AIDA vs. BIVIUM: Break in 1 Dual-Core-Minute

Michael Vielhaber

Hochschule Bremerhaven, FB2
An der Karlstadt 8, D–27568 Bremerhaven, Germany
and
Universidad Austral de Chile, Instituto de Matemáticas
Casilla 567, Valdivia, Chile

vielhaber@gmail.com

Algebraic IV Differential Attack (AIDA), Vielhaber, 2007
/eprint.iacr.org/2007/413

==

Cube Attack, Dinur & Shamir, 2008
/eprint.iacr.org/2008/385

	BIVIUM	TRIVIUM
key bits	80	80
IV bits	80	80
stages	177	288
setup cycles	708	1152

Algebraic IV Differential Attack AIDA

IV $v_i, i \in I$, Key $k_j, j \in J$, BIVIUM: $I = J = \{1, \ldots, 80\}$

$$\text{DNF: } f = \bigvee_{I,J \subset \{1,\ldots,80\}} d_{I,J} \bigwedge_{i \in I} v_i \bigwedge_{i \notin I} \overline{v}_i \bigwedge_{j \in J} k_j \bigwedge_{j \notin J} \overline{k}_j$$

$$\text{ANF: } f = \bigoplus_{I,J \subset \{1,\ldots,80\}} a_{I,J} \bigwedge_{i \in I} v_i \bigwedge_{j \in J} k_j$$

Search for low-complexity part:

$$f = a_{I,\{j\}} (\bigwedge_{i \in I} v_i) \wedge k_j \oplus Z$$

Z includes all $I' \neq I$

I part linear in key, it is bit k_j

Inclusion-Exclusion-Principle == Reed-Muller-Transform

$$a_I = \oplus_{J \subset I} d_J, \qquad d_I = \oplus_{J \subset I} a_J$$

If

$$f = a_{I,\{j\}} \bigwedge_{i \in I} v_i \bigwedge k_j \oplus Z$$

Then

$$k_j = \bigoplus_{M \subset I} f(\overline{v}_M, \overline{k})$$

with

$$\overline{v}_M : v_i = 1, i \in M, v_i = 0, i \notin M,$$

$\overline{k}$ fixed, unknown

The Equations

BIVIUM-B: 56 key bits, 40 directly, 16 inverted or as sum of 2 or 3 bits

(BIVIUM-A omitted, but similar or easier)

24 missing key bits easily recovered by brute force

$K1$ @711 $\{1, 3, 5, 7, 9, 15, 19, 35, 42, 43, 46, 48, \ldots$
$\ldots 50, 51, 55, 59, 63, 67, 69, 73, 75, 77, 79\}$ 23

Simulate, varying the given IV bits $v_1, v_3, \ldots, v_{77}, v_{79}$ (23 bits)

Add all 2^{23} simulation results at time step 711:

Directly gives key bit K_1

K1	@711	{1,3,5,7,9,15,19,35,42,43,46,48,50,51,55,59,63,67,69,73,75,77,79}
K2	@711	{1,5,7,9,11,19,27,35,42,43,46,48,50,51,63,67,69,71,73,75,77,80}
K3	@710	{2,4,8,10,12,23,29,34,36,43,47,51,53,62,64,66,68,70,74,76,80}
K4	@710	{1,3,5,9,15,23,27,35,42,43,44,46,48,50,51,55,63,67,69,71,73,77,80
K5+E	@711	{2,4,6,8,10,14,16,29,32,34,36,38,43,45,47,51,53,60,62,66,74,76,80
K6	@710	{1,3,5,7,9,11,15,23,35,41,43,44,46,48,51,55,59,63,67,71,73,77,80}
K7	@710	{2,4,6,8,10,12,23,29,34,36,38,43,45,47,51,53,60,62,64,66,70,74,78
K9+E	@721	{2,4,6,10,12,14,23,25,32,36,38,. . .
		. . . ,40,43,45,51,53,64,66,68,70,72,74,76,78,80}
K11	@710	{2,4,6,8,10,12,14,23,25,29,32,34,36,43,45,53,62,66,70,72,74,76,78
K13	@711	{2,4,8,10,14,29,32,34,40,43,45,47,51,53,62,64,66,70,74,76,78,80}
K15+K42	@711	{4,6,8,10,14,16,23,29,34,43,45,47,51,53,60,62,64,66,68,78,80}
K16	@711	{4,6,8,10,23,32,34,36,38,43,45,47,51,53,60,62,64,66,68,78,80}
K17+E	@710	{2,4,6,8,10,14,16,23,29,34,36,38,43,45,47,51,62,64,66,70,76,80}
K18	@710	{2,4,6,8,10,14,23,29,32,34,36,47,51,53,62,64,66,68,70,76,78,80}
K19		
+K4+E	@710	{1,3,5,7,9,11,19,23,35,41,42,43,44,46,48,50,51,55,63,71,73,75,77,8

