Speaker: Thomas Schneider, Technische Universität Darmstadt

Title: Efficient Oblivious Transfer Extensions and Applications

Protocols for secure computation enable parties to compute a joint function on their private inputs without revealing anything but the result. A foundation for secure computation is oblivious transfer (OT), which traditionally requires expensive public key cryptography and hence OT was believed to be inefficient. A more efficient way to perform many OTs is to extend a small number of base OTs using OT extensions based on symmetric cryptography.

In this talk we summarize our recent results on optimizations and efficient implementations of OT extensions in the semi-honest model and their applications. We improve OT extensions with respect to communication complexity, computation complexity, and scalability. We give additional optimizations of OT extensions that are tailored to the generic secure computation protocols of Yao and Goldreich-Micali-Wigderson. We give additional applications for secure computation of specific functionalities that benefit from more efficient OT extensions.

Based on joint works with Gilad Asharov, Julien Bringer, Hervé Chabanne, Mélanie Favre, Yehuda Lindell, Alain Patey, and Michael Zohner