

研究終了報告書

「完全秘匿性を実現する量子 IoT アーキテクチャの構築」

研究期間：2019年10月～2023年3月

研究者：松崎 雄一郎

1. 研究のねらい

近年、IoT(モノのインターネット)の進展は目覚ましいものがある。しかし、IoTでは身の回りのものがインターネットにつながるため、セキュリティ対策が重要となる。本研究では、量子性を用いて、完全な秘匿性の保証されたIoTの理論的枠組みを提案する。量子センサ、量子コンピュータ、量子通信を統合化させることで、高効率・高速・安全な情報処理システムを構築して、超スマート社会の実現に貢献する。また量子センサ、量子コンピュータ、量子通信を複合化することで発現する多機能性を有するデバイスの理論的な提案を行う。具体的には、多地点での磁場情報を同時に読み出す量子センサネットワーク、サーバーに入力・出力を隠したままユーザーが計算を実行できるクラウド型のNISQ量子計算、秘匿性を有する遠隔操作量子センサなどの研究を行う。

2. 研究成果

(1) 概要

量子センサ、量子コンピュータ、量子通信のそれぞれの研究を個別に行いつつ、それらの複合化に関する研究を行った。量子センサに関しては、ノイズの影響下でベクトル磁場を高感度に求める方法の提案、スピンを高速に検出する方法の提案、電子スピン共鳴の高感度化プロトコルの提案、高感度量子センサのリソースとなるエンタングルメントの生成方法の提案などを行った。量子通信に関しては、その実現のための有望な素子であるダイヤモンド中の窒素・空孔(NV)中心の基礎的な特性の評価を行い、その新しい制御法の提案や、共同研究者による実験実証を行った。量子コンピュータに関しては、エラー抑制の手法の提案、機械学習の量子アルゴリズムの提案、量子化学のアルゴリズムの提案、超伝導量子ビットの性質の評価、分配関数を計算する量子アルゴリズムの提案、量子ビットのノイズ源となる環境の評価などを行った。量子センサと量子通信の複合化として、位相緩和が及ぼす遠隔量子秘匿センサへの影響の評価、磁場の発生源を秘匿する量子センサの提案、遠隔地における量子化軸の補正法の提案を行った。また、量子コンピュータと量子通信の複合化として、サーバーに入力・出力を秘匿したままユーザーが計算を実行できるクラウド型NISQ量子コンピュータの提案を行った。

(2) 詳細

研究テーマ A「ノイズの影響下でベクトル磁場を高感度に求める方法の提案」

ノイズのない理想的な状況では、エンタングルメントを用いることで、古典限界を超える精度でベクトル磁場の計測が可能であることが知られていた。我々は、ノンマルコフ型の位相緩和と呼ばれるノイズの影響下での、エンタングルメントを用いたベクトル磁場センサの性能を理論的に解析した。

• PHYSICAL REVIEW A 102(2) 1-10 2020

研究テーマ B「スピンを高速で検出する方法の提案」

スピンは磁場を発生するため、磁場センサを用いることでスピンの検出を行うことができる。しかしスピンから発生する磁場は極めて微弱であるために、単一の電子スピンや、比較的少数の核スピンを検出するためには、積算時間が長くなるという問題点があった。そこで我々は、NV 中心の間にエンタングルメントを生成して、エンタングルメント磁場センサを用いることでスピンを検出する方法を提案して、その性能を数値計算で評価した。

• JAPANESE JOURNAL OF APPLIED PHYSICS 60(7) 1-4 2021

• PHYSICAL REVIEW A 102(4) 1-14 2020

研究テーマ C「電子スピン共鳴の高感度化」

電子スピン共鳴は物質の性質を調べるための重要な技術である。しかし測定対象の電子スピンの偏極率が低いと、感度が低下するという問題点があった。そこで我々は、超伝導磁束量子ビットを用いて電子スピンを偏極させる方法を提案した。

• Physical Review A 105(1) 1-12 2022

研究テーマ D「高感度量子センサのリソースとなるエンタングルメントの生成方法」

量子ビットの間にエンタングルメントを生成することで、高感度な磁場センサが実現出来ることが知られている。しかし、量子ビットの間に効率的に大規模エンタングルメントを生成することは極めて難しい。そこで我々は、相互作用する一次元の量子ビットチェーンに、適切な外場を印加することで大規模エンタングルメントを生成する方法を提案した。

