数理・情報のフロンティア
2021 年度採択研究者

2021 年度
年次報告書

水谷 明博

三菱電機(株) 情報技術総合研究所
研究員

現実的な装置を用いた情報理論的安全な量子情報処理の実現

§1. 研究成果の概要

量子暗号は、離れた 2 者間での絶対安全な通信を可能にする。現代広く使われている暗号より強固な安全性を保障できる利点がある一方で、最大の課題は通信速度の遅さにある。量子暗号では、秘密鍵と呼ばれる絶対安全な通信を行うためのビット列を共有するが、通信速度が遅いということは、ある時間量子暗号を行ったときに生成できる秘密鍵の量が少ないことを意味する。より速く秘密鍵を生成する一つの方法は、できる限り沢山の光を単位時間あたりに送受信することである。しかし、このような高速な量子暗号システムでの安全性を保障する理論は十分に確立していないという問題がある。今回、代表的な量子暗号である総当たり差動位相シフト方式を高速に動作させた場合での安全性を研究した。高速に動作させると送信する光同士が相関するため、光同士の相関を数学的にモデル化し、安全性証明を与えた。その結果、本方式は現実的な相関の下でも鍵生成率が大きく低下しないという実用上の利点を持つことを明らかにした。本結果を論文にまとめ米国物理学会が発行する国際雑誌 Physical Review A に投稿し、採択された[1]。

量子計算は、現代の計算機では手に追えない計算を効率的に行うことができる。量子計算機のハードウェア開発も盛んであり、クラウド利用も可能である。将来、さらに開発が進み量子計算機が大規模化しても、現在と同様にクラウド利用が続くと考えられる。このような将来では、利用者目線に立つとクラウドの計算機が正しく動作しているか、ということが気になる。量子計算は、量子状態の生成と測定というプロセスで構成されるため、これらのプロセスが検証できれば量子計算の動作確認を行うことができる。その際、クラウド利用者は古典計算機で検証できることが望ましいが、どのような量子状態の生成や測定が古典検証できるかは分かっていないという課題がある。今回、マジック状態と呼ばれる万能量子計算の実現に不可欠なリソース状態の生成と測定を、量子計算機がどれだけの精度で実行できているかを、LWE 仮定の下で古典検証するプロトコルを設計した。本結果を論文にまとめプレプリントサーバで論文を公開し[2]、暗号と情報セキュリティシンポジウム 2022 で発表を行った[3]。

【代表的な原著論文情報】

[1] A. Mizutani, G. Kato, “Security of round-robin differential-phase-shift quantum key distribution with correlated light sources”, Physical Review A **104**, 062611 (2021).

[2] A. Mizutani, Y. Takeuchi, R. Hiromasa, Y. Aikawa, S. Tani,
“Computational self-testing for entangled magic states”, arXiv:2111.02700v1 (2021).

[3] 竹内 勇貴, 水谷 明博, 廣政 良, 相川 勇輔, 谷 誠一郎, “LWE 問題を用いたマジック状態生成機能の検証”, 暗号と情報セキュリティシンポジウム 2022 (SCIS2022)予稿集