Differential Cryptanalysis

See:
Biham and Shamir,
Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993.

Differential Cryptanalysis

The first method which reduced the complexity of attacking DES below (half of) exhaustive search.

Note: In all the following discussion we ignore the existence of the initial and the final permutations, since they do not affect the analysis.

Motivation:

1. All the operations except for the S-boxes are linear.
2. Mixing the key in all the rounds prohibits the attacker from knowing which entries of the S-boxes are actually used, and thus he cannot know their output.

Differential Cryptanalysis (cont.)

How can we inhibit the key from hiding the information?

The basic idea of differential cryptanalysis: Study the differences between two encryptions of two different plaintexts: P and P^*.

Notation: For any value $\boldsymbol{X}$ during the encryption of P, and the corresponding value $\boldsymbol{X}^*$ during encryption of P^*, denote the difference by $\boldsymbol{X'} = \boldsymbol{X} \oplus \boldsymbol{X}^*$.

Differential Cryptanalysis (cont.)

Advantages: It is easy to predict the output difference of linear operations given the input difference:

- **Unary operations** (E, P, IP):

$$(P(X))' = P(X) \oplus P(X^*) = P(X')$$

- **Binary operations** (XOR):

$$(X \oplus Y)' = (X \oplus Y) \oplus (X^* \oplus Y^*) = X' \oplus Y'$$

- **Mixing the key**:

$$(X \oplus K)' = (X \oplus K) \oplus (X^* \oplus K) = X'$$

Differential Cryptanalysis (cont.)

We conclude that the differences are linear in linear operations, and in particular, **the result is key independent**.

Differences and the S Boxes

Assume we have two inputs X and X^* for the same S-box, and that **we know only their difference X'**.
Denote $Y = S(X)$.
What do we know about Y'?
The simple case: **when $X' = 0$**: $S(X) = S(X^*)$ for any X, and **$Y' = 0$**.
If $X' \neq 0$: we do not know the output difference.
Definition: Lets look on the distribution of the pairs (X', Y') of all the possible inputs X. We call the table containing this information **difference distribution table of the S-box**.

The Difference Distribution Table of S1

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
10_x	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
									⋮							
27_x	10	4	2	0	2	4	2	0	4	8	0	4	8	8	4	4
28_x	12	2	2	8	2	6	12	0	0	2	6	0	4	0	6	2
29_x	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4
$2A_x$	4	2	4	6	0	2	8	2	2	14	2	6	2	6	2	2
$2B_x$	12	2	2	2	4	6	6	2	0	2	6	2	6	0	8	4
$2C_x$	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6
$2D_x$	6	2	6	2	8	4	4	4	2	4	6	0	8	2	0	6
$2E_x$	6	6	2	2	0	2	4	6	4	0	6	2	12	2	6	4
$2F_x$	2	2	2	2	2	6	8	8	2	4	4	6	8	2	4	2
30_x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31_x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32_x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33_x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34_x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35_x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36_x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37_x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38_x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39_x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
$3A_x$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
$3B_x$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
$3C_x$	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
$3D_x$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
$3E_x$	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

The Difference Distribution Table of S1 (cont.)

Observe that:

- In the first row $X' = 0$ and thus all the 64 pairs satisfy $Y' = 0$. $Y' \neq 0$ is impossible.
- In the remaining rows: The average value is 4, the sum in each line is 64. The values are all even in the range 0–16.

  The entries with value 16 mean that for a quarter of the pairs with this input difference X', the output difference is the particular Y'.

  The entries with value 0 mean that there are no pairs with the corresponding input difference X' and the corresponding output difference Y'.

Differences and the S Boxes (cont.)

Definition: If the entry of the input difference X' and the output difference Y' is greater than zero, we say that $\boldsymbol{X' \text{ may cause } Y' \text{ by the S-box}}$, and denote $\boldsymbol{X' \rightarrow Y'}$.

Definition: $\boldsymbol{\text{The probability of } X' \rightarrow Y'}$ is the probability that for a pair with the input difference X', the output difference is Y', among all the possible pairs. In DES, the probability is the corresponding value in the difference distribution table divided by 64.

Similarly we define $\boldsymbol{X' \rightarrow Y' \text{ by the } F\text{-function}}$, and define the probability as the product of the probabilities by the eight S-boxes.

Differences and the S Boxes (cont.)

Differential cryptanalysis uses the entries with large values, and in particular the $0 \rightarrow 0$ entry and the entries with value 16, and other large values.

Observation

Given an input and output differences of an S-box, it is possible to list all the pairs with these differences.
Example: For the entry $09_x \rightarrow 1_x$ the 2 pairs are:

1. 33_x, $3A_x$
2. $3A_x$, 33_x

For the entry $01_x \rightarrow F_x$ the 4 pairs are:

1. $1E_x$, $1F_x$
2. $1F_x$, $1E_x$
3. $2A_x$, $2B_x$
4. $2B_x$, $2A_x$

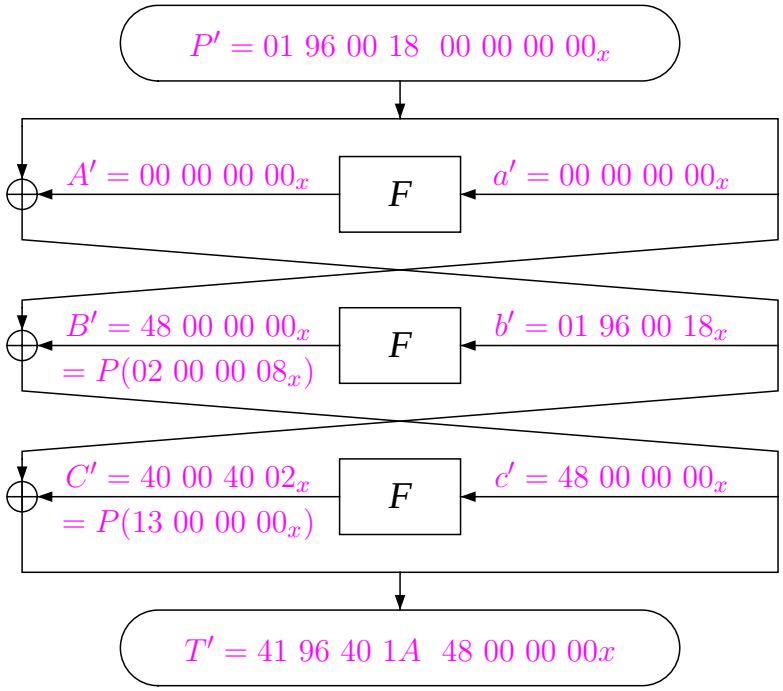
The lists of pairs of all the differences can easily be computed in advance.

Example of a Simple Attack

Assume a 3-round DES, in which for some pair of plaintexts
$P' = 01\ 96\ 00\ 18\ \ 00\ 00\ 00\ 00_x$, and $T' = 41\ 96\ 40\ 1A\ \ 48\ 00\ 00\ 00_x$.
We also assume that $T = 00\ 00\ 00\ 00\ \ 08\ 00\ 00\ 00_x$ and
$T^* = 41\ 96\ 40\ 1A\ \ 40\ 00\ 00\ 00_x$.
(We use the notation T for the ciphertexts, as we use C for the third round intermediate values.)

Example of a Simple Attack (cont.)

Then, the differences in the various rounds are



Example of a Simple Attack (cont.)

We identify that S1 in the third round accepts difference 09_x in the input and outputs difference 1_x in the output. Looking at the difference distribution table, we find only two possible pairs for this combination ((33_x, $3A_x$) and ($3A_x$, 33_x)).
Thus, we get the following equations:

$$S1_E \oplus S1_K = 33_x \text{ or } 3A_x$$
$$S1_E^* \oplus S1_K = 3A_x \text{ or } 33_x.$$

From the known ciphertexts we know that

$$S1_E = 01_x$$
$$S1_E^* = 08_x.$$

Therefore, we can find two possible values for $S1_K$

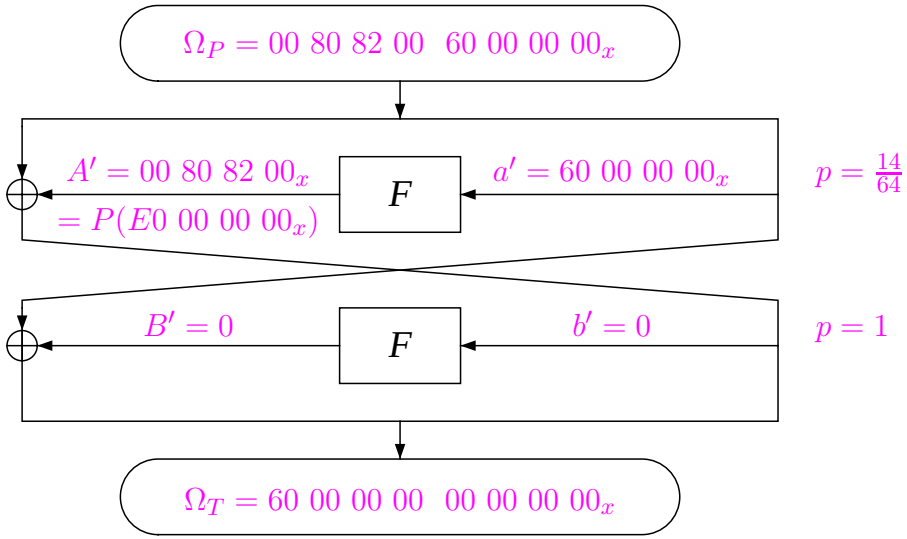
$$S1_K = 32_x \text{ or } 3B_x.$$

(Notice that the difference between these two values is always the input difference, 09_x in this case.)

Characteristics

In differential cryptanalysis we wish to know some statistical information on the differences in intermediate rounds during encryption, given only the plaintext difference.

Example: A **two-round characteristic** with probability $\frac{14}{64}$ (In S1, $0C_x \rightarrow E_x$ with probability $\frac{14}{64}$):



Characteristics (cont.)

Informal Definition: Associated with any pair of encryptions are the XOR value of its two plaintexts, the XOR of its ciphertexts, the XORs of the inputs of each round in the two executions and the XORs of the outputs of each round in the two executions. These XOR values form an ***n*-round characteristic**. A characteristic has a probability, which is the probability that a random pair with the chosen plaintext XOR has the round and ciphertext XORs specified in the characteristic. We denote the plaintext XOR of a characteristic by Ω_P and its ciphertext XOR by Ω_T.

Characteristics (cont.)

Let n be the block size of a Feistel cipher, then

Definition: An ***r*-round characteristic** is a tuple $\boldsymbol{\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)}$ where Ω_P and Ω_T are n-bit numbers and Ω_Λ is a list of r elements $\Omega_\Lambda = (\Lambda_1, \Lambda_2, \ldots, \Lambda_r)$, each is a pair of the form $\Lambda_i = (\lambda_I^i, \lambda_O^i)$ where λ_I^i and λ_O^i are $n/2$-bit long. A characteristic satisfies the following requirements:

$$\begin{aligned}
\lambda_I^1 &= \text{the right half of } \Omega_P \\
\lambda_I^2 &= \text{the left half of } \Omega_P \oplus \lambda_O^1 \\
\lambda_I^r &= \text{the right half of } \Omega_T \\
\lambda_I^{r-1} &= \text{the left half of } \Omega_T \oplus \lambda_O^r
\end{aligned}$$

and for every i such that $2 \le i \le r-1$:

$$\lambda_O^i = \lambda_I^{i-1} \oplus \lambda_I^{i+1}.$$

Characteristics (cont.)

Definition: **Characteristics can be concatenated** if $\text{swap}(\Omega_T^1) = \Omega_P^2$. The resultant characteristic is

$$\Omega = (\Omega_P^1, \Omega_\Lambda^1 || \Omega_\Lambda^2, \Omega_T^2).$$

Definition: A **right pair** with respect to a characteristic Ω and a key K is a pair P, P^*, which satisfies $P' = \Omega_P$, and all whose differences in the rounds $1, \ldots, r$ are as predicted by the characteristic.

Characteristics (cont.)

Definition: An **independent key** is a list of subkeys which is not necessarily derivable from some key via the key scheduling algorithm.

Probability of a Characteristic

Definition: The **probability** of a characteristic is the probability that a random pair P, P^* which satisfies $P' = \Omega_P$ is a right pair with respect to a random independent key.

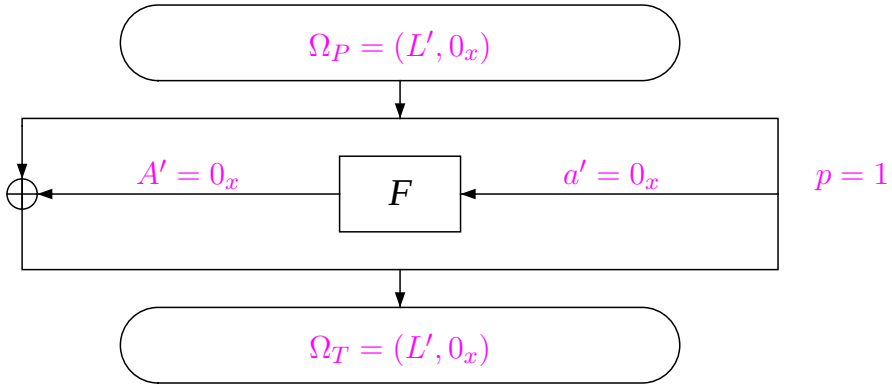
Note: The probability of a characteristic is the product of all the probabilities of the S-boxes in the characteristic.

