのピークを大きくするためにゲート電圧を高める必要があったが，自己差分回路を連結することで微弱なアバランシェパルスを検知することが可能となり，アフターパルスを誘起するゲート電圧を下げることができるようになった。

Self-difference-mode operation of InGaAs avalanche photodiode (APD)

4.2 ギガヘルツ駆動量子暗号鍵配信システム

前述の自己差分方式APDを当社が開発したQKDシステムへ組み込み，有効性を検証した[(2), (3)]。QKDシステムを**図5**に示す。このシステムは，送信器（アリス）側の波長1.55 μmのパルスレーザ，光強度調整器，エンコーダ，減衰器，送受信器を同調させるクロック用レーザ，及び受信器（ボブ）側のデコーダと上記の自己差分型APDを用いた単一光子検知器などで構成される。単一光子信号へのキュービット情報の書込みと読出しを行うエンコーダとデコーダには，マッハーツェンダー干渉計を利用する。光子数分岐攻撃に対する安全性を確保するために，異なる強度の光子信号を用いるデコイ法を採用しており，光強度調整器でパルスレーザの出力光から異なる強度の信号を生成し，最後に，減衰器で平均光子存在数が1以下の微弱な疑似単一光子信号とデコイ信号を生成する。受信器のAPDで検知された単一光子にはタイムスタンプが付与され，1セッションの送受信後に送信結果と照合して最終鍵を生成する。



PC：Phase Controller（位相調整器）
D0：Detector 0（単一光子検知器0）
D1：Detector 1（単一光子検知器1）

図5. 量子暗号鍵配信システム — 光子数分岐攻撃に対する安全性を確保するために，パルスレーザの出力光から光強度調整器で異なる強度の信号を生成し，最後に，減衰器で平均光子存在数が1以下の微弱な疑似単一光子信号とデコイ信号を生成する。

Configuration of high-bit-rate QKD system developed by Toshiba Research Europe Ltd. (TREL)

量子暗号鍵配信の実験は20 kmの光ファイバを用いて行った。信号発生周波数は1.036 GHz，単一光子信号の平均光子存在数は0.55，デコイ信号の平均光子存在数は0.1×10^{-4}と7.6×10^{-4}である。実験を通じてのビットエラー率は2.53 %，1セッション当たりに得られるシフトキーは約8×10^6個であった。エラー訂正と秘密増強後の最終鍵配信速度は1.02 Mビット/sであった。この最終鍵配信速度は，当社がウィーンの実証試験で用いたQKDに比べて100倍以上早く，無条件安全性の条件下で，世界で初めて(注7) 1 Mビット/s以上の鍵配信速度を達成した。

（注7） 2008年10月時点，当社調べ。

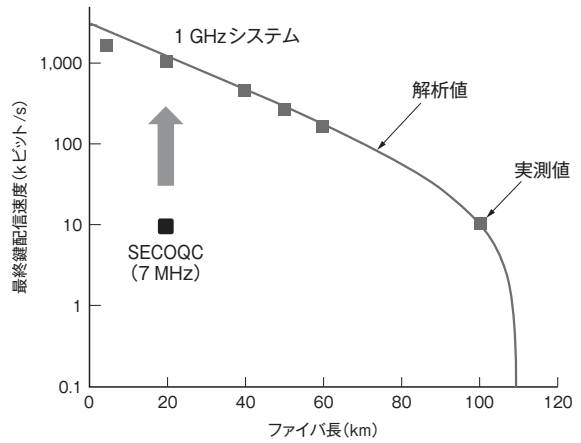


図6. 最終鍵配信速度とファイバ長の関係 ― ウィーンの実証試験（SECOQC）に用いたQKDシステムと比較して，最終鍵配信速度を100倍以上高速化できた。

Dependence of secure bit rate on fiber length for 1 GHz QKD system

ファイバ長と最終鍵配信速度の関係を**図6**に示す。測定に用いた実験パラメータはすべてのファイバ長で同じである。図中の実線はファイバの光損失を0.2 dB/kmとしたときの解析値であり，ファイバ長が5.6 kmの結果を除けば，両者は良い一致を示す。ファイバ長が5.6 kmでの最終鍵配信速度は1.65 Mビット/sと解析値よりも低くなっているが，これは自己差分APDの最大光子カウント数性能の影響によると推定される。ファイバ長が60 kmを超えると，鍵配信速度に対する光子検知器のダークカウント率の影響が大きくなり，図6に示すように，今回の実験条件では110 km以上の鍵配信は不可能であった。ファイバ長100.8 kmでのビットエラー率は4.6 %と鍵生成が可能な範囲にある。この条件でのシフト鍵配信速度は257 kビット/s，最終鍵配信速度は10.1 kビット/sであった。2.5世代携帯電話程度の音声品質であれば，ワンタイムパッド暗号を用いて100 kmの完全秘匿音声通話が実現できることになる。

5　あとがき

計算量的安全性に依存しない究極の暗号通信である量子暗号鍵配信の実用化を目指し，そのネットワーク実証と高速QKDの開発を行った。EUのプロジェクトであるSECOQCがウィーンで行った実証試験では，複数のQKDシステムを用いてネットワーク上の任意のノード間で安全に暗号鍵を共有するプロトコルを実装し，完全な秘匿音声通話や秘匿ビデオ通信のデモンストレーションに成功した。

また，従来，QKDの駆動周波数の制約となっていた単一光子検知器を高速駆動させる自己差分型APDを開発し，駆動周波数を従来比で100倍以上高速化して1 GHzとした。この自己差分型APDをデコイQKDシステムへ実装し，通信距離20 kmでの最終鍵配信速度1.02 Mビット/sを達成した。この鍵配信速度は，無条件に安全な条件下で世界最高速である。

当社は，将来の社会に様々な利益を提供できる，量子力学に基づく安全な暗号通信技術と，安価で高効率な単一光子検知器の開発に今後も取り組んでいく。

文　献

(1) Yuan, Z. L., et al. High speed single photon detection in the near infrared. J. Appl. Phys. Lett. **91**, 041114, 2007, p.041114-1－041114-1.
(2) Yuan, Z. L., et al. Gigahertz quantum key distribution with InGaAs avalanche photodiodes. J. Appl. Phys. Lett. **92**, 201104, 2007, p.201104-1－201104-2.
(3) Dixon, A. R., et al. Gigahertz decoy quantum key distribution with 1Mbit/s secure key rate. J. Opt. Express. **16**, 18790, 2008, p.18790－18797.

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 リーダ，理博。量子情報半導体デバイス，量子暗号通信の研究・開発に従事。
Toshiba Research Europe Ltd., Cambridge Research Lab.

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，量子暗号通信の研究・開発に従事。
Toshiba Research Europe Ltd., Cambridge Research Lab.

和　訳

佐田　　豊
技術企画室 企画担当グループ長
Technology Planning Div.