Rasoolzadeh, Shahram; **Raddum, Håvard**

Faster key recovery attack on round-reduced PRINCE. (English) Zbl 1412.94202

Bogdanov, Andrey (ed.), Lightweight cryptography for security and privacy. 5th international workshop, LightSec 2016, Aksaray, Turkey, September 21–22, 2016. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 10098, 3-17 (2017).

Summary: We introduce a new technique for doing the key recovery part of an integral or higher order differential attack. This technique speeds up the key recovery phase significantly and can be applied to any block cipher with S-boxes. We show several properties of this technique, then apply it to PRINCE and report on the improvements in complexity from earlier integral and higher order differential attacks on this cipher. Our attacks on 4 and 6 rounds were the fastest and the winner of PRINCE Challenge's last round in the category of chosen plaintext attack.

For the entire collection see [Zbl 1358.94003].

MSC:

94A60 Cryptography

Keywords:

PRINCE; lightweight; block cipher; key recovery attack; integral; higher-order differential

Full Text: DOI