Probability of a Characteristic (cont.)

Note: The probability of characteristics of DES is the probability that any specific pair P, P^* $(P' = \Omega_P)$ is a right pair among all random keys. We are more interested in the probability that for a specific (unknown) key, a random pair P, P^* $(P' = \Omega_P)$ is a right pair. In practice, the first probability is a good approximation of the second probability.
We shall return to this issue later on.

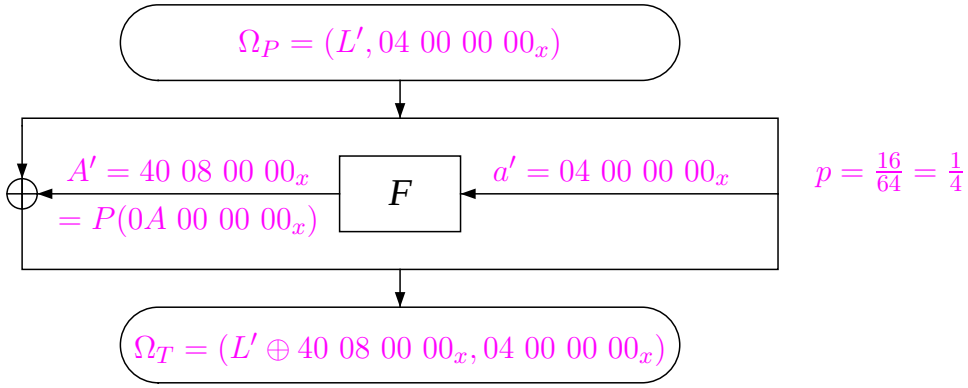
Examples of One-Round Characteristics

Choose the inputs of the S-boxes by the best entries in the difference distribution tables.
Example: An one-round characteristic with probability 1 is (for any L'):



Examples of One-Round Characteristics (cont.)

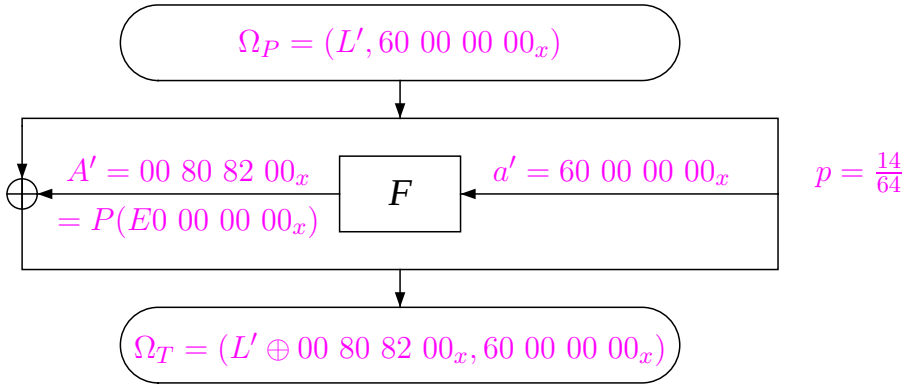
The second best one-round characteristic has probability 1/4, using only one active S-box (S2):



There is a similar characteristic using S6.

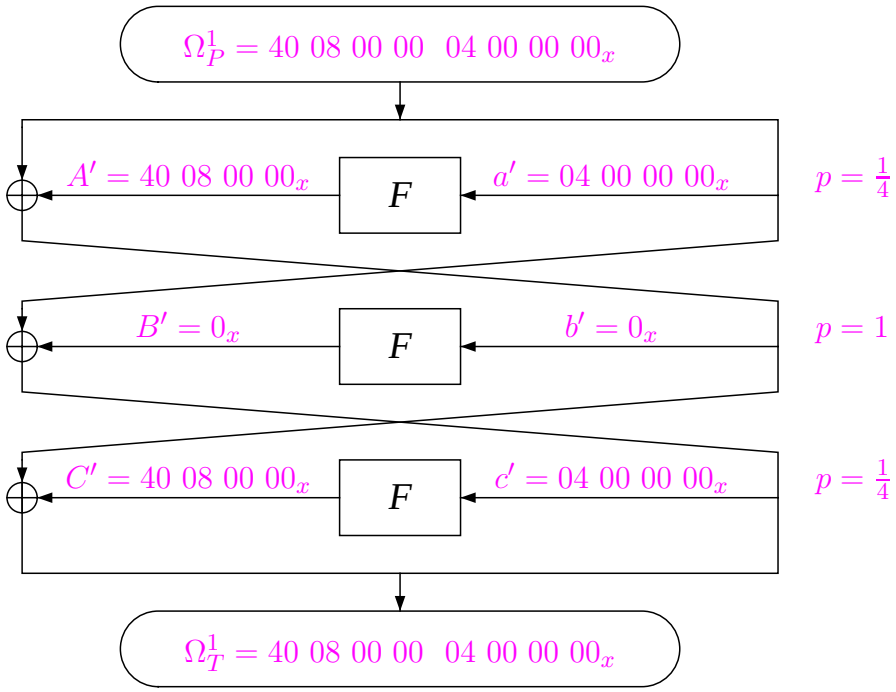
Examples of One-Round Characteristics (cont.)

The next best characteristic has probability $\frac{14}{64}$:



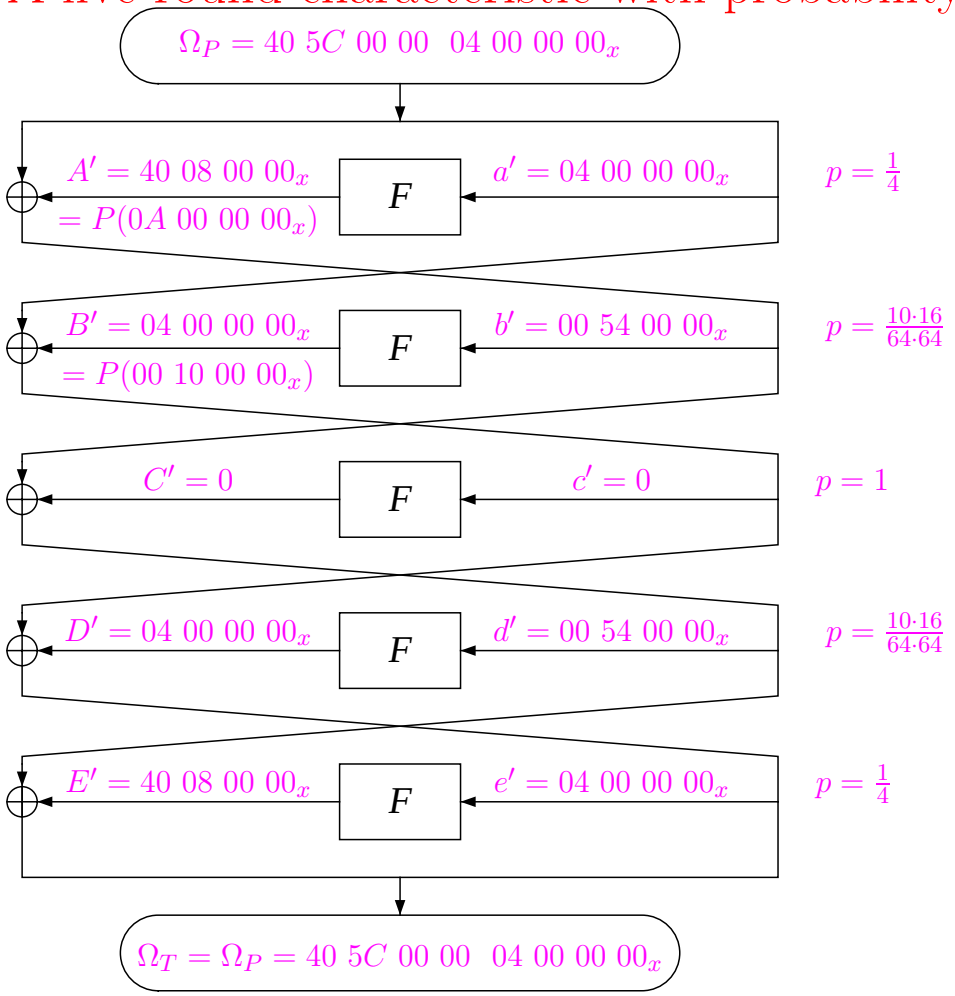
A Three-Round Characteristic

A three-round characteristic with probability 1/16:



A Five-Round Characteristic

A five-round characteristic with probability about 1/10486:



Differential Attacks

The simplest differential attack (0R-attack) breaks ciphers with the same number of rounds as the characteristic. Using 3-round characteristics we can find key bits of 3-round DES, and using 5-round characteristics we can find key bits of 5-round DES.

Differential Attacks (cont.)

Basic Algorithm:

1. Choose some $m = 2p^{-1}$ random pairs P, P^* such that $P' = \Omega_P$, and request the corresponding ciphertexts T and T^* under the unknown key K.

2. Choose only the pairs satisfying $T' = \Omega_T$, and discard the others. About $m(p + 2^{-64})$ pairs remain (from the m pairs): mp right pairs and $2^{-64}m$ wrong pairs. If $p \gg 2^{-64}$ we can assume that all the remaining pairs are right pairs.

Differential Attacks (cont.)

3. Each remaining right pair satisfies the difference predictions of the characteristics and its values of T and T^* are known. The differences of the inputs and the outputs of the S-boxes of the last round are known from $T' = T \oplus T^*$ (and from the characteristic).

   If the input difference is non-zero, not all the inputs are possible, and only a minority of the inputs satisfy the input and output differences: in each pair only about 0–16 possible values for the 6 input bits of the S-box are possible. Each value suggests one value for the 6 corresponding key bits.

   The right value of the 6 key bits must be suggested by all the right pairs, while other values are suggested arbitrarily by only a few of the pairs. By cutting the sets of keys suggested by all the pairs, we receive two possible values for each 6 key bits; in total we receive $2^8 = 256$ possible values for 48 key bits (if all the eight S-boxes are active).

   If a wrong pair still remains, still the keys suggested by the largest number of pairs are likely to include the right key.

Success Rate Analysis

Why 2^{-64} of the remaining pairs are wrong?:
Because if the cipher is a random permutation, given any pair of ciphertexts, the probability that their difference is a given value is 2^{-64} (actually $1/2^{64}-1$) independent of the value.

What is the success rate?:
Let the number of active S-boxes in the last round be s. Each right pair suggests 2^s keys for sure (two options for each active S-box). Each active S-box has actually four possible solutions on average. Hence, each right pair suggests 4^s solutions. Moreover, $m \cdot 2^{-64}$ pairs suggest completely random values in the active S-boxes (again 4^s values on average). But if $p \gg 2^{-64}$, we can easily disregard this option.

Success Rate Analysis (cont.)

The model:

There 64^s possible keys. But, they are actually sorted into equivalence classes, of which 32^s exist. Each right pair suggests the right equivalence class and about $2^s - 1 \approx 2^s$ wrong equivalence classes. So the right class is expected to get suggested mp times, and a wrong class is expected to be suggested $mp \cdot 2^s/32^s = mp/16^s$ times.

The suggestions are modelled as a Poisson distribution, i.e., there is the right key, which is suggested $Poi(mp)$ times, and 32^s wrong classes, each suggested $Poi(mp/16^s)$ times. Let Y be the random variable counting how many times the right class is suggested. Let Y_i's be the random variable counting the number of times the i'th wrong key class is suggested. Then the attack succeeds when $\forall i : Y > Y_i$. And this probability is equal to

$$\sum_{j=1}^{m} \Pr[Y = j] \cdot \prod_{i=1}^{32^s} \Pr[Y_i < j] = \sum_{j=1}^{m} \Pr[Y = j] \cdot (\Pr[Y_i < j])^{32^s}$$

Enhancements: *R-Attacks

We observe that characteristics shorter than the cipher can be used. Attacks using characteristics shorter than the cipher by n rounds (in which the characteristic predicts the differences in the first $r - n$ rounds of the cipher) are called nR-attacks.

0R-attacks In 0R-attacks (as in the previous slides) we know that $T' = \Omega_T$, and thus it is easy to identify the right pairs. Then we use the information on the differences inside the characteristic. Still, we cannot identify between two possible values for each S-box.

1R-Attacks

In these attacks, the characteristic predicts the differences except in the last round, and Ω_T is the predicted difference before the last round. The input difference of the F-function of the last round is known both from the characteristic and the ciphertexts $(T')_R = (\Omega_T)_L$, and it can be used to discard wrong pairs. On the other hand, the difference of the output of the F-function can be calculated as $(T')_L \oplus (\Omega_T)_R$.

Thus, we can use shorter characteristics with higher probabilities, although the identification of the right pairs is somewhat worse.

