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

令和　２ 年　 ５ 月 ２３ 日現在

機関番号：１２６０８
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ０６４１７

研究課題名（和文）通信路を用いた乱数の生成と共有に関する研究

研究課題名（英文）Joint Channel Coding and Channel Intrinsic Randomness

研究代表者
植松　友彦（Uyematsu, Tomohiko）

東京工業大学・工学院・教授

研究者番号：６０１６８６５６

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：本研究では、通信路を利用した乱数の生成と共有について、まだ定式化されていない問題を取り上げ、次の成果を得た。
1)多入力・多出力の一般通信路に対し、通信路の出力列から取り出せる最大の乱数生成レート、誤差εを許容したときの最大の乱数生成レート、および2次のレートを明らかにした。
2)一般通信路、一般盗聴通信路ならびに一般多重アクセス通信路において、送信者が送信した情報を受信者が任意に小さい誤り率で受信すると共に、送信者が送信した情報や傍受者が受信した情報とは独立な乱数を通信路の出力列から受信者が生成する問題を取り上げ、情報伝送レートと乱数生成レートの限界領域(達成可能領域)を明らかにした。

研究成果の学術的意義や社会的意義
情報源を利用した真の乱数生成問題は、intrinsic randomness 問題として知られ、通信路を用いた真の乱数生成問題は、channel intrinsic randomness 問題と呼ばれる。しかしながら、放送型通信路の出力列から各受信者が互いに独立な真の乱数を生成する問題、あるいは多重アクセス通信路の出力列を用いて真の乱数を生成する問題に対する乱数生成レートの限界などは未知であった。本研究では、これらのまだ定式化されていない問題を取り上げ、乱数の生成レートや共有レートを求めた点に学術的な意義がある。また、乱数生成や乱数共有は安全安心な通信の基盤でもあり、社会的意義も大きい。

研究成果の概要（英文）：In this research, we aimed at clarifying the limits of the random number generation rate and the random number sharing rate by tackling the problems that had not been formulated yet, and obtained the following results.
1) For a multi-input / multi-output general channel, we clarify the maximum random number generation rate that can be extracted from the output sequence of the channel, the maximum random number generation rate when the error ε is allowed, and the secondary rate.
2) For the general channel, the general wiretapping channel, and the general multiple access channel, we consider the problem that the receiver obtains the information transmitted by the sender with an arbitrarily small error rate, at the same time the receiver generates random numbers independent of the information transmitted by the sender and the sequence received by the eavesdropper. We clarify the limit area (achievable area) of the information transmission rate and the random number generation rate.

研究分野：情報理論、情報セキュリティ

キーワード：乱数生成問題　達成可能領域　乱数生成レート　情報伝送レート　一般通信路　一般多重アクセス通信路　一般盗聴通信路

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

情報源を利用した真の乱数生成問題は、intrinsic randomness 問題として知られ、1995 年に Vembu と Verdu によって定式化され、最近では相関を有する複数の情報源から互いに独立な乱数を生成する問題も検討されている。一方、この問題の双対問題にあたる通信路を用いた真の乱数生成問題は、2010 年に Bloch によって提案され、channel intrinsic randomness 問題と呼ばれている。Bloch は、通信路の出力列から通信路の入力分布と独立な真の乱数を生成する問題を取り上げ、通信路の 1 出力記号あたり得られる真の乱数のビット数で定義される乱数生成レートの限界を求めている。しかしながら、放送型通信路の出力列から各受信者が互いに独立な真の乱数を生成する問題、あるいは多重アクセス通信路の出力列を用いて真の乱数を生成する問題に対する乱数生成レートの限界は未知であった。

他方、情報源や通信路を利用した乱数の共有問題は common randomness 問題と呼ばれる。特に、傍受者に対して秘密の乱数を共有する問題は秘密鍵共有問題と呼ばれ、1993 年の Maurer や Ahlswede と Csiszar による研究以降、広く研究されている。しかしながら、傍受者が居るときの秘密鍵共有問題の共有レートの限界を求める問題は難しく、未解決であった。

