様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　　６　日現在

機関番号：　３２６６０
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５４２０３８６

研究課題名（和文）カオス符号系列を用いた高セキュリティ光CDMA

研究課題名（英文）High Security Optical CDMA Using Chaotic sequence codes

研究代表者

八嶋　弘幸（Yashima, Hiroyuki）

東京理科大学・工学部・教授

研究者番号：３０２３０１９７

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：本研究では光CDMAシステムにおいて、情報セキュリティ機能を高めるため、従来のユーザ符号に換えてカオス系列に基づくユーザ符号を用いた光CDMAを提案し、多重度、誤り率等の基礎特性を求めるとともに、情報セキュリティ効果について検討し、提案システムに有効性を明らかにした．また、連続するMAIの影響を考慮した光CDMAの特性についても解析し、平均値のみの従来法に比べ、実際の誤り率の推移を求め、干渉量の初期値によりその後の誤り率が大きく異なることを示した．

研究成果の概要（英文）：We propose new Optical Code-Division-Multiple-Access (OCDMA) systems using Extended Chaotic Binary Codes (ECBCs) obtained easily from the extended Bernoulli map. Unlike conventional sequence codes, ECBCs are composed by the map for every information bit, which means that the sequence code varies bit by bit. Therefore, high security against eavesdroppers is expected. Then, we derive the expression for theoretical BER versus the number of simultaneous users of the proposed system and verify that the proposed system is effective in OCDMA system through numerical results. Moreover, we derive BER of OCDMA based on the persistence of MAI, by considering the transition of the interfering users as Markov chain process. From the numerical analysis, the derived BER differs substantially from conventional analysis. We show that the derived BER strongly depends on the initial number of interfering users.

研究分野：　情報通信における光CDMA

キーワード：　光CDMA　カオス　セキュリティ　多元接続干渉　光直交符号　マルコフ連鎖モデル

１．研究開始当初の背景

現代社会においては情報セキュリティは極めて重要なものとなっている．光CDMA(Code Division Multiple Access)は信号が多重化されているため，ユーザ符号を検出されない限り，ある程度情報の機密性は保てるが，一旦，第三者にユーザ符号を検出されると情報の機密性は全くない．これまで光CDMAは機密性がある通信方式であると考えられてきたが，光CDMAのセキュリティ機能に関する研究はあまり行われていなかった．

これまで光CDMAの解析においては、多元接続干渉(Multiple Access Inter- ference : MAI)が連続する信号に対し、同様の干渉をもたらす確率が高いにもかかわらず，これらの性質ついては考慮されていなかった．

２．研究の目的

本研究では、光CDMAシステムにおいて、情報セキュリティ機能を高めるため，従来のユーザ符号に換えてカオス系列に基づくユーザ符号を用いた光CDMAを提案する．提案システムにおいて，多重度，誤り率等の基礎特性を求めるとともに，情報セキュリティ効果について検討し，提案システムの有効性を明らかにする．

また、他ユーザからの干渉の連続性を考慮し，連続するMAIの影響を考慮した光CDMAの誤り率特性についても解析する．

３．研究の方法

（１）本研究ではセキュリティ機能が高く，高多重度の光CDMAを実現するため，カオス写像に基づく２値系列をユーザ符号として用いる光CDMAシステムを提案する．まず，いくつかのカオス写像から発生させた符号系列の統計的性質と自己相関特性および相互相関特性を求め，光CDMAに適した符号系列を選定する．次に，提案した符号を光CDMAに適用し、誤り率特性、多重度等の基礎特性を求める。さらに機密性を高めるため，”0”と”1”の情報に対し，符号の重みの等しい等重み光CDMAシステムを提案し，セキュリティ強度を検証する．以上のように，提案する光CDMAの諸特性を求めて提案法の有効性を示す．