2R-Attacks

Allow to use a characteristic shorter than the cipher by two rounds.
In these attack, the attacker knows

1. The differences of the input to the last F-function, and the inputs themselves.

2. The predicted differences of the input to the F-function in the second-last round (from the characteristic).

3. The differences of the outputs of the last two F-functions can be calculated from Ω_T and T'.

2R-Attacks (cont.)

Identification and discarding of wrong pairs

For each S-box in the last two rounds (a total of 16 S-boxes) we calculate the predicted input and output differences as above. If for some S-box, the input difference may not cause the output difference (value 0 in the difference distribution table) the pair cannot be a right pair.

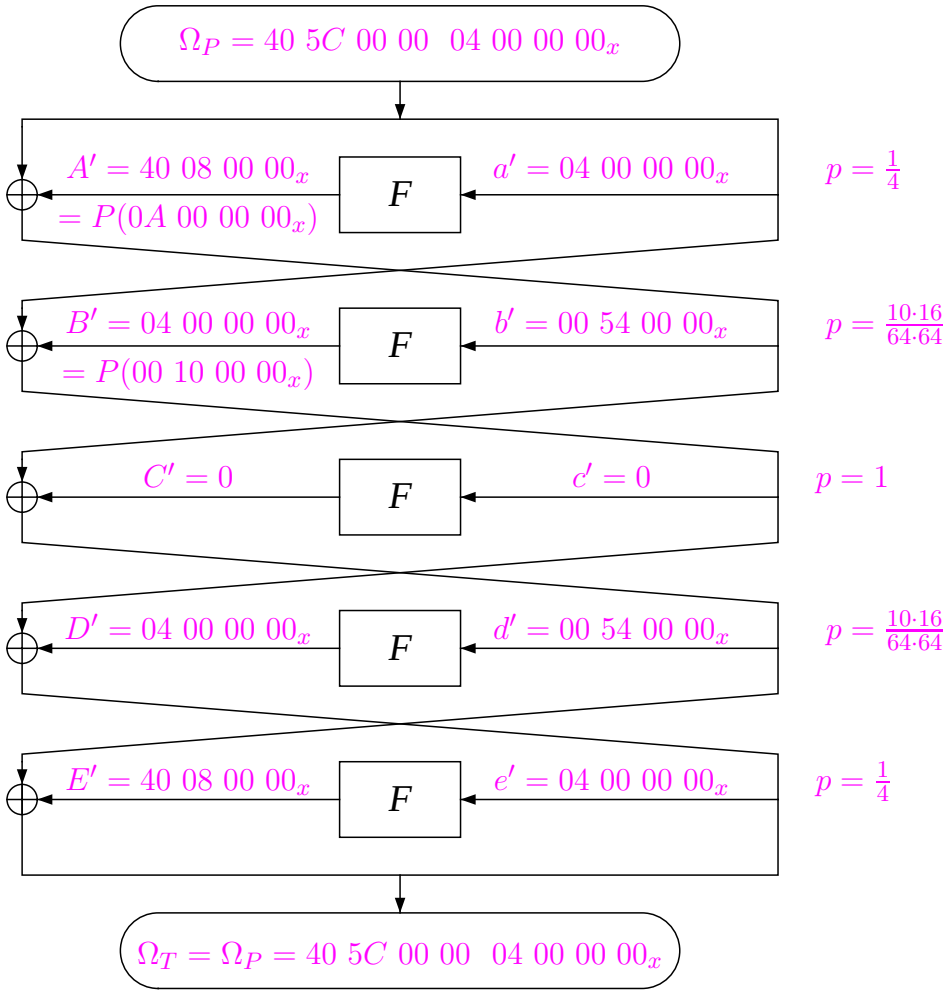
3R-Attacks / Attacking 8 Rounds

Allow to use a characteristic shorter than the cipher by three rounds.

Example: Breaking DES reduced to eight rounds using a 3R-attack:

Use the 5-round characteristic with probability about 1/10486:

3R-Attacks / Attacking 8 Rounds (cont.)



Attacking 8 Rounds: Brief Description

The attacker chooses pairs P, P^* satisfying $P' = \Omega_P$. With probability $p = 1/10486$ the difference after five rounds is Ω_T. In the sixth round $f' = (\Omega_T)_L = 40\ 5C\ 00\ 00_x$: S1:$08_x$, S2:$00_x$, S3:$0B_x$, S4:$38_x$, S5:$00_x$, S6:$00_x$, S7:$00_x$, S8:$00_x$. Thus, the output differences of S2, S5, S6, S7 and S8 are zero as well.

The output differences of S2, S5, S6, S7 and S8 in the last round can be calculated from Ω_T, T' and these zeroes. The inputs to the last round are known, and thus the inputs to the S boxes are known up to XOR with the last subkey K8.

Attacking 8 Rounds: Brief Description (cont.)

We can find several possible values for the key bits entering each of the five S-boxes in the last round, a total of 30 key bits. The right value of these 30 key bits is expected to appear as the most frequent value: it is suggested by all the right pairs (i.e., by about 1/10486 of the pairs). Any other value is suggested by about $\frac{4^5}{2^{30}} = 2^{-20} = \frac{1}{1048576}$ of the pairs.

The right value will be suggested 100 times more frequently than any other value, and thus is easily identified by counting the frequency of the suggested values.

About 100000 pairs (and even less) suffice for this attack.

Attacking 8 Rounds: Detailed Description

1. Choose 100000 pairs P, P^* satisfying $P' = \Omega_P$, and request their ciphertexts T, T^* under the unknown key K.

2. Initialize an array of 2^{30} entries with zeroes.

Attacking 8 Rounds: Detailed Description (cont.)

3. Compute the inputs and the input difference of the last F-function:

$$\begin{aligned} h &= T_R \\ h^* &= T_R^* \\ h' &= h \oplus h^* \end{aligned}$$

and 20 bits of the output difference

$$H' = (\Omega_T)_R \oplus F' \oplus T'_L$$

where 20 bits of F' are known to be zero, and the same 20 bits are calculated for H': the output of five S-boxes.

Attacking 8 Rounds: Detailed Description (cont.)

4. For each of the five S-boxes in the last round for which the inputs X, X^* as well as the output differences Y' are known, calculate all the possible values of their 6 key bits, which satisfy $S(X \oplus k) \oplus S(X^* \oplus k) = Y'$, and create a list of all the possible 30 bits of the key. For each 30-bit value, increment (by one) the corresponding entry in the array.

5. After all the pairs are processed, the highest entry should correspond to the right value of the 30 key bits.

6. Complete the remaining 26 key bits (by exhaustive search or by a differential attack).

A variant of this algorithm requires an array of only 2^{18} bytes, and it finds the key within a few seconds on a PC.

Analysis of the Success Rate

First of all, there are no equivalence classes for the keys. This follows the fact that even though each pair suggests subkeys which are still paired (i.e., comes in pairs), the fact that there are varying input differences to the eighth round, ensures that the relation between the keys for one pair, is very likely to not be maintained by a different pair.

As noted before, the right key is expected to be suggested about $m/10,000$ times. At the same time, a wrong subkey is expected to be suggested about $m/1,000,000$ times. So, using the previous notations, $Y \sim Poi(m/10,000)$, whereas $Y_i \sim Poi(m/1,000,000)$. Let $m = c \cdot 10,000$ (i.e., $Y \sim Poi(c)$), then the success rate is

$$P_s = \sum_{j=1} \Pr[Y = j] \cdot (\Pr[Y_i < j])^{2^{30}}.$$

Analysis of the Success Rate (cont.)

To compute this thing, we can use a slightly different method. We can set a threshold, and assume the only key to pass the threshold is the right one (this gives a lower bound for the success rate), i.e.,

$$P_s \geq \Pr[Y \geq th] \cdot (\Pr[Y_i < th])^{2^{30}}$$

for some threshold th.
For example, if $c = 10$, $Y \sim Poi(10), Y_i \sim Poi(0.1)$. Then, $\Pr[Y_i < th] \approx e^{-0.1} \cdot 0.1^{th}/(th)!$, and for $th = 7$, the probability that a wrong key is suggested more than 6 times is $e^{-0.1} \cdot 0.1^7/7! \approx 2^{-35.7}$. Hence, the probability that all the wrong subkeys are suggested up to 7 times is $(1-2^{-35.7})^{2^{30}} > (1-2^{-5.7}) = 98.1\%$. At the same time, the probability that the right key is suggested more than 6 times is about 87.0%. Hence, the total success rate of this attack is **at least** 85.3%.

Analysis of the Success Rate (cont.)

To increase the success rate, one can apply a more careful analysis, and take into consideration the subkey the pair suggests in the first round.
In this case, each pair suggests 4^6 values for 36 bits of the key. Repeating the analysis shows that $Y \sim Poi(c)$, while $Y_i \sim Poi(c/1600)$. Hence, for $c = 10$, the probability that $Y_i > 4$ is about $e(-1/160) \cdot (1/160)^5/120 \approx 2^{-43.5}$, so the probability that all wrong keys are not suggested more than 4 times is at least 99.5%. The right key is suggested more than 4 times with probability 97.1%.

Complexity Analysis

A simple approach for the implementation of the attack is to take each pair, and partially decrypt the last round, and see whether the output differences "work out".

This is of course not optimal, as the difference distribution table can tell us the exact input values, and thus, can tell us the value after the XOR with the key.

The complexity is therefore the time required to access the difference distribution table 5 or 6 times for each pair. This is about the same time required to actually compute the S-box, i.e., the analysis time of a pair is no more than 10% of the time needed for its encryption. Hence, starting with $m = 100,000$ pairs, the time complexity is about 200,000 encryptions.

Differentials

In nR-attacks, we usually use only the input and output differences (Ω_P and Ω_T) of the characteristics, but not the intermediate differences themselves.

Definition: A **Differential** is a set of all the characteristics with the same Ω_P and Ω_T.

The probability of the differential is the sum of the probabilities of the various characteristics.

In most differential attacks we actually use differentials, rather than characteristics. The probabilities of the characteristics serve as **lower bounds** for the probabilities of the differentials.

Probabilities Versus Number of Rounds

The probabilities of the characteristics reduces very fast with the number of rounds:

Number of rounds	Probability
1	1
2	1/4
3	1/16
4	$\approx 1/800$
5	$\approx 1/10000$
6	$\approx 1/1000000$

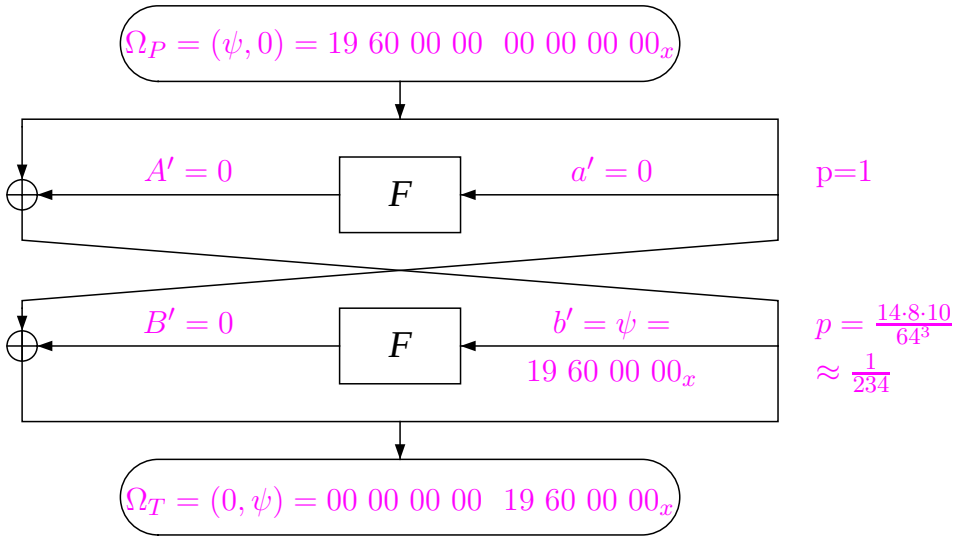
Probabilities Versus Number of Rounds (cont.)

As the number of rounds is increased, the reduction rate grows. By the table, we may expect that at 9–10 rounds, the probabilities are smaller than 2^{-56} or 2^{-64}.

We are interested in longer characteristics with higher probabilities.

Iterative Characteristics

Characteristics which can be concatenated to themselves are called **iterative characteristics**.
The best iterative characteristic of DES is:



where $\psi = 19\ 60\ 00\ 00_x$. Due to the importance of this iterative characteristic, we call it **the iterative characteristic**.
There is another value $\psi^\dagger = 1B\ 60\ 00\ 00_x$ for which the iterative characteristic has the same probability.

Iterative Characteristics (cont.)

These two characteristics are the best when iterated to seven or more rounds.

Note: In DES, in order to receive the same output of the F-function, two different inputs must differ in the input of at least three S-boxes.

Probabilities Versus Number of Rounds

The probability of the iterative characteristic versus the number of rounds:

Number of rounds	Probability
3	$2^{-7.9} \approx 1/234$
5	$2^{-15.7} \approx 1/55000$
7	$2^{-23.6}$
9	$2^{-31.5}$
11	$2^{-39.4}$
13	$2^{-47.2}$
15	$2^{-55.1}$
16	2^{-62}
17	2^{-63}

Are There Better Iterative Characteristics?

