Linear Cryptanalysis

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- Linear Approximations and bias value
- Piling Up Lemma
- Linear Approximation Tables
- Performing the Attack

Product Ciphers

- Most modern day ciphers are product ciphers.
- Sequence of Substitutions and Permutations
- Also called iterated ciphers
- Description includes:
  - round description
  - key schedule

Cipher Transformations

- Round function, say g takes two inputs
  - round key, K^r
  - current state, w^{r-1}
  - next state, $w^r=g(w^{r-1},K^r)$
- Plain-text: w^0
- Cipher-text: w^{Nr}, where Nr is the number of rounds of the cipher
- Decryption is thus achieved by the transformation, g^{-1}.

Definition of SPN Ciphers

- Block length: lm, l and m are integers
- Substitution, S: $\{0,1\}^l \rightarrow \{0,1\}^l$
  - Known as S-Box
- Permutation, P: $\{0,1\}^{lm} \rightarrow \{0,1\}^{lm}$
  - Known as P-Box
- Except the last round all rounds will perform m substitutions, using S, followed by a Permutation.

Algorithm

- **Input, x: $\{0,1\}^{lm}$, K_0 : $\{0,1\}^{lm}$**
- **Output, y: $\{0,1\}^{lm}$**
- **Key-schedule: generates ($K_0, K_1, \ldots, K_{Nr}$)**

Key Whitening

$w^0=x$

for r=1 to Nr-1

$u^r = w^{r-1} \wedge K^{r-1}$

for i = 1 to m

do $v^r_i = S(u^r_i)$

$w^r = v^r_{P(1)}, v^r_{P(2)}, \ldots, v^r_{P(lm)}$

$u^{Nr} = v^{Nr-1} \wedge K^{Nr-1}$

Nr-1 rounds

for i = 1 to m

do $v^{Nr}_i = S(u^{Nr}_i)$

$y = v^{Nr} \wedge K^{Nr}$

last round

Example: GPig Cipher

- l=m=Nr=4
- Thus plain text size is 16 bits
- It is divided into 4 groups of 4 bits each.
- S-Box works on each of the 4 bits
- Consider a S-Box (substitution table)

Table 1: **S-box Representation (in hexadecimal)**

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

GPig (contd.)

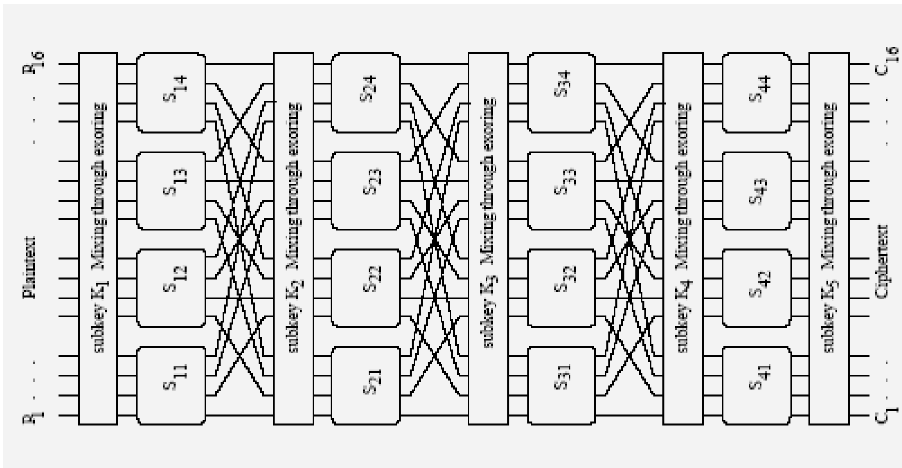
- The Permutation Table is as follows:

Table 2: **Permutation**

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

- Permutation is the transposition of bits
- There are lm=16 bits, which are transposed using the above table

The Cipher Diagram



Modifications or Variations of the SPN Structure

- **Examples: DES, AES**
- **Different S-Boxes instead of a single one**
  - **As done in DES, there are 8 different S-Boxes**
- **Have an additional invertible linear transformation**
  - **As done in AES**
- **Is the GPig Cipher secure?**

