Pro Dialog **23** (2007), 21–32
NAKOM Publishers – Poznań, Poland

Optimizing the Efficiency of Cryptological Processes Based on the RIJNDAEL-AES Algorithm by Means of its Parallel Implementation

Wojciech DOBROSIELSKI, Jacek CZERNIAK

Kazimierz Wielki University in Bydgoszcz, Institute of Technology
ul. Chodkiewicza 30, 85-064 Bydgoszcz, Poland
e-mail: wdobrosielski@ukw.edu.pl, jczerniak@ukw.edu.pl

Received March 26, 2007

Abstract. This article describes research the aim of which was to accelerate cryptographic processes using parallel programming. The application of cryptography has becomes common nowadays. The complexity of operations and the amount of data to be processed place this domain of computer science in a group of those which consume resources greedily. Therefore, the union of cryptology and parallel programming can result in improved working parameters of cryptographic algorithms. This article discusses results of experiments which prove the correctness of such a theory. The values of parameters of parallel programming that were achieved during research, such as acceleration and efficiency, indicate clear benefits of the new method. This paper shows an effective way of improving these parameters used in the Rijndael algorithm, the winner of an open competition on AES.

Key words: cryptography, Rijndael, AES, parallel programming, PCAM, OpenMP