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　５ 年　 ６ 月　 ９ 日現在

機関番号：１２６０８
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ０４１２５

研究課題名（和文）同期ずれを考慮した情報系列の距離・相関のモデル化と符号化法

研究課題名（英文）Distance and correlation modeling for information sequences with synchronization errors and coding methods

研究代表者

金子　晴彦（Haruhiko, Kaneko）

東京工業大学・情報理工学院・准教授

研究者番号：７０３９２８６８

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：本研究では同期（挿入／削除）誤り訂正符号に関して，同期誤り訂正可能なpolar符号の逐次除去復号法，DNAストレージに対する各種誤り訂正符号化（通信路のモデル化，積符号を用いた誤り訂正アルゴリズム，複数トレースからの最大事後確率推定法，制約符号化），などを提案した．また，符号を用いた耐量子計算機暗号(PQC)であるMcEliece暗号に対して同期誤りモデルを適用する準備として，MDPC符号のビットフリッピング復号に関する解析を行った．

研究成果の学術的意義や社会的意義
(1) 同期誤りはDNAストレージやレーストラックメモリ等の次世代ストレージやメモリにおいて観測される誤りであり，これらを効率的に訂正する誤り訂正符号はシステムの実用化と高信頼化に有効である．本研究では符号理論に基づきアプリケーションを考慮した誤り訂正符号を提案した．
(2) 量子計算機の実用化により，現在使用されている公開鍵暗号など，一部の暗号は解読可能となる可能性がある．本研究では耐量子計算機暗号であるMDPC-McEliece暗号の耐攻撃性向上のため，同期誤りモデルを用いた基礎的な検討を行った．

研究成果の概要（英文）：We proposed a successive cancellation decoding algorithm for polar codes that can correct synchronization (insertion/deletion) errors, and several error correction codings for DNA storage (channel modeling, error correction algorithm using product codes, maximum a posteriori probability estimation method from multiple traces, and constraint coding). We also analyzed the bit-flipping decoding algorithm of MDPC codes in preparation for applying the synchronization error model to McEliece cryptosystem, which is a code-based post quantum cryptography (PQC).

研究分野：符号理論

キーワード：同期誤り訂正　DNAストレージ　Polar符号　最大事後確率推定　制約符号　McEliece暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

## １．研究開始当初の背景

通信路符号化，情報源符号化，パターンマッチング，等の情報通信や情報処理に関する多くの分野において，複数の情報系列間の相関性や距離を数学的モデルに基づいて適切に定義することは重要な課題である.従来，系列(ベクトル)間の距離として，ハミング距離，Lee 距離，平均二乗誤差，　等が用いられており，これらは系列の要素ごとの値の差によって距離を定義する点で共通している.

一方で，情報系列に物理的な意味が付随している場合，各要素間の値の差異のみでなく相対的な位置のずれを考えることにより，より適切に距離や相関性をモデル化できることが予測される.例えば，高密度磁気記憶媒体である bit-patterned media (BPM) や，次世代メモリのひとつである racetrack memory (RM) では，受信語に同期誤りが生じる可能性が指摘されており，これらにおける誤りは 2 値系列における位置のずれとして表せると考えられる.DNA ストレージにおいてもシーケンサの構造上，多値の同期誤りが生じることが知られている. また，分散情報源符号化 (distributed source coding (DSC)) では，多数のセンサ等から取得する多値データを符号化することが想定され，異なる場所のセンサで取得するデータには値の差異のみでなく時間的なずれが生じることが予測される.さらに，動画像符号化法のひとつである distributed video coding (DVC) では，　フレーム内挿や外挿により副情報 (side information) を生成するが，非線形な動きを有する領域では，副情報に 2 次元配列上での位置のずれが生じると考えることができる.これら以外にも，パターン認識や生体認証などの多くの領域において，情報系列間の「位置のずれ」をモデル化することは重要であると考えられる.

