Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Garbled Circuit and its Application

Garbled circuit is a cryptographic protocol which was developed by Yao in 1986. It does not target a secure communication or storage, but a secure computation between two untrusted parties. Garbled circuit enables the computation of a function outcome which is dependent on the inputs of both parties without revealing the secret inputs to the other party. Over time the original protocol was improved and new application fields were developed, like the secure evaluation of neural networks by Ball et. al.

The seminar work should shortly introduce the concept of garbled circuit as well as its main optimizations. The second part of the work should give an overview of its different application fields which were developed in the last years.

References:

- A. C. Yao, "How to generate and exchange secrets," 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), Toronto, ON, Canada, 1986, pp. 162-167.
- M. Ball, B. Carmer, T. Malkin, M. Rosulek and N. Schimanski, "Garbled Neural Networks are Practical," IACR Cryptology ePrint Archive, 2019, 338

Contact

[Request Topic]

Advisors

Michaela Brunner