（２）次に，光CDMAにおいて，MAIの影響が持続することを考慮したBERの解析を行う．光CDMAシステムにおいてMAIは他のユーザが与える干渉であるため，各ユーザの送信タイミングが変化するまで所望ユーザが受けるMAIの影響は持続する．特にパケット通信のような短時間で送信が終了する通信の場合，MAIの持続が各パケット内のBERに与える影響が大きい．そこで本論文では，所望ユーザに対する干渉ユーザ数をマルコフ連鎖モデルの各状態とおき，各送信時点ごとのMAIの影響を求めることにより，MAIの持続性を考慮したBERを導出する．その結果，所望ユーザの送信開始時点の干渉ユーザ数によって送信区間内のBERは従来求められていたBERと大きく異なる場合があることを示す．

４．研究成果

（１）一次元写像から生成されるカオス2値符号(Chaotic Binary Code: CBC)を用いた光CDMA通信システムを提案した．まず，拡張ベルヌーイ写像(Extended Bernoulli Map)から生成されるCBC，すなわち拡張カオス2値符号(Extended Chaotic Binary Code: ECBC)を光CDMAのユーザ符号として用いる．従来の光CDMAが連続する送信ビットに同一の符号を繰り返し用いていたのに対し，提案方式はECBCから生成される符号系列を用いて各送信ビット毎に異なる符号を用いる方式である．このため，盗聴者が送信ビット毎の符号を抽出することが困難となり，信号の盗聴が困難になる．

OOCやプライム符号を用いた従来システムとの比較を行い，提案システムの有効性を示す．このとき，符号長F, 重みWのOOCを(F, W)OOCと表す．ここで，ビット誤りを引き起こす要因はMAIのみとし，光ファイバの特性や受光素子などによる影響は無視した． コンピュータシミュレーションを行い，得られたビット誤り率と導出した理論値との比較を行った．

(F,W)ECBCの重みWを変化させたときの提案システムのビット誤り率特性について検討した．図１に，F=300の(F,W)ECBCの重みWを変化させたときの同時接続ユーザ数Nに対するビット誤り率特性を示す．重みWを増やすと接続ユーザ数Nが少ない状況下では優れたビット誤り率特性を示し，ユーザ数が多くなると徐々に劣化することがわかる．図１では，(300,10)ECBCはN = 15のときに(300,6)ECBCと，N = 19のときに(300,4)ECBCと，N = 22のときに(300,3)ECBCのビット誤り率にとほぼ等しくなることが確認できる．以上から，接続ユーザ数Nが多い状況下では重みWを小さく設定し，接続ユーザ数Nが

少ない状況下では大きく設定する必要があることがわかる. (F,W)ECBC はOOC と同様, 符号長 F, 重み W という 2 つのパラメータを有し，更には多重度に制限がないため，設計の柔軟性が極めて高い符号であるといえる. また，提案方式のセキュリティについては、すべての信号を第三者が受信したときの相互情報量を求めることにより評価し、優れたセキュリティ効果を有することを確認した.

（２）本研究では, 光 CDMA 方式において, MAI の影響が持続することを考慮した BER の解析を行った．光 CDMA システムにおいて MAI は他のユーザが与える干渉であるため，各ユーザの送信タイミングが変化するまで所望ユーザが受ける MAI の影響は持続する．特にパケット通信のような短時間で送信が終了する通信の場合, MAI の持続が各パケット内の BER に与える影響が大きい．そこで本研究では，所望ユーザに対する干渉ユーザ数をマルコフ連鎖モデルの各状態とおき, 各送信時点ごとの MAI の影響を求めることで, MAI の持続性を考慮した BER を導出した.

