情報理論における量子情報理論の役割 —非可換拡張を超えて—

Role of Quantum Information Theory in Information Theory:
Beyond the non-commutative extension

林 正人 Masahito HAYASHI

アブストラクト 近年の情報理論の発展の背景には、量子情報理論の成果がある。本稿ではそのような情報理論に対する量子情報理論の影響に注目し、これまで情報理論の発展に対して量子情報理論が果たしてきた役割について解説する。これにより、近年の量子情報理論の成果がその分野内に閉じたものでないことを説明する。

キーワード 量子情報理論, Shannon award, 古典情報理論, 情報理論的セキュリティ, 有限長理論, 二次漸近理論

Abstract There are several interesting results in quantum information theory behind the recent remarkable progress in information theory. This article focuses on the contribution of quantum information theory to information theory, and explains the role of quantum information theory in the progress in information theory, which indicates that the results of quantum information theory are applicable to other research areas.

Key words quantum information theory, Shannon award, classical information theory, information-theoretic security, finite block-length theory, second-order asymptotic theory

1. はじめに

2015 年の Shannon award は量子情報理論を草創期からけん引してきた Alexander S. Holevo 先生に贈られた。Holevo 先生の情報理論分野の中での研究業績は、量子情報理論に限られるため、量子情報理論に関する研究活動が情報理論の全体の中でも高く評価されることになった証拠であり、今回の Holevo 先生の受賞について心から祝福したい。また、その前の年の IEEE Information Theory Society Paper Award は、Marco Dalai 先生の論文 “Lower Bounds on the Probability of Error for Classical and Classical-Quantum Channels” に贈られた。この論文は、量子情報理論と古典情報理論（非量子系の情報理論）にまたがる結果である。（本原稿では、通常非量子系を扱う情報理論のことを、量子情報理論と区別するために、このように呼ぶこととする。）このように量子情報理論の研究が情報理論の中で高く評価されることになった背景について本原稿では考えてみたい。

最近の古典情報理論の発展の背景には、しばしば量子情報理論の成果が登場する。この事実は現時点では多くの情報理論研究者には認識されていないが、今後の情報理論の発展を見極める上で大変重要なポイントである。一見すると、古典情報理論

が本家で、量子情報理論が分家のようなものだから、量子情報理論が一方的に古典情報理論の成果を輸入するだけのように思える。確かに、分野のれい明期にはそのような側面があったが、現在では、双方向の交流が活発に行われている。特に、情報理論の幾つかの分野では、その分野の鍵となる概念が、量子情報理論において初めて導入され、その考え方が一定の形になった後に、古典情報理論に導入されている。これは、量子情報理論が単なる古典情報理論の非可換拡張を超えた意味を持つことの証拠でもある。多くの古典情報理論の研究者にとっては、量子情報理論は自分には関係のない研究分野と感じているかもしれない。このような分野では、量子情報理論の成果へアクセスできることが大きなアドバンテージとなる。したがって、量子情報理論の成果へアクセスできない研究者は大きなハンディを負うことになる。そのため、現在では古典情報理論の発展には、量子情報理論の成果は欠くことのできない部分となっている。なお、ここで注意しておくべきこととして、量子情報理論が古典情報理論を数学的にその特殊例として含んでいる点である。この点は、量子計算の結果が可換な場合の制限として古典計算の結果を含んでいるわけでない点とは対照的である。そのため、量子情報理論の新規の成果が可換な特殊例に限っても新しい場合、自動的に古典情報理論の成果となることを示している。この点が極めて大きい利点であり、後の予期せぬ理論的発展の原動力となる。

今回、Holevo 先生が Shannon award を受賞した背景には、このように量子情報理論が古典情報理論に大きく貢献していることがある。このような古典情報理論への大きな貢献の源流をたどると Holevo 先生の業績にたどりついたため、今回の受賞

図 1 古典情報理論と量子情報理論の関係

になったと推測できる。本原稿では、量子情報理論の草創期からの発展について触れた後に、近年の古典情報理論への影響について触れる。当初、情報理論の成果を吸収する立場であった量子情報理論が、情報理論の発展に積極的に貢献できる分野へといかに変貌を遂げたかについて、筆者が身近に研究してきた量子情報理論の研究内容を中心に説明したい(図 1)。したがって、以下の内容は筆者の視点からのものであり、やや偏った量子情報理論と古典情報理論の関係に関する紹介となっているので、このような見方もあり得ると思って読んで頂けたら幸いである。

以下では、量子情報理論の中でも古典情報理論と接点の大きいセキュリティ解析、仮説検定との関係、二次漸近論について、量子情報理論の枠組みでレビューし、その後、古典情報理論における情報理論的セキュリティ解析、二次漸近理論、有限長理論、情報源符号化やその関連分野において、量子情報理論がどのような役割を果たしたのか解説する。

2. れい明期

量子情報理論の研究が始まったのは、1960 年代の Helstrom 先生の幾つかの論文⁽¹⁾⁽²⁾に遡る。その後、1970 年代には、復号過程と受信過程を統一的に POVM で扱う定式化がなされ^{(3)(註1)}、通信路符号化定理の逆定理に対応する命題が Holevo 先生により示された⁽⁴⁾⁽⁵⁾。また、統計学の量子化ともみなせる方向性の研究もこの時期に重点的になされ、Cramér-Rao 不等式の量子拡張も複数考えられた⁽²⁾⁽⁶⁾⁽⁷⁾。筆者は、直接この時期の研究に携わっていないが、これらの 1970 年代後半までの量子情報理論の草創期の成果は 1980 年に出版された(英訳版は 1982 年) Holevo 先生によるテキスト⁽⁸⁾にまとめられているので、このテキストの参考文献をたどることで当時どのような研究がなされたか理解することができる。

しかし、その後、本格的な量子情報理論の進展はしばらく停滞し、1990 年代になり、Schumacher 先生らを中心として、典型系列の量子拡張や、情報源符号化定理の量子拡張がなされた⁽⁹⁾。筆者が量子情報理論の世界に初めて足を踏み入れたのは、筆者が大学院の修士課程 1 年目であった 1994 年の 10 月頃であった。そのとき、阪大に赴任したばかりの藤原彰夫先生の勧めで上述の Holevo 先生のテキスト⁽⁸⁾を読むことから始めた。そして、大学院時代の筆者の情報源の大半はこのテキストに引用されている論文と電通大の長岡先生の論文であった。今から思えば、そのテキストに引用されている論文の中で Holevo 先生の論文が最も自分にはじっくり来る記述であった。当時、これらの研究論文