２．研究の目的

本研究では、通信路を利用した乱数の生成と共有について、まだ定式化されていない問題を取り上げ、乱数の生成レートや共有レートの限界を明らかにすると共に、限界のレートを達成する乱数生成／共有アルゴリズムを提案することを目的としている。具体的には、通信路の送受信者の間で、送信者が生成した乱数を受信者が共有すると同時に通信路の出力列から共有する乱数とは独立な乱数を生成する問題、送受信者の一方を複数に増やした通信路への拡張などを研究対象とする。他方、応用上重要となる無記憶通信路に対する具体的な乱数生成ならびに乱数共有アルゴリズムについても検討する。

具体的には、次の問題の解決に重点をおく。

a) 一人の送信者と複数の受信者を有する放送型通信路において、複数の受信者が通信路の出力列から互いに独立な真の乱数を生成する問題
b) 放送型通信路において、複数の受信者が互いに独立でありかつ傍受者が得た通信路の出力列とも独立な真の乱数を生成する問題
c) 複数の送信者と一人の受信者から成る多重アクセス通信路において、受信者が通信路の入力列と独立な真の乱数を生成する問題
d) 多重アクセス通信路において、受信者が通信路の入力列のみならず傍受者が得た通信路の出力列とも独立な真の乱数を生成する問題
e) 通信路を用いた乱数共有問題において、受信者と送信者が共有する乱数とは独立な真の乱数を生成する、乱数の同時共有/生成問題
f) 放送型通信路における乱数の同時共有/生成問題
g) 多重アクセス通信路における乱数の同時共有/生成問題

本研究では、定常性やエルゴード性を仮定しない最も広い通信路のクラスである一般通信路に対して、上記の乱数生成問題の乱数生成レートの限界領域を明らかにすると共に、送受信者間で乱数共有を行う際、共有乱数のレートと受信者が生成する乱数のレートの関係を明らかにし、2 つのレートの限界領域を求めるとともに、両者にトレードオフ関係が存在するか否かを明らかにすることを最大の目的とする。

３．研究の方法

本研究では、第一段階として、放送型通信路と多重アクセス通信路を用いて受信者が真の乱数を生成する方法について研究を行う。具体的には、これらの通信路に対して、傍受者がいないときに複数の受信者が互いに独立な乱数を生成する際の生成レートの限界、ならびに傍受者がいるときの生成レートの限界を求める。次に、出力列の長さが有限の場合の近似誤差について厳密な解析を行う。

第二段階としては、受信者における真の乱数生成のみならず、送受信者間で同時に乱数を共有する方法についても検討し、各種通信路における乱数生成レートと乱数共有レートの領域の限界を明らかにする。

以下、具体的な研究方法について述べる。

a) 放送型通信路や多重アクセス通信路において、複数の受信者が互いに独立な真の乱数を生成するときの各生成レートの満たすべき限界の導出

放送型通信路や多重アクセス通信路を一般化した多入力・多出力の一般通信路に対し、通信路の出力列から取り出せる最大の乱数生成レート、および誤差 ε を許容したときの最大の乱数生成レートを明らかにする。更に、通信路の入力列の他に受信者の一部（傍受者）が得た出力列とも独立な乱数を生成する場合を考察し、最大乱数生成レートおよび誤差 ε を許容したときの最大乱数生成レートを明らかにする。

b) 放送型通信路や多重アクセス通信路において、出力列の長さを有限にしたときの近似誤差の解析

無記憶の放送型通信路や多重アクセス通信路において、乱数生成に用いる出力列の長さと乱数の生成レートが与えられたときに、乱数生成写像の満足すべき近似誤差の上限と下限を明ら

