Ghodosi, Hossein; Pieprzyk, Josef

Multi-party computation with omnipresent adversary. (English) Zbl 1227.68015


Summary: Secure multi-party computation (MPC) protocols enable a set of $n$ mutually distrusting participants $P_1, \ldots, P_n$, each with their own private input $x_i$, to compute a function $Y = F(x_1, \ldots, x_n)$, such that at the end of the protocol, all participants learn the correct value of $Y$, while secrecy of the private inputs is maintained. Classical results in the unconditionally secure MPC indicate that in the presence of an active adversary, every function can be computed if and only if the number of corrupted participants, $t_a$, is smaller than $n/3$. Relaxing the requirement of perfect secrecy and utilizing broadcast channels, one can improve this bound to $t_a < n/2$.

All existing MPC protocols assume that uncorrupted participants are truly honest, i.e., they are not even curious in learning other participant secret inputs. Based on this assumption, some MPC protocols are designed in such a way that after elimination of all misbehaving participants, the remaining ones learn all information in the system. This is not consistent with maintaining privacy of the participant inputs. Furthermore, an improvement of the classical results given by Fitzi, Hirt, and Maurer indicates that in addition to $t_a$ actively corrupted participants, the adversary may simultaneously corrupt some participants passively. This is in contrast to the assumption that participants who are not corrupted by an active adversary are truly honest.

This paper examines the privacy of MPC protocols, and introduces the notion of an omnipresent adversary, which cannot be eliminated from the protocol. The omnipresent adversary can be either a passive, an active or a mixed one. We assume that up to a minority of participants who are not corrupted by an active adversary can be corrupted passively, with the restriction that at any time, the number of corrupted participants does not exceed a predetermined threshold. We will also show that the existence of a $t$-resilient protocol for a group of $n$ participants, implies the existence of a $t'$-private protocol for a group of $n'$ participants. That is, the elimination of misbehaving participants from a $t$-resilient protocol leads to the decomposition of the protocol.

Our adversary model stipulates that a MPC protocol never operates with a set of truly honest participants (which is a more realistic scenario). Therefore, privacy of all participants who properly follow the protocol will be maintained. We present a novel disqualification protocol to avoid a loss of privacy of participants who properly follow the protocol.

For the entire collection see [Zbl 1157.94004].

MSC:

68M12 Network protocols
94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Keywords:
Multi-Party Computation; Omnipresent Adversary; Proactive Secret Sharing; $t$-resilient Protocols; $t$-private Protocols

Full Text: DOI