様式 C-19

科学研究費補助金研究成果報告書

平成　２２　年　８　月　３０　日現在

研究種目：　基盤研究（C）
研究期間：　２００７ 年 度　～　２００９ 年 度
課題番号：　１９５００００１５
研究課題名（和文）量子対話知識証明の分析と量子暗号への応用

研究課題名（英文）An Analysis of Quantum Interactive Proofs and Their Application to Quantum Cryptography

研究代表者
山上　智幸（ TOMOYUKI　YAMAKAMI ）
福井大学・大学院工学研究科・教授
研究者番号：　８０２３０３２４

研究成果の概要（和文）：　量子力学の原理に基づく新しい通信形態が量子通信である。安全な量子通信を行うためには、現在の情報処理技術で実現可能な量子暗号システムを構築する必要がある。そのためにより現実的な量子デバイスを用い、量子暗号の基本暗号系の一つである量子ゼロ知識証明暗号系を分析する。また、量子通信の誤り訂正を行う量子リスト復号化法と、量子デバイスの能力を高める外部補助情報であるアドバイスの分析も行う。

研究成果の概要（英文）: Quantum communication has been developed over the past 30 years based on a novel theory of quantum mechanics. To establish secure quantum communication, we need safe and efficient quantum cryptosystems. From a more realistic viewpoint, we discuss quantum cryptographic primitives whose bases are a more realistic model of quantum devices. In particular, we study the strengths and weaknesses of quantum zero-knowledge proof systems. We also study the quantum list decoding of error-correcting codes and the notion of advice given to the quantum devices.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００７年度	1,400,000	420,000	1,820,000
２００８年度	1,100,000	330,000	1,430,000
２００９年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：　計算量理論、量子暗号、量子計算
科研費の分科・細目：　情報学・情報学基礎
キーワード：　量子暗号、量子計算、量子オートマトン、量子ゼロ知識証明、量子リスト復号、アドバイス、量子ハードコア関数

１．研究開始当初の背景

一般に暗号は情報通信のセキュリティ（安全性）の根幹に関わるものであり、近年の広域通信ネットワーク網の充実に伴い安全で有用な暗号システムの構築が急務である。特に無秩序に広がったインターネット空間では、個人のプライバシー保護やID確認がより困難になり、それを補完する有益な暗号システムが必要になった。そうした暗号システムは「基本暗号系」と呼ばれる単純な構成要素を土台として成り立っている。しかし、汎用されて

いる基本暗号系は未だその安全性が理論的に証明されたものがなく、常にある種の数学的問題の計算困難性を前提としている。例えば、現在多用されている公開鍵暗号RSAシステムの安全性は、整数の素因数を求める問題が多項式時間で解けないという経験則に依存している。従って、計算能力の高い計算機の登場で、こうした前提そのものが成り立たなくなる可能性が常にあった。

20世紀と共に幕を開けた量子力学に基づく世界観が漸く定着した1980年代初期、その量子力学の根本原理を利用した新しい通信・計算モデルが提唱された。以来30年以上が経過したが、その間に量子情報処理技術は急速に進歩し、かつては空想科学であった量子通信・計算デバイスが実現しつつある。量子情報は一般に、素粒子の量子的に重なり合った状態を表す「量子ビット」を基本単位として表現される。より正確には、量子ビットは古典ビットの線形１次結合として数学的に定義される。この様な量子情報は、例えば光子を使って量子ビットを実現することで、光軸ケーブルを通して遠隔地へ送信することが可能である。量子情報は量子力学的な制約から一般には複製（コピー）ができない点で、古典情報とは本質的に異なっている。また、２量子ビット以上を組み合わせることで、古典力学では生成できない特殊な「量子絡み合い」状態（EPRペアなどが有名）が構成でき、この状態を用いて任意の量子ビットをケーブルなしでテレポートすることができる。更に、1990年代には素因数分解を効率良く行う量子アルゴリズムが発見され、これを使ってRSA暗号を簡単に解読することが将来可能になった。

