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　２ 年　 ６ 月　 ２ 日現在

機関番号：１２６１１
研究種目：基盤研究(C)（一般）
研究期間：2015～2019
課題番号：１５Ｋ０４８０９

研究課題名（和文）暗号、符号、擬似乱数への代数学の応用

研究課題名（英文）Application of algebra to cryptography, error correcting sequences and pseudo-random number generators

研究代表者
萩田　真理子（Mariko, Hagita）

お茶の水女子大学・基幹研究院・教授

研究者番号：７０３３８２１８

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：暗号、符号、擬似乱数への代数学の応用研究を行った。具体的には、相互に関係の深い以下の３種類の研究を進めた。１．暗号と擬似乱数アルゴリズムの開発と評価研究では、ブロック暗号とストリーム暗号の安全性の評価方法についての研究を進めた。２．シミュレーションのためのグラフの分散彩色アルゴリズム及び分散彩色多項式研究では、応用研究を進め、グラフの重み更新を用いた印象評価方法を提案し、それをレーティング方法として書き換えることで、巨大グラフの中の部分グラフにも使えるように改良した。３．誤り訂正符号系列の存在性と電子署名への応用研究では存在条件についての研究を進めた。

研究成果の学術的意義や社会的意義
１．暗号と擬似乱数アルゴリズムの開発と評価研究は、安全な暗号を安心して使えるようにするための研究で、ブロック暗号とストリーム暗号の安全性の評価方法についての研究を進めた。
２．シミュレーションのためのグラフの分散彩色アルゴリズム及び分散彩色多項式研究では、グラフの重み更新を用いて印象評価を効率よく行う方法を提案した。
３．組合せ論の興味深い研究対象である誤り訂正符号系列の存在条件についての研究を進めた。

研究成果の概要（英文）：We applied algebra to cryptography, error correcting sequences and pseudo-random number generators. Specifically, we conducted the following three studies. 1. Research on cryptographic security evaluation methods. 2. We proposed an impression evaluation method using weighted graph. 3. We have studied the existence conditions of error-correcting sequences.

研究分野：離散数学

キーワード：離散数学　グラフ彩色　暗号　誤り訂正符号　擬似乱数　m系列　印象評価　符号

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

暗号や擬似乱数に代表される数論的アルゴリズムは、世界中の純粋数学及び応用数学の研究機関が興味を持っている分野である。しかしながら、現代の研究は純粋理論なら純粋理論に特化し、実用分野なら実用理論に特化する傾向が強い。また、それらを結びつけるはずの応用数学研究も純粋理論にまで深く切りこむものは少ない。本研究テーマは、「先端的純粋数学理論を実用の視点から眺め研究し、実際に用いられるところにまで到達させる」ことを目的としている。

研究代表者は研究開始当初までに、離散数学を利用して情報通信のセキュリティを高める、暗号鍵更新方法や電子署名強化方法、乱数を用いて既存の暗号化方法を強化し文書の改ざん防止を行う暗号強化方法、暗号用擬似乱数発生システム、暗号化システム及び復号化システムを特許出願し、日本及び米国で権利化されている。また2005 年から2007 年にかけてヨーロッパの暗号関係の中心的な学会であるEuroCrypt から募集されたストリーム暗号の国際標準推奨暗号を決めるプロジェクトECRYPT Stream Cipher Project への応募に、広島大学の松本眞教授らと共に、二つの暗号CryptMT、FUBUKI を提案し、このうちCryptMT は最終選考である第三段階まで候補の一つとして残って、標準暗号の候補として検討された。最終的にはこれまでに使われてきたストリーム暗号と大きく異なる作りになっているため、もう少し検討が必要との理由で標準暗号には採択されなかったものの、CryptMT はそこで提案された他のどのストリーム暗号よりも周期が極端に長いことが証明できている優れた暗号として注目された。次世代の標準的な暗号技術として使われるように研究を続けている。その他に、シミュレーションのためのグラフの分散彩色の存在条件に関する研究、分散彩色アルゴリズムと分散彩色多項式についての研究、誤り訂正系列符号の存在条件に関する研究と、それを用いて電子署名の信頼性を高めるための研究に取り組んでいる。

