Final Project proposal

Matrix in cryptography

The characteristic of an invertible matrix makes it perfect for encrypt and decrypt message. And one of the most well-known algorithms is Hill cipher. The key matrix is used to encrypt the messages, and its inverse is used to decrypt the encoded messages. It is important that the key matrix be kept secret between the message senders and intended recipients. If the key matrix or its inverse is discovered, then all intercepted messages can be easily decoded [1].

Let me give you a simple example. If I want to encrypt 'cat'. $[3 \quad 1 \quad 20]$ will be the corresponding matrix based on the alphabetical order. Let's say we have an invertible matrix

$$A = \begin{bmatrix} 1 & -4 & 2 \\ -2 & 1 & 3 \\ 2 & 6 & 8 \end{bmatrix}$$

We can encrypt it in the following:

$$[3 \quad 1 \quad 20]\begin{bmatrix} 1 & -4 & 2 \\ -2 & 1 & 3 \\ 2 & 6 & 8 \end{bmatrix} = [41 \quad 109 \quad 169]$$

To decrypt the matrix, we just need to multiply A^{-1} then we can get $[3 \quad 1 \quad 20]$ back.

But matrix can not only be just the key to encrypt and decrypt data. In homomorphic encryption, the difference between BFV and BGV is also a topic that I want to dive into. They both use matrix to perform homomorphic encryption. By rotating the matrix, the speed to encrypt the data can be improved. I think I will focus on talking about how does the BFV(Brakerski/Fan-Vercauteren)/BGV homomorphic encryption works and compare these two methods.

There're also some discussions about eigenvalue in cryptography. I think that's also interesting to me. So maybe I will also talk about how those two can be related

Generally, I will start with hill cipher algorithm, then talk about BFV and BGV homomorphic encryption and finally having some discussions talking about things like eigenvalues in cryptography something like that.

Reference

[1]: Joseph Pugliano and Brandon Sehestedt, *Cryptography: Matrices and Encryption*