Liu, Bozhong; **Gong, Zheng**; **Qiu, Weidong**; **Zheng, Dong**

On the security of 4-bit involutive S-boxes for lightweight designs. (English) Zbl 1292.94103

Bao, Feng (ed.) et al., Information security practice and experience. 7th international conference, ISPEC 2011, Guangzhou, China, May 30 – June 1, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-21030-3/pbk). Lecture Notes in Computer Science 6672, 247-256 (2011).

Summary: In this work we investigate all the 4-bit involutive S-boxes with linear, differential and almost resilient analysis. The results show that involutive S-boxes can be optimal against linear attack. We prove that for a 4-bit involutive S-box there always exists a pair of input and output differences such that the Hamming distance is 1, which does not satisfy the strict resistance on differential analysis. Moreover, we find that the almost resilient property is not effective to judge the security of 4-bit involutive S-boxes in practise. How to use the almost resilient property to set up a criterion for an optimal secure S-box needs investigations.

For the entire collection see [Zbl 1213.68026].

MSC:

94A60 Cryptography

Full Text: DOI