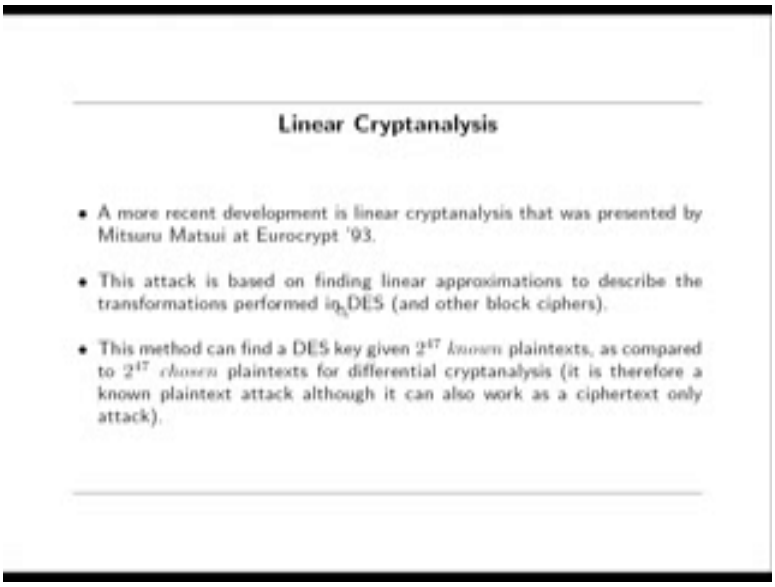
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 50
Linear Cryptanalysis

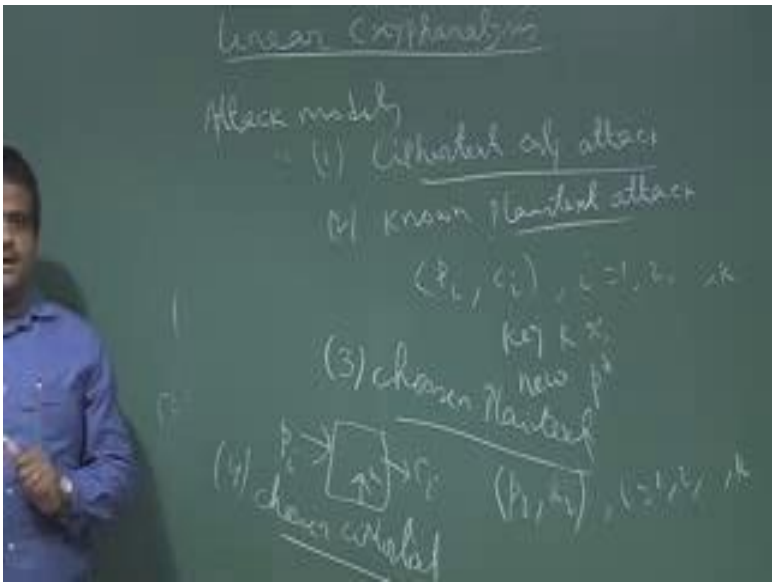
We will talk about another non generic attack on block cipher which is called linear cryptanalysis and it was introduced by in Eurocrypt 93 by Matsui.

(Refer Slide Time: 00:43)



Can you go to the slide please? So, this was introduced in 1993 at Eurocrypt conference and this was proposed to attack the DES and, but this can be carried out for any other block cipher, we will see, how it can be, what is the methodology of this and this attack can find the DES key and this is 2 to the power 47 known plaintext attack.

(Refer Slide Time: 01:23)



We know that there are different attack model like 1 is ciphertext only attack; ciphertext only attack. So, in this scenario we have only the attacker has only the ciphertext then the known plaintext attack; known plaintext attack model.

Here in this scenario, attacker has some plaintext and the corresponding ciphertext for some say k many plaintext and ciphertext pair. So, this is maybe the earlier communication between Alice and Bob. So, Alice and Bob; they are using this symmetric key encryption. So, this maybe some earlier history of their communication so this has no relevant now, but now the goal of this model is now suppose the new plaintext is p star. So, goal is to find out the key k or the current message what is being communicating between Alice and Bob. So, this is the known plaintext attack, in this scenario we have the plaintext and the ciphertext pair and we know the other 2, one is chosen plaintext attack; chosen plaintext attack.