を通じて、非可換性が情報獲得過程である測定過程の選択にいかに関与するか理解でき、伝統的な物理学科で学ぶ量子論のテキストにはない量子論に対する新鮮な(今となっては古臭いが)視点に興奮しながら勉強した記憶がある。物理学科で学ぶ標準的な量子論のテキストでは、そこまで明確に非可換性が測定に及ぼす影響を議論していなかった。当時の物理学科では、測定に関わる問題は全ていわゆる哲学的な観測問題と同一視され、そのような問題は老後に行うものであり、若い人がやる研究ではないと強く言われていた。当時、筆者は Holevo 先生のテキストを読んで、哲学的な傾向を排除して、数学的な問題として測定に関する問題が取り扱えることに大変な驚きを感じ、(周囲に理解されないながらも)このような問題に取り組むことに自信を覚えた。少なくとも、当時の物理学科で議論されている標準的な量子論の議論には存在しない数学的な形式がこのテキストには存在した。どうやら筆者がこの研究テーマを選ぶことができたのは、数学科の大学院に進学したことが大きかったのかもしれない。ちなみに、Holevo 先生は論文を見る限り、初期の論文から一貫して所属は、ロシアの Steklov 研究所であり、これは数学の研究所である。なお、当時、筆者は様々な数学の分野の本を読んで、自分が取り組むべき研究分野を探索したがそのほとんどの問題設定に共感できなかった。Holevo 先生のテキストや論文にある問題設定にだけは共感できた記憶がある。

ところで、この当時、世界の量子情報の研究は分断されており、現在のような研究者間のネットワークは十分に機能していなかった。すなわち、1960 年代の Helstrom 先生に始まる研究の流れは、Holevo 先生のテキストにまとめられているものの、その流れと、1990 年代初頭に始まった Schumacher 先生らを中心とした流れの間には、十分な交流がなかったように思える。そのため、Holevo 先生のテキストから研究をスタートした筆者は、研究開始の当初段階では、上述の Schumacher 先生らの研究については認識していなかった。そのような中、筆者が修士課程 2 年となる 1995 年の夏に、Holevo 先生は日露確率論シンポジウム⁽¹⁰⁾のために来日し、彼が京都大学の数理解析研究所の小嶋先生を訪問したときに、幸運にも Holevo 先生にお会いすることができた。このとき、筆者はこんなにも早く勉強したテキストの著者に会えるとは思ってもいなかったため大変感激した。そのとき、筆者は Holevo 先生に自分の修士論文のアイデアを聞いて頂いた。なお、日露確率論シンポジウムはソ連の崩壊までは日ソ確率論シンポジウムの名称で 6 回開催され、1995 年のものはそれを引き継いだものであった。残念ながら日露確率論シンポジウムは 1995 年の 1 回しか開催されなかった。文献を見る限り Holevo 先生は京都で 1972 年に開催された第 2 回⁽¹¹⁾、タシュケントで 1975 年に開催された第 3 回⁽⁶⁾、トリビシで 1982 年に開催された第 4 回⁽¹²⁾に出席し、量子情報理論に関する研究成果を発表している。しかし、Proceeding の目次を見る限り、関連する発表は存在せず、Holevo 先生の孤軍奮闘振りを察することができる。

その後、1996 年には、箱根で Quantum Communication, Computing, and Measurement と呼ばれる会議が開催され⁽¹³⁾、この会議に出席するため再度 Holevo 先生が来日した。この会議

(注 1): 量子系での測定では、測定対象となる系の初期状態と測定器の双方に応じて、出力となる測定値が従う確率分布が決まる。POVM とは、その確率分布の測定器に対する依存性を表す数学的概念である。具体的には所定の条件を満たす各測定値に対応した半正定値行列(作用素)の組で与えられる。

で Holevo 先生は Schumacher らの研究を知ることになり、この段階で初めて、二つの流れの交流が盛んになり、Holevo 先生はこの会議の直後、滞在中の玉川大学で、あっという間に量子版の通信路符号化定理の順定理を証明したそうである。直後に、Holevo 先生は arXiv に、その成果を投稿した⁽¹⁴⁾。しかし、その査読には2年もの歳月を要し、IEEE Transactions on Information Theory に掲載されたのは1998年であった⁽¹⁵⁾。筆者はこの論文のおかげで arXiv の存在を知ることができた。なお、査読の間に、この順定理は Schumacher 先生、Westmoreland 先生⁽¹⁶⁾によっても独立に証明された。しかしながら、この時点までは量子情報理論は古典情報理論の主要な成果を量子系で再現することが精一杯の状況であり、量子情報理論が古典情報理論に貢献することは全く期待できる状況ではなかった。

3. 量子情報理論における情報とは

以下では最後の章を除き学術的な内容について扱うので、敬称は省略する。上記の発展の後、量子情報理論は、古典情報理論の成果を吸収しつつ、更に、隣接分野の成果も吸収することで、大きな発展を遂げることができた。量子情報理論が古典情報理論と大きく異なる点は、取り扱う情報の種類が一つではないことである。少なくとも扱う情報としては、量子情報と古典情報の二つに分けることができる。古典情報とは、我々が日常的に接している文字列、ビット列などの情報であり、古典情報理論はこの種類の情報の伝送を問題にする。一方、ここでの量子情報について説明するには若干の準備が必要である。量子系では、系の様子は状態若しくは量子状態で記述される。その際、互いに識別可能な状態だけでなく、複数の状態がいわば重なり合った状態が存在する。ここでいう重なり合った状態は、複数の状態が確率的に重なった確率混合とは異なる。特に、そのように、確率混合と異なる重なり合わせは、量子系特有のものであり、コヒーレンスと呼ばれる。一般に、熱雑音などの周辺の系の影響により、コヒーレンスは破壊され、単なる確率混合に変化してしまうことが多い。そのため、量子系の操作においては、このコヒーレンスの保持が一つの大きな問題となり、様々な関心を集めてきた。

なお、人間が直接、認識できるものは古典情報だけに限られるので、量子情報の通信は、情報理論的に重要でないように思われるが、そうではない。量子情報処理の分野では、量子計算や量子暗号のように、コヒーレンスを保持した量子状態を入力として必要とする装置をベースにした情報処理が存在する。そのような装置の間での通信では、コヒーレンスの保持が不可欠な要素となり、量子状態の通信が必要となる(図2)。実は、こ

