TOSHIBA

資料2

2019.5.16

イノベーション政策強化推進のための有識者会議「量子技術イノベーション」

産業界から見た量子暗号通信の現状と政府に対する期待

（株）東芝　執行役専務　斉藤史郎

背景

量子コンピュータでも破られないセキュリティ技術の実現

- 「量子コンピュータ」時代の到来
  - 世界各国にて研究開発加速・投資増加、 2030年頃には実用的な規模の量子コンピュータが登場するとの予測
- 既存暗号通信技術の危殆化
  - RSA等の既存暗号通信技術は、量子コンピュータを使うと短時間で破られる可能性
  - 一旦暗号化されたデータを傍受し保存しておき、時間をかけて解読する攻撃も存在するため、現在の通信データの「長期安全性」も保証されない

- 量子コンピュータ時代のセキュリティ技術

耐量子公開鍵暗号
- 量子コンピュータでも計算困難な数学的問題に基づく
- 安価で導入が容易だが、「情報理論的安全性」は無い
- 米NISTが標準仕様選定中

量子暗号通信
- 量子力学の原理に基づく暗号通信技術
- 無条件安全性が証明済み
- 「光子」の送受信機を含む専用HWが必要

量子暗号の動向（海外）

実用化に向けた動きが加速、急速に市場拡大の可能性

中国：地上・宇宙両面で存在感大

- 世界最大規模の量子暗号ネットワークを構築、国営企業が利用
  - 北京－上海間の政府向けバックボーン、上海－杭州間の商用バックボーン
- 2016年量子通信衛星を打ち上げ、2017年世界初の衛星地上間での量子鍵配送実験に成功(距離1200km、鍵配信速度1kbps)

米国：スタートアップ中心に量子暗号を活用した事業を展開

- 2018年Quantum Xchangeが同国初の量子暗号サービスを発表
  - Boston-Washington DC間で主にWall Streetの金融向け市場が狙い
  - New York-New Jersey間のダークファイバーを初期サービスに活用→**東芝も現地でPoC実証を実施**

https://quantumxc.com/testing-toshibas-quantum-key-distribution-system/

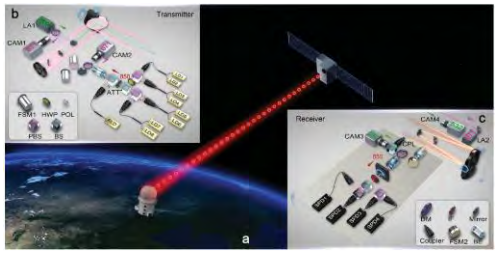
欧州：大手通信キャリアによる実用化に向けた動きが加速

- 英BTが同国初の量子暗号通信網をCambridge-Ipswich間に構築、東芝、IDQ、ADVA等が参画
- テレフォニカ、ファーウェイ、マドリード工科大学が既存商用光通信網での運用実証試験を開始
- ドイツテレコムの実証通信網にSK Telecom/IDQがシステムを提供、2019年商用網への拡大を目指すとの報道

