公開

研 究 終 了 報 告 書

「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」

研究期間: 2021 年 10 月～2024 年 3 月
研 究 者: 水谷 明博

1. 研究のねらい

現代の情報処理を凌駕する次世代の情報処理が量子情報である。量子情報の中でも、本研究では**量子暗号**と**量子計算**にフォーカスする。

量子暗号は、遠く離れた 2 者間での絶対安全な通信を可能にする技術であり、既に量子暗号の製品化や社会実装に向けた取り組みも始まっている。現在広く使われている暗号は攻撃者の計算能力を限定した下での安全性である一方、量子暗号は攻撃者の計算能力無依存に未来永劫通信の安全性を保証できる。量子暗号はこれまでに数多くの方式が提案されているが、それらを実現するためには、方式ごとに安全性証明と呼ばれる理論を構築する必要がある。安全性証明を構築するには、送受信装置の動作を数学的にモデル化する必要がある。しかし、実際の送受信装置が理論で仮定したモデルの通りには動作しておらず理論と実装にギャップが存在するため、実装した量子暗号の安全性が保証できないという問題がある。従って、現実の送受信装置の動作を反映した数学的モデルに基づく安全性証明の構築が急務である。

本研究では代表的な量子暗号方式をターゲットにして、これまで安全性証明に取り込むことが難しかった現実の装置特性や、有限の通信時間において高効率な鍵生成を達成する安全性証明を構築することで、現実の装置を用いた場合でも安全な量子暗号が実現可能になることを目指して研究を行った。

もう一つの研究テーマである量子計算は、現代の計算機では手に負えない複雑な計算を効率的に行うことができる。現在、量子計算機のハードウェア開発も盛んであり、クラウド利用も始まっている。将来さらに量子計算機が大規模化しても、現在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、クラウドの計算機が正しく動作しているかをクラウド利用者が確認できることが重要である。量子計算は量子状態の生成と測定で構成されるため、これらのプロセスが検証できれば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だけを用いて検証(古典検証)できることが望ましいが、どのような量子状態のクラスに対してその生成や測定が古典検証できるか分かっていないという課題がある。

本研究では、古典計算機だけを持つ検証者が単一の量子計算機と古典ビットだけをやり取りするだけで、万能量子計算の実現に不可欠な量子状態の生成や測定が実現できているかを古典検証するプロトコルの構築を目指して研究を行った。

2. 研究成果

(1)概要

本研究では、現実の送受信装置を用いた量子暗号の安全性証明の構築、古典計算機を用いたクラウド量子計算の検証に関する研究を実施した。

量子暗号は絶対安全な通信を可能にするが、それを実現するためには量子暗号方式ごとに安全性証明を構築する必要がある。この安全性証明は、ユーザが用いる送受信装置の動

作を数学的にモデル化したもとで与えられる。これは、実際の装置の振る舞いが装置の数学モデルを満たすならば現実の量子暗号システムの安全性保証が可能になることを意味する。そのため、現実の量子暗号システムの安全性を保証するには、できる限り現実の装置の動作特性を数学的モデルに取り込んだ安全性証明を構築することが重要になる。これまで、現実装置が持つ不完全さを取り込んだ安全性証明の研究は盛んに行われてきたが、一般に不完全さを取り込めば取り込むほど理論が複雑になるため、実験で観測されている現実装置の特性であっても、安全性証明に取り込めていない装置特性が存在していた。また量子暗号では、理論を簡単にするため通信時間が無限の極限という非現実的な状況での安全性証明を考えることが多く、たとえ将来の実用化が期待されている方式であっても、有限時間の通信を行った場合での安全性証明が未確立のため、方式を実装した際の安全性が保証できていないという問題がある。

そこで、これらの問題を解決することで、量子暗号の実現に貢献することを目指した。具体的には、次の研究テーマを実施して成果をあげた。以下のリスト内の文献は本項（2）詳細に記載した。

1. **総当たり差動位相シフト方式を高速に動作させた場合の安全性証明 [1]と、送信パルス間の相関など広範な現実の装置特性を取り入れた BB84 の安全性証明の構築 [2]**
2. **有限時間の通信を行った場合での差動位相シフト方式の安全性証明の構築 [3]**

もう一つの研究の柱である量子計算は、量子状態の生成と測定という計算モデルで計算を実行し、古典計算を凌駕する計算能力を持つと信じられている。現在、量子計算機のハードウェア開発も盛んであり、そのクラウド利用も始まっている。量子計算機がさらに大規模化した将来、安心・安全にクラウド利用するためには、クラウドの量子計算機が真に量子の計算機かを、量子計算機よりも計算能力が低い古典計算機だけを用いてチェックできることが重要になる。

