（資料３－４）

電気通信事業分野における競争ルール等の包括的検証に関する特別委員会：

2030年の通信ネットワークビジョン検討に向けた量子情報技術のご紹介(量子暗号技術を中心に)

TOSHIBA

2018.10.26

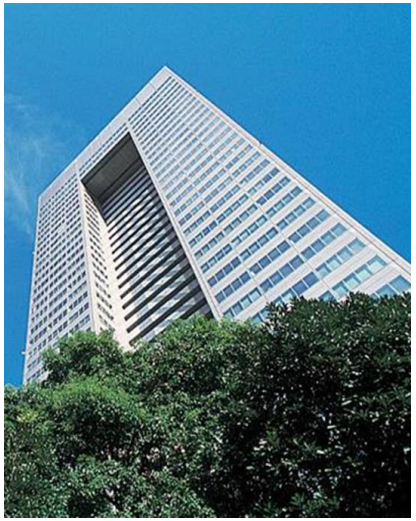
Contents

01

会社紹介

東芝グループ

人々の暮らしと社会を支える社会インフラを核とした事業領域に注力
確かな技術で、豊かな価値を創造し、持続可能な社会に貢献



社名	株式会社 東芝
本社	東京都港区芝浦1-1-1
創業	1875年(明治8年) 7月
代表執行役会長 CEO	車谷 暢昭
代表執行役社長 COO	綱川 智
資本金	2,000億4,400万円（2018年8月3日現在）
年間売上高（連結）	3兆9,476億円（2017年度）
従業員数（連結）	141,256人（2018年3月31日現在）

グローバルR&D体制

東芝欧州研究所

ケンブリッジ研究所
- **量子情報**
- 音声・画像認識

通信研究所
- 無線通信技術


(ケンブリッジ)


(ブリストル)

東芝中国社

研究開発センター
- 音声
- 機械翻訳


(北京)

株式会社東芝　研究開発センター


(川崎)


(ニューヨーク)


(サンノゼ)

東芝ソフトウェア・インド社


(バンガロール)

R＆D部門
- データ解析、ディープラーニング


(ハノイ)

東芝ソフトウェア開発ベトナム社

- ソフトウェア

東芝アメリカ研究所

- クラウド / ビッグデータ

英国ケンブリッジ研究所と国内研究開発センターとで連携し、量子情報技術の研究開発を推進。

東芝における量子情報技術開発の歴史

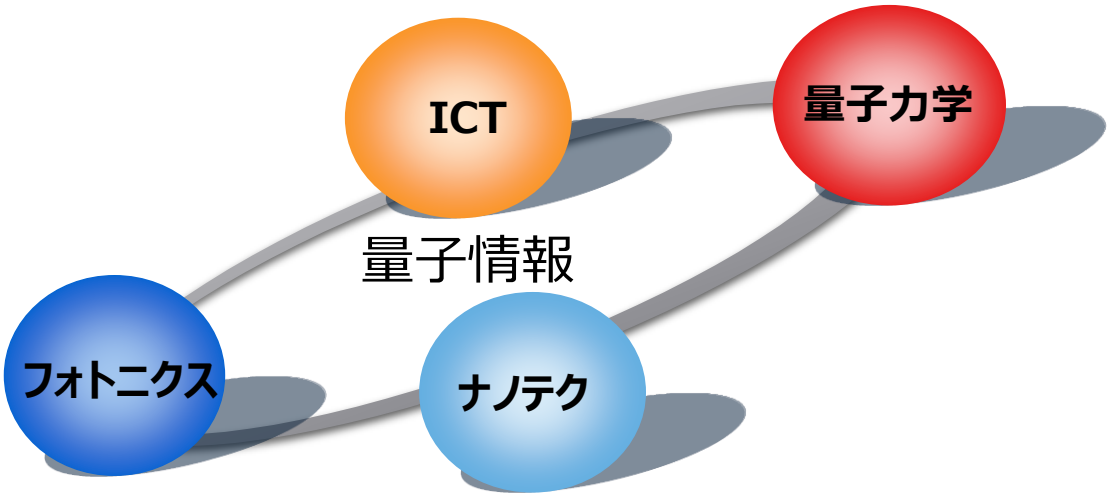
委員会限り

02

量子情報技術の全体像・動向

量子情報技術とは

基礎物理から情報理論までの幅広い領域にまたがった融合技術



量子力学や量子の特徴的な振る舞いを利用した、複数の技術の総称

- 量子コンピュータ：超高速・並列計算
- 量子通信・量子暗号：盗聴不可能な暗号通信
- 量子センサ・イメージング：超高感度・高分解能での情報検出
- etc.