Key Scheduling

- Consider the key to be 32 bits (too small)
- A simple key schedule:
  - Kr is made by taking 16 successive bits from the key starting at (4r + 1) bit position.
- Example: Input Key, K:
  - 0011 1010 1001 0100 1101 0110 0011 1111
  - K^0= 0011 1010 1001 0100
  - K^1= 1010 1001 0100 1101
  - K^2= 1001 0100 1101 0110
  - K^3= 0100 1101 0110 0011
  - K^4= 1101 0110 0011 1111

What is Linear Crypatanalysis (LC)?

- **Aims at obtaining linear approximations relating the plaintext and the states of the ciphers prior to last round**
- **The probability of the approximation should be bounded away from ½, to be called a "good" approximation**
- **The attacker has a large number of plaintext and ciphertext pairs. What kind of attack model is this?**
- **Now we start guessing the last round keys and decrypting the ciphertext to obtain the state previous to the last round.**

LC (Basics)

- We check if the approximation is satisfied.
- We update a frequency table for all the candidate keys
- The correct candidate key will have the largest tally, if the experiment is performed for a large number of times.
- Note that the attack would not have worked if the cipher was a random function, with all approximations having a probability ½
  - LC is nothing but a distinguisher

Piling Up Lemma

- Consider independent random variables:
  - X_1, X_2, …
  - let $Pr[X_1=0]=p_1 \Rightarrow Pr[X_1=1]=1-p_1$
  - let $Pr[X_2=0]=p_2 \Rightarrow Pr[X_2=1]=1-p_2$
  - Thus, $Pr[X_1 \wedge X_2]=0$ is $p_1p_2 + (1-p_1)(1-p_2)$
  - Not let $\epsilon_1=p_1-1/2$ and $\epsilon_2=p_2-1/2$ (these are called bias values of the rv.s)
  - Thus, $\underline{Pr[X_1 \wedge X_2]=0 = 2\epsilon_1\epsilon_2}$

Generalized lemma

Lemma 1 *[1] For n independent, random binary variables $X_1, X_2, \ldots, X_n$, with bias $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$,*

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

Thus if $X_1, X_2, \ldots, X_n$ are n linear approximations then the bias of the linear approximation made out of these n equations is denoted by [2]:

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

Note that if there is one bias on the RHS which is 0, then LHS is also 0

Reminder

- **Piling Up lemma works only when the random variables are independent.**
- **Next we see how to obtain linear approximations of the S-Box**

Linear Approximations of mxn S-Box

- **Input tuple: $(x_1,x_2,\ldots,x_m)$, x_i's are values which r.v X_i takes**
- **Output tuple: $(y_1,y_2,\ldots,y_n)$, y_j's are values which r.v Y_j takes.**
- **The values are {0,1}**
- **Note that the outputs are not independent among themselves or from the inputs.**

Computing the probability of linear approximation

$$\Pr[X_1 = x_1,\ldots, X_m = x_m, Y_1 = y_1,\ldots, Y_n = y_n) = 0$$
$$if \ \ (y_1,\ldots, y_n) \neq S(x_1,\ldots, x_m)$$
$$\Pr[X_1 = x_1,\ldots, X_m = x_m, Y_1 = y_1,\ldots, Y_n = y_n) = 2^{-m}$$
$$if \ \ (y_1,\ldots, y_n) = S(x_1,\ldots, x_m)$$

S-Box in terms of the random variables

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	0	0	0	1	0
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0
1	0	0	0	0	0	1	1
1	0	0	1	1	0	1	0
1	0	1	0	0	1	1	0
1	0	1	1	1	1	0	0
1	1	0	0	0	1	0	1
1	1	0	1	1	0	0	1
1	1	1	0	0	0	0	0
1	1	1	1	0	1	1	1

What is the bias of

X_1 ^ X_4 ^ Y_2?

There are 8 cases when X1 ^ X4 ^ Y2=0

Thus the probability is 8/16=1/2

So, the bias is zero.

