The Cube Attack on CTC Block Cipher

Piotr Mroczkowski and Janusz Szmidt

Warsaw, Poland

Abstract. The cube attack was introduced by I. Dinur and A. Shamir [4] as a known plaintext attack on symmetric primitives. The attack has been applied in the papers [4], [5], [1]. [2] to reduced variants of the stream ciphers Trivium and Grain-128, the reduced to three rounds variant of block cipher Serpent and keyed reduced version of the hash function MD6. In a special case the attack has appeared in the M. Vielhaber ePrint articles [6], [7], where it was named AIDA (*Algebraic Initial Value Differential Attack*) and applied to the modified versions of Trivium. We have applied the cube attack to four rounds of the Courtois Toy Cipher (CTC), where there are presented the experimental results confirming the full recovery of 120-bit key. After that the attack has been extended to five rounds by applying the meet-in-the-middle method in this context.

Key words: Symmetric primitives, Boolean polynomials, CTC block cipher, the meet-in-the-middle method.

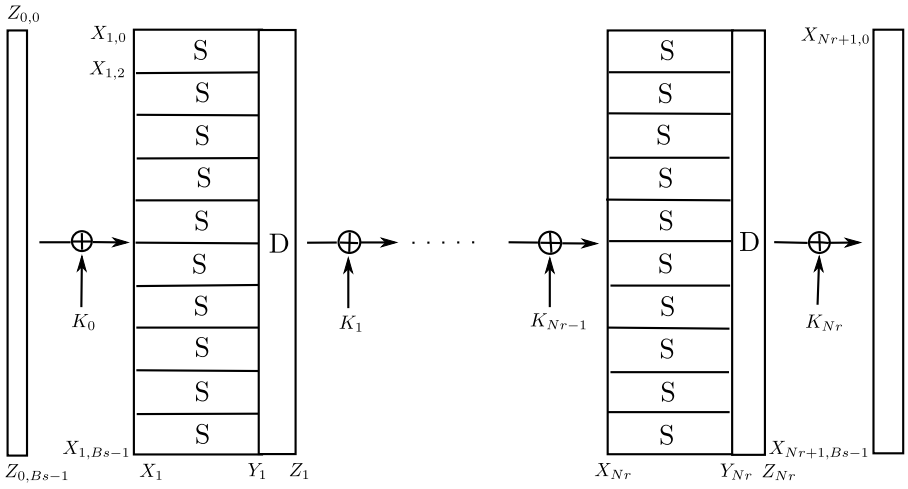


Figure 1: CTC overwiev for B = 10.

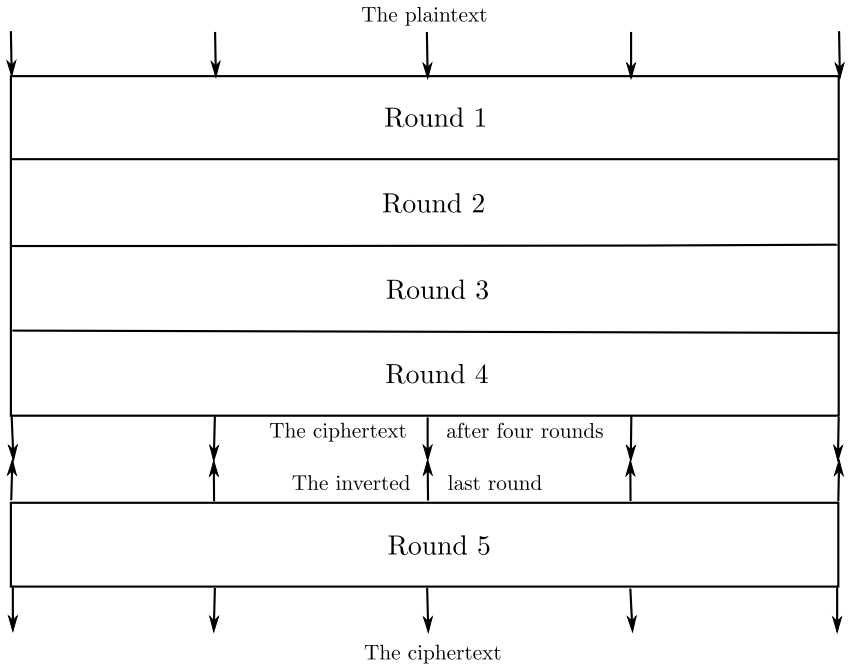
Table 1: The linear expressions for CTC with 4 rounds and 120-bit key.

