大規模MIMOにおけるBP信号検出に対応したカオス暗号へのテント写像の適用

迫田和之[1]・谷口莉菜

Application of Tent Map to Chaotic Encryption in Massive MIMO Using BP Decoding

SAKODA Kazuyuki[1] and TANIGUCHI Rina

(Accepted September 29, 2022)

Abstract　In wireless communications, chaotic encryptions at the physical layer provide enhanced security. Recent study has reported that the chaotic encryption works within a massive MIMO (Multiple-Input Multiple-Output) using Belief-Propagation decoding. However, it is pointed out that the chaos equation used in the previous method is a logistic map, which can be easily incorporated, but is not suitable for an encryption due to the biased distribution of pseudorandom numbers. A chaotic map that can be easily introduced into the previous method is the tent map. The tent map is considered suitable for cryptography because the distribution of pseudorandom numbers is uniform distribution. In this study, we propose a method to introduce a tent map to chaotic encryption. We numerically evaluate decoding accuracy, secrecy capacity and computation time of the proposed method. The results suggest that the proposed method performs as well as or better than the previous method.

Keywords　[Chaos, Encryption, Massive MIMO, BP decoding]

1　序論

近年、PCだけでなく身近な家電もネットワークに繋がることが珍しくなくなっている。それらは無線での接続が主流となりつつあり、無線通信容量の需要は年々拡大している。その傾向に対応した第5世代無線通信サービスにより、莫大な通信量の需要を賄っている。第5世代以降の移動無線通信は、大容量かつ多接続を可能とする大規模MIMO（Multiple Input Multiple Output)が中核技術である[1~4]。大規模MIMOは、第4世代で用いられている複数の送受信アンテナで構成されたMIMOのアンテナ数を、数十～数百本程度まで増やした通信システムである。送受信アンテナ数を増加させることで、多接続と大容量の通信容量を可能とする。しかしながら、アンテナ数を増加させると、受信側での信号検出（受信信号から送信信号を推定する技術）における計算量が増加する。特に、MIMOで用いられる一般的な信号検出である最尤推定法（Maximum Likelihood Detection, MLD）は、アンテナ数に対し指数関数的に計算量が増加し、現実的な計算時間での信号検出が困難である[5,6]。この問題を解決する信号検出法としてBP（Belief Propagation)法を用いた信号検出、BP信号検出がある[7~12]。BP信号検出は、少ない計算量と符号化を施さなくても低い誤り率（BER, Bit Error Rate）であるため、大規模MIMO

1 都城工業高等専門学校電気情報工学科（現 鹿屋体育大学スポーツ情報センター） Department of Electrical and Computer Engineering, National Institute of Technology(KOSEN), Miyakonojo College (Present address: Information Technology Center for Sports Sciences, National Institute of Fitness and Sports in Kanoya)

