



## ムーンショット目標 6

2050年までに、経済・産業・安全保障を飛躍的に発展させる  
誤り耐性型汎用量子コンピュータを実現

# 実施状況報告書

## 2020年度版

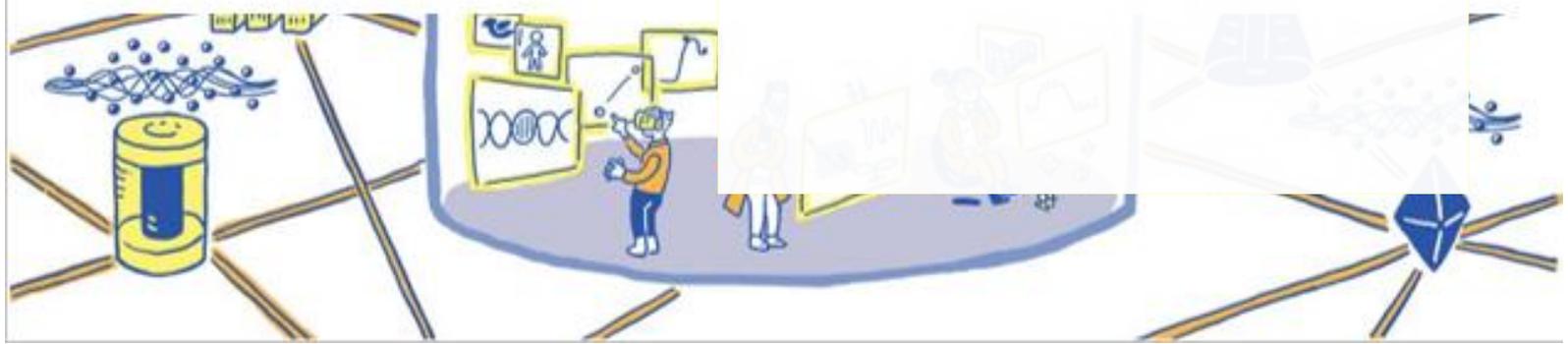
2020年12月～2021年3月

誤り耐性型量子コンピュータにおける理論・

ソフトウェアの研究開発

**小芦 雅斗**

東京大学 大学院工学系研究科



## 研究開発プロジェクト概要

量子情報、アーキテクチャおよび物理系の研究者を結集し、量子ビットの設計、誤り耐性方式の実装、効率的に計算を実行するためのコンパイラや言語までを包含した協調設計モデルを構築します。それにより、2050年には、大規模な量子コンピュータの実現を目指します。

[https://www.jst.go.jp/moonshot/program/goal6/61\\_koashi.html](https://www.jst.go.jp/moonshot/program/goal6/61_koashi.html)

## 課題推進者一覧

課題推進者	所属	役職
徳永裕己	日本電信電話株式会社 セキュアプラットフォーム研究所	特別研究員
小芦雅斗	東京大学 大学院工学系研究科	教授
都倉康弘	筑波大学 数理物質系	教授
越野和樹	東京医科歯科大学 教養部	准教授
Franco Nori	理化学研究所 開拓研究本部	主任研究員
藤井啓祐	大阪大学 先導的学際研究機構	教授
東浩司	日本電信電話株式会社 NTT 先端技術総合研究所	特別研究員
森前智行	京都大学 基礎物理学研究所	講師
杉山太香典	東京大学 先端科学技術研究センター	特任助教
田島裕康	電気通信大学 大学院情報理工学研究科	助教

## 1. 当該年度における研究開発プロジェクトの実施概要

クロスレイヤー協調設計モデルの構築に向けて、研究開発項目1でミニマムモデルの大枠をまとめ、その概要をプロジェクトの参画メンバーと共有した。研究開発項目2では、個別の物理系でこれまで明らかになっている機能や制約の整理を行うとともに、調和振動子系の研究に不可欠なシミュレーション手法の開発や、量子回路のシミュレーションを行うための QuTip モジュールの開発を進めた。研究開発項目3では、現在主流の表面符号の問題点を緩和するため、量子ビット間の接続性を低減する量子誤り訂正符号を構築した。研究開発項目4では、分散型構造を持つ量子コンピュータの基本スキームの前提となる、量子ビット、集積化チップ、バスの間の相互作用についての既知の情報を整理した。その他、量子コンピュータの計算能力に関する重要な定理の証明や、これまでにない安全性を有する量子プロトコルの提案を行った。また、数理科学的手法により、これまで別個に考えられていた量子コンピュータに関する定理を統一的に理解する道を拓いた。

