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　６ 年　 ６ 月 １８ 日現在

機関番号：１２６０８
研究種目：基盤研究(C)（一般）
研究期間：2019～2023
課題番号：１９Ｋ１２１５６

研究課題名（和文）力学系に基づく乱数系列を用いた盗聴耐性付きスパース符号分割通信

研究課題名（英文）Eavesdropping-Resistant Sparse Code Division Multiple Access System using a random number sequence based on dynamical systems

研究代表者

實松　豊（Jitsumatsu, Yutaka）

東京工業大学・工学院・准教授

研究者番号：６０３３６０６３

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：防災や監視などの目的で設置した無線通信を使うIoT機器の情報セキュリティ確保は重要な課題である．
黄金比変換器(Golden Ratio Encoder: GRE)は超小型・低消費電力を目指したアナログ・ディジタル変換機の一種である．本研究ではGREの動作を記述する力学系の不変測度を表現する式を世界で初めて明らかにした．得られた不変測度の式を用いて，GREの基本性能指標である二乗平均量子化誤差の理論式を導出した．また，物理層セキュリティを実現するためコセット符号化法に着目し，有限のブロック長に対して第三者に漏洩する情報量の分布を効率的に計算する手法を提案した．

研究成果の学術的意義や社会的意義
黄金比変換器(GRE)の利点は，精度の低い比較器を利用できるため低価格化と小型化が出来ることであり，低い駆動電圧で動作しても安定的に動作するので低消費電力化にも貢献する．GREを用いて乱数生成できれば，IoT機器のセキュリティ確保に貢献することが出来る．学術的には，GREの動作を記述する力学系はこれまで十分に解析されていなかった．GREは2次元の力学系で記述される．本研究で得られた不変測度に関する結果が一般の多次元の力学系の解析につながることが期待される．

研究成果の概要（英文）：Information security is an important issue for IoT devices using wireless communication installed for disaster prevention and monitoring purposes. The Golden Ratio Encoder (GRE) is a type of analog-to-digital converter that aims at compactness and low power consumption. In this study, we have derived an expression for the invariant measure of a dynamical system that describes the behavior of a GRE. Using the obtained invariant measure expression, we derived a theoretical expression for the mean-square quantization error, which is a basic performance indicator of GREs. In order to realize physical layer security, we focused on the coset coding and proposed a method to efficiently calculate the distribution of the amount of information leaked to third parties for a finite block length.

研究分野：通信工学

キーワード：情報セキュリティ　カオス力学系　エルゴード理論　物理層セキュリティ　乱数生成

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

温度センサーや人感センサーを持つ IoT 機器の普及を背景として Machine-to-Machine (M2M) 通信に注目が集まっている．リモート監視や防災用のセンサーは，メンテナンスなしで電池交換の頻度程度で使えることが望ましい．情報信号が常に第三者の前にさらされる無線通信では情報の保全・保護への対策が必要である．しかし，このような低消費電力や小型化，低廉化が求められる機器には，計算機資源を大量に消費する一般的な暗号化や秘匿化技術は搭載困難である．そこで無線通信の通信方式そのものにセキュリティ機能を組み込む物理層セキュリティが有効と考えられる．物理層セキュリティの技術は，研究開始当初だけでなく現在も注目されている．

２．研究の目的

防災などの目的で設置した IoT 機器における M2M 通信のセキュリティ確保は重要な研究課題である．小型で低消費電力な無線通信機器に物理層セキュリティを搭載させるためには，そのセキュリティ保全の前提となる基礎理論を構築することが重要である．既存の物理層セキュリティの方式の多くは，独立同分布な乱数が利用できることを前提としている．カオス力学系に基づく乱数生成は，センサーノードのような低消費電力な回路でも実装できる．そこで，本研究ではカオスに基づく乱数を用いて物理層セキュリティを実現する方法の確立と，そのために必要となる基礎理論構築を目標とした．