K20	@710	{2,4,8,10,12,16,23,25,29,34,36,43,45,47,51,53,60,62,64,66,68,70,76}	23
K21	@711	{1,3,5,7,9,11,19,23,27,35,41,42,44,46,48,50,51,59,63,67,77,79}	22
K22+E	@710	{1,3,5,9,11,19,23,35,43,44,46,48,50,51,55,59,63,67,69,73,75,77,79}	23
K24	@711	{1,3,7,9,19,23,35,43,46,48,50,51,55,59,63,67,69,71,73,77,80}	21
K25	@711	{1,3,5,7,9,11,19,23,27,41,43,46,48,50,51,55,59,63,67,71,73,80}	22
K26			
+K11+E	@711	{1,3,7,9,15,17,19,23,27,35,43,46,48,50,51,63,67,69,71,73,77,80}	22
E+K27	@711	{6,8,14,16,29,32,34,36,38,43,45,47,51,53,60,62,64,66,68,76,78,80}	22
K28	@711	{1,3,5,7,9,11,19,23,35,41,44,46,48,50,51,55,63,67,73,77,80}	21
K29	@711	{1,3,5,7,9,11,19,23,35,41,43,46,48,50,51,55,63,67,73,77,80}	21
K30	@711	{1,7,9,15,19,23,27,35,41,42,44,46,48,50,51,55,63,67,71,73,77,80}	22
K31+E	@710	{2,4,8,10,12,16,23,29,32,34,36,38,43,45,47,51,62,66,68,70,74,76,80}	23
K32	@711	{5,7,9,11,15,19,23,27,43,44,46,48,50,51,55,59,63,67,71,73,77,80}	22
K33+K31	@711	{1,3,5,7,9,19,23,27,42,43,44,46,47,48,50,51,55,63,67,71,73,75,77,79}	24
K34+K57	@711	{1,5,7,9,11,17,19,23,35,43,44,48,50,51,55,59,63,67,69,73,75,77,79}	23
K35	@721	{2,4,6,10,12,14,25,32,34,36,38,...	
		...,40,43,45,51,53,60,62,64,66,68,70,74,76,78,80}	26
K37	@712	{4,6,8,10,23,29,34,43,45,47,51,53,60,62,64,66,68,72,78,80}	20
K38	@714	{3,5,7,9,11,15,17,19,27,42,44,46,47,48,50,51,55,59,63,67,69,73,75,79}	24
K39+K37	@712	{4,6,8,10,14,23,29,34,43,45,47,51,53,60,62,66,72,74,76,78,80}	21
K40	@711	{1,3,5,7,9,11,15,19,23,35,41,43,44,46,48,50,51,59,63,67,77,80}	22
K41	@710	{2,4,6,8,10,12,29,32,34,36,40,43,45,47,51,53,60,62,64,66,68,70,74,76}	24
K42	@711	{1,3,5,7,9,11,15,19,23,35,41,43,46,48,50,51,55,63,67,69,73,80}	22
K43	@711	{1,3,5,7,9,11,17,19,27,35,42,44,46,48,50,51,55,63,67,73,75,79}	22
K44	@711	{2,4,6,8,12,16,23,29,32,34,36,43,45,47,51,53,60,62,66,70,78,80}	22
K45	@711	{1,3,5,7,9,11,15,19,23,27,35,43,46,48,50,51,55,59,63,67,73,79}	22
K46	@710	{2,4,10,23,25,29,32,36,43,45,47,51,53,64,66,68,70,72,74,76,78,80}	22
K48	@710	{2,4,6,8,10,12,14,23,29,36,47,51,53,60,62,64,66,68,70,72,74,80}	22
K53	@711	{1,3,5,7,9,11,19,23,35,43,44,46,48,50,55,59,63,67,69,71,73,77,79}	23
K54	@712	{4,6,8,10,12,29,34,45,47,51,53,60,62,64,66,70,72,76,78,80}	20
K55	@710	{2,4,8,10,16,23,29,34,36,43,45,47,51,53,64,66,68,70,76,78,80}	21
K56	@712	{4,6,8,10,23,29,34,36,43,47,51,53,60,62,64,66,72,76,78,80}	20
K57	@711	{2,4,6,8,16,23,25,29,34,36,38,43,45,47,51,53,60,62,66,68,78,80}	22
K58	@710	{2,6,8,10,12,14,23,29,36,40,45,47,51,60,62,64,66,70,74,76,78,80}	22
K59	@711	{2,4,6,8,14,23,29,32,34,43,47,51,53,60,62,66,10,70,72,76,80}	21
K60+K24	@711	{1,5,7,9,11,19,23,27,42,43,46,48,50,51,59,63,67,71,73,75,77,80}	22
K61	@711	{2,4,8,10,14,23,29,34,43,45,47,53,60,62,64,66,70,72,76,78,80}	21
K64	@711	{1,3,5,7,9,11,19,27,35,42,46,48,50,51,55,59,63,67,73,77,80}	21
K65	@710	{2,4,6,8,10,12,23,29,36,47,51,53,62,64,66,68,70,72,74,76,78,80}	22
K66+K45			
+K57	@711	{1,3,5,9,11,15,19,23,27,35,42,43,46,48,50,51,63,67,71,75,77,80}	22
K67+E	@711	{1,3,5,7,9,11,17,19,23,35,42,43,44,46,48,50,51,63,69,71,75,77,79,80}	24
K68+K56	@711	{1,3,7,9,15,17,19,27,35,41,42,43,44,46,48,50,51,55,63,67,69,77,79}	23
K69	@711	{4,6,10,16,23,29,34,36,38,43,45,47,51,53,60,64,66,68,70,74,76,78,80}	23

