On the Design of SP Networks from an Information Theoretic Point of View

M. Sivabalan, S. E. Tavares and L. E. Peppard

Department of Electrical Engineering

Queen's University at Kingston

Kingston, Ontario, Canada, K7L 3N6

e-mail : tavares@ee.queensu.ca

Abstract : **The cryptographic strength of an SP network depends crucially on the strength of its substitution boxes (S-boxes). In this paper we use the concept of information leakage to evaluate the strength of S-boxes and SP networks. We define an equivalence class on n×n S-boxes that is invariant in information leakage. Simulation results for a 16×16 SP network suggest that after a sufficient number of rounds the distribution of the output XOR in the SP network looks random. We further present simulation results to show that the information leakage for an SP network diminishes more rapidly with the number of rounds when the S-boxes are cryptographically strong.**

1. Introduction

The concept of "confusion" and "diffusion", which led to the design of Substitution-Permutation Network (SPN) cryptosystems (e.g., DES [1]), was first introduced by Shannon [2] and was elaborated on in concrete and practical ways by Feistel [3] and Feistel, Notz and Smith [4]. The strength of an SP network depends highly on the strength of the substitution boxes (S-boxes). Work on the design and analysis of S-boxes has been presented in [5][6][7][8][9][10].

Kam and Davida [11] presented an approach to the design of S-boxes and SP networks which is guaranteed to satisfy *completeness*, a property which requires that each output bit depends on every input bit. Since then, very little work has been done on the design and analysis of a general SP network [12][13], even though many fully designed cryptosystems have been published [14][15].

In this work we review some previously proposed evaluation criteria based on information leakage and extend them for an n×n bijective S-box. We then define an equivalence class on S-boxes which will enable one to create cryptographically strong S-boxes more efficiently. We also present simulation results to show that cryptographically strong S-boxes improve the performance of an SP network.

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 260-279, 1993.

2. Evaluation Criteria for a Cryptographically Strong S-box

Forré [9] presented a set of cryptographic properties of S-boxes based on information theory. Dawson & Tavares [10] extended Forré's ideas to define an expanded set of design criteria for cryptographically strong S-boxes. The authors viewed an S-box in two different ways : *static view*, which models an S-box when the inputs are steady and *dynamic view*, which models an S-box when the inputs change. Forré's criteria, however, apply to the static model only. In the Dawson & Tavares' design framework both an S-box and its inverse were designed to have low information leakage. The expanded set of design criteria was developed at a "single" bit level, where information leakage between a single output bit and the input bits or between a single output bit and the rest of the output bits were computed. We extend the design criteria to a "multiple" bit level, where information leakage between one or more output bits and the input bits or between one or more output bits and the rest of the output bits are considered. We further show that some of the new design criteria defined in [10] are redundant. We also introduce a useful information theoretic property, which we call "XOR Information Leakage" (XL[I;O]) for an S-box. The attractive feature of this property is that it uses a "single quantity" to compare the XOR distributions of S-boxes and SP networks. The n×n S-box S considered in this section is a bijective S-box with an n-bit input $\mathbf{X}= \{x_1, x_2, ..., x_n\}$ and an n-bit output $\mathbf{Y}= \{y_1, y_2, ..., y_n\}$; where x_i and y_i ; $1 \leq i \leq n$ are binary variables.

2.1. Static Input-Output Information Leakage (SL[I;O])

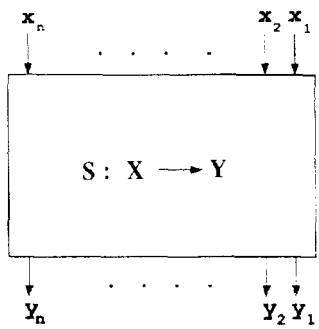


Figure 1. Static view of an n×n S-box

The input-output mapping of an S-box is assumed to be known, i.e., the output is assumed to be known when the input is completely known (or vice versa). In an ideal S-box, however, partial information about the input bits should not reduce the uncertainty in the unknown output bits (or vice versa).

The static view of the S-box is shown in Figure 1. If $\mathbf{X}_k= \{x_{j_1}, x_{j_2}, ..., x_{j_k}\}$; where $1 \leq k \leq n-1$; $1 \leq j_1, j_2, ..., j_k \leq n$, is a subset of the input bits and $\mathbf{Y}_t= \{y_{l_1}, y_{l_2}, ..., y_{l_t}\}$; where $1 \leq t \leq n-1$; $1 \leq l_1, l_2, ..., l_t \leq n$, is a subset

of the output bits, then the Static Input-Output Information Leakage is the mutual information between $\mathbf{Y}_t$ and $\mathbf{X}_k$ which is given by :

$$SL[I;O] = I(\mathbf{Y}_t;\mathbf{X}_k) = H(\mathbf{Y}_t) - H(\mathbf{Y}_t|\,\mathbf{X}_k).$$

The averaged* SL[I;O] matrices of a 4×4 DES S-box and one of the S-boxes found by Dawson & Tavares are given in Table 1. The detailed SL[I;O] matrices for these two S-boxes are given in Tables 2 and 3. In these tables, the information leakage is given in bits/input. The S-boxes considered in the example are as follows :

DES S-box : { 0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8 }
Dawson & Tavares S-box : { 7,9,1,10,12,14,0,5,4,13,11,6,2,3,15,8 }.

k	DES S-box			Dawson & Tavares S-box		
	t			t		
	1	2	3	1	2	3
1	0.0228	0.1060	0.3750	0.0114	0.0786	0.3750
2	0.0865	0.4271	1.0938	0.0786	0.4284	1.1250
3	0.3594	1.0885	2.0000†	0.3750	1.1250	2.0391

Table 1. Averaged SL[I;O] matrices for the DES and the Dawson & Tavares S-box

2.2. Dynamic Input-Output Information Leakage (DL[I;O])

In an ideal S-box information about any changes in the input bits should not reduce the uncertainty in the changes in the output bits.

The dynamic view of an S-box (delta S-box) is shown in Figure 2 in which the steady state value of the input $\mathbf{X}_c$ is assumed to be unknown. If $\Delta\mathbf{X}_k = \{\Delta x_{j_1}, \Delta x_{j_2}, ..., \Delta x_{j_k}\}$; where $1 \le k \le n$; $1 \le j_1, j_2, ..., j_k \le n$, is a set of changes in the input bits and $\Delta\mathbf{Y}_t = \{\Delta y_{l_1}, \Delta y_{l_2}, ..., \Delta y_{l_t}\}$; where $1 \le t \le n$; $1 \le l_1, l_2, ..., l_t \le n$, is a set of changes in the output bits then the Dynamic Input-Output Information Leakage is the mutual information between $\Delta\mathbf{Y}_t$ and $\Delta\mathbf{X}_k$ which is given by :

$$DL[I;O] = I(\Delta\mathbf{Y}_t;\Delta\mathbf{X}_k) = H(\Delta\mathbf{Y}_t) - H(\Delta\mathbf{Y}_t \mid \Delta\mathbf{X}_k).$$

---

* averaged means that for any k and t, the leakage is averaged over all the choices of $\mathbf{Y}_t$ and $\mathbf{X}_k$.