In order to find characteristics with high probabilities we would like to find out which input differences of F can cause zero output difference.
In particular we want to find out which input differences of S1 cause zero output difference:

- 0_x input difference to S1 causes 0_x output difference.
- Furthermore, S1 is designed in such a way that in order to receive 0_x output difference from a non zero input difference at least one of four bits must be non zero. Those four bits are the first two bits and the last two bits (bits $1, 2, 5$ and 6).

Are There Better Iterative Characteristics? (cont.)

- By the expansion E those exact bits are used for other S-boxes. The first 2 are used for S8 and the last 2 are used for S2. Thus, when seeking non zero input and zero output differences for S1 we must involve another S-box.

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
									⋮							
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
									⋮							
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
									⋮							
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
									⋮							

Are There Better Iterative Characteristics? (cont.)

Other S-boxes are designed by the same criteria, i.e.,

$$04_x \not\to 0_x$$
$$08_x \not\to 0_x$$
$$0C_x \not\to 0_x$$

Conclusion: In DES, in order to receive the same output of the F-function, two different inputs must differ in the input of at least **two** S-boxes.

Are There Better Iterative Characteristics? (cont.)

From the difference distribution table of S1 the possibilities for bits $1, 2, 5$ and 6 which can produce zero output difference are:

12	56	12	56
00	00	00	00
	01	10	
	11	00	01
01	01	01	
	11	10	
10	00	11	
	01	10	10
	10	11	
	11	00	11
11	01	01	
	10	10	
	11	11	

Are There Better Iterative Characteristics? (cont.)

From the difference distribution table of S2 the possibilities for bits $1, 2, 5$ and 6 which can produce zero output difference are:

12	56	12	56
00	00	00	00
	01	10	
	11	00	01
01	01	01	
	11	10	
10	00	10	10
	01	11	
	10	00	11
	11	01	
11	10	10	
	11	11	

Note: All S-boxes are designed similarly.

Are There Better Iterative Characteristics? (cont.)

We focus on the following possibilities:

$$\begin{array}{cc||cc} 00 & 01 & 10 & 00 \\ & 11 & & \end{array}$$

We can conclude from these possibilities that when the input difference of S_i is non zero then the only way not to influence S_{i+1} is to use 10 as the first two bits. Furthermore, we have to use 01 or 11 as the last two bits in order not to involve S_{i-1}.
On the other hand:

- If we use 10 as the first two bits then the input difference of S_{i-2} must be non zero.
- If we use 01 or 11 as the last two bits the input difference of S_{i+2} must be non zero.

Are There Better Iterative Characteristics? (cont.)

Conclusion: In DES, in order to receive the same output of the F-function, two different inputs must differ in the input of at least **three** S boxes.

Difficulty of Application to the Full DES

In order to attack the full DES (16-rounds) we need at least $\mathbf{2 \cdot 2^{62}}$ **pairs**:

1. Their encryption costs more than exhaustive search.
2. **Include all the $\mathbf{2^{64}}$ plaintext blocks** (who needs the key in this case?).
3. The identification of right pairs is not so good, since $p \not\gg 2^{-64}$

The Attack on the Full 16-Round DES

Motivation:

1. The 15-round characteristic has probability $2^{-55.1}$, and clearly cannot be used to reduce the complexity of attack below 2^{55}.

2. The 14-round characteristic has probability $2^{-54.1}$.

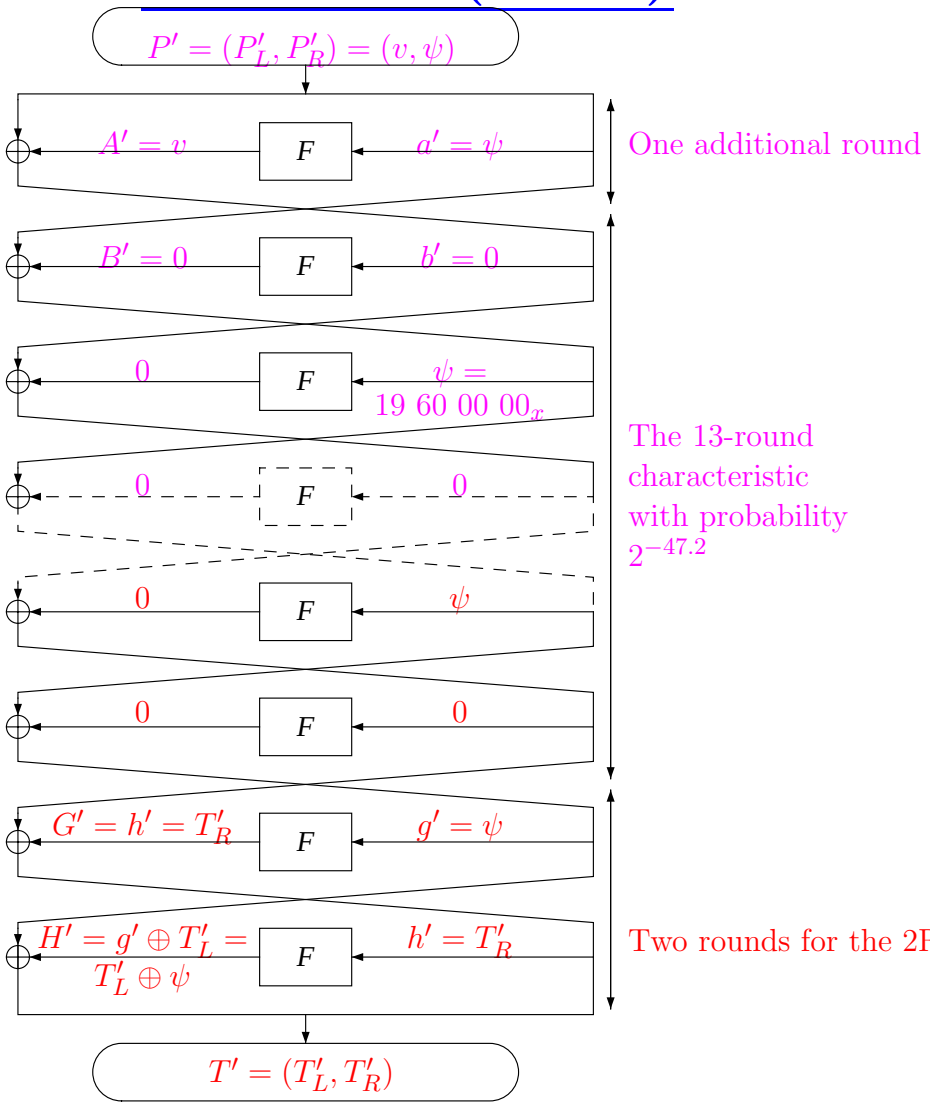
3. In order to attack DES, we must then use characteristics of at most 13 rounds.

4. However, 3R-attacks are infeasible, since due to lack of data the right key cannot be identified.

The Idea

Add an additional round as a **first** round, not included in the characteristic, and **without cost**.

The Idea (cont.)



The Data

1. Let $\{v_j\}$ be the set of 2^{12} possible output values of S1, S2 and S3, after the P permutation, where all the other 20 bits are zero (assume $v_0 = 0$).

2. Choose the plaintexts in structures of 2^{14}, using the two best iterative characteristics:

   (a) Choose (random) P_0.

   (b) $P_1 = P_0 \oplus (0, \psi^1)$, where $\Omega_P^1 = (\psi^1, 0)$.

   (c) $P_2 = P_0 \oplus (0, \psi^2)$, where $\Omega_P^2 = (\psi^2, 0)$.

   (d) $P_3 = P_0 \oplus (0, \psi^1 \oplus \psi^2)$.

   (e) For $0 \le i \le 3$, $0 < j < 2^{12}$: $P_{i+4j} = P_i \oplus (v_j, 0)$.

3. In this structure, for every P_i there is some **unknown** P_j whose difference (before round 2) is Ω_P^1. Similarly for Ω_P^2.

The Data (cont.)

4. Therefore, for each characteristic, there are 2^{13} pairs in the structure, and in total 2^{14} for both characteristics.

5. Right pairs: the 13-round characteristic probability is $2^{-47.2}$. In a structure there are on average $2^{14} \cdot 2^{-47.2} = 2^{-33.2}$ right pairs.

6. One right pair is expected to exist in $2^{33.2}$ structures on average, i.e., in about $2^{47.2}$ chosen plaintexts.

Identification of Wrong Pairs

$\Omega_T = (\psi, 0)$, thus the input of the F-function in the second-last round differs by ψ in the right pairs. ψ is non-zero only in the input to S1, S2 and S3. Thus, the 20-bit output difference of S4,S5,S6,S7,S8 is zero.

The input difference of the last round must be zero in these 20 bits.

This difference can be easily calculated for any pair, and can be used to discard most of the wrong pairs: A wrong pair passes the test with probability 2^{-20}, in total there are 2^{26} pairs in each structure, and thus only about 2^6 wrong pairs pass the test.

These remaining pairs can be found efficiently: Hash the 2^{14} plaintexts by the 20 bits of T_R, and process only those hashed to the same entry. It requires only about 2^{14} steps, instead of 2^{26}.

Identification of Wrong Pairs (cont.)

We now discard additional wrong pairs by examining the other S-boxes in the first, 15th and the 16th, and verifying that their computed input difference may cause their computed output difference. This test discards about $1 - \left(\frac{14}{16} \cdot \frac{13}{16} \cdot \frac{15}{16}\right)^2 \cdot 0.8^8 = 1 - 0.0745 = 92.55\%$ of the remaining wrong pairs. Only about $2^6 \cdot 0.0745 = 4.768$ wrong pairs from each structure remain after this test.

(Consult the book for the exact calculation).

Finding the Key Using One Right Pair

In previous differential attacks we counted the frequency of the keys, and thus needed several right pairs.
We observe that when we count by a large number of bits, it is more efficient to compute a trial encryption to verify key directly.
We first find 52-bit values corresponding to the 48 bits of the last subkey plus 4 bits accessible in rounds 1 and 15. For this, We now take into consideration that the subkeys are not independent.
Instead of counting on the 52 key bits, we complete the 52 bits to 56 bits (with all the possible values of the additional 4 bits), and compute a trial encryption on each of the 56-bit keys:

Finding the Key Using One Right Pair (cont.)

1. Given the $2^{47.2}$ ciphertexts, there is a right pair with a high probability (63%).

2. Discard wrong pairs by the algorithm in the previous slides.

3. For each remaining pair do:

4. Compute all the possible values of the 52 key bits: a total of 4^8 values on average for the last subkey for each pair, complete additional 4 bits using rounds 1 and 15, and discard contradicting values. Each analyzed pair proposes about $2^{52} \cdot \frac{2^{-32}}{0.8^8} \cdot \frac{2^{-12}}{\frac{14}{16}\cdot\frac{13}{16}\cdot\frac{15}{16}} \cdot \frac{2^{-12}}{\frac{14}{16}\cdot\frac{13}{16}\cdot\frac{15}{16}} = 0.84$ values for the 52 bits. Thus, each structure proposes $4.768 \cdot 0.84 = 4$ values on average.

5. Complete the 52 bits to 56 bits by adding all the possible 4-bit values.

Finding the Key Using One Right Pair (cont.)

6. Compute a trial encryption on each of the $4 \cdot 16 = 64$ 56-bit keys proposed by each structure.

7. A total of $2^{47.2}/2^{14} \cdot 64 = 2^{39.2}$ trial encryptions are applied (and it can be reduced further to 2^{37}).

8. During processing of the **first right pair**, the key **must** be found. Then, it can easily be verified with additional tests.

Conversion to a Known Plaintext Attack

Differential chosen plaintext attacks can be converted to known plaintext attacks with higher complexities:

1. Assume a chosen plaintext attack requires m pairs P, P^* with difference $P' = \Omega_P$.
2. Request $2^{32}\sqrt{2m}$ random known plaintexts.
3. There are $(2^{32}\sqrt{2m})^2/2$ pairs in these plaintexts, which are $2^{64}m$ pairs.
4. Each value of P' appears for about 2^{-64} of the pairs, i.e., for about m pairs.
5. In particular, there are about m pairs with the plaintext difference $P' = \Omega_P$. (These pairs can be identified efficiently using hash tables).
6. The original chosen plaintext attack is executed on these m pairs.

Conversion to a Known Plaintext Attack (cont.)

The number of required chosen plaintexts vs. the number of required known plaintexts:

m	$2^{32}\sqrt{2m}$
2	2^{33}
8	2^{34}
2^7	2^{36}
2^{15}	2^{40}
2^{31}	2^{48}
2^{55}	2^{60}

Independence Assumptions

As you might have noted, we used several randomness assumptions:

- That the probability of each round is independent of others.
- That wrong pairs which looks like right ones appear randomly.
- That wrong subkeys are distributed randomly.

