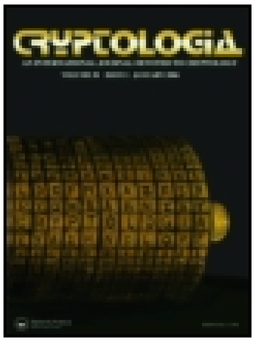

CRYPTOLOGIA

ISSN: 0161-1194 (Print) 1558-1586 (Online) Journal homepage: https://www.tandfonline.com/loi/ucry20

A TUTORIAL ON LINEAR AND DIFFERENTIAL CRYPTANALYSIS

Howard M. Heys

A TUTORIAL ON LINEAR AND DIFFERENTIAL CRYPTANALYSIS

Howard M. Heys

ADDRESS: Electrical and Computer Engineering, Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, NF CANADA A1B 3X5. howard @engr.mun.ca.

ABSTRACT: In this paper, we present a detailed tutorial on linear cryptanalysis and differential cryptanalysis, the two most significant attacks applicable to symmetric-key block ciphers. The intent of the paper is to present a lucid explanation of the attacks, detailing the practical application of the attacks to a cipher in a simple, conceptually revealing manner for the novice cryptanalyst. The tutorial is based on the analysis of a simple, yet realistically structured, basic Substitution-Permutation Network cipher. Understanding the attacks as they apply to this structure is useful, as the Rijndael cipher, recently selected for the Advanced Encryption Standard (AES), has been derived from the basic SPN architecture. As well, experimental data from the attacks is presented as confirmation of the applicability of the concepts as outlined.

KEYWORDS: Symmetric-key cryptography, block ciphers, substitution-permutation networks, linear cryptanalysis, differential cryptanalysis.

1 INTRODUCTION

In this paper, we present a tutorial on two powerful cryptanalysis techniques applied to symmetric-key block ciphers: linear cryptanalysis [16] and differential cryptanalysis [1]. Linear cryptanalysis was introduced by Matsui at EUROCRYPT '93 as a theoretical attack on the Data Encryption Standard (DES) [19] and later successfully used in the practical cryptanalysis of DES [17]; differential cryptanalysis was first presented by Biham and Shamir at CRYPTO '90 to attack DES and eventually the details of the attack were packaged as a book [2]. Although the early target of both attacks was DES, the wide applicability of both attacks to numerous other block ciphers has solidified the pre-eminence of both cryptanalysis techniques in the consideration of the security of all block ciphers. For example, many of the candidates submitted for the recent Advanced Encryption Standard process undertaken by the National Institute of Standards and Technology [20] were designed using techniques specifically targeted at thwarting linear and differential cryptanalysis. This is evident, for example, in the Rijndael cipher [6], the encryption algorithm selected to be the new standard. The concepts discussed in this paper could be used to form an initial understanding required to comprehend the design principles and security analysis of the Rijndael cipher, as well as many other ciphers proposed in recent years.

The paper is structured as a tutorial and, as such, is intended to not be rigorously mathematical. It introduces the basic concepts of linear and differential cryptanalysis but is by no means a definitive source for understanding all the many refinements and improvements of the attacks over the years. The basic purpose of the paper is to use a simple (yet somewhat realistic) cipher structure to study the most basic concepts of the two attacks. Other more formal discussions exist on the topic. For example, overviews of the attacks as applied to Substitution-Permutation Networks (the cipher structure to be considered in this paper) are presented in [10, 11]. For a general introduction to block ciphers and their analysis, see [14].

The need for a tutorial on the attacks arises from the very difficult nature of both attacks and the lack of *simplified*, yet detailed, reference material describing the attacks. Most published material detailing the attacks has a research focus and gives little intuition and explanation for the non-expert. When the basic concepts of the attack are described in the literature (as in Matsui's and Biham and Shamir's original papers), they are typically presented in reference to DES which is, in nature, somewhat convoluted in a manner which interferes with the understanding of the cryptanalytic concepts.

2 A BASIC SUSTITUTION-PERMUTATION NETWORK CIPHER

The cipher that we shall use to present the concepts is a basic Substitution-Permutation Network (SPN). We will focus our discussion on a cipher, illustrated in Figure 1, that takes a 16-bit input block and processes the block by repeating the basic operations of a round four times. Each round consists of (1) substitution, (2) transposition of the bits (i.e., permutation of the bit positions), and (3) key mixing. This basic structure was presented by Feistel back in 1973 [8] and these basic operations are similar to what is found in DES and many other modern ciphers, including Rijndael. So, although we are considering a somewhat simplified structure, an analysis of the attack of such a cipher presents valuable insight into the security of larger, more practical constructions.

2.1 Substitution

In our cipher, we break the 16-bit data block into four 4-bit sub-blocks. Each sub-block forms an input to a 4×4 S-box (a substitution with 4 input and 4 output bits), which can be easily implemented with a table lookup of sixteen 4-bit values, indexed by the integer represented by the 4 input bits. The most fundamental property of an S-box is that it is a nonlinear mapping, i.e., the output bits cannot be represented as a linear operation on the input bits.

For our cipher, we shall use the same nonlinear mapping for all S-boxes. (In DES all the S-boxes in a round are different, while all rounds use the same set of S-boxes.) The attacks of linear and differential cryptanalysis apply equally whether there is one mapping or all S-boxes are different mappings. The mapping chosen for our cipher, given in Table 1, is chosen from the S-boxes of DES. (It is the first row of the first S-box.) In the table, the most significant bit of the hexadecimal notation represents the leftmost bit of the S-box in Figure 1.

input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Table 1. S-box Representation (in hexadecimal).

2.2 Permutation

The permutation portion of a round is simply the tranposition of the bits or the permutation of the bit positions. The permutation of Figure 1 is given in Table 2 (where the numbers represent bit positions in the block, with 1 being the leftmost bit and 16 being the rightmost bit) and can be simply described as: output i of S-box j is connected to input j of S-box i. Note that there would be no purpose for a permutation in the last round and, hence, our cipher does not have one.

input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
output	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Table 2. Permutation.

2.3 Key Mixing

To achieve the key mixing, we use a simple bit-wise exclusive-OR between the key bits associated with a round (referred to as a subkey) and the data block input to a round. As well, a subkey is applied following the last round, ensuring that the last layer of substitution cannot be easily ignored by a cryptanalyst that simply works backward through the last round's substitution. Normally, in

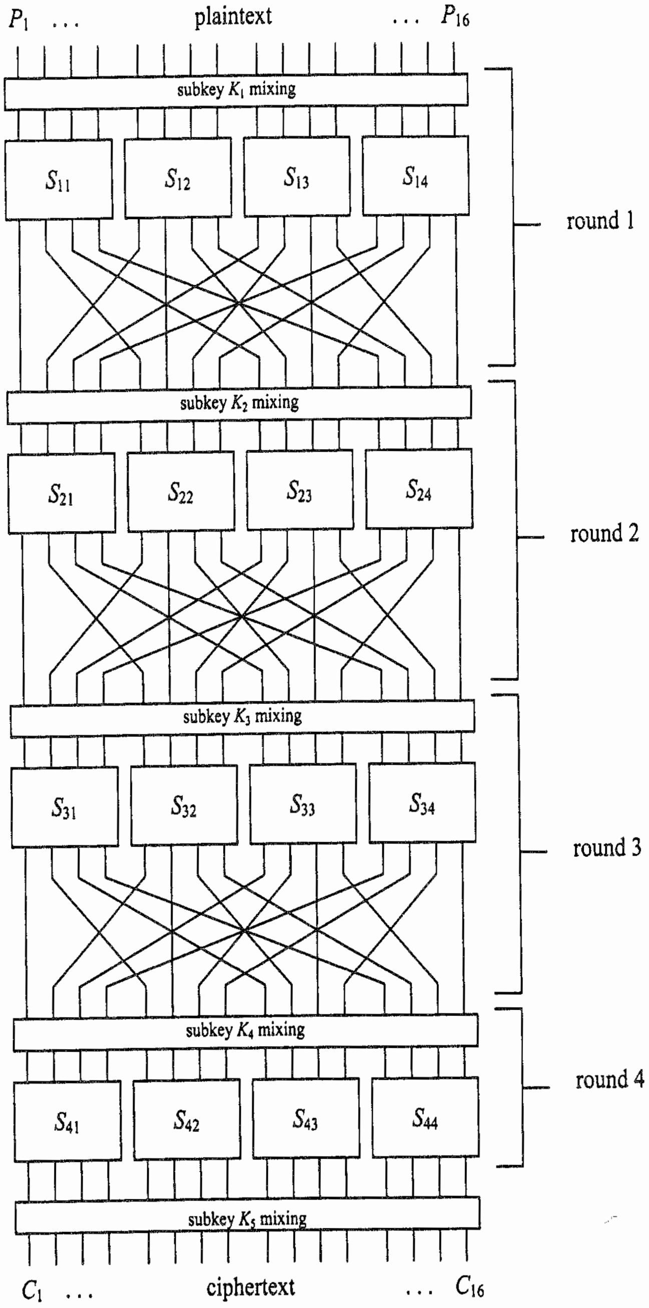

Figure 1. Basic Substitution-Permutation Network (SPN) Cipher.

a cipher, the subkey for a round is derived from the cipher's master key through a process known as the key schedule. In our cipher, we shall assume that all bits of the subkeys are independently generated and unrelated.

