資料４

量子セキュリティ/量子ネットワークの今後について

2021年12月6日

日本電信電話株式会社　特別研究員

東　浩司

量子インターネット（量子もつれ供給ネットワーク）とは？

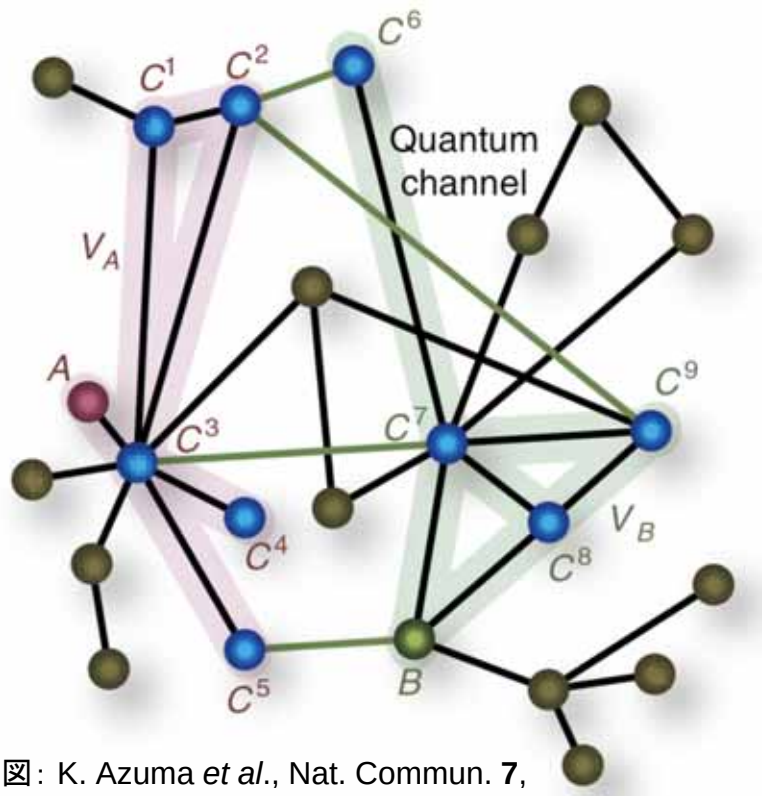
量子インターネット ―究極的には従来のインターネットの量子版

ノード：量子情報処理ノード
（例：量子中継器、量子コンピュータ）
エッジ：量子通信路
（例：光ファイバ）

物理学で許される情報処理の究極形で、分野の至高の目標

- 無条件安全な通信の提供
- 量子マネー
- 量子テレポーテーション
- 離れた原子時計の超精密同期
- 超長基線望遠鏡（天文学）
- クラウド量子計算
- リーダー選挙
- 分散量子計算
- 量子コンピュータネットワーク

S. Wehner *et al.*,
Science **362**, 303 (2018).



図：K. Azuma *et al.*, Nat. Commun. **7**, 13523 © 2016 NPG (under CC BY 4.0)

ノイズを持つ現実的な物理レイヤ（例：光ファイバネットワーク）を用いても、量子中継ができれば、効率的な量子インターネットが構築できる

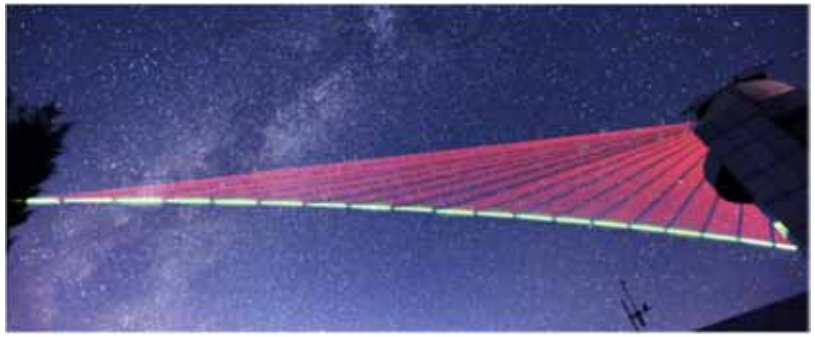
K. Azuma *et al.*, Nat. Commun. **7**, 13523 (2016).
K. Azuma & G. Kato, Phys. Rev. A **96**, 032332 (2017).