韓国：実用化を視野に国主導で通信キャリアが実証試験

- SK Telecomが、2018年にスイスのID Quantique(IDQ)へ65百万ドルを投資し自社R&D部門と統合、量子暗号システムの研究開発を推進

北京－上海間のバックボーン*1



中国の衛星と地上局間の量子暗号*2

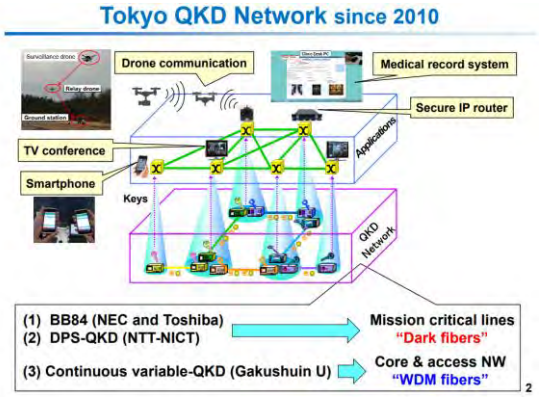
米Quantum Xchangeのサービス網*3

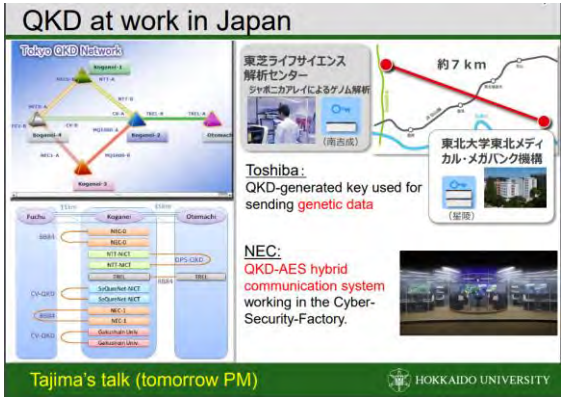
*1 https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S01_WORLD_TOUR/IDQQTEC_HUANG.pdf
*2 https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S01_WORLD_TOUR/USTC_PENG.pdf
*3 https://quantumxc.com/

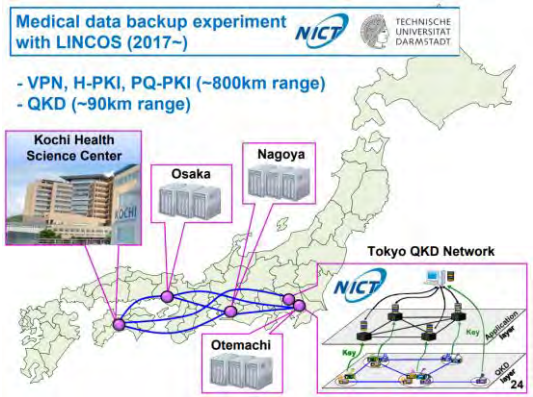
量子暗号の動向（日本）

実用化に向け高性能装置を開発、実証試験を継続

- NICT主導でテストベッドを構築(東京QKDネットワーク)
- ImPACT 量子セキュアネットワークプロジェクトにて、都市圏QKDネットワークを実証
- 2018年度から、内閣府の戦略的イノベーション創造プログラム(SIP)「光・量子を活用したSociety5.0 実現化技術」にて、量子暗号と秘密分散を統合した社会実装に取り組む
- 国プロ成果も活用し、東芝は量子暗号システムを2020年度に出荷予定