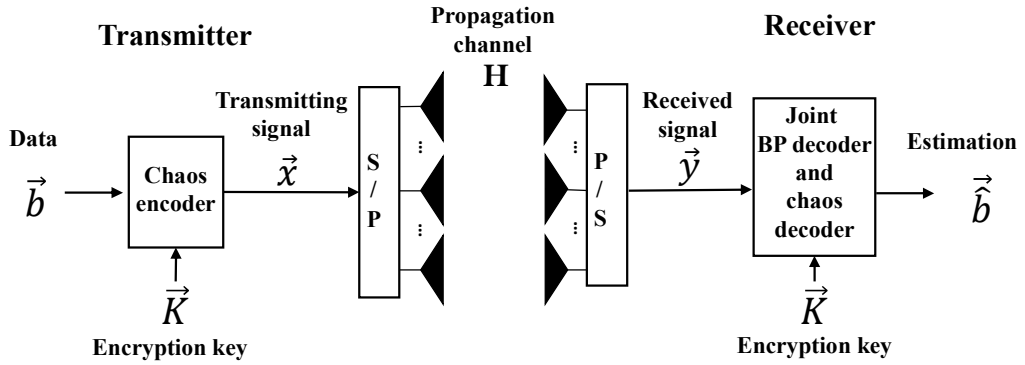

Fig.1 Chaotic encryption and BP decoding applied to massive MIMO

の信号検出として注目されている。

一方、様々なものがネットワークにつながることで、通信容量の課題とは別に、セキュリティの向上も求められている。無線通信でセキュリティを向上させるための暗号技術として、上位レイヤを対象とした AES (Advanced Encryption Standard)などが多いが、近年では下位レイヤである物理レイヤで、暗号化を追加する技術が提案されている [13,14]。物理レイヤでの暗号化は、情報を伝搬する電磁波に指向性を持たせ正規の受信者に電磁波が漏れないようにするビームフォーミング技術や電磁波の位相を乱雑に置き換えて情報を秘匿する技術がある。特に、電磁波の位相をカオス写像により乱雑に置き換えるカオス暗号は、比較的簡易な回路で構築でき、導入への障壁が小さい [15]。カオス暗号を MIMO に適応したカオス MIMO は、復号における精度の高さとセキュリティの高さで注目されている [16,17]。しかしながら、カオス MIMO を大規模 MIMO 化すると、復号に MLD を用いているため、計算量爆発を起こし、現実的な計算量での復号が困難である。そこで、カオス MIMO に BP 信号検出を用い大規模 MIMO 化を可能とする手法（Fig.1）が報告されている [18,19]。これにより、大規模 MIMO の物理レイヤに暗号化を導入でき、セキュリティの向上が見込める。このカオス暗号で用いられるカオス写像は、ロジスティック写像である。ロジスティック写像は、カオスの特性により、疑似乱数を発生させることができるが、その値がとる頻度分布に偏りが存在する（Fig. 2-1）。その偏りにより、暗号化された信号も偏りのある信号となる。暗号化された信号を盗聴者が解読を試みる場合、一般的には疑似乱数に偏りがないため全てのパターンを探索する必要があり、解読が困難となる。信号に偏りが存在すると、発生頻度の高い値から探索することで解読にかかる時間を短縮しうる可能性がある。そのためロジスティック写像は暗号に適していないという指摘がなされている [19]。

そこで本研究では、カオス暗号に、疑似乱数の頻度分布に偏りのないテント写像（Fig. 2-2）を導入する手法を提案し、その性能を数値実験により評価する。2 章では無線通信のシステムモデルと前手法を紹介する。3 章では提案手法を述べる。4 章では提案手法の数値実験結果、5 章では考察とまとめを述べる。

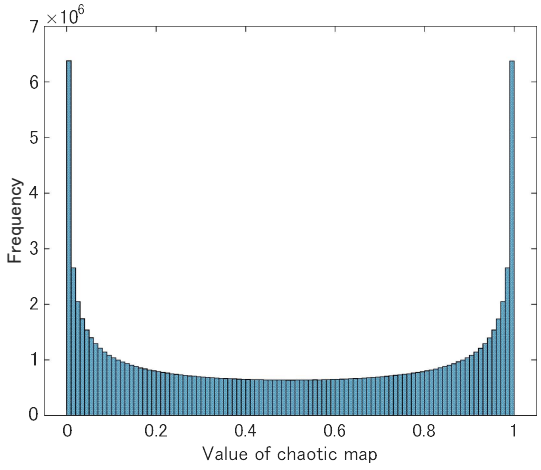

Fig. 2-1 Frequency distribution of the logistic map

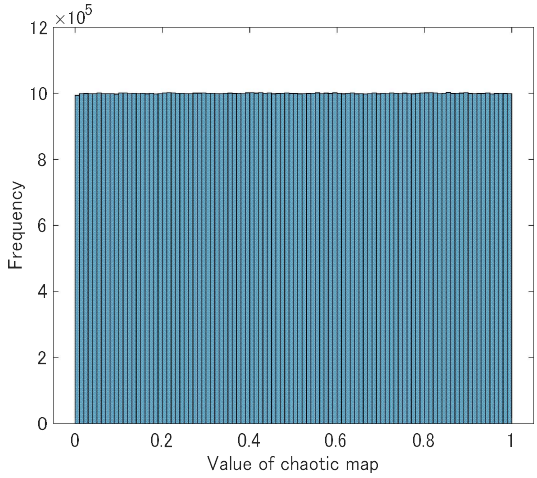

Fig. 2-2 Frequency distribution of the tent map

2　システムモデルと前手法

ここではシステムモデルであるカオス暗号及び BP 信号検出を用いた大規模 MIMO のシステムモデルと前手法でのカオス暗号化の手順を紹介する。

2．1　システムモデル

システムモデルは、送信アンテナ数 N_t、受信アンテナ数 N_r の大規模 MIMO 通信方式を考える。送信機は、カオス暗号器、直並列変換器（Serial Parallel Conversion, S/P）と送信アンテナで構成され、受信機は、受信アンテナ、並直列変換器 (Parallel Serial Conversion, P/S)と BP 信号検出器で構成される(Fig. 1)。この通信システムは共通鍵暗号方式であり、送信側と受信側で M 個の要素を持つ共通暗号鍵