2.4 Decryption

In order to decrypt, data is essentially passed backwards through the network. Hence, decryption is also of the form of an SPN as illustrated in Figure 1. However, the mappings used in the S-boxes of the decryption network are the inverse of the mappings in the encryption network (i.e., input becomes output, output becomes input). This implies that, in order for an SPN to allow for decryption, all S-boxes must be bijective, that is, a one-to-one mapping with the same number of input and output bits. As well, in order for the network to properly decrypt, the subkeys are applied in reverse order and the bits of the subkeys must be moved around according to the permutation, if the SPN is to look similar to Figure 1. Note also that the lack of the permutation in the last round ensures that the decryption network can be the same structure as the encryption network. (If there was a permutation after the last substitution layer in the encryption, the decryption would require a permutation before the first layer of substitution.)

3 LINEAR CRYPTANALYSIS

In this section, we outline the approach to attacking a cipher using linear cryptanalysis based on the example cipher of our basic SPN.

3.1 Overview of Basic Attack

Linear cryptanalysis tries to take advantage of high probability occurrences of linear expressions involving plaintext bits, "ciphertext" bits (actually we shall use bits from the 2^{nd} last round output), and subkey bits. It is a known plaintext attack: that is, it is premised on the attacker having information on a set of plaintexts and the corresponding ciphertexts without, however, the attacker having any way to select which plaintexts (and corresponding ciphertexts) are available. In many applications and scenarios it is reasonable to assume that the attacker has knowledge of a random set of plaintexts and the corresponding ciphertexts.

The basic idea is to approximate the operation of a portion of the cipher with an expression that is linear where the linearity refers to a mod-2 bit-wise operation (i.e., exclusive-OR denoted by "$\oplus$"). Such an expression is of the form:

$$X_{i_1} \oplus X_{i_2} \oplus \ldots \oplus X_{i_u} \oplus Y_{j_1} \oplus Y_{j_2} \oplus \ldots \oplus Y_{j_v} = 0 \qquad (1)$$

where X_i represents the i^{th} bit of the input $X = [X_1, X_2, \ldots]$ and Y_j represents the j^{th} bit of the output $Y = [Y_1, Y_2, \ldots]$. This equation is representing the exclusive-OR "sum" of u input bits and v output bits.

The approach in linear cryptanalysis is to determine expressions of the form above which have a high or low probability of occurrence. (No obvious linearity such as above should hold for all input and output values or the cipher would be trivially weak.) If a cipher displays a tendency for equation (1) to hold with high probability or to hold with low probability, this is evidence of the cipher's poor randomization abilities. Consider that if we randomly selected values for $u + v$ bits and placed them into the equation above, the probability that the expression would hold would be exactly 1/2. It is the deviation or bias from the probability of 1/2 for an expression to hold that is exploited in linear cryptanalysis: the further away that a linear expression is from holding with a probability of 1/2, the better the cryptanalyst is able to apply linear cryptanalysis. In the remainder of the paper, we refer to the amount by which the probability of a linear expression holding deviates from 1/2 as the *linear probability bias*. Hence, if the expression above holds with probability p_L for randomly chosen plaintexts and the corresponding ciphertexts, then the probability bias is $p_L - 1/2$. The higher the magnitude of the probability bias, $|p_L - 1/2|$, the better the applicability of linear cryptanalysis with fewer known plaintexts required in the attack.

There are several ways to mount the attack of linear cryptanalysis. In this paper, we shall focus on what Matsui calls Algorithm 2 [16]. We investigate the construction of a linear approximation involving plaintext bits as represented by X in (1) and the input to the last round of the cipher (or equivalently the output of the 2nd last round of the cipher) as represented by Y in (1). The plaintext bits are random and consequently so are the input bits to the last round.

Equation (1) could be equivalently reformulated to have the right side being the sum of a number of subkey bits. However, in (1) as written with the right side of "0", the equation implicitly has subkey bits involved: these bits are fixed but unknown (as they are determined by the key under attack) and implicity absorbed into the "0" on the right side of equation (1) and the probability p_L that the linear expression holds. If the sum of the involved subkey bits is "0", the bias of (1) will have the same sign (+ or −) as the bias of the expression involving the subkey sum and, if the sum of the involved subkey bits is "1", the bias of (1) will have the opposite sign.

Note that $p_L = 1$ implies that linear expression (1) is a perfect representation of the cipher behaviour and the cipher has a catastrophic weakness. If $p_L = 0$, then (1) represents an affine relationship in the cipher, also an indication of a catastrophic weakness. For mod-2 addition systems, an affine function is simply the complement of a linear function. Both linear and affine approximations, indicated by $p_L > 1/2$ and $p_L < 1/2$, respectively, are equally susceptible to linear cryptanalysis and we shall generally use the term linear to refer to both linear and affine relationships.

The natural question to ask is: How do we construct expressions which are highly linear and, hence, can be exploited? This is done by considering the properties of the cipher's only nonlinear component: the S-box. When the nonlinearity properties of the S-box are enumerated, it is possible to develop linear approximations between sets of input and output bits in the S-box. Consequently, it is possible to concatenate linear approximations of the S-boxes together so that intermediate bits (i.e., data bits from within the cipher) can be cancelled out and we are left with a linear expression which has a large bias and involves only plaintext and the last round input bits.

3.2 Piling-Up Principle

Before we consider constructing a linear expression for the example cipher of this paper, we need some basic tools. Consider two random binary variables, X_1 and X_2. We begin by noting the simple relationships: $X_1 \oplus X_2 = 0$ is a linear expression and is equivalent to $X_1 = X_2$; $X_1 \oplus X_2 = 1$ is an affine expression and is equivalent to $X_1 \neq X_2$.

Now, assume that the probability distributions are given by

$$\Pr(X_1 = i) = \begin{cases} p_1 & , \text{if } i = 0 \\ 1 - p_1 & , \text{if } i = 1 \end{cases}$$

and

$$\Pr(X_2 = i) = \begin{cases} p_2 & , \text{if } i = 0 \\ 1 - p_2 & , \text{if } i = 1 \; . \end{cases}$$

If the two random variables are independent, then

$$\Pr(X_1 = i, X_2 = j) = \begin{cases} p_1 p_2 & , \text{if } i = 0, j = 0 \\ p_1(1 - p_2) & , \text{if } i = 0, j = 1 \\ (1 - p_1)p_2 & , \text{if } i = 1, j = 0 \\ (1 - p_1)(1 - p_2) & , \text{if } i = 1, j = 1 \end{cases}$$

and it can be shown that

$$\begin{aligned}\Pr(X_1 \oplus X_2 = 0) &= \Pr(X_1 = X_2)\\ &= \Pr(X_1 = 0, X_2 = 0) + \Pr(X_1 = 1, X_2 = 1)\\ &= p_1 p_2 + (1 - p_1)(1 - p_2).\end{aligned}$$

Another perspective is to let $p_1 = 1/2 + \epsilon_1$ and $p_2 = 1/2 + \epsilon_2$, where ϵ_1 and ϵ_2 are the probability biases and $-1/2 \leq \epsilon_1, \epsilon_2 \leq +1/2$. Hence, it follows that

$$\Pr(X_1 \oplus X_2 = 0) = 1/2 + 2\epsilon_1\epsilon_2$$

and the bias $\epsilon_{1,2}$ of $X_1 \oplus X_2 = 0$ is

$$\epsilon_{1,2} = 2\epsilon_1\epsilon_2.$$

This can be extended to more than two random binary variables, X_1 to X_n, with probabilities $p_1 = 1/2+\epsilon_1$ to $p_n = 1/2+\epsilon_n$. The probability that $X_1 \oplus \ldots \oplus X_n = 0$ holds can be determined by the Piling-Up Lemma which assumes that all n random binary variables are independent.

PILING-UP LEMMA (Matsui [16]): For n independent, random binary variables, X_1, X_2, ..., X_n,

$$\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 1/2 + 2^{n-1} \prod_{i=1}^{n} \epsilon_i$$

or, equivalently,

$$\epsilon_{1,2,\ldots,n} = 2^{n-1} \prod_{i=1}^{n} \epsilon_i$$

where $\epsilon_{1,2,\ldots,n}$ represents the bias of $X_1 \oplus \ldots \oplus X_n = 0$.

Note that if $p_i = 0$ or 1 for all i, then $\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 0$ or 1. If only one $p_i = 1/2$, then $\Pr(X_1 \oplus \ldots \oplus X_n = 0) = 1/2$.

In developing the linear approximation of a cipher, the X_i values will actually represent linear approximations of the S-boxes. Consider three independent random binary variables, X_1, X_2, and X_3. Let $\Pr(X_1 \oplus X_2 = 0) = 1/2 + \epsilon_{1,2}$ and $\Pr(X_2 \oplus X_3 = 0) = 1/2 + \epsilon_{2,3}$ and consider the sum $X_1 \oplus X_3$ to be derived by adding $X_1 \oplus X_2$ and $X_2 \oplus X_3$ together. Hence,

$$\Pr(X_1 \oplus X_3 = 0) = \Pr([X_1 \oplus X_2] \oplus [X_2 \oplus X_3] = 0).$$

So we are combining linear expressions to form a new linear expression. If we treat variables $X_1 \oplus X_2$ and $X_2 \oplus X_3$ as if they were independent[1], we can use the Piling-Up Lemma, to determine

$$\Pr(X_1 \oplus X_3 = 0) = 1/2 + 2\epsilon_{1,2}\epsilon_{2,3}$$

and, consequently,

$$\epsilon_{1,3} = 2\epsilon_{1,2}\epsilon_{2,3}.$$

As we shall see, the expressions $X_1 \oplus X_2 = 0$ and $X_2 \oplus X_3 = 0$ are analogous to linear approximations of S-boxes and $X_1 \oplus X_3 = 0$ is analogous to a cipher approximation where the intermediate bit X_2 is eliminated. Of course, the real analysis will be more complex involving many S-box approximations.

