**Yaşar Üniversitesi**
**Bilgisayar Mühendisliği Bölümü**
**COMP 4920 Mezuniyet Tasarım Projesi II, Bahar 2020**
**Bitirme Projesi Özeti**

| | |
|---|---|
| **Proje Kodu ve Adı:** | FIWE - Factoring Integers with ECM |
| **Proje Takımı:** | Asena Durukan, asenadurukann@gmail.com<br>Aslı Altıparmak, as.altp@hotmail.com.tr<br>Elif Özbay, eozbayelif@gmail.com<br>Hasan Ozan Soğukpınar, sogukpinarozan@gmail.com<br>Nuri Furkan Pala, nurifurkanpala@outlook.com |
| **Proje Danışmanları:** | Dr. Hüseyin Hışıl |
| **Proje Çıktıları:** | 1. Final Raporu<br>2. Yazılım Gereksinim Dokümanı<br>3. Tasarım Dokümanı<br>4. Kullanım Kılavuzu<br>5. Yazılım<br>6. Poster<br>7. İnternet Sitesi |
| **Proje Web Adresi:** | - |

**Proje Özeti**

**1. Giriş**

Arjen K. Lenstra tarafından 1987 yılında geliştirilen Eliptik Eğri Metodu (EEM), tam sayıları çarpanlarına ayıran bir algoritmadır. Bu algoritma tam sayıları çarpanlarına ayırırken Weierstrass, Edwards ve Montgomery gibi eliptik eğrileri kullanır. Bu projede hızından ve uygunluğundan dolayı Montgomery eğrileri seçilmiştir. Eğriler ve eğrilerin üzerindeki noktalar afin ve projektif koordinatlar ile temsil edilebilir. Projektif koordinatların afin koordinatlardan daha hızlı olması sebebiyle, EEM algoritmasının uygulaması projektif koordinatlar kullanılarak yapılmıştır. EEM algoritmasının ihtiyaç duyduğu modüler ters alma ve Ortak Bölenlerin En Büyüğü (OBEB) işlemi için, hızı ve güncel olması dolayısıyla, safegcd algoritması gerçeklenmiş, ECM algoritmasına eklenmesi gelecek çalışması olarak belirlenmiştir. Algoritma, GPU'nun SIMD mimarisi üzerinde optimize ve paralelize edilmiştir. Bu sayede, çok basamaklı birden fazla sayı aynı anda çarpanlarına ayrılır.

**2. Gereksinimler**

Eliptik Eğri Metodu'nu gerçekleyebilmek için fonksiyonel ve fonksiyonel olmayan gereksinimler bulunmaktadır. Fonksiyonel gereksinimler üçe ayrılabilir:

- **Matematiksel Gereksinimler:**
    - Büyük sayı temsili ve işlemleri.
    - Eliptik eğri temsili, nokta temsili ve işlemleri
    - OBEB işlemi
    - Modüler ters alma işlemi

- **Paralelleştirme Gereksinimleri:**
    - Çok basamaklı birden fazla sayının aynı anda çarpanlarına ayrılabilmesi.
- **Kullanım Gereksinimleri:**
    - Çok basamaklı bir sayının çarpanlarına kolayca ayrılabildiği bir komut satırı.

Fonksiyonel olmayan bir gereksinim ise OBEB işleminin kısa sürede çalışmasıdır.

**3. Tasarım**

Sistem, EEM algoritmasının, GPU'nun SIMD mimarisi üzerinde gerçeklenmesinden meydana gelir. Ayrıca yazılım, farklı matematiksel işlevlere ihtiyaç duyar ve bu işlevler farklı kütüphaneler oluşturularak sağlanmıştır. Bu kütüphanelerin isimleri; Çok Basamaklı Sayı Kütüphanesi Montgomery Kütüphanesi, EEM Kütüphanesi'dir. Bu kütüphaneler birçok yapıyı ve fonksiyonu içerir. Sistem beş ana bölümden oluşur:

- Çok Basamaklı Sayı Kütüphanesi'nin kurulması
- Montgomery Eğri Kütüphanesi'nin kurulması
- EEM Kütüphanesi'nin kurulması
- Safegcd'nin gerçeklenmesi
- Yazılımın SIMD mimarisinde paralelleştirilmesi

**4. Uygulama ve Testler**

Projenin gerçeklenmesi, EEM algoritmasının C dilinde kodlanması ile başladı. Daha sonra C dilinde yazılmış olan kodlar CUDA diline çevrildi. Bu çevirme sayesinde paralelleştirilme süreci başladı. Bu sürecin sonunda, çok basamaklı birden fazla sayının çarpanlarına ayrılması mümkün oldu.

Proje boyunca yazılan her bir fonksiyon birer birer test edildi. Bütün test prosedürleri C ve CUDA dillerinde kodlandı ve modüllere eklendi. Bütün fonksiyonlar 10000 kere test edildi ve %100 başarı sağlandı.

**5. Sonuçlar**

Proje, literatür taraması ile başladı. Araştırmaların rehberliğinde, Tasarım Dokümanı oluşturulmaya başlandı. Eş zamanlı olarak, EEM ve safegcd algoritmalarının gerçeklenmesine C dili kullanılarak başlandı. Daha sonra, paralelleştirme amacıyla CUDA diline geçildi.

**Maliyet Analizi**
Bu proje için dokuz ayda toplamda 242 adam günü harcandı. Bir başka deyişle, her proje üyesi 48 adam günü harcadı.

**Projenin Faydaları**
Projenin faydalarından bir tanesi kriptoloji, kriptanaliz ve ilgili alanlarda çalışacak olan insanlara rehberlik edebilecek bir kaynak sunmak. Yazılımı herhangi biri raporları okuyarak ve kaynak kodları inceleyerek anlayabilir ve kullanabilir. Dahası, grup üyelerinin, bu projenin konusu olan çarpanlarına ayırma problemini ve çözümünü anlamasına yardımcı oldu.

**Gelecekteki Çalışmalar**

- EEM algoritmasının ikinci fazı uygulanabilir.
- EEM algoritmasının gerçeklenmesinde afin koordinatlar kullanılabilir ve bir karşılaştırma yapılabilir.
- Yazılımın paralelleştirme kısmı, yeni GPU'lar veya farklı mimariler üzerinde gerçeklenebilir.
- Safegcd algoritmasının ECM algoritmasına eklenmesi.