Security analysis of fully homomorphic encryption systems

©A.E. Malinskiy

Bauman Moscow State Technical University, Moscow, 105005, Russia

Cloud computing is currently one of the most important markets in the IT business. Security of cloud solutions is based on the assumption that one can trust cloud computing provider with their private data. If there is no such guarantee fully homomorphic encryption systems solve this problem [1]. Such system allows computation of arbitrary operations on ciphertexts without of secret key. This allows cloud client to compute in the cloud without trusting the cloud. This articles focuses on vulnerabilities of fully homomorphic systems, algorithms for ciphertexts decryption for any possible fully homomorphic system implementation and derives the complexity of such decryption operation. Decryption algorithm allows to derive upper bound for number of fully homomorphic systems and to eliminate the practical need to develop fully automorphic system.

Keywords: cloud computing, homomorphism, cryptography, encryption.

Malinskiy A.E., graduate of the Computer Security Department of Bauman Moscow State Technical University. e-mail: anton@malinskiy.com