

Application of the cube attack to stream and block ciphers

Piotr Mroczkowski and Janusz Szmidt
Military Communication Institute
Military University of Technology
Warsaw, Poland

June 2, 2009

Extended abstract

In 2008 Itai Dinur and Adi Shamir presented a new type of algebraic attack on symmetric ciphers. The ciphertext bits y_i , produced by these algorithms, are values of polynomials depending on public variables v_1, \dots, v_m being bits of the plaintext for block cipher or bits of the initial vector for stream cipher and depending on secret variables x_1, \dots, x_n being bits of the key: $y_i = f(v_1, \dots, v_m, x_1, \dots, x_n)$. The attack is a known plaintext one and it has two stages. In the first *preprocessing* stage the attacker has an access to public and secret variables and does the summation of some output variables over chosen k -dimensional cubes in public variables, where the key variables are fixed. Doing this for different choices of keys the attacker obtains a function depending on key bits. The task of this stage is to find the cases where this function is a linear one and reconstruct it. In the next *on line* stage of the attack the key is secret and the attacker has only an access to public variables. Now the attacker does the summation over the same cubes as in the preprocessing stage obtaining this way the right hand sides of the linear equations. Having the system of linear equations the attacker solves it and gets some values of the key bits (the rest values can be obtained by brute force searching). The main problem of this attack is to find linear expressions for the key bits in the preprocessing stage. The used tools here are the linear tests and some heuristic about possible algebraic degree of the involved polynomial f . In general the explicit form of this polynomial is not known and the cipher can be even a black box, but the cube attack can be still applicable. Dinur and Shamir have applied the cube attack to the reduced version of stream cipher Trivium and to three rounds of the block cipher Serpent. We have applied this attack to four rounds of the block cipher CTC (Courtois Toy Cipher) for its versions with 120-bit and 255-bit blocks and keys. There were done up to 10.000 linear tests to ensure

the exact key recovery, which has been confirmed experimentally. Then we can effectively obtain all values of the key bits with the complexity much smaller than the exhaustive search.

References

- [1] Itai Dinur and Adi Shamir, *Cubic Attacks on Tweakable Black Box Polynomials*, Eurocrypt, 2009.
- [2] J-P. Aumasson, W. Meier, I. Dinur, A. Shamir, *Cube Testers and Key Recovery Attacks on Reduced Round MD6 and Trivium*, Fast Software Encryption, 2009.
- [3] I. Dinur, A. Shamir, *Side Channel Cube Attacks on Block Ciphers*, IACR Cryptology ePrint Archive, 2009/127.
- [4] J-P. Aumasson, I. Dinur, L. Henzen, W. Meier, A. Shamir, *Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128*, IACR Cryptology ePrint Archive, 2009/218.
- [5] S. S. Bedi and R. Pillai, *Cube attacks on Trivium*, IACR Cryptology ePrint Archive, 2009/15.
- [6] M. Vielhaber, *Breaking ONE.TRIVIUM by AIDA an Algebraic IV Differential Attack*, IACR Cryptology ePrint Archive, 2007/413.