CS641

Modern Cryptology
Indian Institute of Technology, Kanpur

Group Name: Enciphered
Anindya Ganguly (21111261), Gargi Sarkar,
Utkarsh Srivastva

End Semester Examination

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

Solution 1

Lattice

- **Method: 1**
  Idea: Since $\hat{L}$ is a non singular, so it has a n basis element each of them has length n. So, in hand we have basis. Also note that $\hat{L}$ is matrix having coefficient from $\mathbb{Q} \subset \mathbb{R}$. Apply GSO to get an orthogonal basis. This completes the proof. Here we use l_2 norm.

  We know that $\hat{L} = U \cdot L \cdot R$. In addition we also have $R \cdot R^T = 1$, and $L = nI$. So

  $$\det(\hat{L}) = \det(U) \cdot \det(L) \cdot \det(R) = 1 \cdot (n.1) \cdot \pm 1 = \pm n$$

  Since n is nonzero, thus $\hat{L}$ is a $n \times n$ non-singular matrix. Suppose $\{a_1, a_2, \cdots, a_n\}$ is the basis of the corresponding matrix. Now we use the Gram Schmidt Orthogonalization (GSO) mechanism to construct an orthogonal basis[1]. Suppose $\{v_1, v_2, \cdots, v_n\}$ denotes the orthogonal basis computed via GSO.

  Here we are explaining the GSO.

  $$\begin{aligned} v_1 &= a_1 \\ v_2 &= a_2 - \frac{\langle a_2, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 \\ v_3 &= a_3 - \frac{\langle a_3, v_1 \rangle}{\langle v_1, v_1 \rangle} v_1 - \frac{\langle a_3, v_2 \rangle}{\langle v_2, v_2 \rangle} v_2 \end{aligned}$$

$$\vdots$$

$$v_n = a_n - \frac{\langle a_n, v_1\rangle}{\langle v_1, v_1\rangle} v_1 - \cdots - \frac{\langle a_n, v_{n-1}\rangle}{\langle v_{n-1}, v_{n-1}\rangle} v_n$$

Each v_i has length n, since a_i has length n. Thus $\hat{L}$ has a basis consisting of n orthogonal vectors, each of length n.

- **Method: 2**

  Statement: Two bases $B_1, B_2 \in \mathbb{R}^{m\times n}$ are equivalent if and only if $B_2 = B_1 U$ for some unimodular matrix U.

  Proof: First assume that $\mathcal{L}(B_1) = \mathcal{L}(B2)$. Then for each of the n columns b_i of $B_2, b_i \in \mathcal{L}(B_1)$. This implies that there exists an integer matrix $U \in \mathbb{Z}^{nn}$ for which $B_2 = B_1 U$. Similarly, there exists a $V \in \mathbb{Z}^{n\times n}$ such that $B_1 = B_2 V$. Hence $B_2 = B_1 U = B_2 V U$, and we get $B_2^T B_2 = (VU)^T B_2^T B_2 (VU)$. Taking determinants, we obtain that $\det(B_2^T B_2) = (\det(VU))^2 \det(B_2^T B_2)$and hence $\det(V)\det(U) = \pm 1$. Since V, U are both integer matrices, this means that $\det(U) = \pm 1$, as required. For the other direction, assume that $B_2 = B_1 U$ for some unimodular matrix U . Therefore each column of B_2 is contained in $\mathcal{L}(B_1)$ and we get $\mathcal{L}(B_2) \subseteq \mathcal{L}(B_1)$. In addition, $B_1 = B_2 U^{-1}$, and since U^{-1} is unimodular we similarly get that $\mathcal{L}(B_1) \subseteq \mathcal{L}(B_2)$. We conclude that $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ as required. (Proof is available in Oded Regev's class notes.)

  Now we apply it. Since L and R^T are already orthogonal matrix, so it has an orthogonal basis, that is $L \cdot R^T$ has an orthogonal basis. Marked this product matrix as L_1. Thus $\hat{L} = U \cdot L_1$, where $U \in \mathbb{Z}^{n\times n}$ is an unitary matrix, that is, $\det U = 1$. Thus we have $\hat{L} = U \cdot L_1$. Now apply above theorem here. This says that $\hat{L}$ and L_1 has same basis, as L_1 has an orthogonal basis of length n so $\hat{L}$ has also an orthogonal basis of length n.