そこで本研究では、万能量子計算の実現に欠かせない量子の性質の有無を古典計算機だけを用いて検証する手法を確立した。具体的には、次の研究テーマを実施して成果をあげた。

3. **単一の量子計算機に対するマジック状態の古典検証プロトコルの確立 [4]**

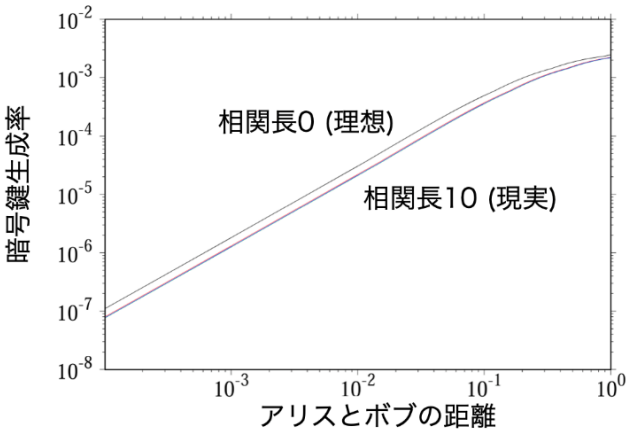
マジック状態を用いない量子計算(具体的にはクリフォードユニタリ操作だけから成る量子計算)は古典計算でも効率的にシミュレート可能だが、そこにマジック状態を追加することで任意の量子計算が可能になるため古典計算でシミュレートすることが困難になる。そのため、マジック状態は量子計算を量子計算たらしめている量子の証拠と言える。つまり、研究テーマ 3 の結果を用いることで、万能量子計算に不可欠な量子の性質をクラウドの計算機が持っているかをチェックすることができるようになる。

（2）詳細

研究テーマ 1: 総当たり差動位相シフト方式を高速に動作させた場合の安全性証明と、送信パルス間の相関など広範な現実の装置特性を取り入れた BB84 の安全性証明の構築

公開

量子暗号は、現在広く使われている暗号に比べて高い安全性を達成できる利点がある一方、最大の課題は通信速度の遅さにある。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暗号鍵の量が少ないことを意味するが、これを克服する一つ方法として、単位時間あたりにできるだけ沢山の光パルスを高速に送受信することが考えられる。しかし、このような高速な量子暗号システム（具体的には、送受信の繰り返し周波数が1GHz以上）では、送信する光パルス同士が互いに相関することが実験で確認されている。これまでの通常の安全性証明では、送信パルス同士は独立であることを仮定しているため、i番目の送信パルスにはi番目の鍵情報しかないことが保証されていた。安全性証明はつまるところ、i番目の鍵情報がどれだけ盗聴者に漏洩したかを示すことであり、送信パルス同士の独立性を仮定すると、i番目の鍵情報の漏洩評価にはi番目のパルスだけを扱えばよくなる。しかし、送信パルスが互いに相関する現実の状況では、i番目の鍵情報がi番目以外の送信パルスにも伝搬するため、i番目の鍵情報の安全性評価に複数の送信パルスを扱う必要が出てくるため、安全性証明が難しくなる。



[右(左)：短(長)距離]

図 1：送信パルスの相関を取り込んだ総当たり差動位相シフト量子暗号方式の鍵生成率と通信距離の関係

本テーマでは、送信パルス同士の相関（相関長はℓcと仮定)を安全性証明に取り込む際、「$\mathrm{mod}(\ell c+1)$の値ごとに送信パルスを分類すると、$\mathrm{mod}(\ell c+1)$番目のパルス同士は互いに独立とみなせるため、$\mathrm{mod}(\ell c+1)$ごとに別々の安全性証明を行うことで$\mathrm{mod}(\ell c+1)$の全ての値の送信パルスから暗号鍵が取れる」という着想を得た。$\mathrm{mod}(\ell c+1)$の値ごとに安全性証明を分離することで、結果的に光パルスが互いに独立な状況での安全性証明に帰着することができた。

本アイデアを以下の代表的な量子暗号方式に適用し、送信パルスに相関がある場合での安全性証明を構築した。

(i) 総当たり差動位相シフト方式 [Nature **509**, 475 (2014)]:
現実には十分長いと想定される相関長$\ell c = 10$を仮定した場合でも暗号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（図 1)。

(ii) BB84 方式 [Bennett, Brassard (1984)]:
送信する光パルスの変調の揺らぎや、光の多モード性、光パルス同士の相関を含む現実の送信機が持つ不完全性を取り込んだ安全性証明を確立した。

