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　３ 年　 ６ 月 ２９ 日現在

機関番号：１２６１２
研究種目：基盤研究(C)（一般）
研究期間：2016～2020
課題番号：１６Ｋ０６３４０

研究課題名（和文）高い信頼性と安全性を保証する通信・記録システムの実現に向けた情報変換法の性能解析

研究課題名（英文）Analysis of Data Conversion for Highly Reliable and Secure Communication/Storage Systems

研究代表者
八木　秀樹（Yagi, Hideki）

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：６０４０９７３７

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：一様分布に従う乱数を変換して所望の確率分布を生成する問題はResolvability問題と呼ばれる．この問題では，確率分布の生成にかかるコストを削減するために，一様乱数が取る値域のサイズ（乱数生成レート）をできる限り小さくすることが求められる．
本研究では，Resolivability 問題において可変長符号化の概念を提案し，このシステムに対する性能解析を行った．定常無記憶情報源またはその混合分布を所望の確率分布とした場合には，系列長に依存しない形式で最小乱数生成レートの公式を導出した．また，固定長のResolbability問題における確率分布の近似尺度の拡張を行った．

研究成果の学術的意義や社会的意義
本研究で導出し可変長のResolvability問題における最小乱数生成レートの公式から，固定長の問題に対する最小乱数生成レートよりも平均的に変換のコストを下げられることを示している．さらにこの結果から，定常無記憶情報源やマルコフ情報源を近似する最小乱数生成レートは，この情報源からの出力系列を符号化する際の最小符号化レートと一致することがわかり，系列長に依存しない形式で最小乱数生成レートの公式が得られる．系列長に依存しない定数オーダの計算量で一様乱数の最少レートを計算することが可能になり，乱数生成アルゴリズムの設計の指針を与える結果と言える．

研究成果の概要（英文）：The conversion of a uniformly distributed random number to approximate a given target distribution is generally called random number generation. In this study, we consider the problem of minimizing the size of the value set in which the uniform random number takes while the approximation is done within some precision. This problem is called the problem of resolvability. This study introduces the problem of resolvability based on the idea of variable-length coding, and the minimum resolvability rate is investigated. When the target distribution is a stationary memoryless source or a mixture of such sources, the minimum resolvability can be characterized in a form which does not depend on the length of source sequences. In addition, we extend the approximation measure between two probability distributions in the problem of fixed-length resolvability.

研究分野：情報理論

キーワード：情報理論　符号化　情報セキュリティ　乱数生成　情報源符号化

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

大量のデータが伝送・蓄積される現代の通信・記録システムでは，情報伝送・情報記録の信頼性および安全性の保証が重要な課題となっている．例えば，クラウドシステム等の複数のノードから構成されるネットワークにおいて，他ノードに情報を秘匿したまま宛先のノードに正しく情報を送り届けることや，秘密情報を複数のノードに分散して蓄積しておき，安全に秘密情報を管理することなどが，そのようなシステムの例として挙げられる．

情報理論は様々な通信・記録システムにおける**符号化**（より一般には**情報変換**）法の性能限界を数理的に明らかにしてきた．例えば，情報系列が定常かつエルゴード的な確率分布を持つ情報源から生起する際に，誤りなく復元できる情報源符号化の圧縮率の最小値は確率分布の**情報エントロピー**で記述できることや，通信路を介して情報伝送を行う通信路符号化システムにおいて，『符号長 $n$ の増大とともに復号誤り率を任意に小さくできる符号化法が存在する情報伝送速度の最大値』である**通信路容量**が様々な確率構造を持つ通信路に対して明らかにされてきた．このように，情報変換法の性能限界を理論的に示すことは，情報・符号化システムの設計者に目指すべき目標値を明確に与えるという点で重要である．

