Multi-Party Computation summary

donderdag 19 januari 2023 18:31

GMW scheme

A scheme which reduces multi-part computation of AND to two-party computation. The scheme in its entirety provides for implementations of AND and XOR, which together form a complete set of operations.

Oblivious transfer

A method for B to send one message out of two to A, without A having to tell B which message she desires. A mechanism exists which is only secure with passive adversaries; in this mechanism, A sends two public keys to B, where she has the private key for only one of the public keys. This does not work against active adversaries.

Security properties of MPC

- Completeness: if all parties are honest, the end-results are correct.
- Fairness: either all parties or no party receives their result.
- Soundness: the scheme is 'secure'

Fairness requires an honest majority, an arbiter scheme or encrypting results and sharing the keys one bit at a time.

Simulation-based security notions

- Adversary may corrupt a subset of all participants
  - Learns their in-/outputs and some pre-defined leakage (e.g. message length)
- The scheme is secure if a simulated transcript (under ideal functionality) of in-/outputs is indistinguishable from a real transcript.

It is possible for a scheme to be secure against active attacks while being insecure against passive attackers.