量子情報技術に関する各国動向

委員会限り

本プレゼンでは、

量子情報技術の究極目標とも言われ、注目度の高い

「量子コンピュータ」

量子情報技術の中でも最も実用化が近いと言われている

「量子暗号」

にフォーカスいたします。

03

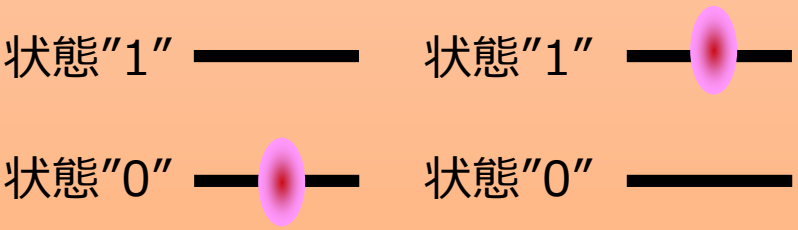
量子コンピュータ

量子コンピュータの基本原理

量子の”重ね合わせ状態”を利用し、同時に複数の状態を表現・計算できる。

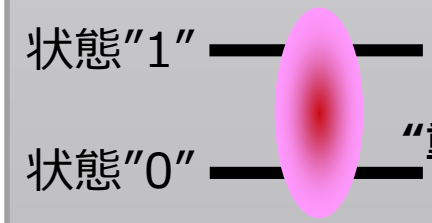
一般的なコンピュータ

情報の単位
0または1



量子コンピュータ

情報の単位
量子ビット（Qubit）



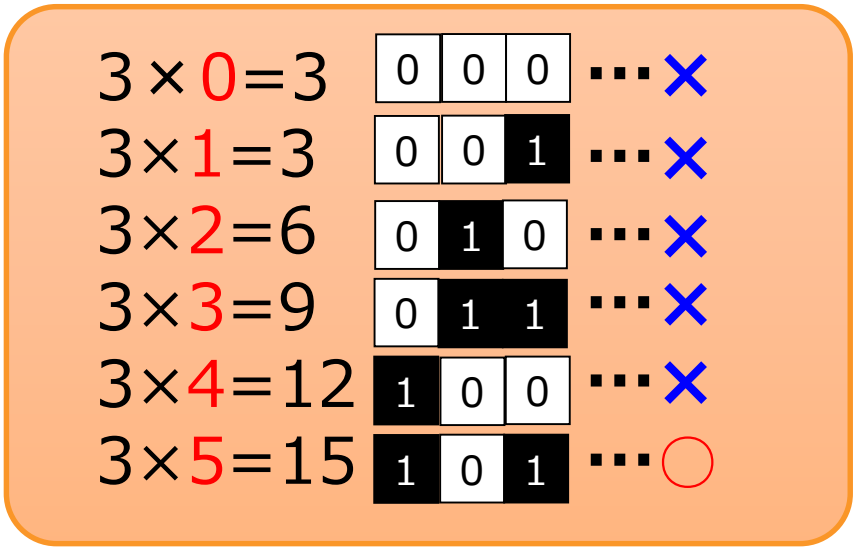
量子力学的
“重ね合わせ状態”