のコヒーレンスのおかげで、量子情報理論は、古典情報理論では持ち得なかった他分野との接点を持つことができ、その大きな進展につながった。

4. 量子情報におけるセキュリティ解析

このような事情から、量子情報理論では、自然にコヒーレンスの保持をも要請する量子情報の伝送を目的とする通信路符号化を扱うようになった。実は、上述の Holevo らによる量子系での通信路符号化定理は、量子素子を用いて古典情報を伝送する問題に関するものであり、別途、量子情報を伝送する問題に関する通信路符号化定理が必要となる。一般に、量子状態の伝送の精度を議論する際、基本となる計算基底を固定して議論することが多い。すると、その精度は、計算基底に関する情報のエラーと計算基底に関する重ね合わせの度合い、すなわちコヒーレンスの保持の二つに分けて議論することができる。前者は古典情報の伝送に関するエラーの解析に帰着できる。後者の評価については二つの手法が知られている。一つは、計算基底と相補的な基底(しばしば双対基底または位相基底と呼ばれる)でのエラーの解析に帰着する方法である⁽¹⁷⁾⁽¹⁸⁾。実は、量子系ではモノガミー(単婚性)と呼ばれる性質が知られており、二つの系が完全にもつれ合っている(エンタングルしている)とき、他の系との相関が全くないことが保証できることが知られている^{(19)~(22)}。もう一つは、このモノガミーの性質を用いて、受信者が持つ系を基準にした場合での環境系を考え、その環境系への漏えい情報量の解析に帰着させる方法である。更に、量子情報理論では、受信者への通信路の形から、環境系への情報漏えいの形が完全に決定できることが知られている。そのため、環境系への情報漏えいを盗聴者への情報漏えいとして捉えた形での盗聴通信路の解析を通じて、量子状態の伝送のための通信路符号化定理を導出することが可能となる⁽²⁴⁾。そのため、量子系では古典系にない形で、盗聴通信路の解析が強く要請されていた。この要請のため量子情報理論の文脈から早い段階で、通信路 resolvability と盗聴通信路のセキュリティ解析の関係が注目されることとなった^{(24)~(26)}。

また、研究費獲得の形態から、量子情報理論は量子情報処理の一分野としての側面が、情報理論の一部としての側面よりも、強く意識されることが多かった。特に、量子暗号は情報理論的安全性をうたっている関係から、量子情報理論からの量子暗号へのアプローチが一つの課題であった。一方で、2000年代の後半からチューリッヒの Renner のグループを中心として、暗号理論から量子暗号へのアプローチが精力的になされた^{(27)~(32)}。暗号理論では、left over hashing lemma⁽³³⁾⁽³⁴⁾、最小エントロピー、smooth 最小エントロピー⁽³⁵⁾などの概念が提唱されていたが、このアプローチにより、これらの概念を量子情報理論にも、量子拡張を経た上で持ち込まれた⁽²⁷⁾。そのため、2010年代に入ってから、これらの概念を用いた研究が盛んに行われた。一方、古典系の left over hashing lemma が当初最初に掲載された論文の一つは IEEE Transactions on Information Theory

$$01001010 \quad \alpha|001001100\rangle + \beta|10100101\rangle$$

古典的な情報
量子的な情報

図2 古典な情報と量子的な情報 量子情報では、複数の情報の重ね合わせまで伝送する。

図3 ハッシュ関数, left over hashing lemma, 最小エントロピー, smooth 最小エントロピーなどの浸透の経路

に掲載された論文⁽³³⁾であり^(注2), 古典情報理論の人にも分かる記述でありながら, 古典情報理論のコミュニティには, この成果は当初は十分に浸透しなかった (図3)。

このような事情から, 量子情報理論の一つのテーマとして, 量子暗号での安全性評価が一つのテーマとなった。特に, 量子情報処理の分野では, 2000 年代初頭の時期に実験系を中心として夢物語を語ってばかり大な予算を獲得した関係から, 可能な限り早い時期に, 現実に動作する何らかの成果物を出すことが強く求められていた。残念ながら現在の技術レベルでは量子計算ではそのような成果物は期待できないため, 量子暗号にその期待が集まることは自然な成り行きであった。そのため, 筆者をはじめとする量子情報理論の一部の研究者の間では現実に実行可能な鍵蒸留プロトコルと最終鍵の評価式の導出が重要なテーマとなった。したがって, 鍵蒸留プロトコルの存在定理では十分ではなく, プロトコルの実行のために必要な計算時間及び計算スペースを考慮に入れた議論が必要となる。幸いにして, 鍵蒸留プロトコルは, 誤り訂正と秘匿性増強の二つのプロトコルを組み合わせることで実行可能であり, 特に, 誤り訂正については, 既に実行可能なプロトコルが実装されているので, 必要な部分は, 後半の秘匿性増強となる。秘匿性増強は, left over hashing lemma などにより, 元々は認証のために暗号理論で導入された universal2 hash 関数^{(36) (37)}やその変形版である双対 universal2 hash 関数^{(38)(注3)}を用いることで実現できる。そのため, これらのハッシュ関数を実装するための計算コストが重要となるが, Toeplitz 行列を用いることで, 少ない計算量で実現できる⁽⁴⁰⁾。安全性評価においては, シヤノン理論的な漸近評価ではなく現実には有限サイズでの安全性評価式が求められる。しかも, 安全性評価であるため, 近似式では十分とは認められず, 厳密に成り立つ漏えい情報量の上限式が必要となる。そのため, 量子情報理論では, 早い段階から有限長での評価式の重要性が指摘され^{(28) (41)}, 有限長の量子暗号の安全性評価が研究されてきた^{(17) (18) (42) (43)}。更に, 量子暗号装置の実現のため, 早い段階から理論サイドが実験の事情を考慮して研究してきた点も注目に値する。

5. 仮説検定をベースにした情報理論の再定式化

情報源や通信路に独立同一性や定常無記憶性などの性質を要請せずに扱う情報理論の枠組みとして, 韓・Verdú によって定式化された情報スペクトルが知られている。量子情報理論では, 日

(注2): 文献(34)は当初暗号系の国際会議で発表されたこともあり, 論文誌への掲載はかなり遅れた。

(注3): 古典情報理論の用語による双対 universal2 hash 関数の解説は文献(39)にある。

図4 量子情報理論への展開では非可換化のフィルタにより, より本質的なアイデアに蒸留される。

本の研究者を中心として, いち早く, 情報スペクトルとの関連に注目していた。量子系の場合, たとえ情報源や通信路が独立同一性や定常無記憶性などの性質を満たしていても, 測定過程において, 複数の系にまたがる操作を行うと, 測定によって得られるデータ列に注目すると, 一般には, 独立同一性や定常無記憶性などの性質は成り立たない。そのため, そのようなデータ列に対して議論を適用するには情報スペクトルの考え方が有効となる⁽⁴⁴⁾。

また, 量子情報理論における議論が, そこに現れる非可換性のため数学的に難解であることももう一つの要因である。古典情報理論の枠組みで, 情報源符号化定理や通信路符号化定理を証明することは極めて容易であり, さほど, その問題の数学的構造を深く考えることは求められない。しかし, 量子系で同じ問題を考えることになると, とたんにその問題の数学的難易度が上がってしまう。そもそも量子系は測ったら壊れてしまうものであるので, 容易に可視化した描像を得ることができない。問題や定理の主張そのものの量子化を考えることは比較的容易であるが, 多くのよく知られている証明の手法は, そのステップに量子拡張が不可能であるものが含まれている。そのため, 何が鍵となるか, 注意深く考え, より見通しの良いアプローチは何か考えないといけない。一見すると, 量子拡張を考えることは, これまでにない苦労を無駄に背負い込んでいるだけのようにも見えるが, そのような苦労ばかりではない。量子拡張を考えることで, 量子拡張が不可能なアイデアは全て淘汰され, 本当に本質を突いたアイデアだけが残る利点がある (図4)。このような視点は, 長岡により提唱され, 当時の日本の量子情報理論研究者の共通した認識であった。実は量子情報スペクトルは, そのようなハードルを乗り越えたアイデアの一つである。この量子情報スペクトルから, 後になって Princeton 大学の古典情報理論のグループから再発見された二つのアイデアが提案された。双方とも, 通信路符号化定理と単純仮説検定に関するアイデアであり, 近年では, 単純仮説検定は情報理論の基礎を与えると多くの研究者が考えるようになった。一つは, 後に dependence test bound と呼ばれる通信路符号化定理におけるランダム符号化法を用いた場合での復号誤り確率の仮説検定を用いた上限である^(45, Remark14)。もう一つは, 後に meta converse bound と呼ばれる通信路符号化定理における復号誤り確率の仮説検定を用いた下限である⁽⁴⁶⁾。また, 情報源符号化や盗聴通信路について, 洗練された形で仮説検定との関連が定式化された^{(25) (26, Chapter9)}。なお, 古典の情報スペクトルの時点でも, このような仮説検定との関連は