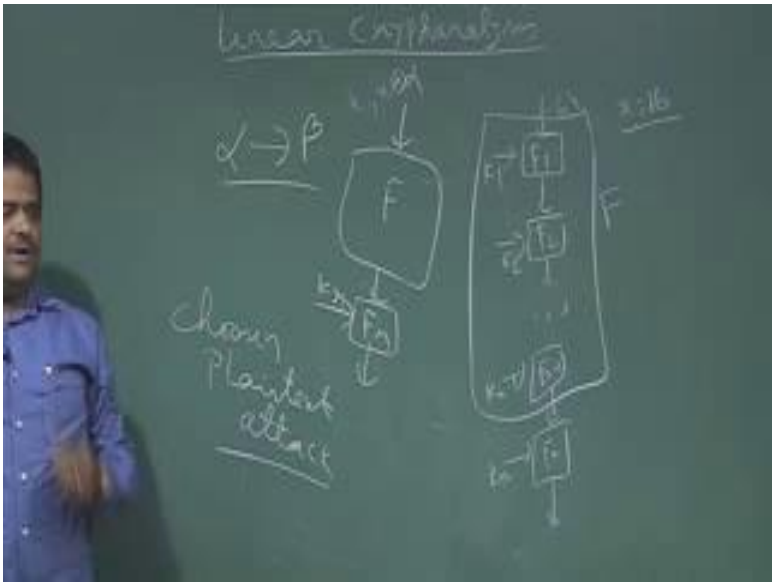
Here, attacker can choose the plaintext and can get the corresponding ciphertext. So, as if we are giving the temporary access to the encryption missionary to the attacker. So, that attacker can give their own plaintext and can get the so, this is the temporary access to this encryption machinery. So, attacker can get the plaintext corresponding ciphertext. So, there is bit difference between this is more powerful in the sense we have giving more power to the attacker that we are giving the temporary access of the encryption

machinery to the attacker. So, attacker can choose a plaintext and get the corresponding ciphertext. So, this is p i c i for certain number of p r attacker can generate.

And again the goal is same, goal is to get the key, key is not revealed to the attacker, goal is to get the key or the current the new plaintext or the new message what is being communicating between Alice and Bob and another scenario is the chosen ciphertext only attack chosen ciphertext. So, attacker can choose the ciphertext and can get the corresponding plaintext.

We are giving the temporary access to the decryption machinery to the attacker to this.

(Refer Slide Time: 05:14)



So, now, we have seen the differential cryptanalysis, in the differential cryptanalysis if we recall, we have to get the so, this is up to this is the r th round. So, anyway typical block cipher is like this. So, we have these are the round function. So, dot, dot, dot, so this is r minus 1 eth round and this is r th round and for each round we need a round key, k 1 k 2 dot, dot, dot, k r minus 1 and the k r. So, this is the and this k r, k is are coming from the which we know the key scheduling algorithm which is a public algorithm which is taking the input of the secret key and giving us the round key as many as we need.

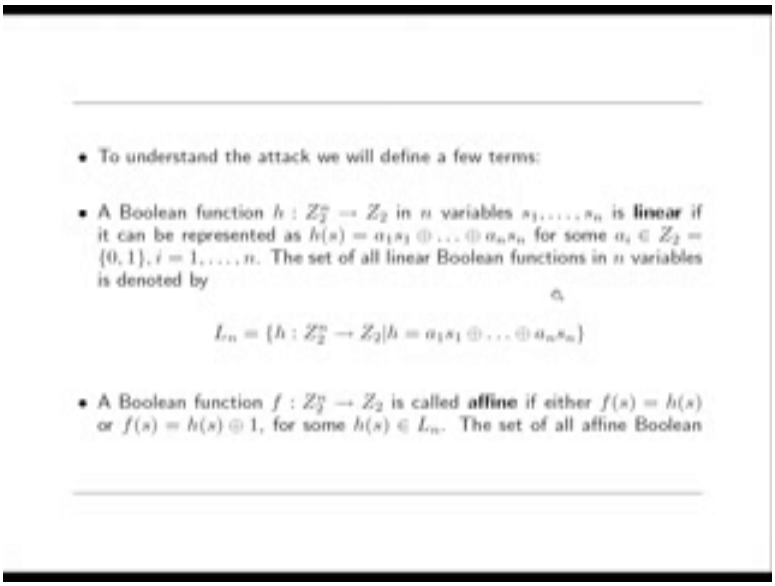
So, for r round we need r round key for DES r is 16 and this is for DES it is a 64 bit block cipher. So, this in n, n is 64 bit. So, now, for we have seen for differential cryptanalysis or differential attack, we consider this to be a function F this is the function

F and we assume that there is a differential characteristics in this F so; that means, this there is a differential to l in this F so; that means, if the input difference is alpha then the output difference will output difference will be beta with some significant probability.

