超ロバスト量子計算

今井浩

情報理工学系研究科コンピュータ科学専攻

概 要

本サブプロジェクトでは，量子状態のデコヒーレンスと操作エラーに基づく計算困難性を克服する研究と，デコヒーレンスによりもたらされる状態を活用する研究との両面から，超ロバスト量子計算について研究する．さらに，量子暗号においても，ロバスト性の確立を目指している．本報告では，主に今年度遂行した量子数え上げアルゴリズムにおけるデコヒーレンス解析に関する成果と，量子暗号における量子誤り訂正符号を用いた安全性解析の研究成果について述べる．

1 はじめに

量子コンピュータは，量子力学原理に基づいて動作するコンピュータである．すなわち，量子状態を内部での情報表現として用い，ある量子状態を他の量子状態に変換する量子的操作を計算手段とし，そして量子測定を情報獲得法としたものである．理論的には素因数分解を既存コンピュータより超高速に行えることが示され，現代の RSA 暗号など公開鍵暗号系のセキュリティに強いインパクトを与えているものの，実現はまだ先だと思われている．その一因は，量子状態が脆く，外界と作用して生じるデコヒーレンスエラーや，計算での操作エラーが存在する中で，ロバストで正しい計算ができる方式・解析が行われていないことにある．

本報告では，主に今年度遂行した量子数え上げアルゴリズムにおけるデコヒーレンス解析と，デコヒーレンスの活用に関する成果と，量子暗号における量子誤り訂正符号を用いた安全性解析の研究成果について述べる．

2 量子数え上げアルゴリズムのロバスト性

量子数え上げアルゴリズムは，対象問題の解の個数を数えることを古典アルゴリズムより平方根的に速く行うものであり，2 大量子アルゴリズムである Grover のデータ探索アルゴリズムと Shor の量子フーリエ変換から構成されている．本年度の研究では，この量子アルゴリズムにおいてデコヒーレンスという量子特有のエラーが起ったときに，出力結果が単に丸め的に近似解となるのではなく，数え上げの数という観点では 0 と全体の要素数を解として出力する確率が高くなることを見いだし，その理論的解析に成功した．以下，この量子アルゴリズム特有のエラー耐性についてまず述べる．

まず，Grover のアルゴリズムを概説する．この量子アルゴリズムは，N 個の整列されていないデータの中で「正しい」データが 1 つある場合に，$O(\sqrt{N})$ 回の操作だけで正しいデータを見つける．古典コンピュータ上では明らかに $O(N)$ 回の操作が必要であるので，平方根的なスピードアップとなっている．Grover のデータ探索アルゴリズムは，欲しい解の振幅を増幅していくことで正しい解を得る．振幅を増幅するために，Grover 演算子 G というユニタリ演算子を反復適用する．この Grover 演算子 G は，対象空間を解状態とそうでない状態に 2 分割したとき，それぞれの均等重ね合わせがなす 2 次元のグローバー空間上での回転としても表すことができる．具体的には，データ探索で

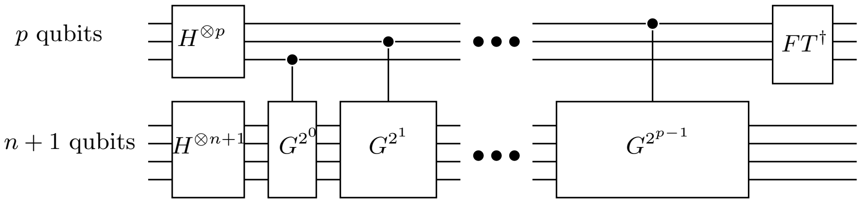

図 1: 量子数え上げ回路 (a)

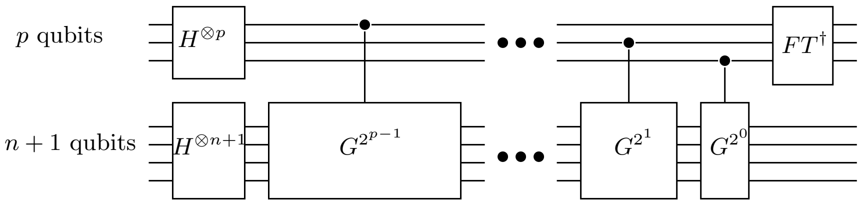

図 2: 量子数え上げ回路 (b)

