教員名	萩田　真理子　(HAGITA Mariko)
所　属	理学部情報科学科
学　位	2000 年 3 月博士（理学）慶應義塾大学
職　名	助教授
URL／E-mail	http://www.ecrypt.eu.org/stream／hagita@is.ocha.ac.jp

◆研究キーワード

暗号理論　／　離散数学　／　暗号乱数　／　誤り訂正符号　／　グラフ彩色

◆主要業績

・論文
author= {Makoto Matsumoto, Hagita Mariko, Takuji Nishimura and Mutsuo Saito},
title= {"Mersenne Twister and Fubuki Stream/Block Cipher"},
howpublished = {{eSTREAM}, {ECRYPT} Stream Cipher Project, Report 2005/003},
・論文
author= {Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura and Mariko Hagita},
title= {"Cryptanalysis of CryptMT: Effect of Huge Prime Period and Multiplicative Filter"},
howpublished = {{eSTREAM}, {ECRYPT} Stream Cipher Project, Report 2005/083},
・特許
発明者名　= 萩田　真理子　権利者名　= 学校法人　慶應義塾
発明の名称　= 暗号鍵更新方法　番号（特許番号）= 特許第 3695526 号
取得日　= 平成 17 年 7 月 8 日

◆研究内容

情報技術の発展に伴い、機密性の高いデータがネットワーク上を流れることが多くなり、数学的に安全性の裏付けられた、より強力な情報セキュリティが必要とされている。
これまでに、離散数学を利用して情報通信のセキュリティを高めるための研究を進め、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る。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。現在はこれらのアルゴリズムの性質の良さを定量的に証明し、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た研究を進めている。また、2005 年度に暗号の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する暗号用擬似乱数発生システムを特許出願し、eSTREAM 標準ストリームサイファの募集に応募している。

◆教育内容

研究室の学生は格子グラフの彩色問題を研究テーマとして、離散数学についての基礎知識を見につけるのと平行して様々な彩色アルゴリズム及びプログラムを作成し、研究集会等で積極的に発表しています。
この分野では学部生が研究発表を行うことはとても難しいのですが、なるべく扱いやすいテーマを選び早くから発表の場に立ち、しっかり研究をしていることをアピールできるように誘導したいと思っています。

◆Reseach Pursuits

We propose two stream ciphers based on a non-secure pseudorandom number generator (called the mother generator).
The mother generator is here chosen to be
the Mersenne Twister (MT), a widely used 32-bit integer generator having 19937 bits of internal state and period $2^{19937}-1$.
One proposal is CryptMT, which computes the accumulative product of the output of MT, and use the most significant 8 bits as a secure random numbers. Its period is proved to be $2^{19937}-1$, and it is 1.5-2.0 times faster than the most optimized AES in counter-mode.
The other proposal, named Fubuki, is designed to be usable also as a block cipher.
It prepares nine different kinds of encryption functions (bijections from blocks to blocks),
each of which takes a parameter.
Fubuki encrypts a sequence of blocks (= a plain message) by applying these encryption functions iteratedly to each of the blocks. Both the combination of the functions and their parameters are pseudorandomly chosen by using its mother generator MT. The key and the initial value are passed to the initialization scheme of MT.

◆特許

・周期の長いストリーム暗号 CryptMT
・安全性の高い暗号 Fubuki
・数列によるブロック暗号の強化方法
（この特許は出願中です）
・共有鍵更新方法

◆将来の研究計画・研究の展望

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。これからも「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」ことを目的とした研究を進めて、離散数学での研究経験を生かして情報社会に貢献して行きたいと考えている。