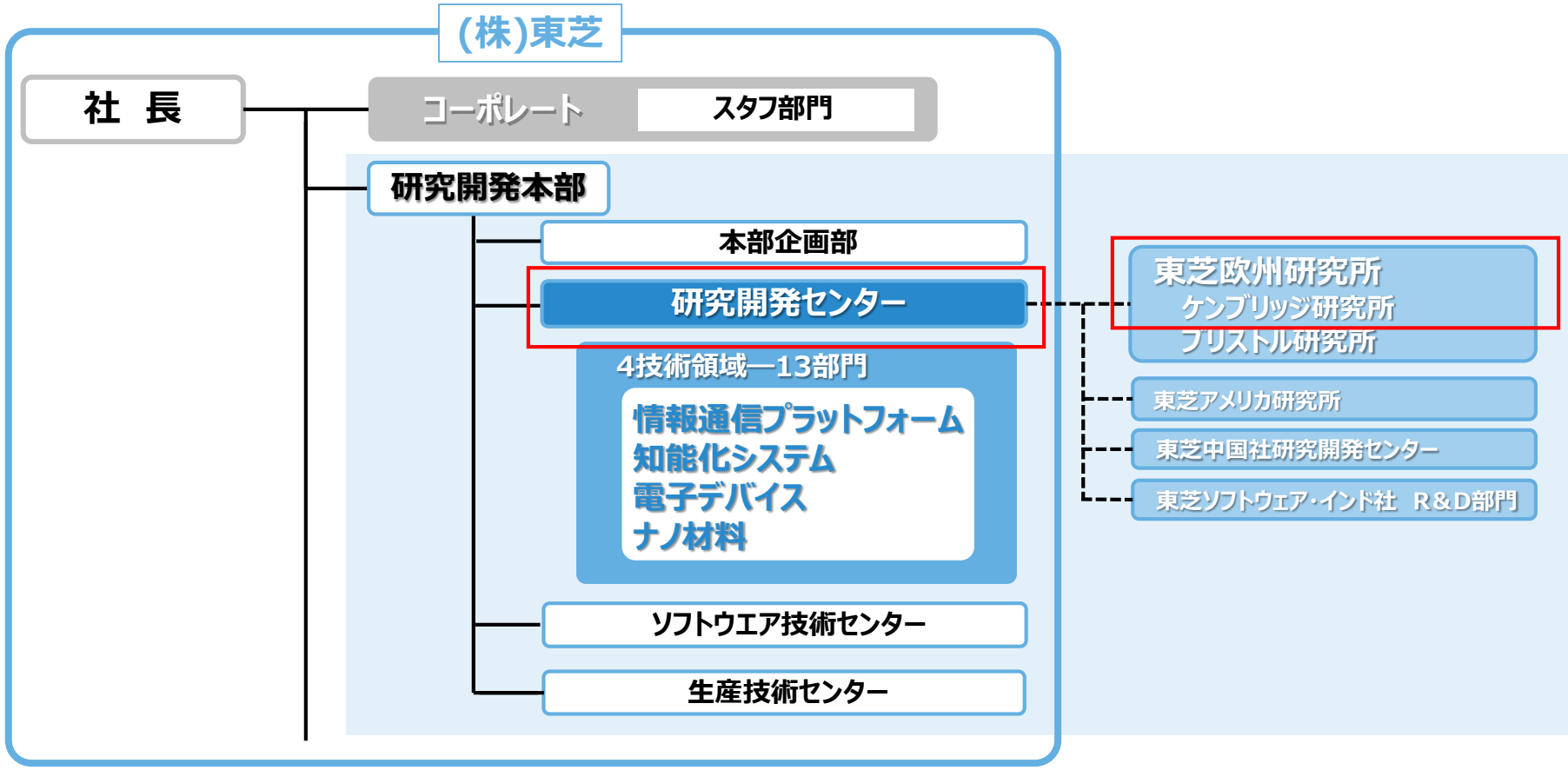






https://docbox.etsi.org/Workshop/2016/201609_QUANTUMSAFECRYPTO/TECHNICAL_TRACK/HokkaidoU_Tomita.pdf
https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S01_WORLD_TOUR/NICT_SASAKI.pdf

東芝の研究開発体制



東芝エネルギーシステムズ（株）	エネルギー事業領域
東芝インフラシステムズ(株)	社会インフラ事業領域
東芝デバイス＆ストレージ(株)	電子デバイス事業領域
東芝デジタルソリューションズ(株)	デジタルソリューション事業領域

東芝における量子暗号研究開発の歴史

技術開発

【主要論文】 Science (2002), Nature (2006), Nature Photonics (2007, 2008), Nature (2010),Nature Communications (2012)
Applied Physics Letters (2004), Applied Physics Letters (2007) Nature(2013), Nature Communications (2013)

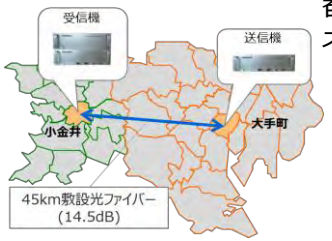
1991	…	2000	2004	2008	2010	2012	2017	2019
東芝ケンブリッジ研究所設立		単一光子検出器の開発成功	実環境で1ヶ月以上の無人安定運転	距離20km、速度1Mbps（世界最速）	距離50km、速度1Mbps（世界最速）	量子信号とデータ信号多重化	距離10km、速度10Mbps（世界最速）	