(i)の結果はアメリカ物理学会が発行する国際学術雑誌である Physical Review A (Impact Factor 3)より出版された [1]。

(ii)の結果はアメリカ物理学会が発行する国際学術雑誌である Physical Review Research (Impact Factor 3.9)より出版された [2]。

公開

研究テーマ 2: 有限時間の通信を行った場合での差動位相シフト方式の安全性証明の構築

代表的な量子暗号に差動位相シフト (DPS)方式がある。DPS 方式は実装する送受信装置の構成が簡易であるため他の方式と比べて簡易な実験系で実装できるという利点がある。また実用化に向けた期待も高く、2011 年から現在まで運用されている東京 QKD ネットワークでも採用されている方式である。DPS 方式の安全性証明は、2019 年に量子力学の相補性に基づく理論を我々が与えた。その結果、送信機に対しては送信状態間の独立性と送信状態の光子数統計を仮定するだけで安全性が保証できることがわかった。しかし、これまでの DPS 方式の安全性証明では、解析を簡単にするためアリスが送信する光パルス数は無限の極限という非現実的な状況を仮定していた。DPS 方式を実際に実装するためには、通信時間が有限の場合での暗号鍵生成性能を明らかにする必要がある。

この問題を解決するため、今回 DPS 方式の有限長安全性解析を行い、有限の通信時間での暗号鍵生成率を導出した。本解析の肝は、受信者ボブが検出に成功したブロック（ブロック: 送信者アリスが送信する 3 連パルス）の中で、3 光子以上を放出したブロック数の期待値（$E3$）の推定にある。この期待値を実験で観測されるデータから推定する際に、典型的な確率集中不等式である Azuma の不等式を用いると、推定誤差が大きくなり有限時間での鍵生成率が無限時間の鍵生成率から大きく乖離することが分かった。これはアリスが送信するパルスの平均光子数が 1 に比べて十分小さいため、3 光子放出事象が非常に稀であることが原因である。稀な事象に関する期待値の推定には、2020 年に発明された確率集中不等式である Kato の不等式が有効であることが近年の Twin-Field 量子暗号方式の研究でも示唆されている。そこで、上記$E3$の推定に Kato の不等式を適用した結果、鍵生成率が大幅に向上する結果が得られた。また、損失通信路と現実的な送受信装置を仮定して数値計算を行った結果、77km 離れたアリスとボブの間で 8.3 時間の量子通信を行うことで 3 メガビットの暗号鍵が生成できることが明らかになり、実際の実験セットアップを用いた場合で DPS 方式が実現可能であることがわかった。

本結果はアメリカ物理学会が発行する国際学術雑誌である Physical Review Research (Impact Factor 3.9)より出版された [3]。

研究テーマ 3: 単一の量子計算機に対するマジック状態の古典検証プロトコルの確立

量子計算機が指定された量子状態を生成し、測定しているかを古典計算機で確認するプロセスは「セルフテスト」と呼ばれる。従来は、互いに通信していない複数の量子計算機に対するセルフテストしか構築できていなかった。2021 年に、耐量子計算機暗号の標準的な仮定である Learning with Errors (LWE)問題を量子計算機が量子多項式時間で解けないことを仮定することで、単一の量子計算機に対するセルフテストが可能であることが示された [Metger, Vidick, Quantum **5**,544 (2021)]。しかし、単一の量子計算機に対するセルフテストはベル状態という特

公開

定の状態でしか提案されていなかった。ベル状態はスタビライザ状態というクラスに属する 2 量子ビットのエンタングル状態だが、スタビライザ状態を多項式個用いて量子計算（具体的には、量子状態にクリフォードユニタリで時間発展させて計算基底で測定する量子計算)を実行しても古典計算で効率的にシミュレート可能である。そのため、ベル状態に対するセルフテストでは、クラウドの計算機が量子計算の実現に不可欠な量子性を持っているかを検証することに利用できない。

