Optimal Resistance Against the Davies and Murphy Attack

Thomas Pornin

École Normale Supérieure, 45 rue d'Ulm, 75005 Paris, France,
thomas.pornin@ens.fr

Abstract. In recent years, three main types of attacks have been developed against Feistel-based ciphers, such as DES[1]; these attacks are linear cryptanalysis[2], differential cryptanalysis[3], and the Davies and Murphy attack[4]. Using the discrete Fourier transform, we present here a quantitative criterion of security against the Davies and Murphy attack. Similar work has been done on linear and differential cryptanalysis[5,11].

1 Introduction

The Feistel scheme is a simple design which allows, when suitably iterated, the construction of efficient block cipher, whose deciphering algorithm is implemented in a similar way. The most famous block cipher using a Feistel scheme is DES, where the scheme is iterated 16 times, with 16 subkeys extracted from a unique masterkey. The deciphering algorithm is just the same; the only difference is that the subkeys are taken in reverse order.

The masterkey of DES is only 56 bits long; this is vulnerable to exhaustive search. Indeed, specialized DES chips, able to calculate half a million DES ciphers per second, have been considered since 1987[6] and their cost evaluated; it is estimated that a five millions dollars machine using a few thousands of such chips could break a DES with a single plaintext/ciphertext pair in two or three hours[7]; other more recent estimates give lower prices, thanks to continuous technological progress. More recently, following a challenge proposed by RSA Inc., a 56 bits DES key was retrieved from a plaintext/ciphertext pair using only the idle time of a few thousands generic purpose workstations around the world[8].

Although exhaustive search is quite feasible, other attacks have been developped. These may be applicable to other schemes than DES. The first one was differential cryptanalysis[3]; it was based upon the existence of pairs of plaintext, so that the corresponding ciphertexts differ in some predictable way related to the difference of the plaintexts, with a small but not negligible probability. DES appeared to be extremely well protected against this cryptanalysis, and, indeed, it is now established that the NSA, which created DES as an improvement over the Lucifer scheme from IBM, knew about this attack and strengthened its algorithm against it. The attack requires 2^{47} chosen plaintexts and their corresponding ciphertexts

K. Ohta and D. Pei (Eds.): ASIACRYPT'98, LNCS 1514, pp. 148–159, 2000.

In 1993, following his earlier work, Matsui[2] discovered linear cryptanalysis, which exploited some linear properties of DES; more specifically, Matsui was able to build a linear equation of some of the bits of the plaintext, the ciphertext and the key, which stand with a probability slightly different from 0.5. Matsui described and implemented a method to use this equation in order to recover a DES key from 2^{43} plaintext/ciphertext pairs. The linear and differential cryptanalysis have been unified in a common formalism by Chabaud and Vaudenay[5].

In 1993, Davies and Murphy[4] presented another attack, which uses the fact that the output of the confusion function used in the Feistel scheme is not truly random, and that this bias depends upon several key bits. Using a large quantity of plaintext/ciphertext pairs, it is thus possible to guess these key bits with a reasonnable probability of success. This attack has not proven very efficient in the case of DES, but the same attack may work on other Feistel-based ciphers. The resistance of a Feistel-based cipher against linear and differential cryptanalysis has already been formally quantified[5]; we present here a similar quantification for the Davies and Murphy attack.

2 Notations

We here present a description of the Feistel scheme that is used in DES. More complete explanations may be found in [1].

We consider a message space $\mathcal{M}$ which consists of binary messages of a fixed length; we assume that this length is an even number, so that the messages may be divided in two parts of same length (the left one, with the most significant bits, and the right one, with the least significant bits). We note $\mathcal{N}$ the space of half-messages.

We also consider a confusion function f which takes two arugments, one from $\mathcal{N}$ and the other, K, from a subkey space denoted $\mathcal{K}$; f returns a value in $\mathcal{N}$.

If we consider a message (L, R) where L and R are in $\mathcal{N}$, the Feistel scheme calculates the message (L', R'), so that:

$$\begin{aligned} L' &= R \\ R' &= L \oplus f(R, K) \end{aligned}$$

where $\oplus$ is the bitwise "exclusive or" operation.

