Cryptology	8th September, 2015

Lecture 9: Modern Block Ciphers; Linear and Differential Attacks

Instructor: Dr. Goutam Paul *Scribe: Mayank Raikwar*

1 Product Cipher

A product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistant to cryptanalysis.

$y_1 = E_{k_1}(x)$
$y_2 = E_{k_2}(y_1)$
$y_2 = E^{(2)}_{k_2}(E^{(1)}_{k_1}(x))$
$y_2 = (E^{(2)}_{k_2}.E^{(1)}_{k_1})(x)$
$x = D^{(1)}_{k_1}.D^{(2)}_{k_2}(y_2)$
For example consider $E^{(1)}$: Multplication and $E^{(2)}$:Shift (Affine Cipher)

2 Iterated Block Cipher

An iterated block cipher is one that encrypts a plaintext block by a process that has several rounds. In each round, the same transformation or round function is applied to the data using a subkey. The set of subkeys are usually derived from the user-provided secret key by a key schedule. So basically it consist of:

1. Round function $g()$,working for r (say 16) rounds.
2. Key Scheduling Algorithm (to get keys for each round).

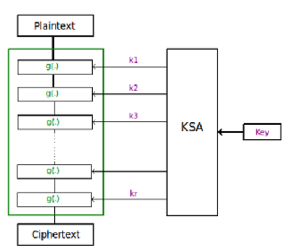

Figure 1: Iterated Block Cipher

3 Substitution-Permutation Network

One important type of iterated block cipher known as a substitution-permutation network (SPN) takes a block of the plaintext and the key as inputs, and applies several alternating rounds consisting of a substitution stage followed by a permutation stage to produce each block of ciphertext output.

