

どんな研究？

- 役に立つ量子プロトコルを設計するための方法論を確立
- 量子通信のもつ理論的性質の解明
- 量子通信と通常の通信との差異の明確化

もたらされる変革

- 量子プロトコル設計の生産性が飛躍的に高まり、様々な効率的量子プロトコルを実現
- 絶対安全な電子マネーなど、量子通信以外では不可能な量子プロトコルを実現

展示紹介

- 効率的かつ有効な量子プロトコルを構築するために必要な要素技術の構築

①量子プロトコル設計法

量子プロトコルを設計する際に仮定するネットワークモデルは簡単なものでよいことを解明

②量子ビットの性質

量子ビットのコピーの困難さを定量的に評価

研究のゴール

絶対に情報が漏れない・絶対に詐称できないなどの性質を持つ量子プロトコルの効率的な実現

なぜそのようなことが可能か

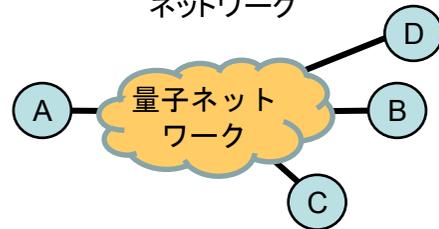
量子ビットには、その情報を読取ると変化するという性質があります。これによって、**絶対に安全な共通鍵配送プロトコル**を作ることができます。

このように、**量子ビットと通常のビットの違い**をうまく使う事で、他にも有用なプロトコルができると信じられています。

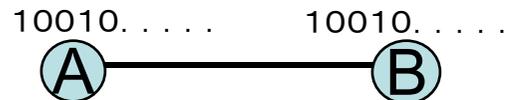
どのような研究が必要か

- (1) 量子特有の性質が、巨大なネットワークでのプロトコル設計にどのように影響するかを知る必要があります。
- (2) 量子ビットの性質を使って作られている共通鍵配送のプロトコルのように、量子通信だからこそできるプロトコルを作るには量子ビットの性質を評価することが必要です。

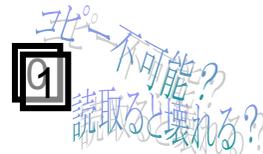
量子ビットをやりとりするネットワーク



共通鍵を量子ネットワークを通じて共有



量子ビットが持つ通常のビットに無い性質



この展示では、この二つの切り口から得られた成果をご説明します。

連絡先： 加藤豪
協創情報研究部
情報基礎理論研究グループ

