CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

Group Name: Goldfish
Akshay Kumar Chittora (21111007), Alok Kumar Trivedi (21111008), Jeet Sarangi (21111032)

End Semester Examination

Submission Deadline:
May 5, 2022, 11:55hrs

Solution 1

Lattice

Your solution goes here.
As given in the question defination:

$$\hat{L} = U * L * R$$

Then,$\hat{L}$ =U*n*I*R (As per the defination of L in the question)
Now,

$$\hat{L} = U * n * R$$

Here, U is an unitary matrix as given in the question as $|U| = 1$.
Let n*R be a matrix A.So,

$$\hat{L} = U * A$$

Now, we can say that A has orthogonal bases as A = n*R and where R is an Orthogonal matrix which will have orthonormal rows/ column vectors but A will not have orthonormal rows/columns but will definitely have orthogonal rows/columns which will have magnitude n.
Hence, as per the theorem given in "Galbraith, 2012" we can say that $\hat{L}$ will also have orthogonal bases and will span the same lattice as A that is n*R.Reason for this is U is an unitary matrix and A has Orthogonal basis.

[pro] [Ort] [Ngu99]

Decryption

As we know
L̂ = U*L*R
,Given that, L̂ is Public key and R is Private key
Plaintext m is an n bit long vector filled with binary entries.
We define encrypted text as
c = V*L̂ + m
where V is a random vector $\in Z^n$
For Decryption of the encrypted message by the receiver, we determine

$$\begin{aligned} d &= c * R^T \\ &= (V * \hat{L} + m) * R^T \\ &= (V * (U * L * R) + m) * R^T \\ &= V * U * L * R * R^T + m * R^T \\ &= V * U * L + m * R^T \qquad \text{as } R * R^T = I \end{aligned} \tag{2.1}$$

Upon Taking d modulo n , V*U*L matrix will become a zero matrix
as L is diagonal matrix with n in diagonal , U is a unitary matrix $\in Z^n$ and V is a random vector $\in Z^n$
As plain text m has only binary values and and R^T is orthogonal matrix with vector length 1, so they wont be affected by the modulo n operation.
Hence ,$\hat{d} = m * R^T$
Now ,

$$\hat{d} * R = m * R^T * R = m$$

as R is a Square matrix and $R * R^T = I$, so $R^T * R = I$
As we can see we are able to find out m, hence we can say that decryption works correctly.
[?] [Ort] [Ngu99]

Cryptosystem Security

We have been
Given

$$c = v.\hat{L} + m$$

Assuming we have an orthogonal basis of lattice as $[e_i]$ for i=1 to n. Taking $c = v.\hat{L} + m$ and the orthogonal basis $[x_i]$ and doing the eucledian inner product, we get,

$$< c, e_i > = < v\hat{L} + m, e_i >$$

Then,this can be written as

$$< c, e_i > = < v\hat{L}, e_i > + < m, e_i >$$

Here $<, >$ represents eucledian inner dot product or the dot product. We can write,

$$< v\hat{L}, e_i > = < c, e_i > - < m, e_i >$$

Taking $< v\hat{L}, e_i >$ as v_i and$< c, e_i >$ as c_i We can say that,

$$v_i = c_i - < m, e_i >$$

And we can also write,

$$v\hat{L} = \sum v_i.e_i$$

As e_i is the orthogonal basis of $\hat{L}$ and $v\hat{L}$ would be one of the element in this lattice produced by $\hat{L}$.
In the above equation since e_i is known and replacing v_i with the $c_i - < m, e_i >$

$$v\hat{L} = \sum (c_i - < m, e_i >).e_i$$

we can see that v_i is only the function of m_i as we know all c_i and e_i
Finally, We can represent $v\hat{L}$ in terms of m as

$$f(c_1, c_2, ..., c_n, m_1, m_2, m_3, m_4, ...m_n)$$

$v\hat{L}$ is now can be seen as a function of c_i,m,and e_i

Then, as we know

$$c = v\hat{L} + m$$

We can use $v\hat{L} = \sum(c_i - < m, e_i >).e_i$ to replace $v\hat{L}$ as

$$c = \sum(c_i - < m, e_i >).e_i + m$$

and we get the above equation only in terms of m_i, c_i, e_i which has only m_i as unknowns.

Hence we can get n linear equations for each i from 1 to n which will have unknowns as $f(m_1, m_2, ...m_n)$.

Then in order to solve these n linear equations we can use Gaussian elimination method to solve the above n equations in polynomial time. Hence we are able to find out m using a orthogonal basic of $\hat{L}$ and hence the security is broken.

Other ways to break the security

We will be using Babai's Closest Vector algorithm to break the security.
As encrypted message is c = v*L̂ + m
In order to leak some information about we will take modulus of c with 2*n and add a vector s which contains values only in multiples of n
c + s = v* + m + s (mod 2*n)
c + s = m (mod 2*n)
Now , we will denote m $(mod 2 * n)$ as $m2s$
Now we will subtract
c - m2s = (m - m2s) + v*L̂ As (m - m2s) is a vector of form 2*n*m$_p$
$c - m2s = 2 * n * m_p + v * \hat{L}$
(c - m2s)/2*n = m$_p + v * \hat{L}/2 * n$
we will call,
(c - m2s)/2*n as c$_p$
so, c$_p = m_p + v * \hat{L}/2 * n$
We have changed the original close vector problem to a reduced close vector problem , where it is easier to extract the original message by using the same process as we did above.This way we can break the security again.

[?] [Ngu99] [GGH]

References

[GGH] The GGH Cryptosystem. https://kel.bz/post/lattices/. Accessed: 2016-11-23.

[Ngu99] Phong Q. Nguyen. Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 288–304. Springer, 1999.

[Ort] Orthonormal Vectors, Orthogonal Matrices and Hadamard Matrix. https://medium.com/linear-algebra/part-23-orthonormal-vectors-orthogonal-matrices-and-hadamard-matrix-bee6857c05c ~:text=A%20square%20matrix%20whose%20columns,will%20be%20an%20orthogonal%20matrix. Accessed: 2016-11-23.

[pro] Property. https://math.stackexchange.com/questions/3852/if-ab-i-then-ba-i. Accessed: 2016-11-23.