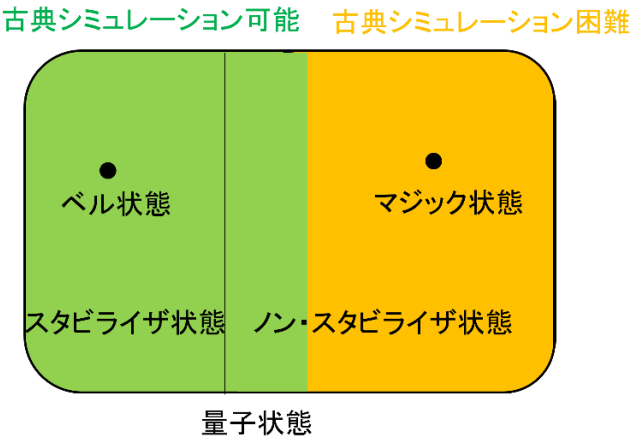


図2：量子状態のクラスと古典シミュレーション困難性

そこで本テーマでは、量子状態のもう一つのクラスであるノン・スタビライザ状態に属するマジック状態に対するセルフテストを構成した（図 2)。つまり、LWE 問題が量子多項式時間で解けないことを仮定することで、単一の量子計算機に対するマジック状態の生成と測定を古典計算機だけで検証するプロトコルを設計した。このマジック状態とは 3 量子ビットのエンタングル状態(3 つの重ね合わせ状態に制御・制御・パウリ Z ゲートをかけて作られる状態)であり、このマジック状態を高々多項式個用いれば古典シミュレーションが困難になる。今回設計したプロトコルは次の(i)～(iii)で構成される。

(i) LWE 問題から作られる関数を正しく計算しているかのチェック

(ii) パウリ Z, X 基底での測定を正しく実行しているかのチェック

(iii) マジック状態の一般化スタビライザ測定の結果を正しく出力しているかのチェック

(i)～(iii)のチェックで検証者がクラウドの計算機を拒否する確率から、マジック状態を検証者が指定した測定基底で測定したときの確率分布と、実際にクラウドが準備した状態を測定したときの確率分布の差を知ることができる。また、今回設計したマジック状態のセルフテストを用いることで、クラウドの計算機がマジックという万能量子計算の実現に不可欠な量子の性質を持っているかを古典計算機でチェックするプロトコルも構成した。

本結果はアメリカ物理学会が発行する国際学術雑誌である Physical Review A (Impact Factor 3)から、**特に重要な新結果として発表される Letter という論文タイプ**で出版された [4]。

引用した成果:

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

[2] M. Pereira, G. Currás-Lorenzo, Á. Navarrete, A. Mizutani, G. Kato, M. Curty, and K. Tamaki, Modified BB84 quantum key distribution protocol robust to source imperfections, Physical Review Research **5**, 023065 (2023).

[3] A. Mizutani, Y. Takeuchi, and K. Tamaki, Finite-key security analysis of differential-phase-shift quantum key distribution, Physical Review Research **5**, 02132 (2023).

[4] A. Mizutani, Y. Takeuchi, R. Hiromasa, Y. Aikawa, and S. Tani, Computational self-testing for entangled magic states, Physical Review A **106**, L010601 (2022).

公開

[5] R. Hiromasa, A. Mizutani, Y. Takeuchi, and S. Tani, Rewindable Quantum Computation and Its Equivalence to Cloning and Adaptive Postselection, In Proceedings of the 18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2003), pp. 9:1–9:23.

3. 今後の展開

量子暗号については、今回述べた成果などにより、ユーザが用いる送受信装置の現実の物理特性を反映した安全性証明が確立しつつある。今後は、安全性証明で仮定した装置の特性を実験でどのように評価するのかを議論することが重要である。例えば、今回安全性証明に取り込んだ送信パルスの相関の場合は、実際の送信機が与えられたときに相関長ℓ_cの値を知る実験手法を確立することが不可欠になる。このような装置仮定がどのように満たされているかを実験で検証する研究は理論家だけではなく、実験家とのコラボレーションも不可欠になっていくと考える。

量子計算については、今回古典計算機だけを用いた量子性の検証手法を構築したが、クラウドが検証に受理されるには、複雑な量子エンタングル状態を正確に準備できる必要があるため、正規のクラウドが作成した量子計算機であっても本検証に受理することが困難であったり、検証プロトコルのチェックにわずかに失敗するだけでも理想とは大きく乖離する判定をしたりしてしまう問題がある。これは古典計算機だけで検証手法を構築していることが問題であるため、今後は古典計算機だけではないが、それでも十分に簡易と考えられる装置(例えばレーザー光源など成熟した量子の技術)を追加で用いることで、より効率の良い検証手法を構築していくことが重要であると考える。

4. 自己評価

・研究目的の達成状況:本研究では当初より「現実の送受信装置を用いた量子暗号の安全性証明」と「量子計算の検証手法の確立」をテーマに設定していた。量子暗号は計画していたテーマで成果をあげ、アメリカ物理学会が発行する国際学術雑誌から3本論文を出版することができた。また、2023 年 9 月にウォータールー大学量子コンピュータ研究所で開催された招待制の量子鍵配送ワークショップで上記成果[3]に関する口頭発表を行っている。このように当初想定していたテーマで着実に研究を進展できた。

