Thesis Experiment

Md. Mohsin Ali Khan

March 28, 2015

All experiments are done on SMALLPRESENT-4. The SSA trail is the middle two bits of the second and third S-boxes. Master key is: $0x00000000000000000000$

1 ML and SSA Capacities:

Rounds	ML Capacity	$C = \frac{1}{\lvert I \rvert}\Sigma_{a \in I} C(a)$	Experimental $\sigma^2_{C(a)}$	Theoretical $\sigma^2_{C(a)} = \frac{2C^2}{\lvert Y \rvert - 1}$
1	1.25	1.25	0	0.208333
2	0.086426	0.086426	0.000054	0.000996
3	0.02632	0.02632	0.000082	0.000092
4	0.008473	0.008473	0.000012	0.00001
5	0.004661	0.004661	0.000003	0.000003
6	0.003985	0.003985	0.000002	0.000002
7	0.002969	0.002969	0.000001	0.000001
8	0.00417	0.00417	0.000001	0.000002
9	0.004113	0.004113	0.000003	0.000002
10	0.002946	0.002946	0.000001	0.000001
11	0.003092	0.003092	0.000001	0.000001
12	0.003489	0.003489	0.000002	0.000002
13	0.003855	0.003855	0.000001	0.000002
14	0.003542	0.003542	0.000001	0.000002
15	0.003362	0.003362	0.000001	0.000002
16	0.004004	0.004004	0.000002	0.000002
17	0.003356	0.003356	0.000001	0.000002
18	0.003396	0.003396	0.000001	0.000002
19	0.003528	0.003528	0.000001	0.000002
20	0.003635	0.003635	0.000003	0.000002
21	0.003418	0.003418	0.000001	0.000002
22	0.003517	0.003517	0.000005	0.000002
23	0.002967	0.002967	0.000001	0.000001
24	0.002681	0.002681	0.000001	0.000001
25	0.003571	0.003571	0.000002	0.000002
26	0.003308	0.003308	0.000001	0.000001
27	0.003259	0.003259	0.000001	0.000001
28	0.003513	0.003513	0.000002	0.000002
29	0.003263	0.003263	0.000001	0.000001
30	0.003845	0.003845	0.000003	0.000002
31	0.003246	0.003246	0.000001	0.000001

2 Experiment on the Hypothesis:

For a given η the distribution of p_η over different fixations is assumed to be normally distributed with mean $\mu_{p_\eta(a)}$ and variance $\sigma^2_{p_\eta(a)}$. We have calculated the variance theoretically. The below table compares theoretical and experimental values. Let C be the average capacity of the distribution at the output of the trail over all possible fixation and it is equal to the capacity of the ML distribution.

2.1 15 Rounds

η	$\mu_{p_\eta(a)}$	experimental $\sigma^2_{p_\eta(a)}$	Theoretical $\sigma^2_{p_\eta(a)} = \frac{C}{\lvert Y\rvert\lvert Y-1\rvert}$
0x0000	0.062500	0.000009	0.000014
0x0001	0.062500	0.000008	0.000014
0x0010	0.062500	0.000015	0.000014
0x0011	0.062500	0.000013	0.000014
0x0100	0.062500	0.000017	0.000014
0x0101	0.062500	0.000019	0.000014
0x0110	0.062500	0.000013	0.000014
0x0111	0.062500	0.000013	0.000014
0x1000	0.062500	0.000012	0.000014
0x1001	0.062500	0.000014	0.000014
0x1010	0.062500	0.000015	0.000014
0x1011	0.062500	0.000014	0.000014
0x1100	0.062500	0.000010	0.000014
0x1101	0.062500	0.000007	0.000014
0x1110	0.062500	0.000022	0.000014
0x1111	0.062500	0.000009	0.000014

2.2 16 Rounds

η	$\mu_{p_\eta(a)}$	experimental $\sigma^2_{p_\eta(a)}$	Theoretical $\sigma^2_{p_\eta(a)} = \frac{C}{\lvert Y\rvert\lvert Y-1\rvert}$
0x0000	0.062500	0.000015	0.000014
0x0001	0.062500	0.000016	0.000014
0x0010	0.062500	0.000016	0.000014
0x0011	0.062500	0.000012	0.000014
0x0100	0.062500	0.000018	0.000014
0x0101	0.062500	0.000009	0.000014
0x0110	0.062500	0.000018	0.000014
0x0111	0.062500	0.000021	0.000014
0x1000	0.062500	0.000020	0.000014
0x1001	0.062500	0.000010	0.000014
0x1010	0.062500	0.000019	0.000014
0x1011	0.062500	0.000012	0.000014
0x1100	0.062500	0.000014	0.000014
0x1101	0.062500	0.000017	0.000014
0x1110	0.062500	0.000021	0.000014
0x1111	0.062500	0.000012	0.000014

2.3 17 Rounds

η	$\mu_{p_\eta(a)}$	experimental $\sigma^2_{p_\eta(a)}$	Theoretical $\sigma^2_{p_\eta(a)} = \frac{C}{\lvert Y\rvert\lvert Y-1\rvert}$
0x0000	0.062500	0.000010	0.000014
0x0001	0.062500	0.000021	0.000014
0x0010	0.062500	0.000016	0.000014
0x0011	0.062500	0.000011	0.000014
0x0100	0.062500	0.000009	0.000014
0x0101	0.062500	0.000013	0.000014
0x0110	0.062500	0.000016	0.000014
0x0111	0.062500	0.000014	0.000014
0x1000	0.062500	0.000012	0.000014
0x1001	0.062500	0.000013	0.000014
0x1010	0.062500	0.000010	0.000014
0x1011	0.062500	0.000010	0.000014
0x1100	0.062500	0.000014	0.000014
0x1101	0.062500	0.000010	0.000014
0x1110	0.062500	0.000009	0.000014
0x1111	0.062500	0.000021	0.000014