➡ 量子中継技術の開発が大事

量子通信ネットワークに関する海外の研究状況

中国：

量子通信衛星の打ち上げ
（2016年9月）



量子鍵配送と量子テレポーテーションの実験

Photo (left)：D. Castelvecchi, Nature news (15th Sep. 2016) © 2016 NPG

Photo（Right）：S.-K. Liao *et al.*, Nature **549**, 43 © 2017 NPG

EU：Quantum Internet Alliance (2018-2028)

目標：機能的なハードとソフトのサブシステムの開発、統合、デモを通じて、量子もつれに基づく量子インターネットの青写真を描く。

EU quantum flagship

コーディネーター：
Stephanie Wehner （TU Delft）

予算：10百万€ (2021年までの3年間)

Quantum Software Consortium (2017-)

目標：小規模の量子コンピュータや量子インターネット用のソフトウェア開発を目指す。

コーディネーター：
Harry Buhrman （UvA）

予算：18.8百万€

米国：National Quant. Initiative Act（2018-）

予算：12.5億＄（量子ネット研究にDOEから6.1百万$）

設置された研究部局：Chicago Quantum Exchange, Joint Quantum Institute, etc.

スタートアップ：Quantum Xchange, IonQ, etc.

日本：グローバル量子暗号通信網構築のための研究開発（総務省）（2020-2025）

目標：（トラステッドノード技術を含む）中継を用いたメッシュ型大規模量子鍵配送ネットワーク

予算：令和2年度　14.4億円上限

JST-CREST（2016- 2022）

グローバル量子ネットワーク（阪大　井元信之）

量子インターネットタスクフォース (2019-)