† In all the DES S-boxes, when t=k=3 the static input-output information leakage is 2 bits/input which is the minimum possible value for $I(\mathbf{Y}_3,\mathbf{X}_3)$ in a 4×4 S-box.

Input Bit(s)	Output Bit(s)													
	y_1	y_2	y_3	y_4	y_1y_2	y_1y_3	y_1y_4	y_2y_3	y_2y_4	y_3y_4	$y_1y_2y_3$	$y_1y_2y_4$	$y_1y_3y_4$	$y_2y_3y_4$
x_1	0.0000	0.0000	0.0000	0.0456	0.0000	0.0000	0.0944	0.0000	0.0944	0.0944	0.0000	0.7500	0.2500	0.2500
x_2	0.0456	0.0456	0.0000	0.0000	0.3444	0.0944	0.0944	0.0944	0.0944	0.0000	0.5000	0.5000	0.2500	0.2500
x_3	0.0456	0.0456	0.0456	0.0000	0.3444	0.0944	0.0944	0.0944	0.0944	0.0944	0.5000	0.5000	0.2500	0.5000
x_4	0.0000	0.0000	0.0456	0.0456	0.0000	0.0944	0.0944	0.0944	0.0944	0.3444	0.2500	0.2500	0.5000	0.5000
x_1x_2	0.0944	0.0944	0.1887	0.0944	0.5000	0.5000	0.3750	0.5000	0.6250	0.5000	1.0000	1.3750	1.0000	1.1250
x_1x_3	0.0944	0.0944	0.0944	0.0944	0.5000	0.5000	0.6250	0.2500	0.3750	0.3750	1.0000	1.3750	1.1250	1.0000
x_1x_4	0.0000	0.0000	0.0944	0.0944	0.0000	0.2500	0.2500	0.2500	0.2500	0.6250	1.0000	1.0000	1.0000	1.0000
x_2x_3	0.0944	0.0944	0.0944	0.0000	0.7500	0.3750	0.2500	0.3750	0.2500	0.2500	1.1250	1.0000	1.1250	1.0000
x_2x_4	0.0944	0.0944	0.0944	0.0944	0.7500	0.3750	0.3750	0.3750	0.3750	0.7500	1.1250	1.1250	1.1250	1.1250
x_3x_4	0.0944	0.0944	0.0944	0.0944	0.7500	0.3750	0.3750	0.3750	0.3750	0.6250	1.1250	1.1250	1.0000	1.2500
$x_1x_2x_3$	0.2500	0.2500	0.5000	0.2500	1.0000	1.1250	1.0000	1.1250	1.0000	1.0000	2.0000	2.0000	2.0000	2.0000
$x_1x_2x_4$	0.2500	0.2500	0.5000	0.5000	1.0000	1.1250	1.0000	1.0000	1.1250	1.3750	2.0000	2.0000	2.0000	2.0000
$x_1x_3x_4$	0.2500	0.2500	0.5000	0.5000	1.0000	1.1250	1.1250	1.0000	1.0000	1.2500	2.0000	2.0000	2.0000	2.0000
$x_2x_3x_4$	0.5000	0.2500	0.2500	0.2500	1.5000	1.0000	1.0000	1.0000	1.0000	1.1250	2.0000	2.0000	2.0000	2.0000‡

Table 2. Detailed SL[I;O] matrix for the DES S-box

‡ Minimum value of SL[I;O] when t=k=3

Input Bit(s)	Output Bit(s)													
	y_1	y_2	y_3	y_4	y_1y_2	y_1y_3	y_1y_4	y_2y_3	y_2y_4	y_3y_4	$y_1y_2y_3$	$y_1y_2y_4$	$y_1y_3y_4$	$y_2y_3y_4$
x_1	0.0000	0.0000	0.0000	0.0456	0.1887	0.0000	0.0944	0.0000	0.0944	0.0944	0.5000	0.5000	0.2500	0.2500
x_2	0.0000	0.0000	0.0456	0.0000	0.0000	0.0944	0.0000	0.0944	0.1887	0.0944	0.2500	0.5000	0.2500	0.5000
x_3	0.0456	0.0000	0.0000	0.0000	0.0944	0.0944	0.0944	0.0000	0.0000	0.1887	0.2500	0.2500	0.5000	0.5000
x_4	0.0000	0.0456	0.0000	0.0000	0.0944	0.0000	0.1887	0.0944	0.0944	0.0944	0.2500	0.5000	0.5000	0.2500
x_1x_2	0.1887	0.0000	0.0944	0.0944	0.5000	0.5000	0.5000	0.2500	0.5000	0.6250	1.1250	1.2500	1.1250	1.1250
x_1x_3	0.0944	0.0000	0.0000	0.0944	0.5000	0.2500	0.6250	0.0000	0.2500	0.5000	1.0000	1.1250	1.1250	1.0000
x_1x_4	0.0000	0.0944	0.0000	0.0944	0.5000	0.0000	0.5000	0.2500	0.6250	0.2500	1.0000	1.2500	1.0000	1.1250
x_2x_3	0.0944	0.1887	0.0944	0.0000	0.5000	0.6250	0.2500	0.5000	0.5000	0.5000	1.1250	1.1250	1.1250	1.1250
x_2x_4	0.0000	0.0944	0.0944	0.1887	0.2500	0.2500	0.5000	0.6250	0.6722	0.5000	1.0000	1.2500	1.1250	1.2500
x_3x_4	0.0944	0.0944	0.1887	0.0000	0.3750	0.5000	0.5000	0.5000	0.2500	0.5000	1.1250	1.0000	1.2500	1.1250
$x_1x_2x_3$	0.5000	0.5000	0.2500	0.2500	1.2500	1.1250	1.1250	1.0000	1.1250	1.1250	2.0000	2.1250	2.0000	2.0000
$x_1x_2x_4$	0.5000	0.2500	0.2500	0.5000	1.1250	1.0000	1.2500	1.1250	1.2500	1.1250	2.0000	2.1250	2.0000	2.1250
$x_1x_3x_4$	0.2500	0.2500	0.5000	0.2500	1.1250	1.0000	1.1250	1.0000	1.0000	1.1250	2.0000	2.0000	2.0000	2.0000
$x_2x_3x_4$	0.2500	0.5000	0.5000	0.5000	1.0000	1.1250	1.1250	1.2500	1.2500	1.2500	2.0000	2.0000	2.1250	2.1250

Table 3. Detailed SL[I;O] matrix for the Dawson & Tavares S-box

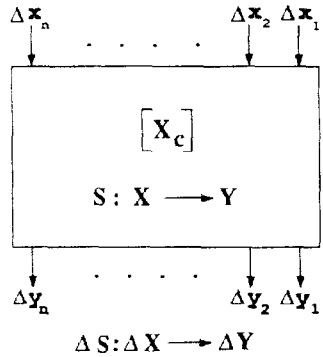


Figure 2. An n × n delta S-box

The averaged DL[I;O] matrices of the 4×4 DES S-box and the Dawson & Tavares S-box of the above example are given in Table 4. The detailed DL[I;O] matrix for the DES S-box is given in Table 5. In these tables, the information leakage is given in bits/input change.

