Scribe: Cryptography and Network Security (Class.7.A)

Akash Tiwari

18-Sep-2020

1 Linear Cryptanalysis

In this lecture, we define and look at the properties of a Linear Cryptosystem and then look at the approach of the attacks on them.For The attack we also have a look at piling up lemma for biases.

- Section 2 - Product Ciphers and Cipher Transformations
- Section 3 - SPN Ciphers
- Section 4 - Algorithm
- Section 5 - An example of Linear CryptoSystem
- Section 6 - Defining Bias and piling up lemma
- Section 7 - H.W Problem on Bias calculation

2 Product Ciphers and Cipher Transformation

Product Ciphers basically use a combination of permutations and substitutions for diffusion and confusion. To Define a product Cipher we need to define 2 things-

- Round Description i.e the process of what happens in a single round.
- Key schedule which determines the key for each individual rounds.

Now we look at Cipher transformations in a block cipher. We define the following

- r : represents the current round under study/focus
- K^r : represents the current round key obtained from key schedule.
- W^{r-1} : represents the current state or the input to the current round.

- $W^r = g(W^{r-1}, K^r)$: represents the next state or the output of the current round which is a function of previous state/input and the current key.

Observations from our definitions-

- W^0 : This will be our plain text.
- W^{Nr} is the cipher text given the no of rounds = N.
- Decryption can be done by the g^{-1} function.

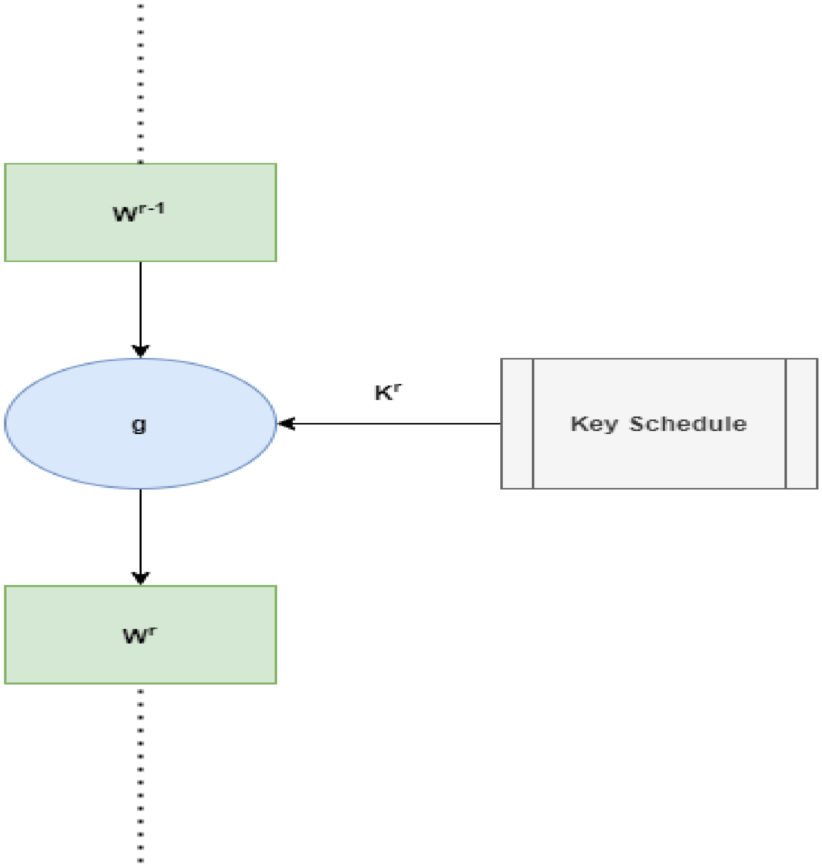


Figure 1: Eg- 1 round- Transformation.

3 SPN ciphers

We define an SPN cipher with -

- Block length : l*m where m is the number of divisions each of length l.
- Substitution : Done by S boxes, can be treated as a relation $S : \{0,1\}^l \rightarrow \{0,1\}^l$
- Permutation : Done by P boxes, can be treated as a relation $R : \{0,1\}^{lm} \rightarrow \{0,1\}^{lm}$
- We do substitution using S for every round.
- We do permutation after S using P except the last round.

