The Complete Distribution of Linear Probabilities of MARS' s-box

Kazumaro Aoki (NTT Laboratories)*

June 30, 2000

Abstract

This paper shows the complete linear probability distribution of MARS' s-box. The best bias is $\frac{84}{2^9}$ ($= 2^{-2.61}$), while the designers' estimation is $\frac{64}{2^9}$ and the best previously known bias is $\frac{82}{2^9}$.

Knudsen showed that the designers' estimation of the maximum linear probability of MARS' s-box is not rigorous in their submission document for AES [1]. The fact was also pointed out by Robshaw and Yin [2]. However, two papers said that they had insufficient computational power to calculate all linear probabilities of MARS' s-box.

When reading their papers, we wanted to know the maximum bias, and fortunately, we have sufficient computational power to calculate all linear probabilities of MARS' s-box. Using about 2 months idle time of our processors[1], we successfully calculated all linear probabilities of MARS' s-box. As a result, we have the following equation.

$$\#\{x \in \mathrm{GF}(2)^9 \mid x \bullet \texttt{0x185} = s(x) \bullet \texttt{0x8c29952a}\} = 2^8 + 84$$

The complete distribution is shown in Table 1. Note that Table 1 does not show the 0 frequency.

Table 1: Linear Probability Distribution of MARS' s-box

bias$\times 2^9$	frequency	bias$\times 2^9$	frequency	bias$\times 2^9$	frequency	bias$\times 2^9$	frequency
0	77498737588	22	23436811453	44	78537345	66	5116
1	154403399557	23	19654715551	45	55634661	67	2956
2	152613000039	24	16354783059	46	38766823	68	1748
3	149664380489	25	13508041742	47	26922474	69	1040
4	145634858332	26	11061383868	48	18356631	70	568
5	140608578512	27	8988754470	49	12658700	71	309
6	134709616782	28	7248964608	50	8593540	72	200
7	128054979415	29	5797310622	51	5751620	73	112
8	120762019591	30	4599995243	52	3800517	74	54
9	113025372318	31	3624000238	53	2482800	75	31
10	104960005739	32	2833493771	54	1597448	76	24
11	96699764273	33	2196222265	55	1057322	77	6
12	88396049740	34	1688077226	56	705080	78	4
13	80186907969	35	1287471249	57	436911	79	3
14	72170300625	36	974239933	58	292650	81	1
15	64441546502	37	730478919	59	179229	82	2
16	57098291177	38	545180326	60	105547	83	1
17	50195559280	39	403400289	61	62880	84	1
18	43787190914	40	294700718	62	38524	256	1
19	37886631283	41	214842695	63	23306		
20	32538165661	42	154945424	64	14136		
21	27722837170	43	111210140	65	8466		

References

[1] L.R. Knudsen and H. Raddum: "Linear approximations to the MARS S-box," Public Comments on AES Candidate Algorithms — Round 2, 2000 (available at `http://csrc.nist.gov/encryption/aes/round2/pubcmnts.htm`)

[2] M.J.B. Robshaw and Y.L. Yin: "Potential Flaws in the Conjectured Resistance of MARS to Linear Cryptanalysis," Public Comments on AES Candidate Algorithms — Round 2, 2000 (available at `http://csrc.nist.gov/encryption/aes/round2/pubcmnts.htm`)

*Email: `maro@isl.ntt.co.jp`

[1] 21264 (500MHz), 21164 (500MHz), 21064 (266MHz), and 2 Pentium II (400MHz).