| | |
|---|---|
| 教員名 | 萩田　真理子　(HAGITA　Mariko) |
| 所　属 | 理学部情報科学科情報数理講座 |
| 学　位 | 博士（理学）（2000 慶應義塾大学） |
| 職　名 | 助教授 |
| URL　／　E-mail | hagita@is.ocha.ac.jp |

## ◆研究キーワード

離散数学／暗号／電子署名／ストリームサイファ／グラフ彩色／誤り訂正符号

## ◆主要業績　　総数　（　2　）件

・Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura and Mariko Hagita,
"CryptMT version 2.0：A Large State Generator with Faster Initialization",{eSTREAM},
ECRYPT Stream Cipher Project, Report 2006/023, http://www.ecrypt.eu.org/stream,(2006).

・松本眞，西村拓士，斎藤 睦夫，萩田真理子　(出願人：国立大学法人お茶の水女子大学，国立大学法人広島大学)
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，特許公開２００６－３１７８０２．

## ◆研究内容

１．擬似乱数メルセンヌツイスターを用いた周期の長いストリームサイファの構成
ストリームサイファの国際標準規格を決めるプロジェクト ECRYPT Stream Cipher Project への応募で、二つの暗号 CryptMT、FUBUKI を提案している。これらは今回提案された他のどのストリームサイファよりも周期が極端に長いことが証明できている。さらに CryptMT は高速性、FUBUKI は安全性に特化した暗号となっている。

２．グラフの分散彩色とシミュレーション用擬似乱数の配置問題について
　シミュレーションのための格子グラフの分散彩色の存在条件を求めた。また、いくつかの特別なグラフについて、分散彩色を与えるアルゴリズムを作成した。他のグラフについての拡張を目指し、この研究は現在も続けている。

３．誤り訂正系列符号の存在性について
　誤り訂正符号の存在性についての成果をあげて、論文を投稿中である。また、本研究成果を電子署名の強化に利用するための研究を進めている。

## ◆教育内容

担当した講義とその内容は以下の通り．

１．微分積分学Ⅲ：重積分、微分方程式の解法、ベクトルの微積分、線積分、面積分などを解説した。

２．グラフ理論：グラフの定義と基本的な性質を解説する。他の関連する情報科学科専門科目のための基礎科目として、様々なテーマを紹介した。

３．情報代数学：素数、整数、有限体の具体的な扱い方を学び、素数判定法、乱数発生法、符号理論や暗号理論といった通信やシミュレーションのための応用例を紹介した。

４．英文講読：英文の情報科学関連文献の読み方を学ぶ。指定したテキストを輪講形式で読み進め、英語と情報科学と発表の仕方を指導した。

５．離散数学特論（大学院専門教育）：離散数学のトピックとして、地図の塗り分けと４色定理、グラフ彩色アルゴリズム、グラフのネットワーク、ブロックデザインと配置の問題などを解説した。

６．有限数学第２（慶應義塾大学）：離散数学関連のトピックを解説する。半順序集合と Dilworth の定理、グラフの彩色問題、最大流最小カット定理などを扱う。

７．数理情報特選Ｇ（山形大学集中）：組合せ論の最近の話題を解説する。グラフの彩色問題と彩色アルゴリズム、半順序集合と Dilworth の定理、最大流最小カット定理、ブロックデザインと配置の問題などを紹介した。

## ◆Research Pursuits

１．CryptMT: effect of huge prime period and multiplicative filter, and a tweak on faster initialization.

２．Dispersive Colourings of Lattice Graphs.

We have proved that there exists optimal dispersive colouring for 2 dimensional lattice, and proved some properties for the minimum number of colours for existence of d-dispersive colouring of the 3-dimensional lattice.

３．Error-Correcting Sequence over GF(q).

(N,k,d) error-correcting sequence over X is a periodic sequence a_i, i=0,1,…(a_i ¥in X) with period N, such that its sub k-tuples form an error-correcting code with minimum distance d. Admitting a moderate conjecture on the existence of primitive polynomials whose coeffients constitute a De Bruijn sequence, we prove the existence of a binary (2^{2^m-m-2}-1,2^m-2,3) error-correcting sequence for m¥geq 3.

## ◆Educational Pursuits

１．Lecture on Calculus (undergraduate students)

２．Lecture on Graph Theory (undergraduate students)

３．Lecture on Algebra for Information Science (undergraduate students)

４．Readings of English Journals on Information Science (undergraduate students)

５．Lecture on Applied Discrete Mathematics (graduate students)

## ◆共同研究例

・周期が長く高速で安全なストリームサイファの構成とその評価

## ◆共同研究可能テーマ

・擬似乱数を用いたブロックサイファの強化

## ◆将来の研究計画・研究の展望

１．これまでに構成したストリームサイファ FUBUKI に使われている関数選択の手法を用いて、安全性の高いブロックサイファを構成する.

２．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を調べる理論研究とアルゴリズムの作成を、これまでは格子グラフを中心に行ってきたが、ランダムグラフについても同様の研究をすすめる.

３．誤り訂正符号を用いた電子書名の強化についての研究をすすめる.

## ◆研究の実用化　(実用化済のテーマ)　　特許件数　(　1　)件

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

## ◆研究の実用化　(今後実用化したいテーマ)

鍵情報を関数選択に利用することを特徴とするブロックサイファ

## ◆受験生等へのメッセージ

インターネットを用いて秘密の手紙を送るときには、データは暗号化して送られています。このような情報セキュリティ技術を支えているのが離散数学です。基礎理論をしっかりと身につけることで、実用的な応用研究で良い成果をあげることができますから、受験が終わっても気を抜かず、学部１，２年次の専門科目を頑張ってマスターしてください。