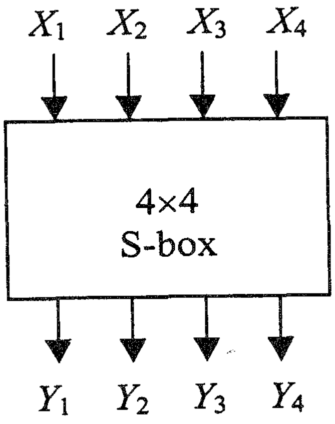

Figure 2. S-box Mapping.

3.3 Analyzing the Cipher Components

Before considering the attack in any more detail on the overall cipher, we first require knowledge of the linear vulnerabilities of an S-box. Consider the S-box representation of Figure 2 with input $X = [X_1, X_2, X_3, X_4]$ and a corresponding output $Y = [Y_1, Y_2, Y_3, Y_4]$. All linear approximations can be examined to determine their usefulness by computing the probability bias for each. Hence, we are examining all expressions of the form of equation (1) where X and Y are the S-box input and output, respectively.

[1] Only under very strict conditions are they actually independent: $\epsilon_1 = 0$, $\epsilon_3 = 0$, or $\epsilon_2 = \pm 1/2$. However, in practice, when applying the linear attack, we typically assume that the Piling-Up Lemma may be applied as if $X_1 \oplus X_2$ and $X_2 \oplus X_3$ are independent, in order to get an estimate of the bias of the overall linear approximation of the cipher.

For example, for the S-box used in our cipher, consider the linear expression $X_2 \oplus X_3 \oplus Y_1 \oplus Y_3 \oplus Y_4 = 0$ or equivalently

$$X_2 \oplus X_3 = Y_1 \oplus Y_3 \oplus Y_4.$$

Applying all 16 possible input values for X and examining the corresponding output values Y, it may be observed that for exactly 12 out of the 16 cases, the expression above holds true. Hence, the probability bias is $\frac{12}{16} - \frac{1}{2} = \frac{1}{4}$. This is presented in Table 3.

Similarly, for equation

$$X_1 \oplus X_4 = Y_2$$

it may be seen that the probability bias is 0 and for equation

$$X_3 \oplus X_4 = Y_1 \oplus Y_4$$

the probability bias is $\frac{2}{16} - \frac{1}{2} = -\frac{3}{8}$. In the last case, the best approximation is an affine approximation as indicated by the minus sign. However, the success of the attack is based on the magnitude of the bias and, as we shall see, affine approximations can be used equivalently to linear approximations.

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	X_2 $\oplus X_3$	Y_1 $\oplus Y_3$ $\oplus Y_4$	X_1 $\oplus X_4$	Y_2	X_3 $\oplus X_4$	Y_1 $\oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

Table 3. Sample Linear Approximations of S-box.

		Output Sum															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I	1	0	0	-2	-2	0	0	-2	+6	+2	+2	0	0	+2	+2	0	0
n	2	0	0	-2	-2	0	0	-2	-2	0	0	+2	+2	0	0	-6	+2
p	3	0	0	0	0	0	0	0	0	+2	-6	-2	-2	+2	+2	-2	-2
u	4	0	+2	0	-2	-2	-4	-2	0	0	-2	0	+2	+2	-4	+2	0
t	5	0	-2	-2	0	-2	0	+4	+2	-2	0	-4	+2	0	-2	-2	0
	6	0	+2	-2	+4	+2	0	0	+2	0	-2	+2	+4	-2	0	0	-2
	7	0	-2	0	+2	+2	-4	+2	0	-2	0	+2	0	+4	+2	0	+2
S	8	0	0	0	0	0	0	0	0	-2	+2	+2	-2	+2	-2	-2	-6
u	9	0	0	-2	-2	0	0	-2	-2	-4	0	-2	+2	0	+4	+2	-2
m	A	0	+4	-2	+2	-4	0	+2	-2	+2	+2	0	0	+2	+2	0	0
	B	0	+4	0	-4	+4	0	+4	0	0	0	0	0	0	0	0	0
	C	0	-2	+4	-2	-2	0	+2	0	+2	0	+2	+4	0	+2	0	-2
	D	0	+2	+2	0	-2	+4	0	+2	-4	-2	+2	0	+2	0	0	+2
	E	0	+2	+2	0	-2	-4	0	+2	-2	0	0	-2	-4	+2	-2	0
	F	0	-2	-4	-2	-2	0	+2	0	0	-2	+4	-2	-2	0	+2	0

Table 4. Linear Approximation Table.

A complete enumeration of all linear approximations of the S-box in our cipher is given in the *linear approximation table* of Table 4. Each element in the table represents the number of matches between the linear equation represented in hexadecimal as "Input Sum" and the sum of the output bits represented in hexadecimal as "Output Sum" minus 8. Hence, dividing an element value by 16 gives the probability bias for the particular linear combination of input and output bits. The hexadecimal value representing a sum, when viewed as a binary value, indicates the variables involved in the sum. For a linear combination of input variables represented as $a_1 \cdot X_1 \oplus a_2 \cdot X_2 \oplus a_3 \cdot X_3 \oplus a_4 \cdot X_4$ where $a_i \in \{0, 1\}$ and "$\cdot$" represents binary AND, the hexadecimal value represents the binary value $a_1 a_2 a_3 a_4$, where a_1 is the most significant bit. Similarly, for a linear combination of output bits $b_1 \cdot Y_1 \oplus b_2 \cdot Y_2 \oplus b_3 \cdot Y_3 \oplus b_4 \cdot Y_4$ where $b_i \in \{0, 1\}$, the hexadecimal value represents the binary vector $b_1 b_2 b_3 b_4$. Hence, the bias of linear equation $X_3 \oplus X_4 = Y_1 \oplus Y_4$ (hex input 3 and hex output 9) is $-\frac{6}{16} = -\frac{3}{8}$ and the probability that the linear equation holds true is given by $\frac{1}{2} - \frac{3}{8} = \frac{1}{8}$.

Some basic properties of the linear approximation table can be noted. For example, the probability that any sum of a non-empty subset of output bits is equal to the sum involving no input bits is exactly 1/2 since any linear combination of output bits must have an equal number of zeros and ones for a bijective S-box. Also, the linear combination involving no output bits will always equal the linear combination of no input bits resulting in a bias of +1/2 and a table value of +8 in the top left corner. Hence, the top row of the table is all zeros, except for the leftmost value. Similarly, the first column is all zeros except for the topmost value. It can also be noted the sum of any row or any column must be either +8 or -8. We leave the proof of this as an exercise for the reader.

3.4 Constructing Linear Approximations for the Complete Cipher

Once the linear approximation information has been compiled for the S-boxes in an SPN, we have the data to proceed with determining linear approximations of the overall cipher of the form of equation (1). This can be achieved by concatenating appropriate linear approximations of S-boxes. By constructing a linear approximation involving plaintext bits and data bits from the output of the second last round of S-boxes, it is possible to attack the cipher by recovering a subset of the subkey bits that follow the last round. We illustrate with an example.

Consider an approximation involving S_{12}, S_{22}, S_{32}, and S_{34} as illustrated in Figure 3. Note that this actually develops an expression for the first 3 rounds of the cipher and not the full 4 rounds. We shall see how this is useful in deriving the subkey bits after the last round in the next section.

We use the following approximations of the S-box:

$S_{12} : X_1 \oplus X_3 \oplus X_4 = Y_2$	with probability 12/16 and bias +1/4
$S_{22} : X_2 = Y_2 \oplus Y_4$	with probability 4/16 and bias -1/4
$S_{32} : X_2 = Y_2 \oplus Y_4$	with probability 4/16 and bias -1/4
$S_{34} : X_2 = Y_2 \oplus Y_4$	with probability 4/16 and bias -1/4

Letting U_i (V_i) represent the 16-bit block of bits at the input (output) of the round i S-boxes and $U_{i,j}$ ($V_{i,j}$) represent the j^{th} bit of block U_i (V_i) (where bits are numbered from 1 to 16 from left to right in the figure of the cipher). Similarly, let K_i represent the subkey block of bits exclusive-ORed at the input to round i, with the exception that K_5 is the key exclusive-ORed at the output of round 4.