指摘されていたが⁽⁴⁷⁾、量子情報理論を経ることで、この関連がより明確に定式化された。

6. 二次漸近論との関係

近年、二次の漸近理論は従来の情報理論の成果を精緻化する理論として注目を浴びている。二次の漸近理論は Strassen により 1960 年代の研究の優れた研究があるが、その後この方向性の研究は忘れられていた。二次の漸近理論が注目を浴び、今日のように重点的に研究されるようになる経緯において、量子情報理論は大きな役割を果たしている。二次の漸近論の基本的な部分は、上述の情報スペクトルにおいて、大数の法則が用いられる箇所を中心極限定理に置き換えることで得られる (図 5)。この事実は、一様乱数生成と固定長情報源符号化の場合に最初に指摘され⁽⁴⁸⁾、付加情報がある場合での固定長情報源符号化にも適用されている⁽⁴⁹⁾。このような基本的なアイデアの導出の背景には、量子情報理論を経由した情報スペクトルの定式化の洗練が挙げられる^{(45) (50)}。このアイデアは大変有効でこのアイデアに基づく様々な問題設定において、自然にマルコフ過程の場合へ拡張が可能となる^{(51)–(53)}。

更に、量子暗号との関連も見逃せない。上述のように、量子暗号では有限サイズの符号及びハッシュ関数を用いた場合での安全性評価が必要となる。先に述べたように量子暗号では有限サイズでのセキュリティ評価が重要なポイントとなる。特に、量子暗号では、秘匿性増強の際に用いる線形なハッシュ関数と双対な関係にある線形な誤り訂正符号に注目することが多い。なぜなら、その線形な誤り訂正符号を用いて位相誤りを訂正した場合での位相誤り確率を用いて、セキュリティ評価が可能となるからである^{(17) (18)}。したがってセキュリティ評価のため、有限サイズでの上述の位相誤り確率の評価が必要となる。この問題を解決するために、線形な誤り訂正符号に限ってランダム符号化を行った場合での二次の漸近理論が始めに議論された⁽¹⁷⁾。このように、量子情報理論における需要から二次の漸近論の研究がなされている。その後、2008 年から 2009 年にかけて、その議論をより深める方向から、筆者による通信路符号化に関する二次の漸近論が、情報スペクトルを用いることで、古典情報理論の枠組みでなされた⁽⁵⁴⁾。

図 5 情報スペクトルのアイデア

7. 古典情報理論との関係

以下、上述のテーマ及び関連テーマについて、古典情報理論との関係を議論する。

7.1 情報理論的セキュリティ解析

古典情報理論において、量子暗号に対応する概念は情報理論的セキュリティを実現すると考えられている物理層セキュリティであろう。この分野は、Wyner⁽⁵⁵⁾によって、盗聴通信路モデルとして定式化され、その後、Csiszár-Körner⁽⁵⁶⁾によって深められた。また、Ahlsvede, Csiszár⁽⁵⁷⁾, Maurer⁽⁵⁸⁾による秘密鍵蒸留も見逃せない。その後、先に述べたように、Bennett ら⁽³³⁾による left over hashing lemma に関する論文が、IEEE Transactions on Information Theory に掲載されているが、この研究は、やや、情報理論の研究の流れから離れたところになされた感じがする。いずれにせよ、その後、情報理論でのこの方向の研究は、多端子への拡張に重点が置かれ、現実の物理層への応用を意識した研究は少なかった。一つには、古典情報理論分野の研究が、それだけで独立してなされることが多く、無理をして(身の丈を超えた)多額の研究費を獲得する必要がなかったため、従来の興味のある方向性を維持することができた点がある。そのため物理層セキュリティの実装を意識した研究が遅れてしまったように見える。例えば、無線通信をベースにした物理層セキュリティの研究は通信サイドからも研究されつつあるが^{(59)–(62)}、これらと古典情報理論サイドが連携した研究はなされていない。国際的な量子暗号の研究集会には、量子暗号の理論家と実験家に参加することが多い⁽⁶³⁾。しかし、筆者はこの1年間に2件の情報理論的暗号に関する国際的な研究集会に参加したが⁽⁶⁴⁾、符号理論を含めた理論家だけの研究集会であり、物理層セキュリティを意識した通信システムの専門家の参加は見られなかった。

また、セキュリティシステムへの実用を意識すると、漏えい情報量の評価基準が重要となり、相互情報量などの量を正規化せずに、その基準量が0に収束することを要請するのが自然になる。このような安全性基準は strong security と呼ばれ、暗号理論では重視されてきたが、古典情報理論は、この考え方の普及について量子情報理論と比較しても遅れを取ってしまった。盗聴通信路における strong security は、Csiszár⁽⁶⁵⁾によって最初に示されたが、現在知られている指数的な減少率の中で最も強いものは、量子盗聴通信路の研究⁽⁶⁵⁾を受けてなされた研究である⁽⁶⁶⁾。また、Han-Verdú によって情報スペクトルの創成期に議論された通信路 resolvability⁽⁶⁷⁾と盗聴通信路の関係が知られているが、この関係はこの研究によって初めて明示的に指摘された。現在では、盗聴通信路の研究において通信路 resolvability の考え方は欠くことのできない要素となっており、その起源の一部が量子情報理論にあることは興味深い。また、プロトコルの計算量や符号・ハッシュ関数のサイズの有限性を考慮した研究は、先に述べたように、量子情報理論で先行的に研究され、それを輪

入する形で、古典情報理論に数々の実用的な成果をもたらされた^{(39) (40) (68) (69)}。更に、最近、筆者は、このようなギャップを埋めるべく、現実の無線通信をモデル化し、そのモデルの下で盗聴者が最適な戦略を行っても、盗聴者に情報漏えいが定量的に評価できる秘密鍵を生成するプロトコルを提案した⁽⁷⁰⁾。

