Masking and MPC: When Crypto Theory Meets Crypto Practice

Nigel P. Smart
Dept. of Comp. Sci., University of Bristol.

ABSTRACT

I will explain the linkage between threshold implementation masking schemes and multi-party computation. The basic principles that need to be taken from multi-party computation will be presented, as well as some basic protocols. The different natures of the resources and threat models between the two different applications of secret sharing will also be covered.

Tis'16 October 24-24 2016, Vienna, Austria

ACM ISBN 978-1-4503-4575-0/16/10.

DOI: http://dx.doi.org/10.1145/2996366.2996372