Hence, $U_1 = P \oplus K_1$ where P represents the block of 16 plaintext bits and "$\oplus$" represents the bit-wise exclusive-OR. Using the linear approximation of the 1st round, we then have

$$\begin{aligned} V_{1,6} &= U_{1,5} \oplus U_{1,7} \oplus U_{1,8} \\ &= (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8}) \end{aligned} \tag{2}$$

with probability $\frac{3}{4}$. For the approximation in the 2nd round, we have

$$V_{2,6} \oplus V_{2,8} = U_{2,6}$$

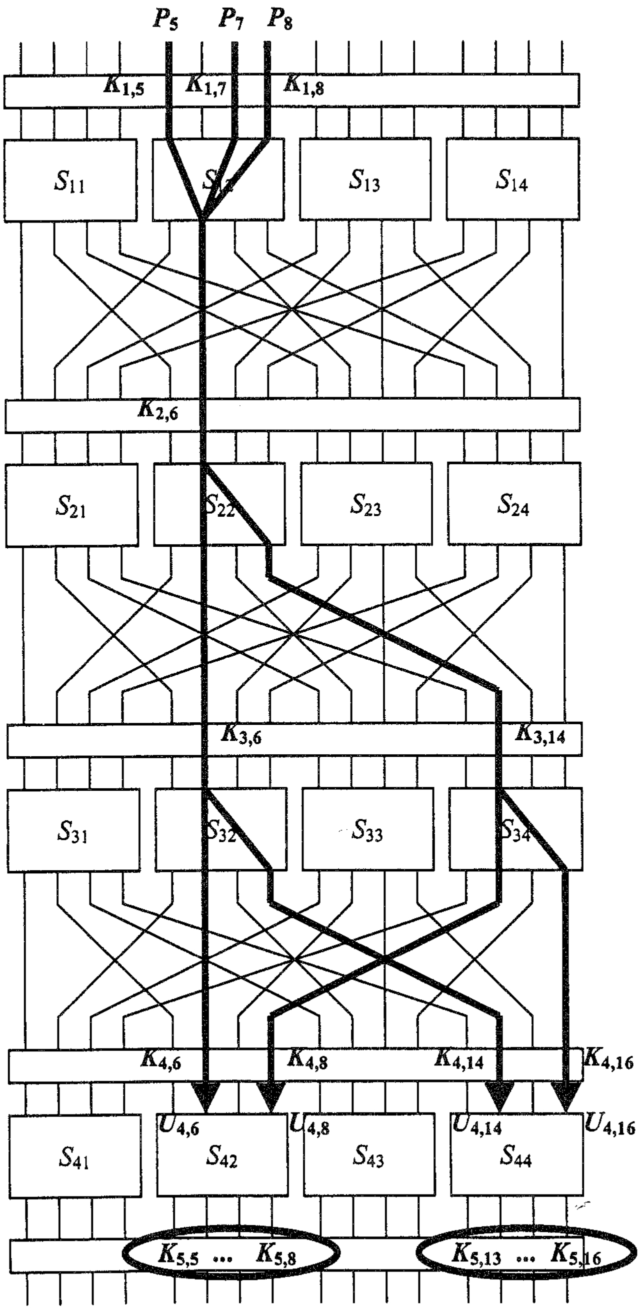

Figure 3. Sample Linear Approximation.

with probability $\frac{1}{4}$. Since $U_{2,6} = V_{1,6} \oplus K_{2,6}$, we can get an approximation of the form

$$V_{2,6} \oplus V_{2,8} = V_{1,6} \oplus V_{2,6}$$

with probability $\frac{1}{4}$ and combining this with (2) which holds with probability of $\frac{3}{4}$ gives

$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} = 0 \qquad (3)$$

which holds with probability of $\frac{1}{2}+2(\frac{3}{4}-\frac{1}{2})(\frac{1}{4}-\frac{1}{2}) = \frac{3}{8}$ (that is, with a bias of $-\frac{1}{8}$) by application of the Piling-Up Lemma. Note that we are using the assumption that the approximations of S-boxes are independent which, although not strictly correct, works well in practice for most ciphers.

For round 3, we note that $V_{3,6} \oplus V_{3,8} = U_{3,6}$ with probability $\frac{1}{4}$ and $V_{3,14} \oplus V_{3,16} = U_{3,14}$ with probability $\frac{1}{4}$. Hence, since $U_{3,6} = V_{2,6} \oplus K_{3,6}$ and $U_{3,14} = V_{2,8} \oplus K_{3,14}$,

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} = 0 \qquad (4)$$

with probability of $\frac{1}{2} + 2(\frac{1}{4} - \frac{1}{2})^2 = \frac{5}{8}$ (that is, with a bias of $+\frac{1}{8}$). Again, we have applied the Piling-Up Lemma.

Now combining (3) and (4), to incorporate all four S-box approximations, we get

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} = 0.$$

Noting that $U_{4,6} = V_{3,6} \oplus K_{4,6}$, $U_{4,8} = V_{3,14} \oplus K_{4,8}$, $U_{4,14} = V_{3,8} \oplus K_{4,14}$, and $U_{4,16} = V_{3,16} \oplus K_{4,16}$, we can then write

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0.$$

where

$$\Sigma_K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16}$$

and $\sum_K$ is fixed at either 0 or 1 depending on the key of the cipher. By application of the Piling-Up Lemma, the above expression holds with probability $\frac{1}{2} + 2^3(\frac{3}{4} - \frac{1}{2})(\frac{1}{4} - \frac{1}{2})^3 = \frac{15}{32}$ (that is, with a bias of $-\frac{1}{32}$).

Now since $\sum_K$ is fixed, we note that

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0 \qquad (5)$$

must hold with a probability of either $\frac{15}{32}$ or $(1 - \frac{15}{32}) = \frac{17}{32}$, depending on whether $\sum_K = 0$ or 1, respectively. In other words, we now have a linear approximation of the first three rounds of the cipher with a bias of magnitude $\frac{1}{32}$. We must now discuss how such a bias can be used to determine some of the key bits.

3.5 Extracting Key Bits

Once an $R-1$ round linear approximation is discovered for a cipher of R rounds with a suitably large enough linear probability bias, it is conceivable to attack the cipher by recovering bits of the last subkey. In the case of our example cipher, it is possible to extract bits from subkey K_5 given a 3 round linear approximation. We shall refer to the bits to be recovered from the last subkey as the *target partial subkey*. Specifically, the target partial subkey bits are the bits from the last subkey associated with the S-boxes in the last round influenced by the data bits involved in the linear approximation. A general algorithm for determining bits from the last subkey is given below:

1. Determine a good linear approximation of $R-1$ rounds of the cipher.
2. Collect a large number, N_L, of known plaintext/ciphertext samples.
3. Initialize counts for all target partial subkey values to zero.
4. For all target partial subkey values:

   For each ciphertext:

   - Partially decrypt the last round of the cipher.
   - If the linear approximation for the input to the last round holds true, increment the count for the target partial subkey value.
5. The correct value for the target partial subkey is assumed to be the target partial subkey value with the count which is furthest away from $N_L/2$.

The process followed involves partially decrypting the last round of the cipher. Specifically, for all possible values of the target partial subkey, the corresponding ciphertext bits are exclusive-ORed with the bits of the target partial subkey and the result is run backwards through the corresponding S-boxes. This is done for all known plaintext/ciphertext samples and a count is kept for each value of the target partial subkey. The count for a particular target partial subkey value is incremented when the linear expression holds true for the bits into the last round's S-boxes (determined by the partial decryption) and the known plaintext bits. The target partial subkey value which has the count which differs the greatest from half the number of plaintext/ciphertext samples is assumed to represent the correct values of the target partial subkey bits. This works because it is assumed that the correct partial subkey value will result in the linear approximation holding with a probability significantly different from $\frac{1}{2}$. (Whether it is above or below $\frac{1}{2}$ depends on whether a linear or affine expression is the best approximation and this depends on the unknown values of the subkey bits implicitly involved in the linear expression.) An incorrect subkey is assumed to result in a relatively random guess at the bits entering the S-boxes of the last round and as a result, the linear expression will hold with a probability close to $\frac{1}{2}$.

Let's now put this into the context of our example. The linear expression of (5) affects the inputs to S-boxes S_{42} and S_{44} in the last round. For each plaintext/ciphertext sample, we would try all 256 values for the target partial subkey $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}]$. For each partial subkey value, we would increment the count whenever equation (5) holds true, where we determine the value of $[U_{4,5} \ldots U_{4,8}, U_{4,13} \ldots U_{4,16}]$ by running the data backwards through the target partial subkey and S-boxes S_{42} and S_{44}. The count which deviates the largest from half of the number of plaintext/ciphertext samples is assumed to be the correct value. Whether the deviation is positive or negative will depend on the values of the subkey bits involved in $\sum_K$. When $\sum_K = 0$, the approximation of (5) will serve as the estimate with probability less than $\frac{1}{2}$ and when $\sum_K = 1$, (5) will hold with a probability greater than $\frac{1}{2}$.

We have simulated attacking our basic cipher by generating 10000 known plaintext/ciphertext values and following the cryptanalytic process described for partial subkey values $[K_{5,5} \ldots K_{5,8}] = [0010]$ (hex 2) and $[K_{5,13} \ldots K_{5,16}] = [0100]$ (hex 4). As expected, the count which differed the most from 5000 corresponded to target partial subkey value $[2, 4]_{\text{hex}}$, confirming that the attack has successfully derived the subkey bits.

Table 5 highlights a partial summary of the data derived from the subkey counts. (The complete data involves 256 data entries, one for each target partial subkey value.) The values in the table indicate the bias magnitude derived from

$$|\text{bias}| = \frac{|\text{count} - 5000|}{10000}$$

where the count is the count corresponding to the particular partial subkey value.