情報の単位として“0でも1でもある状態”を用いる

量子コンピュータの基本原理

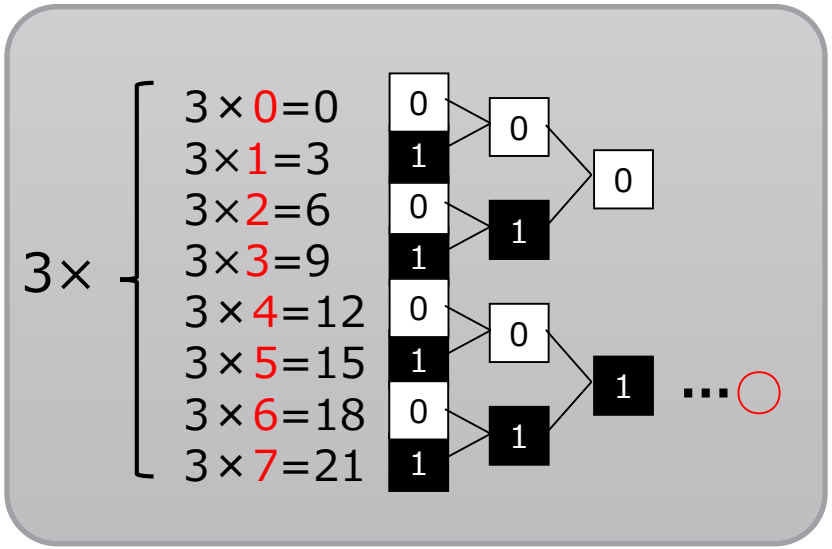
例えば3bitで15=3×5という因数分解を解く場合…

一般的なコンピュータ



1通りずつ順番に計算

量子コンピュータ



2^3通りを同時に計算可能

量子力学の原理で、超並列計算を実現

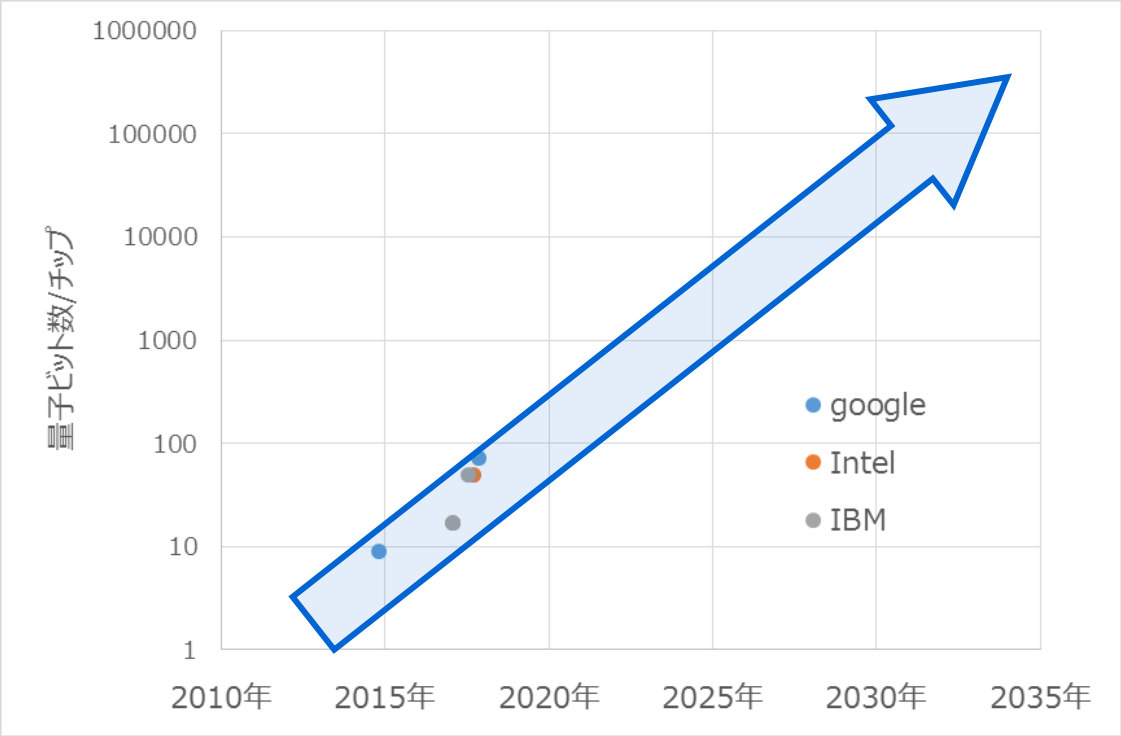
量子コンピュータの種類

	量子コンピュータ：量子効果を用いて計算を行うマシン			
種類	量子ゲート方式		量子最適化方式	
機能	量子効果をゲート動作に用いて、万能量子計算を行う汎用コンピュータ		量子効果を用いて組み合わせ最適化問題解決を行う専用コンピュータ	
代表的な実装方法	超伝導	シリコン	超電導	光ネットワーク
ビット数	72	2	2048	2048
企業	Google, IBM, Intel, Riggeti, NTT, Microsoft	Intel	D-wave	NTT

量子ゲート方式(超伝導方式)の量子コンピュータに注目・投資が集まっている

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing
https://quantumcomputingreport.com/scorecards/qubit-count/
https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html
https://newsroom.intel.com/press-kits/quantum-computing/
https://www.research.ibm.com/ibm-q/
https://www.nii.ac.jp/qis/first-quantum/newsLetter/pdf/newsletter_no15.pdf
https://www.technologyreview.jp/s/23001/can-a-powerful-new-quantum-computer-convince-the-skeptics/
https://qistokyo.wordpress.com/research/coherent-ising-machine/

量子コンピュータ研究開発の状況



2030年台には実用的(*1)な量子コンピュータが登場！？ (*2)

*1) 100万~1,000万量子ビットの量子コンピュータ(量子ゲート方式)ができれば
実用的と言われている

*2) 1年間で2倍のペースでビット数増加すると想定した場合

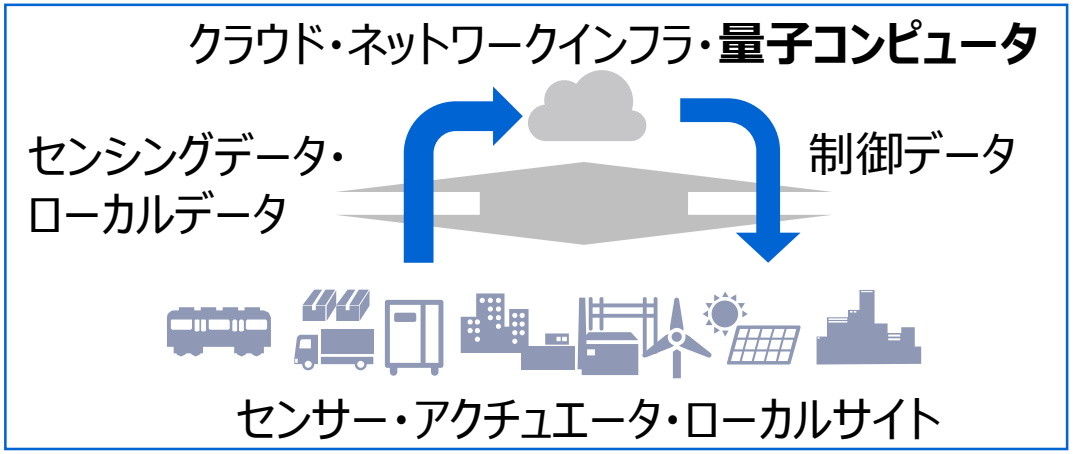
https://en.wikipedia.org/wiki/Timeline_of_quantum_computing
https://quantumcomputingreport.com/scorecards/qubit-count/
https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html
https://newsroom.intel.com/press-kits/quantum-computing/
https://www.research.ibm.com/ibm-q/
https://www.nii.ac.jp/qis/first-quantum/newsLetter/pdf/newsletter_no15.pdf

