様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月１２日現在

機関番号：１２４０１
研究種目：基盤研究(B)
研究期間：2009～2011
課題番号：21300002
研究課題名（和文）量子情報理論と量子計算量理論の融合技術の展開

研究課題名（英文）Advances in crossover between quantum information theory and quantum computational complexity theory

研究代表者
小柴　健史（KOSHIBA TAKESHI）
埼玉大学・大学院理工学研究科・准教授
研究者番号：60400800

研究成果の概要(和文)：量子情報理論と量子計算量理論の融合技術を発展させて，対話型証明，暗号理論，ネットワーク理論などの諸問題に対して適用した．量子対話型証明に関しては，複数証明者間の量子エンタングルメントの効果を追究し，量子対話型証明の理論を発展させた．また，ネットワーク符号化における量子通信の可能性を検討し，効率化通信手法の提案を行った．従来の古典暗号の枠組みでは証明困難であったハードコア述語に対して量子暗号理論を介することでその証明を構築可能にした．量子暗号理論へのフィードバックを行うため，様々な古典暗号プロトコルの考案を行った．

研究成果の概要（英文）：We developed useful techniques in quantum information theory and quantum computational complexity theory and applied them to interactive proof systems, cryptography, network theory and so on. With respect to quantum interactive proof systems, we investigated effects of quantum entanglements among multiple provers. Moreover, we considered the possibility of quantum communication in network coding and proposed efficient protocols. We proved the hard-core property of a function by the quantum computational complexity theory, while it had not been proved from the classical theory. Furthermore, we proposed several classical cryptographic protocols, which bring some ideas to quantum cryptography.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	4,600,000	1,380,000	5,980,000
2010 年度	3,300,000	990,000	4,290,000
2011 年度	3,200,000	960,000	4,160,000
年度			
総　計	11,100,000	3,330,000	14,430,000

研究分野：総合領域
科研費の分科・細目：情報学・情報基礎
キーワード：量子計算量理論，量子情報理論，暗号理論，量子アルゴリズム

１．研究開始当初の背景

量子情報科学は，量子力学の原理に基づいた計算・通信モデルを考えることにより，従来の情報科学の限界を超えたより強力な情報処理を可能にする分野として注目され発展してきている．量子情報理論の最大の成果の一つである量子鍵配送(例えば，Bennett & BrassardによるBB84プロトコル)は二者間通信に

おける究極の暗号基礎技術を与える一方で，現代暗号の中心的成果である多者間の多様なプロトコルは鍵配送のみでは実現しない．しかも多者間通信を想定した現代暗号の安全性の重要な根拠である素因数分解の困難性の仮定はShorによる量子アルゴリズムの存在により崩れるため，量子計算機の存在下でも安全な暗号系の構築が最重要課題となっている．さらに，ビットコミットメントやコイン投げなどの基本プロトコルは，量子情報理論的に完全な安全性は達成不可能であると証明されている．そのため量子計算量的な安全性概念によるアプローチと量子情報理論的な安全性概念の緩和によるアプローチが取られている．この流れにおいて，当該研究のテーマである量子情報理論と量子計算機科学，特に量子計算量理論との融合は，将来の暗号・通信技術の核となる要素技術や基礎理論の確立に重要な役割を果たすと考えられる．

また(量子ではない)従来の情報理論と計算機科学の融合による成功事例は数多く存在し，例えば確率的検査可能証明や統計的ゼロ知識証明の研究などがある．特に前者は計算量クラスNPの新たな特徴付けを与え，近似不可能性という新たな理論体系の開拓や，符号理論に対する新展開など，計算機科学と情報理論双方の進展に大きく寄与した．一方，擬似乱数生成や計算量的エントロピーなど，情報理論的概念に計算量理論的概念を導入することにより新たな研究分野を創成した事例がある．量子の場合においても，量子情報理論と量子計算機科学，特に量子計算量理論の融合は，量子情報科学分野全体に貢献することができると期待される．量子暗号においては量子情報と量子計算の境界が十分に近い事例が既に見出されている．例えば，一方向性関数の逆計算の困難性に基づくLamport署名の量子版であるGottesman-Chuangの方式は，量子情報理論的に逆計算が困難な量子関数の構成を与えることにより計算量的な仮定を除去している．また，研究代表者らの提案による量子公開鍵暗号は公開鍵の発行数に応じて量子計算量理論的な安全性から量子情報理論的な安全性へと変化する性質を持つ．これらの性質を体系的に整備することにより量子暗号理論の確立に貢献できると期待できる．また，量子エンタングルメントの数理的な性質を解明することにより，研究分担者らによって量子ゼロ知識証明が理論整備され，多証明者量子対話証明の能力が解明されつつある．量子エンタングルメントは量子情報および量子計算の分野の至るところに現れるため，その解明は量子情報科学全般への発展へ寄与するものと期待できる．