• PHYSICAL REVIEW A 103(6) 1-10 2021

• New Journal of Physics 24(3) 1-16 2022

• SCIENTIFIC REPORTS 12(1) 2022

研究テーマ E「NV 中心の制御法の開発」

NV 中心は、量子コンピュータ、量子通信、量子センサを実現するための有望な素子である。NV 中心はスピン1であるために、三つの準位を持つ。我々はその三つの準位間を、すべて振動磁場で直接遷移させる方法を提案して、慶応大学にて実験実証を行っていただいた。

• Japanese Journal of Applied Physics 59(11) 1-5 2020

研究テーマ F「エラー抑制手法の提案」

ノイズあり中規模量子 (NISQ) コンピュータの研究が理論・実験の双方からすすめられている。NISQ のアルゴリズムを実行する際に重要なのはエラーの抑制である。我々は、NISQ コンピューティングにおいて、ノンマルコフノイズの影響を抑制する手法、コヒーレントエラーと確率的エラーの両方を抑制する手法をそれぞれ開発した。

• Physical Review Letters 129(2) 1-6 2022

• Physical Review A 103(1) 1-7 2021

研究テーマ G「量子機械学習のアルゴリズムの提案」

ボルツマンマシンは、機械学習のための有望なアプローチの一つである。我々は、NISQ コンピューティングを用いてボルツマン機械学習を実行する新しいアルゴリズムを提案した。

• PHYSICAL REVIEW A 104(3) 1-12 2021

研究テーマ F「分配関数を計算する量子アルゴリズムの提案の提案」

分配関数は物性の情報を知るための重要な量である。我々は NISQ コンピューティングを用いて、分配関数を求める方法を提案した。

• Japanese Journal of Applied Physics 61(4) 1-11 2022

研究テーマ H「量子化学のアルゴリズムの提案」

量子化学において、分子のエネルギーを求めることができれば製薬などへの応用が可能であることが知られている。我々は、量子アニーリングを用いて、分子のエネルギーを求める新しい手法を提案した。

• New Journal of Physics 24(11) 113009-113009 2022

• Physical Review A 106(4) 2022

• Journal of the Physical Society of Japan 91(6) 1-6 2022

• Japanese Journal of Applied Physics 60(SB) 1-4 2021

• JOURNAL OF THE PHYSICAL SOCIETY OF JAPAN 90(5) 1-11 2021

研究テーマ I「超伝導量子ビットの性質の評価」

超伝導パラメロンと呼ばれる超伝導量子ビットの特性評価法の提案と、新しい制御法の提案を行った。具体的には、二周波のマイクロ波を同時に印加して分光測定をした際の、反射係数を計算して、超伝導パラメロンのパラメータを推定する方法を提案した。

• New Journal of Physics 23(9) 1-16 2021

• Scientific Reports 11(1) 1-9 2021

• Physical Review Applied 18(3) 2022

研究テーマ J「量子ビットのノイズ源となる環境の評価」

エネルギー緩和が起こった場合、量子系の情報は環境に流入していく。そのため秘匿性を持つ量子情報処理を実行する際には、エネルギー緩和が問題になる可能性があるため、緩和の性質を理解することは重要である。系から環境への情報の流入はエントロピー生成により定量化できることが知られている。我々は、環境が有限自由度である場合の、エントロピー生成率の振る舞いを定量的に解析した。

• Physical Review A 103(5) 1-15 2021

• Physical Review Letters 128(18) 1-7 2022

研究テーマ K「位相緩和が及ぼす遠隔量子秘匿センサへの影響の評価」

量子センサで得た情報を盗聴されることなく顧客に送信する、遠隔量子秘匿センサの研究が

行われている。しかし、量子センサはノイズに対して脆弱であり、遠隔量子秘匿センサがノイズの影響下でも秘匿性を保つことができるかは、非自明な問題として残されていた。我々は、遠隔量子秘匿センサが磁場と相互作用する際に、位相緩和の影響を受けた場合の秘匿性を評価した。

•Physical Review A 104(6) 1-18 2021

研究テーマ L「遠隔地における量子化軸の補正法の提案」

量子センサネットワークを形成する際に、離れた地点での量子ビットの量子化軸を同じ方向にそろえることは重要な課題である。我々は、エンタングルメントを利用することで、量子化軸の補正を高精度で実行する方法を提案した。

•Physical Review Applied 16(6) 1-16 2021

研究テーマ M「磁場の発生源を秘匿する量子センサの提案」

量子センサでネットワークを構成するには通常、1. 磁場の強度、2. 磁場の発生源の位置の、ふたつの情報を取得する。そこで我々は、量子センサネットワークにおいて、磁場の強度の情報は取得するが、磁場発生源の位置情報は取得しない、新しいプロトコルを提案した。筑波大学との共同研究成果である。