探す「正しいデータの状態」を $|w\rangle$,「正しくないデータの状態」を $|r\rangle$ としたとき，正規直交基底 $\{|w\rangle, |r\rangle\}$ によって張られる空間をグローバー空間という．グローバー演算子 G はこのグローバー空間上での角度 θ の回転と書くことができる．

量子数え上げアルゴリズムは，対象問題の N 個の要素の中に t 個の解が存在するとしたとき，その解の個数 t を求めるもので，Grover 演算子 G を繰り返し適用し，それで構成される周期が解情報をもつようにしておいて，量子フーリエ変換によってその情報を得るものである．図 1 にその量子回路図を示す．

第 1 レジスタの p 量子ビットは解の個数に関する情報を含む位相 θ を推定するために用いられ，第 2 レジスタの $n+1$ 量子ビットは $N = 2^n$ 個の要素と解に関するオラクル量子ビットを表現するために用いられる．量子数え上げアルゴリズムは，グローバー演算子 G の回転角 θ を位相推定アルゴリズムを用いることで正解に十分近い解を高い確率で求める．

量子計算独特のエラーであるデコヒーレンスエラーのモデルとして，depolarizing channel を考える．このモデルでは，回路の深さが 1 増えるごとに各量子ビットに独立にエラーが発生する．それぞれの量子ビットには確率 d でエラーが発生し，確率 $1-d$ では状態は変化しない．エラーが発生した場合には，エラー演算子 $\sigma_x, \sigma_y, \sigma_z$ がそれぞれ 等確率 $(\frac{1}{3})$ で適用される．したがって，デコヒーレンスエラーの影響は，回路の深さと量子ビット数の積，すなわち回路のサイズに比例することになる．

量子数え上げ回路 (a) と等価な回路として，次の量子回路数え上げ回路 (b) を考える (図 2)．Grover 演算子を多数かけるところは，このように可換になっており，理論的にはこれら 2 つの回路は等価である．しかし，デコヒーレンスが存在するときには次のように全く違った挙動を示す．

量子計算シミュレータシステム上で 10000 回の試行を行った平均を図 3,4,5 に示す．解いている問題は，台集合のサイズが 64 で，解の個数が 13 のものである．図 3 は，デコヒーレンスエラーがないときの得られる近似解の得られる確率を示したもので，図 4 と図 5 は，それぞれ量子回路 (a), (b) に対して $d = 10^{-4}$ のデコ

ヒーレンスエラーがあった際に得られる結果を示したものである．

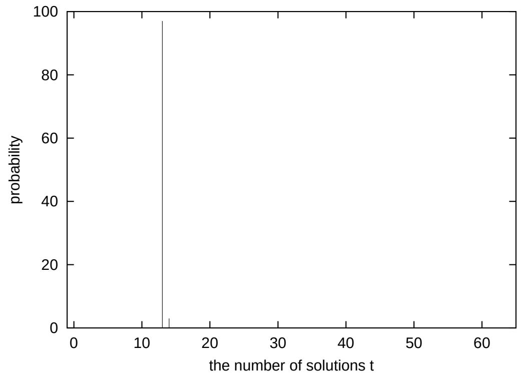

図 3: エラー無しの場合 ($d = 0$)

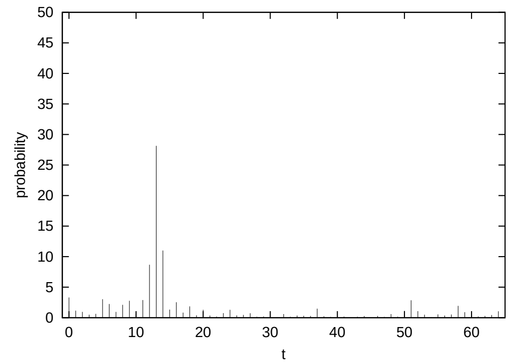

図 4: デコヒーレンスエラー $d = 10^{-4}$ の下の量子回路 (a) での観測確率

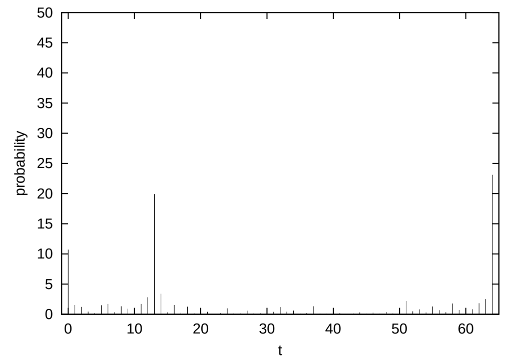

図 5: デコヒーレンスエラー $d = 10^{-4}$ の下の量子回路 (b) での観測確率

このように，エラーがある下ではこの量子数え上げ回路 (a) と (b) は全く違う結果を示す．回路 (a) は正解の 13 の周辺の数を多く出力するが，回路 (b) は解とは全く関係のない 0 と台集合の要素数 $N = 64$ を出力する確率が高い．すなわち，デコヒーレンスに対して，Grover 演算子 G は可換ではないことになる．

