

量子コンピュータと量子インターネットがある世界

株式会社メルカリ R4D(研究開発部)シニアリサーチャー
量子インターネットタスクフォース 代表
永山翔太



QUANTUM INTERNET
TASK FORCE

mercari

自己紹介: 永山翔太

- 博士(政策・メディア)
- 専門: 量子インターネットアーキテクチャ
- 活動目的: 量子技術の情報システムとしての実現
- 現在
 - メルカリ(2018.4~) R4D シニアリサーチャー
 - 量子インターネット・量子コンピュータ・量子アニーリング
 - 産学官連携研究コンソーシアム 量子インターネットタスクフォース <https://qitf.org/>
ファウンダー・ボードメンバー・代表(2019.5~)
 - 情報処理学会 量子ソフトウェア研究会 運営委員(2020.4~)
- 過去
 - 内閣サイバーセキュリティセンター 研究・産学官連携戦略 WG 委員(2020.8~2021.3)
 - IPA未踏ターゲット採択(2018~2020)
 - テーマ「分散量子計算プラットフォーム」
 - ポスドク留学(2017~2018)
 - 機械学習 @Eotvos Lorand 大学
 - 慶應義塾大学より博士号取得(2017.3)

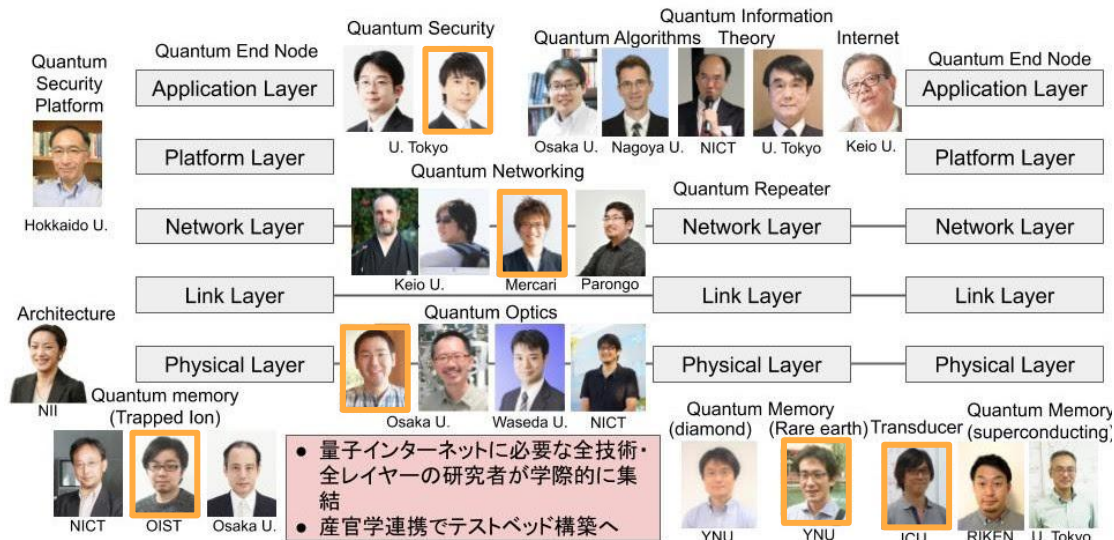


mercari **R4D**



我々の取り組み(量子インターネットタスクフォース)

- 量子で世界を繋げるために日本の貢献も必要
- 特に初期のネットワーク実証実験での存在感
- ハードからアプリまで学際的に協力して研究開発を推進する枠組みとしてQITF設立
 - 2019年5月、任意団体として設立
 - 2020年夏、慶應義塾大学に事務局を置いて正式コンソーシアム化
- 全体
 - 総会、勉強会など実施
- WG設置による議論の推進
 - インターフェースWG
 - テストベッドWG
- 若手ボードメンバー**による運営(30年先に責任を持つ)
 - 生田力三 助教(大阪大学)
 - 佐々木寿彦 講師(東京大学)
 - 佐藤貴彦 特任講師(慶應義塾大学)
 - 高橋優樹 准教授(沖縄科学技術大学院大学)
 - 達本吉朗 研究員(情報通信研究機構)
 - 永山翔太 シニアリサーチャー(株式会社メルカリ・代表)
 - 堀切智之 准教授(横浜国立大学)
 - 山崎歴舟 准教授(国際基督教大学)



- アドバイザリーボード(重鎮)によるサポート体制
 - 井元信之 特命教授(東京大学) 特任教授(大阪大学)
 - 小坂英男 教授(横浜国立大学)
 - 根本香絵 教授(国立情報学研究所)
 - Rodney Van Meter 教授(慶應義塾大学)
 - 村井純 教授(慶應義塾大学)
 - 山本俊 教授(大阪大学)

量子インターネットのホワイトペーパー

執筆体制

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



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/>

目次

- メルカリの狙い
- 量子インターネットの利用目的
- 研究開発の進捗
- 世界の大規模プロジェクトと強み
- 学会など
- 仕組み前段: 量子コンピュータの仕組み
- 量子インターネットの仕組み
- 研究紹介、インターネット技術者が取り組むべき研究開発



新たな価値を生みだす世界的な マーケットプレイスを創る

Create value in a global marketplace where anyone can buy & sell

A background image showing a group of people, including children and adults, sitting around a table and playing with colorful LEGO bricks. The scene is brightly lit, suggesting an indoor setting with large windows.

mercari R4D

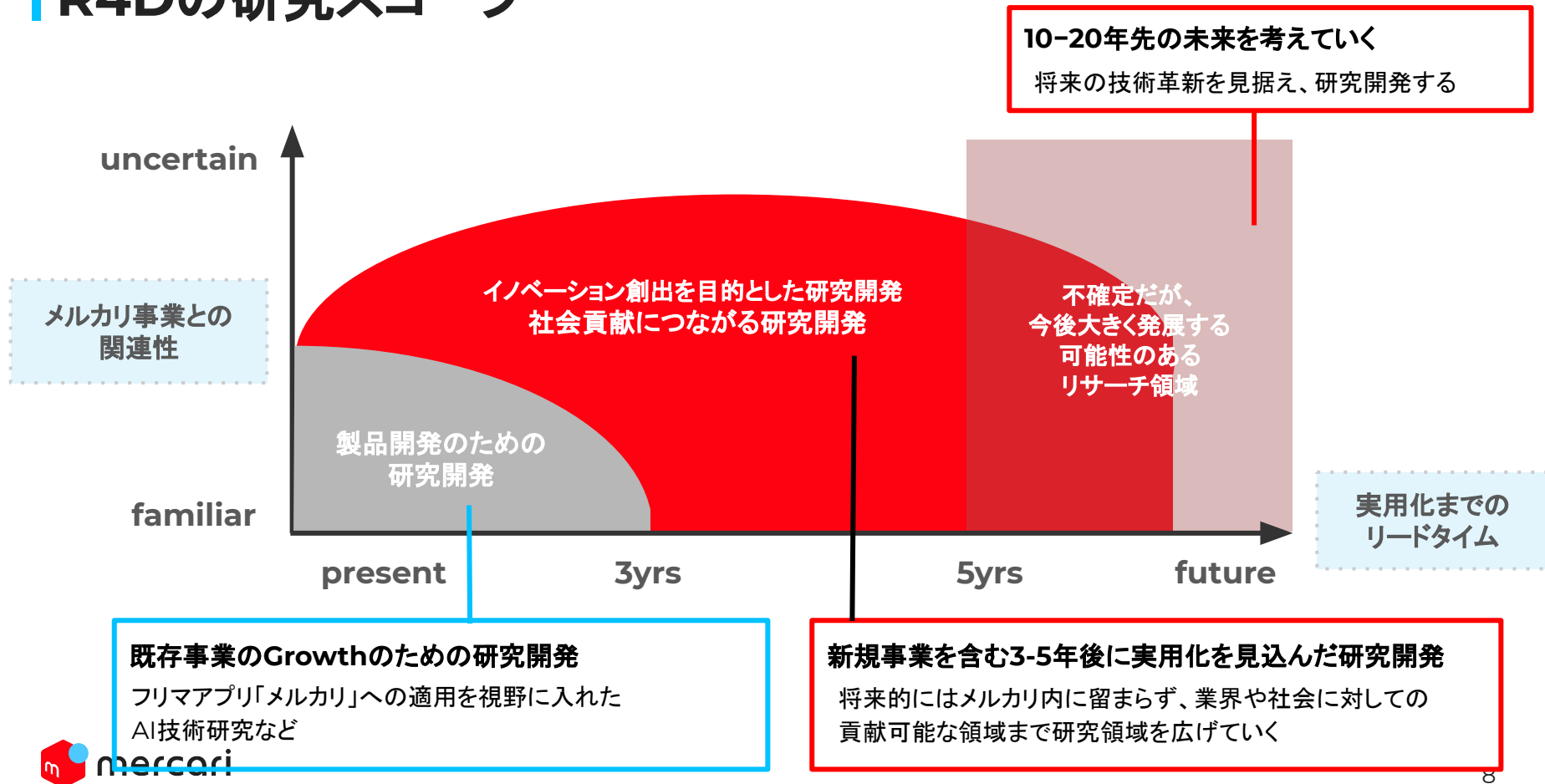
Research for

Design
Development
Deployment
Disruption

mercari R4Dは、株式会社メルカリが2017年12月に設立した社会実装を目的とした研究開発組織です

R4Dには、研究(Research)に加えて、設計(Design)・開発(Development)・実装(Deployment)・破壊(Disruption)という4つのDを意味する言葉が含まれており、主に3～5年後のメルカリの未来を作る研究開発に取り組んでいます

R4Dの研究スコープ



“新たな価値を生み出す世界的なマーケットプレイスを創る”

メルカリのミッションを実現するための研究開発

価値交換

Poimo

LCA

DIGITAL MEASUREMENT

安心・安全

ELSI研究

Biometrics

FAKE DETECTION

D&I

Inclusive Design

評価研究

INTERNATIONALIZATION

価値交換工学

上記を支えるインフラ技術

AI

Blockchain

量子情報技術

メルカリにおける量子情報技術領域、外部との連携状況

量子インターネット

目的:

量子コンピュータ・デバイスがグローバルに繋がる「次世代インターネット」による安心・安全なメルカリの実現。

期待される成果:

- ①Best effortかつEnd to endで動く「量子のTCP/IP」の開発
- ②情報技術・物理の専門家らを巻き込んだテストベッドの運用や検証

共同研究先



量子コンピューター

目的:

配送経路や売買マッチング等、メルカリにおける最適化問題の解決。大規模データの機械学習の性能向上。

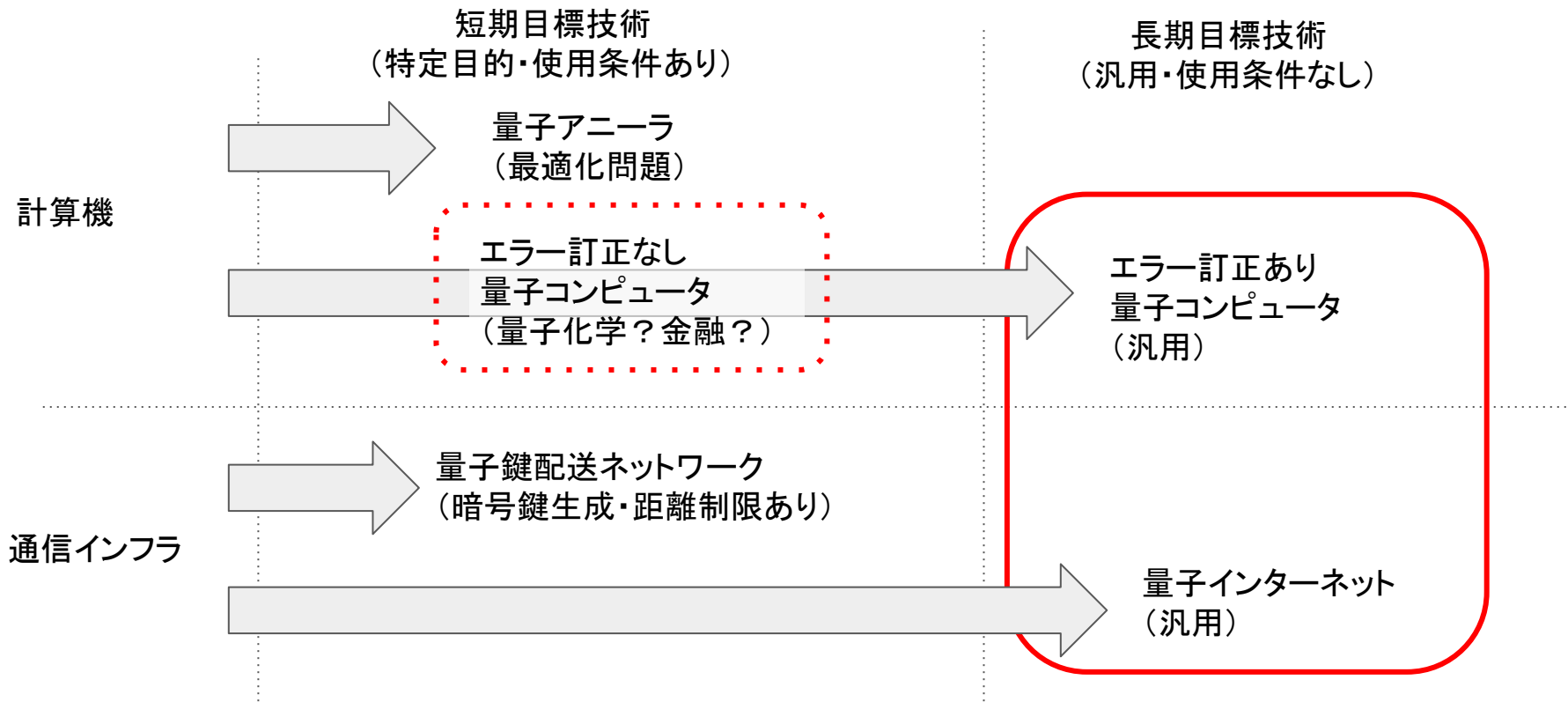
期待される成果:

- ①量子アニーラの有益性を引き出すアルゴリズムの開発
- ②ゲート型量子コンピューターにおけるアルゴリズム開発

共同研究先

- 慶應義塾大学
- 大阪大学
- 株式会社QunaSys
- 産業技術総合研究所

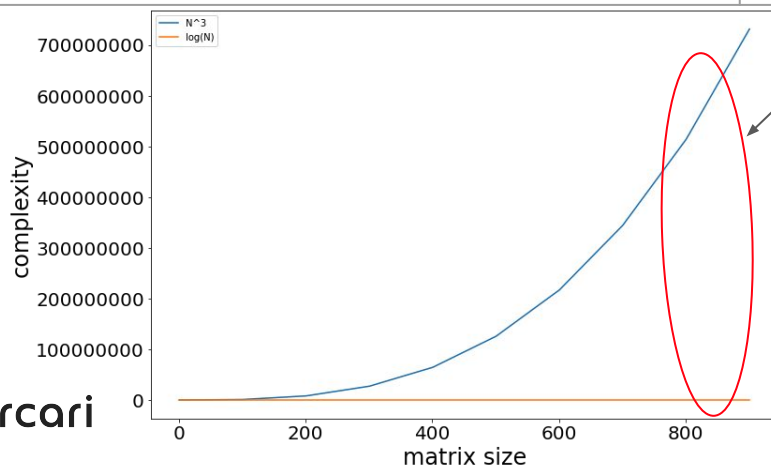
メルカリでの量子情報技術の整理



メルカリで取り組む必要があるもの

メルカリと計算、そして量子コンピュータ

メルカリでの課題	量子コンピュータによるソリューション
信用リスク評価、需要予測	確率微分方程式(不確実な未来を予測可能にする)
投資戦略、意思決定への応用	非線形微分方程式(複雑な未来を予測可能にする)
個人ごと、商品ごとの最適化	量子機械学習、最適化問題(最適な一手を予測可能にする)



解きたい領域

R4D量子チームの研究(確率微分方程式)

[Variational quantum simulations of stochastic differential equations](#)
Kubo, Nakagawa, Endo, Nagayama [2020]

エラー訂正なし量子コンピュータ

- エラー管理
 - エラーが発生する前に計算が終われば OK
 - 何度も同じ計算を繰り返して、結果の平均を取ればエラーは紛れるのではないか？
- 用途
 - 量子化学と金融が有力か？
- メルカリ
 - 金融で使えるならメルカリ(メルペイ)でも使い道があり、有益

R4D量子チームの研究(確率微分方程式)

[Variational quantum simulations of stochastic differential equations](#)
Kubo, Nakagawa, Endo, Nagayama
[<https://arxiv.org/abs/2012.04429>, 2020]

エラー訂正あり量子コンピュータ

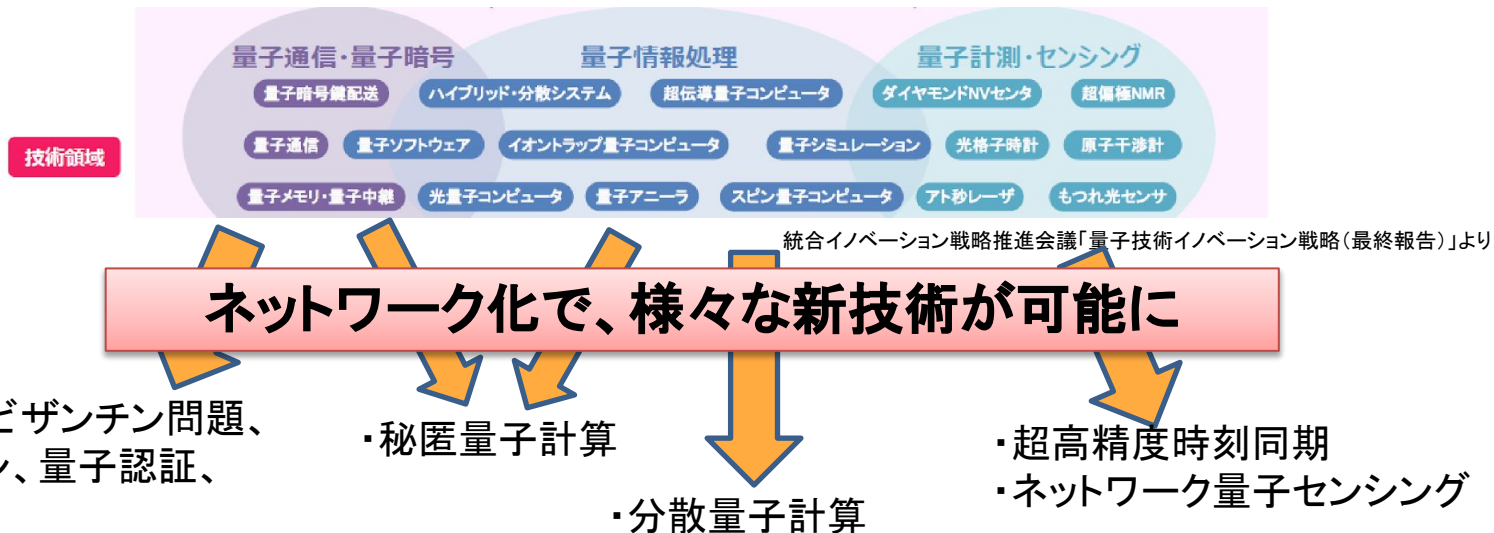
- 量子コンピュータの本命
- エラー管理
 - エラー訂正するので問題なし
- 用途(多岐)
 - 量子の性質をそのまま使う: 超多項式的加速
 - 量子シミュレーション → 創薬、材料開発
 - 問題の構造をexploit: 超多項式的加速
 - 素因数分解、離散対数問題、パターンマッチング、半正定値計画問題(近似)、逆行列計算、etc.
 - 汎用的に干渉を取り扱う: 多項式的加速
 - 逆関数計算(検索)、etc.
- メルカリでの生の声(例)
 - 「逆行列計算 $\log(N)$ ができるの **すご**
 - 「逆行列計算の高速化ができるといういろいろ便利 ...より興味が増した！」

メルカリと通信、そして量子情報技術

- 全てのお客様とメルカリを繋ぐ最重要インフラ
- 決済情報・個人情報・購買履歴などプライバシー情報満載
- 量子コンピュータによる暗号の危殆化
 - 大問題！
 - 余談だけど、これは悪いことじゃない。むしろ、既存の暗号技術が、人類の科学の未熟(素因数分解できない)をうまく突いていただけ
- サステナブルな安心・安全な通信とは？
 - 量子インターネットによる End-to-End 量子暗号技術

量子インターネットの利用目的

量子インターネットとは、量子情報のネットワーク化



「量子インターネット」= 量子技術・情報のネットワーク化を追求する技術分野

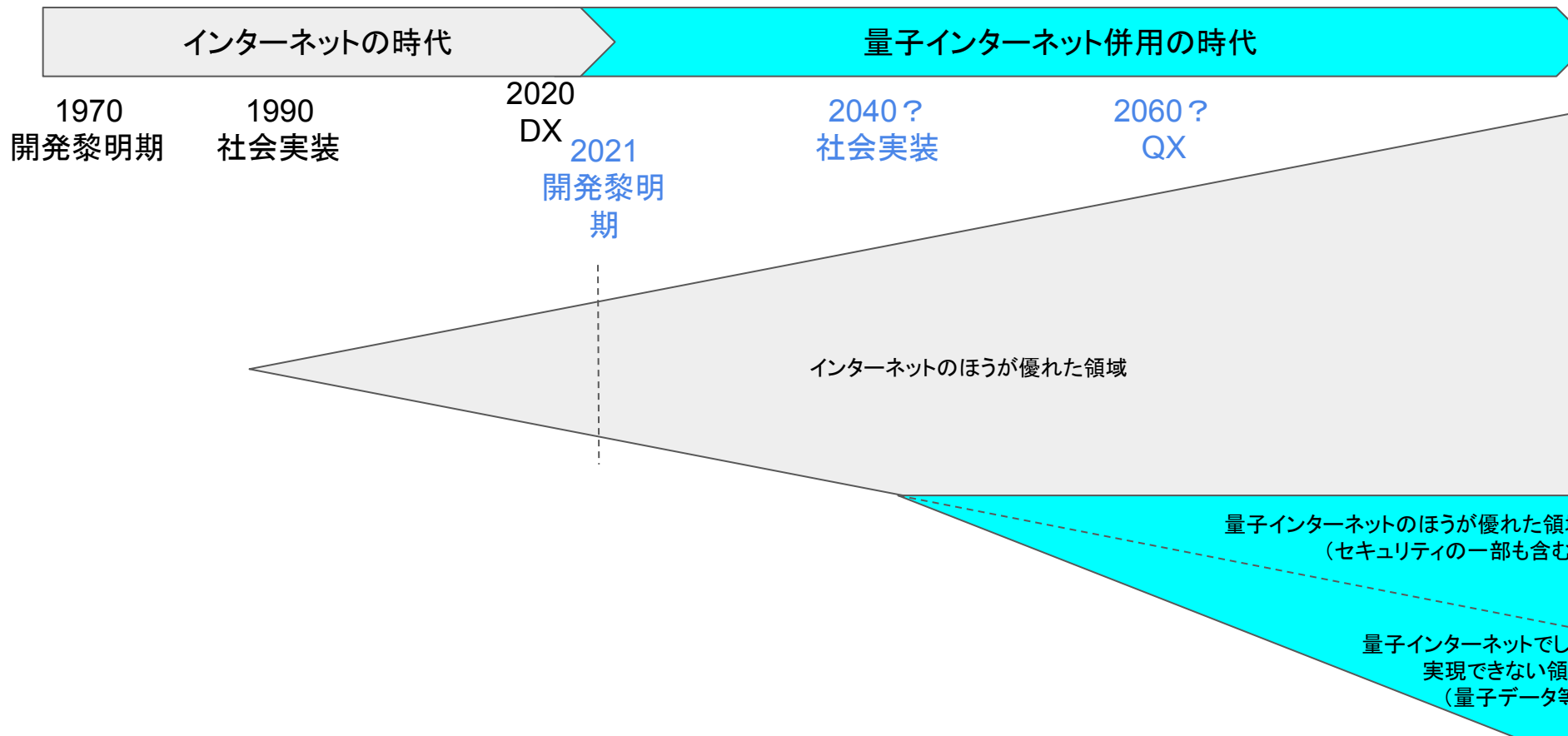
従来のインターネットが計算機・センサーなどを繋ぎ始めて新たな領域に。

→ 量子技術をネットワーク化するのも自然な流れ

➡ 最終出口: 量子技術・情報の広域通信プラットフォーム

(インフラとしての「量子インターネット」)

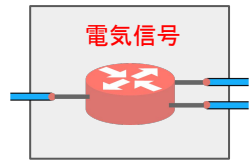
ユースケース・情報通信市場の発展イメージ



研究開発の進捗

量子インターネットマイルストーン

①



量子信号は一旦
古典電気信号に変換

アプリケーション

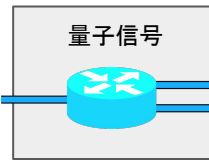
古典中継の量子暗号

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

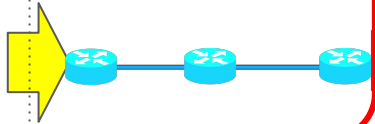


量子信号中継
Proof of Concept
実験室内

- 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

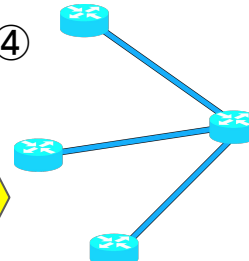
アプリケーション

- 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

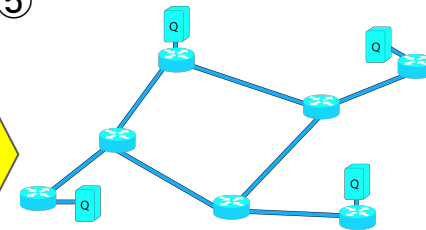
都市規模 量子インターネット

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
- 量子秘密分散
- 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

世界の大規模プロジェクトと強み

世界の量子インターネット施策と特徴・ 国際協力のカウンターパート候補

EU: Quantum Internet Alliance

2021年までの3年総額

約12.4億円

- 量子信号中継(ダイヤモンド量子ビット)をいち早く実証
- ボトムアップ型研究に強み

中国: Jian-Wei Panのグループによる研究

CQN(Arizona, Harvard, Yale, MIT) によるNSF予算のテストベッド

DoE

BOUGHTON ROAD TOLL PLAZA

Argonne NATIONAL LABORATORY

米国: National Quantum Initiative

United States: National Quantum Initiative

Quantum center

Including 80-mile QI testbed

6600万ドル (2021)

3900万ドル (2020)

Quantum Internet Individual Budget

[DoE]

1億ドル (req. For each 2022-26)

2500万ドル (2021)

[NSF]

4585万ドル (req. 2022)

3586万ドル (2021)

3271万ドル (2020)

[NIST]

\$10 million (req. for each 2022-26)

- 2020年に突然力を入れ始める・政府主導。量子暗号の発案者を擁する



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)

DoE



ドイツ: Quantum Link Extention

2021年までの3年総額
約18.3億円

プロジェクト
テストベッド

シンガポールの大学(複数)

オーストラリアの大学(複数)

学会など

Quantum Internet Research Group

- <https://datatracker.ietf.org/rq/qirg/about/>
- (共同)チェア
 - Rodney Van Meter (Keio Univ.)
 - Wojciech Kozlowski (QuTech/TU Delft)
 - Stephanie Wehner (Quantum Internet Alliance 主宰)と交代
- メーリングリスト: <https://irtf.org/mailman/listinfo/qirg>
- Charter で明言されてるテーマ
 - Routing
 - Resource allocation
 - Connection establishment
 - Interoperability
 - Security
 - API design
 - Applications for a Quantum Internet
 - Multi-party states and multi-party transfers such as network coding

一番ホットなI-D

- Architectural Principles for a Quantum Internet
- <https://datatracker.ietf.org/doc/draft-irtf-qirg-principles/>

Architectural Principles for a Quantum Internet 構成

いつもの量子の基本の話

- 1. Introduction 3
- 2. Quantum information 4
 - 2.1. Qubit 4
 - 2.2. Multiple qubits 5
- 3. Entanglement as the fundamental resource 6
- 4. Achieving quantum connectivity 7
 - 4.1. Challenges 8
 - 4.1.1. The measurement problem 8
 - 4.1.2. No-cloning theorem 8
 - 4.1.3. Fidelity 8
 - 4.1.4. Inadequacy of direct transmission 9
 - 4.2. Bell pairs 9
 - 4.3. Teleportation 10
 - 4.4. The life cycle of entanglement 11
 - 4.4.1. Elementary link generation 11
 - 4.4.2. Entanglement swapping 12
 - 4.4.3. Error Management 13
 - 4.4.4. Delivery 16



通信に着目したときの量子の基本の話

量子インターネットアーキテクチャと基本概念

- 3. Architecture of a quantum internet 16
 - 5.1. Challenges 16
 - 5.2. Classical communication 18
 - 5.3. Abstract model of the network 19
 - 5.3.1. One control plane and two data planes 19
 - 5.3.2. Elements of a quantum network 19
 - 5.3.3. Putting it all together 21
 - 5.4. Network boundaries 22
 - 5.4.1. Boundaries between different physical architectures 22
 - 5.4.2. Boundaries between different administrative regions 22
 - 5.4.3. Boundaries between different error management schemes 22
 - 5.5. Physical constraints 23
 - 5.5.1. Memory lifetimes 23
 - 5.5.2. Rates 23
 - 5.5.3. Communication qubits 23
 - 5.5.4. Homogeneity 24
- 6. Architectural principles 24
 - 6.1. Goals of a quantum internet 24
 - 6.2. The principles of a quantum internet 27
- 7. Comparison with classical networks 29
- 8. Security Considerations 31
- 9. IANA Considerations 31
- 10. Acknowledgements 31
- 11. Informative References 31
- Authors' Addresses 36

現行インターネットとの比較

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

| IEEE/ACM

- IEEE Transactions on Quantum Engineering
 - <https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8924785>
- ACM
 - SIGCOMMでもちよくちよく発表される

取り組むべき研究開発

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 (今の量子イノベ戦略は量子中継のハード開発しか書いていない)

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

必要
源管
今の
→し
→量

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

- 計
- 多くの応用は全ての物理系(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.)