7.2 二次漸近理論と有限長理論

二次漸近論は、1960年代の Strassen⁽⁷¹⁾の研究の後、停滞が見られた。2000年代の後半に LDPC 符号⁽⁷²⁾の研究が盛んに行われるようになって、以下の経緯から二次漸近論が注目を集めるようになった。LDPC 符号はある種の制約を課すと、漸近的に通信路容量を達成することが知られている。しかし、幾らサイズの大きな LDPC 符号を作成しても、その伝送レートは、通信路容量と完全に一致することはなかった。そのため現実の達成可能な伝送レートはどこにあるのかという疑問が浮上した。2008年から、この問題を近似的に解決するために、Verdúを中心とした Princeton 大学のグループは、様々なアイデアを開発した。一つは通信路符号化と単純仮説検定を結び付ける上述の dependence test bound⁽⁷³⁾と meta converse⁽⁷³⁾であり、もう一つは、その極限として自然に得られる二次漸近論であった⁽⁷³⁾。しかし、前者の二つのアイデアは、上述の量子情報理論で既に提案されたアイデアと同一の内容である。また後者の基礎的な部分は、Strassen によって既になされた成果の再発見であり、ガウス通信路に関するものは、Strassen によってはなされていないが、先に述べた量子情報理論の影響を受けて筆者が先に行っている^(注4)。また、二次漸近理論と情報スペクトルとの親和性は現在の二次漸近論の研究では基礎となる部分であるが、研究の当初段階においては Princeton 大学のグループはこの点を余り強調していなかった。このように、Princeton 大学のグループによる基礎的な貢献と考えられがちな部分の多くは、量子情報理論の中で先に生まれてきた。そのうち、前者の2件は、非可換性の克服の中で極めて思弁的な経緯を経て得られたものであり、後者は現実の量子暗号システムの評価という極めて実利的な要請を経て得られたものである。このように、二次漸近論及び有限長理論に限っても、量子情報理論は全く二つの側面から古典情報理論に大きな影響を与えている。

7.3 情報源符号化との関係

古典情報理論で採用される情報源符号化の定式化は、復号誤り確率を復号基準に用いるものが標準的であるが、これ以外に rate distortion を用いるものがある。しかし、情報源で与えられる情報と復号時に評価の対象となる情報が異なり、各入力に応じて与えられた確率分布のみを復号時には、再現すればよいという設定は余り存在しない。しかし、量子系ではこのような

問題は、情報源符号化の一般化として自然に考えることができる⁽⁷⁵⁾。すなわち、このような方向性は量子情報理論では盛んに研究されているにもかかわらず、古典情報理論では欠けていた視点である。

この問題では、メモリには雑音が無いことを仮定しているので、メモリは雑音のない通信路と見なすことができる。一方、要請されている問題では、個々の入力に対して分布を与えるので、少ないサイズの雑音のない通信路を用いて、ある特定の雑音のある通信路を実現することが求められているとみなすこともできる。このように捉えると、通信路符号化定理の逆の操作を考えているとみなすことができる。このような問題の捉え方をした場合、量子情報理論ではこの問題は Reverse Shannon Theorem と呼ばれる。Reverse Shannon Theorem は Bennett ら⁽⁷⁶⁾によって、量子情報理論におけるエンタングル補助型の通信路符号化定理の逆定理を証明する過程で導入された^(注5)。この経緯は通信路 resolvability が同定符号の逆定理の証明のために導入された経緯⁽⁶⁷⁾と類似している。この問題も情報スペクトル的な視点で捉えることができるのであるが^(26, Section 10.8)、情報源の情報までも量子情報としてしまうととてつもなく難しい問題となる。この問題の奇妙なところは、送受信者の間での共通乱数を許すか許さないかに応じて、レートが異なってくる点である。その後、この問題は古典情報理論の研究者の興味を引き、古典の場合に、乱数の量と通信の量のトレードオフを扱う研究がなされた⁽⁷⁷⁾。そこでは、likelihood encoder と呼ばれる概念が提唱されており、その後、古典情報理論の枠組みでのネットワーク情報理論において、この概念をベースに likelihood coder と呼ばれる手法が提案された⁽⁷⁸⁾。この手法は、論文⁽⁴⁵⁾で提案された量子情報理論で復号の際に頻繁に用いられる pretty good measurement と呼ばれる復号化法の古典版とみなすことができる⁽⁷⁹⁾。この likelihood coder は強力な手法で、付加情報付きの古典情報理論の問題において、二次漸近理論の枠組みでの新しいバウンドを導出する際に用いられた⁽⁸⁰⁾。

8. ま と め

近年、量子情報理論が古典情報理論に与えた影響について解説した。しかし、現在でも量子情報理論が古典情報理論から学ばねばならないことは多数あり、現時点でもたくさんの古典情報理論の成果を量子情報理論は導入中である。そのため量子情報理論が一方向的に古典情報理論に影響を及ぼしているわけでない。本原稿では、全く予期しない量子情報理論からの影響を受けた古典情報理論の発展について扱ってきた。このように、当事者が全く予期していない方向から分野が発展することは数学ではよくあることである。確かに、数値計算主体のほかの工学理論では、そのような形態の発展はまれかもしれない。古典情報理論がこのような形態の発展が可能なのは、情報という極めて普遍性の高い概念と深い数学的構造に根ざした工学理論であ

(注4): 筆者の論文の投稿日は 2008 年 8 月であるが、Princeton 大学のグループの論文⁽⁵⁴⁾の投稿日は 2008 年 11 月であり、掲載は 2009 年 10 月であり、掲載日は 2010 年 4 月である。また、Princeton 大学の ISIT2008 年の論文⁽⁷⁴⁾では、ガウス通信路については扱っていない。

(注5): この Bennett ら⁽⁷⁶⁾の論文の後に、Holevo⁽²³⁾は量子情報理論におけるエンタングル補助型の通信路符号化定理の逆定理について、Reverse Shannon Theorem を用い方法よりも単純な証明手法を与えている。現在ではこちらのアイデアが用いられることが多い^(26, Section 9.3)。

るためである．更にもう一つの要因として，同じ問題や同じ量を量子情報理論の体系で書いた場合，古典情報理論の体系の下で書いた場合と比較して，記述が短くなる場合が多い．これは意外に大きな要因で，研究を進めていく上で案外無視できないメリットとなっている場合が多い．今後も古典情報理論と量子情報理論は，その対象の普遍性のため互いに予期しない形で影響を及ぼし合いながら発展することが期待できる．

振り返ってみると，Holevo 先生は，2000 年代に入ってから量子情報理論で重要な成果を挙げているが⁽²³⁾，それらを含めても，Holevo 先生の業績が古典情報理論に直接的な影響を与えたわけではない．しかし，上述のような量子情報理論の成果が古典情報理論に与えた影響の源流をたどると，必ず，Holevo 先生による量子通信路符号化定理にたどり着く．例えば，量子相互情報量の正当な意味付けは，量子通信路符号化定理なしに不可能である．

