# T-79.5501
# Cryptology

Lecture 6

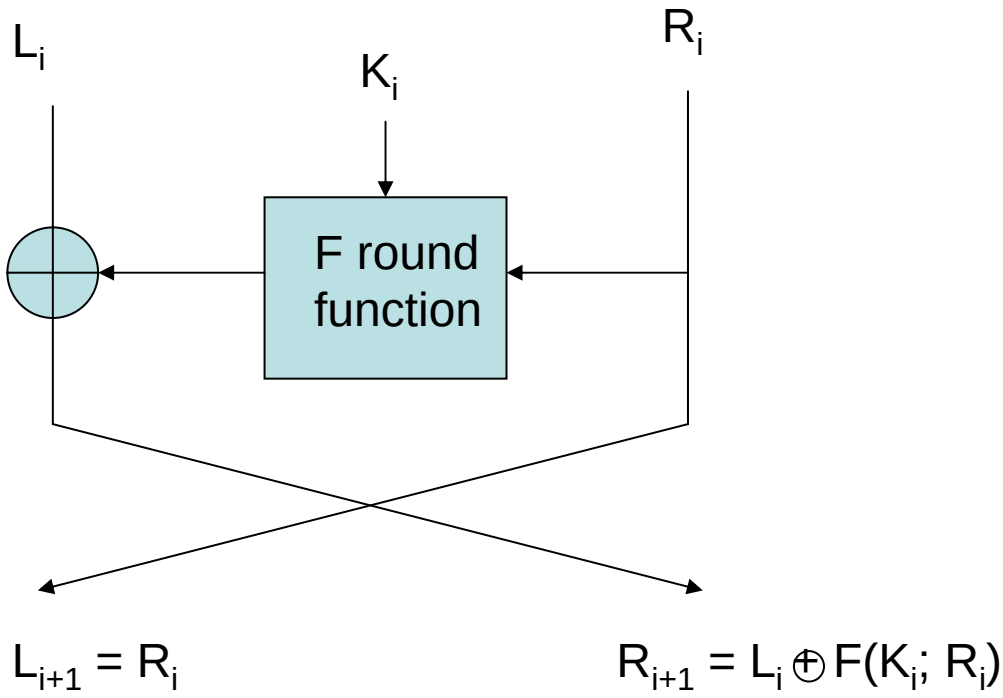
February 20, 2007

# Linear cryptanlysis

- Feistel ciphers, Stinson 3.5 and slides 2-3
- Linear approximation of Boolean functions (example: slide 4)
- Boolean functions and algebraic normal form (ANF), see Handout 3, pages 1-3
- Walsh transform and Parseval's theorem, see Handout 3, pages 3-7

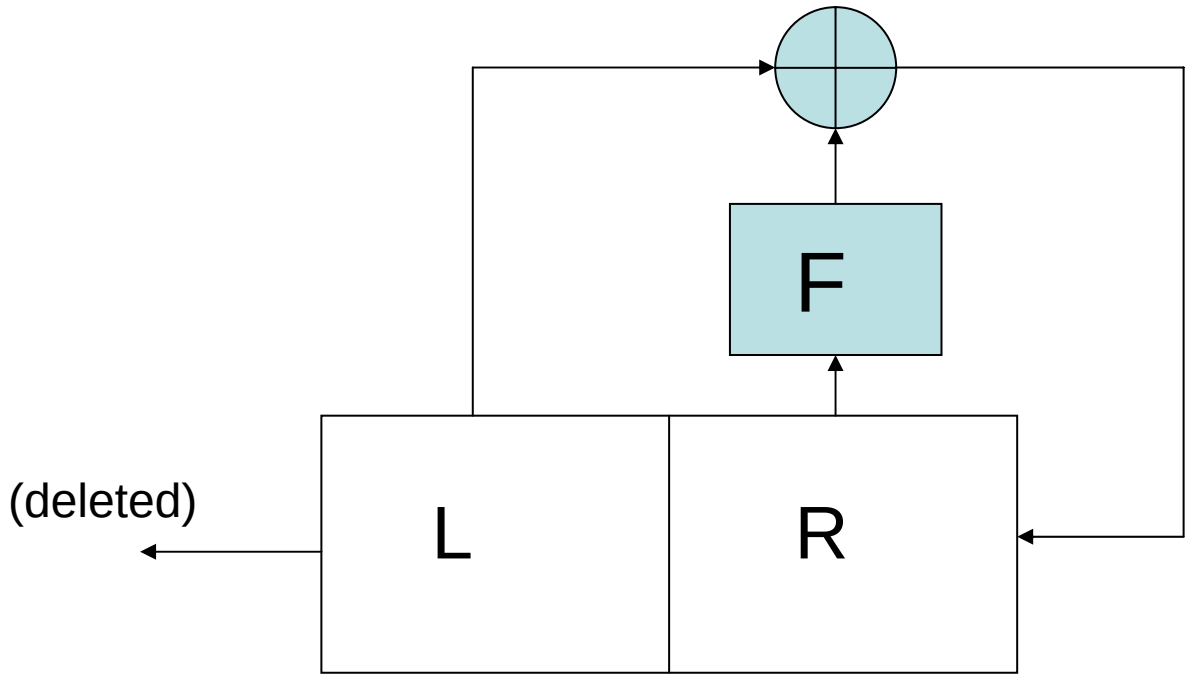
# Feistel Ciphers

- Special structure to make it invertible
- S-boxes and round-functions need not be invertible
- Example: DES (Section 3.5)



# Feistel cipher

Seen as a nonlinear feedback shift register:



# Example: A linear approximation of the first row of DES S-box $S_3$

| Y | $X_1X_2X_3X_4$ | $Y_1Y_2Y_3Y_4$ | $Y_3$ | $X_3 \oplus X_4$ | =? |
|---|---|---|---|---|---|
| 10 | 0 0 0 0 | 1 0 1 0 | 1 | 0 | no |
| 0 | 0 0 0 1 | 0 0 0 0 | 0 | 1 | no |
| 9 | 0 0 1 0 | 1 0 0 1 | 0 | 1 | no |
| 14 | 0 0 1 1 | 1 1 1 0 | 1 | 0 | no |
| 6 | 0 1 0 0 | 0 1 1 0 | 1 | 0 | no |
| 3 | 0 1 0 1 | 0 0 1 1 | 1 | 1 | yes |
| 15 | 0 1 1 0 | 1 1 1 1 | 1 | 1 | yes |
| 5 | 0 1 1 1 | 0 1 0 1 | 0 | 0 | yes |
| 1 | 1 0 0 0 | 0 0 0 1 | 0 | 0 | yes |
| 13 | 1 0 0 1 | 1 1 0 1 | 0 | 1 | no |
| 12 | 1 0 1 0 | 1 1 0 0 | 0 | 1 | no |
| 7 | 1 0 1 1 | 0 1 1 1 | 1 | 0 | no |
| 11 | 1 1 0 0 | 1 0 1 1 | 1 | 0 | no |
| 4 | 1 1 0 1 | 0 1 0 0 | 0 | 1 | no |
| 2 | 1 1 1 0 | 0 0 1 0 | 1 | 1 | yes |
| 8 | 1 1 1 1 | 1 0 0 0 | 0 | 0 | yes |

a = 0011

b = 0010

bias (a,b) =

$6/16 - ½ = -2^{-3}$