Security and Communication Networks

Special Issue on
Secure Multiparty Computation

WILEY | Hindawi

CALL FOR PAPERS

The recent advances in network technologies for the wired and the wireless media have created the attractive possibility of running distributed computations at an unprecedented scale. In this vein, Multiparty Computation (MPC) allows a set of mutually distrustful parties in a distributed network to compute a joint function of their private inputs without disclosing anything beyond what is already revealed by the function output.

Since its conception, MPC has been successfully applied in many contexts, making it possible to realize surprising tasks, which were unforeseen in the past. Prominent examples include allowing running statistics on a distributed database in a privacy preserving manner, the ability to outsource arbitrary computations from computationally weak clients to a more powerful server "in the cloud" (a.k.a. verifiable computation), and electronic voting and digital cash systems. However, while in theory any function can be securely evaluated by means of an MPC protocol, the field is full of challenging open problems, and many obstacles still need to be overcome before MPC can eventually be deployed on a massive scale in applications.

This special issue aims at providing both theoreticians and practitioners with a forum to present their research on various aspects of secure computation in distributed information systems. The purpose is to investigate theoretical and practical aspects, design new applications, and explore new solutions for overcoming major challenges in this exciting research area. We particularly welcome papers whose results are backed up by a rigorous security analysis (in the style of "provable security"), but papers focused on more applied aspects related to secure computation are also in scope.

Potential topics include but are not limited to the following:

- Card-based protocols
- Coin tossing
- Communication/round complexity of MPC
- Differential privacy
- Digital cryptocurrencies
- Electronic voting
- Engineering and implementation aspects of MPC
- Game-theory and MPC
- Garbling schemes and randomized encodings of functions
- Homomorphic cryptography and applications
- Interactive arguments/proofs
- Oblivious transfer
- Privacy preserving data mining
- Private information retrieval
- Proofs of storage and proofs of retrievability
- Real world deployments of MPC
- Searchable encryption
- Secret sharing
- Secure auctions
- Secure consensus protocols and applications of the block chain to secure computation
- Theoretical aspects of MPC
- Verifiable computation
- Zero knowledge and application

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/scnsc/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Daniele Venturi, Sapienza University of Rome, Rome, Italy
venturi@di.uniroma1.it

Guest Editors
Ignacio Cascudo, Aalborg University, Aalborg, Denmark
ignacio@math.aau.dk

Arpita Patra, Indian Institute of Science, Bangalore, India
arpita@iisc.sc.in

Alessandra Scafuro, North Carolina State University, Raleigh, USA
ascafur@ncsu.edu

Submission Deadline
Friday, 29 December 2017

Publication Date
May 2018