Schwaemm and Esch: Lightweight Authenticated Encryption and Hashing using the Sparkle Permutation Family

– Submission to the NIST Lightweight Cryptography Standardization Process –

Christof Beierle[1], Alex Biryukov[1], Luan Cardoso dos Santos[1], Johann Großschädl[1],
Léo Perrin[2], Aleksei Udovenko[1], Vesselin Velichkov[3], and Qingju Wang[1]

[1]SnT and CSC, University of Luxembourg, Luxembourg
[2]Inria, Paris, France
[3]University of Edinburgh, U.K.

Submission name:
Sparkle

Corresponding submitter:

Prof. Dr. Alex Biryukov
Email: alex.biryukov@uni.lu
Phone: +352 466644-6793

University of Luxembourg
Maison du Nombre, 6, Avenue de la Fonte,
L–4364 Esch-sur-Alzette,
Luxembourg

Contact email for the whole Sparkle group:

sparklegrupp@googlegroups.com

Homepage of Schwaemm, Esch and Sparkle:

http://cryptolux.org/index.php/Sparkle