New Representations of the AES Key Schedule

Clara Pernot

Inria, Paris, France
clara.pernot@inria.fr

Keywords: AES · Key schedule · mixFeed · ALE · Impossible Differential Attack

Abstract

The AES is the most widely used block cipher today. It was designed by Daemen and Rijmen in 1999 and selected for standardization by NIST. Like all symmetric cryptography primitives, the security of the AES can only be evaluated with cryptanalysis, and there is a constant effort to study its resistance again old and new attacks, and to evaluate its security margin. There are three versions of AES, with different key sizes, and different number of rounds: AES-128 with 10 rounds, AES-192 with 12 rounds, and AES-256 with 14 rounds. After twenty years of cryptanalysis, many different attacks have been applied to AES, and we have a strong confidence in its security: the best attacks against AES-128 in the single-key setting reach only 7 rounds out of 10. The best attacks known so far are either impossible differential attacks or meet-in-the-middle attacks.

In this work we present a new representation of the AES key schedule, with some implications to the security of AES-based schemes. In particular, we show that the AES-128 key schedule can be split into four independent parallel computations operating on 32 bits chunks, up to linear transformation. Surprisingly, this property has not been described in the literature after more than 20 years of analysis of AES. We show two consequences of our new representation, improving previous cryptanalysis results of AES-based schemes.

First, we observe that iterating an odd number of key schedule rounds results in a function with short cycles. This explains an observation of Khairallah on mixFeed, a second-round candidate in the NIST lightweight competition. Our analysis actually shows that his forgery attack on mixFeed succeeds with probability 0.44 (with data complexity 220GB), breaking the scheme in practice. The same observation also leads to a novel attack on ALE, another AES-based AEAD scheme.

Our new representation also gives efficient ways to combine information from the first subkeys and information from the last subkeys, in order to reconstruct the corresponding master keys. In particular we improve previous impossible differential attacks against AES-128 and we obtain the best attack so far when the amount of memory is limited (*eg.* below 2^{75}). We also slightly improve the Square attack against AES-192, the impossible differential attack against Rijndael-256/256 and the related-key impossible differential attack against AES-192.

This is a joint work with Gaëtan Leurent, and it was published at Eurocrypt 2021. See full version at https://eprint.iacr.org/2020/1253 .