A Pragmatic Introduction to Secure Multi-Party Computation

Suggested Citation: David Evans, Vladimir Kolesnikov and Mike Rosulek, *A Pragmatic Introduction to Secure Multi-Party Computation*. NOW Publishers, 2018.

David Evans
University of Virginia
evans@virginia.edu

Vladimir Kolesnikov
Georgia Institute of Technology
kolesnikov@gatech.edu

Mike Rosulek
Oregon State University
rosulekm@eecs.oregonstate.edu

now
the essence of knowledge
Boston — Delft

A Pragmatic Introduction to Secure Multi-Party Computation

David Evans[1], Vladimir Kolesnikov[2] and Mike Rosulek[3]

[1] *University of Virginia; evans@virginia.edu*
[2] *Georgia Institute of Technology; kolesnikov@gatech.edu*
[3] *Oregon State University, rosulekm@eecs.oregonstate.edu*

ABSTRACT

Secure multi-party computation (MPC) has evolved from a theoretical curiosity in the 1980s to a tool for building real systems today. Over the past decade, MPC has been one of the most active research areas in both theoretical and applied cryptography. This book introduces several important MPC protocols, and surveys methods for improving the efficiency of privacy-preserving applications built using MPC. Besides giving a broad overview of the field and the insights of the main constructions, we overview the most currently active areas of MPC research and aim to give readers insights into what problems are practically solvable using MPC today and how different threat models and assumptions impact the practicality of different approaches.

David Evans, Vladimir Kolesnikov and Mike Rosulek, *A Pragmatic Introduction to Secure Multi-Party Computation*. NOW Publishers, 2018. (Last revision: July 11, 2019)