Case Study – Secure Multi-Party Calculation.

In an SMPC, a given number of participants, p1, p2, ..., pN, each have private data, respectively d1, d2, ..., dN. Participants want to compute the value of a public function on that private data: F(d1, d2, ..., dN) while keeping their own inputs secret. Can you think of any practical situations where secure multiparty calculations would be required? Can symmetric key encryption alone suffice the needs of secure multiparty calculations? If yes, what are the possible issues/constraints? Is an arbitrator mandatory in such a scheme?

Secure multiparty computation (MPC / SMPC) is a cryptographic protocol which 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.

For example, suppose a city has a growing traffic problem and there are many ridesharing applications running around the city which has slowed down the commutes. The concept of secure multiparty computation can be used to find out how ride-sharing apps can influence traffic congestion. In this method, the organization input data which is mainly the pickup and drop locations of their clients are taken by the company application which is splitted into pieces and masked by adding random numbers. The splitted pieces are then sent to multiple servers ensuring data privacy. The organization's main data is never shared with the servers rather the data which is encoded data are compared . In this way multiparty computation , helps the organizations to work together without ever knowing one another's confidential information.

There are a wide range of practical applications, varying from simple tasks such as coin tossing to more complex ones like electronic auctions (e.g. compute the market clearing price), electronic voting, or privacy-preserving data mining. The other practical applications where secure multiparty computation can be used in examining big questions and solving complex problems like traffic plan which helps to alleviate drive-time headaches, predicting health outcomes to better treat the patients and also help the students choose their college by forecasting the earning potential of the degree.

The most basic properties that a multi-party computation protocol aims to ensure are:

• Input privacy: No information about the private data held by the parties can be inferred from the messages sent during the execution of the protocol. The only information that can be inferred about the private data is whatever could be inferred from seeing the output of the function alone.

• Correctness: Any proper subset of adversarial colluding parties willing to share information or deviate from the instructions during the protocol execution should not be able to force honest parties to output an incorrect result. This correctness goal comes in two flavours: either the honest parties are guaranteed to compute the correct output (a“robust” protocol), or they abort if they find an error (an MPC protocol “with abort”).

No, symmetric key encryption alone cannot suffice the needs of secure multiparty calculations. Symmetric encryption is a main ingredient of 2PC protocols, as opposed to SMPC protocols whose main ingredient is secret sharing and asymmetric encryption. A multi-party computation protocol must be secure to be effective. In modern cryptography, the security of a protocol is related to a security proof. The security proof is a mathematical proof where the security of a protocol is reduced to that of the security of its underlying primitives. Nevertheless, it is not always possible to formalize the cryptographic protocol security verification based on the party knowledge and the protocol correctness. For MPC protocols, the environment in which the protocol operates is associated with the Real World/Ideal World paradigm. The parties can't be said to learn nothing, since they need to learn the output of the operation, and the output depends on the inputs. In addition, the output correctness is not guaranteed, since the correctness of the output depends on the parties’ inputs, and the inputs have to be assumed to be corrupted.

No, an arbitrator is not obligatory in SMPC. The presence of an arbitrator method means that if any dispute arises, each party must expose its contractual relationships and data with the alternative parties, which is going in opposition to the complete concept of SMPC. A party may not be inclined to have his relationship with another to be found out. Information of a personnel, such as that concerning inventions, information, advertising and marketing, value margins and economic data are sensitive regions that many parties might not prefer to show to all of the parties to the arbitration proceeding.