2023 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	2023 年 4 月 1 日～2024 年 3 月 31 日

研究成果の概要

計算量的な仮定と量子的な性質をハイブリッドで用いることによりこれまでにない新しい機能を持つ暗号技術を作るのが本研究の目的である。特に、量子の性質を用いることにより、古典の暗号では一方向性関数が必須であるようなものであっても、それを使わないで実現することが可能となり、従来よりもより安全な暗号が可能となる。今年度は、特に、量子コミットメントの構成を行った。ランダムな量子状態を利用できるような common Haar random model という設定を考え、その状況において、送信者と受信者の両方がそのランダム量子状態を使えるもとでの、コミットメントの安全性を証明した。このような設定の場合、計算量的仮定を用いることなく、任意の量子多項式時間の攻撃者に対して安全な量子コミットメントを構成できることを示した。本成果は暗号のトップ国際会議 crypto に採択された。

また、公開鍵暗号を一方向性関数から実現することにも成功した。古典暗号の場合、公開鍵暗号は一方向性関数からは構成できず、より強い仮定が必要であろうと信じられている。ところが、量子の場合、量子状態の区別不可能性と変換不可能性の双対性をうまく利用することにより、電子署名から公開鍵暗号が構成できることが証明できた。さらに、電子署名は一方向性関数から構成できるため、これは、量子の場合、古典と異なり、一方向性関数のみから公開鍵暗号が可能であることを意味する。本成果も、暗号のトップ国際会議 crypto に採択された。