この様な量子情報の情報処理技術の近年の発展は優れた量子通信や量子計算を実現可能にしたが、それに伴い、これまでの古典暗号では量子情報処理に対応できなくなった。そこで新しいタイプの暗号システムの開発が必要になった。それが量子暗号である。1980年代半ばには量子鍵配送暗号システムBB84が提案され、幾つもの技術革新を経て近年漸く実用化の域に達しつつある。この暗号系は、量子情報の複製が不可能であると言う原理を利用し、情報理論的にも無条件に安全であることが証明されている。また21世紀の量子通信技術に基づく量子暗号の幅広い応用には、量子鍵配送暗号システム以外にも様々な役割を担う量子暗号システムを構築することが必要であった。

複雑な量子暗号システムを支える量子デバイスは、量子力学的に可能なユニタリ変換（つまりノルムを保存する線形一次変換）を各量子ビットに施すことで、情報処理（或いは計算）を実行する。ただし計算結果は一般に量子情報の形を取る為、「量子観測」と呼ばれる操作を行ってその内部情報を「見る」必要がある。このとき、量子情報はある確率で（０と１から成る）古典情報に崩壊してしまう。様々な物理的要因から、現在のところ量子計算機は７量子ビットまでしか取り扱えていない。理想的とされる多項式時間計算が実現されるのはまだ先になろう。また、現実の量子ビットは不安定で容易に崩壊してしまうため、より複雑な量子計算を行うために必要な量子メモリは未だ研究途上であり、新しい技術革新がなければ現在の技術水準での実現は困難であろう。

量子デバイスが一般に使用される社会を目指すためには乗り越えなければならない障害がまだ多数存在する。こうした障害を克服し、実用的で汎用な量子暗号システムを構築するためには、現在の量子情報処理技術に適合した量子計算機とそれに基づく量子基本暗号系の詳細な分析・研究が望まれていた。

２．研究の目的

この研究は量子暗号の今後の発展を支えるための基礎研究であり、将来の実用的な応用を考慮した、汎用性のある量子暗号システムを構築するための敷石を築くことを目標とする。研究課題の一つは、量子情報工学の現状に適合した通信処理能力を有する量子デバイスの分析であり、もう一つはそうしたデバイスに基づいた実用的で汎用性の高い基本暗号系の基礎的な解析である。

この研究の独自性は、計算モデルとして現実度の高いより制限された量子計算機を使用している点である。現在の科学技術で実現可能な量子計算機は、量子計算理論で主流な（理想的とされる）多項式時間計算モデルとは異なり、様々な物理学的及び技術的な制約を受けている。一般の量子暗号理論が取り扱う暗号システムは強力な量子計算を要求しているため、現在の科学技術では実現が困難である。この欠点を補うために、より現実的な視点から量子暗号システムを見直し、現在の技術水準で十分実現可能でしかも有用性の高い量子暗号システムを構築する必要がある。そのために、ユーザが使用する量子デバイスの情報処理能力に明確な限界を設定した量子情報処理モデルを使った新しい理論を展開する。この様に極端に制限のある量子デバイスを取り扱う理論は、通常の多項式時間計算可能性の理論と性格を異とするが、今後の科学技術の方向性を示唆する上で大切である。これまでのところ、そのような研究は数少ない。ここでは独自の量子メモリを持たない量子計算機モデルを研究の基礎に据え、量子基本暗号系の計算能力の分析を行う。

量子通信網を通しての古典情報の送受信では、通信過程での量子情報の崩壊が起こり

易い。このため、古典入力語（メッセージ）の符号化とその逆の復号化が如何に正確に効率よく行われるかが鍵となる。量子通信過程での符号語の量子的崩壊が極端に大きくなると、ごく少数の入力語の候補者リストを作成する復号化法（リスト復号と呼ばれる）が必要になる。特に、効率の良い量子リスト復号化法はある種の量子基本暗号系と密接に関連があり、リスト復号化の分析はそれを基にした量子暗号システムの分析にも繋がる。