読者の中には 2000 年以後の脚光を浴びた量子情報理論の姿しか知らない方もいるかもしれない．少なくとも 1990 年代の日本では量子情報理論は決して日の当たる分野ではなかった．量子情報理論は境界領域と言えば響きは良いが，当時の量子情報理論は言わば様々な分野の間の隙間に落ちた分野であり，どの主要な研究分野からも十分に理解される分野ではなかった．そのような状況の中，1970 年代から継続的に Holevo 先生が量子情報理論に取り組んできた結果として得られたものが今日の量子情報理論の基盤であると言える．そもそも，冒頭にも述べたように，1990 年代の時点では，現在考えられているような，量子情報理論の数学的な形式は，それほど一般的ではなかった．少なくとも物理学科では十分には知られていなかった．1960 年代の Helstrom 先生の論文に始まり，Holevo 先生を中心とした細々とした息の長い流れがこのような量子情報理論の数学的な形式を作ったのである．現在の研究者から見れば空気のように当たり前であるこの数学的形式が，全く当たり前でなかった時代があり，その背後には長い歴史が存在する．Holevo 先生をはじめとする量子情報理論の先達は，見えない貢献を積み重ねてきたのである．この基盤の上に，これまで述べてきたように部分的であるものの本家とも言える古典情報理論をしのぐ成果が得られたのである．恐らく，量子情報理論がその内部でのみ評価される成果の蓄積にとどまっていたのであれば，今回の受賞はなかったかもしれない．このように考えると，Holevo 先生の主な量子情報理論での成果は 20 年近く前のものであるが，そのインパクトが情報理論の観点から正当に評価されるにはこれだけ長い年月を要したことも納得できる．今回，Holevo 先生が Shannon award を受賞したことは，このような長期的な意味での Holevo 先生の研究活動を正当に評価したものであり心から祝福したい．

このように量子情報理論は，古典情報理論に対して，大きな貢献を果たしてきたのであるが，まっすぐにその方向に進んだわけではない．これは Holevo 先生の量子通信路符号化定理の証明から受賞が 20 年経ていることから分かることであるが，当初は紆余曲折があり，当初段階では古典情報理論へのフィードバックにまで言及できるほどの余裕はなかった．ほとんどの量子情報理論の研究がその分野独自の方向性に基づいて進展し，

古典情報理論の研究者が見た場合，皆目見当の付かない研究がほとんどであった．その中から，本原稿で述べたような古典情報理論に対して貢献できる研究が出てきたと言える．

量子情報理論は，当初段階では，古典情報理論の成果を量子系で再現することに重点が置かれていたが，このような方向性の問題は，一部の難解な問題（例えば，ランダム符号化におけるガラガー限界の量子拡張など）を除いて，基本的な部分についてはかなり解決されている．そのため，現状では，古典情報理論の枠組みの量子拡張を超えて，量子情報特有の問題を扱ったテーマ設定が扱うことが自然であり，多くのテーマは必ずしも古典情報理論に対する貢献にはならない．特にその構想段階では，古典情報理論の観点からはよく理解できないものも多い．情報理論を従来の枠組みを超えて発展させるには，今後は，そのような野心的な研究に対しても継続的にサポートする必要があると考える．ここで，量子情報理論の成果の展開先は必ずしも古典情報理論に限られないことも指摘しておきたい．筆者らは最近量子論に基づく熱力学の導出に取り組んでおり，この方面でも，量子情報理論の考え方が重要な役割を果たす⁽⁸¹⁾ ⁽⁸²⁾．また，この他に，筆者らはマルコフ過程のパラメータ推定や情報理論にも取り組んだが，ここにおいては，直接的に量子情報理論の成果は用いられることはないが，量子情報理論を研究する過程で身に着けた（若しくは蒸留された）考え方が重要な役割を果たす⁽⁸³⁾ ⁽⁸⁴⁾．このように，量子情報理論の評価を考える上では，このような表に現れない貢献についても考慮する必要がある．

最後になるが，筆者自身もここで述べた有限符号長の情報理論及び量子情報理論の研究に関して，日本学術振興会賞及び日本学士院学術奨励賞を受賞することができた．これは，近年の情報理論及び量子情報理論の成果が分野の垣根を越えて他の分野にも評価されたことの証拠である．筆者がこのような成果を出すこともできたことは，Holevo 先生をはじめとする量子情報理論の先達とその基盤を確立してくれたからである．Holevo 先生をはじめとする量子情報理論の開拓者に加え，これらのテーマと一緒に研究してくれた共同研究者をはじめとする関係者各位に，この場を借りて感謝の意を表したい．

謝辞 情報通信研究機構・電気通信大学の韓太舜先生，電気通信大学の長岡浩司先生には情報スペクトルや関連事項について多くのことを御教示して頂きました．東京工業大学の松本隆太郎先生，東京農工大学の渡辺峻先生，三菱電機の鶴丸豊広博士には本原稿で扱った情報理論のセキュリティに関して多くの内容を御教示して頂きました．特に，東京農工大学の渡辺峻先生からは文献⁽⁷⁷⁾-(⁸⁰)を教えて頂きました．また，群馬大学の森前智行先生から本原稿について有益なコメントを頂きました．

文 献

- (1) C. W. Helstrom, "Detection theory and quantum mechanics," Inf. Control, vol. 10, pp. 254-291, 1967.
- (2) C. W. Helstrom, "Minimum mean-square error estima-