Note that doing a permutation at the end does not add any security and is just an additional overhead if done. We prove this here -

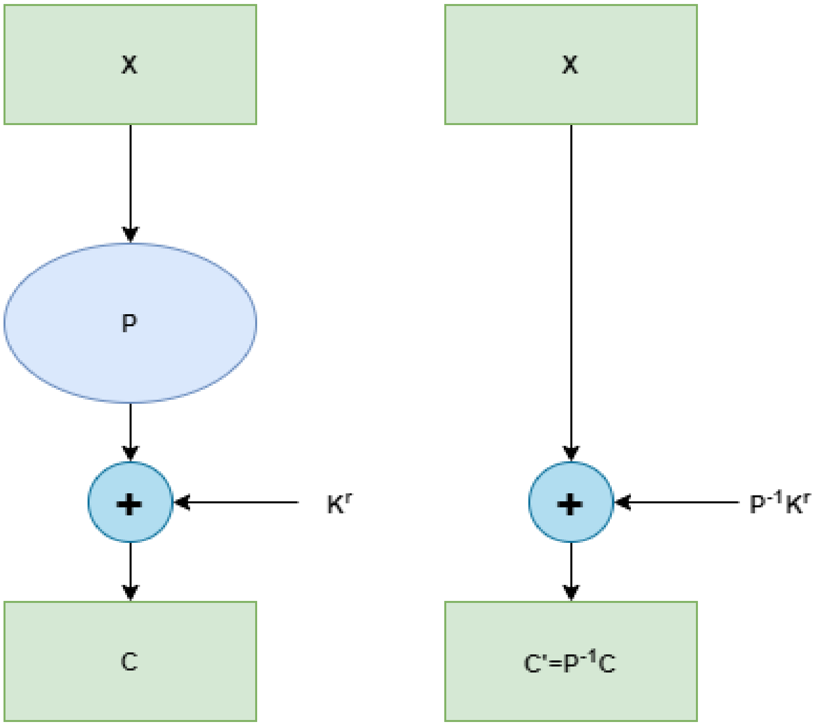


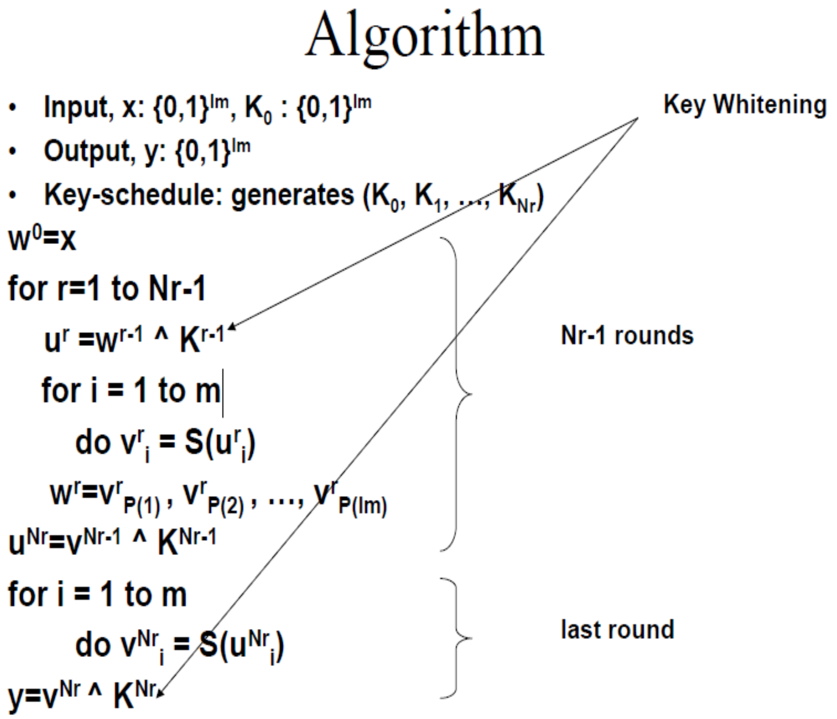
Figure 2: Original round and Equivalent round

$$C = P(x) \oplus K^r$$
$$C = P(x \oplus P^{-1}K^r)$$
$$C' = P^{-1}C = x \oplus P^{-1}K^r$$

We can construct an equivalent model as shown in figure

- If the attacker knows C then he also knows C' since P and P^{-1} are known.
- Thus breaking the equivalent model and managing to get $P^{-1}K^r$ is equivalent to getting K^r and hence P^{-1} doesn not allow any additional security.