### (1) 研究開発項目1: クロスレイヤー協調設計モデルの開発と拡張

ミニマムモデルの大枠をまとめ、その概要をプロジェクトの参画メンバーと共有した。また、現時点でミニマムモデルの構築において最も欠けている部分である、具体的なアプリケーションから表面符号や格子手術などの誤り耐性量子計算の基本的な操作へのコンパイルに関し、関連する文献の調査を行い、上位レイヤのリソース見積もりの見通しを明確にするとともに、誤り耐性量子計算において早期の実用化が見込まれている量子化学の分子ハミルトニアンに対する位相推定の調査を行った。

### (2) 研究開発項目2: 誤り耐性型量子コンピュータのハードウェア制御法の開発とその性能解析

ゲート制御型半導体量子ドットを用いた量子ビットの研究の現状について、項目1で構築が進められるモデルと適合を考慮しながら、誤り耐性型の量子メモリの実現に必要な機能と現状の課題について整理した。超伝導量子ビット系において、どのようにして量子ビットの長寿命化や制御・測定時間の短縮化が図られているかについて情報収集を行った。GKP 符号などの状態生成のための回路構成の探索などに有用な、多項式時間でシミュレートできる一般的な非ガウス状態生成手法を考案した。量子回路のシミュレーションを行うモジュール qip.noise の拡充により、QuTip において、現実的なノイズを取り込み、時間変化するパルスによって駆動される量子ゲートのシミュレーションが可能となった。

### (3) 研究開発項目3: 誤り耐性型量子コンピュータの性能改善のための量子誤り訂正法の開発とその性能解析

シンδροーム測定のカギ化や、符号距離の小さな符号との接続符号化などの新たなアプローチで、量子ビット間の接続性を低減する新たな量子誤り訂正符号の構築を行っ

た。具体的には、表面符号のデータ量子ビットおよびシンドローム量子ビットをそれぞれ2量子ビットのパリティ検査を実行する単純な符号で符号化する、というアイデアを用いた。その結果、隣接する3つの量子ビットとの2量子ビット演算のみでシンドローム測定が構成できることが明らかになった。これは、クロストーク低減のための量子ビットの周波数割り当ての設計等に有利であると考えられる。

#### (4) 研究開発項目4: 分散型構造を持つ誤り耐性型量子コンピュータの研究開発

量子ビットや集積化チップとバス間の相互作用は一般に、想定する量子ビットの種類や集積化チップの形状、バスの種類に依存するが、比較的広範な量子ビットに対して適用可能な特定の相互作用に注目し、そのモデル化を行う必要がある。今後の理論の拡張性を考慮に入れると、このモデルは量子ビットの違いをパラメータで吸収できるものが望ましい。これらの目標達成に向けた最初のステップとして、近年利用可能とされているバスと量子ビット間の相互作用について調査・情報収集を行った。特に、最新の高Q値共振器で可能となってきたことや、超伝導量子ビットとマイクロ波間の強い相互作用に注目し、情報収集を行った。

上記以外に、ムーンショット目標に資する研究として、任意のハミルトニアン基底状態の量子コンピュータ上での効率的生成が困難であることを、古典計算量理論で信じられている仮定への還元により示した。この結果は量子コンピュータの真の性能を理解する上で重要である。

#### (5) 研究開発項目5: 誤り耐性型量子コンピュータの新規手法・応用の萌芽的研究開発

証明者にランダムにBB84状態を送り、検証者にその古典的記述を送る Trusted center を導入することにより、完全古典かつ情報理論的健全な検証プロトコルの構築を行った。さらに、情報理論的安全性を持つ Non-interactive zero-knowledge proof の構築へと発展させた。

