44 量子加算回路 ～量子アルゴリズムの効率的な実行方法～

SCIENCE PLAZA 2010

Motivation どんな問題に取り組むのか？

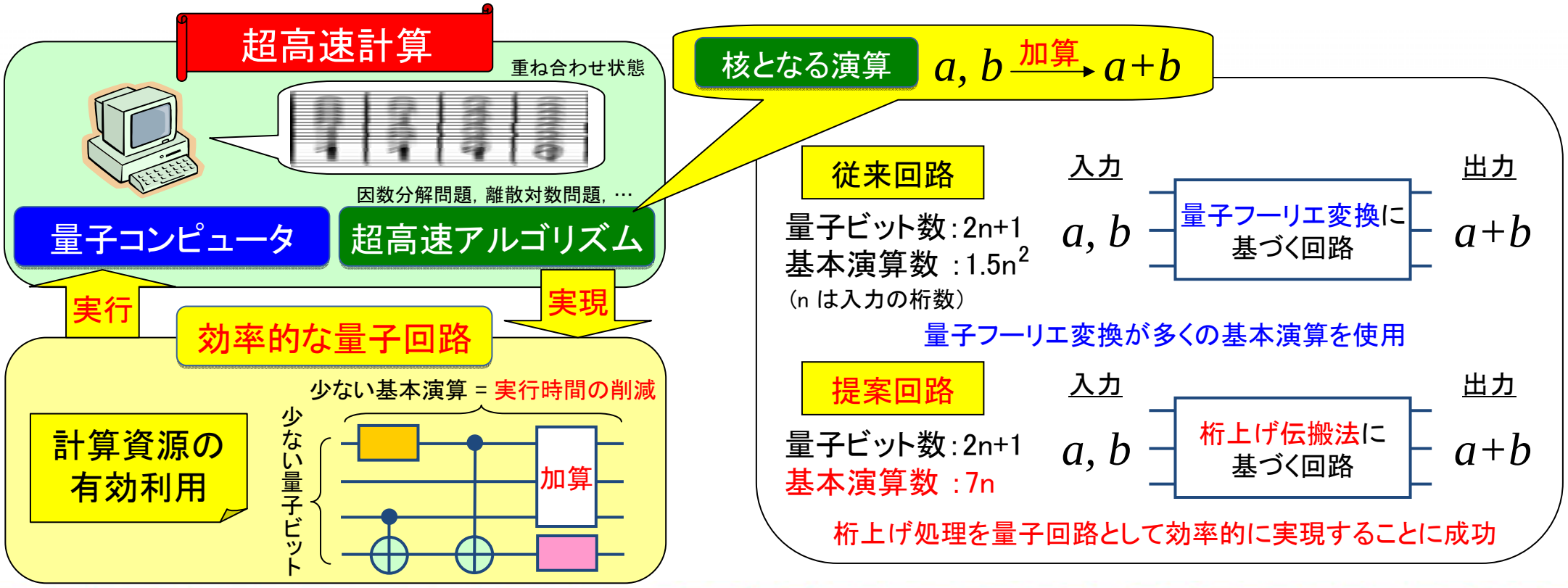
量子コンピュータによる超高速計算の実現が期待されていますが，情報を表現する基本単位である量子ビット等，量子コンピュータの計算資源には限りがあります．そこで，計算資源を有効に利用し，超高速アルゴリズムを効率的に実行する方法（量子回路）が必要となります．

Originality 得られた結果はどう新しいのか？

超高速アルゴリズムの核となる自然数の加算について，少ない量子ビットしか使わず，実行時間に対応する基本演算数を大きく節約した量子回路の構成方法を発見しました．さらに，これを超高速アルゴリズムに応用し，従来より高速に楕円曲線暗号が破られることを示しました．

Impact この研究が成功した場合のインパクトは？

少ない計算資源しかもたない量子コンピュータにおいて，様々な超高速アルゴリズムの実行が可能となり，現在のコンピュータでは不可能な超高速計算が実現できます．また，様々な暗号システムについて，量子コンピュータに対する安全性の分析が可能となります．



NTT

NTTコミュニケーション科学基礎研究所
NTT Communication Science Laboratories

連絡先
高橋 康博（Yasuhiro Takahashi） takahasi@theory.brl.ntt.co.jp
加藤 豪 （Go Kato） kato@theory.brl.ntt.co.jp
河野 泰人（Yasuhito Kawano） kawano@theory.brl.ntt.co.jp