同期誤り通信路に対する符号化法として，挿入/削除/反転 (insertion/deletion/substitution (IDS)) 誤り訂正符号が研究されており，数論的な符号構成により一定数の IDS 誤りを訂正する符号，マーカーやウォーターマークと LDPC 符号を連接した符号化，空間結合符号を用いた符号化，　等が提案されている.

## ２．研究の目的

本研究の目的は，従来の IDS 誤り訂正符号等の研究を基に,「位置のずれ」を考慮したより一般的な情報系列の距離・相関モデルを構築し，従来よりも優れた通信路符号化，を提案するとともに，新たな応用分野を探求することである.具体的な目標は以下のとおりである.

1. 「位置のずれ」を考慮した情報系列の距離・相関モデルを構築する.
2. 通信路符号化法として，例えば，高速データバス，BPM 等の高密度磁気メディア，RM 等の次世代メモリ，DNA ストレージ，等に適した同期誤り訂正符号化法を提案する.
3. 符号ベース耐量子計算機暗号である McEliece 暗号について，誤りベクトル生成において同期誤りモデルを採用することにより，リアクション攻撃等に対する耐性を向上する手法を検討する

## ３．研究の方法

本研究は主に，1．情報系列間の距離・相関モデルの構築，2．通信路/情報源符号化法の構築，3．復号法の構築，及び 4.アプリケーションへの特化，からなり，理論からアプリケーションまでを併せて統合的に研究を行った.具体的な研究方針は以下のとおりとした.

1. 距離・相関モデル: 位置のずれを考慮したモデルを構築する.従来の IDS 誤りモデル，ドリフトモデル，等を包含し，かつシンボル間干渉，系列や位置のずれのマルコフ性，などを表現できるモデルを検討する.さらに，このモデルを多値系列，多次元系列，等へ拡張する.
2. 通信路・情報源符号化法: 本研究に関連する通信路符号化法として，数論的符号，制約符号化，マーカー挿入，LDPC 符号，空間結合符号，Polar 符号，等が考えられ，またこれらを組み合わせた積符号，連接符号，等も想定される.本研究では，これらを基に新しい通信路符号化法を構築する.例えば，非線形写像を用いた非線形符号，符号構成の一部に発見的アルゴリズムを用いる手法，等が考えられる.
3. 復号法: 本研究に関連する復号法として，様々な限界距離復号法，Sum-Product アルゴリズム，BCJR アルゴリズム，等が考えられ，また，これらを組み合わせたマルチパス復号やターボ復号なども想定される.本研究では，復号性能のみでなくアプリケーションに応じた複雑度を有する復号法を検討する.例えば，計算機のデータバスや RM に対する符号では，低遅延性が求められることから，組み合わせ回路で実装可能な並列復号が有効であり，DNA ストレージなどでは，計算量が多くても性能の高い復号法が有効であると考えられる.非線形符号に対しては大規模なルックアップテーブルを用いた復号法も検討する.

4．アプリケーションへの特化と新しい応用：通信路符号化について，BPM，RM，DNA ストレージへの適用を想定した評価を行う．また，符号ベース耐量子計算機暗号を考慮した符号及び復号について検討する．

## ４．研究成果

本研究の主な成果は以下のとおりであり，国際会議，研究会，等において発表を行った．

(1) Polar 符号は無記憶通信路において通信路容量を達成する符号として知られているが，本研究では同期誤り通信路に対する Polar 符号の復号法を提案した．数値評価の結果，符号長が十分に大きい場合に従来の LDPC 符号などより低い誤り率を与えることを示した．

(2) DNA ストレージに おいては，単一の書き込みデータ(ベクトル)に対して，異なる(独立な)同期誤りを有する複数の読み出しベクトルが得られる場合がある．本研究では同期誤りを有する複数の読み出しベクトルから，書き込みデータの各シンボルを最大事後確率推定する計算手法を提案した．

