CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

End Semester Examination

Group Name: Lazarus
Aditya Loth (21111004), Harsh Agarwal (21111030), Varun Vankudre (21111064)

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

Solution 1

Lattice

A Matrix $A \in \mathbb{Z}^{n \times n}$ is called Unimodular Matrix if $|A| = \pm 1$.

If A is Unimodular then A^{-1} is Unimodular and also $A^{-1} \in \mathbb{Z}^{n \times n}$

Note :- As we are doing $v \cdot \hat{L}$ as part of encryption, therefore v should be a row vector and so vectors in $\hat{L}$ and all other basis are also considered to be row vectors.

Theorem 1.1. Two bases $B_1, B_2 \in \mathbb{Q}^{n \times n}$ are equivalent if and only if $B_2 = A \cdot B_1$ for some Unimodular Matrix A [DS]

Proof. For first direction , lets assume that $\mathcal{L}(B_2) = \mathcal{L}(B_1)$ ($\mathcal{L}(O)$ represents Lattice generated by basis matrix O).
Then for each of the n rows b_i of B_2 , $b_i \in \mathcal{L}(B_1)$. This implies that there exists an integer matrix $A_1 \in \mathbb{Z}^{n \times n}$ for which $B_2 = A_1 \cdot B_1$.
Similarly, there exists a matrix $A_2 \in \mathbb{Z}^{n \times n}$ such that $B_1 = A_2 \cdot B_2$.
Hence ,

$$\begin{aligned} B_2 &= A_1 \cdot B_1 \\ &= (A_1 \cdot A_2) \cdot B_2 \end{aligned}$$

Post-Multiply by B_2^T on both sides we get,

$$B_2 \cdot B_2^T = (A_1 \cdot A_2) \cdot B_2 \cdot B_2^T \cdot (A_1 \cdot A_2)^T$$

Taking Determinant on both sides, we get

$$|B_2 \cdot B_2^T| = |B_2 \cdot B_2^T| * (|A_1 \cdot A_2|)^2$$

This means that

$$|A_1 \cdot A_2| = \pm 1$$

Since A_1, A_2 are both integer matrices, this means that $|A_1| = \pm 1$ as required

For other direction, assume that $B_2 = A_1 \cdot B_1$ for some Unimodular matrix A_1. Therefore each row of B_2 is contained in $\mathcal{L}(B_1)$ and we get $\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1)$. In addition, $B_1 = A_1^{-1} \cdot B_2$ and since A_1^{-1} is Unimodular as stated above, we similarly get that $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$. So we can conclude that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ as required. □

We know that $R \in \mathbb{Q}^{n \times n}$ and it is given in question that $R \cdot R^T = 1$. Therefore R, R^T are both orthogonal matrix. Therefore we can conclude that any two rows or columns of R are orthogonal to each other. Same is the case for R^T

If we multiply all the elements of R with a scalar s then still any two rows or columns are orthogonal to each other. Same is observed for R^T

Let lattice generated by $n \cdot R$ be $\mathcal{L}(nR)$.

Let lattice generated by $\hat{L}$ be $\mathcal{L}(\hat{L})$.

Using Theorem 1.1 we can prove that $\mathcal{L}(nR) = \mathcal{L}(\hat{L})$, if we are able to find an Unimodular matrix, say U_n that relates $\hat{L} = U_n \cdot (n \cdot R)$.

$$
\begin{aligned}
\hat{L} &= U \cdot L \cdot R \\
&= U \cdot n \cdot I \cdot R \quad (L = n \cdot I \text{ is given}) \\
&= U \cdot n \cdot R \quad (I \cdot R = R \text{ as I is identity matrix}) \\
\hat{L} &= U \cdot (n \cdot R)
\end{aligned}
$$

In the above equation U is an Unimodular Matrix as it is given in the question that $|U| = 1$ and $U \in \mathbb{Z}^{n \times n}$

So we can conclude that $\mathcal{L}(nR) = \mathcal{L}(\hat{L})$ as there exists an Unimodular Matrix U such that $\hat{L} = U \cdot (n \cdot R)$.