Such a scheme can be iterated several times, with different subkeys. Each iteration will be called a round. If we have r rounds, we can note (L_i, R_i) the input of the i-th round (i is between 1 and r) and (L_{i+1}, R_{i+1}) its output. The subkey used for round i is named K_i. We then have the following equations:

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus f(R_i, K_i). \end{aligned}$$

When used in a cryptographic scheme, L_{r+1} and R_{r+1} are often exchanged. Thus we have:

$$(L, R) = (L_1, R_1)$$
$$(L', R') = (R_{r+1}, L_{r+1}).$$

With this last operation, the deciphering operation is implemented exactly the same way the enciphering is; only the subkeys K_i are taken in reverse order.

A four-rounds Feistel cipher is schematically represented in the figure 1.

In DES, there are 16 rounds ($r = 16$) and the elements of $\mathcal{N}$ are 32 bits long. The subkeys are 48 bits long, extracted from a 56 bits masterkey with a fixed and public algorithm. A known permutation is applied to the message before entering the 16 consecutive Feistel rounds, and the reverse of this permutation is applied afterwards. These permutations are fixed by the standard and can be easily inverted, so we forget them here.

We may note an interesting property of such ciphers; this property was discovered and used by Davies and Murphy in their attack[4]. For each round i, we have:

$$f(R_i, K_i) = L_i \oplus R_{i+1}$$

and, if i is not r:

$$R_{i+1} = L_{i+2}.$$

Therefore, if i is not r, we have:

$$f(R_i, K_i) = L_i \oplus L_{i+2}.$$

This remark is true for each round except the last one (where $i+2$ has no sense). If we take the exclusive or of these equations for i even, we obtain the following:

$$R \oplus L' = \bigoplus_{j=1}^{r/2} f(R_{2j}, L_{2j}).$$

We can make the same operation with the odd rounds, and get the following equation:

$$L \oplus R' = \bigoplus_{i=1}^{r/2} f(R_{2i-1}, L_{2i-1}).$$

Each plaintext/ciphertext pair thus gives access to the XORed value of the outputs of the f functions of the even rounds, and also the XORed value of the outputs of the f function of the odd rounds. That is why a non-uniform distribution of the output of the f function may be revealed by observing a large quantity of plaintext/ciphertext pairs.

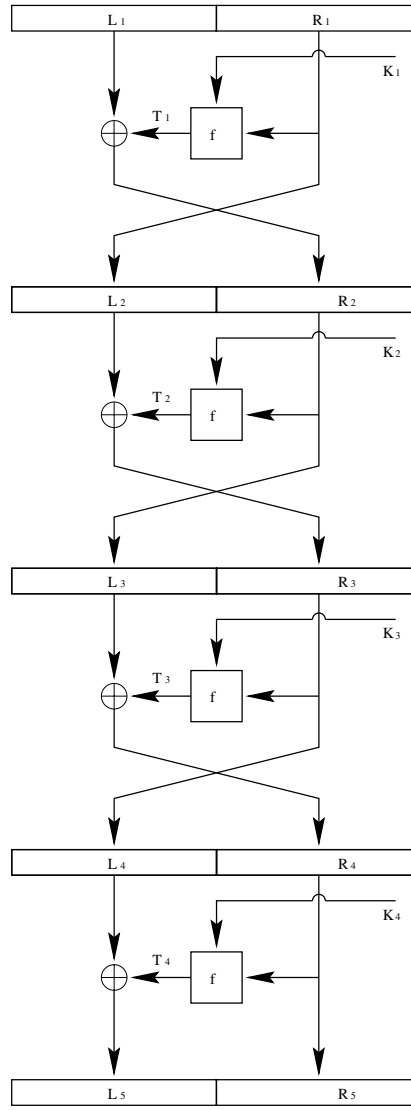

Figure 1: a four rounds Feistel cipher

3 Davies and Murphy Attack

This attack was presented in [4] and improved by Biham and Biryukov[10].

We assume that there exists a pattern of n bits, in the output of f, so that the 2^n values this pattern may get are not equidistributed, for a given key K and uniformly distributed random input R. We also assume that the distribution of the 2^n values may vary with some bits of the key, in a theorically predictable way. Thus, we have a set of possible distributions, depending on the key, and identifying the actual distribution in this set gives us some information on the key.

