DISSERTATION

Defence held on 09/04/2019 in Esch-sur-Alzette

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN INFORMATIQUE

by

Aleksei Nikolaevich UDOVENKO

Born on 12th of January 1992 in Tiksi (Russian Federation)

DESIGN AND CRYPTANALYSIS OF SYMMETRIC-KEY ALGORITHMS IN BLACK AND WHITE-BOX MODELS

Dissertation defence committee

Dr Alex Biryukov, Dissertation Supervisor
Professor, Université du Luxembourg

Dr Gregor Leander
Professor, Ruhr-Universität Bochum

Dr Jean-Sébastien Coron, Chairman
Professor, Université du Luxembourg

Dr Matthieu Rivain
Cryptographer, CryptoExperts

Dr Volker Müller, Vice Chairman
Associate Professor, Université du Luxembourg