This is also a probalstic attack. So, unless we have this alpha beta pair the differential trial then we cannot mound this attack. So, then we have seen the attack scenario like we choose a x and then x, x or alpha. So, that input difference will be alpha then we have seen the details of this attack how to get the k r, but this the this is a differential attack, this is a chosen plaintext attack; chosen plaintext attack because we have to choose the plaintext like this. So, that input difference should be alpha to ensure that the output difference there at this stage will be beta now in the linear cryptanalysis, it is a known plaintext attack. So, it is slightly more powerful than the differential attack.

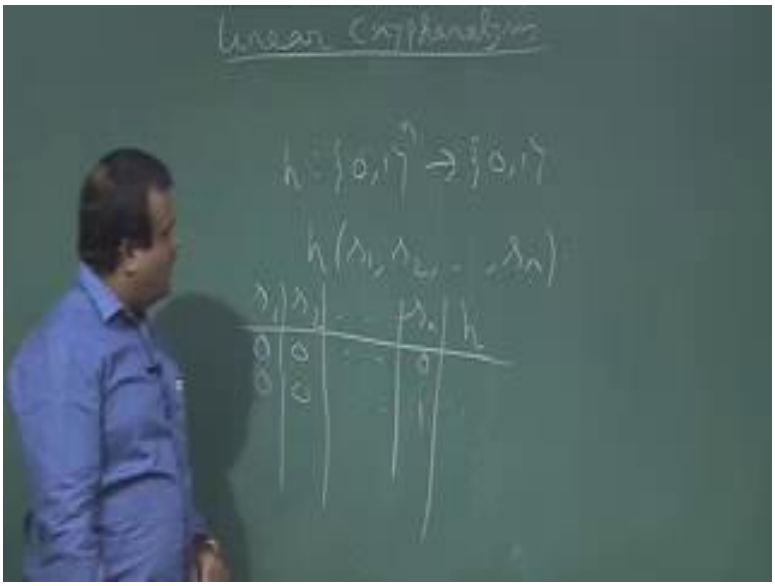
Can you go back to the slide please? So, this method this is a known plaintext attack. So, it needs 2 to the power 47 known plaintext compared to 2 to the power 47 chosen plaintext for differential cryptanalysis.

(Refer Slide Time: 08:22)



And so, to understand this attack we have to use some terminology like what is a Boolean function? So, basically Boolean function is a it takes the n variable s, s 1, s 2, s n and it is giving us a; it is basically function from 0 1 to the power n to 0 1.

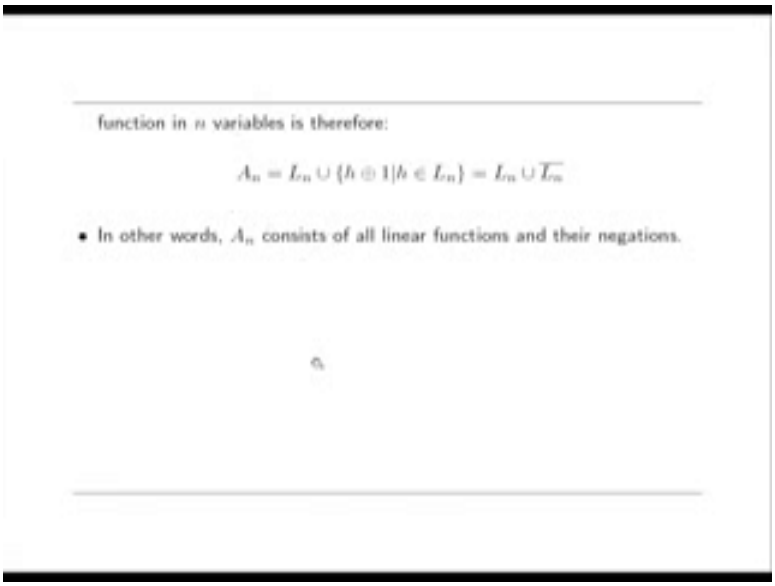
(Refer Slide Time: 08:45)