更に、物理的に制限のある量子情報処理を行う量子デバイスの情報処理能力を高める方法の一つに、適切に前処理した補助情報を外部から付与するものがある。この補助情報は入力データと共に量子デバイスに与えられ、計算の過程で有効に活用される。そうした方法の中で、入力長にのみ依存する補助情報は、1980年代から古典計算量理論の中で研究が続けられている。この概念の量子計算理論への応用は2004年になって初めてなされた。この研究では、この補助情報が量子計算に与える役割・影響を明らかにする。

量子情報工学は未だ発展途上であり、その進歩は今後の研究に大いに委ねられている。この研究は、こうした量子情報工学の発展に寄与すると共に、量子力学の本質の理解を深め、今後の量子情報研究の方向を指し示す足掛かりになることを最終目標とする。

３．研究の方法論

まず、研究の基盤である情報処理能力に制限のある量子デバイスを考察し、そのデバイスの計算効率を分析・評価する。続いて、そこで得られた結果を利用し、現実的な枠組みの中で基本暗号系の能力の分析を行う。こうした分析は、幾つかのテーマに分けられ、それぞれのテーマごとに特有の研究手法を用いて行われる。

これまでの多くの研究とは異なり、より現実的な視点から特に量子メモリのない量子計算機モデル(特に一方向量子オートマトンと呼ばれるモデル）を研究の基礎に据え、量子基本暗号系の計算能力の分析を行う。多項式時間計算量に基づく従来の量子暗号システムは一般にある種の数学的な仮定を必要とする。これに対し制限のある計算モデルを取り扱うことで、こうした仮定なしで暗号システムの能力を議論することが可能である。

量子鍵配送暗号システムに関しては多くの論文が書かれているが、この研究では、それ以外の「量子対話証明系」と呼ばれる特殊な基本暗号系を考察する。この暗号系は、基本的に証明者と呼ばれる「証明」を提供する通信者と、判定者（或いは評価者）と呼ばれる「証明」の正しさを判定する通信者の間の通信から成る基本暗号系である。この量子対話証明系に更にゼロ知識と呼ばれる条件を付加したものが「量子ゼロ知識証明系」である。古典通信の場合、この基本暗号系は計算機ネットワークユーザのID認識などの管理システムとして実際に機能している。例えば、悪意のある第３者（ハッカーなど）が不正にネットワーク接続を要請した場合、管理者は使用者の個人情報（プライバシー）を知ることなくその要請を却下することができる。この研究では、判定者が量子オートマトンを使用した場合の量子対話証明系並びに量子ゼロ知識証明系の受理能力の分析を、古典の場合と比較しながら総合的に行う。

ここで量子通信そのものに目を向けると、そこで重要な争点の一つは、送信者が如何に情報を効率良く符号化し受信者が如何に正確に復号化できるのか、ということである。特に通信回線の誤り確率が高い場合には、通常の復号化法ではなく「リスト復号」と呼ばれる特殊な手法を用いることがある。効率の良い量子リスト復号化法を持った性質の良い誤り訂正符号からは、基本暗号系の一つである「量子ハードコア関数」を構成することができる。特に、古典ハードコア関数からは、応用の広い「擬似乱数発生器」を構築することが可能である。この研究では、効率の良い量子リスト復号化法を持つ誤り訂正符号の分析を行う。この時、NP完全問題との関連性を示すことで、情報処理計算の困難さを議論する。