非スタビライザ符号である YCLO 符号については、表面符号との定量的な比較を行った結果、YCLO 符号は、符号効率は高いものの、閾値の高さや実装の容易さという観点からは表面符号よりも性能が低いことがわかった。

対称性を扱うリソース理論を多変数の一般的な対称性に拡張し、Fisher 情報量行列がリソース指標となることを示した。また、対称性があるダイナミクスの下で実行した任意の量子操作からの情報復元に関する統一的な制限を与える定理を与えた。この定理からは、従来知られていた、ユニタリダイナミクスの実装に関する制限、および、トランスバーサル符号の誤差と符号語数のトレードオフに関する定理が導かれる。量子コンピュータに関わりが深いこれらの定理は、全く別個のものとして捉えられていたが、この成果により統一的に理解することが可能となった。

## 2. 当該年度の研究開発プロジェクトの実施内容

### (1) 研究開発項目1: クロスレイヤー協調設計モデルの開発と拡張

#### 研究開発課題1-1: クロスレイヤー協調設計モデルの開発と拡張

当該年度実施内容:

ミニマムモデルの大枠をまとめ、プロジェクトの参画メンバーと共有した。また、現時点でミニマムモデルの構築において最も欠けている部分である、具体的なアプリケーションから表面符号や格子手術などの誤り耐性量子計算の基本的な操作へのコンパイルに関し、関連する文献の調査を行い、上位レイヤのリソース見積もりの見通しを明確にするとともに、誤り耐性量子計算において早期の実用化が見込まれている量子化学の分子ハミルトニアンに対する位相推定の調査を行った。

ミニマムモデルを構築するには、本プロジェクトに属する各レイヤに詳しい研究者との連携を図ることが不可欠である。このため、各研究項目の代表的な研究者と個別に議論を行い、今後のミニマムモデルの構築と3年目以降の連携に向けて意識を共有し、令和3年度の研究の指針を整理した。

上記以外に、ムーンショット目標に資する研究として、量子ビット数を増やさずにノイズを抑制する量子誤り抑制の機能を追加することにより、実行的に符号長や回路サイズを小さくする新理論の構築、現実的な量子デバイスに対して誤り抑制を実装する方式提案、量子ビットなどのリソースの使用量が効率的な量子アルゴリズム提案、超伝導回路を用いた量子誤り訂正向けオンライン復号器の提案、超伝導回路を用いたマイクロ波光子量子状態の生成と検証、共振器量子電磁力学系を用いた量子ゲートや量子通信方式の提案、を行った。

課題推進者: 徳永裕己(日本電信電話株式会社)

#### 研究開発課題1-2: クロスレイヤー協調設計モデルの開発と拡張

当該年度実施内容:

項目1で目標としているミニマムモデルについて、課題1-1と協力し、ミニマムモデルの大枠を構築した。現時点でミニマムモデルの構築において最も欠けている部分である、具体的なアプリケーションから表面符号や格子手術などの誤り耐性量子計算の基本的な操作へのコンパイルに関し、関連する文献の調査を行い、上位レイヤのリソース見積もりの見通しを明確にするとともに、誤り耐性量子計算において早期の実用化が見込まれている量子化学の分子ハミルトニアンに対する位相推定の調査を行った。

課題推進者: 小芦雅斗(東京大学)

## (2) 研究開発項目2: 誤り耐性型量子コンピュータのハードウェア制御法の開発とその性能解析

### 研究開発課題1-1: 量子ビットをベースとする要素技術の研究開発

当該年度実施内容:

ゲート制御型半導体量子ドットを用いた量子ビットの研究の現状について、「半導体材料」、「量子ビットの構成方法」、「単一/二量子ビット演算」、「量子状態読み出し」、「スケールビリティ」、「誤り耐性の検討」の項目に分割して検討を行い、項目1で構築が進められるモデルと適合を考慮しながら、誤り耐性型の量子メモリの実現に必要な機能と現状の課題について整理した。

