Implementing Secure Multiparty Computation using Sealing

Lamya Abdullah

Abstract

We investigate the problem of Secure Multiparty Computation (SMC) in a synchronous system with Byzantine failures. We formalize the concept of \emph{sealing} as the ability to bind data and computation to a particular hardware environment and limit the physical access to code and data in time. Thus, sealing is close to the security guarantees given by Hardware Security Modules (HSM).

We show that the concept of sealing can be used to solve SMC for any number of faulty processes. We argue that sealing can also be achieved in any context where critical data can be erased from storage before a physical attack succeeds.Later, we describe a practical solution that achieves sealing but does not employ HSMs.