T-79.5501
Cryptology

Lecture 6 (Oct 18, 2005):

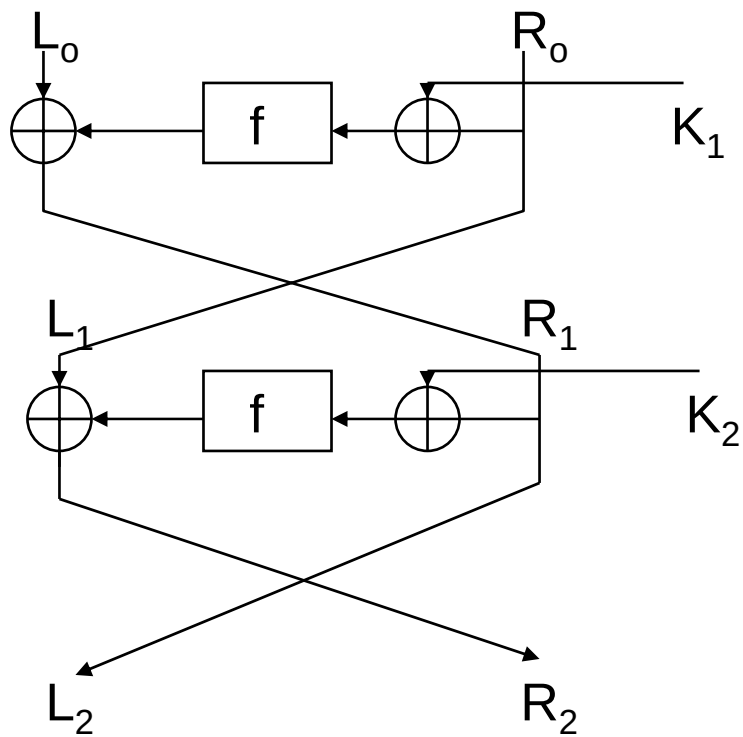
- Linear approximations over Feistel ciphers
- Differential cryptanalysis
- Boolean functions

Linear Cryptanalysis for Feistel Ciphers

Consider a Feistel cipher and assume, for simplicity, that the round-key is put in using xor-operation, that is, the f-function is of the form:

$$F(X ; K) = f(X \oplus K),$$

where f: $\mathbf{Z_2^m} \rightarrow \mathbf{Z_2^m}$ is a function, X is the data input block and K is the round key, both of equal length m. Consider two rounds:



$$R_i = L_{i-1} \oplus f(R_{i-1} \oplus K_i)$$

$$L_i = R_{i-1}$$

Linear Cryptanalysis for Feistel Ciphers

We shall study how linear approximations work for a Feistel cipher.

Fix $b_1 \in \mathbf{Z}_2^m$. Then

$$b_1 \cdot R_1 = b_1 \cdot L_o \oplus b_1 \cdot f(R_0 \oplus K_1).$$

Assume that for a random input X to the function f we know that

$$b_1 \cdot f(X) = a_1 \cdot X$$

holds with certain probability $Pr[b_1 \cdot f(X) = a_1 \cdot X] = p[a_1,b_1] \neq ½$.

Then

$$b_1 \cdot R_1 = b_1 \cdot L_o \oplus a_1 \cdot (R_0 \oplus K_1) \qquad (3)$$

with the same probability $p(a_1,b_1)$, provided that we can assume that $X = R_0 \oplus K_1$ is uniformly distributed.