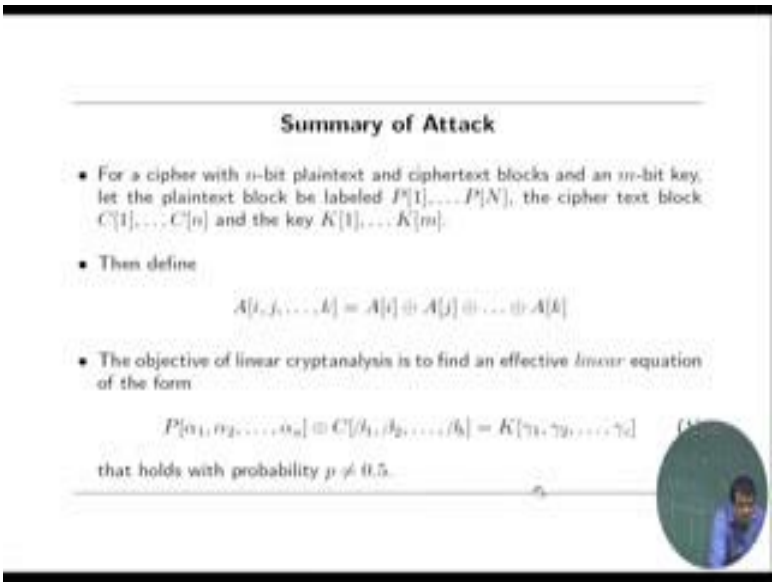
So, basically it is a s 1, s 2, s n. So, like if we have if we have a 2 table, we can have the 2 table for these, these are all binary values. So, this is our h. So, for different values of this 0, 0, we have different values for the output. So, this is the typical Boolean function, a Boolean function takes the n bit input and get a one bit output. So, now, a Boolean function is linear is linear if it can be written in this linear form like h a 1 x 1 s 1 XOR with a 2 s 2 where a A i's are basically 0 or 1 it is either 0 or 1.

If this forms then we call this function to be linear function. So, in this linear attack our aim is to find out the linear relationship between plaintext ciphertext and the key space we will come to that and this function is offline function if it is either h of x or it is h of x plus 1.

(Refer Slide Time: 10:14)

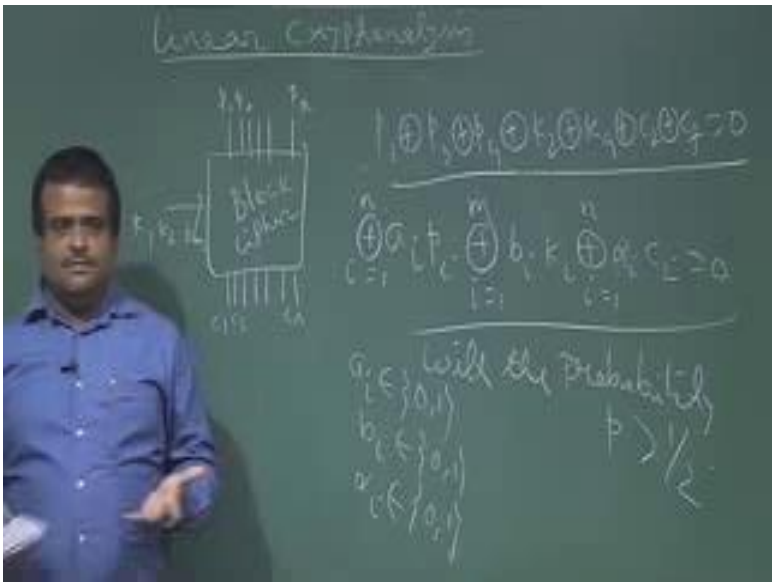


(Refer Slide Time: 10:16)



This is the set of all offline function we define. So, this is the idea of this attack. So, we have the so, basically it is a block cipher. So, n bit plaintext and n, n bit key suppose n bit key, so, this should be capital N. So, this plaintext; we are writing as p 1, p 2, p n and the ciphertext b 2 we are writing as c 1, c 2, c capital N and the key we are writing as k 1 k 2 this. So, basically we denote these a i i j k is basically this linear XOR operation basically. So, our m is to find out this alpha beta this i 1, alpha 1, alpha 2, alpha a and beta 1, beta 2, beta a, beta b, equal to k gamma 1 gamma 2 gamma a with some probability.

