CS674A Assignment

CS674A: Post Quantum Security
Indian Institute of Technology Kanpur

Instructor Dr. Debapriya Basu Roy

Course https://www.cse.iitk.ac.in/pages/CS798C.html

Instruction We encouraged discussions but you should implement your code and honorably acknowledge the sources if any. Make sure you have not copied from others (or internet resources) and do not share your solution with others. For such circumstances, you may have been heavily penalized. Dishonest behavior and cheating in the assignment will be penalized with extreme measures.

See: https://www.cse.iitk.ac.in/pages/AntiCheatingPolicy.html.

Kindly submit a ZIP folder at Hello IITK platform (do not email). Your name of the folder should be ROLLNO.zip, eg 21111261.zip. This folder should contains the code and a READme.

If you have any doubt regarding the assignment, please feel free to write Suraj Mandal (surajm22@iitk.ac.in).

Question 1

Write a software code for performing negative wrapped convolution using Number Theoretic Transformation (NTT) for the parameters $n = 512$, $q = 12289$, $\gamma = 10968$ for $R_q = \mathbb{Z}_q[X]/X^n + 1$. Your code must have three distinct functions:

- A function that will take the input in R_q and will convert the input into its corresponding NTT transformation using radix-2 Cooley-Tukey method.
- A function that will take the two inputs which are already transformed by NTT and will produce their point wise multiplication
- A function that will take the inputs in NTT transformed domain and will perform inverse NTT using the radix-2 Gentleman-Sande method.