Consider, X_3^ X_4 ^ Y_1 ^ Y_4

The bias turns out to be -3/8

Representing the Approximations

- **Any expression can be written in the form:**

$$\left(\bigoplus_{i=1}^{4} a_i \mathbf{X_i}\right) \oplus \left(\bigoplus_{i=1}^{4} b_i \mathbf{Y_i}\right)$$

- **Here a_iЄ{0,1} and b_i Є{0,1}**
- **Thus each of a and b can be denoted by hexadecimal numbers from 0 to F**
- **They can be stored in a table**

Linear Approximation Table (LAT)

a \ *b*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
4	8	10	8	6	6	4	6	8	8	6	8	10	10	4	10	8
5	8	6	6	8	6	8	12	10	6	8	4	10	8	6	6	8
6	8	10	6	12	10	8	8	10	8	6	10	12	6	8	8	6
7	8	6	8	10	10	4	10	8	6	8	10	8	12	10	8	10
8	8	8	8	8	8	8	8	8	6	10	10	6	10	6	6	2
9	8	8	6	6	8	8	6	6	4	8	6	10	8	12	10	6
A	8	12	6	10	4	8	10	6	10	10	8	8	10	10	8	8
B	8	12	8	4	12	8	12	8	8	8	8	8	8	8	8	8
C	8	6	12	6	6	8	10	8	10	8	10	12	8	10	8	6
D	8	10	10	8	6	12	8	10	4	6	10	8	10	8	8	10
E	8	10	10	8	6	4	8	10	6	8	8	6	4	10	6	8
F	8	6	4	6	6	8	10	8	8	6	12	6	6	8	10	8

for X3^ X4 ^ Y1 ^ Y4

a=(0011)=3

b=(1001)=9

Thus T[3,9]=2

Bias = 2/16-1/2=-3/8

Thus Bias

=(T[a,b]/16)-1/2

Linear Attack

- **We need to form a linear approximation, involving the plain-text, key and the state before the last rounds, which has a good bias.**
- **The non-linear components in the cipher are only the S-Boxes.**
- **So, we use the LAT to obtain the good linear approximations.**

Linear Approximations of the 3(=4-1) round Cipher

- **Approximations of the S-Boxes with high values:**

- In S_2^1, the random variable $\mathbf{T_1} = \mathbf{U_5^1} \oplus \mathbf{U_7^1} \oplus \mathbf{U_8^1} \oplus \mathbf{V_6^1}$ has bias $1/4$
- In S_2^2, the random variable $\mathbf{T_2} = \mathbf{U_6^2} \oplus \mathbf{V_6^2} \oplus \mathbf{V_8^2}$ has bias $-1/4$
- In S_2^3, the random variable $\mathbf{T_3} = \mathbf{U_6^3} \oplus \mathbf{V_6^3} \oplus \mathbf{V_8^3}$ has bias $-1/4$
- In S_4^3, the random variable $\mathbf{T_4} = \mathbf{U_{14}^3} \oplus \mathbf{V_{14}^3} \oplus \mathbf{V_{16}^3}$ has bias $-1/4$

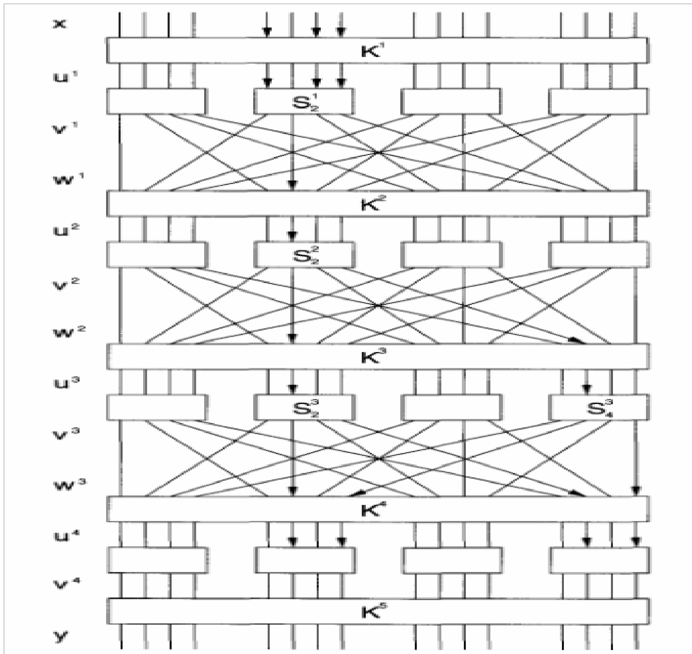
- **If we assume that the 4 random variables are independent we can combine them by the Piling Up Lemma.**