代表：メルカリ　永山翔太

なぜ量子中継が必要か？

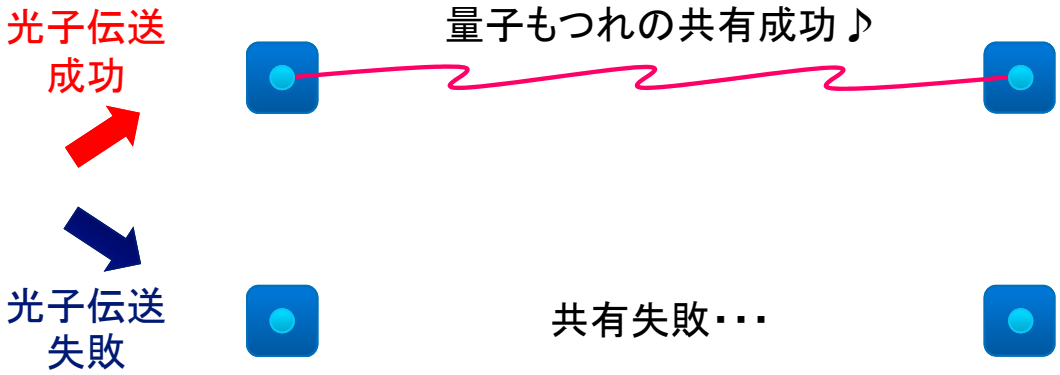
量子通信 ～ 量子もつれ共有

任意の量子通信プロトコルが実装できる。
量子もつれは量子通信の万能リソース！

これまでの量子もつれ生成方法

ポイント・ツー・ポイント（P2P）方式：

送信者が量子もつれ状態にある光子を準備し、
光子を光ファイバを通じて受信者に伝送



典型的な光ファイバの透過率：

ファイバの長さ	透過率 （光子伝送の成功確率）
50 km	～ 10 %
100 km	～ 1 %
150 km	～ 0.1%
200 km	～ 0.01%

光ファイバ中の損失によって、その透過率は50kmごとに0.1倍される

→ 長距離になるとP2P方式はほとんど失敗（400 kmが限界）

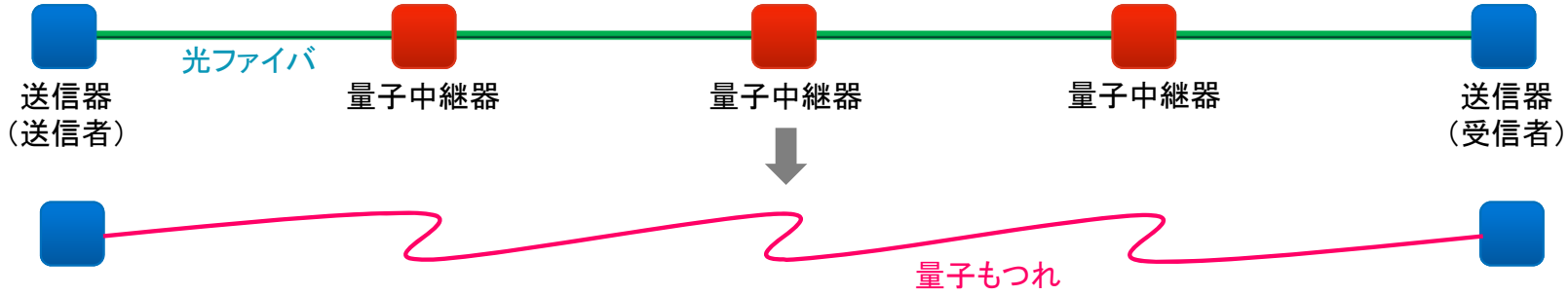
ファイバではなく、衛星を使う？

- ✓ （静止衛星でないため）通信時間が短い（約5分）
- ✓ ユーザーが限られる

→ 地球規模の量子通信には量子中継が必要

量子中継とは

量子中継の目標：量子中継器を利用した送受信者間への量子もつれ（量子通信のリソース）の提供



量子メモリに基づく中継方式

1）量子もつれ生成

①光子の伝送

②量子もつれができるまで待つ
（物質量子メモリが必要）

2）量子もつれスワッピング

③量子演算（失敗は許されない）

3）完成！

特徴：「待ち時間」/「失敗無き量子演算」が必要
⇒ メモリが必要/通信レートに制限
⇒ 量子メモリ/インターフェースが必要

反転

全光中継方式

1）量子もつれスワッピング

①量子演算（失敗が許容される）

2）量子もつれ生成

②光子の伝送

3）完成！

特徴：待ち時間なし
⇒ 多数の光子が必要/高速通信が可能
⇒ 光子源/大規模光回路が必要

NTTにおけるP2P量子通信の研究

1995 量子鍵配送（QKD）に関する
NTTでの最初の論文
PRA **51**, 1863 (1995).

PHYSICAL REVIEW A VOLUME 51, NUMBER 3 MARCH 1995

Quantum cryptography with coherent states

B. Huttner and N. Imoto
NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-01, Japan

N. Gisin
Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland

T. Mor
Department of Physics, Technion-Israel Institute of Technology, 32000 Haifa, Israel
(Received 12 July 1994)

VOLUME 89, NUMBER 3 PHYSICAL REVIEW LETTERS 15 JULY 2002

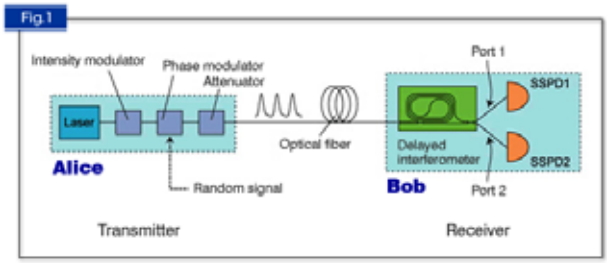
Differential Phase Shift Quantum Key Distribution

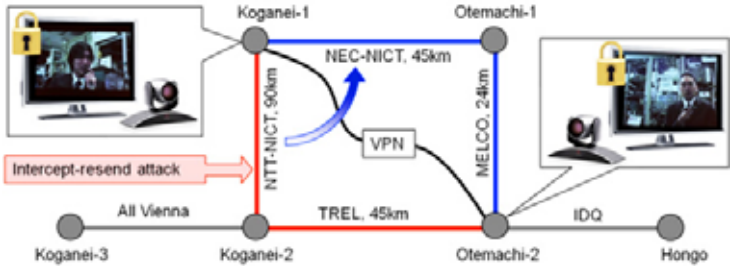
Kyo Inoue*
NTT Basic Research Laboratories, NTT Corporation, Atsugi-shi, 243-0198 Japan
and E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085

Edo Waks and Yoshihisa Yamamoto†
E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085
(Received 30 October 2001; revised manuscript received 25 March 2002; published 27 June 2002)

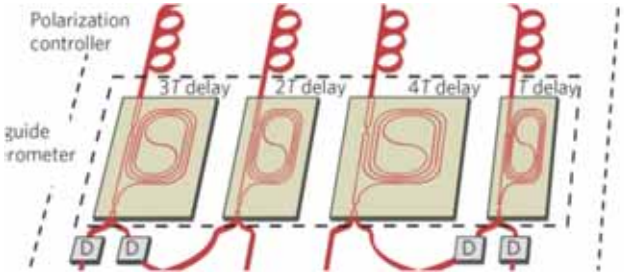
2002 差動位相シフトQKD方式の考案
PRL **89**, 037902 (2002).

