量子暗号通信の紹介と海底光ファイバ通信への応用

2024年12月5日

NEC アドバンストネットワーク研究所
前田和佳子

Outline

1. 海底光ファイバ通信
2. 量子暗号通信

海底光ファイバ通信

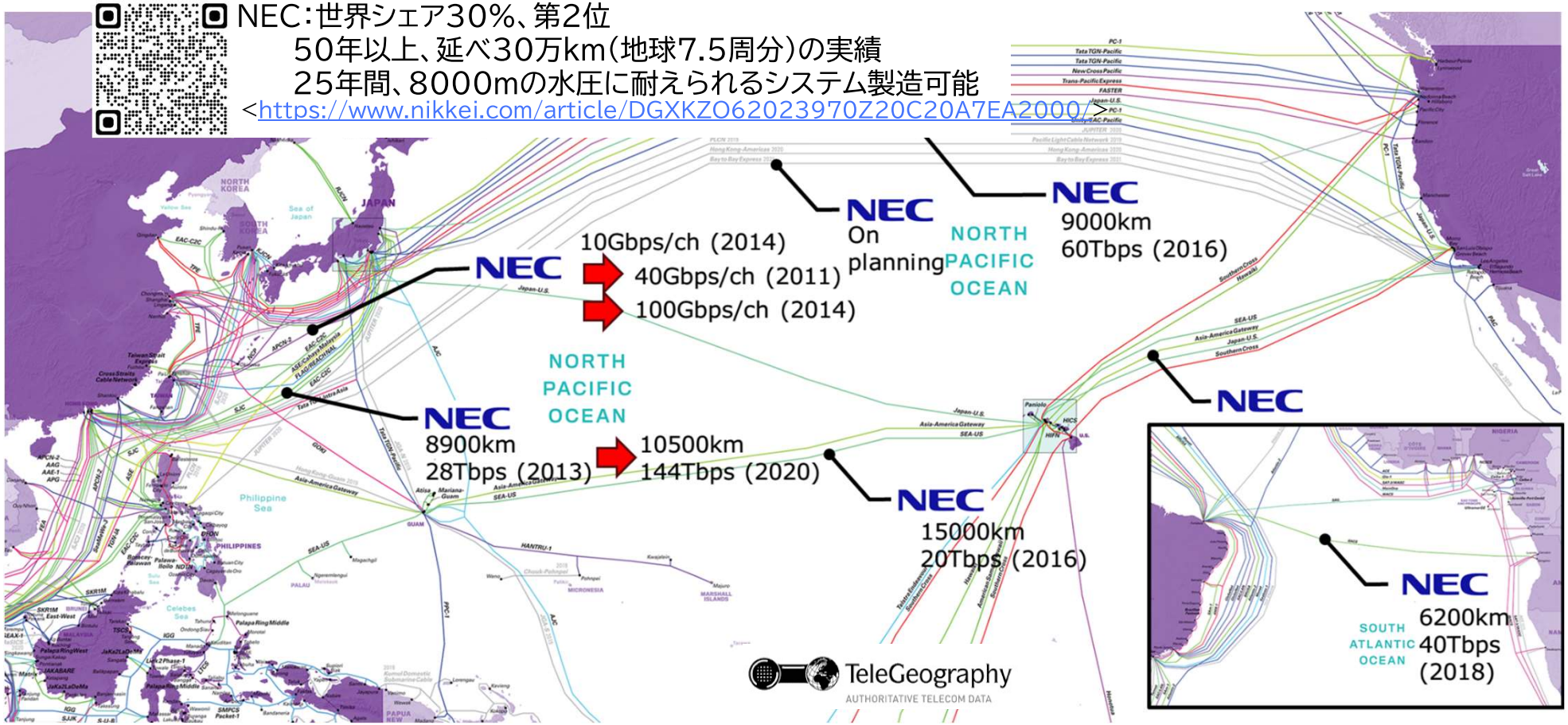
海底から宇宙まで

世界中の多岐に渡る業種のお客さまに幅広く価値を提供

世界の海底ケーブルマップ

海底光ケーブルシステム(敷設済み)

NEC:世界シェア30%、第2位
50年以上、延べ30万km(地球7.5周分)の実績
25年間、8000mの水圧に耐えられるシステム製造可能
<https://www.nikkei.com/article/DGXKZO62023970Z20C20A7EA2000/>