Fast Reed-Muller Transform

Do not try several N-hypercubes sequentially,

but one $N+4$-hypercube and its subcubes

$$\binom{N+4}{N} \approx \frac{N^4}{24} \quad N\text{-dimensional subcubes}$$

Effort naively $O(3^N)$

Evaluation by Fast Reed-Muller Transform $2^N \cdot N$

Linearity Test by Wavefront Model

Assume that equations are of the form

$k_a \oplus k_b \oplus 1$ or smaller: $(k_a, k_a + 1, k_a + k_b)$

$$2 \cdot \left(1 + 80 + \binom{80}{2}\right) < 2^{13}$$

possible cases.

$T + 13$ simulations rule out all false positives except a fraction 2^{-T}

Better than BLR (Blum-Luby-Rubinfeld) test or Gaussian elimination

already for $n \geq 7$ (currently needed: $N \geq 32$)

Conclusion

1. Don't proliferate plagiarism!

Call the attack AIDA, not "cube"

2. AIDA breaks BIVIUM (A and B) in no time at all, faster than SAT solvers

3. TRIVIUM is safe from (linear) AIDA (EC'09).

4. Tool I: Fast Reed-Muller transform

5. Tool II. Wavefront Model

eprint (submitted), ISKE 2009, my homepage (end September)