様式 C-19

科学研究費補助金研究成果報告書

平成２３年５月２４日現在

機関番号：22604
研究種目：若手研究（Ｂ）
研究期間：2008～2009
課題番号：20760242
研究課題名（和文）　量子暗号に適した量子誤り訂正符号の開発
研究課題名（英文）Construction of quantum error-correcting codes for quantum cryptography

研究代表者
藤田　八郎（HFujita Hachiro）
首都大学東京・システムデザイン研究科・助教
研究者番号：30431795

研究成果の概要（和文）：量子暗号は原理的に解読が困難な暗号であり，従来の RSA 暗号のような，手間暇をかければ必ず解読できる暗号とは一線を画す．量子暗号はこのような高い安全性を有する一方，秘密鍵の生成レートが低いという問題点がある．本研究では，量子暗号の高レート化を実現するべく，より効率的な誤り訂正方式の確立を目指した．研究の第１段階では，拡張 CSS 符号と呼ばれる量子誤り訂正符号に着目し，その性能についていくつかの知見を得た．次にこの知見に基づいて効率的な量子暗号のプロトコルを構成し，その安全性証明を試みた．残念ながら証明の一部に誤りが見つかり，研究期間内に目標を達成できなかった．

研究成果の概要（英文）：Quantum cryptography cannot be broken in principle. This is a big advantage over the RSA cryptosystem that can be broken if an adversary has a powerful computer. Although quantum cryptography is secure, its key generation rate is small. The aim of this research is to construct higher key rate quantum cryptography. The research project consists of two steps. In the 1st step we investigate properties and decoding of the enlarged CSS code and in the 2nd step we use the results obtained in the 1st step to construct a higher key rate protocol. Unfortunately, we have not yet proved the security of the protocol.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	400,000	120,000	520,000
2009 年度	400,000	120,000	520,000
年度			
年度			
年度			
総　計	800,000	240,000	1,040,000

研究分野：符号理論，情報セキュリティ
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：量子暗号，量子誤り訂正符号，ＣＳＳ符号

１．研究開始当初の背景

（１）安心安全な社会を実現するため，暗号技術・情報セキュリティ技術の重要性はますます高まっている．近年，インターネットに

よる商取引が一般的になり，安全性の高い暗号方式が求められている．現在広く利用されている暗号方式はＲＳＡ暗号（代表的な公開鍵暗号）と共通鍵暗号を組合せたハイブリッド方式である．この方式は，共通鍵暗号の秘密鍵をＲＳＡ暗号で暗号化してまず正規の送受２者間で秘密鍵を共有し，その後，共通鍵暗号で平文を暗号化するというものであり，ＲＳＡ暗号の安全性が方式の安全性に影響する．ＲＳＡ暗号の解読技術は日進月歩に進んでおり，またハードウェアの性能向上とも相まってＲＳＡ暗号の解読の脅威は増大する一方である．また，量子コンピュータが実現すれば，ショアの素因数分解アルゴリズムにより現実的な時間でＲＳＡ暗号が破られることも分かっている．

（２）量子暗号はその安全性の根拠を量子力学の基本原理に置いており，（量子力学が正しいと仮定すれば）情報理論的に安全であることが証明されている．理論ばかりでなく実用化研究も盛んで多数の実装実験が報告されており，一部商用化も始まっている．

量子暗号の課題は，単一光子の生成・検出といった物理や量子エレクトロニクスの課題から，誤り訂正・プライバシー増幅といった情報理論の範中の課題まで多岐にわたる．誤り訂正は量子暗号の長距離化や鍵生成レートの改善につながるため，効率的な誤り訂正方式が求められていた．

本研究ではこのような状況を鑑み，量子暗号に適した効率的な誤り訂正方式を確立することを目指した．

２．研究の目的

（１）量子暗号の安全性を証明するアプローチにはいくつかの方法があるが，中でもショアとプレスキルによる安全性証明（以下，ＳＰ証明法）は構成がシンプルで理解しやすく，様々な量子暗号プロトコルの安全性証明に応用されている．ＳＰ証明法のキーポイントはＣＳＳ(Calderbank-Shor-Steane)符号と呼ばれる量子誤り訂正符号の適用である．自然な問いとしてＣＳＳ符号以外の量子誤り訂正符号を用いた場合のＳＰ証明法の拡張が考えられる．

（２）ＣＳＳ符号と類似し，かつより効率的な量子誤り訂正符号のクラスに拡張ＣＳＳ符号がある．図１に拡張ＣＳＳ符号とＣＳＳ符号の相対最小距離（最小距離を符号長で割ったもの）と符号化レートのトレードオフの関係を示す．　図から拡張ＣＳＳ符号は同じ最小距離をもつＣＳＳ符号よりも効率がよいことが分かる．

（３）本研究ではＳＰ証明法で用いられているＣＳＳ符号を拡張ＣＳＳ符号で置き換え，量子暗号の鍵生成レートを改善することを目指した．

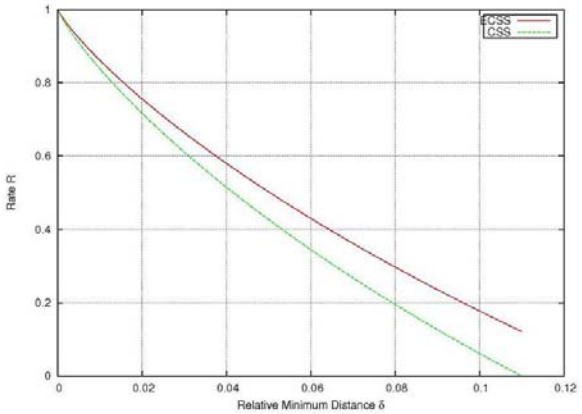

図１．相対最小距離と符号化レートのトレードオフ関係（赤色の曲線が拡張ＣＳＳ符号，緑色がＣＳＳ符号を表す）

３．研究の方法

（１）ＣＳＳ符号は約１５年前に量子コンピュータや量子メモリの高信頼化のために考案された量子誤り訂正符号であり，これまでに多くの知見が得られている．一方，拡張ＣＳＳ符号についてはその定義といくつかの具体的な符号パラメータが知られているものの，復号法や漸近的な復号性能については（筆者の知る限り）まだ明らかにされていない．まず研究の第１段階として，ＣＳＳ符号と対比しながら拡張ＣＳＳ符号の復号法と漸近的な復号性能を明らかにしていく．