情報理論に基づいて通信・記録システムの安全性を論じる研究分野は**情報理論的セキュリティ**と呼ばれる．この分野では，情報理論的安全性の尺度が用いられ，この尺度によりハードウェアの技術発展に影響されない根本的な安全性を評価することが可能となる．情報理論で明らかにされている符号化手法の性能限界の解析は，情報理論的セキュリティの分野にも活かされてきた．例えば，盗聴者が存在する盗聴通信路における符号化，プライバシー保護を目的とした符号化問題，乱数生成問題や確率分布の近似問題などがその一例である．情報セキュリティを目的とした情報変換問題において，乱数の扱いは非常に重要である．情報理論分野において古くから議論されてきたテーマであるが，近年の情報源符号化・通信路符号化における解析手法の洗練化にともない，様々な情報変換問題に対してもより詳細な解析が期待できる．

２．研究の目的

情報源符号化や通信路符号化の枠組みで鍵となるのが，『復号誤り確率を正定数 $\varepsilon$ まで許容する符号化問題』である．この種の符号化問題では，送信する対象の情報源系列も，それを符号化して得られる符号語も長さが固定される符号化(**固定長符号**と呼ぶ)が仮定されてきた．一方，符号語の長さが可変となる**可変長符号**に対して復号誤りを $\varepsilon$ まで許容すると，固定長符号よりも効率的な符号化が行えることが近年示されている．本研究においても可変長情報源符号化の考え方をベースに，関連する符号化とセキュリティの問題を扱う．

一様分布に従う乱数（**一様乱数**）を変換して所望の確率分布を近似する問題は**Resolvability 問題**と呼ばれる．この問題では確率分布の生成にかかるコストを削減するため，一様乱数がとる値域のサイズ（**乱数生成レート**）をできる限り小さくすることが求められる．特に，通信路の出力分布を近似する問題（通信路 Resolvability）は，盗聴者が存在する通信において，盗聴者に情報を漏らさないように符号化する際に鍵となる技術として知られている．本研究では，情報源符号化における可変長符号の考え方を応用し，可変長の一様乱数を変換する可変長 Resolvability 問題を導入する．この問題における最小乱数生成レートと可変長符号化システムにおける最小符号化レートの関係を調べる．また，通信路符号化の枠組みにおいても理論の精密化と関連の深い情報セキュリティ問題への応用を検討する．

３．研究の方法

本研究では，(i) 可変長一様乱数を用いた通信路 Resolvability 問題の導入，(ii) 固定長一様乱数を用いた情報源 Resolvability 問題における近似尺度クラスの拡張，(iii) プライバシー保護を目的とした情報消去問題について議論する．詳細を以下にまとめる．

(i) 本研究では，可変長一様乱数を用いた通信路 Resolvability 問題を定式化する．また**情報スペクトル**的手法に基づいて，定常性もエルゴード性も仮定しない一般情報源・通信路に対する最小乱数生成レートを求める．最終的には情報源の系列長 $n$ を限りなく大きくした時の極限の状況を解析するが，その際にまず有限の $n$ に対する乱数生成レートの上界式・下界式を導出する．

(ii) Resolvability 問題における確率分布の近似尺度は，変動距離や Kullback–Leibler (KL)ダイバージェンスが用いられることが多い．特に，変動距離を $\varepsilon$ としたときの情報源

Resolvability 問題は，復号誤り確率を $\varepsilon$ まで許容した情報源符号化問題における最小符号化レートと一致することが知られている．一方，応用上は他の近似尺度を用いることが多い．近年，変動距離や KL ダイバージェンスを特別な場合として含む f ダイバージェンスに対して，固定長の情報源 Resolvability レートが情報スペクトル的な手法に基づいて解析されている．本研究では他の情報量を用いて最小乱数生成レートを特徴づけることを試みる．

(iii) ディスク等に保存されている機密データを一様乱数を用いて消去する際に，消去にかかるコストと情報漏洩量を一定値に抑える問題は，**情報消去問題**と呼ばれる．この問題は情報源 Resolvability 問題の拡張と位置付けられる．本研究において情報源 Resolvability レート（最小の乱数生成レート）を解析する手法を拡張し，情報消去問題における最小乱数生成レートを明らかにする．

## ４．研究成果

### （１） 一般情報源・通信路における Resolvability 問題

最も一般的な場合を想定して，定常性もエルゴード性も仮定しない一般通信路に対して，変動距離と KL ダイバージェンスを近似尺度とした可変長の通信路 Resolvability レートを特徴づけた．通常の固定長の一様乱数を変換する場合に比べて，可変長の通信路 Resolvability レートが必ず小さくなることを示した．

