An Investigation into Adversarial and Rational Behavioral Approaches to Secure Multi-Party Computation

Sourya Joyee De

24 March 2014

In the information age, information security and privacy breaches have had severe repercussions in terms of lost revenue and reputation for businesses, loss of trust of customers on service providers, fear of adoption of emerging and otherwise highly beneficial technologies like cloud computing. Security of data i.e. confidentiality, integrity and availability has to be ensured both during storage and computation as either of these may be a source of leakage. In addition, to ensure confidentiality of data used for computations, secure computation must also deal with correctness of results, guaranteed output delivery etc. In multi-party computation scenarios, fairness of obtaining results of a computation also becomes an important factor. Development of secure algorithms is only possible if we know the behaviour of adversaries and parties in general, to assess the kinds of threats data and computations may face.

Traditionally, the literature on secure multiparty computation (SMC) has considered semi-honest and malicious adversarial behaviour. More recently, however, researchers have obtained a series of interesting results by considering rational behaviour of parties in the context of secret sharing. We contribute further in this direction by proposing rational secret reconstruction mechanisms for different scenarios. Specifically, we propose a fair rational secret reconstruction protocol which is also correct, in the presence of rational parties that try to mislead others in believing in an incorrect value of the secret. We show that our protocol is independent of the utility of misleading. Moreover, we also propose a protocol for correct rational secret reconstruction that is fair even in the presence of arbitrary side information. Both protocols have been proposed for the non-simultaneous channel model, in which the particular problems arise. We also briefly explore the concept of 'correctness' in a two-party function computation scenario. In this thesis, we introduce the concept of 'silent' players that prefer to obtain the secret, incurring as little cost of communication and computation as possible. We present a rational secret reconstrucion protocol that tolerates such 'silent' players. The concept of a rational adversary, as opposed to semi-honest and malicious adversaries, has been used in the literature to overcome some impossibility results for the Byzantine Agreement problem. We draw inspiration from such a scenario to model a rational adversary in the context of online sealed bid auctions and propose an algorithm for secure online auction in presence of rational parties as well as rational adversaries.

Security of data and computations outsourced to the cloud is a flourishing area of research. Encryption schemes are however not enough for providing cloud data security because it is impossible to compute arbitrary functions on encrypted data. Recently, the use of secret sharing and SMC for data and computation security in the cloud has been proposed. In this context, we analyze different adversarial models for Cloud Service Providers and propose security frameworks based on secret sharing and SMC for secure enterprise data and computation outsourcing to the cloud. Using a similar framework, we also propose how users of mobile devices can ensure secure data and computation offloading to the cloud for achieving energy efficiency. Apart from this, we construct a privacy aware preference aggregation service considering different adversarial models for parties involved and an online service provider as a facilitator. In this context, we also propose a privacy-preserving multi-party preference aggregation protocol.