k	DES S-box				Dawson & Tavares S-box			
	t				t			
	1	2	3	4	1	2	3	4
1	0.0014	0.0102	0.0462	0.1725	0.0007	0.0104	0.0437	0.1333
2	0.0066	0.0371	0.1586	0.4958	0.0104	0.0476	0.1484	0.3558
3	0.0317	0.1286	0.4362	1.0202	0.0437	0.1484	0.3756	0.7741
4	0.1333	0.4220	0.9866	1.7541	0.1333	0.3558	0.7741	1.4024

Table 4. Averaged DL[I;O] matrices for the DES and the Dawson & Tavares S-box

In [10] Output-Input Information Leakage, which is the same as the Input-Output Information Leakage, except that the input and the output are interchanged, has been defined as a separate property in both the static and the dynamic cases. But due to the symmetry in mutual information, i.e., $I(A;B) = I(B;A)$, the output-input information leakage matrix is simply the transposition of the input-output information leakage matrix in both the static and the dynamic cases for any bijective S-box. Therefore, the output-input information leakage is a redundant criterion for both the static and the dynamic conditions for any bijective S-box.

Input Change	Output Change														
	y_1	y_2	y_3	y_4	y_1y_2	y_1y_3	y_1y_4	y_2y_3	y_2y_4	y_3y_4	$y_1y_2y_3$	$y_1y_2y_4$	$y_1y_3y_4$	$y_2y_3y_4$	$y_1y_2y_3y_4$
x_1	0.0000	0.0000	0.0000	0.0028	0.0000	0.0000	0.0057	0.0000	0.0057	0.0057	0.0000	0.2557	0.0114	0.0114	0.2901
x_2	0.0028	0.0028	0.0000	0.0000	0.0516	0.0057	0.0057	0.0057	0.0057	0.0000	0.0578	0.0578	0.0114	0.0114	0.1333
x_3	0.0028	0.0028	0.0028	0.0000	0.0516	0.0057	0.0057	0.0057	0.0057	0.0057	0.0578	0.0578	0.0114	0.0578	0.1333
x_4	0.0000	0.0000	0.0028	0.0028	0.0000	0.0057	0.0057	0.0057	0.0057	0.0516	0.0114	0.0114	0.0578	0.0578	0.1333
x_1x_2	0.0057	0.0057	0.0456	0.0057	0.0578	0.0578	0.0164	0.0578	0.0618	0.0578	0.1333	0.3830	0.0776	0.1279	0.5186
x_1x_3	0.0057	0.0057	0.0057	0.0057	0.0578	0.0578	0.0618	0.0114	0.0164	0.0164	0.1333	0.3830	0.1279	0.0776	0.5186
x_1x_4	0.0000	0.0000	0.0057	0.0057	0.0000	0.0114	0.0114	0.0114	0.0114	0.0618	0.2901	0.2901	0.0776	0.0776	0.6676
x_2x_3	0.0057	0.0057	0.0057	0.0000	0.1099	0.0164	0.0114	0.0164	0.0114	0.0114	0.1279	0.1333	0.2778	0.0776	0.5186
x_2x_4	0.0057	0.0057	0.0057	0.0057	0.1099	0.0164	0.0164	0.0164	0.0164	0.1099	0.1279	0.1279	0.1279	0.1279	0.3603
x_3x_4	0.0057	0.0057	0.0057	0.0057	0.1099	0.0164	0.0164	0.0164	0.0164	0.0618	0.1279	0.1279	0.0776	0.1659	0.3909
$x_1x_2x_3$	0.0114	0.0114	0.0578	0.0114	0.1333	0.1279	0.0776	0.3423	0.0776	0.0776	0.5186	0.5590	0.4591	0.5022	1.0990
$x_1x_2x_4$	0.0114	0.0114	0.0578	0.0578	0.1333	0.1279	0.0776	0.0776	0.1279	0.2093	0.5186	0.5186	0.3249	0.3249	1.0319
$x_1x_3x_4$	0.0114	0.0114	0.0578	0.0578	0.1333	0.1279	0.1279	0.0776	0.0776	0.1659	0.5186	0.5186	0.3444	0.3295	1.0472
$x_2x_3x_4$	0.0578	0.0578	0.0114	0.0114	0.3444	0.0776	0.0776	0.0776	0.0776	0.1320	0.3909	0.3909	0.4591	0.3013	0.9027
$x_1x_2x_3x_4$	0.1333	0.1333	0.1333	0.1333	0.5000	0.3909	0.3608	0.5590	0.3608	0.3608	1.1173	0.9847	0.9222	0.9222	1.7541

Table 5. Detailed DL[I;O] matrix for the DES S-box

2.3. Dynamic Ouput-Output Information Leakage (DL[O;O])

For any given change $\Delta \mathbf{X}$ at the input, if $\Delta \mathbf{Y}_k = \{\Delta y_{j_1}, \Delta y_{j_2}, ..., \Delta y_{j_k}\}$; where $1 \leq k \leq n-1$; $1 \leq j_1, j_2, ..., j_k \leq n$, is a set of changes in the output bits and $\Delta \mathbf{Y}_t = \{\Delta y_{l_1}, \Delta y_{l_2}, ..., \Delta y_{l_t}\}$; where $1 \leq t \leq n-1$; $1 \leq l_1, l_2, ..., l_t \leq n$, is another set of changes in the output bits such that $\Delta \mathbf{Y}_k \cap \Delta \mathbf{Y}_t = \{\emptyset\}$, then the Dynamic Output-Output Information Leakage (with respect to $\Delta \mathbf{X}$) is the mutual information between $\Delta \mathbf{Y}_k$ and $\Delta \mathbf{Y}_t$ which is given by :

$$\mathrm{DL[O;O]} = I(\Delta \mathbf{Y}_t; \Delta \mathbf{Y}_k) = H(\Delta \mathbf{Y}_t) - H(\Delta \mathbf{Y}_t \mid \Delta \mathbf{Y}_k).$$

In any bijective S-box, under the static condition, for any given subset of output bits $\mathbf{Y}_k$, each of the 2^t combinations of the bits from another subset of output bits $\mathbf{Y}_t$ (such that $\mathbf{Y}_k \cap \mathbf{Y}_t = \{\emptyset\}$) occurs with equal probability over all the possible static states. Therefore, the mutual information between $\mathbf{Y}_k$ and $\mathbf{Y}_t$ must be zero. This may not be true under the dynamic condition where the correlation in the output bits could be exploited to gain information about the unknown changes in the output bits. Thus, this information theoretic property is cryptographically meaningful only under the dynamic condition for a bijective S-box.