量子コンピュータの応用分野

- 様々な応用が期待されている
  新薬や新素材の開発、物流・交通の最適化、金融予測、災害予測、etc…

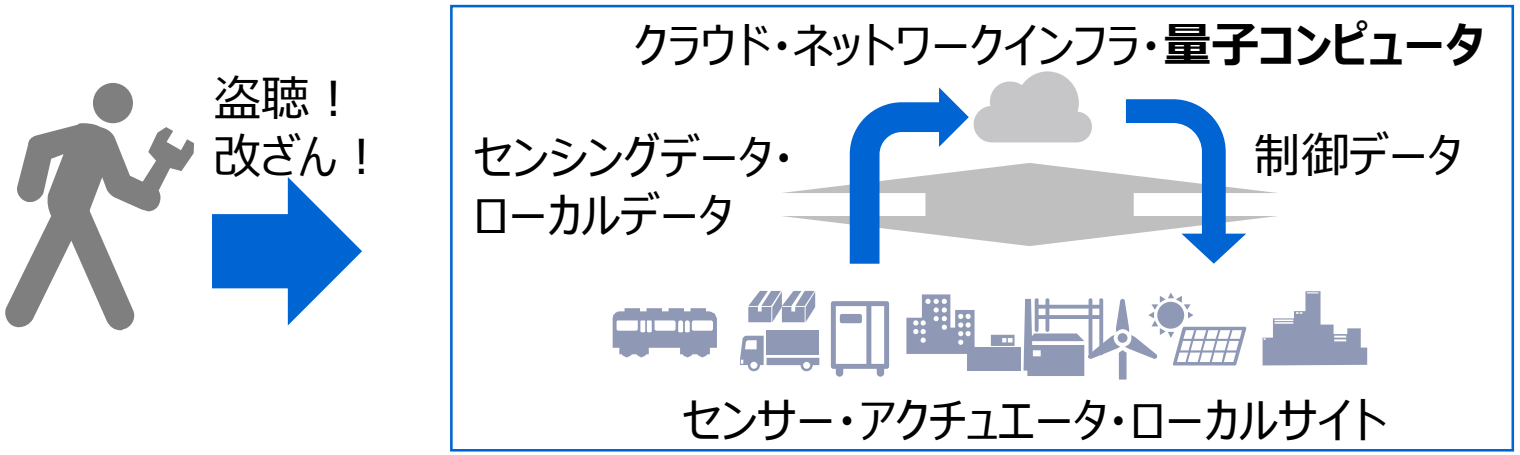
- 近年では、量子コンピュータによる高速機械学習や高速ビッグデータ探索への応用への注目が高まっている

サイバーフィジカルシステムを支える「頭脳」としての役割



その反面…

- 量子コンピュータを使うと、現在インターネットで一般的に利用されている暗号(RSA, etc.)が短時間で解読されてしまう！
  - RSAは、一般的なコンピュータでは因数分解等の数学の問題を解くことに時間がかかることを安全の根拠にしている。
  - 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。



量子コンピュータによっても解読できない
安全安心なセキュリティソリューションが必要

量子コンピュータ登場に向けた対策

量子コンピュータによっても解読できない
安全安心なセキュリティソリューションが必要

大きく２つのアプローチ

- アプローチ１：耐量子暗号アルゴリズム
  - 量子コンピュータによっても計算が難しいと考えられている数学的問題に基づく。
  - 安価で組み込み機器への導入等が容易な反面、「情報理論的安全性」は無い。
  - NIST(米国立標準技術研究所)では、標準仕様の選定中。
  - 2025年頃から標準技術として利用開始予定。

- アプローチ２：量子暗号(量子鍵配送)技術
  - 量子情報技術(量子力学)に基づく、新しい暗号技術
  - 「光子」の送受信機を含むハードウェアの導入が必要（現時点で高価）。
  - 「情報理論的安全性」を実現する唯一のセキュリティ技術

➡ 以下では量子暗号技術にフォーカスします。

04

量子暗号

量子暗号の市場動向

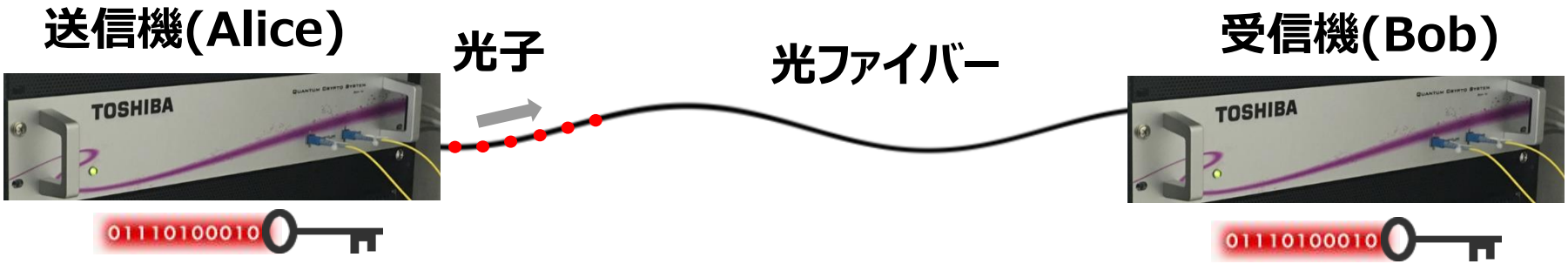
委員会限り

各国の実証実験・大型プロジェクト等

委員会限り

量子暗号技術とは

- 量子暗号技術とは、情報を安全にやり取りするために用いられる暗号通信技術の一つ
  - 離れた２地点間の暗号通信に使う鍵を安全に共有する技術



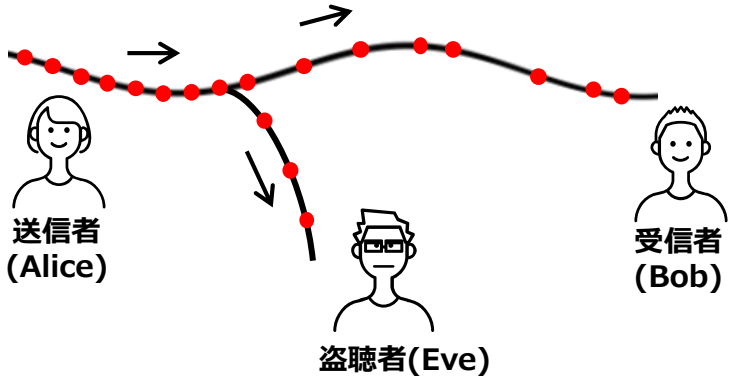
- 他の暗号通信技術に対してユニークな点
  - 性能：「情報論的安全性」を実現する。
    - 量子暗号技術によって守られる暗号通信は、理論上解読不可能。
  - 原理：量子力学の原理に基づく。