- tion in quantum statistics,” *Phys. Lett.*, vol. 25A, pp. 101–102, 1967.
- (3) A. S. Holevo, “An analog of the theory of statistical decisions in noncommutative theory of probability,” *Trudy Moskov. Mat. Obšč.*, vol. 26, pp. 133–149, 1972 (in Russian). (English translation: *Trans. Moscow Math. Soc.*, vol. 26, pp. 133–149, 1972.)
 - (4) A. S. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” *Probl. Pereda. Inf.*, vol. 9, pp. 3–11, 1973. (in Russian). (English translation: *Probl. Inf. Transm.*, vol. 9, pp. 177–183, 1975.)
 - (5) A. S. Holevo, “On the capacity of quantum communication channel,” *Probl. Pereda. Inf.*, vol. 15, no. 4, pp. 3–11, 1979 (in Russian). (English translation: *Probl. Inf. Transm.*, vol. 15, pp. 247–253, 1979.)
 - (6) A. S. Holevo, “Noncommutative analogues of the Cramer-Rao inequality in the quantum measurement theory,” *Proceedings of the Third Japan-USSR Symposium on Probability Theory*, G. Maruyama and J.V. Prokhorov, eds.), Trashkent, USSR, pp. 194–222, 1975.
 - (7) H. Yuen and M. Lax, “Multiple-parameter quantum estimation and measurement of nonselfadjoint observables,” *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 740 – 750, 1973.
 - (8) A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, (North-Holland, Amsterdam, 1982); originally published in Russian, 1980.
 - (9) B. Schumacher, “Quantum coding,” *Phys. Rev. A*, vol. 51, pp. 2738–2747, 1995.
 - (10) 佐藤健一, “日ソ・日露確率論シンポジウムの27年,” *数学*, vol. 48, no. 4, pp. 425–431, 1996.
 - (11) A. S. Holevo, “Statistical problems in quantum physics,” *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, G. Maruyama and J.V. Prokhorov, eds., pp. 104–119, Kyoto, Japan, 1972.
 - (12) A. S. Holevo, “Bounds for generalized uncertainty of the shift parameter,” *Proceedings of the Fourth Japan-USSR Symposium on Probability Theory*, G. Maruyama, J.V. Prokhorov, eds., pp. 243–251 Tbilisi, USSR, Aug. 1982.
 - (13) O. Hirota, A. S. Holevo, and C. M. Caves, *Quantum Communication, Computing, and Measurement*, Springer 1997.
 - (14) A. S. Holevo, “Capacity of quantum channel with general signal states,” 1996, <http://arxiv.org/abs/quant-ph/9611023>
 - (15) A. S. Holevo, “The capacity of the quantum channel with general signal states,” *IEEE Trans. Inf. Theory*, vol. 44, p. 269, 1998.
 - (16) B. Schumacher and M. D. Westmoreland, “Sending classical information via noisy quantum channels,” *Phys. Rev. A*, vol. 56, p. 131, 1997.
 - (17) M. Hayashi, “Practical evaluation of security for quantum key distribution,” *Phys. Rev. A*, vol. 74, 022307, 2006.
 - (18) M. Hayashi, “Upper bounds of eavesdropper’s performances in finite-length code with the decoy method,” *Phys. Rev. A*, vol.76, 012329, 2007; *Phys. Rev. A*, vol.79, 019901(E), 2009.
 - (19) B. M. Terhal, “Is entanglement monogamous?,” 2003, <http://arxiv.org/abs/quant-ph/0307120>
 - (20) R. F. Werner, “An application of Bell’s inequalities to a quantum state extension problem,” *Lett. Math. Phys.*, vol. 17, pp. 359–363, 1989.
 - (21) A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, “A complete family of separability criteria,” *Phys. Rev. A*, vol. 69, 022308, 2004.
 - (22) M. Koashi and A. Winter, “Monogamy of quantum entanglement and other correlations,” *Phys. Rev. A*, vol. 69, 022309, 2004.
 - (23) A. S. Holevo, “On entanglement-assisted classical capacity,” *J. Math. Phys.*, vol. 43, pp. 4326–4333, 2002.
 - (24) I. Devetak, “The private classical capacity and quantum capacity of a quantum channel,” *IEEE Trans. Inf. Theory*, vol. 51, pp. 44–55, 2005.
 - (25) 林 正人, *量子情報理論入門*, サイエンス社, 2004.
 - (26) M. Hayashi, *Quantum Information: An Introduction*, Springer, 2006.
 - (27) R. Renner, “Security of quantum key distribution,” PhD thesis, Dipl. Phys. ETH, Switzerland, 2005, <https://arxiv.org/abs/quant-ph/0512258>
 - (28) M. Tomamichel, “A framework for non-asymptotic quantum information theory,” PhD thesis, Department of Physics, ETH Zurich, 2012; M. Tomamichel, *Quantum Information Processing with Finite Resources - Mathematical Foundations*, SpringerBriefs in Mathematical Physics, 2016.
 - (29) J. M. Renes and R. Renner, “One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys,” *IEEE Trans. Inf. Theory*, vol. 58, p. 1985, 2012.
 - (30) J. Mueller-Quade and R. Renner, “Composability in quantum cryptography,” *New J. Phys.*, vol. 11, 085006, 2009.
 - (31) M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, “Leftover hashing against quantum side information,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524 – 5535, 2011.
 - (32) V. Scarani and R. Renner, “Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing,” *Phys. Rev. Lett.*, vol. 100, 200501, 2008.
 - (33) C.H.Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, “Generalized privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.
 - (34) J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, “A pseudorandom generator from any one-way function,” *SIAM J. Comput.*, vol. 28, p. 1364, 1999.
 - (35) R. Renner and S. Wolf, “Smooth Renyi entropy and applications,” *Proceedings of 2004 IEEE International Symposium on Information Theory (ISIT 2004)*, p. 232, Chicago, USA, June - July, 2004; R. Renner and S. Wolf, “Simple and tight bounds for information reconciliation and privacy amplification,” *Proc. ASIACRYPT, Lect. Notes Comput. Sci.*, vol. 3788, pp. 199–216, Springer-Verlag, 2005.
 - (36) L. Carter and M. Wegman, “Universal classes of hash functions,” *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, 1979.
 - (37) M. N. Wegman and J. L. Carter, “New hash functions and their use in authentication and set inequality,” *J. Comput. Syst. Sci.*, vol. 22, pp. 265–279, 1981.
 - (38) T. Tsurumaru and M. Hayashi, “Dual universality of hash functions and its applications to quantum cryptography,” *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4700–4717, 2013.
 - (39) M. Hayashi, “Security analysis of epsilon-almost dual universal2 hash functions: smoothing of min entropy vs. smoothing of Renyi entropy of order 2,” *IEEE Trans. Inf. Theory*, vol. 2, no. 6, pp. 3451 – 3476, 2016.
 - (40) M. Hayashi and T. Tsurumaru, “More efficient privacy amplification with less random seeds via dual universal hash function,” *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 2213 – 2232, 2016.
 - (41) M. Tomamichel and M. Hayashi, “A hierarchy of information quantities for finite block length analysis of quantum tasks,” *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7693–7710, 2013.
 - (42) M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, “Tight finite-key analysis for quantum cryptography,” *Nat. Commun.*, vol. 3, p. 634, 2012.
 - (43) M. Hayashi and T. Tsurumaru “Concise and tight security analysis of the Bennett-Brassard 1984 protocol

with finite key lengths,” *New J. Phys.*, vol. 14, 093014, 2012.