As can be seen from the partial results in the table, the largest bias occurs for partial subkey value $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}] = [2, 4]_{\text{hex}}$ and this observation was, in fact, found to be true over the complete set of partial subkey values.

partial subkey $[K_{5,5}\ldots K_{5,8}, K_{5,13}\ldots K_{5,16}]$	$\|$bias$\|$	partial subkey $[K_{5,5}\ldots K_{5,8}, K_{5,13}\ldots K_{5,16}]$	$\|$bias$\|$
1 C	0.0031	2 A	0.0044
1 D	0.0078	2 B	0.0186
1 E	0.0071	2 C	0.0094
1 F	0.0170	2 D	0.0053
2 0	0.0025	2 E	0.0062
2 1	0.0220	2 F	0.0133
2 2	0.0211	3 0	0.0027
2 3	0.0064	3 1	0.0050
2 4	**0.0336**	3 2	0.0075
2 5	0.0106	3 3	0.0162
2 6	0.0096	3 4	0.0218
2 7	0.0074	3 5	0.0052
2 8	0.0224	3 6	0.0056
2 9	0.0054	3 7	0.0048

Table 5. Experimental Results for Linear Attack.

The experimentally determined bias value of 0.0336 is very close to the expected value of $\frac{1}{32} = 0.03125$. Note that, although the correct target partial subkey has clearly the highest bias, other large bias values occur indicating that the examination of incorrect target partial subkeys is not precisely equivalent to comparing random data to a linear expression (where the bias could be expected to be very close to zero). Inconsistencies in the experimental biases can occur for several reasons including the S-box properties influencing the partial decryption for different partial subkey values, the imprecision of the independence assumption required for use in the Piling-Up Lemma, and the influence of *linear hulls* (to be discussed in the next section).

3.6 Complexity of Attack

We refer to the S-boxes involved in the linear approximation as *active* S-boxes. In Figure 3, the four S-boxes in rounds 1 to 3 influenced by the highlighted lines are active. The probability that a linear expression holds true is related to the linear probability bias in the active S-boxes and the number of active S-boxes. In general, the larger the magnitude of the bias in the S-boxes, the larger the magnitude of the bias of the overall expression. Also, the fewer active S-boxes, the larger the magnitude of the overall linear expression bias.

Let ϵ represent the bias from $\frac{1}{2}$ of the probability that the linear expression for the complete cipher holds. In his paper, Matsui shows that the number of known plaintexts required in the attack is proportional to ϵ^{-2} and, letting N_L represent the number of known plaintexts required, it is reasonable to approximate N_L by

$$N_L \approx \frac{1}{\epsilon^2}.$$

In practice, it is generally reasonable to expect some small multiple of ϵ^{-2} known plaintexts are required. Although strictly speaking, the complexity of the cryptanalysis could be characterized in both time and space (or memory) domains, we refer to the data required to mount the attack when considering the complexity of the cryptanalysis. That is, we assume that if we are able to acquire N_L plaintexts, we are able to process them.

Since the bias is derived using the Piling-Up Lemma where each term in the product refers to an S-box approximation, it is easy to see that the bias is dependent on the biases of the S-box linear approximations and the number of active S-boxes involved. General approaches to providing security against linear cryptanalysis have focused on optimizing the S-boxes (i.e., minimizing the largest bias) and finding structures to maximize the number of active S-boxes. The design principles of Rijndael are an excellent example of such an approach.

It must be cautioned, however, the concept of a "proof" of security to linear cryptanalysis cannot be premised on the nonexistence of highly likely linear approximations. The computation of the probability of such linear approximations is based on the assumption that each S-box approximation is independent (so that the Piling-Up Lemma can be used) and on the assumption that one linear approximation scenario is sufficient to determine the best linear expression between plaintext bits and data bits at the input to the last round. The reality is that the S-box approximations are not independent and this can have significant impact on the computation of the probability. Also, linear approximation scenarios involving the same plaintext and last round input bits but different intermediate bits and even different sets of active S-boxes can combine to give a linear probability higher than that predicted by one linear approximation scenario. This concept is referred to as a *linear hull* [21]. Most notably for example, a number of linear approximation scenarios may have very small biases and on their own seem to imply that a cipher might be immune to a linear attack. However, when these scenarios are combined, the resulting linear expression of plaintext and last round input bits might have a very high bias. Nevertheless, the approach outlined in this paper, tends to work well for many ciphers because the independence assumption is a reasonable approximation and when one linear approximation scenario of a particular set of active S-boxes has a high bias, it tends to dominate the linear hull.

4 DIFFERENTIAL CRYPTANALYSIS

In this section, we now turn our focus to the application of differential cryptanalysis to the basic SPN cipher.

4.1 Overview of Basic Attack

Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher. For example, consider a system with input $X = [X_1, X_2, \ldots, X_n]$ and output $Y = [Y_1, Y_2, \ldots, Y_n]$. Let two inputs to the system be X' and X'' with the corresponding outputs Y' and Y'', respectively. The input difference is given by $\Delta X = X' \oplus X''$ where "$\oplus$" represents a bit-wise exclusive-OR of the n-bit vectors and, hence,

$$\Delta X = [\Delta X_1, \Delta X_2, \ldots, \Delta X_n]$$

where $\Delta X_i = X_i' \oplus X_i''$ with X_i' and X_i'' representing the i^{th} bit of X' and X'', respectively.

Similarly, $\Delta Y = Y' \oplus Y''$ is the output difference and

$$\Delta Y = [\Delta Y_1, \Delta Y_2, \ldots, \Delta Y_n]$$

where $\Delta Y_i = Y_i' \oplus Y_i''$.

In an ideally randomizing cipher, the probability that a particular output difference ΔY occurs, given a particular input difference ΔX, is $\frac{1}{2^n}$ where n is the number of bits of X. Differential cryptanalysis seeks to exploit a scenario where a particular ΔY occurs, given a particular input difference ΔX, with a very high probability p_D (i.e., much greater than $\frac{1}{2^n}$). The pair $(\Delta X, \Delta Y)$ is referred to as a *differential*.

Differential cryptanalysis is a chosen plaintext attack, meaning that the attacker is able to select inputs and examine outputs in an attempt to derive the key. For differential cryptanalysis, the attacker will select pairs of inputs, X' and X'', to satisfy a particular ΔX, knowing that for that ΔX value, a particular ΔY value occurs with high probability.

In this paper, we investigate the construction of a differential $(\Delta X, \Delta Y)$ involving plaintext bits as represented by X and the input to the last round of the cipher as represented by Y. We shall do this by examining highly likely *differential characteristics* where a differential characteristic is a sequence of input and output differences to the rounds so that the output difference from one round corresponds to the input difference for the next round. Using the highly likely differential characteristic gives us the opportunity to exploit information coming into the last round of the cipher to derive bits from the last layer of subkeys.

As with linear cryptanalysis, to construct highly likely differential characteristics, we examine the properties of individual S-boxes and use these properties to determine the complete differential characteristic. Specifically, we consider the input and output differences of the S-boxes in order to determine a high probability difference pair. Combining S-box difference pairs from round to round so that the nonzero output difference bits from one round correspond to the non-zero input difference bits of the next round, enables us to find a high probability differential consisting of the plaintext difference and the difference of the input to the last round. The subkey bits of the cipher end up disappearing from the difference expression because they are involved in both data sets and, hence, considering their influence on the difference involves exclusive-ORing subkey bits with themselves, the result of which is zero.

4.2 Analyzing the Cipher Components

We examine now the difference pairs of an S-box. Consider the 4 × 4 S-box representation of Figure 2 with input $X = [X_1, X_2, X_3, X_4]$ and output $Y = [Y_1, Y_2, Y_3, Y_4]$. All difference pairs of an S-box, $(\Delta X, \Delta Y)$, can be examined and the probability of ΔY given ΔX can be derived by considering input pairs (X', X'') such that $X' \oplus X'' = \Delta X$. Since the ordering of the pair is not relevant, for a 4 × 4 S-box we need only consider all 16 values for X' and then the value of ΔX constrains the value of X'' to be $X'' = X' \oplus \Delta X$.

Considering the S-box of our cipher given in Section 2, we can derive the resulting values of ΔY for each input pair $(X', X'' = X' \oplus \Delta X)$. For example, the binary values of X, Y, and the corresponding values for ΔY for given input pairs $(X, X \oplus \Delta X)$ are presented in Table 6 for ΔX values of 1011, 1000, and 0100. The last three columns of the table represent ΔY values for the value of X (as given by the row) and the particular ΔX value for each column. From the table, we can see that the number of occurrences of $\Delta Y = 0010$ for $\Delta X = 1011$ is 8 out of 16 possible values (i.e., a probability of $\frac{8}{16}$); the number of occurrences of $\Delta Y = 1011$ given $\Delta X = 1000$ is 4 out of 16; the number of occurrences of $\Delta Y = 1010$ given $\Delta X = 0100$ is 0 out of 16. If the S-box could be "ideal", the number of occurrences of difference pair values would all be 1 to give a probability of $\frac{1}{16}$ of the occurrence of a particular ΔY value given ΔX . (It turns out that such an "ideal" S-box is not mathematically possible.)

