光集積チップを使った安全な量子暗号通信システム

Secure Quantum Communication System Using Photonic Integrated Chips

タオフィク パライソ Taofiq K. PARAISO　　アンドリュー シールズ Andrew J. SHIELDS

量子鍵配送（QKD）では，量子力学の法則によって最高レベルの通信の秘匿性が保障される。QKDを広く使用できるようにするには，コストや，大量生産，標準的な通信インフラとの互換性などの課題を効率的に解決する必要がある。近年，これらの課題解決に向けて光集積チップを使ったソリューションの開発が世界的に行われているが，主要な機能を全てチップ化したチップベースQKDシステムの実証には至っていなかった。

東芝欧州社 ケンブリッジ研究所は，QKDの主要な機能を実装した３種類の光集積チップを開発し，これらを適用した世界初（注1）のチップベースQKDシステムを実証した。実験の結果，実用的な動作条件で数日間にわたって安定に動作することを確認した。

Quantum key distribution (QKD) exploits the laws of quantum mechanics to offer the highest possible level of communication secrecy. In order to make QKD widely accessible, it is necessary to provide effective solutions to various issues including cost, volume production, and compatibility with standard telecom and datacom infrastructures. Over the past few years, efforts have been made worldwide to provide such solutions using photonic integrated chips. However, the demonstration of a complete chip-based QKD system has remained a considerable challenge.

The Cambridge Research Laboratory of Toshiba Research Europe Limited has achieved a substantial breakthrough by demonstrating the world's first standalone chip-based QKD system, which is the highest level of system integration of three types of photonic integrated chips. We have confirmed that this system is capable of autonomous operation under practical operating conditions with high stability over several days.

1. まえがき

20年前の2002年に，先駆的な量子鍵配送（Quantum Key Distribution：QKD）の実証で，広範囲にわたる通信の安全を確保できる可能性が示された。それ以来，通信ノード数は増加し，距離は主要都市内，都市間，更には国家間と延長され，現在では衛星通信による大陸間QKDの研究開発も行われている[1]。

QKDを用いて広く通信の安全を確保するには，実用的かつ持続可能な手法が必要である。QKDは既に商用化されている成熟した技術だが，克服すべき課題として，通信距離及び帯域幅の拡大，生産・運用コストの低減，そして既存光通信インフラとの互換性の確保という三つがある[2]。

東芝欧州社は，この分野における先駆者として，これらの課題に対して，(1)独自のTwin Field QKDプロトコルによる通信距離限界の拡大[3]，(2)通信ネットワークへのQKDの展開促進[4]，(3)光集積チップを用いた生産性やスケーラビリティーの拡大といった取り組みを行っている。特に，(3)に関する成果として，当社は，QKDの主要な機能を実装した３種類の光集積チップを開発し，これらを適用した世界初のチップベースQKDシステムを実証した[5]。

ここでは，QKDの主要機能を実行する光集積チップ，及びそれらを実装した独立動作するチップベースQKDシステムの実証について述べる。

2. QKD向け光集積チップ

2016年から2019年にかけて，量子乱数生成器（QRNG：Quantum Random Number Generator），QKD送信器（QTx），及びQKD受信器（QRx）の機能をそれぞれ実装した，３種類の光集積チップを開発した。これらのチップは，高いパフォーマンスのQKDを実現するために，一般に用いられているBB84プロトコルを変形した独自のT12プロトコル[6]を用い，GHzオーダーの周波数で高速に連携動作するよう設計されている。T12プロトコルでは，高いセキュリティーレベルを確保するため，複数の光量（デコイ強度）の非常に弱いレーザーパルスを使用し，二つの時間の区間に分割されたレーザーパルスの位相差に情報が符号化される。これらのチップは，それぞれの仕様に応じて，異なるフォトニックプラットフォーム上に実装されている。

（注1） 2020年12月時点，当社調べ。

2.1　QRNGチップ

QRNGは，QKDで最も重要なセキュリティー構成要素の一つである量子乱数を，元来予測できない不規則性を持つ量子のゆらぎから抽出する。QKDのセキュリティーは光子がどのように符号化されたか直接予測することが不可能であることに依存しているため，量子乱数は重要なセキュリティー構成要素である。従来用いられている疑似乱数生成器は，広範囲のアプリケーションに使用されているが，アルゴリズムに基づいて乱数が生成されるため，初期状態を知られてしまうと完全な予測が可能で，高度な暗号化には適さない。

