Motivation

Homomorphic encryption allows some operation to be done on the encrypted data.

Paillier cryptosystem is a partial homomorphic encryption scheme that supports addition of ciphertexts, which means anyone can compute the encryption of the addition of two independent messages (m1, m2) as long as the encryption of m1 and the encryption of m2 are given.

Privacy Preserving Photo Sharing
Mentee: Xusheng Zhang
Mentor: Naveed Muhammad

Facebook and other social networking providers store users’ photo and they have access to all of the photos, which raises many privacy concerns.

Naive Solution

After uploading, users intent to edit pictures using Facebook’s image processing services.

Naive encryption could offer privacy, but then photo services of Facebook would not work.

Operations we support

- flipping
- scaling
- blurring
- brightness correction
- rotation 90, 180, 270

Facebook can perform image processing operations on the encrypted image.

Facebook can’t see the contents of the photo.

Our System

The decrypted picture would be the original picture after flipping.

Acknowledgement

Special thanks to my mentor Naveed Muhammad and P.U.R.E Commitee.