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　４ 年　 ６ 月　 １ 日現在

機関番号：１２７０１
研究種目：若手研究
研究期間：2019～2021
課題番号：１９Ｋ１４９８７

研究課題名（和文）高速周波数ホッピングのテンソル遅延検波による低干渉な無線秘匿通信

研究課題名（英文）Differential-encoding aided physical-layer security

研究代表者
石川　直樹（Ishikawa, Naoki）

横浜国立大学・大学院工学研究院・准教授

研究者番号：００８０１７１３

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：スマートフォン等の無線端末に加え、自動車・医療・インフラ分野の急速な市場拡大にともない、無線通信の需要は世界的に増加傾向にある。限られた公共の資源である無線周波数帯域の効率的利用を可能とする技術としてマルチアンテナ無線通信があり、移動通信システムや無線LAN (local area network) システム等に採用されてきた。2010年頃からはアンテナ本数を大幅に増やす大規模拡張方式が盛んに研究されており、電波干渉を極限まで低減できる特性から、世界的に多くの関心を集めている。

研究成果の学術的意義や社会的意義
研究代表者はこれまでに、大規模アンテナアレイシステムで動作する非同期検波に基づく通信方式「非正方差動符号化」を提案してきた。通信オーバーヘッドと情報漏洩リスクを高める基準シンボルの送信を高速移動体環境においてどこまで減らすことができるだろうか。本研究では非正方差動符号化を発展させ、電波の指向性制御による干渉低減が可能であるか、また、差動符号化による信号点の攪乱が物理層セキュリティの改善に寄与するか、これ2点について理論的側面から検証し、IEEE国際誌筆頭4編、共著2編、その他5編の発表に至った。

研究成果の概要（英文）：The intensive demand for wireless communications has increased worldwide due to the rapid market growth in the automotive, medical, infrastructure sectors, etc. In contrast, the radio spectrum is a public resource that no longer has much room for wireless communications. Multiple-input multiple-output (MIMO) is a representative technology to improve the spectrum efficiency, which has been adopted in typical wireless standards. Since around 2010, its large-scale extension, massive MIMO, has been extensively studied due to its capability to mitigate interference, where the number of transmit antennas is increased as much as possible.

研究分野：通信工学

キーワード：無線通信　物理層セキュリティ　カオス理論　秘密容量　大規模アンテナアレイ　差動符号化　インデックス変調

１．研究開始当初の背景

スマートフォン等の無線端末に加え、自動車・医療・インフラ分野の急速な市場拡大にともない、無線通信の需要は世界的に増加傾向にある。限られた公共の資源である無線周波数帯域の効率的利用を可能とする技術としてマルチアンテナ無線通信があり、移動通信システムや無線 LAN (local area network) システム等に採用されてきた。2010 年頃からはアンテナ本数を大幅に増やす大規模拡張方式 [Marzetta IEEE TWC2010] が盛んに研究されており、電波干渉を極限まで低減できる特性から、世界的に多くの関心を集めている。

研究代表者はこれまでに、大規模アンテナアレイシステムで動作する非同期検波に基づく通信方式を提案してきた [Ishikawa+ IEEE TWC2017, Ishikawa+ IEEE TCOM2018]。電波伝搬係数の推定を不要とする非同期な差動符号化方式は、古くは 2000 年頃から提案されているが、正方のユニタリ行列を用いる必要があるためアンテナ数の増加とともに指数関数的に複雑化する。例えば、送信アンテナ本数 4 本かつ送信レートが 1 シンボル時間あたり 4 ビットという、MIMO 空間多重システムでは容易に実現できる場合であっても、差動符号化では2^{16}種類の4×4複素行列を事前に設計する必要がある。この問題を解決するため、代表者は正方行列を非正方行列に射影するという独自のコンセプト（図 1）を提案してきた。特に、M本のアンテナを用いる場合に時間計算量と空間計算量の両方を$1/2^{M}$程度に削減できる。

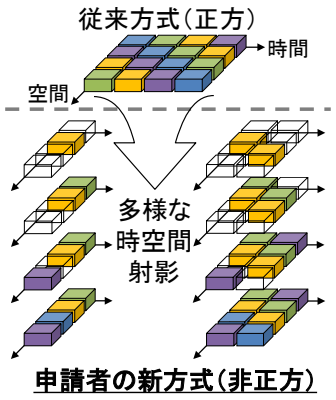


図 1　非正方差動符号化

同方式の課題として以下の 2 点がある。

課題 1　電波干渉　現代の無線通信では大量のデータトラフィックを時間・空間・周波数の高度なスケジューリングにより支えている。異なる端末が異なる時間スロット・周波数スロットにおいて通信し、電波の指向性を制御して空間的に分離する。スケジューリングにおいて、基地局は各携帯端末の電波伝搬環境を定期的に推定し、この負担は実効スループットを低下させている。非正方差動符号化では電波伝搬係数の推定を不要にできる一方で、それらの情報が入手できないため、スケジューリング、適応符号化、指向性制御（ビームフォーミング）などの点で課題を抱えている。特に、ミリ波通信環境においてビームフォーミングは必要不可欠である。