4 Algorithm



Algorithm

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

```
$w^0=x$
for r=1 to Nr-1
    $u^r = w^{r-1} \wedge K^{r-1}$
    for i = 1 to m
        do $v^r_i = S(u^r_i)$
    $w^r = v^r_{P(1)}, v^r_{P(2)}, \ldots, v^r_{P(lm)}$
$u^{Nr} = v^{Nr-1} \wedge K^{Nr-1}$
for i = 1 to m
        do $v^{Nr}_i = S(u^{Nr}_i)$
$y = v^{Nr} \wedge K^{Nr}$
```

Key Whitening

Nr-1 rounds

last round

Figure 3: Pseudo-code for the algorithm of encryption(taken from slides)

Note in the last round that permutation is not done as we discussed earlier. Key whitening - The first and last xor with the keys are also known as Key Whitening Since they are protecting the system from the top and bottom.

5 An example of Linear CryptoSystem

- Longer Rectangle boxes represent the Xor-ring of the key and the input.
- S_{ij} represent s boxes

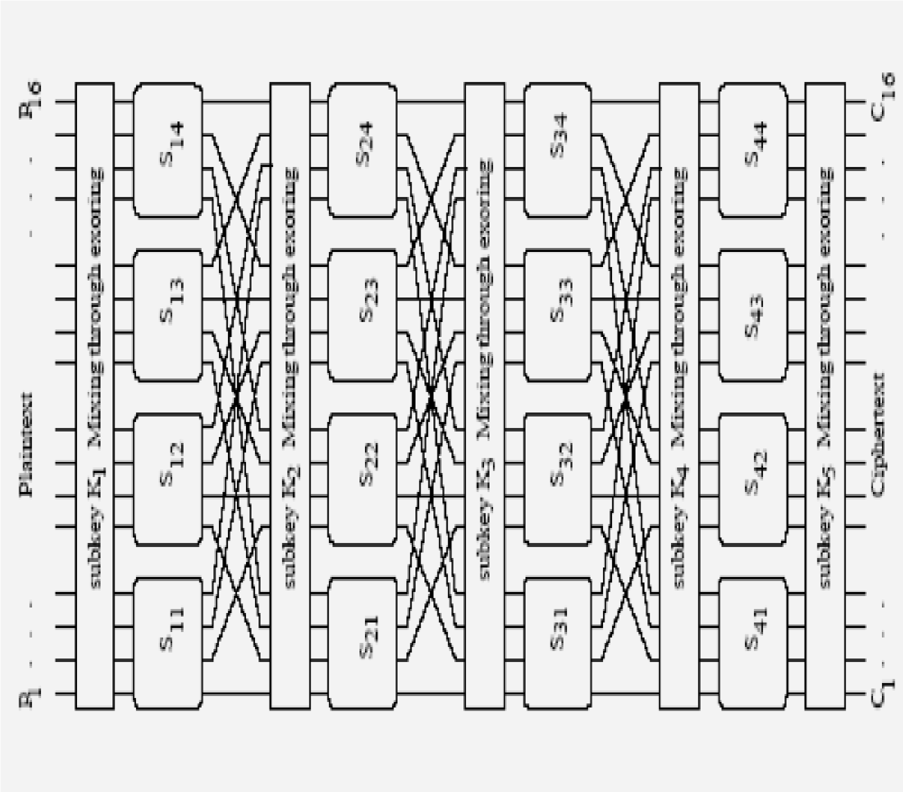

Plaintext
P_1
P_{16}
subkey K_1 Mixing through exoring
S_{11}
S_{12}
S_{13}
S_{14}
subkey K_2 Mixing through exoring
S_{21}
S_{22}
S_{23}
S_{24}
subkey K_3 Mixing through exoring
S_{31}
S_{32}
S_{33}
S_{34}
subkey K_4 Mixing through exoring
S_{41}
S_{42}
S_{43}
S_{44}
subkey K_5 Mixing through exoring
Ciphertext
C_1
C_{16}

Figure 4: Implementation of Gpig Cipher discussed in class(taken from slides)