通信路が無雑音の場合，この問題は情報源 Resolvability 問題となる．与えた通信路 Resolvability レートの表現から，可変長の情報源 Resolvability レートの表現式も容易に導出できる．固定長 Resolvability レートは固定長の情報源符号化における最小符号化レートと一致することが知られてきた．これに対し，可変長の情報源 Resolvability レートは，固定長の情報源からの出力を可変長の符号語に符号化する固定長-可変長情報源符号化における最小の平均符号化レートと等しくなることを示した．このことから，様々な情報源に対する情報源符号化の最小レートを求めるには，変動距離を近似尺度とした情報源 Resolvability レートを求めればいいことが明らかとなった．

### （２） 定常無記憶な情報源・通信路に対する Resolvability 問題

情報源と通信路が定常無記憶性を有する場合に対し，通信路 Resolvability レートを系列長に依存しない形式で特徴づけた．これにより系列長によらない定数オーダの計算量で，一様乱数の最小生成レートを求めることが可能となる．また，この結果を情報源が定常無記憶情報源の混合分布で与えられる場合（**混合無記憶情報源**という）に拡張し，この情報源に対しても系列長に依存しない形で通信路 Resolvability レートが求められることを示した．

情報源系列長 $n$ を増大させたとき，最小乱数生成レートが通信路 Resolvability レート近づき方は**最適二次情報レート**と呼ばれ，近年盛んに研究されている．混合無記憶情報源に対して，最適な二次の通信路 Resolvability レートも特徴づけられることを明らかにした．この結果を固定長－可変長情報源符号化にフィードバックすることにより，従来知られていなかった混合情報源に対する最小二次符号化レートの公式も明らかにした．

### （３） 固定長 Resolvability 問題における近似尺度クラスの拡張

情報確率分布の近似尺度を変動距離やＫＬダイバージェンスに限らない一般の尺度に拡張して議論すると，様々な尺度クラスを一括して扱えることにつながる．ここでは固定長の情報源 Resolvability 問題に限定し，変動距離やＫＬダイバージェンスを一般化した **f ダイバージェンス**のクラスを近似尺度とした場合において，スムース情報エントロピーに基づいて一般情報源に対する固定長 Resolvability レートを解析した．f ダイバージェンスは凸関数 f を元に定義される尺度である．関数 f が単調減少な関数であるとき，関数 f の逆関数から計算される値まで復号誤り確率を許容した固定長の情報源符号化問題における最小符号化レートと密接な関係があることを示した．一般的な情報源に関する表現式から，定常情報源や混合無記憶情報源においては，系列長 $n$ に依存しない形式で情報源 Resolvability レートを表現することが可能となる．

このステップでは，可変長一様乱数に対する結果は得られていない．この解析については今後の課題である．

### （４） プライバシー保護を目的とした情報消去問題

情報消去問題において，機密データが定常無記憶情報源から生起することを仮定し，従来知られていなかった最小乱数生成レートの公式を導出した．この公式から，少々レートを求める問題が，凸関数の最小化問題（凸計画問題）として定式化できることを明らかにした．この結果から二次の最小乱数生成レートを導出することも可能である．このシステムに対して，可変長一様乱数を用いた場合の解析は今後の課題である．

（５）　その他の研究成果

上記の研究の他，複数の固体の生体データをデータベースに登録し，生体データが観測されたときにデータベースに保存されているどの生体に対応するかを識別する**生体識別システム**に関する研究成果を得た．特に，符号化に用いる一様乱数を利用して，生体データからより多くの乱数列を取り出すシステムを提案し，符号語からの生体データに関する情報漏洩量を解析した．またガウス分布に従う情報源と通信路からなるシステムに拡張して，詳細な解析を行った．

