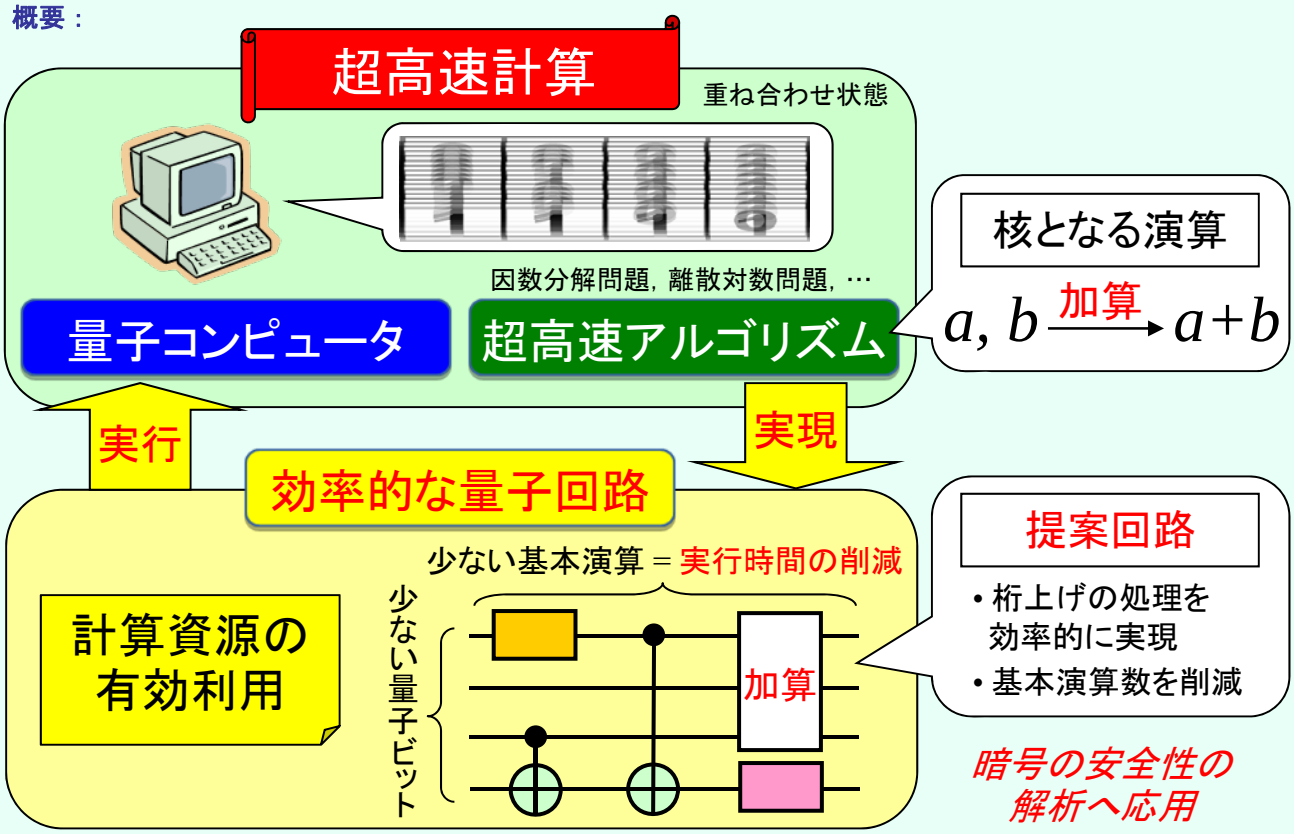
量子コンピュータ
―超高速計算を実現する量子回路―

背景・課題：次世代の超高速コンピュータとして期待される量子コンピュータの実現に向け，広く研究が進められています．しかし，情報を表現する基本単位である量子ビット等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）が不可欠です．

アプローチ：２つの自然数の加算は因数分解問題や離散対数問題を解く超高速アルゴリズムの核となります．そこで，加算を実行する効率的な量子回路を提案します．量子ビット数を増やさずに実行時間に対応する基本演算数を節約するため，現在のコンピュータ上のアルゴリズムである桁上げ伝搬法を利用します．

到達点：桁上げの処理を量子回路として効率的に実現することに成功し，従来と同数の量子ビットで基本演算数を大きく節約した加算回路を構成しました．これを超高速アルゴリズムに応用し，従来と同数の量子ビットからなる量子コンピュータにより楕円曲線暗号が高速に破られてしまうことを明らかにしました．

概要：



高橋 康博　河野 泰人　加藤 豪

関連文献

Yasuhiro Takahashi, Seiichiro Tani, and Noboru Kunihiro, “Quantum addition circuits and unbounded fan-out,” Asian Conference on Quantum Information Science, pp. 45-46, 2009.

連絡先

高橋 康博（Yasuhiro Takahashi）

協創情報研究部 情報基礎理論研究グループ