$$\vec{K} = (K_1, K_2, \dots, K_M) \tag{1}$$

を持つ。この鍵を用いて、送信側は暗号化し、受信側は暗号化された信号を復号する。暗号鍵を持っていない第三者は受信信号を傍受しても復号が困難であるため秘匿通信となる。送信データは、N_t 個の送信ビット

$$\vec{b} = \left(b_1, b_2, \dots, b_{N_t}\right), \quad b_i \in \{0,1\} \text{ for } i = 1,2,\cdots,N_t \tag{2}$$

で、カオス暗号器により、送信信号 $\vec{x}$ は、

$$\vec{x} = \left(x_1, x_2, \cdots, x_{N_t}\right), \quad x_i = x_i\left(b_i, \vec{K}\right), \quad i = 1,2,\cdots,N_t \tag{3}$$

となる。前手法での暗号化の詳細は 2.2 節、提案手法での暗号化の詳細は 3 章で述べる。x_i を送信シンボルと呼び、送信アンテナに 1 つずつ割り当てられ、同時刻同周波数で受信アンテナに送信される。電磁波が通る空間中の経路はマルチパスチャネルと呼ばれ、N_r 行 N_t 列の通信路行列 $\mathbf{H}$ で表される。受信信号 $\vec{y}$ は

$$\vec{y} = \mathbf{H}\vec{x} + \vec{n} \tag{4}$$

と表せる。ここで $\vec{n}$ は平均 0 で分散 σ_n^2 の白色雑音である。

受信機では、受信信号 $\vec{y}$ から送信データ $\vec{b}$ を BP 信号検出で推定する。従って、推定データ $\vec{\hat{b}}$ は、$\mathbf{H}$ を既知として、$\vec{y}$、$\mathbf{H}$ と $\vec{K}$ の関数

$$\vec{\hat{b}} = \vec{\hat{b}}\left(\vec{y}, \mathbf{H}, \vec{K}\right) \tag{5}$$

と書ける。なお、ここでの BP 信号検出は前手法 [19] にあるカオス暗号に適したものである。

2．2　前手法でのカオス暗号

ここでは筆者らの先行研究である前手法 [19] での BP 信号検出に適合したカオス暗号について説明する。前手法でのカオス暗号は、カオス MIMO での暗号化を基に、BP 信号検出できるように再構築されている。その詳細については文献 19)を参照されたい。まず、送信側では暗号鍵の要素 K_m を初期値とし、カオス写像であるロジスティック写像で $i \times l$ 回写像することで、複素変数

$$k_{mi} = f^{i\times l}(\mathrm{Re}[K_m]) + jf^{i\times l}(\mathrm{Im}[K_m]) \tag{6}$$

を得る。ここで、$f(\cdot)$はロジスティック写像

$$f(z) = 3.91z(1-z) \tag{7}$$

であり、lは写像回数を決めるパラメータである。さらに、生成された M 個の要素を

$$s_i = \frac{1}{M}\sum_{m=1}^{M}(\mathrm{Re}[k_{mi}] + \mathrm{Im}[k_{mi}]) \cdot \exp[8\pi j(\mathrm{Re}[k_{mi}] - \mathrm{Im}[k_{mi}])] \tag{8}$$

のように加算平均する。最終的に暗号化した送信シンボルは、

$$x_i = \begin{cases} \exp\left[2j\tan^{-1}\dfrac{\mathrm{Im}[s_i]}{\mathrm{Re}[s_i]}\right], & b_i = 1 \\ \exp\left[2j\left(\tan^{-1}\dfrac{\mathrm{Im}[s_i]}{\mathrm{Re}[s_i]} + \pi\right)\right], & b_i = 0 \end{cases} \tag{9}$$

である。

3　提案手法

ここでは、前手法のロジスティック写像をテント写像に置き換えた提案手法でのカオス暗号について述べる。

3．1　提案手法

提案手法でのカオス暗号は、前手法の式(7)をテント写像

Table 1 Simulation condition

	提案手法	前手法	参考手法 1	参考手法 2
Modulation method	Choatic encryption			BPSK
Chaotic map	tent	Logistic	Henon	−
Num. of chaotic map iteration	$l = 10$			−
Size of encryption key	$M = 10$			−
Num. of antennas	$N_{\mathrm{t}} = N_{\mathrm{r}} = 12$			
Channel	i.i.d. Rayleigh fading			
Receive channel state information	Perfect			
Decoding method	BP decoding			
Num. of BP iteration	$N_{\mathrm{iter}} = 20$			

$$g(z) = \begin{cases} 2z, & z < \frac{1}{2} \\ 2(1-z), & z \geq \frac{1}{2} \end{cases} \tag{10}$$