cube idices	expression	out. bit	cube indices	expression	out. bit
{4,5,22,52}	1+x66+x68	c66	{1,60,62,90 }	x27+x28	c105
{16,17,60,110}	1+x58	c18	{29,38,61,106}	1+x14	c80
{41,55,64,115}	1+x54+x56	c36	{5,10,22,89}	1+x115+x116	c66
{73,74,75,118}	1+x43	c11	{48,68,77,110}	x69+x70	c28
{73,76,93,104}	1+x25	c70	{10,39,70,118}	x78+x79	c114
{16,43,65,97}	1+x77	c87	{1,28,29,36}	x81+x82	c35
{36,37,41,65}	1+x55+x56	c36	{10,37,59,91}	1+x83	c81
{57,71,110,112}	1+x61	c12	{14,35,64,67}	1+x56	c57
{1,26,29,59}	x62	c112	{10,12,32,41}	x105	c7
{21,23,81,101}	1+x37	c42	{7,11,43,53}	1+x111+x113	c104
{14,17,46,113}	1+x103+x104	c90	{53,59,80,91}	x68	c43
{35,50,90,104}	x27	c45	{38,45,70,116}	1+x73	c89
{10,17,40,98}	1+x78+x80	c62	{65,80,97,107}	x41	c38
{14,28,41,88}	x107	c102	{2,48,76,77}	1+x70	c17
{2,34,80,94}	x119	c14	{10,45,47,96}	1+x22	c54
{46,69,74,116}	x48+x49	c47	{26,28,94,116}	1+x26	c18
{14,76,106,113}	1+x7+x8	c110	{2,34,82,100}	1+x36+x38	c34
{6,14,55,67}	x111	c111	{17,81,101,109}	x36+x37	c54
{28,55,66,68}	1+x65	c15	{10,70,77,99}	x18+x19	c54
{26,100,101,111}	x6	c102	{5,19,83,98}	x116	c39
{10,71,83,115}	x50	c24	{29,77,98,119}	x2	c54
{9,56,70,97}	x108	c110	{19,50,91,116}	1+x99+x101	c87
{58,79,84,107}	1+x34	c70	{38,70,77,100}	1+x18+x20	c2
{29,67,69,95}	x48	c61	{14,41,97,110}	1+x106+x107	c33
{14,18,52,65}	1+x100	c96	{40,64,65,76}	1+x80	c66
{18,20,72,79}	x45	c63	{19,23,61,92}	1+x57+x59	c33
{37,44,95,115}	1+x5	c28	{0,1,51,88}	1+x67	c63
{10,53,85,94}	1+x108+x110	c22	{24,37,43,116}	x93+x94	c33
{59,76,117,119}	1+x44	c18	{17,71,92,112}	1+x28+x29	c103
{1,16,78,95}	1+x40	c36	{9,29,51,53}	1+x109	c24
{1,68,100,104}	1+x16+x17	c52	{82,83,85,103}	1+x33+x35	c30
{22,29,81,83}	x92	c17	{27,45,47,100}	x90+x91	c90
{4,34,64,104}	1+x86	c60	{16,83,103,115}	1+x17	c6
{46,90,92,119}	1+x74	c75	{15,29,76,80}	x102	c90
{13,23,100,115}	1+x20	c74	{21,37,50,97}	x96	c111
{34,47,53,98}	1+x84+x86	c72	{10,21,74,89}	1+x97	c84
{23,35,86,87}	x30+x31	c103	{68,74,95,106}	x53	c58
{7,20,44,112}	1+x76+x77	c10	{19,78,80,109}	1+x9+x11	c3
{0,61,83,115}	x117	c45	{57,91,104,113}	x60+x61	c35
{1,22,64,89}	1+x98	c55	{20,41,42,82}	x75+x76	c73

