

FUN-ECMプロジェクト

FUN-ECM Project

池野竜将

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

広報班

活動目的

広報班の目的は、世界にFUN-ECMの活動を発信し、多くの人に私たちの活動を知ってもらうことで楕円曲線法や公開鍵暗号技術について広めることを目標としている。

活動内容

FUN-ECMの活動を多くの人に知ってもらうために、誰でも手軽に閲覧することが可能であることからウェブページを作成することにした。このウェブページはターゲットを主に情報系の大学生向けとして学部1年生でもある程度理解が可能であるコンテンツを重視して作成することにした。

活動成果

ウェブページはGitHub Pagesを使用して公開し、誰でも見るようにした。(URL; <https://neglect-yp.github.io/funecm-website/index.html>) 目標としていたECMについての基礎的な部分の紹介ページだけでなく、楕円曲線法のプログラム作成に興味の持った人や来年度のプロジェクトメンバーへ向けたよりコアな内容のコンテンツも作成した。また、1年間の活動記録なども掲載することで私たちの活動をより表面化して多くの興味を持ってもらうようにした。

しかし、公開してどれくらい理解しやすいか、興味を持てたかについての統計を取ることができなかったのでウェブページの作成後に効果の研究をすることはできなかった。

ECMについて

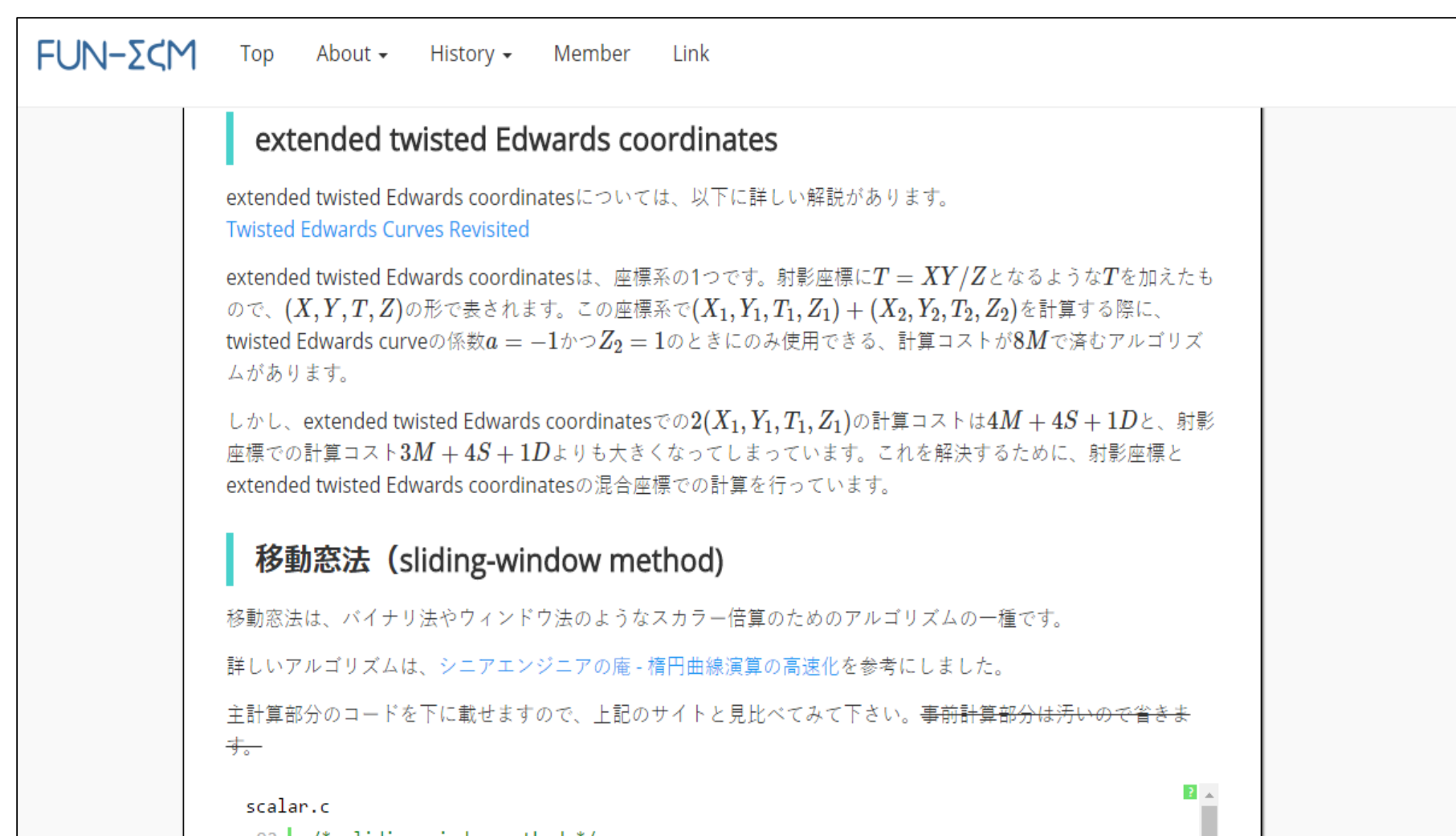
ECMの解説ページでは中間・最終発表で紹介した基礎的なECMの理論について解説しています。時間の制限される発表に比べ、解説をより詳細にし、多くのことを理解できるようにしました。



ECMの基礎理論解説ページ

次期プロジェクトに向けて

プログラムの解説ページでは実際に今年度作成したプログラムの一部を掲載しながら項目別の解説を行っています。今回のプレゼンで扱ったアルゴリズムに加えて、さらに基本的な実装についての解説も行っています。



ECMのプログラム解説ページ



WebサイトのQRコード

4月
構想9月
活動
開始11月
完成12月
公開