これは，Grover 演算子 G のデコヒーレンスに対する振る舞いが直接的に数え上げの解に現れたものである．このことは，Grover 演算子 G の固有ベクトル空間を解析することにより，回路 (b) の場合でデコヒーレンスによって状態ベクトルが 0 と全体要素数の方に触れることを理論的に示すことができる．回路 (a) でも正解 13 の周辺で「なまる」状態を理論的に示すこともできる．

このように，デコヒーレンスエラーがないときには完全に同じ回路であっても，量子計算において避けがたいデコヒーレンスが存在する際には全く違った挙動を示すことがある．これは，量子回路設計において，デコヒーレンスを考慮した設計を行わないといけないことを示しており，単なる量子アルゴリズムの記述だけでは通常のロバスト性を確保できないことを示している．このような量子回路設計理論を構築していくことは，超ロバスト性の確立につながるものである．

3　量子暗号のデコヒーレンスエラーに対するロバスト性

量子暗号は，量子状態そのものを通信することにより，物理原理に基づいた安全性を保持することを目指すものである．今の公開鍵暗号がたとえば素因数分解を解くのが難しいといった計算量仮定にその安全性を依存しているのに対して，物理原理によって安全性が保証される暗号を目指している．その基づく物理原理とは，量子状態は観測すると波束の収斂が起こって状態そのものが変わってしまうことなどである．

量子暗号の原理を簡単に説明する．1 量子ビットは 2 次元複素ベクトル空間の長さ 1 の点に対応する．基底を $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ と $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ で表したとき，一般の状態

$$\phi_\theta = \cos\theta|0\rangle + \sin\theta|1\rangle$$

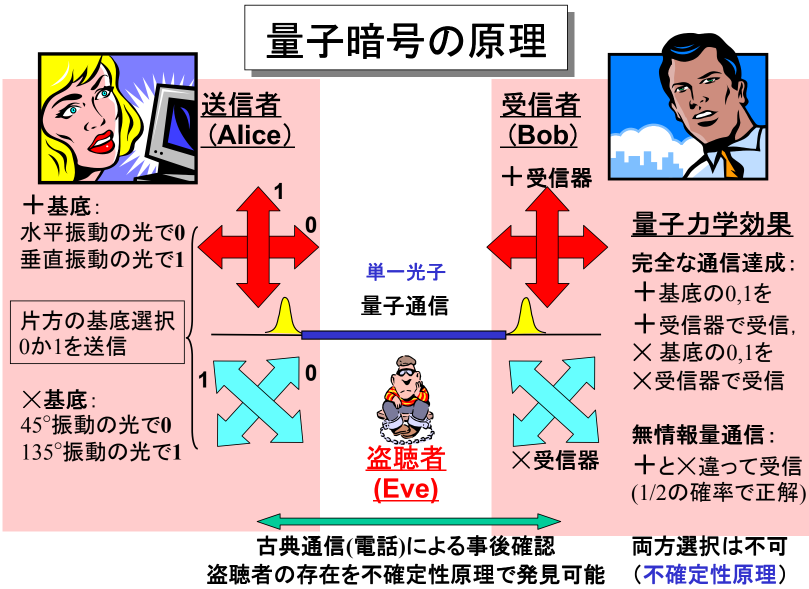

図 6: BB84 という量子暗号系

を単純に正規直交基底で測定をすると，$|0\rangle$ を確率 $\cos^2\theta$ で測定して状態が $0\rangle$ になり，$|1\rangle$ を確率 $\sin^2\theta$ で測定して状態が $1\rangle$ になる．ということは，$\phi_{\pi/4}$ と $\phi_{3\pi/4}$ を測定すると，0 と 1 が確率 1/2 で測定されて元の状態が壊れることになる．すなわち，$\psi_{\pi/4}$ と $\psi_{3\pi/4}$ のどちらであったかは全く区別ができず，かつ，さっきまであった状態も壊して再度観測することもできなくなってしまう．