Linear Cryptanalysis for Feistel Ciphers

Let us consider a second linear approximation relation for f,

$$b_2 \cdot f(X) = a_2 \cdot X,$$

which is known to hold with probability $Pr[b_2 \cdot F(X) = a_2 \cdot X] = p[a_2, b_2] \neq ½$, and apply it to the second round of our Feistel network:

$$b_2 \cdot R_2 = b_2 \cdot L_1 \oplus b_2 \cdot f(R_1 \oplus K_2)$$

to obtain

$$b_2 \cdot R_2 = b_2 \cdot L_1 \oplus a_2 \cdot (R_1 \oplus K_2) \qquad (4)$$

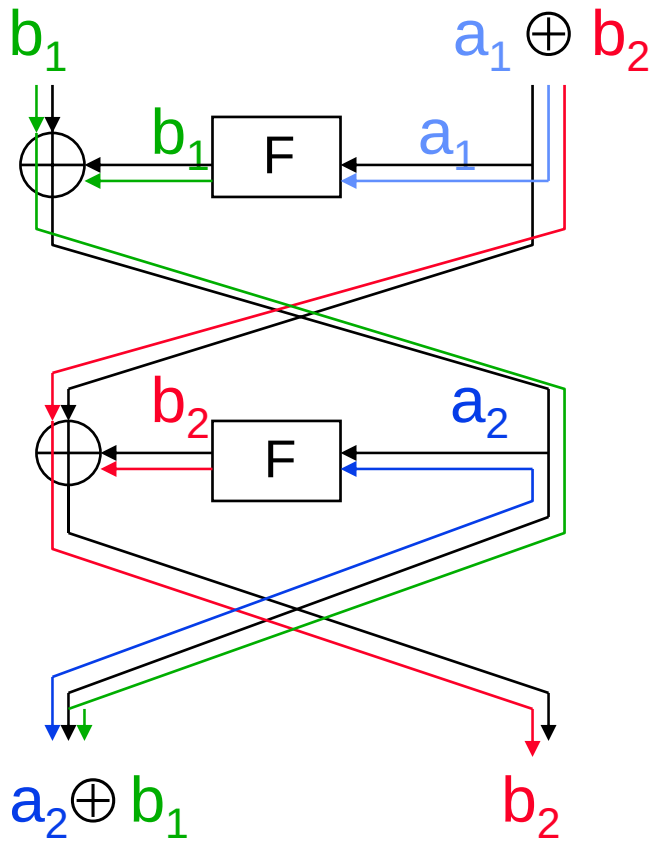
Xoring the equations (3) and (4) together and recalling that $R_{i-1} = L_i$, gives

a two-round **linear characteristic**

$$b_1 \cdot L_o \oplus (a_1 \oplus b_2) \cdot R_0 \oplus (b_1 \oplus a_2) \cdot L_2 \oplus b_2 \cdot R_2 \oplus a_1 \cdot K_1 \oplus a_2 \cdot K_2 = 0 \qquad (5)$$

which is depicted on the next page.

2- round linear approximation



$$b_1 \cdot L_o \oplus (a_1 \oplus b_2) \cdot R_0 \oplus (b_1 \oplus a_2) \cdot L_2 \oplus b_2 \cdot R_2 \oplus a_1 \cdot K_1 \oplus a_2 \cdot K_2 = 0$$

Let us now consider the probability of the two round linear characteristic:

$p = Pr[b_1 \cdot L_o \oplus (a_1 \oplus b_2) \cdot R_0 = (b_1 \oplus a_2) \cdot L_2 \oplus b_2 \cdot R_2]$.

Denote by p' the probability of (5). Expression (5) and the above expression differ only by the constant term $a_1 \cdot K_1 \oplus a_2 \cdot K_2$, since the round keys are fixed. Then $|p - ½| = |p' - ½|$.

We assume that the random variables at round 1, expression (3), and round 2, expression (4), are independent. Also recall that (5) was obtained by xoring (3) and (4). Then the Piling-up Lemma applies and we get

$|p - ½| = |p' - ½|$

$= 2|Pr[b_1 \cdot R_1 = b_1 \cdot L_o \oplus a_1 \cdot (R_0 \oplus K_1)] - ½||Pr[b_2 \cdot R_2 = b_2 \cdot L_1 \oplus a_2 \cdot (R_1 \oplus K_2)] - ½|$

$= 2\,|Pr[b_1 \cdot F(R_0 \oplus K_1) = a_1 \cdot (R_0 \oplus K_1)] - ½|\,|Pr[b_2 \cdot F(R_1 \oplus K_2) = a_2 \cdot (R_1 \oplus K_2)] - ½|$

$= 2\,|p[a_1, b_1] - ½|\,|p[a_2, b_2] - ½|$.