（２）（１）で得られた知見をもとにＳＰ証明法を見直し，拡張ＣＳＳ符号を用いた証明法を確立する．

（３）上の誤り訂正方式は通信路の特性に依らないユニバーサルな方式と言える．鍵生成レートを改善するための別のアプローチとして通信路の記憶（メモリー）を利用する方法も考えられる．物理的に実現可能な量子通信路の多くで記憶があり，通信路雑音に相関があることが少なくない．通信路の記憶はバースト誤りを発生する厄介な問題であるが，

ディジタル通信やディジタル記録では通信路の記憶を逆に利用し，伝送容量の増大に役立てている．このアイデアを量子暗号に適用すれば鍵生成レートを改善できる可能性がある．量子暗号の実装で一般的に利用される量子通信路は既設の光ファイバである．現実の通信路をモデル化することは容易ではないので，本研究では通信路の特性と盗聴者による擾乱を簡単な数学モデルで近似した場合の理論的な考察を行う．

４．研究成果

（１）３節の研究の方法（１）で述べた課題，すなわち，拡張ＣＳＳ符号の復号法と漸近的性能に関する研究についてはその結果を雑誌論文の①に纏めた．この論文の中で，拡張ＣＳＳ符号もＣＳＳ符号と同様に制御 NOT ゲートとアダマール変換を用いてシンドロームを計算できること，シンドロームから誤りパターンを効率的に算出できることを明らかにした．なお，拡張ＣＳＳ符号では通常のＣＳＳ符号と異なり，ビット反転誤りと位相反転誤りを独立に訂正することはできない．拡張ＣＳＳ符号の漸近的な復号性能についても同論文で明らかにしている．ただし，ここで得られた拡張ＣＳＳ符号の漸近的性能は特定の復号法に基づくため最適であるとは限らず，改善の余地がある．また，３節の研究の方法（２）の研究のために必要な準備として，拡張ＣＳＳ符号の一般化を定義し，その性質を明らかにした．

（２）論文①で得られた結果をもとに，ＳＰ証明法に沿って拡張ＣＳＳ符号を用いた量子暗号プロトコルを構成し，その安全性の証明を試みた．残念ながら証明の一部に論理的ギャップが見つかり，計画通り研究が進まなかった．この証明の問題点は，（１）で述べた拡張ＣＳＳ符号の最適復号性能の問題と，拡張ＣＳＳ符号におけるビット反転誤りと位相反転誤りの不分離性の２つの問題と関連している．この問題点については集中的に検討したものの，研究期間内に解決することができなかった．

（３）３節の研究の方法（３）で述べたアイデアは当初の研究計画では計画しておらず，本研究課題の期間中に着想したものである．まず，記憶のある量子通信路の雑音を簡単なマルコフ連鎖でモデル化し，誤り訂正符号としてＣＳＳ符号を用いた場合の達成可能レートを導出した．このレートは記憶通信路の量子容量に一致することが分かっている．次にこの通信路を仮定した上でエンタングルメント純粋化に基づく鍵配送プロトコルを構成した．このプロトコルは通信路雑音を静的なマルコフ連鎖と仮定すれば安全であることが証明できる．

このプロトコルの問題点はエンタングルメントを準備，伝送する必要があること，量子誤り訂正符号を用いるため量子コンピュータと量子メモリを必要とすることである．これらを実現することは現時点では技術的に困難であり，提案プロトコルは実現できない．この問題を解決するため，ＳＰ証明法に倣ってプロトコルの簡略化を行った．これにより，エンタングルメントを必要とせず，また量子コンピュータと量子メモリの不要な，いわゆる準備測定型のプロトコルに等価に変換できる．ただし厳密に言うと両者は等価ではなく，エンタングルメント型のプロトコルと準備測定型のプロトコルの間には安全性レベルの点でギャップがある．大雑把に言うと，エンタングルメント型は指数的に安全であるのに対して，準備測定型は準指数的な安全性しか保証できない．

記憶のある量子通信路の雑音が静的なマルコフ連鎖で記述できると仮定した上で記憶特性を利用する提案プロトコルと記憶特性を利用しない従来のプロトコルを比較すると，提案プロトコルの達成可能な鍵生成レートは一般に記憶特性を利用しないプロトコルの鍵生成レートよりも高くなることが証明できる．実際，簡単な例で鍵生成レートを計算して提案プロトコルの優位性を確認している．

以上の研究成果を論文にまとめ，しかるべき国際会議または学術雑誌に投稿することを計画している．

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１件）

① H. Fujita, On Steane’s enlargement of Calderbank-Shor-Steane codes, Quantum Information & Computation, Vol.10, pp.0981-0993, 2010. 査読有

〔学会発表〕（計１件）

① H. Fujita, Using enlarged Calderbank-Shor-Steane codes in quantum cryptography, Quantum Communication, Measurement and Computing, August 23, 2008, Calgary, Canada.

６．研究組織

(1)研究代表者

藤田　八郎（Fujita Hachiro）
首都大学東京・システムデザイン研究科・助教
研究者番号：30431795

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：