特に、シミュレーションのための擬似乱数の配置問題は、実際に並列計算を用いた大規模シミュレーションを行っている人たちにはまだあまり必要性を認識されていないが、擬似乱数の専門家が必要性を強調している重要な問題である。この擬似乱数の配置問題や、誤り訂正符号系列の存在性についての研究には、グラフ理論及び代数的組合せ論の知識が不可欠だが、これらの専門家があまり深く関与していないため、研究課題が多く残されている。組合せ論の研究者の取り組むべき問題だと考えている。

また、研究代表者は代数学を用いて離散数学や情報セキュリティの研究を行ってきたことを踏まえて、使えるようにするための代数学の解説書「暗号のための代数入門」を執筆した。立場の違う研究者に代数学の重要性と、その使い方を伝える役割も担って行きたいと考えている。

２．研究の目的

これらの代数学を用いた情報セキュリティアルゴリズムは、現在使われているアルゴリズムよりも数学的に優れていることが証明でき、情報化社会を支える重要なアルゴリズムとなることが期待できる。本研究テーマでは、これらのアルゴリズムを数学を知らない人でも使えるように、誰でも簡単に使える形にして提供することを目的としている。具体的には、相互に関係の深い、以下の３種類の研究を行う。

１．暗号と擬似乱数アルゴリズムの開発と評価、２．シミュレーションのためのグラフの分散彩色アルゴリズム及び分散彩色多項式、３．誤り訂正符号系列の存在性と電子署名への応用。

３．研究の方法

１：既に特許出願している暗号鍵更新方法、電子署名強化方法、暗号通信システム、暗号用擬似乱数発生システムに関連するアルゴリズムの作成・評価・改良を行う。これらの暗号を評価するため、小さな空間での同種の暗号化関数のプログラムをつくり、現在使われている他の暗号化関数をモデル化したものと比較する。同じ変換を繰り返し施して暗号化する場合には、変換回数を減らして混ざり具合を計ることで変換の乱数性を評価する。

２:擬似乱数発生法の並列化の際に独立性を保障するグラフの分散彩色アルゴリズムと分散彩色多項式についての研究を行う。並列計算を用いたシミュレーションを行う場合、擬似乱数の配置の仕方により偏ったデータが出てしまうことがある。この問題は、擬似乱数を割り当てる場所を頂点とし、相関の大きな２点を隣接させたグラフの分散彩色を求めれば解決する。グラフの分散彩色問題とは、与えられた色数で、グラフの頂点を同色の異なる二点の距離の最小値が大きくなるように彩色する問題で、これまでの研究で、シミュレーションに現れることの多い格子グラフの分散彩色の存在範囲を決定し､その他のグラフについても効率よく彩色するいくつかのアルゴリズムのアイデアを提案した。さらに、印象評価への応用研究を進める。

３:誤り訂正系列符号の存在条件についての研究を行う。誤り訂正系列符号は電子署名の強化アルゴリズムをつくるために必要なGF(q)の元の巡回系列で、そのk 部分列の集合が符号となるものである。これまでにM系列と呼ばれる巡回系列と、符号理論の両方の研究手法を用いて存在条件を調べてきた。有限体を生成するための原始既約多項式として、よく探されている３項式とは逆に、項数が半分くらいでバラバラに散らばっているものが必要になり、また随分昔に研究されていたド・ブライン系列が役立つなど、応用に適さないと思われていた離散構造が実用化に結びつきそうになっているため、これも今回の研究計画の中で研究を進めたい。

４．研究成果

研究目的にあげた相互に関係の深い３種類の研究を進め、それぞれ以下の研究成果を得た。

１．暗号と擬似乱数アルゴリズムの開発と評価

開発した暗号を評価するため、小さな空間での同種の暗号化関数のプログラムをつくり、現在使われている他の暗号化関数をモデル化したものと比較する研究を進めた。同じ変換を繰り返し施して暗号化する場合には､変換回数を減らして混ざり具合を計ることで変換の乱数性を評価することができた。

２．シミュレーションのためのグラフの分散彩色アルゴリズム及び分散彩色多項式

擬似乱数発生法の並列化の際に独立性を保障するグラフの分散彩色アルゴリズムと分散彩色多項式についての研究を進めた。シミュレーションに現れることの多い格子グラフの分散彩色の存在範囲を決定し､その他のグラフについても効率よく彩色するいくつかのアルゴリズムのアイデアを提案した。さらに、印象評価への応用研究を進めた。

