様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１５　日現在

機関番号：　１３９０１
研究種目：　基盤研究(A)（一般）
研究期間：　2011～2015
課題番号：　２３２４６０７１

研究課題名（和文）マルチユーザ型量子ネットワーク

研究課題名（英文）Multi-user quantum network

研究代表者
林　正人（HAYASHI, Masahito）

名古屋大学・多元数理科学研究科・教授

研究者番号：４０３４２８３６

交付決定額（研究期間全体）：（直接経費）　　37,400,000円

研究成果の概要（和文）：本研究では，ユーザが複数存在するネットワークにおける量子通信技術について研究を行った．特に，従来技術が苦手とする情報理論的な秘匿性について，量子通信技術をベースに研究した．情報理論的安全性を実現するには多くの場合、秘匿性増強とよばれる情報処理を符号を用いて行うが，先行研究では，１つの符号の長さの有限性を考慮した安全性評価は不十分であったため，それを明らかにした．さらに，秘匿性を保持した形で計算を依頼する秘匿依頼計算についても情報理論的安全性の枠組みで研究し，測定型量子計算の枠組みで具体的な手法を提案し，その計算結果の正しさを保証する枠組みを与えた．

研究成果の概要（英文）：We have studied quantum communication technology on a multi-user network. Especially, we have studied the information theoretic security based on quantum communication technology because its realization is not easy for existing communication technology. The information theoretic security is usually realized by privacy amplification based on a code. We have clarified the effect by the finiteness of the length of the code while it had not been studied sufficiently. Further, we have investigated the blind computation based on quantum communication, which enables the client to ask the server the difficult computation without informing the server the knowledge of the request, whose security can be guaranteed information theoretically. We have derived the formula for guaranteeing the correctness of the computation result with a given significance level.

研究分野：　量子情報

キーワード：　量子情報　情報理論的安全性　秘匿依頼計算　安全性評価　有限長評価　ハッシュ関数　秘匿性増強

１．研究開始当初の背景
高度情報化社会の実現には，より多機盗能でより安全性の高い暗号技術に基づくネットワークが必要である．しかしながら，従来技術では，安全性， 聴検出などの性能や匿名性について限界があり，それを超える技術として量子通信技術が注目されている．特に，ユーザ数が多い場合，ネットワークの特性を十分考慮しないと，それに比例した通信量や符号化コストが必要となり，それらを削減したプロトコルが望まれる．

２．研究の目的
本研究では，ユーザが複数存在するネットワークにおいて、量子通信技術を用いることで、どのようなことが可能となるか明らかにする．そして，マルチユーザ型量子秘匿通信プロトコルやより高機能な暗号技術の量子プロトコルを提案する．

３．研究の方法
本研究では，上記のように量子通信技術を用いたネットワークの可能性とその限界を明らかにすることを目的とした。このように量子情報技術に重点をおいて研究を行う予定であった。一般に，量子情報技術の研究においては，量子力学的特性を用いない従来の通信形態は、古典力学的描像に従うため，古典通信技術もしくは単純に、古典通信と呼ばれる。量子情報技術の研究の過程では、対応する様々な古典通信技術に関する理論が必要となることが多い。基本的な問題については、対応する古典版の問題は整備されえおり、それらの成果に基づいて量子版の研究を行うことにエネルギーを集中することができる。しかしながら、セキュリティに関しては、一部のテーマについては、量子情報コミュニティの研究の方が進んでいるのが現状である。特に、従来技術でのセキュリティは主に計算量に基づくものでるが、一方、量子通信に基づくセキュリティは情報理論的なものであるため、意外にも古典通信に基づく情報理論的セキュリティは研究の開始時に置いて、十分整備されていなかったものが多かった。そのため、本研究では、古典通信における情報理論的セキュリティの研究から整備することとなった。