長距離大容量通信

350Tbps, 10,000km伝送を実現する光(海底ケーブル)通信システム

NEC to build new trans-Pacific cable

- Cable to provide the largest data capacity between the US and Japan -

News Room

Corporate/Financial

Sustainability

R&D

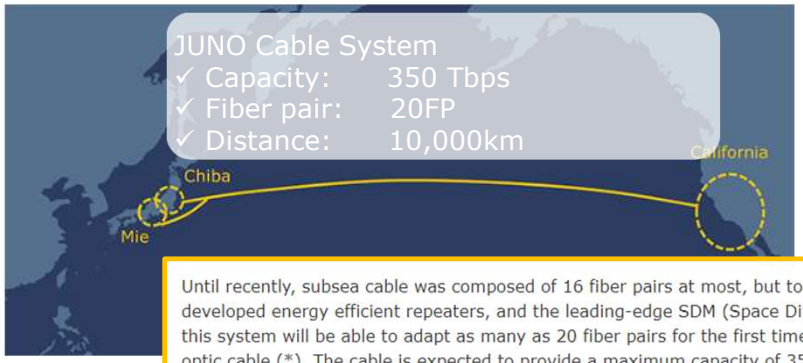
Services/Solutions

Computers/Hardware

Customer Wins

Search by date

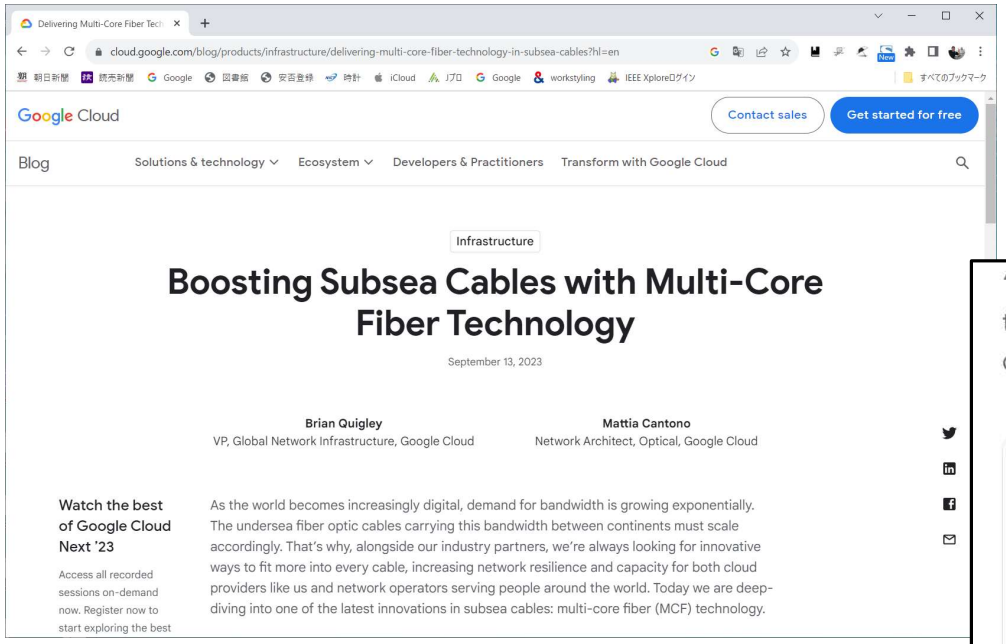
Tokyo, July 21, 2022 - NEC Corporation (NEC; TSE: 6701) today announced that it has been contracted by Seren Juno Network Co., Ltd., a company established by NTT Ltd Japan Corporation, PC Landing Corp. Mitsui & Co., Ltd. and JA Mitsui Leasing, Ltd. to build a trans-Pacific subsea fiber-optic cable, "JUNO Cable System," connecting California in the US with Chiba prefecture and Mie prefecture in Japan. This cable will provide the largest data capacity between the US and Japan, spanning a total distance of approximately 10,000 km, and is expected to be completed by the end of 2024.



Until recently, subsea cable was composed of 16 fiber pairs at most, but today, by using NEC's newly developed energy efficient repeaters, and the leading-edge SDM (Space Division Multiplexing) technology, this system will be able to adapt as many as 20 fiber pairs for the first time in a trans-Pacific subsea fiber-optic cable (*). The cable is expected to provide a maximum capacity of 350Tbps, the largest among any existing cable system between the US and Japan.

