氏名： 萩田　真理子　（HAGITA Mariko）
所属： 人間文化創成科学研究科自然・応用科学系
学位： 博士（理学）／ Ph.D. in Science
職名： 准教授
専門分野： 離散数学、情報数学、暗号理論
E-mail： hagita@is.ocha.ac.jp

◆研究キーワード　／　Keywords

組み合わせ論／グラフの彩色／暗号理論
Combinatorics ／ Coloring ／ Cryptography

◆主要業績　　総数（２）件

・Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura and Mariko Hagita,
"CryptMT Stream Cipher Version 3", {eSTREAM}, {ECRYPT} Stream Cipher Project, Report 2007/028 (SASC 2007), {http://www.ecrypt.eu.org/stream},(2007).
・Matsumoto, M., Saito, M., Nishimura, T. and Hagita, M.
"A Fast Stream Cipher with Huge State Space and Quasigroup Filter for Software", Selected Areas in Cryptography 2007,
Lecture Notes in Computer Science (LNCS), vol. 4876, pp. 246 - 263, 2007.

◆研究内容　／　Research Pursuits

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。2005 年度に eSTREAM 標準ストリームサイファの募集に応募し、この改良を進めている。

この他に、グラフの彩色アルゴリズムに関する研究を行い研究集会等で発表した。この研究成果についてはさらに研究を進めて論文発表を予定している。

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.

◆教育内容　／　Educational Pursuits

研究室の学生は暗号の実装と評価、擬似乱数の乱数性の高さの評価方法の研究、グラフの彩色問題などを研究テーマとして、離散数学と情報数学についての基礎知識を見につけ、積極的に研究を進めています。

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。

◆研究計画

最先端の離散数学を用いて、情報セキュリティに必要な数学を研究します。理論から実用までを見通して研究を行い、実際に高速に動くものをつくることが目的です。数学的には同一のオーダーの計算量を持つアルゴリズムでも、実装して実験してみると速度に大きな差があることも多くあります。本研究では、実際に計算機実験を重ねることで先端的純粋数学理論のどの部分が実用に供せるかを探るという点で、旧来の研究形態を超えた成果を狙っています。

数学的に質の良さを保証された情報セキュリティアルゴリズムを提供することで、情報化社会の発展に貢献できると期待しています。

◆メッセージ

研究の場で活躍するためには十分な基礎学力を身につけることが必要です。高校の勉強はもちろんのこと、大学に入学してからは授業で習うだけではなく、できるだけたくさんの専門書を読んで、幅広く学んでください。学術的に大切なものが何なのか、自分が面白いと思う分野、得意な分野が何なのか探して自分に合った専門分野を見つけましょう。