BabyDH 2

The following text is generated by ChatGPT

This question mainly tests the participants' abilities in reading academic papers and programming. It requires participants to have a certain understanding of lattice reduction algorithms and the Coppersmith method.

Description

The question describes a scenario where the server simulates a DH key exchange between Alice and Bob. Subsequently, we, as a third party, can engage in a DH exchange with Alice, while also being provided with an additional Oracle that can be accessed multiple times. This Oracle can leak the low-order bits of the x-coordinate of the point negotiated between us and Alice. Our task is to recover the shared secret key negotiated between Alice and Bob.

求解思路

The scenario described in this question is equivalent to solving the ECHNP.

The participants need to programmatically reproduce the research presented at the 2022 AsiaCrypt conference. It's worth noting that the original paper discusses scenarios involving high-bit leakage. Therefore, modifications need to be made to the lattice construction for solving this question.

Note that the time limit for this question is relatively short. Considering this, it's advisable to use the flattertool for fast lattice reduction. Based on empirical testing, setting parameters n = 5，d = 3，t = 2, on a single-core Ubuntu virtual machine, the solution can be obtained in approximately 18 seconds.