量子力学に基づく、解読不可能な暗号通信技術

量子暗号の原理

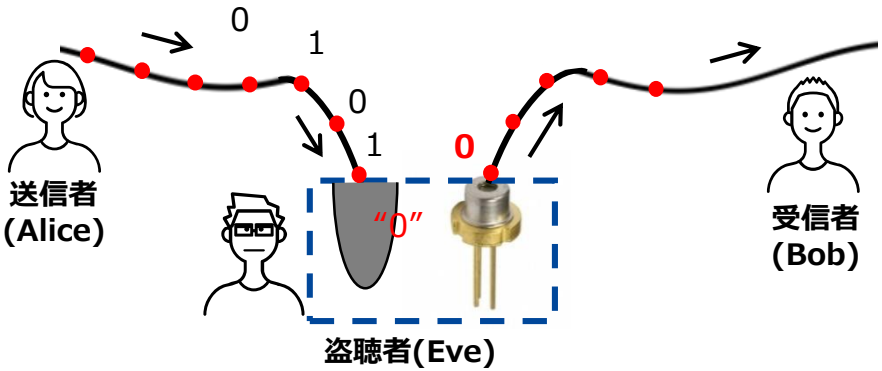
- 「暗号鍵情報」を”単一光子”にコード化して交換する。
- ”光子”の２つの特殊な振る舞いを利用する。