•Journal of the Physical Society of Japan 91(7) 1-12 2022

研究テーマ N「秘匿性を有するクラウド型 NISQ 量子コンピュータの提案」

NISQ のクラウド量子コンピュータを行うとき、現状の手法ではユーザーの情報がサーバーに漏洩してしまう問題点が存在する。我々は、NISQ のクラウド量子コンピュータにおいて、ユーザーの入力・出力などの情報が原理的にサーバーに漏洩しない手法を理論的に提案した。

•Physical Review A 105(2) 1-10 2022

3. 今後の展開

量子センサ・量子通信・量子コンピュータの組み合わせにより秘匿性を持つ新しいプロトコルを提案したので、今後はその実験実証を検討していく。実用化するために、より低スペックのデバイスでも作動できるように、プロトコルをよりノイズロバスタなものに改良していく。これは実験家の方と共同研究をしながら、実験での主なノイズ源を特定して、それによる影響を抑制できるパルス操作を理論的に考案する作業になっていく。これを今後、十年程度を目処にいく。

4. 自己評価

- 研究目的の達成状況: 量子センサ、量子通信、量子コンピュータの個別のプロトコルについて多くの理論提案を行い、さらにそれらを複合化させたプロトコルの提案も行った。多くの論文を出版できたので、非常に高い評価だと考えている。
- 研究の進め方: 実施体制としては、研究補助としてのリサーチアシスタントを雇用して、ま

た研究者を招聘することで、効率よく研究をすすめることができた。

・研究成果の科学技術及び社会・経済への波及効果:現在、量子技術は国家の安全保障のためにも重要だと認識され、世界中で研究・開発が進められている。本プロジェクトは、これまでにない「量子センサ・量子通信・量子コンピュータの複合化」というアイデアを実現させるための理論研究であり、その成果として新しいプロトコルを提案することに成功した。

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:27件

1.
<p>Yuta Shingu, Yuki Takeuchi, Suguru Endo, Shiro Kawabata, Shohei Watabe, Tetsuro Nikuni, Hideaki Hakoshima, Yuichiro Matsuzaki, Variational secure cloud quantum computing, <i>Physical Review A</i>, 2022, 105 1-10</p> <p>概要:変分量子アルゴリズム(VQA)は、NISQ デバイスの有用なアプリケーションとして考えられている。一方、ブラインド量子コンピューティング(BQC)は、クラウドネットワークを利用し、量子アルゴリズムに安全性を持たせる。しかし、BQC は誤り訂正機能付きの量子コンピューティングを想定しているため、多くの補助量子ビットが必要となり、NISQ デバイスには適さない。そこで我々は、顧客の安全性を保証した NISQ コンピューティングを効率的に実現する方法を提案した。本手法において、顧客が選んだパラメータと、アルゴリズムの出力の情報が、サーバーに流出しないことを厳密に証明した。</p>
2.
<p>Hideaki Okane, Hideaki Hakoshima, Yuki Takeuchi, Yuya Seki, Yuichiro Matsuzaki, Quantum remote sensing under the effect of dephasing, <i>Physical Review A</i>, 2021, 104 1-18</p> <p>概要:遠隔量子秘匿センサは、量子センサで得た情報の秘匿性を保ちながら顧客に送信する手法である。しかしながら量子センサはノイズに脆弱であるという問題点を持つ。そこで我々は、遠隔量子秘匿センサの位相緩和に対する耐性を理論的に解析した。その結果、積算回数が多いときは、位相緩和と状態準備のエラーが同程度の影響を与えて、秘匿性を落とすことがわかった。</p>
3.
<p>Yuichiro Matsuzaki, Hideaki Hakoshima, Kenji Sugisaki, Yuya Seki, Shiro Kawabata, Direct estimation of the energy gap between the ground state and excited state with quantum annealing, <i>Japanese Journal of Applied Physics</i>, 2021, 60, 1-4</p> <p>概要:量子化学における分子のエネルギーを知ることは、製薬などで重要となる。従来の手法では、量子アニーリングを用いることで、分子の基底エネルギーを求める手法は知られてきた。本論文では、基底エネルギーと励起エネルギーの差を量子アニーリングで求める方法を提案する。初期状態に重ね合わせをもちいることが従来の量子アニーリングの手法と大きな違いである。また非断熱的遷移と呼ばれるノイズに対してロバストであることも示した。</p>

(2) 特許出願

(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)