４．研究成果

（１）１つ目の主要な成果は、部分的に情報漏洩がある乱数から情報漏洩の無い乱数を生成する技術である秘匿性増強に関する研究である。秘匿性増強には、ハッシュ関数を用いる必要があるが、具体的なハッシュ関数をより少ない計算量で実現する必要がある。また、そのようなハッシュ関数を別の乱数を消費するが、そこで必要となる乱数の数をより少なくすることが求められる。本研究では、秘匿性増強に用いることができるハッシュ関数のクラス分けを行い、新たなハッシュ関数のクラスを提案した[47]。そして、そのハッシュ関数のクラスの中から、従来のハッシュ化数よりもより少ない数の乱数を用いるものを与えた[10]。なお、この研究では、新に導入したハッシュ関数のクラスの下で従来通り、古典通信、量子通信の双方の枠組みで安全性が保証できることも確認した[47,12,38]。量子系でこの事実を確認するために、非可換系での情報量に関する不等式を導出した。さらに、誤り訂正を含めて、秘匿性増強を用いて、安全な一様乱数を生成する問題についても取り組んだ。この問題では、生成される一様乱数の性能がそこで用いられる符号の１ブロックの長さにも依存するので、その符号長の有限性を考慮した解析も行った[38,13,49,9]。

（２）次に、部分的に情報漏洩がありうる設定、すなわち、盗聴通信路モデルで、情報を伝送する方法について考えた。最初に、量子通信路枠内で盗聴通信路モデル分類を行った[57]。ユーザの数が多い場合、基地局間の通信では、多くのユーザの情報を纏めて送ることが普通である。この場合、秘匿性を保証するために、攪乱乱数を用いて秘匿性を保証することが従来の手法であった。この方法には、攪乱乱数の分だけメッセージの伝送速度が遅くなる問題があった。本研究では、別のユーザのメッセージを攪乱乱数として使う方法を提案した（multiplex coding）[55]。これにより、実質的に速度を落とさずに、秘匿性を確保してメッセージを伝送することが可能となる。しかし、攪乱乱数と異なり、別のユーザのメッセージは、一様乱数とはみなせない。そのため、一様でない乱数を攪乱乱数として用いた場合での解析が必要となる。本研究では、攪乱乱数の非一様性も考慮した安全性評価も行った[11]。本研究では、このような問題を、古典通信の枠組みから初めて研究し、量子通信の枠組みでも研究した[20]。

（３）さらに量子鍵配送についても研究した。量子鍵配送は、ほぼ量子盗聴通信路モデルの特殊例とみなせるが、量子盗聴通信路モデルと異なる点は、盗聴者への通信路の推定が必要な点である[7]。特に、最も実用に近いとされる弱コヒーレント光を用いる方法では、部分的に多光子が生成されるため、通信路途中でどの程度の割合が、多光子性を利用した攻撃にさらされうるか、推定する必要がある。この推定のために、弱コヒーレント光の強度を意図的にランダマイズする方法が用いられる。これに統計処理を加えることで、ワーストケースの盗聴者への通信路を推定することが可能となる。量子鍵配送では、秘匿性増強を含めた符号化を行うが、符号の１ブロックごとに、盗聴者への通信路の推定を行う必要がある。そのため、その推定精度は符号

の１ブロックの長さに依存してしまう。近年、１ブロックの長さを考慮した符号の性能評価が注目されているが、本研究においても、この議論は本質となる。本研究では適切に、統計誤差を扱い、上記の弱コヒーレント光を用いた場合について、安全性を与える理論を確立した[36]。

（４）さらに、ユーザ数が多い場合、ネットワークを経由した情報通信を行うのが一般的である。本研究では、ネットワークを経由した、古典通信及び量子通信についても研究した。本研究では、古典通信の枠組みで、ハッシュ関数の理論を用いることで、ネットワーク上の通信路で盗聴されたものの数が一定の範囲であれば、その盗聴箇所がどの通信路であっても、一様に安全性が確保できる符号化を与えた [33]。さらに、その成果を multiplex coding の枠組み拡張子、メッセージが従う分布の非一様性を考慮した安全性解析も行った[6]。さらに、既存の古典通信のネットワーク符号から、量子ネットワーク符号を構成する手法を提案した[62]。これにより、量子通信の枠組みでも、様々なネットワーク符号が使えるようになった。さらに、特殊例である並列型のネットワークは、秘密分散とよばれる問題と一致する。本研究では、量子秘密分散の枠組みで、ランプ型のプロトコルを与えた[43]。

（５）また、ユーザ数が多い場合の量子情報処理の資源となる量子エンタングル状態にも取り組んだ。エンタングル状態を資源として取り扱う場合、局所操作と古典通信のみを許す設定を採用することが多い。この場合に、エンタングル状態の変換理論に取り組み、そのロスの形について研究した[2]。さらに、その変換の際に、エンタングル状態をストレージに一時貯蔵した場合に、変換効率とストレージサイズのトレードオフについても扱った[3]。また、同じ設定の下で、エンタングル状態の識別についても取り組んだ[39,24]。さらに、エンタングル状態の変換の一種であるスワッピングについても扱い、その最適成功確率を明らかにした[30]。