- (44) M. Hayashi, “Optimal sequence of POVMs in the sense of Stein’s lemma in quantum hypothesis,” *J. Phys. A Math. Gen.*, vol. 35, pp. 10759–10773, 2002.
- (45) M. Hayashi and H. Nagaoka, “General formulas for capacity of classical-quantum channels,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 1753–1768, 2003.
- (46) H. Nagaoka, “Strong converse theorems in quantum information theory,” *Proc. ERATO Conference on Quantum Information Science (EQIS) 2001*, p. 33 2001. (also appeared *Asymptotic Theory of Quantum Statistical Inference*, M. Hayashi eds., Chap. 3)
- (47) 韓 太舜, 情報理論における情報スペクトルの方法, 培風館, 1998; T.-S. Han, *Information-Spectrum Methods in Information Theory*, Springer, Berlin, 2003.
- (48) M. Hayashi, “Second-order asymptotics in fixed-length source coding and intrinsic randomness,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4619 – 4637, 2008.
- (49) S. Watanabe, R. Matsumoto, and T. Uyematsu “Strongly secure privacy amplification cannot be obtained by encoder of Slepian-Wolf code,” *IEICE Trans. Fundamentals*, vol. E93-A, no. 9, pp. 1650-1659, Sept. 2010.
- (50) H. Nagaoka and M. Hayashi, “An information-spectrum approach to classical and quantum hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 53, pp. 534–549, 2007.
- (51) M. Hayashi and S. Watanabe, “Non-asymptotic bounds on fixed length source coding for Markov chains,” *Proceedings of 51st Annual Allerton Conference on Communication, Control, and Computing*, pp. 875 - 882, Allerton House, Monticello, Illinois, USA, Oct. 2013.
- (52) M. Hayashi and S. Watanabe, “Non-asymptotic and asymptotic analyses on Markov chains in several problems,” *Proceedings of 2014 Information Theory and Applications Workshop*, pp. 1 - 10, Catamaran Resort, San Diego, USA, Feb. 2014.
- (53) M. Hayashi and S. Watanabe, “Uniform random number generation from Markov chains: Non-asymptotic and asymptotic analyses,” *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1795-1822, 2016.
- (54) M. Hayashi, “Information spectrum approach to second-order coding rate in channel coding,” *IEEE Trans. Inf. Theory*, vol. 55, no.11, pp. 4947 – 4966, 2009.
- (55) A. D. Wyner, “The wire-tap channel,” *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- (56) I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- (57) R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography part I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- (58) U. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, 1993.
- (59) C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N.B. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” *IEEE Trans. Inf. Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.
- (60) J.W. Wallace and R. K. Sharma, “Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis,” *IEEE Trans. Inf. Forensics and Security*, vol. 5, no. 3, pp. 381 – 392, 2010.
- (61) S.N. Premnath, S. Jana, J. Croft, and P.L. Gowda, “Secret key extraction from wireless signal strength in real environments,” *IEEE Trans. Mob. Comput.*, vol. 12, no. 5, pp. 917 – 930, 2013.
- (62) C. Chen and M.A. Jensen, “Secret key establishment using temporally and spatially correlated wireless channel coefficients,” *IEEE Trans. Mob. Comput.*, vol. 10, no. 2, pp. 205 – 215, 2011.
- (63) 例えば, 国際会議のシリーズ「Qcrypt」が挙げられる.
- (64) Mathematical Tools of Information-Theoretic Security Workshop, Paris, France, Sept. 2015; Nexus of Information and Computation Theories, IHP Spring 2016 Thematic Program, Secrecy and Privacy Theme, March - April 2016. 後者については, 以下を参考のこと. 渡辺 峻, 「IHP 滞在記」SITA フォーラム 2016/04/11.
- (65) I. Csiszár, “Almost independence and secrecy capacity,” *Probl. Inf. Transm.*, vol. 32, no. 1, pp. 40–47, 1996.
- (66) M. Hayashi, “General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, 2006.
- (67) T. S. Han and S. Verdú, “Approximation theory of output statistics,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, 1993.
- (68) M. Hayashi, “Tight exponential analysis of universally composable privacy amplification and its applications,” *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7728 – 7746, 2013.
- (69) M. Hayashi, “Exponential decreasing rate of leaked information in universal random privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3989–4001, 2011.
- (70) M. Hayashi, “Security guaranteed secure wireless communication based on reverse reconciliation,” 2016, <http://arxiv.org/abs/1604.00635>
- (71) V. Strassen, “Asymptotische abschätzungen in Shannon’s informationstheorie,” *Transactions of the Third Prague Conference on Information Theory etc*, pp. 689-723, Czechoslovak Academy of Sciences, Prague, 1962.
- (72) D. J.C. MacKay, *Information theory, Inference and Learning Algorithms*, Cambridge University Press, 2003.
- (73) Y. Polyanskiy, H.V. Poor, and S. Verdú, “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307 – 2359, 2010.
- (74) Y. Polyanskiy, H. V. Poor, and S. Verdu, “New channel coding achievability bounds,” *Proceedings of 2008 IEEE International Symposium on Information Theory (ISIT 2008)*, pp. 1763 - 1767, Toronto, ON, Canada, July 2008.
- (75) M. Horodecki, “Limits for compression of quantum information carried by ensembles of mixed states,” *Phys. Rev. A*, vol. 57, pp. 3364–3369, 1998.
- (76) C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, “Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem,” *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, 2002.
- (77) P. Cuff, “Distributed channel synthesis,” *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7071 - 7096, 2013.
- (78) M. H. Yassaee, M. R. Aref, and A. Gohari, “A technique for deriving one-shot achievability results in network information theory,” *Proceedings of 2013 IEEE International Symposium on Information Theory (ISIT 2013)*, pp. 1287 - 1291, Istanbul, Turkey, July 2013.
- (79) S. Beigi and A. Gohari, “Quantum achievability proof via collision relative entropy,” *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7980 - 7986, 2014.
- (80) S. Watanabe, S. Kuzuoka, and V. Y. F. Tan, “Nonasymptotic and second-order achievability bounds for coding with side-information,” *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1574 – 1605, 2015.
- (81) M. Hayashi and H. Tajima, “Measurement-based formulation of quantum heat engine,” 2015, <http://arxiv.org/abs/1504.06150>
- (82) H. Tajima and M. Hayashi, “Optimal efficiency of heat engines with finite-size heat baths,” 2014, <http://arxiv.org/abs/1405.6457>
- (83) S. Watanabe and M. Hayashi, “Finite-length analysis on tail probability for Markov chain and application to

simple hypothesis testing,” Accepted for publication in Annals of Applied Probability.

- (84) M. Hayashi and S. Watanabe, “Information geometry approach to parameter estimation in Markov chains,” Accepted for publication in Annals of Statistics

林 正人 (正員)

1994 京大・理卒．1998 日本学術振興会特別研究員 (DC2)．1999 京大大学院理学研究科数学・数理解析専攻博士後期課程了．2000 理化学研究所脳科学総合研究センター脳数理研究チーム研究員．2003 科学技術振興機構 ERATO 今井量子計算機構プロジェクト技術参事．2006 科学技術振興機構 ERATO-SORST 量子情報システムアーキテクチャグループ

リーダー．2007 東北大学院情報科学研究科准教授．2012 名大大学院多元数理科学研究科教授．2009 からシンガポール国立大量子技術研究センター客員研究准教授を兼務 (2012 から客員研究教授)．量子情報理論，量子暗号，情報理論の研究に従事．理博．2010 日本 IBM 科学賞コンピュータ・サイエンス分野，2011 船井学術賞 コンピュータサイエンス分野，2011 IEEE Information Theory Society Paper Award，2016 日本学術振興会賞及び日本学士院学術奨励賞各受賞．著書「量子情報理論入門」，「量子情報科学入門」，「量子論のための表現論」，「量子情報への表現論的アプローチ」，「Introduction to Quantum Information Science, Graduate Texts in Physics」など．