We can tabularize the complete data for an S-box in a *difference distribution table* in which the rows represent ΔX values (in hexadecimal) and the columns

X	Y	ΔY		
		$\Delta X = 1011$	$\Delta X = 1000$	$\Delta X = 0100$
0000	1110	0010	1101	1100
0001	0100	0010	1110	1011
0010	1101	0111	0101	0110
0011	0001	0010	1011	1001
0100	0010	0101	0111	1100
0101	1111	1111	0110	1011
0110	1011	0010	1011	0110
0111	1000	1101	1111	1001
1000	0011	0010	1101	0110
1001	1010	0111	1110	0011
1010	0110	0010	0101	0110
1011	1100	0010	1011	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

Table 6. Sample Difference Pairs of the S-box.

		Output Difference															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
I	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n	1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
p	2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
u	3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
t	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
D	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
i	7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
f	8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
f	9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
e	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
r	B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
e	C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
n	D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
c	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
e	F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Table 7. Difference Distribution Table.

represent ΔY values (in hexadecimal). The difference distribution table for the S-box of Table 1 is given in Table 7. Each element of the table represents the number of occurrences of the corresponding output difference ΔY value given the input difference ΔX. Note that, besides the special case of ($\Delta X = 0$, $\Delta Y = 0$), the largest value in the table is 8, corresponding to ΔX = B and $\Delta Y = 2$. Hence, the probability that $\Delta Y = 2$ given an arbitrary pair of input values that satisfy ΔX = B is $\frac{8}{16}$. The smallest value in the table is 0 and occurs for many difference pairs. In this case, the probability of the ΔY value occurring given the ΔX value is 0.

There are several general properties of the difference distribution table that should be mentioned. First, it should be noted that the sum of all elements in a row is $2^n = 16$; similarly the sum of any column is $2^n = 16$. Also, all element values are even: this results because a pair of input (or output) values represented as (X', X'') has the same ΔX value as the pair (X'', X') since $\Delta X = X' \oplus X'' = X'' \oplus X'$. As well, the input difference of $\Delta X = 0$ must lead to an output difference of $\Delta Y = 0$ for the one-to-one mapping of the S-box. Hence, the top left corner of the table has a value of $2^n = 16$ and all other values in the first row and first column are 0. Finally, if we could construct an ideal S-box, which gives no differential information about the output given the input value, the S-box would have all elements in the table equal to 1 and the probability of occurrence of a particular value for ΔY given a particular value of ΔX would be $\frac{1}{2^n} = \frac{1}{16}$. However, as the properties discussed above must hold, this is clearly not achievable.

Before we proceed to discuss the combining of S-box difference pairs to derive a differential characteristic and an estimate of a good differential to use in the attack, we must discuss the influence of the key on the S-box differential. Consider Figure 4. The input to the "unkeyed" S-box is X and the output Y. However, in the cipher structure we must consider the keys applied at the input of each S-box. In this case, if we let the input to the "keyed" S-box be $W = [W_1, W_2, W_3, W_4]$, we can consider the input difference to the keyed S-box to be

$$\Delta W = [W_1' \oplus W_1'', W_2' \oplus W_2'', W_3' \oplus W_3'', W_4' \oplus W_4'']$$

where $W' = [W_1', W_2', W_3', W_4']$ and $W'' = [W_1'', W_2'', W_3'', W_4'']$ represent the two input values.

Since the key bits remain the same for both W' and W'',

$$\begin{aligned} \Delta W_i &= W_i' \oplus W_i'' = (X_i' \oplus K_i) \oplus (X_i'' \oplus K_i) \\ &= X_i' \oplus X_i'' = \Delta X_i \end{aligned}$$

since $K_i \oplus K_i = 0$. Hence, the key bits have no influence on the input difference value and can be ignored. In other words, the keyed S-box has the same difference distribution table as the unkeyed S-box.

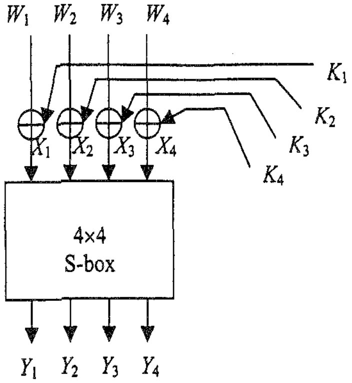

Figure 4. Keyed S-box.

4.3 Constructing Differential Characteristics

Once the differential information has been compiled for the S-boxes in an SPN, we have the data to proceed with determining a useful differential characteristic of the overall cipher. This can be done by concatenating appropriate difference pairs of S-boxes. By constructing a differential characteristic of certain S-box difference pairs in each round, such that a differential involves plaintexts bits and data bits to the input of the last round of S-boxes, it is possible to attack the cipher by recovering a subset of the subkey bits following the last round. We illustrate the construction of a differential characteristic with an example.

Consider a differential characteristic involving S_{12}, S_{23}, S_{32}, and S_{33}. As was the case for linear cryptanalysis, it is useful to visualize the differential characteristic in the form of a diagram as shown in Figure 5. The diagram illustrates the influence of non-zero differences in bits as they traverse the network, highlighting the S-boxes that may be considered as *active* (i.e., for which there is a non-zero differential). Note that this develops a differential characteristic for the first 3 rounds of the cipher and not the full 4 rounds. We shall see how this is useful in deriving bits from the last subkey in the next section.

We use the following difference pairs of the S-box:

$$
\begin{array}{ll}
S_{12} : \Delta X = \mathrm{B} \rightarrow \Delta Y = 2 & \text{with probability } \frac{8}{16} \\
S_{23} : \Delta X = 4 \rightarrow \Delta Y = 6 & \text{with probability } \frac{6}{16} \\
S_{32} : \Delta X = 2 \rightarrow \Delta Y = 5 & \text{with probability } \frac{6}{16} \\
S_{33} : \Delta X = 2 \rightarrow \Delta Y = 5 & \text{with probability } \frac{6}{16}
\end{array}
$$

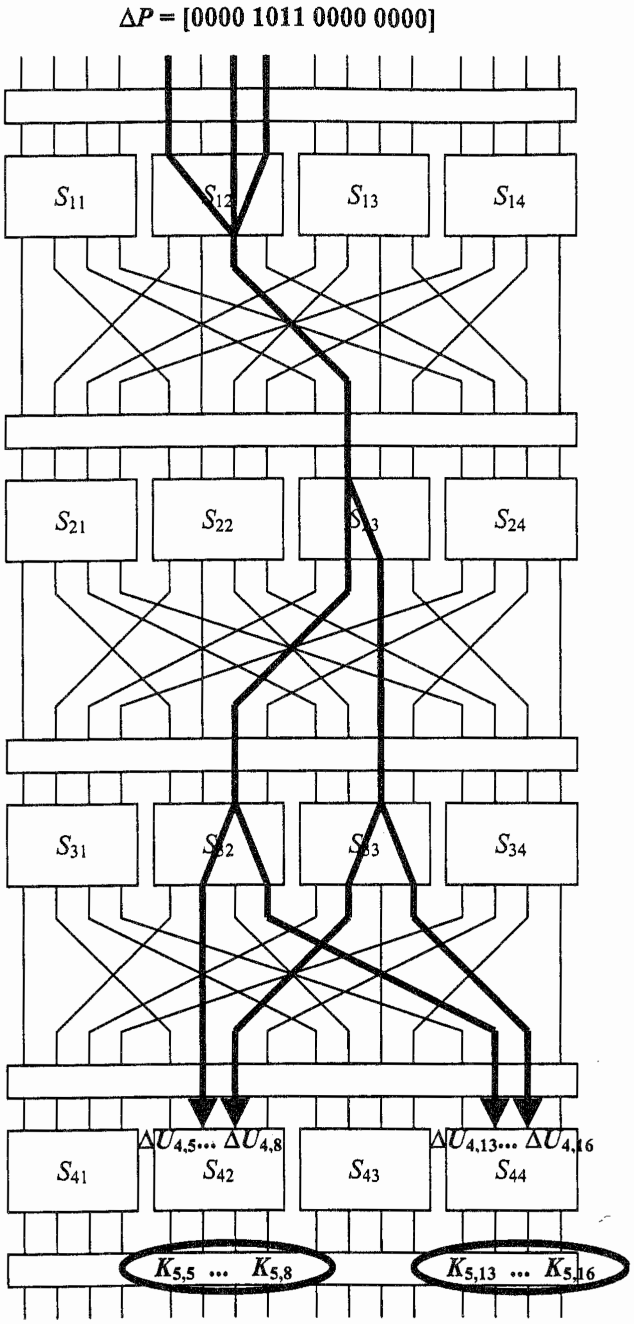

Figure 5. Sample Differential Characteristic.

All other S-boxes will have zero input difference and consequently zero output difference.

