On the Security of DES

Adi Shamir
Applied Mathematics
The Weizmann Institute
Rehovot, Israel
(abstract)

The purpose of this note is to describe some anomalies found in the structure of the S-boxes in the Data Encryption Standard. These anomalies are potentially dangerous, but so far they have not led to any successful cryptanalytic attack. While their significance is still unknown, they clearly demonstrate the deficiencies of current certification techniques and the need for provably secure cryptosystems.

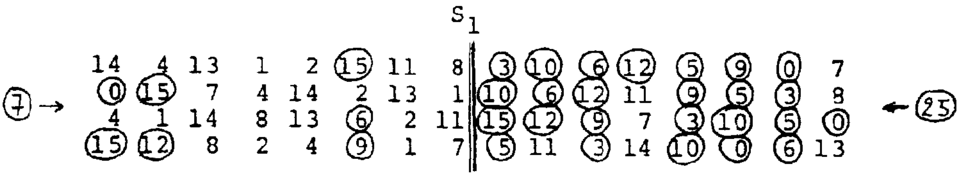
Each S-box is a mapping from six input bits ABCDEF to four output bits WXYZ. Even though they are visually random, they have a lot of intentional structure, which seems to have a positive effect on the security of DES. However, the design criteria used by IBM and the NSA were never made public.

Fig. 1 describes our main observation. It circles all the WXYZ entries in which $W \oplus X \oplus Y \oplus Z = 0$ (0,3,5,6,9,10,12,15). There is a clear correlation between this function and input bit B (which determines the left/right half of each S-box). Furthermore, the minorities in each half are located in such a way that there are exceptionally simple boolean polynomials (XOR's of AND's) which describe the 64 values of $W \oplus X \oplus Y \oplus Z$ in each S-box with very small number of errors. A detailed description of these observations, along with possible lines of attack based on them, will appear in the full paper.

Remarks: (1) The correlation between the XOR of the outputs and input bit B was independently observed by Matthew Franklin from Berkeley in his M.Sc. Thesis (submitted May 1985). I am grateful to Gilles Brassard for bringing this to my attention.

(2) Preliminary analysis by Ernie Brickell and Don Coppersmith suggests that the observed properties of the S-boxes could be an unintentional consequence of some of the design criteria.

S_1



	14	4	13	1	2	⑮	11	8	③	⑩	⑥	⑫	⑤	⑨	⓪	7	
⑦ →	⓪	⑮	7	4	14	2	13	1	⑩	⑥	⑫	11	⑨	⑤	③	8	← ㉕
	4	1	14	8	13	⑥	2	11	⑮	⑫	⑨	7	③	⑩	⑤	⓪	
	⑮	⑫	8	2	4	⑨	1	7	⑤	11	③	14	⑩	⓪	⑥	13	

Figure 1

(continued on next page)

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 280-281, 1986.

S_2

	⑮	1	8	14	⑥	11	③	4	‖	⑨	7	2	13	⑫	⓪	⑤	⑩	
⑩ →	③	13	4	7	⑮	2	8	14	‖	⑫	⓪	1	⑩	⑥	⑨	11	⑤	← ㉒
	⓪	14	7	11	⑩	4	13	1	‖	⑤	8	⑫	⑥	⑨	③	2	⑮	
	13	8	⑩	1	③	⑮	4	2	‖	11	⑥	7	⑫	⓪	⑤	14	⑨	

S_3

	⑩	⓪	⑨	14	⑥	③	⑮	⑤	‖	1	13	⑫	7	11	4	2	8	
㉑ →	13	7	⓪	⑨	③	4	⑥	⑩	‖	2	8	⑤	14	⑫	11	⑮	1	
	13	⑥	4	⑨	8	⑮	③	⓪	‖	11	1	2	⑫	⑤	⑩	14	7	← ⑪
	1	⑩	13	⓪	⑥	⑨	8	7	‖	4	⑮	14	③	11	⑤	2	⑫	

S_4

	7	13	14	③	⓪	⑥	⑨	⑩	‖	1	2	8	⑤	11	⑫	4	⑮	
⑳ →	13	8	11	⑤	⑥	⑮	⓪	③	‖	4	7	2	⑫	1	⑩	14	⑨	← ⑫
	⑩	⑥	⑨	⓪	⑫	11	7	13	‖	⑮	1	③	14	⑤	2	8	4	
	③	⑮	⓪	⑥	⑩	1	13	8	‖	⑨	4	⑤	11	⑫	7	2	14	

S_5

	2	⑫	4	1	7	⑩	11	⑥	‖	8	⑤	③	⑮	13	⓪	14	⑨	
⑥ →	14	11	2	⑫	4	7	13	1	‖	⑤	⓪	⑮	⑩	③	⑨	8	⑥	← ㉖
	4	2	1	11	⑩	13	7	8	‖	⑮	⑨	⑫	⑤	⑥	③	⓪	14	
	11	8	⑫	7	1	14	2	13	‖	⑥	⑮	⓪	⑨	⑩	4	⑤	③	

S_6

	⑫	1	⑩	⑮	⑨	2	⑥	8	‖	⓪	13	③	4	14	7	⑤	11	
㉑ →	⑩	⑮	4	2	7	⑫	⑨	⑤	‖	⑥	1	13	14	⓪	11	③	8	← ⑪
	⑨	14	⑮	⑤	2	8	⑫	③	‖	7	⓪	4	⑩	1	13	11	⑥	
	4	③	2	⑫	⑨	⑤	⑮	⑩	‖	11	14	1	7	⑥	⓪	8	13	

S_7

	4	11	2	14	⑮	⓪	8	13	‖	③	⑫	⑨	7	⑤	⑩	⑥	1	
⑨ →	13	⓪	11	7	4	⑨	1	⑩	‖	14	③	⑤	⑫	2	⑮	8	⑥	← ㉓
	1	4	11	13	⑫	③	7	14	‖	⑩	⑮	⑥	8	⓪	⑤	⑨	2	
	⑥	11	13	8	1	4	⑩	7	‖	⑨	⑤	⓪	⑮	14	2	③	⑫	

S_8

	13	2	8	4	⑥	⑮	11	1	‖	⑩	⑨	③	14	⑤	⓪	⑫	7	
⑧ →	1	⑮	13	8	⑩	③	7	4	‖	⑫	⑤	⑥	11	⓪	14	⑨	2	← ㉔
	7	11	4	1	⑨	⑫	14	2	‖	⓪	⑥	⑩	13	⑮	③	⑤	8	
	2	1	14	7	4	⑩	8	13	‖	⑮	⑫	⑨	⓪	③	⑤	⑥	11	