(Refer Slide Time: 11:18)



We want to see the linear relationship between the plaintext and ciphertext and the key space. So, this is the block cipher. So, we have a key over here. So, this is say p 1, p 2, p n. So, n bit block cipher we can take small n and this is c 1, c 2, c n, n bit. So, these are the cipher, this is the block cipher, it could be DES, it could be AES, anything block cipher encryption and we have key k bit key k 1 k 2 I mean k n, now we want to see some linear relationship between this suppose we want to see whether this p 1 XOR p 3 XOR p 5 XOR k 2 XOR k 9 XOR c 2 XOR c 7, these equal to 0 or not so; that means, we want to see some linear relationship between the plaintext key and ciphertext. So, in general we can see this XOR with a i p i, this i is from 1 to n XOR with b i k i, i is equal to k is varying from k is 1 to n XOR with c, we have used. So, d i or say alpha i c i, this i is varying from 1 to n again. So, with some probability with the probability p and p must be greater than half in order to mound this linear attack on this block cipher.

Basically we want to get; we want to try to get the linear relationship between the plaintext. So, this a i e and b i e is a i e is either 0 or 1 b i e is also either 0 or 1 and alpha is e also 0 or 1. So, we want to get, we want to try to get the linear relationship between then we can have the attack if we know this linear then we can we have the linear equations and then we can try to solve the linear equation to get the key. Key is unknown here and this is a known plaintext attack because we know the plaintext and the corresponding ciphertext if we know some relationship between these linear relationship and then if we know some plaintext and the corresponding ciphertext that is why it is

known plaintext attack then we have some linear equations and from that linear equation we can solve this linear equation to get this key. But how to get this such a linear equation so, because this block cipher is having many rounds, so it may be very difficult to find a linear relationship for a long round. So, what we can do?

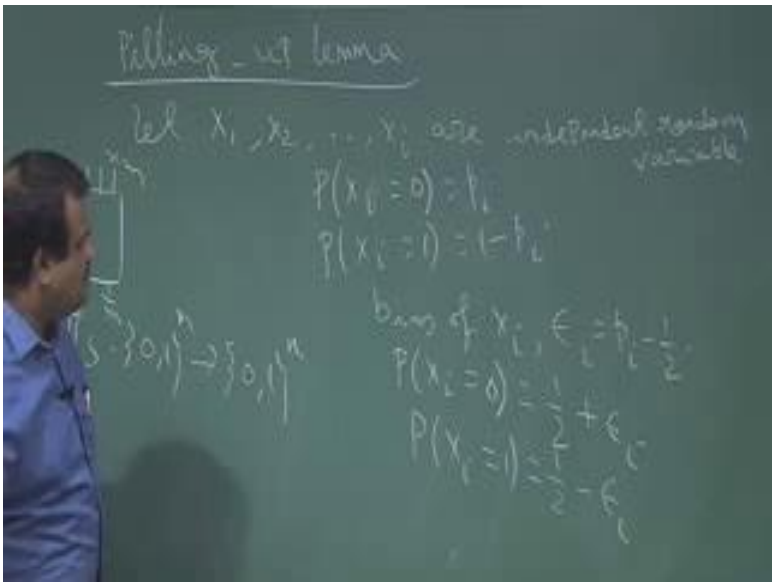
(Refer Slide Time: 14:59)

Suppose we want to find so this is say F 1, these are the round function we have k 1 k 2 like this F r and finally so, they have we have some entity now suppose for this, these are all round function suppose we want to see the linear relation say some linear relationship between in this F one say some say suppose x 1 say x i 1 XOR x i 2 XOR x i k XOR for this round key better use a superscript say j 1 j 2 j n XOR. Now, here this is the output after the first round and so suppose this is say we denote by y 1. So, y 1 superscript 1 so suppose y k 1 k we have used for key. So, y l 1 XOR y l 2 XOR dot, dot, dot, y l some value say alpha fine, this is 0, suppose we have some linear relationship in the first round and again suppose we have a linear relationship again in the second round in for the second round function.

