**Abdelraheem, Mohamed Ahmed**; **Blondeau, Céline**; **Naya-Plasencia, María**; **Videau, Marion**; **Zenner, Erik**

**Cryptanalysis of ARMADILLO2.** (English) Zbl 1227.94019

Lee, Dong Hoon (ed.) et al., Advances in cryptology – ASIACRYPT 2011. 17th international conference on the theory and application of cryptology and information security, Seoul, South Korea, December 4–8, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-25384-3/pbk). Lecture Notes in Computer Science 7073, 308-326 (2011).

Summary: ARMADILLO2 is the recommended variant of a multipurpose cryptographic primitive dedicated to hardware which has been proposed by *S. Badel* et al. in ["ARMADILLO: a multipurpose cryptographic primitive dedicated to hardware", Lect. Notes Comput. Sci. 6225, 398–412 (2010; Zbl 1227.94027)]. In this paper, we describe a meet-in-the-middle technique relying on the parallel matching algorithm that allows us to invert the ARMADILLO2 function. This makes it possible to perform a key recovery attack when used as a FIL-MAC. A variant of this attack can also be applied to the stream cipher derived from the PRNG mode. Finally we propose a (second) preimage attack when used as a hash function. We have validated our attacks by implementing cryptanalysis on scaled variants. The experimental results match the theoretical complexities.

In addition to these attacks, we present a generalization of the parallel matching algorithm, which can be applied in a broader context than attacking ARMADILLO2.

For the entire collection see [Zbl 1227.94002].

**MSC:**

94A60 Cryptography

Cited in **2** Documents

**Keywords:**

ARMADILLO2; meet-in-the-middle; key recovery attack; preimage attack; parallel matching algorithm

**Software:**

Armadillo

**Full Text:** DOI