量子半導体物理の基礎研究 → 量子暗号鍵配信 世界最高レベル → 性能改善＆更なる安定化、世界最高速の鍵配信速度 → **実用化に向け日英の研究開発体制構築 実証試験を活用し実用性を検証**

実証試験

SECOQC PJ (ウィーン)

NICT委託研究
Tokyo QKDネットワーク



77日間安定稼働、
1.33Tbitの総鍵配信量

ImPACT
都市圏QKD
ネットワーク

SIP
「光・量子を活用した Society5.0 実現化技術」

ゲノム解析データ送信
(東北大共同研究)

英国QComHub PJ
Cambridge–London–Bristol間のQKD Network

- **英国で基礎技術開発し実用化向け体制を日本に構築**
- **日英での国プロ活用による実証試験で長期運用実績**

東芝の量子暗号技術概要

世界最速の量子暗号装置を開発、安定稼働を実証

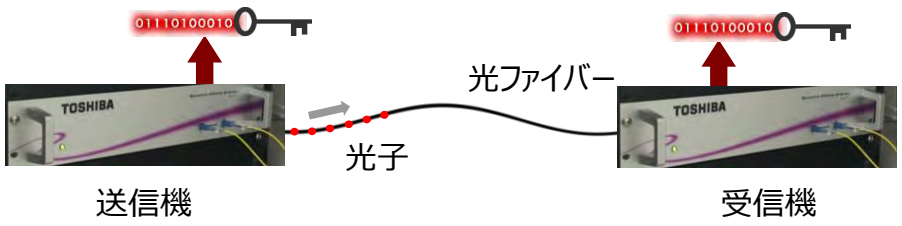
鍵配信速度の向上および安定動作が通信インフラとしての主要課題

高速化：光子検出時のノイズを低減する制御回路を開発、光子検出と鍵蒸留処理の速度・効率を向上し、距離10kmで10Mbpsを超える鍵配信速度を達成

安定化：光ファイバーの振動・環境の温度変化等によって生じる「ゆらぎ」をフィードバック技術により安定化

相互運用性：暗号鍵を提供するWebベースAPIを開発、ETSIで標準化完(2019年2月)

実証試験：東京QKDネットワーク、仙台ゲノム伝送、英国ケンブリッジ-ロンドン-ブリストル間を結ぶネットワークで実用化に向けた運用実績



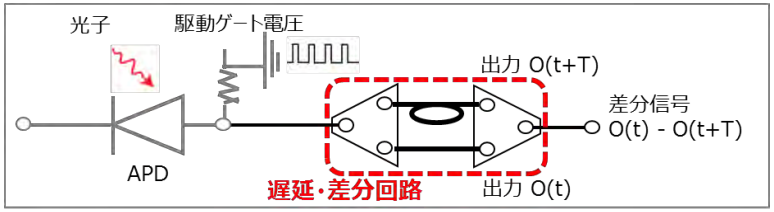
東芝の高速量子暗号装置

仙台での実証試験

東芝の量子暗号技術詳細

高速化

- 光子検出にAPD(Avalanche Photo Diode)を利用。光子検出率向上のため、周期的なバックグラウンドノイズを除去する自己差分型回路技術を開発、光学素子制御と信号処理技術の融合で1GHzクロックでの動作を実現。



L.C. Comandar, B. Fröhlich, J.F. Dynes, A.W. Sharpe, M. Lucamarini, Z.L. Yuan, R. V. Penty, and A.J. Shields, "Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm," *J. Appl. Phys.* **117**, 083109 (2015)

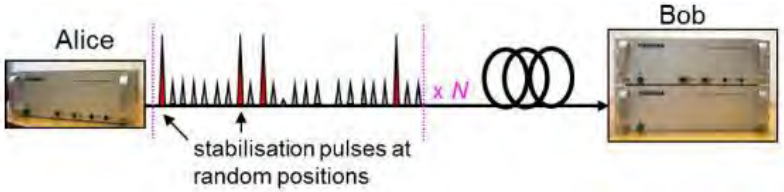
- 処理負荷の高い秘匿性増強処理(大規模行列演算)を並列実行するアルゴリズムを開発、計算量を低減し暗号鍵生成処理のスループット向上で10Mbpsの鍵配信速度を実現。

