Chapter 3: Basics and Terminology

This chapter includes the terminology used throughout this research work. The input-output structure of S-boxes of DES and the sole S-box of AES are also discussed here for reference purpose.

3.1 Preliminaries

3.1.1 Terminology

Truly Random Sequence
An n bit sequence is a truly random sequence if each bit is independent from every other bit in the sequence.

Informally, it can be stated that the probability of regeneration of a truly random sequence is very low, though we cannot guarantee the non-regeneration of such a sequence **[1]**.

Relatively Random Sequence
Two *n* bit sequences are relatively random if the number of bit-by-bit successful matches between the two sequences is *n/2* **[1]**.

3.1.2 Notations Used

$\mathbb{Z}$	The set of integers
$\mathbb{Z}_2^n$	The *n* dimensional vector space over the finite field $\mathbb{Z}_2 - GF(2)$
$\oplus$	The addition over $\mathbb{Z}_2^n$, or, the bitwise exclusive-OR (XOR)
H	Hamming distance
wt (..)	Hamming weight function
C_2^n	*N* dimensional vector with Hamming weight 1 at the i^{th} position
N_F	Nonlinearity of an S-box
L_F	Linearity of an S-box

Table 3.1 Used Notation

3.1.3 Substitution Box (S-box)

The S-box of a block cipher, as shown in Figure 3.1, can be represented as an $m \times n$ mapping $S: \{0,1\}^m \rightarrow \{0,1\}^n$, and is designed using the principle laid down by Shannon (1949) **[23]**.

Thus there are n component functions, each being a map from m bits to 1. S-box may express security against particular a class of attack.

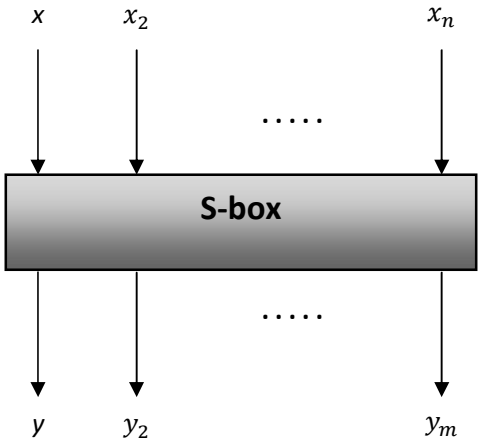

Figure 3.1: Substitution Box (S-Box)

Introduction of correlation attack **[24]** results the study of Boolean function and S-boxes in cryptography. Nonlinearity N_F and linearity L_F of an S-box is defined as

$$N_F = \min_{b \in F_2^m / \{0\}} N_{b.F} \text{ and } L_F = \max_{b \in F_2^m / \{0\}} L_{b.F}$$

The study of cryptographic properties of an S-box related to the linearity needs to consider all non-zero linear combination of S-box components **[25]**. So, an S-box can be represented by a vector$(f_0, f_1, \dots, f_{m-1})$, where f_i is one of the Boolean functions from $\{0,1\}^m$ to $\{0,1\}^n$.

3.1.3.1 Properties of an Ideal S-Box

In the "Practical S-Box Design" **[46]** the following properties has been identified that an ideal S-Box would possess:

- All linear combinations of S-Box columns are bent.
- All entries in the S-Box XOR table are 0 or 1.
- The S-Box satisfies MOSAC **[46]** [Minimum Order Strict Avalanche Criterion].
- The S-Box satisfies MOBIC **[46]** [Minimum Order Bit Independence Criterion].
- The set of weights of rows has a binomial distribution with mean $^n/_2$.
- The set of weights of all pairs of rows has a binomial distribution with mean $^n/_2$.

Substitution process ensures the security of data because it is a non-linear transformation which performs confusion of bits. Non-linear transformation is very essential in modern encryption algorithms and it is proved to be a strong cryptographic primitive against linear and differential cryptanalysis **[47]**.

