FUN-ΣCM

Project18 : 楕円曲線法を用いた素因数分解プログラムを作成するプロジェクト。

Project to create prime factorization program using elliptic curve method.

学生 青山和弘 Kazuhiro Aoyama，鳴海雄登 Yuto Narumi，染川眞輝 Masaki Somekawa，矢和田航平 Kohei Yawata，池田晴輝 Haruki Ikeda，上田隼人 Hayato Ueda，小泉建敬 Takehiro Koizumi

担当教員 白勢政明 Masaaki Shirase，由良文孝 Fumitaka Yura

システム班

素因数分解待ちキューの実装

昨年度までに作成された素因数分解プログラムは、プログラムの実行毎にワークステーションにアクセスし、引数をプログラムに受け渡す必要があった。そこでこれまでプログラムを実行するために受け渡していた引数を格納するキューを用意し、一度のプログラム実行で複数回分の処理に用いる引数を受け渡せるようにした。

処理結果の外部出力

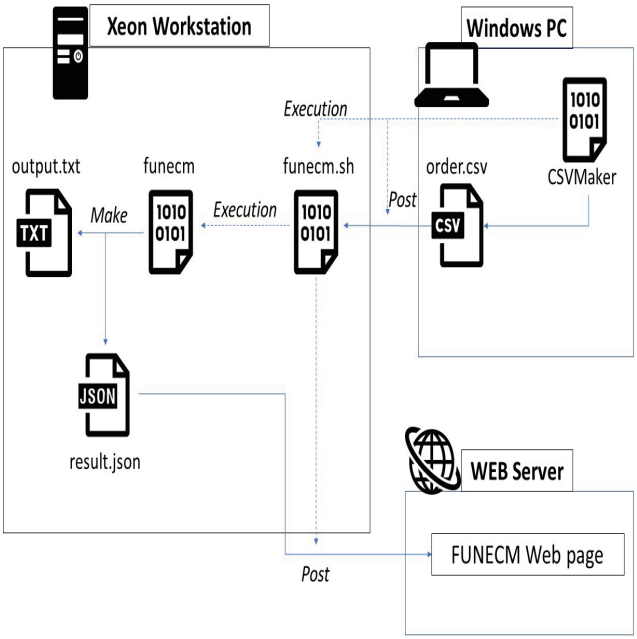
昨年度までのプログラムでは、処理結果の確認のためにワークステーションにアクセスし出力結果を確認する必要があった。これではプログラムの処理が終わったのかどうかを外部から確認するための手段がなかったため、プログラムの終了から次の実行までの時間が空くことがあった。この空き時間を減らす方法として、外部から処理結果を確認することが挙げられた。処理結果を Web ページにアップロードすることで処理状況と、簡易的な処理結果を確認できるようにした。

FUNECM システムのフロントエンド作成

上述の通り、プログラムの実行にはその都度ワークステーションにアクセスする必要があった。そこ 00 で外部から実行に必要な引数を格納したファイルを作成し、ワークステーションに送信、その後ワークステーションに SSH 接続し素因数分解プログラムを実行するアプリケーションを作成することでシステムのフロントエンド化を行った。

既存プログラムとの統合

本年度実装した機能を昨年度までに制作されたプログラムと結合し、FUNECM システムとした。システムの挙動は以下の図の通りである。



FPGA 班

FPGA について

FPGA とは Field Programmable Gate Array の略で直訳すると、現場で書き換え可能な論理回路の多数配列である。その名の通りにハードウェア言語で誤った回路設計をしても、即座にハードウェア言語によって修正ができるデバイスである。FPGA で回路を構成することは高い並列性が期待できる分野やアルゴリズムに効果的で、暗号解読や総当たりがその典型例であるこの長所が ECM の高速化にも効果的であると考えたため、FPGA に ECM を構成することとなった。

後期活動内容

右図が今期に設計した FPGA による ECM の回路図である。ECM では「分解したい合成数を N、任意の楕円曲線の適当な点を P として十分に大きな n に対して nP を計算し nP の x 座標の分母と N の最大公約数を取れば、ある確率で N の素因数が得られる。」という事実を用いため nP を何度も計算する必要がある。そこでこの FPGA の FUNECM では従来の FUNECM と比較して、nP を計算する処理の高速化が図られている。具体的にしたこととしては、使用した n は 4300 万までの素数ごとの 4300 万を超えない中で最大の累乗の総乗（例えば 10 までの素数ごとの 10 を超えない中で最大の累乗の総乗は (2^3=8)×(3^2=9)×5×7 で 2520 となる。）なので計算に多大な時間がかかる。そこで 4300 万までの素数ごとの 4300 万を超えない中で最大の累乗のリストを作成することで高速化を図っている。この回路図は現在、シミュレータ ModelSTM で動作確認中である。