

# **Secure Distributed Computing**

**Speaker:**

**C. Pandurangan**

**Department of Computer Science & Engineering  
Indian Institute of Technology Madras**

## **Abstract**

Research in Secure Distributed computing is contributing to the foundations of both Distributed computing and Cryptology. This tutorial attempts to highlight the intricate and inherent relationship that exist between these areas and show how the challenges in both have lead to some exciting results in the recent past. We begin with a taxonomy for this area which allows one to categorize all the problems in this domain in a unified fashion and lead to more systematic study of this area. Then we discuss various protocols for secure message transmission that is perfect under various fault models such as passive, fail-stop, Byzantine and Hybrid).We move on to more fundamental problems in cryptology such as verifiable secret sharing(VSS), and Multi-party Computations( MPC) in the second part of the tutorial. besides discussing key design methodologies, we discuss few open problems as well that may act as a trigger for fruitful future research.

## **Tutorial Outline**

1. A Taxonomy for message transmission protocols.
2. Perfect security and complexity measures
3. Possibility, feasibility and optimality of protocols.
4. Multi-party computations
5. Information checking, WSS, and VSS protocols.
6. Protocols for synchronous and asynchronous MPC and Byzantine agreement problems.
7. Conclusions and open problems.

## **About the Speaker**

Prof C.Pandu Rangan served at IIT, Madras for the past 27 years and he has extensively published on various aspects of cryptology in the past ten years. He is a Fellow of Indian national academy of Engg (FNAE) and serves as Vice president for CRSI (Cryptology Research Society of India). He is in the editorial boards of LNCS series published by Springer Verlag and in the editorial board of Int. Journal on Parallel and Distributed Computing.