In the standard DES, we can consider the output of two neighbouring S-boxes in the i-th round. This is an 8-bit output; these 8 bits can be observed in the output of the f function: in the DES, a fixed permutation is applied to the output of the S-boxes, and this permutation is the same for the 16 rounds; so the 8 bits form a fixed pattern in the output of f.

Two neighbouring S-boxes have an input size of 12 bits; 12 bits of K_i but only 10 bits of R_i are combined to be used as this input. Two bits of R_i are duplicated; the two instances of each of these bits are XORed with two different key bits, and then go into the two S-boxes. This is shown in the figure 2.

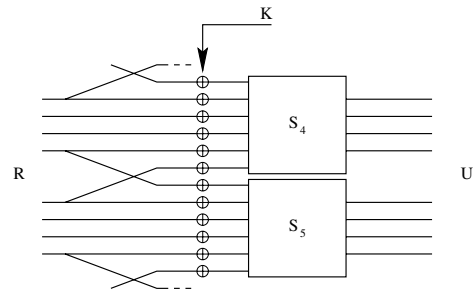

Figure 2: two neighbouring S-boxes in the DES

For each duplicated bit, the key bits condition whether the two instances of this bit are equal or opposite when entering the two S-boxes. For random R, this only implies a non-uniformity of the 12 bits input of the two S-boxes. There are two duplicated bits, and therefore four possible sets of 12 bits inputs, depending upon four key bits. Theses sets and the according output distribution of the two S-boxes can be easily enumerated.

As noted in section 2, for each plaintext/ciphertext pair, we have access to the XORed value of the outputs of the f functions of odd rounds, and thus access to the XORed value of the corresponding 8-bits paterns. If each f function of each round may have four output distributions, then the XORed value of 8 such

outputs may take 165 possible distributions: the XOR is commutative, so that the order of the rounds does not matter; what only matters is the number of distributions of each of the four types described above. This leads to $\binom{11}{3} = 165$ possibilities.

Strangely enough, in DES, we end up with only two possible distributions; this is due to the specific definition of S-boxes (for a S-box, the output is a permutation of the 16 values taken by the four middle bits, and the two extreme bits determine which permutation to apply among four), which leads to some simplifications in the enumeration of the distributions. The details of this calculation may be found in [4]. The actual distribution depends upon the XORed value of several key bits (that is, an indirect key bit, that help us reduce the complexity of the exhaustive search of the key).

Therefore, identifying the actual distribution among the two possible reveals one indirect key bit. As this can be done for odd rounds as well as for even rounds, with the same plaintext/ciphertext pairs, the attack may give us two key bits.

The most efficient statistical test known is the maximum likelihood method: for each of the possible distributions, one calculates the probability of the event actually measured; the distribution which gives the highest probability is then supposed to be the right one. In the case of DES neighbouring S-boxes, we then have two distributions, which may be represented as two vectors u and v in $\mathbf{R}^{256}$; u_i with i between 0 and 255 is the probability of obtaining the 8-bits value i. Obviously, for each i, u_i is a real number between 0 and 1, and we have:

$$\sum_{i=0}^{255} u_i = 1.$$

We can also define u' (and similarly v') where

$$u_i = \frac{1}{256} + u'_i.$$

Thus we have:

$$\sum_{i=0}^{255} u'_i = 0.$$

As a consequence of the peculiar definition of S-boxes, we have:

$$u' + v' = 0.$$

More detailed explanations about this fact may be found in [4]; this is not a general property of Feistel schemes, but an artefact of the structure of the S-boxes.

Let us assume that we have access to M plaintext/ciphertext pairs; among these M pairs, each 8-bits value i appeared m_i times. If the theorical distribution is u, the probability of such an event is:

$$p_1 = \prod_{i=0}^{255} u_i^{m_i}.$$

p_2 is also defined, in the v case. Comparing p_1 and p_2 is equivalent to comparing their logarithms. We have:

$$\log p_1 = \sum_{i=0}^{255} m_i \log u_i.$$

So we have:

$$\log p_1 = \sum_{i=0}^{255} m_i \log(\frac{1}{256} + u'_i)$$

As the sum of all m_i's is M, we have the following:

$$\log p_1 = \sum_{i=0}^{255} m_i \log(1 + 256u'_i) - M \log 256$$

As $256u'_i$ is relatively small, compared to 1 (for a perfect cipher, u' should be 0; DES is well-designed, and a simple experiment on a few millions random plaintexts confirms that the deviation u' we deal with is really small, and thus many pairs plaintext/ciphertext are required), we can approximate the logarithms on the right hand side, which gives:

$$\log p_1 + M \log 256 \approx 256 \sum_{i=0}^{255} m_i u'_i.$$

Similarly, we have:

$$\log p_2 + M \log 256 \approx 256 \sum_{i=0}^{255} m_i v'_i.$$

Thus we compare the scalar product of m with u' and the scalar product of m with v'. We can bound these products using euclidian norms over $\mathbf{R}^{256}$. If we note $N(x)$ the euclidian norm of x, our two scalar products are:

$$s_1 = m \cdot u' \leq N(m)N(u')$$
$$s_2 = m \cdot v' \leq N(m)N(v').$$

m is what we obtain by analyzing the plaintext/ciphertext pairs; it follows a precise distribution, but may vary around this one. m_i is a random variable which counts the number of times the pattern value i was obtained among the M pairs. The probability of obtaining i for each pair is close to $1/256$, therefore the mean value of m_i is close to $M/256$, and its variance is near $(M/256)(255/256)$, which we approximate by $M/256$.

So the difference between m and its theorical value (namely M times its distribution vector) is a vector whose coordinates have an average absolute value of $(\sqrt{M})/16$; so the norm of this vector is close to $\sqrt{M}$ (where $N(m)$ is close to

$M/16$). To conclude anything from the pairs plaintext/ciphertext, the expected deviation (the difference between s_1 and s_2) must not be smaller than the standard deviation (which is the average deviation of a measure from its distribution — when dealing with uni-dimensional random variables, the standard deviation is the square root of the variance). Therefore, M must be sufficiently big so that:

$$N(m)(N(u') + N(v')) \geq \sqrt{M}.$$

This can be rewritten:

$$M \geq \frac{256}{(N(u') + N(v'))^2}.$$

In the actual DES, this leads to an attack with at least 2^{52} pairs, which may reveal two key bits. This is achieved with the two S-boxes 7 and 8. With 2^{55} pairs, the probability of success of the attack (that is, guessing correctly the two indirect key bits) is above 50%. The other pairs of S-boxes are much worse, as far as we deal with attacks.

4 The General Feistel Scheme Case

We now consider the general case of the Davies and Murphy attack; thus we ignore all simplifications induced by the specific definition of DES. We have a Feistel-based cipher, with r rounds (r is even), with a confusion function f, so that n particular bits of the output of the f function form a pattern whose 2^n possible values are not equidistributed. We also assume that the distribution of these values may vary, depending on some of the key bits of the considered round. We suppose we have q possible distributions, represented by q vectors of $\mathbf{R}^{2^n}$, denoted as u^1, u^2,... u^q.

For each plaintext/ciphertext pair, we have acces to the XORed value of $r/2$ patterns of n bits. This value follows a distribution which depends upon some key bits; we can theorically calculate these distributions, and we want to be able to determine, using several plaintext/ciphertext pairs, which distribution among the possible ones is the one actually in use; this would give us the corresponding information about the key bits involved.

The XOR operation is commutative; in each round, the pattern may have one distribution among q; what only matters in the distribution of the XORed value of the $r/2$ patterns is the number of each distribution we have among the $r/2$ rounds. The number of possible combinations is then:

$$\binom{r/2 + q - 1}{q - 1}.$$

Some of these distributions may in fact be alike, just as is the case with DES, where there are only two distributions.

We now introduce another representation for distributions of n-bits patterns, that we considered for the moment as vectors in $\mathbf{R}^{2^n}$. Such a vector can be viewed as a function from $\mathbf{Z}_2^n$ to $\mathbf{R}$, which associates to an n-bit binary vector

the coordinate associated with the integer number the binary vector represents. Such a function may be decomposed using Fourier transform[9].

We consider the Fourier basis of function v_y for each vector y in $\mathbf{Z}_2^n$, so that for each vector x, we have:

$$v_y(x) = (-1)^{y \cdot x}$$

where $y \cdot x$ denotes the scalar product of y and x (namely the number of bits set to 1 in $y\&x$, where & is the bitwise AND operation).

