User enter a random number

Stores (ID, S­k, hash)

Generate secret key using (hash, msk, x)

User generates a master secret key(msk) from hash value

Take the hash of the random number

User computes c=Encrypt(hash, msk, y)

If d<T, verified

Calculate hamming distance,d =(x-z)/2

Server decrypt(hash, sk, c)