- Random wiring represents the permutation

6 Defining Bias and piling up lemma

let us define a linear property say p which takes values either 0 or 1. Then we define Bias as-

$$Bias = |P(p = 0) - 0.5| = |P(p = 1) - 0.5|$$

Now the piling up lemma-
Let X_1 and X_2 be two independent random variables-

$$P[X_1 = 0] = p_1$$
$$P[X_1 = 1] = 1 - p_1$$
$$P[X_2 = 0] = p_2$$
$$P[X_2 = 1] = 1 - p_2$$
$$P[X_1 \oplus X_2 = 0] = p_1 * p_2 + (1 - p_1) * (1 - p_2)$$
$$P[X_1 \oplus X_2 = 0] = p_1 * p_2 + 1 - p_1 - p_2 + p_1 * p_2$$
$$P[X_1 \oplus X_2 = 0] = 0.5 - p_1 + 0.5 - p_2 + 2 * p_1 * p_2$$
$$substitute \rightarrow \epsilon_1 = p_1 - 0.5$$
$$substitute \rightarrow \epsilon_2 = p_2 - 0.5$$
$$P[X_1 \oplus X_2 = 0] = 0.5 + 2\epsilon_1\epsilon_2$$

We can generalise this to-

$$P[X_1 \oplus X_2 \oplus x_3 .... \oplus x_n = 0] = 0.5 + 2^{n-1} \prod_{i=1}^{n} \epsilon_i$$

Thus bias of n independent variables can be represented as-

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

The bias of a property gives us a very good indication of a "good" approximation or property, i.e High bias is a good approximation for the attacker. Now using this,parts of the key can be guessed as we will see in the next lecture.

7 H.W Problem on Bias calculation

Calculate the bias for random variables

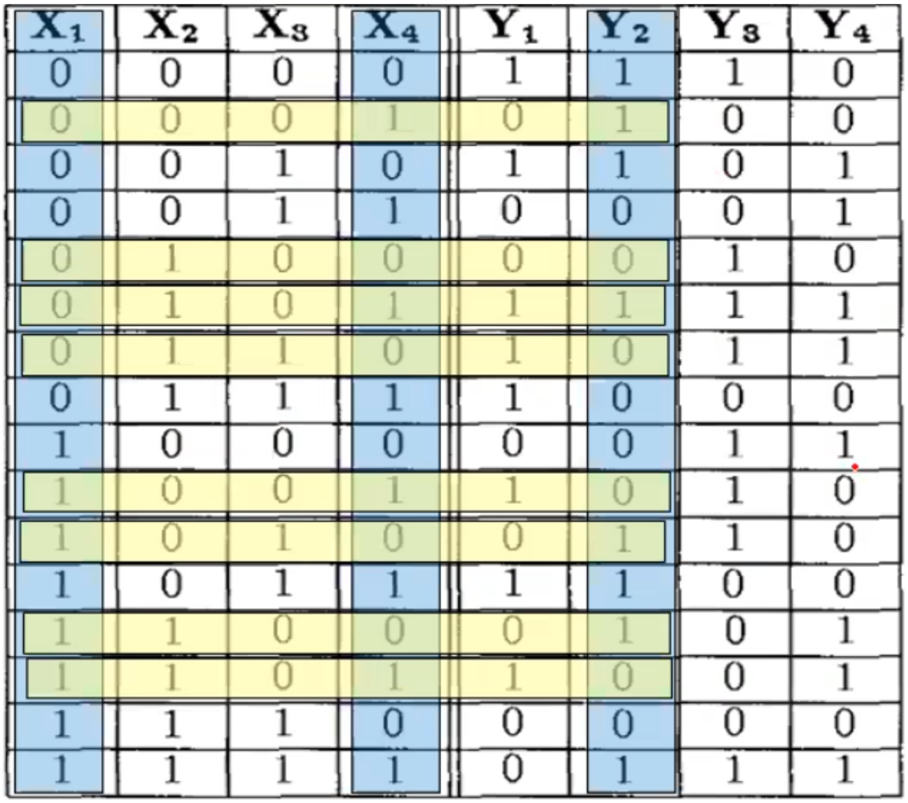
$$X_3 \oplus X_4 \oplus Y_1 \oplus Y_4$$

We find the instances when -

$$X_3 \oplus X_4 \oplus Y_1 \oplus Y_4 = 0$$

We see that only row 5 and row 10 satisfy the above property in figure 5 -

$$\epsilon_{1,2,3,4} = |0.5 - \frac{2}{16}|$$
$$\epsilon_{1,2,3,4} = \frac{3}{8}$$



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

Figure 5: Data for problem, ignore the highlighted parts(taken from slides)

8 Conclusion

Thus we have looked into properties of Linear cryptosystems, bias and it's calculation and the piling up lemma. In the next lecture, the use of bias to guess part of keys will be discussed.