かにする。すなわち、理想的な乱数生成写像によってどこまで小さな近似誤差が達成できるのかを明らかにすると共に、乱数生成写像を構成することにより近似誤差の上限を明らかにする。

c）通信路を利用した送受信者間の乱数の共有と受信者による独立乱数の同時生成の検討

送受信者が共に 1 人の無記憶通信路において、送信者が生成した乱数を受信者が共有すると共に、送信者が生成した乱数とは独立な乱数を、通信路の出力列から受信者が生成する問題を取り上げる。このとき、共有できる乱数のレートと生成できる乱数のレートの限界領域を明らかにすることで、2 つのレートの間にトレードオフ関係があるか否かを明らかにする。また、具体的な乱数共有法についても検討する。更に、無記憶通信路のみならず一般通信路へも成果を拡張する。

d）通信路を利用した乱数の共有と受信者による独立乱数の同時生成における誤り率と近似誤差の指数的限界式の導出

c)で取り上げた問題において、生成された乱数の分布と理想的な分布との変動距離および復号誤り率が共に符号長に対して指数関数的に減少することを明らかにする。

e）一般盗聴通信路における盗聴者に秘密の乱数の共有と独立な乱数の同時生成

送信者が 1 人、受信者が 2 人の通信路である一般盗聴通信路において、一方の受信者を正当な受信者、もう一方の受信者を盗聴者と呼ぶ。送信情報を盗聴者には秘密にしたまま、正当な受信者が任意に小さい誤り率で受信すると共に、送信者の送信情報ならびに盗聴者の受信情報とは独立な乱数を通信路の出力列から受信者が生成する問題を取り上げ、盗聴者がいない場合と同様に達成可能領域を明らかにする。

f）一般多重アクセス通信路を利用した送受信者間の乱数の共有と受信者による独立乱数の同時生成

送信者が二人、受信者が一人である多重アクセス通信路における送受信間の乱数の共有と受信者による独立乱数の同時生成問題を考察し、二人の送信者の情報伝送レートと乱数生成レートの限界領域(達成可能領域)を明らかにする。また、定常無記憶多重アクセス通信路、加法的雑音を有する多重アクセス通信路ならびに混合多重アクセス通信路に対して、具体的な達成可能領域を求める。

４．研究成果

平成 29 年度は、通信路の出力列から真の乱数を受信者が生成する方法について研究を行い、次の 3 つの研究実績を得た。

1)多入力・多出力の一般通信路において、通信路の出力列から取り出せる最大の乱数生成レート、および誤差 ε を許容したときの最大の乱数生成レートを明らかにした。更に、通信路の入力列の他に受信者の一部(傍受者)が得た出力列とも独立な乱数を生成する場合についても最大乱数生成レートおよび誤差 ε を許容したときの最大乱数生成レートを明らかにした。

2)上記問題において、2 次の最大乱数生成レートを明らかにし、乱数生成に用いる出力列の長さと乱数の生成レートが与えられたときに、乱数生成写像の近似誤差の上限と下限を明らかにした。

3)送受信者が共に 1 人の無記憶通信路において、送信者が送信した情報を受信者が任意に小さい誤り率で受信すると共に、通信路の出力列から送信者が送信した情報とは独立な乱数を受信者が生成する問題を取り上げ、情報伝送レートと乱数生成レートの限界領域(達成可能領域)を明らかにした。また通信路の入力分布を固定した場合、2 つのレートの間にトレードオフ関係が存在しないことを示すと共に、多重アクセス通信路の達成可能領域と同様に、通信路の入力分布を取り替えることによって、トレードオフが生じることを明らかにした。

これらの研究実績について、1)と 2)は電子情報通信学会英文論文誌に再録された。また、3)は、電子情報通信学会基礎境界ソサイエティ主催の研究集会である「情報理論とその応用シンポジウム」にて発表を行なった。

平成 30 年度は、各種の通信路に関して次の 3 つの研究実績を得た。

1)昨年度の 3)の成果を一般通信路へ拡張し、一般通信路において、送信者が送信した情報を受信者が任意に小さい誤り率で受信すると共に、通信路の出力列から送信者が送信した情報とは独立な乱数を受信者が生成する問題を取り上げ、情報伝送レートと乱数生成レートの限界領域(達成可能領域)を明らかにした。

2)離散無記憶通信路において 1)と同様な問題を考察したとき、生成された乱数の分布と理想的な分布との変動距離および復号誤り率が共に符号長に対して指数関数的に減少することを明らかにした。また、情報伝送と乱数生成を同時に行っても、復号誤り率についてはランダム符号化による誤り指数が達成できることを示した。