The input difference to the cipher is equivalent to the input difference to the first round and is given by

$$\Delta P = \Delta U_1 = [0000\ 1011\ 0000\ 0000]$$

where again, as with our presentation of linear cryptanalysis in Section 3, we are using U_i to represent the input to the i^{th} round S-boxes and V_i to represent the output of the i^{th} round S-boxes. Hence, ΔU_i and ΔV_i represent the corresponding differences. As a result,

$$\Delta V_1 = [0000\ 0010\ 0000\ 0000]$$

considering the difference pair for S_{12} listed above and following the round 1 permutation

$$\Delta U_2 = [0000\ 0000\ 0100\ 0000]$$

with probability of $\frac{8}{16} = \frac{1}{2}$ given the plaintext difference ΔP

Now the second round differential using the difference pair for S_{23} results in

$$\Delta V_2 = [0000\ 0000\ 0110\ 0000]$$

and the permutation of round 2 gives

$$\Delta U_3 = [0000\ 0010\ 0010\ 0000]$$

with probability $\frac{6}{16}$ given ΔU_2 and a probability of $\frac{8}{16} \times \frac{6}{16} = \frac{3}{16}$ given ΔP. In determining the probability given plaintext difference ΔP, we have assumed that the differential of the first round is independent of the differential of the 2nd round and, hence, the probability of both occurring is determined by the product of the probabilities.

Subsequently, we can use the differences for the S-boxes of the third round, S_{32} and S_{33}, and the permutation of the third round to arrive at

$$\Delta V_3 = [0000\ 0101\ 0101\ 0000]$$

and

$$\Delta U_4 = [0000\ 0110\ 0000\ 0110] \qquad (6)$$

with a probability of $\left(\frac{6}{16}\right)^2$ given ΔU_3 and, hence, a probability of $\frac{8}{16} \times \frac{6}{16} \times \left(\frac{6}{16}\right)^2 = \frac{27}{1024}$ given plaintext difference ΔP, where again we have assumed independence between the difference pairs of S-boxes in all rounds.

During the cryptanalysis process, many pairs of plaintexts for which $\Delta P =$ [0000 1011 0000 0000] will be encrypted. With high probability, $\frac{27}{1024}$, the differential characteristic illustrated will occur. We term such pairs for ΔP as *right pairs*. Plaintext difference pairs for which the characteristic does not occur are referred to as *wrong pairs*.

4.4 Extracting Key Bits

Once an $R-1$ round differential characteristic is discovered for a cipher of R rounds with a suitably large enough probability, it is conceivable to attack the cipher by recovering bits from the last subkey. In the case of our example cipher, it is possible to extract bits from subkey K_5. The process followed involves partially decrypting the last round of the cipher and examining the input to the last round to determine if a right pair has probably occurred. We shall refer to the subkey bits following the last round at the output of S-boxes in the last round influenced by non-zero differences in the differential output as the *target partial subkey*. A partial decryption of the last round would involve, for all S-boxes in the last round influenced by non-zero differences in the differential, the exclusive-OR of the ciphertext with the target partial subkey bits and running the data backwards through the S-boxes, where all possible values for the target subkey bits would be tried. A general algorithm for determining bits from the last subkey is given below:

1. Determine a high probability differential characteristic of $R-1$ rounds of the cipher.
2. Collect a large number, N_D, of plaintext/ciphertext sample pairs where the plaintext pairs are chosen with the appropriate difference for the characteristic.
3. Initialize counts for all target partial subkey values to zero.
4. For all target partial subkey values:

   For each ciphertext pair:

   - Partially decrypt the last round of the cipher.
   - If the difference to the last round of the cipher is consistent with the characteristic, increment the count for the target partial subkey value.
5. The correct value for the target partial subkey is assumed to be the target partial subkey value with the largest count.

A partial decryption is executed for each pair of ciphertexts corresponding to the pairs of plaintexts used to generate the input difference ΔP for all possible target partial subkey values. A count is kept for each value of the target partial subkey value. The count is incremented when the difference for the input to the last round corresponds to the value expected from the differential characteristic. The partial subkey value which has the largest count is assumed to indicate the correct values of the subkey bits. This works because it is assumed that the correct partial subkey value will result in the difference to the last round being frequently as expected from the characterstic (i.e., the occurrence of a right pair) since the characteristic has a high probability of occurring. (When a wrong pair has occurred, even with the partial decryption with the correct subkey, the count for the correct subkey will likely not be incremented.) An incorrect subkey is assumed to result in a relatively random guess at the bits entering the S-boxes of the last round and, as a result, the difference will be as expected from the characteristic with a very low probability.

Considering the attack on our example cipher, the differential characteristic affects the inputs to S-boxes S_{42} and S_{44} in the last round. For each ciphertext pair, we would try all 256 values for $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}]$. For each partial subkey value, we would increment the count whenever the input difference to the final round determined by the partial decryption is the same as (6), where we determine the value of $[\Delta U_{4,5} \ldots \Delta U_{4,8}, \Delta U_{4,13} \ldots \Delta U_{4,16}]$ by running the data backwards through the partial subkey and S-boxes S_{42} and S_{44}. For each partial subkey value, the count represents the number of occurrences of differences that are consistent with right pairs (assuming that the partial subkey is the correct value). The count that is the largest is taken to be the correct value since we assume that we are observing the high probability occurrence of the right pair.

Note that it is not necessary to execute the partial decryption for every ciphertext pair. Since the input difference to the last round only influences 2 S-boxes, when the characteristic has occurred (i.e., for right pairs), the ciphertext bit differences corresponding to S-boxes S_{41} and S_{43} must be zero. Hence, we can *filter* out many wrong pairs by discarding ciphertext pairs for which zeros do not appear in the appropriate sub-blocks of the ciphertext difference. In these cases, since the ciphertext pair cannot correspond to a right pair, it is not necessary to examine $[\Delta U_{4,5} \ldots \Delta U_{4,8}, \Delta U_{4,13} \ldots \Delta U_{4,16}]$.

We have simulated attacking our basic cipher keyed using randomly generated subkeys by generating 5000 chosen plaintext/ciphertext pairs (i.e., 10000 encryptions with plaintext pairs satisfying $\Delta P = [0000\ 1011\ 0000\ 0000]$) and following the process described above. The correct target partial subkey value was $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}] = [0010, 0100] = [2, 4]_{\text{hex}}$. As expected, the largest count was observed for partial subkey value $[2,4]_{\text{hex}}$, confirming that the attack successfully derived the subkey bits. Table 8 highlights a partial summary of the data derived from the subkey counts. (The complete data involves 256 data entries, one for each partial subkey value.) The values in the table indicate the estimated probability of the occurrence of right pairs for the candidate partial subkey derived from

$$\text{prob} = \frac{\text{count}}{5000}$$

where the count is the count corresponding to the particular partial subkey value.

As can be seen from the sample results of the table, the largest probability occurs for partial subkey value $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}] = [2,4]_{\text{hex}}$ and this observation was, in fact, found to be true over the complete set of partial subkey values.

partial subkey $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}]$	prob	partial subkey $[K_{5,5} \ldots K_{5,8}, K_{5,13} \ldots K_{5,16}]$	prob
1 C	0.0000	2 A	0.0032
1 D	0.0000	2 B	0.0022
1 E	0.0000	2 C	0.0000
1 F	0.0000	2 D	0.0000
2 0	0.0000	2 E	0.0000
2 1	0.0136	2 F	0.0000
2 2	0.0068	3 0	0.0004
2 3	0.0068	3 1	0.0000
2 4	**0.0244**	3 2	0.0004
2 5	0.0000	3 3	0.0004
2 6	0.0068	3 4	0.0000
2 7	0.0068	3 5	0.0004
2 8	0.0030	3 6	0.0000
2 9	0.0024	3 7	0.0008

Table 8. Experimental Results for Differential Attack.

In our example, we would expect the probability of the occurrence of the right pair to be $p_D = \frac{27}{1024} = 0.0264$ and we found experimentally the probability for the correct subkey value $[2,4]_{\text{hex}}$ gave a probability of 0.0244. Note that sometimes other large count values occur for incorrect target partial subkeys. This indicates that the examination of incorrect target partial subkeys is not precisely equivalent to comparing random differences to the expected differential value. There are several factors which influence the counts to be different then our theorized expectations including the S-box properties influencing the partial decryption for different partial subkeys, the imprecision of the independence assumption required for determination of the characteristic probability, and the concept that *differentials* are composed of multiple differential characteristics (to be discussed in the next section).

4.5 Complexity of the Attack

For differential cryptanalysis, we refer to the S-boxes involved in a characteristic which have a non-zero input difference (and hence a non-zero output difference) as *active* S-boxes. In general, the larger the differential probabilities of the active S-boxes, the larger the characteristic probability for the complete cipher. Also, the fewer active S-boxes, the larger the characteristic probability. As with linear cryptanalysis, we refer to the data required to mount the attack when considering the complexity of the cryptanalysis. That is, we assume that if we are able to acquire N_D plaintext pairs, we are able to process them.

In general it is very complex to determine exactly the number of chosen plaintext pairs required to mount the attack. However, it can be shown that a good rule-of-thumb for the number of chosen plaintext pairs, N_D, required to distinguish right pairs when trying subkey candidates is

$$N_D \approx c/p_D \tag{7}$$

where p_D is the differential characteristic probability for the $R-1$ rounds of the R-round cipher and c is a small constant. Assuming that the occurrences of difference pairs in each active S-box are independent, the differential characteristic probability is given by

$$p_D = \prod_{i=1}^{\gamma} \beta_i \tag{8}$$

where the number of active S-boxes is represented by γ and the occurrence of the particular difference pair in the i^{th} active S-box of the characteristic has a probability represented by β_i.

