Cryptology ePrint Archive: Report 2011/274

A Splice-and-Cut Cryptanalysis of the AES

Dmitry Khovratovich and Christian Rechberger

Abstract: Since Rijndael was chosen as the Advanced Encryption Standard, improving upon 7-round attacks on the 128-bit key variant or upon 8-round attacks on the 256-bit key variant has been one of the most difficult challenges in the cryptanalysis of block ciphers for more than a decade. In this paper we present a novel technique of block cipher cryptanalysis with bicliques, which leads to the following results:

- The first key recovery attack on 9 out of 14 rounds of AES-256 with computational complexity 2^{253.1} and success rate 1.

- The first key recovery attacks on 8 out of 10 rounds of AES-128. The best attack has computational complexity 2^{124.8} and success rate 0.63.

- The first combination of a non-random property and an algorithm that allows to distinguish the full 10-round AES-128 from an ideal cipher in a non-trivial way. This may be interpreted as a weak deviation from an ideal behavior in a model where the adversary is allowed to choose the key, and has some relevance when AES-128 is used in a compression function of a cryptographic hash function.

In contrast to most shortcut attacks on AES variants, we do not need any related-keys. As our attacks are of high complexity, yet practically verified to large extent, they do not threaten the practical use of AES-128 or AES-256 in any way.

Category / Keywords: secret-key cryptography / Advanced Encryption Standard, AES, block cipher, hash function, meet-in-the-middle attack, splice-and-cut, key recovery, distinguisher, non-randomness

Date: received 27 May 2011, last revised 28 May 2011, withdrawn 13 Aug 2011

Contact author: khovratovich at gmail com, christian rechberger@groestl info

Available formats: (-- withdrawn --)

Version: 20110814:012127 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]