Ciphertext Policy Attribute based Homomorphic Encryption (CP-ABHERLWE): a fine-grained access control on outsourced cloud data computation

Abstract

Recently, homomorphic encryption is becoming one of the holy grail in modern cryptography research and serve as a promising tools to protect outsourced data solutions on cloud service providers. However, most of the existing homomorphic encryption schemes are designed to achieve Fully Homomorphic Encryption that aimed to support arbitrary computations for only single-data ownership scenario. To bridge these gaps, this paper proposed a non-circuit based Ciphertext Policy-Attribute Based Homomorphic Encryption (CP-ABHER-LWE) scheme to support outsourced cloud data computations with a fine-grained access control under the multi-user scenario. First, this paper incorporates Attribute Based Encryption (ABE) scheme into homomorphic encryption scheme in order to provide a fine grained access control on encrypted data computation and storage. Then, the proposed CP-ABHER-LWE scheme is further extended into non-circuit based approach in order to increase the practical efficiency between enterprise and cloud service providers. The result shows that the non-circuit based CP-ABHER-LWE scheme has greatly reduced the computation time and ciphertext size as compared to circuit based approach. Subsequently, the proposed CP-ABHER-LWE scheme was proven secure under a selective-set model with the hardness of Decision Ring-LWEd,q,ई problem.