世界初マルチコアファイバを収容する海底ケーブル

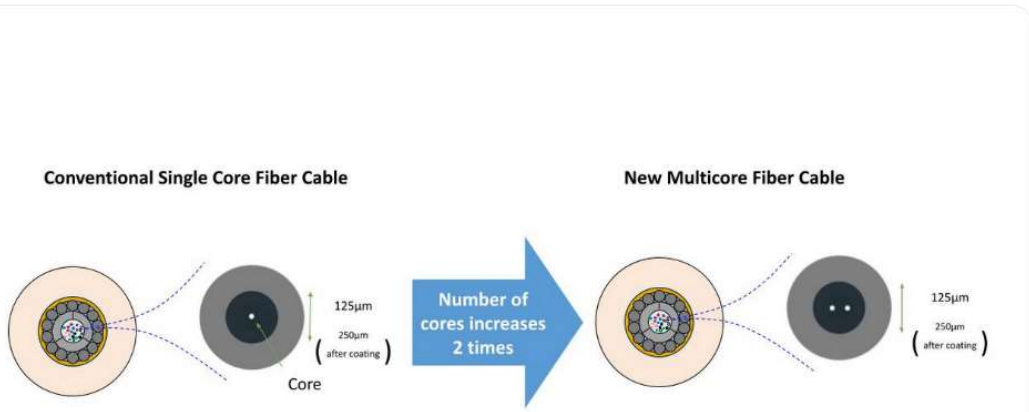
Google blogより



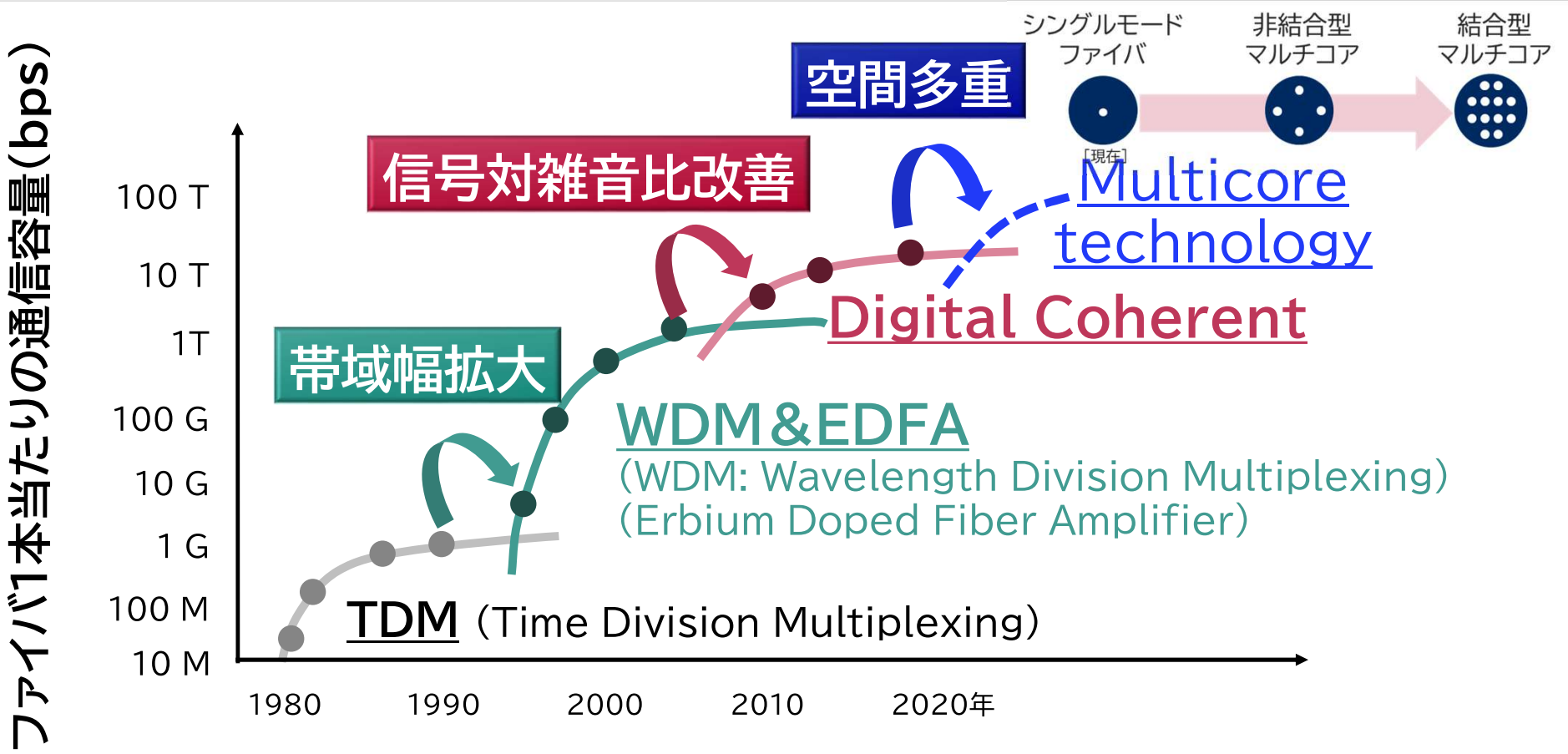
https://cloud.google.com/blog/products/infrastructure/delivering-multi-core-fiber-technology-in-subsea-cables?hl=en