「光子は分割できない」



⇒ 光子の数から盗聴を検出

「光子状態は完全にはコピーできない」



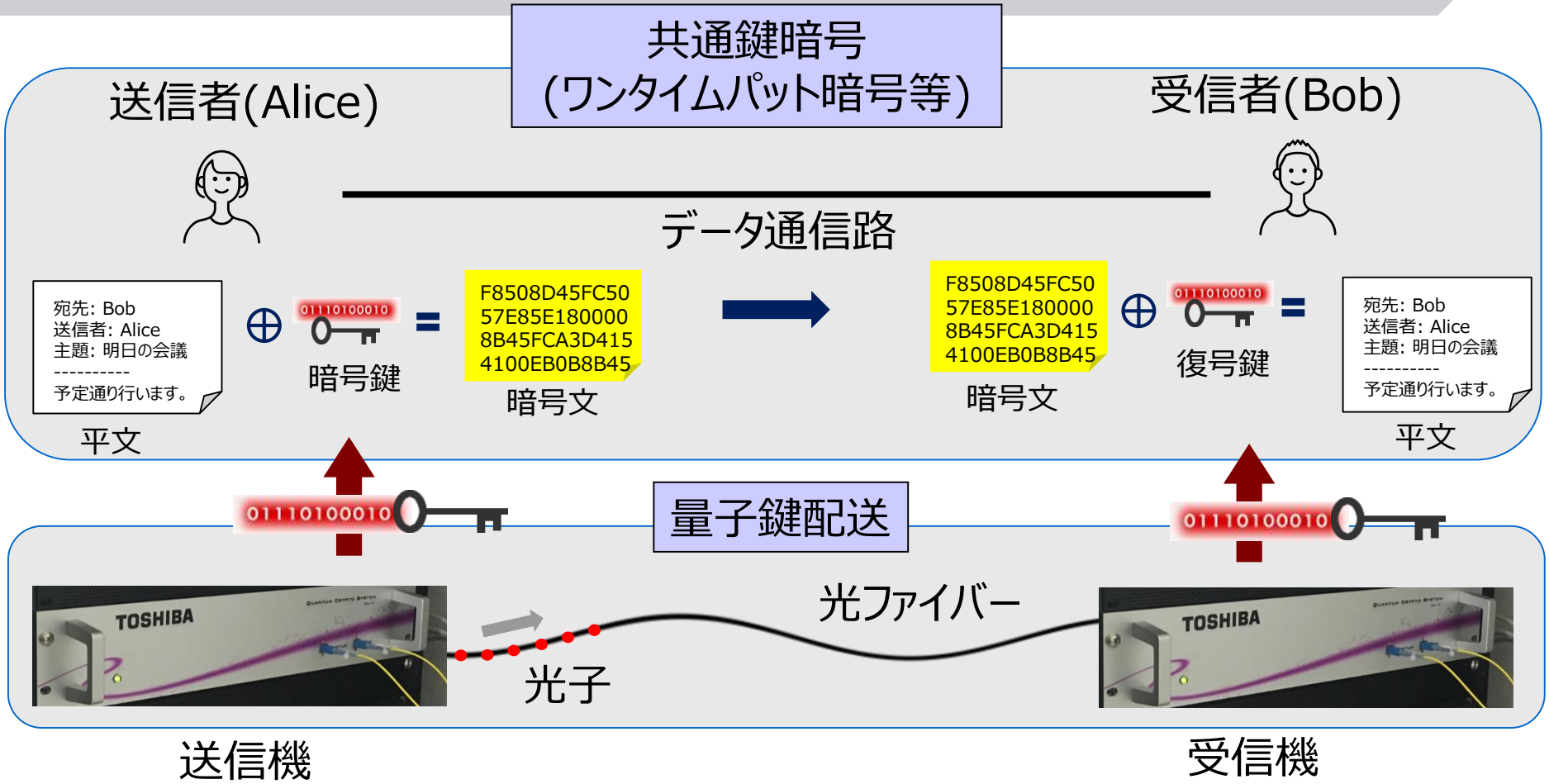
⇒ 光子の状態から盗聴を検出

受診者(Bob)は、送信者(Alice)に確認することで、確実に盗聴を検出できる。

- 盗聴されずに交換された”光子”の「暗号鍵情報」に基づいて、「暗号鍵」を生成・共有する。

光子の量子的振る舞いに基づいて、
盗聴されていないことが保証された「暗号鍵」を共有

量子暗号通信システム

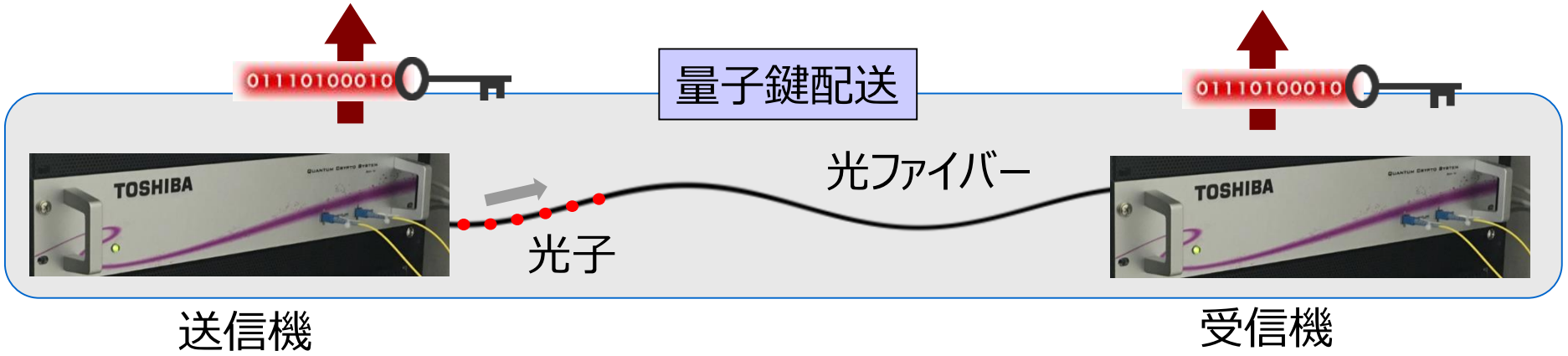


- ワンタイムパッド暗号は、平文と同じ長さの暗号鍵を使い捨てる方式
- 量子鍵配送とワンタイムパッド暗号の組み合わせによって、「情報論的安全性」を保証

量子暗号通信 =
量子鍵配送(QKD, Quantum Key Distribution) + 共通鍵暗号

量子暗号技術実現のための基礎技術(株式会社東芝)

- 高速化：光子検出素子の制御回路を開発。光子検出の動作速度・効率を向上し高速化(10Mbps超(*1))
- 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光子到着の「ゆらぎ」をフィードバック技術により安定化(2ヶ月以上の安定動作(*2))



量子暗号の高速化と安定化を実現
様々な実証実験を通じて実証

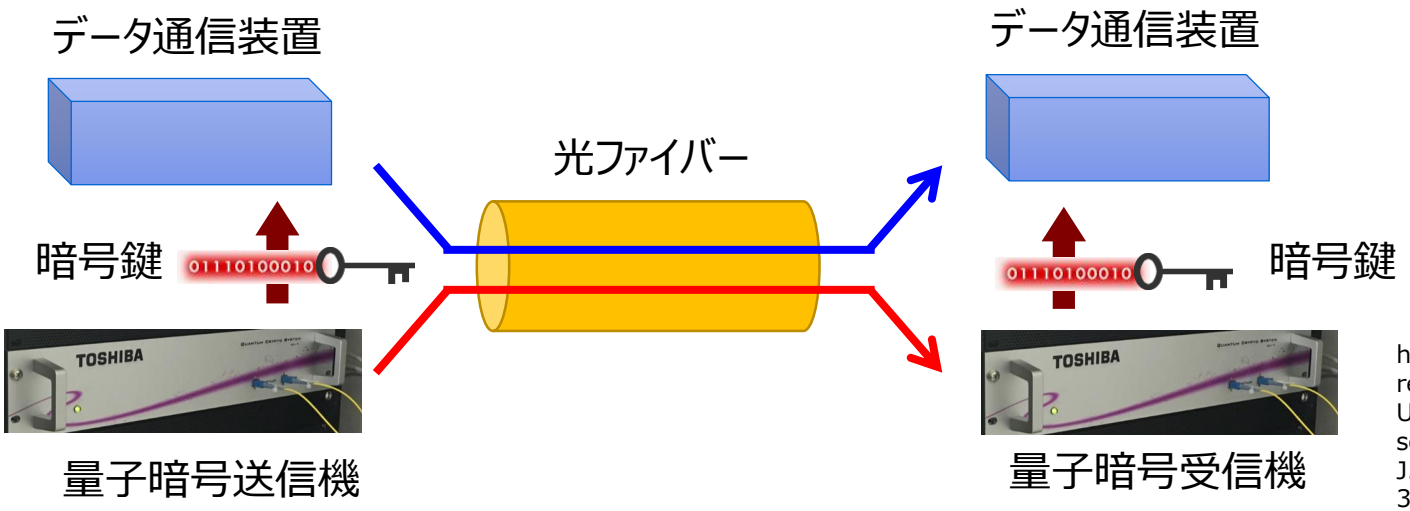
*1) https://www.toshiba.co.jp/about/press/2018_08/pr_j2701.htm
*2) https://www.nature.com/articles/s41598-017-01884-0

実証実験

委員会限り

量子暗号技術の改善手法(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、光子検出制御とフィルタ技術を組み合わせ、量子暗号のための光子通信と、100Gbpsの一般的な光データチャネル(同一方向)との多重化に成功(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。