３．研究の方法

M2M 通信向けの物理層セキュリティ実現のため，以下の 3 つの小テーマを実施した．

(1) テーマ①では，超低消費電力な黄金比符号化器（Golden Ratio Encoder; GRE）による乱数生成器の性能解析を行った．Daubechies らの提案した黄金比変換機（The Golden Ratio Encoder: Daubechies et al., *IEEE Trans. Inform. Theory*, 2010）は超小型，低消費電力を目指したアナログディジタル変換器（AD 変換器）の一種であり，これを使って偏りのない理想的な乱数を生成する．生成された乱数は様々な用途に利用できる．β 変換機や GRE の動作はカオス力学系によって記述され，エルゴード理論の観点からその特性を解釈することができる．本研究では，GRE の AD 変換の精度の理論値を導出するために不可欠な不変測度を明らかにすることを目標にした．

(2) テーマ②では，盗聴対策のためのコセット符号化法に着目し，その情報漏洩量の評価法確立を目指した．コセット符号化法はよく利用されるメッセージの秘匿化方法であり，誤り訂正符号の線形符号に類似した方法である．情報ビット列と乱数ビット列を連接したブロックに対して，線形符号を用いて誤り訂正符号化する．正規の受信者は，乱数ビット列も含めて情報ビット列をすべて正しく復号化できるが，不正な受信者（盗聴者）には正しく復号できないことが求められる．不正な受信者は，正しくできなくとも情報の一部だけでも復号しようとする．我々の研究では，盗聴者に漏洩してしまう情報量の確率分布を把握することを目標とした．研究代表者らは，いくつかの通信路モデルで情報漏洩量の分布を求めることに成功した．

(3) テーマ③ では，テーマ②の結果を応用し，誤り訂正符号の一種であるスパース重ね合わせ符号と組み合わせたときの性能を考察した．スパース重ね合わせ符号は，圧縮センシングに基づく反復復号により，ガウス型通信路で通信路容量を達成することが証明されている誤り訂正符号であり将来の実用化が期待されている重要な誤り訂正符号である．

４．研究成果

(1) 黄金比符号器（GRE）を記述する力学系の不変測度を特定した．黄金比符号器の力学系は，増幅率パラメータ$\alpha \in [1,3]$と閾値パラメータθ $\left(|\theta| \le \min\left\{\alpha - 1, \phi^{-1}\frac{3-\alpha}{3-\phi}\right\}\right)$ に対して，$u_{n+1} = u_n + u_{n-1} - b_n$，$b_n = Q(\alpha - u_n + u_{n-1} - \theta)$ と表される．ただし，$\phi = \frac{1+\sqrt{5}}{2}$，$Q$は閾値関数$Q(x) = 1 \text{ if } x \ge 0, Q(x) = -1 \text{ if } x < 0$ を表す. アナログ入力値xに対し，初期値を$(u_0, u_1) = (0, x)$とする．このとき，ディジタル値b_nは$x = \sum_{n\ge 0} b_n \phi^{-n}$を満たす$\phi$進展開を与える．この力学系の不変測度を調査した．不変測度は，GRE の性能を表す基本的指標である二乗平均量子化誤差の評価に必要なため重要である．調査の結果，不変測度は，図 1 のような図形上の一様分布になることを世界で初めて明らかにした．この結果は，雑誌論文(3)に掲載された．図 1 はあるパラメータの組に

対する不変集合（不変測度の台）を表したものである．さらに，不変集合を 6 つの排他的な部分集合に分割する方法を与え，写像がマルコフ連鎖をなすことを示した．この結果に基づく，二乗平均量子化誤差の 2 つのパラメータを含む閉形式の表現を世界で初めて与えた．二乗平均量子化誤差は，AD 変換器としての性能を評価する最も基本的な量である．