量子メモリを持たない量子デバイスに外部情報を補助的に与えることで、情報処理能力を飛躍的に高めることができる。この研究では、「アドバイス」と呼ばれる外部補助情報を付与した場合、如何なる計算能力の跳躍が起こるのかを、古典デバイスと比較しながら解析する。特に、決定性アドバイス、確率アドバイス、及び量子アドバイスなどの異なる種類のアドバイスを考察し、それらの特性を分析することでオートマトンの言語認識能力の差を明らかにする。量子アドバイスは量子メモリ同様その保持が困難であるため、確率アドバイスで代用できるのが望ましい。このために、どの様な場合に代用が利くのかを論じる。特に、アルゴリズムの複雑さと共に、受理される言語の構造的な複雑さを議論する。

４．研究成果

方法論の節で述べたように、本研究は大きく4つのテーマに分けられ、以下の節ではそれぞれのテーマごとに主だった研究結果について、非専門家にも概略が掴めるように数式を廃し簡潔に述べる。

（１）[計算モデルの分析]　より現実的な視点から新しい理論を展開するためには、情報処理能力の制限された量子通信・計算モデル

を導入する必要がある。特に、量子メモリは未だ実現のめどが立っていない点を踏まえ、固有の量子メモリを持たない量子計算機モデルとして、「量子（有限）オートマトン」と呼ばれる数学的なモデルを考察する。一般に、有限オートマトンは入力情報（入力語と呼ぶ）が書かれたテープとその情報を読み込むテープヘッド、更に与えられたアルゴリズムを実行するCPUとから成り立っている単純なデバイスである。CPUは与えられたアルゴリズムの各命令をステップ毎に実行する。即ち、テープヘッドを移動させ、テープ上の入力記号を読み取り、CPU内部の状態を更新する。CPUが受理または非受理の特別な内部状態になった時点で全ての動作が終了する。オートマトンによって受理される入力語の全体を受理言語と呼ぼう。量子オートマトンは古典（有限）オートマトンの量子版として1997年に導入されたものであり、その動作の仕方によって幾つかの種類がある。中でも量子オートマトンのCPU内部の量子状態の量子観測を各ステップ毎に行うモデル（多数観測量子オートマトンと呼ばれる）を用い、これを応用した量子システムについて分析を行った。特に入力情報を読み込むテープヘッドが（左から右へ）一方向にしか移動できないモデルは、実時間で入ってくる入力データ（及び通信情報）を瞬時に処理していくオンライン計算に対応している。

この様な量子オートマトンに関し、本研究ではその特性の一端を明らかにした。量子オートマトンの動作の分析は量子観測操作のために複雑であるが、ここでは量子オートマトンの受理できる言語の特性を同値類の概念を使って表現した。これによって、量子オートマトンでは認識不可能である言語を示すことがより容易になった。

また、判定者の使用する計算機を量子オートマトンに制限した量子対話証明系は、西村ー山上（2004年）が導入した概念であり、この研究の基礎となるものである。ここで用いる量子オートマトンは入力テープと対話用の通信機能を備え、各ステップ毎に証明者と通信を行いながら計算を進めていく。ただし、量子オートマトンはCPUのごく限られた記憶容量を除き、一般の量子メモリを持たないので、証明者との対話全てを記録しておくことは不可能である。

（２）[量子対話証明システムの能力の分析]
量子対話証明系は、多項式時間計算量理論の枠組みの中で2000年に導入された。これは証明者と判定者間の通信を介して次の二つの条件を満足する暗号系である。(i) 肯定の解答を持つ入力語に対し、証明者が正しい証明を送った時、判定者は高い確率で入力語を受理する。(ii) それ以外の入力語に対しては、証明者がどの様な偽の証明を送っても、判定者は高い確率で非受理（または拒絶）する。通常、証明者は無制限の計算能力を有するが、これに対し判定者の計算能力は有限である。この研究では特に、判定者の計算能力を量子メモリを持たない量子オートマトンに限定する。この様なより現実的な制約のあるシステムの研究は、今まであまり例がない。古典の場合ですら、1990年代初頭に確率オートマトンを使った古典対話証明系の研究例があるだけである。