Each of these assumptions is actually wrong.
The subkeys depend on each other, and thus there are relations between different rounds. If there is a differential characteristic with high probability, there are usually several characteristics with comparable probability. And the wrong subkeys are not really distributed randomly (for example, in our case, a right pair suggests the right key, s keys which are right up to one S-box, $s(s-1)/2$ keys which are right up to two S-boxes, etc.).
However, differential cryptanalysis works. When running experiments on DES, you will get roughly the same success rate as predicted. This is also true for most other ciphers.

Independent Subkeys — Where we Cheated

The assumption that the probability of a differential characteristic is the product of all the one-round characteristics that compose it assumes that all subkey are independent. Moreover, it assumes that the keys are chosen *during* the differential attack, and for each new pair of plaintexts, they are chosen again at random.

This is of course wrong, as the key is fixed **a priori**, and the only source of "randomness" in the experiment is the plaintext pair.

Hence, we need to assume *Stochastic Equivalence*, i.e.,

$$\Pr[\Omega_T = \beta | \Omega_P = \alpha] =$$

$$\Pr[\Omega_T = \beta | \Omega_P = \alpha \wedge K = (k_1, k_2, \ldots)]$$

for almost all keys K.

Markov Ciphers [LMM91]

A cipher is a Markov cipher if

$$\Pr[\Omega_T = \beta | \Omega_P = \alpha, P = \gamma]$$

is independent of γ when K is chosen at random.
Alternatively, a Markov cipher satisfies:

$$\forall \gamma : \Pr_K[\Omega_T = \beta | \Omega_P = \alpha, P = \gamma] = \Pr_K[\Omega_T = \beta | \Omega_P = \alpha]$$

In other words, the propagation of differences are independent of the values in each round. Hence, for an r-round Markov cipher:

$$\Pr[\Omega_P = \beta_0 \rightarrow \beta_r = \Omega_T] = \sum_{\beta_1} \sum_{\beta_2} \cdots \sum_{\beta_r} \prod_{i=1}^{r} \Pr[\beta_{i-1} \rightarrow \beta_i]$$

for all β_0 and β_r
Note that we cannot verify this assumption experimentally, but evidence of experiments done shows that most of the block ciphers, most of the time satisfy this model.

Markov Ciphers [LMM91] (cont.)

Known exceptions are ciphers where the value of the key affects the encryption process very strongly (e.g., IDEA) and cases where the probability of the differential characteristic is close to (or lower) than the random probability.

Results

Summary of the cryptanalysis of DES: The number of operations and plaintexts required to break the specified number of rounds.

No. of Rounds	Dependent Key		Independent Key	
	Chosen Plaintexts	Known Plaintexts	Chosen Plaintexts	Known Plaintexts
4	2^3	2^{33}	2^4	2^{33}
6	2^8	2^{36}	2^8	2^{36}
8	2^{14}	2^{38}	2^{16}	2^{40}
9	2^{24}	2^{44}	2^{26}	2^{45}
10	2^{24}	2^{43}	2^{35}	2^{49}
11	2^{31}	2^{47}	2^{36}	2^{50}
12	2^{31}	2^{47}	2^{43}	2^{53}
13	2^{39}	2^{52}	2^{44}	2^{54}
14	2^{39}	2^{51}	2^{51}	2^{57}
15	2^{47}	2^{56}	2^{52}	2^{58}
16	2^{47}	2^{55}	2^{60}	2^{61}

Results (cont.)

XOR-Differences in the Presence of Additions

Consider the operation $Z = X + Y$. If $X' = Y' = 0$, then necessarily $Z' = 0$.

But when $X' = 1_x, Y' = 0$, there are several possible XOR-differences of Z'. $X' = 1_x$ means that $X = X^* + 1$ or vice versa (we shall continue under the assumption that $X = X^* + 1$). Both are added with $Y = Y^*$, to obtain Z and Z^*, respectively.

If the least significant bit of $Y = Y^*$ is zero, then the difference in Z is going to be only in the least significant bit (i.e., $Z' = 1_x$).

When the least significant bit of $Y = Y^*$ is one, there is going to be carry in $X+Y$ but no carry in X^*+Y^*. This means, that the same process is repeated (i.e., if the second least significant bit of $Y = Y^*$ is 0, the *carry chain* ends here, otherwise, there is difference in the carry).

XOR-Differences in the Presence of Additions (cont.)

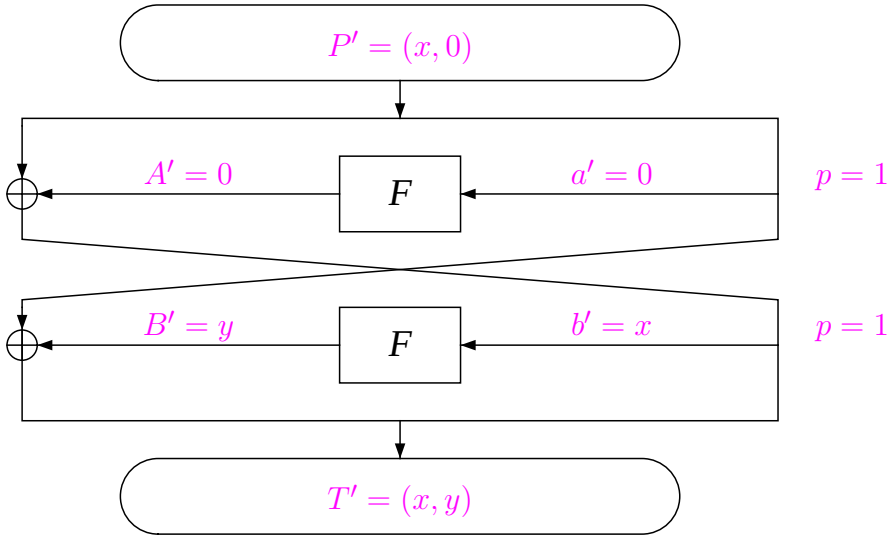
There is a special bit which causes a very short carry chain. A difference in the most significant bit, *does not* generate a carry chain, as the modular reduction cancels the difference. Hence, when we are dealing with the most significant bit there is no probability associated with it.

If X' has two active bits, the carry chain from the lower bit, can cancel the difference in the more higher order bit. The probability of each carry/no carry decision is 1/2 (where of course, after no-carry decision, there is no more carries).

If $Y' \neq 0$ as well, one can repeat the previous analysis. Each active bit (either in X' or in Y') may cause a carry (or not cause a carry) with probability 1/2.

Truncated Differentials

Truncated differential are an extension of differential cryptanalysis where the difference is not fully specified. For example, consider the following 2-round truncated differential:



Truncated Differentials (cont.)

Using truncated differentials in differential attacks is similar to the use of regular differentials. There are two small differences:

1. The probability that a wrong pair looks as if it is a correct one is $S \cdot 2^{-64}$, where S is the number of possible differences (in the example above, x and y can be any value, and thus, $S = 2^{64}$).

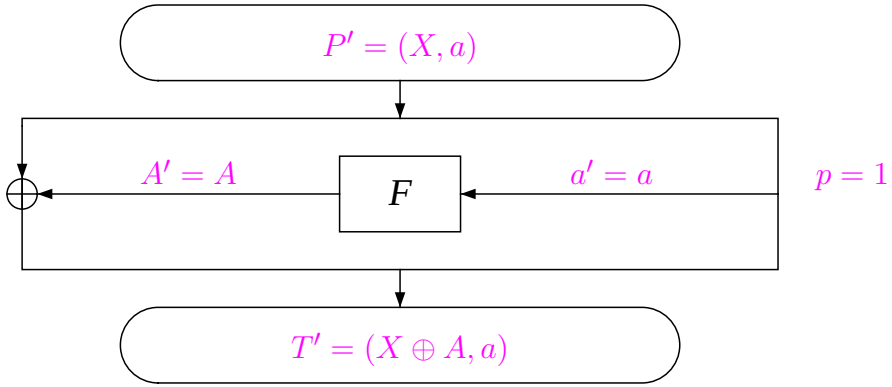
2. In differential cryptanalysis, the probability of the differential is independent of the direction (encryption/decryption). In the case of truncated differentials, this is not the case. For example, inverting the order of the rounds in the above example yields a truncated differential with probability 2^{-32}.

Some Caveats

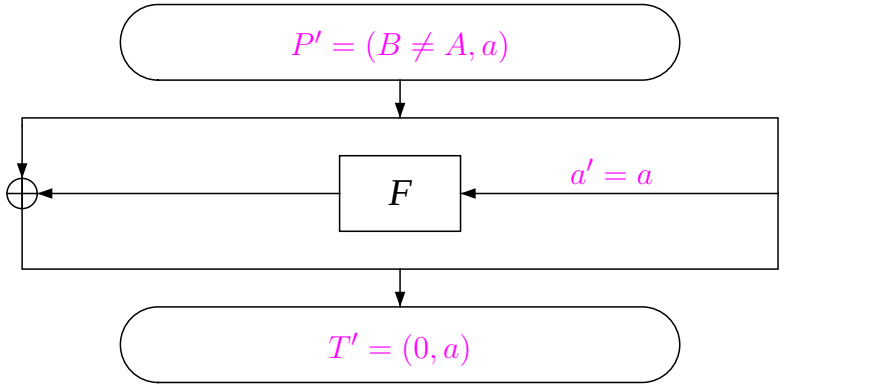
Usually truncated differentials are really useful to handle. The reason for that is that transitions of the form $a \rightarrow b$ can be approximated with the probability 2^{-w} (for $a \neq 0$, $|b| = w$), independent of a and b.
Of course, this is under the assumption that a may cause difference b. If the round function is bijective, and $a \neq 0$ then b cannot be 0.

Some Caveats (cont.)

Let us assume that for a specific a, A:

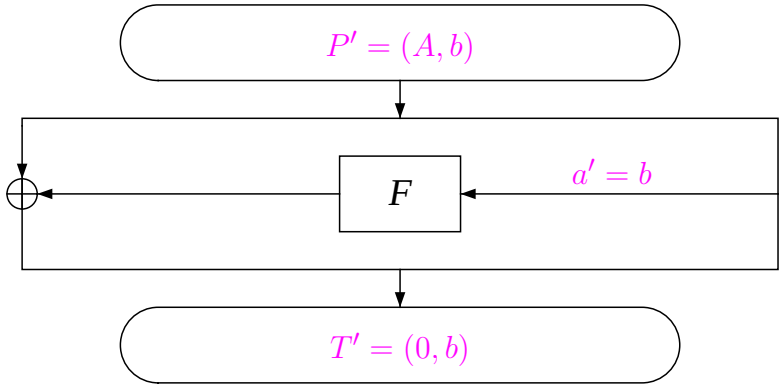


Then, the probability of following truncated differential is 0:



Some Caveats (cont.)

The following truncate differential may also have probability 0:



Extensions of Differential Cryptanalysis

1. Conditional characteristics (Ben-Aroya, Biham)
2. Higher-order differential cryptanalysis (Lai ; Biham)
3. Markov Ciphers (Lai, Massey)
4. Truncated Differentials (Knudsen)
5. Provable Security against Differential Attacks (Knudsen, Nyberg)
6. Impossible Differentials (1998, Biham, Biryukov, and Shamir).
7. Boomerang, amplified boomerang, and rectangle attacks (Wagner; Kelsey, Kohno, Schneier; Biham, Dunkelman, Keller)..

Appendix - The Difference Distribution Tables

The Difference Distribution Table of S1

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
10_x	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
11_x	6	8	2	4	6	4	8	6	4	0	6	6	0	4	0	0
12_x	0	8	4	2	6	6	4	6	6	4	2	6	6	0	4	0
13_x	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6
14_x	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0
15_x	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4
16_x	0	8	10	8	0	2	2	6	10	2	0	2	0	6	2	6
17_x	4	4	6	0	10	6	0	2	4	4	4	6	6	6	2	0
18_x	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2
19_x	2	6	2	4	0	8	4	6	10	4	0	4	2	8	4	0
$1A_x$	0	6	4	0	4	6	6	6	6	2	2	0	4	4	6	8
$1B_x$	4	4	2	4	10	6	6	4	6	2	2	4	2	2	4	2
$1C_x$	0	10	10	6	6	0	0	12	6	4	0	0	2	4	4	0
$1D_x$	4	2	4	0	8	0	0	2	10	0	2	6	6	6	14	0
$1E_x$	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2
$1F_x$	2	4	10	6	2	2	2	8	6	8	0	0	0	4	6	4

The Difference Distribution Table of S1 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	10	0	12	8	2	0	6	4	4	4	2	0	12
21_x	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8
22_x	10	4	6	2	2	8	2	2	2	2	6	0	4	0	4	10
23_x	0	4	4	8	0	2	6	0	6	6	2	10	2	4	0	10
24_x	12	0	0	2	2	2	2	0	14	14	2	0	2	6	2	4
25_x	6	4	4	12	4	4	4	10	2	2	2	0	4	2	2	2
26_x	0	0	4	10	10	10	2	4	0	4	6	4	4	4	2	0
27_x	10	4	2	0	2	4	2	0	4	8	0	4	8	8	4	4
28_x	12	2	2	8	2	6	12	0	0	2	6	0	4	0	6	2
29_x	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4
$2A_x$	4	2	4	6	0	2	8	2	2	14	2	6	2	6	2	2
$2B_x$	12	2	2	2	4	6	6	2	0	2	6	2	6	0	8	4
$2C_x$	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6
$2D_x$	6	2	6	2	8	4	4	4	2	4	6	0	8	2	0	6
$2E_x$	6	6	2	2	0	2	4	6	4	0	6	2	12	2	6	4
$2F_x$	2	2	2	2	2	6	8	8	2	4	4	6	8	2	4	2
30_x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31_x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32_x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33_x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34_x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35_x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36_x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37_x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38_x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39_x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
$3A_x$	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
$3B_x$	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
$3C_x$	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
$3D_x$	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
$3E_x$	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
$3F_x$	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