もう一つのテーマである量子計算は、耐量子計算機暗号と量子情報の融合分野において、新しいクラスの量子状態の古典検証手法を構築できた。本研究は、量子情報の研究者だけでなく耐量子計算機暗号の研究者とも議論を行うことで成果をあげ、アメリカ物理学会が発行する国際学術雑誌から重要な新結果として発表される Letter というタイプで論文を 1 本出版することができた。また、本成果は量子情報の国際会議でも口頭講演を行っている。

さらに、当初の計画にはなかったテーマであるが、耐量子計算機暗号の研究者と研究で繋がることができたことで、可逆な量子計算の計算複雑性に関する研究も共同で行うことができた。この研究では、量子計算の全てのプロセスを可逆操作にすることで、現状の量子計算からどれだけ計算能力が向上するかを代表的な計算量クラスとの包含関係を明らかにすることで示した。本結果 [5]は量子情報の主要国際会議である TQC2023 の口頭講演に選ばれ、論文はプロシーディングとして出版されている。

公開

・研究費執行状況：21 年度と 22 年度は概ね計画通りに予算執行ができた。23 年度は殆どを旅費に使用することを想定していたが、採録された論文の出版費用が別途必要になったため出版費用分だけ増額を行っている。23 年度も概ね計画通りに執行できる見込みである。

・研究成果の科学技術及び社会・経済への波及効果：将来の実現が期待されている量子情報技術において、代表的な技術である量子暗号と量子計算に関して、量子暗号については実装安全性証明の構築、量子計算についてはクラウド量子計算機を安全に利用できるようにする検証手法を確立したことで、これら量子情報技術の実現を促進する理論研究ができたと考える。

5. 主な研究成果リスト

（1）代表的な論文（原著論文）発表

研究期間累積件数： 5 件

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

概要：高速に送受信する実際の量子暗号システムでは、送信機から放出する光パルスは互いに独立とはみなせず、互いに相関することが実験で確認されている。2020 年に我々は送信パルスの相関を取り込んだ安全性証明の一般的な枠組みを与えた。本論文では、この一般理論を代表的な量子暗号方式である RRDPS に適用し、相関のある送信機を用いた RRDPS の安全性証明を与えた。その結果、本方式は送信機の相関に対して強い耐性があることがわかった。これは、光の送受信速度を上げていっても、1つの送信光から生成される鍵の量は大して低下しないという、実用上嬉しい特性を持っていることを意味する。

2. A. Mizutani, Y. Takeuchi, and K. Tamaki,
Finite-key security analysis of differential-phase-shift quantum key distribution,
Physical Review Research **5**, 02132 (2023).

概要：代表的な量子暗号である差動位相シフト方式(DPS)は、他の方式と比べて簡易な実験系で実装でき、実用化に向けた期待も高い。2019 年に与えられた安全性証明は無限長解析であるため、通信時間が無限という非現実的な場合でしか安全性を担保できていない。DPS を実装するためには、通信時間が有限の場合での鍵生成性能を明らかにする必要がある。今回我々は DPS の有限長安全性解析を行い、有限の通信時間での鍵生成レートを導出し、実際の実験セットアップで DPS が実現可能であることがわかった。

3. A. Mizutani, Y. Takeuchi, R. Hiromasa, Y. Aikawa, and S. Tani, Computational self-testing for entangled magic states, Physical Review A **106**, L010601 (2022).

概要：クラウドの計算機が「量子性」を持つ計算機かどうかを、現代のコンピュータ(古典計算機)だけでチェックする検証プロトコルを構成した。具体的には、万能量子計算の実行に不可欠な「マジック状態」の生成と測定をクラウドの計算機がどれだけ正確に実行する能力があるかを検証する暗号プロトコルを構成した。

（2）特許出願

研究期間全出願件数： 0 件

公開

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

- 国際会議口頭講演

1. A. Mizutani, Y. Takeuchi, R. Hiromasa, Y. Aikawa, and S. Tani, Computational self-testing for entangled magic states, Beyond IID in Information Theory 10 (2022).
2. R. Hiromasa, A. Mizutani, Y. Takeuchi, and S. Tani, Rewindable Quantum Computation and Its Equivalence to Cloning and Adaptive Postselection, 18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023).
3. A. Mizutani, DPS QKD, Workshop on Security Proofs in QKD (2023).

- 招待講演

4. 水谷明博, 量子計算の古典検証, 耐量子計算機暗号と量子情報の数理 (2022)

ほか査読なし国内会議発表 6 件