Indian Institute of Technology, Kanpur

Proposal for a New Course

1. Course No: CS710
2. Course Title: **Lattice-Based Cryptography**
3. Per Week Lectures: **03** (L), Tutorial: **0** (T), Laboratory: **0** (P), Additional Hours[0-2]: **0** (A), Credits (3*L+2*T+P+A): **09** Duration of Course: **Full Semester**
4. Proposing Department/IDP : **Computer Science and Engineering**

   Other Departments/IDPs which may be interested in the proposed course:

   Other faculty members interested in teaching the proposed course:
5. Proposing Instructor(s): **Anshu Yadav**
6. Course Description:

   A) Objectives:

   With the rapid advancement of quantum computing, many classical cryptographic systems are expected to become insecure, motivating the study of post-quantum cryptography. Among the leading post-quantum candidates, lattice-based cryptography stands out due to its strong security guarantees and versatility.

   This course aims to provide a rigorous theoretical foundation of lattice-based cryptography, along with its applications in constructing various cryptographic primitives from lattice-based assumptions. The course will emphasize formal correctness and security proofs of these constructions.

   B) Contents (preferably in the form of 5 to 10 broad titles):

S. No	Broad Title	Topics	No. of Lectures
1	Foundations of Cryptography and motivation for Post-Quantum Cryptography	A quick refresher on basic cryptographic primitives (one-way functions (OWF), pseudorandom generators (PRG), pseudorandom function (PRF), secret key and public key encryption schemes, digital signatures), and formal security definitions; Classical hard problems and their quantum solutions; overview of post quantum cryptography domains (lattices, isogenies, code-based cryptography).	4

2	Introduction to Lattices	Lattices and lattice basis; hard problems in lattices and relations between them; LLL algorithm for lattice basis reduction and its application.	6
3	LWE and SIS problem and applications	LWE (search and decision) and SIS problem; worst case to average case hardness; trapdoor generation; variants and relationships; Constructions of basic cryptographic primitives from these assumptions, including OWF, secret key and public key encryption schemes, digital signatures.	12
4	Learning with Rounding (LWR)	Definition of LWR and reduction from LWE; construction of PRG and PRF from LWR.	4
5	Advanced cryptographic constructions from Lattices	Homomorphic encryptions and other selected advanced cryptographic primitives from lattice-based assumptions: definitions, formal constructions, various associated security notions and extensions.	11
6	Class Presentations	Class project involving reading and presenting research papers on foundational or advanced topics in cryptography.	3
Total			**40**

C) Pre-requisites, if any (examples: a- PSO201A,or b- PSO201A or equivalent):

No formal prerequisites. The course assumes mathematical maturity and involves rigorous analysis, including proofs and reductions. Familiarity and comfort with basic linear algebra and probability is required. Overall, interest and aptitude for theoretical computer science are expected.

D) Short summary for including in the Courses of Study Booklet.

This course focuses on introducing key concepts in lattices and building foundational as well as advanced cryptographic primitives with rigorous analysis.

Topics: Quick refresher on foundations of cryptography; introduction to lattices, lattice basis, and hard problems in lattices; Learning With Errors (LWE) and Short Integer Solution (SIS) problems; worst case to average case analysis; trapdoor generation; construction of basic cryptographic primitives from these assumptions, including OWF, secret key and public key encryption, and digital signatures; Learning With Rounding (LWR) and its applications; advanced cryptographic constructions from lattices, including homomorphic encryption schemes, and other expressive primitives, with different associated security definitions and extensions.

7. Recommended books:

   Textbooks: Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell

   Reference books: Foundations of Cryptography by Oded Goldreich Volume 1 and 2

   Other useful resources: Course webpages: Vinod Vaikuntanathan's course on Lattices, LWE and PQC, Oded Regev's course on Lattices in Computer Science, Shweta Agrawal's course on PQC, other similar course pages.

8. Any other remarks: Evaluation will consist of assignments, mid-semester and end-semester exams, and a paper reading project with class presentation and/or viva.

Dated: 18-03-2026 Proposer: Anshu Yadav

Dated: 18-March-2026 ~~DUGC~~/DPGC Convener:

The course is approved / not approved

Chairman, SUGC/SPGC

Dated: