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

Lecture - 49
More on Differential Cryptanalysis

We talked about; we have seen the differential attack which is a non generic attack on block cipher. So, we will continue that and we talk about some variant of differential attack like impossible differential attack, truncated differential attack, high order differential attacks. So, those are some variant of differential attack. So, in this talk, we will talk about one variant like which is called boomerang attack; boomerang attack on a block cipher this is also a non generic attack. So, let us just recall, what is the differential attack we discussed?

(Refer Slide Time: 00:55)

For the differential attack, it is attack on a block cipher on the r round block cipher. So, if we have a r round block cipher that mean you have the are many round function then the last round is F r. And this is the plaintext, this is the ciphertext, now if we have some this we called F and this is the rth round key and if we have some differential exists alpha is going to beta in F with significant probability high probability then we have seen we can find the here I mean the rth round key by mounting the differential cryptanalysis, but for that we need to have this. So, let us write the step of this attack.

(Refer Slide Time: 02:15)

These are the step of this attack step 1. So, this is the differential attack all block cipher r round block cipher. In the first step, what we do? We will try to find out that alpha beta. So, find n r minus 1 round differential alpha is going to beta; that means, if the input difference is alpha then the output difference will be beta in F with high enough, with high probability is the first step. So, we need to have this alpha beta otherwise it will not we cannot have the differential attack to one, this step 1.

Step 2: once we have this alpha beta then we can think of finding the rth round key or k r. For that we keep a counter for each possible rth round key k r and initialize this by counter 0, all the counter value are 0. This we have already discussed in the last lecture. Then step 3; step 3 what we are doing we are picking a plaintext. So, suppose plaintext is a n bit. So, this is our F this is our k r and this is our ciphertext. So, we know we have a alpha beta here if the input difference is alpha output difference will be beta. So, alpha is this differential we have.

Now we need to choose the input difference alpha in a plaintext. So, for that we take care uniformly we P k plaintext x uniformly at random add a random; that means, we just if the plaintext is say if it is n bit then the plaintext place is all possible n bits. So, we choose a x from this and number which is n bit number 0 1 bit at random. And then we choose we take x star which is basically x x r alpha is another plaintext so that their difference will be alpha. And we encrypt both this plaintext; encrypt both x and x star,

this is a chosen plaintext attack. So, we can choose the plaintext and can get the ciphertext because we have to choose the plaintext such a way that their difference is alpha. So, we encrypt both x y and we get the ciphertext say c 1, c n, c star.

And then we use this candidate key to; then we use a candidate k r to inverse to compute y which is basically if r inverse. So, for this we need to have so this is on c, we need to have k r and y star which is basically F r inverse c star k r. So, you choose a candidate key with this you have to do for all possible keys and then we check whether y x or y star is beta or not. If it is beta then we increase the counter corresponding to k r by 1; if is beta then increase the counter value of key r value of k r by 1. And then we will again go to we repeat step 3 we again choose a x. So, we do for all possible x until we get a significantly more value in the counter for some x r.

This is the step 4, we repeat step 3 many times until some k r has significant counter value; that means, suppose almost or count all counter values are say 10 12 and suddenly 1 counter we are of observing is more like.

(Refer Slide Time: 09:29)

