

量子通信におけるイノベーション

慶應義塾大学 政策・メディア研究科 特任准教授
メルカリ R4D シニアリサーチャー
永山 翔太

Global Quantum
Internet

世を革新する技術の発展

半導体
(コンピュータ)

インターネット

AI

量子
(コンピュータ)

分散量子
コンピュータ

量子インターネット

1970~

1990~

2012~

2030?~

2035?~

自己紹介



永山翔太 / Shota Nagayama

- ざっくり言うと: インターネット技術を基礎に量子情報技術をやってきた異色人間
- 博士(政策・メディア)
- 動機: 量子技術の情報システムとしての実現
- 研究テーマ: 量子インターネット・分散量子コンピュータ
- 所属
 - 株式会社メルカリ 研究開発部 R4D シニアリサーチャー
 - 慶應義塾大学 政策・メディア研究科 特任准教授
- **Co-innovation** 活動

mercari
R4D



■MOONSHOT
JSTムーンショット目標6内
「スケラブルで強靱な統合的量子
通信システム」PJ
(プロジェクトマネージャー)



量子コンピューティング



インターネット

量子インターネット

■WIDE PROJECT
80'に東大/慶大/東工大を繋げ、米
国に接続し、日本のインターネットを
開始したコンソーシアム
(ボードメンバー)



■QITF
量子インターネットの多組織連携コンソーシアム
(ファウンダー・代表)



https://www.riken.jp/pr/news/2023/20230324_1/
<https://www.fujitsu.com/global/about/research/technology/quantum/>

量子コンピュータを利用できる「量子計算クラウドサービス」開始

－国産超伝導量子コンピュータ初号機の公開－

English Page

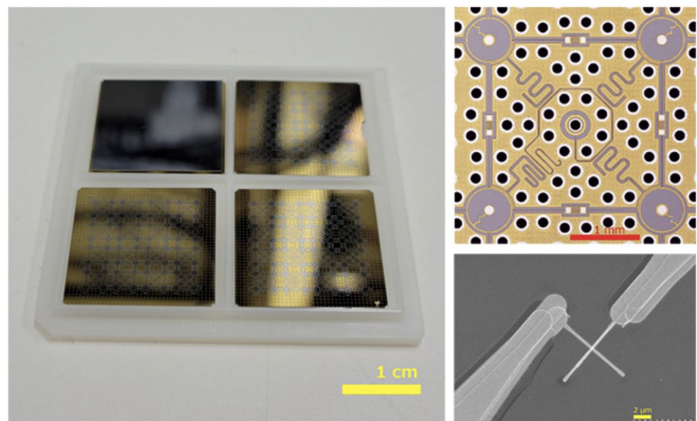


図1 64量子ビット集積回路チップ



最新情報 量子コンピュータ関連情報 量子コンピューティングへの取り組み 何が解決されるのか 技術 研究ロードマップ 量子アプリケーション開拓への取り組み

量子コンピュータ最新情報

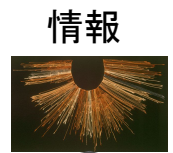
ハイブリッド量子コンピューティングプラットフォーム

富士通は、64量子ビットの超伝導量子コンピュータと40量子ビットの量子シミュレータを連携し、最適な量子計算を可能にするハイブリッド量子コンピューティングプラットフォームを開発しました。富士通は、本プラットフォームを富士通と理研との共同研究を通して、企業や研究機関に提供していきます。

現状の量子コンピュータは量子ビットエラーなどの問題があり、長いステップの計算が正確に行えない課題があります。一方、量子シミュレータは、エラーの問題がないため長いステップの量子計算シミュレーションが実行可能ですが、従来コンピュータ上で量子計算を模擬するシステムであり、量子コンピュータの実現により期待されている計算の加速、いわゆる、量子加速は実現できません。



計算道具の系統図



情報

計算補助



そろばん(紀元前～)
仕組み: 石
動力: 人間

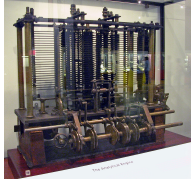


計算尺(17世紀～)
仕組み: 目盛り
動力: 人間

機械式デジタル



パスカルの計算機
(17世紀～)
仕組み: 歯車
動力: 人間



解析機関(19世紀; 未完成)
仕組み: 歯車
動力: 蒸気機関

機械式アナログ



微分解析機(20世紀)
仕組み: 様々
動力: 蒸気機関



連立方程式求解機(1936)
仕組み: プレートの角度

電子式デジタル



ENIAC(1946)
仕組み: 電子式
(真空管)
動力: 電力



IBM System/360
(1964)
仕組み: 電子式(IC)
動力: 電力



今日の一般的な
コンピュータ
(1970年代～)
仕組み: 電子式(LSI)
動力: 電力

計算道具の系統図

情報

量子情報

(古典)情報



計算補助



そろばん



計算尺

機械式
デジタル



パスカルの計
算機



解析機関

機械式
アナログ



微分解析機



連立方程式求解機

電子式
デジタル



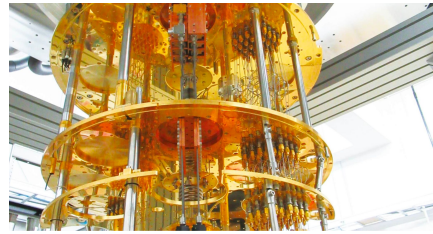
ENIAC



IBM System/360



一般的コンピュータ



計算道具の系統図

情報

(古典)情報



計算補助



そろばん



計算尺

機械式デジタル



パスカルの計算機



解析機関

機械式アナログ



微分解析機



連立方程式求解機

電子式デジタル



ENIAC

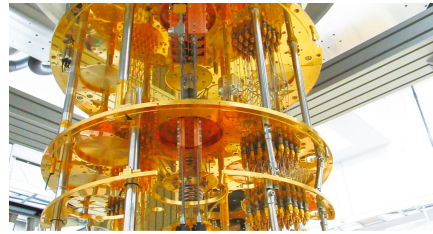


IBM System/360



一般的コンピュータ

量子情報



情報表現はアナログ(しかも複素数)だけど、エラー管理はデジタルにできる**不思議**コンピュータ

※ただし、このアナログ量を直接outputできるわけではない

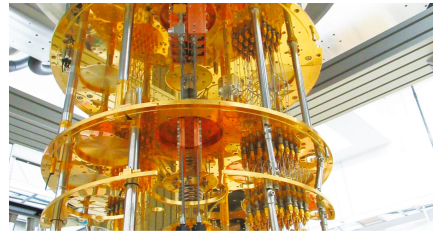
計算道具の系統図

情報

(古典)情報



量子情報



計算補助



そろばん



計算尺

機械式
デジタル



パスカルの計算機



解析機関

機械式
アナログ



微分解析機



連立方程式求解機

電子式
デジタル



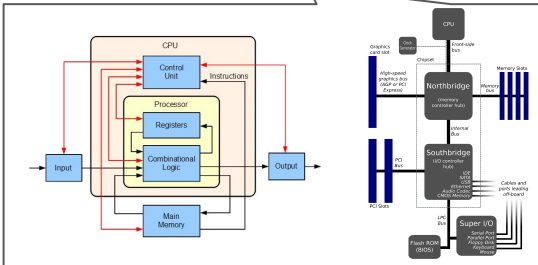
ENIAC



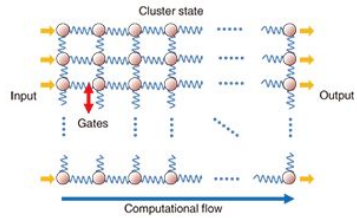
IBM System/360



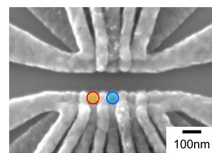
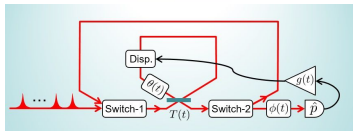
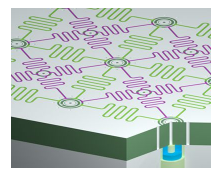
一般的コンピュータ



光量子ビット



固定タイプの量子ビット



https://www.jst.go.jp/erato/nakamura_mqm/project_overview/p01.html

https://www.riken.jp/press/2020/20200325_2/index.html#note10

<http://www.takedalab.t.u-tokyo.ac.jp/research/>

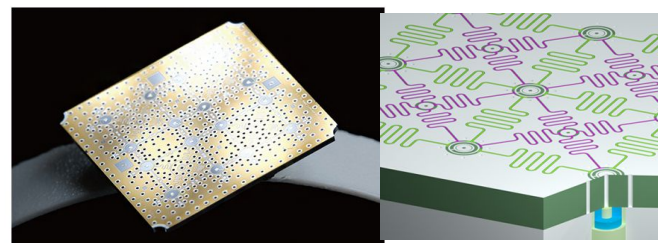
<https://www.nit-review.jp/archive/nittechnical.php?contents=ntr201107ra1.html>

量子コンピュータとは

- 量子力学(に基づく情報科学)で作られたコンピュータ

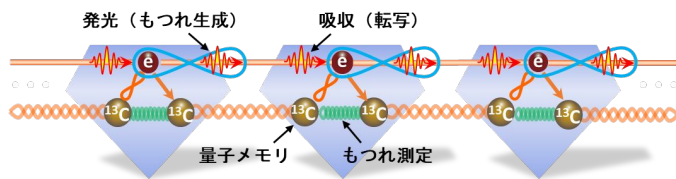
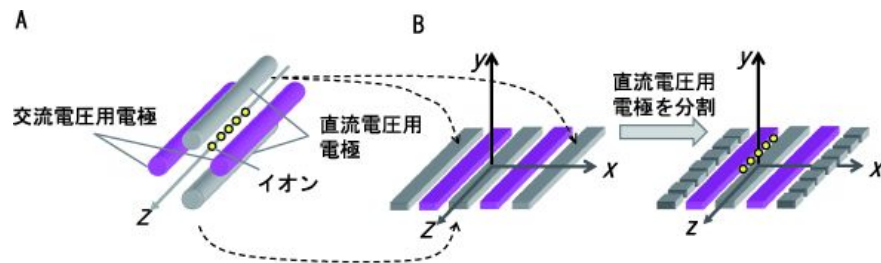
⇔ 古典力学(に基づく情報科学)で作られたコンピュータ(いわゆるデジタルコンピュータ)

量子コンピュータの素子

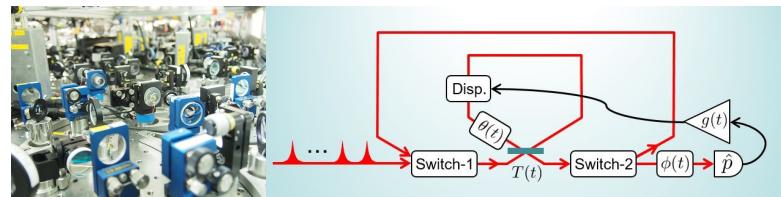


ゲート型・アニーリング型といった計算方法の種別の他に、素子の種別もある
(ゲート処理速度や寿命などが異なる)

- 超伝導型
- イオン型
- 光型
- ダイヤモンドNV-center型
- 単一原子型
- 集団原子型
- 希土類型



など



https://www.jst.go.jp/erato/nakamura_mqm/project_overview/p01.html
https://www.riken.jp/pr/closeup/2021/20210531_1/index.html
<https://www.nict.go.jp/quantum/about/iontrap.html>
https://www.u-tokyo.ac.jp/adm/fsi/ja/projects/quantum/project_00005.html
<https://kosaka-lab.ynu.ac.jp/news.html>

(違いの一例) 現行コンピュータとは情報処理の進め方が異なる

Jones et al. Phys. Rev. X 2, 031007. 2012.

- 現行計算機: 物體的な回路の入力線にデータや制御信号を流し込み、出力線から結果を得る
→データを移動させて、固定された回路を通して情報処理する
- 量子計算機: 物體的な量子ビットにレーザーパルス等を当てて状態を変化させるのが量子回路
→回路(を構成するゲート操作の集団)のほうで固定された量子ビットまでやってくる

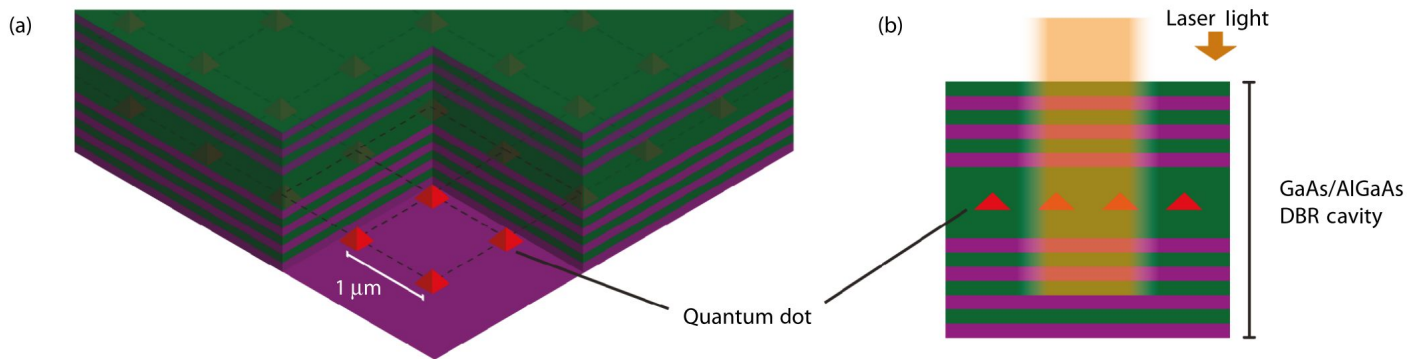


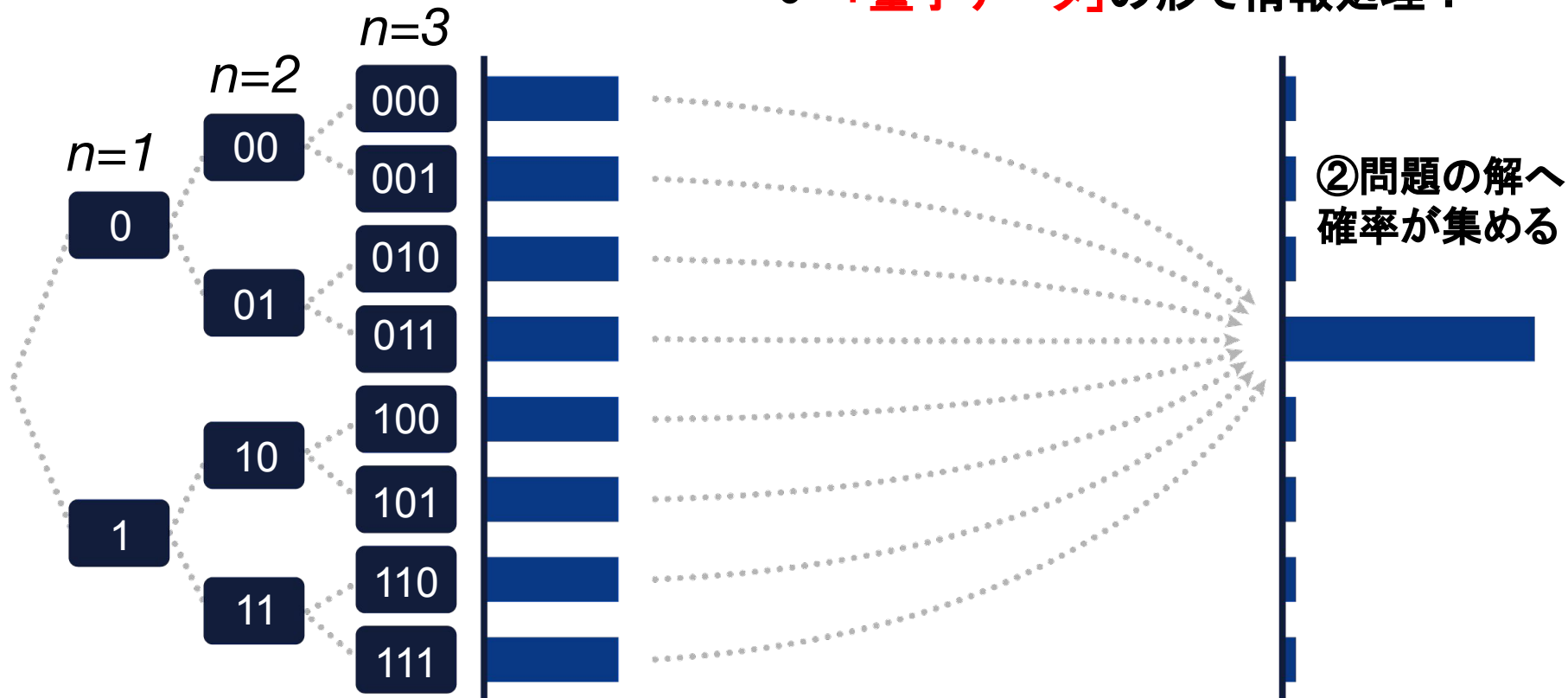
FIG. 3. Quantum dots in a planar optical microcavity form the basis of the QuDOS hardware platform. (a) The quantum dots are arranged $1 \mu\text{m}$ apart in a two-dimensional square array. The quantum dots trap single electrons, whose spins will be used for quantum information processing. (b) Side view. The electron spins are manipulated with laser pulses sent into the optical cavity from above, and two neighboring quantum dots can be coupled by a laser optical field that overlaps them. The purple and green layers are AlGaAs and GaAs, grown by molecular-beam epitaxy. The alternating layers form a distributed-Bragg-reflector (DBR) optical cavity which is planar, confining light in the vertical direction and extending across the entire system in horizontal directions.