量子乱数の生成は，レーザーの発光開始時の自然放出位相ノイズを利用することで実現できる。発光開始時のレーザーパルスの位相は，真空のゆらぎに起因する自然放出位相ノイズによって決まることから，量子ランダム性の発生源となる。そこで，ゲイン切り替えに伴うレーザーダイオードの自然放出位相ノイズを利用するQRNGチップを開発した[7]。**図1**に，開発したQRNGチップとその回路を示す。このチップは，レーザーのようなアクティブコンポーネントと高速光検出器を同じ導波路チップ上に導入できる，インジウムリン（InP：Indium Phosphide）プラットフォームを用いている。二つの分布帰還型（DFB：Distributed Feedback）レーザーダイオード（LD1及びLD2）から発生したパルスが，可変光減衰器（VOA）の役割を果たす調整可能な熱光学マッハツェンダー干渉計（MZI：Mach-Zehnder Interferometer）を通して，マルチモード干渉計（MMI）で干渉する構造となっている。干渉強度は完全にランダムであるため，量子乱数の抽出に用いることができる。当社は2019年に，リアルタイムに4Gビット/sで乱数を生成するQRNGチップを実証した[7]。

2.2　QTxチップ

QTxチップは，直接変調及び光注入同期（OIL：Optical Injection Locking）を介して光子を符号化する，直接位相変調光源である[8]。直接位相変調光源スキームは，2016年に当社が開発したものであり[9]，その長所は，高い繰り返し速度（2 GHz）で，忠実度の高い，短い継続時間の位相エンコードパルスを生成する点である。また，電気光学位相変調器が不要で小型であるため，チップ化する際に電力効率が高い。QTxチップもInPプラットフォームを使用し，二つのDFBレーザーダイオード，MZI，電界吸収型変調器（EAM：Electro-Absorption Modulator）を含む。当社は，2019年の実証実験で，EAMを使わないチップで効率的に光パルスを符号化し，当時のチップベースQKDにおける鍵配送速度の最高記録を達成した[10]。**図2**に示す新しいバージョンのチップは，EAMを使ってパルス強度を変調することで，デコイ強度を生成することができる。

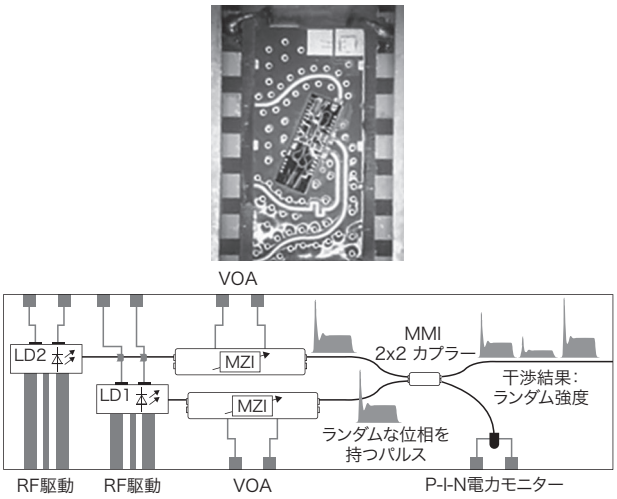


図1．開発したQRNGチップ

完全にランダムな干渉強度を用いて量子乱数を抽出し，リアルタイムに4Gビット/sで乱数を生成できる。

Newly developed quantum random number generator (QRNG) chip

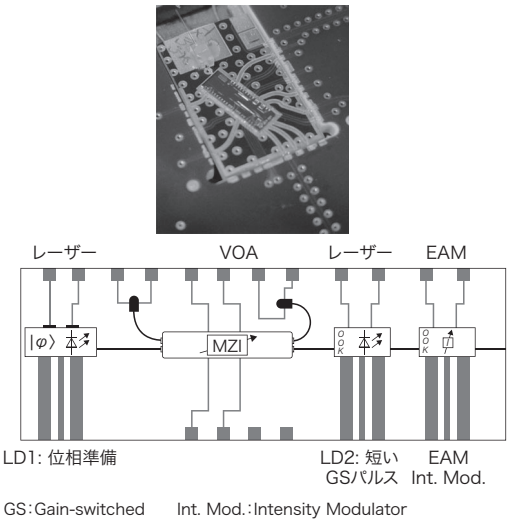


図2．開発したQTxチップ

2 GHzの高い繰り返し速度で，忠実度の高い，短い継続時間の位相エンコードパルスを生成できる。

Newly developed QKD transmitter chip

2.3　QRxチップ

受信器における損失は，通信距離の拡大に悪影響を及ぼすため，損失の低減は受信器の主要な技術課題である。光学的にアクティブな素材はパッシブな素材よりも1～2桁高い損失を生じることから，QRxチップは，導波路の伝搬損失を最小化するために，パッシブなシリコンベースのプラット

