The Oribatida Family of Lightweight Authenticated Encryption Schemes

Version v1.2
Submission to the NIST Lightweight Competition
Sep 27, 2019

Arghya Bhattacharjee[1], Eik List[2],
Cuauhtemoc Mancillas López[3] and Mridul Nandi[1]

[1] Indian Statistical Institute, Kolkata, India
[2] Bauhaus-Universität Weimar, Weimar, Germany
[3] Computer Science Department, CINVESTAV-IPN, Mexico, Mexico

Changelog

Changes from Version v1.1 (2019-03-29) to v1.2 (2019-09-27):

- **Security Goals:** The goals have been clarified further.
- **Security Bounds:** Bounds for nonce-based authenticated encryption and integrity under release of unverified plaintexts have been added.
- **Through the document:** Fixed typos (often $\oplus_s$ instead of $\oplus$) and reformulated a few sentences for easier readability. Added a short remark on the heuristic for the two-step permutation.

Changes from Version v1.0 (2019-02-25) to v1.1 (2019-03-29):

- **Specification:** The figure and the algorithm of the key schedule in SimP have been corrected to match that of Simon.
- **Implementation:** The reference implementation of Oribatida has been corrected to use 26 key-update rounds for SimP-192 and 34 key-update rounds for SimP-256 per step. The previous implementation used two rounds per step less since Simon directly uses the master key as subkeys of the first two rounds.