Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

TUM

Seminar

Analog Privacy-Preserving Coded Computing

In privacy-preserving coded computing, a main nodes offloads computations to a set of worker nodes without leaking information about the it's private data (unless too many workers collude).

Many approaches in the literature consider computations over finite fields. However, in many applications in practice, e.g. machine learning, computations over (approximations of) the reals are required.

The goal of this seminar work is to review the recent approaches from the literature on privacy-preserving coded computing over analog domains and highlight their benefits and drawbacks.

Relevant literature:

- M. Soleymani, H. Mahdavifar and A. S. Avestimehr, "Analog Privacy-Preserving Coded Computing," 2021 IEEE International Symposium on Information Theory (ISIT), 2021, pp. 1865-1870, doi: 10.1109/ISIT45174.2021.9517715.
- M. Soleymani, H. Mahdavifar and A. S. Avestimehr, "Analog Lagrange Coded Computing," in IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, pp. 283-295, March 2021, doi: 10.1109/JSAIT.2021.3056377.

Prerequisites

- Coding theory
- Information theory
- Linear algebra
- Having attended the course on "Security in Communications and Storage" would be helpful (but is not required)

Advisors

Christoph Hofmeister