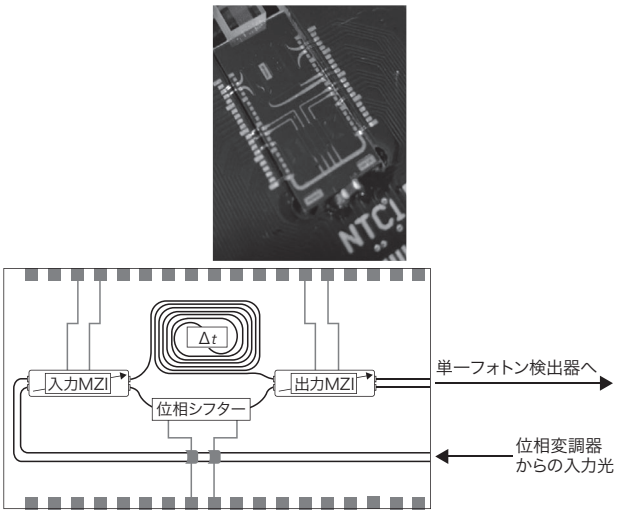


図3. 開発したQRxチップ

導波路の伝搬損失を最小化するため，光学的にパッシブなシリコンベースのプラットフォーム上に実装されている。

Newly developed QKD receiver chip

フォーム上に実装されている。開発した光集積回路（**図3**）は，送信器から送出される連続パルス間の位相差を測定する非対称MZIで構成される。非対称MZIは，その時間差の遅延に対応する長短2本の経路を持ち，経路の出力電力バランスを調整する入力MZI，50:50ビームスプリッターとして機能する出力MZI，短経路上の基準位相調整用の位相シフターにより，この遅延を調整する。非対称MZIから出力された光子は，二つの外部アバランシェフォトダイオード（APD：Avalanche Photodiode）を介して検出される。また，QRxチップは完全にパッシブなため，測定基底選択のための高速変調は，外部の位相変調器を使って行う。

3. チップベースQKDシステム

独立なチップベースQKDシステムとして動作させるには，三つのチップが協調して動作できるように，適切な光学–電気インターフェースを設計，開発する必要がある。システム統合と呼ばれるこの段階では，パッケージング，駆動電子回路，フィードバック制御，及びリアルタイム動作の実現といった課題に対処する必要がある。

3.1 光集積回路のパッケージング

光集積回路のパッケージングは，チップの内部と外部の間の，電子的，及び光学的インターフェースを提供するために不可欠である。また，パッケージングにより，光集積回路に機械的な保護を提供し，これによってチップの温度が制御される。当社は，QTxチップとQRxチップについて，高帯域光通信で広く使われているCFP（C Form-Factor Pluggable）2フォームファクターに準拠した着脱可能モジュールを設計した。ホスト電子機器にモジュールを差し込むだけでモジュールの使用準備が整うため，システムメンテナンスが簡素化されるだけでなく，モジュールの世代間で互換性が維持され，同じホスト電子機器で利用することが可能となる。温度制御については，0.005 ℃以上変動しない良好な温度安定性を確認した。

