The authenticated encryption schemes Kravatte-SANE and Kravatte-SANSE

Guido Bertoni[1], Joan Daemen[3], Seth Hoffert, Michaël Peeters[2], Gilles Van Assche[2] and Ronny Van Keer[2]

[1] Security Pattern
[2] STMicroelectronics
[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 = 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 = 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

[1] G. Bertoni, J. Daemen, S. Hoffert, S. Mella, M. Peeters, G. Van Assche, and R. Van Keer, KECCAKTOOLS *software*, October 2018, https://github.com/KeccakTeam/KeccakTools.

[2] G. Bertoni, J. Daemen, S. Hoffert, M. Peeters, G. Van Assche, and R. Van Keer, *Farfalle: parallel permutation-based cryptography*, IACR Trans. Symmetric Cryptol. **2017** (2017), no. 4, 1–38.

[3] J. Daemen, S. Hoffert, G. Van Assche, and R. Van Keer, *Xoodoo cookbook*, IACR Cryptology ePrint Archive **2018** (2018), 767.

[4] G. Van Assche, R. Van Keer, and Contributors, *Extended* KECCAK *code package*, October 2018, https://github.com/XKCP/XKCP.