２．研究の目的

量子情報理論と量子計算機科学，特に量子計算量理論との双方向での融合を通して，量子暗号を始めとして，量子計算，量子通信など，量子情報科学の分野全体の進展に貢献できる基礎理論の構築を大目標とする．量子情報理論と量子計算量理論の双方の特長を生かした量子暗号の要素技術が確立しつつある現状を踏まえて，まず，それを発展させ量子暗号の理論として整備することを主目的とする．さらに，量子情報理論的概念を計算量理論的立場から解析し量子情報理論への新展開を与えることや，量子計算量理論に量子情報理論的手法を応用し個々の計算機科学的問題の解決につながる新しい統一的な視点や技法を追求することも目指す．

３．研究の方法

本研究の方法をアプローチごとに大別すると以下のようになる．

(A) 量子情報理論的概念の計算量理論的立場からの解析を通じた量子情報理論への新展開
(B) 量子情報理論と量子計算量理論の双方の特長を生かした量子暗号の要素技術確立
(C) 量子計算量理論への量子情報理論的手法の応用による計算機科学的諸問題解決へ向けた新しい統一的視点・技法の追究

の３つに分類され，アプローチごとに量子情報理論と量子計算量理論の融合技術の展開を図る．各アプローチのテーマとして，(a) 量子エンタングルメントや量子通信路の計算機科学的性質の解析，(b) 量子暗号基礎プロトコルの理論整備，(c) 量子情報理論から量子アルゴリズム論へのフィードバックについて研究を行う．(a)の量子エンタングルメントの理解は量子多パーティセキュア計算の敵対者を想定するときに必要な技術であり，量子通信路の理解は暗号通信技術に必須である．また，(b)で必要とする量子エンタングルメント

や量子通信路の数理的理解を(a)のテーマとしてフィードバックさせることができる．暗号技術はアルゴリズムの技術であり，(b)のテーマで必要な技術を(c)から得ることができる．このように(a)(b)(c)の各テーマが相互連携することにより相乗効果を高めるとともに研究サイクルを速く循環させることを狙う．

(A)は情報理論的側面が強い研究で，主に松本，小林が担当する．(C)は計算量理論的側面が強い研究で，主に河内が担当する．(B)は中間的な研究で主に小柴と田中が担当する．(B)が対象とする量子暗号理論には量子情報理論と量子計算量理論が混在しており，量子計算量理論を量子情報理論に活かす技術として(A)が存在し，量子情報理論を量子計算量理論に活かす技術として(C)が存在する．小柴と田中の役割分担は，量子暗号理論は広範な分野であるため，分野を二分してそれぞれを守備領域として担当する．また，応用として量子暗号理論のみに限定しないように，(A)と(C)は(B)の支援を超えて新たな応用領域の拡大も視野にいれる．各サブテーマは独立ではなく相互に連携しているため横断的な研究が存在する．つまり，(A)にもアルゴリズム的な要素が要求される一方で，(C)でも情報理論的な要素が要求され，相互に連携を図りつつ研究を遂行する．

４．研究成果

まず，対話証明と呼ばれる証明者と検証者間のプロトコルについての成果について言及する．対話証明の基本的な性質に完全性と健全性がある．完全性とは，証明者は検証者にある主張に対する証明を持っていることを納得させるという性質で，健全性とは，証明者が偽の証明を提示してきたときには検証者はそれを拒絶するという性質である．まず，量子対話型証明において複数証明者間の共有エンタングルメントの効果に関する研究を行い，検証者は古典のままであるが，証明者らにエンタングルメントを用いることを認める多証明者対話型証明において，PSPACE が２証明者１ラウンド証明を持つことを示した．一方，計算量クラス NEXP に対する２証明者対話型証明構成の既存の試みの問題点を指摘し，３証明者の場合と異なる可能性も指摘した．誤り確率に制限のない量子対話型証明において決定性指数時間計算量クラス EXP を含み，有限誤りの場合の多項式領域計算量クラス PSPACE を(EXP≠PSPACE という予想の下)大きく凌駕することを示した．NP の量子版である QMA に関して，完全性に誤りのない片側誤り証明モデルが一般の両側誤り証明モデルと同等の証明能力を持つか否かは長年の未解決問題である．この解決に向けて，証拠が古典情報で与えられる QMA に関しては，この問題が肯定的に解決されることを示した．これは量子オラクルと呼ばれる古典オラクルの量子版において相対化された世界では否定的な結果が示されていたものであり，量子オラクルによる状況証拠を乗り越えることが可能な，量子的に相対化されない初の非自明な結果としても注目される．また，証明に用いた加法的に受理確率を調整する技法は，簡潔でありながら汎用性もあり，今後様々な問題に広く応用されることが期待される．

