ISS-P-029

WebGL を用いた GPGPU による NTRU 暗号の鍵生成の高速化

斎藤　広貴†　　村尾　裕一†
† 電気通信大学大学院　情報理工学研究科

1. はじめに

近年ではスマートフォンにも GPU が当たり前のように搭載されている。このような多様なプラットフォームに搭載されている GPU を同じソースで使用する方法の一つとして挙げられるのが WebGL である。また量子コンピュータの登場により新たな公開鍵暗号が必要になることがすでに知られている [1]。新たな暗号の例として格子暗号と呼ばれるものがあり、その中の 1 つに NTRU 暗号 [2]というものが存在する。しかしこの暗号は計算量がこれまでの暗号に比べると多いため、スマートフォンなどの場合 CPU だけでは演算に時間がかかってしまう。そのため GPU を使用することを考慮する必要がある。すでに WebGL を用いて NTRU 暗号の暗号化部分を実装した例が存在する [3]が、復号や鍵生成の部分を実装した例はない。NTRU 暗号は安全性の問題からより複雑なものが提案されており、その一つが NTRU-HRSS-KEM というものである [4]。一方 WebGL も新たな機能が追加されているため、これを用いてこの暗号の鍵生成の高速化を行う。

2. WebGL と WebGL での GPGPU

WebGL は 3DCG 処理を行うための機構である OpenGL をベースに、これをブラウザ上で実行できるように開発された JavaScript API である。HTML5 にて導入された canvas タグ上に描画を行う。近年の主要なブラウザでは標準機能となっているため OS などの環境に依存しない汎用性の高い API として利用できる。

WebGL で GPGPU を行う方法はテクスチャ利用法、Transform Feedback 利用法、Compute shader 利用法の 3 つがあり、WebGL のバージョンによって使用できる方法が異なる。初期バージョンはテクスチャ法のみ、次世代バージョンは Transform Feedback 法とテクスチャ法、WebGL2-Compute はすべてを使用できる。WebGL2-Computeは現在試作段階であるため OS が Windows のマシンで Chrome Canary にある WebGL2-Compute の flag を enable にすることで使用可能になる。

3. 格子暗号と NTRU 暗号

格子暗号とは耐量子性のある暗号の中で、安全性が格子点探索問題の困難性に依存する公開鍵暗号の総称である。格子点探索問題の最短ベクトル問題を利用して作られたのが NTRU 暗号である。

NTRU-HRSS-KEM 方式とは NTRU 暗号の改良版で、鍵生成時に KEM 処理を加えることで安全性を引き上げているが、それにより計算が複雑になっている。

4. 実装内容

本研究では Compute shader を利用する方法で 4 つ、テクスチャを利用する方法を 4 つの計 8 個実装した。

5. 測定結果

実行時間の測定には全部で 4 台のマシンを使用した。図 1 はその中の 1 台で CPU が Intel i5-5200U、GPU が Intel HD Graphics 5500 のマシン(M2)での測定結果である。

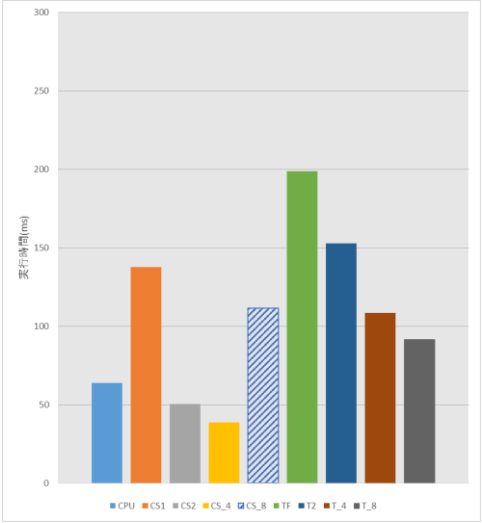

図 1　M2 の測定結果

測定したところ Compute shader を使用した場合は高速化が達成できたが、それ以外では達成できなかった。

6. 今後の課題

測定結果の破線部は正しく演算が行えていない結果であるため、その発生原因の究明が必要である。また iOS,macOS がすでに OpenGL を非推奨としているため Compute shader が正式にリリースされたとしても、これらの OS のマシンでは利用できない可能性が高いため、代替物となる WebGPU での実装を考慮する必要がある。また今回の測定は CPU の性能がそれほど高くないマシンを使ったため大きな影響はなかったが、CPU の性能が上がると GPU との通信コストが無視できなくなるため CPU だけで処理するために WebAssembly の使用を考慮する必要もある。

参考文献

[1] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM J.* Oct. 1997, pp. 1484–1509

[2] J. Hoffstein, J. Pipher, J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” *Proceedings of the Third International Symposium on Algorithmic Number Theory*, Springer-Verlag, 1998, pp. 267--288.

[3] D. Win, “ Development and Examination of In-browser GPU Accelerated Cryptography” Auckland University of Technology, Master thesis, 2016.

[4] H. Andreas, R. Joost, J. M. Schanck, S. Peter, “ NTRU-HRSS-KEM Algorithm Specifications And Supporting Documentation,” 2017.