2007 DPS QKDの実証実験
Nat. Photon. **1**, 343 (2007).



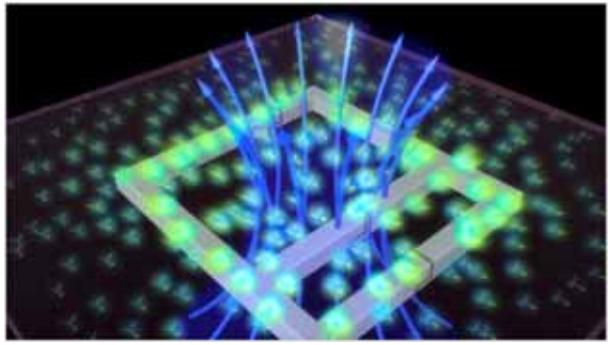


2010 東京QKDネットワークを利用
したセキュアなビデオ会議
Opt. Exp. **19**, 10387 (2011).



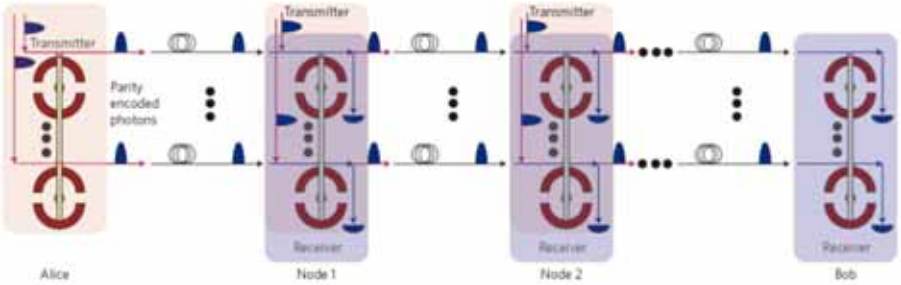
2015 RRDPS QKDの実証実験
Nat. Photon. **9**, 827 (2015).

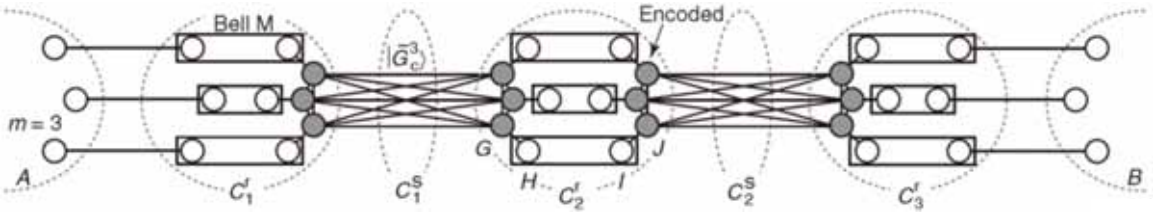
NTTにおける量子中継技術に資する研究



2011 超伝導量子ビットとダイヤモンド中の
NV中心間の量子インターフェース
Nature **478**, 221 (2011).

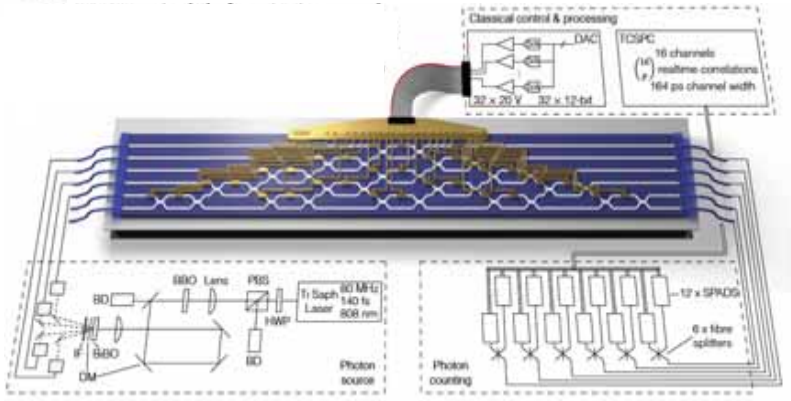
2012 メモリー機能不要の量子中継
方式の考案
Nat. Photon. **6**, 777 (2012).