量子コンピュータの大別

種別	量子アニーラ (アニーリング型 量子コンピュータ)	(ゲート型)量子コンピュータ	
		NISQ量子コンピュータ	誤り訂正型量子コンピュータ
実現時期	2011年～ R&D向けの商用販売・ クラウドアクセス開始	2014年～ R&D向けクラウドアクセス開始	2030年～？
やれること	組合せ最適化問題	化学計算や金融計算が有力	<ul style="list-style-type: none">● 量子シミュレーション<ul style="list-style-type: none">○ 創薬・材料開発など● 問題の構造を利用<ul style="list-style-type: none">○ 素因数分解・離散対数問題・パターンマッチング・半正定値計画問題(近似)など● 逆関数計算<ul style="list-style-type: none">○ 検索(とよく言われる)
目下の課題	システムの大規模化 キラーアプリ探索	システムの大規模化 キラーアプリ探索	誤り訂正の実現

量子コンピュータとは

- n 量子ビットは 2 個の状態を持つ
- 「量子データ」の形で情報処理！

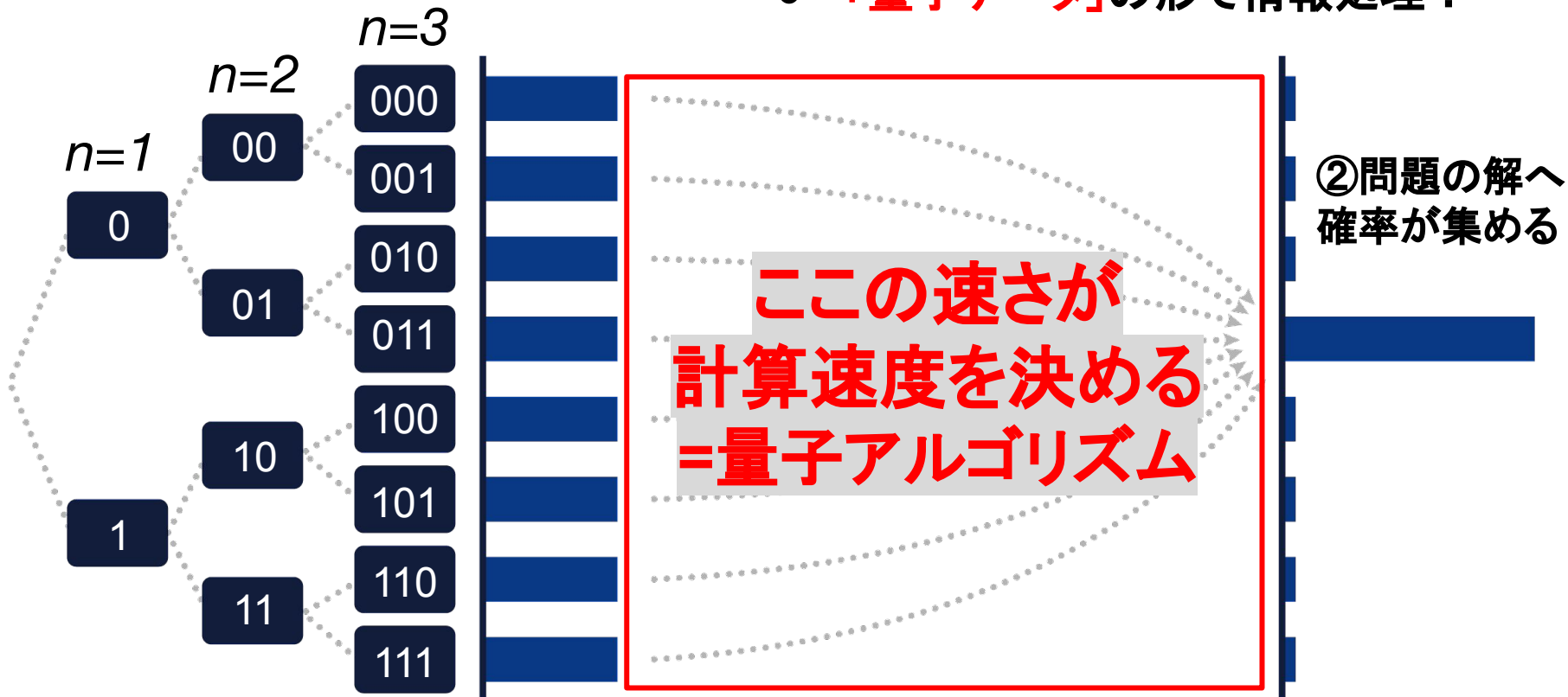


①各状態が出現確率を持っている

②問題の解へ
確率が集める

量子コンピュータとは

- n 量子ビットは 2^n 個の状態を持つ
- 「量子データ」の形で情報処理！



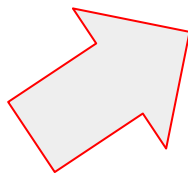
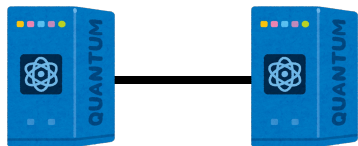
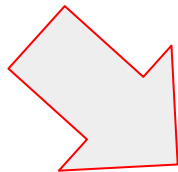
①各状態が出現確率を持っている

分散量子コンピュータ

10量子ビット: 2^{10} = 約1000個の候補の中から解を高速に見つけ出す

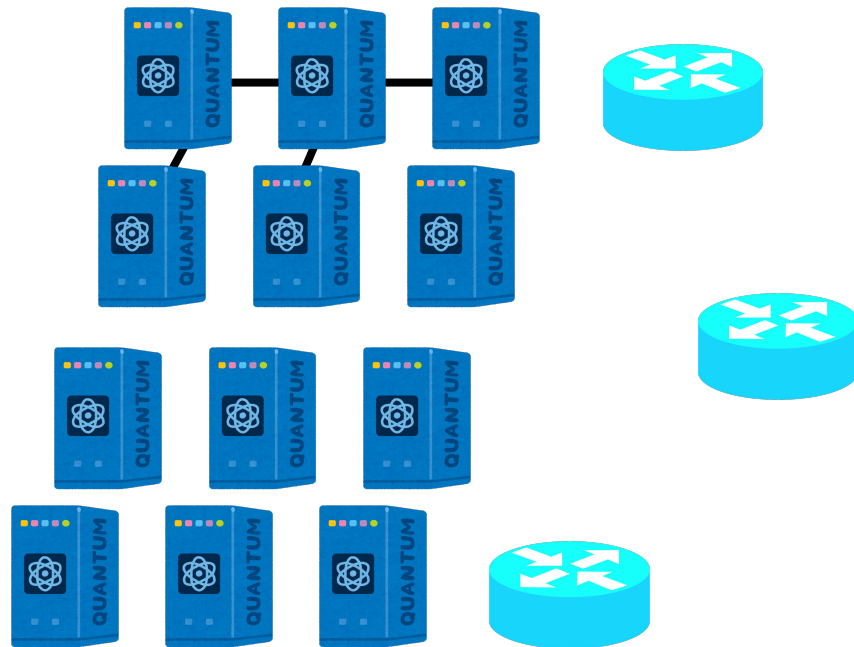


量子ネットワーク化！
=「量子データ」で繋ぐ



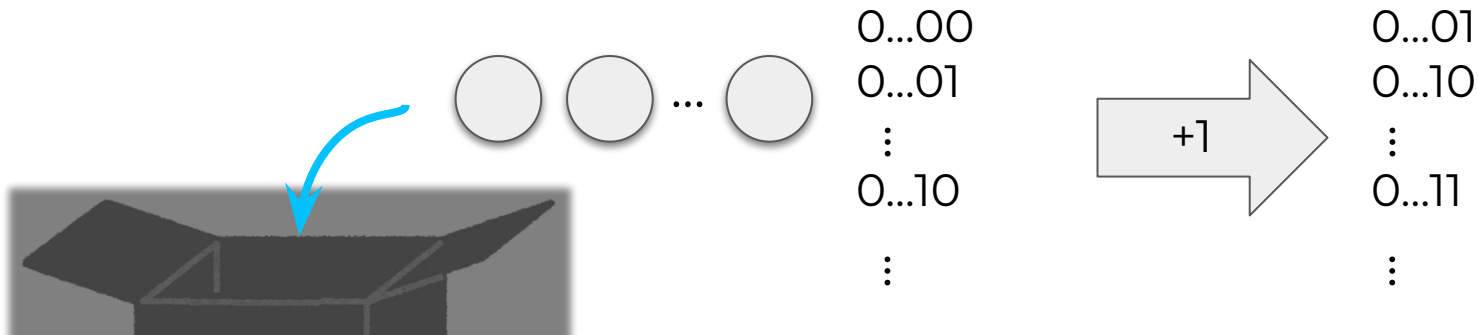
10+10量子ビット: 2^{20} = 約100万個の候補の中から解を高速に見つけ出す

もっとたくさん使いたい！



量子コンピュータの計算方法

- 並列計算とよく言われる
- 実際のところは？



たしかに、並列に計算はできる。

ただし、目的の解だけを取り出すことが難しい。

→この困難要因の克服数法が存在する手続きが量子アルゴリズム
(と、対応する問題)

I 量子コンピュータにとって何がキツイか

1. エラー
2. エラー
3. エラー

計算機の歴史的には

- 歯車: 角度がズれる
- 電気: 逃げる、
もしくは飛んでくる(電波ノイズ)

とにかく、計算機の歴史はエラーとの戦い

I NISQ量子コンピュータ

- Noisy Intermediate-Scale Quantum 技術
 - エラーのある、中規模(50~100量子ビット)の量子効果を利用する技術
- NISQ量子コンピュータ=エラーが発生する前に計算を終えようという発想

シミュレーションできない領域

・50量子ビットのシミュレーション → ペタバイトレベルのデータを高速に処理する必要がある

何かしら利用可能だろうという期待

・キラーアプリ探索が盛ん → 化学計算・金融計算など

エラー訂正あり量子コンピュータ

- 量子コンピュータの本命
- エラー管理
 - エラー訂正するので問題なし
- 用途(多岐)
 - 量子の性質をそのまま使う: 超多項式的加速
 - 量子シミュレーション → 創薬、材料開発
 - 問題の構造をexploit: 超多項式的加速
 - 素因数分解、離散対数問題、パターンマッチング、半正定値計画問題(近似)、逆行列計算、etc.
 - 汎用的に干渉を取り扱う: 多項式的加速
 - 逆関数計算(検索)、etc.
- メルカリでの生の声(例)
 - 「逆行列計算 $\log(N)$ ができるのすごい」
 - 「逆行列計算の高速化ができるといろいろ便利 ...より興味が増した！」

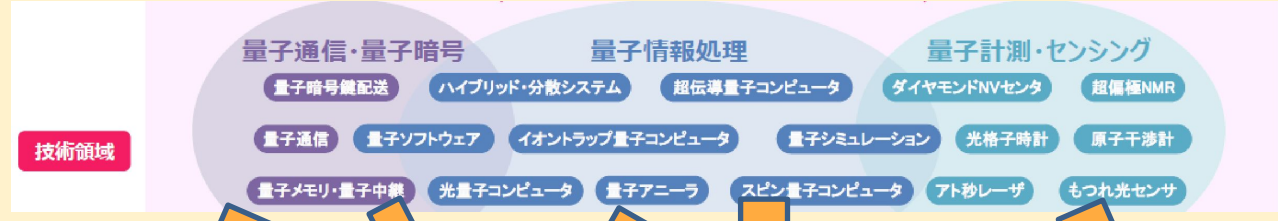


量子通信

量子インターネットとは、量子情報のネットワーク化

概要

統合イノベーション戦略推進会議「量子技術イノベーション戦略(最終報告)」より



ネットワーク化で、様々な新技術が可能に

量子データ通信、デジタルインターネットを2Eに量子で守る、広範囲量子センサーネットワーク、など

- ・リーダー選挙、ビザンチン問題、量子ビットコイン、量子認証、量子鍵配送、etc.
- ・秘匿量子計算
- ・分散量子計算
- ・超高精度時刻同期
- ・超長基線電波望遠鏡
- ・ネットワーク量子センシング

「量子インターネット」=本格的な量子技術時代のコンピュータ・ネットワーク基盤

従来のインターネットが計算機・センサーなどを繋ぎ始めて新たな領域に。
→ 量子技術・情報をネットワーク化する技術分野の創出 も自然な流れ

➡ **社会実装: 量子技術・情報の広域通信プラットフォーム**

他の量子通信技術との違い

量子技術による **量子データ伝送ネットワーク**
=量子インターネット

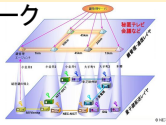
※E2E暗号



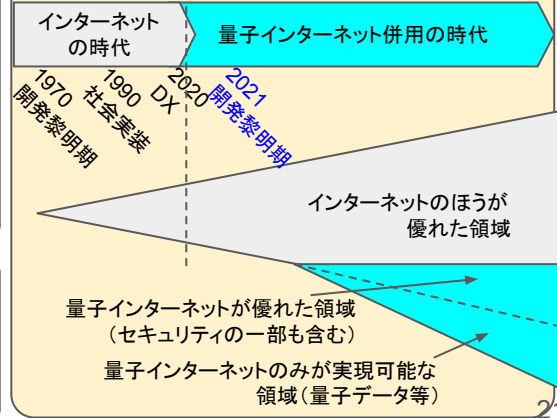
量子技術による **デジタルデータ (=暗号鍵) 伝送ネットワーク**
=量子暗号ネットワーク
(総務省推進)

※E2E暗号ではない

画像出典 <https://www.nict.go.jp/press/2010/10/14-1.html>



情報通信市場への広がり



出口

- インフラ: 光ファイバー事業者、接続事業者
- ハードウェア: 通信機器・メモリ等部品、etc.
- ソフトウェア・(直接的)サービス: クラウド量子コンピュータとの量子接続、量子IoT、量子計測・同期、量子セキュリティ基盤 (E2Eの量子暗号に加え、認証・秘匿計算)、など



Global Quantum
Internet

目指す社会像(2050年): 量子コンピュータネットワークによる、世界中で量子データが自由に生み出され、流通し、自在に処理される “Advanced” Society 5.0

社会実装

微弱信号センシング ・巨大分子の創薬シミュによる医療新時代	材料革命による高効率エネルギー・脱炭素・高機能材料・物流革命	世界規模の金融計算による経済危機ゼロ社会	真に安心・安全で高速・正確な新・情報社会	医療・防災など多様な環境のあらゆる信号のセンシングによる超高度予測社会	次世代情報処理が実現するイノベーション加速による新・科学技術/情報技術立国
----------------------------------	--------------------------------	----------------------	----------------------	-------------------------------------	---------------------------------------

など、「量子前提」が可能にする新社会の実現

量子情報の生成・流通・処理基盤が必要=量子ネットワークによる、分散量子コンピュータ・量子インターネット

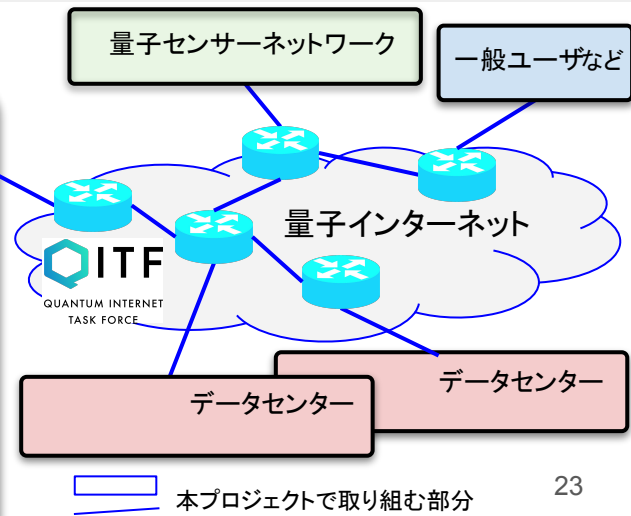
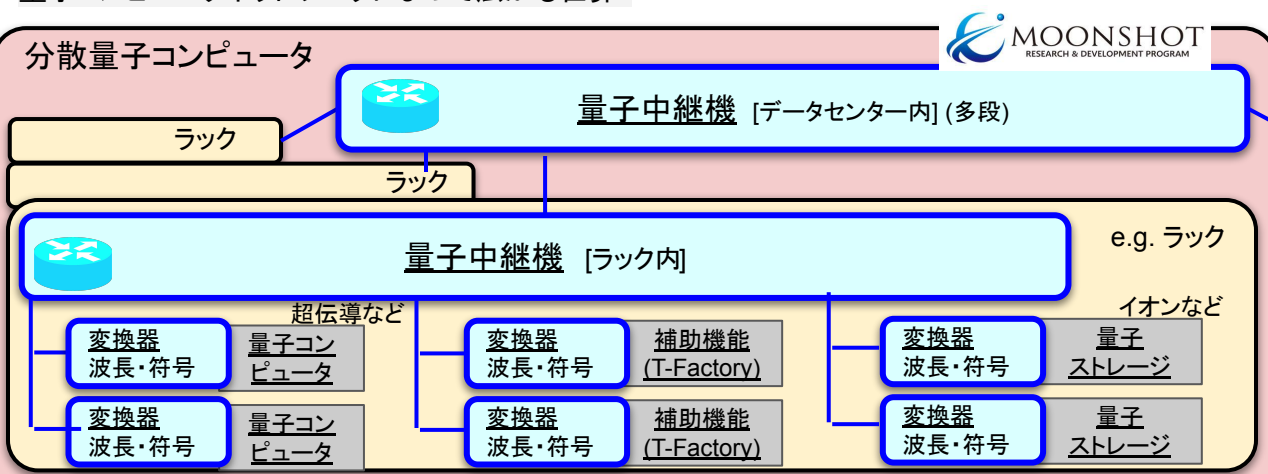
プロダクト

