Multi-Party Computation (MPC)

Return to Glossary

Multi-Party Computation (MPC), also known as **Secure Multi-Party Computation (SMPC)**, is a cryptographic protocol that distributes a computation across multiple parties where no individual party can see the other parties' data.

Secure multiparty computation protocols can enable data scientists and analysts to compliantly, securely, and privately compute on distributed data without ever exposing or moving it.

The most central properties of MPC are[1)]:

1. ***Privacy:*** *No party should learn anything more than its prescribed output. In particular, the only information that should be learned about other parties' inputs is what can be derived from the output itself. For example, in an auction where the only bid revealed is that of the highest bidder, it is clearly possible to derive that all other bids were lower than the winning bid. However, nothing else should be revealed about the losing bids.*
2. ***Correctness:*** *Each party is guaranteed that the output that it receives is correct. To continue with the example of an auction, this implies that the party with the highest bid is guaranteed to win, and no party such as the auctioneer can influence this.*
3. **Independence of Inputs:** Corrupted parties must choose their inputs independently of the honest parties' inputs. This property is crucial in a sealed auction, where bids are kept secret and parties must fix their bids independently of others. We note that independence of inputs is not implied by privacy. For example, it may be possible to generate a higher bid, without knowing the value of the original one. Such an attack can actually be carried out on some encryption schemes (that is, given an encryption of $100, it is possible to generate a valid encryption of $101, without knowing the original encrypted value).
4. ***Guaranteed output delivery:*** *Corrupted parties should not be able to prevent honest parties from receiving their output. In other words, the adversary should not be able to disrupt the computation by carrying out a "denial of service" attack.*
5. ***Fairness:*** *Corrupted parties should receive their outputs if and only if the honest parties also receive their outputs. The scenario where a corrupted party obtains output and an honest party does not should not be allowed to occur. This property can be crucial, for example, in the case of contract signing. Specifically, it would be very problematic if the corrupted party received the signed contract and the honest party did not. Note that guaranteed output delivery implies fairness, but the converse is not necessarily true.*

Source: https://inpher.io/technology/what-is-secure-multiparty-computation/

1)

Yehuda Lindell , Communications of the ACM, January 2021, Vol. 64 No. 1, Pages 86-96, Accessed: 21 January 2022, https://cacm.acm.org/magazines/2021/1/249459-secure-multiparty-computation/fulltext