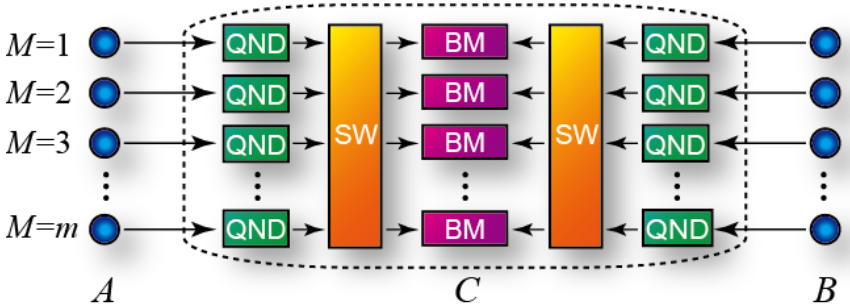
2015 全光量子中継方式の考案
Nat. Commun. **6**, 6787 (2015).

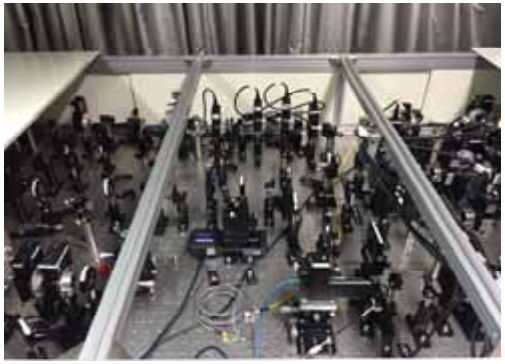
2015 プログラマブルな線形光回路の実現
Science **349**, 711 (2015).



NTTにおける量子中継技術に資する研究

2015 量子中継なしにQKDの達成距離を2倍にする方式の考案
Nat. Commun. **6**, 10171 (2015).





2019 全光量子中継の原理検証実験
Nat. Commun. **10**, 378 (2019).

2019 簡潔なセットアップでQKDの通信距離を倍にするツインフィールドQKDの提案
npj Quant. Info. **5**, 64 (2019).

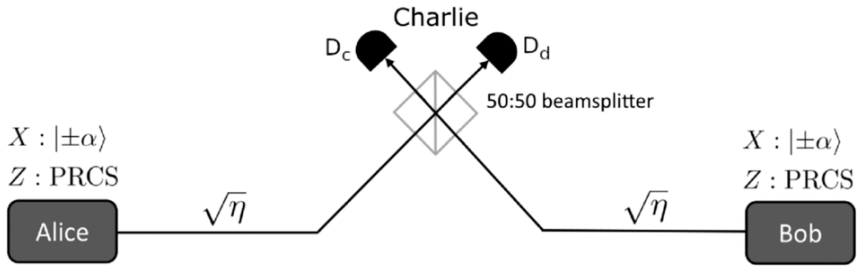
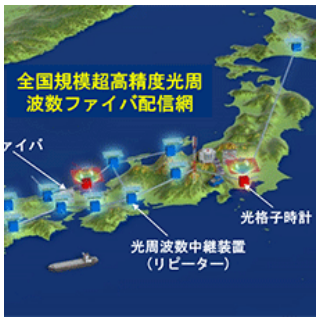


Figure from G. Currás-Lorenzo *et al.*, npj Quantum Info. **7**, 22 (2021).



2020 超高精度光周波数の240 kmファイバ伝送に成功
Opt. Exp. **28**, 7, 9186 (2020).