Now the question is this is with some probability. So, this has this is with some probability. So, now, the question is how we can combine these to get a linear relationship for the whole round I mean for this input and the output input is basically so this is the plaintext and after last round, this is the ciphertext. So, now, the question is how we can have a, so we have a small this small linear relationship throughout the

round function. So, how we can combine these to get a linear relationship between the plaintext and the ciphertext with the round keys? So, this is this is by a theorem or lemma which is called piling up lemma. So, we have to understand what, how it is working then we will come back to this.

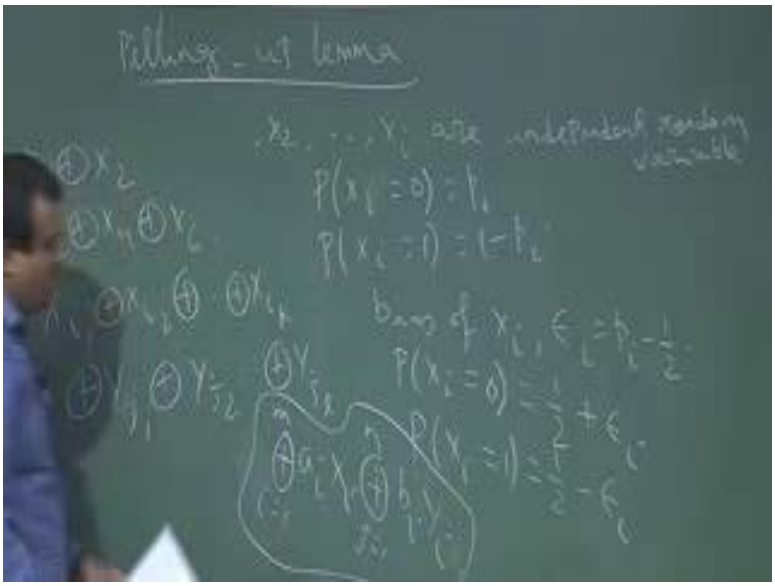
(Refer Slide Time: 17:56)



Let us talk about piling up lemma. So, some probability part we need to so to; understand this, let us take the random variable let x 1, x 2, dot, dot, dot, x i are independent random variable random variables basically these are basically input say suppose we have a S-box and we have say S-box is say n bit to n bit S-box n. So, we have n bit say this is x 1, x 2, x n, x m and we have y 1, y 2, y n. So, this is S-box and we want to see is there any linear approximation for this S-box is possible or not is there any linear relationship between input and output is possible or not. So, so these we are denoting by these x 1 x 2. So, obvious input so, these are 0 1 bits. So, these can take either values 0 and 1. So, the probability of this is what is called Bernoulli distribution. So, this is p i and probability of x i equal to 1 is 1 minus p i.

Now we define the bias of x i, bias of x i is basically denoted by epsilon i which is basically p i minus half so; that means, if p i is half then the bias is 0. So, this is a truly random bit then now if p i is not half then we have a bias and in that case probability of x i is 0 is basically bias plus half plus epsilon i and this probability of x i equal to 1 is basically half minus epsilon i. So, now, we want to so, this is the bias for epsilon i.

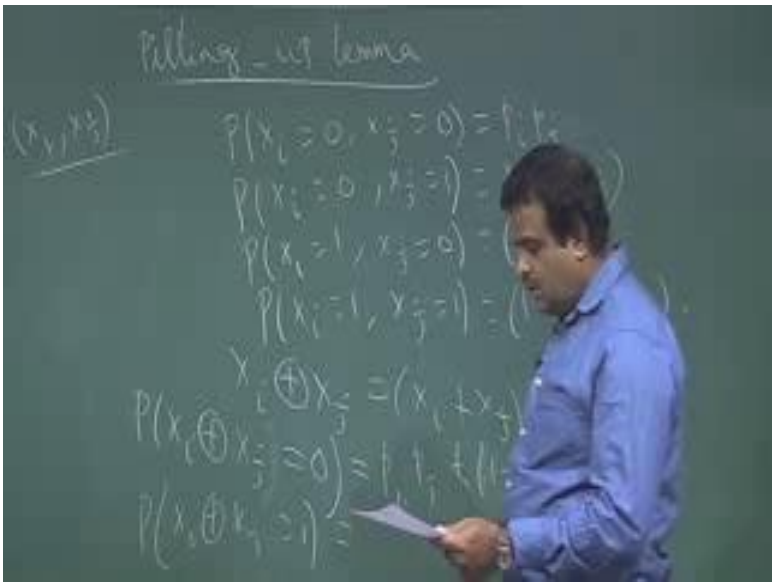
(Refer Slide Time: 20:50)



