2021 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	2021 年 4 月 1 日～2022 年 3 月 31 日

研究成果の概要

本年度は、Certified deletion に関する 2 件の成果を得た。Certified deletion というのはサーバーにデータをアップロードし、必要がなくなったら消してもらいその消した証拠を発行してもらうというものである。消した証拠が有効なものである場合は、データはたしかに消去されたことが保証できる。古典の場合はデータはコピーを取ることができるため、Certified deletion は明らかに不可能であるが、量子を使うと、No-cloning と不確定性原理により、可能である。

我々はこれまでは Symmetric key encryption にしか適用されていなかった Certified deletion を公開鍵暗号に拡張した。さらに、送信者は従来は量子状態を送信する必要があったが、送信者を完全に古典にすることにも成功した。これには、耐量子暗号の有力候補として研究されている Learning with errors という格子に関する問題から作られる Trapdoor つき Claw-free 関数を利用している。本成果は暗号の 3 大国際会議である ASIACRYPT に採択された。

また、Certified deletion をゼロ知識証明に適用することにより、Everlasting なゼロ知識証明の構成も行った。ゼロ知識証明というのはある命題が正しいことを、それ以外の情報を漏らさずに相手に納得される暗号プロトコルであり、現在身の回りのいろいろなところで応用されている重要な概念である。我々は NP の量子版である QMA に対するゼロ知識証明を Everlasting にすることに成功した。これまで考えられてきた Broadbent と Grilo による QMA のゼロ知識証明に Certified deletion を組み込むことにより、Certified everlasting という新しい概念を構成した。これは、従来のゼロ知識証明に加えて、QMA の命題が正しいことの証明を削除すると有効な証拠が発行されるというものであり、いったんこの証拠が発行されると、命題が正しいこと以外の情報は今後どんなに攻撃者の計算能力が向上しても漏れることがない。本成果は暗号のトップ国際会議である CRYPTO に採択された。