

Name of the proposed cryptosystem

Ascon-Sign

Principal submitter

Vikas Srivastava
National Institute of Technology Jamshedpur
2020rsma011@nitjsr.ac.in, vikas.math123@gmail.com
Department of Mathematics,
National Institute of Technology Jamshedpur
Adityapur-2, 831014, India

Name(s) of auxiliary submitter(s).

Naina Gupta, Nanyang Technological University, Singapore
Arpan Jati, Nanyang Technological University, Singapore
Anubhab Baksi, Nanyang Technological University, Singapore
Jakub Breier, Silicon Austria Labs, Graz, Austria
Anupam Chattopadhyay, Nanyang Technological University, Singapore
Sumit Kumar Debnath, National Institute of Technology Jamshedpur, India
Xiaolu Hou, Slovak University of Technology, Bratislava

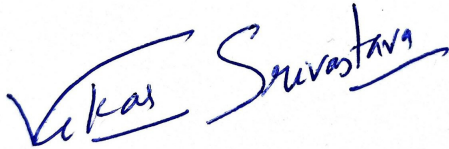
Inventors of the cryptosystem

The work is based on SPHINCS+ (Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Bas Westerbaan) and ASCON (Christoph Dobraunig, Maria Eichlseder Florian Mendel Martin Schläffer). The submitters Vikas Srivastava, Naina Gupta, Arpan Jati, Anubhab Baksi, Jakub Breier, Anupam Chattopadhyay, Sumit Kumar Debnath, Xiaolu Hou contributed to this cryptosystem.

Name of the owner

None (dedicated to the public domain)

Signature of the principal submitter

A handwritten signature in blue ink, reading "Vikas Srivastava". The signature is fluid and cursive, with the first name "Vikas" and the last name "Srivastava" clearly distinguishable.

Alternative point of contact(s)

- Anubhab Baksi
anubhab001@e.ntu.edu.sg, anubhab.baksi@ntu.edu.sg
Temasek Laboratories,
Nanyang Technological University,
50 Nanyang Drive, Research Techno Plaza, Border X Block, Level 8
Singapore 637553
- Jakub Breir
breier@jbreier.com
Silicon Austria Labs, Graz
Austria