５．主な発表論文等

〔雑誌論文〕　計15件（うち査読付論文　15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<br>Naruaki Amada, Hideki Yagi | ４．巻<br>5 |
| ２．論文標題<br>Single-letter characterizations for information erasure under restriction on the output distribution | ５．発行年<br>2021年 |
| ３．雑誌名<br>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences | ６．最初と最後の頁<br>805～813 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transfun.2020EAP1014 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Vamoua Yachongka, Hideki Yagi | ４．巻<br>1 |
| ２．論文標題<br>Fundamental limits of biometric identification system under noisy enrollment | ５．発行年<br>2021年 |
| ３．雑誌名<br>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences | ６．最初と最後の頁<br>283~294 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transfun.2020EAP0001 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>雲居玄道，八木秀樹，後藤正幸，平澤茂一 | ４．巻<br>13 |
| ２．論文標題<br>多値文書分類のため情報理論的基準による２元符号語表の構成法 | ５．発行年<br>2020年 |
| ３．雑誌名<br>情報処理学会論文誌 数理モデル化と応用 | ６．最初と最後の頁<br>1～12 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>なし | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Toshihiro Niinomi, Hideki Yagi, Shigeichi Hirasawa | ４．巻<br>E103.A |
| ２．論文標題<br>Decision Feedback Scheme with Criterion LR+Th for the Ensemble of Linear Block Codes | ５．発行年<br>2020年 |
| ３．雑誌名<br>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences | ６．最初と最後の頁<br>334～345 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transfun.2019EAP1045 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Ryo Nomura, Hideki Yagi | 4．巻<br>65 |
| 2．論文標題<br>Optimum Overflow Thresholds in Variable-Length Source Coding Allowing Non-Vanishing Error Probability | 5．発行年<br>2019年 |
| 3．雑誌名<br>IEEE Transactions on Information Theory | 6．最初と最後の頁<br>8213～8221 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/TIT.2019.2920417 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Tomoya Hamada, Hideki Yagi | 4．巻<br>E101.A |
| 2．論文標題<br>Construction of Locally Repairable Codes with Multiple Localities Based on Encoding Polynomial | 5．発行年<br>2018年 |
| 3．雑誌名<br>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences | 6．最初と最後の頁<br>2047～2054 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transfun.E101.A.2047 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Vamoua Yachongka, Hideki Yagi | 4．巻<br>22 |
| 2．論文標題<br>Fundamental Tradeoff among Identification, Secrecy and Compression Rates in Biometric Identification System | 5．発行年<br>2018年 |
| 3．雑誌名<br>Journal of Signal Processing | 6．最初と最後の頁<br>337～342 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.2299/jsp.22.337 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Toshihiro Niinomi, Hideki Yagi, Shigeichi Hirasawa | 4．巻<br>E101.A |
| 2．論文標題<br>On the DS2 Bound for Forney's Generalized Decoding Using Non-Binary Linear Block Codes | 5．発行年<br>2018年 |
| 3．雑誌名<br>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences | 6．最初と最後の頁<br>1223～1234 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transfun.E101.A.1223 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| 1．著者名 | 4．巻 |
|---|---|
| Toshihiro Niinomi, Hideki Yagi, Shigeichi Hirasawa | vol. E101-A, no. 8 |
| 2．論文標題 | 5．発行年 |
| On the DS2 bound for Forney's generalized decoding using non-binary linear block codes | 2018年 |
| 3．雑誌名 | 6．最初と最後の頁 |
| IEICE Trans. Fundamentals | 印刷中 |
| 掲載論文のDOI（デジタルオブジェクト識別子） | 査読の有無 |
| なし | 有 |
| オープンアクセス | 国際共著 |
| オープンアクセスではない、又はオープンアクセスが困難 | － |

| 1．著者名 | 4．巻 |
|---|---|
| Hideki Yagi, Ryo Nomura | vol. E100-A, no. 8 |
| 2．論文標題 | 5．発行年 |
| Variable-length coding with cost allowing non-vanishing error probability | 2018年 |
| 3．雑誌名 | 6．最初と最後の頁 |
| IEICE Trans. Fundamentals | 1683-1692 |
| 掲載論文のDOI（デジタルオブジェクト識別子） | 査読の有無 |
| 10.1587/transfun.E100.A.1683 | 有 |
| オープンアクセス | 国際共著 |
| オープンアクセスではない、又はオープンアクセスが困難 | － |