Now, we want to know the bias for say these kind of expression x or say simply x 1 x 2 what is the bias for epsilon what is the bias for x 1 XOR x 2 or any other thing x 2 XOR x 4 XOR x 6. So, this bias will give us the linear relationship or we can have this x x i 1 XOR x i 2 XOR dot, dot, dot, x i k XOR y now we have to bring the y, y i 1 y j 1 XOR y j 2 dot, dot, dot, y j l say. So, we want to know the bias of this. So, if we can have a bias which is not 0 then we can have a linear relationship between this. So, in general we are looking for this type of expression thus XOR summation of XOR a i x i one to n for S-box this is also XOR summation 1 to n b i y i.

We want to know the bias for this, if we know the bias then we can say the bias is not 0 then there is a linear relationship there.

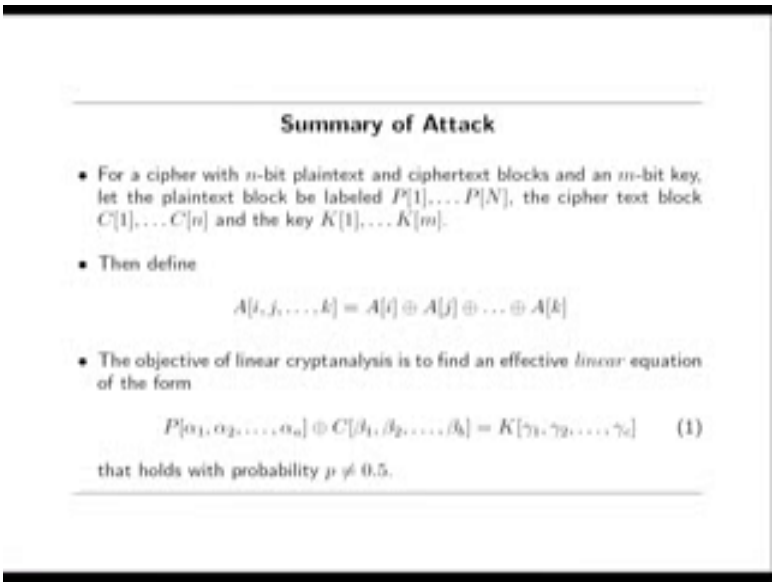
(Refer Slide Time: 22:55)



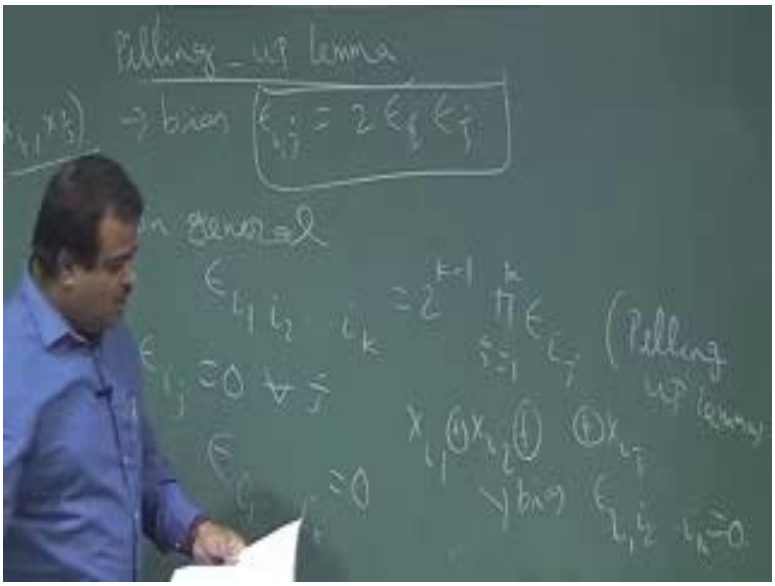
Let us calculate this, how we can get the bias for this say x 1 plus x 2 this kind of expression. So what is the probability of x i equal to 0 x equal to? So, we want to know the joint distribution of x i x j. So, this is basically these are independent random variable. So, probability is basically they are product p i p j. So, the probability of x i equal to 0 x j equal to 1 is basically p i 1 minus p j. So, probability of x i equal to 1 x equal to 0 is basically one minus p i p j and similarly this is coming from the independentness of this 2 random variable x y. So, this is one minus p i and one minus p j. So, now, we want to know this is x i XOR x j. So, this is basically a function of this joint random variable x j mod 2. So, so we want to know their probability. So, actually we want to find out the bias probability these equal to 0 when this can be 0 if both are 0 or both are 1. So, these or these, so, this is basically p i p j plus 1 minus p i 1 minus p j.

