Rasoolzadeh, Shahram; **Raddum, Håvard**

Cryptanalysis of PRINCE with minimal data. (English) Zbl 1404.94107

Pointcheval, David (ed.) et al., Progress in cryptology – AFRICACRYPT 2016. 8th international conference on cryptology in Africa, Fes, Morocco, April 13–15, 2016. Proceedings. Cham: Springer (ISBN 978-3-319-31516-4/pbk; 978-3-319-31517-1/ebook). Lecture Notes in Computer Science 9646, 109-126 (2016).

Summary: We investigate two attacks on the PRINCE block cipher in the most realistic scenario, when the attacker only has a minimal amount of known plaintext available. The first attack is called accelerated exhaustive search, and is able to recover the key for up to the full 12-round PRINCE with a complexity slightly lower than the security claim given by the designers. The second attack is a meet-in-the-middle attack, where we show how to successfully attack 8- and 10-round PRINCE with only two known plaintext/ciphertext pairs. Both attacks take advantage of the fact that the two middle rounds in PRINCE are unkeyed, so guessing the state before the first middle round gives the state after the second round practically for free. These attacks are the fastest until now in the known plaintext scenario for the 8 and 10 reduced-round versions and the full 12-round of PRINCE.

For the entire collection see [Zbl 1334.94029].

MSC:

94A60 Cryptography

Keywords:

prince; lightweight cipher; cryptanalysis; exhaustive search; meet-in-the-middle

Full Text: DOI