It is not difficult to rationalize that (7) is true. It simply indicates that a few occurrences of the right pair are enough to give a count to the correct target partial subkey value that is significantly greater than the counts for the incorrect target partial subkey values. Since a right pair is expected to occur for about every $1/p_D$ pairs examined, in practice, it is generally reasonable to use some small multiple of $1/p_D$ chosen plaintext pairs to successfully mount the attack.

Approaches to providing resistance to differential cryptanalysis have focused on the S-box properties (i.e., minimizing the difference pair probability of an S-box) and finding structures to maximize the number of active S-boxes. Rijndael is a good example of a cipher designed to provide high resistance to differential cryptanalysis.

As with linear cryptanalysis, caution must be exercised in "proving" immunity to differential cryptanalysis. The computation of the differential characteristic probability is premised on the independence of the S-boxes involved in the characteristic and, in a real cipher, there is a dependence between the data entering different S-boxes. Hence, the probability p_D is an estimate only. In practice, in many ciphers it has proven to be reasonably accurate.

Most importantly, different differential characteristics with the same input difference and output difference (i.e., the same differential) can combine to imply a probability for the differential that is larger than is implied by the consideration of one differential characteristic alone [15]. (This is analogous to the concept of linear hulls.) In order to prove security to differential cryptanalysis, it is necessary to prove that the probability of all differentials are below some acceptable threshold, not just that the probability of all differential characteristics are below some acceptable threshold. For many ciphers, though, it is a reasonable assumption that, when a differential characteristic has a high probability, it dominates the occurrence of a differential and the probability of the characteristic gives a good approximation of the differential probability.

5 ADVANCED CONCEPTS

Several extensions and modifications to the basic attacks of linear and differential cryptanalysis have been proposed and analyzed since the original presentation of the attacks. We do not present these advanced concepts and analyses in detail here, but encourage the reader to pursue these concepts further. Note the papers cited in this section represent a small sampling of work built on the two attacks.

We have mentioned, for example, the concepts of linear hulls [21] and differentials [15]: both concepts are integral to understanding the nature of provable security to the two cryptanalysis methods (an elusive goal!). There have been discussions of the similarities of concepts between the two attacks [3, 5] and the analysis of the combination of the attacks into what is referred to as linear-differential cryptanalysis [9].

Several refinements to the cryptanalyses have attempted to improve the attacks for some circumstances. Truncated differential cryptanalysis [12] proposes the exploitation of differences at the cipher output where only some of the ciphertext bits have their differences predicted. Higher order differential cryptanalysis [12] attempts to exploit higher order differentials and is applicable to ciphers where the ciphertext bits are represented as functions of low nonlinear order.

Impossible differential cryptanalysis [4] uses the non-existence of differences to derive cipher subkey bits, as opposed to the existence of highly likely differences that are exploited in normal differential cryptanalysis. Also, it should be noted that, in general, in differential cryptanalysis, differences need not be based on bit-wise exclusive-OR but may be a difference of another form, such as a difference as in the subtraction of one word of size n from another modulo 2^n [15]. Extensions to linear cryptanalysis have included the utilization of multiple linear approximations [23] and the use of nonlinear approximations in combination with linear cryptanalysis [13].

Many papers in recent years have discussed the application of linear and differential cryptanalysis to ciphers proposed before the existence of the attacks was known. As well, many techniques in cipher design have been proposed to make the application of the attacks difficult, focusing on the constructions of cipher components such as S-boxes [22, 10] and the interconnection between layers of S-boxes [10, 7, 24]. As a result, the attacks and their extensions are now very well understood and proposals such as Rijndael [6] have been especially constructed with security against the attacks in mind.

Finally, we note that our presentation of the attacks does not discuss the method for determining the best linear approxmation and differential characteristic. However, this is discussed, for example, in [18].

6 CONCLUSION

In this paper, we have strived to present the fundamental concepts of linear and differential cryptanalysis as applied to a basic cipher. This cipher is a basic Substitution-Permutation Network and is not of a realistic scale to be used as a practical cipher. However, the structure is useful in examining the applicability of the attacks and this example cipher has formed the cornerstone for the explanation of the two attacks.

REFERENCES

1. Biham, E. and A. Shamir. 1991. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*. 4(1): 3-72.

2. Biham, E. and A. Shamir. 1993. *Differential Cryptanalysis of the Data Encryption Standard*. New York: Springer-Verlag.

3. Biham, E. 1995. On Matsui's Linear Cryptanalysis. In *Advances in Cryptology - EUROCRYPT '94 (Lecture Notes in Computer Science No. 950)*. New York: Springer-Verlag. 341-355.

4. Biham, E., A. Biryukov, and A. Shamir. 1999. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In *Advances in Cryptology - EUROCRYPT '99 (Lecture Notes in Computer Science No. 1592).* New York: Springer-Verlag. 12-23.

5. Chabaud, F. and S. Vaudenay. 1995. Links Between Differential and Linear Cryptanalysis. In *Advances in Cryptology - EUROCRYPT '94 (Lecture Notes in Computer Science No. 950).* New York: Springer-Verlag. 356-365.

6. Daemen, J. and V. Rjimen. 2002. *The Design of Rijndael: AES-The Advanced Encryption Standard.* New York: Springer-Verlag.

7. De Win, E., A. Bosselaers, B. Preneel, J. Daemen, and V. Rijmen. 1996. The Cipher SHARK. In *Fast Software Encryption (Lecture Notes in Computer Science No. 1039).* New York: Springer-Verlag. 99-112.

8. Feistel, H. 1973. Cryptography and Computer Privacy. *Scientific American.* 228(5): 15-23.

9. Hellman, M. and S. Langford. 1994. Differential-Linear Cryptanalysis. In *Advances in Cryptology - CRYPTO '94 (Lecture Notes in Computer Science No. 839).* New York: Springer-Verlag. 7-25.

10. Heys, H. M. and S. E. Tavares. 1996. Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis. *Journal of Cryptology.* 9(1): 1-19.

11. Keliher, L. Unpublished. Linear and Differential Cryptanalysis of SPNs.

12. Knudsen, L. R. 1995. Truncated and Higher Order Differentials. In *Fast Software Encryption (Lecture Notes in Computer Science No. 1008).* New York: Springer-Verlag. 196-211.

13. Knudsen, L. and M. J. B. Robshaw. 1996. Nonlinear Approximations in Linear Cryptanalysis. In *Advances in Cryptology - EUROCRYPT '96 (Lecture Notes in Computer Science No. 1070).* New York: Springer-Verlag. 224-236.

14. Knudsen, L. 1998. Block Ciphers: A Survey. In *State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptography (Lecture Notes in Computer Science No. 1528).* New York: Springer-Verlag. 18-48.

15. Lai, X., J. L. Massey, and S. Murphy. 1991. Markov Ciphers and Differential Cryptanalysis. In *Advances in Cryptology - EUROCRYPT '91 (Lecture Notes in Computer Science No. 547).* New York: Springer-Verlag. 17-38.

16. Matsui, M. 1994. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology - EUROCRYPT '93 (Lecture Notes in Computer Science No. 765).* New York: Springer-Verlag. 386-397.

17. Matsui, M. 1994. The First Experimental Cryptanalysis of the Data Encryption Standard. In *Advances in Cryptology - CRYPTO '94 (Lecture Notes*

in Computer Science No. 839). New York: Springer-Verlag. 1-11.

18. Matsui, M. 1995. On Correlation Between the Order of S-boxes and the Strength of DES. In *Advances in Cryptology - EUROCRYPT '94 (Lecture Notes in Computer Science No. 950)*. New York: Springer-Verlag. 366-375.

19. National Bureau of Standards. 1977. *Data Encryption Standard*. Federal Information Processing Standard 46.

20. National Institute of Standards, Advanced Encryption Standard (AES) web site: `csrc.nist.gov/encryption/aes`.

21. Nyberg, K. 1995. Linear Approximations of Block Ciphers. In *Advances in Cryptology - EUROCRYPT '94 (Lecture Notes in Computer Science No. 950)*. New York: Springer-Verlag. 439-444.

22. Nyberg, K. 1994. Differentially Uniform Mappings for Cryptography. In *Advances in Cryptology - EUROCRYPT '93 (Lecture Notes in Computer Science No. 765)*. New York: Springer-Verlag. 55-64.

23. Robshaw, M. J. B. and B. S. Kaliski. 1994. Linear Cryptanalysis Using Multiple Approxmations. In *Advances in Cryptology - CRYPTO '94 (Lecture Notes in Computer Science No. 839)*. New York: Springer-Verlag. 1-11.

24. Youssef, A. M., S. Mister, and S. E. Tavares. 1996. On the Design of Linear Transformations for Substitution Permutation Encryption Networks, In *Workshop on Selected Areas of Cryptography (SAC '96): Workshop Record*. Kingston Ontario CANADA: Queen's University. 40-48.

BIOGRAPHICAL SKETCH

Howard M. Heys obtained a BESc in Electrical Engineering from the University of Western Ontario in London, Ontario, Canada and a PhD in Electrical and Computer Engineering from Queen's University in Kingston, Ontario, Canada. Dr. Heys is now an Associate Professor of Electrical and Computer Engineering at Memorial University of Newfoundland, Canada. He worked for several years as a software designer at Nortel in Ottawa and Toronto. His current research interests include cryptography and communication networks.