Similarly, for 1 these will be either this or this. So, sum of these 2 so; that means so what is the bias for this?

(Refer Slide Time: 25:13)



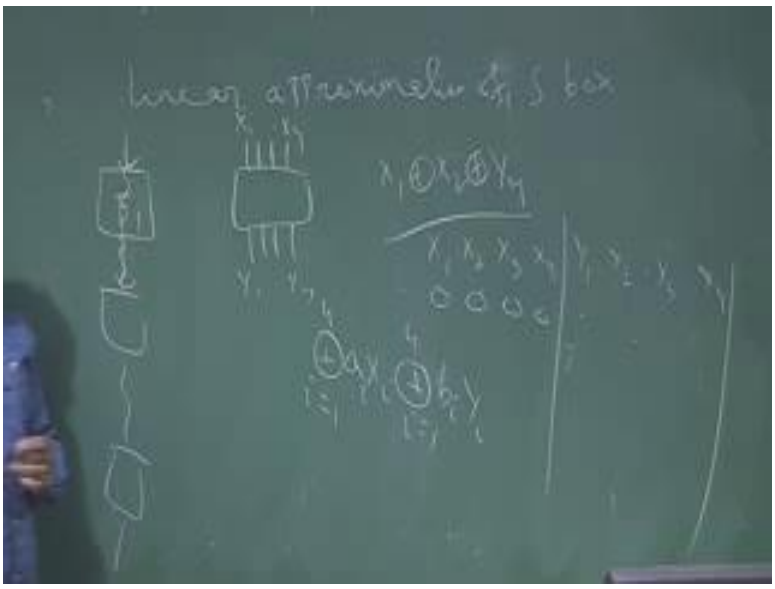
(Refer Slide Time: 25:15)



If we denote these so, if we denote the bias for this is epsilon 1 2, this is basically 2 of epsilon sorry epsilon i 1 i 2 because this is i j i 1 epsilon i epsilon i 1 epsilon i j is basically epsilon i epsilon j. So, this is the expression for the bias. So, now, the general version of this is called piling up lemma. So, the general version of this is basically in general we have this expression epsilon i 1 i 2 i k 2 to the power k minus 1 product of epsilon i j, j is equal to 1 2 k.

So, this is called piling up lemma this general form and this can be proved by induction because this is true for k is equal to 2 and by induction hypothesis we can assume this is true for k is equal to some m. So, it can be proved that this is true for general m, now if all the biased for this x i has 0 say x i j is 0 for all j then the biased for this is also 0 so; that means, x i 1 XOR x i 2 this is x i k. So, bias for this is basically epsilon i 1 i 2 i k. So, these will be also 0 if the all biased are 0. So, these way we can use this is the bias, so this formula we can use to find out the bias in general. How we can use this for, sorry.

(Refer Slide Time: 27:48)



How we can use this for linear approximation of the S-box? So, basically suppose we have 4 by 4 S-box, this is x 1, x 2, x 4, y 1, y 2, y 4. So, basically we will try to get see some expression like x 1, x 2, x 3, x 2, x 4 what is the biased of this if the bias is not 0 then we have a linear relationship like this. So, this we can just try to calculate from the true table of this S-box y 2 y 3 y 4. So, we have some values over here. So, these way we can calculate this try to get the we can take different different a x i, a i, x i, b i, y i. So, we can take different different values of a i and y i and we can use the piling up lemma to get the biased for this expression. So, if it is not 0 then we have a linear relationship.

So, these way we get the for block cipher we try to so this is F 1. So, we try to get some linear biased over here then here. So, we combine these 2 by piling up lemma then finally, we should get the biased between the plaintext here and the ciphertext and involve some key. So, then we have a linear relationship if the bias is not 0 then we have

a linear relationship or linear approximation then we have a then we can solve this with the unknown key and then it give us the solution. So, this is the linear attack.

Thank you.