GGH Cryptosystem

The complexity of solving CVP (Closest Vector Problem) has been proved to be NP-Hard on average cases, the GGH Cryptosystem is based on the hardness of solving CVP. The GGH Cryptosystem has two parameters, the dimension ‘n’ and the security parameter ’. The Private Key constructed is an approximately orthogonal basis considered as good basis and the Public Key constructed is a bad basis which is not close to being orthogonal. The Babai’s rounding off algorithm, for the target point, the good basis can find the closest lattice point with a high possibility while the bad basis cannot compute CVP (Closest Vector Problem) in the lattice. The paper we chose proposes two addition functions to prevent the information leakage, namely and .

**Algorithm:**

1. Key Generation: Party 1 starts constructing a Private Key V,

Here, . The columns in V are reasonably orthogonal to each other.

A Public Key W can be created by computing,

Here, ‘U’ is a random unimodular matrix with .

1. Encryption: The ciphertext can be computed by,

Here, ‘m’ is the message to be encrypted while ‘E’ is a randomly chosen error matrix, .

An additional function here takes cipher text ‘C’ as input and shuffles it to generate ‘Cout’.

1. Decryption: To decrypt the cipher text ‘Cout’,

Here, , reconstructs the cipher text C.

And then compute,

Here, ‘round()’ is the Babai’s rounding technique.