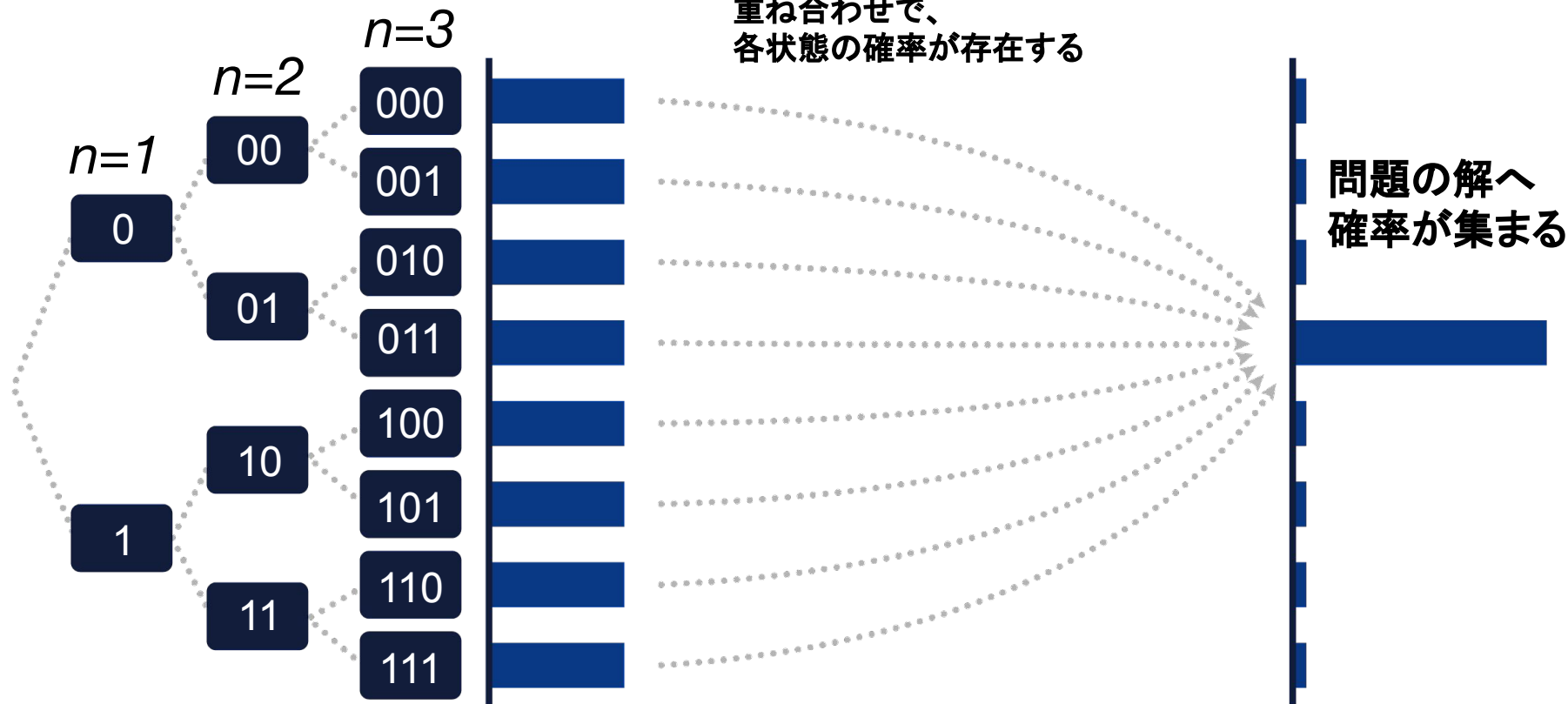
様々な領域の研究者が連携して統合的に進めないと良いものにならない

産・官・学・民によるエコシステムの重要性

- 自由な開かれたインフラを作っていくために、エコシステムが重要
- インターネットの健全な発展にはマルチステークホルダーによる自由なエコシステムが必要
 - インターネットが成功した鍵＝自律分散協調
 - 技術的のみならず社会的にもスケール
 - 特定の中央集権的な主体を持たない
 - 産・学・官のマルチステークホルダーが各々のネットワークを管理・運用し、連携して相互接続して世界規模インフラを構築
 - 民を含むユーザが自由に事業者や利用サービスを選ぶことにより、競争と自浄作用が生まれる
- ちょっと早くも思える今エコシステムを作り始め、量子インターネットのあるべき姿について検討し、プロトタイプを作っていくべき

仕組み前段：量子コンピュータについて

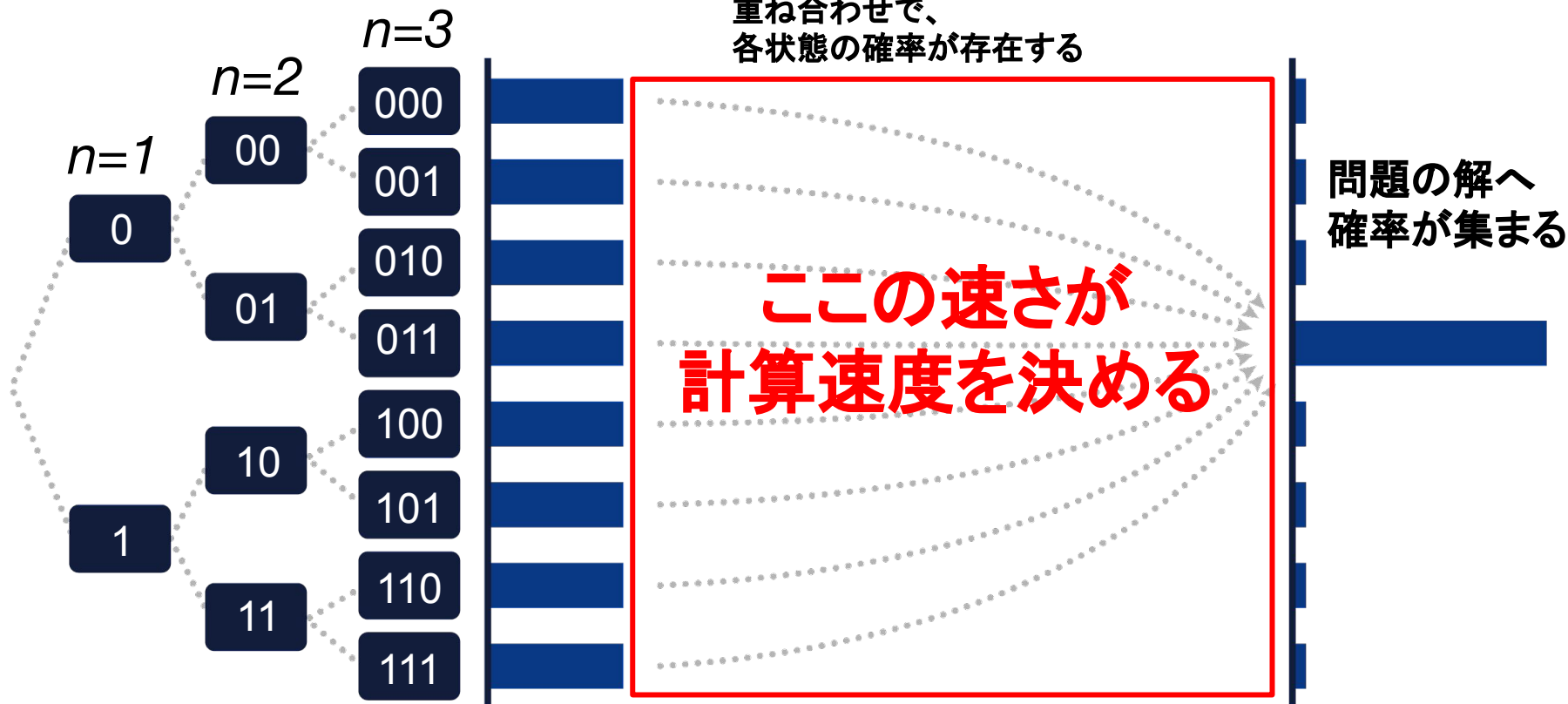
量子コンピュータとは



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

重ね合わせで、
各状態の確率が存在する



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**
 - 「逆行列計算の高速化ができるといういろいろ便利 ...より興味が増した！」

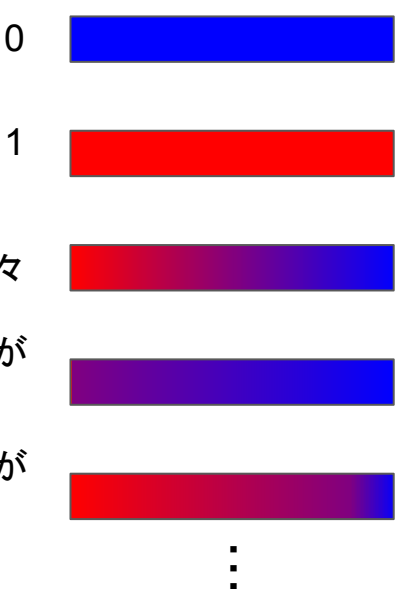
何故こうなってるかは人類の誰も知らないが、自然現象がそうなってるから便利に使おう！

量子コンピュータ(というか量子力学)のふしぎ1

古典コンピュータ



量子コンピュータ



量子状態の
「重ね合わせ」

0と1が半々
かなり0っぽい
1っぽいもある
かなり1っぽい
0っぽいもある

何故こうなってるかは人類の誰も知らないが、自然現象がそうなってるから便利に使おう！

量子コンピュータ(というか量子力学)のふしぎ2

量子状態の定式化

基底ベクトル $|0\rangle$ 基底ベクトル $|1\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

0っぽさ
(複素数)

1っぽさ
(複素数)

量子状態の
「重ね合わせ」

量子コンピュータ



0と1が半々



かなり0っぽいが
1っぽさもある



かなり1っぽいが
0っぽさもある



⋮

何故こうなってるかは人類の誰も知らないが、自然現象がそうなってるから便利に使おう！

量子コンピュータ(というか量子力学)のふしぎ3

- 量子もつれ

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

- 25% $|00\rangle$
- 25% $|01\rangle$
- 25% $|10\rangle$
- 25% $|11\rangle$

2量子状態
の4基底

2量子状態

$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

分解可能
(違う量子なので当然)

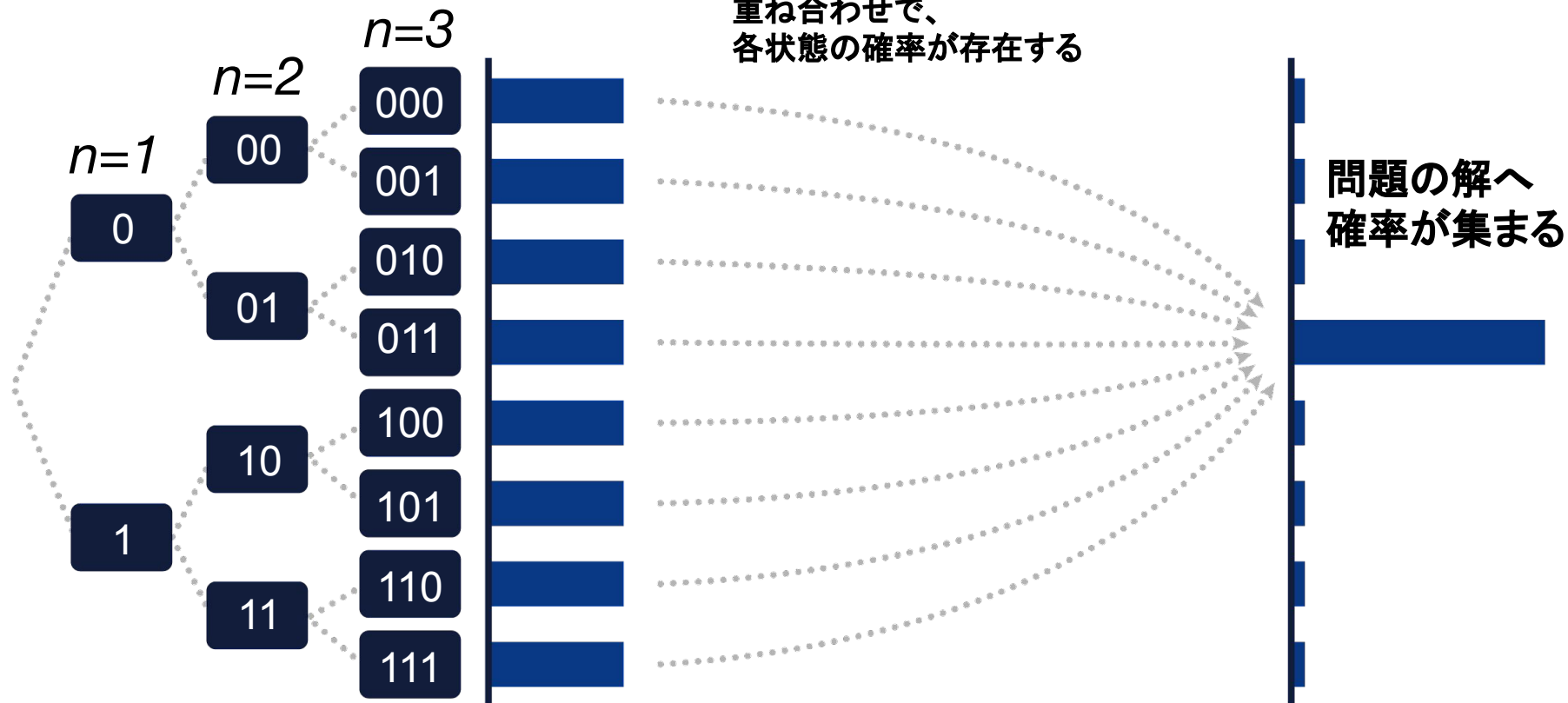
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- 50%
- 0%
- 0%
- 50%

$$= \frac{1}{\sqrt{2}} \left[\begin{array}{|c|} \hline ? \\ \hline \end{array} \right] \otimes \left[\begin{array}{|c|} \hline ? \\ \hline \end{array} \right]$$

