

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.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

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

© 2016 Copyright held by the owner/author(s).

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

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