また、量子ビットのデコヒーレンスの解析モデルとして量子マスター方程式/Floquet 量子マスター方程式を整備し、電子スピンのシャトリングへの適用を念頭に、断熱操作における量子状態制御の検討を進めた。特に固体中の開放量子系で重要となる非マルコフ性の効果についても解析を行い、非断熱条件では非マルコフ効果が顕在化することを明らかにした。固体量子ビットの性能評価に有用な様々なトモグラフィの手法について調査を行った。簡単なモデルにおいて Python を用いたシミュレーションプログラム作成を行った。物理的制約の把握に必要な理論的ツールである量子マスター方程式の定式化を進め、演算速度、散逸の評価を開始した。デバイスの基本性能評価に用いる各種トモグラフィのツールの整備を進めた。

課題推進者: 都倉康弘(筑波大学)

### 研究開発課題1-2: 量子ビットをベースとする要素技術の研究開発

当該年度実施内容:

国内外量子コンピューティングのための超伝導量子ビットの集積化は、Google や IBM などの外国企業において特に研究が進んでいるが、それらの研究グループの有する量子ビット系において、どのようにして量子ビットの長寿命化や制御・測定時間の短縮化が図られているかを、文献調査により情報収集を行った。

課題推進者: 越野和樹(東京医科歯科大学)

### 研究開発課題2: 調和振動子モードをベースとする要素技術の研究開発

当該年度実施内容:

任意の非ガウス状態生成手法において、古典計算機における量子状態の時間発展シミュレートのための計算量が、生成回路サイズに対して指数増大する問題があった。そこで効率的なアルゴリズム技法である分割統治法を応用することで、多項式時間で非ガウス状態生成をシミュレートできることを示した。これは、GKP 符号などの状態生成のための回路

構成の探索などに有用である。また、GKP 符号 とマルコフ決定過程による量子誤り訂正符号を組み合わせることで、計算量が線形かつ高い誤り耐性を持つ量子誤り訂正の手法を考案した。これにより復号にかかる計算量を大幅に削減できる可能性を示した。

課題推進者： 小芦雅斗(東京大学)

### 研究開発課題3: デバイス研究推進のためのソフトウェア技術開発

当該年度実施内容：

QuTip において量子回路のシミュレーションを行うモジュール qip.noise を拡充した。これにより、実験において現実的なノイズを取り込み、時間変化するパルスによって駆動される量子ゲートのシミュレーションが可能となる。ノイズの影響化で量子ゲートを実装する際に、事前に種々のパラメータの最適化を行えるなど、様々な状況で役立つと考えられる。

課題推進者： Franco Nori(理化学研究所)

### (3) 研究開発項目3: 誤り耐性型量子コンピュータの性能改善のための量子誤り訂正法の開発とその性能解析

#### 研究開発課題1: 新たな量子誤り訂正方式の開発

当該年度実施内容：

シンドローム測定のカテゴリ化や、符号距離の小さな符号との接続符号化などの新たなアプローチで、量子ビット間の接続性を低減する新たな量子誤り訂正符号の構築を行った。具体的には、表面符号のデータ量子ビットおよびシンドローム量子ビットを、それぞれ2量子ビットのパリティ検査を実行する単純な符号で符号化する、というアイデアを用いた。その結果、隣接する3つの量子ビットとの2量子ビット演算のみでシンドローム測定が構成できることが明らかになった。これは、クロストーク低減のための量子ビットの周波数割り当ての設計等に有利であると考えられる。また、忠実度が低い測定などの影響でシンドローム測定回路に導入されるエラーによる性能低下を改善するために、シンドローム測定を適応的に行う、適応的シンドローム測定法を構築した。この新方式では、シンドローム値が得られるステップが時間的に不均一になるという点があり、既存の表面符号のデコーダが利用できない。このため、時空間的に不均一なシンドロームから復号を行う復号アルゴリズムの構築も行なった。

課題推進者： 藤井啓祐(大阪大学)