本研究で導出した理論式の妥当性を示すため計算機シミュレーションの結果と比較した．比較に用いたパラメータは(F;W;N) = (100; 3; 4); (300; 5; 7)，1 パケットのデータビット数を D = 1200 とする．シミュレーションにおいては，所望ユーザの送信開始時点の干渉ユーザ数が異なるように他ユーザの送信タイミングを設定し、所望ユーザの送信開始時点での他ユーザの送信ビット数を，それぞれ 1 から D ビットの内からランダムに設定した．以上の設定で送信開始時点から $j(1 <= j <= D)$ビット経過後の所望ユーザのビット誤りをカウントし，十分な回数を繰り返し各送信時点における BER を導出した. 図２は導出した BER の理論値とシミュレーションで得られた結果との比較である．図２より光ハードリミタ(OHL) の有無にかかわらずシミュレーション値と理論値がよく一致していることがわかる.

本解析手法を用いることにより送信パケット内での BER の変化や, 送信開始時点の干渉値の差による各送信時点における BER の違いが明らかになった．これにより従来法により求められた長時間の平均による BER とパケット内の各ビットの BER は, 送信開始時点の干渉値の差に依存して大きく異なることを示した.

図３はOHLを用いないとき，パラメータを $(F;W;N)$ = (300; 5; 7)，送信開始時点の干渉ユーザ数を M_1 = 0; 1; 5; 6 としたときの各送信時点 j におけるBER である．図３より，M_1の値によってBER が大きく異なっていることがわかる．M_1 が小さい場合と大きい場合を比較すると，jが大きくなるにしたがってBER の差は小さくなっているが j = 1200 付近においてもBER に大きな差があるとが確認できる. 特に M_1 = 0 と M_1 = 1 を比較すると，送信開始時点の干渉ユーザ数が１違うだけで，送信区間内のBER は常に大きな差が見られることがわかる.

図４はOHLを用いたとき、パラメータを $(F;W;N)$ = (300; 5; 7)，送信開始時点の干渉ユーザ数をそれぞれ$(m_1;1;m_2;1; _ _ _ ;m_W;1)$ = (0; 0; 0; 0; 0)，(1; 0; 0; 0; 0)，(1; 1; 1; 1; 1) としたときの各送信時点j におけるBERである．図４より，OHL を用いていない場合と同様にMAIの初期値によってBER が大きく異なっていることがわかる．また今回用いたパラメータでは，従来の解析法によるBER は10^{-8} 程度となっているが, 送信開始時点の干渉ユーザ数が(1; 1; 1; 1; 1)のときはBER が悪い区間が継続していることがわかる.

以上のように，本研究では光 CDMA システムにおいて，情報セキュリティ機能を高めるため、従来のユーザ符号に換えてカオス系列に基づくユーザ符号を用いた光 CDMA を提案し、多重度，誤り率等の基礎特性を求めるとともに、情報セキュリティ効果、および送受信間での符号同期の問題について検討し，提案システムの有効性を明らかにした．また，連続する MAI の影響を考慮した光 CDMA の特性についても解析し，平均値のみの従来法に比べ，実際の誤り率の推移を求めることができた。

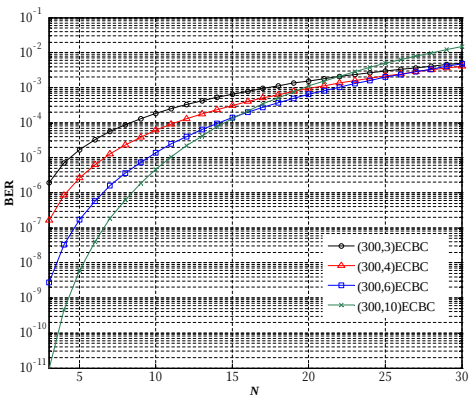

図１: 重み W を変化させたときの ECBC を用いた光 CDMA 通信システムの同時接続ユーザ数 N に対するビット誤り率 (F=300)