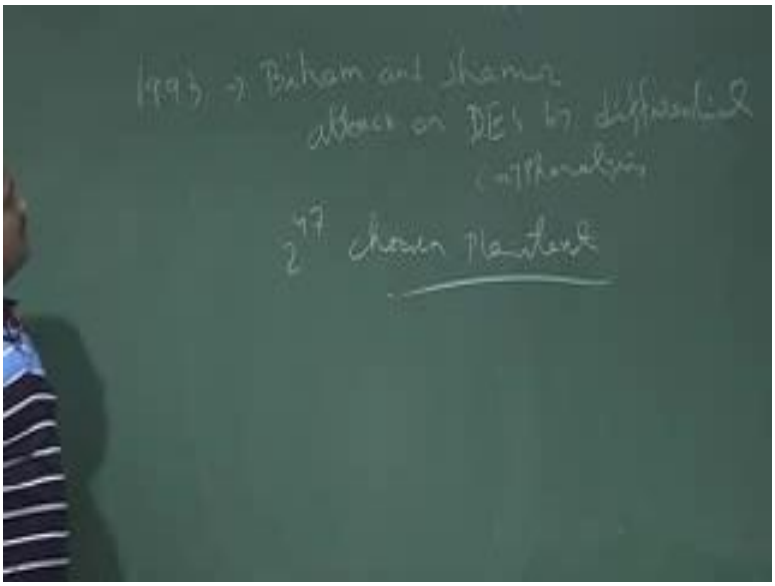
We have k r. So, we are taking all possible values of k r says 0 1 2 depending on the size of the k, k, k bit if k is say l bit then it is 2 to the power l minus 1. So, we take a particular k r and all are initialized by 0 then we do this once it is matching then we add a one like this. So, this process will repeat until we get a significant values in this counter

for a for a particular k r and that corresponding k r is say for k k m we get got a 100 and this like this then; obviously, this will be the key.

This is the version of the differential attack and for impossible differential attack there is one variant of this differential attack which is called impossible differential attack. So, this attack is similar. So, instead of high probability we have with very low probability. So, so we have a alpha beta difference here which is having very low probability. So, that is that is why it is called impossible and in this counter what we do we just repeat this and we just increase the counter like this and if we see in this counter we repeat the step 3 if some significantly counter value is low; has significant low value; low counter value.

So; that means, say all are say 50, 90 I say 81, 90, 79 suddenly 1 value said 2 then 2 is because we have this low probability for this. So, this is the version of impossible differential attack which was introduced by Biham in 1999 and this differential cryptanalysis was introduced on d s to break d s by Biham and by Biham and Shamir in 1993, I think 1993 and they broke the DES. So, this is the best known attack after the exhaustive search attack of electronics founder foundation.

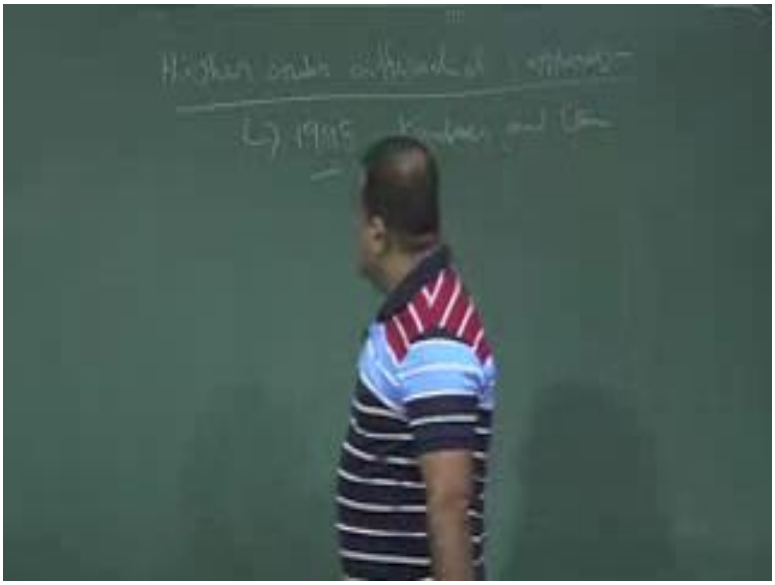
(Refer Slide Time: 12:29)



This is the, so, I think in 1993, I think have 1993 Biham and Shamir; Shamir attack on DES, my differential cryptanalysis analysis and for this attack they have to they have the chosen the size of the plaintext 2 to the power forty seven chosen plaintext. So, this is

chosen plaintext attack and size of the plaintext they have chosen is 2 to the power 47. So, that is the complex city of this attack. So, this was broke the DES was broke by this differential cryptal they have a book on this and so, there are some other variant of differential attack is also they are like truncated differential attack higher order differential attack.

