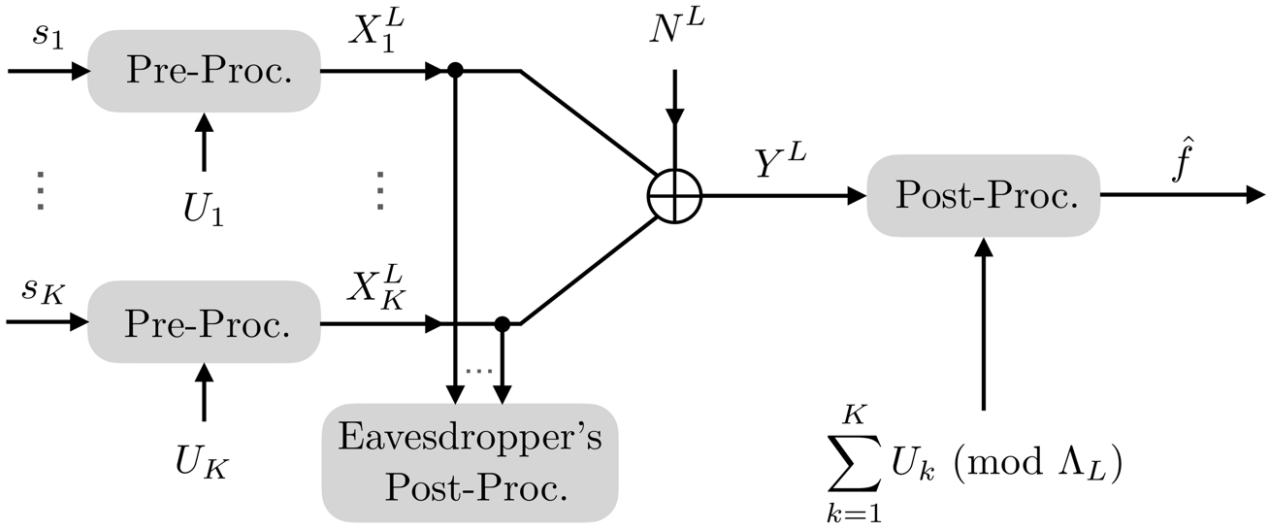
6G-RIC
Research and
Innovation Cluster

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Private and Secure Over-the-Air Multi-Party Communication

JAN JONAS BRUNE, MATTHIAS FREY, FELIX KLEMENT, IGOR BJELAKOVIĆ, STEFAN KATZENBEISSER AND SŁAWOMIR STAŃCZAK

How can data aggregation with Over-the-Air computation be made secure and private, while also ensuring reliability? Are there lattices for which our pre- and post-processing schemes fulfill secrecy, privacy and reliability guarantees?



The goal of the receiver is to obtain a reliable estimate ∫ˆof a real-valued function f from a specific function class, aggregating the data s_1,...,s_K over a multiple-access channel with additive white Gaussian noise. An agreed-upon lattice introduces a modulo operation. The transmitters keep their individual data private from both eavesdropper and legitimate receiver, by using randomly generated keys U_1,...,U_K at pre-processing, drawn from the fundamental cell of the lattice. The legitimate receiver's key (mod-sum of the U_1,...,U_K) only allows to reconstruct the estimate ∫ˆduring post-processing.

KEY FINDINGS

In this paper, we introduce Over-the-Air Multi-Party Communication, a novel approach to achieve efficiently scalable, private, secure, and dependable data aggregation using Over-the-Air computation. The main idea of our approach lies in a combination of techniques from lattice coding, Over-the-Air computation and secure Multi-Party Computation to securely and confidentially aggregate data over a multiple-access channel with additive white Gaussian noise. Our theoretical analysis of the proposed analog scheme developed in this work satisfies the necessary reliability, security, and privacy criteria. Among the potential applications of our approach are smart metering, distributed machine learning, and data aggregation in wireless sensor networks.

Jan Jonas Brune, Matthias Frey, Felix Klement, Igor Bjelaković, Stefan Katzenbeisser, Sławomir Stańczak / Private and Secure Over-the-Air Multi-Party Communication, ASILOMAR, Pacific Grove, CA 93950, USA, October 2023, to appear