CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

End Semester Examination

Group Name: Noobs
Manu Shukla (21111040), Divyansh Bisht (21111027), Rishabh Lakhwani (18817611)

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

Solution 1

[lat22][GGH22]

(a)

In this question, we need to prove that lattice generated by $\hat{L}$ has a basis consisting of n orthogonal vectors, each of length n. According to the question, we are given that:

$L = n \cdot I$, where n is an integer and I is an n * n identity matrix.

U is a unitary matrix, i.e., detU=1

R is a rigid rotation matrix,i.e., $R \cdot R^T = I$.

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

Now, we'll try to prove that lattice generated by $\hat{L}$ has a basis consisting of n orthogonal vectors, each of length n. All matrices U,L and R are n*n matrices and R is also rational. So, we can conclude that $\hat{L} \in Q^{n*n}$.

Lemma: B and C generate the same lattice if they are related by a unitary matrix as $B = U \cdot C$.

Proof: The lattice generated by a matrix B is the set: $\mathcal{L}(B) = \{x \cdot B : x \in Z\}$, where x is a row vector. Also, if U is a unitary, clearly U^{-1} is also unitary, as $det(U) \cdot det(U^{-1}) = 1$. Thus, if $B = U \cdot C$, then $C = U^{-1} \cdot B$. Clearly, as $x \cdot B = xU \cdot C$, where x is a row vector, thus $\mathcal{L}(B) \subseteq \mathcal{L}(C)$. Also, as $C = U^{-1} \cdot B$, thus $\mathcal{L}(C) \subseteq \mathcal{L}(B)$. The above two statements prove that $\mathcal{L}(C) = \mathcal{L}(B)$.

Using the above lemma we can say that the lattice generated by $U.(nR)$ is same as nR and we know that $\hat{L} = n.U.(R) = U.(nR)$ which means that $\hat{L}$ has same lattice as (nR).Now we are given $R.R^T = R^T \cdot R = I$ so R is an orthogonal matrix and we know

that rows of orthogonal matrix form orthogonal basis.Since R is orthogonal matrix so will be the nR matrix so lattice generated by $n.R$ will have orthogonal basis as rows of matrix n.R each of length n , thus using lemma we can say that lattice generated by $\hat{L} = U.(nR)$ also has orthogonal basis consisting n orthogonal vectors each of length n. Hence proved

(b)

To check whether decryption works correctly we first have to understand what's happening in the encryption part and check what do we have to prove. So in encryption we are choosing a random vector $v \in \mathbb{Z}^c$ .Now using $\hat{L}$ and v we are encoding a n-bit long message m which has only binary entries given in question and we output vector $c = v.\hat{L} + m$. As given in question $\hat{L} = U.L.R$ so we can write $c = n.v.U.R + m$.
Now while decrypting the message we have matrix R and now we are computing $d = c.R^T$ which can also be written as $d = n.v.U.R.R^T + m.R^T$ since $R.R^T = I$ so $d = n.v.U + m.R^T$.
As mentioned in the question(decryption part) $m = \hat{d}.R$. Since we have to calculate $\hat{d}$, now we have to take modulo n for every entry in the d which will make entry's values between 0 and $n - 1$ (all integer values). But we observe that ,since entries in matrix R are rational so entries in R^T will also be rational and taking mod of rational values won't be correct so to tackle this issue we calculate the **LCM** of the denominators of the entries in matrix R^T and make all entries have denominator = **LCM** and take this denominator out of the matrix so the entries will be integers in the matrix.We don't have to do the above process for $n.v.U$ since entries are integers already.We now re-write d as $d = n.v.U + \alpha.m.R'^T$ where α is the adjustment of entries of R^T using the LCM we discussed above and R'^T is the resultant matrix after adjustment .We observe that every entries of the matrix $n.v.U$ is multiple of n so when we modulo d with n this matrix will become zero matrix so we are basically calculation mod of $\alpha.m.R'^T$. Now the expression for d mod $n = \alpha.m.R'^T$ mod n.So to make absolute values of entries of d mod n $< n/2$ we will subtract n from the entry's whose values is $>= n/2$, since this will not affect their modulo and hence making absolute values $< n/2$ and the resulting matrix we get is $= \hat{d}$.So now we just have to prove $f = m$ where $f = \hat{d}.R$.

But wait a second we recall the entries of m is binary so now we will compute f mod n instead of first computing $\hat{d}$ or d mod n as we just have to find the position of non-zero entries in m since m has only binary entries. So f mod n = $\hat{d}.R$ mod n which is $= d.R$ mod n so

$f \bmod n = \alpha.m.R'^{T}.R \bmod n$.
R'= $p.R$ where p is some constant so $R'^{T}.R = p.I$ so now
$f \bmod n = \beta.m \bmod$ n where β is some constant but since we are only interested in finding the postions of the the non zero entries of m we can ignore β so
$f \bmod n = m \bmod n = m$ as entries of m are binary. Hence we have checked that decryption works correctly.

(c)

Now, we'll be checking if the decryption works correctly or not.
Let an orthogonal basis of $\hat{L}$ be $\hat{P}$.

Let the lattice formed by $\hat{L}$ be L.

We can write $\hat{P} = n\hat{L}$ (columns of $\hat{P}$ are linear combinations of columns of $\hat{L}$ since both are basis vectors)

$\hat{P}\hat{P}^T = (A\hat{L})(A\hat{L})^T$
$I = (AULR)(AULR)^T$
$I = AULRR^TL^TU^TA^T$
$I = AULL^TU^TA^T$
$I = n^2AUU^TA^T$
$LL^T = nI(nI)^T = n^2(I/n^2) = (AU)^T$
$AU = (\frac{1}{n^2})^T$
$\Rightarrow AU = (\frac{1}{n^2})$
$U = (\frac{A^{-1}I}{n^2})$

If we obtain U we can obtain private key R using U and public key $\hat{L}$.

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

Since, $\hat{P}$ is the basis vector for $\hat{L}$

$$\hat{c} = a\hat{P}$$

where a is one dimensional vector.

$$a = \hat{c}(\hat{P})^{-1}$$

Using babai's algorithm we round the elements of a to the nearest integers.
Let it be $\hat{a}$

$\hat{c}_1 = \hat{a}\hat{p}$
$\hat{c}_1$ is the closest point vector to $\hat{c}$
$m = |c - \hat{c}_1|$
Since the contents of m are binary bits we can easily retrieve m.
Hence, the decryption works correctly.

References

[GGH22] GGH. Link, 2022.

[lat22] Wiki lattices. Link, 2022.