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　２７　年　　６　月　２２　日現在

機関番号：　１２６１１
研究種目：　若手研究(B)
研究期間：　2011～2014
課題番号：　２３７４００７０

研究課題名（和文）暗号、符号、擬似乱数のための離散数学研究

研究課題名（英文）Discrete mathematics for cryptography, code and pseudo random number generator

研究代表者
萩田　真理子（HAGITA, Mariko）

お茶の水女子大学・大学院人間文化創成科学研究科・准教授

研究者番号：７０３３８２１８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：誤り訂正系列符号は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、M系列もその例となっている。M系列を生成する原始既約多項式は、ド・ブライン系列を係数とするのが理想的だが、ド・ブライン系列となるための組み合わせ論的な条件と、原始多項式となるための代数的な条件を同時に満たす列はGF(3)上以外では存在できない。最適解が存在しないところで、１つパラメータを下げたところでの解の状況について調べ、具体的な解の無限列を作成した。よい系列が存在しない場合に、M系列と同様の方法で２つの原始多項式の積から生成すると、より良い誤り訂正符号系列が生成できる場合があることを示し、構成法を拡張した。

研究成果の概要（英文）：We define an (N,k,d) error-correcting sequence over X as a periodic sequence {a_i}_{i=0,1,\ldots} (a_i \in X) with period N, such that its sub k-tuples {(a_i, a_{i+1}, \ldots, a_{i+k-1})|i=0,1,\ldots, N-1} (multiset) are all distinct for 0 \leq i \leq N-1, and that they form an error-correcting code with minimum distance d:= \min_{0 \leq s<t \leq N-1}{\sum_{i=0,1,2,...,k-1}\delta(a_{i+s},a_{i+t})}, where \delta(x,y)=1 for x \neq y and =0 for x=y. If d \geq 2e+1, then one can correct up to e errors in a k-tuple, so the sequence is said to be e-error correcting.
An m-sequence over GF(q) of period {q to the n} -1 is a ({q to the n}-1,n,1) error-correcting sequence. We considered when an m-sequence will be an error-correcting sequencewith minimum distance d=3 or d=5 and we gave some new constructions of error-correcting sequences.

研究分野：　離散数学

キーワード：　離散数学　暗号　符号　擬似乱数　誤り訂正符号系列　グラフ彩色　m系列　ド・ブライン系列

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。

本研究の研究代表者は研究開始時までに、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や、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を特許出願していた。また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 を提案した。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 は今回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。

その他に、シミュレーションのためのグラフの分散彩色研究、一般のグラフの彩色アルゴリズムの改良、誤り訂正系列符号を用いて電子署名の信頼性を高めるための研究に着手し、いくつかの成果をあげていた。

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た。

また、本研究の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、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ことに取り組んでいた。

２．研究の目的

これらの離散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、論文だけではなく実際にプログラムを作り実験して、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）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。

また、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できると期待している。

（２）擬似乱数発生法の並列化の際に独立性を保障する彩色問題の研究を行う。

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ている。本研究の目的は、グラフの分散彩色の存在条件についての研究を進めることと、与えられたグラフと色数について、多項式時間で適切な分散彩色を与えるアルゴリズムを見つけることである。分散彩色アルゴリズムについては評価方法もなかったため、計算量や計算空間の他に、同色 2 頂点間の距離の最小値の大きな彩色、同色 2 頂点間の距離の逆数の和、または同色 2 頂点間の距離の 2 乗の逆数の和（以下重みという）の小さな彩色を良い分散彩色として、評価することを考えている。これらの評価方法が実際に目的に合っているか、どちらの重みが良い指標となるかの検討も進めていく。

（３）誤り訂正系列符号の存在性についての研究をすすめて、電子署名と暗号の強化やノイズの多い通信で同期をとるために利用できるようにする。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。現在、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求めている。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数学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て実用化したいと考えている。