量子インターネット研究の今後

量子インターネットに対する学術的理解は総説論文が出る状況となってきており、成熟しつつある。
量子インターネット構築に向けて、今後必要とされるのは？

計算と通信の違い:

✓ （量子）計算機はそれ単独で機能が閉じている。
独自の規格で発展可能で、製造や販売までをも単独で行える。

✓ （量子）通信ネットワークは万人に使われることで機能性が充実し、本当に意味のあるものとなる。
あくまでインフラであるため、拡張可能なグランドデザインに基づき、協調して国家レベルで構築・拡大していく必要がある。

- ✓ テストベット構築を通じたノウハウ蓄積
- ✓ どこに量子中継器を配置すべきか？海底？衛星？
- ✓ 新しいデバイスを加えても動作するプロトコルは？
- ✓ 標準化
- ✓ 量子中継器の作成
  - 量子メモリ
  - 量子インターフェース
  - 光子源
  - 大規模光回路
  - 光子検出器など

現在の世界的動向

中国）量子中継開発と並行して、人工衛星を加えることで量子鍵配送ネットワークを拡大
Nature **589**, 214 (2021)

米国）エネルギー省が量子インターネット研究に対し、61百万ドル
From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint Workshop

欧州）デルフト工科大を中心とする「Quantum internet alliance」でプロジェクトが進行中
https://quantum-internet.team/

日本は？

量子中継/量子インターネットを主とするプロジェクトはまだない。

量子計算（矛）		量子通信（盾）
Q-LEAP: NISQコンピュータとシミュレータ	対応	総務省：グローバル量子暗号通信網構築のための研究開発（主はトラステッドノード量子暗号ネットワークの開発）
Moonshot: 誤り耐性型汎用量子コンピュータ	対応	ない（量子インターネット構築に資する研究プロジェクト？）

量子インターネット研究の今後

米国の量子インターネット開発におけるタイムラインとマイルストーン：

APPENDIX C: TIMELINE AND MILESTONES FOR QUANTUM INTERNET (see Sec. III B)

	Three year	Five year	Ten year
Major achievements	Detected photonic entanglement rate beyond 10^8 ebits/sec	Quantum repeaters with error correction against operation errors	Forward error-corrected photonic quantum states for one-way repeaters
Distance and rates	Entangled quantum memory over >10 km distance	Verifiable quantum entanglement distribution over >100 km at >1 M-ebits/sec; distillable entanglement rates >100k-ebits/sec	Quantum networks reaching transcontinental scales of thousands of km
Capability of repeater nodes	Quantum repeater node via entanglement swapping beyond direct transmission	Active error correction against operation errors; many-party protocols demonstrated in fielded quantum networks	Full error correction against loss and operation errors; hybrid nodes with different functions.
Number of repeater nodes	Quantum networks with >3 memory nodes and >10 user nodes	Networks of >10 quantum repeaters and quantum computers in superposition	Networks with >100 of repeater nodes
Free-space quantum network	Constellation of 3–5 mobile platforms demonstrated	Entanglement swapping between space earth	Transcontinental entanglement distribution via quantum-memory-enabled satellite
Quantum network applications	Quantum-secured communication rate exceeding 1 MB/sec over 100 km	Network-based quantum metrology	Blind Quantum Computing

D. Awschalom *et al.*, PRX Quantum **2**, 017002 (2021)

量子インターネット研究の今後

米国の量子インターネット開発におけるタイムラインとマイルストーン：

APPENDIX C: TIMELINE AND MILESTONES FOR QUANTUM INTERNET (see Sec. III B)

	Three year	Five year	Ten year
Major achievements	Detected photonic entanglement rate beyond 10^8 ebits/sec	Quantum repeaters with error correction against operation errors	Forward error-corrected photonic quantum states for one-way repeaters
Distance and rates	Entangled quantum memory over >10 km distance	Verifia… 誤り訂正機能付き量子中継器の作成 …gleme… >100 km at >1 M-ebits/sec; distillable entanglement rates >100k-ebits/sec	Quantum networks reach-ng transcontinental scales of thousands of km
Capability of repeater nodes	Quantum repeater node via entanglement swapping beyond direct transmission	Active error correction against operation errors; many-party protocols demonstrated in fielded quantum networks	Full error correction against loss and operation errors; hybrid nodes with different functions.
Number of repeater nodes	Quantum networks with >3 memory nodes and >10 user nodes	Networks of >10 quantum repeaters and quantum computers in superposition	Networks with >100 of repeater nodes
Free-space quantum network	Constellation of 3–5 mobile platforms demonstrated	Entanglement swapping between space earth	Transcontinental entanglement distribution via quantum-memory-enabled satellite
Quantum network applications	Quantum-secured communication rate exceeding 1 MB/sec over 100 km	Network-based quantum metrology	Blind Quantum Computing

