FUN-ECMプロジェクト

FUN-ECM Project

池野竜將 Ryusuke Ikeno　伊藤有輝 Yuki ito　亀谷浩也 Hiroya Kametani　駒ヶ嶺壮 So Komagamine　千葉大樹 Daiju Chiba　橋本和典 Kazunori Hashimoto　源啓多 Keita Minamoto　山下哲平 Teppei Yamashita

概要　Abstract

活動目的　Purpose

・より大きな桁数の素因数を見つけ「ECM-NET」にランクインすること
・ECMを利用した素因数分解プログラムの改善
・FUN-ECMの活動発信

・Finding primes with larger digits, and rank it in “ECM-NET”
・Improvement of the integer factorization program
・Dissemination of "FUN-ECM" activities

背景　Background

約30年前、(※1)RSA暗号が登場し、現在もインターネット上の通信で広く利用されている。RSA暗号は、大きな数の素因数分解が難しいことによって、安全性が保証されている。すなわち、安全性の評価という点で素因数分解は重要なテーマである。そこで私たちは、大きな数の素因数分解に挑戦することによって、RSA暗号の安全な鍵長を確かめることを目的に活動している。

※1　素因数分解が困難であることを安全性の根拠とした公開鍵暗号の一つ

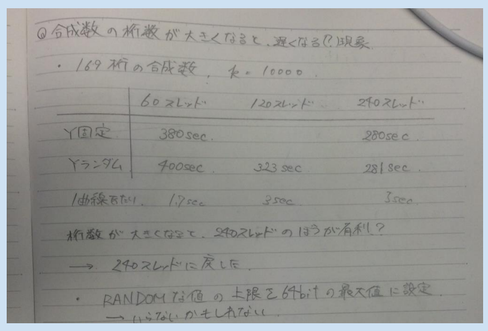
About thirty years ago, RSA was developed, and it is widely used on the internet today. The RSA is based on the practical difficulty of factoring the product of two large prime numbers. So, prime factorization is an important theme of safety evaluation. Therefore, we aim to check the secure key length of RSA by challenging prime factorization of large numbers.

成果　Product

理論班　Theory Group

理論班は、前期の活動でプログラム高速化のための手法であるAtkin-Morain ECPPを文献から見つけ、そのアルゴリズムを理解することができた。後期の活動では本年度プログラム班の作成したプログラムが前年度と比べてどれだけ高速化したか検証をした。その結果、大きな桁数の素因数分解になるほど素因数分解の処理時間が短くなったため、本年度作成したプログラムが高速化に成功したことが分かった。

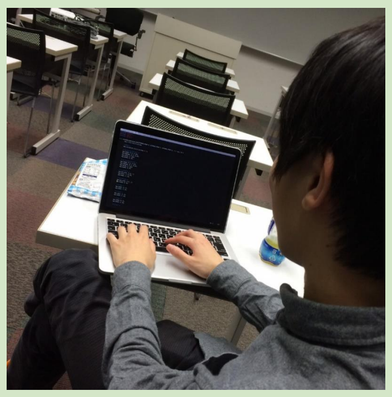
In the first semester, theory group have read Atkin-Morain ECPP algorithm which is method of speeding up program. In the second semester, theory group verified how much program of this fiscal year is faster compared to that of last fiscal year. As a result, calculation using time of the program of this fiscal year is shorter than that of last fiscal year, so we made clear to make program of this fiscal program was succeed.



プログラム班　Programming Group

プログラム班は、1年を通してECMプログラムを改善した。まず、前年度のプログラムの不備を改善した。その後、楕円曲線の生成法やスカラー倍算のアルゴリズムを変更し、演算の回数を減らした。その結果、前年度よりもプログラムの高速化に成功した。また、発見できた素数の桁数も大きくなった、さらに、前年度までは実装していなかったStage2の実装を行った。

Programming group improved program of ECM throughout the year. At first, we improved program of preceding fiscal year. Thenceforth, we reduced the number of operation to alter generation method of elliptic curve and algorithm of scalar multiplication. As a result, we succeeded speeding up program of ECM preceding fiscal year. Once more, figure length of prime was discovered becomes larger. Even still, we implemented Stage2 is not implemented preceding fiscal year.



広報班　PR Group

広報班は、私たちの活動を多くの方に知ってもらうためのウェブページを作成した。ウェブページはGitHub Pages(※3)というサービスを利用して公開し、誰でも簡単に閲覧できるようにした。(URL;https://neglect-yp.github.io/funecm-website/index.html)また、来年度のプロジェクトメンバーに向けて、プログラムや理論の解説ページを作成した。

※3　GitHubを使用してウェブページを公開できるサービス

PR group made the webpage for the purpose of many people know about our activity. This webpage was released using the service called “GitHub Pages” so that anyone can easily browse it.(URL;https://neglect-yp.github.io/funecm-website/index.html) And we made explanation about program and theory page for next fiscal year FUN-ECM.

まとめ　Conclusion

プログラムは昨年度より高速化することができたが、ECMNETのランクインは出来なかった。また、今年度のプロジェクトでは新しい試みとして、広報班を設立しウェブページを作成し、外部への発信を行った。しかし、活動期間が短く、ウェブサイトの公開開始が遅れたため、理解度の調査ができなかった。来年度は理解度調査を行い、結果をウェブサイトに反映させるようにしてほしい。

Though we have succeeded in accelerating ECM program than last year but the program is out of radar range in ECMNET. As a new tried, we have launched PR group from this year and generated the webpage for disseminating of information about ECM. But, we could not measure effectiveness because activity period of PR Group is short also our webpage was opened late for public. Therefore, we want to measure effectiveness in next year and its result put on our webpage.