QRNGチップについては，必要な入出力が，レーザー用

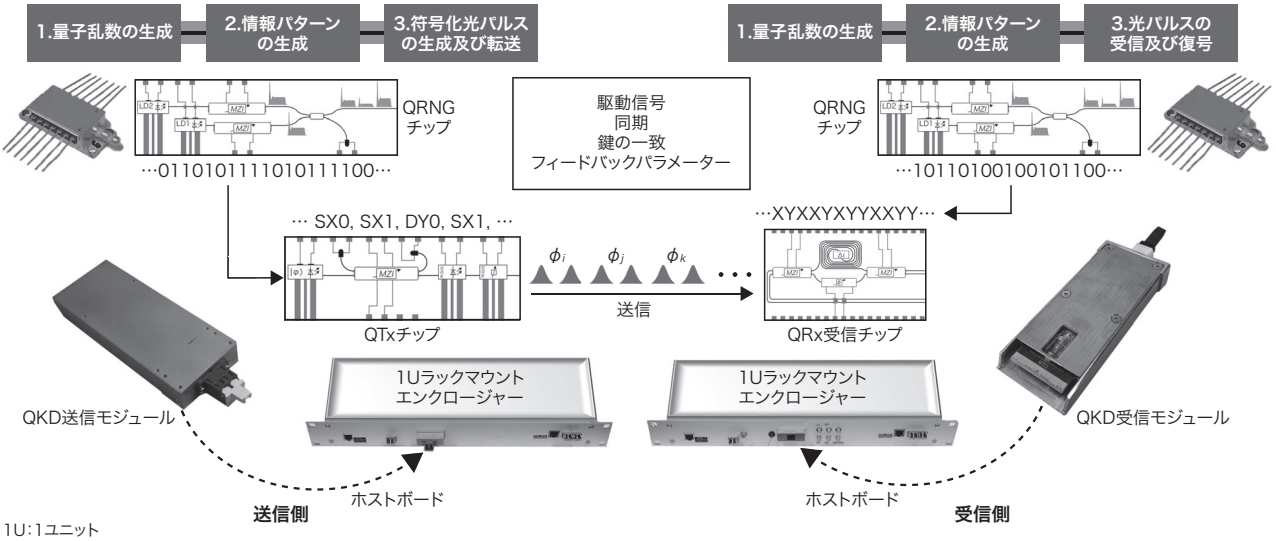
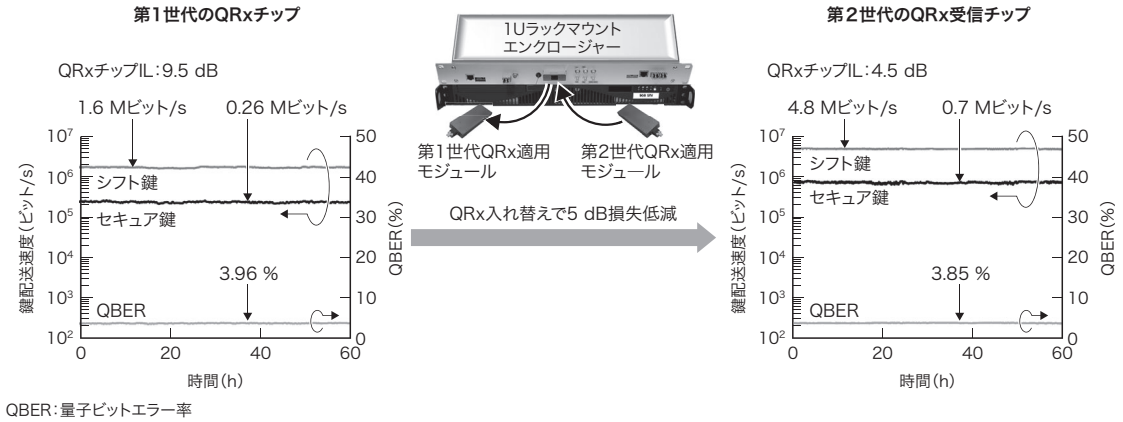


図4. 試作したチップベースQKDシステムの概要

小型の電子回路と着脱可能なQKD送信・受信モジュールを用いてリアルタイム動作する。

Overview of prototype chip-based QKD system



QBER：量子ビットエラー率

図5. 着脱可能モジュールの利点

より性能の高いチップを搭載したモジュールに入れ替えることで，システムの性能が改善する。

Advantages of pluggable module

の2本のバイナリー信号，幾つかの直流（DC）信号，及び光ファイバー1本の信号だけのため，標準の14ピンバタフライパッケージを選択した。

3.2 リアルタイム独立動作のための電子回路

図4は，チップベースQKDシステム，及びその中で使用されている光集積チップの概略を示している。各チップは，ホストボードに実装されている。QRNGボード上には，高速フォトダイオード，ADC（アナログデジタル変換器），及びFPGA（Field Programmable Gate Array）が実装され，駆動電子回路と演算電子回路の両方の処理が機能する。QKD送信モジュールとQKD受信モジュールがそれぞれのホストボードにプラグインされると，電子機器が駆動し，チップに入力されるRF（Radio Frequency）信号とDC信号が生成される。RF信号は中央のFPGAコアからのデジタル入力に基づいてリアルタイムに生成され，QRNGボードからの乱数列をフォトニック量子ビットの準備又は測定を行うためのパターンに変換する。継続動作させるためのフィードバックシステムも設計し，これを用いて，人手を加えることなしに数日間にわたって安定して動作することを確認した。