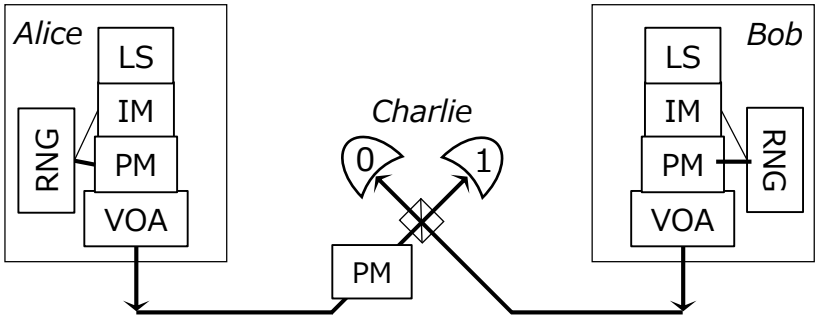


http://www.nature.com/articles/srep35149
Ultra-high bandwidth quantum secured data transmission
J. F. Dynes, et al., Sci. Rep., vol 6, 35149 (6 pages), 2016

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。

量子暗号技術の改善手法(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

05

まとめ

まとめ

- 量子暗号・量子コンピュータを含む量子情報技術への投資は世界各国で増加しています。
- 実用的な量子コンピュータは2030年代頃に登場すると見込まれています。
- 量子コンピュータには様々な応用分野があり、例えばサイバーフィジカルシステムの「頭脳」として使われる可能性があります。
- 量子コンピュータを使うと、現在の暗号技術は容易に解読されてしまうため、量子暗号・耐量子暗号の導入を進める必要があります。
- 量子暗号技術は、量子コンピュータでも決して解読できない情報論的安全な暗号通信を実現します。通信距離やコスト等の条件はありますが、技術的には成熟してきており、実用化に向けた研究開発・検証フェーズです。

2030年の通信ネットワークビジョン(一例)

一部のクラウド・拠点内で**量子コンピュータ**が利用される

クラウド・データセンター・
ネットワークインフラ・**量子コンピュータ**

クラウド・データセンター間接続には**量子暗号**も活用される。一部は衛星通信ベース。

各種IoT機器等のデータ・ローカルデータは、一部はローカルサイトで利用され、一部はクラウドへアップロードされ、解析・利活用される。

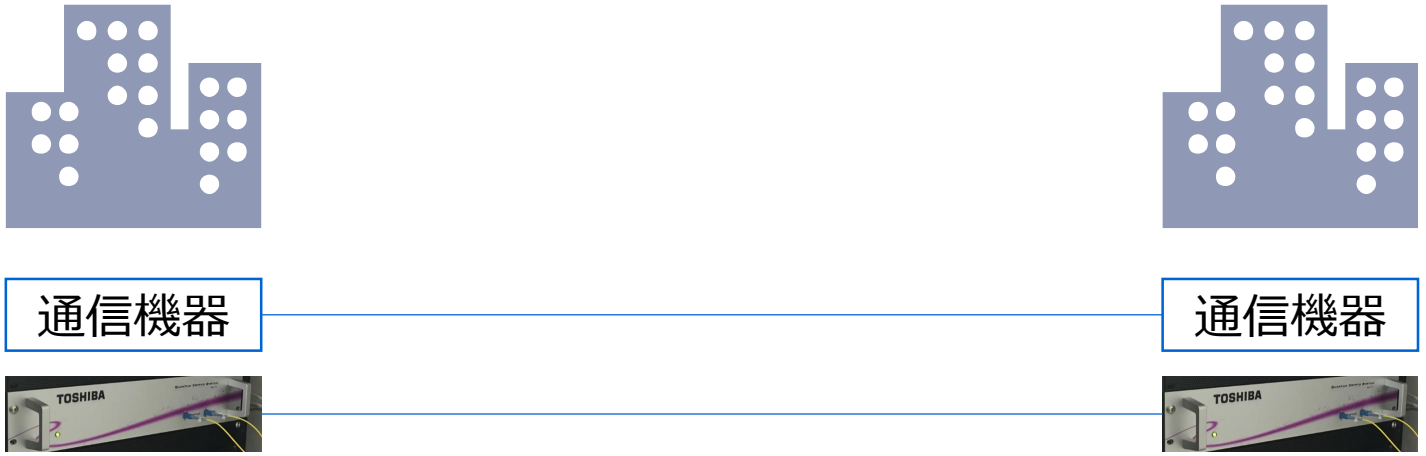
組み込み機器・小型軽量機器の通信セキュリティは耐量子暗号で実現

重要拠点間通信・医療データ通信のセキュリティ確保には**量子暗号**が利用される。

センサー・アクチュエータ・ローカルサイト

量子暗号のユースケース例(1/3)

