Secure Composition of Cryptographic Protocols

Vipul Goyal

Microsoft Research, India
vipul@microsoft.com

1 Talk Overview

General positive results for secure computation were obtained more than two decades ago. These results were for the setting where each protocol execution is done in isolation. With the proliferation of the network setting (and especially the internet), an ambitious effort to generalize these results and obtain concurrently secure protocols was started. However it was soon shown that designing secure protocols in the concurrent setting is unfortunately impossible in general. In this talk, we will first describe the so called chosen protocol attack. This is an explicit attack which establishes general impossibility of designing secure protocols in the concurrent setting. The negative results hold for the so called plain model where there is no trusted party, no honest majority, etc.

On the other hand, several *positive* results for protocols composition have been established in various related settings (which are either weaker or incomparable). A few examples are the setting of resettable computation (where the parties may not be able to keep state during the protocol execution and may be run several times with the same random tape), bounded concurrent secure computation (where there is an apriori bound on the total number of concurrent sessions), standalone protocol execution with man-in-the-middle (i.e., the setting of non-malleable protocols), the single input setting (where the honest party uses the same input in all polynomially unbounded concurrent protocol executions), etc.

We will survey known results as well various open problems in each of the above settings. We also given an overview of an emerging technique which has been used to construct secure protocols in several of these settings. We will focus on the plain model throughout the talk.