Now as $n \cdot R$ is also a basis of lattice generated by $\hat{L}$. We can conclude that lattice generated by $\hat{L}$ has a basis consisting of n orthogonal vectors each of length n because as previously stated that $R \in \mathbb{Q}^{n \times n}$, so any two rows of R is orthogonal with respect to each other and length of each row is n and there are n rows in R. Also as stated above, multiplying two orthogonal vectors by same scalar, does not affect thier orthogonality and in our case this scalar is n.

So in conclusion we can say that each of the n row's of $n \cdot R$ matrix is an orthogonal vector of length n in basis of lattice generated by $\hat{L}$

Decryption

It is given that ,

$L = n \cdot I$ and $L \in \mathbb{Z}^{n \times n}$

$U \in \mathbb{Z}^{n \times n}$ and is a Unitary Matrix, that is $|U| = 1$

$R \in \mathbb{Q}^{n \times n}$ and is a Rigid Rotation Matrix, that is $R \cdot R^T = 1$ therefore R,R^T are Orthogonal Matrix

$$\begin{aligned}
\hat{L} &= U \cdot L \cdot R \\
&= U \cdot n \cdot I \cdot R \quad (L = n \cdot I \text{ is given}) \\
&= U \cdot n \cdot R \quad (I \cdot R = R \text{ as I is identity matrix}) \\
\hat{L} &= n \cdot U \cdot R \quad \ldots\ldots \quad 1
\end{aligned}$$

$m \in \mathbb{Z}^n$ where entries are binary and therefore m is a n-bit long message with values 0 or 1

$v \in \mathbb{Z}^n$ is a random vector

$$c = v \cdot \hat{L} + m \quad \ldots\ldots \quad 2$$

$$\begin{aligned}
d &= c \cdot R^T \\
&= (v \cdot \hat{L} + m) \cdot R^T \qquad \text{(From 2)} \\
&= (v \cdot n \cdot U \cdot R + m) \cdot R^T \qquad \text{(From 1)} \\
&= (n \cdot v \cdot U \cdot R + m) \cdot R^T \\
&= n \cdot v \cdot U \cdot R \cdot R^T + m \cdot R^T \\
&= n \cdot v \cdot U + m \cdot R^T \qquad \text{(As } R \cdot R^T = 1 \text{ as already given)}
\end{aligned}$$

$$
\begin{aligned}
\hat{d} &= d \mod n \\
&= (n \cdot v \cdot U + m \cdot R^T) \mod n \\
&= [(n \cdot v \cdot U) \mod n + (m \cdot R^T) \mod n] \mod n \\
&= [0 + (m \cdot R^T) \mod n] \mod n \quad \text{(As } n \cdot v \cdot U \text{ is a multiple of n, therefore modulo n is 0)} \\
&= (m \cdot R^T) \mod n
\end{aligned}
$$

Taking norm of m

$$norm(m) = \|m\| = \sqrt{\sum_{i=1}^{n} (m_i)^2}$$

As the bit of the message only can either be 0 or 1 hence the maximum value can be $\sqrt{n}$

Let P be the resultant matrix after applying rigid rotation to message m

$$P = m \cdot R^T$$

Hence $\|P\|_{max} = \|m\|_{max} = \sqrt{n} = \max\left(\sqrt{\sum_{i=1}^{n} P_i^2}\right)$

For $n > 4$, $n/2$ is always greater than $\sqrt{n}$

$$\hat{d} = m \cdot R^T \qquad \ldots\ldots (3)$$

$$
\begin{aligned}
m &= \hat{d} \cdot R \\
&= m \cdot R^T \cdot R \qquad \text{(From 3)} \\
&= m \qquad (R^T \cdot R = 1 \text{ , given earlier)}
\end{aligned}
$$

As can be seen Left Hand Side is equal to Right Hand Side, therefore decryption works correctly.

