The authenticated encryption schemes
Kravatte-SANE and Kravatte-SANSE

Guido Bertoni\textsuperscript{1}, Joan Daemen\textsuperscript{3}, Seth Hoffert, Michaël Peeters\textsuperscript{2},
Gilles Van Assche\textsuperscript{2} and Ronny Van Keer\textsuperscript{2}

\textsuperscript{1} Security Pattern
\textsuperscript{2} STMicroelectronics
\textsuperscript{3} Radboud University

This note defines Kravatte-SANE and Kravatte-SANSE. Both are session authenticated encryption schemes and differ in their robustness with respect to nonce misuse. They are defined as instantiations of deck function modes, where a deck function is a keyed function with variable-length input strings, an arbitrary-length output and certain incrementality properties [3, Section 1.1].

Kravatte-SANE is the deck function mode Deck-SANE [3] instantiated with Kravatte and can be seen as a fixed version of of Farfalle-SAE [2].

Definition 1. Kravatte-SANE is Deck-SANE($F = \text{Kravatte}, t = 128, \ell = 8$).

Kravatte-SANSE is the deck function mode Deck-SANSE [3] instantiated with Kravatte and can be seen as a fixed version of Farfalle-SIV [2].

Definition 2. Kravatte-SANSE is Deck-SANSE($F = \text{Kravatte}, t = 256$).

We make no specific security claims for these schemes as their claimed security follows immediately from that of Kravatte in [2].

For a description of the modes of operation Deck-SANE and Deck-SANSE, and of the reasons why we introduced them to replace Farfalle-SAE and Farfalle-SIV respectively, we refer to [3, Sections 4 and 5].

A reference implementation in C++ of Kravatte-SANE and Kravatte-SANSE is available as part of KeccakTools [1], and we will make optimized implementations available as part of the eXtended Keccak Code Package [4].

References