### (4) 研究開発項目4: 分散型構造を持つ誤り耐性型量子コンピュータの研究開発

#### 研究開発課題1: 分散型構造を持つ誤り耐性型量子コンピュータの研究開発

当該年度実施内容：

量子ビットや集積化チップとバス間の相互作用は一般に、想定する量子ビットの種類や集積化チップの形状、バスの種類に依存するが、3年目のマイルストーン「分散型誤り耐性量子計算方式のミニマルモデル構築」に向け、比較的広範な量子ビットに対して適用可能な特定の相互作用に注目し、そのモデル化を行う必要がある。今後の理論の拡張性を考慮に入れると、このモデルは量子ビットの違いをパラメータで吸収できるものが望ましい。これらの目標達成に向けた最初のステップとして、近年利用可能とされているバスと量子ビット間の相互作用について調査・情報収集を行った。特に、最新の高Q値共振器で可能となってきたことや、超伝導量子ビットとマイクロ波間の強い相互作用に注目し、情報収集を行った。

上記以外に、ムーンショット目標に資する研究として、任意のハミルトニアン基底状態の量子コンピュータ上での効率的生成が困難であることを示した。具体的には、3ローカルハミルトニアン基底状態が、ポストセレクションが許された量子コンピュータでたとえ近似的にでも効率的に生成することができるなら、 $PP=PSPACE$  という計算機科学的に成立しないと予想される等号が導かれることを示した。この成果は、量子コンピュータの真の性能を理解する上で重要である。

課題推進者： 東浩司(日本電信電話株式会社)

#### (5) 研究開発項目5： 誤り耐性型量子コンピュータの新規手法・応用の萌芽的研究開発

##### 研究開発課題1-1: 誤り耐性型量子コンピュータの新規手法・応用の萌芽的研究開発

当該年度実施内容：

証明者にランダムに BB84 状態を送り、検証者にその古典的記述を送る Trusted center を導入することにより、完全古典かつ情報理論的健全な検証プロトコルの構築を行った。さらに、このプロトコルにおいて、Trusted center が検証者に送る古典情報を、ランダムに選んだ一部に制限することにより、新たな Non-interactive zero-knowledge (NIZK) proof を構築した。Trusted center が現状は Secret parameter (SP) model (証明者と検証者に異なる秘密メッセージを送るモデル) になっているという欠点を改善する方法についても提案した。これらの成果は、従来多くの NIZK が LWE 仮定に基づく計算量的なものであるのに対し、Soundness と Zero-knowledge property の両方、あるいはいずれかを情報理論的安全性にできるというこれまでにない大きな特長を持つ。

課題推進者： 森前智行(京都大学)

##### 研究開発課題1-2: 誤り耐性型量子コンピュータの新規手法・応用の萌芽的研究開発

当該年度実施内容：

非スタビライザ符号の非可換構造と符号性能の関係を明らかにするために、既知の非スタビライザ符号である YCLO 符号の性能評価に取り組んだ。接合方式に対する擬似閾値の概算を行った結果は、表面符号の閾値と比べて極めて小さいことがわかった。また、YCLO 符号では符号化と復号化で 3 量子ビットゲートを必要とすることから、YCLO 符号は、符号効率は高いものの、閾値の高さや実装の容易さという観点からは表面符号よりも性能が低いことがわかった。

課題推進者： 杉山太香典(東京大学)

### 研究開発課題1-3:誤り耐性型量子コンピュータの新規手法・応用の萌芽的研究開発

当該年度実施内容：

Resource theory of asymmetry (RToA) は対称性を扱うリソース理論の一種であり、covariant code をはじめとして誤り耐性型量子計算においても重要な役割を担うことが期待されている。群  $U(1)$  や  $R$  で定められる場合のように、対称操作が単一の保存則によって制限されるような場合には、Fisher 情報量がリソース指標として使いやすいことが分かってきている。当該年度は、これをより一般の対称性の場合に拡張する最初の段階として、任意の連続群対称性について、一般に Fisher 情報量行列をリソース指標として使用できることを示した。さらに、この Fisher 情報量行列が、物理量の揺らぎとどのように関係するかについて、定量的な研究を完成させた。

また、上記研究以外に、対称性があるダイナミクスの下で実行した任意の量子操作からの情報復元に関する統一的な制限を与える定理を与えた。この定理からは、従来知られていた、ユニタリダイナミクスの実装に関する制限、および、トランスバーサル符号の誤差と符号語数のトレードオフに関する定理が導かれる。量子コンピュータに関わりが深いこれらの定理は、全く別個のものとして捉えられていたが、この成果により統一的に理解することが可能となった。