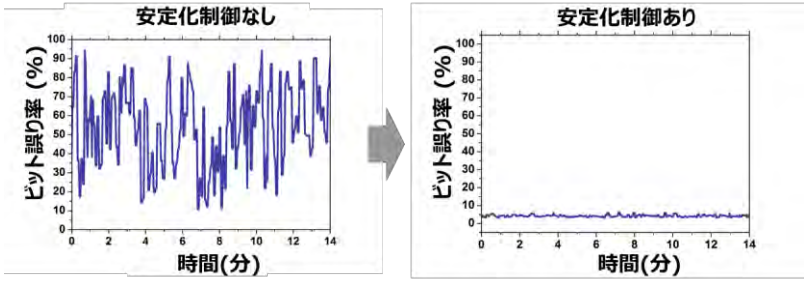
出力データ (約25Mbit) = 秘匿性増強行列A × 入力データ (100Mbit)

$$\begin{pmatrix} O_1 \\ \vdots \\ O_n \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} \begin{pmatrix} I_1 \\ \vdots \\ I_m \end{pmatrix}$$

安定化

光子が光ファイバー中を伝搬する際に、環境による温度変化、光路長変化の影響を受けて位相や偏光が変化する。安定化パルスを一定量送ることで、平常動作時からのずれを検出し、ずれを解消するよう制御。
強風時の光ファイバー振動による安定動作への影響を東京、仙台における実証試験で確認、制御方式を改良。



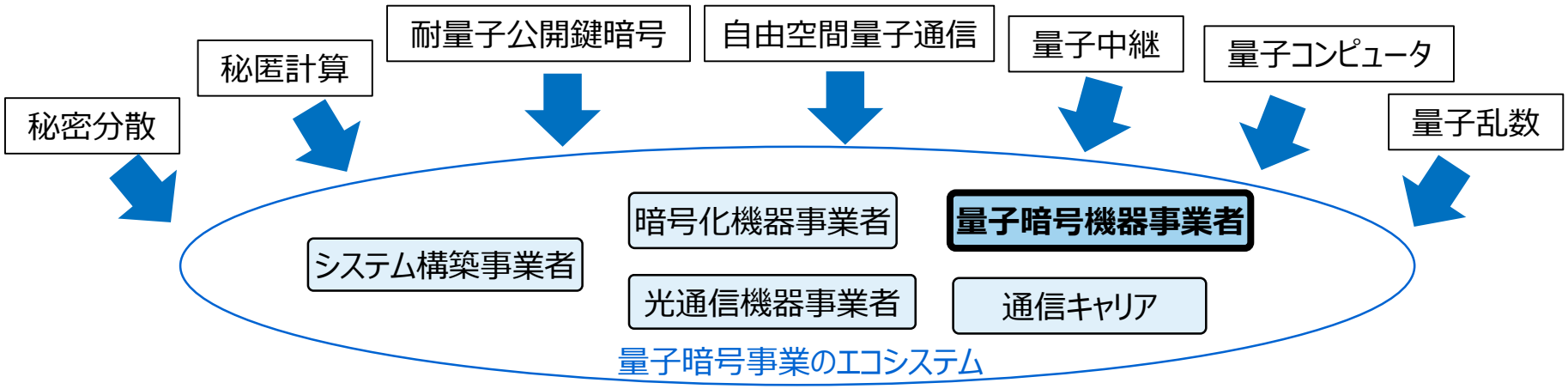


J.F. Dynes, I. Choi, A.W. Sharpe, A.R. Dixon, Z.L. Yuan, M. Fujiwara, M. Sasaki, and A.J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," *Opt. Express*, **20**, 16339, (2012)