10kmを超える量子もつれ共有

量子計測

クラウド量子計算

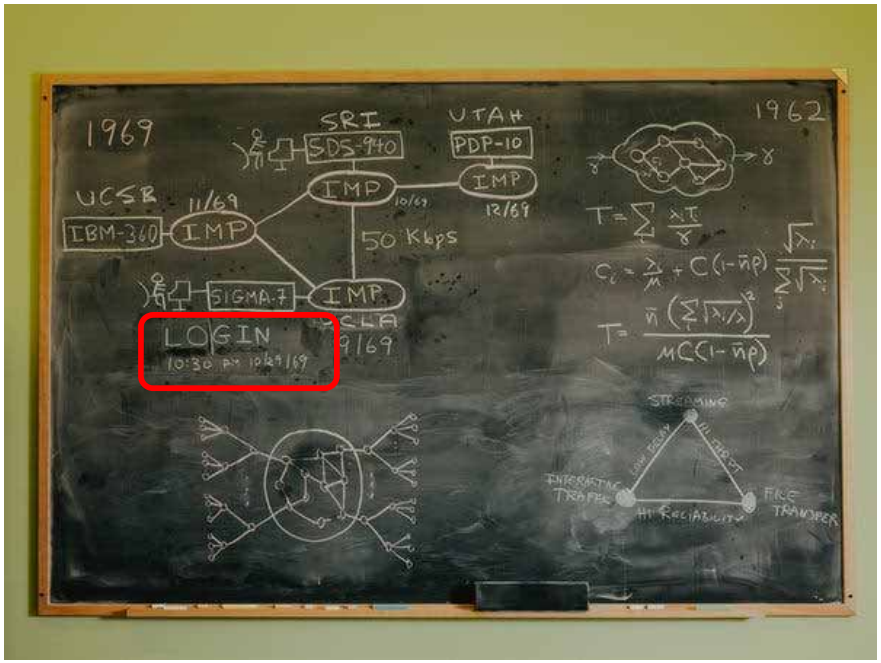
D. Awschalom *et al.*, PRX Quantum **2**, 017002 (2021)

量子インターネット研究の今後

量子インターネットを実現する価値について

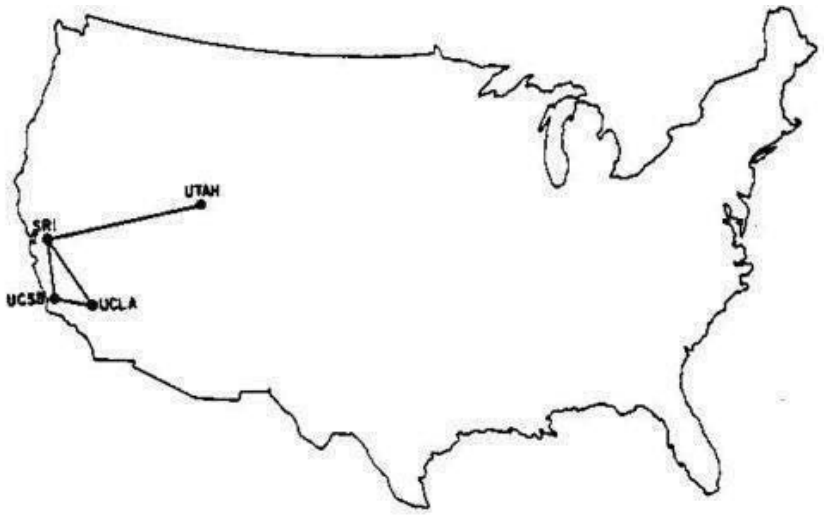
現在のインターネットの起源は1969年10月29日に作られたARPANET:

ARPANET(Advanced Research Projects Agency Network)



https://www.nytimes.com/2019/11/01/us/leonard-kleinrock-internet-50th-anniversary.html

1969/10/29



https://www.businessinsider.com/internet-in-1969-2014-1

世界最初の量子インターネット ←対応→ ARPANET

- 小規模(市内間)
- 遅い/不安定
- 機能に制限

→
- ✓ エンドツーエンド(E2E)だけで安全性が保障できる暗号通信
- ✓ 市内の量子コンピュータのクラウド利用(量子コンピュータのサプライヤーに依らずに安全利用)
- ✓ デファクト・スタンダードの獲得