Linear approximations can be chained from round to round. The data inputs are not truly independent, but in practical applications, the Piling-up Lemma is usually found to give good estimates of the overall bias.

Iterative linear approximations, that is, linear approximations that can be chained with itself, are sometimes useful. However, the best linear approximations over more than five rounds of the DES are based on a 3-round characteristic which is chained with a trivial zero-to-zero approximation (p[0,0] = 1!) followed by itself in the inverse order. The strongest linear approximations over DES always involve at most one S-box at each round. The bias of the best linear approximation over 14 rounds of the DES has (estimated) bias $1.19 \cdot 2^{-21}$ [M. Matsui: Linear Cryptanalysis Method for DES Cipher, Eurocrypt '93, LNCS 765].

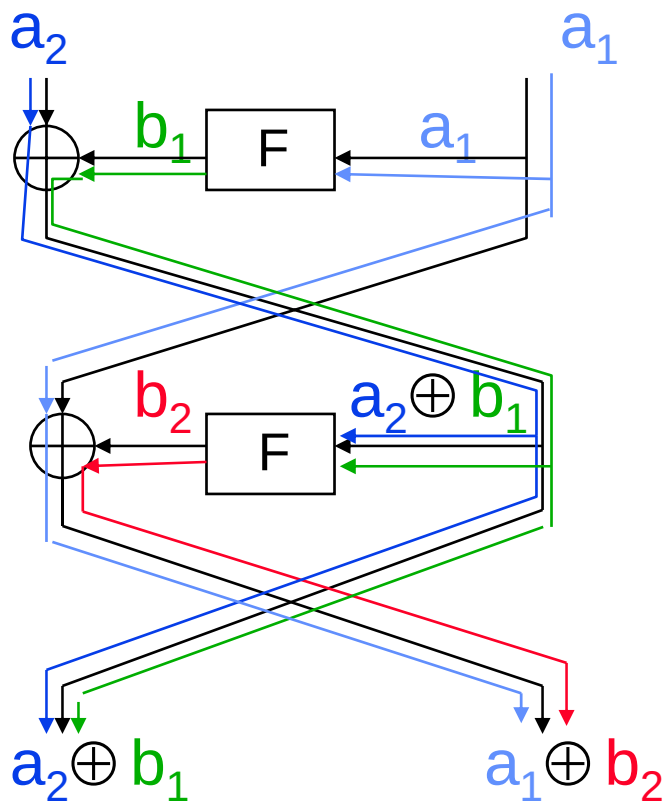
If the function f is bijective then $p[0,b] = Pr(0 \cdot X = b \cdot f(X)) = ½$, for all $b \neq 0$. Then it is possible to show that certain linear approximation are not possible.

For example: If f is bijective and $a_1 = 0$, then the approximation relation (5) can have a positive bias only if $b_1 = 0$.

Differential Cryptanalysis

See Text-book: Section 3.4

2- round differential characteristic for a Feistel cipher



For example, if f is bijective, then it is impossible to have b1 = 0, unless $a_1 = 0$.

Boolean functions

Algebraic Normal Form

see background paper Section 1.4

Nonlinearity of Boolean functions

see background paper Section 2.1

(correlation = 2·bias)

Definition: A Boolean function f of n variables is bent if $c(f,A) = 2^{-n/2}$ for all linear and affine Boolean functions A of n variables.

Boolean functions in SHA

see background paper Example 6

Perfect nonlinear functions

see background paper Section 2.3

Fact: A Boolean function is perfect nonlinear if and only it is bent.