分解可...不可能！？→エンタングルメント(量子もつれ)

量子コンピュータとは



量子インターネットの仕組み

量子インターネットの基本方針

- E2Eでエンタングルメントを作る
 - 量子通信の基本リソースをまず作る
 - 作り直し自由！
- 作ったエンタングルメントを使って量子テレポーテーションする
 - 量子情報の伝送
 - 大切な情報は、インターネットのようにロスしうる環境を通さない

量子インターネットの実際

データプレーン
(量子プレーン)

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

どっちかが0ならもう一方も0

どっちかが1ならもう一方も1

0か1かは測定してみるまでわからないという相関(いわゆる量子相関)

エンタングルメント(運命の赤い糸)

量子さん



エラー
(時間依存)



- エラー管理
- ルーティング管理
- リンク管理
- 到達(エンタングルメント生成)確認
- Swap管理
- コネクション管理
- etc.



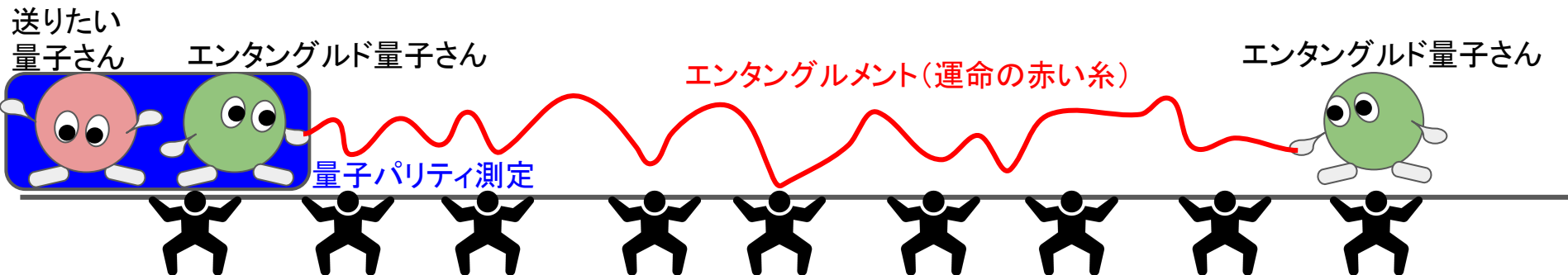
メモリ揮発



コントロールプレーン
(現行インターネットプレーン)

エンタングルメント(量子相関)を消費して量子データを送受信できる(量子テレポーテーション)

データプレーン
(量子プレーン)



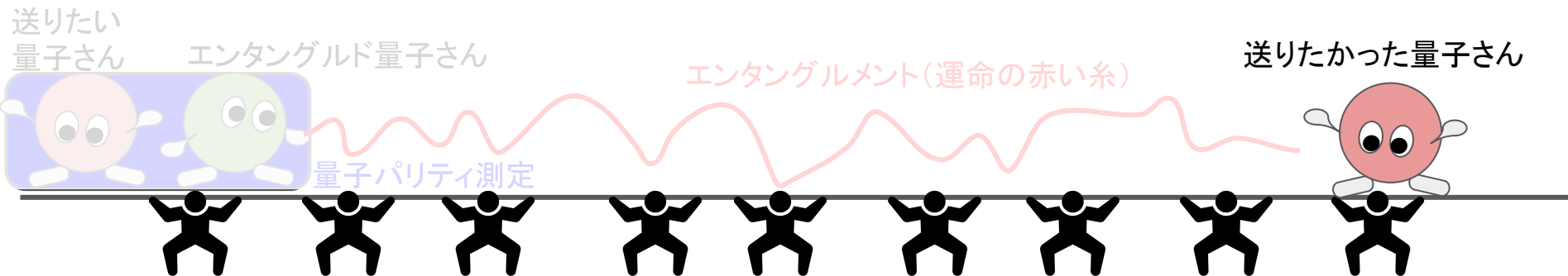
コントロールプレーン
(現行インターネットプレーン)



測定結果の
データ

エンタングルメント(量子相関)を消費して量子データを送受信できる(量子テレポーテーション)

データプレーン
(量子プレーン)



コントロールプレーン
(現行インターネットプレーン)

困難1:光子ロス

- ファイバー自体も物質なので、ファイバー内を光子が進行中に、原子に吸収されてしまう可能性がある
 - Attenuation rate: 22km毎に $1/e$ に減衰していく
 - →Direct Transmissionの限界
- 中継地点でいわゆる「増幅」をできない(吸収されてしまった光子は取り戻せない)ので、大変厄介な話
 - したがって、中継ノードがあっても、hop by hopで送る限り、距離に比例して到達率が指数的に0に近づく
 - →hop by hopの限界
- →大事なデータを失ってしまう恐れ

I 困難2: 量子複製不可能定理

- 量子状態はクローン(コピー)できないという定理
- 複製不可能定理のせいで、量子データはバックアップを取れない
- →失われたデータを復帰できない

量子インターネットの実際

データプレーン
(量子プレーン)

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

どっちかが0ならもう一方も0

どっちかが1ならもう一方も1

0か1かは測定してみるまでわからないという相関(いわゆる量子相関)

エンタングルメント(運命の赤い糸)

量子さん



エラー
(時間依存)



- エラー管理
- ルーティング管理
- リンク管理
- 到達(エンタングルメント生成)確認
- Swap管理
- コネクション管理
- etc.



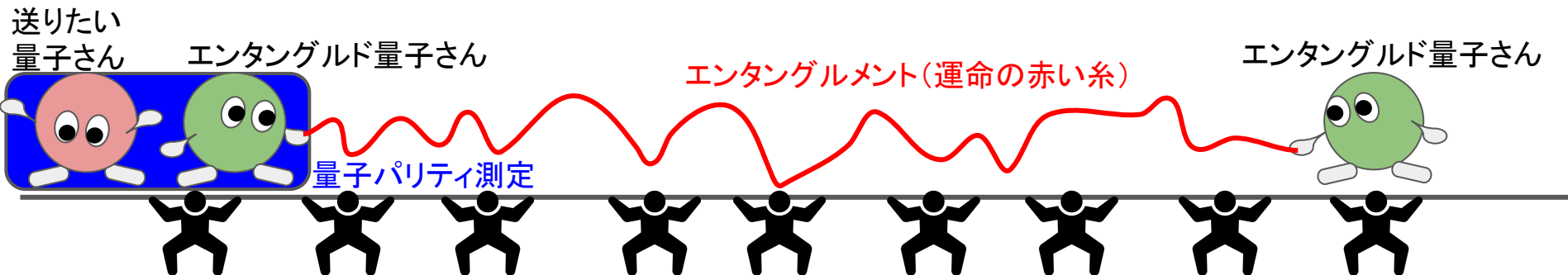
メモリ揮発



コントロールプレーン
(現行インターネットプレーン)

エンタングルメント(量子相関)を消費して量子データを送受信できる(量子テレポーテーション)

データプレーン
(量子プレーン)



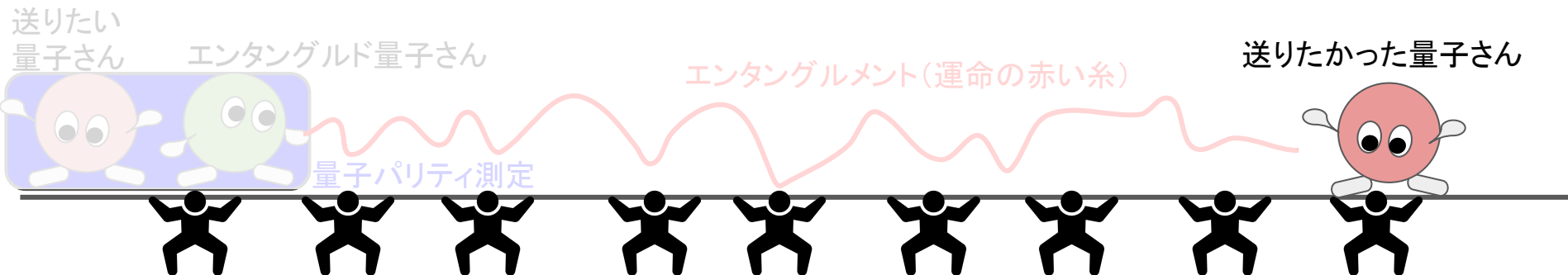
コントロールプレーン
(現行インターネットプレーン)



測定結果の
データ

エンタングルメント(量子相関)を消費して量子データを送受信できる(量子テレポーテーション)

データプレーン
(量子プレーン)



コントロールプレーン
(現行インターネットプレーン)

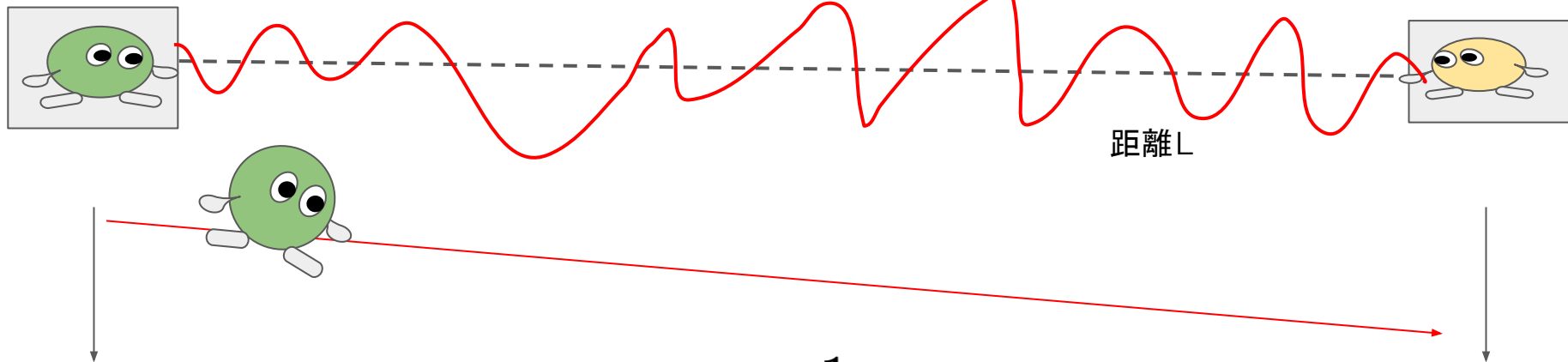


測定結果の
データ

量子インターネットの基本方針

- **E2Eでエンタングルメントを作る**
 - 量子通信の基本リソースをまず作る
 - 作り直し自由！
- **作ったエンタングルメントを使って量子テレポーテーションする**
 - 量子情報の伝送
 - 大切な情報は、インターネットのようにロスしうる環境を通さない

困難3: 光子ロス (again; 通信速度への影響)