３．誤り訂正符号系列の存在性と電子署名への応用

誤り訂正系列符号の存在条件についての研究をすすめた。有限体上の原始多項式を用いてM系列を生成して誤り訂正符号系列とするときには、よく探されている３項式とは逆に、項数が半分くらいでバラバラに散らばっている原始多項式が必要になる。さらに、原始多項式ではない多項式からM系列のように生成した系列を考えると周期は短くなるが符号としては良いパラメータが得られる場合があることなどを示した。

５．主な発表論文等

〔雑誌論文〕　計12件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 佐久間織江、辻有万里、萩田真理子	４．巻 2018
２．論文標題 印象評価のためのグラフの重み更新アルゴリズムについて	５．発行年 2018年
３．雑誌名 応用数学合同研究集会予稿集2018	６．最初と最後の頁 207-214
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 森下奈保子,塩谷祥加,浅本紀子,伊藤貴之,萩田真理子	４．巻 2017
２．論文標題 グラフ彩色を用いた写真選出の評価	５．発行年 2017年
３．雑誌名 応用数学合同研究集会予稿集2017	６．最初と最後の頁 104-109
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 西島奈津季，萩田真理子	４．巻 2016
２．論文標題 関数選択を用いた暗号化の乱数性の評価	５．発行年 2016年
３．雑誌名 応用数学合同研究集会予稿集2016	６．最初と最後の頁 46-49
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 野月麻衣，萩田真理子	４．巻 2016
２．論文標題 ペアの円順列での同要素の最短距離について	５．発行年 2016年
３．雑誌名 応用数学合同研究集会予稿集2016	６．最初と最後の頁 50-53
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 森下奈保子，萩田真理子，塩谷祥加，伊藤貴之	４．巻 2016
２．論文標題 グラフ彩色を用いた写真選出手法	５．発行年 2016年
３．雑誌名 応用数学合同研究集会予稿集2016	６．最初と最後の頁 106-109
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 西島奈津季，萩田真理子	４．巻 2015
２．論文標題 AES暗号の安全性評価	５．発行年 2015年
３．雑誌名 応用数学合同研究集会予稿集2015	６．最初と最後の頁 48-51
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 清水蘭，萩田真理子	４．巻 2015
２．論文標題 グラフ理論の分割問題を用いた旅行計画アプリケーションの提案	５．発行年 2015年
３．雑誌名 応用数学合同研究集会予稿集2015	６．最初と最後の頁 78-81
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 野月麻衣，萩田真理子	４．巻 2015
２．論文標題 オイラー閉路における同頂点間距離の最小値について	５．発行年 2015年
３．雑誌名 応用数学合同研究集会予稿集2015	６．最初と最後の頁 98-105
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 辻有万里，萩田真理子	４．巻 2015
２．論文標題 印象評価への組合せ構造の応用	５．発行年 2015年
３．雑誌名 応用数学合同研究集会予稿集2015	６．最初と最後の頁 112-117
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 萩田真理子	４．巻 2015
２．論文標題 誤り訂正符号系列の存在性について	５．発行年 2015年
３．雑誌名 2015年度日本数学会秋季総合分科会　総合講演・企画特別講演アブストラクト	６．最初と最後の頁 21-30
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 三輪華子，萩田真理子	４．巻 2019
２．論文標題 グラフの重み更新アルゴリズムに代わる頂点のレーティング方法の提案	５．発行年 2019年
３．雑誌名 応用数学合同研究集会予稿集2019	６．最初と最後の頁 76-83
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 西田珠実，小林千洋，萩田真理子	４．巻 2019
２．論文標題 GF(2) 上のm系列でない優れたパラメータを持つ誤り訂正符号系列について	５．発行年 2019年
３．雑誌名 応用数学合同研究集会予稿集2019	６．最初と最後の頁 92-94
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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19件（うち招待講演　2件／うち国際学会　0件）