Table 1 (cont.):

cube idices	expression	out. bit	cube indices	expression	out. bit
{0,56,71,97}	1+x118	c34	{46,53,73,85}	1+x47	c37
{16,17,94,116}	1+x4+x5	c12	{2,37,53,74}	1+x46+x47	c93
{19,20,22,109}	1+x11	c51	{2,10,26,89}	1+x94+x95	c30
{29,35,62,86}	x59	c111	{35,38,78,104}	x39	c70
{10,26,38,47}	x95	c22	{17,23,50,74}	x71	c99
{23,37,54,65}	x63	c116	{6,58,86,100}	1+x112	c59
{5,40,45,100}	x72	c37	{4,30,83,109}	x87+x88	c17
{35,37,86,115}	1+x81+x83	c111	{1,33,109,110}	1+x85	c111
{3,35,64,76}	x114	c60	{61,82,89,108}	1+x10	c73
{11,49,80,86}	1+x34+x35	c105	{32,58,59,118}	1+x0+x2	c60
{13,15,41,62}	x102+x103	c31	{7,8,32,85}	x89	c5
{39,40,89,118}	1+x31+x32	c102	{63,65,105,118}	x12+x13	c108
{13,40,56,119}	1+x64+x65	c60	{23,79,92,114}	x3+x4	c15
{11,65,80,105}	x12	c102	{4,5,101,111}	x6+x7	c6
{67,71,107,112}	1+x51+x53	c103	{27,31,53,116}	x90	c28
{35,56,86,89}	x32	c78	{20,32,43,44}	1+x88+x89	c45
{32,75,118,119}	x42	c60	{34,82,97,110}	1+x21+x23	c41
{19,34,47,93}	x24	c108	{7,82,95,117}	x0+x1	c18
{4,5,97,101}	1+x23	c6	{66,73,74,119}	x51+x52	c75
{18,22,50,97}	x99+x100	c111	{32,80,101,102}	x15+x16	c57

1 The Cube Attack and the Meet-in-the-Middle Method



References

1. J-P. Aumasson, I. Dinur, L. Henzen, W. Meier, and A. Shamir. *Efficient FPGA Implementations of High-Dimensional Cube Teters on the Stream Cipher Grain-128*. IACR Cryptology ePrint Archive, 2009/218.
2. J-P. Aumasson, I. Dinur, W. Meier, and A. Shamir. *Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium*. In: Fast Software Encryption 2009. O. Dunkelman, editor. LNCS. Springer, to appear.
3. N. Courtois. *How Fast can be Algebraic Attacks on Block Ciphers ?*. IACR Cryptology ePrint Archive, 2006/168.
4. I. Dinur and A. Shamir. *Cube Attacks on Tweakable Black Box Polynomials*. In: EUROCRYPT 2009. A. Joux, editor. LNCS, vol 5479, pp. 278-299. Springer.
5. I. Dinur and A. Shamir. *Side Channel Cube Attacks on Block Ciphers*. IACR Cryptology ePrint Archive, 2009/127.
6. M. Vielhaber. *Breaking One.Fivium by AIDA an Algebraic IV Differential Attack*. IACR Cryptology ePrint Archive, 2007]413.
7. M. Vielhaber. *AIDA Braeks BIVIUM (A&B) in 1 Minute Dual Core CPU Time*. IACR Cryptology ePrint Archive, 2009]402.
8. MAGMA
9. SAGE