判定者の計算能力がこの様に制限された場合、暗号系としての能力はどの程度であろうか。オンライン入力方式の一方向量子オートマトンに限定された判定者は、(形式言語理論の)「正規言語」のみしか受理することができない。量子オートマトン単独では受理できない正規言語が存在する事実と比較すると、以上の結果から、証明者の存在が暗号系の受理能力を高めていることが分かる。

この暗号系の実際の運用を考えると、証明者と判定者との一回あたりの通信量は固定され、また通信回数にも制限が存在しよう。では、対話回数は対話証明系の能力に影響を与えるのであろうか。これに関し、対話回数が一回の場合と多数の場合とでは言語の受理能力に本質的な差があることが（どの様な仮定もなしで）証明できる。

これまで述べてきた量子対話証明系は原則的に証明者と判定者の二者間の通信モデルであった。この基本暗号系の拡張として、お互いに見識のない多数のハッカーが攻撃を仕掛けた場合を想定し、複数の証明者が参加する通信モデルを考える。ただし、面識がないため証明者間の通信はないものする。古典の系では、多数の証明者を巧妙に利用することで受理可能な言語集合が飛躍的に広がることが知られているが、量子対話知識証明系ではどうであろうか。ここでは、量子オートマトンを確率オートマトンで模倣（シミュレーション）することで量子暗号系を古典暗号系に還元し、量子暗号系としての計算能力を分析するという証明手法を用いる。このために、証明者間に通信が禁じられているという性質を逆に利用し、証明者同士を互いの監視に使う、つまり、一方の証明者が提供する証明の真偽を、他方の証明者からの情報を使って判断する。しかし、この還元性は自明ではない。それは、量子力学的な性質の一つである「量子絡み合い」が証明者間に生成されることで、何らかの情報の共有が起こるからである。シミュレーションにおいてこの情報共有を排除できることが証明の要である。

量子対話証明系に更に次の条件（ゼロ知識条件と呼ばれる）を付け加えたものが、量子ゼロ知識証明系である。(iii) 証明者は対話を通して判定者からどんな有益な情報も高確率

では得られない。このゼロ知識条件が、ID確認などの暗号システムに応用される要因である。証明はより複雑になるが、量子ゼロ知識証明系についても量子対話証明系と同様の結果が得られる。つまり、複数の証明者を持つ量子ゼロ知識証明系はNEXP言語を受理する。ここでNEXPは非決定性のアルゴリズムを用いて指数時間で受理できる言語の集合である。

（3）[量子リスト復号化法の分析] 量子通信を通して受信した符号語は、通常量子崩壊などによる誤り(エラー）を含むので、符号化前の入力語を復号する特別な方法（復号化法）が必要である。その方法の一つに「リスト復号」がある。これは、誤り確率が非常に大きな場合に、一意に復号化する代わりにごく少数の入力語の候補者リストを生成するものである。このリストから正しい入力語を選択するアルゴリズムが与えられれば、通常の復号化が得られる。

古典リスト復号は既に様々な分野への応用が成されているが、量子リスト復号化の概念は2006年になって漸く河内－山上によって提案された。量子リスト復号は、量子暗号の基本暗号系の一つである「量子ハードコア関数」を簡単に構成できる重要な概念である。ハードコア関数は「一方向性関数」を用いて定義される。この一方向性関数は基本暗号系の一つであり、入力から関数の値を効率良く計算できるが、関数の値から入力を求めることは困難である関数である。ハードコア関数の値は、どの様な一方向性関数の値のみからも効率良く計算することができないという性質を持つ。

では、どの様な誤り訂正符号が効率の良い量子リスト復号化法を持つのであろうか。その様な性質の良い符号を見出すことが河内－山上の主な結果であったが、そうした符号は技巧的なものが多い。例えば、(内積の値を使った)「アダマール符号」や（ルジャンドル記号の値を求める)「ルジャンドル記号符号」などは多項式時間で量子リスト復号が可能であるが、それらの「入力変換率」は指数的に小さいという欠点がある。ここで入力語変換率は、入力語とそれを符号化して得られた符号語との割合を指す。固定アルファベットを持ち入力変換率が多項式的に小さく、更に効率の良い量子リスト復号可能性を持つ符号は未だ見つかっていない。その様な符号は存在するのであろうか。