実用化に向けた期待

省庁向けシステムで運用実績を得て、民生用途へ展開・普及

- 防衛、省庁、金融、医療など秘匿性の高いデータを扱う分野での活用を想定
  - 民生向けは普及に時間がかかるため、まずは防衛装備庁や国家安全保障局など政府、省庁内での重要データ共有向けに積極導入を期待
- 量子暗号普及に向けたガイドラインや標準の策定
- 量子暗号システム事業のエコシステムを構築し、裾野の広い通信インフラ事業として展開
  - 将来の「量子セキュリティ技術」のプラットフォームとして量子暗号普及を加速



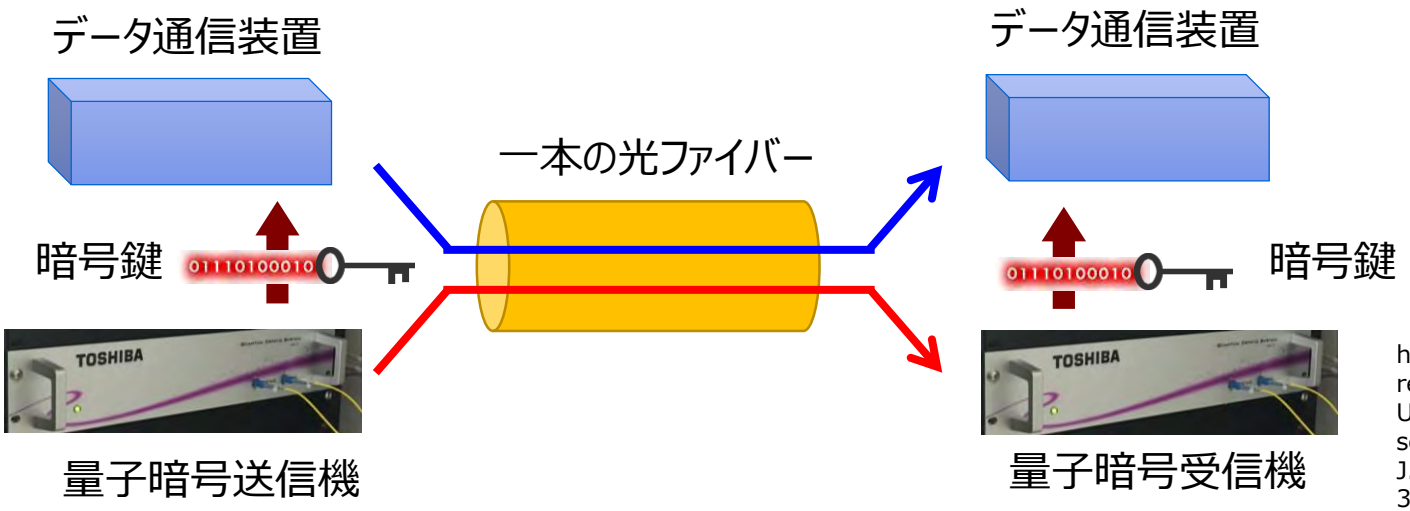
量子セキュリティ技術分野の創出に向け量子暗号の普及を加速

TOSHIBA

参考情報

東芝の量子暗号技術(1/2):信号多重化

- 量子暗号で用いる「光子」は非常に微弱な光信号であるため、本来、一般のデータトラフィックと多重化することは難しい。
- WDM(光波長多重化)技術を活用し、光子と一般的なデータトラフィックの「あいのり」技術を実証(2016年)。
- 量子暗号のための専用光ファイバー敷設を不要とし、導入コストを低減可能。

