Abstract

Homomorphic encryption schemes are malleable by design. In the field of homomorphic encryption schemes have made it possible to implement a variety of schemes using different techniques and programming languages. In this paper, we choose the model to increase the efficiency and security. Basically this technique is a method of encryption that combines two or more encryption technique and usually includes a combination of symmetric and asymmetric (public-key) encryption to take benefit of the strengths of each type of encryption. Fully homomorphic encryption schemes, we observe that the main bottleneck for this scheme is slow running speed and large cipher text.

References


Index Terms

Computer Science

Information Sciences

Keywords

Cryptography, Homomorphic Encryption, Symmetric and Asymmetric Encryption.