LILLIPUT-AE: a New Lightweight Tweakable Block Cipher for Authenticated Encryption with Associated Data

Submission to the NIST Lightweight Cryptography Standardization Process

Alexandre Adomnicai[1], Thierry P. Berger[2], Christophe Clavier[2], Julien Francq[3], Paul Huynh[4], Virginie Lallemand[4], Kévin Le Gouguec[3], Marine Minier[4], Léo Reynaud[2], and Gaël Thomas[5]

[1]Trusted Objects - Europarc de Pichaury, Bât. B8, 1330 rue Guillibert de la Lauzière, 13290 AIX-EN-PROVENCE - France, email: a.adomnicai@trusted-objects.com
[2]Université de Limoges - 123 avenue Albert Thomas, 87060 LIMOGES Cedex - France, email: thierry.berger, christophe.clavier, leo.reynaud@xlim.fr
[3]Airbus CyberSecurity - ZA Clef Saint-Pierre, 1 Bd Jean Moulin, CS 40001, MetaPole, 78996 ELANCOURT Cedex - France, email: julien.francq, kevin.legouguec@airbus.com
[4]Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique - BP 239, 54506 VANDOEUVRE-LES-NANCY - France, email: paul.huynh, virginie.lallemand, marine.minier@loria.fr
[5]DGA Maîtrise de l'information - BP 7, 35998 RENNES CEDEX 9 - France, email: gael.thomas.87@gmail.com

Corresponding Submitter's Name: Julien Francq
Email: julien.francq@airbus.com
Telephone: (+33) 1 61 38 71 39
Organization: Airbus CyberSecurity
Postal Address: Airbus CyberSecurity - ZA Clef Saint-Pierre, 1 Bd Jean Moulin, CS 40001, MetaPole, 78996 ELANCOURT Cedex - France

Backup Point of contact: Marine Minier
Email: marine.minier@loria.fr
Telephone: (+33) 6 87 10 68 58
Organization: Université de Lorraine, CNRS, Inria, LORIA
Postal Address: Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique - BP 239, 54506 VANDOEUVRE-LES-NANCY - France