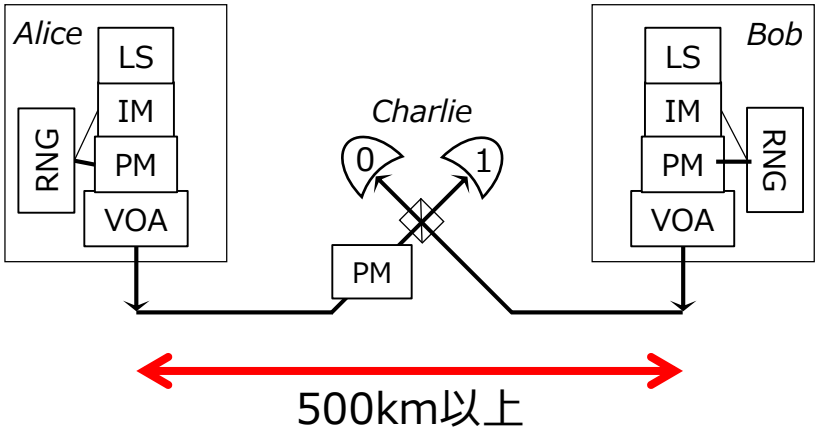


http://www.nature.com/articles/srep35149
Ultra-high bandwidth quantum secured data transmission
J. F. Dynes, et al., Sci. Rep., vol 6, 35149 (6 pages), 2016

光波長多重化技術で光ファイバー敷設コスト・負荷を低減、既設光回線でも利用可能に

東芝の量子暗号技術(2/2):長距離化

- 一式の量子暗号装置によって通信(暗号鍵共有)可能な距離は、従来技術では最大100~200kmに限られる。これは、光子が光ファイバー上で減衰してしまう物理的な制約によるもの。
- 量子暗号の新しいプロトコルを考案し、光ファイバーを使った量子暗号で500kmを超える通信(暗号鍵共有)が可能となることを示した(2018年)。
- 本技術はTwin-Field QKDと呼ばれる。光子送信を両端の拠点から行い、中央の拠点で光子検出を行う構成。