2023年9月13日

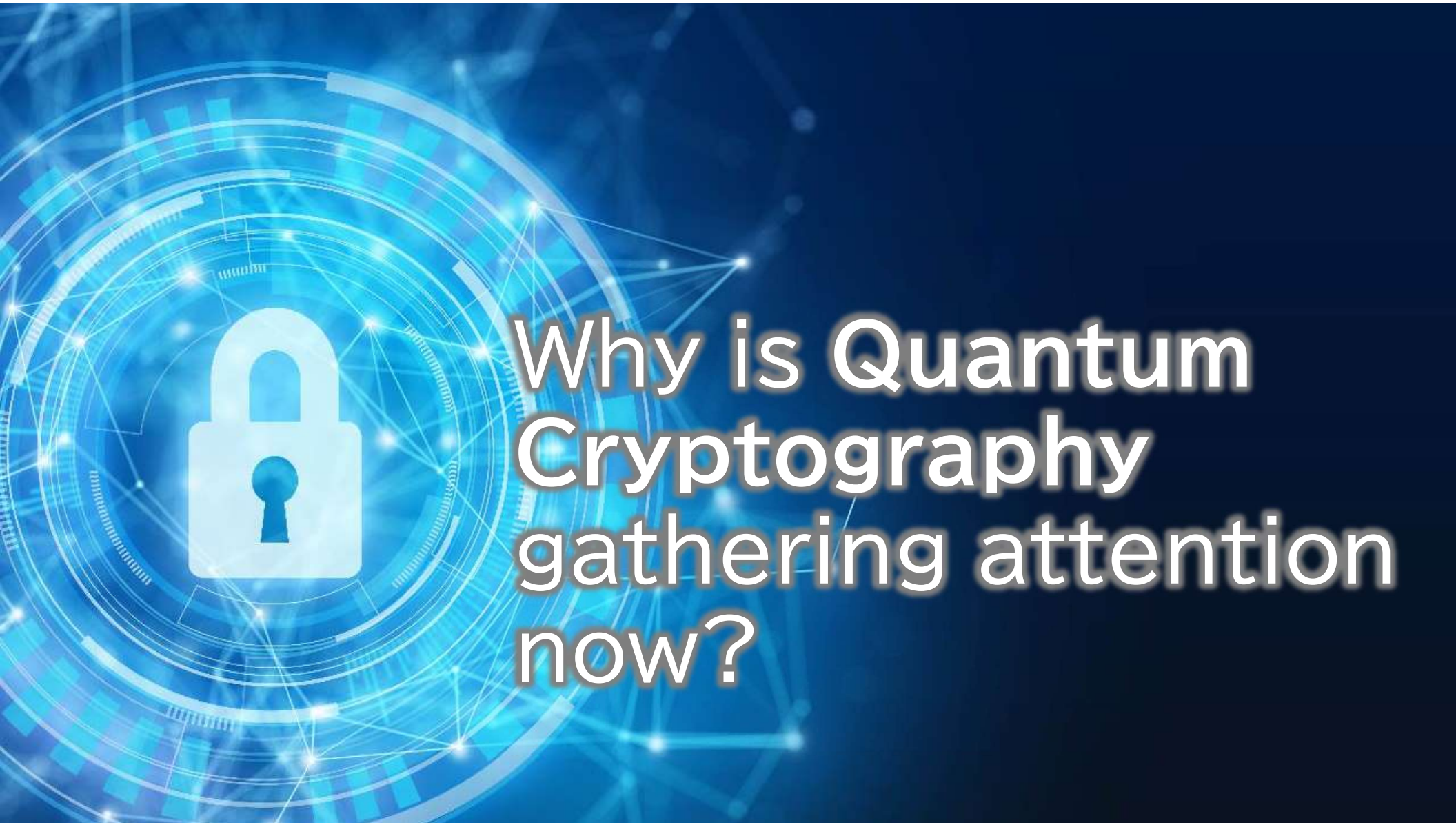
"This first implementation of MCF in submarine networks represents a fundamental milestone towards next-generation systems with larger capacity, more efficient connectivity and lower cost/bit," says Eduardo Mateo, Director of Technology Strategy at NEC.



大容量化の変遷



量子暗号通信


Why is Quantum Cryptography gathering attention now?

