Engineering secure two-party computation protocols : design, optimization, and applications of efficient secure function evaluation

Schneider, Thomas, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20410461&lokasi=lokal

----

Abstrak

The author offers an extensive overview of the most practical and efficient modern techniques used in the design and implementation of secure computation and related protocols. After an introduction that sets secure computation in its larger context of other privacy-enhancing technologies such as secure channels and trusted computing, he covers the basics of practically efficient secure function evaluation, circuit optimizations and constructions, hardware-assisted garbled circuit protocols, and the modular design of efficient SFE protocols.