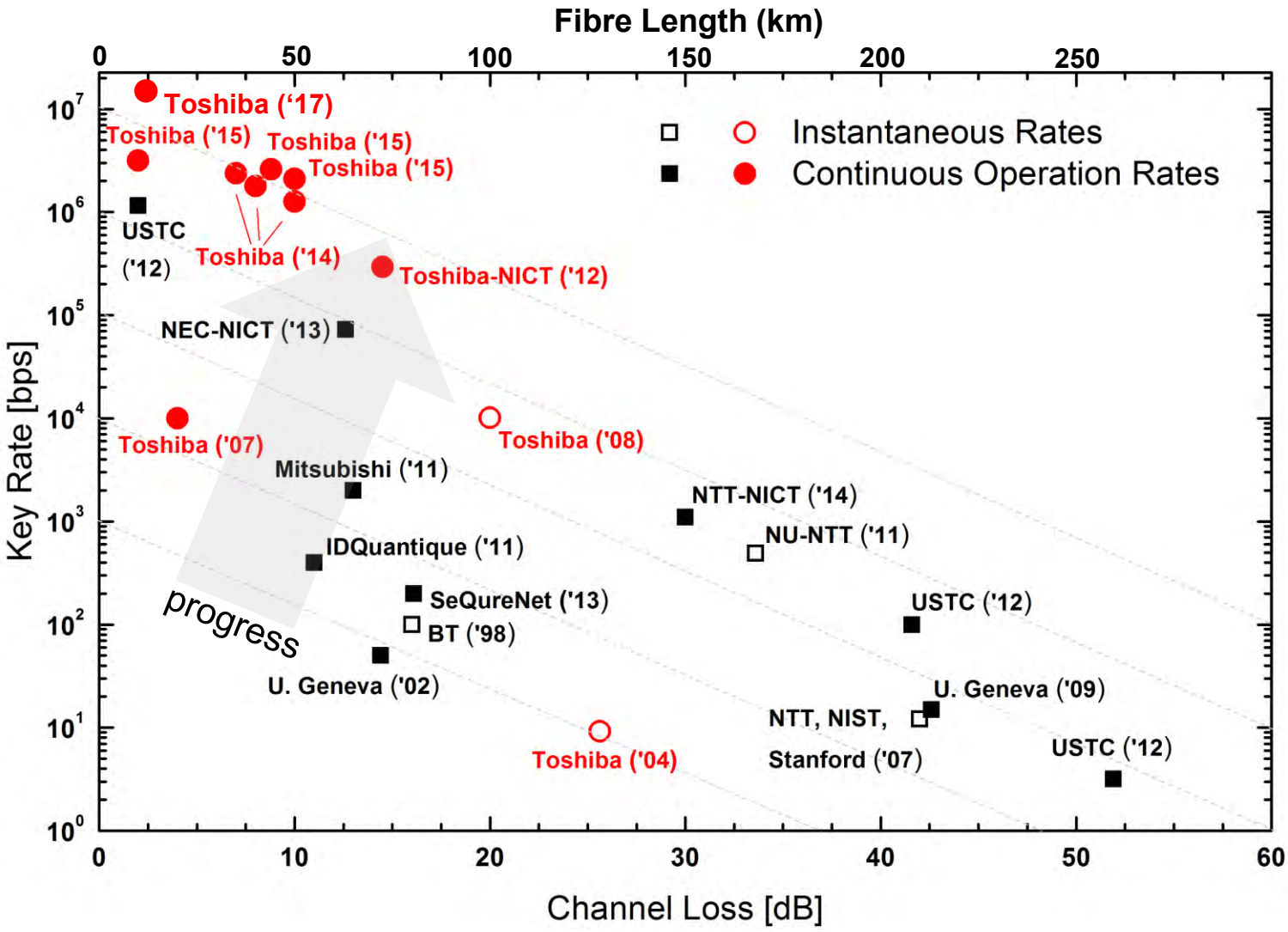


Laser sources (LS)
Intensity modulators (IM)
Phase modulators (PM)
Variable Optical Attenuators (VOA)
Random Number Generators (RNG)

https://www.nature.com/articles/s41586-018-0066-6
Overcoming the rate-distance limit of quantum key distribution without quantum repeaters
M. Lucamarini, et al.
Nature, vol 557, pp. 400-403, 2018

将来の長距離化に向けて新プロトコルを提案・開発

鍵配信速度の比較



実用化の動向

IDQuantique

スイス・ジュネーブ大学からのスピンオフ企業。ジュネーブ投票システムや金融機関のリカバリネットワーク、バックボーンリンクへの適用など、数多くの実証実績がある。さらに欧州のR&Dプログラムに参加することで学術機関とも関係を持ち、最先端のプロジェクトで主要な役割を果たしている。2017年英BTとQKDを利用した100Gbpsイーサネット伝送のデモンストレーションに成功している。
2018年韓国SK Telecomが買収。

https://www.idquantique.com/single-photon-systems/products/clavis3-qkd-platform/
https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/

Clavis 3

Cerberis QKD Blade

QuantumCTek

2009年に中国科学技術大学と個人投資家によって設立された。2000kmの長距離中国ネットワーク計画に参画。中国の量子情報技術標準化団体のリーダーを務める。最近では2018年に66kmファイバーで3.6Tbpsの古典データと量子信号の同時送信の成功を報告している。

QKD-PHA300-S
http://www.quantum-info.com/English/product/quantum/2017/1013/407.html

Yingqiu Mao et al, “Integrating quantum key distribution with classical communications in backbone fiber network ” *Optics Express*, 26, 6010 (2018)

Qasky

Wuhu Construction and Investment Ltd.と中国科学技術大学の共同出資によって2009年に設立された。P2Pの量子暗号通信技術、量子暗号通信ネットワーキング技術、量子暗号通信コアデバイスを提供している。中国の150km超のQKDネットワーク実証に参画。

GHz quantum key distribution terminal
http://www.qasky.com/en/display.asp?id=781

S. Wang, et al, “Field and long-term demonstration of a wide area quantum key distribution network,” *Optics Express*, Vol. **22**, 21739 (2014)