実はここでの測定は $|0\rangle$, $|1\rangle$ の直交基底で測定で，同様に $0'\rangle = \phi_{\pi/4}$ と $|1'\rangle = \phi_{3\pi/4}$ の直交基底で測定することもできる．その場合には，$|0\rangle, |1\rangle$ をその基底で測定すると，確率 1/2 で $0'$ と $1'$ を測定して元の状態が壊れる．一方，$|0\rangle$, $|1\rangle$ を元の自分自身の基底で測定すると，確率 1 で 0 と 1 の対応するものを測定して，情報のロスは起らない．

このように違う基底で測定すると完全に曖昧な情報しか得られずかつ元の状態は壊れることと，正しい基底で測定するとロスなく情報が得られることを，うまくプロトコルとして設計して，量子通信する 2 人が完全にランダムな秘密鍵を共有するようにすることができる．そして，その 2 者の間で盗聴しようとしても，量子状態を測定すると状態が収束してしまって違った基底で測定すると元を壊すという物理原理から，盗聴があったことを判定することが可能であるようにプロトコルが設計できる．図 6 に，量子暗号の代表的なものである BB84 の説明図を示す．

量子暗号は実験レベルでは実現され，100km を越えて可能であることも示されており，数年内にも実際に使える技術になる可能性がある．ただし，そのような長距離の間で量子状態を伝送において，当然エラーが生じる．このエラーに対するロバスト性を確立することは，量子暗号の実システム化において不可欠である．

量子暗号の安全性は，盗聴者に漏る情報量がいくらでも小さくできることを示すことによって確保される．伝送エラーが存在するときには，伝送エラーと盗聴者による撹乱を区別することはできない．これを逆に発想すると，安全性を理論的に保証するには，盗聴者による撹乱もエラーとして広義のエラーを考え，その存在のもとで正しく情報が送れ，かつ盗聴者にもれる情報量をいくらでも小さくできることを示せばよいことになる．この線での安全性の証明は，Shor, Preskill によって量子誤り訂正符号の理

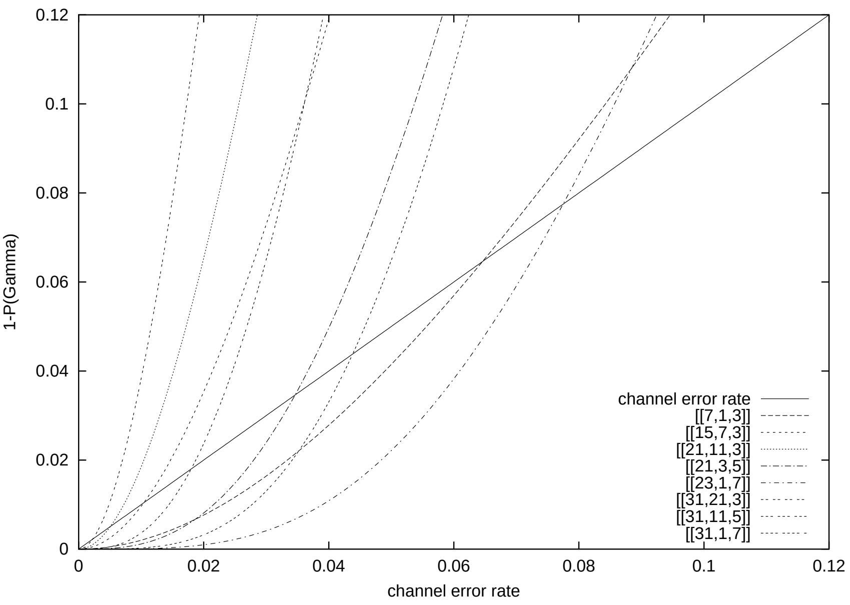

図 7: エラー率 $1-P(\Gamma)$

論を用いて2000年に示された．その証明では，Shannon限界を用いて，エラー率が11%までならBB84の安全性が過去歩できることが示されている．ERATOの実験では，100km伝送でエラー率10%，90km伝送で5%のエラー率で単一光子伝送に成功しているので，その意味で100kmの伝送での安全性は理論的には示されている．ただし問題は，Shannon限界はいわば存在定理であって，そういう理想的な誤り訂正符号はあることは保証するが，今ここにそういう符号があるとはいえないことだ．実際に，これまでのBB84の安全性の研究で，具体的符号で安全性が議論されてはきていなかった．

本年度の研究で，具体的な量子誤り訂正符号として量子BCH符号に着目し，その中でより高い安全性が確保できる符号を解析した．そして，量子Golay符号が色々な観点から望ましい性質をもっていることを示し，実際にその連接符号を4次まで考えることによって7.3-7.7%の量子エラーを許容することができることを示した．

