**Lallemand, Virginie**; **Rasoolzadeh, Shahram**

**Differential cryptanalysis of 18-round PRIDE.** (English) Zbl 1429.94062

Patra, Arpita (ed.) et al., Progress in cryptology – INDOCRYPT 2017. 18th international conference on cryptology in India, Chennai, India, December 10–13, 2017. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 10698, 126-146 (2017).

Summary: The rapid growth of the Internet of Things together with the increasing popularity of connected objects have created a need for secure, efficient and lightweight ciphers. Among the multitude of candidates, the block cipher PRIDE is, to this day, one of the most efficient solutions for 8-bit microcontrollers. In this paper, we provide new insights and a better understanding of differential attacks of PRIDE. First, we show that two previous attacks are incorrect, and describe (new and old) properties of the cipher that make such attacks intricate. Based on this understanding, we show how to properly mount a differential attack. Our proposal is the first single key differential attack that reaches 18 rounds out of 20. It requires $2^{61}$ chosen plaintexts and recovers the 128-bit key with a final time complexity of $2^{63.3}$ encryptions, while requiring a memory of about $2^{35}$ blocks of 64 bits.

For the entire collection see [Zbl 1380.94006].

**MSC:**

94A60 Cryptography

**Keywords:**

block cipher; PRIDE; differential cryptanalysis

**Full Text:** DOI