If a is a function from $\mathbf{Z}_2^n$ to $\mathbf{R}$, we can compute its Fourier coefficients $\hat{a}(y)$ (for each vector y) as follows:

$$\hat{a}(y) = \sum_x a(x) v_y(x).$$

Using these coefficients, we can find the a function with the inverse Fourier transform:

$$a(x) = 2^{-n} \sum_y \hat{a}(y) v_y(x) = 2^{-n} \hat{\hat{a}}(x)$$

for each vector x.

The XOR operation between the output of two rounds of the cipher is, in the Fourier formalism, a convolution of the two distributions of outputs. Indeed, if a is the function representing the distribution of the output of the first round, and b is the output of the second round, then the distribution of the bitwise XOR of these two rounds will be c, where, for each x:

$$c(x) = \sum_{y \oplus z = x} a(y) b(z).$$

But, the addition in $\mathbf{Z}_2^n$ is nothing else that the XOR operation, and, for each x, we have $x \oplus x = 0$. Therefore, the equation may be rewritten this way:

$$c(x) = \sum_y a(x - y) b(y).$$

A convolution is simply calculated by multiplying term by term the Fourier coefficients. This means that, using the preceding notations, we have, for each x:

$$\hat{c}(x) = \hat{a}(x) \hat{b}(x).$$

We shall prove a similar property for the deviations to equiprobability: if we consider a', b' and c' such that $a(x) = 2^{-n} + a'(x)$ for all x, then, if c is the convolution product of a and b, then c' is the convolution product of a' and b'. Indeed, if we note d the constant function equal to 2^{-n}, its Fourier coefficients $\hat{d}(x)$ are 1 if $x = 0$, 0 otherwise. Therefore, we have the following:

$$\begin{aligned}
\hat{a} &= \hat{a}' + \hat{d} \\
\hat{b} &= \hat{b}' + \hat{d} \\
\hat{c} &= \hat{c}' + \hat{d} \\
\hat{c} &= \hat{a}\hat{b}
\end{aligned}$$

So we have, by replacing a, b and c in the last equation by their expression in a', b' and c':

$$\hat{c'} + \hat{d} = \hat{a'}\hat{b'} + \hat{d}^2 + \hat{d}(\hat{a'} + \hat{b'})$$

We have clearly $\hat{d}^2 = \hat{d}$ (as $\hat{d}(x) = 0$ or 1 for each x), and $\hat{a'}(0) = \hat{b'}(0) = 0$ (for a function u, the first Fourier coefficient $\hat{u}(0)$ is the sum of all its values over $\mathbf{Z}_2^n$, so it is 0 in the case of a' and b', as these are the deviation of a distribution to the uniform distribution, which is the constant function equal to 2^{-n}).

In order to set a minimal bound for the complexity of the Davies and Murphy attack, we want to get a maximal bound for the size of the deviation of the pattern of the output of the f function to the uniform distribution. If we consider the m/M vector, this will follow the distribution a, which deviates from the uniform distribution by a'. The m vector comes from an actual "measure" (the plaintext/ciphertext pairs), so it will deviate from its distribution by an average distance of $\sqrt{M}$ (this is the same calculus as at the end of the section 3). We use the maximum likelihood method, so we compare the scalar products of m with the possibles deviations to equidistributions.

So we find that, if Y is a maximal bound for the euclidian norm of the deviation (in $\mathbf{R}^{2^n}$), the scalar products we consider are the number M of plaintext/ciphertext pairs needed for a succesful attack must be such that:

$$2\frac{M}{2^{n/2}}Y \geq \sqrt{M}$$

($2Y$ is a maximum for the distance between two possible distributions) which can be rewritten this way:

$$M \geq \frac{2^n}{4Y^2}$$

We note that this result stands with the approximations used in the section 3, in particular n is big enough to neglect 2^{-n} with respect to 1.

