Techniques for Efficient Secure Computation Based on Yao's Protocol*

Yehuda Lindell

Dept. of Computer Science
Bar-Ilan University, Israel
lindell@biu.ac.il

Abstract. In the setting of secure two-party computation, two parties wish to securely compute a function of their joint private inputs. The theoretical foundations of this problem were laid down in the 1980s, and it has been heavily studied due to its generality and many applications. However, until recently, secure computation was considered a theoretical problem of purely theoretical interest. This has changed, and progress on the question of efficient secure computation has been extraordinarily fast in the past five years. In this talk, we survey some of this recent progress and describe the main techniques used for obtaining fast two-party computation, based on Yao's garbled circuit protocol. We will present the main algorithmic/protocol improvements, as well as implementation issues that have turned out to be a big factor in obtaining concrete efficiency. In addition, we will relate to the settings of semi-honest, covert and malicious adversaries, and will describe the challenges that arise for each along with the solutions and major open questions.

* This work was funded by the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 239868.

K. Kurosawa and G. Hanaoka (Eds.): PKC 2013, LNCS 7778, p. 253, 2013.