Secure Computation Under Network and Physical Attacks

Alessandra Scafuro

Abstract

This thesis proposes several protocols for achieving secure computation under concurrent and physical attacks. Secure computation allows many parties to compute a joint function of their inputs, while keeping the privacy of their input preserved. It is required that the privacy one party's input is preserved even if other parties participating in the protocol collude or deviate from the protocol.

In this thesis we focus on concurrent and physical attacks, where adversarial parties try to break the privacy of honest parties by exploiting the network connection or physical weaknesses of the honest parties' machine.

In the first part of the thesis we discuss how to construct protocols that are Universally Composable (UC for short) based on physical setup assumptions. We explore the use of Physically Uncloneable Functions (PUFs) as setup assumption for achieving UC-secure computations. PUF are physical noisy source of randomness. The use of PUFs in the UC-framework has been proposed already in [14]. However, this work assumes that all PUFs in the system are *trusted*. This means that, each party has to trust the PUFs generated by the other parties. In this thesis we focus on reducing the trust involved in the use of such PUFs and we introduce the Malicious PUFs model in which only PUFs generated by honest parties are assumed to be trusted. Thus the security of each party relies on its own PUF only and holds regardless of the goodness of the PUFs generated/used by the adversary. We are able to show that, under this more realistic assumption, one can achieve UC-secure computation, under computational assumptions. Moreover, we show how to achieve *unconditional* UC-secure commitments with (malicious) PUFs and with stateless tamper-proof hardware tokens. We discuss our contribution on this matter in Part I. These results are contained in papers [80] and [28].

In the second part of the thesis we focus on the concurrent setting, and we investigate on protocols achieving *round optimality* and *black-box* access to a cryptographic primitive. We study two fundamental

functionalities: commitment scheme and zero knowledge, and we focus on some of the round-optimal constructions and lower bounds concerning both functionalities. We find that such constructions present subtle issues. Hence, we provide new protocols that actually achieve the security guarantee promised by previous results.

Concerning physical attacks, we consider adversaries able to reset the machine of the honest party. In a reset attack a machine is forced to run a protocol several times using the same randomness. In this thesis we provide the first construction of a witness indistinguishable argument system that is *simultaneous resettable* and *argument of knowledge*. We discuss about this contribution in Part III, which is the content of the paper [24].