課題推進者： 田島裕康(電気通信大学)

## 3. 当該年度のプロジェクトマネジメント実施内容

### (1) 研究開発プロジェクトのガバナンス

#### 進捗状況の把握

- ・東京大学工学系研究科に PM 支援体制チームを構築している。事務系統は研究科の支援を受けている。PM 補佐は適任者が見つからなかったため、次年度に持ち越しとなった。
- ・研究開発プロジェクトの推進に関する重要事項について必要な連絡及び調整を行うため、運営会議を設置した。運営会議の構成は、PM を議長とし、参加機関等（代

表機関、研究開発機関および JST) を参加者とする。3 月に運営会議を開催し、令和 3 年度からの新たな課題推進者/研究開発機関について承認した。

- ・課題推進者の研究の進捗状況の把握に努めた。

#### 研究開発プロジェクトの展開

- ・「研究開発項目 1 : クロスレイヤー協調設計モデルの開発と拡張」は、本プロジェクトの中でも、課題推進間の連携のハブ的な位置づけとなっている。項目 1 の担当機関にミニマルモデルの概要についてセミナー講演を依頼し、プロジェクト参画者の理解を深めた。また、その後、項目 1 と他の項目の参画機関間のミーティングを促した。
- ・令和 3 年度から追加する課題推進者 3 名の調整を行った。
- ・ポストク雇用のために人件費を有効活用するには、参画機関個別の運用規則なども勘案し、きめ細かい対応が必要であるとの認識から、JST と協議しながら令和 3 年度の人件費予算の配分方法を決定した。

#### (2) 研究成果の展開

- ・知的財産権の運用について協議する場として、必要があれば、知財運用会議を設置することとしていた。知財運用会議の構成は、PM を議長とし、協議の対象となる知的財産権に直接的または間接的に利害関係を有する研究開発機関等の一部または全部、および JST を参加者とする。今年度は、知財運用会議を開催する案件は生じなかった。
- ・最新の技術動向の把握に務めた。