3.3 実用性の確認

図5は，着脱可能なQKD送信・受信モジュールの利点を示す。第1世代のQRxチップは，挿入損失（IL）が9.5 dBと高く，鍵配送速度が低下している。第2世代のQRxチップでは，ILが4.5 dB（30 kmのファイバーと同等）で，モジュールを入れ替えることで，セキュア鍵の配送速度が0.26 Mビット/sから0.7 Mビット/sに改善した。このようにチップ性能が改善した場合に，システム全体ではなく，モジュールだけを入れ替えることで全体の性能を向上させることができる。

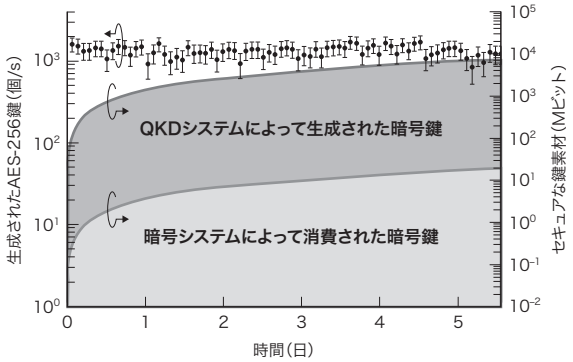


図6. チップベースQKDシステムを用いたデータ暗号化

5日以上にわたって安定に高い性能で自律動作した。

Data encryption using prototype chip-based QKD system

開発したチップベースQKDシステムを暗号通信に適用する際の実用性を確認するため，工業用グレードのデータ暗号化システムに暗号鍵を配送する実証実験を行った。用いた暗号化システムは，最大速度100 Gビット/sで送信されるデータの暗号化及び復号にAES（Advanced Encryption Standard）-256を使用している。暗号化システムは，標準化された鍵管理ソフトウェアを介して，毎分352ビットのQKD鍵を消費した（AES鍵に毎分256ビット，初期化ベクトルに毎分96ビット）。

図6は，5日以上にわたって，10 kmの光ファイバーリンクで毎秒1,300個のAES-256鍵が安定に生成されたことを示している。また，暗号鍵の総生成量と総消費量を比較して，開発したチップベースQKDシステムは，複数のAES暗号化システムに同時に暗号鍵を供給できる性能を備えていることを確認した。

4. あとがき

この論文では，実用的な量子暗号通信システムに量子光集積チップを利用できることを示した。QKDシステムの低コスト化と小型化によって，システムの製造性と信頼性の向上に貢献できる。また，QTxチップ，QRxチップのモジュール化によって，システムを容易にアップグレードできることも示した。これは，QKDシステムのオペレーションコストの削減につながる。

ここで述べた成果の一部は，英国政府のIndustrial Strategy Challenge Fundを通じてInnovateUK共同研究開発プロジェクトAQuaSeCの支援によるものである。

文　献

(1) Cao, Y. et al. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. IEEE Communications Surveys & Tutorials. 2022, **24**, 2, p.839–894.

(2) Diamanti, E. et al. Practical challenges in quantum key distribution. npj Quantum Information. 2016, **2**, Article number: 16025.

(3) Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilization. Nature Photonics. 2021, **15**, p.530–535.

(4) Dynes, J. F. et al. Cambridge quantum network. npj Quantum Information. 2019, **5**, Article number: 101.

(5) Paraïso, T.K. et al. A photonic integrated quantum secure communication system. Nature Photonics. 2021, **15**, p.850–856.

(6) Lucamarini, M. et al. Efficient decoy-state quantum key distribution with quantified security. Optics express. 2013, **21**, 21, p.24550–24565.

(7) Roger, T. et al. Real-time interferometric quantum random number generation on chip. J. Opt. Soc. Am. B. 2019, **36**, p.B137–B142.

(8) Paraïso, T.K. et al. "Advanced Laser Technology for Quantum Communications (Tutorial Review)". ADVANCED QUANTUM TECHNOLOGIES. 2021, **4**, 2100062, p.1–4. <https://onlinelibrary.wiley.com/doi/full/10.1002/qute.202100062>, (accessed 2022-08-05).

(9) Yuan, L. et al. Directly Phase-Modulated Light Source. Phys. Rev. X. 2016, **6**, p.031044-1- 031044-8.

(10) Paraïso, T. K. et al. A modulator-free quantum key distribution transmitter chip. npj Quantum Information. 2019, **5**, Article number: 42.

タオフィク パライソ　Taofiq K. PARAISO, Ph.D.
東芝欧州社 ケンブリッジ研究所
博士（理学）
SPIE, The Optical Society 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.