The Difference Distribution Table of S2

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	2	6	4	0	14	8	6	8	4	6	2
2_x	0	0	0	2	0	4	6	4	0	0	4	6	10	10	12	6
3_x	4	8	4	8	4	6	4	2	4	2	2	4	6	2	0	4
4_x	0	0	0	0	0	6	0	14	0	6	10	4	10	6	4	4
5_x	2	0	4	8	2	4	6	6	2	0	8	4	2	4	10	2
6_x	0	12	6	4	6	4	6	2	2	10	2	8	2	0	0	0
7_x	4	6	6	4	2	4	4	2	6	4	2	4	4	6	0	6
8_x	0	0	0	4	0	4	0	8	0	10	16	6	6	0	6	4
9_x	14	2	4	10	2	8	2	6	2	4	0	0	2	2	2	4
A_x	0	6	6	2	10	4	10	2	6	2	2	4	2	2	4	2
B_x	6	2	2	0	2	4	6	2	10	2	0	6	6	4	4	8
C_x	0	0	0	4	0	14	0	10	0	6	2	4	4	8	6	6
D_x	6	2	6	2	10	2	0	4	0	10	4	2	8	2	2	4
E_x	0	6	12	8	0	4	2	0	8	2	4	4	6	2	0	6
F_x	0	8	2	0	6	6	8	2	4	4	4	6	8	0	4	2
10_x	0	0	0	8	0	4	10	2	0	2	8	10	0	10	6	4
11_x	6	6	4	6	4	0	6	4	8	2	10	2	2	4	0	0
12_x	0	6	2	6	2	4	12	4	6	4	0	4	4	6	2	2
13_x	4	0	4	0	8	6	6	0	0	2	0	6	4	8	2	14
14_x	0	6	6	4	10	0	2	12	6	2	2	2	4	4	2	2
15_x	6	8	2	0	8	2	0	2	2	2	2	2	2	14	10	2
16_x	0	8	6	4	2	2	4	2	6	4	6	2	6	0	6	6
17_x	6	4	8	6	4	4	0	4	6	2	4	4	4	2	4	2
18_x	0	6	4	6	10	4	0	2	4	8	0	0	4	8	2	6
19_x	2	4	6	4	4	2	4	2	6	4	6	8	0	6	4	2
$1A_x$	0	6	8	4	2	4	2	2	8	2	2	6	2	4	4	8
$1B_x$	0	6	4	4	0	12	6	4	2	2	2	4	4	2	10	2
$1C_x$	0	4	6	6	12	0	4	0	10	2	6	2	0	0	10	2
$1D_x$	0	6	2	2	6	0	4	16	4	4	2	0	0	4	6	8
$1E_x$	0	4	8	2	10	6	6	0	8	4	0	2	4	4	0	6
$1F_x$	4	2	6	6	2	2	2	4	8	6	10	6	4	0	0	2

The Difference Distribution Table of S2 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	2	0	12	10	4	0	0	0	2	14	2	8	10
21_x	0	4	6	8	2	10	4	2	2	6	4	2	6	2	0	6
22_x	4	12	8	4	2	2	0	0	2	8	8	6	0	6	0	2
23_x	8	2	0	2	8	4	2	6	4	8	2	2	6	4	2	4
24_x	10	4	0	0	0	4	0	2	6	8	6	10	8	0	2	4
25_x	6	0	12	2	8	6	10	0	0	8	2	6	0	0	2	2
26_x	2	2	4	4	2	2	10	14	2	0	4	2	2	4	6	4
27_x	6	0	0	2	6	4	2	4	4	4	8	4	8	0	6	6
28_x	8	0	8	2	4	12	2	0	2	6	2	0	6	2	0	10
29_x	0	2	4	10	2	8	6	4	0	10	0	2	10	0	2	4
$2A_x$	4	0	4	8	6	2	4	4	6	6	2	6	2	2	4	4
$2B_x$	2	2	6	4	0	2	2	6	2	8	8	4	4	4	8	2
$2C_x$	10	6	8	6	0	6	4	4	4	2	4	4	0	0	2	4
$2D_x$	2	2	2	4	0	0	0	2	8	4	4	6	10	2	14	4
$2E_x$	2	4	0	2	10	4	2	0	2	2	6	2	8	8	10	2
$2F_x$	12	4	6	8	2	6	2	8	0	4	0	2	0	8	2	0
30_x	0	4	0	2	4	4	8	6	10	6	2	12	0	0	0	6
31_x	0	10	2	0	6	2	10	2	6	0	2	0	6	6	4	8
32_x	8	4	6	0	6	4	4	8	4	6	8	0	2	2	2	0
33_x	2	2	6	10	2	0	0	6	4	4	12	8	4	2	2	0
34_x	0	12	6	4	6	0	4	4	4	0	4	6	4	2	4	4
35_x	0	12	4	6	2	4	4	0	10	0	0	8	0	8	0	6
36_x	8	2	4	0	4	0	4	2	0	8	4	2	6	16	2	2
37_x	6	2	2	2	6	6	4	8	2	2	6	2	2	2	4	8
38_x	0	8	8	10	6	2	2	0	4	0	4	2	4	0	4	10
39_x	0	2	0	0	8	0	10	4	10	0	8	4	4	4	4	6
$3A_x$	4	0	2	8	4	2	2	2	4	8	2	0	4	10	10	2
$3B_x$	16	4	4	2	8	2	2	6	4	4	4	2	0	2	2	2
$3C_x$	0	2	6	2	8	4	6	0	10	2	2	4	4	10	4	0
$3D_x$	0	16	10	2	4	2	4	2	8	0	0	8	0	6	2	0
$3E_x$	4	4	0	10	2	4	2	14	4	2	6	6	0	0	6	0
$3F_x$	4	0	0	2	0	8	2	4	0	2	4	4	4	14	10	6

The Difference Distribution Table of S3

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	4	2	12	0	14	0	4	8	2	6	10
2_x	0	0	0	2	0	2	0	8	0	4	12	10	4	6	8	8
3_x	8	6	10	4	8	6	0	6	4	4	0	0	0	4	2	2
4_x	0	0	0	4	0	2	4	2	0	12	8	4	6	8	10	4
5_x	6	2	4	8	6	10	6	2	2	8	2	0	2	0	4	2
6_x	0	10	6	6	10	0	4	12	2	4	0	0	6	4	0	0
7_x	2	0	0	4	4	4	4	2	10	4	4	8	4	4	4	6
8_x	0	0	0	10	0	4	4	6	0	6	6	6	6	0	8	8
9_x	10	2	0	2	10	4	6	2	0	6	0	4	6	2	4	6
A_x	0	10	6	0	14	6	4	0	4	6	6	0	4	0	2	2
B_x	2	6	2	10	2	2	4	0	4	2	6	0	2	8	14	0
C_x	0	0	0	8	0	12	12	4	0	8	0	4	2	10	2	2
D_x	8	2	8	0	0	4	2	0	2	8	14	2	6	2	4	2
E_x	0	4	4	2	4	2	4	4	10	4	4	4	4	4	2	8
F_x	4	6	4	6	2	2	4	8	6	2	6	2	0	6	2	4
10_x	0	0	0	4	0	12	4	8	0	4	2	6	2	14	0	8
11_x	8	2	2	6	4	0	2	0	8	4	12	2	10	0	2	2
12_x	0	2	8	2	4	8	0	8	8	0	2	2	4	2	14	0
13_x	4	4	12	0	2	2	2	10	2	2	2	2	4	4	4	8
14_x	0	6	4	4	6	4	6	2	8	6	6	2	2	0	0	8
15_x	4	8	2	8	2	4	8	0	4	2	2	2	2	6	8	2
16_x	0	6	10	2	8	4	2	0	2	2	2	8	4	6	4	4
17_x	0	6	6	0	6	2	4	4	6	2	2	10	6	8	2	0
18_x	0	8	4	6	6	0	6	2	4	0	4	2	10	0	6	6
19_x	4	2	4	8	4	2	10	2	2	2	6	8	2	6	0	2
$1A_x$	0	8	6	4	4	0	6	4	4	8	0	10	2	2	2	4
$1B_x$	4	10	2	0	2	4	2	4	8	2	2	8	4	2	8	2
$1C_x$	0	6	8	8	4	2	8	0	12	0	10	0	4	0	2	0
$1D_x$	0	2	0	6	2	8	4	6	2	0	4	2	4	10	0	14
$1E_x$	0	4	8	2	4	6	0	4	10	0	2	6	4	8	4	2
$1F_x$	0	6	8	0	10	6	4	6	4	2	2	10	4	0	0	2

The Difference Distribution Table of S3 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	0	0	4	4	8	0	2	2	4	10	16	12	2
21_x	10	8	8	0	8	4	2	4	0	6	6	6	0	0	2	0
22_x	12	6	4	4	2	4	10	2	0	4	4	2	4	4	0	2
23_x	2	2	0	6	0	2	4	0	4	12	4	2	6	4	8	8
24_x	4	8	2	12	6	4	2	10	2	2	2	4	2	0	4	0
25_x	6	0	2	0	8	2	0	2	8	8	2	2	4	4	10	6
26_x	6	2	0	4	4	0	4	0	4	2	14	0	8	10	0	6
27_x	0	2	4	16	8	6	6	6	0	2	4	4	0	2	2	2
28_x	6	2	10	0	6	4	0	4	4	2	4	8	2	2	8	2
29_x	0	2	8	4	0	4	0	6	4	10	4	8	4	4	4	2
$2A_x$	2	6	0	4	2	4	4	6	4	8	4	4	4	2	4	6
$2B_x$	10	2	6	6	4	4	8	0	4	2	2	0	2	4	4	6
$2C_x$	10	4	6	2	4	2	2	2	4	10	4	4	0	2	6	2
$2D_x$	4	2	4	4	4	2	4	16	2	0	0	4	4	2	6	6
$2E_x$	4	0	2	10	0	6	10	4	2	6	6	2	2	0	2	8
$2F_x$	8	2	0	0	4	4	4	2	6	4	6	2	4	8	4	6
30_x	0	10	8	6	2	0	4	2	10	4	4	6	2	0	6	0
31_x	2	6	2	0	4	2	8	8	2	2	2	0	2	12	6	6
32_x	2	0	4	8	2	8	4	4	8	4	2	8	6	2	0	2
33_x	4	4	6	8	6	6	0	2	2	2	6	4	12	0	0	2
34_x	0	6	2	2	16	2	2	2	12	2	4	0	4	2	0	8
35_x	4	6	0	10	8	0	2	2	6	0	0	6	2	10	2	6
36_x	4	4	4	4	0	6	6	4	4	4	4	4	0	6	2	8
37_x	4	8	2	4	2	2	6	0	2	4	8	4	10	0	6	2
38_x	0	8	12	0	2	2	6	6	2	10	2	2	0	8	0	4
39_x	2	6	4	0	6	4	6	4	8	0	4	4	2	4	8	2
$3A_x$	6	0	2	2	4	6	4	4	4	2	2	6	12	2	6	2
$3B_x$	2	2	6	0	0	10	4	8	4	2	4	8	4	4	0	6
$3C_x$	0	2	4	2	12	2	0	6	2	0	2	8	4	6	4	10
$3D_x$	4	6	8	6	2	2	2	2	10	2	6	6	2	4	2	0
$3E_x$	8	6	4	4	2	10	2	0	2	2	4	2	4	2	10	2
$3F_x$	2	6	4	0	0	10	8	2	2	8	6	4	6	2	0	4

The Difference Distribution Table of S4

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	0	0	16	16	0	0	16	16	0	0	0	0	0
2_x	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
3_x	8	6	2	0	2	4	8	2	6	0	4	6	0	6	2	8
4_x	0	0	0	8	0	0	12	4	0	12	0	4	8	4	4	8
5_x	4	2	2	8	2	12	0	2	2	0	12	2	8	2	2	4
6_x	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
7_x	4	2	6	4	6	0	16	6	2	0	0	2	4	2	6	4
8_x	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
9_x	8	4	4	4	4	0	8	4	4	0	0	4	4	4	4	8
A_x	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
B_x	0	12	0	8	0	0	0	0	12	0	0	12	8	12	0	0
C_x	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
D_x	8	4	4	4	4	0	0	4	4	8	0	4	4	4	4	8
E_x	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
F_x	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
10_x	0	0	0	0	0	8	12	4	0	12	8	4	0	4	4	8
11_x	4	2	2	16	2	4	0	2	2	0	4	2	16	2	2	4
12_x	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
13_x	8	2	6	0	6	4	0	6	2	8	4	2	0	2	6	8
14_x	0	8	8	0	8	0	8	0	8	8	0	0	0	0	0	16
15_x	8	4	4	0	4	8	0	4	4	0	8	4	0	4	4	8
16_x	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
17_x	4	6	2	4	2	0	0	2	6	16	0	6	4	6	2	4
18_x	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
19_x	4	4	4	0	4	4	16	4	4	0	4	4	0	4	4	4
$1A_x$	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
$1B_x$	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
$1C_x$	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
$1D_x$	4	4	4	0	4	4	0	4	4	16	4	4	0	4	4	4
$1E_x$	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
$1F_x$	0	0	12	8	12	0	0	12	0	0	0	0	8	0	12	0