３．研究の方法

研究代表者はこれまでに、鍵情報を関数に組み込むだけでなく関数の選択に利用することを特徴とした新しいストリーム暗号を提案しているが、この方式はストリーム暗号よりもブロック暗号に適した暗号化方式のため、ブロック暗号版を作成し、評価する研究を進めたい。その他に、シミュレーションのためのグラフの分散彩色研究、誤り訂正系列符号の存在性と、これを用いて電子署名の信頼性を高めるための研究に着手し、いくつかの成果をあげている。

これらの研究から得られる離散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る、信頼性の高い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的に評価・改良し、数学を知らない人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。

４．研究成果

相互に関係の深い、以下の３種類の研究を行い、次のような成果が得られた。

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。

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 に応募した２つのアルゴリズムのうち、速度が遅いためもう一方より評価の低かった FUBUKI は、鍵情報を関数に組み込むだけでなく関数の選択に利用することを特徴とした新しいストリーム暗号だが、この方式はストリーム暗号よりもブロック暗号に適した暗号化方式のため、ブロック暗号の評価・改良に向けた研究を行った。サンプルとして現在広く使われている暗号化関数 AES をモデル化したものの、混ざり具合の評価を行った。AES は同じ変換を繰り返し施して暗号化するため、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した。評価手法の一つとして、小さな空間での同種の暗号化関数のプログラムと、現在使われている他の暗号化関数をモデル化したものを、統計的検定により乱数性の評価を行うことで比較した。同等な割合で変換する空間を小さくすることと、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下げることで変換の乱数性に差が出て比較できた。

２：擬似乱数発生法の並列化の際に独立性を保障する彩色問題の研究。

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、一般のグラフで指定した距離まで異なる色を割り当てるプログラムを作成している。また一般のグラフの彩色アルゴリズムの改良や、いくつかの分散彩色アルゴリズムを提案していた。

ここではグラフの分散彩色の存在条件についての研究を進め、与えられたグラフと色数について、適切な分散彩色を与えるアルゴリズムを作成した。分散彩色アルゴリズムの評価方法としては、与えられた色数で、同色 2 頂点間の距離の最小値を大きくする他に､同色 2 頂点間の距離の逆数の和、または同色 2 頂点間の距離の 2 乗の逆数の和（以下重みという）を小さくすることを目標とし、その妥当性を評価した。

いくつかのアイデアでプログラムを作成して、100 頂点程度のグラフをランダムに 1000 個程度作り彩色したときの､これらの重みを比較することでアルゴリズムの比較、改良を行った。

３：誤り訂正系列符号の存在性と電子署名への応用のための研究。

電子署名の強化アルゴリズムをつくるために必要になった、誤り訂正系列符号の存在性についての研究を進めてきた。これは 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、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求めている。この研究では、M系列と符号理論、有限体の原始多項式の性質やド・ブライン系列、ド・ブライングラフとの関わりが深いことに着目し、これらの研究手法や研究成果を取り入れて、既にいくつかの存在条件についての定理を得ている。

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､1950 年代に研究されたド・ブライン系列が役立つことがわかった。しかし、ド・ブライン系列が存在するための組み合わせ論的な条件と、原始多項式が存在するための代数的な条件を同時に満たす理想的なパラメータは GF(3)上以外では存在できないことがわかっていた。

最適解が存在しないところで、１つパラメータを下げたところでの解の状況について調べて、非存在の結果と合わせて発表した。また、実際に存在するところで具体的な解の無限列を作成した。M 系列でよい誤り訂正符号が存在しない場合に、M 系列と同様の方法で、原始多項式ではなく２つの原始多項式の積から生成すると、より良い誤り訂正符号系列が生成できる場合があることを示し、構成法を拡張した。これらの結果は国際会議等で発表している。

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 3 件）
（１）小林千洋，清水蘭，萩田真理子
誤り訂正符号系列の最小距離について
応用数学合同研究集会報告集 2014 p.110-111
2014 年 12 月，査読なし