新たな研究分野として，ネットワーク符号化における量子通信の可能性について研究し，複数対の情報を各情報源から各目的地に送信する問題において，補助的に古典情報を送ることを許せば，古典ネットワーク符号化が可能な全ての通信網で，任意の未知量子状態を効率よく完全に送信することを可能にする符号化技法の構成に成功し，量子ネットワーク符号化の可能性の道を拓いた．さらに，複数対の情報を各情報源から各目的地に送信する問題において，補助的に古典情報を送ることを許すことにより，非線形符号化も含め古典線形ネットワーク符号化が可能な全ての通信網で，任意の未知量子状態を効率よく完全に送信可能な符号化技法の構成に成功した．

量子計算と暗号理論の境界領域の研究として，量子一方向性関数の逆計算の困難性および量子ビット委託方式について考察した．特に，量子一方向性関数から量子計算機に対しても安全で，かつ今までに知られていないようなハードコア述語を構成することに成功した．ハードコア述語は暗号理論において重要かつ基礎的な概念であり，量子計算理論的な観点から暗号理論に新たな視点を導入するものと期待できる．量子暗号からのアプローチとして，インタラクティブハッシュと BB84 状態の同等性に関する結果を得て，量子一方向性関数から非対話の統計的秘匿量子ビット委託プロトコルの構成に成功した．量

子計算を用いて安全なマルチパーティ計算を実現する方法として，量子特有な方法が散発的に検討されている．その実現へ向けて，暗号理論の観点から量子テレポーテーション型の観測ベース量子計算の可能性について考察し，安全な代理計算方式が実現できることを示した．

量子情報および量子計算へのフィードバックを掛ける意味で，古典対話型証明の研究も同時に遂行した．古典対話型証明における乱数の重要性について考察し，ある種の乱数を用いた対話型証明が乱数を必要としない対話型証明で模倣できたとすると，論理回路族に対する非常に高い計算量の下界が得られることを示した．古典暗号理論においては，弱い理想化された圧縮関数によるハッシュ関数，tag-KEM/DEM フレームワークと呼ばれる公開鍵暗号方式，より現実的な紛失通信方式に着目し新たな方式の提案や安全性について考察した．情報理論的安全性の観点から対称鍵暗号の情報理論的頑強性について研究を行い，情報理論的頑強性とその他の情報理論的安全性との関係性を明らかにし，その応用として既存の情報理論的頑強性を持つ対称鍵暗号の鍵長サイズが最適であることを示した．紛失通信と呼ばれる暗号基本プロトコルに対して，既存モデルで前提であった敵の動作制限を無くし敵に任意動作を許すような新しいモデルのもとで、暗号理論的な安全性と等価なゲーム理論的安全性についての考察を与えた．また，情報漏洩に対して安全な暗号が近年注目されているが，公開鍵暗号の暗号化アルゴリズムで用いられた乱数が漏洩した場合も安全性を保つ公開鍵暗号方式の構成を行った．量子攻撃耐性を持つ暗号系構成の基礎として，情報理論的な頑健性の定義と最も基本的な秘匿性の一般化が等価であることを示した．この結果を応用することで既存の情報理論的な頑健性を持つ秘密鍵暗号系の秘密鍵長の最適性を証明することができた．また量子アルゴリズムの設計にも利用される Gowers 一様性を応用し，多項式の次数評価に対する質問計算量の解析手法を与えた．

これらの研究成果は量子情報理論と量子計算量理論の融合技術の発展的成果であるが，融合技術の適用領域は主に通信プロトコルに関するものが大半である．今後は分野を創成すべく幅広く研究するよりもトピックを絞って深く発展させることを目指し，基盤研究(A)「量子プロトコル理論の深化」(課題番号：2424001，研究代表者：小柴健史，2012 年度～2016 年度)において継続研究を行う．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 23 件）