The Difference Distribution Table of S4 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	8	0	0	0	12	0	0	0	12	8	12	12	0
21_x	0	4	8	0	8	4	8	8	4	0	4	4	0	4	8	0
22_x	8	2	2	0	2	4	8	6	2	8	4	6	0	6	6	0
23_x	4	6	2	8	2	4	0	2	6	0	4	6	8	6	2	4
24_x	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
25_x	0	8	4	4	4	0	0	4	8	8	0	8	4	8	4	0
26_x	0	6	6	0	6	4	8	2	6	8	4	2	0	2	2	8
27_x	4	6	2	8	2	4	0	2	6	0	4	6	8	6	2	4
28_x	16	4	4	0	4	4	4	4	4	4	4	4	0	4	4	0
29_x	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
$2A_x$	0	2	2	16	2	4	4	2	2	4	4	2	16	2	2	0
$2B_x$	8	0	4	0	4	8	16	4	0	0	8	0	0	0	4	8
$2C_x$	8	4	4	4	4	0	8	4	4	8	0	4	4	4	4	0
$2D_x$	4	2	6	4	6	8	0	6	2	0	8	2	4	2	6	4
$2E_x$	16	0	0	0	0	16	0	0	0	0	16	0	0	0	0	16
$2F_x$	16	0	0	0	0	0	16	0	0	16	0	0	0	0	0	16
30_x	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
31_x	0	8	4	4	4	0	0	4	8	8	0	8	4	8	4	0
32_x	16	6	6	4	6	0	4	2	6	4	0	2	4	2	2	0
33_x	0	2	6	4	6	8	8	6	2	0	8	2	4	2	6	0
34_x	0	12	12	8	12	0	0	0	12	0	0	0	8	0	0	0
35_x	0	4	8	0	8	4	8	8	4	0	4	4	0	4	8	0
36_x	0	2	2	4	2	0	4	6	2	4	0	6	4	6	6	16
37_x	0	2	6	4	6	8	8	6	2	0	8	2	4	2	6	0
38_x	0	4	4	0	4	4	4	4	4	4	4	4	0	4	4	16
39_x	0	6	2	8	2	4	0	2	6	8	4	6	8	6	2	0
$3A_x$	0	4	4	0	4	8	8	4	4	8	8	4	0	4	4	0
$3B_x$	16	4	4	0	4	0	0	4	4	0	0	4	0	4	4	16
$3C_x$	0	4	4	4	4	0	8	4	4	8	0	4	4	4	4	8
$3D_x$	4	2	6	4	6	8	0	6	2	0	8	2	4	2	6	4
$3E_x$	0	2	2	8	2	12	4	2	2	4	12	2	8	2	2	0
$3F_x$	8	4	0	8	0	0	0	0	4	16	0	4	8	4	0	8

The Difference Distribution Table of S5

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	10	8	6	0	4	2	2	12	10	2	4
2_x	0	0	0	4	0	10	6	4	0	6	4	2	4	8	10	6
3_x	8	2	4	6	4	4	2	2	6	8	6	4	4	0	2	2
4_x	0	0	0	8	0	4	10	6	0	6	6	4	8	6	0	6
5_x	12	2	0	4	0	4	8	2	4	0	16	2	0	2	0	8
6_x	0	8	4	6	4	6	2	2	4	4	6	0	6	0	2	10
7_x	2	0	4	8	4	2	6	6	2	8	6	2	2	0	6	6
8_x	0	0	0	2	0	8	10	4	0	4	10	4	8	4	4	6
9_x	8	6	0	4	0	6	6	2	2	10	2	8	6	2	0	2
A_x	0	6	8	6	0	8	0	0	8	10	4	2	8	0	0	4
B_x	4	2	2	4	8	10	6	4	2	6	2	2	6	2	2	2
C_x	0	0	0	10	0	2	10	2	0	6	10	6	6	6	2	4
D_x	10	4	2	2	0	6	16	0	0	2	10	2	2	4	0	4
E_x	0	6	4	8	4	6	10	2	4	4	4	2	4	0	2	4
F_x	4	4	0	8	0	2	0	2	8	2	4	2	8	4	4	12
10_x	0	0	0	0	0	4	4	12	0	2	8	10	4	6	12	2
11_x	6	6	10	10	4	0	2	6	2	4	0	6	2	4	2	0
12_x	0	2	4	2	10	4	0	10	8	6	0	6	0	6	6	0
13_x	0	0	6	2	8	0	0	4	4	6	2	8	2	8	10	4
14_x	0	12	2	6	4	0	4	4	8	4	4	4	6	2	4	0
15_x	4	8	0	2	8	0	2	4	2	2	4	2	4	8	8	6
16_x	0	6	10	2	14	0	2	2	4	4	0	6	0	4	6	4
17_x	0	6	8	4	8	4	0	2	8	4	0	2	2	8	6	2
18_x	0	10	8	0	6	4	0	4	4	4	6	4	4	4	0	6
19_x	0	4	6	2	4	4	2	6	4	2	2	4	12	2	10	0
$1A_x$	0	2	16	2	12	2	0	6	4	0	0	4	0	4	4	8
$1B_x$	2	8	12	0	0	2	2	6	8	4	0	6	0	0	8	6
$1C_x$	0	10	2	6	6	6	6	4	8	2	0	4	4	4	2	0
$1D_x$	4	6	2	0	8	2	4	6	6	0	8	6	2	4	2	4
$1E_x$	0	2	6	2	4	0	0	2	12	2	2	6	2	10	10	4
$1F_x$	0	6	8	4	8	8	0	6	6	2	0	6	0	6	2	2

The Difference Distribution Table of S5 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	8	0	8	2	6	0	4	4	4	6	6	8	8
21_x	0	0	0	6	6	2	6	4	6	10	14	4	0	0	4	2
22_x	14	4	0	10	0	2	12	2	2	2	10	2	0	0	2	2
23_x	2	0	0	4	2	2	10	4	0	8	8	2	6	8	0	8
24_x	6	2	8	4	4	4	6	2	2	6	6	2	6	2	2	2
25_x	6	0	0	8	2	8	2	6	6	4	2	2	4	2	6	6
26_x	12	0	0	4	0	4	4	4	0	8	4	0	12	8	0	4
27_x	12	2	0	2	0	12	2	2	4	4	8	4	8	2	2	0
28_x	2	8	4	6	2	4	6	0	6	6	4	0	2	2	2	10
29_x	6	4	6	8	8	4	6	2	0	0	2	2	10	0	2	4
$2A_x$	4	4	0	2	2	4	6	2	0	0	6	4	10	4	4	12
$2B_x$	4	6	2	6	0	0	12	2	0	4	12	2	6	4	0	4
$2C_x$	8	6	2	6	4	8	6	0	4	4	0	2	6	0	6	2
$2D_x$	4	4	0	4	0	6	4	2	4	12	0	4	4	6	4	6
$2E_x$	6	0	2	4	0	6	6	4	2	10	6	10	6	2	0	0
$2F_x$	10	4	0	2	2	6	10	2	0	2	2	4	6	2	2	10
30_x	0	4	8	4	6	4	0	6	10	4	2	4	2	6	4	0
31_x	0	6	6	4	10	2	0	0	4	4	0	0	4	6	12	6
32_x	4	6	0	2	6	4	6	0	6	0	4	6	4	10	6	0
33_x	8	10	0	14	8	0	0	8	2	0	2	4	0	4	4	0
34_x	0	4	4	2	14	4	0	8	6	8	2	2	0	4	6	0
35_x	0	4	16	0	8	4	0	4	4	4	0	8	0	4	4	4
36_x	4	4	4	6	2	2	2	12	2	4	4	8	2	4	4	0
37_x	4	2	2	2	4	2	0	8	2	2	2	12	6	2	8	6
38_x	0	4	8	4	12	0	0	8	10	2	0	0	0	4	2	10
39_x	0	8	12	0	2	2	2	2	12	4	0	8	0	4	4	4
$3A_x$	0	14	4	0	4	6	0	0	6	2	10	8	0	0	4	6
$3B_x$	0	2	2	2	4	4	8	6	8	2	2	2	6	14	2	0
$3C_x$	0	0	10	2	6	0	0	2	6	2	2	10	2	4	10	8
$3D_x$	0	6	12	2	4	8	0	8	8	2	2	0	2	2	4	4
$3E_x$	4	4	10	0	2	4	8	8	2	2	0	2	6	8	4	0
$3F_x$	8	6	6	0	4	2	2	4	4	2	8	6	2	4	6	0

The Difference Distribution Table of S6

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	6	2	0	4	2	4	6	16	14	2
2_x	0	0	0	2	0	10	6	10	0	2	4	8	6	6	8	2
3_x	0	8	0	8	0	6	4	6	4	4	4	12	2	4	2	0
4_x	0	0	0	8	0	0	8	0	0	6	8	10	2	4	10	8
5_x	10	2	4	4	4	8	8	4	2	2	0	4	0	8	0	4
6_x	0	8	4	4	8	4	2	2	12	0	2	6	6	2	2	2
7_x	6	6	4	0	2	10	2	2	2	2	6	6	8	0	6	2
8_x	0	0	0	6	0	2	16	4	0	2	6	2	4	12	6	4
9_x	10	4	2	6	0	2	6	2	4	0	8	6	4	4	2	4
A_x	0	14	4	4	0	2	2	2	10	4	4	4	6	4	2	2
B_x	4	6	2	0	2	2	12	8	2	2	2	6	8	2	0	6
C_x	0	0	0	12	0	10	4	6	0	8	4	4	2	12	2	0
D_x	12	0	2	10	6	4	4	2	4	2	6	0	2	6	0	4
E_x	0	6	4	0	4	4	10	8	6	2	4	6	2	0	6	2
F_x	2	2	2	2	6	2	6	2	10	4	8	2	6	4	4	2
10_x	0	0	0	8	0	8	0	12	0	4	2	6	8	4	6	6
11_x	6	2	6	4	6	2	6	4	6	6	4	2	4	0	6	0
12_x	0	8	4	2	0	4	2	0	4	10	6	2	8	6	4	4
13_x	6	6	12	0	12	2	0	6	6	2	0	4	0	2	4	2
14_x	0	4	6	2	8	6	0	2	6	10	4	0	2	4	6	4
15_x	2	2	6	6	4	4	2	6	2	6	8	4	4	0	4	4
16_x	0	4	14	6	8	4	2	6	2	0	2	0	4	2	0	10
17_x	2	6	8	0	0	2	0	2	2	6	0	8	8	2	12	6
18_x	0	4	6	6	8	4	2	2	6	4	6	4	2	4	2	4
19_x	2	6	0	2	4	4	4	6	4	8	6	4	2	2	6	4
$1A_x$	0	6	6	0	8	2	4	6	4	2	4	6	2	0	4	10
$1B_x$	0	4	10	2	4	4	2	6	6	6	2	2	6	6	2	2
$1C_x$	0	0	8	2	12	2	6	2	8	6	6	2	4	0	4	2
$1D_x$	2	4	0	6	8	6	0	2	6	8	6	0	2	4	0	10
$1E_x$	0	10	8	2	8	2	0	2	6	4	2	4	6	4	2	4
$1F_x$	0	6	6	8	6	4	2	4	4	2	2	0	2	4	2	12