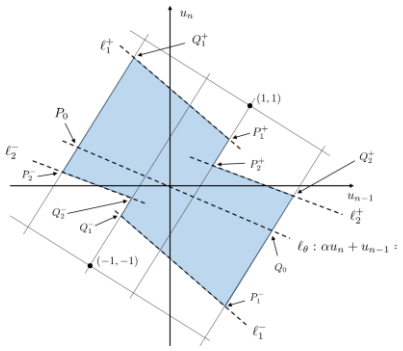

図 1. 黄金比変換機の不変集合

(2) コセット符号化により情報を秘匿化したときの盗聴者に漏洩する情報量の分布を効率的に計算する手法を与えた（雑誌論文(2)）．この種の研究では，正規の送信者(Alice)から正規の受信者(Bob)への通信を傍受しようとする第三者(Eve)のモデルを考える．従来，Eve への情報漏洩量は相互情報量によって評価されていた．研究代表者らは，受信信号z^nが与えられたもとでの条件付き情報漏洩量を，$L(z^n) = H(S^m) - H(S^m|Z^n = z^n)$によって評価することを提案した．ここで$H$はエントロピー関数を表し，$n$はブロック長，$S^m$ は秘密情報を表す$m\,(<n)$ビットの一様確率変数である．情報理論的セキュリティの立場では，盗聴者がnの指数的な計算量を仮定しても解読できないことを要求する．したがって，漏洩する情報量をシミュレーションによって実験することは通常は不可能である．そのため一連の研究では，ブロック長nが無限大の極限で情報漏洩量がゼロに収束することを証明することが重要視される．我々の提案は，あえて漏洩する情報量を数値計算することを目指した．従来研究では$L(z^n)$の第 2 項は，受信信号z^nについて平均化されなければならない．Eve が何を受信するかは Alice も Bob も知らないので期待値によって評価するというのは理にかなっている．しかし，本研究では Eve をシミュレートするので，z^nは入手可能である．本研究が明らかにした手法を用いると，z^nが与えられた下での情報漏洩量を効率的に計算することができる．研究開始前の着想に基づき数値実験を行い，また情報理論的考察を加えた論文が論文誌に採録された（雑誌論文(2)）．計算量は，nに関しては線形であるもののmについて指数的な計算量が必要となる．mをnに比例させて増大させる場合には，やはりnの指数の計算量が必要であるものの，$m \ll n$の状況では，提案法はとても高速に計算することができる．図 2 は，Eve の獲得した情報量のヒストグラムを表している．連続値をとる通信路では情報漏洩量も連続値をとる．従来の理論研究は，情報が全く洩れない$L = 0$の確率がnとともに 1 に収束することを証明することに力が注がれていた．本研究は情報漏洩の状況を把握するときに力を発揮する．

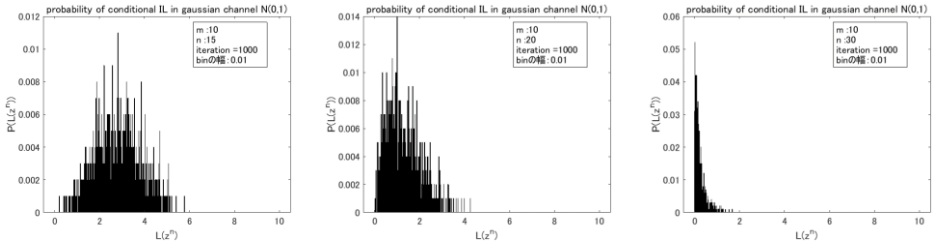

図 2. ガウス型通信路における情報漏洩量のヒストグラム．シミュレーション回数 1000, 情報ビット数$m = 10$, ブロック長 $n = 15$(左), $n = 20$(中央), $n = 30$(右).

(3) スパース重ね合わせ符号とコセット符号化を組み合わせた手法を検討した．スパース重ね合わせ符号は有限の符号長でも極めて良好な誤り訂正能力を示す．本研究ではコセット符号化と組みわせた場合の有効性について検証した．しかし，この場合は結果(2)で示したような条件付き情報漏洩量の分布を効率的に計算することが出来なくなった．研究実施期間内に，素朴な総当たり以外の効率的な計算方法を発見することは出来なかった（学会発表(2)，(4)，(6)，(10)）．本研究で得た知見をもとに，今後さらに検討を重ねてゆく．

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Li Xiaolong、Shinohara Katsutoshi	４．巻 42
２．論文標題 On super-exponential divergence of periodic points for partially hyperbolic systems	５．発行年 2022年
３．雑誌名 Discrete & Continuous Dynamical Systems	６．最初と最後の頁 1707～1707
掲載論文のDOI（デジタルオブジェクト識別子） 10.3934/dcds.2021169	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 Yutaka JITSUMATSU, Ukyo MICHIWAKI, Yasutada OOHAMA	４．巻 E104
２．論文標題 Conditional Information Leakage Given Eavesdropper's Received Signals in Wiretap Channels	５．発行年 2021年
３．雑誌名 IEICE Transactions on Fundamentals	６．最初と最後の頁 295-304
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAP1017	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 －