The averaged DL[O;O] matrices of the 4×4 DES S-box and the Dawson & Tavares S-box of the above examples are given in Table 6. The detailed DL[O;O] matrix for the DES S-box is given in Table 7. In these tables, the information leakage is given in bits/output change.

k	DES S-box			Dawson & Tavares S-box		
	t			t		
	1	2	3	1	2	3
1	0.1659	0.4600	0.6766	0.0952	0.3040	0.5280
2	0.4600	0.9707	-§	0.3040	0.7368	-
3	0.6766	-	-	0.5280	-	-

Table 6. The averaged DL[O;O] matrices for the DES and the Dawson & Tavares S-box

In fact, there is an averaged DL[O;O] matrix for each value of $\Delta \mathbf{X}$ (i.e., for each pattern of input change). In this paper, however, the average values of DL[O;O] for each value of $\Delta \mathbf{X}$ (from a single bit change to four bit change) are calculated and averaged again to form a single matrix. Note that due to the symmetry in mutual information the element a_{ij} is equal to the element a_{ji} in the DL[O;O] matrix.

§ " - " means $\Delta \mathbf{Y}_k \cap \Delta \mathbf{Y}_t \neq \{\emptyset\}$

Change in Output (Subset 2)	Change in Output (subset 1)													
	y_1	y_2	y_3	y_4	y_1y_2	y_1y_3	y_1y_4	y_2y_3	y_2y_4	y_3y_4	$y_1y_2y_3$	$y_1y_2y_4$	$y_1y_3y_4$	$y_2y_3y_4$
y_1	-	0.2490	0.1327	0.1005	-	-	-	0.4534	0.5234	0.4567	-	-	-	0.7453
y_2	0.2490	-	0.3119	0.1005	-	0.6327	0.5234	-	-	0.4567	-	-	0.7453	-
y_3	0.1327	0.3119	-	0.1005	0.5163	-	0.4567	-	0.4567	-	-	0.6786	-	-
y_4	0.1005	0.1005	0.1005	-	0.3748	0.4245	-	0.2453	-	-	0.5371	-	-	-
y_1y_2	-	-	0.5163	0.3748	-	-	-	-	-	0.9529	-	-	-	-
y_1y_3	-	0.6327	-	0.4245	-	-	-	-	1.0693	-	-	-	-	-
y_1y_4	-	0.5234	0.4567	-	-	-	-	0.8900	-	-	-	-	-	-
y_2y_3	0.4534	-	-	0.2453	-	-	0.8900	-	-	-	-	-	-	-
y_2y_4	0.5234	-	0.4567	-	-	1.0693	-	-	-	-	-	-	-	-
y_3y_4	0.4567	0.4567	-	-	0.9529	-	-	-	-	-	-	-	-	-
$y_1y_2y_3$	-	-	-	0.5371	-	-	-	-	-	-	-	-	-	-
$y_1y_2y_4$	-	-	0.6786	-	-	-	-	-	-	-	-	-	-	-
$y_1y_3y_4$	-	0.7453	-	-	-	-	-	-	-	-	-	-	-	-
$y_2y_3y_4$	0.7453	-	-	-	-	-	-	-	-	-	-	-	-	-

Table 7. Detailed DL[O;O] matrix for the DES S-box

‖ $\Delta Y_t \cap \Delta Y_k \neq \{\emptyset\}$

2.4. XOR Input-Output Information Leakage (XL[I;O])

The XOR distribution gives the probability distribution of the input XOR and the output XOR for an S-box. Biham & Shamir [16] first used the XOR distribution for their differential attack on DES-like cryptosystems. The XOR distribution of the DES S-box of the above example is given in Table 8.

If ΔX is the input XOR and ΔY is the output XOR, then the XOR Input-Output Information Leakage is the mutual information between ΔX and ΔY and is given by :

$$XL[I;O] = I(\Delta Y; \Delta X) = H(\Delta Y) - H(\Delta Y \mid \Delta X).$$

In an n×n S-box, for any given input XOR, if each output XOR occurs with equal probability, the XOR distribution must have all identical entries. Such an XOR distribution is called a "uniform" or "flat" distribution. The "differential probability" corresponding to an entry in the XOR distribution is obtained by dividing that entry by 2^n, where n is the block size of the S-box (or SP-network). Thus, in a uniform XOR distribution the highest differential probability is $1/2^n$. For a uniform XOR distribution XL[I;O] is zero. However, due to the nature of the XOR operation, each output XOR either occurs an even number of times or does not occur at all. Further, in an S-box when $\Delta X = 0$, $\Delta Y = 0$. Thus, a zero input XOR and the corresponding output XORs are trivial.

In the XOR distribution for an n×n S-box the sum of the entries in a row is 2^n, and if the S-box is bijective the sum of the entries in a column is also 2^n. Therefore, in the "best possible distribution" for an n×n S-box, an entry corresponding to a non-zero input XOR can be either 0 or 2. Thus, for a non-zero input XOR half of the possible output XORs do not occur. For a 4×4 S-box with the best possible distribution, XL[I;O] will be 1.1875 bits/input XOR which is the minimum value of XL[I;O] for any 4×4 S-box. However, Adams [17] showed that an n×n S-box with the best possible XOR distribution cannot be bijective when n is even.

It should be noted that in an n×n S-box, XL[I;O] is the same as DL[I;O] when t = k = n. Thus, XL[I:O] is not an independent evaluation criterion. However, XL[I;O] is useful in measuring how far an XOR distribution deviates from a uniform XOR distribution, using a single "quantity". Further, due to the symmetry in mutual information, the XOR output-input information leakage is the same as the XOR input-output information leakage, i.e., XL[O;I]=XL[I;O].

XL[I;O] for the DES S-box and the Dawson & Tavares S-box of the above examples are 1.7541 bits/input XOR and 1.4024 bits/ input XOR respectively (note that these values correspond to DL[I;O] in Table 4 when t = k = 4). The highest XL[I;O] among the 4×4 DES S-boxes is 1.8438 bits/input XOR. We note that using S-boxes with uniform XOR distribution does not necessarily increase the immunity of an SPN cryptosystem against a differential attack [18]. In order to develop resistance to a differential attack, other design criteria must also be taken into consideration.

XL[I;O] = 1.7541 bits / input XOR

Input XOR	Output XOR															
	0000	0001	0010	0100	1000	0011	0101	1001	0110	1010	1100	0111	1011	1101	1110	1111
0000	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	0	0	0	0	0	2	0	0	0	0	8	2	2	0	0	2
0010	0	0	0	0	0	4	0	0	2	2	0	2	2	4	0	0
0100	0	0	0	0	0	6	2	0	0	2	0	0	0	2	2	2
1000	0	0	0	0	0	0	0	4	0	2	0	4	2	0	2	2
0011	0	4	0	2	2	0	0	0	2	2	0	0	0	0	0	4
0101	0	2	2	2	2	0	0	2	2	0	0	0	0	0	0	4
1001	0	0	2	0	2	0	4	0	2	0	2	0	4	0	0	0
0110	0	0	0	0	0	0	2	4	2	0	0	0	0	2	6	0
1010	0	0	2	6	0	0	0	0	0	2	2	0	0	4	0	0
1100	0	2	0	6	0	0	0	2	0	4	2	0	0	0	0	0
0111	0	2	6	0	0	0	4	2	0	2	0	0	0	0	0	0
1011	0	4	0	0	4	2	0	0	2	0	0	0	2	0	2	0
1101	0	0	0	0	4	0	2	0	4	0	0	2	0	2	0	2
1110	0	2	2	0	0	2	0	2	0	0	0	6	0	0	2	0
1111	0	0	2	0	2	0	2	0	0	0	2	0	4	2	2	0

Table 8. XOR distribution for the DES S-box

3. An Equivalence Class on S-boxes

Consider the n×n S-box S′ created by XORing X_r and Y_s with the input and the output respectively of the n×n S-box S as shown in Figure 3. X_r and Y_s are arbitrary fixed n-bit binary vectors.