| 1．著者名 | 4．巻 |
|---|---|
| Quang Thanh Pham, Hideki Yagi | vol. 6, no. 7 |
| 2．論文標題 | 5．発行年 |
| Generalized construction of cyclic (r, t)-locally repairable codes using trace function | 2017年 |
| 3．雑誌名 | 6．最初と最後の頁 |
| IEICE Communications Express | 449-453 |
| 掲載論文のDOI（デジタルオブジェクト識別子） | 査読の有無 |
| 10.1587/comex.2017XBL0055 | 有 |
| オープンアクセス | 国際共著 |
| オープンアクセスとしている（また、その予定である） | － |

| 1．著者名 | 4．巻 |
|---|---|
| Vamoua Yachongka, Hideki Yagi | vol. E100-A, no. 5 |
| 2．論文標題 | 5．発行年 |
| Reliability function and strong converse of biometrical identification systems based on list-decoding | 2017年 |
| 3．雑誌名 | 6．最初と最後の頁 |
| IEICE Trans. Fundamentals | 1262-1266 |
| 掲載論文のDOI（デジタルオブジェクト識別子） | 査読の有無 |
| 10.1587/transfun.E100.A.1262 | 有 |
| オープンアクセス | 国際共著 |
| オープンアクセスではない、又はオープンアクセスが困難 | － |

| | |
|---|---|
| １．著者名<br>Hideki Yagi, Te Sun Han, Ryo Nomura | ４．巻<br>Vol. 62, No. 8 |
| ２．論文標題<br>First- and second-order coding theorems for mixed memoryless channels with general mixture | ５．発行年<br>2016年 |
| ３．雑誌名<br>IEEE Trans. Information Theory | ６．最初と最後の頁<br>4395-4412 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/TIT.2016.2573310 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Vamoua Yachongka, Hideki Yagi | ４．巻<br>Vol. E100-A, No. 5 |
| ２．論文標題<br>Reliability function and strong converse of biometrical identification systems based on list-decoding | ５．発行年<br>2017年 |
| ３．雑誌名<br>IEICE Trans. Fundamentals | ６．最初と最後の頁<br>1262-1266 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transfun.E100.A.1262 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Quang Thanh Pham, Hideki Yagi | ４．巻<br>Vol. 6 |
| ２．論文標題<br>Generalized construction of cyclic (r, t)-locally repairable codes using trace function | ５．発行年<br>2017年 |
| ３．雑誌名<br>IEICE Communications Express | ６．最初と最後の頁<br>未定 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/comex.2017XBL0055 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

〔学会発表〕　計58件（うち招待講演　0件／うち国際学会　31件）

| |
|---|
| １．発表者名<br>Toshihiro Niinomi, Hideki Yagi, Shigeichi Hirasawa |
| ２．発表標題<br>Upper bounds on the error probability for the ensemble of linear block codes with mismatched decoding |
| ３．学会等名<br>Proc. of 2020 Int. Symposium on Information Theory and its Applications (ISITA2020)（国際学会） |
| ４．発表年<br>2020年 |

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
Biometric identification systems with both chosen and generated secrecy

３．学会等名
Proc. of 2020 Int. Symposium on Information Theory and its Applications (ISITA2020) (国際学会)

４．発表年
2020年

１．発表者名
Ryo Nomura, Hideki Yagi

２．発表標題
Optimum source resolvability rate with respect to f-divergences using the smooth Renyi entropy

３．学会等名
Proc. of 2020 IEEE Int. Symposium on Information Theory (ISIT2020) (国際学会)

４．発表年
2020年

１．発表者名
Naruaki Amada, Hideki Yagi

２．発表標題
The minimum cost of information erasure for stationary memoryless sources under restriction on the output distribution

３．学会等名
Proc. 54the Annual Conference on Information Sciences and Systems (CISS2020) (国際学会)

４．発表年
2020年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
A new characterization of the capacity region of identification system under noisy enrollment

３．学会等名
Proc. 54the Annual Conference on Information Sciences and Systems (CISS2020) (国際学会)

４．発表年
2020年

１．発表者名
Lingyun Chen, Vamoua Yachongka and Hideki Yagi

２．発表標題
Sum-capacity region of a multi-enrollment rate-constrained system using PUF observations