3)一般盗聴通信路において、送信情報を盗聴者には秘密にしたまま、正当な受信者が任意に小さい誤り率で受信すると共に、送信者の送信情報ならびに盗聴者の受信情報とは独立な乱数を通信路の出力列から受信者が生成する問題を取り上げ、盗聴者がいない場合と同様に達成可能領域を明らかにした。また通信路の入力分布を固定した場合、2 つのレートの間にトレードオフ関係が存在しないことを示すと共に、多重アクセス通信路の達成可能領域と同様に、通信路の入力分布を取り替えることによって、トレードオフが生じることを明らかにした。

これらの研究実績について、1)の成果は電子情報通信学会英文論文誌に採録され、2)と 3)の

成果は国際会議 International Symposium on Information Theory and its Applications 2018 において発表を行った。

令和元年度は、送信者が二人、受信者が一人である多重アクセス通信路における送受信間の乱数の共有と受信者による独立乱数の同時生成問題を考察し、次の研究成果を得た。

1)必ずしも定常性やエルゴード性を持たない一般多重アクセス通信路において、二人の送信者の情報(乱数)を受信者が任意に小さい誤り率で復号すると共に、二人の送信者の送信情報とは統計的に独立な乱数を通信路の出力列から受信者が生成する問題を取り上げ、二人の送信者の情報伝送レートと乱数生成レートの限界領域(達成可能領域)を明らかにした。また通信路の入力分布を固定した場合、2 つの情報伝送レートと乱数生成レートの間にはトレードオフ関係が存在しないことを示すとともに、通信路の入力分布を取り替えることによって、トレードオフが生じることを明らかにした。更に、片方の送信者が情報を送らない場合、一般通信路において求めた達成可能領域が導かれることを明らかにした。

2)定常無記憶多重アクセス通信路、加法的雑音を有する多重アクセス通信路ならびに混合多重アクセス通信路に対して、具体的な達成可能領域を求めた。定常無記憶多重アクセス通信路においては、通信路出力のエントロピーが入出力間の相互エントロピーと乱数生成レートの和に等しいことを示した。また、加法的雑音を有する多重アクセス通信路においては、最大の乱数生成レートが雑音のエントロピーレート下限に一致することを示した。更に、混合多重アクセス通信路においては、情報伝送レートの上限が小さい方の多重アクセス通信路によって定まり、乱数生成レートの上限が小さい方の多重アクセス通信路によって定まることを明らかにした。

これらの研究実績について、1)と 2)の成果は電子情報通信学会基礎境界ソサイエティ主催の研究集会「第 11 回シャノン理論ワークショップ」において発表を行なった。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 UYEMATSU Tomohiko, MATSUTA Tetsunao	４．巻 E101.A
２．論文標題 Joint Channel Coding and Intrinsic Randomness	５．発行年 2018年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 2091～2098
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.2091	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Tomohiko Uyematsu and Tetsunao Matsuta	４．巻 E100-A
２．論文標題 Second-Order Intrinsic Randomness for Correlated Non-Mixed and Mixed Sources	５．発行年 2017年
３．雑誌名 IEICE Trans. Fundamentals	６．最初と最後の頁 2615-2628
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.2615	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Tomohiko Uyematsu
２．発表標題 Error Exponents of Joint Channel Coding and Intrinsic Randomness for Memoryless Channels
３．学会等名 International Symposium on Information Theory and its Applications 2018（国際学会）
４．発表年 2018年

１．発表者名 Natsuki Hirotani
２．発表標題 Joint Secure Communication and Independent Random Number Generation against Eavesdropper
３．学会等名 International Symposium on Information Theory and its Applications 2018（国際学会）
４．発表年 2018年

１．発表者名
Tomohiko Uyematsu

２．発表標題
Joint Channel Coding and Channel Intrinsic Randomness

３．学会等名
第40回情報理論とその応用シンポジウム（SITA2017）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	松田　哲直 (Matsuta Tetsunao) (00638984)	東京工業大学・工学院・助教 (12608)	