分散型量子コンピュータ
(ラック内/一台の量子中継機)
/周辺拠点から量子通信で利用

分散型量子コンピュータ
(データセンター内/多数の量子中継機)
/離れた拠点からの量子通信による利用

分散型量子コンピュータ
(多数のデータセンター連携)
/量子インターネットの普及

量子コンピュータネットワークによって広がる世界



世界の量子インターネット施策と特徴

QuTech 量子インターネット部門

- 量子インターネットに加え、分散量子コンピュータネットワークを視野に
- 2022年後半から7年間の新プロジェクト(QIA)
 - 最初の3.5年で2400万ユーロ(約35億円)
 - (2018~2021年:1000万ユーロ(約14.5億円))
- **強み:** HWの実装が早い。
- システムチームがHWを使えるのは2週間/年
- 量子信号中継実証(ダイヤモンド量子ビット(2021)・リンクプロトコル実証(2022))
- 量子ネットワークOS提案: 初期概念のみ(2023)

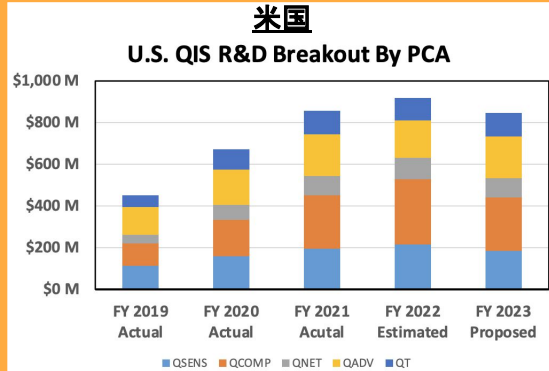
中国

- 全光量子中継を阪大に次いで実証
- 原子集団による確率的量子中継実証
- Qike Quantumの分散量子計算研究
- 衛星もつれ配送の実証 など



QUANTUM INTERNET TASK FORCE

- メモリ技術ダイバーシティ
- インターネット研究・運用の知見を生かしたトップダウン型研究に強み
- 人材は必要分野に広く薄く (教育が今後の鍵)

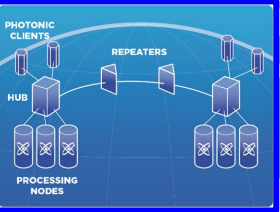


(画像出典: NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2023 BUDGET)

- 政府: 2020年に量子NWIに注力開始
- **国家量子イニシアチブ法の改定で量子ネットワーク予算を大規模追加 (1億ドル(約150億円)/年; 5年間)**
- **科学技術情報局レポート: A Roadmap for Quantum Interconnects (2022年)**
- **IONQが量子通信ベンチャーを買収、分散処理の体制構築 (2023年)**
- **IBMは、長距離量子通信に強いシカゴ大学と連携して、量子ネットワーク化による0万量子ビットを目指す(次ページ)**
- 他、DoE・NSF・NIST等が量子インターコネク트에研究開発投資

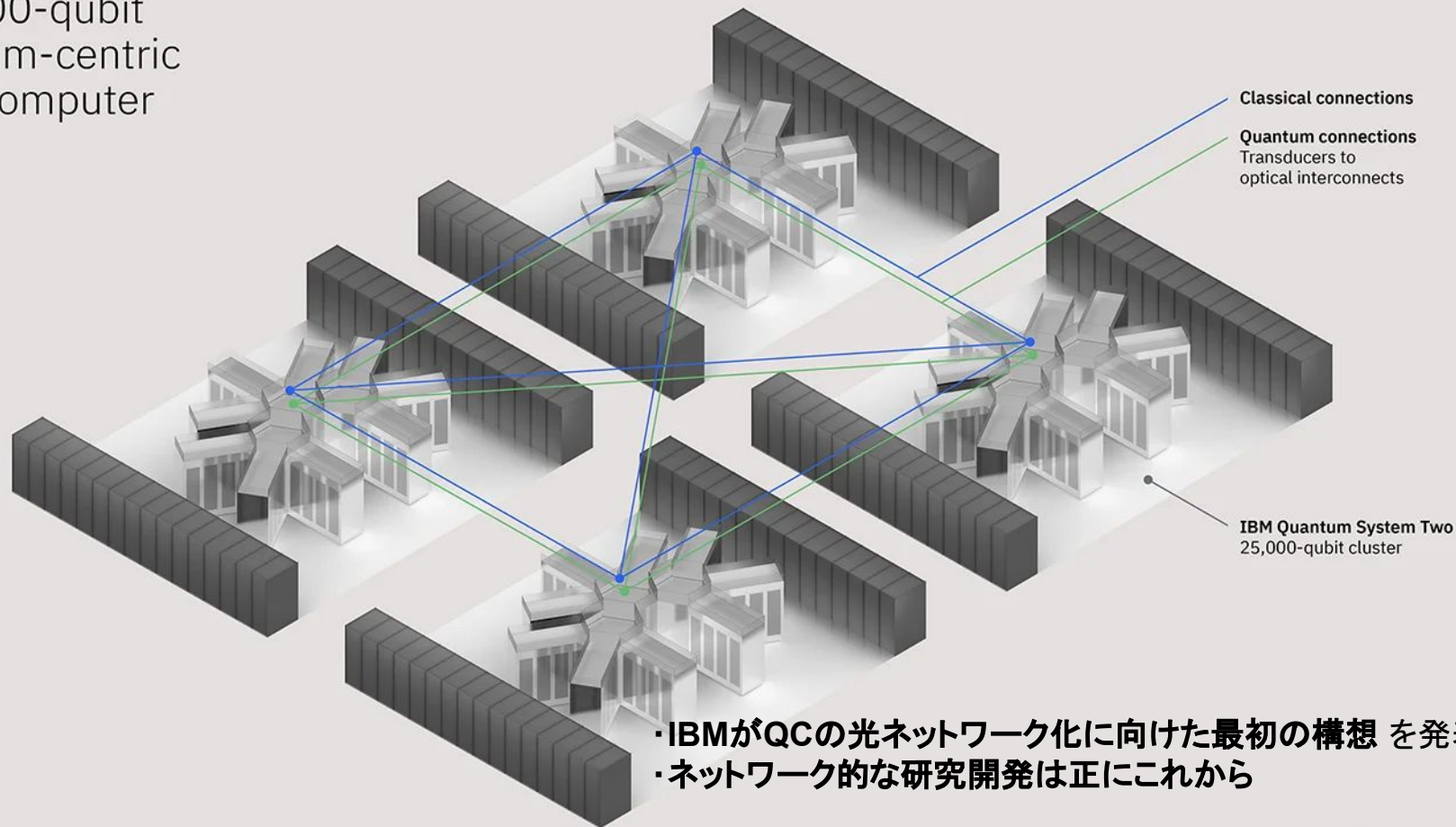
オーストリア

230mイオントラップ間接続 by インスブルック大学



100,000-qubit
quantum-centric
supercomputer

—
2033



- ・IBMがQCの光ネットワーク化に向けた**最初の構想**を発表
- ・ネットワーク的な研究開発は正にこれから

メディア露出・実績など

日本経済新聞に掲載。全日本の量子インターネットテストベッドの取り組みとして。

- [日本経済新聞電子版](#) 2021/3/5
- [日本経済新聞朝刊](#) 2021/3/8

日経クロステックに掲載。

- [突発、量子ネット大戦](#) 2021/5/19

[量子インターネットホワイトペーパー執筆・公開](#)

[量子インターネットの設計指標に係る文書の共同執筆@IRTF](#)

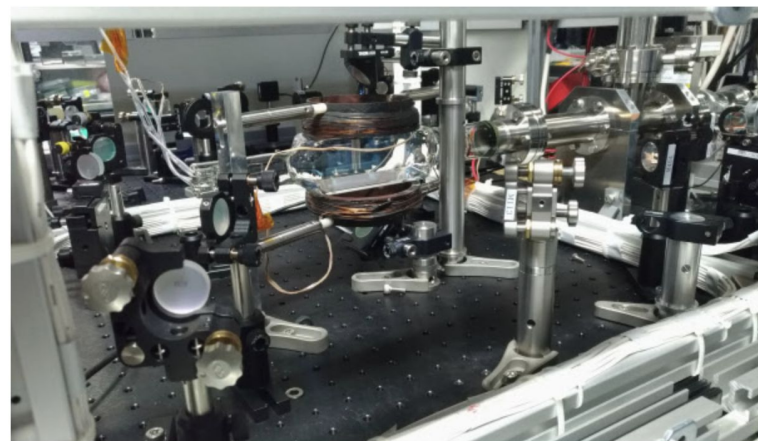
- IRTFは、TCP/IPやHTTP等を定めた標準化団体 IETF の姉妹組織。長期的な課題に取り組む。

- インタフェースWG ([2020年9月発足](#))
- テストベッドWG ([2020年12月発足](#))
- 総会(2019年5月発足)
- 他、勉強会・研究会など開催
- 応用物理学会 研究会「量子技術ホライズン—量子物理から量子インターネットを展望する」を共催
- など

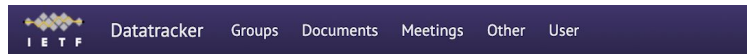
量子でネット安全性堅固に メルカリ・東大など試験計画、不正侵入を完全防止

日経新聞朝刊 2021/3/8

2021年3月8日 2:00 [有料会員限定]

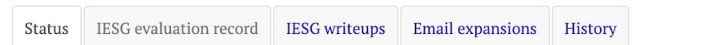


量子インターネットは安全性がより高まる=阪大提供



Architectural Principles for a Quantum Internet

draft-irtf-qirg-principles-04



量子インターネットのホワイトペーパー

ホワイトペーパー

“The” 量子インターネット

-この宇宙の物理法則に許されるサイバー空間の極致-

産官学連携研究開発コンソーシアム
量子インターネットタスクフォース



執筆体制

主筆	永山翔太	株式会社メルカリ	シニアリサーチャー
	生田力三	大阪大学	助教
	小坂英男	横浜国立大学	教授
	佐々木寿彦	東京大学	講師
	高橋優樹	沖縄科学技術大学院大学	准教授
	根本香絵	国立情報学研究所	教授
	堀切智之	横浜国立大学	准教授
	山崎歴舟	国際基督教大学	准教授
	山本俊	大阪大学	教授
	Rodney Van Meter	慶應義塾大学	教授

<https://qitf.org/news/20210210-whitepaper/>

RFC9340!!!

This first document (not even standards track) took four years.

初の量子インターネット(量子通信)
概念の仕様書の策定には、
4年間かかった。

Stream: Internet Research Task Force (IRTF)
RFC: 9340
Category: Informational
Published: January 2023
ISSN: 2070-1721
Authors: W. Kozlowski, S. Wehner, R. Van Meter, B. Rijsman
QuTech, *QuTech*, *Keio University*, *Individual*
A. S. Cacciapuoti, M. Caleffi, S. Nagayama
University of Naples Federico II, *University of Naples Federico II*, *Mercari, Inc.*

RFC 9340 Architectural Principles for a Quantum Internet

Abstract

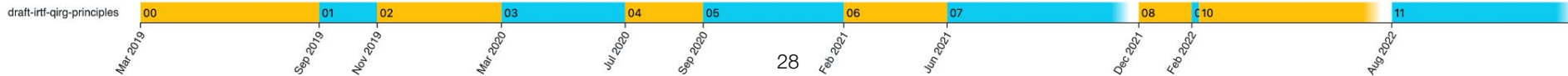
The vision of a quantum internet is to enhance existing Internet technology by enabling quantum communication between any two points on Earth. To achieve this goal, a quantum network stack should be built from the ground up to account for the fundamentally new properties of quantum entanglement. The first quantum entanglement networks have been realised, but there is no practical proposal for how to organise, utilise, and manage such networks. In this document, we attempt to lay down the framework and introduce some basic architectural principles for a quantum internet. This is intended for general guidance and general interest. It is also intended to provide a foundation for discussion between physicists and network specialists. This document is a product of the Quantum Internet Research Group (QIRG).

Architectural Principles for a Quantum Internet draft-irtf-qirg-principles-11

Status [IRSG evaluation record](#) [IESG evaluation record](#) [IESG writeups](#) [Email expansions](#) [History](#)

Versions:

00 01 02 03 04 05 06 07 08 09 10 11

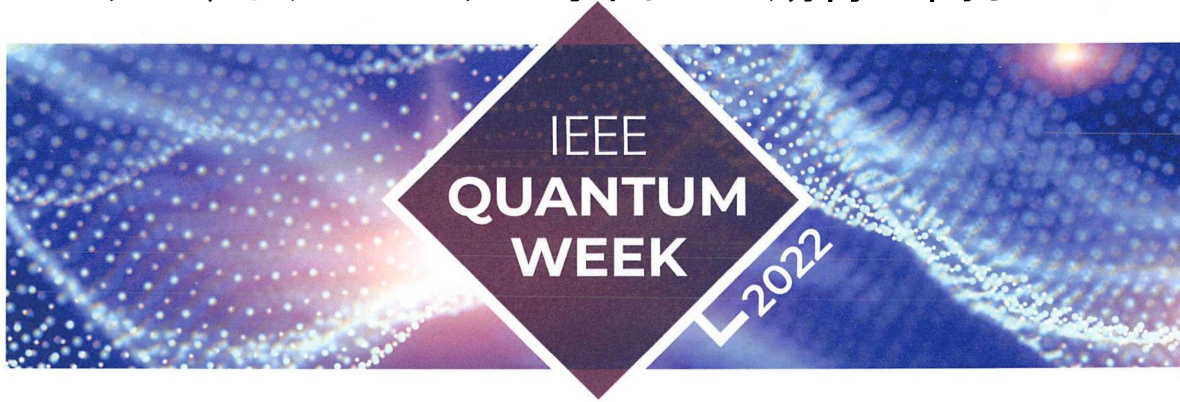


Architectural Principles for a Quantum Internet

アブスト & イントロ

- アブスト
 - 量子通信を地球上の任意の 2地点間で
 - 量子もつれのための量子ネットワークスタックが必要
 - how to organise, utilise, and manage such networks.
 - このメモでは、フレームワーク起工とアーキテクチャ概念紹介をおこなう
 - 一般的ガイダンスや興味のため
 - **また、物理学者とネットワークスペシャリストを繋げ、議論できるようにするため**
- イントロ
 - 量子現象を使ったネットワーク
 - 発展度合いによって、光子を用意して送って測定するだけのものから、量子コンピュータ・ネットワークまである
 - 現行インターネットを replaceするものではない
 - 問題意識
 - 実際に作られた、ネットワークの動かし方の提案がない
 - デバイス同士を繋げるにも、送受信、バッファ管理、コネクション同期などに関するインタフェースがない
 - 量子状態を送る物理的メカニズムは存在するが、ロバストなプロトコルがない
 - つまり、システム！

量子ネットワークの、ネットワーク工学面への期待が高まっている



BEST PAPER AWARD

Presented to

**Ryosuke Satoh, Michal Hajdušek, Naphan Benchasattabuse, Shota Nagayama,
Kentaro Teramoto, Takaaki Matsuo, Sara Ayman Metwalli, Poramet Pathumsoot,
Takahiko Satoh, Shigeya Suzuki, and Rodney Van Meter**

Track: Quantum Networking and Communications

Paper Title: QuISP: a Quantum Internet Simulation Package



Greg Byrd
QCE22 General Chair
NC State University



Bert de Jong
QCE22 Program Chair
Lawrence Berkeley National Laboratory



Hausi Müller
QCE22 Finance Chair
QCE22 Workshops Co-Chair
Co-Chair Quantum Initiative
University of Victoria



Stephan Eidenbenz
QCE22 Workshops Co-Chair
Los Alamos National Laboratory

sfc-aqua / RuleSetSpec

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

RuleSetSpec Public

main 1 branch 0 tags

Go to file Add file Code

Chibikuri added explanation for ruleset termination bd11d21 on Jun 2 54 commits

- img added ruleset execution specification 3 months ago
- rfc-spec added connection setup and teardown 2 months ago
- 1.Overview.md updated structures 2 months ago
- 2.0.Specifications.md fixed explanation last month
- 2.1.ConnectionSetupSpec.md added explanation for ruleset termination last month
- 2.2.RuleSetSpec.md fixed explanation last month
- 2.3.RuleSetExecutionSpec.md added sequence diagram 3 months ago
- 2.4.DataStructures.md added sequence diagram 3 months ago
- 3.Examples.md added instructions for actions 3 months ago
- 4.References.md added condition clausez 3 months ago
- CHANGELOG.md added first table of contents 3 months ago
- Discussions.md updated explanation 2 months ago
- Notes.md updated table of contents 2 months ago
- README.md updated structures 2 months ago

README.md

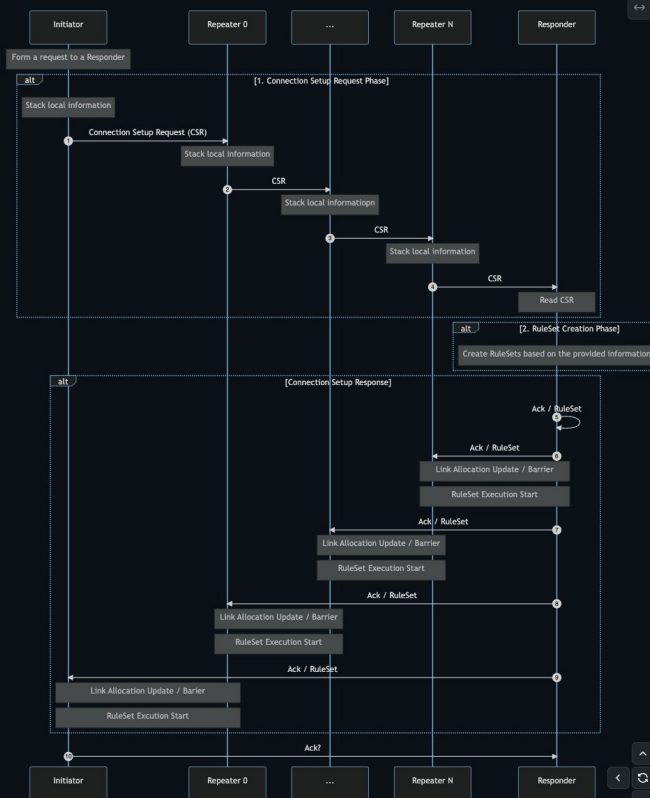
Specification

Specification for Connection Setup (Teardown) and RuleSet

4.9 Connection Setup Example in single network

The following diagram shows a full example of connection setup.

