
ACE: An Authenticated Encryption and Hash Algorithm

Submission to the NIST LWC Competition

SUBMITTERS/DESIGNERS:

Mark Aagaard, Riham AlTawy, Guang Gong,
Kalikinkar Mandal, and Raghvendra Rohit*

*Corresponding submitter:

Email: rsrohit@uwaterloo.ca

Tel: +1-519-888-4567 x45650

COMMUNICATION SECURITY LAB

Department of Electrical and Computer Engineering

University of Waterloo

200 University Avenue West

Waterloo, ON, N2L 3G1, CANADA

<http://comsec.uwaterloo.ca/>

March 29, 2019