(Refer Slide Time: 13:43)



We will not discuss all this. So, higher order. So, instead of first order will take second order difference higher order differential attacks differential cryptanalysis. So, these are there in the literature if you are interested you can have a look. So, this was introduced in 1995, i think 1995 by Knudsen and Lai and then another version is the truncated value truncated differential attack was introduced by Knudsen in 1995 and another version of this differential attack is boomerang attack which we will discuss here.

(Refer Slide Time: 14:49)

We will talk about boomerang attack boomerang attack on block cipher.

It is a variant of differential attack. So, we are looking for so, in differential attack what we are doing? We have a r round block cipher and we are just looking for a for F r and then we are just looking for a difference in this long round like r minus one rounds. So, we are looking for a difference alpha is going to beta in this long round. So, that difference may exist may not exist. So, that is the problem with differential attack because this is a long round.

The idea is if we instead of long round if we have a short round short difference like if we have difference up to this then if you have difference up to this then can you can you mound a attack. So, that is the version of that is the version of differential attack that is called boomerang attack. So, in boomerang attack what we have say we have a plaintext a we have this block cipher which is basically n bit n bit and suppose we break this into E 0 i mean E one E 0 so; that means, you have E 0 then we have a E one over here.

Now, suppose we know that there is some difference alpha is going to beta here with probability p. So, we know this suppose the difference exists suppose the differential alpha is going to beta with probability P P is high probability exists in E 0 and and suppose here also beta is going to some delta.

So, beta is going to delta with probability q in E 1. So, suppose these 2 difference we have like alpha is going to beta and beta is going to delta instead of having long difference if we can find out some short difference on shorter round this is the shorter round then whole round. So, like this then we can mound the and if this to probability are significantly high like more than half then we can think of then one can mound the differential boomerang attack. So, how so, basically what we will do here. So, idea of this attack is.

(Refer Slide Time: 18:37)

We know in, we know the different differential here is alpha beta when here differential is beta delta now what we do we first choose a plaintext over here. So, this is our block sample we will first choose a plaintext P 1 P 2 such that P 1 x r P 2 is alpha and this is a chosen plaintext attack not only chosen plaintext it is also chosen ciphertext attack. So, this boomerang attack is boomerang attack it is chosen plaintext as well as chosen ciphertext my chosen ciphertext will comes in a moment. So, now, the input difference is alpha now we. So, this is the block cipher. So, this is chosen plaintext attack. So, it will give us c 1 c 2. So, c 1 c 2 is the ciphertext corresponding to P 1 P 2.

Now, what we do we choose c 3 c 4 such that c 3 is basically c 1 x or delta and c 4 is basically c 2 x 1 delta now? So, that c 1 c 3 if you take there in put it they are difference is delta now if the difference is delta now here. So, if we have alpha over here will get beta over here will get delta over here with high probability. So, that is the difference we

have. So, if alpha is the difference over here and if the delta is the difference over here then we should have difference over here beta.

So, how can mound this attack? So, now we choose a c 1 c 3 c 4 like this. So, they are input differences. So, now, this is a chosen ciphertext only attack also. So, now, we get corresponding plaintext we will give the input as the ciphertext. So, we will get P 3 P 4.

Now, this is now P 3 P 4 we get. So, now, we know this fact that c one. So, we know this fact c 3. So, if we come back here c 3 export x o r with E 1 inverse c 4. So, this should give us beta which is again same as E 0 P 3 x o r E 0 P 4 so; that means, we check we check this if E 0 if this is. So, we check this if this is alpha then we increase the counter by 1. So, we are expecting this to be alpha because we are choosing this delta so; that means, we should get here beta so; that means, if we get here beta then their difference should be alpha.