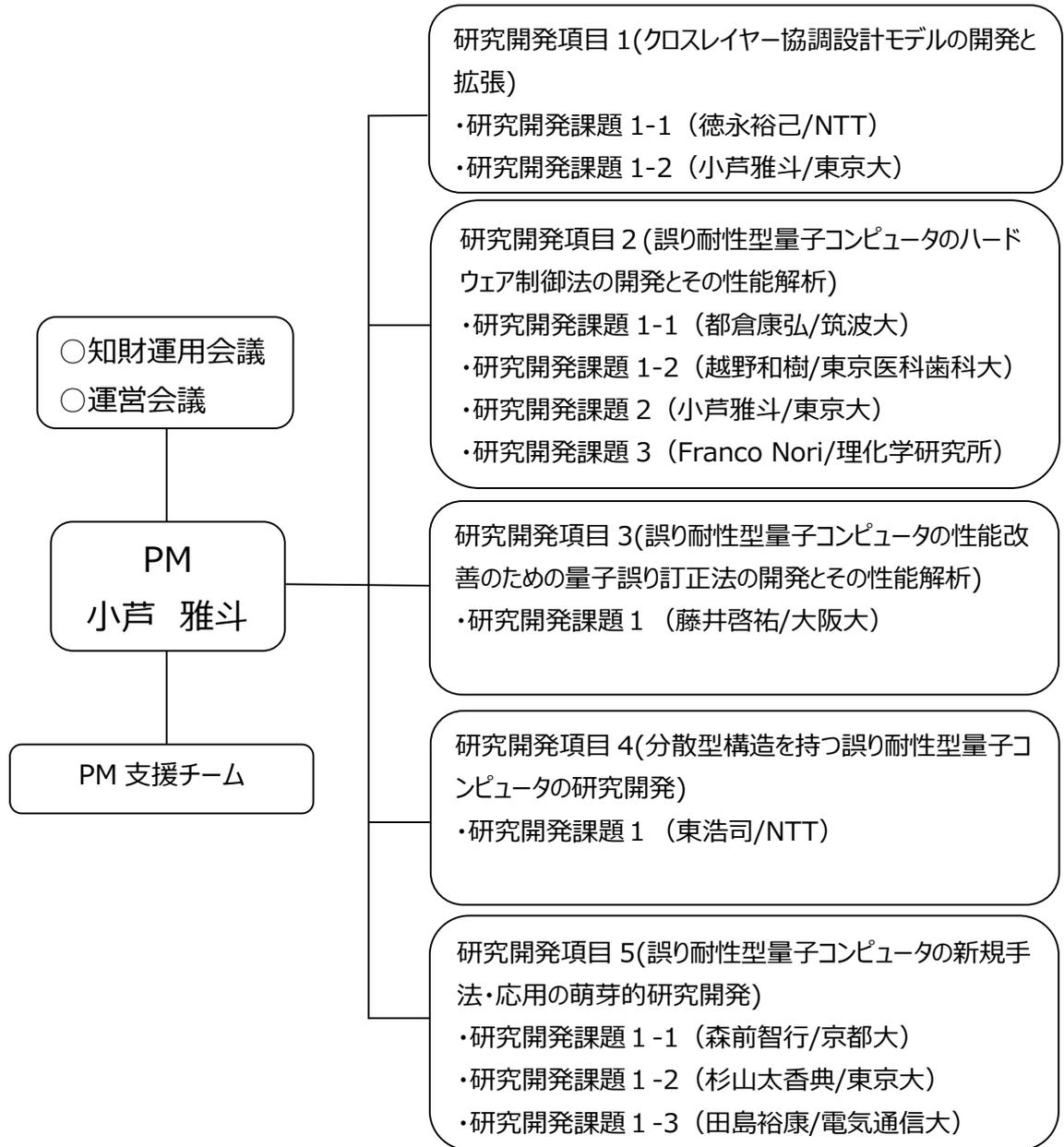
#### (3) 広報、アウトリーチ

- ・代表機関において、量子ネイティブ教育の取り組みを全学的に行う量子ネイティブ育成 WG に参加し、量子ネイティブ教育の質の向上に貢献した。
- ・数理科学分野をはじめとする関連分野の研究者との連携はまだ十分に開始されていない。引き続き次年度に検討を続ける。
- ・代表機関に所属する他のムーンショット事業 PM とも連携し、ホームページ等のデジタル媒体を利用した効果的な広報活動の準備を行っている。

#### (4) データマネジメントに関する取り組み

- ・データマネジメントプランに基づき、適切なデータ管理に務めた。報告すべき事項を課題推進者に周知し、年次計画開始時のプランに基づき、申告された案件の状況把握を行った。

#### 4. 当該年度の研究開発プロジェクト推進体制図



#### 知財運用会議 構成機関と実施内容

議長:PM、参加者: JST および協議の対象となる知的財産権に直接的または間接的に利害関係を有する研究開発機関等の一部または全部。当該年度は該当案件なし。

#### 運営会議 実施内容

3月に開催 令和3年度からの新たな課題推進者/研究開発機関について承認した。

## 5. 当該年度の成果データ集計

知的財産権件数				
	特許		その他産業財産権	
	国内	国際(PCT含む)	国内	国際
未登録件数	0	0	0	0
登録件数	0	0	0	0
合計(出願件数)	0	0	0	0

会議発表数			
	国内	国際	総数
招待講演	1	0	1
口頭発表	11	3	14
(うち、査読有)	0	0	0
ポスター発表	0	2	2
合計	12	5	17

原著論文数(※proceedingsを含む)			
	国内	国際	総数
件数	0	3	3
(うち、査読有)	0	3	3

その他著作物数(総説、書籍など)			
	国内	国際	総数
総説	1	0	1
書籍	0	0	0
その他	0	0	0
合計	1	0	1

受賞件数		
国内	国際	総数
0	0	0

プレスリリース件数
0

報道件数
0

ワークショップ等、アウトリーチ件数
4