All we need is the value of Y. If the function of the distribution of the XORed value of the output of the $r/2$ rounds is a, then we may obtain Y from its Fourier coefficients $\hat{a}$. Indeed, the euclidian norm over $\mathbf{R}^{2^n}$ corresponds to the L^2 norm in the function space, and the scalar product becomes the following:

$$a \cdot b = \sum_x a(x)b(x)$$

The Fourier transform simply computes the coordinates of a function a' over the orthogonal basis (v_y). All v_y have $2^{n/2}$ as L^2 norm. We can therefore calculate the L^2 norm of a function a using the Fourier coefficients $\hat{a}$:

$$N(a') = 2^{-n/2}N(\hat{a'})$$

Therefore we have:

$$N(a) \leq 2^{n/2} \max_x |\hat{a}(x)|$$

where $N(a)$ is the L^2 norm of a. Thus, we have the proposed value Y:

$$Y = \max_x |\hat{a}(x)|$$

We have seen that the Fourier coefficients of a are obtained by multiplying those of the functions associated to each round. We then have the following security criterion:

- Calculate the Fourier coefficients of the functions representing the possible bias towards equiprobability of the distribution of the chosen pattern in the output of the confusion function of one round. This is done in the DES by expliciting the distribution of the pattern, by exhaustive enumeration of the possible inputs of two neighbouring S-boxes.
- Take the largest of these coefficients in absolute value, noted μ.
- Raise it to the r power.
- This peculiar pattern is secure against Davies and Murphy attacks up to:

$$\frac{1}{4\mu^r}$$

The global security of the scheme is therefore a question of enumeration of possible biased patterns. The criterion uses some approximations, so the actual security may in fact be higher. In the DES case, with the same pattern as the one used by Davies and Murphy to find the attack in 2^{52} (but Davies and Murphy consider the attack as useful only if it gives two correct key bits with a probability better than 0.5, and therefore calculate a complexity of 2^{55} in this case) we find a security of at least 2^{52}.

5 The Approximations Used

It must be noted that we made, in the calculation, several approximations. The main one is that we want to bound the euclidian distance between possible distributions, and we do it by bounding the deviation of these distributions to equiprobability; this is just what is necessary in the DES case, as the two possible deviations to equiprobability are just symmetric. That is why we obtain the exact result in this case.

The other calculations are also subject to some approximations. We considered that the 2^n coordinates of the m vector are gaussian independant random variables; they are not, in fact, independant, as their sum is M. If 2^n is sufficiently big, this will not be a problem. In the DES case, $n = 8$, so we neglect this effect. The m_i values follow binomial distributions, which can be approximated by a gaussian distribution if M is big enough, using the central limit theorem. Considering the precision needed, any M above 1000 will do it (and indeed M is largely above 1000). We also assume that the final distribution is close to the equiprobable one, which is desirable anyway in any symetric cipher scheme.

6 Conclusion and Open Problems

We described a method to calculate a minimal bound for the Davies and Murphy attack against a Feistel scheme. In order to apply it efficiently to a given

scheme, one must first identify the patterns of bits in the output of the confusion function, whose possible values are not equidistributed. Once identified, their output distribution must then be calculated precisely, which may not be easy, depending on the scheme.

References

1. National Bureau of Standards, *Data Encryption Standard*, U.S. Department of Commerce, FIPS pub. 46, January 1977.
2. M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'93, pp. 386–397, 1993.
3. E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
4. D. Davies, S. Murphy, *Pairs and Triplets of DES S-Boxes*, Journal of Cryptology, Vol. 10, No. 3, pp. 195–206, 1997.
5. F. Chabaud, S. Vaudenay, *Links between Differential and Linear Cryptanalysis*, LIENS, Ecole Normale Supérieure, March 1994.
6. F. Hoornaert, J. Goubert, Y. Desmedt, *Efficient Hardware Implementation of the DES*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'84, p. 147, 1984.
7. M.E. Hellman, Comments at 1993 RSA Data Security conference, 14-15 January 1993.
8. The results of the DES challenge teams were published only on the World Wide Web; see http://www.frii.com/~rcv/deschall.htm for further information.
9. W. Rudin, *Fourier Analysis on Groups*, Interscience Publishers Inc., New York, 1962.
10. E. Biham, A. Biryukov, *An Improvement of Davies' Attack on DES*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'94, pp. 461–467, 1994.
11. K. Nyberg, *Perfect Nonlinear S-boxes*, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'91, pp. 378–385, 1991.