
ACE: An Authenticated Encryption and Hash Algorithm

Submission to the NIST LWC Competition

SUBMITTERS/DESIGNERS:

Mark Aagaard, Riham AlTawy¹, 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

<https://uwaterloo.ca/communications-security-lab/lwc/ace>

September 27, 2019

¹Currently with Department of Electrical and Computer Engineering, University of Victoria, 3800 Finnerty Rd, Victoria, BC, V8P 5C2, CANADA