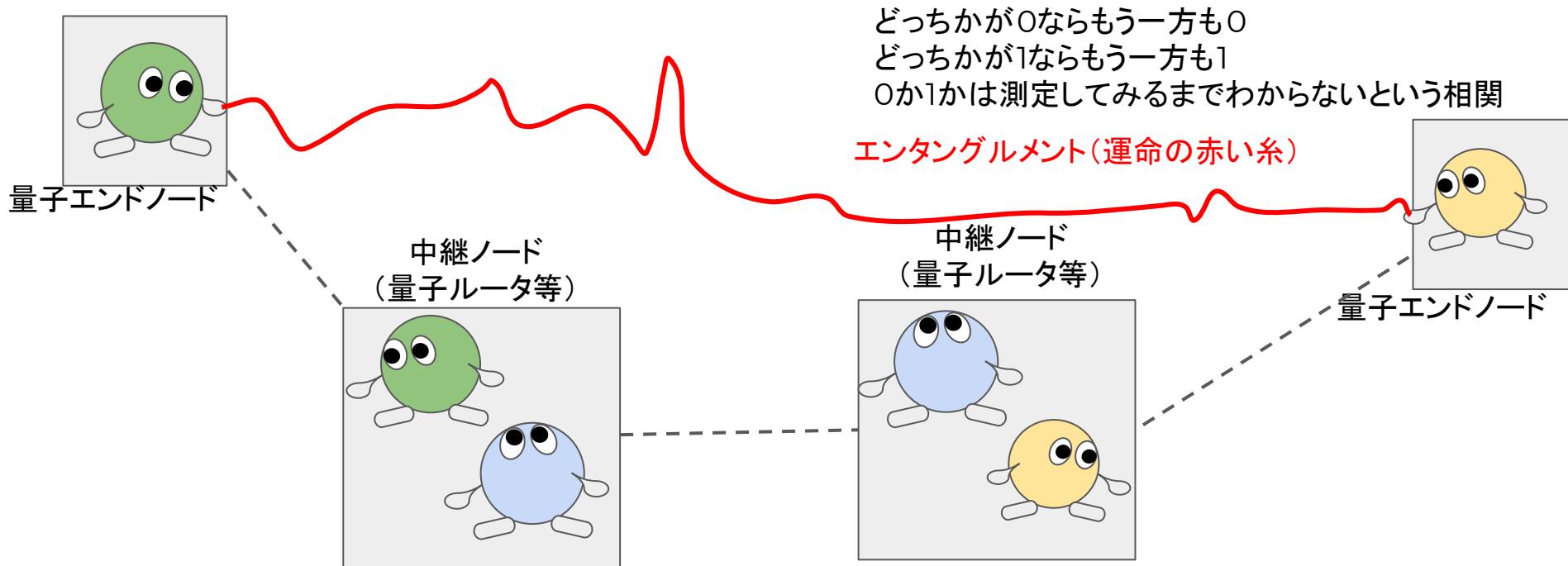
到達確率 $\frac{1}{e^{\frac{L}{22}}}$

正確には $\frac{1}{e^{\frac{L}{L_0}}}$

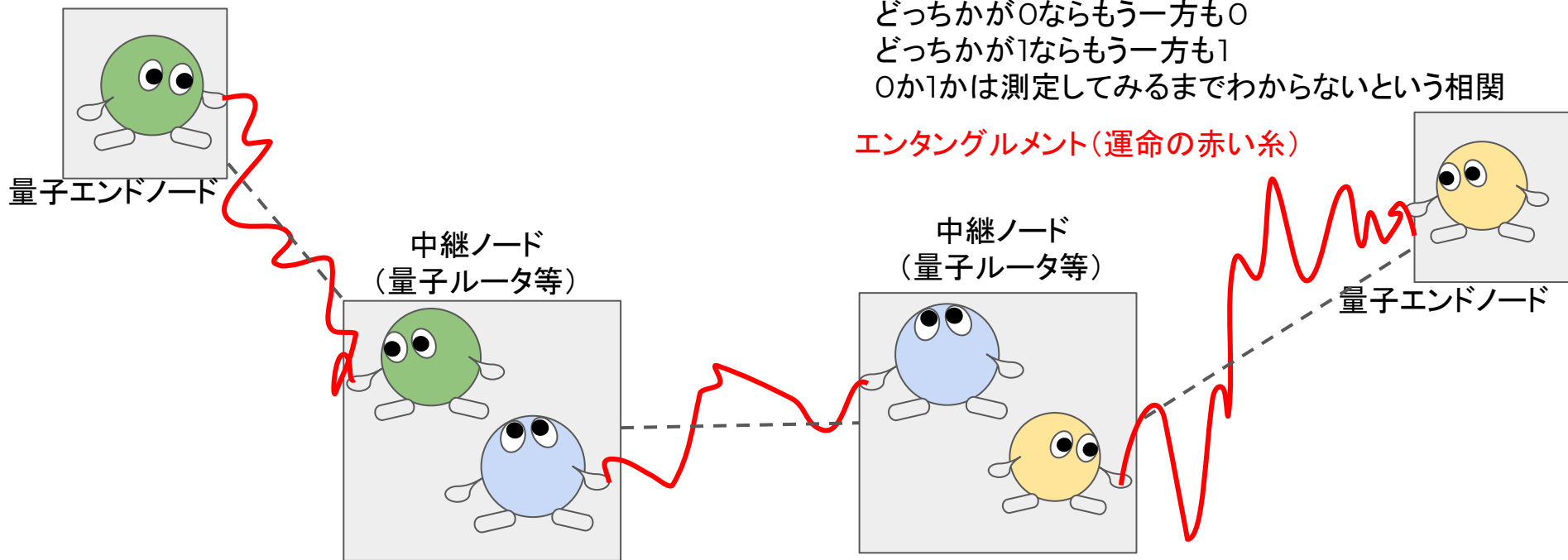
長距離を飛ばしたり、届いたものを hop by hop で転送すると、指数的に到達数が減っていく

L_0 : 減衰しにくさの度合い
→ 約22kmで1/e倍

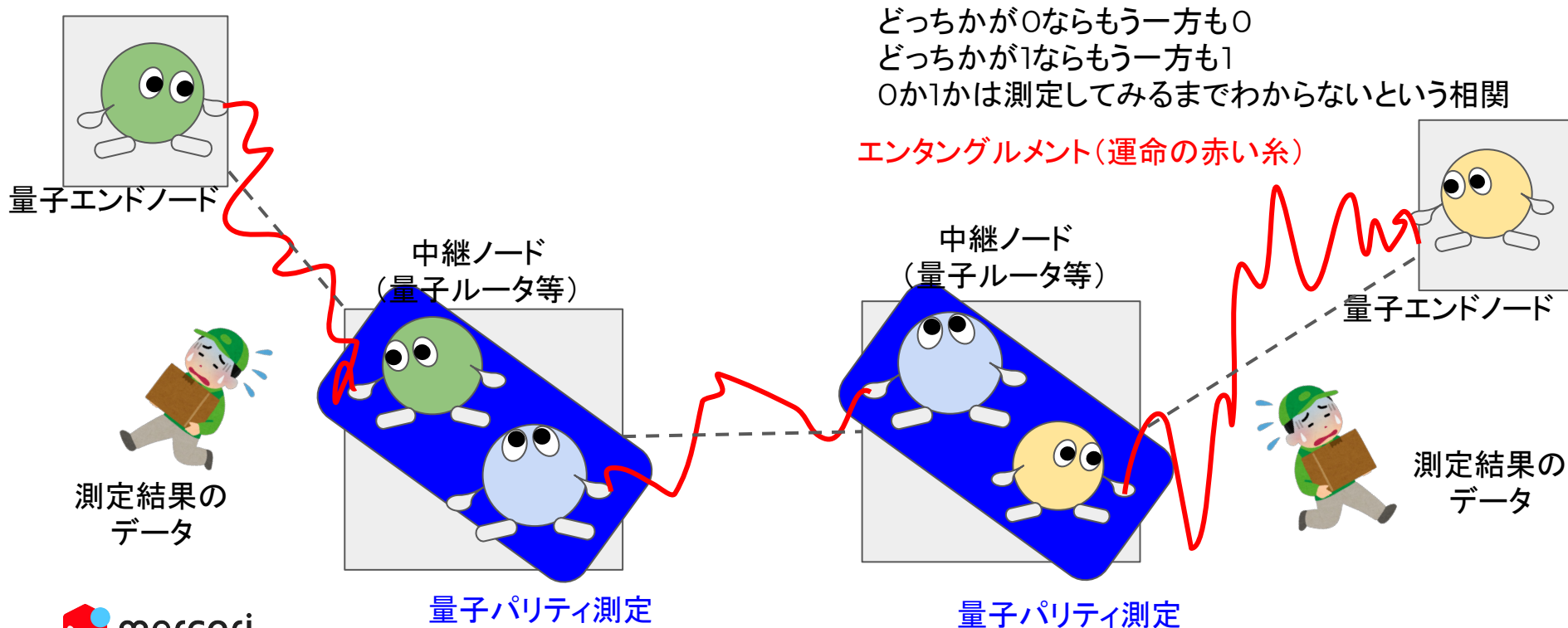
量子インターネットに必要なのは、データ送信ではなく、 ”量子相関”の作成



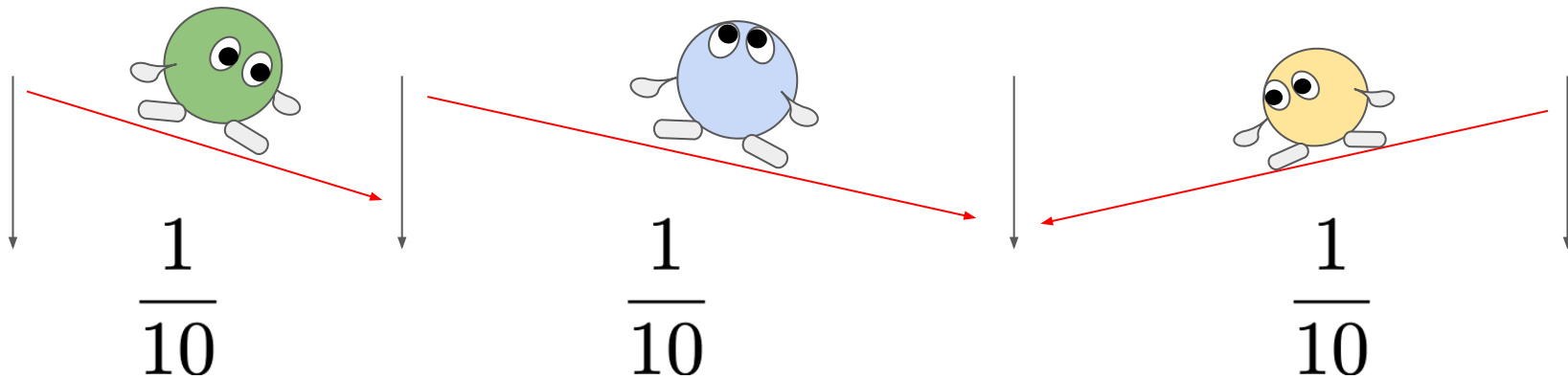
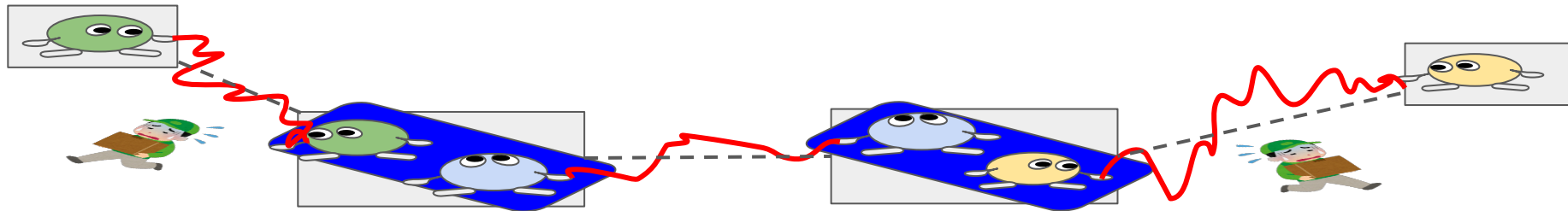
量子インターネットに必要なのは、データ送信ではなく、 ”量子相関”の作成



Entanglement Swapping と呼ばれる(量子)パリティ測定



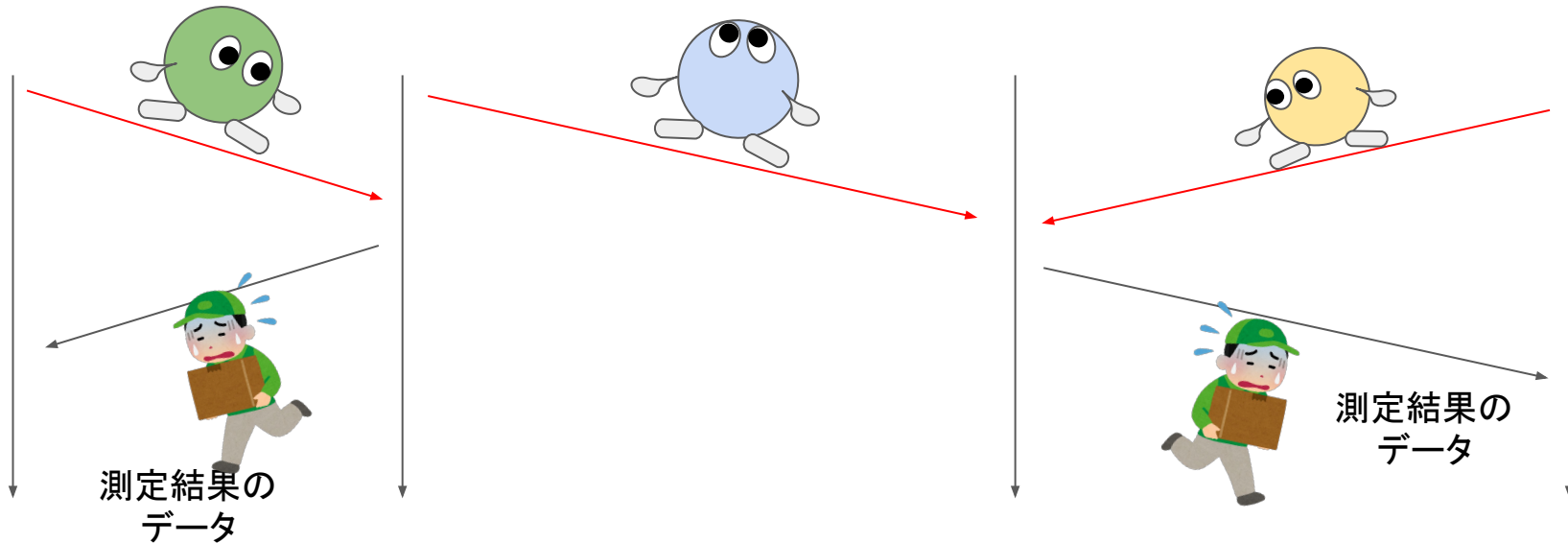
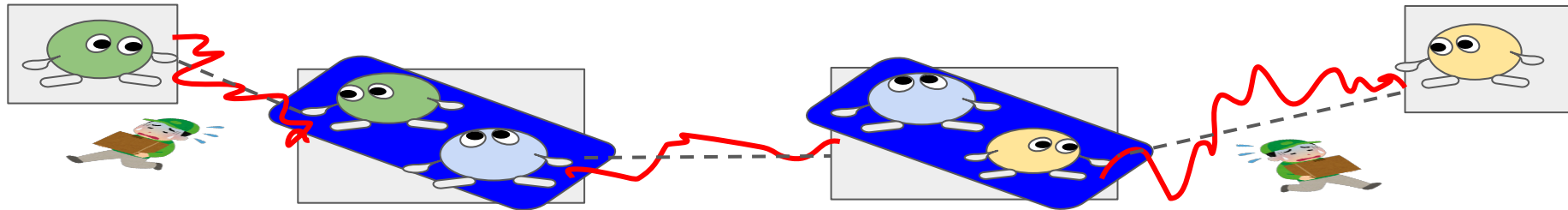
各リンクで量子もつれを作って繋げる(例)