Cryptosystem Security

Breaking using Orthogonal Basis

We know that,

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

Let orthogonal basis of lattice generated by $\hat{L}$ be O

Then $\forall i \in [1, n]$

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

where, $< a, b >$ is the Euclidean inner product in $\mathbb{R}^n$

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

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

For simplicity lets rewrite above equation as

$$v_i = c_i - < m, O_i > \cdots\cdots (I)$$

where, v_i is $< v \cdot \hat{L}, O_i >$ and c_i is $< c_i, O_i >$

Therefore, $v_i = f(c_i, m_1, \ldots, m_n)$

We know that $v \cdot \hat{L}$ is an vector in lattice generated by $\hat{L}$, so we can say that

$$v \cdot \hat{L} = \sum_{i=1}^{n} v_i \cdot O_i$$

Using (I) , As we know O, we can write $v \cdot \hat{L}$ in terms of $c = (c_1, \ldots, c_n)$ and $m = (m_1, \ldots, m_n)$

$$v \cdot \hat{L} = F(c_1, \ldots, c_n, m_1, \ldots, m_n) \cdots\cdots (II)$$

Substituting (II) in $c = v \cdot L + m$, we get

$$c = F(c_1, \ldots, c_n, m_1, \ldots, m_n) + m$$

In above equation only unknowns are m, therefore we get n linear simultaneous equations, which we can solve using Gaussian elimination method efficiently.

NOTE : We can also use Babai's Rounding Technique to break the cryptosystem using Orthogonal basis efficiently. We have detailed this procedure on next page

Other Ways To Break Cryptosystem

Good and Bad Basis

Any lattice in dimension of 2 and above have infinitely many bases. These bases are categorized into two categories, that is good and bad basis, based on two parameters, their length or norm and orthogonality of basis vectors. A lattice basis with long and non-orthogonal basis vectors are categorized as bad basis generally and a lattice basis with short and orthogonal basis vectors is generally categorized as good basis.[MKA19]

Babai's Rounding Technique

Babai's Rounding Technique [Gal12] is an alternative to Babai's Nearest Plane method. It does not require computing a Gram-Schmidt basis, so it is computationally inexpensive. This method works for any basis of a lattice but its efficiency depends on type of basis.

When Babai's Rounding Technique is used with a basis categorized as good, then the method works efficiently by finding a lattice vector that is close to the target vector. When used with a basis categorized as bad, then the algorithm works inefficiently by returning a lattice vector which is far from the target vector.[MKA19]

Let $b_1, \ldots, b_n \in \mathbb{Q}^{n \times n}$ be a basis of lattice generated by $\hat{L}$ and denoted by $\mathbb{B}$.

Our target vector is $c \in \mathbb{Q}^n$, which is our cipher text. Then we can say

$$c = \sum_{i=1}^{n} a_i \cdot b_i$$

where $a_i \in \mathbb{R}$. We can compute values of $a_i \forall i \in [1, n]$ by either solving a system of n linear simultaneous equations or by computing vector $c \cdot B^{-1}$.

Once all a_i values have been computed, then we compute a_i' by taking closest integer to real number a_i. Then using a_i' values, we compute a vector in lattice which is close to our target vector c as

$$w = \sum_{i=1}^{n} a_i' \cdot b_i$$

Therefore we can compute $m_i = |c_i - w_i| \ \forall i \in [1, n]$

Embedding Technique

The success of embedding technique [Gal12] depends on the size of m compared with the length of short vectors in the original lattice generated by $\hat{L}$.

Let B be a basis of lattice generated by $\hat{L}$ and $c \in \mathbb{Q}^n$ is the cipher-text.
One Crucial criteria for efficiency of this technique is that the magnitude of error (in our case message) should be small , that is

$$m = c - \sum_{i=1}^{n} a_i \cdot b_i$$

where $a_i \ in \mathbb{Z}$. Then $||m|| shouldbesmall$
Define a Lattice L' that contains short vector m. Let $M \in \mathbb{Q}_{>0}$. The Lattice L' is defined by the vectors which are basis for $\mathbb{Q}^{n+1}$

$$(b_1, 0), \ldots\ldots, (b_n, 0), (c, M)$$

If we take linear combination of rows with coefficients $(-a_1, \cdots, -l_n, 1)$, we get a vector

$$(m, M)$$

Hence, we might be able to find m by solving the Shortest Vector problem in the Lattice L'

References

[DS] V. Bronstein D. Sieradzki. Introduction to lattice.

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, USA, 1st edition, 2012.

[MKA19] A Mandangan, H Kamarulhaili, and M A Asbullah. Good basis vs bad basis: On the ability of Babai's Round-off Method for solving the Closest Vector Problem. *Journal of Physics: Conference Series*, 1366(1):012016, nov 2019.