FUN-ECM プロジェクト

FUN-ECM Project

山本健太 石川夏樹 小野嘉翔 九島拓実 土田祐介 辻田陸

Kenta Yamamoto　Natsuki Ishikawa　Yoshiharu Ono　Takumi Kushima　Yusuke Tsuchida　Riku Tsujita

概要 Abstract

プロジェクト名の由来 Origin of project name

FUN-ECMとは、FUNは公立はこだて未来大学のことを意味し、ECMとはElliptic Curve Method つまり楕円曲線法のことを意味する。

The origin of FUN-ECM is that FUN means Future University Hakodate and ECM means Elliptic Curve Method.

目的 Purpose

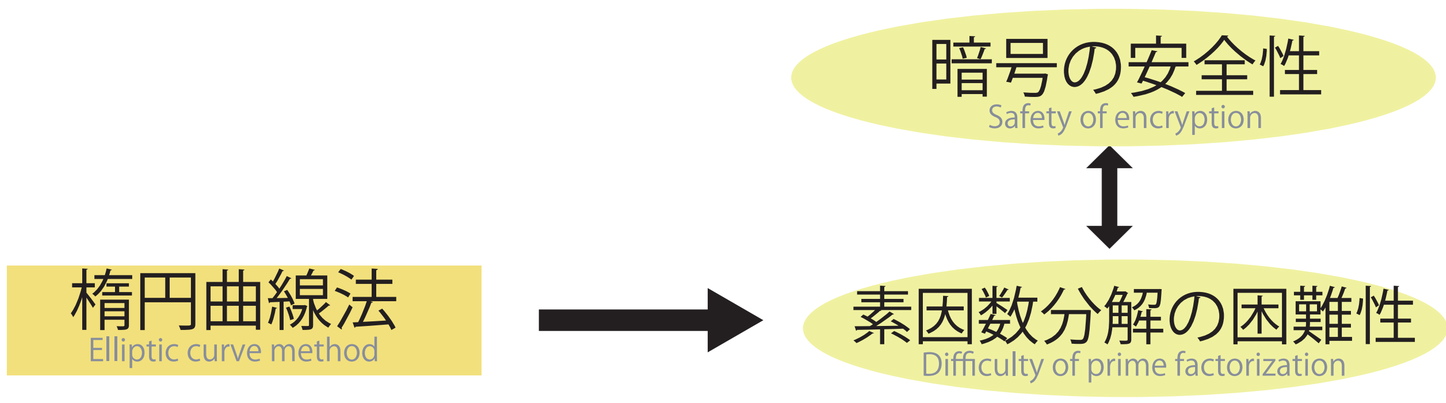
本プロジェクトの目的はできるだけ大きな素因数を見つけ、「ECMNET」のランキングに載ることである。

The purpose of our project is to find a prime factor as big as possible and to put the name on ranking of ECMNET.

背景 Background

大きな数の素因数分解は30数年前から非常に重要な研究対象となってきた。このプロジェクトで扱う楕円曲線法(ECM)は、素因数分解を行う最良な方法の一つである。RSA暗号の安全性は、素因数分解の困難さに大きく関わっている。

The prime factorization of the big number has been very important study subject since about 30 years ago. The elliptic curve method to used by this project is one of the best methods to perform the prime factorization. The safety of the RSA encryption is deeply concerned with the difficulty of prime factorization.



プロジェクトの活動内容 Project's activity

前期の活動では主に白勢先生・由良先生の指導のもと楕円曲線法について学習した。そして簡単な素因数分解のプログラムの作成を行った。後期の活動では目的のECMNETランクインに必要なECMプログラムの改良と評価を行った。今年度のECMプログラムの改良点は射影座標とエドワーズ曲線を導入したことである。その実装と評価のためにプロジェクトを以下の3つの班に分け活動を進めた。

In the first term, we learned ECM under the guidance of Mr.Shirase and Mr.Yura and we created easy program of prime factorization. In the latter term, we improved and assessed ECM program to rank in ECMNET. Features of ECM program of this year are to innovate projective transformation and Edwards-curve. We were separated into below three groups to implement and assess.

統計班 Statistics team

昨年度作成されたECMプログラムと今年度作成したECMプログラムの比較と評価を行った。結果として、今年度のプログラムは前年度の約15%の処理速度の向上が確認された。

We compared and assessed ECM program of last year and this year. As a result, we confirmed ECM program processing speed of this year is about 15% faster.

射影班 Projection team

ECMプログラムの高速化を図るために、ECMプログラムに射影変換とエドワーズ曲線を導入することにした。
これにより、計算コストを約15%削減することができた。

To accelerate ECM program processing, we decided to innovate projective transformation and Edwards-curve. Thereby, we were able to reduce about 15% of the calculation cost.

プログラム班 Program team

ECMプログラムの高速化と並列化を実現し素数を発見する確率を高めるためにECMプログラムの改良を行った。
プログラムの性能評価として、40桁の素数同士の積、79桁の合成数を素因数分解したところ、2時間13分ほどで素因数を発見できた。

We improved ECM program to accelerate ECM program processing, be parallelized and improve probability to find prime. Today we can find fourty‐digit prime in two hours 13 minutes when seventy-nine‐digit composite number as benchmark test.

成果・展望 Result and Prospect

射影変換とエドワーズ曲線の導入により、従来の15%の計算コスト削減に成功し、プログラムの処理時間も15%高速化した。
また、40桁の素数同士の積、79桁の合成数を素因数分解したところ、2時間13分ほどで素因数を発見できた。

現在、より大きな桁数の素因数を発見するためにプログラムを動かし続けている。
また、より速いプログラムを目指し、更なる改良を試みる。

To innovate projective transformation and Edwards-curve, we can succeed in reducing about 15% of the calculation cost and accelerating about 15% of ECM program processing speed. In addition, when seventy-nine‐digit composite number of two same digit prime numbers factor we can find fourty‐digit prime in two hour 13 minutes.

Today, we want to find more greater prime number. Furthermore, we want to improved ECM program so that it is faster.