1 R. Nishimaki, E. Fujisaki, K. Tanaka, An efficient non-interactive universally composable string-commitment scheme, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E95A**, 2012, pp.167-175, 査読有

2 R. Nishimaki, E. Fujisaki, K. Tanaka, A multi-trapdoor commitment scheme from the RSA assumption, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E95A**, 2012, pp.176-184, 査読有

3 A. Kawachi, H. Tanaka, O. Watanabe, Estimating the Gowers norm of modulo functions over prime fields, *IEICE Transactions on Information and Systems* **E95D**, 2012, pp.755-762, 査読有

4 A. Kawachi, C. Portmann, K. Tanaka, Characterization of the relations between information-theoretic non-malleability, secrecy, and authenticity, *Lecture Notes in Computer Science* **6673** (ICITS 2011), 2011, pp.6-24, 査読有

5 A. Bogdanov, A. Kawachi, H. Tanaka, Hard functions for low-degree polynomials over prime fields, *Lecture Notes in Computer Science* **6907** (MFCS 2011), 2011, pp.120-131, 査読有

6 K. Tanaka, A. Yamada, K. Yasunaga, Weak oblivious transfer from strong one-way functions, *Lecture Notes in Computer Science* **6980** (ProvSec 2011), 2011, pp.34-51, 査読有

7 H. Namiki, K. Tanaka, K. Yasunaga, Randomness leakage in the KEM/DEM framework, *Lecture Notes in Computer Science* **6980** (ProvSec 2011), 2011, pp.309-323, 査読有

8 M. Larangeira, K. Tanaka, Programmability

in the generic ring and group models, *Journal of Internet Services and Information Security* **1**, 2011, pp.57-73, 査読有

9 K. Matsumoto, Test of purity by LOCC, *Progress in Informatics* **8**, 2011, pp.111-113, 査読有

10 C. Portmann, K. Tanaka, Information -theoretic secrecy with access to decryption oracles, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E94A**, 2011, pp.1585-1590, 査読有

11 T. Koshiba, S. Sawada, Public discussion must be back and forth in Secure Message Transmission, *Lecture Notes in Computer Science* **6829** (ICISC 2010), 2011, pp.325-337, 査読有

12 A. Kawachi, T. Yamakami, Quantum hardcore functions by complexity -theoretical quantum list decoding, *SIAM Journal on Computing* **39**, 2010, pp.2941-2969, 査読有

13 T. Matsuda, R. Nishimaki, K. Tanaka, CCA proxy re-encryption without bilinear maps in the standard model, *Lecture Notes in Computer Science* **6056** (PKC 2010), 2010, pp.261-278, 査読有

14 A. Kawachi, A. Numayama, K. Tanaka, K. Xagawa, Security of encryption schemes in weakened random oracles, *Lecture Notes in Computer Science* **6056** (PKC 2010), 2010, pp.403-419, 査読有

15 T. Hirano, K. Tanaka, Key generation for fast inversion of the Paillier encryption function, *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences* **E93A**, 2010, pp.1111-1121, 査読有

16 J. Kempe, H. Kobayashi, K. Matsumoto, T. Vidick, Using entanglement in quantum multi-prover interactive proofs, *Computational Complexity* **18**, 2009, pp.273-307, 査読有

17 H. Kobayashi, K. Matsumoto, T. Yamakami, Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, Article 3, 2009, 査読有

18 H. Kobayashi, F. Le Gall, H. Nishimura, M. Rötteler, General scheme for perfect quantum network coding with free classical communication, *Lecture Notes in Computer Science* **5555** (ICALP 2009), 2009, pp.622-633, 査読有

19 A. Numayama, K. Tanaka, On the weak ideal compression functions, *Lecture Notes in Computer Science* **5594** (ACISP 2009), 2009, pp.232-248, 査読有

20 T. Matsuda, R. Nishimaki, A. Numayama, K. Tanaka, Security on hybrid encryption with the tag-KEM/DEM framework, *Lecture Notes in Computer Science* **5594** (ACISP 2009), 2009, pp.343-359, 査読有

21 K. -Y. Cheong, T. Koshiba, S. Nishiyama, Strengthening the security of distributed oblivious transfer, *Lecture Notes in Computer Science* **5594** (ACISP 2009), 2009, pp.377-388, 査読有

