Ring-LWE Based Face Encryption and Decryption System on a GPU

Tuy Nguyen Tan, Yujin Hyun, Jisu Kim, Dongwoo Choi, and Hanho Lee
Department of Information and Communication Engineering
Inha University, Incheon, Korea
hhlee@inha.ac.kr

Abstract—This paper presents a novel method to implement ring learning with errors (ring-LWE) cryptography for video-based face encryption and decryption on a graphics processing unit (GPU). By conducting ring arithmetic operations in parallel on a GPU, the processing time of these operations is significantly reduced. Consequently, ring-LWE encryption and decryption operations are remarkably improved. The simulation results conducted on GPU and CPU platforms using CUDA C++ show that the ring-LWE based face encryption and decryption operations implemented on a GPU are approximately 100 times faster than that implemented on a CPU.

Keywords: cryptography; decryption; encryption; graphics processing unit; ring-LWE

I. INTRODUCTION

Ring learning with errors (ring-LWE) cryptography [1–3], a well-known post quantum cryptosystem, has attracted great attention from research community recently. Since the security of ring-LWE cryptography is based on the worst-case hardness of lattice problems, it is difficult to solve this problem with any existing computer. Among several arithmetic operations in ring-LWE cryptography, polynomial multiplication is a complex one that requires the most computation time. The operations in ring-LWE cryptography include key generation, encryption, and decryption, detailed in [4]. Various software and hardware implementations of ring-LWE cryptography have been discussed in [4-7]. In [4], authors presented a fingerprint authentication system using ring-LWE cryptography. Fingerprint data are encrypted before sending over the network to make it more confidential. A security system for biomedical image storing and transmitting was also introduced in [7].

In this paper, we present a novel method to implement ring-LWE cryptography scheme for face encryption and decryption on a graphics processing unit (GPU). Faces appear in video are detected and encrypted before sending over the network using ring-LWE encryption scheme to ensure the confidentiality. At the receiver side, these faces are decrypted using ring-LWE decryption scheme when needed. By allowing polynomial multiplication to work in parallel on a GPU, multiplication time is significantly reduced. In addition, polynomial addition is conducted in parallel. As a result, ring-LWE encryption and decryption operations for face image are remarkably improved in terms of processing time.

The rest of this paper is structured as follows: Section II describes the proposed scheme to implement ring-LWE cryptography for video-based face encryption and decryption in detail. Simulation results and performance comparison are presented in Section III. Finally, conclusions are drawn in Section IV.

II. PROPOSED RING-LWE CRYPTOGRAPHY SCHEME FOR FACE ENCRYPTION AND DECRYPTION SYSTEM ON A GPU

The proposed video-based face encryption and decryption system is described in Figure 1. In this system, the face in video is detected using support functions in OpenCV library. The detected face is then encrypted using ring-LWE encryption function. Encrypted data are transmitted to a central server for further processing. When the original data are needed, server runs ring-LWE decryption function to recover the original face.

Ring-LWE encryption and decryption operations require polynomial multiplication and polynomial addition. In the proposed system, we implement number theoretic transform (NTT) and inverse NTT (INTT) processes of the NTT polynomial multiplication on a GPU platform, allowing polynomial multiplication to execute in parallel to speed up the encryption and decryption operations. Polynomial addition is also processed in parallel. The details of ring-LWE these operations on the GPU platform are described in Figure 2. In ring-LWE encryption and decryption schemes, each pixel of face image is considered as a text message \( m \). The encryption function encrypts the detected face into cipher messages before sending them to the remote server.

![Figure 1. Proposed face encryption and decryption system using ring-LWE cryptography.](image-url)
Figure 2. Proposed ring-LWE cryptography scheme for face encryption and decryption system on a GPU.

Inputs of encryption function include public key \((a, p)\), input message \(m\), and three error polynomials \((e_1, e_2, e_3)\) generated from a Gaussian sampler. Encrypted image is stored as the form of cipher-text matrix \((c_1, c_2)\). When the original face image is needed, ring-LWE decryption function is used to recover necessary information. To perform image decryption, private key \(r_2\) and cipher message \((c_1, c_2)\) are required. Note that polynomial multiplication and polynomial addition in encryption and decryption operation are implemented on the GPU platform to work in parallel.

III. SIMULATION RESULTS AND COMPARISON

The proposed ring-LWE cryptography scheme for video-based face encryption and decryption is conducted on GPU and CPU platforms using CUDA C++ on a Windows 10 OS computer. Simulation results for 1-frame face encryption and decryption from video on GPU and CPU platforms are presented in Table I. As can be seen from Table I, the proposed ring-LWE cryptography scheme for face encryption and decryption implemented on a GPU is much better than that on a CPU in terms of processing time. Specifically, the total encryption and decryption time of the proposed scheme on GPU platform is about 100 times faster than that on CPU.

Additionally, by employing NTT polynomial multiplication on GPU platform, the encryption and decryption operations are significantly boosted. The implementation results on a same computer for an image (1-frame video) show that the proposed system can process encryption and decryption approximately 4 times faster than the scheme presented in [8].

IV. CONCLUSIONS

A ring-LWE based face encryption and decryption system on a GPU is presented in this paper. Face image detected from video is encrypted using ring-LWE encryption scheme before sending to the server to increase the level of security. By deploying ring arithmetic operations in parallel on a GPU, ring-LWE encryption and decryption latency are significantly reduced. Noticeably, the processing time for 1-frame face encryption and decryption is only about 0.02 s on a GPU. Therefore, the proposed system can be applied in real-time face detection and encryption systems.

REFERENCES