に置き換える。提案手法は、これを用いたカオス暗号をBP信号検出を用いた大規模MIMOに導入したものである。

4　数値実験による評価

提案手法の性能を評価するため、信号検出にかかる計算時間、誤り率とセキュリティ性能について数値実験を行い、前手法、参考手法1、2と比較する。
参考手法 1 はカオス写像にエノン写像を用いたもの、参考手法 2 はカオス暗号を行わず、無線通信で一般的な変調方法の BPSK（Binary Phase Shift Keying）を用いたものである。なお、エノン写像は後述する式(11)で表され、生成される疑似乱数に偏りがない。それらに共通する諸元は Table 1 の通りとした。送信データの要素は等確率で 0 または 1 をとるとし、無作為に生成した。チャネル行列の要素は平均 0、分散 1 の複素ガウス分布$\mathcal{CN}(0,1)$に従う乱数とした。受信信号に含まれる雑音は白色雑音と仮定し、複素ガウス分布$\mathcal{CN}(0,\sigma_{\mathrm{n}}^2)$に従う乱数とした。雑音の分散は信号電力と雑音電力の比である SN 比（SNR, Signal to Noise Ratio）を用いて、$\sigma_{\mathrm{n}}^2 = 10^{-\mathrm{SN}/}$ とした。全ての乱数は互いに独立に生成した。これらの数値実験は MATLAB®で行った。

4．1　計算時間

4 つの手法での BP 信号検出と暗号の復号にかかる計算時間を比較した結果を Table 2 に示す。それぞれの値は、10^3回試行にかかった計算時間を$N_{\mathrm{t}} = 2$の参考手法 2 で規格化したものである。N_{t}が増えるとどの手法も計算時間が増加する。提案手法と参考手法 1 を比較すると、参考手法 1 の計算時間が長くなった。エノン写像は、

$$\begin{cases} x_{n+1} = 1 - 1.4x_n^2 + z_n \\ z_{n+1} = 0.3x_n \end{cases} \tag{11}$$

で表される 2 変数連立写像であるため、1 変数写像である提案手法よりも計算時間が長くなったと考えられる。提案手法と前手法を比較すると、わずかながら提案手法の計算時間が短くなった。テント写像とロジスティック写像のどちらも 1 変数写像であるが、テント写像では計算に必要な項の数が平均的に少なくなることが要因であると考えられる。暗号化を行う 3 手法の中では、提案手法の計算時間が一番短いことがわかった。なお、暗号化を行わない参考手法 2 の計算時間が一番短くなることは自明である。

Table 2 Computation time for decoding

N_{t}	2	4	5	8	12	16	24	32	64
Proposed method	1.06	1.15	1.22	1.54	2.07	3.22	5.10	7.46	22.75
Previous method	1.16	1.29	1.38	1.74	2.36	3.62	5.65	8.21	23.81
Method 1(Henon)	2.22	2.44	2.62	3.38	4.75	7.23	11.05	16.14	47.27
Method 2(BPSK)	1	1.01	1.04	1.20	1.52	2.45	3.95	5.89	19.63