３．学会等名
Proc. of 2020 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2020)（国際学会）

４．発表年
2020年

１．発表者名
Qipeng Wu, Hideki Yagi

２．発表標題
The Shannon cipher system with causal disclosure over separate noisy channel

３．学会等名
Proc. of 2020 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2020)（国際学会）

４．発表年
2020年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
Identification, secrecy, template, and privacy-leakage of biometric identification system under noisy enrollment

３．学会等名
Proc. of 2019 IEEE Int. Symposium on Information Theory (ISIT2019)（国際学会）

４．発表年
2019年

１．発表者名
Ryo Nomura, Hideki Yagi

２．発表標題
Optimum source resolvability rate with respect to f-divergence and smooth Renyi entropy

３．学会等名
Proc. 2019 Shannon Theory Workshop (STW2019)

４．発表年
2019年

１．発表者名
Qipeng Wu, Hideki Yagi

２．発表標題
The Shannon cipher system over noisy channel with causal disclosure

３．学会等名
Proc. 2019 Symposium on Information Theory and its Applications (SITA2019)

４．発表年
2019年

１．発表者名
Naruaki Amada, Hideki Yagi

２．発表標題
A single-letter characterization for the minimum cost of information erasure under restriction on the output distribution

３．学会等名
Proc. 2019 Symposium on Information Theory and its Applications (SITA2019)

４．発表年
2019年

１．発表者名
Lingyun Chen, Vamoua Yachongka and Hideki Yagi

２．発表標題
Sum-capacity region of an SRAM-PUF multi-enrollment rate-constrained system

３．学会等名
Proc. 2019 Symposium on Information Theory and its Applications (SITA2019)

４．発表年
2019年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
A new characterization of the capacity region of biometric identification system under noisy enrollment

３．学会等名
Proc. 2019 Symposium on Information Theory and its Applications (SITA2019)

４．発表年
2019年

１．発表者名
Qipeng Wu, Hideki Yagi

２．発表標題
The Shannon cipher system over noisy channel with causal disclosure

３．学会等名
2019 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2019)（国際学会）

４．発表年
2019年

１．発表者名
Lingyun Chen、Vamoua Yachongka、Hideki Yagi

２．発表標題
On the capacity region of an SRAM-PUF 2-enrollment rate-constrained system without cell-permutation symmetry

３．学会等名
2019 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2019)（国際学会）

４．発表年
2019年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
Fundamental trade-off among identification, secrecy and template rates in identification system

３．学会等名
2018 Int. Symposium on Information Theory and its Applications (ISITA2018)（国際学会）

４．発表年
2018年

１．発表者名
Tomoya Hamada, Hideki Yagi

２．発表標題
A new bound of (r,\delta)-locally repairable codes over finite field of small order

３．学会等名
2018 Int. Symposium on Information Theory and its Applications (ISITA2018)（国際学会）

４．発表年
2018年

１．発表者名
Ryo Nomura, Hideki Yagi

２．発表標題
Overflow probability of codeword cost in variable-length coding problem allowing non-vanishing error probability

３．学会等名
2018 Int. Symposium on Information Theory and its Applications (ISITA2018)（国際学会）

４．発表年
2018年

１．発表者名
Shota Saito, Hideki Yagi, Toshiyasu Matsushima

２．発表標題
New results on variable-length lossy compression allowing positive overflow and excess distortion probabilities

３．学会等名
2018 Int. Symposium on Information Theory and its Applications (ISITA2018)（国際学会）

４．発表年
2018年

１．発表者名
Toshihiro Niinomi, Hideki Yagi, Shigeichi Hirasawa

２．発表標題
Decision feedback scheme with criterion LR+Th for the ensemble of linear block codes

３．学会等名
2018 Int. Symposium on Information Theory and its Applications (ISITA2018)（国際学会）

４．発表年
2018年

１．発表者名
Gendo Kumoi, Hideki Yagi, Manabu Kobayashi, Masayuki Goto, Shigeichi Hirasawa

２．発表標題
A greedy construction approach of codeword table on error correcting output coding for multivalued classification and its evaluation by using artificial data