（６）本研究ではより付加価値の高い機能である秘匿依頼計算（ブランド計算）についても研究を行った。秘匿依頼計算は古典系では、計算量的に安全な方法は知られているが、情報理論的に安全な方法は知られていない。秘匿依頼計算の情報理論的安全性は、量子計算によってはじめて実現される機能の１つである。そのために、量子対話式証明について研究し、証明が古典の場合における成功確率を増幅する手法を発見した[60]。そして、テレポーテーション型の測定型量子計算の枠組みでの秘匿依頼計算の方式である測定型量子秘匿依頼計算に注目し，アンシラ系と計算系の間に事前にエンタングル状態を準備し、アンシラ系のみ測定を行うアンシラ駆動型の量子秘匿依頼計算を提案した[51]。また、測定型量子秘匿依頼計算の計算結果の正確さを検証する手法を与え、その最適性についても一定の範囲内で証明した[26]。この成果は、量子秘匿依頼計算の枠組みを超え、量子計算の精度保証においても重要な役割を果たす。また、秘匿依頼計算の特殊例である秘匿情報検索についても量子計算の枠組みで取り組み、従来手法と比較して、通信量を大幅に減らすことに成功した[61]。

５．主な発表論文等

〔雑誌論文〕（計 60 件）すべて査読あり。

[1] M. Hayashi, and V. Y. F. Tan, “Equivocations, Exponents, and Second-Order Coding Rates Under Various Rényi Information Measures,” IEEE Transactions on Information Theory, Volume 63, Issue 2, 975 – 1005 (2017). DOI: 10.1109/TIT.2016.2636154

[2] W. Kumagai, M. Hayashi, “Second-Order Asymptotics of Conversions of Distributions and Entangled States Based on Rayleigh-Normal Probability Distributions,” IEEE Transactions on Information Theory, Volume 63, Issue 3, 1829 - 1857 (2017). DOI: 10.1109/TIT.2016.2645223

[3] W. Kumagai, M. Hayashi, “Random Number Conversion and LOCC Conversion via Restricted Storage,” IEEE Transactions on Information Theory, Volume 63, Issue 4, 2504 - 2532 (2017). DOI: 10.1109/TIT.2017.2657514

[4] R. Matsumoto, D. Ruano, O. Geil, List Decoding Algorithm based on Voting in Grobner Bases for General One-Point AG Codes, Journal of Symbolic Computation, Vol. 79, 384-410 (2017); DOI: 10.1016/j.jsc.2016.02.015

[5] M. Hayashi, Finite-Block-Length Analysis in Classical and Quantum Information Theory, Proceedings of the Japan Academy, Series B, Vol. 93, 99-124 (2017); DOI: 10.2183/pjab.93.007

[6] Ryutaroh Matsumoto, Masahito Hayashi, Universal Secure Multiplex Network Coding with Dependent and Non-Uniform Messages, IEEE Transactions on Information Theory, Volume: 63, Issue:6, 3773 - 3782 (2017). DOI: 10.1109/TIT.2017.2694012

[7] H. Zhu, M. Hayashi, and L. Chen, “Universal steering criteria,” Phys. Rev. Lett. vol. 116, 070403 (2016). DOI: 10.1103/PhysRevLett.116.070403

[8] M. Hayashi, “Optimal decoy intensity for decoy quantum key distribution,” Journal of Physics A: vol. 49, 165301 (2016); DOI: http:

10.1088/1751-8113/49/16/165301
[9] M. Hayashi, S. Watanabe, “Uniform Random Number Generation from Markov Chains: Non-Asymptotic and Asymptotic Analyses,” IEEE Transactions on Information Theory Volume 62, Issue 4, 1795 - 1822 (2016); DOI: 10.1109/TIT.2016.2530084
[10] M. Hayashi, T. Tsurumaru, “More Efficient Privacy Amplification with Less Random Seeds via Dual Universal Hash Function,” IEEE Transactions on Information Theory Volume 62, Issue 4, 2213 - 2232, (2016); DOI: 10.1109/TIT.2016.2526018
[11] M. Hayashi, R. Matsumoto, “Secure Multiplex Coding with Dependent and Non-Uniform Multiple Messages,” IEEE Transactions on Information Theory, Volume 62, Issue 5, 2355 - 2409 (2016); DOI: 10.1109/TIT.2016.2530088
[12] M. Hayashi, “Security analysis of epsilon-almost dual universal2 hash functions: smoothing of min entropy vs. smoothing of Renyi entropy of order 2,” IEEE Transactions on Information Theory, Vol. 62, 3451 - 3476 (2016); DOI: 10.1109/TIT.2016.2535174
[13] M. Hayashi, Himanshu Tyagi, and S. Watanabe, “Secret Key Agreement: General Capacity and Second-Order Asymptotics,” IEEE Transactions on Information Theory, Vol. 62, 3796 - 3810 (2016). DOI: 10.1109/TIT.2016.2567440
[14] M. Hayashi, S. Watanabe, Information Geometry Approach to Parameter Estimation in Markov Chains, Annals of Statistics, Vol. 44, 1495-1535 (2016); doi:10.1214/15-AOS1420
[15] M. Hayashi, “Fourier Analytic Approach to Quantum Estimation of Group Action,” Communications in Mathematical Physics, Volunme 347, 3-82 (2016). doi:10.1007/s00220-016-2738-0
[16] Y. Yang, G. Chiribella, M. Hayashi, “Optimal compression for identically prepared qubit states,” Physical Review Letters, vol. 117, 090502 (2016).DOI:10.1103/PhysRevLett.117.090502
[17] M. Hayashi, M. Tomamichel, “Correlation Detection and an Operational Interpretation of the Rényi Mutual Information,” Journal of Mathematical Physics, vol. 57, 102201 (2016); DOI: 10.1063/1.4964755
[18] Masaya Yasuda, Takeshi Shimoyama, Narishige Abe, Shigefumi Yamada, Takashi Shinzaki, Takeshi Koshiba, Privacy-preserving fuzzy commitment for biometrics via layered error-correcting codes, Lecture Notes in Computer Science, Vol. 9482, 117-133 (2016); DOI: 10.1007/978-3-319-30303-1_8
[19] M. Hayashi, “Precise evaluation of leaked information with secure randomness extraction in the presence of quantum attacker,” Communications in Mathematical Physics, Volume 333, Issue 1, pp 335-350, (2015). DOI: 10.1007/s00220-014-2174-y
[20] M. Hayashi, “Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information,” IEEE Transactions on Information Theory, Volume 61, Issue 10, 5595-5622 (2015). DOI: 10.1109/TIT.2015.2464215
[21] M. Bloch, M. Hayashi, A. Thangaraj, “Error-Control Coding for Physical-Layer Secrecy,” Proceedings of IEEE, Volume 103, Issue 10, pp. 1725-1746 (2015) DOI: 10.1109/JPROC.2015.2463678
[22] T. Morimae, M. Hayashi, H. Nishimura, K. Fujii, “Quantum Merlin-Arthur with Cliford Arthur,” Quantum Information and Computation, Volume 15, 1420-1430 (2015)
[23] M. Hayashi, V. Tan, “Asymmetric Evaluations of Erasure and Undetected Error Probabilities,” IEEE Transactions on Information Theory, Volume 61, Issue 12, 6560 - 6577 (2015). DOI: 10.1109/TIT.2015.2495258
[24] M. Owari, M. Hayashi, “Local Hypothesis Testing Between a Pure Bipartite State and the White Noise State,” IEEE Transactions on Information Theory, Volume 61, Issue 12, 6995 - 7011 (2015). DOI: 10.1109/TIT.2015.2492958
[25] K. Ito, W. Kumagai, M. Hayashi, “Asymptotic compatibility between local operations and classical communication conversion and recovery,” Phys. Rev. A, Vol. 92, 052308 (2015). DOI 10.1103/PhysRevA.92.052308
[26] M. Hayashi, T. Morimae, “Verifiable measurement-only blind quantum computing with stabilizer testing,” Phys. Rev. Lett., vol. 115, 220502 (2015). DOI 10.1103/PhysRevLett.115.220502
[27] Milán Mosonyi, Tomohiro Ogawa, Quantum Hypothesis Testing and the Operational Interpretation of the Quantum Rényi Relative Entropies, Communications in Mathematical Physics, Vol. 334, No. 3, 1617-1648 (2015); DOI: 10.1007/s00220-014-2248-x
[28] Hirotada Kobayashi, François Le Gall and Harumichi Nishimura, Stronger Methods of Making Quantum Interactive Proofs