（２）加藤　知美，萩田　真理子
通信を必要としない鍵更新方法を用いた共有鍵暗号の強化
応用数学合同研究集会報告集 2013 p.114-115
2013 年 12 月，査読なし

（３）萩田真理子，松本眞
GF(2)上の 2-誤り訂正符号系列の存在条件
応用数学合同研究集会報告集 2012,p.50-51
2012 年 12 月，査読なし

〔学会発表〕（計 17 件）
（１）萩田 真理子 「誤り訂正符号系列の構成法」
研究集会「有限幾何と組合せデザイン」
2015 年 3 月 6 日～3 月 7 日，東京理科大学

（２）萩田真理子「組合せ構造の存在性について」
熊本組合せ論研究集会（代数的デザイン論とその周辺）2015 年 1 月 9 日～ 11 日，熊本大学　くすの木会館　レセプションルーム

（３）小林千洋，清水蘭，萩田真理子，「有限体上の誤り訂正符号系列の最小距離について」
2014 年度応用数学合同研究集会，2014 年 12 月 18 日-20 日，龍谷大学理工学部

（４）辻 有万里，萩田 真理子
「印象評価への組合せ構造の応用」（ポスター発表） 日本応用数理学会 2014 年度年会，2014 年 9 月 3 日～5 日，政策研究大学院大学

（５）清水 蘭，萩田 真理子
「グラフ理論を用いた旅行計画アプリケーションの提案」（ポスター発表），日本応用数理学会 2014 年度年会，2014 年 9 月 3 日～5 日，政策研究大学院大学

（６）萩田真理子「印象評価のためのグラフとデザインの配置問題」
離散数学とその応用研究集会 2014
2014 年 8 月 20 日～22 日
新潟総合テレビ・ゆめディア 301～303

（７）清水蘭，萩田 真理子
「グラフ理論を用いた旅行計画アプリケーションの提案」
日本応用数理学会研究部会連合発表会，2014 年 3 月，京都大学

（８）小林千洋，中田有紗，萩田 真理子
「グラフの分散彩色多項式」
日本応用数理学会研究部会連合発表会，2014 年 3 月，京都大学

（９）萩田真理子
「グラフの分散彩色多項式」
組合せ数学セミナー（COMA ゼミ），2014 年 1 月 31 日，東京大学

（１０）加藤　知美，萩田　真理子
「通信を必要としない鍵更新方法を用いた共有鍵暗号の強化」応用数学合同研究集会，2013 年 12 月，龍谷大学

（１１）中田有紗，萩田真理子
「グラフの彩色多項式」日本応用数理学会研究部会連合発表会，2013 年 3 月，東洋大学

（１２）高橋絢那，萩田真理子
「擬似乱数の評価方法の検証」日本応用数理学会研究部会連合発表会，2013 年 3 月，東洋大学

（１３）萩田真理子，松本眞
「GF(2)上の 2-誤り訂正符号系列の存在条件」応用数学合同研究集会，2012 年 12 月，龍谷大学

（１４）Mariko Hagita
“2-error correcting sequence’’
WilsonFest: A Conference in Honor of Rick Wilson, Caltech(アメリカ)2012 年 3 月

（１５）萩田真理子，菊池智子，山口真実
「グラフの分散彩色の評価」日本応用数理学会研究部会連合発表会，2012 年 3 月，九州大学

（１６）萩田真理子
「2-誤り訂正符号系列の存在条件」，関西グラフ理論研究集会，2012 年 3 月，加計国際学術交流センター

（１７）萩田真理子
「誤り訂正符号系列について」

研究集会『離散数理構造とその応用』，2011年 11 月，名古屋大学

６．研究組織

(1)研究代表者

萩田　真理子（HAGITA,Mariko）
お茶の水女子大学・大学院人間文化創成科学研究科・准教授
研究者番号：70338218

(2)研究分担者：なし

(3)連携研究者：なし