Sequence diagram



Internet Engineering Task Force (IETF)

Internet Research Task Force (IRTF)

- IETF: Standardization organization for the Internet (TCP/IP, http, etc.)
- IRTF: Corresponding research organization
- 116th meeting 2023/3/27-31 @Yokohama, Japan
 - Quantum Internet Research Group meeting in IRTF
 - Host Speaker Series
 - “The Future & Roadmap to the Quantum Internet - Testbed Efforts in Japan -”
 - Shota Nagayama & Rodney Van Meter
 - more than 10% of participants (top classical network specialists) of IETF/IRTF joined the session.
 - Quantum Internet Lab Tour to Yokohama National Univ.
 - <https://ietf116.jp/tour/>

物理工学EP・工学研究院
横浜国立大学 堀切研究室
Horikiri Lab@YNU

[トップページ](#) | [研究内容](#) | [研究実績](#) | [アクセス](#) | [メンバー](#) | [アルバム](#) | [リンク](#)

堀切研究室について



この研究室では、**光と物質を用いた量子技術の研究**をしています。特に量子力学と情報理論の融合で誕生した量子情報科学を用いて、新しい社会基盤技術の創出を目指しています。

キーワード：量子情報・量子通信・量子コンピュータ



QUANTUM INTERNET LAB TOUR

Host Speaker Series

The Thursday 30 March Host Speaker Series talk will focus on Quantum Internet. The WIDE Project has been working on and supporting the research and development of quantum networking/quantum Internet for more than 15 years. The talk will discuss that research with particular emphasis on testbed-related activities in Japan.

MENU

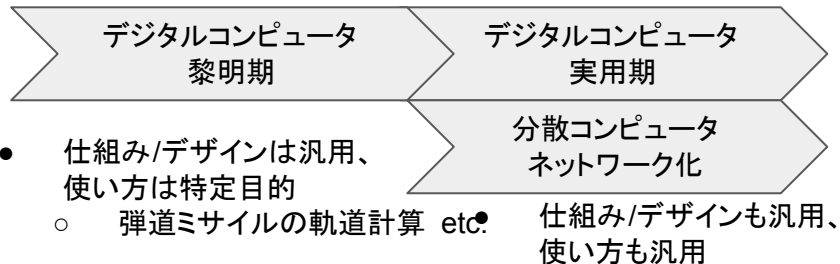
TOP



Technological Diversity of
Quantum Internet

技術史における量子インターネット

デジタルコンピュータ



重要概念:

コンピュータの汎用化と
コンピュータネットワーク化

→ 情報が「いつでも、どこでも手に入り、自在に処理できる」ものに

→ 古典IT革命
→ **量子IT革命**

量子コンピュータ黎明期

- 仕組み/デザインは汎用、使い方は特定(?)目的
 - 化学・金融・機械学習・etc.

量子コンピュータ実用期

- 分散コンピュータネットワーク化
- 仕組み/デザインも汎用、使い方も汎用

1950

1960

2020

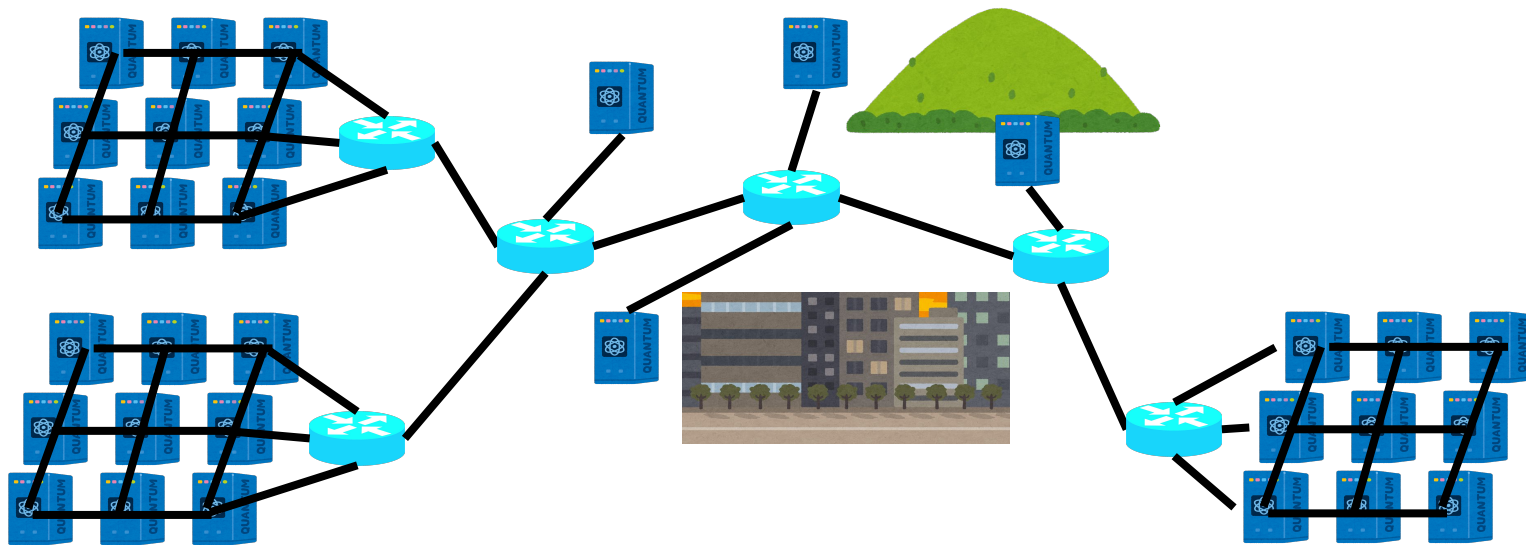
2030

2050

- 余談: 量子アニーラは仕組み/デザインから特定目的

量子インターネット

- 広域分散量子コンピューティング
 - 量子データの伝送



インターネットはなぜすごいのか

1. 情報を「適切な時に、適切な場所に、適切に処理できる形で存在する」ものにした
 - 任意の場所で任意のデータを即時に得られる(送れる)ことで達成
- 世界中が1つのネットワークで繋がっている
 - (逆に考えてみると)Aさんと会話するには東京と通信する用のこの通信網で通信Bさんは神奈川にいるから会話できない、Cさんは米国にいるから会話できない、....。
- 汎用的に使える
 - 1用途にしか使えない通信デバイスを大量に持ちたいか
 - 昔は持っていた: 音声通話(電話)、文字会話(ポケベル)、画像送信(FAX)
- 低遅延
 - 1通送るのに1日かかるメッセージアプリを使いたいか
 - 昔は使っていた: 手紙

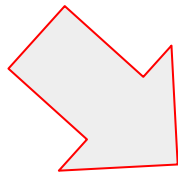
量子情報で同じ世界を実現する分野＝量子インターネット

量子で「汎用コンピュータ通信」できるありがたさ

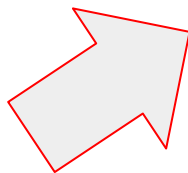
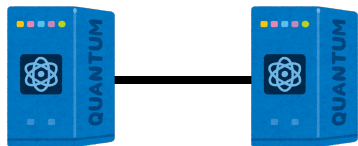
- 「ちょっと量子で保存しとくかー」
 - 量子データではなく、量子ファイル → 量子ファイルの送信
- 「途中までうちの大学の量子サーバで処理しておいて、残りは理研の量子スパコンだな」
 - c.f. : 機械学習における、データの前処理と学習処理
 - 例: QRAMへのデータ入力をローカル量子クライアントで、量子情報処理を強力なりモート量子サーバで
- 「うちの大学の量子サーバじゃスペック足りないから、あの大学の量子サーバと並列計算 (分散量子計算)しよう」
- 「機械学習の量子モデルを欲しがってたから、作って送っておこう」

分散量子コンピュータ

10量子ビット: 2^{10} = 約1000個の候補の中から解を高速に見つけ出す

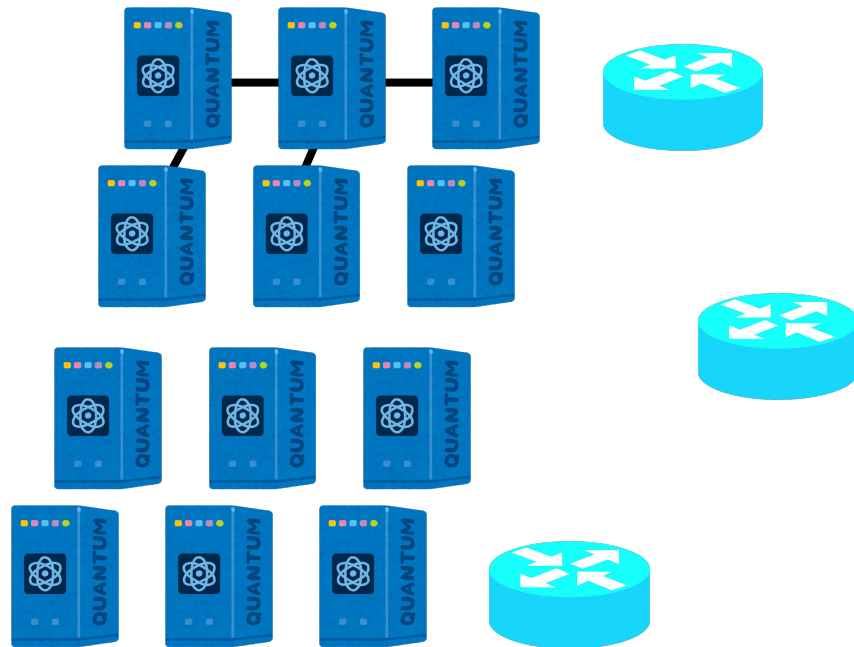


量子ネットワーク化！
=「量子データ」で繋ぐ



10+10量子ビット: 2^{20} = 約100万個の候補の中から解を高速に見つけ出す

もっとたくさん使いたい！





Quantum
Internet

インターネットはなぜすごいのか

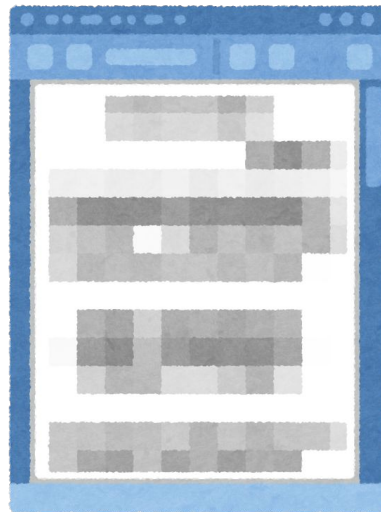
2. インターネット自身を支える基盤系の機能を自前で持っている
 - セキュリティ
 - 品質管理
 - さらに、近年ではブロックチェーンなど
3. 高速分散アルゴリズムの存在
 - 金融、ゲーム、etc.

量子インターネットでのセキュリティ

- 理論上解読不可能な暗号
 - 解くのに100万年かかる暗号
※量子コンピュータだと1日



- 理論上解読不可能な暗号へ

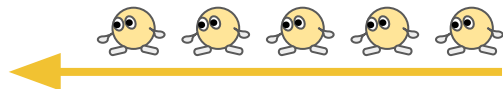


秘匿量子計算(概要)

- 目的: クライアントが遠隔にある量子コンピュータ(サーバー)を安全に使う。
 - クライアントの能力はサーバーよりずっと低い
 - クライアントは1量子ビットを2種類の基底で切り替えて測定するだけ
 - サーバーはクライアントが何をしているか一切わからない。
- 方法
 1. サーバーは測定型量子計算が可能になる多体エンタングル状態を作り、その qubitをひとつずつクライアントに送る。
 2. クライアントは順次測定していく。測定基底の選択はそれ以前の測定基底の選択や測定結果に依存する。
- 安全性
 - そもそもサーバーは決まった状態を送っているだけなので何も知りようがない。

クライアント

基底切り替え可能
測定装置



サーバー



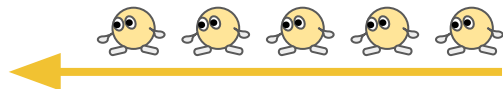
- Morimae, Fujii, PRA **87**, 050301(R) (2013)
- cf. : A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE, Piscataway, NJ, 2009), p. 517.

秘匿量子計算(概要)

- 目的: クライアントが遠隔にある量子コンピュータ(サーバー)を安全に使う。
 - クライアントの能力はサーバーよりずっと低い
 - クライアントは1量子ビットを2種類の基底で切り替えて測定するだけ
 - サーバーはクライアントが何をしているか一切わからない。
- 方法
 1. サーバーは測定型量子計算が可能になる多体エンタングル状態を作り、その qubitをひとつずつクライアントに送る。
 2. クライアントは順次測定していく。測定基底の選択はそれ以前の測定基底の選択や測定結果に依存する。
- 安全性
 - そもそもサーバーは決まった状態を送っているだけなので何も知りようがない。

クライアント

基底切り替え可能
測定装置



サーバー

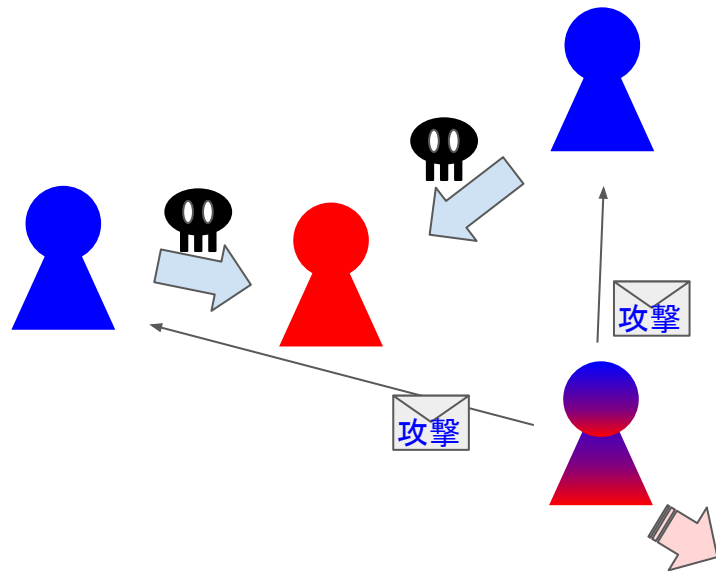


- Morimae, Fujii, PRA **87**, 050301(R) (2013)
- cf. : A. Broadbent, J. Fitzsimons, and E. Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE, Piscataway, NJ, 2009), p. 517.