Perfectly Complete, SIAM Journal on Computing, Vol. 44(2), pp. 243-289, 2015. DOI:10.1137/140971944
[29]Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba, New packing method in somewhat homomorphic encryption and its applications, Security and Communication Networks, Vol. 8, 2194-2213 (2015); DOI 10.1002/sec.1164
[30] T. Ikuto and S. Ishizaka, Entanglement and swap of quantum states Quantum Information and Computation Vo. 15, 0923-0931 (2015).
[31] Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba, Secure statistical analysis using RLWE-based homomorphic encryption, Lecture Notes in Computer Science, vol. 9144, 471-487 (2015); DOI: 10.1007/978-3-319-19962-7_27
[32] R. Matsumoto, Strong Security of the Strongly Multiplicative Ramp Secret Sharing Based on Algebraic Curves, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E98-A, 1576-1578 (2015); DOI: 10.1587/transfun.E98.A.1576
[33] J. Kurihara, R. Matsumoto, and T. Uyematsu, Relative Generalized Rank Weight of Linear Codes and Its Applications to Network Coding, IEEE Transactions on Information Theory, Vol. 61, 3912-3936 (2015); DOI: 10.1109/TIT.2015.2429713
[34] R. Matsumoto, Optimal multiple assignment scheme for strongly secure ramp secret sharing schemes with general access structures, IEICE Communications Express, Vol. 4, 317-320 (2015); DOI: 10.1587/comex.4.317
[35] K Sakakibara, R Matsumoto, Exact computation of tail probability of hypergeometric distribution and its application to Quantum Key Distribution, IEICE Communications Express 3 (2), 68-73 (2014).
[36] M. Hayashi, and R. Nakayama, "Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths," New Journal of Physics, 16 063009 (2014); doi:10.1088/1367-2630/16/6/063009
[37] Marco Tomamichel, Mario Berta, and Masahito Hayashi, "Relating different quantum generalizations of the conditional Rényi entropy," J. Math. Phys. 55, 082206 (2014); DOI: 10.1063/1.4892761
[38] M. Hayashi, "Large deviation analysis for quantum security via smoothing of Renyi entropy of order 2," IEEE Transactions on Information Theory, Volume 60, Issue 10, 6702 - 6732 (2014). DOI: 10.1109/TIT.2014.2337884.
[39] M. Owari, and M. Hayashi, "Asymptotic local hypothesis testing between a pure bipartite state and the completely mixed state", Physical Review A, Volume 90, 032327 (2014). DOI:10.1103/PhysRevA.90.032327
[40] Yuji Sekino and Satoshi Ishizaka, Quantum-information division and an optimal uncorrelated channel, Phys. Rev. A 89, 034304 (2014); DOI:10.1103/PhysRevA.89.034304
[41] Olav Geil, Stefano Martin, Ryutaroh Matsumoto, Diego Ruano, Yuan Luo, Relative Generalized Hamming Weights of One-Point Algebraic Geometric Codes, IEEE Transactions on Information Theory Vol. 60, No. 10 (2014); DOI: 10.1109/TIT.2014.2345375
[42] Shun Watanabe, Ryutaroh Matsumoto, Tomohiko Uyematsu, Optimal axis compensation in quantum key distribution protocols over unital channels, Theoretical Computer Science, vol. 560, 91-106 (2014); DOI:10.1016/j.tcs.2014.09.020
[43] Paul Zhang, Ryutaroh Matsumoto, Quantum strongly secure ramp secret sharing, Quantum Information Processing Vol. 14, No. 2, 715-729 (2014) DOI: 10.1007/s11128-014-0863-2
[44] Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba, Privacy-Preserving Wildcards Pattern Matching Using Symmetric Somewhat Homomorphic Encryption, Lecture Notes in Computer Science book series (LNCS, volume 8544) pp. 338-353 (2014) DOI: 10.1007/978-3-319-08344-5_22
[45] Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, Takeshi Koshiba, On the exact decryption range for Gentry-Halevi's implementation of fully homomorphic encryption, Journal of Mathematical Cryptology, Vol. 8, 305-329 (2014): DOI: 10.1515/jmc-2013-0024
[46] Wataru Kumagai, Masahito Hayashi, "Quantum hypothesis testing for quantum Gaussian states: Quantum analogues of chi-square, t and F tests" Communications in Mathematical Physics, Vol. 318, No. 2, 535-574 (2013).
[47] Toyohiro Tsurumaru, Masahito Hayashi, "Dual Universality of Hash Functions and Its Applications to Quantum Cryptography" IEEE Transactions on Information Theory, Vol. 59, No. 7,