海底ケーブルのセキュリティ

意外と簡単な光海底ケーブルの盗聴

光ケーブルの盗聴は、意外といっていいほど簡単にできる。2011年には「光ファイバーの盗聴：その方法と注意点（Optical fiber tapping: Methods and precautions）」（Zafar M. Iqbal/Habib Fathallah/Nezih Belhadj著）という論文が発表されている。また、13年にはエドワード・スノーデンが、英国政府通信本部（GCHQ）の光ケーブルの盗聴の実態やニュージーランドの政府通信保安局（GCSB）が光海底ケーブル「サザンクロス」の盗聴を行っていたことを暴露している。

https://wedge.ismedia.jp/articles/-/30727

海底ケーブルは陸揚げポイントがリスクとなる

基本的に海中でケーブルを盗聴する可能性はほとんど技術的に不可能だという。ただ、リポートは

「海底ケーブルに関する重要な物理的セキュリティの問題のいくつかは、ケーブルが海岸に近づき、データが地上ケーブルに変換されるポイントであるケーブル・ランディング・ステーション(CLS)に接続されるときに発生する」

と指摘している。

米国は実際、米グーグルなどが設置を進めていた米ロサンゼルスと香港を結ぶ太平洋横断海底ケーブルに安全保障上の懸念を表明したことがある。これを受け、グーグルなどは2020年2月、米FCC（連邦通信委員会）に対し、アジア側の陸揚げポイントを香港から台湾・フィリピンに変更するとした。

https://gendai.media/articles/-/115618?page=2

海底ケーブルで相次ぐセキュリティー事案

高まる盗聴・切断リスク　金融取引や遠隔手術に影響も

貴島 逸斗　日経NETWORK

2023.08.29

全2441文字

沖縄近海に敷設された海底ケーブルに盗聴器が取り付けられていた――。複数の報道機関が、在沖縄米軍向け情報誌「This Week on Okinawa」の2023年6月4日号を引用する形で報じている。

盗聴リスクが発生する可能性が最も高いのは、「海底ケーブルの製造工程で盗聴装置を組み込まれること」（慶応義塾大学大学院政策・メディア研究科の土屋大洋教授）だという。製造工程ではなく後付けで盗聴装置を取り付けた場合、光信号は盗み出せても、第三者が通信内容を把握するには、光信号を電気信号に変換する大規模な装置が必要だからだ。加えて、盗聴したい相手のIP（Internet Protocol）アドレスやメールアドレスといった基本情報などを事前に把握していないと、光信号の中から特定のデータを探すのに膨大な手間がかかる。