１．著者名 Yutaka JITSUMATSU	４．巻 12
２．論文標題 Invariant Set of Two-Dimensional Dynamics of Golden Ratio Encoders,	５．発行年 2021年
３．雑誌名 Nonliner Theory and Its Applications, IEICE,	６．最初と最後の頁 75-87
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/nolta.12.75	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 －

１．著者名 Jitsumatsu Yutaka、Oohama Yasutada	４．巻 66
２．論文標題 A New Iterative Algorithm for Computing the Correct Decoding Probability Exponent of Discrete Memoryless Channels	５．発行年 2020年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 1585～1606
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2019.2950678	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 －

〔学会発表〕　計29件（うち招待講演　1件／うち国際学会　1件）

１．発表者名
實松豊

２．発表標題
Gabor分割スペクトル拡散方式によるパルスレーダにおける遅延・ドップラー推定の高精細化

３．学会等名
電子情報通信学会無線通信システム研究会

４．発表年
2024年

１．発表者名
實松豊

２．発表標題
時間・周波数領域スペクトル拡散信号によるレーダ

３．学会等名
令和5年度 情報数理ワークショップ

４．発表年
2023年

１．発表者名
張慧杰，久原重英，竹内純一，實松豊

２．発表標題
MRIのマルチパラメータマッピングにおける適応的撮像パラメータ選択

３．学会等名
電子情報通信学会 医用画像研究会

４．発表年
2023年

１．発表者名
Yutaka Jitsumatsu

２．発表標題
Computation of Marton's Error Exponent for Discrete Memoryless Sources

３．学会等名
Int. Symp. Inform. Theory (ISIT2023)

４．発表年
2023年

１．発表者名
實松豊

２．発表標題
ガボール分割スペクトル拡散信号による遅延・ドップラー推定

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2023年

１．発表者名
實松豊

２．発表標題
遅延・ドップラー同時推定のためのレーダ波形設計

３．学会等名
電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（招待講演）

４．発表年
2023年

１．発表者名
實松豊

２．発表標題
Discrete Prolate Spheroidal Sequencesを用いた位相変調パルスレーダのための系列設計

３．学会等名
電子情報通信学会技術研究報告，SIP2022-2

４．発表年
2022年

１．発表者名
實松豊，大濱靖匡

２．発表標題
有歪み情報源符号化の正復号指数を求める新しいアルゴリズム

３．学会等名
電子情報通信学会技術研究報告，IT2022-17

４．発表年
2022年

１．発表者名
實松豊

２．発表標題
時間領域と周波数領域のスペクトル拡散信号に基づく伝搬遅延とドップラー周波数の推定

３．学会等名
電子情報通信学会技術研究報告，NLP2022-38

４．発表年
2022年

１．発表者名
Huijie Zhang, Otsuma Kawano, Yutaka Jitsumatsu, Shigehide Kuhara, Jun'ichi Takeuchi

