

Name of the proposed cryptosystem:

SPHINCS⁺

Principal submitter:

Andreas Hülsing
Eindhoven University of Technology
✉ andreas@huelising.net
☎ +31 40-247 6088
✉ Eindhoven University of Technology
P.O. Box 513
5600 MB Eindhoven
The Netherlands

Auxiliary submitters:

Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijnveld, Peter Schwabe, and Bas Westerbaan

Inventors of the cryptosystem

Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, Zooko Wilcox-O'Hearn, Panos Kampanakis, and Scott Fluhrer; based on a large collection of previous work, most importantly by Ralph C. Merkle, Leslie B. Lamport, Robert Winternitz, Oded Goldreich, Leonid Reyzin, Natan Reyzin, Johannes Buchmann, and Erik Dahmen.

Owner of the cryptosystem

None (dedicated to the public domain)



Andreas Hülsing

Alternative point of contact:

Peter Schwabe
Radboud University
✉ peter@cryptojedi.org
☎ +31 24-365-2031
✉ Radboud University
Toernooiveld 212
6525 EC Nijmegen
The Netherlands