MMI713

APPLIED PARALLEL PROGRAMMING ON GPU

GPU Accelerated
Symmetric
Encryption & Decryption

Project Proposal

M. Caner TOL

2031466

26.03.2019

1. Problem Definition

Since the very early ages, encrypting messages before sending them is a need. Kings, Presidents, Ambassadors etc. do not want other people to see their messages.

As the computers are developed, messages are sent through the computer networks. Therefore, encryption and decryption of the messages are done by the computers also. However, the computational power of the computers is also very large now. In order to produce strong ciphers against the brute force attacks, very complicated cryptosystems are developed and used.

In complicated cryptosystems, the encryption and decryption latency is an issue. As the data size increases, we have to wait for encryption and decryption of the data before sending or receiving it.

One of the very well-known ciphers is 3DES algorithm. 3DES is a block cipher which takes the plain text, divides it to the blocks of certain sizes. After dividing the plain text to the blocks, it encrypts the blocks separately and creates the cipher text.

Since the blocks are independently encrypted and decrypted, we can easily implement the 3DES algorithm in CUDA and have a large performance gain in terms of throughput.

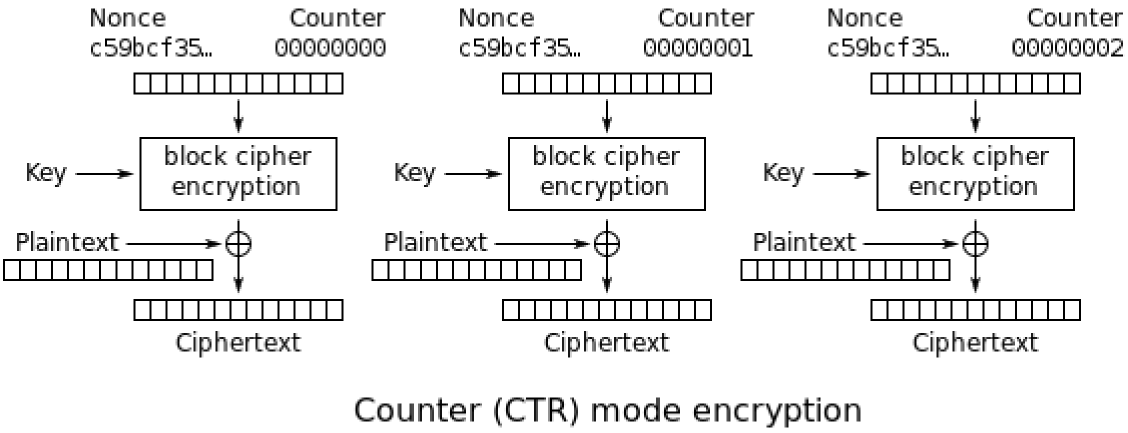
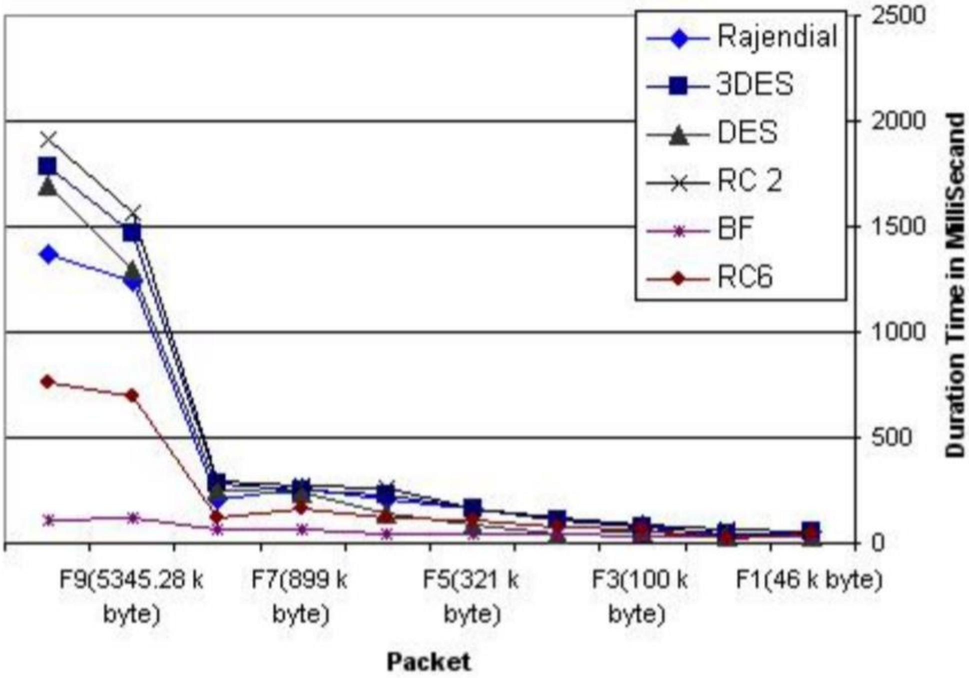


Figure 1 An instance of block cipher

2. Related Work



Elminaam et al. Show that as the data size increases, encryption time is also increasing very sharp.

3. Reference

Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M. (2008). Performance evaluation of symmetric encryption algorithms. IJCSNS International Journal of Computer Science and Network Security, 8(12), 280-286.