入札停止は中国リスク警戒か

海底ケーブルに盗聴装置を組み込まれる懸念から、海底ケーブルの入札が停止された例もある。2020年5月まで入札が行われた、ミクロネシア連邦とキリバス、ナ

https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/081800221/

現代暗号の危殆化に伴う量子暗号への期待

量子コンピューティングの進化に対して現代暗号への対策が急務

現代暗号の安全性

【安全性の根拠】　現在の計算機で解読するには天文学的な時間がかかる

量子コンピュータによる

RSAなど現代暗号の危殆化

耐量子計算機暗号

格子暗号

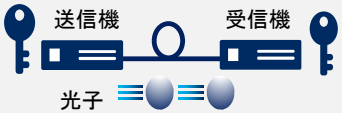
鍵配送

デジタル署名

計算量に基づく安全性（評価中）

- ソフトウェアだけで実現可能
- 量子コンピュータが苦手なアルゴリズムを採用

量子暗号

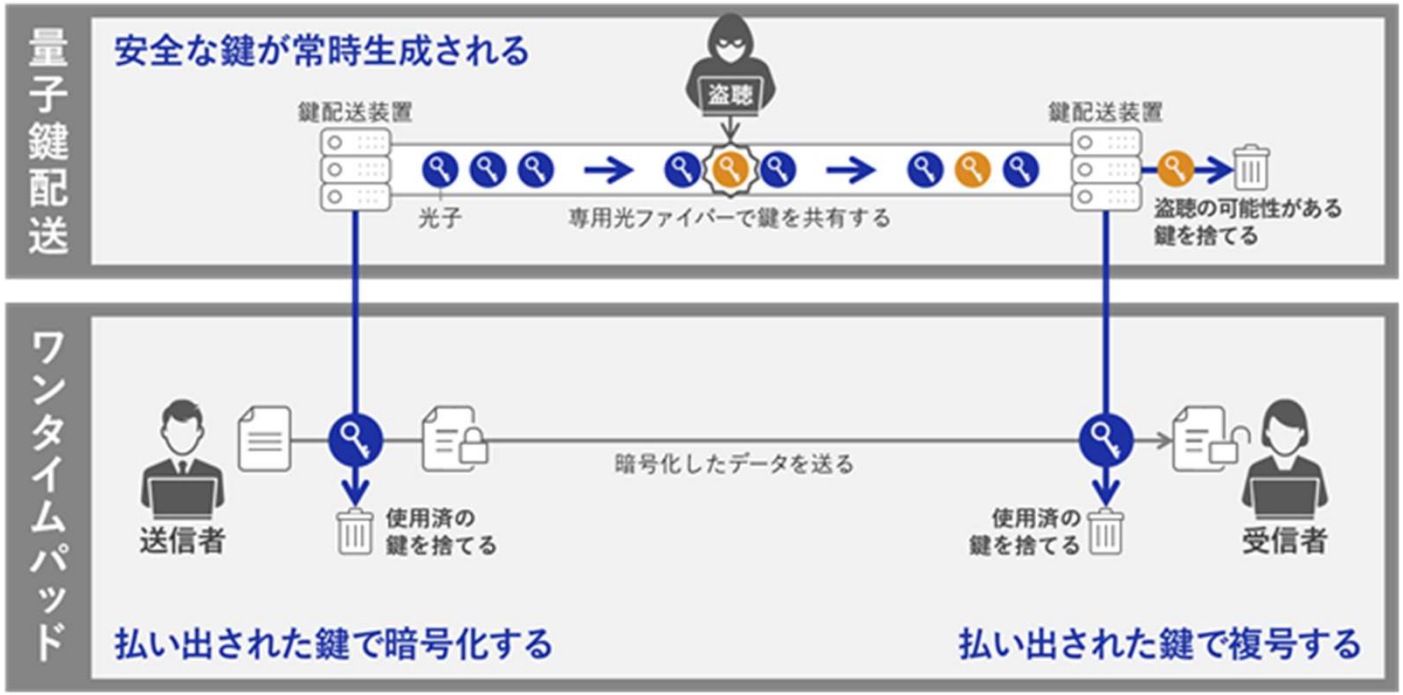


情報理論・量子力学に基づく安全性

- 専用の量子鍵配送装置が必要
- **量子コンピュータ含め未来の計算機でも解読不可**

量子暗号とは

量子暗号＝量子鍵配送＋ワンタイムパッド



量子鍵配送(Quantum Key Distribution)のしくみ

1粒の光子に鍵情報(1bit)をのせて光ファイバ上を伝送
盗聴されていないことが保証された暗号鍵を共有

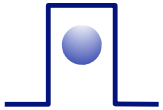
物理法則に基づく
理論的に安全な暗号鍵の共有

メリット1 盗聴者は通信者と同じ鍵情報を取得できない

通常の光通信

多光子(>10,000)/bit
