Elephant – List of Changes – Final Round

Tim Beyne¹, Yu Long Chen¹, Christoph Dobraunig², and Bart Mennink³

¹ KU Leuven and imec-COSIC, Leuven, Belgium
² Lamarr Security Research, Austria
³ Radboud University, Nijmegen, The Netherlands
elephant@cs.ru.nl

May 17, 2021

– Elephant v2 replaces the variant of the Wegman-Carter-Shoup MAC function in v1 and v1.1 by a variant of the protected counter sum MAC function. The new version v2 achieves confidentiality and authenticity in the nonce-respecting setting, as v1 and v1.1 did, but in addition it achieves authenticity under nonce-reuse.
– A minor change in the positioning in the masks has been made to make v2 slightly more efficient. The roles of the masks are now (·,0) for associated data authentication (used to be encryption), (·,1) for encryption (used to be ciphertext authentication), and (·,2) for ciphertext authentication (used to be associated data authentication).
– Appendix B (Security of Elephant Mode) has been adapted to the new version, and has furthermore been generalized to cover multi-user security. Section 3 (Parametrization of Elephant) has been expanded to include a high-level discussion on the multi-user security result.
– The implementation has been updated to the new version.
– Appendix A (List of Cryptanalysis) has been updated, and in Section 5.1, a paragraph discussing the quantum analysis of Bonnetain and Jaques [27] has been added.