２．発表標題
機械学習に基づくMulti-Parameter Mapping (MPM)の推定精度改善

３．学会等名
第50回日本磁気共鳴医学会大会

４．発表年
2022年

１．発表者名
村田英一，井田悠太，丸田一輝，實松豊，牟田修，岡田啓，岡本英二，眞田幸俊，西村寿彦，田野哲

２．発表標題
端末連携によって実現する新たな無線通信システム ～ 最近の結果とアップリンクへの適用 ～

３．学会等名
電子情報通信学会技術研究報告，RCS2022-149

４．発表年
2022年

１．発表者名
實松豊

２．発表標題
ドップラー周波数と無線通信

３．学会等名
九州大学マスフォアインダストリ研究所研究集会(II)「情報通信の技術革新のための基礎数理」

４．発表年
2022年

１．発表者名
實松豊

２．発表標題
Arimotoの指数計算アルゴリズム

３．学会等名
電子情報通信学会総合大会，企画セッション「Arimoto-Blahutアルゴリズムの50年」

４．発表年
2023年

１．発表者名
韓 楽歴，實松 豊

２．発表標題
Coarse格子を正単体とする入れ子格子符号

３．学会等名
第44回情報理論とその応用シンポジウム予稿集

４．発表年
2021年

１．発表者名
釜野 太郎，實松 豊，辻 健

２．発表標題
3次元CNNとResNetを用いた岩石の浸透率推定

３．学会等名
電子情報通信学会，信学技報，ニューロコンピューティング研究会

４．発表年
2022年

１．発表者名
繁恒樹，辻健，實松豊，池田達紀，蒋飛，澤山和貴

２．発表標題
機械学習を用いて岩石CT画像から弾性波速度を推定する手法の開発

３．学会等名
物理探査学会

４．発表年
2020年

１．発表者名
黒崎 将，Tania Sultana，實松 豊，久原 重英，竹内 純一

２．発表標題
深層学習超解像による復元画像を用いた 脳腫瘍MRI画像のセグメンテーション

３．学会等名
第23回情報論的学習理論ワークショップ（IBIS2020）

４．発表年
2020年

１．発表者名
釜野太郎，實松豊，辻建

２．発表標題
畳み込みニューラルネットワークによる岩石物性の推定

３．学会等名
電子情報通信学会，信号処理研究会

４．発表年
2020年

１．発表者名
立和名 隼人，實松 豊

２．発表標題
スパース重ね合わせ符号を用いたダウンリンクNOMA

３．学会等名
電子情報通信学会，情報理論研究会

４．発表年
2020年

１．発表者名
Wei Jianchen，Yutaka Jitsumatsu

２．発表標題
MRI Tumor Recognition Based on Transfer Learning

３．学会等名
電子情報通信学会，情報理論研究会

４．発表年
2020年

１．発表者名
柏原芳克・實松　豊

２．発表標題
黄金比変換器の平均2乗量子化誤差の近似式

３．学会等名
電子情報通信学会，非線形問題研究会

４．発表年
2021年

１．発表者名
Zicong Tan, Yutaka Jitsumatsu

２．発表標題
A Fast MRI Reconstruction with Generative Adversarial Networks

３．学会等名
RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing 2021

４．発表年
2021年

１．発表者名
立和名 隼人，實松 豊

２．発表標題
スパース重ね合わせ符号による多元接続の性能評価

３．学会等名
第42回情報理論とその応用シンポジウム

４．発表年
2019年

１．発表者名
佐藤 大祥，實松 豊

２．発表標題
テプリッツ行列の低ランク補間のMRIへの応用

３．学会等名
第42回情報理論とその応用シンポジウム

４．発表年
2019年

１．発表者名
立和名 隼人，實松 豊

２．発表標題
スパース重ね合わせ符号を用いた多元接続の誤り率の性能

３．学会等名
革新的無線通信技術に関する横断型研究会（MIKA）

４．発表年
2019年

１．発表者名
立和名 隼人，實松 豊

２．発表標題
大規模マシンタイプ通信におけるスパース重ね合わせ符号

３．学会等名
通信方式研究会(2月)

４．発表年
2020年

１．発表者名
渡邉一輝・實松　豊

２．発表標題
Cooperative Jammingにおける妨害者の計画的設置の検討

３．学会等名
通信方式研究会(2月)

４．発表年
2020年

１．発表者名
Tania Sultana, Sho Kurosaki, Yutaka Jitsumatsu, Junichi Takeuchi

２．発表標題
Accuracy of Brain Tumor Detection and Classification Based on Under Sampled k-Space Signals

３．学会等名
情報論的学習理論と機械学習研究会（IBISML）

４．発表年
2020年

１．発表者名
Kitazaki, S., Kawakita, M., Jitsumatsu, Y., Kuhara, S., Hiwatashi, A., Takeuchi, J.

２．発表標題
Magnetic Resonance Angiography Image Restoration by Super Resolution Based on Deep Learning

３．学会等名
The European Society for Magnetic Resonance in Medicine and Biology Congress 2019 (ESMRMB2019)（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
磁気共鳴画像高速再構成法及び磁気共鳴イメージング装置	竹内純一，實松豊，川喜田雅則，北崎自然，久原重英	同左
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2020-025707	2020年	国内

〔取得〕　計0件

〔その他〕

實松研究室
https://www.me.inf.kyushu-u.ac.jp/jitsumatsu/
實松研究室　スライド資料
https://www.me.inf.kyushu-u.ac.jp/jitsumatsu/slide/

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	篠原　克寿 (Shinohara Katsutoshi) (50740429)	一橋大学・大学院経営管理研究科・准教授 (12613)	

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			
オランダ	Eindhoven University of Technology	Leiden University		