以下，このことを述べる．量子誤り訂正符号に対する理論として，Stabilizer符号の理論，そしてその具体的符号であるCalderbank-Shor-Steane符号(CSS符号と呼ばれる)がある．CSS符号は，古典線形符号でその双対符号の部分集合になっているものから構成される．量子BCH符号は，古典のBCH符号で n を符号長，k を情報長，d を最小距離なる古典符号 $[n, k, d]$ があるとき，$2k-n \geq 1$ ならば符号長 n, 情報長 $2k-n$, 最小距離 d のCSS符号である量子BCH符号が構成でき，量子符号 $[[n, 2k-n, d]]$ と表される．

伝送路にエラー(ノイズ)があるときのBB84プロトコルは，まずノイズがない場合と同じ手順でAliceとBobはのランダムビット列を送受信し，次に古典通信路でその内の用いている量子誤り訂正符号の許す誤り数以下か確認して，一致しないビットが誤り訂正可能ビット数より多い場合はプロトコルを止め，そうでない場合は線形符号の剰余類をうまく使ってさらに秘密の度合いを増大させながらうまく誤り訂正して秘密の共有鍵を構築する．

CSS符号を使う理由は，ノイズのある伝送路でも最終的に両者の鍵の一致させる(Information reconciliation)ことと，剰余類を用いて秘匿性の増強(Privacy amplification)を行うためである．

本年度の研究では，送信者の鍵と盗聴者が盗

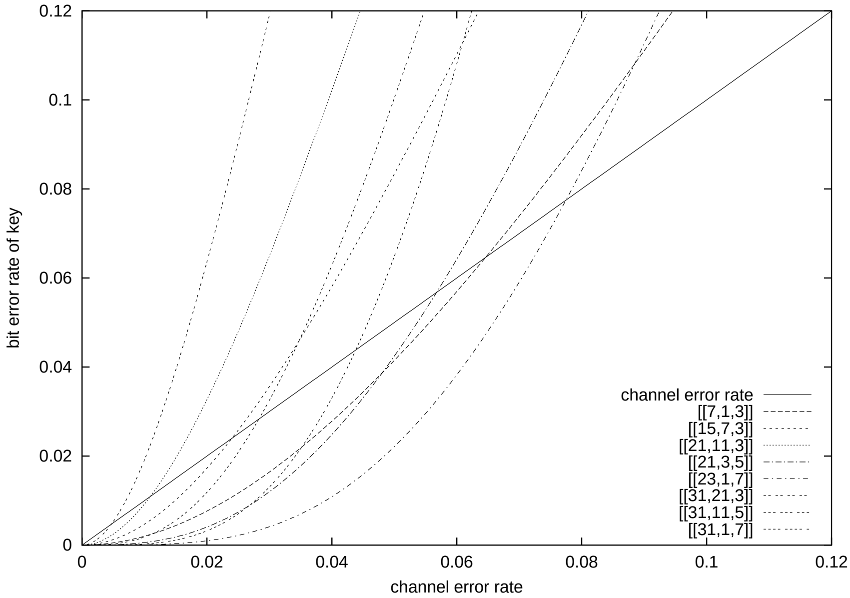

図 8: 理論的なエラー率

んで得る鍵との相互情報量を表す Schumacher による上界をさらに Stabilizer 符号・CSS 符号の理論を使って解析していくことにより，CSS 符号で何を評価すれば安全性を確認する量を導出できるかを明らかにした．ここではその解析を具体的に代表的な量子 BCH 符号に対して計算して解析したグラフを示す．

図 7 は，連接せずに直接量子 BCH 符号を用いた場合を示す．縦軸の $1 - P(\Gamma)$ が横軸の伝送路のエラー率より小さければ効果があることを示しており，[[23,1,7]] の量子 Golay 符号が最もよいことが見てとれる．

次に図 8 に，量子 Golay 符号を連接した場合に安全度がどう高まっていくかというグラフを示す．この [[23,1,7]] の符号が，エラー率 7.7%でも安全性を確保 (伝送路エラー率より低いこと) していることがわかる．

最後に実際にノイズをシミュレートして何度連接すれば安全性が確保できるかをシミュレートしたものを図 9 に示す．これによると，4 次の連接を量子 BCH 符号に対して行うと，7.3%のエラー率まで許容できることがわかる．他の量子 BCH 符号でもさらに調べている．このように具体的符号で十分高いエラー率でも安全性を確保できることを始めて示した．