３．学会等名
2018 Int. Conf. on Engineering, Technology, and Applied Sciences (ICETA2018)（国際学会）

４．発表年
2018年

１．発表者名
Hideki Yagi, Te Sun Han

２．発表標題
Variable-length resolvability for mixed sources and its application to variable-length source coding

３．学会等名
2018 IEEE Int. Symposium on Information Theory (ISIT2018)（国際学会）

４．発表年
2018年

１．発表者名
Hideki Yagi, Te Sun Han

２．発表標題
Variable-length channel resolvability for discrete memoryless sources and channels

３．学会等名
2018 IEEE Int. Symposium on Information Theory (ISIT2018)（国際学会）

４．発表年
2018年

１．発表者名
Hideki Yagi, Shigeichi Hirasawa

２．発表標題
Error exponent analysis for biometric identification systems with nonlegitimate entities

３．学会等名
第41回情報理論とその応用シンポジウム

４．発表年
2018年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
Fundamental trade-off among identification, secrecy, template, and privacy-leakage rates in biometric identification system

３．学会等名
第41回情報理論とその応用シンポジウム

４．発表年
2018年

１．発表者名
藤田隆寛，八木秀樹

２．発表標題
2つの秘匿メッセージを有する放送型通信路において強安全性を達成するポーラ符号の構成

３．学会等名
第41回情報理論とその応用シンポジウム

４．発表年
2018年

１．発表者名
濱田寛也，八木秀樹

２．発表標題
(r,δ)-Locally Repairable符号の次元の上界式の改善

３．学会等名
第41回情報理論とその応用シンポジウム

４．発表年
2018年

１．発表者名
濱田寛也，八木秀樹

２．発表標題
Locally Repairable 符号の次元に関する上界式の改善

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2018年

１．発表者名
天田成昭，八木秀樹

２．発表標題
定常無記憶情報源に対する情報消失システムにおける最小コスト

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2018年

１．発表者名
Yuming Yang and Hideki Yagi

２．発表標題
A simple proof of polarization for memoryless sources with and without side information

３．学会等名
2018 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2018)（国際学会）

４．発表年
2018年

１．発表者名
Takahiro Fujita and Hideki Yagi

２．発表標題
Polar codes achieving strong secrecy for broadcast channel with confidential messages

３．学会等名
2018 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2018)（国際学会）

４．発表年
2018年

１．発表者名
Tomoya Hamada and Hideki Yagi

２．発表標題
Construction of locally repairable codes with multiple localities based on encoding polynomial

３．学会等名
2018 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2018)（国際学会）

４．発表年
2018年

１．発表者名
Vamoua Yachongka and Hideki Yagi

２．発表標題
Fundamental tradeoff among identification, secrecy and compression rates in biometric identification system

３．学会等名
2018 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2018)（国際学会）

４．発表年
2018年

１．発表者名
Brian M. Kurkoski, Hideki Yagi

２．発表標題
Single-bit quantization of binary-input, continuous-output channels

３．学会等名
2017 IEEE Int. Symposium on Information Theory (ISIT2017)（国際学会）

４．発表年
2017年

１．発表者名
Hideki Yagi, Te Sun Han

２．発表標題
Variable-length resolvability for general sources

３．学会等名
2017 IEEE Int. Symposium on Information Theory (ISIT2017)（国際学会）

４．発表年
2017年

１．発表者名
Shota Saito, Hideki Yagi, Toshiyasu Matsushima

２．発表標題
Variable-length lossy compression allowing positive overflow and excess distortion probabilities

３．学会等名
2017 IEEE Int. Symposium on Information Theory (ISIT2017)（国際学会）

４．発表年
2017年

１．発表者名
稲葉顕則，八木秀樹

２．発表標題
強安全性条件とコスト制約を課した双方向放送型通信路

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2018年

１．発表者名
楊 玉明，八木秀樹

２．発表標題
定常無記憶情報源に対するポーラ分極の簡潔な証明と非定常無記憶情報源への拡張

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2018年

１．発表者名
吉岡佑起，八木秀樹

２．発表標題
レート分割法に基づく強干渉通信路に対する格子符号

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2018年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
The capacity region of identification, secrecy and compression rates in biometric identification systems