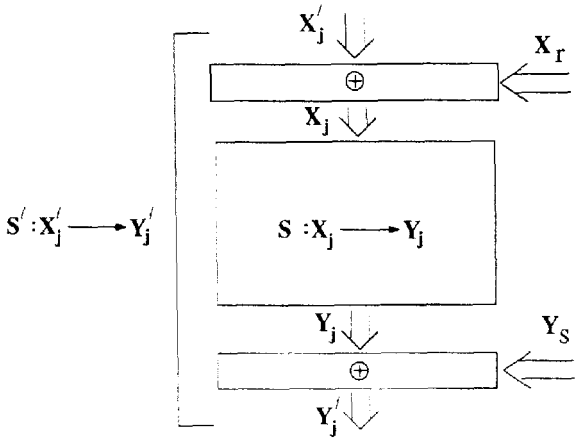


Figure 3. Equivalent S-boxes S and S′ with invariant information leakage

Since

$$Prob(\mathbf{X}_j) = Prob(\mathbf{X}'_j \oplus \mathbf{X}_r) = Prob(\mathbf{X}'_j)$$

and

$$Prob(\mathbf{Y}_j) = Prob(\mathbf{Y}'_j \oplus \mathbf{Y}_s) = Prob(\mathbf{Y}'_j)$$

the SL[I;O] of S is the same as that of S′. Also, since the properties related to the changes in the input and the output bits are invariant to the XOR operations at the input and the output, all the dynamic information leakages (DL[I;O], DL[O;O] and XL[I;O]) will be the same for both S and S′. Therefore, in this fashion, we can generate 2^{2n} equivalent n×n S-boxes with invariant information leakage and with different input-output mapping.

A new S-box S″ can be generated by permuting the input and/or output bits of the original S-box S. S″ will have similar cryptographic properties to S. However, due to the bit permutation, the entries of the leakage matrices and the XOR distribution of S″ may be located differently. Starting with S″, a new class of S-boxes can be generated using the above procedure. Hence, if a single S-box with low information leakage is found (possibly through a computer search), a large number of S-boxes with similar information leakage can be created easily.

4. Differential Attack on SP Networks

The differential attack developed by Biham & Shamir is a statistical chosen plaintext attack on DES-like block ciphers. If a pair of distinct plaintexts with known XOR difference ΔX produces a pair of $(r-1)^{th}$ round ciphertexts Y_{r-1} and Y'_{r-1} such

that $\mathbf{Y}_{r-1} \oplus \mathbf{Y}'_{r-1} = \Delta\mathbf{Y}_{r-1}$; then an r round cipher is vulnerable to the differential attack if and only if the following conditions hold [19] :

I. There exists a pair of (r-1)th round outputs $\mathbf{Y}_{r-1}$ and $\mathbf{Y}'_{r-1}$ such that $Prob(\Delta\mathbf{Y}_{r-1} \mid \Delta\mathbf{X})$ is greater than $1/2^m$, where m is the cipher block size.

II. Given some pairs of $\mathbf{Y}_{r-1}$ and $\mathbf{Y}'_{r-1}$ it is possible to determine some key bits in the rth round.

The effectiveness of this line of attack depends on how confidently the (r-1)th round XOR values (corresponding to the chosen input XOR) can be predicted in the SP network. In the cryptosystem, if XL[I;O] is zero after the (r-1)th round then the maximum differential probability reaches the ideal value which is $1/2^m$ (m is the cipher block size). Hence, the first condition will be satisfied. However, due to the nature of the XOR operation, an SP network with even the best possible XOR distribution will have a differential probability of $1/2^{m-1}$ (i.e., $2/2^m$).

In an SP network, keying can be introduced in one of the two ways shown in Figure 4. DES uses a combination of these two methods. In Figure 4 (a), the (r-1) th

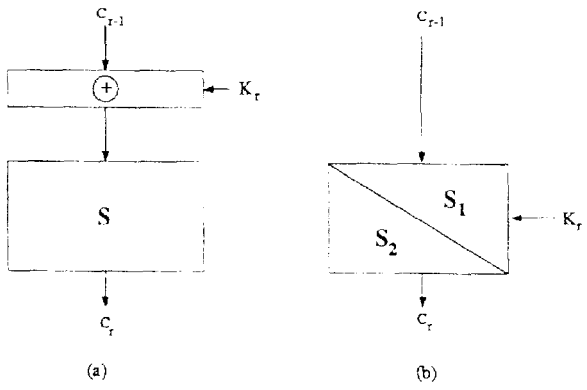


Figure 4. Two possible methods of keying

round ciphertext C_{r-1} is XORed with the r th round key K_r to form the actual input to the S-box. A given $(\Delta C_{r-1}, \Delta C_r)$ pair, where $\Delta C_{r-1} \neq 0$, restricts the possible values for the actual input to the S-box. Using the actual input and the value of C_{r-1} (if known) the uncertainty in K_r can be reduced. However, in an SPN cryptosystem using this keying arrangement, if the value of C_{r-1} is not available (note that this condition is not satisfied in DES-like systems), a differential cryptanalyst cannot learn about the key using the knowledge of the input XOR and the output XOR of the S-box.

In Figure 4 (b), one bit in K_r is used to select one of the two S-boxes : S_1 and S_2. In this arrangement, K_r is not mixed with C_{r-1} to form the actual input to the S-box in the r th round. Since in this illustration only two S-boxes are used, a single key bit is sufficient to select an S-box. This arrangement is vulnerable to a differential attack if the two S-boxes do not have identical XOR distributions [13]. It has been pointed out by Heys [20] that a differential attack is possible, even if the S-boxes have identical XOR distributions (i.e., if S_1 and S_2 are chosen from an equivalence class). This can be explained with the help of Figure 5.