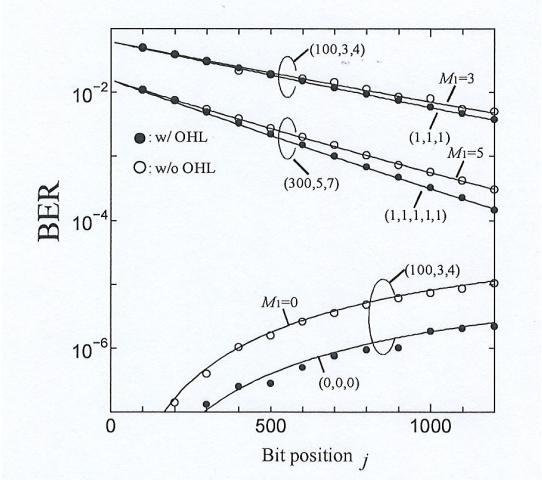

図２ シミュレーション結果および理論値の BER 特性比較$(F;W;N)$ = (100; 3; 4); (300; 5; 7)

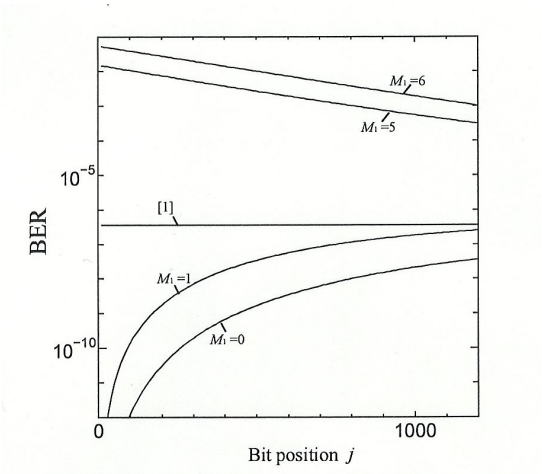

図３ OHL を用いない場合の送信ビット数に対する各送信時点のBER $(F;W;N)$ = (300; 5; 7)

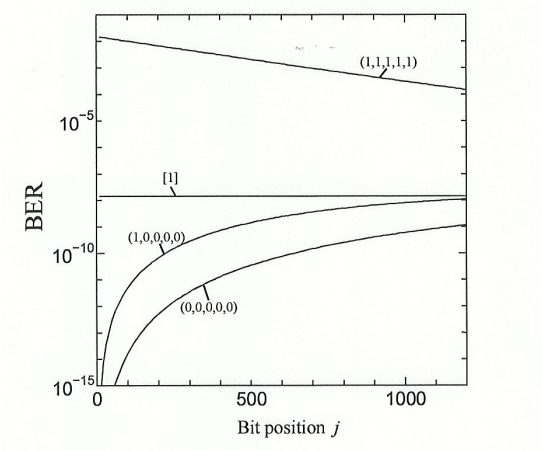

図４OHL を用いた場合の送信ビット数に対する各送信時点のBER $(F;W;N)$ = (300; 5; 7)

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　６件）

[1] 寺尾優史, 細谷 剛, 八嶋弘幸, ``OCDMA における MAI の持続性を考慮した BER の解析," 電子情報通信学会論文誌 (A), vol.J99-A, no.5, pp.185--193, May, 2016.
http://search.ieice.org/bin/summary.php?id=j99-a_5_185&category=&year=2016&lang=J&abst=

[2] G. Hosoya, ``An Improved Iterative Decoding Algorithm of Rate-Compatible Punctured LDPC Codes," Far East Journal of Electronics and Communications, vol.15, no.2, pp.133--149, Dec. 2015.
DOI: 10.17654/FJECDec2015_133_149

[3] 五十嵐保隆, 大野光平, 寺尾優史, 細谷剛, 八嶋弘幸, ``次世代ネットワークを支える暗号, 誤り訂正符号, OCDMA および UWB と情報通信技術の最近の発展動向," 信号処理, vol.18, no.1, pp.1--15, Jan. 2014.
DOI: 10.2299/jsp.18.1

