Cryptology ePrint Archive: Report 2011/449

Biclique Cryptanalysis of the Full AES

Andrey Bogdanov and 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 192/256-bit key variants 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:

1) The first key recovery attack on the full AES-128 with computational complexity 2126.1. 2) The first key recovery attack on the full AES-192 with computational complexity 2^189.7. 3) The first key recovery attack on the full AES-256 with computational complexity 2^254.4. 4) Attacks with lower complexity on the reduced-round versions of AES not considered before, including an attack on 8-round AES-128 with complexity 2^124.9. 5) Preimage attacks on compression functions based on the full AES versions.

In contrast to most shortcut attacks on AES variants, we do not need to assume any related-keys. Most of our attacks only need a very small part of the codebook and have small memory requirements, and are practically verified to a large extent. As our attacks are of high computational complexity, they do not threaten the practical use of AES in any way.

Category / Keywords: secret-key cryptography / block ciphers, bicliques, AES, key recovery, preimag

Publication Info: The full version of a paper accepted to ASIACRYPT'11

Date: received 16 Aug 2011, last revised 31 Aug 2011

Contact author: andrey bogdanov at esat kuleuven be, dkhovrat@microsoft com, christian rechberger@groestl info,

Available formats: PDF | BibTeX Citation

Version: 20110831:221002 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]