Byzantine 合意問題 (Byzantine 将軍問題)

- 目的: 全員で共通の値(0 or 1)で合意したい。
- 制約
 - 構成員の全結合グラフの量子通信路 (+古典通信路)がある。
 - 一部反逆者がいる (1/3以下)
 - 反逆者の計算能力に制限なし
 - 通信は同期的
- 問題: 誠実な構成員が同じ値で合意するために何ラウンドの通信が必要になるか。
- ラウンド数
 - 古典: $\Omega(\sqrt{\frac{n}{\log(n)}})$
 - 量子: $O(1)$

例:
3部隊で攻めると勝てるが、
2部隊以下で攻めると負ける



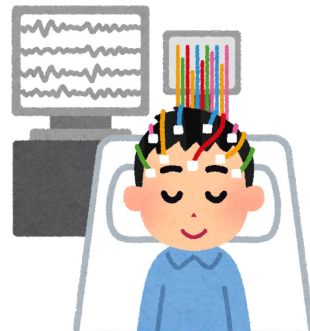
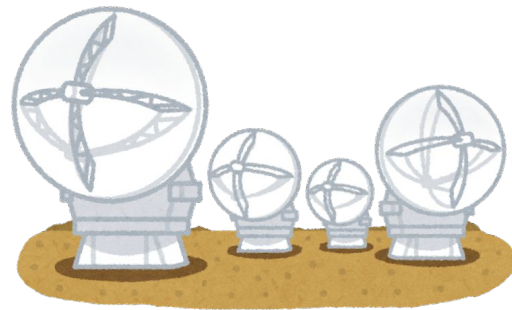
量子で「汎用コンピュータ通信」できるありがたさ

- 世界を1つの超巨大量子系にできる



量子インターネット

- 量子センサーネットワーク(量子IoT)
 - 宇宙からの超微弱な電波の取得
 - 遠くの天体の構造
 - 宇宙の成り立ち
 - 地中
 - 地震の予兆
 - 人体
 - 小さな小さな病気の種



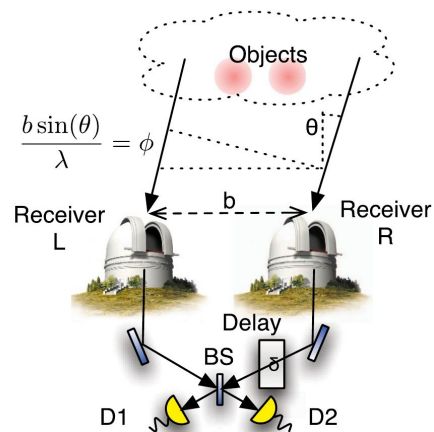
量子インターネットアプリケーション

量子インターネットのすごさ1

『量子情報を「適切な場所に、適切に処理できる形で、適切な時に存在する」ものにする』は別格として

● 現在わかっている量子インターネットアプリケーション例

- End-to-End 量子鍵配送(すごさ2)
 - 情報理論安全な共有秘密鍵を生成
- 量子デジタル署名(すごさ2)
 - 情報理論安全な認証を実現
- 秘匿量子計算(すごさ2)
 - サーバ管理者・クラウド事業者にもデータや処理内容が漏洩し得ない秘匿計算
- 超長基線望遠鏡(すごさ3)
 - 微弱な信号を検出可能
- 高速Byzantine合意(すごさ3)



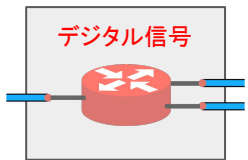


Ultimate Security
over
Quantum Internet

† 2方向に発展、現在地点
‡ 次の重要ステップ

量子インターネットマイルストーン

①



量子信号は一旦
電子デジタル信号に変換

アプリケーション

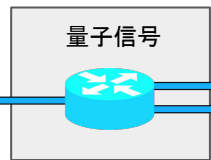
古典中継の量子暗号

出口

Trusted Node †
量子鍵配送ネットワーク
(東京QKDネットワーク等)
※E2E暗号ではない

②

※現在この段階に到達



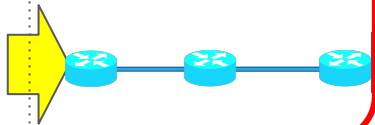
量子信号中継
Proof of Concept
実験室内

- 量子メモリなし
全光アーキテクチャ
(大阪大学, 2019)
- 量子メモリあり
ダイヤモンド内室素
アーキテクチャ
(デルフト工科大学, 2021)
- 今後数年で他のハード
ウェアでもPoCの期待

全く別物

③

†



離れたノード間の
量子中継システム・
プロトコルの動作実証

アプリケーション

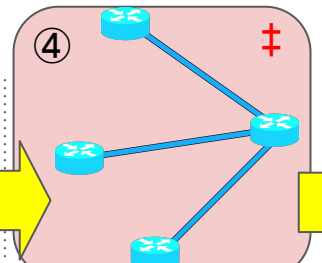
- 分散量子計算
 - ネットワーク量子センシング
 - 超高精度時刻同期
 - E2E量子鍵配送、等
- アプリケーション側からの研究と並行

出口

都市規模 量子インターネット

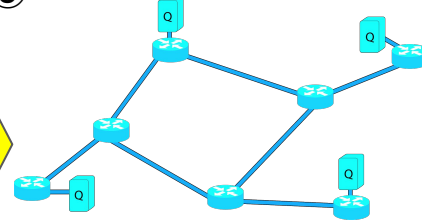
④

‡



大規模ネットワーク
に繋がるシステム・
プロトコルの
最小構成での動作実証

⑤



大規模な複雑ネットワーク
へのスケール実証

- 秘匿量子計算
- 量子セキュリティ
- リーダー選挙
- ビザンチン将軍問題
- 量子ビットコイン、等

国家規模 量子インターネット
世界規模 量子インターネット

量子インターネットとは: 量子暗号ネットワークとの差分

量子通信による古典(デジタル)ビット (=暗号鍵)伝送ネットワーク =量子暗号ネットワーク



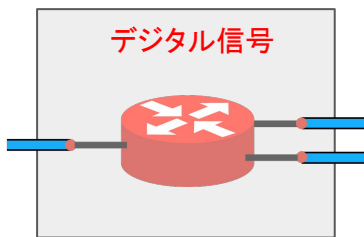
- 共有秘密鍵生成機能のみ
 - 特定用途ネットワーク
- 量子コンピュータに対しても安全
 - いわゆる長期安全性
- ただし、非End-to-End暗号
 - 中継しないならある意味 E2E
- 技術的に実現済み

量子通信による量子ビット 伝送ネットワーク =量子インターネット

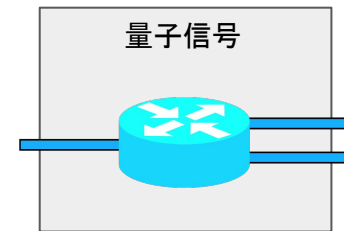


- 量子の汎用ネットワーク
- 多目的・多様・E2Eなアプリケーション
 - 量子鍵配送を含む暗号、センサー、分散計算など
 - End-to-End安全なセキュリティ
- 基礎研究段階

技術レベルに
多段ステップの
乖離がある
(Wehner, Elkouss,
Hanson, 2018)



量子信号は一旦
電子デジタル信号に変換



量子信号をそのまま
処理・中継・活用

量子インターネットとは: 量子暗号ネットワークとの差分

量子通信による古典(デジタル)ビット (=暗号鍵)伝送ネットワーク =量子暗号ネットワーク



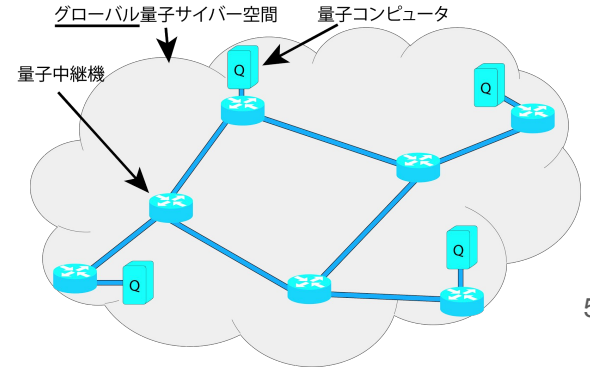
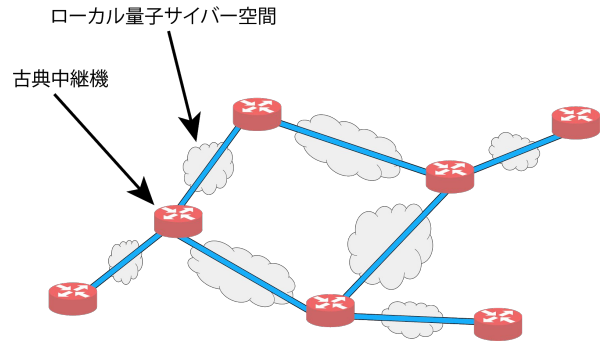
- 共有秘密鍵生成機能のみ
 - 特定用途ネットワーク
- 量子コンピュータに対しても安全
 - いわゆる長期安全性
- ただし、非End-to-End暗号
 - 中継しないならある意味 E2E
- 技術的に実現済み

量子通信による量子ビット 伝送ネットワーク =量子インターネット



- 量子の汎用ネットワーク
- 多目的・多様・E2Eなアプリケーション
 - 量子鍵配送を含む暗号、センサー、分散計算など
 - End-to-End安全なセキュリティ
- 基礎研究段階

技術レベルに
多段ステップの
乖離がある
(Wehner, Elkouss,
Hanson, 2018)



量子鍵配送の課題 by NSA

Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

HOME > CYBERSECURITY > QUANTUM

Synopsis
NSA continues to evaluate the usage of quantum key limitations below are over

What are Quantum Key Dis
Quantum key distribution u
special purpose technolo
communications link. Publ
standard cryptography.

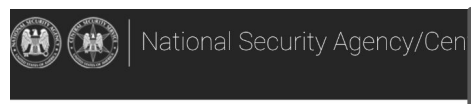
Quantum-resistant algorith
cryptographic protocols pro
quantum computer. The Na
resistant (or post-quantum
15.

Understanding the QKD/QC
Quantum key distribution a
offers "guaranteed" securit
the engineering required to
dependent rather than assu

Technical limitations

1. **Quantum key distribution is only a partial solution.** QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.
2. **Quantum key distribution requires special purpose equipment.** QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches.
3. **Quantum key distribution increases infrastructure costs and insider threat risks.** QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.
4. **Securing and validating quantum key distribution is a significant challenge.** The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than in most physical engineering scenarios making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.²
5. **Quantum key distribution increases the risk of denial of service.** The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

量子鍵配送の課題 by NSA



Quantum Key Dist

HOME > CYBERSECURITY > QUANTUM

Synopsis
NSA continues to evaluate the usage of quantum key limitations below are over

What are Quantum Key Dis
Quantum key distribution u
special purpose technolo
communications link. Publ
standard cryptography.

Quantum-resistant algorith
cryptographic protocols pro
quantum computer. The Na
resistant (or post-quantum
15.

Understanding the QKD/QC
Quantum key distribution a
offers "guaranteed" securit
the engineering required to
dependent rather than assu



それぞれの段落を1文に要約してもらえますか



もちろんです。

1. 量子鍵配送（QKD）は部分的なセキュリティ解決策であり、送信元の認証には非対称暗号や事前設置鍵が必要です。
2. QKDは特別なハードウェアと物理層の通信に依存しており、ソフトウェアや既存のネットワーク設備と容易に統合できません。
3. QKDネットワークは信頼できるリレーが必要で、これが追加のコストとインサイダー脅威のリスクをもたらします。
4. QKDの実際のセキュリティは理論的なものではなく、ハードウェアとエンジニアリングの限界によって制約され、その検証は非常に困難です。
5. QKDのセキュリティは傍受者への感度に基づいているため、サービス拒否（DoS）攻撃のリスクが高まります。

これらの要約が、QKDの技術的制限についての理解を深める助けになることを願っています。

Such keying assurance that create the QKD authentication. in a better

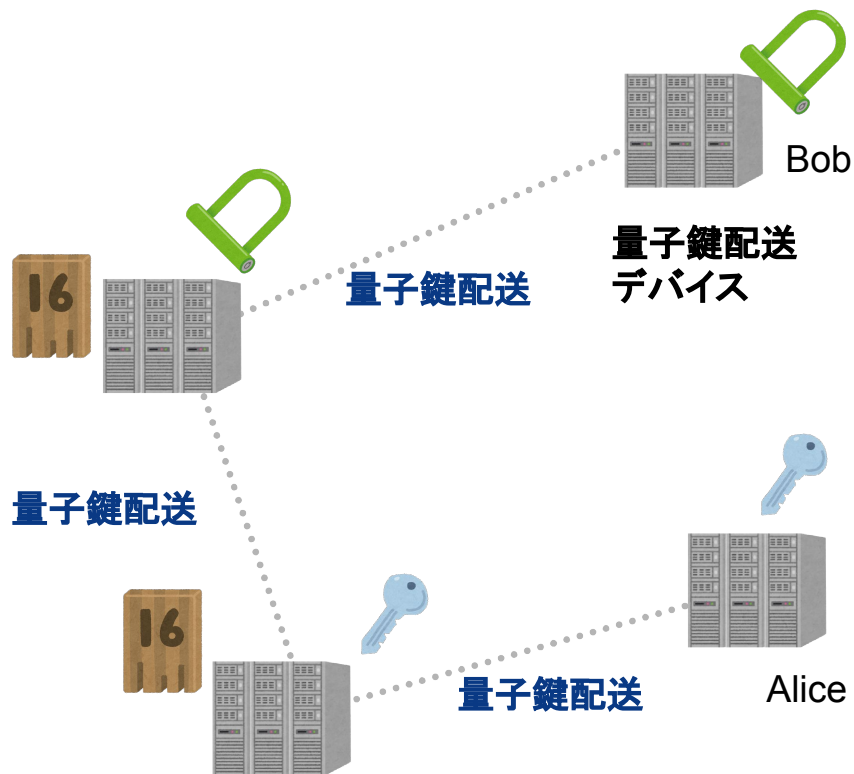
physical layer implemented in so lacks

lays, entailing

tical ed by hardware sical g in several

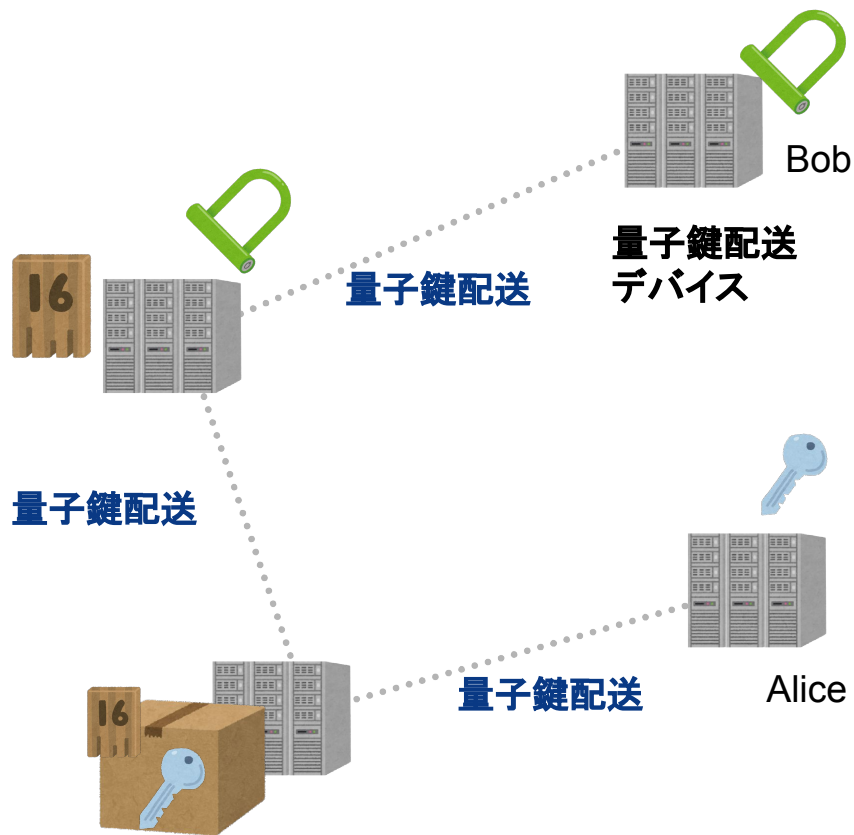
y claims also

Trusted Node 量子鍵配送ネットワーク



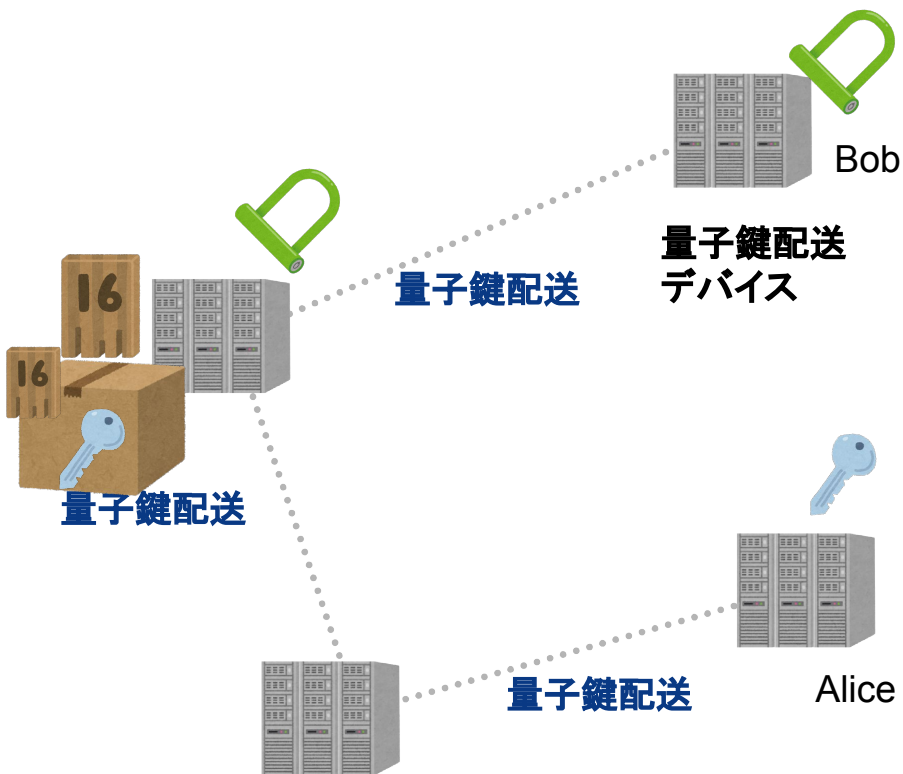
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



