AIDA vs. TRIVIUM

1st	640	:	1152	(5:9)	2007
2nd	792	:	1152	(13:18)	2009
Final Score	980	:	1152	(17:20)	∞

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

AIDA vs. TRIVIUM

Time Step	Hypercube Dimension	# Key Bits	Who? When?
576	6	44	Vielhaber 2007
640	8	1	Vielhaber 2007
735	23	80	Dinur/Shamir 2008
770	33	1	Dinur/Shamir 2008
767	29	35	Dinur/Shamir 2009
793	35	4(6)	Vielhaber 2009

Key Bit	*Clock Cycle*	*IV–Bits used (omitted)*
56	793	$I \backslash \{27, 39\}$
58	793	$I \backslash \{1, 33, 57, 59\}$
60	789	$I \backslash \{1, 35, 45, 58, 77\}$
62	788	$I \backslash \{39, 42, 53, 67, 73\}$
64	793	$I \backslash \{1, 49, 57\}$
66	793	$I \backslash \{1, 49, 57, 59\}$

Table 3 : *Linear equations*

The given IV hypercubes are subcubes of
$I = \{1,2,4,6,8,11,13,15,18,21,23,25,31,33,\ 35,38,39,41,42,49,$
$51,53,55,57,58,59,\ 60,64,66,67,69,71,1,27,45,73,75,77,79\}$
$|I| = 38$

However, ...
AIDA (or the "cube" attack) will NOT break
full setup (1152) TRIVIUM with linear relations:

We used:
One 40-dimensional hypercube
NO linearity tests (Too time-consuming)
Decision Zero/Linear/Higher Order by constant term = 0 vs. 1
(*i.e.* "Linearity Check by all-zero key")
Slight, unknown, systematic deviations from true linearity time step
BUT independent from hypercube dimension I

Our interest:
Growth of $|I|$ vs. attackable setup length

i	min	med	$\#_{max}$	avg	max	Δ
12	595	595	595	595	595	–
13	595	625	627	622	640	27
14	597	637	638	633	660	11
15	598	638	638	641	679	8
16	598	649	638	650	690	9
17	598	652	638	659	707	9
18	598	673	675	667	715	8
19	598	676	675	675	720	8
20	626	682	675	682	730	7
21	637	690	675	688	742	6
22	637	695	701	694	755	6
23	638	700	701	699	772	5
24	638	704	701	703	778	4
25	638	708	701	708	785	5
26	639	710	709	712	785	4
27	652	715	718	716	787	4
28	652	717	718	720	794	4
29	653	720	718	724	795	4
30	675	726	718	728	795	4
31	686	730	731	732	794	4
32	696	734	731	736	794	4
33	700	742	743	741	789	5
34	701	744	744	745	788	4
35	713	745	744	748	787	3
36	718	751	744	751	783	3
37	722	754	755	754	779	3
38	744	755	755	756	776	2

Some key points:

1. The average for $\#I = 37$ lies at 754.
2. From $\#I = 23$ to $\#I = 34$, the achievable setup length grows by 4 (sometimes 5) with each added IV bit. It grows faster before, and less later on.
3. The difference between avg and max is 77 at $\# = 25$, its maximum observed difference here.

We therefore can safely extrapolate that ...

4. The average for $\# = 75$ will be at or below $754 + 4 \cdot (75 - 37) = 906$.
5. The average for $\# = 80$ will be at or below $754 + 4 \cdot (80 - 37) = 926$.

i	min	med	$\#_{max}$	avg	max	Δ
20	626	682	675	682	730	7
21	637	690	675	688	742	6
22	637	695	701	694	755	6
23	638	700	701	699	772	5
24	638	704	701	703	778	4
25	638	708	701	708	785	5
26	639	710	709	712	785	4
27	652	715	718	716	787	4
28	652	717	718	720	794	4
29	653	720	718	724	795	4
30	675	726	718	728	795	4
31	686	730	731	732	794	4
32	696	734	731	736	794	4
33	700	742	743	741	789	5
34	701	744	744	745	788	4
35	713	745	744	748	787	3
36	718	751	744	751	783	3
37	722	754	755	754	779	3
38	744	755	755	756	776	2
39	755	757	755	760	773	4
40	755	755	755	755	755	−5
75				(906)	(983)	
80				(926)	(926)	

Attackable Setup Length

6. Maximum for $\#I = 75$: Some 77 higher than the average, at 983 or so.
7. For $\#I = 80$, only one hypercube = average!
8. *Actually feasible* attack: $\#I = 45$, 3 timesteps per IV bit, hence $max \approx 754 + 3 \cdot (45 - 37) + 77 = 855$ ($\approx$ 3 full rounds of the (4-round) setup)

Trivium seems to remain secure against AIDA,
but by a surprisingly small margin.

Conclusion:

1. Don't proliferate plagiarism!

Don't support plagiators!

Call the attack AIDA, not "cube"

2. AIDA is promising, TRIVIUM is weaker than expected, nevertheless ...

3. TRIVIUM is safe from (linear) AIDA.