Time: 3:30 PM, 2nd June, 2025

Location: KD101, Kadim Diwan Building

Speaker: Dr. Anshu Yadav

Title: Designing advanced cryptographic primitives in distributed settings.

Bio of Dr. Anshu Yadav

Dr. Anshu Yadav is currently a postdoctoral researcher at IST Austria in Prof. Krzysztof Pietrzak's group. She received her PhD from IIT Madras, guided by Prof. Shweta Agrawal. Her research interests are in the area of theoretical cryptography in building various cryptographic primitives largely from post-quantum lattice-based cryptographic assumptions and some from classical assumptions as well. She has worked on problems related to threshold and blind signatures, and multi-input attribute-based and functional encryption systems.

Details of the Talk

Title: Designing advanced cryptographic primitives in distributed settings.

Abstract:

In today's world, the rapid advancement of technology has led to the generation of vast amounts of sensitive data, which must be accessed in a secure and controlled manner to facilitate research across various domains. Often this data, associated with a single logical entity, is generated in a distributed manner, yet must be protected with the same level of security as if it were produced by a single source. Furthermore, distributing authority among multiple entities is essential to avoid a single point of security failure. These are natural, yet complex challenges in modern cryptography. My research focuses on exploring how advanced cryptographic primitives can provide effective solutions to such problems. In this talk, I will begin with a brief overview of my research interests and profile. I will then focus on the themes discussed above. In particular, I will briefly talk about a result on multi-input attribute based encryption which is a generalization of attribute-based encryption (ABE) - a novel encryption paradigm enabling expressive access control on encrypted data. In ABE, a message m is encrypted under an attribute x, and decryption keys are associated with a policy f. Decryption is possible if and only if $f(x)=1$, unlike traditional public key encryption scheme where a single key can decrypt all ciphertexts. In the multi-input setting, data is

generated by k non-interacting parties, with each party contributing an input (x_i, m_i), so that x=(x_1,...,x_k) and m=(m_1,...,m_k). The function f is now a k-ary predicate. The goal is for each party to independently encrypt their data as ct_1,...,ct_k, and for a decryption algorithm with key sk_f to recover (m_1,...,m_k) if and only if f(x_1,...,x_k)=1. We formally defined the notion of multi-input ABE (k-ABE) and presented constructions for different k under different cryptographic hardness assumptions. I will describe the key challenges in designing cryptographic schemes in the multi-input setting and how our work addresses these challenges. If time permits, I will also briefly talk about my work in threshold cryptography - a very useful and active field of cryptography with advanced practical applications in distributed environments (e.g., block chains, distributed key generation, etc.). In threshold cryptography, a privileged operations—such as 'signing' in digital signature scheme or 'decryption' in an encryption scheme—is distributed among n parties, ensuring that at least a threshold t of them are required to perform the operation. In this area, my research has mostly focussed on threshold signatures, where we improve the security of post-quantum threshold signature scheme. Finally, I will conclude the talk with a discussion of my future research directions, including open problems in the areas discussed above.