課題 2 低セキュリティ　無線通信において信号波の漏洩は本質的に避けられない。無線 LAN 等の小電力無線であっても、見通しを確保できれば 100m 程度は電波を観測できる。現在普及している無線通信規格において、物理層では通信内容を表現するデータシンボルが暗号化されていない。つまり、定期的にやり取りされる基準シンボルを元に、第三者がデータシンボルを推定可能である。他のレイヤで高度な暗号化が施されているために通信内容の復号は困難であるが、現在の最新技術で暗号化済みのビット系列であっても、数十年後のスーパーコンピュータや量子コンピュータを用いれば解読可能となる恐れがある。リスクを高める基準シンボルのやり取りを出来る限り減らし、無線端末の負担を軽減したままデータシンボル自体を秘匿する必要がある。

２．研究の目的

本研究では、オーバーヘッドとリスクを高める基準シンボルの送信をできる限り減らす。非正方差動符号化方式であっても、指向性制御による干渉低減が可能であるか、また、差動符号化による信号点の攪乱が物理層セキュリティの改善に寄与するか、これらの検証を目的とする。

３．研究の方法

代表者の従来方式である非正方差動符号化を発展させ、ミリ波 MIMO-OFDM など電波の指向性制御が必要不可欠な環境で評価する。このような環境でも従来技術に対する優位性を確認できたら、次は物理層セキュリティ方式として発展させられるか検討する。差動符号化は構成によっては符号語の位数が発散することが分かっており [Xu+ IEEE TCOM2019]、この特性は機密性の改善に役立てられる可能性がある。符号語の非ゼロ成分数を制限することで、アンテナホッピングや周波数ホッピングに対応できるよう工夫し、秘密容量の観点で安全性を評価する。

４．研究成果

[成果 1] 課題 1 と対応して、非正方差動符号化方式を時変性ミリ波チャネルにおいて評価した。S/N 比のフィードバックに基づくアナログビームフォーミングを前提に、ミリ波 MIMO-OFDM チャネルをテンソルにより表現し（図 2）、同シナリオに適した符号語の構成法を提案した。具体的には、グラムシュミットの直

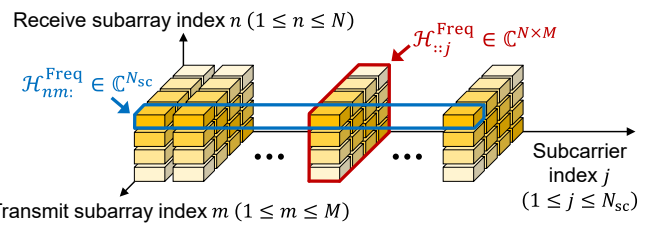
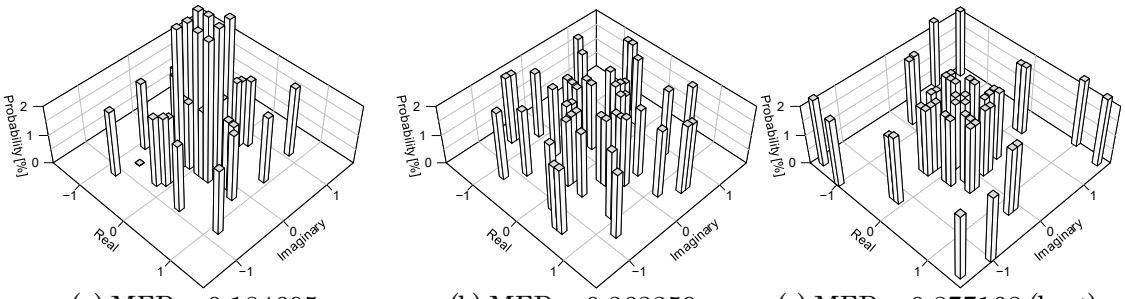


図 2　テンソルにより表現した MIMO-OFDM チャネル (c) IEEE [Ishikawa+ IEEE JSTSP2019]



(a) MED = 0.184695. (b) MED = 0.363259. (c) MED = 0.877168 (best).

