Session Types: Applications, Foundations and Flow Security (STAFFS)

Serbia-India Bilateral Scientific and Technological Cooperation

The project is financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia and The Scientific and the Ministry of Science and Technology of the Republic of India

Duration: 2022-2024

Institutions:

from India: **Indian Institute of Technology Delhi**

from Serbia: **Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade**

Project coordinators:

1. **Sanjiva Prasad**, Indian Institute of Technology Delhi, sanjiva@cse.iitd.ac.in

2. **Silvia Ghilezan**, Mathematical Institute SANU, Belgrade, gsilvia@uns.ac.rs

Other project members
from **India**:

1. **Samalam Arun-Kumar,** Indian Institute of Technology Delhi
2. **PhD students**, Indian Institute of Technology Delhi

from **Serbia**:

1. **Zoran Ognjanović**, Mathematical Institute of the Serbian Academy of Sciences and Arts
2. **Simona Kašterović**, PhD student, University of Novi Sad, Faculty of Technical Sciences
3. **Tamara Stefanović**, PhD student, University of Novi Sad, Faculty of Technical Sciences

Project description:

Session types provide a discipline to distributed communicating systems that ensures the absence of undesirable occurrences such as deadlocks and unmatched communication events. Their formal foundations lie in the close nexus between logic, proof theory and programming, where propositions are related to types, proofs to programs, and proof normalisation to program execution. Since the proposal of linear logic as a substructural logic and the proposal of (higher-order) pi-calculi about 3 decades ago, there have been several efforts to provide a quintessential connection between calculi for concurrency and classical logics and their proof systems, much the same way that the lambda calculus is the computational counterpart to intuitionistic logic and Natural Deduction. However, even the most innovative of such proposals have shortcomings, which motivates the foundational aspects of this proposal.

Security of information flow is also an essential property required of communicating systems. Security type systems have been proposed which ensure confidentiality (and dually, integrity). The Continuation Passing Style, intimately related to translations of classical to intuitionistic logic, provides a detailed account of control flow. CPS is also used as a technique for proving non-interference, the semantic property corresponding to secure information flow. This project aims at exploring the logical connections, mediated by CPS, between security properties, control constructs and type systems.

An integral part of this project will explore secure session types and their applications to multiparty interactions, and to develop analysis techniques and software tools.

Project key objectives:

1. To explore the proof theoretic foundations of well-formed concurrent computation.
2. To provide a framework which supports the integration of logic, computation and secure information flow for concurrent and functional paradigms.
3. To develop analysis techniques and software tools that ensure secure and safe multiparty interactive systems.
4. To establish long-term research connections between IITD and the Mathematical Institute of the Serbian Academy of Science and Arts and University of Novi Sad, and broader educational and research ties between the two countries.