The Cube Attack on Courtois Toy Cipher

Tytuł
The Cube Attack on Courtois Toy Cipher

Typ publikacji
Referat konferencyjny

Rok
2017

Data dokładna

Autorzy słownie

Autorzy
Szmidt Janusz

ISBN/ISSN
Print ISBN: 978-3-319-76619-5, Online ISBN: 978-3-319-76620-1

Informacje dodatkowe
[Referat wygłoszony na: konferencji NuTMiC - Number Theory Mathods and Cryptography, Wraszawa, Instytut Matematyki Uniwersytetu Warszawskiego, 11 – 13.09. 2017 r.]

Opublikowany w: Number Theory Mathods and Cryptography str. 241-253, (LNCS, volume 10737)

https://doi.org/10.1007/978-3-319-76620-1_14
Abstract: The cube attack has been introduced by Dinur and Shamir as a known plaintext attack on symmetric primitives. The attack has been applied to reduced variants of stream ciphers Trivium and Grain-128 , a reduced to three rounds variant of the block cipher Serpent and a reduced version of the keyed hash function MD6. In another form the attack appeared in the Vielhaber ePrint articles, where it was named AIDA (Algebraic Initial Value Differential Attack) and applied to reduced variants of Trivium. We applied the cube attack to the reduced variant of Courtois Toy Cipher (CTC) consisting of four rounds and 120-bit key.

After that we extended the attack to five rounds of CTC by applying the 4 + 1 cryptanalytic principle. The article also presents experimental results of recovering the key.
Keywords: Cube attack Symmetric primitives Boolean polynomials CTC The 4 + 1 cryptanalytic principle

Powiązane publikacje

-

Adres url strony

https://link.springer.com/chapter/10.1007/978-3-319-76620-1_14