عنوان مقاله:

Parallel Implementation of Somewhat Homomorphic Encryption

محل انتشار:

همایش ملی مهندسی برق مجلسی (سال: 1395)

تعداد صفحات اصل مقاله: 7

نویسندگان:

Ali Mirzaei - *Department Of Information Technology Engineering, College of Science, Kerman Branch, Islamic Azad University, Kerman,Iran*

Amir Sabbagh Molahosseini - *Associate Professor, Department Of Computer Engineering, College of Science, Kerman Branch, Islamic Azad University,Kerman, Iran*

خلاصه مقاله:

In this paper our purpose is to carry out a parallel implementation of somewhat homomorphic encryption usingOpenMP programming technique to reduce the running time. We implemented our study on two laptops with differentdual-core processors: (1) IntelCoreTM 2Duo CPU P8700 (3M cache, 2.53GHz, 4G RAM), and (2) IntelCoreTM i5-2410M CPU (3M cache, 2.30 GHz, 4G RAM). We presented parallel implementation of somewhat homomorphicencryption on OpenMP by parallelizing the scheme's three algorithms (keygen, encryption and evaluate).The resultsshowed that in sample processor no.1, OpenMP techniques improved the speed of the algorithms of keygen,encryption and evaluation as 1.67, 1.87, and 8.63 ms respectively, while in sample 2, these improvements in speedwere reported as 2.1, 1.63, and 8.53 ms, respectively. We concluded that OpenMP reduces the running time andaccelerates the somewhat homomorphic encryption process, especially in applications that require thousands ofsimultaneous encryption bits.

کلمات کلیدی:

Homomorphic encryption, Somewhat homomorphic encryption, OpenMP, data security