

中間評価（ステージゲート審査）結果

1. 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
2. 研究代表者： 森前 智行（京都大学 基礎物理学研究所 准教授）
3. 中間評価（ステージゲート審査）コメント

本課題は、量子計算機でも破ることのできない暗号（耐量子暗号）とのハイブリッド型の量子暗号プロトコルを構築することを目指すものである。フェーズ1では、暗号・計算分野のトップ国際会議に7件の論文を通して、本成果をきっかけとして、UC Berkeleyにおいて暗号技術のための量子仮定のワークショップが企画されるなど、当該分野のコミュニティ作りにも貢献している。量子暗号の分野で先進的な成果を挙げ、国際的な研究者としての地位を確立している。フェーズ2では、強力な量子暗号プリミティブに必要な十分な、安全性の高い仮定の理論的な研究計画を立てており、挑戦的であり期待する。

以上