SWITS Abstract: Multi-party Hybrid Homomorphic Encryption

Anton Israelsson
RISE, Research Institutes of Sweden Cybercampus
anton.israelsson@ri.se

Abstract

Collaborative data analysis is often hindered by privacy, regulatory, or proprietary constraints, especially in sensitive domains like healthcare. Secure Multi-Party Computation (MPC) allows joint computation without exposing raw data, but traditional MPC protocols are communication-heavy and scale poorly with the number of parties. FHE-based MPC shifts the computational burden to a powerful, untrusted server by enabling operations on encrypted data via Fully Homomorphic Encryption (FHE), reducing client-side complexity. We propose an FHE-based MPC scheme combining hybrid homomorphic encryption (transciphering) with multi-party FHE to address ciphertext bloat and scalability issues. The approach potentially enables efficient, privacy-preserving computation across multiple resource-limited data sources using symmetric encryption, with a central computing party converting and processing encrypted data, lowering overhead for clients and supporting scalable, secure collaboration.

I plan to present a poster.