22 K. -Y. Cheong, T. Koshiba, Reducing complexity assumptions for oblivious transfer, *Lecture Notes in Computer Science* **5824** (IWSEC 2009), 2009, pp.110-124, 査読有

23 T. Hirano, K. Wada, K. Tanaka, Primitive power roots of unity and its application to encryption, *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences* **E92A**, 2009, pp.1836-1844, 査読有

〔学会発表〕（計 13 件）

1 T. Ito, H. Kobayashi, J. Watrous, Quantum interactive proofs with weak error bounds, Innovations in Theoretical Computer Science 2012 (ITCS 2012), 2012 年 1 月 9 日, Cambridge, MA, USA

2 M. –H. Nguyen, K. Tanaka, K. Yasunaga, Leakage-resilient CCA2 public-key encryption from 4-wise independent hash functions, 2011 International Conference on Advanced Technologies for Communications, 2011 年 8 月 2 日, Nang, Vietnam

3 H. Kobayashi, F. Le Gall, H. Nishimura, M. Rötteler, Constructing quantum network coding schemes from classical nonlinear protocols, 2011 IEEE International

Symposium on Information Theory (ISIT 2011), 2011 年 8 月 1 日, St. Petersburg, Russia

4 H. Kobayashi, F. Le Gall, H. Nishimura, M. Rötteler, Constructing quantum network coding schemes from classical nonlinear protocols, The 14th Workshop on Quantum Information Processing (QIP 2011), 2011 年 1 月 13 日, Singapore

5 T. Koshiba, T. Odaira, Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function, The 14th Workshop on Quantum Information Processing (QIP 2011), 2011 年 1 月 11 日, Singapore

6 T. Ito, H. Kobayashi, J. Watrous, Quantum interactive proofs with weak error bounds, The 14th Workshop on Quantum Information Processing (QIP 2011), 2011 年 1 月 10 日, Singapore

7 H. Kobayashi, F. Le Gall, H. Nishimura, M. Rötteler, Perfect quantum network communication protocol based on classical network coding, 2010 IEEE International Symposium on Information Theory (ISIT 2010), 2010 年 6 月 18 日, Austin, Texas, USA

8 D. Gutfreund, A. Kawachi, Derandomizing Arthur-Merlin games and approximate counting implies exponential-size lower bounds, The 25th Annual IEEE Conference on Computational Complexity (CCC 2010), 2010 年 6 月 9 日, Cambridge, Massachusettes, USA

9 T. Koshiba, Interactive hashing and BB84 states, Quantum Information in Paris, 2010 年 5 月 27 日, Paris, France

10 K. Matsumoto, On monotone 'metrics' in the channel spaces (Invited Talk), The 5th Workshop ad memoriam of Carlo Novero, 2010 年 5 月 26 日, Turin, Italy

11 H. Kobayashi, F. Le Gall, H. Nishimura, M. Rötteler, Perfect quantum network coding with free classical communication, The 13th Workshop on Quantum Information Processing (QIP 2010), 2010 年 1 月 21 日, Zurich, Switzerland

12 K. Matsumoto, Monotone ‘metric’ in the channel space: Resource conversion approach, The 13th Workshop on Quantum Information Processing (QIP 2010), 2010 年 1 月 20 日, Zurich, Switzerland

13 T. Ito, H. Kobayashi, K. Matsumoto, Oracularization and two-prover one-round interactive proofs against nonlocal strategies, The 24th Annual IEEE Conference on Computational Complexity (CCC 2009), 2009 年 7 月 17 日, Paris, France

６．研究組織

(1)研究代表者

小柴　健史（KOSHIBA TAKESHI）
埼玉大学・大学院理工学研究科・准教授
研究者番号：60400800

(2)研究分担者

松本　啓史（MATSUMOTO KEIJI）
国立情報学研究所・情報学プリンシプル研究系・准教授
研究者番号：60272390

小林　弘忠（KOBAYASHI　HIROTADA）
国立情報学研究所・情報学プリンシプル研究系・研究員
研究者番号：60413936

田中　圭介（TANAKA KEISUKE）
東京工業大学・大学院情報理工学研究科・准教授
研究者番号：20334518

河内　亮周（KAWACHI　AKINORI）
東京工業大学・大学院情報理工学研究科・助教
研究者番号：00397035