SHAKE Modes of Operation (extended abstract)

Joan Daemen[1], Seth Hoffert[2], Silvia Mella[1] and Gilles Van Assche[3]

[1] Radboud University, Nijmegen, The Netherlands
[2] Lincoln, Nebraska, USA
[3] STMicroelectronics, Diegem, Belgium

Currently, the vast majority of symmetric-key cryptographic schemes are built as modes of block ciphers. What would cryptography look like if it was built around another primitive?

In this presentation, we would like to explain our method to authentication, encryption and authenticated encryption (AE) using a standard sponge function like SHAKE128 or SHAKE256, or a reduced-round variant thereof, TurboSHAKE128 or TurboSHAKE256 [NIS15, BDH+23]. In more details, we consider two approaches, as illustrated in Figure 1.

- The first one consists in using a sponge-based mode inspired of *SpongeWrap* [BDPV11] to build an efficient AE scheme whose security can be reduced to that of (Turbo)SHAKE.
- The second one consists in first defining a *deck function* on top of (Turbo)SHAKE, and then using one of the different available modes of operation defined in [BDH+22, Hof22].

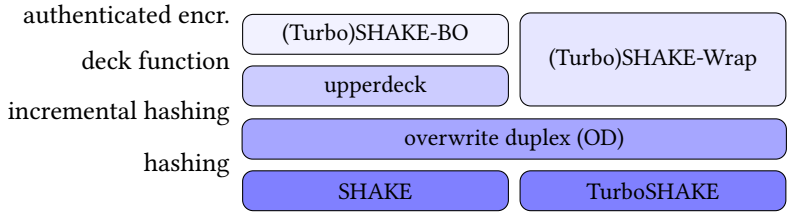

Figure 1: Our approaches to authenticated encryption. Note that BO is just one example of mode on top of a deck function—the choice depends on the desired properties.

The two approaches are specified in details in [DMV23]. They have different properties, also depending on the chosen mode of use on top of the deck function. Nevertheless, both methods lead to *committing* AE. An AE scheme is committing in the strongest sense when it is impossible to generate the same ciphertext for different $(K, [N,]A, P)$ tuples, with K the key, N the nonce, A the associated data and P the plaintext.

Also, both methods support to *sessions*. In modern applications, parties do not limit to exchange individual messages, but usually have to encrypt and authenticate sequences of messages in bi-directional communications. A session deals with the authentication of such sequences of messages by intermediate tags, which ensure that a message is authenticated in the context of previously sent messages.

SpongeWrap-like approach

The main advantage of this first approach is the performance of the resulting AE scheme. Modes like SpongeWrap make use of the duplex construction that can absorb and produce keystream

for one block per call to the underlying permutation. There is therefore almost no overhead in the speed of doing AE compared to the plain sponge function.

Deck function-based approach

The main advantage of this second approach is the rich variety of the modes, as well as their robustness.

In [BDH+22], we describe five modes with different robustness properties. Four of these modes, namely, BO, JAMBO, BOREE and JAMBOREE, are variations around a Feistel network structure, with a consistent and unified approach. This Feistel network has two mandatory central rounds and two optional outer rounds. The central rounds provide AE with *nonce-misuse* robustness, while the optional round at the beginning reduces the ciphertext expansion and the optional round at the end adds resistance against *release of unverified plaintext* (RUP). In fact, JAMBOREE is constructed from a fully fledged *tweakable wide block cipher* that is SPRP secure.

In another paper [Hof22], we describe more modes that encrypt the nonce and any available redundancy, as well as modes suitable for onion routing.

References

[BDH+22] Norica Băcuieți, Joan Daemen, Seth Hoffert, Gilles Van Assche, and Ronny Van Keer. Jammin' on the deck. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part II*, volume 13792 of *Lecture Notes in Computer Science*, pages 555–584. Springer, 2022.

[BDH+23] Guido Bertoni, Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, Ronny Van Keer, and Benoît Viguier. TurboSHAKE. *IACR Cryptol. ePrint Arch.*, page 342, 2023.

[BDPV11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Duplexing the sponge: Single-pass authenticated encryption and other applications. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - SAC 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 320–337. Springer, 2011.

[DMV23] Joan Daemen, Silvia Mella, and Gilles Van Assche. Committing authenticated encryption based on SHAKE. Draft, 2023.

[Hof22] Seth Hoffert. Nonce-encrypting AEAD modes with Farfalle. *IACR Cryptol. ePrint Arch.*, page 1711, 2022.

[NIS15] NIST. Federal information processing standard 202, SHA-3 standard: Permutation-based hash and extendable-output functions, August 2015. http://dx.doi.org/10.6028/NIST.FIPS.202.