Secure Computation for Big Data

Tal Malkin

Columbia University, New York NY, USA
tal@cs.columbia.edu

Abstract. Secure computation has been a powerful and important research area in cryptography since the first breakthrough results in the 1980s. For many years this area was purely theoretical, as the feasibility results have not been considered even close to practical. Recently, it appears to have turned a corner, with several research efforts showing that secure computation for large classes of functions, and even generic secure computation, has the potential to become truly practical. This shift is brought on by algorithmic advancements and new cryptographic tools, alongside advancements in CPU speed, parallelism, and storage capabilities; it is further motivated by the explosion of new potential application domains for secure computation.

A compelling motivation for making secure computation practical is provided by the burgeoning field of *Big Data*, representing the deluge of data being generated, collected, and stored all around us. Protocols for secure computation on big data can provide critical value for many business, medical, legal, and personal applications. However, conventional approaches to secure computation are inherently insufficient in this setting, where even linear computation can be too prohibitive.

In this talk I discuss challenges and solutions related to secure computation for big data, following two thrusts:

- Overcoming inherent theoretical bounds of (in)efficiency; and
- Satisfying immediate practical needs in a theoretically sound way.

Both goals require the development of new models of secure computation, allowing for theoretically and practically meaningful relaxations of the standard model. In particular, I discuss a few works I have participated in over the last decade, which address the challenge of achieving efficient secure computation for massive data. I also share some experiences from the last few years working on secure search over massive data sets. This research has externally imposed practical constraints, such as strict performance requirements. I focus on my perspective as a theoretical cryptographer and discuss some open cryptographic challenges in this emerging domain.

A. Sahai (Ed.): TCC 2013, LNCS 7785, p. 355, 2013.