図 3　非ゼロ成分密度を調整可能な符号語　(c) IEEE [Ishikawa+ IEEE JSTSP2019]

交化法により、符号語の非ゼロ成分密度を調整可能とし、電波の直進性が強いためチャネル行列の階数が低下する傾向にあるミリ波環境でも低いビット誤り率を達成できるように工夫した。非ゼロ成分数に制約を設けることで、図 3 のようにらせん状の信号点が現れる。また、適応検出器が高速移動環境特有の位相ずれを緩和可能であることを明らかにした。通信環境によっては、通信オーバーヘッドの大きい同期検出に漸近する性能を達成できる点を特徴としている。本成果は IEEE Journal of Selected Topics in Signal Processing (IF=6.856) の特集号に投稿し、採録に至った。

[成果 2] [成果 1]の提案方式について、エラー伝搬も含めた平均ビット誤り率の代数的解析に成功した [Xiao+ IEEE TCOM2020]。非正方差動符号化はエラー伝搬の影響を受けるため、一般に誤り率の解析は困難である。ここで、送信符号語を制限した場合に限り、場合分けが単純になり導出が可能となった。また、検出処理の時間計算量を 75～97%程度削減可能な軽量検出器を提案した。順列行列のパターンおよび送信シンボルを閉形式で計算することで簡易化を可能とした。解析がより難しいアンテナホッピングの場合を対象としているが、サブキャリアホッピングの場合に容易に拡張できる。

[成果 3] 課題 2 と対応して、本論文では、カオス理論に基づく時変性ユニタリ行列を提案し、[成果 1]と同様に符号語を構成した [Ishikawa+ IEEE OJ-COMS2021]。[成果 1]で得た知見を応用し、対角ユニタリ符号を用いることで、送信インデックスに応じて信号点の位数を指数関数的に増やすことができる。提案法の攻撃アルゴリズムを考案し、第三者による検出は困難である可能性が高いことを示した。また、提案法の秘密容量を導出し、図 4 に示すように、対角ユニタリ符号の信号点を増やすほど単調に改善することを明らかにした。さらに、提案する時変性ユニタリ行列は共有した秘密鍵にごくわずかな誤りがある場合、正規受信者はカオス系列による適応補正法が可能となる一方で、第三者は位相不確定性のために復号できない特性を明らかにした。

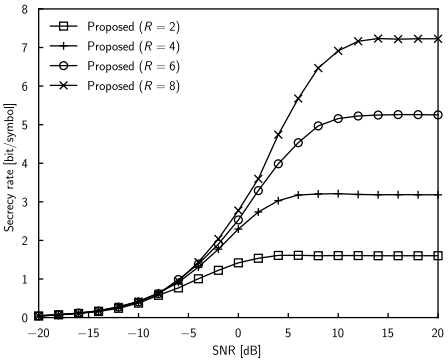


図 4　提案法の秘密容量 (c) IEEE [Ishikawa+ IEEE OJ-COMS2021]

[成果 4] [成果 3]で提案した時変性ユニタリ行列に基づく通信方式の性能限界を解析した [Zhai+ IEEE WCL2022]。具体的には、一般化レイリーフェージングを仮定し、積率母関数を用いて平均ビット誤り率の上界と下界の導出に成功した。

[成果 5] 以上の成果に関連して、ビット誤り率や平均相互情報量をシミュレーション可能なオープンソースソフトウェアを開発した。モンテカルロシミュレーションやモンテカルロ積分をテンソル演算として記述することで、CPU だけでなく GPU においても高速に実行できる。本成果は単著のジャーナル論文として発表した [Ishikawa IEEE Access2019]。

[成果 6] [成果 3]の提案方式を対象に、量子計算機による攻撃アルゴリズムを検討する過程で、量子計算と無線通信の間に類似性を見出した。インデックス変調に代表されるスパース符号化はオン（1）とオフ（0）で情報を表現するため、量子重ね合わせと量子もつれを利用する量子計算と相性がよい。インデックス変調の符号語最適化問題を、グローバー適応探索と呼ばれる量子アルゴリズムにより求解する方法を着想したため、単著のジャーナル論文として発表した [Ishikawa IEEE Access2021]。

以上、IEEE 国際誌筆頭 4 編、共著 2 編、その他 5 編の採録に至ったのは、科研費若手のご支援に加え、若手として職務に集中できる環境が整っていたおかげであり、深く感謝している。

５．主な発表論文等

〔雑誌論文〕　計11件（うち査読付論文　11件／うち国際共著　9件／うちオープンアクセス　5件）

１．著者名 Lixia Xiao, Pei Xiao, Hang Ruan, Naoki Ishikawa, Lei Lu, Yue Xiao, Lajos Hanzo	４．巻 68
２．論文標題 Differentially-Encoded Rectangular Spatial Modulation Approaches the Performance of Its Coherent Counterpart	５．発行年 2020年
３．雑誌名 IEEE Transactions on Communications	６．最初と最後の頁 7593-7607
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCOMM.2020.3021117	査読の有無 有
オープンアクセス 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 該当する

