

**CHENNAI – PONDICHERRY**

**Secure Distributed Computing with Straggling Servers Using Polynomial Codes**

**Abstract**

In this paper, we consider a secure distributed computing scenario in which a master wants to perform matrix multiplication of confidential inputs with multiple workers in parallel. In such a setting, a master does not want to reveal information about the two input matrices to the workers in an information-theoretic sense. We propose a secure distributed computing scheme that can efficiently cope with straggling effects by applying polynomial codes on sub-tasks assigned to workers. The achievable recovery threshold, i.e., the number of workers that a master needs to wait for to get the final product, of our proposed scheme is revealed to be order-optimal to the number of workers. Moreover, we derive the achievable recovery threshold of the proposed scheme is within a constant multiplicative factor from information-theoretic lower bound. As a byproduct, we extend our strategy to secure distributed computing for convolution tasks on confidential data.