The Forge-and-Lose Technique and Other Contributions to Secure Two-Party Computation with Commitments

Submitted in partial fulfillment of the requirements for
the degree of
Doctor of Philosophy
in
Electrical & Computer Engineering

Luís T. A. N. Brandão

Licenciado, Engenharia Física Tecnológica,
Instituto Superior Técnico, Universidade Técnica de Lisboa (Portugal)

Carnegie Mellon University
Pittsburgh PA, USA

December, 2016

This thesis was also submitted to Faculdade de Ciências, Universidade de Lisboa (Portugal), in partial fulfillment of the requirements for the degree of Doutor em Informática. This work was supported through the CMU|Portugal dual-degree doctoral program between Universidade de Lisboa and Carnegie Mellon University.