Title:
Secure Multiparty Computation –
State of the Art and Applications to Medical Domain on the Basis of the Sharemind Platform

Abstract:

Privacy wishes of data owners and data subjects are an important consideration in the design of information systems. When data from many owners has to be processed at once, then there may be no single processor to which all owners agree to upload their data. Secure multiparty computation is a cryptographic technique that can help.

In this talk, I will give a high-level overview of this technique, explain its capabilities and limitations, and give examples of its use. The latter focuses mostly on the Sharemind platform and the protocol sets it uses, but we will also mention important applications built with other technologies.

Speaker: Dr. Peeter Laud, Cybernetica AS