Homomorphic encryption is the encryption scheme which means the operations on the encrypted data. Homomorphic encryption can be applied in any system by using various public key algorithms. When the data is transferred to the public area, there are many encryption algorithms to secure the operations and the storage of the data. But to process data located on remote server and to preserve privacy, homomorphic encryption is useful that allows the operations on the cipher text, which can provide the same results after calculations as the working directly on the raw data. In this paper, the main focus is on public key cryptographic algorithms based on homomorphic encryption scheme for preserving security. The case study
Survey of Various Homomorphic Encryption algorithms and Schemes

on various principles and properties of homomorphic encryption is given and then various homomorphic algorithms using asymmetric key systems such as RSA, ElGamal, Paillier algorithms as well as various homomorphic encryption schemes such as Brakerski-Gentry-Vaikuntanathan (BGV), Enhanced homomorphic Cryptosystem (EHC), Algebra homomorphic encryption scheme based on updated ElGamal (AHEE), Non-interactive exponential homomorphic encryption scheme (NEHE) are investigated.

References

- Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity
Survey of Various Homomorphic Encryption algorithms and Schemes


- Taher elgamal, member, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE transactions on information theory, vol. it-31, no. 4, july 1985.


1998.

Index Terms

Computer Science Security

Keywords

Cryptography Homomorphic Encryption Paillier algorithm RSA ElGamal BGV
EHC

NEHE

AHEE