4700-4717, (2013); DOI: 10.1109/TIT.2013.2250576
[48] Masahito Hayashi, “Tight exponential analysis of universally composable privacy amplification and its applications,” IEEE Transactions on Information Theory, Vol. 59, No. 11, 7728-7746 (2013); DOI: 10.1109/TIT.2013.2278971
[49] M. Tomamochel and M. Hayashi, “A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks,” IEEE Transactions on Information Theory, Vol. 59, No. 11, 7693-7710 (2013); DOI: 10.1109/TIT.2013.2276628
[50] W. Kumagai and M. Hayashi, “Entanglement concentration is irreversible,” Physical Review Letters, Vol. 111, No. 13, 130407 (2013); DOI: 10.1103/PhysRevLett.111.130407
[51] Takahiro Sueki, Takeshi Koshiba, and Tomoyuki Morimae, Ancilla-driven universal blind quantum computation, Phys. Rev. A 87, 060301(R) (2013) DOI:10.1103/PhysRevA.87.060301
[52] Ryutaroh Matsumoto, Gilbert-Varshamov-type bound for relative dimension length profile, IEICE Communications Express, Vol. 2, No. 8, 343-346 (2013) DOI:10.1587/comex.2.343
[53] R. Matsumoto, D. Ruano, O. Geil, Generalization of the Lee-O'Sullivan list decoding for one-point AG code, J. Symb. Comput., Vo. 55, 1-9, (2013).
[54] O Geil, R Matsumoto, D Ruano, Feng-Rao decoding of primary codes Finite Fields and their Applications 23, 35-52 (2013).
[55] Daisuke Kobayashi, Hirosuke Yamamoto, Tomohiro Ogawa, Secure Multiplex Coding Attaining Channel Capacity in Wiretap Channels, IEEE Transactions on Information Theory, Vol. 59, No. 12 (2013)
[56] Masahito Hayashi, Toyohiro Tsurumaru “Concise and Tight Security Analysis of the Bennett-Brassard 1984 Protocol with Finite Key Lengths ” New Journal of Physics, Vol. 14, 093014, (2012), DOI:doi:10.1088/1367-2630/14/9/093014
[57] Shun Watanabe, Private and quantum capacities of more capable and less noisy channels, Physical Review A, Vol. 85, 012326 (2012).
[58] J. Kurihara, T Uyematsu, and R. Matsumoto, Secret Sharing Schemes Based on Liner Codes Can Be Precisely Characetrized by the Relative Generalized Hamining Weight, IEICE Transactions on Fundamental of Electronics, Communications and Computer Sciences E95-A 2067-2075 (2012)
[59] Francois Le Gall, Shota Nakagawa, and Harumichi Nishimura, On QMA protocols with two short quantum proofs, Quantum Information and Computation Vol. 12 589-600 (2012)
[60] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumich Nishimura, Achieving perfect completeness in classical-witness quantum Merlin-Authur proof system, Quantum Information and Computation Vol. 12 461-471 (2012)
〔学会発表〕(計２件)(後に上記の雑誌論文として発表されたものなどは省略.)

[61] Takeshi Koshiba, Private information retrieval via blind computation, Australia-Japan Workshop on Multi-user quantum Networks October 22-24 2014, Sydney, Australia.査読なし
[62] Harumichi Nishimura, Quantum network coding - How can network coding be applied to quantum information, presented at 2013 IEEE International Symposium on Network Coding (NetCod2013), Jun. 2013.査読あり

６．研究組織

(1)研究代表者
林　正人 (HAYASHI, Masahito)
名古屋大学・多元数理科学研究科・教授
研究者番号：40342836

(2)研究分担者
小川　朋宏 (OGAWA Tomohiro)
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：00323527

松本　隆太郎 (MATSUMOTO Ryutaroh)
東京工業大学・工学院・准教授
研究者番号：10334517

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

石坂　智 (ISHIZAKA Satoshi)
広島大学・総合科学研究科・教授
研究者番号：10443631

西村　治道 (NISHIMURA Harumichi)
名古屋大学・情報科学研究科・准教授
研究者番号：70433323

渡辺　峻 (WATANABE Shun)
東京農工大学・工学研究科・准教授
研究者番号：70546910