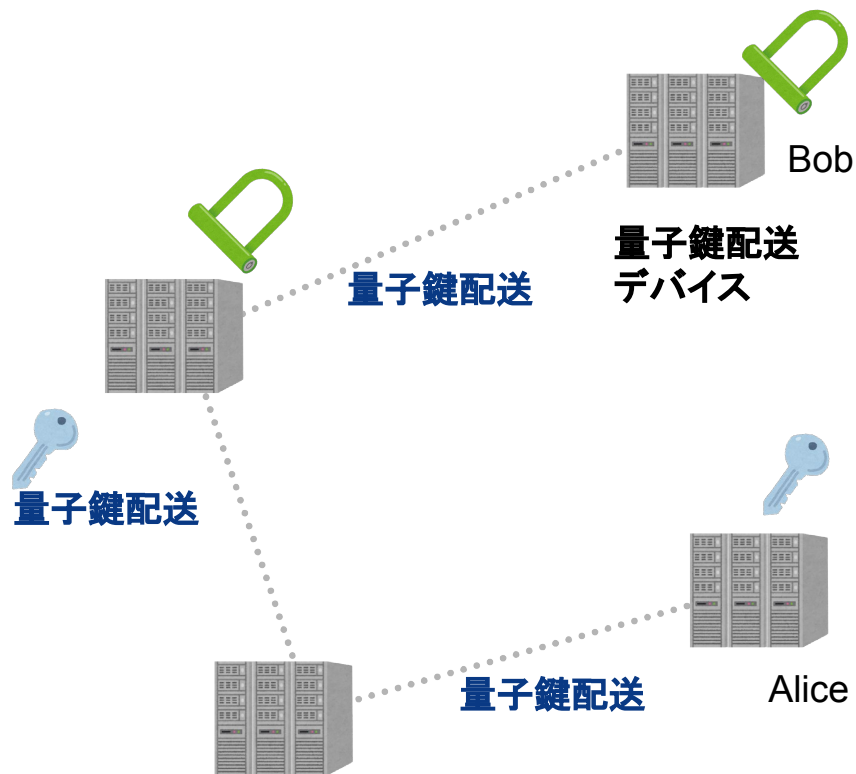
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



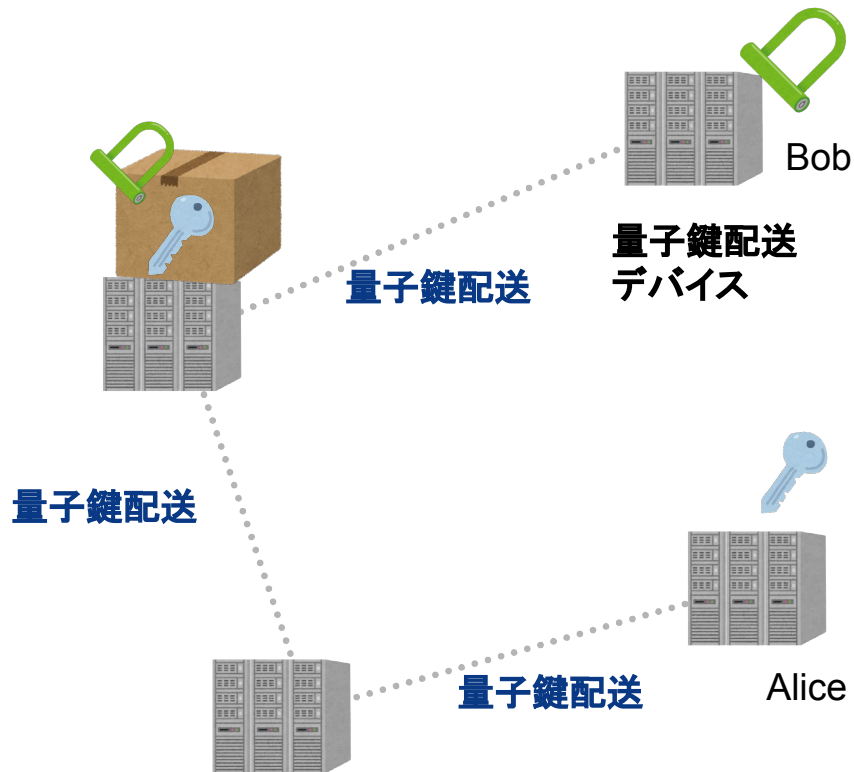
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



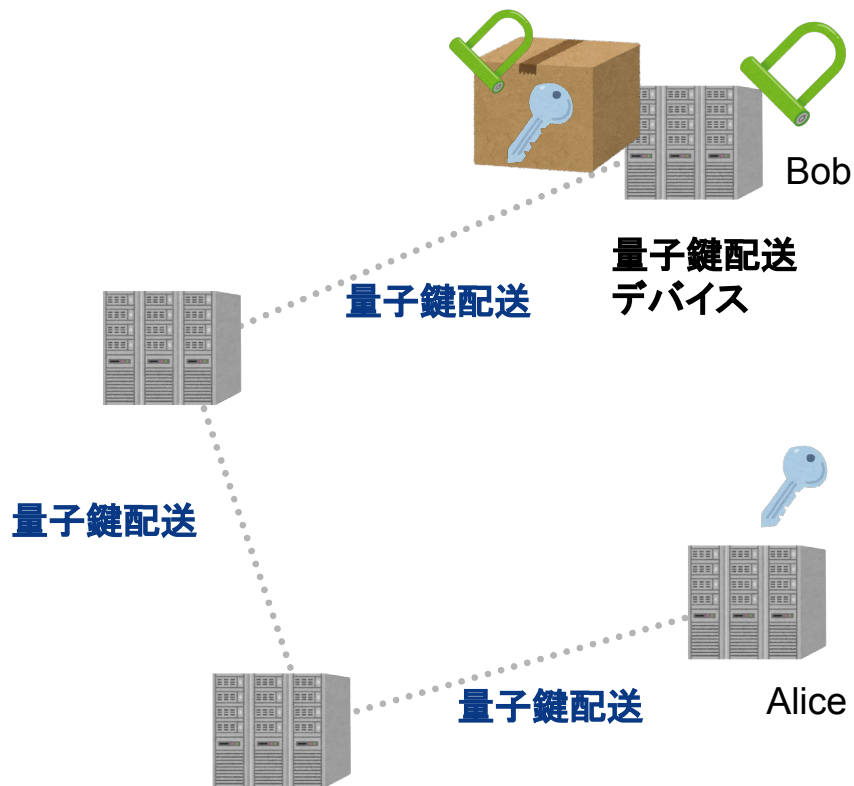
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



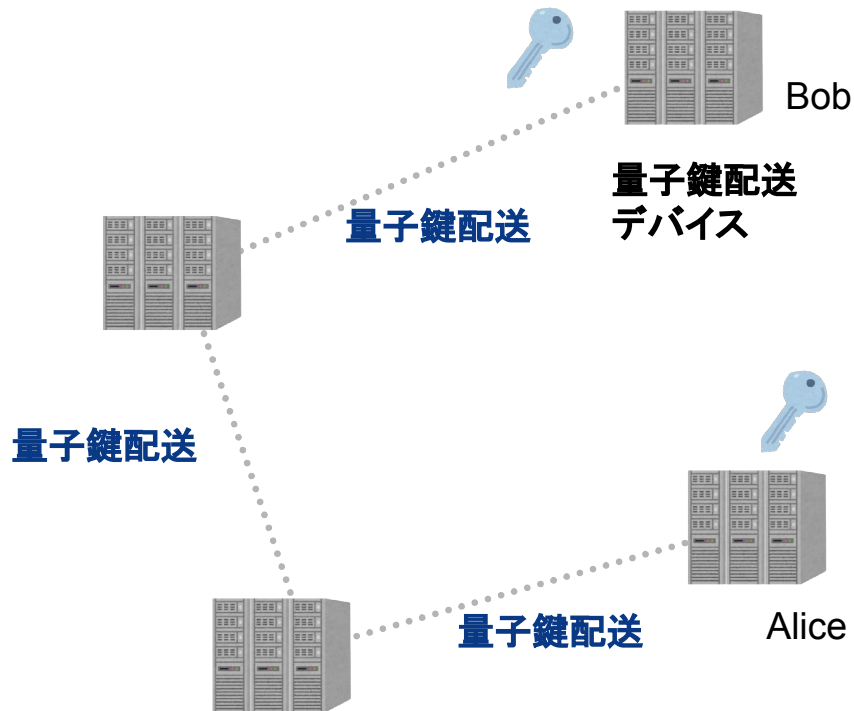
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



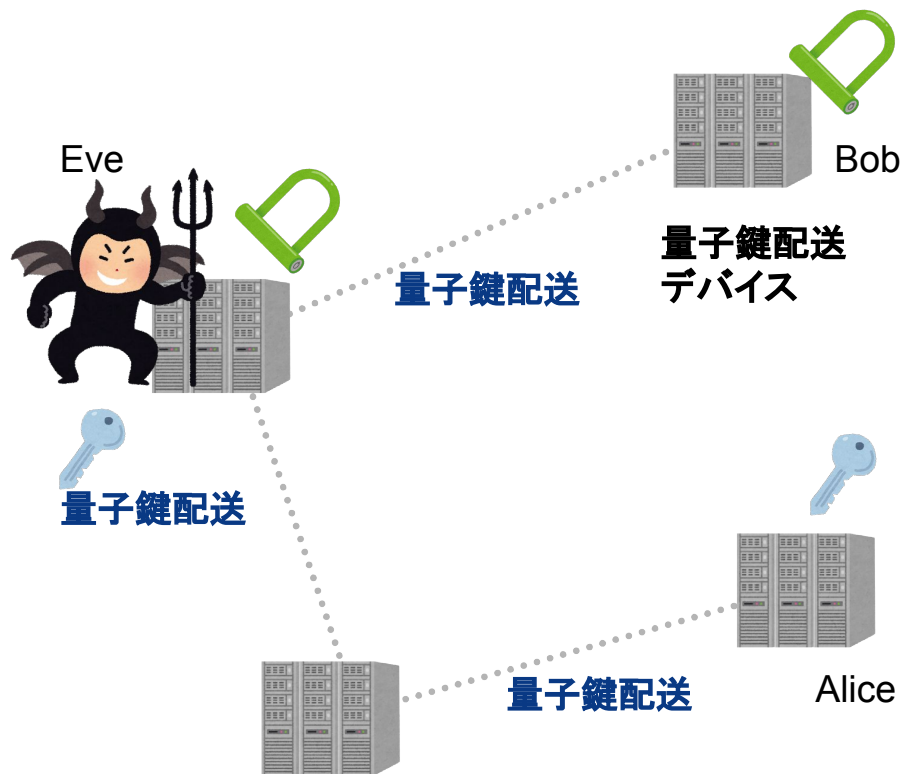
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



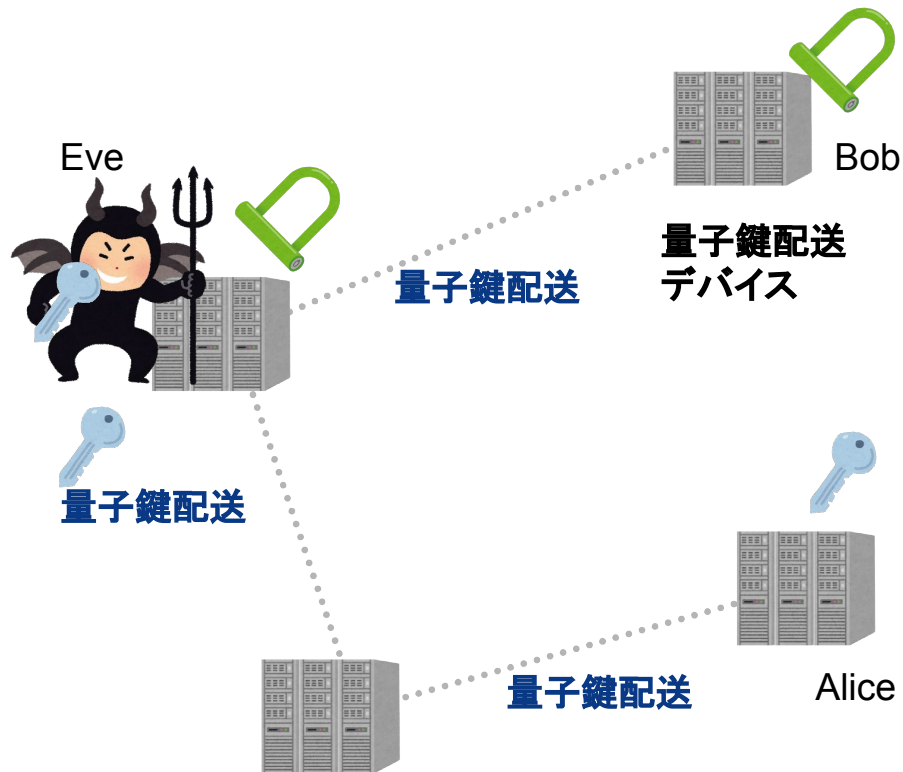
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



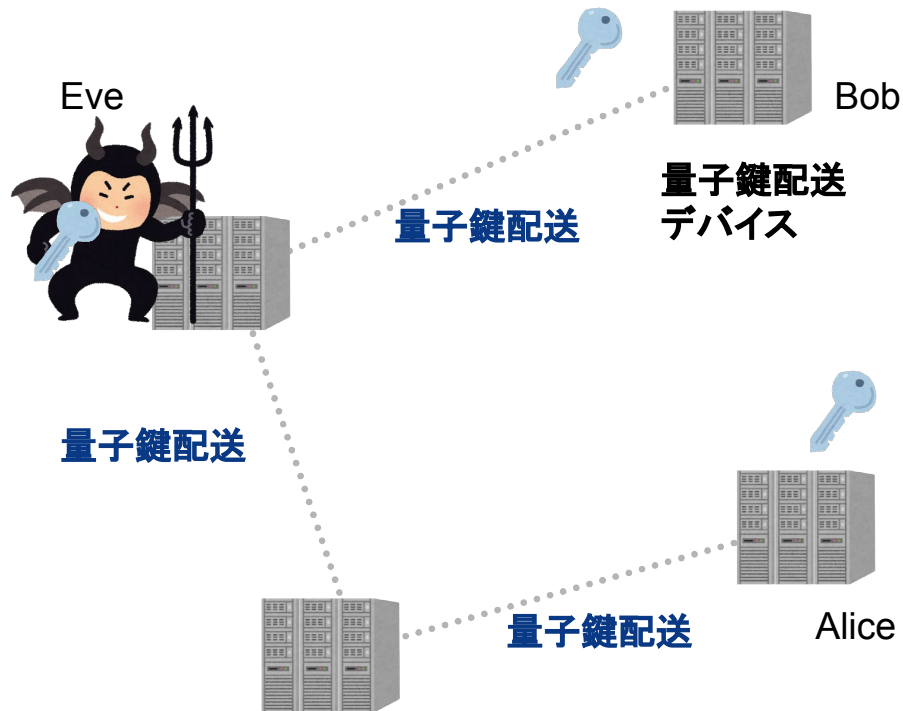
- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）

Trusted Node 量子鍵配送ネットワーク



- “量子通信”は1hopのみ可能と割り切る
- 各リンクの鍵は量子鍵配送で作る
- 古典インターネット上で量子セキュアに鍵配送（鍵カプセル化）
- ノードが全て信頼できる前提＝Trusted Node

プレスリリース 2023年

ソフトバンクと東芝デジタルソリューションズ、 IPsec QKD-VPNの実証実験に成功

～Beyond 5G/6G時代の量子セキュアネットワークの実現に向けて共創を開始～

2023年9月20日
ソフトバンク株式会社
東芝デジタルソリューションズ株式会社

ソフトバンク株式会社（以下「ソフトバンク」）と東芝デジタルソリューションズ株式会社（以下「東芝デジタルソリューションズ」）は、Beyond 5G/6G時代の量子セキュアネットワークの実現に向けて共創を開始し、量子暗号技術であるQKD（Quantum Key Distribution、量子鍵配送）を用いた拠点間VPN（Virtual Private Network）通信の実証実験に成功しましたので、お知らせします。



卒業論文 2009年度 (平成21年度)

量子鍵配送を利用したIPsecのための
IKE拡張

慶應義塾大学 総合政策学部

氏名：永山 翔太

量子インターネット: 3つの研究開発要素

1. ハードウェア

- 量子情報の伝送 → 「量子もつれ」の中継・長距離配送に

必要な技術開発: 量子中継、量子メモリ、量子-光子インターフェース、周波数変換など量子光技術、etc.

2. ネットワークアーキテクチャ・プロトコル

- 量子の物理的特徴に最適化されたアーキテクチャ・プロトコル・ミドルウェア設計
- 量子インターネットの良し悪しを決定
→ 信頼性・安定性・インシデント耐性・高パフォーマンス性・メンテナンス性・スケーラビリティなど
- しかも、40年以上使用される (今のインターネットを動かしているTCP/IPは1970年代に開発され、今も現役)

必要な技術開発: 自律分散協調システム、各レイヤーの責任分解・抽象化・インターフェース、相互接続性、互換性、資源管理、ルーティング、E2E接続、スケーラビリティ、動的制御、トラストアンカー、etc.