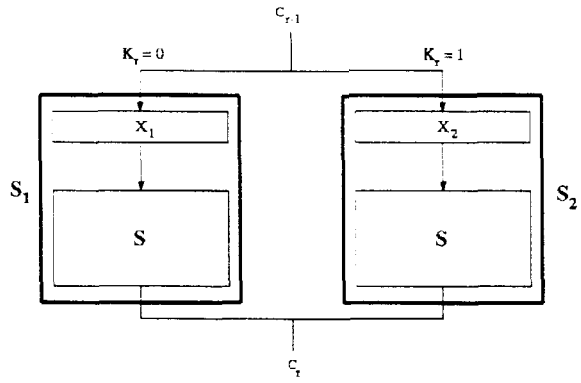


Figure 5. Differential attack on the arrangement shown in Figure 4 (b)

Assume that in Figure 5 the equivalent S-boxes S_1 and S_2 are derived by XORing the vectors X_1 and X_2 respectively at the input of the S-box S. The knowledge of a $(\Delta C_{r-1}, \Delta C_r)$ pair, where $\Delta C_{r-1} \neq 0$, would suggest the actual values of the input of S. Using these suggested values and the values of C_{r-1} (assumed to be known) we can obtain the possible values of the vectors X_1 and X_2, and compare them with the known values of X_1 and X_2 to get the keying information. Since only two S-boxes were used in this example, the described attack does not seem efficient. However, if a large number of S-boxes are used in this fashion, the differential attack would become more efficient.

Therefore, an SP network using one or a combination of the above keying techniques should be designed to minimize the maximum entry in the XOR distribution (i.e., maximum differential probability), in order to increase the immunity against differential attack.

5. Analysis of a 16-bit SP Network

In an r round SPN cryptosystem the substitution-permutation function is iterated r times so that the final product (ciphertext) is cryptographically stronger than the intermediate products. The number of rounds required depends strongly on the strength of the individual layers. If the individual layers are strong, the number of rounds required can be smaller which means that higher data encryption/decryption rates can be achieved. In order to study the influence of the S-boxes on the cryptographic properties of an SP network, a 16×16 SP network (which is tractable) shown in Figure 6 was evaluated with respect to various criteria explained above. The DES, Dawson & Tavares and some randomly selected S-boxes were used for this analysis. We found that some of the DES S-boxes are relatively stronger than the others with respect to information leakage. Therefore, under each evaluation criterion, the DES S-boxes with relatively low information leakage (DES-L) and relatively high information leakage (DES-H) were analyzed separately.

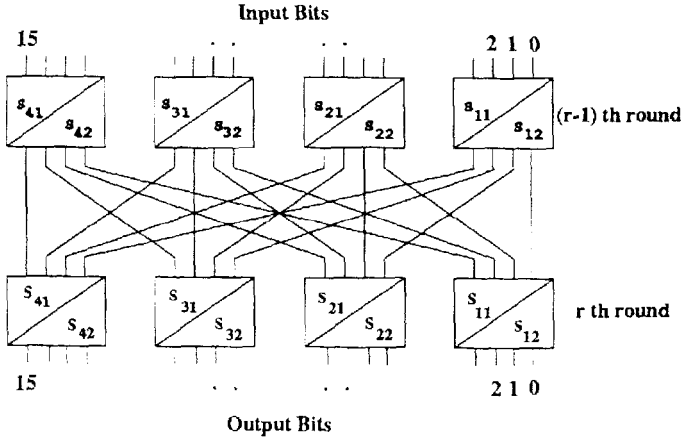


Figure 6. A 16 bit SP network

We first studied how the maximum differential probability of the SP network varies with the number of rounds (for the purpose of this test DES S-boxes were ranked according to their XL[I;O]). We know that even in the best case a non-zero minimum entry in the XOR distribution of the SP network is 2. Hence, for any non-zero input XOR, at least 50% of the output XORs do not occur. Since the S-boxes used are bijective, the 16–bit SP network is also bijective. As in the case of an S-box, a bijective SP network with XOR distribution containing only 0's and 2's is not realizable when the block size is even, which is true for the 16–bit SP network. Therefore, we can expect some entries in the XOR distribution which are greater than 2. Figure 7 shows the variation of the maximum entry in the XOR distribution (for 100 randomly selected non-zero input XORs) with the number of rounds. For all the S-boxes used, the highest entry in the XOR distribution converged to 14 (i.e., the maximum differential probability is $14/2^{16}$) after 5 rounds. Further, after 3 rounds there was not much difference in the maximum differential probability regardless of the selection of S-boxes. However, the S-boxes with low XL[I;O] led to faster convergence. In addition, we noted that for all the S-boxes the percentage of 0's (in a row) was 60.7% of the number of possible output XORs, once the convergence was achieved. We and Heys [20] observed that the distribution of entries in a given row in the XOR distribution, after a sufficient number of rounds, behaves like a random placement of $n/2$ balls in n bins, where each ball has a value of 2. The maximum entry in a row corresponding to the random placements was observed to be less than or equal to 14.

A well designed SP network can be regarded as a large strong S-box. Hence an ideal SP network should satisfy all the cryptographic properties of an ideal S-box. We then examined the 16–bit SP network on a round-by-round basis with respect to the four types of information leakages. For selected input and output bits the system was tested exhaustively, where feasible, or using a large number of randomly chosen inputs. The simulation results are shown in Figures 8 through 11.

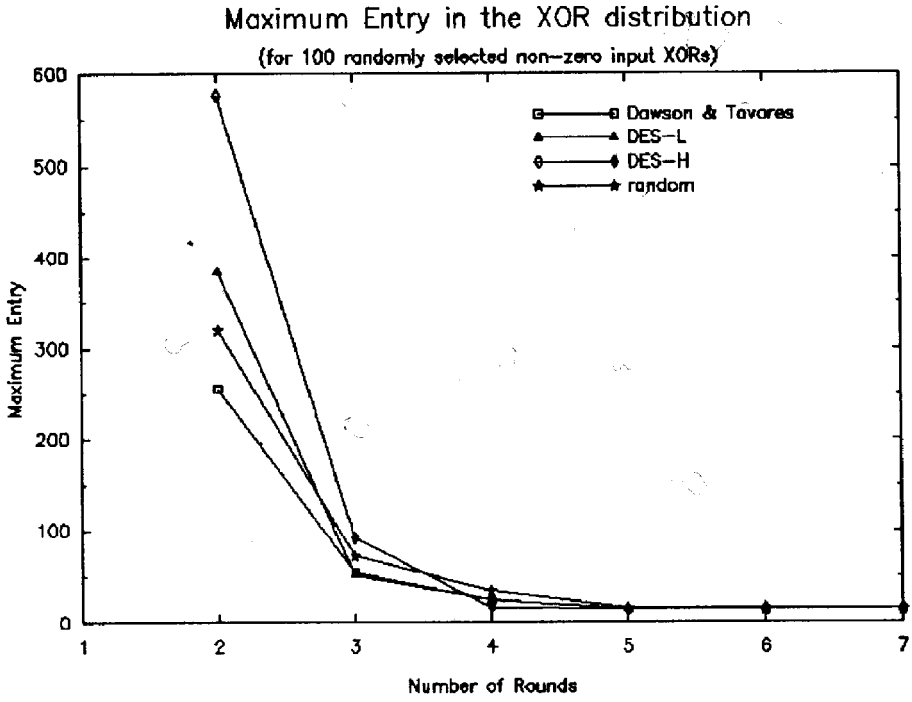


Figure 7. Variation of Maximum Entry in the XOR distribution with number of rounds for the 16–bit SP network