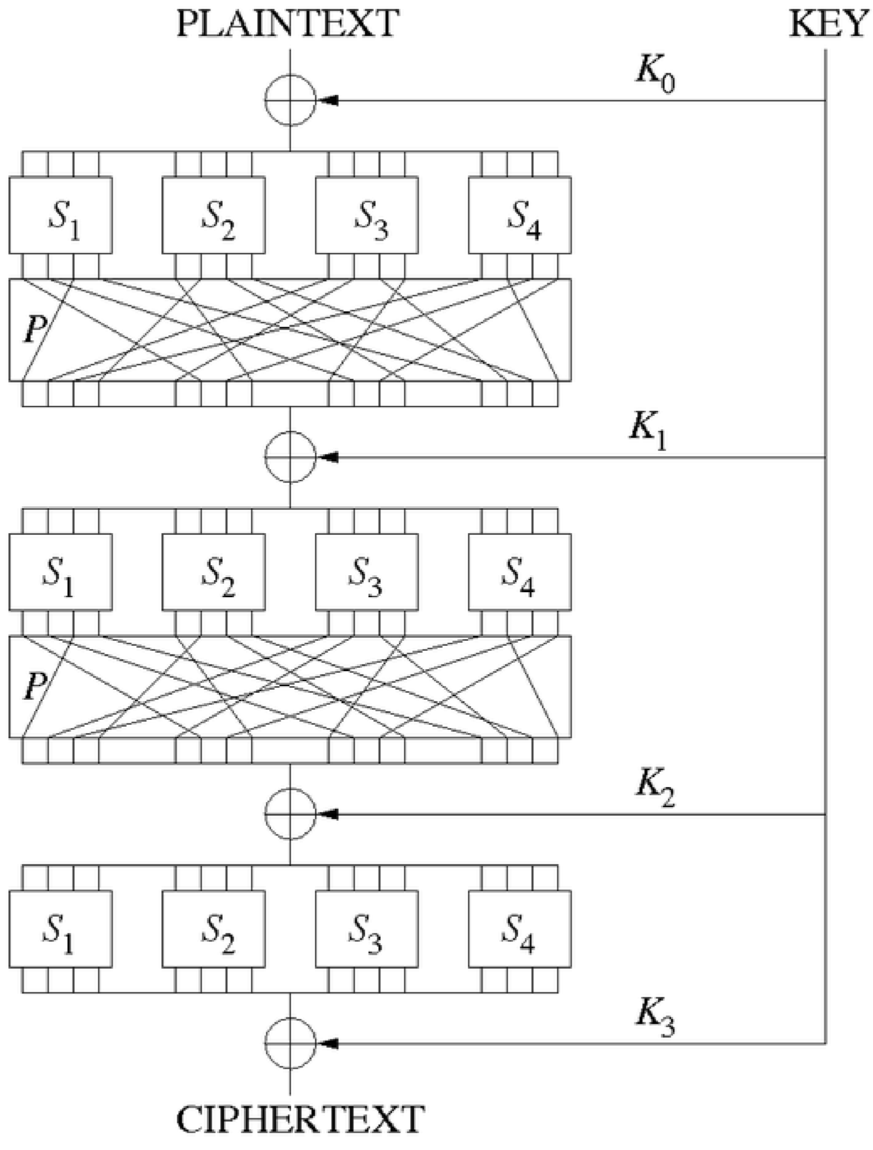

Figure 2: Substitution-Permutation Network

4 Linear Analysis

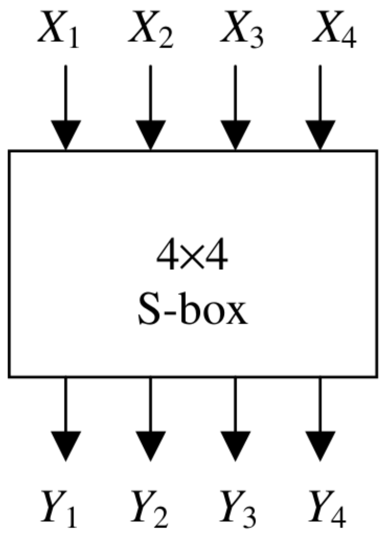

Figure 3: Idea behind Linear Analysis

1. Inputs : $X_1, ..., X_m$
2. Outputs : $Y_1, ..., Y_n$
3. Linear Approximation:
   $\Pr(\sum a_i X_i \oplus \sum b_j Y_j = 0) = p \neq \frac{1}{2}$
4. Complete enumeration of all linear approximations is performed through a $2^m \times 2^n$ Linear Approximation Table (LAT) indexed by all possible values of a and b.

4.1 Piling-up Lemma

Suppose $X_1, X_2, ...X_n$ are independent bernoulli variables with $\Pr(X_i = 0) = p_i$ for $i =$ 1,2.......n
What is $\Pr(\sum X_i = 0) = ?$

Suppose X_1 and X_2 are two independent bernoulli variables and ϵ_1,ϵ_2 are the biases respectively so
$X_1 \xrightarrow{0} p_1 \rightarrow \frac{1}{2} + \epsilon_1$
$X_2 \xrightarrow{0} p_2 \rightarrow \frac{1}{2} + \epsilon_2$

$\Pr(X_1 \oplus X_2 = 0)$
$= \Pr(X_1 = 0, X_2 = 0) + \Pr(X_1 = 1, X_2 = 1)$

$= \Pr(X_1 = 0) \cdot \Pr(X_2 = 0) + \Pr(X_1 = 1) \cdot \Pr(X_2 = 1)$
$= p_1 p_2 + (1 - p_1)(1 - p_2)$
$= (\frac{1}{2} + \epsilon_1)(\frac{1}{2} + \epsilon_2) + (\frac{1}{2} - \epsilon_1)(\frac{1}{2} - \epsilon_2)$
$= \frac{1}{2} + 2\epsilon_1\epsilon_2$

From piling-up lemma :

$$\Pr(\sum X_i = 0) = \tfrac{1}{2} + 2^{n-1} \prod_{i=1}^{n} \epsilon_i$$

Proof. Proof by Induction:
• Base case: For two variables as done before.
• Hypothesis: $\Pr(X_1 + X_2 + ... + X_k = 0) = \frac{1}{2} + 2^{k-1} \prod_{i=1}^{k} \epsilon_i$ (+ denotes XOR here)
• Inductive step:
$\Pr(\underbrace{X_1 + X_2 + ... + X_k}_{\text{Y}} + X_{k+1} = 0)$
$= \Pr(Y + X_{k+1} = 0)$

$= \frac{1}{2} + 2^{k} \prod_{i=1}^{k+1} \epsilon_i$ (from base case of two variables)

□

4.2 Key Recovery using Linear Cryptanalysis

1. After piling up till last-but-one round, let $\Pr(\sum P_i \oplus \sum V_j \oplus \sum K_l = 0) = p \neq \frac{1}{2}$,where V_j is the partial decryption of C_j by inverting the last round.

2. $\sum K_l$ is fixed at 0 or 1;Hence over many pairs of P and C, $\Pr(\sum P_i \oplus \sum V_j = 0) = p$ or 1-p respectively.

