Cryptology ePrint Archive: Report 2011/072

AES Variants Secure Against Related-Key Differential and Boomerang Attacks

Jiali Choy and Aileen Zhang and Khoongming Khoo and Matt Henricksen and Axel Poschmann

Abstract: In this paper, we summarize the recent related-key differential and boomerang attacks on AES by Biryukov et al. and present a framework for protection against these attacks. Then we study an alternative AES key schedule proposed by May et al. at ACISP 2002 as a possible candidate to protect against these related key attacks. We find that there exist equivalent keys for this key schedule and in response, we propose an improvement to overcome this weakness. We proceed to prove, using our framework, that our improved May et al.'s key schedule is secure against related-key differential and boomerang attacks. Since May et al.'s key schedule is not on-the-fly (which is a requirement for some hardware implementations), we propose an on-the-fly AES key schedule that is resistant against related-key differential and boomerang attacks.

Category / Keywords: secret-key cryptography / Related-key attacks, differential cryptanalysis, boomerang attacks, AES key schedule

Date: received 10 Feb 2011

Contact author: cjiali at dso org sg