2022 年度

創発的研究支援事業　年次報告書

研究担当者	森前智行
研究機関名	京都大学
所属部署名	基礎物理学研究所
役職名	准教授
研究課題名	耐量子暗号によるハイブリッド型量子暗号プロトコル
研究実施期間	2022 年 4 月 1 日～2023 年 3 月 31 日

研究成果の概要

古典暗号においては一方向性関数が最も基礎的な仮定であるが、一方向性関数なしで様々な量子暗号プリミティブが構成できることを初めて示し、暗号のトップ国際会議 Crypto に採択された。また、量子物理でよく知られている状態の区別、変換の Duality を利用して新たなコミットメントの変換方式と、古典では構成方法が知られていない仮定から公開鍵暗号を初めて構成し、暗号のトップ国際会議 Eurocrypt に採択された。量子超越性を示す一つの方法である Proofs of quantumness は、これまで、collision resistance が必要であったが、今回初めて、トラップドア Permutation のみから構成し、理論計算機科学のトップ国際会議 ITCS に採択された。さらに、Guided local Hamiltonian 問題がさまざまなパラメーターやより物理的な設定でも QMA 完全であることを証明し、理論計算機科学のトップ国際会議 ICALP に採択された。