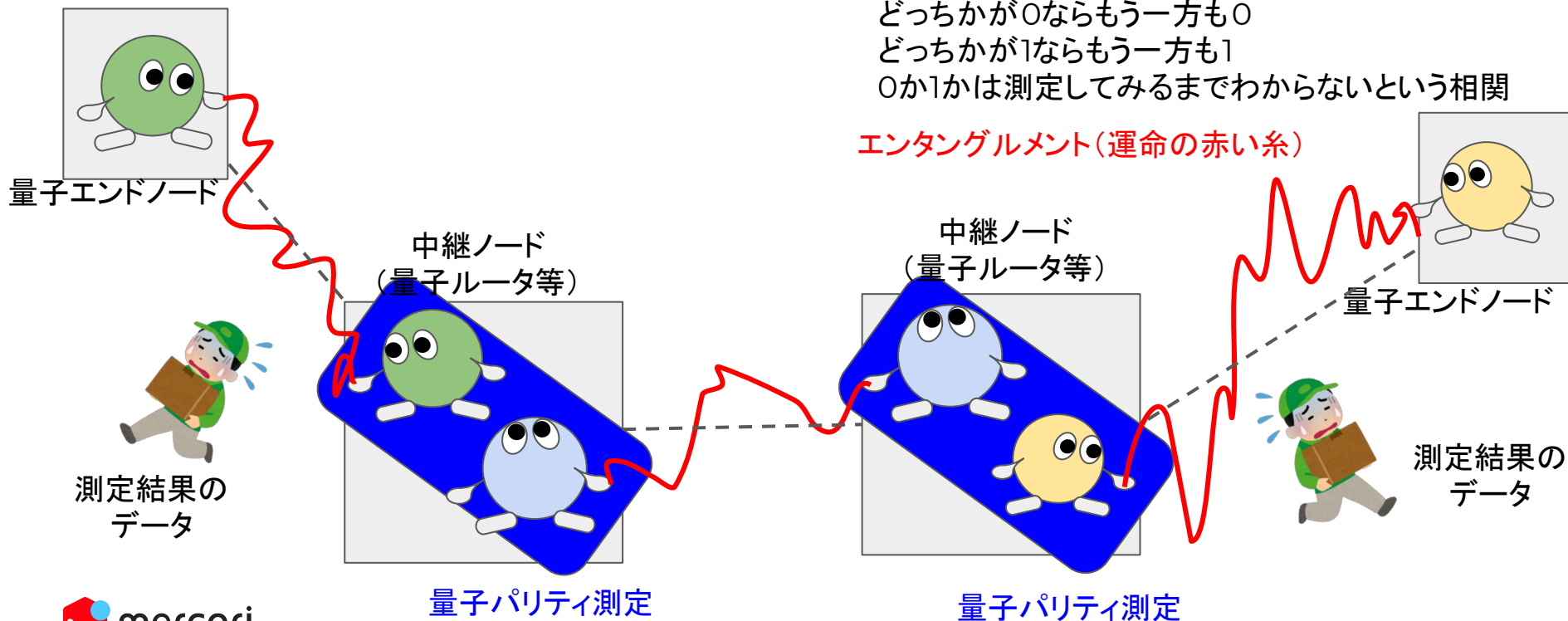
出来た光子同士を繋げば $\frac{1}{10}$ >

Hop by Hop もしくは
直接送信なら $\frac{1}{1000}$

その後、インターネットで測定結果を伝送



store & forwardでなくてOK (各リンクで作っておいた量子相関のパリティを見たいだけ)



量子インターネットの実際

データプレーン
(量子プレーン)

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

どっちかが0ならもう一方も0

どっちかが1ならもう一方も1

0か1かは測定してみるまでわからないという相関(いわゆる量子相関)

エンタングルメント(運命の赤い糸)

量子さん



エラー
(時間依存)



- エラー管理
- ルーティング管理
- リンク管理
- 到達(エンタングルメント生成)確認
- Swap管理
- コネクション管理
- etc.



メモリ揮発

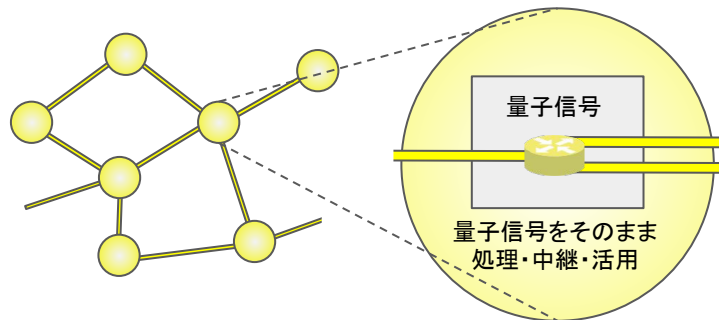


コントロールプレーン
(現行インターネットプレーン)

研究紹介、 インターネット技術者が取り組むべき研究 開発

Layer 1: Physical Layer

量子インターネットのハードウェア (HW)



量子信号を格納・処理する HW が必要

量子インターネットHW の要件

- 数十量子ビットの長寿命量子メモリ
- 高精度のローカル量子操作
- ファイバー波長の光子との高効率な変換・接続
- 高効率な単光子検出器

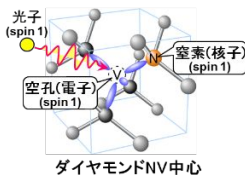
候補

- ダイヤモンド格子欠陥
- イオントラップ
- 原子トラップ
- 希土類結晶
- 超伝導量子回路
- 全光
(メモリなしアーキテクチャ)
- etc.

アプリケーションとHW

計測・センシング

- 原子トラップ
- ダイヤモンド格子欠陥



通信・セキュリティ

- 任意のHW



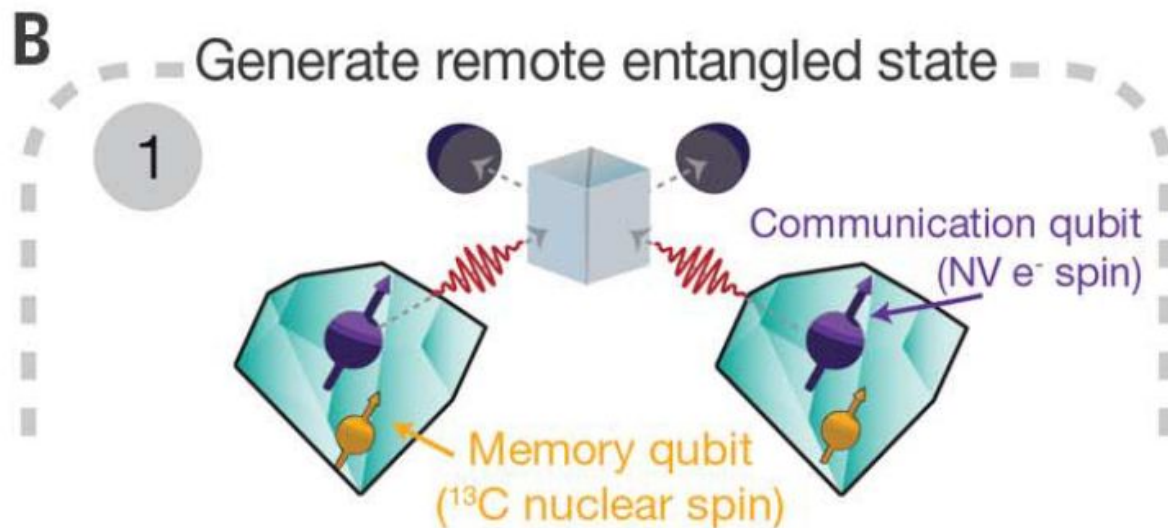
量子計算

- 超伝導量子回路
 - 超伝導回路と光の変換
- イオントラップ



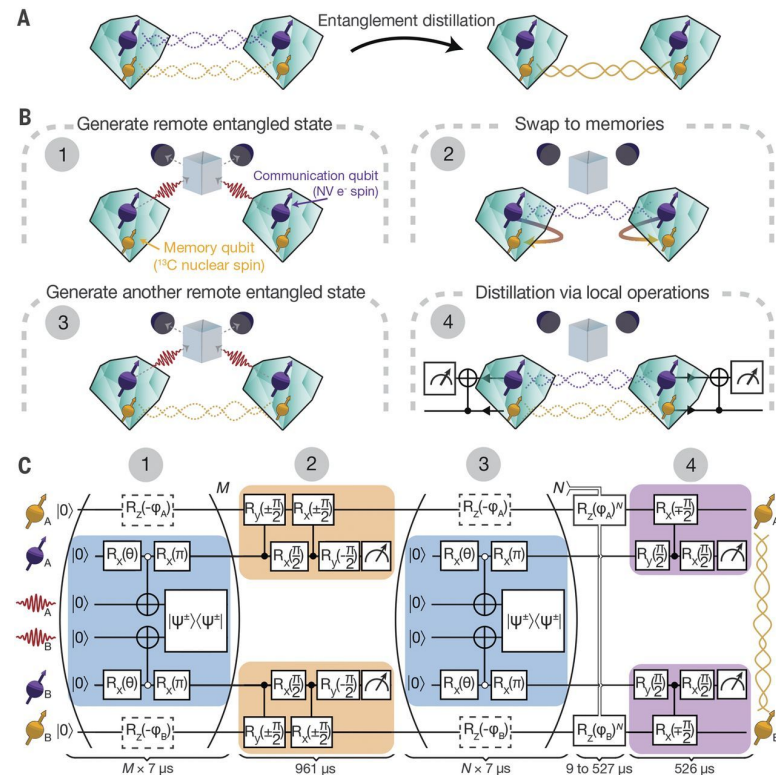
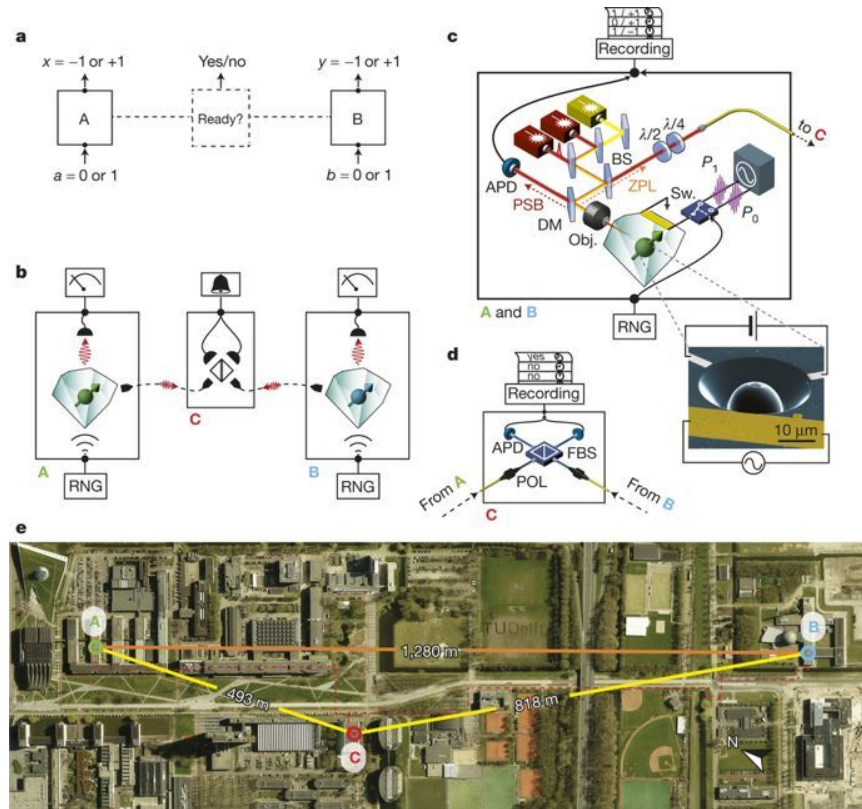
Herald

- エンタングルメントが出来たことを知る必要がある



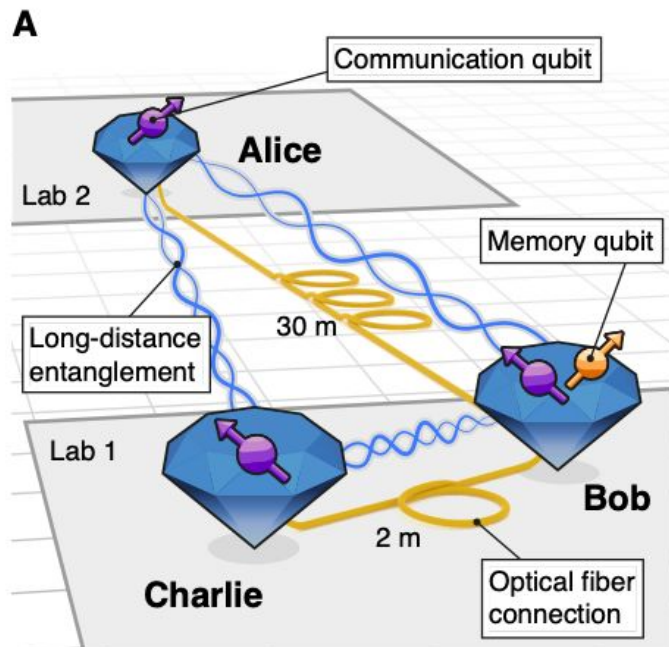
両側のノードから発光させて、中間の補助ノードで Bell測定する仕組み

Delft 工科大学の量子中継機を目指した実験

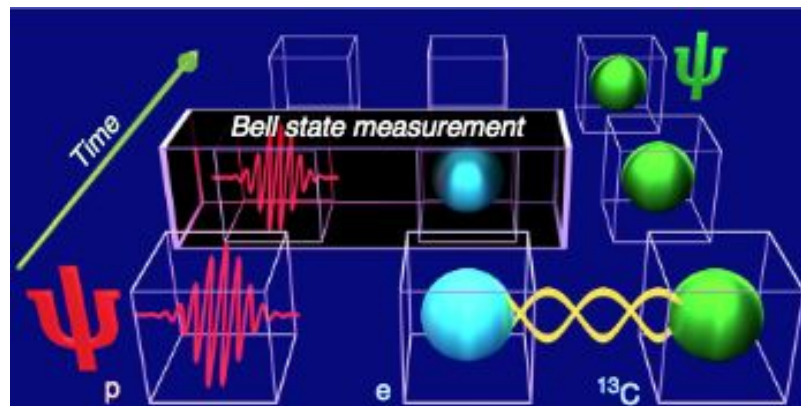
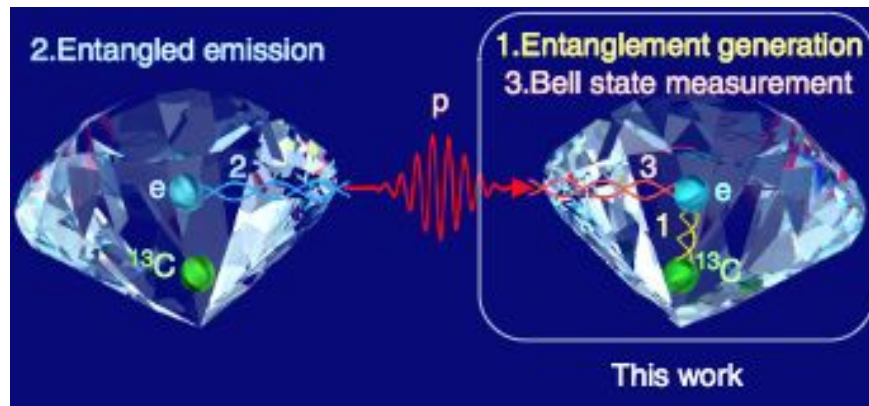


