Secure Multi-Party Computation (MPC)

DNA Layer employs Secure Multiparty Computation (SMPC or MPC) for provable cryptographic security across the network. SMPC is a cryptographic protocol that enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. Each participant in the computation has a piece of the overall data puzzle, yet none can see the other parties' pieces. This method ensures that intermediate information remains undisclosed to any participating party throughout the process, with only the final output being revealed to the designated recipient.

On DNA Layer, this is crucial for tasks where both data privacy and collaboration are necessary. However, due to the intensive computational requirements generally associated with SMPC, we have optimized its application to be restricted to lightweight tasks throughout the network. This selective application allows us to benefit from the strong provable cryptographic security guarantees of SMPC where it matters most, without overwhelming the system with undue computational processing demands.

As a result, our project not only adheres to rigorous security standards but also maintains a high level of practicality and performance efficiency when handling the strictest data confidentiality measures.

Previous
Trusted Execution Environment (TEE)

Next
Verifiable Random Function (VRF)

Last updated 1 month ago