これに関しては、もし多項式の値を使った「一般リード・ソロモン符合」が効率良く量子リスト復号可能であれば、この符号とアダマール符号とを組み合わせることで、要求された符号が得られる。この研究では、一般リード・ソロモン符合の効率の良い量子リスト復号化が困難なことを示した。詳しくは、もしこの符号が多項式時間量子リスト復号可能ならば、全てのNP完全問題が効率良く解けることを証明した。NP完全問題とは、非決定性の多項式時間アルゴリズムで受理される問題の中で最も難しい問題のことである。このようなNP完全問題を解く多項式時間アルゴリズムは存在しないと信じられているので、一般リード・ソロモン符号は効率の良い量子リスト復号アルゴリズムを持たないであろう。この結果は、量子リスト復号化法の性格を特徴付けるものと考えられる。通信過程での符号語の量子的崩壊度を表すため、符号語が量子的に正しく送られる平均的な確率から1/2を引いた値を単に「バイアス」と呼ぶ。この値が小さい程通信の正確さが失われ、符号語の量子的崩壊が大きいと言える。このバイアスが極端に大きな場合に限って、一般リード・ソロモン符合が多項式時間量子リスト復号アルゴリズムを持つことを示した。この量子アルゴリズムは、幾つかのサンプル値から隠された多項式を復元する古典アルゴリズムを利用している。

（4）[外部補助情報の役割の分析] 一般に、量子メモリを持たない量子オートマトンの言語受理能力は極端に限られているため、その能力を向上させるためにコンパクトな外部情報の活用を考える。古典暗号でもこの様な外部補助情報を用いた研究は多く、如何により多くの情報をアドバイスに埋め込み、如何にその情報を制限された計算資源を使って引き出すのかが重要な争点となっている。

この研究では、そうした外部補助情報の一つである「アドバイス」を用いる。これは1980年代初頭に古典計算量理論に導入された概念であり、入力長にのみ依存する補助情報である。アドバイスは通常の入力の他に外部から計算機に与えられ、この補助情報を有効に活用することで、計算機は要求された結果を導出する。多項式時間計算量理論の枠組みでは、量子計算へのアドバイスの導入は西村－山上（2004年）によって始められた。アドバイスの種類として、決定性アドバイスや確率アドバイス、並びに量子アドバイスなどがあり、それらの役割や情報圧縮能力について分析を行った。決定性アドバイスとは異なり、確率アドバイスでは全ての古典情報がある確率分布に従って生成され、また量子アドバイスでは量子情報が生成される。

本研究では、只木－山上－Lin（2004年）が導入したアドバイス方式を使用する。即ち、補助情報は通常入力と同時に実時間でオンライン提供される。これは、補助情報を入力語を読む以前に前処理しておく方式と本質的に異なり、実時間で入力情報を処理する計算モデルという観点からは自然である。

量子計算との比較対象として、決定性アド

バイスが与えられた古典オートマトンが受理できる言語の新しい特徴付けを与え、古典計算におけるアドバイスの能力の有益性の分析を行った。別な観点から、アドバイスはオンライン処理可能な情報圧縮技法と見ることもできる。その意味では、決定性アドバイスは情報圧縮率が極めて低い。これと対照的に、確率アドバイスはある種の確率アルゴリズムの計算能力を飛躍的に増大することを示した。特に、誤り確率が50%になった場合、簡単な確率アドバイスを使って全ての決定問題を解くことが可能である。

