Report/Write Up

Minor Project- Development of Fully Homomorphic Encryption Scheme

By: Tarun Chauhan(2022JCS2670)

Supervisor: **Prof. Ashok K Bhateja**

In this semester, major part of my project involved literature survey about the Homomorphic Encryption Schemes and their types such as Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE) and Fully Homomorphic Encryption (FHE). I learned about the need to have fully homomorphic encryption schemes and limitations of current cryptographic schemes. This semester, I have focused only on the Partially Homomorphic Encryption Schemes and Somewhat Homomorphic Encryption schemes and referred to research papers regarding these schemes only. Understanding these PHE and SWHE schemes have provided me with the foundation of working on a Fully Homomorphic Encryption scheme later.

Partially Homomorphic Schemes:

1. RSA (Multiplicative Homomorphism)
2. GM cryptosystem (Additive Homomorphism)
3. El-Gamal (Multiplicative Homomorphism)
4. Paillier Cryptosystem (Additive Homomorphism)

Somewhat Homomorphic Schemes:

1. BGN Cryptosystem (Unlimited addition and one multiplication)

I have implemented the RSA and Paillier PHE schemes. I evaluated and verified their respective homogenous property. This gave me a better understanding of the working of these schemes and the mathematics involved behind it. I also implemented a SWHE scheme - the BGN cryptosystem. The BGN cryptosystem supports an arbitrary number of additions and one multiplication by keeping the ciphertext size constant. This property is not visible in PHE schemes.

In the implementation of the above mentioned schemes,

1. The keys of different sizes were generated and used to encrypt the messages.
2. Homomorphic operations were performed on encrypted messages.
3. After performing homomorphic operations, the final ciphertext was decrypted.
4. The resultant plaintext message was equivalent to, as if the homomorphic operation was performed on plaintext messages only.

   i.e, $E(m1 * m2) = E(m1)*E(m2)$

Thus, very important homomorphic properties of the schemes were verified.