1．発表者名
佐久間織江、辻有万里、萩田真理子

2．発表標題
印象評価のためのグラフの重み更新アルゴリズムについて

3．学会等名
応用数学合同研究集会

4．発表年
2018年

1．発表者名
萩田真理子

2．発表標題
有限体上の誤り訂正符号系列の存在条件について

3．学会等名
組合せ論的符号理論

4．発表年
2019年

1．発表者名
萩田真理子

2．発表標題
有限体上の誤り訂正符号系列の存在条件について

3．学会等名
Japanese Conference on Combinatorics and its Applications (JCCA- 2017) 離散数学とその応用研究集会2017

4．発表年
2017年

1．発表者名
森下奈保子・塩谷祥加・浅本紀子・伊藤貴之・萩田真理子

2．発表標題
グラフ彩色を用いた写真選出の評価

3．学会等名
応用数学合同研究集会

4．発表年
2017年

１．発表者名
萩田真理子

２．発表標題
組み合わせ構造の存在性とその応用

３．学会等名
組合せ論サマースクール2016（招待講演）

４．発表年
2016年

１．発表者名
西島奈津季，萩田真理子

２．発表標題
関数選択を用いた暗号化の乱数性の評価

３．学会等名
2016年度応用数学合同研究集会

４．発表年
2016年

１．発表者名
野月麻衣，萩田真理子

２．発表標題
ペアの円順列での同要素の最短距離について

３．学会等名
2016年度応用数学合同研究集会

４．発表年
2016年

１．発表者名
森下奈保子，萩田真理子，塩谷祥加，伊藤貴之

２．発表標題
グラフ彩色を用いた写真選出手法

３．学会等名
2016年度応用数学合同研究集会

４．発表年
2016年

１．発表者名
野月麻衣，萩田真理子

２．発表標題
印象評価における比較順序の提案

３．学会等名
日本応用数理学会第13回研究部会連合発表会

４．発表年
2017年

１．発表者名
辻有万里，萩田真理子

２．発表標題
印象評価への組合せ構造の応用

３．学会等名
日本応用数理学会第13回研究部会連合発表会

４．発表年
2017年

１．発表者名
西島奈津季，萩田真理子

２．発表標題
関数選択を用いた暗号化の乱数性の評価

３．学会等名
日本応用数理学会第13回研究部会連合発表会

４．発表年
2017年

１．発表者名
松村恵里，萩田真理子

２．発表標題
有限体上の誤り訂正符号系列の存在条件について

３．学会等名
日本応用数理学会第13回研究部会連合発表会

４．発表年
2017年

１．発表者名
西島奈津季，萩田真理子

２．発表標題
AES暗号の安全性評価

３．学会等名
応用数学合同研究集会

４．発表年
2015年

１．発表者名
清水蘭，萩田真理子

２．発表標題
グラフ理論の分割問題を用いた旅行計画アプリケーションの提案

３．学会等名
応用数学合同研究集会

４．発表年
2015年

１．発表者名
野月麻衣，萩田真理子

２．発表標題
オイラー閉路における同頂点間距離の最小値について

３．学会等名
応用数学合同研究集会

４．発表年
2015年

１．発表者名
辻有万里，萩田真理子

２．発表標題
印象評価への組合せ構造の応用

３．学会等名
応用数学合同研究集会

４．発表年
2015年

１．発表者名
萩田真理子

２．発表標題
誤り訂正符号系列の存在性について　（企画特別講演）

３．学会等名
日本数学会（招待講演）

４．発表年
2015年

１．発表者名
三輪華子，萩田真理子

２．発表標題
グラフの重み更新アルゴリズムに代わる頂点のレーティング方法の提案

３．学会等名
応用数学合同研究集会

４．発表年
2019年

１．発表者名
西田珠実，小林千洋，萩田真理子

２．発表標題
GF(2) 上のm系列でない優れたパラメータを持つ誤り訂正符号系列について

３．学会等名
応用数学合同研究集会

４．発表年
2019年

〔図書〕　計2件

１．著者名 神保雅一監訳、澤正憲、萩田真理子訳	４．発行年 2018年
２．出版社 丸善出版	５．総ページ数 324
３．書名 ヴァン・リント＆ウィルソン組み合わせ論上	

１．著者名 神保　雅一、澤　正憲、萩田　真理子	４．発行年 2019年
２．出版社 丸善出版	５．総ページ数 348
３．書名 ヴァン・リント&ウィルソン　組合せ論 下	

〔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