

## 分散量子計算プラットフォーム

### — 量子インターネットで繋がった量子コンピュータの計算力相互融通 —

永山翔太 (株式会社メルカリ)

中島博敬 (株式会社メルカリ)

#### 皆の量子コンピュータを繋げたスーパー量子コンピュータを皆で使う

##### 背景

- エラー訂正量子コンピュータで素因数分解などのいわゆる高速な計算を実行するには、 $|A\rangle$ というリソース量子状態(\*1)が大量に必要
- $|A\rangle$ は量子状態なので、量子インターネット(\*2)で集めたい→分散計算

##### 目的

- 量子インターネットを介して世界中の量子コンピュータから $|A\rangle$ を集められる**量子計算力相互融通システム**を提案・開発

##### 想定:

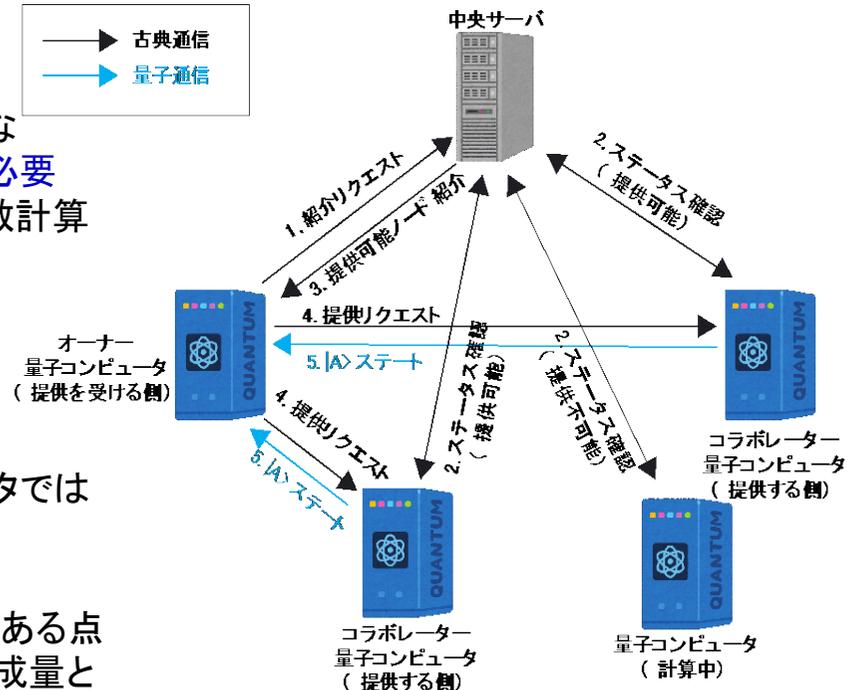
エラー訂正量子コンピュータと量子インターネットの存在

##### 効果

- 各ユーザが量子計算力を相互融通して、各々の量子コンピュータでは**実行不可能なサイズの量子計算を実行可能**になる

##### 新規性・優位性

- ユーザを想定した分散計算システム**やプラットフォームの提案である点
- エラー訂正量子コンピュータのワークロード管理指標に $|A\rangle$ の生成量と生成速度 (**AKEPS; A ket per second**↔古典計算のFLOPSに相当) を用いた点
- 量子データと量子回路を送受信して分散実行する既存提案に対するpros/cons
  - Pros
    - コラボレーターが異常シャットダウン等しても量子データを失わない (**ノード異常への耐性**が有る)
    - 量子アルゴリズムについての情報を**完全に秘匿**して他ノードの計算力を利用できる
  - Cons: 大量の量子通信を必要とする



\*1: ユニバーサル量子ゲートセットを実行する際に消費される”補助”量子状態

\*2: 量子情報を通信するための専用大域網

## 量子情報革命の機会平等を提供する

- 解決する課題と社会への影響
  - 将来予測: エラー訂正付き量子コンピュータによる革新的な発見や高速情報処理が社会や人類の発展を牽引する
    - 資金で優位に立てる一部の企業や研究機関の場合
      - 常に最新最大の量子コンピュータを有して競争で優位に立ち続ける
    - 他の企業や研究機関の場合
      - [課題] 比較的中小規模の量子コンピュータしか利用できず、量子前提時代における競争で不利になる
  - [社会への影響] 中小規模の量子コンピュータを集めて大規模量子コンピューティングプラットフォームを作り、**お互いに量子計算力を扶助し合うことで、誰でも最新最大規模の量子計算力を利活用できる** (←本プロジェクトの成果)
- 実装機能
  - 中央サーバ
    - ノード登録・管理機能
    - 認証局機能
    - ジョブ管理機能
    - データベース機能
    - 可視化機能
  - クライアント
    - 中央サーバ登録機能
    - 認証局クライアント機能
    - |A>供給リクエスト機能 (オーナー機能)
    - |A>供給機能 (クライアント機能)
    - 量子通信機能 (シミュレーション)
  - プラットフォーム全体機能
    - 中央サーバ-ノード間通信機能
    - ノード間通信機能
- 特に検討した事項
  - 量子コンピュータ完成後の暗号通信・認証
    - **耐量子の標準化**が進行中のプロトコル等の利用
    - 解読される前に次の鍵に移行する仕組みの検討
  - 相互扶助を促進するインセンティブ機構
  - 量子データと量子回路を送受信して分散実行する分散量子計算を実行するpros (本プロジェクトの開発内容ではないが、新規性のある考察)
    - 古典計算:  $1\text{CPU} \times 100\text{時間} = 100\text{CPU} \times 1\text{時間} = 100\text{CPU時間}$   
(総計算力面で相互扶助するprosが特にない)
    - 量子計算:  $1\text{量子CPU} \times 100\text{時間}$ より、**100量子CPU × 1時間のほうがエンタングルメントと重ね合わせの効果**でより大きな空間を扱って計算できる (分散計算にprosがあり、相互扶助のインセンティブになる)