Delft 工科大学の量子中継機を目指した実験

実験室内での Entanglement Swapping(量子中継)の実証(2021年)

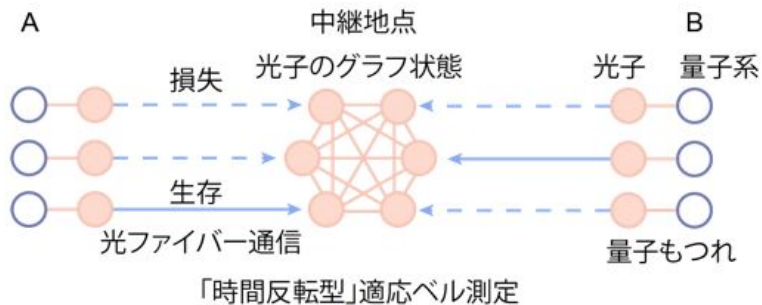


光子の量子情報を量子メモリに保存する実験(横国大)



発光・吸収形

全光量子中継ネットワーク原理検証実験(阪大他)



AB間の長距離量子もつれ

図2：全光量子中継の概念図

3光子のグラフ状態を発生

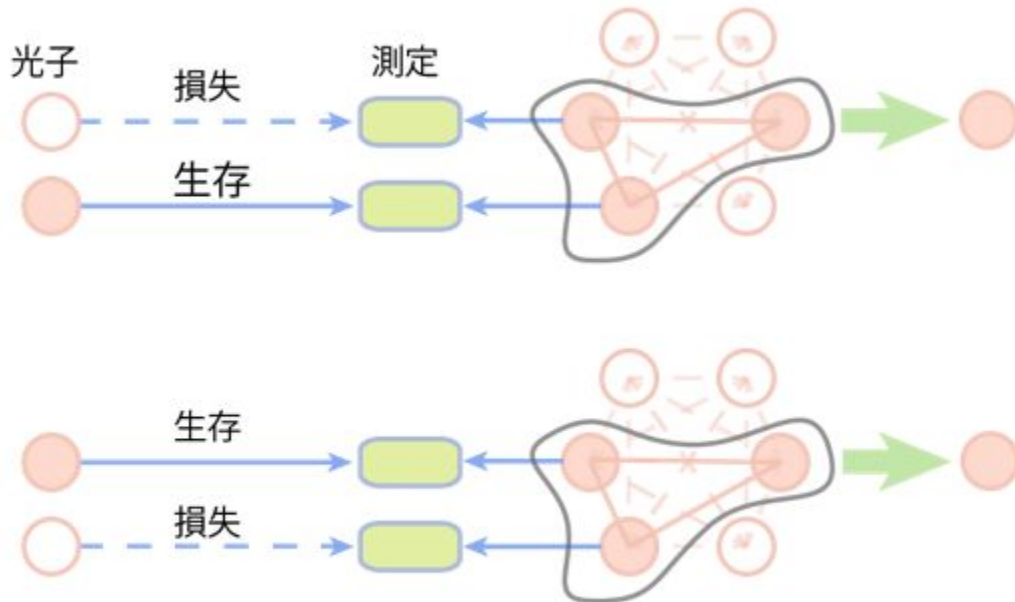


図3：今回の実験概要。生存した光子の量子状態が3光子グラフ状態の残りの光子に量子テレポーテーションされる。これにより損失耐性付量子テレポーテーションが実現する。

Layer 2: Link Layer

Layer 2: Link Layer

Application	
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

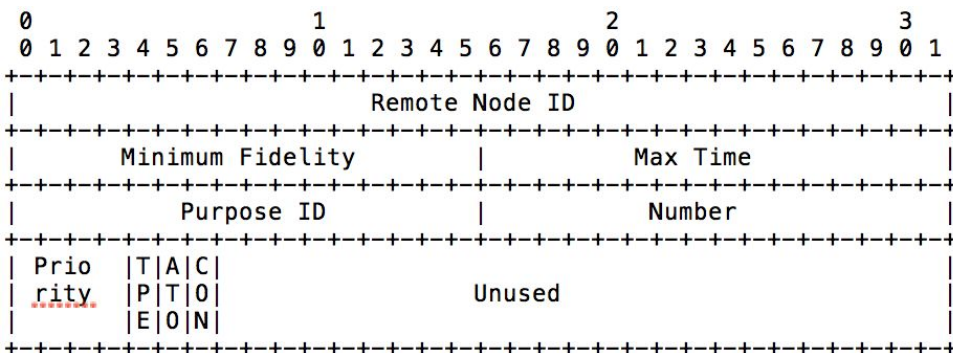


Figure 1: CREATE message header format

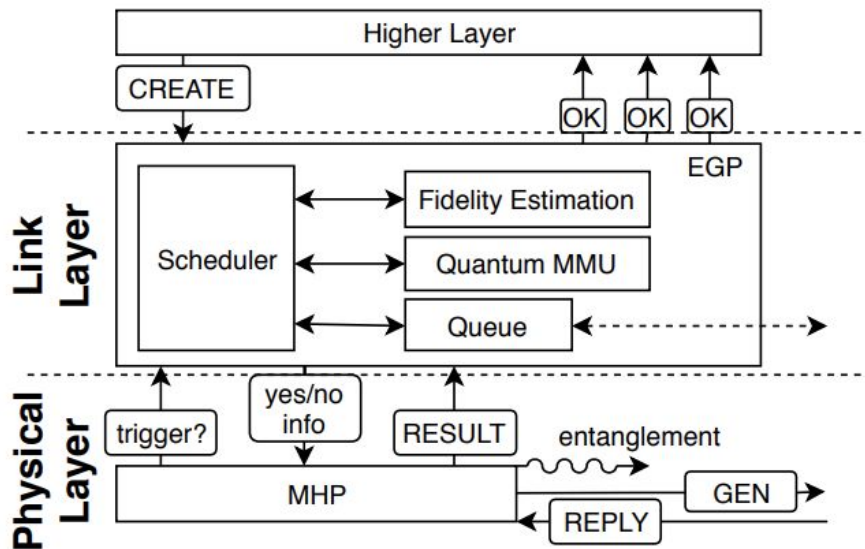
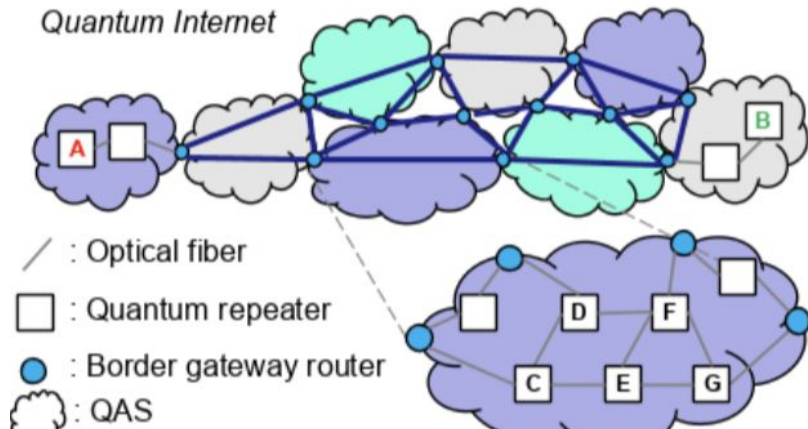


Figure 5: Flow diagram of the MHP and EGP operation. The EGP handles CREATE requests and schedules entanglement generation attempts are issued to the MHP. Replies from the midpoint are parsed and forwarded to the EGP from request management.

Layer 3: Internet Layer

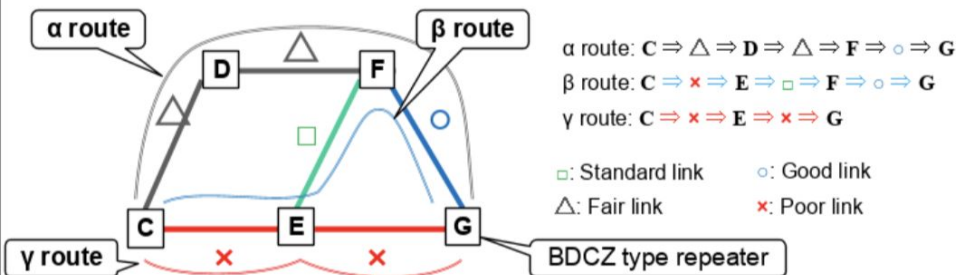
Layer3: Internet Layer

Quantum Internet

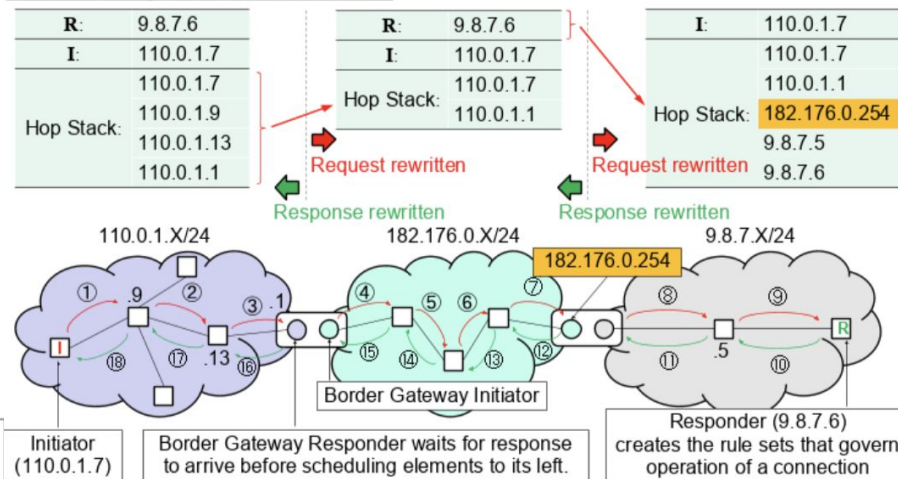


3. IGP: Routing within a QAS [4]

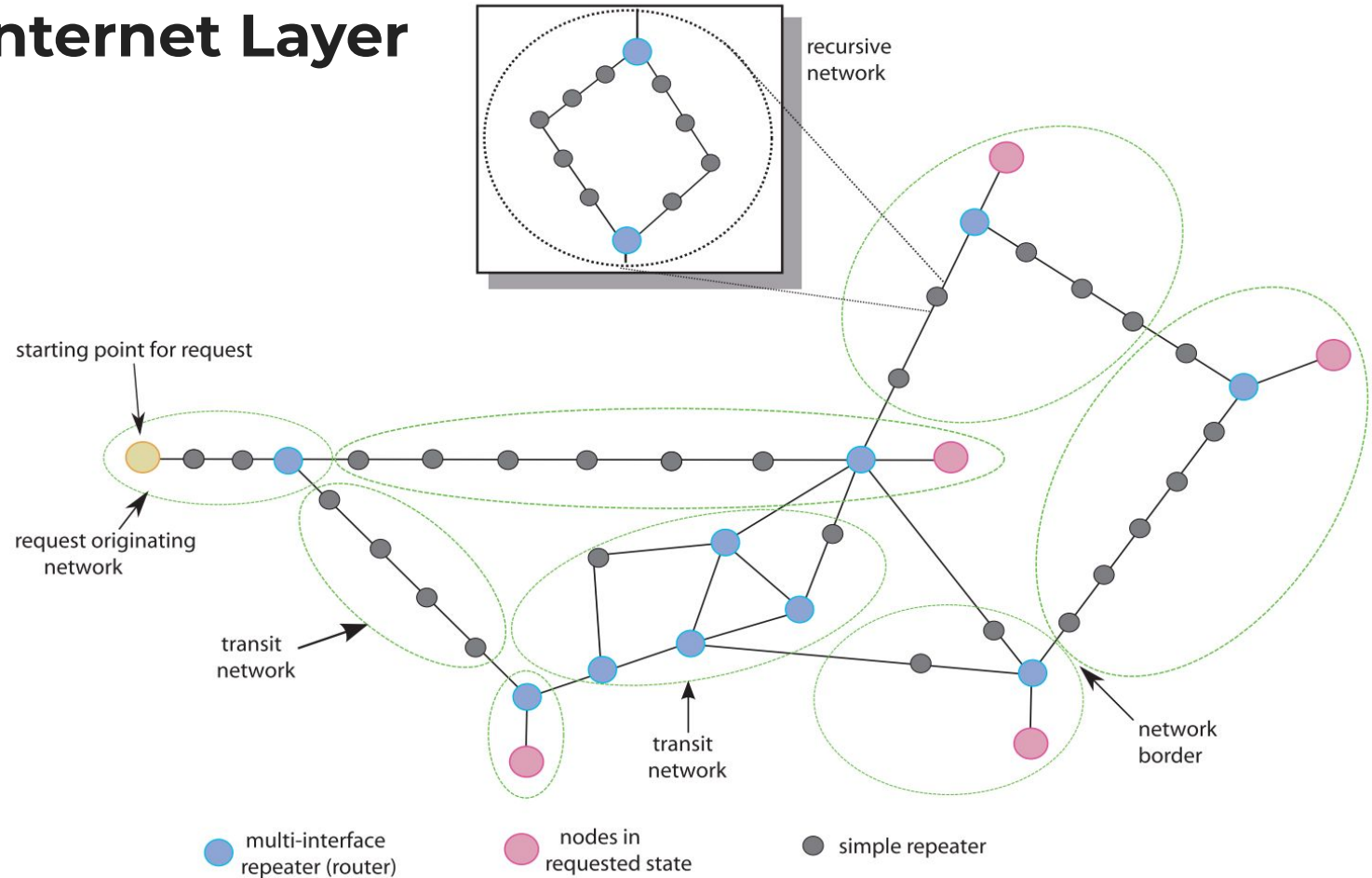
When we communicate from C to G, which route is faster?