Linear Approx (contd.)

- So, the bias of:

$$\mathbf{T_1} \oplus \mathbf{T_2} \oplus \mathbf{T_3} \oplus \mathbf{T_4}$$

  is $2^3(1/4)(-1/4)^3=-1/32$
- This is by Piling Up lemma
- T_1, T_2, T_3 and T_4 have the property that their input and output are expressible in terms of Plaintext, the key bits and u^4 (the input to the last round of S-Boxes)



Linear Approx (contd.)

- In S_2^1, the random variable $\mathbf{T_1} = \mathbf{U_5^1} \oplus \mathbf{U_7^1} \oplus \mathbf{U_8^1} \oplus \mathbf{V_6^1}$ has bias $1/4$
- In S_2^2, the random variable $\mathbf{T_2} = \mathbf{U_6^2} \oplus \mathbf{V_6^2} \oplus \mathbf{V_8^2}$ has bias $-1/4$
- In S_2^3, the random variable $\mathbf{T_3} = \mathbf{U_6^3} \oplus \mathbf{V_6^3} \oplus \mathbf{V_8^3}$ has bias $-1/4$
- In S_4^3, the random variable $\mathbf{T_4} = \mathbf{U_{14}^3} \oplus \mathbf{V_{14}^3} \oplus \mathbf{V_{16}^3}$ has bias $-1/4$

$$
\begin{aligned}
\mathbf{T_1} &= \mathbf{U_5^1} \oplus \mathbf{U_7^1} \oplus \mathbf{U_8^1} \oplus \mathbf{V_6^1} = \mathbf{X_5} \oplus \mathbf{K_5^1} \oplus \mathbf{X_7} \oplus \mathbf{K_7^1} \oplus \mathbf{X_8} \oplus \mathbf{K_8^1} \oplus \mathbf{V_6^1} \\
\mathbf{T_2} &= \mathbf{U_6^2} \oplus \mathbf{V_6^2} \oplus \mathbf{V_8^2} = \mathbf{V_6^1} \oplus \mathbf{K_6^2} \oplus \mathbf{V_6^2} \oplus \mathbf{V_8^2} \\
\mathbf{T_3} &= \mathbf{U_6^3} \oplus \mathbf{V_6^3} \oplus \mathbf{V_8^3} = \mathbf{V_6^2} \oplus \mathbf{K_6^3} \oplus \mathbf{V_6^3} \oplus \mathbf{V_8^3} \\
\mathbf{T_4} &= \mathbf{U_{14}^3} \oplus \mathbf{V_{14}^3} \oplus \mathbf{V_{16}^3} = \mathbf{V_8^2} \oplus \mathbf{K_{14}^3} \oplus \mathbf{V_{14}^3} \oplus \mathbf{V_{16}^3}.
\end{aligned}
$$

Linear Approx (contd.)

$$T_1 \oplus T_2 \oplus T_3 \oplus T_4 =$$

$$X_5 \oplus X_7 \oplus X_8 \oplus V^3_6 \oplus V^3_8 \oplus V^3_{14} \oplus V^3_{16} \oplus K^1_5 \oplus K^1_7 \oplus K^1_8 \oplus K^2_6 \oplus K^3_6 \oplus K^3_{14}$$

has a bias of -1/32.

The following equations are substituted in the above equation:

$$V^3_6 = U^4_6 \oplus K^4_6$$
$$V^3_8 = U^4_{14} \oplus K^4_{14}$$
$$V^3_{14} = U^4_8 \oplus K^4_8$$
$$V^3_{16} = U^4_{16} \oplus K^4_{16}$$

Linear Approx (contd.)