[4] T. Ogihara, K. Mikawa, M. Goto, and G. Hosoya, ``Multi-valued document classification based on generalized Bradley-Terry classifiers utilizing accuracy information," China-USA Business Review, vol.12, No.9, pp.911--917, Sep. 2013.
http://www.davidpublishing.com/show.html?13708

[5] G. Hosoya and H. Yashima, ``Log-likelihood ratio calculation for iterative decoding on Rayleigh fading channels using Pad¥'e approximation," Journal of Applied Mathematics, vol.2013, Article ID 970126, pp.1--10, Aug. 2013.
DOI: 10.1155/2013/970126

[6] G. Hosoya, K. Osada, and M. Goto, ``Rate-compatible punctured LDPC codes with two subgraphs," Far East Journal of Electronics and Communications, vol.10, no.2, pp.83--104, Jun. 2013.
http://www.pphmj.com/abstract/7764.htm

〔学会発表〕（計　２３件）

[1] 柴田 凌, 細谷 剛, 八嶋 弘幸, ``Insertion/Deletion/Substitution 通信路に対する確定シンボルを用いた同期処理法," 電子情報通信学会技術研究報告, vol.115, no.500, IT2015-108, pp.43--48, Mar. 2016.

[2] F. Sato, G. Hosoya, and H. Yashima, ``All-optical NOR gate using XPM and XGM in QD-SOA based MZI," Proc. 2016 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'16), pp.351--354, Honolulu, Hawaii, Mar. 2016.

[3] M. Nishino, G. Hosoya, and H. Yashima, ``All optical CDMA using all optical device," Proc. 2016 RISP International Workshop on

Nonlinear Circuits, Communications and Signal Processing (NCSP'16), pp.359--362, Honolulu, Hawaii, Mar. 2016.

[4] K. Iwamoto, G. Hosoya, and H. Yashima, ``All-optical error correcting system using (7,4) Hamming code," Proc. 2016 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'16), pp.558--561, Honolulu, Hawaii, Mar. 2016.

[5] T. Matsumoto, G. Hosoya, and H. Yashima, ``All Optical error correcting system using horizontal and vertical parity checks," Proc. 2016 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'16), pp.550--553, Honolulu, Hawaii, Mar. 2016.

[6] G. Hosoya and H. Yashima, ``Constellation shaping for non-uniform signals in bit-interleaved coded modulation combined with multi-stage decoding," Proc. 2016 Australian Communications Theory Workshop (AusCTW2016), pp.175--180, Melbourne, Australia, Jan. 2016.

[7] **佐藤文也**, **細谷 剛**, **八嶋弘幸**, ``QD-SOA **における** XPM **と** XGM **を用いた全光** NOR **ゲート**," 2015 **年電子情報通信学会ソサエティ大会**, B-12-2, **仙台**, Sep. 2015.

[8] **吉田光範**, **原田裕生**, **細谷 剛**, **八嶋弘幸**, ``**干渉期間をシフトした** 2 **つの** FSR-MZI **を用いる全光** OFDM **受信機**," 2015 **年電子情報通信学会ソサエティ大会**, B-12-3, **仙台**, Sep. 2015.

[9] Y. Furuya, G. Hosoya, and H. Yashima, ``Noise suppression effects on QD-SOA-based MZI --Simulation Results for Ultrafast Optical Signals--," Proc. 2015 International Workshop on Vision, Communications and Circuits (IWCC'15), pp.71--74, Yokohama, Japan, Oct./Nov. 2015.

[10] Y. Furuya, G. Hosoya, and H. Yashima, ``All-Optical noise suppression by QD-SOA based MZI," Proc. 2015 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'15), pp.122--125, Kuala Lumpur, Malaysia, Mar. 2015.

[11] H. Harada, M. Yoshida, G. Hosoya, and H. Yashima, ``All-Optical OFDM receiver using Odd-Even separator based on double Mach-Zender interferometers and optical switching," Proc. 2015 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'15), pp.130--133, Kuala Lumpur, Malaysia, Mar. 2015.