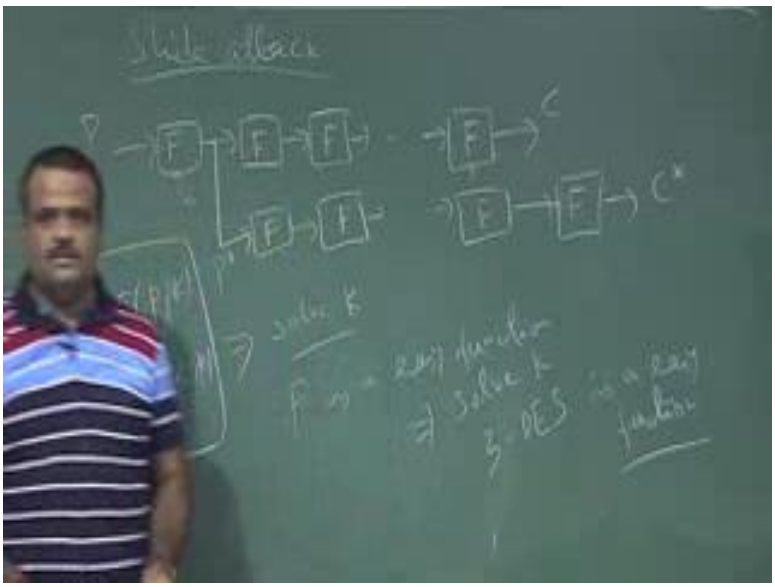
So, if we get alpha then we will increase the counter by one like this. So, this is basically the attack model of this boomerang attack, but here we have we are we do not require the long differential we can have short differential then also we can just mound the differential attack by this way. So, let us just write the attacking formal way step by step so, boomerang attack.

(Refer Slide Time: 23:01)

We just step 1. So, we know the alpha beta difference is there. So, we ask for we choose a plaintext P 1 P 2 such that P 1 x o r P 2 is alpha and we get the corresponding ciphertext from here we get the corresponding ciphertext c 1 and c 2. So, this is the step 1. So, step 2 is basically we choose c 3 which is basically c 1 x o r delta and c 4 is basically c 2 x o r delta so; that means, c one c 3 are difference delta and c 2 c 4 is the difference delta and then we ask though this is a chosen ciphertext also. So, you ask to decrypt this plaintext to get to get the decrypt the ciphertext to get P 3 P 4.

Once you are have P 3 P 4 then we check this is the step 3 then we check whether P 3 P 4 is alpha or not if it is alpha then we increase the counter. So, we repeat this step until we get some significant probability a significant frequency in this step. So, this is the boomerang attack now last attack now you will just give you the idea of slide attack which was introduced by Birupa of in 1999 Birupa (Refer Time: 25:04). So, this is slide attack this is also attack on block cipher.

(Refer Slide Time: 25:05)



Idea is we can slide the block. So, block cipher is r round. So, here in this attack we assume all the round functions are similar which is F. So, this is this is r round block cipher. So, this is plaintext, this is ciphertext and we are assuming. So, this is the ideal case, we are assuming all the round functions are same, for AES, for DES all most they are same because they are all (Refer Time: 25:43) structure, but in the first round we have a i P of we have a extra permutation operation and in the a E s we have same, but in

the last round we do not have the mix column operation. So, anyway, so, this is the say block cipher if where you are as if for in order to have this slide attack to work we need to have all the these are same and we have the same key now what we do we slide this one position.

Suppose this is P and this is c, this is plaintext this is ciphertext now we take these as a plaintext over here we slide this structure in one position. So, another F must be there and if we denote this by P star, so, P star is basically F of P and then what is the c star then the c star will because this is c basically. So, c star will be basically F of c now from these 2 equation if we can solve the key. So, key are we are assuming same. So, we have a same key for all round same key so, comma k comma k. So, from this if we can solve k solve k. So, that is that attack if you have this equation if we can solve k. So, this is not always it is possible to get the solution if this F is a easy function then one can then we can solve k from this and one example of easy function is 3 round DES is the easy function. So, this attack; they have applied on 3 round DES, this slide again, so, reduce round DES so.

Thank you.