Key Committing Security of AEZ

Abstract

Yu Long Chen, Antonio Flórez-Gutiérrez, Akiko Inoue, Ryoma Ito, Tetsu Iwata,
Kazuhiko Minematsu, Nicky Mouha, Yusuke Naito, Ferdinand Sibleyras, Yosuke Todo

For an Authenticated Encryption with Associated Data (AEAD) scheme, the key committing security refers to the security notion of whether the adversary can produce a pair of distinct input tuples, including the key, that yields the same output. While the key committing security of various nonce-based AEAD schemes is known, the security analysis of Robust AE (RAE) is largely unexplored.
In particular, we are interested in the key committing security of AEAD schemes built on the Encode-then-Encipher (EtE) approach from a wide block cipher. We first consider AEZ v5, the classical and the first dedicated RAE that employs the EtE approach. We focus our analysis on the core part of AEZ to show our best attacks depending on the length of the ciphertext expansion.

In the general case where the Tweakable Block Cipher (TBC) is assumed to be ideal, we show a birthday attack and a matching provable security result. AEZ adopts a simpler key schedule and the prove-then-prune approach in the full specification, and we show a practical attack against it by exploiting the simplicity of the key schedule. The complexity is $O(2^{27})$, and we experimentally verify the correctness with a concrete example. We also cover two AEAD schemes based on EtE. One is built on Adiantum, and the other one is built on HCTR2, where both wide block ciphers are used in real applications. We present key committing attacks against these schemes when used in EtE and matching proofs for particular cases.