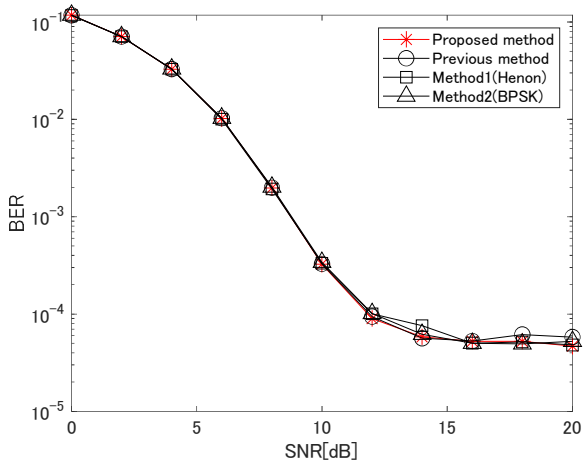

Fig. 3 BERs in massive MIMO for proposed method, previous method, method 1 and 2

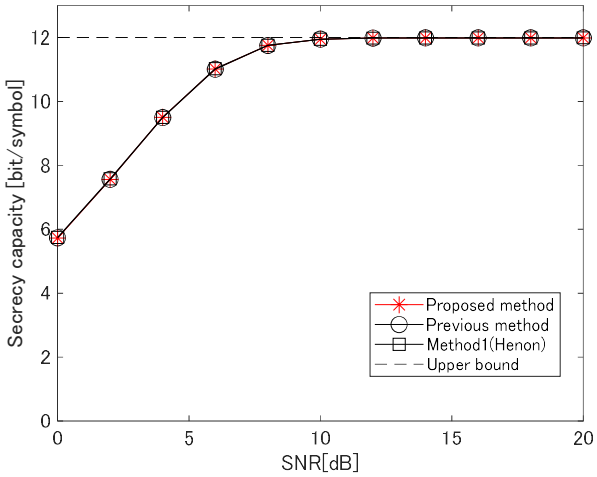

Fig. 4 Secrecy capacity in proposed method and previous method

4．2　誤り率

ここではBit Error Rate(BER)を用いて誤り率（1ビット当りの推定結果が誤る確率）の評価を行う。提案手法、前手法と参考手法1、2のBERを比較した結果がFig.3である。縦軸をBER、横軸をSNRとし、提案手法をアスタリスク、前手法を円、参考手法1を四角、参考手法2を三角で表示した。BERは10^5試行の平均値とした。全ての手法でSNRが大きくなると、BERは徐々に低下しある値に漸近した。BERがある値に漸近する理由は、BP信号検出特有のものであり、その詳細は文献19)を参照されたい。BERの特性は手法間で差がなかった。テント写像を用いることによるBERの増加は起きないことが示唆された。

4．3　セキュリティ性能

セキュリティ性能を示す一般的な指標である秘匿容量を用いて提案手法とその他の手法を比較し評価した。秘匿容量は、

$$C_{\mathrm{S}} = C_{\mathrm{R}} - C_{\mathrm{E}} \tag{12}$$

で与えられる。ここで、C_{R}は正規受信者のチャネル容量で、C_{E}は盗聴者のチャネル容量であり、

$$C_{\mathrm{R}} = qN_{\mathrm{t}}[1 + P_{\mathrm{R}}\log_2 P_{\mathrm{R}} + (1-P_{\mathrm{R}})\log_2(1-P_{\mathrm{R}})], \tag{13}$$
$$C_{\mathrm{E}} = qN_{\mathrm{t}}[1 + P_{\mathrm{E}}\log_2 P_{\mathrm{E}} + (1-P_{\mathrm{E}})\log_2(1-P_{\mathrm{E}})] \tag{14}$$

で表される。P_{R}とP_{E}はそれぞれ正規受信者と盗聴者のBERで、qは変調多値数であり、本研究では$q=1$である。チャネル容量は、その値が上限値に近いほど正確に情報が伝わる。つまり、秘匿容量は、正規受信者に正確に情報を伝達し盗聴者に情報が洩れない場合に上限値に近くなり、セキュリティ性能を示す指標となる。しかしながら、カオス写像での疑似乱数の偏りを起因とするセキュリティ性能の優劣をこの指標で示すことができないことに注意されたい。

提案手法と前手法の秘匿容量を比較した結果がFig.4である。縦軸を秘匿容量、横軸をSNRとし、提案手法をアスタリスク、前手法を円、参考手法1を四角、秘匿容量の上限を破線で表示した。秘匿容量は10^5試行の平均値とした。全ての手法で、SNRが大きくなると、秘匿容量が増加し上限値に漸近した。SNR≥10では、正規受信者に正確に情報を伝達でき、盗聴者には情報が洩れていないことを示しており、秘匿通信が成り立っていると示唆される。一方SNR<10では、上限値に届いていないが、盗聴者に情報が漏れているのではなく、ノイズにより正規受信者が正確に信号検出できていないためである。秘匿容量の特性は手法間で差がなかった。そのためテント写像を用いることによる秘匿容量の低下は起きないことが示唆された。

5　まとめ

本研究では、カオス暗号に、疑似乱数の頻度分布に偏りのないテント写像を導入する手法を提案した。そのカオス暗号を大規模MIMOに適用して提案手法とし、数値実験により計算時間、誤り率と秘匿容量を評価した。その結果、提案手法の誤り率と秘匿容量は、前手法と比べ、ほとんど差がないことが確かめられた。計算時間では、わずかながら提案手法の計算時間が短いことが確かめられた。これらの点から、提案手法が、前手法の欠点であるロジスティック写像による疑似乱数の偏りを回避し、前手法と同等以上の性能を持つことを示すことができた。今後の課題として、本研究