[12] S. Takeuchi, H. Terao, G. Hosoya, and H. Yashima, ``OCDMA using code shift keying and interference cancellation," Proc. 2015 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'15), pp.138--141, Kuala Lumpur, Malaysia, Mar. 2015.

[13] M. Nishino, H. Terao, G. Hosoya, and H. Yashima, ``Theoretical analysis of OPPM OCDMA with consecutive MAI," Proc. 2015 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'15), pp.567--570, Kuala Lumpur, Malaysia, Mar. 2015.

[14] Y. Taniguchi, G. Hosoya, and H. Yashima, ``Coded modulation with constellation shaping for QAM," Proc. 2015 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP'15), pp.575--578, Kuala Lumpur, Malaysia, Mar. 2015.

[15] G. Hosoya and H. Yashima, ``Box-Plus BP-Based algorithm by linear approximation," Proc. 37th Symposium on Information Theory and its Applications (SITA2014), pp.403--408, Toyama, Japan, Dec. 2014.

[16] G. Hosoya and H. Yashima, ``An improvement of approximate BP decoding," Proc. 2014 International Symposium on Information Theory and its Applications (ISITA2014), pp.186--190, Melbourne, Australia, Oct. 2014.

[17] F. Sato, K. Iwamoto, Y. Furuya, T. Irie, G. Hosoya, and H. Yashima, ``All-Optical AND gate using optical hard limiter with QD-SOA based on self-phase modulation," Proc. 2014 International Symposium on Nonlinear Theory and its Applications (NOLTA2014), pp.213--216, Luzern, Switzerland, Sep. 2014.

[18] K. Iwamoto, F. Sato, Y. Furuya, T. Irie, G. Hosoya, and H. Yashima, ``Multiple connected optical hard limiter and optical power equalizer using Quantum-Dot semiconductor," Proc. 2014 International Symposium on Nonlinear Theory and its Applications (NOLTA2014), pp.304--307, Luzern, Switzerland, Sep. 2014.

[19] T. Irie, G. Hosoya, and H. Yashima, ``8-input all-optical XOR circuit using QD-SOA-Based MZIs and AOWCs," Proc. Optics ¥& Photonics Taiwan, the International Conference 2013 (OPTIC 2013), S0206-O003, Taipei, R.O.C., Dec. 2013.

[20] K. Ogawa, Y. Furuya, T. Irie, G. Hosoya, and H. Yashima, ``All optical NOR gate using QD-SOA based on cross gain modulation," Proc. Optics ¥& Photonics Taiwan, the International Conference 2013 (OPTIC 2013), P0201-P005, Taipei, R.O.C., Dec. 2013.

[21] **寺尾優史**, **細谷 剛**, **八嶋弘幸**, ``**疑似乱数による符号を用いた** CDMA **システムの** BER **特性評価**," **第** 36 **回情報理論とその応用シンポジウム予稿集**, pp.323--328,

静岡, Nov. 2013.
[22] 入江孝憲, 細谷 剛, 八嶋弘幸, ``QD-SOA MZI と全光波長変換器を用いた8入力全光XOR回路,'' 2013年電子情報通信学会ソサエティ大会, B-12-12, 福岡, Sep. 2013.
[23] 古谷侑茉, 小川顕太郎, 入江孝憲, 細谷剛, 八嶋弘幸, ``QD-SOAを用いたXGM型全光NORゲート,'' 2013年電子情報通信学会ソサエティ大会, B-12-13, 福岡, Sep. 2013.

６．研究組織

(1) 研究代表者
八嶋　弘幸(YASHIMA Hiroyuki)
東京理科大学　工学部　情報工学科　教授
研究者番号：３０２３０１９７

(2) 研究分担者
細谷 剛(HOSOYA Gou)
東京理科大学　工学部　情報工学科　助教
研究者番号：６０５１４４０３