Chapter 10
Computational Aspects of Lattice-Based Cryptography on Graphical Processing Unit

Sedat Akleylek
Ondokuz Mayis University, Turkey

Zaliha Yuce Tok
Middle East Technical University, Turkey

ABSTRACT

In this chapter, the aim is to discuss computational aspects of lattice-based cryptographic schemes focused on NTRU in view of the time complexity on a graphical processing unit (GPU). Polynomial multiplication algorithms, having a very important role in lattice-based cryptographic schemes, are implemented on the GPU using the compute unified device architecture (CUDA) platform. They are implemented in both serial and parallel way. Compact and efficient implementation architectures of polynomial multiplication for lattice-based cryptographic schemes are presented for the quotient ring both $Z_p[x]/(x^n-1)$ and $Z_p[x]/(x^n+1)$, where p is a prime number. Then, by using these implementations the NTRUEncrypt and signature scheme working over $Z_p[x]/(x^n+1)$ are implemented on the GPU using CUDA platform. Implementation details are also discussed.

INTRODUCTION

Immediately after Shor proposed a polynomial time algorithm to solve integer factorization and discrete logarithm problem on a quantum computer (Shor, 1997), the demand to post-quantum cryptographic schemes started to increase. After this proposal, RSA, El-Gamal cryptosystem, elliptic curve based schemes became unreliable which causes a high demand for secure cryptographic protocols. These advancements also raise the importance of the studies on finding alternative systems that have efficient implementations on software/hardware platforms which are resistant to quantum attacks.

DOI: 10.4018/978-1-4666-9426-2.ch010

Post-quantum cryptographic schemes refer to the algorithms that are resistant to quantum attacks. These are the alternatives of public key cryptographic schemes such as RSA, DLP-based and elliptic curve based schemes. These schemes have been proposed for public key encryption, signature schemes and hash functions. Post-quantum cryptographic schemes can be classified as: code-based, hash-based, multivariate and lattice-based cryptography (Bernstein et al., 2009). The main problem in most of the post-quantum cryptographic schemes (code-based, multivariate and lattice-based cryptography) is the large key sizes. In hash-based schemes key sizes are relatively small such as 368-bit for 80-bit security. Due to large key sizes, in some cases they are not suitable for embedded devices such as smart cards, FPGAs. Another concern is the multiplication operation must be efficiently implemented in lattice-based cryptographic schemes since it is the most frequently used arithmetic operation.

Lattice-based cryptographic schemes are one of the most widely studied post-quantum cryptographic protocols. The security of these schemes depends on the hardness of lattice problems under some parameters (Bernstein et al., 2009). For several years lattice-based cryptographic schemes have only been considered secure for large system parameters causing inefficient implementations. Therefore, it's thought that they were not practical. In 1998, NTRU cryptosystem was proposed as a public key cryptographic scheme over polynomial rings using the computational properties of hard problems over lattices as an alternative to factorization or discrete logarithm problem based schemes (Hoffstein et al., 1998). Standardization of the NTRU is drafted in IEEE P1363 (IEEE, 2008) still in progress and commercialized by Security Innovation (Security Innovation, 2014). After this draft was published, the progress has shown that the design has robustness against different kind of attacks. Its encryption process is almost 10 times faster and decryption processes is almost 100 times faster than RSA for the 1024-bit security level. Furthermore, there is no evidence that it's vulnerable to practical or quantum attacks (Steinfeld, 2014). In this chapter, we focus on the arithmetic over the quotient ring $\mathbb{Z}_p[x]/(x^n-1)$ used in NTRU schemes and also $\mathbb{Z}_p[x]/(x^n+1)$ used in a signature scheme (Güneysu et al., 2012). The quotient ring $\mathbb{Z}_p[x]/(x^n+1)$ can work with Fast Fourier Transform-based multiplications resulting in a more efficient scheme. This is why this quotient ring is preferred in most of the recent ring-based cryptographic schemes (Banerjee et al. 2012; Lyubashevsky et al., 2008; Lyubashevsky et al., 2013).

Graphical processing units (GPU) have attracted attention due to having high performance computing abilities. The main application area of GPUs is to execute commands in parallel with the computer graphics; hence they have been produced for gaming community. A general purpose GPU, having many cores (for example NVIDIA Quadro 600 has 96 cores), has a place on high performance computing applications. Due to processing unit having multiple processors, there is a need to implement such protocols on these platforms. There are several studies on parallel implementations of cryptographic protocols since they are useful for operations requiring lots of processing units (Cook et al., 2006). In this study, we give some ideas to combine advances of lattice-based cryptographic schemes and GPU implementations of them.

Arithmetic operations on the GPU have been widely studied for public key cryptographic schemes such as RSA and elliptic curve based protocols. Now, we give a brief information on how GPUs are utilized for various applications and academic studies. In (Szerwinski et al., 2008) efficient implementations of computationally expensive operations in RSA-1024 and 2048 and curve-based cryptographic schemes on NVIDIA 880GTS graphic card were presented. Standard radix form and residue number system approaches were used. This was the first study using the CUDA framework for general purpose GPU in public key cryptography. Shortly after (Szerwinski et al., 2008), (Gutierrez et al., 2008) proposed a