ではセキュリティ性能の評価を秘匿容量のみで行ったため、盗聴者の持つ鍵と正規の鍵との近さに対するセキュリティ性能の依存性についても調査し、評価したいと考えている。

参考文献

1) T. L. Marzetta : Noncooperative Cellular Wireless with Unlimited Numbers of Base Station Antennas, IEEE Trans. Wireless Commun., Vol.9, pp.3590-3600, 2010
2) F. Rusek, D. Persson, B. K. Lau, et al. : Scaling Up MIMO Opportunities and Challenges with Very Large Arrays, IEEE Signal Process. Mag., Vol.30, pp.40-60, 2013
3) E. Telatar : Capacity of Multi-antenna Gaussian Channels, European Transactions on Telecommunications, Vol.10, pp.585-595, 1999
4) L. Lu, G. Y. Li, A. L. Swindlehurst, et al. : An Overview of Massive MIMO: Benefits and Challenges, IEEE J. Sel. Topics Signal Process., 8, pp.742-758, 2014
5) S. Yang, L. Hanzo : Fifty Years of MIMO Detection the Road to Large-scale MIMOs, IEEE Commun. Surveys Tuts., 17, pp.1941-1988, 2015
6) D. Araújo, T. Maksymyuk, A. L. F. Almeida, et al. : Massive MIMO: Survey and Future Research Topics, IET Commun., 10, pp.1938-1946, 2016
7) J. Yang, C. Zhang, X. Liang, et al. : Improved Symbol-based Belief Propagation Detection for Large-scale MIMO, Proc. IEEE Workshop on Signal Processing Systems, pp.1-6, 2015
8) W. Fukuda, T. Abiko, T. Nishimura, et al. : Low-complexity Detection Based on Belief Propagation in a Massive MIMO System, Proc. IEEE Vehicular Technology Conf., pp.1-5, 2013
9) T. Takahashi, S. Ibi, S. Sanpei, et al. : On Normalization of Matched Filter Belief in GaBP for Large MIMO detection, Proc. IEEE Vehicular Technology Conf., pp.1-6, 2016
10) P. Som, T. Datta, A. Chockalingam, B. S. Rajan, et al. : Improved large-MIMO Detection Based on Damped Belief Propagation, Proc. IEEE Trans. inf. Theory, pp.1-5, 2010
11) J. Yang, W. Song, S. Zhang, et al. : Low-Complexity Belief Propagation Detection for Correlated Large-Scale MIMO Systems, J Sign. Process. Syst., 90, pp.585-599, 2018
12) K. Sakoda, H. Hata and S. Hata : Residue Effect of Parallel Interference Canceller in Belief Propagation Decoding in Massive MIMO Systems, International Journal of Electrical and Electronic Engineering & Telecommunications, Vol.9, pp.13-17, No.1, 2020
13) M. Bloch and J. Barros : Physical-Layer Security, Cambridge University Press, Cambridge, 2011
14) L. Dong, Z. Han, A. P. Petropulu and H. V. Poor : Improving Wireless Physical Layer Security via Cooperating Relays, IEEE Trans. Signal Processing, Vol.58, No.3, pp.1875-1888, 2010
15) Y. Shiu, S. Y. Chang, H. Wu, S. C. Huang and H. Chen : Physical Layer Security in Wireless Networks: a Tutorial, IEEE Wireless Commun., Vol.18, No.2, pp.66–74, 2011
16) E. Okamoto : A Chaos MIMO Transmission Scheme for Channel Coding and Physical-layer Security, IEICE Trans. Commun., Vol.E95-B, No.4, pp.1384-1392, 2012
17) E. Okamoto and Y. Inaba : Multilevel Modulated Chaos MIMO Transmission Scheme with Physical Layer Security, NOLTA IEICE, Vol.5, No.2, pp.140-156, 2014
18) K. Sakoda, H. Hata and S. Hata : Chaotic Encryption for Belief Propagation Decoding in Massive MIMO Systems, Journal of Communications Technology and Electronics, Vol.65, No.2, pp.172-178, 2020
19) K. Sakoda, H. Hata and S. Hata : Chaotic Encryption for Massive MIMO using BP decoding, IEICE Trans. Commum., Vol.J105-B, No.7, pp.535-542, 2022