１．著者名 Chao Xu, Yifeng Xiong, Naoki Ishikawa, Rakshith Rajashekar, Shinya Sugiura, Zhaocheng Wang, Soon Ng, Lie-Liang Yang, and Lajos Hanzo	４．巻 -
２．論文標題 Space-, Time-and Frequency-Domain Index Modulation for Next-Generation Wireless: A Unified Single-/Multi-Carrier and Single-/Multi-RF MIMO Framework	５．発行年 2021年
３．雑誌名 IEEE Transactions on Wireless Communications	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TWC.2021.3054068	査読の有無 有
オープンアクセス 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 該当する

１．著者名 Chao Xu, Naoki Ishikawa, Rakshith Rajashekar, Shinya Sugiura, Robert G. Maunder, Zhaocheng Wang, Lie-Liang Yang, Lajos Hanzo	４．巻 7
２．論文標題 Sixty Years of Coherent Versus Non-Coherent Tradeoffs and the Road From 5G to Wireless Futures	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 178246-178299
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2957706	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 該当する

１．著者名 Rakshith Rajashekar, Chao Xu, Naoki Ishikawa, Lie-Liang Yang, Lajos Hanzo	４．巻 68
２．論文標題 Subcarrier Subset Selection-Aided Transmit Precoding Achieves Full-Diversity in Index Modulation	５．発行年 2019年
３．雑誌名 IEEE Transactions on Vehicular Technology	６．最初と最後の頁 11031-11041
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TVT.2019.2942634	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Naoki Ishikawa, Rakshith Rajashekar, Chao Xu, Mohammed El-Hajjar, Shinya Sugiura, Lie-Liang Yang, Lajos Hanzo	4．巻 13
2．論文標題 Differential-Detection Aided Large-Scale Generalized Spatial Modulation is Capable of Operating in High-Mobility Millimeter-Wave Channels	5．発行年 2019年
3．雑誌名 IEEE Journal of Selected Topics in Signal Processing	6．最初と最後の頁 1360-1374
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSTSP.2019.2913130	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Chao Xu, Peichang Zhang, Rakshith Rajashekar, Naoki Ishikawa, Shinya Sugiura, Zhaocheng Wang, Lajos Hanzo	4．巻 37
2．論文標題 “Near-Perfect” Finite-Cardinality Generalized Space-Time Shift Keying	5．発行年 2019年
3．雑誌名 IEEE Journal on Selected Areas in Communications	6．最初と最後の頁 2146-2164
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSAC.2019.2929450	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Naoki Ishikawa	4．巻 7
2．論文標題 IMToolkit: An Open-Source Index Modulation Toolkit for Reproducible Research Based on Massively Parallel Algorithms	5．発行年 2019年
3．雑誌名 IEEE Access	6．最初と最後の頁 93830-93846
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2928033	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 Rakshith Rajashekar, Chao Xu, Naoki Ishikawa, Lie-Liang Yang, Lajos Hanzo	4．巻 7
2．論文標題 Multicarrier Division Duplex Aided Millimeter Wave Communications	5．発行年 2019年
3．雑誌名 IEEE Access	6．最初と最後の頁 100719-100732
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2930333	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 該当する

1．著者名 Naoki Ishikawa	4．巻 9
2．論文標題 Quantum Speedup for Index Modulation	5．発行年 2021年
3．雑誌名 IEEE Access	6．最初と最後の頁 111114-111124
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2021.3103207	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 Naoki Ishikawa, Jehad M. Hamamreh, Eiji Okamoto, Chao Xu, Lixia Xiao	4．巻 2
2．論文標題 Artificially Time-Varying Differential MIMO for Achieving Practical Physical Layer Security	5．発行年 2021年
3．雑誌名 IEEE Open Journal of the Communications Society	6．最初と最後の頁 2180-2194
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/OJCOMS.2021.3112486	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 該当する

1．著者名 Xiaodan Zhai, Guochao Song, Lixia Xiao, Guanghua Liu, Naoki Ishikawa, Tao Jiang	4．巻 -
2．論文標題 Error Probability Analysis for Time-Varying Chaos Unitary Matrix based Differential MIMO System	5．発行年 2022年
3．雑誌名 IEEE Wireless Communications Letters	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LWC.2022.3170873	査読の有無 有
オープンアクセス 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 該当する

〔学会発表〕　計1件（うち招待講演　1件／うち国際学会　0件）

1．発表者名 石川 直樹
2．発表標題 今日から使えるインデックス変調
3．学会等名 第26回フォトニックネットワークチュートリアル講演会（招待講演）
4．発表年 2021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

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			
英国	University of Southampton	University of Surrey		
インド	Broadcom			
中国	精華大学	華中科技大学	電子科技大学	