今のネットワークアーキテクチャは、ハードとソフトが試行錯誤して時間をかけて発展 (電話網からインターネット、電気から光)

→ しかし、今のインターネットをそのままコピーすればよいわけではない。

→ 量子でどのようにすべきか不明。研究開発要素 膨大

3. アプリケーション

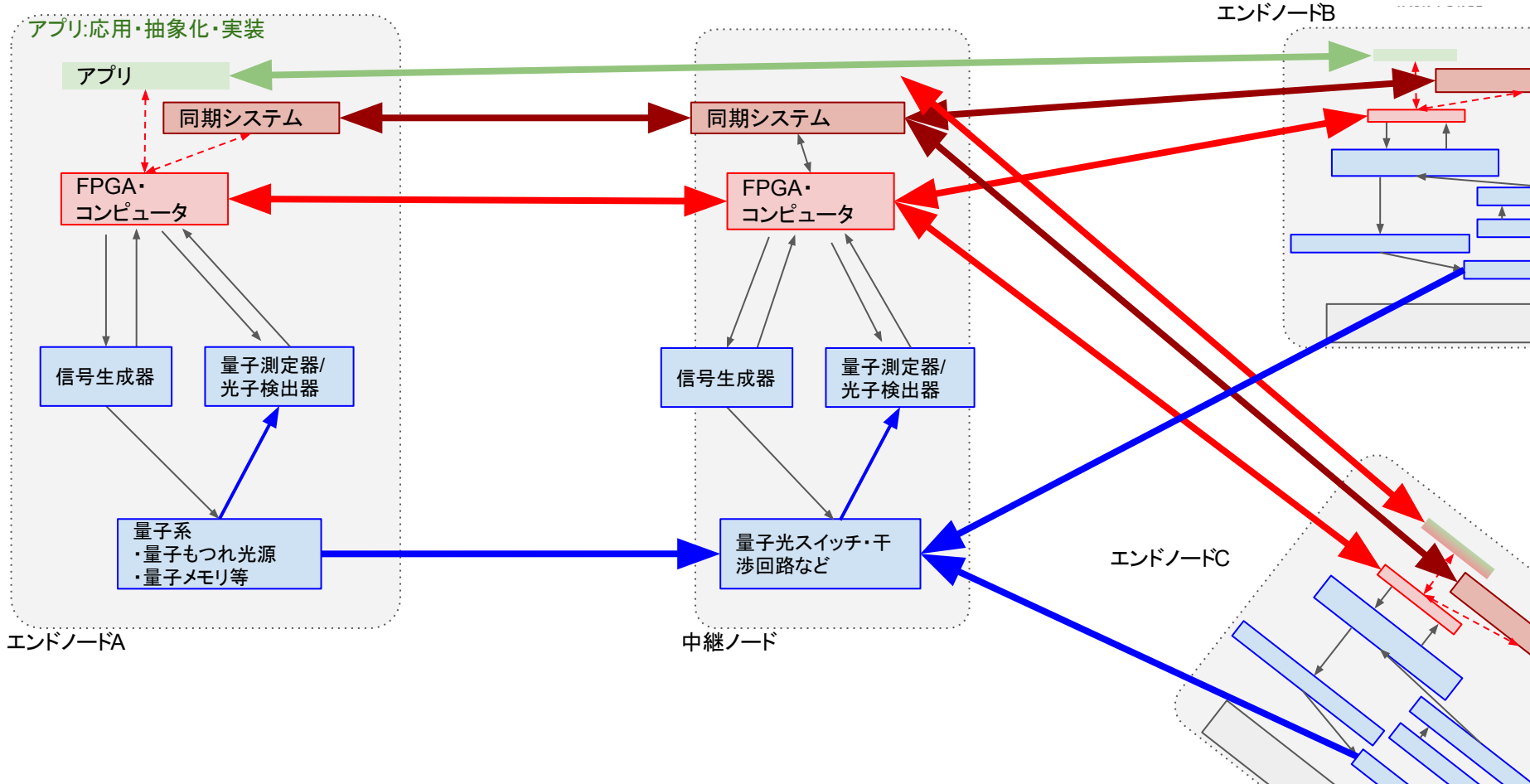
- 計算機・センシング・通信にまたがる横断的な分野
- 多くの応用はその物理系(ハードウェア)と密接に関係
 - 量子計算に向けた物理系、センシングに向けた物理系、 etc.
- ネットワークの設計・物理系選択とも密接に関連

必要な技術開発: 3分野の理論・実験、実用化を見越した開発、NISQ 量子インターネットアルゴリズム、今のインターネットとの統合(言語、ライブラリ、etc.)

様々な領域の研究者が連携して統合的に進めないと良いものにならない

完成形イメージ図

ネットワークシステムソフトウェア
ネットワークシステムハードウェア
(ネットシステム)
量子ハードウェア/量子制御装置(ハードウェア)

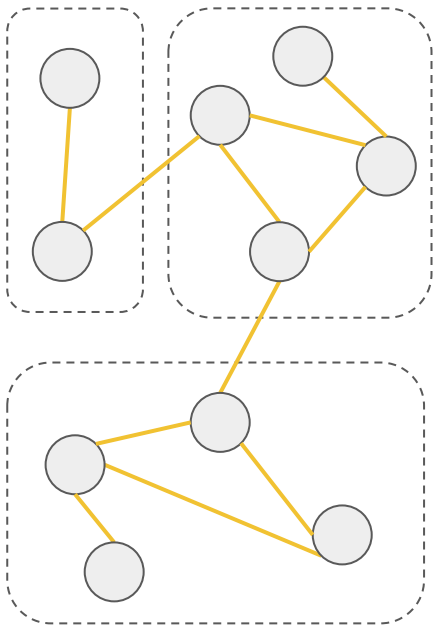


インターネット

○ : 古典力学的ノード

— : 古典力学的通信路 (e.g. 光ファイバー)

□ : 自律ネットワーク



社会実装

インフラ化

ELSI(倫理・法律・社会)

情報学(理論+工学)

分散アルゴリズム

アプリケーション

計算機工学

ネットワーク理論
・グラフ理論

ソフトウェア工学
・システムソフトウェア
・分散システム
・セキュリティ

通信理論/通信工学
・符号

ネットワーク工学
・プロトコルスタック

古典力学

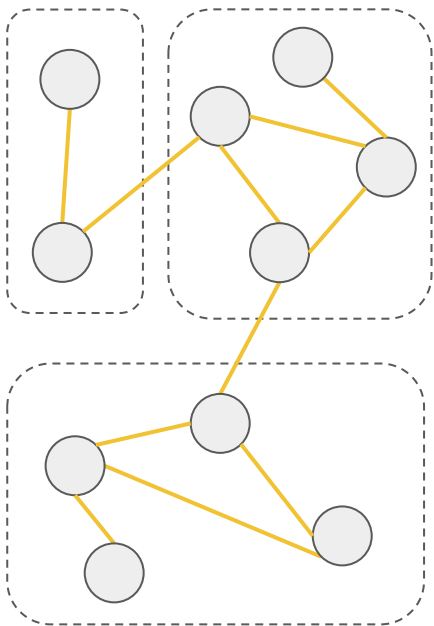
エレクトロニクス
光学
制御工学
物性 etc.

量子インターネット

○ : 量子ノード

— : 量子通信路 (e.g. 光ファイバー)

□ : 自律ネットワーク



社会実装

インフラ化

ELSI(倫理・法律・社会)

情報学(理論+工学)

分散アルゴリズム

アプリケーション

計算機工学

ネットワーク理論
・グラフ理論

ソフトウェア工学
・システムソフトウェア
・分散システム
・セキュリティ

通信理論/通信工学
・符号

ネットワーク工学
・プロトコルスタック

量子力学・光学 (理論+工学)

量子エレクトロニクス、量子デバイス、
量子光学、光物性、非線形光学
量子制御工学、物性 etc.

社会実装

・ELSI(倫理・法律・社会)

・ELSI(倫理・法律・社会)

情報学(理論+工学)

分散アルゴリズム

アプリケーション

計算機工学

ソフトウェア工学
・システムソフトウェア
・セキュリティ

ネットワーク理論
・グラフ理論

ソフトウェア工学
・システムソフトウェア
・セキュリティ

通信理論/通信工学
・符号

ネットワーク工学
・プロトコルスタック

量子力学・光学
(理論+工学)

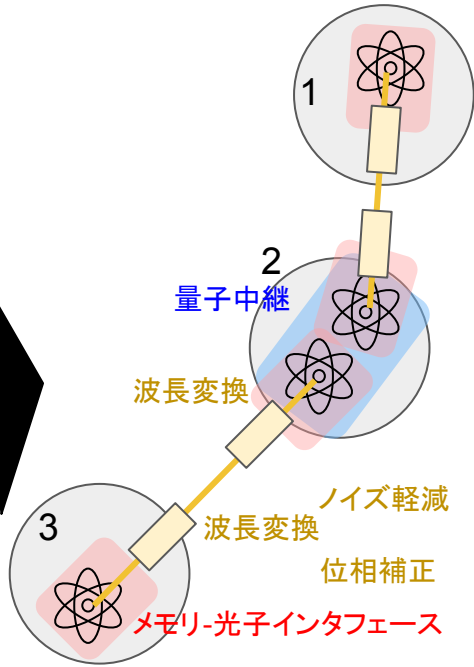
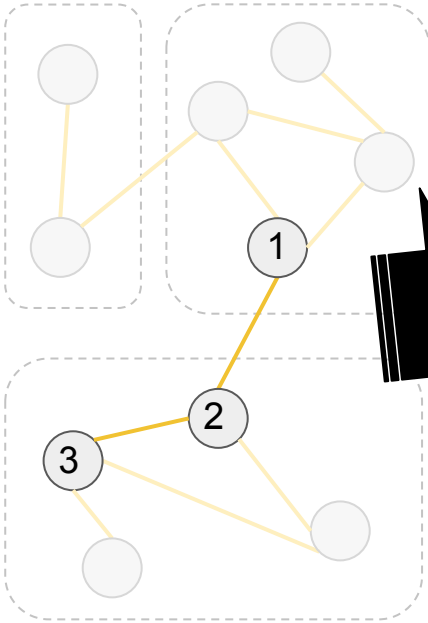
量子エレクトロニクス、量子デバイス、
量子光学、光物性、非線形光学
量子制御工学、物性 etc.

量子インターネット

○ : 量子ノード

— : 量子通信路(e.g. 光ファイバー)

□ : 自律ネットワーク

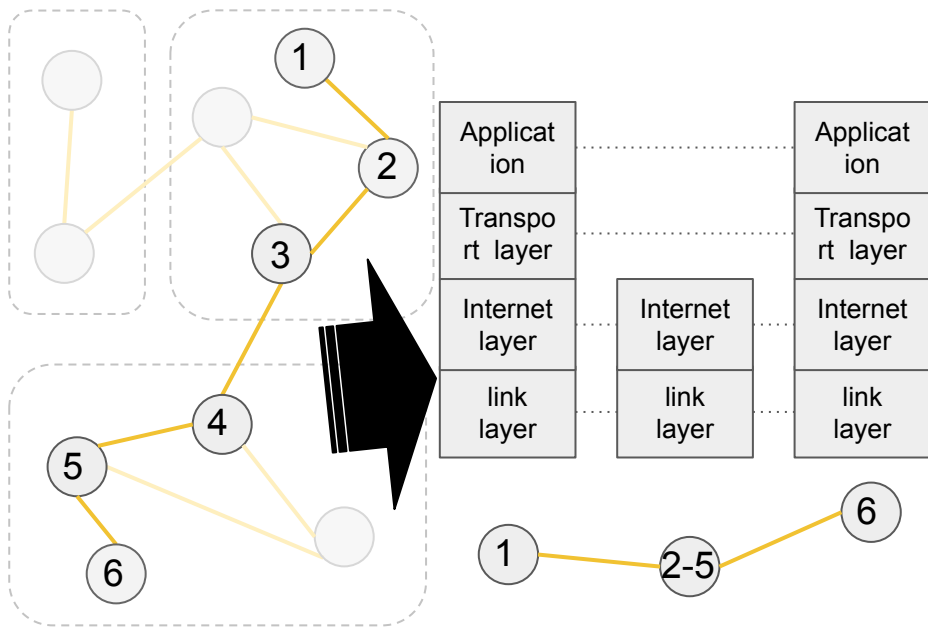


量子インターネット

○ : 量子ノード

— : 量子通信路 (e.g. 光ファイバー)

□ : 自律ネットワーク



社会実装

・ELSI(倫理・法律・社会)

・ELSI(倫理・法律・社会)

情報学(理論+工学)

分散アルゴリズム

アプリケーション

計算機工学

ソフトウェア工学
・システムソフトウェア
・分散システム
・セキュリティ

ネットワーク理論
・グラフ理論

通信理論/通信工学
・符号

ネットワーク工学
・プロトコルスタック

量子力学 (理論+工学)

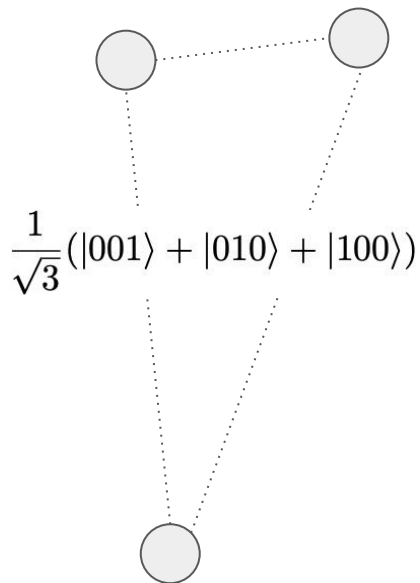
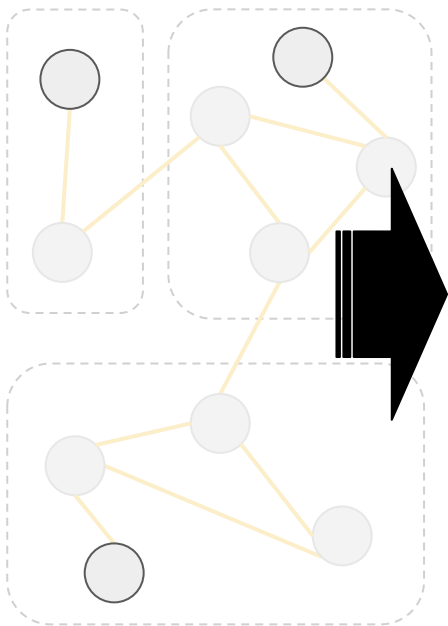
量子エレクトロニクス、量子デバイス、
量子光学、光物性、非線形光学
量子制御工学、物性 etc.

量子インターネット

○ : 量子ノード

— : 量子通信路 (e.g. 光ファイバー)

□ : 自律ネットワーク



社会実装

・ELSI(倫理・法律・社会)

・ELSI(倫理・法律・社会)



情報学(理論+工学)

分散アルゴリズム

アプリケーション

計算機工学

ネットワーク理論
・グラフ理論

ソフトウェア工学
・システムソフトウェア
・分散システム
・セキュリティ

通信理論/通信工学
・符号

ネットワーク工学
・プロトコルスタック

量子力学 (理論+工学)

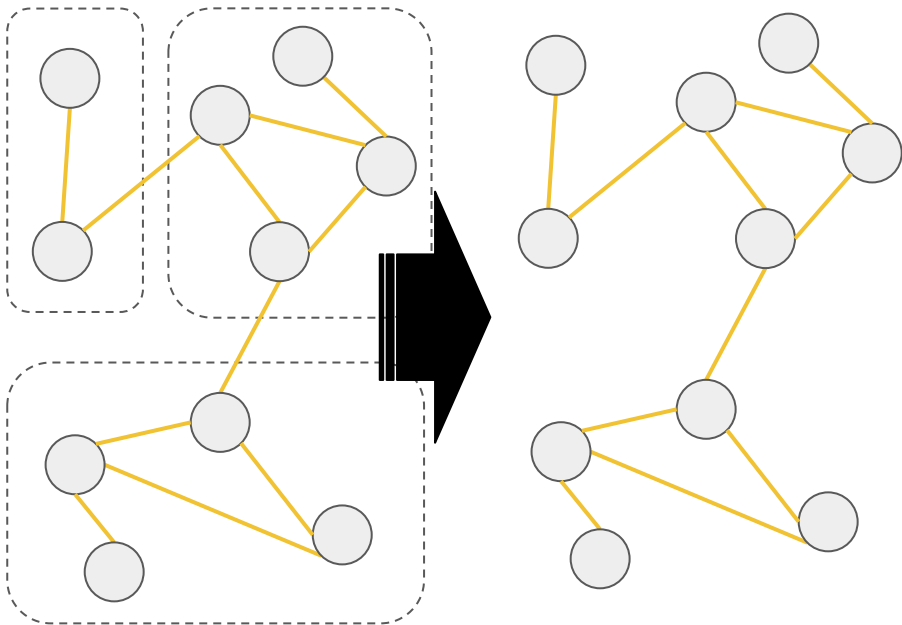
量子エレクトロニクス、量子デバイス、
量子光学、光物性、非線形光学
量子制御工学、物性 etc.