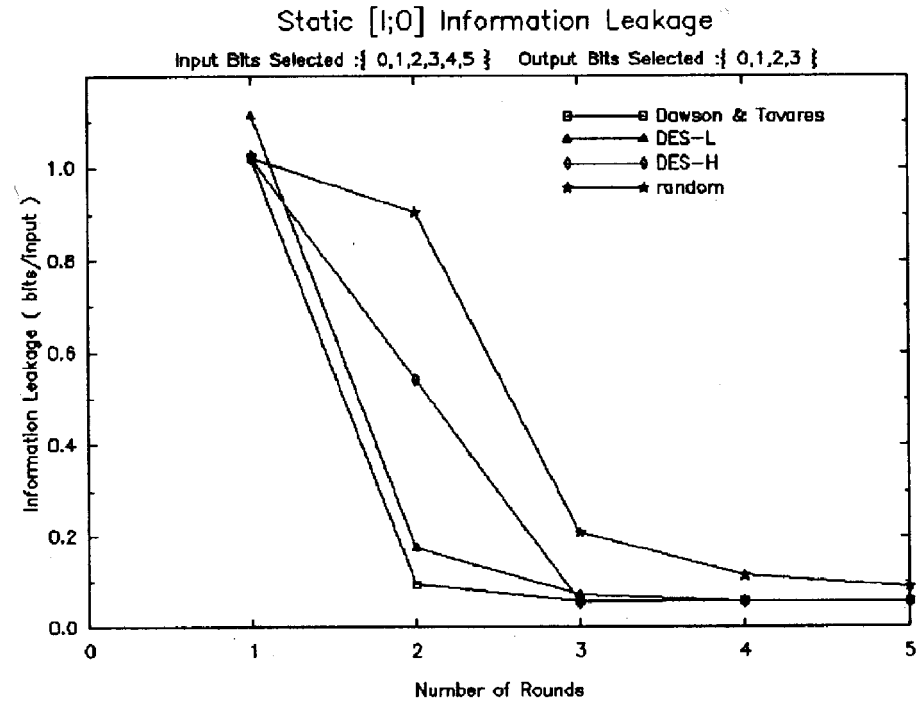


Figure 8. Variation of SL[I:O] with number of rounds for the 16–bit SP network

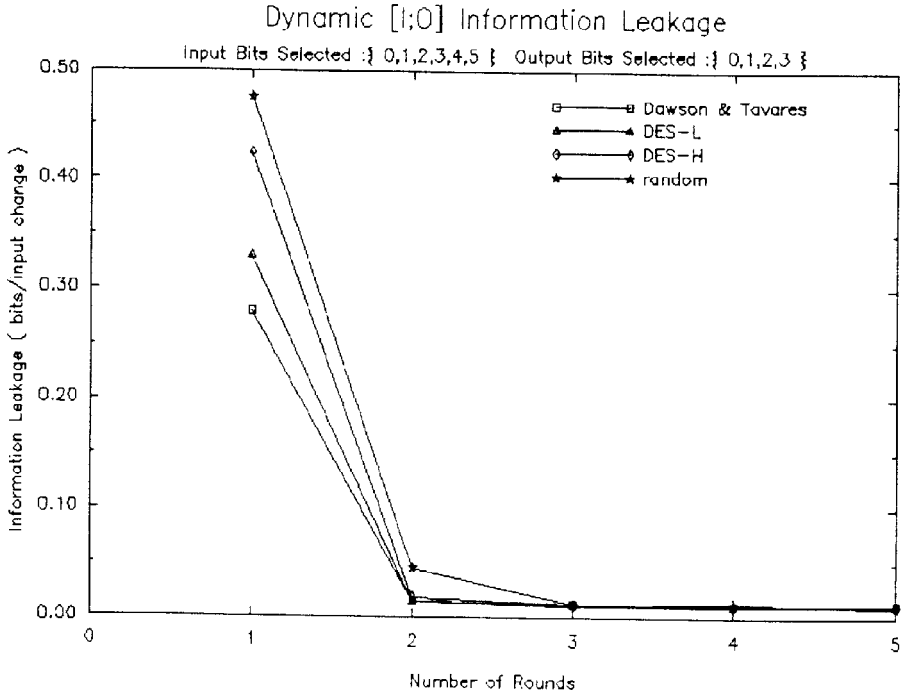
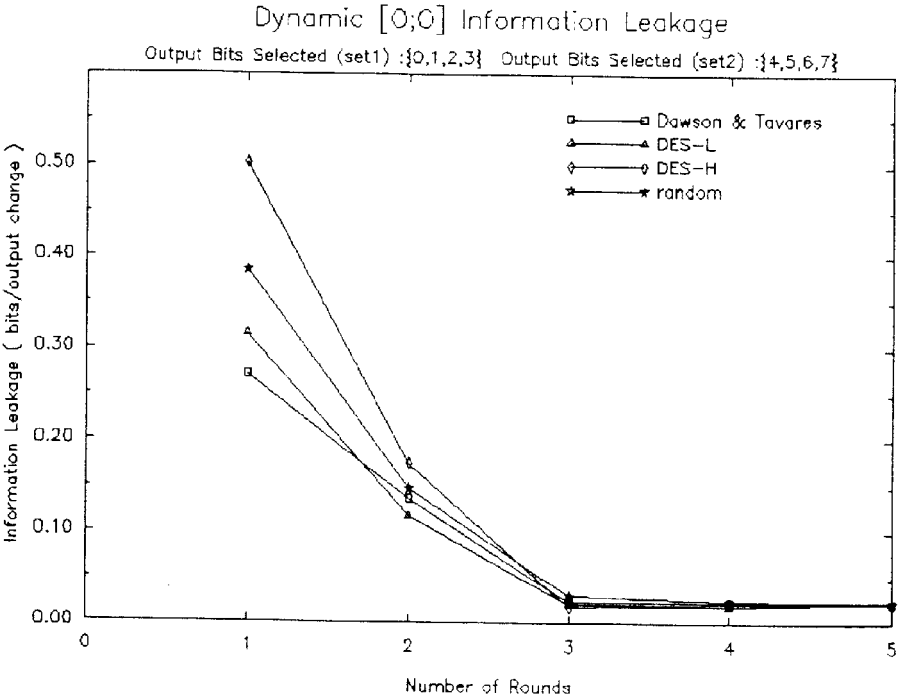