重要拠点間の接続

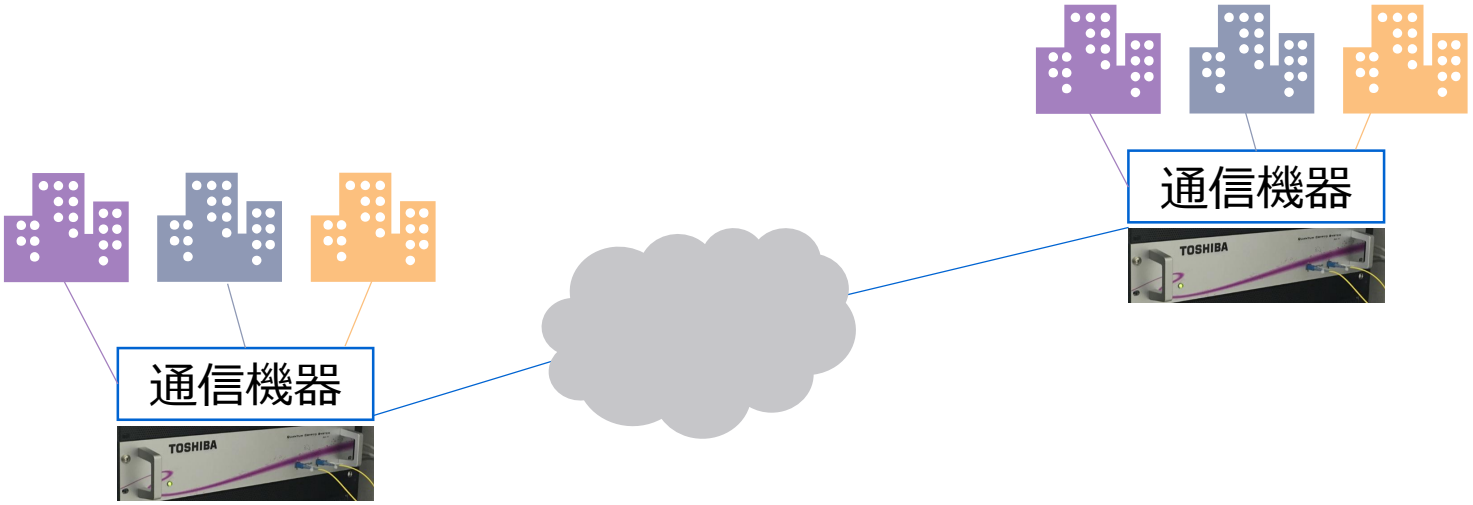


- 官公庁拠点間
- クラウド・データセンター間接続
- 大企業拠点間
- 地域拠点病院間
- etc.

- 量子暗号装置は、既存通信機器にアドオンする形で追加導入
- あるいは、量子暗号装置は、通信機器と同時に導入・保守
- あるいは、量子暗号機能が一体化した通信機器として導入・保守

量子暗号のユースケース例(2/3)

セキュアコネクションサービス

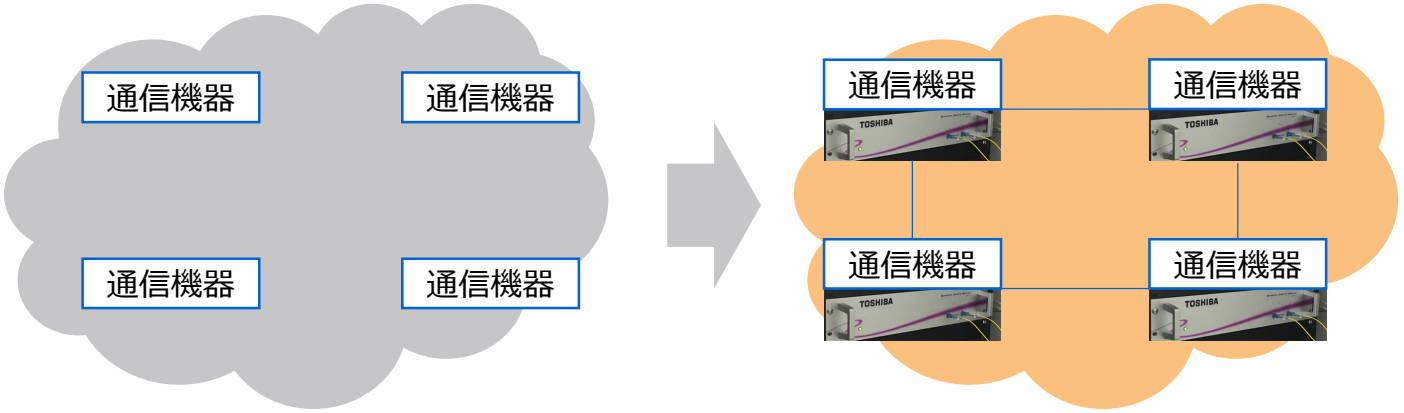


- 例えば、東京-大阪間等、多くの組織が接続・通信したい拠点に量子暗号リンクを敷設・運用(*1)。
- 複数組織に対して、量子暗号セキュア通信サービスを利用してもらい、そのサービス対価を得る(量子暗号通信サービスのスライス化)。

*1 東京大阪間は、現在の量子暗号技術を用いた場合、2,3の中間拠点を(例えば、名古屋、静岡等に)設けて実現する必要がある。

量子暗号のユースケース例(3/3)

通信キャリア網導入



- 通信キャリアが、例えばコアネットワークに量子暗号技術を導入する。
- キャリア網利用者は、意識することなくそのセキュリティ機能を利用する。
- 量子暗号によるセキュリティをプレミアムサービスとして別の網で提供することも可能。

2030年の通信ネットワークビジョン検討に向けて

- インフラ
  - 量子暗号は既設光ファイバー網も利用可能。量子技術と親和性の高い光通信インフラがますます重要に。
  - 量子暗号性能・運用の観点からは、ファイバー品質が高いこと(低ロスであること)、柔軟なファイバー接続・運用が可能であること(接続拠点において、増幅器やAD変換等を介さない接続を許容する等)が望ましい。
- セキュリティ政策
  - 量子コンピュータの研究開発等に伴って暗号解読技術が向上してゆく中、データを取り扱う際のセキュリティ対策の重要性が高まる。
  - 特に、国家安全、個人の生命・財産(医療・ゲノム情報等)、企業の技術・経営等に関わる情報など、長期安全性が必要なデータは、(例えば、情報論的安全性が担保されるセキュリティ等による)特別な管理が必要と考えられる。
- 人材育成
  - 量子コンピュータ・量子暗号時代に備えて、既存の電気通信関連技術(電気、情報、制御、プログラミング、etc.)に加え、「量子」の考え方に精通した技術者・指導者が必要。
  - 上記技術者・指導者は、量子コンピュータや量子暗号等の量子情報関連の技術・機器を社会に導入する上で必要な、製品認定システム・法令/規定等の策定・改定でも重要な役割を果たすと思われる。

TOSHIBA

ご清聴ありがとうございました