Decryption

Goal is to establish the relation $m = \hat{d} \cdot R^T$

1. Given that ciphertext $c = v \cdot \hat{L} + m$
2. In decryption part receiver computes $d = c \cdot R^T$.
3. Now mathematically simplify above equation.

$$\begin{aligned} d =& (v\hat{L} + m) \cdot R^T \\ =& v \cdot \hat{L} \cdot R^T + mR^T \end{aligned}$$

4. From key generation phase we know that $\hat{L} = U \cdot L \cdot R$
5. In addition we also have $R \cdot R^T = 1$, and $L = nI$
6. We deploy these knowledge,

$$\begin{aligned} d =& v \cdot (U \cdot L \cdot R) \cdot R^T + mR^T \\ =& v \cdot U \cdot n(I * I) + mR^T \\ =& nvU + mR^T \end{aligned}$$

7. Reduce every entry of d modulo n so that the entry becomes $< n/2$ in absolute value. Let the resulting vector be $\hat{d}$.

$$\begin{aligned} \hat{d} =& (nvU + mR^T) \mod n \\ =& mR^T \end{aligned}$$

8. Compute $\hat{d} \cdot R = mR^T \cdot R = m$
9. Hence this establishes the correctness of the decryption algorithm

Cryptosystem Security

- **Part: 1** Encryption scheme tells us that $c = v\hat{L} + m$. Now assuming that we have an orthogonal basis $\{e_i\}_{i=1}^{n}$ of lattice generated by $\hat{L}$ this tells us that

  $$< c, e_i > = < v\hat{L} + m, e_i >, \forall i \in \{1, 2...n\}$$

  where $\langle , \rangle$ is the Euclidean inner product l_2 in $\mathbb{R}^n$

  $$\Rightarrow \langle c, e_i \rangle = < v\hat{L}, e_i > + < m, e_i > \text{ due to the linearity of ip}$$
  $$\Rightarrow c_i = v_i + < m, e_i >, \forall i \in \{1, 2...n\} \text{ where } c_i = < c, e_i >, v_i = < v\hat{L}, e_i >$$

  as $\{e_i\}_{i=1}^{n}$ is a orthogonal basis of lattice $\hat{L}$ and as $v\hat{L}$ is an element in the lattice , hence
  $$v\hat{L} = \sum_{i=1}^{n} v_i e_i$$
  as $\{e_i\}_{i=1}^{n}$ is known , we can represent $v\hat{L}$ in term of $m = (m_1, m_2...m_n)$ and thus obtained a system of n linear equations in $m = (m_1, m_2...m_n)$. This trick can be handled by Gaussian Elimination in polynomial time. Now, we came to retrieve m, one should know $v\hat{L}$ or in other words we have to know v but to $v\hat{L}$ we basically need to know its reciprocal in an orthogonal basis of $\hat{L}$.

  So the problem reduces to finding an orthogonal basis of lattice generated by $\hat{L}$. Finding an orthogonal basis essentially involves solving a no linear system of equation with integral solution, which is a Hard Problem.

- **Part: 2** Here we are putting some important observations. These help us to break the cryptosystem.

  $\mathcal{O}$: denotes the encryption oracle.
  $\mathcal{A}$: denotes adversary who wants to break the cryptosystem.

  Suppose m_1 and m_2 are two plaintexts/messages. Now call $\mathcal{O}$ for encryption and get

  $$c_1 = v \cdot \hat{L} + m_1$$
  $$c_2 = v \cdot \hat{L} + m_2$$

So, v is fixed for both the encryption the retrieving the message is easy with one message-ciphertext pair. Because, the relation tells $c_1 - c_2 = m_1 - m_2$. If (m_1, c_1) is the known message-ciphertext pair, then $m_2 = m_1 - (c_1 - c_2)$.

We know that $\hat{L} = U \cdot L \cdot R$. Goal is to retrieve U or R from $\hat{L}$. Knowing one matrix helps to get back another matrix. We now decompose the matrix $\hat{L}$. Apply singular value decomposition on $\hat{L}$. Since $\det(U) = 1$, so eigen values of U has modula 1, similarly for R also. So the diagonal matrix L has the eigen values L which are n. $\hat{L} \cdot \hat{L}^T = (U \cdot L \cdot R) \cdot (R^T \cdot L^T \cdot U^T) = U \cdot L^2 \cdot U^T$. Now clearly L^2 has eigen values n^2 and U is orthonormal eigen vector of $\hat{L} \cdot L$, similarly R^T has orthonormal eigen vectors of $\hat{L}^T \cdot \hat{L}$. So with the knowledge of $\hat{L}$ and $\hat{L}^T$ we can able to decompose the matrix $\hat{L}$. IN addition the singular value decomposition is "almost unique".

References

[1] Von Zur Gathen, Joachim, and Jürgen Gerhard. Modern computer algebra. Cambridge university press, 2013.