Figure 9. Variation of DL[I:O] with number of rounds for the 16–bit SP network



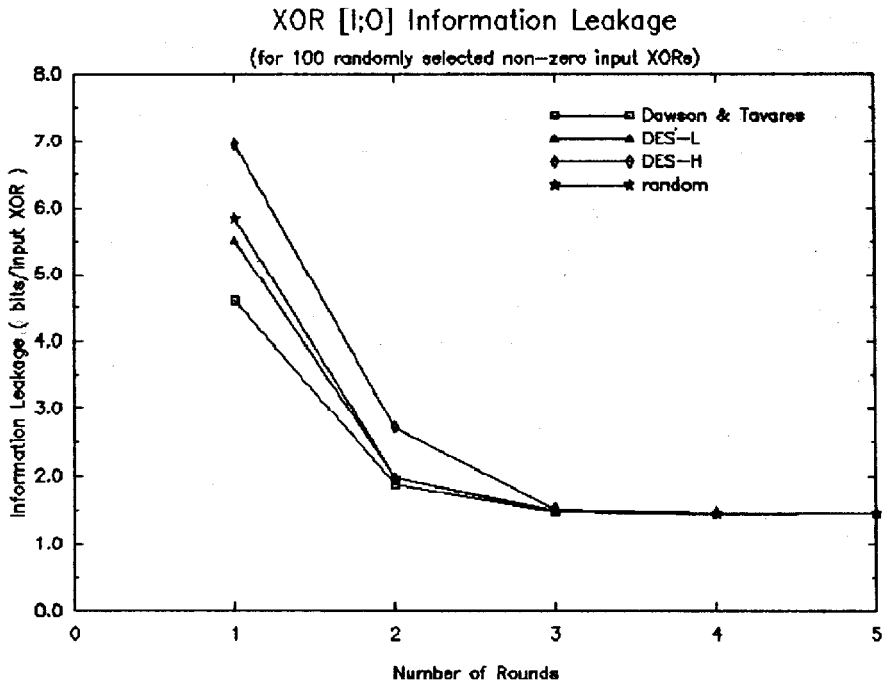


Figure 11. Variation of XL[I:O] with number of rounds for the 16-bit SP network

7. Conclusions

We reviewed evaluation criteria for n×n bijective S-boxes based on information leakage and introduced the concept of XOR Information Leakage (XL[I;O]), which is useful in comparing the XOR distributions of S-boxes. We then defined an equivalence class on n×n S-boxes which have invariant information leakage. The equivalence classes will reduce the search space for the design of cryptographically strong S-boxes with low information leakage. We also found that not all the DES S-boxes are equally strong with respect to information leakage.

We studied the impact of the choice of S-boxes on the cryptographic properties of a 16×16 SP network using various S-boxes. Sample S-boxes were chosen from the DES, Dawson & Tavares, and randomly constructed ones. The variation of the maximum entry in the XOR distribution with the number of rounds is shown in Figure 7. This experimental XOR distribution (corresponding to 100 randomly selected non-zero input XORs) closely approximates a random distribution of the output XORs after 5 rounds. After 3 rounds there is not much difference in the maximum entry in the XOR distribution regardless of the selection of S-boxes. However, the S-boxes with low XL[I;O] lead to faster convergence to the random XOR distribution.

We finally studied the influence of the S-boxes on the information leakage of the SP network. The simulation results are shown in Figures 8 through 11. Here four types of information leakages are plotted against the number of rounds. After 3 rounds there is not much difference in the information leakage of any kind, regardless

of the selection of the S-boxes. However, the choice of the S-boxes influences how fast the information leakage achieves the minimum value. Using the S-boxes which produce the fastest convergence in the SP network will lead to a more efficient and faster implementation of a substitution-permutation network cryptosystem. XL[I;O] for the SP network is of special interest with respect to a differential attack because it is a good measure of how confidently an output XOR can be predicted from a known input XOR in the SP network. For all the S-boxes used, the minimum value of XL[I;O] achieved is 1.45 bits / input XOR after 5 rounds. The value of XL[I;O] for a random distribution of 16–bit XORs is also 1.45 bits / input XOR. These observations suggest that, after a sufficient number of rounds, the XOR distribution of the 16–bit SP network converges to a distribution obtained by placing the output XOR pairs at random in the XOR distribution.

Bibliography

[1] N. B. of Standards, "Data Encryption Standard," No. 46, U.S. Department of Commerce, 1977.

[2] C. E. Shannon, "Communication theory of secrecy systems," in *Bell Systems Technical Journals*, vol. 28, pp. 656–715, 1949.

[3] H. Feistel, "Cryptography and Computer privacy," in *Scientific American*, vol. 228, pp. 15–23, 1973.

[4] H. Feistel, W. Notz, and J. L. Smith, "Some Cryptographic Techniques for Machine-to-Machine Data Comminications," in *Proc. of the IEEE*, vol. 63, pp. 1545–1554, 1975.

[5] A. F. Webster and S. E. Tavares, "On the Design of S-boxes," in *Advances in Cryptology, Proc. of CRYPTO '85*, pp. 523–534, Springer-Verlag, New York, 1986.

[6] E. F. Brickell, J. H. Moore, and M. R. Purtill, "Structure in the S-boxes of the DES (extended abstract)," in *Advances in Cryptology : Proc. of CRYPTO '86*, pp. 3–8, Springer-Verlag, New York, 1987.

[7] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," in *IEE Proceedings, Part E : Computers and Digital Techniques*, vol. 135, pp. 325–335, 1988.

[8] C. A. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," in *Journal of Cryptology*, vol. 3, pp. 27–41, 1990.

[9] R. Forré, "Methods and Instruments for designing S-boxes," in *Journal of Cryptology*, vol. 2, pp. 115–130, 1990.

[10] M. H. Dawson and S. E. Tavares, "An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-Like Attacks," in *Advances in Cryptology, Proc. of EUROCRYPT' 91*, pp. 352–367, Springer-Verlag, New York, 1992.

[11] J. B. Kam and G. I. Davida, "Structured Design of Substitution-Permutation Encryption Networks," in *IEEE Transaction on Computers*, C-28, pp. 747–753, 1979.

[12] A. F. Webster, "Plaintext/Ciphertext Bit Dependence in Cryptographic Systems," Master's thesis, Queen's University at Kingston, Canada, 1985.

[13] L. O'Connor, "A Differential-like cryptanalysis of SP-networks," tech. rep., Department of Computer Science, University of Waterloo, Canada, 1992. , (submitted for publication).

[14] A. Shimizu and S. Miyaguchi, "Fast data encryption algorith FEAL," in *Advances in Cryptology, EUROCRYPT '87*, pp. 267–278, 1988.

[15] L. Brown, J. Pieprzyk, and J. Seberry, "LOKI - cryptographic primitive for authentication and secrecy applications," in *Advances in Cryptology, Proc. of AUSCRYPT '90*, pp. 229–236, Springer-Verlag, New York, 1990.

[16] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystem," in *Journal of Cryptology*, vol. 4, pp. 3–72, 1991.

[17] C. A. Adams, "On immunity against Biham and Shamir's "differential cryptanalysis"," in *Information Processing Letters*, vol. 41, pp. 77–80, 1992.

[18] E. Biham, *Differential Cryptanalyst of Iterative Cryptosystem*. PhD thesis, Weizmann Institute of Science, Rehovolt, Israel, 1992.

[19] X. Lai and J. Massey, "Markov Ciphers and Differential Cryptanalysis," in *Advances in Cryptology, Proc. of EUROCRYPT' 91*, pp. 17–38, Springer-Verlag, New York, 1992.

[20] H. Heys , Department of Electrical Engineering, Queen's University, Kingston, Canada, (personal communication).