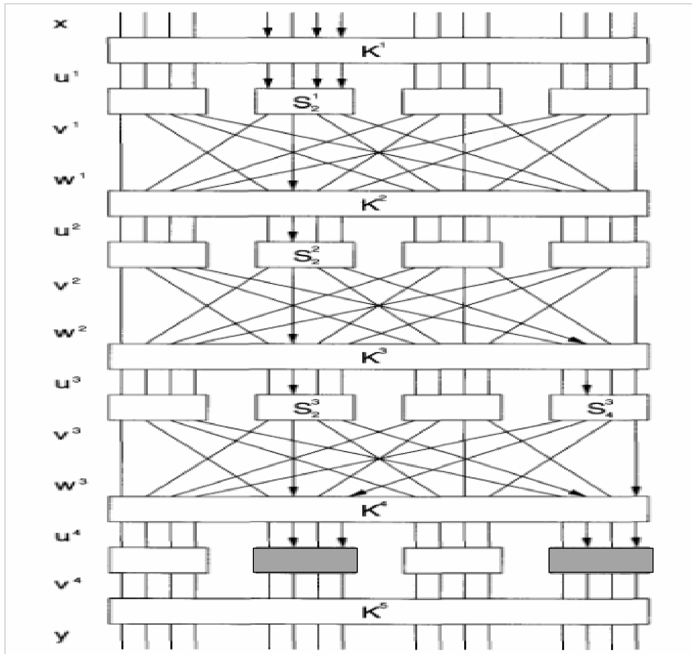
- Note that the final expression involves the plaintext, key bits and u^4:

$$X_5 \oplus X_7 \oplus X_8 \oplus U^4_6 \oplus U^4_8 \oplus U^4_{14} \oplus U^4_{16} \oplus K^1_5 \oplus K^1_7 \oplus K^1_8 \oplus K^2_6 \oplus K^3_6 \oplus K^3_{14} \oplus K^4_6 \oplus K^4_8 \oplus K^4_{14} \oplus K^4_{16}$$

- Note that the bias of the expression is 1/32.
- Also note that the term,

$$K^1_5 \oplus K^1_7 \oplus K^1_8 \oplus K^2_6 \oplus K^3_6 \oplus K^3_{14} \oplus K^4_6 \oplus K^4_8 \oplus K^4_{14} \oplus K^4_{16}$$

can either be 1 or 0.
- Hence the bias of $X_5 \oplus X_7 \oplus X_8 \oplus U^4_6 \oplus U^4_8 \oplus U^4_{14} \oplus U^4_{16}$ is ±1/32



The Attack

- Note that the expression has bits in U^4, which are there in the second and fourth S-Box of the last round.
- The attacker obtain large number of ciphertexts from the plaintexts he knows.
- Then he guesses 8 key bits, K_5[5-8], K_5[13-16]
- He makes a frequency table, where for each key a count is stored to denote the number of cases the above expression is satisfied.
- If we inspect T plaintext, ciphertext pairs then for a wrong guess in T/2 cases the expression will be satisfied.
- For a correct guess, in case of about T/2±T/32, the expresssion is satisfied.
- Roughly, T=8000.

Further Reading

- Douglas Stinson, *Cryptography Theory and Practice, 2nd Edition*, Chapman & Hall/CRC
- B. A. Forouzan, *"Cryptography and Network Security",* TMH
- Howard Heys, "*A Tutorial on Linear and Differential Cryptanalysis",* 2001

Exercise

Suppose that X_1, X_2 and X_3 are independent discrete random variables defined on the set $\{0, 1\}$. Let ϵ_i denote the bias of X_i, for $i = 1, 2, 3$. Prove that if $X_1 \oplus X_2$ is independent of $X_2 \oplus X_3$, then either $\epsilon_1, \epsilon_3 = 0$ or $\epsilon_2 = \pm 1/2$.

Next Days Topic

- Differential Cryptanalysis