Chapter 12
A Novel Approach of Symmetric Key Cryptography using Genetic Algorithm Implemented on GPGPU

Srinivasa K. G.
M. S. Ramaiah Institute of Technology, India

Siddesh G. M.
M. S. Ramaiah Institute of Technology, India

Srinidhi Hiriyannaiah
M. S. Ramaiah Institute of Technology, India

Anusha Morappanavar
M. S. Ramaiah Institute of Technology, India

Anurag Banerjee
M. S. Ramaiah Institute of Technology, India

ABSTRACT

The world of digital communication consists of various applications which uses internet as the backbone for communication. These applications consist of data related to the users of the application, which is confidential and integrity needs to be maintained to protect against unauthorized access and use. In the information hiding field of research, Cryptography is one of the wide techniques used to provide security to the internet applications that overcome the challenges like confidentiality, integrity, authentication services etc. In this paper, we present a novel approach on symmetric key cryptography technique using genetic algorithm that is implemented on CUDA architecture.

DOI: 10.4018/978-1-7998-1763-5.ch012

INTRODUCTION

In the internet era of applications, confidentiality, security, integrity and authentication services are increasingly becoming more important (Viega & McGraw, 2001). One of the key techniques used for providing secure communication is cryptography. Cryptography generally deals with exchange of messages between the sender and the receiver using some secure keys with encryption (encoding) and decryption (decoding). A brief introduction of cryptography, key components of it and its different types are discussed in section 1.

In the evolution of nature, a biological entity that adapts to the changes in the environment has better chances of survival according to the Darwin's theory of evolution. This analogy is applied to genetic programming, which uses theory of evolution steps to draw a better solution to a problem being solved by an algorithm (Kahn, 1996). The steps involved in genetic algorithm or programming is discussed in section 2.

With the advent of increasing multi-core processors, applications being developed need to utilize the threads functionality of these processors. Compute Unified Device Architecture (CUDA), a unified programming model was introduced by Nvidia, which facilitates programming both sequential and parallel portions of a program within a single unit (Nickolls et al., 2008). The different components of CUDA and its architecture are discussed in section 3.

Random numbers are generally used in cryptography for encryption and decryption. Many methods can be used in generating random numbers. The method of creating pseudo- random numbers using genetic algorithms involves more computation power, which can be processed using GPU using CUDA architecture. These pseudo random numbers are generated with linear congruential method. With the help of genetic algorithms implemented using CUDA architecture, the pseudo random numbers are used for encryption and decryption. The algorithm is compared with computation time spent on the CPU and the results are encouraging with CUDA. The paper is organized as follows. In section 1 we discuss briefly concepts related to cryptography, section 2 on genetic algorithms, section 3 on CUDA, section 4 on pseudo random generation and in the later sections, proposed approach and experimental results are discussed.

1. CRYPTOGRAPHY

In our daily life of internet applications and email systems, keeping data and messages confidentially is more important, for example in the launch of nuclear codes and other mission critical systems, in spy's profession the data confidentiality is not compromised. The science of protection of data and communications is called Cryptography (Viega & McGraw, 2001) and (Stinson, 2005). There are many applications where cryptography is applied currently in the fields of e-commerce transactions where examples include purchase using credit cards, wire money transfer etc. In this section, we discuss basic terminologies that are used in cryptography.

The transmission of a message involves two key elements namely the sender and the receiver. In Cryptography the messages are sent between sender and the receiver using encryption and decryption techniques, ensuring the information is received by the intended receivers without any intruders in the middle of the communication (Kessler, 2015). The basic model and different terminologies used in the cryptography are as shown in the Figure 1.