111550113 謝詠晴

Cryptography Engineering Quiz. 6

Problem 1

a) **Please showcase the recursive process of the Walsh-Hadamard Transform using the pseudocode provided above.**

Recursive process:

1. Define the 1*1 Hadamard Transform $H_0 = 1$
2. For m>0, Define $H_m = \frac{1}{\sqrt{2}}\begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}$ Sometimes, we will omit $\frac{1}{\sqrt{2}}$ which is used for normalization.
3. The recurrence relation is mostly represented as $H_m = H_1 \otimes H_{m-1}$. $\otimes$ is the symbol of Kronecker product.

   Its definition is: $A \otimes B = \begin{pmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{pmatrix}$

   * For example,

   $H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

   $H_2 = H_1 \otimes H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

   $= \left[\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right]$

4. The provided pseudocode is the iterative version. If implemented in recursive version, the base case occurs when the len(x) is 1. And we will adjust the length of the signal to the nearest power of 2 same as in iterative version before computing. Then, we split the signal into two halves and repeated this splitting process recursively until reaching the base case. After obtaining the two halves, we combine them as [left + right, left - right] and do normalization.

b) **Examine different applications of the Walsh-Hadamard Transform, highlighting how its properties offer advantages in each specific application.**

1. Image compression:

   One of the key properties of the WHT is energy concentration, this property allows for efficient image compression. Images are typically divided into blocks, and the WHT is applied to each block independently.

2. Signal processing:

   The WHT basis functions are orthogonal, facilitating efficient signal representation and compression. Algorithms like the Fast Walsh-Hadamard Transform (FWHT) provide computational efficiency, making the WHT suitable for real-time signal processing applications.

3. Cryptography:

   WHT has various application in cryptography due to its properties such as orthogonality, balance, and good correlation properties. For example, it can be used in stream cipher, encryption, Pseudo-Random Sequence Generation, etc.

Problem 2

a) **What happens when we apply the Miller-Rabin test to numbers in the format pq, where p and q are large prime numbers?**

   The Miller-Rabin test has a high probability of detecting its compositeness. The test examines multiple random bases to identify whether pq is a composite number under modular operations. However, Miller-Robin is a probabilistic test, if the interval is quite large, there's a chance that it may result in false positive, given a wrong answer.

b) **Can we break RSA with it?**

   No, we cannot break RSA with Miller-Rabin test. RSA relies on the security assumption that factoring large composite numbers into their prime factors is computationally infeasible. And the Miller-Rabin test is only useful for identifying whether a number is likely composite by testing its primality with high probability but cannot effectively find the prime factors of a composite number.