There are several properties available for S-box as listed below **[48]**:

- Robustness: If $F = (f_1, f_2 \ldots . f_n)$ be an $n \times n$ S-box then F must be robust against differential cryptanalysis.
- Balancing: $S: \{0,1\}^n \longrightarrow \{0,1\}^m$ is balanced, if $HW(f) = 2^{n-1}$.
- Strict Avalanche Criterion (SAC).
- Non-linearity.
- Differential Uniformity: The smaller the differential uniformity, the better is the S-box resistance against differential cryptanalysis.
- Linear Approximation: The smaller the linear approximation, the better is the S-box resistance against linear cryptanalysis.
- Algebraic Complexity: The S-Box should be able to resist interpolation and algebraic attacks.
- Bit Independence Criterion

3.1.4 Structure of S-box of DES

The number of S-boxes of DES is 8 and every S-box contains 4 rows and 16 columns matrix form and each row consists of values ranging from $(0)_{10}$ to $(15)_{10}$. The structure of an S-box is illustrated in Figure 3.1. A 6 bit input to the S-box of DES generates 4 bit output as below:

$S = matrix\ 4 \times 16, values\ from\ 0\ to\ 15$
$B\ (6\ bit\ input) = \boldsymbol{b_1} b_2 b_3 b_4 b_5 \boldsymbol{b_6}$
$\boldsymbol{b_1 b_6} \rightarrow r = row\ of\ the\ matrix\ (2\ bits: 0,1,2,3)$
$b_2 b_3 b_4 b_5 \rightarrow c = column\ of\ matrix\ (4\ bits: 0,1, \ldots . ,15)$
$C\ (4\ bit\ output) = Binary\ representation\ S(r, c)$

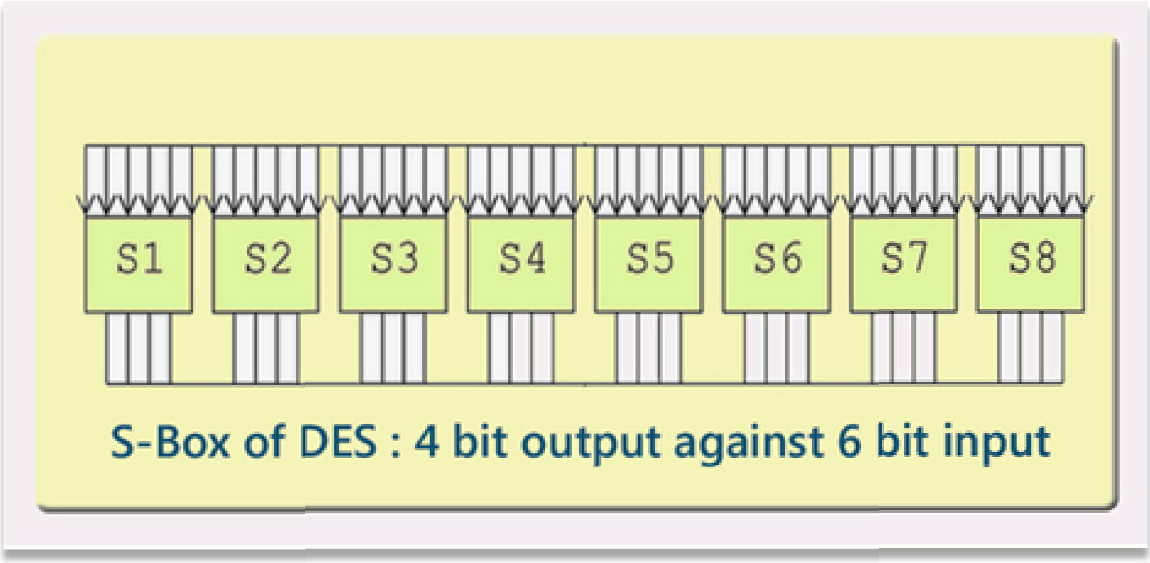

Figure 3.2: Structure of an S-box of DES

3.1.5 Structure of S-box of AES

There is a single non-linear S-box in AES with matrix structure of 16×16 where every individual element is a HEX value. Every 8-bit block of input generates 8-bit block of output. The structure of the S-box of AES is shown Figure 3.2. The evaluation method of output is as follows:

$S = matrix\ 16 \times 16, in\ HEX, values\ from\ 0\ to\ F$
$B\ (8\ bit\ input) = b_1 b_2 b_3 b_4 \boldsymbol{b_5 b_6 b_7 b_8}$
$b_1 b_2 b_3 b_4 \rightarrow r = row\ of\ the\ matrix\ for\ output$
$\boldsymbol{b_5 b_6 b_7 b_8} \rightarrow c = column\ of\ the\ matrix\ for\ output$
$C\ (8\ bit\ output) = Binary\ representation\ of\ hex\ value\ S(r, c)$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 3.3: Structure of S-box of AES