EGP for Quantum Internet

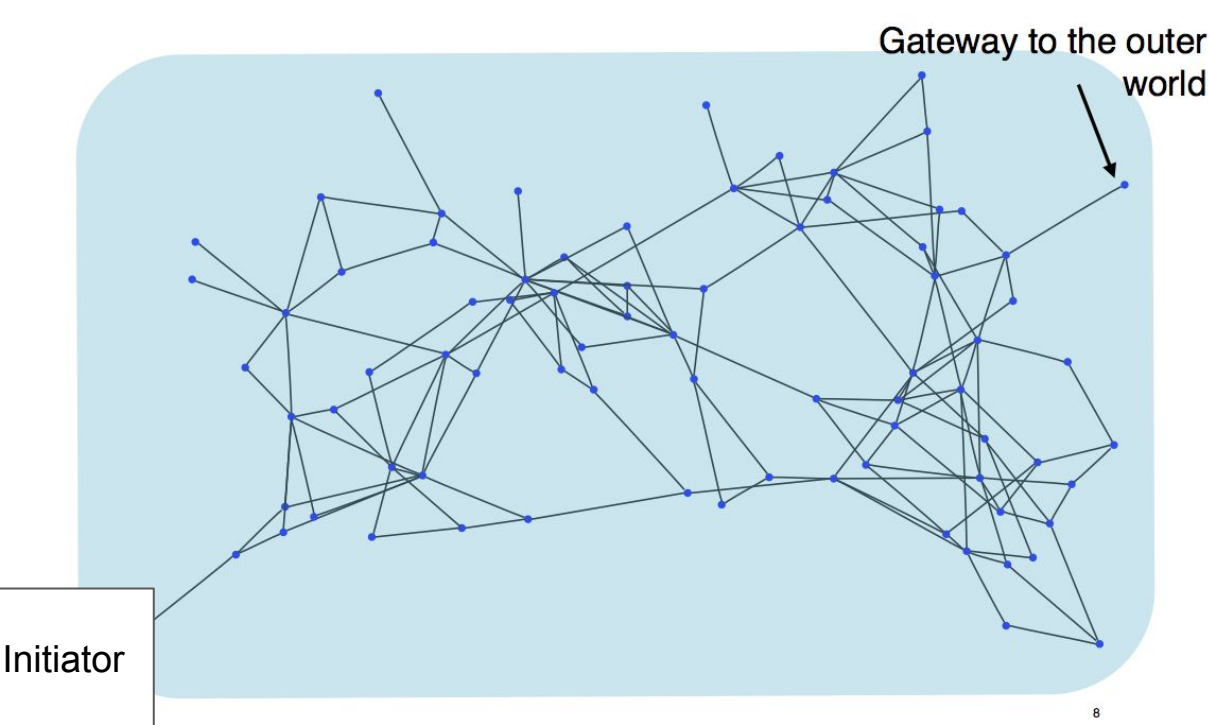


Layer3: Internet Layer



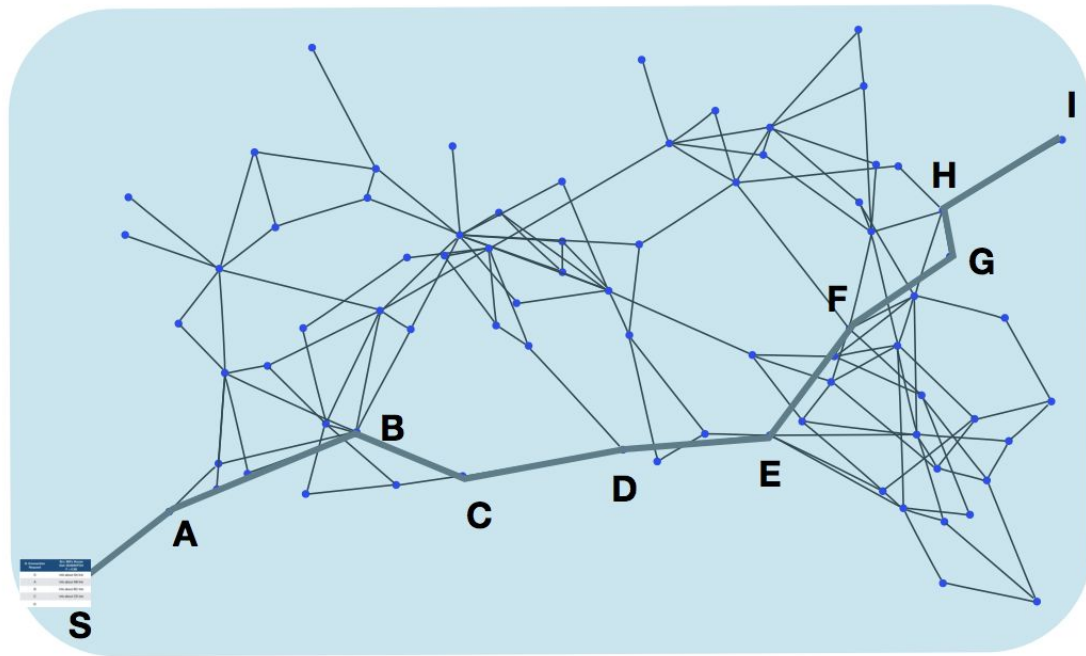
Layer 3&4: Internet & Transport Layer

Layer 3&4: Internet & Transport Layer



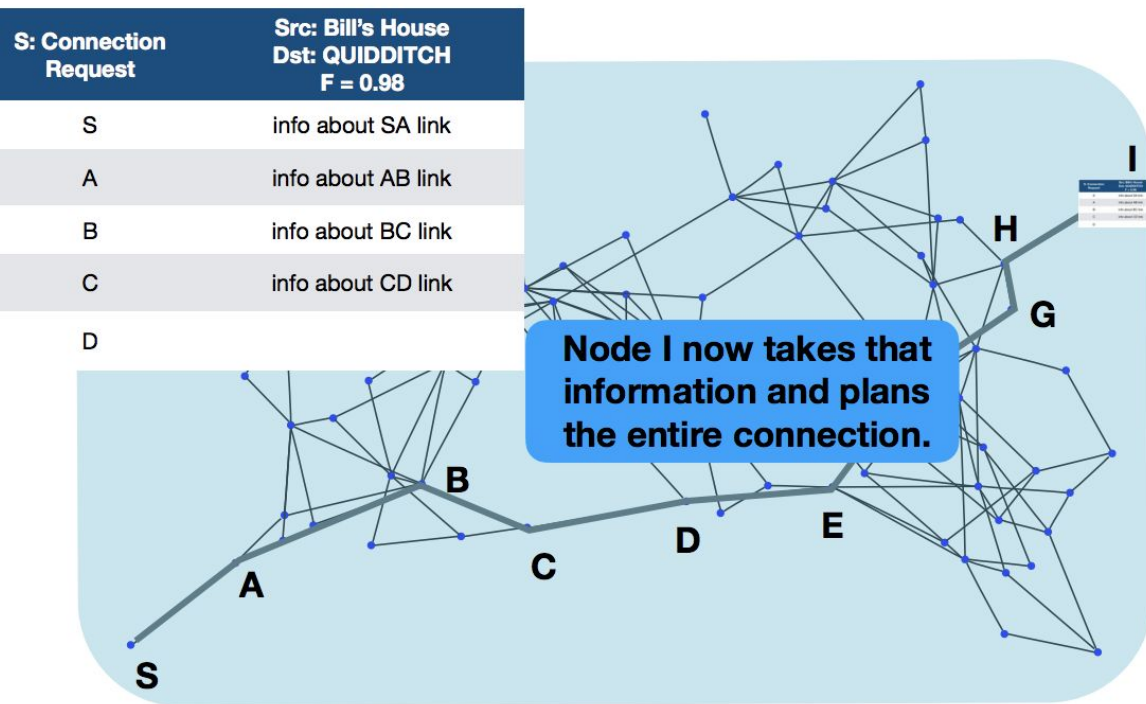
1. Initiator からResponder までのpath を見つけ出す
2. pathを見つけないながら、各link の特性を収集する
3. Responder が各link の RuleSet を作る
4. 各link にRuleSet を配布する
5. 量子通信開始

Layer 3&4: Internet & Transport Layer



1. Initiator からResponder までのpath を見つけ出す
2. pathを見つけないながら、各 link の特性を収集する
3. Responder が各link の RuleSet を作る
4. 各link にRuleSet を配布する
5. 量子通信開始

Layer 3&4: Internet & Transport Layer

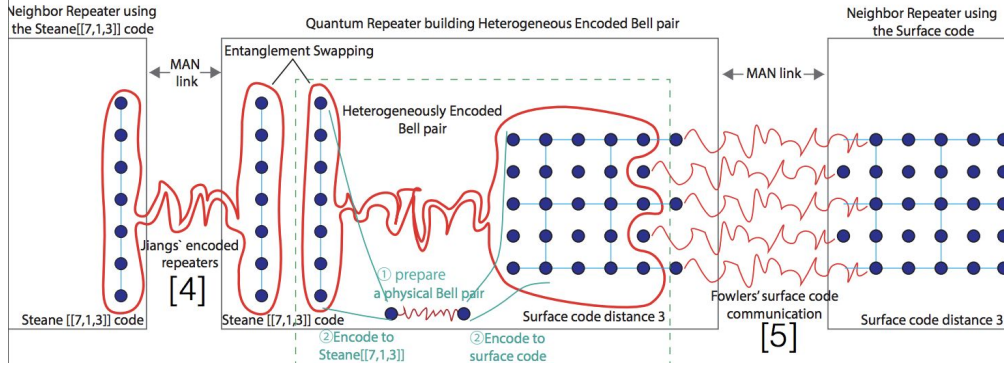


1. Initiator からResponder までのpath を見つけ出す
2. pathを見つけないがら、各link の特性を収集する
3. Responder が各link の RuleSet を作る
4. 各link にRuleSet を配布する
5. 量子通信開始

量子ルータアーキテクチャ

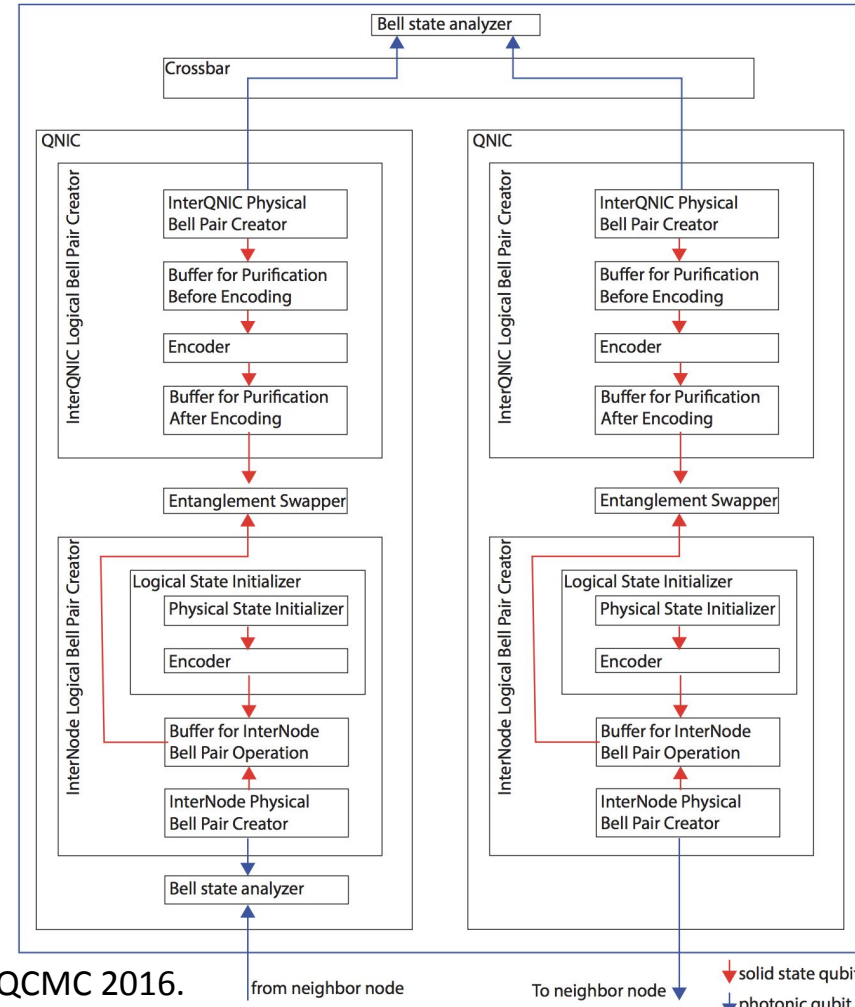
Heterogeneously encoded Bell Pair

- To get heterogeneous, coded Bell pairs by encoding each qubit building from physical Bell pairs, to a different code[3].



S. Nagayama, B.-S. Choi, S. Devitt, S. Suzuki, and R. Van Meter,
Phys. Rev. A 93, 042338 (2016).

Nagayama et al. Encoded Router Architecture with Interoperability. QCMC 2016.



量子インターネットへの攻撃まとめ論文

- Attacking the Quantum Internet
- 量子インターネットコンポーネントへの攻撃をまとめた初めての論文
 - 量子インタフェースへの攻撃
 - コントローラへの攻撃
 - etc.
- 機密性・完全性・可用性への影響を分析
- 今後の展望: 安全な量子インターネットアーキテクチャ

まとめ(目次)

- メルカリの狙い
- 量子インターネットの利用目的
- 研究開発の進捗
- 世界の大規模プロジェクトと各国の強み
- 学会など
- 前段: 量子コンピュータの仕組み
- 量子インターネットの仕組み
- 研究紹介、インターネット技術者が取り組むべき研究開発