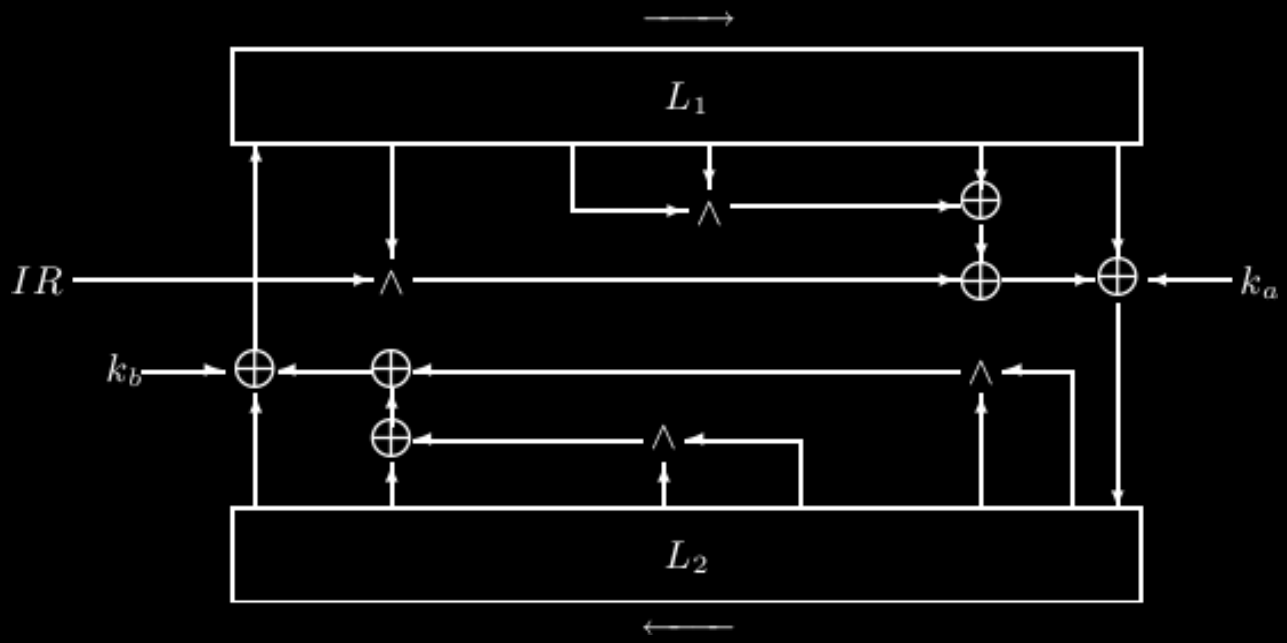
Tiny Results against Reduced KTANTAN32

January 13, 2010

The Cipher



Security

- Best 42-round differential characteristic has probability at most 2^{-11}.
- Best 42-round linear approximation has probability at most 2^{-6}.
- "...one can see that after 32 rounds (for KATAN32) the degree of each internal state bit is at least 2, which means that after 160 rounds, the degree of each internal state bit can reach 32. ...Hence, as the degree can reach to the maximal possible value (and there are some more rounds to spare), it is expected that the KATAN and KTANTAN families are secure against algebraic attacks."

Security

- Best 42-round differential characteristic has probability at most 2^{-11}.
- Best 42-round linear approximation has probability at most 2^{-6}.
- "...one can see that after 32 rounds (for KATAN32) the degree of each internal state bit is at least 2, which means that after 160 rounds, the degree of each internal state bit can reach 32. ...Hence, as the degree can reach to the maximal possible value (and there are some more rounds to spare), it is expected that the KATAN and KTANTAN families are secure against algebraic attacks."

Applying "Algebraic Cryptanalysis of Curry and Flurry using Correlated Messages" (GB) I

N_r	$\log_2 n$	db	t	N_r	$\log_2 n$	db	t
58	4	2	19.73	58	4	3	102.47
59	4	2	–	59	4	3	–
58	5	2	23.89	58	5	3	25.17
59	5	2	27.43	59	5	3	29.06
60	5	2	37.37	60	5	3	39.77
61	5	2	–	61	5	3	47191.97
62	5	2	–	62	5	3	–
58	6	2	66.81	58	6	3	73.38
59	6	2	75.32	59	6	3	82.68
60	6	2	86.32	60	6	3	95.17
61	6	2	103.46	61	6	3	113.53
62	6	2	262.66	62	6	3	282.85

Applying "Algebraic Cryptanalysis of Curry and Flurry using Correlated Messages" (SAT) I

N_r	$\log_2 n$	t	N_r	$\log_2 n$	t
60	3	7353.70	60	4	987.03
61	3	17316.40	61	4	13683.50
62	3	41191.10	62	4	120.98
63	3	14676.10	63	4	9375.71
64	3	191432.00	64	4	6632.50
65	3	–	65	4	–
60	5	13.54	60	6	1178.47
61	5	488.27	61	6	374.73
62	5	4524.71	62	6	13343.70
63	5	46256.40	63	6	49401.50
64	5	12034.20	64	6	39518.80
65	5	59004.10	65	6	122397.00

Applying "Algebraic Techniques in Differential Cryptanalysis" (GB)

N_r	r	$\log_2 p$	t_{min}	t_{avg}	t_{med}	t_{max}	$\log_2 \#\text{trials}$
91	71	-31	0.050	0.059	0.060	0.260	14
96	71	-31	0.050	0.065	0.060	0.290	14
100	71	-31	0.050	∞	∞	∞	12
103	71	-31	0.050	0.050	0.064	0.250	11
110	71	-31	0.050	∞	∞	∞	3
110	71	-31	∞	∞	∞	∞	0

Applying "Algebraic Techniques in Differential Cryptanalysis" (SAT)

N_r	r	$\log_2 p$	t_{min}	t_{avg}	t_{max}	#trials
84	42	-12	0.448	37.011	151.613	1024
84	42	-12	0.540	38.011	243.355	1024
84	42	-12	0.256	37.827	228.834	1024
113	71	-31	0.000	2.798	153.622	984
113	71	-31	0.000	2.600	148.569	931
113	71	-31	0.000	4.135	188.636	908
113	**71**	**-31**	**0.000**	**1.700**	**103.130**	**8192**
116	71	-31	0.000	74.946	4988.250	2701
116	71	-31	0.000	61.022	2626.380	3190
116	71	-31	0.000	65.218	11565.000	3033
120	71	-31	0.000	∞	∞	2
120	71	-31	0.000	∞	∞	9
120	71	-31	0.000	∞	∞	55

Other Techniques?

We can combine pretty much everything with anything:

- Algebraic Differential & Integral Attacks: we tried, not faster
- Algebraic Differential & linear Attacks: we tried: not faster
- Algebraic Sandwich Attack: we tried, not faster
- Algebraic Half-Boomerang: we tried, not faster