⇒数個盗られても判らない

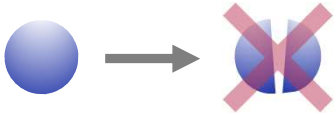
量子鍵配送の光通信



1光子/bit

光子の性質1

量子力学的に、
光子1粒はそれ以上分割できない



▶ **光子(鍵情報)が盗まれると、受信側には鍵情報が届かない ⇒ 暗号鍵に使用しない**

メリット2 盗聴を検知できることで、変化した光子は使用しない

光子の性質2

量子力学的に、
光子は観測すると状態が変化する

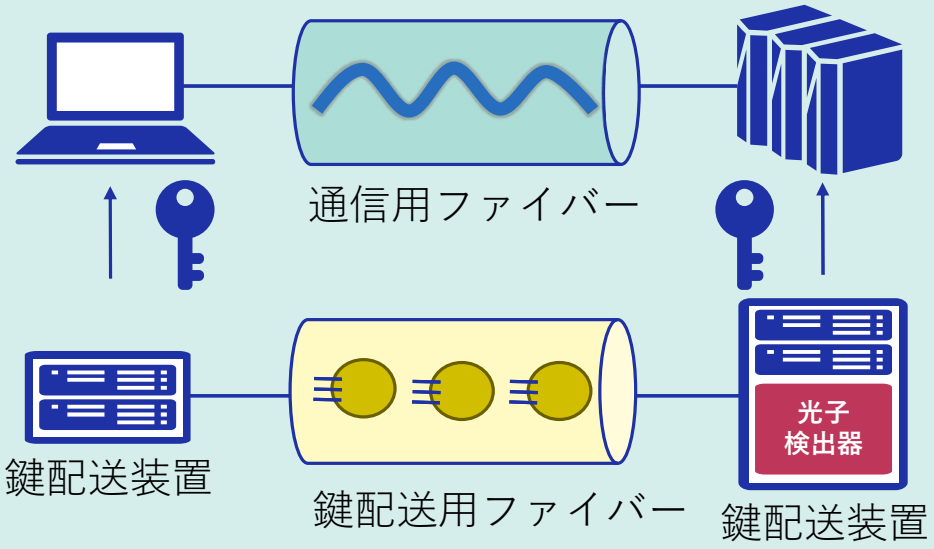
▶ **鍵情報を盗み見ただけで、受信側で盗聴が判る ⇒ 暗号鍵に使用しない**

量子鍵配送を実現する２つの方式

NECは「**BB84方式**」「**CV-QKD方式**」双方の開発を推進

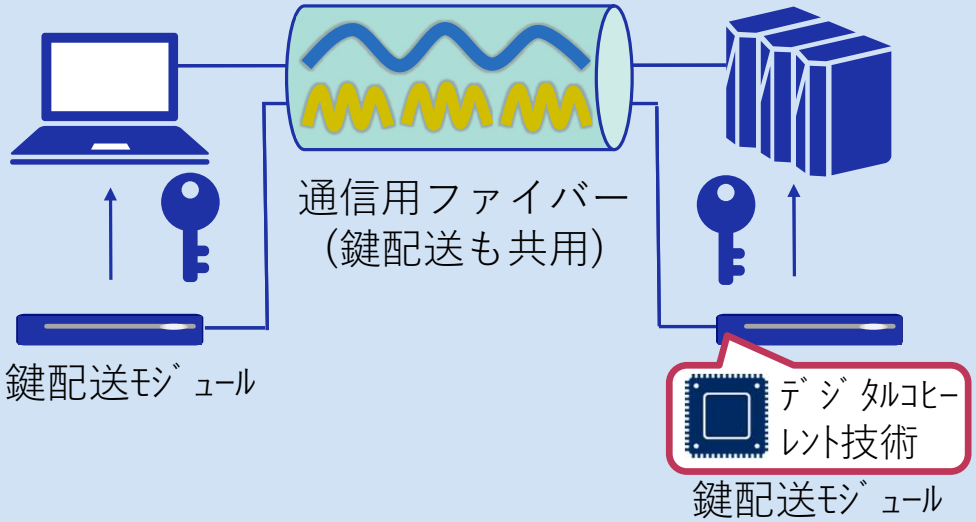
BB84方式(光子検出)

専用光デバイス(光子検出器)が必要
鍵配送専用ファイバーが必要



CV-QKD方式(光波検出)

一般的な通信用光デバイスを活用
鍵配送専用ファイバーが不要




reddot award 2023
winner
Quantum Key
Distribution System
Concept Design
DESIGN
AWARD
2024

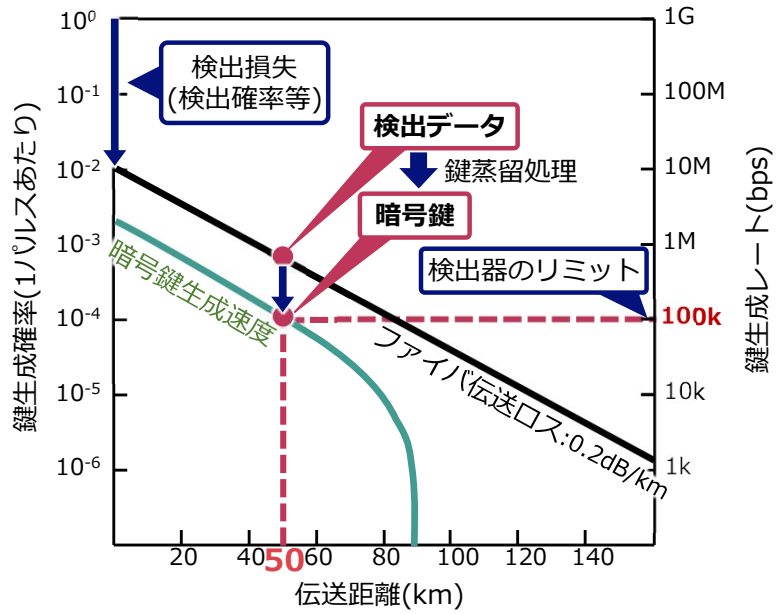
量子鍵配送の速度制限と距離制限

速度制限と距離制限の要因

- **光ファイバの伝送ロス(距離が伸びるほど伝送できる光子が減少)**
- **光子検出性能の限界**
- **無条件絶対安全の追及**

約50kmの通信距離が限度

NEC製QKD装置の性能(1波長あたり)