新たに開始した研究

今年度において，新たに量子通信路容量の計算問題と，Bell 不等式に関する凸多面体解析の研究を開始した．

量子通信路容量計算については，1 量子ビットの通信路で，これまで未知であった 4 量子状態によって初めて容量が達成される場合を発見した．また，その過程で内点法による 1 量子ビット通信路容量計算に対する高精度近似アルゴリズムが構成できることも示し，初めて量子通信路容量を大域的に最適化するアルゴリズムを示せた．ており，量子通信路容量の加法性や量子エンタングルメントの加法性に関するさらなる研究を現在進めている．

Bell 不等式については，組合せ的凸多面体論などでこれまで深く研究されてきたカット凸多面体と Bell 不等式研究とが密接に関係していることを見出し，これまで知られていなかったタイプの Bell 不等式を多数生成することに成功している．これをさらに Bell 凸多面体研究として拡張して取り組んでおり，次年度以降に

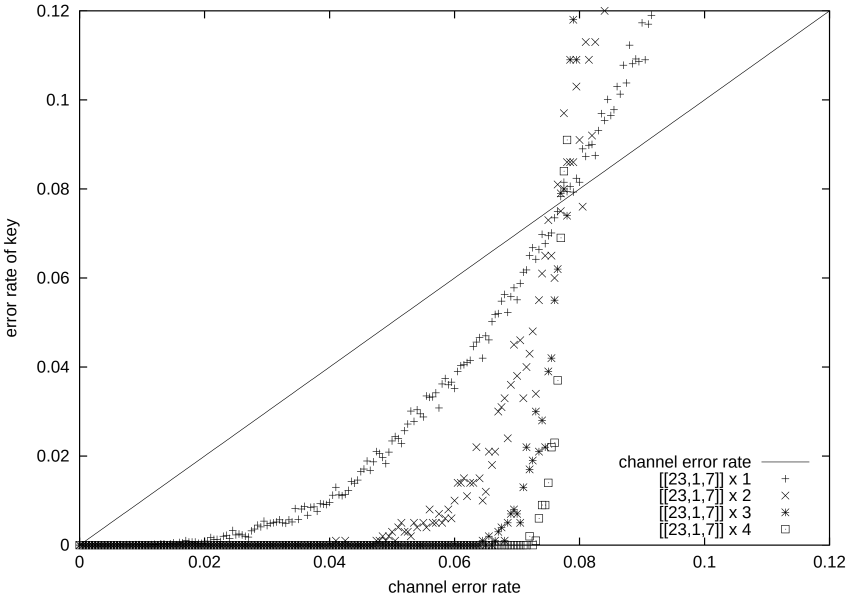

図 9: 量子 BCH 符号を連接したときのエラー率のシミュレーション結果

多くの成果が出ることが期待できる.

参考文献

[1] W.-Y. Hwang, K. Matsumoto, H. Imai, J. Kim, and H.-W. Lee: Shor-Preskill-type Security Proof for Concatenated Bennett-Brassard 1984 Quantum-key-distribution Protocol. *Physical Review A*, 67:024302, 2003.

[2] H. Fan, H. Imai, K. Matsumoto, and X.-B. Wang: Phase-covariant Quantum Cloning of Qudits. *Physical Review A*, 67:022317, 2003.

[3] T. Yamasaki, H. Kobayashi, and H. Imai: Analysis of Absorbing Times of Quantum Walks. *Physical Review A*, 68:012302, 2003.

[4] J. Hasegawa and F. Yura: An Analysis of Quantum Search and Counting Against Errors. In *Proceedings of the 7th Japan-Korea Workshop on Algorithms and Computation*, pages 27–42, July 2003.

[5] T. Yamada, J. Niwa, F. Yura, and H. Imai: An Analysis of Quantum Factorization Algorithm by Simulation — Thorough Simulation and Effects of Approximate Fourier Transform. In *Proceedings of the 7th Japan-Korea Workshop on Algorithms and Computation*, pages 43–60, July 2003.

[6] T. Yamada, J. Niwa, F. Yura and H. Imai: Simulation Analysis of the Robustness of the Order-finding Circuit against Errors. ERATO Conference on Quantum Information Science (EQIS 2004), Poster, September 2003.

[7] J. Hasegawa and F. Yura: Quantum Counting with Decoherence Errors — Influence of Circuits' Order. ERATO Conference on Quantum Information Science (EQIS 2004), Poster, September 2003.