(3) DNA ストレージで用いられるナノポアシーケンサにおける同期誤りモデルについて基礎的な検討を行い，積符号等を用いた誤り訂正法を提案した．

(4) 耐量子計算機公開鍵暗号の候補のひとつである QC-MDPC McEliece 暗号 について，本暗号の欠点である復号誤り率を低減するために，新たな復号法を構築した．また，多元符号を用いた公開鍵暗号や，暗号化で用いる誤りベクトルの生成に同期誤り通信路などの有限状態通信路を用いる手法について，基礎的な検討とシミュレーションによる評価を行った．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計16件（うち招待講演　0件／うち国際学会　5件）

| |
|---|
| １．発表者名<br>中田 良祐，金子 晴彦 |
| ２．発表標題<br>Synchronization and Asymmetric Error Correction for Nanopore Sequencing |
| ３．学会等名<br>IEEE Int. Conf. Consumer Electronics-Taiwan（国際学会） |
| ４．発表年<br>2021年 |

| |
|---|
| １．発表者名<br>Haruhiko Kaneko |
| ２．発表標題<br>Look-Ahead Bit-Flipping Decoding of MDPC Code |
| ３．学会等名<br>IEEE Int. Symp. Information Theory（国際学会） |
| ４．発表年<br>2022年 |

| |
|---|
| １．発表者名<br>申 永貴， 金子 晴彦 |
| ２．発表標題<br>Soft information set decoding における尤度比分布と計算量の関係 |
| ３．学会等名<br>電子情報通信学会技術研究報告 |
| ４．発表年<br>2021年 |

| |
|---|
| １．発表者名<br>申 永貴， 金子 晴彦 |
| ２．発表標題<br>QC-MDPC 符号に対する pairwise bit-flipping 復号の誤り率評価 |
| ３．学会等名<br>第44回情報理論とその応用シンポジウム |
| ４．発表年<br>2021年 |

１．発表者名
市原 和希，金子 晴彦

２．発表標題
DNA ストレージの塩基配列に対する Runlength limited および GC-content 制約化アルゴリズム

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2022年

１．発表者名
飯山 祐介，金子 晴彦

２．発表標題
Bit-Flipping 復号を用いた QC-MDPC McEliece 暗号に対する Reaction-Based Attack の検討

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2022年

１．発表者名
金子 晴彦

２．発表標題
DNAストレージに対する誤り訂正符号（チュートリアル）

３．学会等名
電子情報通信学会総合大会

４．発表年
2022年

１．発表者名
Ryo Sakogawa, Haruhiko Kaneko

２．発表標題
Symbolwise MAP Estimation for Multiple-Trace Insertion/Deletion/Substitution Channels

３．学会等名
2020 IEEE Int. Symp. Information Theory（国際学会）

４．発表年
2020年

１．発表者名
Leo Otani, Haruhiko Kaneko

２．発表標題
Polar Coding for Oversampling Drift Channel

３．学会等名
2020 Int. Symp. Information Theory and Its Applications（国際学会）

４．発表年
2020年

１．発表者名
大谷怜央，金子晴彦

２．発表標題
オーバーサンプリングドリフト通信路に対するpolar符号化法の検討

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2020年

１．発表者名
中田 良祐，金子 晴彦

２．発表標題
ナノポアシーケンシングにおける同期誤りと非対称誤りに対する訂正法

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2020年

１．発表者名
迫川凌，金子晴彦

２．発表標題
DNAストレージに対するファクターグラフを用いた挿入／削除誤り訂正手法

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2019年

１．発表者名
石松 佑太，金子 晴彦

２．発表標題
タイミングドリフト通信路におけるPolar符号を用いた逐次除去復号法

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
迫川凌，金子晴彦

２．発表標題
DNAストレージに対する複数の受信語を用いたMAP推定法

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
Hikari Koremuta, Haruhiko Kaneko

２．発表標題
Successive Cancellation Decoding of Polar Codes for Insertion/Deletion Error Correction

３．学会等名
IEEE International Symposium on Information Theory（国際学会）

４．発表年
2019年

１．発表者名
金子晴彦

２．発表標題
タイミングドリフトとISIが生じる通信路の検討

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

〔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 |
|---|---|