The Difference Distribution Table of S6 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	0	0	6	6	4	0	4	8	8	4	6	10	8
21_x	2	8	6	8	4	4	6	6	8	4	0	4	0	2	2	0
22_x	16	2	4	6	2	4	2	0	6	4	8	2	0	2	2	4
23_x	0	4	0	4	4	6	10	4	2	2	6	2	4	6	6	4
24_x	10	8	0	6	12	6	10	4	8	0	0	0	0	0	0	0
25_x	0	2	4	2	0	4	4	0	4	0	10	10	4	10	6	4
26_x	2	2	0	12	2	2	6	2	4	4	8	0	6	6	8	0
27_x	8	4	0	8	2	4	2	4	0	6	2	4	4	8	2	6
28_x	6	8	4	6	0	4	2	2	4	8	2	6	4	2	2	4
29_x	2	4	4	0	8	8	6	8	6	4	0	4	4	4	2	0
$2A_x$	6	0	0	6	6	4	6	8	2	4	0	2	2	4	6	8
$2B_x$	12	0	4	0	0	4	2	2	2	6	10	6	10	2	4	0
$2C_x$	4	2	6	0	0	6	8	6	4	2	2	8	4	6	4	2
$2D_x$	6	2	2	6	6	4	4	2	6	2	4	8	4	2	4	2
$2E_x$	4	6	2	4	2	4	4	2	4	2	4	6	4	10	4	2
$2F_x$	10	0	4	8	0	6	6	2	0	4	4	2	6	2	2	8
30_x	0	12	8	2	0	6	0	0	6	6	0	2	8	2	6	6
31_x	2	6	10	4	2	2	2	4	6	0	2	6	0	2	4	12
32_x	4	2	2	8	10	8	8	6	0	2	2	4	4	2	2	0
33_x	4	2	2	2	6	0	4	0	10	6	6	4	0	4	8	6
34_x	0	4	4	2	6	4	0	4	6	2	6	4	2	8	0	12
35_x	6	12	4	2	4	2	2	4	8	2	2	0	6	4	4	2
36_x	0	2	2	4	4	4	4	0	2	10	12	4	0	10	4	2
37_x	10	2	2	6	14	2	2	6	2	0	4	6	2	0	4	2
38_x	0	4	14	0	8	2	0	4	4	4	2	0	8	2	4	8
39_x	2	4	8	0	6	2	0	6	2	6	4	2	8	6	2	6
$3A_x$	8	4	0	4	6	2	0	4	6	8	6	0	6	0	4	6
$3B_x$	0	4	6	6	2	2	2	14	0	12	0	4	2	2	8	0
$3C_x$	0	6	16	0	2	2	2	8	4	2	0	12	6	2	2	0
$3D_x$	0	6	2	2	2	6	8	2	4	2	6	2	6	2	4	10
$3E_x$	4	2	2	4	4	0	6	10	4	2	4	6	6	2	6	2
$3F_x$	0	4	6	6	4	8	4	0	4	8	4	0	4	8	2	2

The Difference Distribution Table of S7

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	2	0	4	4	14	0	12	4	6	2	6	6	4
2_x	0	0	0	0	0	12	2	2	0	4	0	4	8	12	6	14
3_x	8	2	12	2	6	8	6	0	6	4	4	2	2	0	0	2
4_x	0	0	0	8	0	4	4	8	0	8	8	12	2	6	2	2
5_x	6	0	0	2	8	0	8	4	0	2	6	0	10	6	6	6
6_x	0	2	12	0	8	4	8	2	4	4	4	2	6	0	6	2
7_x	4	6	4	12	0	4	2	0	0	14	2	6	4	0	0	6
8_x	0	0	0	8	0	0	6	10	0	4	12	4	6	6	0	8
9_x	10	8	4	8	6	2	2	0	2	6	8	2	0	6	0	0
A_x	0	10	6	2	12	2	4	0	4	4	6	4	4	0	0	6
B_x	0	2	2	2	4	8	6	4	4	0	4	2	6	4	2	14
C_x	0	0	0	4	0	4	8	4	0	2	6	0	14	12	8	2
D_x	6	6	2	4	2	6	4	6	6	4	8	8	0	2	0	0
E_x	0	12	10	10	0	2	4	2	8	6	4	2	0	0	2	2
F_x	2	0	0	0	6	8	8	0	6	2	4	6	8	0	6	8
10_x	0	0	0	4	0	2	8	6	0	6	4	10	8	4	8	4
11_x	6	10	10	4	4	2	0	4	4	0	2	8	4	2	2	2
12_x	0	0	8	8	2	8	2	8	6	4	2	8	0	0	8	0
13_x	4	4	2	2	8	6	0	2	2	2	0	4	6	8	14	0
14_x	0	8	6	2	8	8	2	6	4	2	0	2	8	6	0	2
15_x	4	4	8	2	4	0	4	10	8	2	4	4	4	2	0	4
16_x	0	6	10	2	2	2	2	4	10	8	2	2	0	4	10	0
17_x	8	2	4	2	6	4	0	6	4	4	2	2	0	4	8	8
18_x	0	16	2	2	6	0	6	0	6	2	8	0	6	0	2	8
19_x	0	8	0	2	4	4	10	4	8	0	6	4	2	6	2	4
$1A_x$	0	2	4	8	12	4	0	6	4	4	0	2	0	6	4	8
$1B_x$	0	6	2	6	4	2	4	4	6	4	8	4	2	0	10	2
$1C_x$	0	8	4	4	2	6	6	6	6	4	6	8	0	2	0	2
$1D_x$	4	4	4	0	0	2	4	2	4	2	2	4	10	10	8	4
$1E_x$	0	0	2	2	12	6	2	0	12	2	2	4	2	6	8	4
$1F_x$	2	2	10	14	2	4	2	4	4	6	0	2	4	8	0	0

The Difference Distribution Table of S7 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	14	0	8	4	2	0	4	2	8	2	6	0	14
21_x	4	2	6	2	12	2	4	0	6	4	10	2	4	2	2	2
22_x	10	6	0	2	4	4	10	0	4	0	12	2	8	0	0	2
23_x	0	6	2	2	2	4	6	10	0	4	8	2	2	6	0	10
24_x	4	2	0	6	8	2	6	0	8	2	2	0	8	2	12	2
25_x	2	0	2	16	2	4	6	4	6	8	2	4	0	6	0	2
26_x	6	10	0	10	0	6	4	4	2	2	4	6	2	4	2	2
27_x	4	0	2	0	2	2	14	0	4	6	6	2	12	2	4	4
28_x	14	4	6	4	4	6	2	0	6	6	2	2	4	0	2	2
29_x	2	2	0	2	0	8	4	2	4	6	4	4	6	4	12	4
$2A_x$	2	4	0	0	0	2	8	12	0	8	2	4	8	4	4	6
$2B_x$	16	6	2	4	6	10	2	2	2	2	2	2	4	2	2	0
$2C_x$	2	6	6	8	2	2	0	6	0	8	4	2	2	6	8	2
$2D_x$	6	2	4	2	8	8	2	8	2	4	4	0	2	0	8	4
$2E_x$	2	4	8	0	2	2	2	4	0	2	8	4	14	6	0	6
$2F_x$	2	2	2	8	0	2	2	6	4	6	8	8	6	2	0	6
30_x	0	6	8	2	8	4	4	0	10	4	4	6	0	0	2	6
31_x	0	8	4	0	6	2	2	6	6	0	0	2	6	4	8	10
32_x	2	4	0	0	6	4	10	6	6	4	6	2	4	6	2	2
33_x	0	16	6	8	2	0	2	2	4	2	8	4	0	4	6	0
34_x	0	4	14	8	2	2	2	4	16	2	2	2	0	2	0	4
35_x	0	6	0	0	10	8	2	2	6	0	0	8	6	4	4	8
36_x	2	0	2	2	4	6	4	4	2	2	4	2	4	16	10	0
37_x	6	6	6	8	4	2	4	4	4	0	6	8	2	4	0	0
38_x	0	2	2	2	8	8	0	2	2	2	0	6	6	4	10	10
39_x	4	4	16	8	0	6	4	2	4	4	2	6	0	2	2	0
$3A_x$	16	6	4	0	2	0	2	6	0	4	8	10	0	0	4	2
$3B_x$	2	0	0	2	0	4	4	4	2	6	2	6	6	12	12	2
$3C_x$	0	0	8	0	12	8	2	6	6	4	0	2	2	4	6	4
$3D_x$	2	4	12	2	2	2	0	4	6	10	2	6	4	2	0	6
$3E_x$	4	6	6	6	2	0	4	8	2	10	4	6	0	4	2	0
$3F_x$	14	0	0	0	8	0	6	8	4	2	0	0	4	8	4	6

The Difference Distribution Table of S8

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	16	10	0	0	0	6	0	14	6	2	4
2_x	0	0	0	8	0	10	4	2	0	10	2	4	8	8	6	2
3_x	6	0	2	8	2	6	4	0	6	6	6	2	2	0	8	6
4_x	0	0	0	2	0	4	6	12	0	6	8	4	10	4	8	0
5_x	4	10	6	0	0	2	6	0	4	10	4	6	8	2	0	2
6_x	0	0	10	4	6	4	4	8	2	6	4	2	4	2	2	6
7_x	6	2	8	2	8	10	6	6	4	2	0	4	0	0	0	6
8_x	0	0	0	4	0	6	4	2	0	8	6	10	8	2	2	12
9_x	8	4	0	6	0	4	4	6	2	4	6	2	12	2	0	4
A_x	0	0	16	4	6	6	4	0	4	6	4	2	2	0	0	10
B_x	2	8	0	6	2	6	0	4	4	10	0	2	10	2	6	2
C_x	0	0	0	2	0	10	10	6	0	6	6	6	2	6	10	0
D_x	6	0	4	10	2	0	8	6	2	2	6	10	2	2	2	2
E_x	0	0	6	8	4	8	0	2	10	6	2	4	6	2	4	2
F_x	8	0	4	2	2	4	2	2	2	6	4	6	0	2	14	6
10_x	0	0	0	4	0	0	8	12	0	0	8	8	2	10	6	6
11_x	0	6	4	6	2	2	6	6	4	6	4	6	0	4	4	4
12_x	0	4	0	8	6	2	8	4	2	4	4	6	2	4	10	0
13_x	4	2	2	6	8	6	2	2	14	2	2	4	2	2	2	4
14_x	0	16	4	2	6	0	2	6	4	0	4	6	4	6	4	0
15_x	0	10	6	0	6	0	2	8	2	2	0	8	2	6	6	6
16_x	0	12	6	4	6	0	0	0	8	6	6	2	2	6	4	2
17_x	0	6	8	0	6	2	4	6	6	0	2	6	4	4	2	8
18_x	0	12	2	2	8	0	8	0	10	4	4	2	4	2	0	6
19_x	6	4	8	0	8	0	4	2	0	0	12	2	4	6	2	6
$1A_x$	0	4	6	2	8	8	0	4	8	0	0	0	6	2	0	16
$1B_x$	2	4	8	10	2	4	2	8	2	4	8	2	0	2	4	2
$1C_x$	0	12	6	4	6	4	2	2	6	0	4	4	2	10	2	0
$1D_x$	8	6	0	0	10	0	0	8	10	4	2	2	2	8	4	0
$1E_x$	0	4	8	6	8	2	4	4	10	2	2	4	2	0	6	2
$1F_x$	4	2	4	2	6	2	4	0	2	6	2	2	2	16	8	2

The Difference Distribution Table of S8 (cont.)

Input XOR	Output XOR															
	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
20_x	0	0	0	16	0	4	0	0	0	14	6	4	2	0	4	14
21_x	0	0	2	10	2	8	10	0	0	6	6	0	10	2	2	6
22_x	8	0	6	0	6	4	10	2	0	6	8	0	4	4	2	4
23_x	4	8	0	6	0	4	8	6	2	2	10	4	8	0	0	2
24_x	4	0	4	8	4	6	2	4	8	6	2	0	0	4	4	8
25_x	0	4	6	8	2	8	8	0	4	2	4	4	2	2	6	4
26_x	2	6	0	6	4	4	4	6	6	0	4	4	10	4	2	2
27_x	6	6	0	0	2	2	6	2	4	4	6	10	2	6	2	6
28_x	10	2	6	2	4	12	12	0	2	2	4	0	0	0	2	6
29_x	4	0	0	14	2	10	4	2	8	6	4	0	4	2	2	2
$2A_x$	8	8	0	2	0	2	4	0	2	6	8	14	2	8	0	0
$2B_x$	2	2	0	0	4	2	10	4	6	2	4	0	6	4	8	10
$2C_x$	2	6	6	2	4	6	2	0	2	6	4	0	6	4	10	4
$2D_x$	8	0	4	4	6	2	0	0	6	8	2	4	6	4	4	6
$2E_x$	6	2	2	4	2	2	6	12	4	0	4	2	8	8	0	2
$2F_x$	8	12	4	6	6	4	2	2	2	2	4	2	2	4	0	4
30_x	0	4	6	2	10	2	2	2	4	8	0	0	8	4	6	6
31_x	4	6	8	0	4	6	0	4	4	6	10	2	2	4	4	0
32_x	6	6	6	2	4	6	0	2	0	6	8	2	2	6	6	2
33_x	6	6	4	2	4	0	0	10	2	2	0	6	8	4	0	10
34_x	0	2	12	4	10	4	0	4	12	0	2	4	2	2	2	4
35_x	6	4	4	0	10	0	0	4	10	0	0	4	2	8	8	4
36_x	4	6	2	2	2	2	6	8	6	4	2	6	0	4	10	0
37_x	2	2	8	2	4	4	4	2	6	2	0	10	6	10	2	0
38_x	0	4	8	4	2	6	6	2	4	2	2	4	6	4	4	6
39_x	4	4	4	8	0	6	0	6	4	8	2	2	2	4	8	2
$3A_x$	8	8	0	4	2	0	10	4	0	0	0	4	8	6	8	2
$3B_x$	8	2	6	4	4	4	4	0	6	4	4	6	4	4	4	0
$3C_x$	0	6	6	6	6	0	0	8	8	2	4	8	4	2	4	0
$3D_x$	2	2	8	0	10	0	2	12	0	4	0	8	0	2	6	8
$3E_x$	6	4	0	0	4	4	0	10	6	2	6	12	2	4	0	4
$3F_x$	0	6	6	0	4	4	6	10	0	6	8	2	0	4	8	0