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2018年

１．発表者名
雲居玄道，三川健太，八木秀樹，後藤正幸，平澤茂一

２．発表標題
人口データを用いた誤り訂正符号に基づく多値分類法における符号語表構成に関する一考察

３．学会等名
第40回情報理論とその応用シンポジウム

４．発表年
2017年

１．発表者名
雲居玄道，八木秀樹，後藤正幸，平澤茂一

２．発表標題
符号理論の観点による二値判別器の相関に着目した多値文書分類のための符号語構成法

３．学会等名
情報処理学会 数理モデル化と問題解決研究会

４．発表年
2017年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
Biometric identification system with protected templates under noisy enrollment

３．学会等名
電子情報通信学会 2017年基礎・境界ソサイエティ／NOLTAソサイエティ大会

４．発表年
2017年

１．発表者名
野村亮，八木秀樹

２．発表標題
微少な誤り確率を許容する可変長符号化における楽観的符号化定理

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2017年

１．発表者名
平澤茂一，八木秀樹，小林学，笠原正雄

２．発表標題
ユニットメモリトレリス符号により構成されたブロック符号の誤り指数

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2017年

１．発表者名
藤田隆寛，八木秀樹

２．発表標題
秘匿メッセージを有する放送型通信路において強安全性を達成するポーラ符号の構成

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2017年

１．発表者名
濱田寛也，八木秀樹

２．発表標題
符号化多項式を用いた多重局所性を持つLocally Repairable符号の構成法

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2017年

１．発表者名
Hideki Yagi

２．発表標題
Channel resolvability theorems for general sources and channels

３．学会等名
2017 IEEE Int. Symposium on Information Theory (ISIT2017)（国際学会）

４．発表年
2017年

１．発表者名
Yuki Yoshioka, Hideki Yagi

２．発表標題
Lattice codes for Gaussian broadcast channel with a common message

３．学会等名
2017 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2017)（国際学会）

４．発表年
2017年

１．発表者名
Akinori Inaba, Hideki Yagi

２．発表標題
Capacity region of Gaussian bidirectional broadcast channel with common and confidential messages

３．学会等名
2017 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2017)（国際学会）

４．発表年
2017年

１．発表者名
Hideki Yagi, Ryo Nomura

２．発表標題
Variable-length coding with cost allowing non-vanishing error probability

３．学会等名
2016 Int. Symposium on Information Theory and its Applications (ISITA2016)（国際学会）

４．発表年
2016年

１．発表者名
Vamoua Yachongka, Hideki Yagi

２．発表標題
Reliability function and strong converse of biometrical identification systems

３．学会等名
2016 Int. Symposium on Information Theory and its Applications (ISITA2016)（国際学会）

４．発表年
2016年

１．発表者名
Ryo Nomura, Hideki Yagi

２．発表標題
Variable-length lossy source coding allowing some probability of union of overflow and excess distortion

３．学会等名
2016 IEEE Int. Symposium on Information Theory (ISIT2016)（国際学会）

４．発表年
2016年

１．発表者名
野村　亮，八木秀樹

２．発表標題
微少な誤り確率を許容する可変長符号化におけるオーバーフロー確率について

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2017年

１．発表者名
Hideki Yagi

２．発表標題
Optimistic channel resolvability and the strong converse property

３．学会等名
第39回情報理論とその応用シンポジウム(SITA2016)

４．発表年
2016年

１．発表者名
八木秀樹

２．発表標題
Channel resolvability over single and compound channels

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2016年

１．発表者名
吉岡佑起，八木秀樹

２．発表標題
共通メッセージを有するガウス型放送通信路に対する格子符号

３．学会等名
電子情報通信学会 情報理論研究会

４．発表年
2016年

| |
|---|
| １．発表者名<br>稲葉顕則，八木秀樹 |
| ２．発表標題<br>出力アルファベットを拡張した双方向放送型通信路におけるポーラ符号の構成 |
| ３．学会等名<br>電子情報通信学会 情報理論研究会 |
| ４．発表年<br>2016年 |

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
|---|---|