量子インターネット

○ : 量子ノード

— : 量子通信路 (e.g. 光ファイバー)

□ : 自律ネットワーク



社会実装

・ELSI(倫理・法律・社会)

・ELSI(倫理・法律・社会)



情報学(理論+工学)

分散アルゴリズム

アプリケーション

計算機工学

ネットワーク理論
・グラフ理論

ソフトウェア工学
・システムソフトウェア
・分散システム
・セキュリティ

通信理論/通信工学
・符号

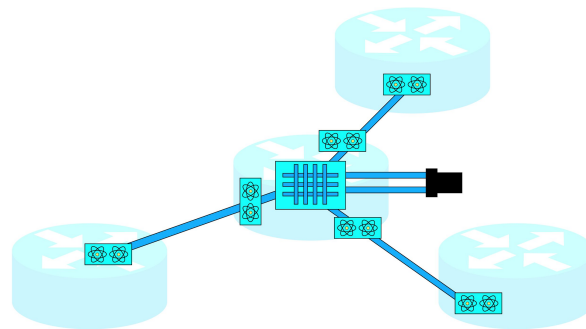
ネットワーク工学
・プロトコルスタック

量子力学 (理論+工学)

量子エレクトロニクス、量子デバイス、
量子光学、光物性、非線形光学
量子制御工学、物性 etc.

I 構想1: 室内ネットワーク

超短距離量子コンピュータネットワーク

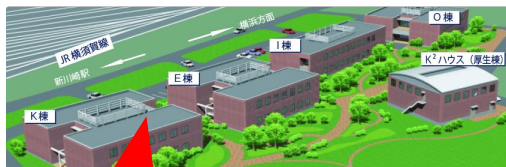


多領域の研究者による各種要素技術を統合し、**量子ネットワークを実証**

- かわさき新産業創造センター (KBIC)
 - 4ノードの星型ネットワークを構築
 - ルーティング等を含む、ネットワークシステム全体像を実現

Ⅰ 構想2: データセンターサイズネットワーク

キャンパス内フィールド実験 (データセンターサイズネットワーク)



約200m



- かわさき新産業創造センター (KBIC)
 - 4ノードの星型ネットワークを構築
 - ルーティング等を含む、ネットワークシステム全体像を実現

- 慶應義塾大学新川崎キャンパス
 - 量子光技術の要素研究 @ムーンショット

Ⅰ 構想3: キャンパス間ネットワーク

キャンパス間フィールド実験 (インターネット)

東京方面へ



約200m



- かわさき新産業創造センター (KBIC)
 - 4ノードの星型ネットワークを構築
 - ルーティング等を含む、ネットワークシステム全体像を実現
- 慶應義塾大学新川崎キャンパス武岡研究室
 - 量子光技術の要素研究 @ムーンショット
- 慶應義塾大学矢上キャンパス
- 横浜国立大学
- さらに拡大へ

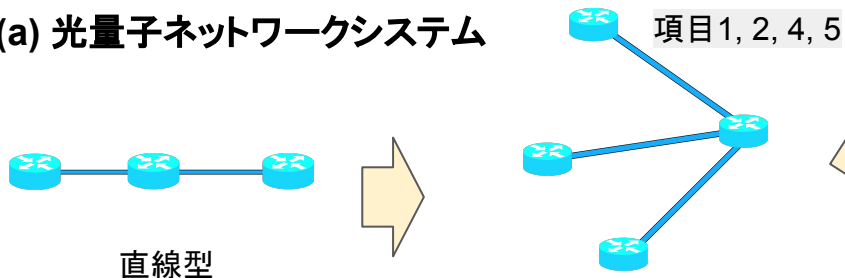
量子コンピュータネットワーク長期マイルストーン

現在の実施課題

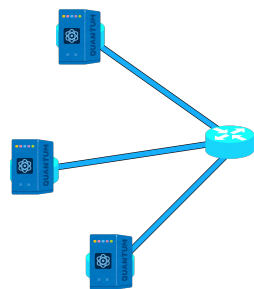
2030年

2040年~

(a) 光量子ネットワークシステム

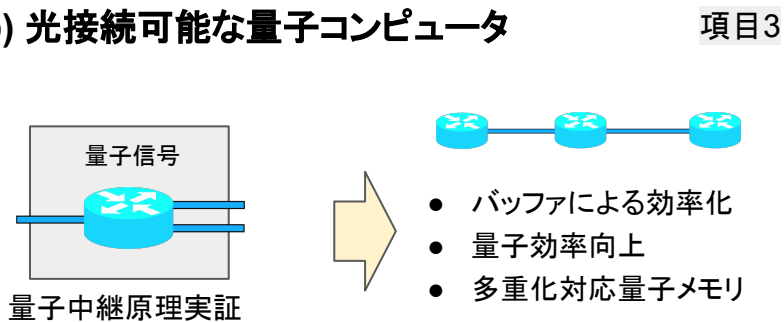


スケーラブルで強靱な
統合的量子通信システム



大規模QCネットワーク

(b) 光接続可能な量子コンピュータ



- スター型NWの実証
- スケール検証(シミュレーション)

小規模分散量子計算

広域/狭域 大規模分散量子計算

社会実装

量子インターネット: 3つの研究開発要素

1. ハードウェア

- 量子情報の伝送 → 「量子もつれ」の中継・長距離配送に

必要な技術開発: 量子中継、量子メモリ、量子-光子インターフェース、周波数変換など量子光技術、etc.

2. ネットワークアーキテクチャ・プロトコル

- 量子の物理的特徴に最適化されたアーキテクチャ・プロトコル・ミドルウェア設計
- 量子インターネットの良し悪しを決定
→ 信頼性・安定性・インシデント耐性・高パフォーマンス性・メンテナンス性・スケーラビリティなど
- しかも、40年以上使用される (今のインターネットを動かしているTCP/IPは1970年代に開発され、今も現役)

必要な技術開発: 自律分散協調システム、各レイヤーの責任分解・抽象化・インターフェース、相互接続性、互換性、資源管理、ルーティング、E2E接続、スケーラビリティ、動的制御、トラストアンカー、etc.

今のネットワークアーキテクチャは、ハードとソフトが試行錯誤して時間をかけて発展 (電話網からインターネット、電気から光)

→ しかし、今のインターネットをそのままコピーすればよいわけではない。

→ 量子でどのようにすべきか不明。研究開発要素 膨大

3. アプリケーション

- 計算機・センシング・通信にまたがる横断的な分野
- 多くの応用はその物理系(ハードウェア)と密接に関係
 - 量子計算に向けた物理系、センシングに向けた物理系、 etc.
- ネットワークの設計・物理系選択とも密接に関連

必要な技術開発: 3分野の理論・実験、実用化を見越した開発、NISQ 量子インターネットアルゴリズム、今のインターネットとの統合(言語、ライブラリ、etc.)

様々な領域の研究者が連携して統合的に進めないと良いものにならない

量子インターネット: 3つの研究開発要素

1. ハードウェア

- 量子情報の伝送 → 「量子もつれ」の中継・長距離配送に

必要な技術開発:
量子中継、量子メモリ、
量子-光子インターフェース、etc.

2. ネットワーク

- 量子
- 量子
- 量子

量子インターネット = 量子情報技術の総合格闘技

量子暗号の技術や量子計算の技術、さらにインターネットの知見も活用しつつ、
量子インターネットのためのネットワークデザインやアーキテクチャを
理論研究・工学的に実現し、量子情報(量子もつれ)の伝送をおこなう、
大複合領域

3. アプリケーション

- 量子計算
- 多くの応用は他の物理系(ハードウェア)と密接に関連
 - 量子計算に向けた物理系、センシングに向けた物理系、 etc.
 - ネットワークの設計・物理系選択とも密接に関連

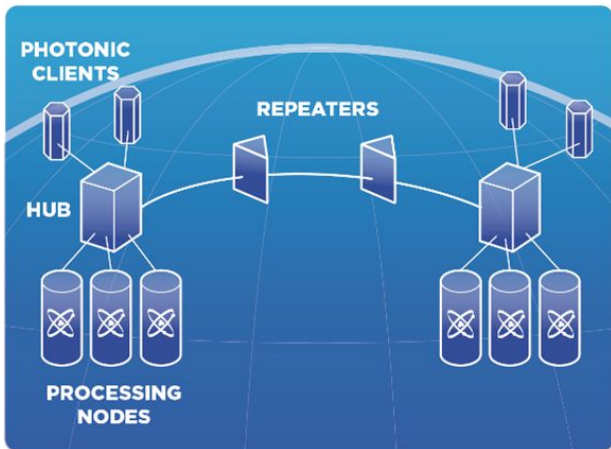
インターネットアルゴリズム、今のインターネットとの統合(言語、ライブラリ、etc.)

様々な領域の研究者が連携して統合的に進めないと良いものにならない

海外の取り組みの中身

EUの取り組み

- 都市規模ネットワーク2つを接続するプロトタイプ計画



<https://quantum-internet.team/mission/>

1 Quantum NL R&D network with three quantum processors realized | 2023

2 Online remote access to the NL Q-Staging network | 2023

3 Quantum NL Staging Network with ≥ 5 Quantum nodes (incl. embedding cloud) | 2026

<https://quantumdelta.nl/TUQ/wp-content/uploads/2021/05/Catalyst-Programme-2-National-Quantum-Network.pdf>

- 量子インターネットのチームが分散量子コンピュータも担っている (どちらも量子コンピュータネットワークとして推進している)

量子インターネット部門

量子インターネット

量子インターネットのマイルストーン

量子インターネットデモンストレーター

私達がすること

地球上の任意の2つの場所間の量子通信

将来の量子インターネットは、世界中の(量子)コンピューターを接続します。量子力学の法則に従った量子ビット(キュービット)を使って情報を送受信できるようになります。量子インターネット部門の目標は、地球上の任意の2つの場所間で量子通信を可能にする技術を開発することです。

この根本的に新しい技術について、ゲームを変える可能性のあるいくつかの主要な新しいアプリケーションがすでに特定されています。そのようなアプリケーションの1つは、物理法則によってプライバシーが保証される、根本的に安全な通信方法を提供することです。また、量子プロセッサを量子ネットワークに接続して、大規模な量子コンピューティングクラスターを構築することもできます。このアプローチはネットワーク化された量子コンピューティングと呼ばれ、量子コンピューティングの作業を補完するスケラビリティへの自然な道を提供します。量子インターネットとネットワーク化された量子コンピューターを組み合わせることで、リモートユーザー/プロバイダーは「クラウド内」で安全な量子コンピューティングを実行できます。

<https://qutech.nl/research-engineering/quantum-internet/>
(Chromeの機能による自動翻訳)

米国の取り組み

米国エネルギー省(DoE)のBlueprint

Priority Research Directions.....

2.1. PRD 1: Provide the Foundational Building Blocks for a Quantum Internet.....

2.2. PRD 2: Integrate Multiple Quantum Networking Devices

2.3. PRD 3: Create Repeating, Switching, and Routing for Quantum Entanglement..

2.4. PRD 4: Enable Error Correction of Quantum Networking Functions.....

Blueprint Roadmap Milestones.....

3.1. Milestone 1: Verification of Secure Quantum Protocols over Fiber Networks.....

3.2. Milestone 2: Inter-campus and Intra-city Entanglement Distribution

3.3. Milestone 3: Intercity Quantum Communication using Entanglement Swapping.....

3.4. Milestone 4: Interstate Quantum Entanglement Distribution using Quantum Repeaters

3.5. Milestone 5: Build a Multi-institutional Ecosystem between Laboratories, Academia, and Industry to Transition from Demonstration to Operational Infrastructure

多拠点でテストベッドエフォートを推進(DoE, NSFなど)

- [Berkeley lab, ESnet, UC Berkeley, Caltech \(1250万ドル\)](#)
- [Oak Ridge National Lab \(1250万ドル\)](#)
- [Brookhaven Natinal Lab](#)
- [Chicago Quantum Exchange \(UChicago, アルゴンヌ研究所, etc\)](#)
- [Brookhaven National Lab](#)
- [アリゾナ大学 \(2600万ドル\(ボストンエリアを含む予算\)\)](#)
- [ボストンエリア\(ハーバード、MITなど\)](#)
- [DC-QNET \(ワシントン周辺の政府機関HQを接続する計画\)](#)



中国の量子もつれに関する実験

衛星から量子もつれを飛ばして200km離れた2地点に共有

衛星から飛ばした量子もつれを使った暗号鍵生成のデモンストレーション

原子集団による確率的量子中継の実証

nature photonics

Explore content ▾ About the journal ▾ Publish with us ▾

[nature](#) > [nature photonics](#) > [articles](#) > article

Article | [Published: 25 February 2021](#)

Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments

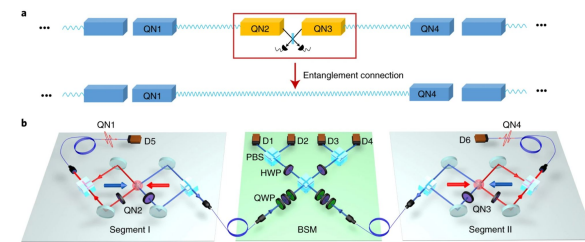
[Yun-Fei Pu](#), [Sheng Zhang](#), [Yu-Kai Wu](#), [Nan Jiang](#), [Wei Chang](#), [Chang Li](#) & [Lu-Ming Duan](#) ✉

[Nature Photonics](#) **15**, 374–378 (2021) | [Cite this article](#)

3906 Accesses | 15 Citations | 30 Altmetric | [Metrics](#)

Fig. 1: The quantum repeater protocol and the experimental set-up.

From: [Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments](#)



a. A sketch of entanglement connection (swapping) in the quantum repeater protocol. QN represents a quantum repeater node. **b.** The whole experimental set-up consists of three parts: segment I (QN1 and QN2) and segment II (QN3 and QN4), together with a Bell state measurement (BSM) station in the centre. QN2 and QN3 are two similar atomic memory nodes separated by 3 m in space. QN1 and QN4 are photons in this experiment and are measured by detectors D5 and D6. A sandwich structure consisting of a quarter-wave plate (QWP), a half-wave plate (HWP) and another QWP is introduced to compensate for the polarization change in the fibre transmission. The coincidence events between the single-photon detectors D1 and D4 (or D2 and D3) project the two idler photons onto one of the four Bell states $|\Phi^{\pm}\rangle$.

nature

Explore content ▾ Journal information ▾ Publish with us ▾ Subscribe

[nature](#) > [articles](#) > article

Article | [Published: 15 June 2020](#)

Entanglement-based secure quantum cryptography over 1,120 kilometres

Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, Rong Shu, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Xiang-Bin Wang, Feihu Xu, Jian-Yu Wang, Cheng-Zhi Peng ✉, Artur K. Ekert & Jian-Wei Pan ✉



Satellite-based entanglement distribution over 1200 kilometers

Juan Yin^{1,2}, Yuan Cao^{1,2}, Yu-Huai Li^{1,2}, Sheng-Kai Liao^{1,2}, Liang Zhang^{2,3}, Ji-Gang Ren^{1,2}, Wen-Qi Cai^{1,2}, Wei-Yue Liu^{1,2}, Bo Li^{1,2}, Hui Dai^{1,2}, Guang-Bing Li^{1,2}, Qi-Ming Lu^{1,2}, Yun-Hong Gong^{1,2}, Yu Xu^{1,2}, Shuang-Lin Li^{1,2}, Feng-Zhi Li^{1,2}, Ya-Yun Yin^{1,2}, Zi-Qing Jiang³, Ming Li³, Jian-Jun Jia³, Ge Ren⁴, Dong He⁴, Yi-Lin Zhou⁵, Xiao-Xiang Zhang⁵, Na Wang⁷, Xiang Chang⁸, Zhen-Cai Zhu⁵, Nai-Le Liu^{1,2}, Yu-Ao Chen^{1,2}, Chao-Yang Lu^{1,2}, Rong Shu^{2,3}, Cheng-Zhi Peng^{1,2,7}, Jian-Yu Wang^{2,3,7}, Jian-Wei Pan^{1,2,7}

¹Department of Modern Physics and Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China.

²Chinese Academy of Sciences (CAS) Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China.

³Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China.

⁴Key Laboratory of Optical Engineering, Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu 610209, China.

⁵Shanghai Engineering Center for Microsatellites, Shanghai 201203, China.

⁶Key Laboratory of Space Object and Debris Observation, Purple Mountain Observation, Chinese Academy of Sciences, Nanjing 210008, China.

⁷Xinjiang Astronomical Observatory, Chinese Academy of Sciences, Urumqi 830011, China.

⁸Yunnan Observatories, Chinese Academy of Sciences, Kunming 650011, China.

*Corresponding author. Email: pcz@ustc.edu.cn (C.-Z.P.); jywang@mail.stp.ac.cn (J.-Y.W.); pan@ustc.edu.cn (J.-W.P.)

– Hide authors and affiliations

AAAS Become a Member

Science

Contents ▾ News ▾ Careers ▾ Journals ▾

SHARE RESEARCH ARTICLES PHYSICS



まとめ

- 量子インターネット=
量子データのグローバルな伝送と分散量子処理を可能にする量子コンピュータNW
- アプリケーション: 研究開発の本格化はこれから
分散量子情報処理、量子センサーネットワーク、
インターネットと同じ使い方が可能かつ理論上解読不可能な暗号、etc.
- 2010年代に量子コンピュータのプロトタイプ実装が幕を開けたように、
2020年代は量子ネットワークの実装幕開け
 - 量子インターネット自体のみならず、量子コンピュータの発展にも貢献(分散処理)