3. **Strategy**: For each value of last round subkey, for each ciphertext sample, invert and count if the above relation holds. The total count for only the correct subkey will match with p.
   Number of samples required is proportional to $\frac{1}{(p-\frac{1}{2})^2}$

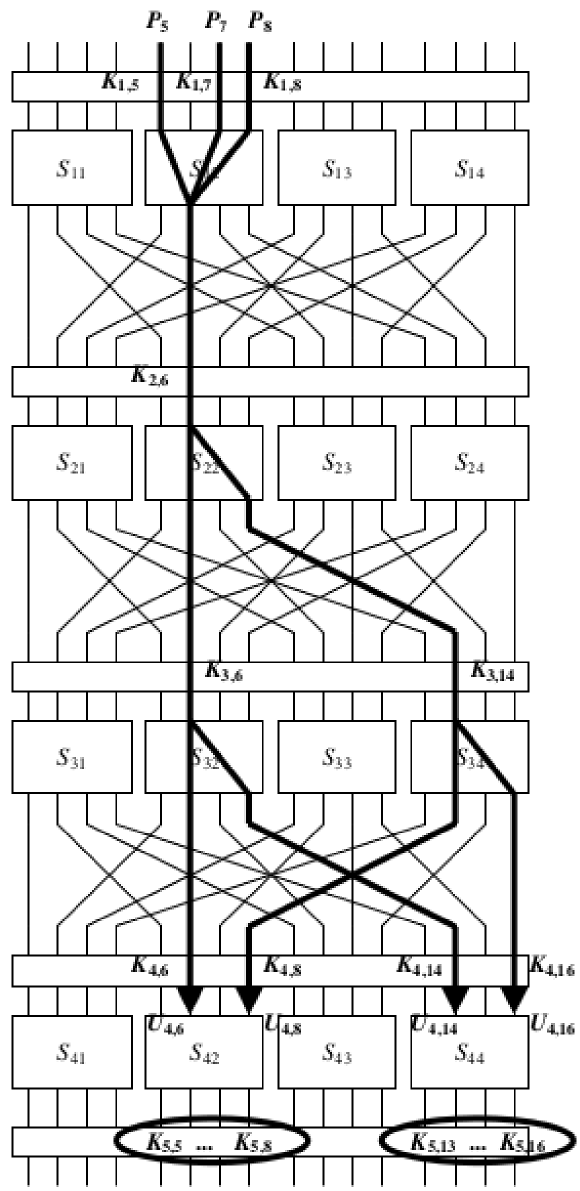

Figure 4: Piling up along Linear Trail

5 Differential Analysis

1. If $Y_1 = X_1 + K$ and $Y_2 = X_2 + K$, then $\triangle Y = \triangle X$
   Similarly, $Y_1 = AX_1$ and $Y_2 = AX_2$, then $\triangle Y = A\triangle X$.
   Thus, key-independent distinguishing attack is possible.

2. If $\Pr(\triangle Y \mid \triangle X) = p \neq \frac{1}{2}$ the pair ($\triangle X$,$\triangle Y$) is called a Differential.Complete enumeration of all differential biases is performed through a $2^m \times 2^n$ Difference Distribution Table (DDT) indexed by all possible values of $\triangle X$ and $\triangle Y$.

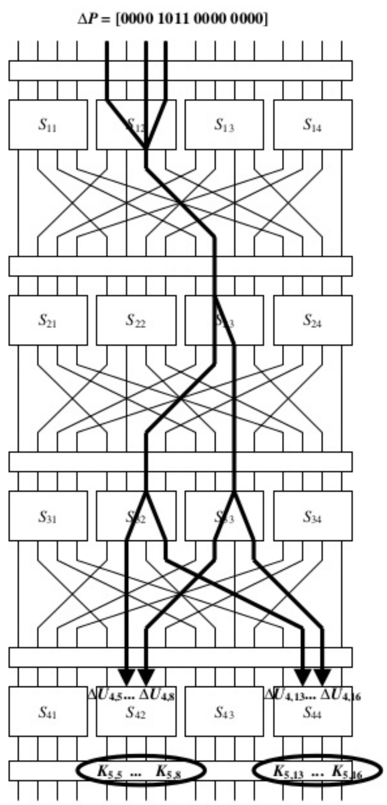

Figure 5. Sample Differential Characteristic

24

Figure 5: Differential Trail connecting P and C

5.1 Key Recovery using Differential Cryptanalysis

Find differential characteristic till last-but-one round;let $\Pr(\triangle Y_j \mid \triangle X_i) = p \neq \frac{1}{2}$,where V_j is the partial decryption of C_j by inverting the last round.

Strategy: For each value of last round subkey, for each sample (1 plaintext pair + 1 ciphertext pair) invert and count if $(\triangle P_i, \triangle V_j)$ is a valid differential. The total count for only the correct subkey will match the differential characteristics.
Number of samples required is proportional to $\frac{1}{p}$