確率アドバイスのもう一つの優れた性質は、誤り確率が比較的小さな確率アルゴリズムを決定性アルゴリズムに帰着させる能力である。つまり、確率アドバイスは誤り確率の小さな確率アルゴリズムを必要としない。これは量子アドバイスとは本質的に異なる点である。反対に、誤り確率の小さな確率アルゴリズムでは、どの様な確率アドバイスを使用しても全ての（形式言語理論の）文脈自由言語を認識することが不可能である。これは、確率アドバイスの限界の一つと考えられる。これを示すには、ゲーム理論の基本定理を確率アルゴリズムに応用するという手法を用いる。

アドバイスの能力の限界を示すには幾つかの方法があるが、次に、ある特別な構造的性質を有するか否かで示そう。自由文脈言語が「免疫性」と呼ばれる構造的な性質を持つことは既に知られているが、アドバイスを持つ有限オートマトンの分析を通して、更に強い免疫性（「主要免疫性」と呼ぶ）を持つことを示した。この免疫性の概念は1960年代に古典計算量理論に導入され、どの様な無限部分集合も有限オートマトンでは認識できないという性質を指す。別な言い方をすると、決定性アドバイスが十分な情報を有限オートマトンに提供できないため、自由文脈言語すら認識することができない。主要免疫性は基本暗号系の一方向性関数と密接な関係があり、有限オートマトンの計算に限ると、決定性アドバイスを用いても一方向性関数が存在し得ないことを証明できる。しかし、その条件を緩めてスタックを記憶媒体として許すと、弱い意味での一方向性関数が構成できる。即ち、その関数値はスタックを用いて計算可能であるが、その逆関数の値はどの様なアドバイス付き有限オートマトンでも計算不可能である。

量子アドバイスは多くの情報を含む量子情報を生成するが、量子オートマトンでは全ての自由文脈言語を受理できるほどには能力が増加しない。量子オートマトンに肯定的な視点は、量子アドバイスを確率アドバイスで代用できる点であろう。つまり、量子アドバイスを量子的に生成する代わりに、古典的な手段で確率アドバイスを生成し使用しても、量子オートマトンの計算能力は変わらない。これは、一方向量子オートマトンが量子メモリを持たないことと、その動作が一方向に制限されていることから証明できる。

［本研究が社会に与える影響と今後の展望］
シリコンチップに基づいた現在の計算機は、チップ容積を小さくすることで計算の高速化を実現してきたが、近い将来物理的な限界に達し、社会は新たな技術革新を要求するであろう。限界のその先の選択の一つが量子情報処理であり、それを応用する量子通信・計算である。この研究はこのような量子暗号の発展に寄与するものであり、将来の量子情報産業の育成とその方向性を指し示す上で多大な貢献をするものと思われる。

しかし、本研究が明らかにしたものは、量子情報処理分野が抱える課題のごく一部であり、未解決の問題が未だ数多く残されている。こうした問題を一つずつ解決して行くことが今後の研究課題である。

５．主な発表論文等

〔雑誌論文〕（計６件）
① T. Yamakami. “The roles of advice to one-tape linear-time Turing machines and finite automata.” Accepted for publication at International Journal of Foundations of Computer Science, 2010. A conference version appeared in ISAAC 2009, Lecture Notes in Computer Science, Vol.5878, pp.933—942, Honolulu, USA, 2009.

〔国際会議発表〕（計５件）
① T. Yamakami. “Quantum list decoding from quantumly corrupted codewords for classical block codes of polynomially small rate.” Proceedings of the Thirteenth Computing: The Australasian Theory Symposium (CATS 2007), pp.153—162, Ballarat, Australia, 2007.

〔研究会発表〕（計３件）
① T. Yamakami. “Quantum finite automata with advice.” 情報処理学会、第127回アルゴリズム研究会、論文番号127-4、８ページ、名古屋大学、2009年。

〔その他〕
ホームページ
http://TomoyukiYamakami.ORG

６．研究組織
(1)研究代表者
山上　智幸（ TOMOYUKI YAMAKAMI ）
福井大学・大学院工学研究科・教授
研究者番号：８０２３０３２４