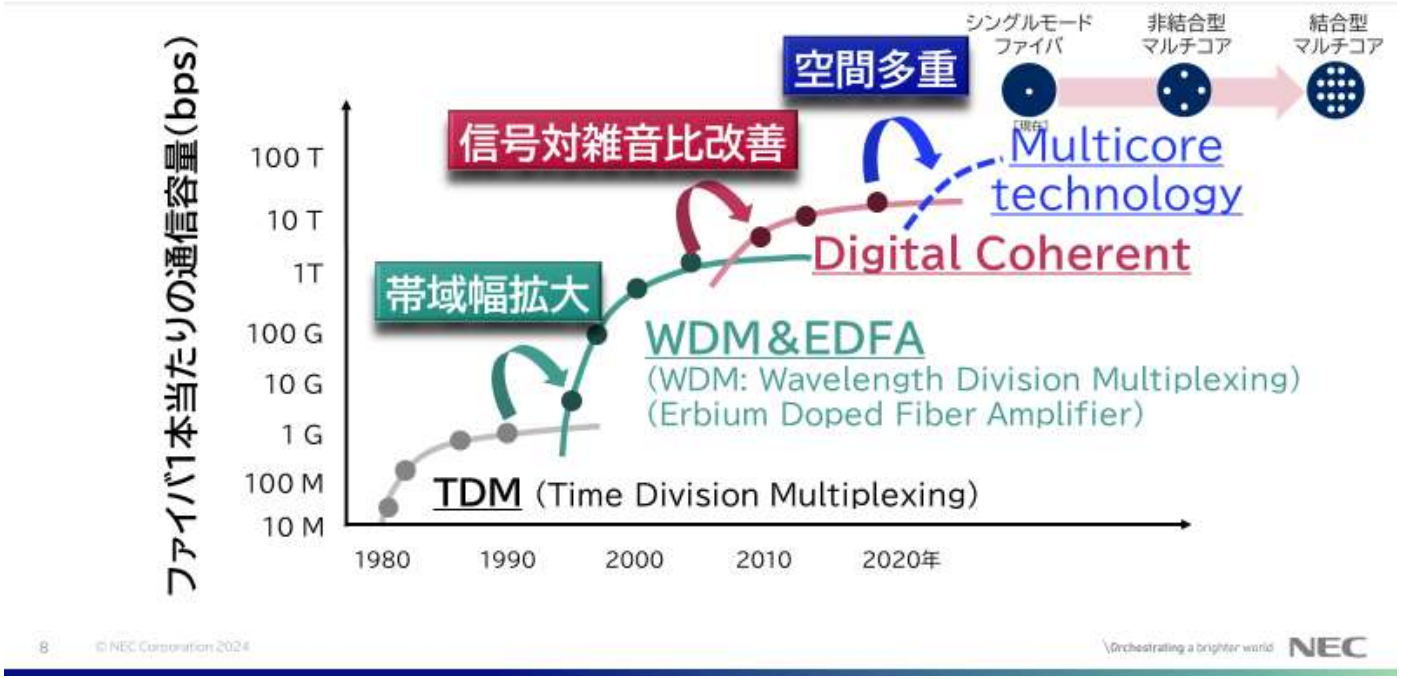
BB84方式における現時点での性能(1波長あたり)

- 距離　：最大50km
- 鍵生成：50～100kbps
  (通信条件により変動)

デジタルコヒーレント技術を活用した超小型CV-QKD

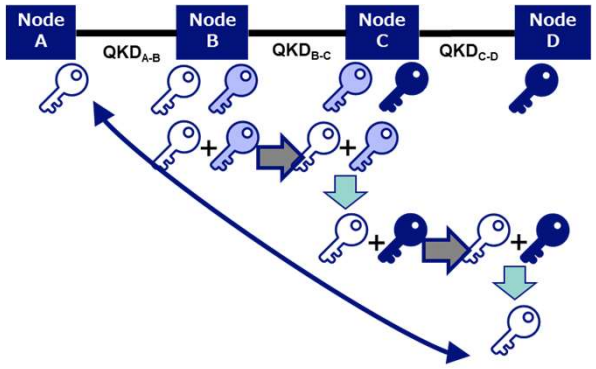
長距離大容量通信で培ったデジタルコヒーレント技術を量子鍵配送に適用し超小型CV-QKDの実現を目指す

大容量化の変遷



デジタルコヒーレント
＋
CV-QKD
↓
超小型化

別途研究開発を進める**鍵リレー技術**により距離制限を解決



\Orchestrating a brighter world