Workshop on Lattice-based Post-Quantum Cryptography
July 17-19, 2023
Department of Computer Science, Ashoka University

[Schedule]

Day1: Jul 17, 2023

Session-1: 2 PM - 3:30 PM
Lattice Problems
Mahavir Jhawar

Tea Break

Session-2: 4 PM - 5:30 PM
Lattice Problems
Mahavir Jhawar

Day 2, Jul 18, 2023

Session-3: 9:30 AM - 11:00 AM
LWE Based Encryption
Mahavir Jhawar

Tea Break

Session-4: 11:30 AM - 1:00 PM
RLWE Based Encryption, ModuleLWE based Encryption: Kyber (NIST Standard) - Part1
Mahavir Jhawar

Lunch Break: 1 PM - 2 PM

Session-5: 2 PM - 3:30 PM
ModuleLWE based Encryption: Kyber (NIST Standard) - Part2
Mahavir Jhawar

Tea Break

Session-6: 4 PM - 5:30 PM
Lab for Encryption

Day3: Jul 19, 2023

Session-7: 9:30 AM - 11:00 AM
Lattice-based Signature Schemes
Mahavir Jhawar

Tea Break

Session-8: 11:30 AM - 1:00 PM
Lattice-based Signature Scheme Dilithium (NIST Standard)
Mahavir Jhawar

Lunch Break: 1 PM - 2 PM

Session-9: 2 PM - 3:30 PM
Key Management Framework with PQ Security
Mahavir Jhawar, Aarav Varshney, Adit Dhawan

Tea Break

Session-10: 4 PM - 5:30 PM
Key Management Framework with PQ Security
Mahavir Jhawar, Aarav Varshney, Adit Dhawan

Day1: Jul 17, 2023

Session-1: 2 PM - 3:30 PM
Topic: Lattice Problems

Tea Break

Session-2: 4 PM - 5:30 PM
Topic: Lattice Problems

Day 2, Jul 18, 2023

Session-3: 9:30 AM - 11:00 AM
Topic: LWE Based Encryption

Tea Break

Session-4: 11:30 AM - 1:00 PM
Topic: RLWE Based Encryption, ModuleLWE based Encryption: Kyber (NIST Standard) - Part1

Lunch Break: 1 PM - 2 PM

Session-5: 2 PM - 3:30 PM
Topic: ModuleLWE based Encryption: Kyber (NIST Standard) - Part2

Tea Break

Session-6: 4 PM - 5:30 PM
Topic: Lab for Encryption

==========

Day3: Jul 19, 2023

Session-7: 9:30 AM - 11:00 AM
Topic: Lattice-based Signature Schemes

Tea Break

Session-8: 11:30 AM - 1:00 PM
Topic: Lattice-based Signature Scheme Dilithium (NIST Standard)

Lunch Break: 1 PM - 2 PM

Session-9: 2 PM - 3:30 PM
Topic: Key Management Framework with PQ Security
Tea Break

Session-10: 4 PM - 5:30 PM
Key Management Framework with PQ Security

==========