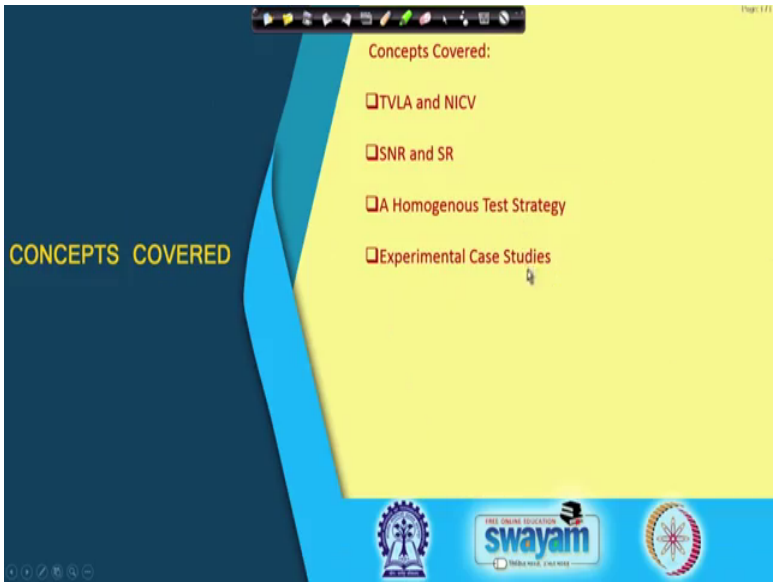
Hardware Security
Prof. Debdeep Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 41
Power Analysis-XVII

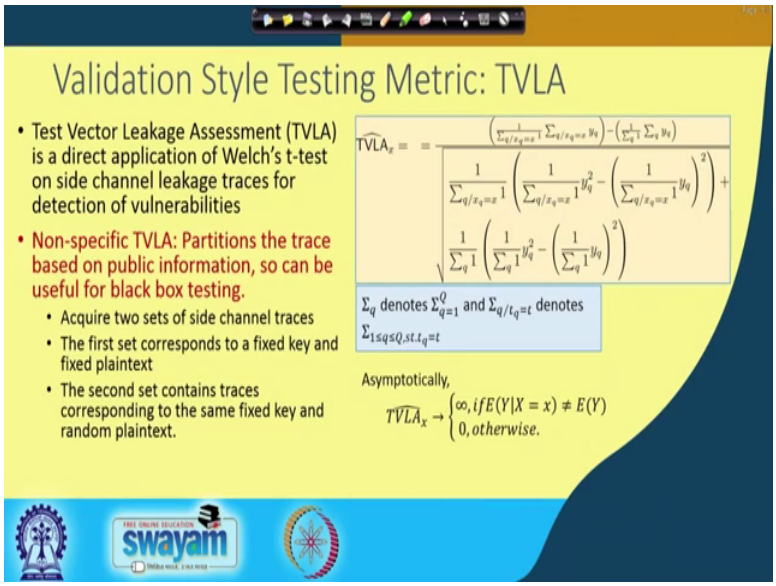
So, welcome back. So, we shall be continuing our discussions on TVLA or Test Vector Leakage Assessment.

(Refer Slide Time: 00:25)



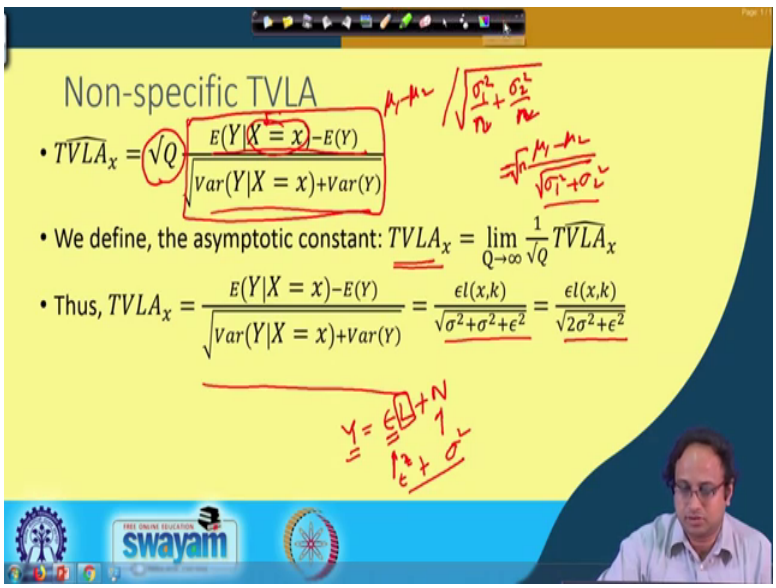
So, in particular right we shall be looking into TVLA and NICV and their connections between the like with SNR and the success rate and trying to see that how we can develop a homogeneous test strategy trying to combine both the conformance approach as well as the FIPS approach.

(Refer Slide Time: 00:37)



So, this is essentially where we stopped in the last class. So, this is the definition of TVLA which essentially in numerator part we have got the difference of two means and in the denominator part we have got like square root of sigma 1 square by n 1 plus sigma 2 square by n 2 as we have defined in the last class and as I said that, if the means are kind of different right; essentially you expect the TVLA will increase with the observations whereas, if the means are different means are similar in both the bins like when you are keeping the input constant and if you are varying the input at randomly, then you are expecting that this TVLA will approach 0 ok.

(Refer Slide Time: 01:16)



So, now with this background, let us try to see how we can you know like apply this. So, let us try to look into essentially that the formulation that I gave about TVLA. So therefore, so this is how we can define TVLA x ok. So, this is Q stands for the number of observations you are doing when; so this is an asymptotic I would say that the asymptotic expression of TVLA x ok. So, therefore, TVLA x right essentially stands for as I as we discussed, so in the denominator you have got sigma 1 square plus n 1 divided by n 1 plus sigma 2 square by n 2. So if you assume that n 1 and n 2 are roughly same then essentially you can replace both of them as by n whereas, in the numerator you have got mu 1 minus mu 2.

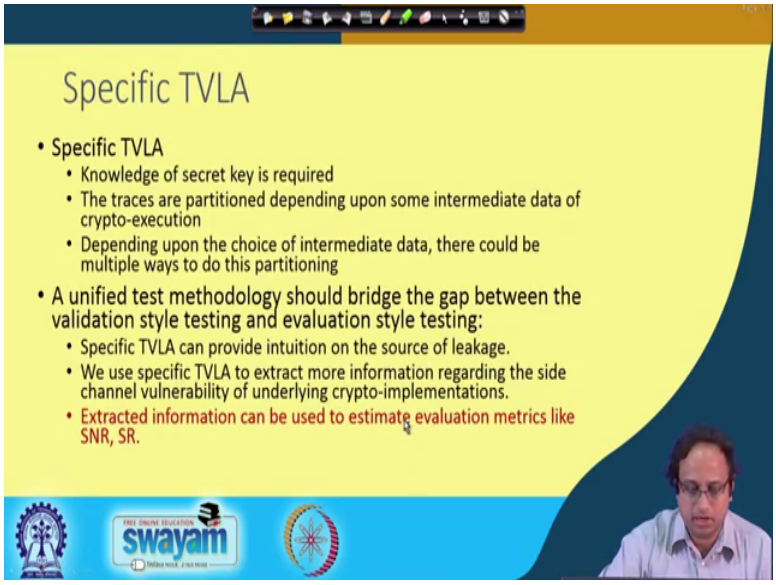
So, therefore, you can expect that this you can write as mu 1 minus mu 2 divided by square root of sigma 1 square plus sigma 2 square and this root n will come at the top right we will basically get multiplying numerator. So, that is essentially standing for this root Q, basically which kind of showing you the number of observations and square root of that and this essentially is pretty much the difference of these two means. In one case you have kept the input X equal to small x which is essentially holding it x and other case you are varying the input at random and the denominator is nothing but the sum of the two variances which is essentially shown over here.

So, therefore, the, I mean the asymptotic constant of this right essentially you leave out this part is only this part this is your asymptotic constant. So, therefore, the asymptotic constant is what we denote it as TVLA x ok. So, TVLA x is nothing but this, but you are removing this root k part. So, therefore, TVLA x stands for this expression which is E Y of E Y given X equal to small x minus E of E Y and divided by square root of variance of Y given X equal to small x plus variance of Y.

So, again right if I apply our expectation theorem and again remember that Y is equal to epsilon l plus l plus n then; that means, right when you are holding up X equal to small x and again taking the expectation, then again the noise component will vanish and therefore, you will only have epsilon l x comma k ok. Observe that here l takes a specific value and it is not a random variable, it is a value that it is taking. And what is epsilon Y I mean expectation Y? Expectation of Y is 0 ok. So, therefore, in the numerator I have got only epsilon small l divided by the variance of Y given X equal to small x.

Now this right essentially can be found in a similar way and this would stand up for sigma square I mean this is essentially standing for sigma square and the variance of Y will stand as sigma square plus epsilon square right because as you remember right that Y is equal to epsilon L plus N. So if I take the variance of Y, then that would mean that the variance for this will be epsilon square and this will contribute to sigma square and the variance of L is 1 ok. So, you will have got epsilon square plus sigma square and therefore, and if I add up these two things I will have got 2 sigma square plus epsilon square.

(Refer Slide Time: 04:41)

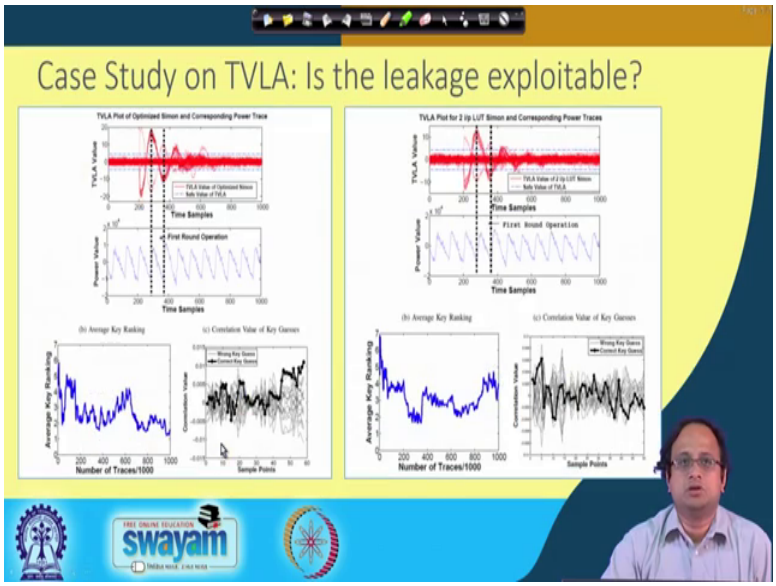


So, therefore, right this is with this you know like background we can go ahead and so this is essentially what is called as a nonspecific TVLA test. Now there is another version of TVLA which is called as specific TVLA. In the specific TVLA it is something like as we have seen in the difference of mean attacks. So, you basically target a specific location, you essentially have to know the secret key in this case. So again in this case you have to know the secret key as unlike the nonspecific TVLA and why you need to know the secret key because you will be targeting that targeting a register or targeting a specific location and then you will partition the trace depending upon the intermediate data of that target value. So, therefore, right depending upon the choice of intermediate data, there could be multiple ways of doing this partitioning because you can target at different locations and therefore, the partitions will of course, vary.

So, now, the question is right I mean you have got you know like both these approaches like you have got the CC test as well as the FIPS test and the question is whether you can develop a unified test methodology because unified test methodology should reach the gap between the validation style testing and the evaluation style testing because the specific TVLA while you know like so there are certain interesting observations like for example, the specific TVLA it can produce an provide an intuition on the source of leakage why because it is essentially based upon the secret key and therefore, right is kind of having an information about how the leakage is working inside your device.

So, we use specific TVLA to extract more information regarding the side channel, vulnerability of underlying crypto implementations. As of now right even the specific TVLA is just a yes no test because it again tells you that whether there is a leakage or whether there is no leakage, but it does not do any quantification. So, we will see how to do that quantification and more precisely we will try to use that extracted information to estimate the evaluation matrix like signal to noise ratio, success rate and so on.

(Refer Slide Time: 06:34)



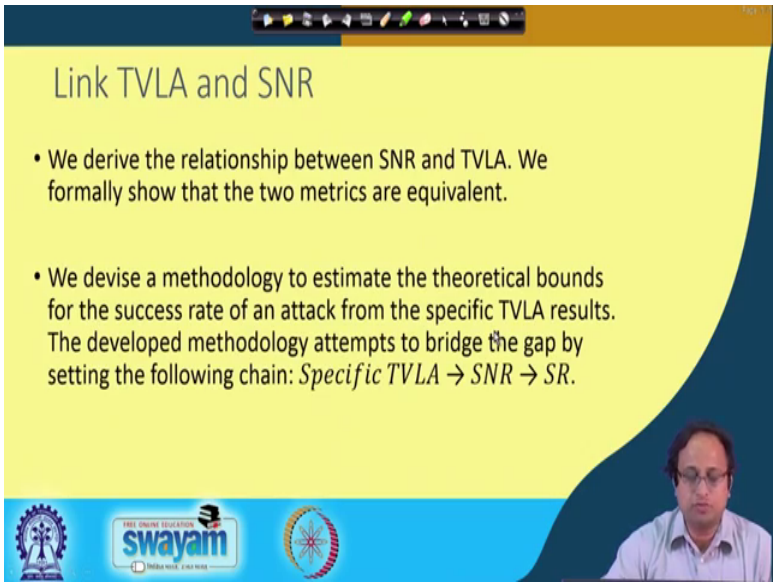
So, why; so these are very interesting experiment because it tells you that or tells you that whether TVLA can tell you whether the leakage is exploitable or not and the answer is negative. So, here is an kind of a implementation of a cipher which is called as Simon and Simon has been implemented at TVLA test has been done and as you can see right if you see the TVLA plot, so this is a you know like; you know like you know like at

corresponding TVLA which is been done on an optimized version of Simon and you can see that in this graph we have plotted the TVLA value with the time samples and if you observe there is a blue threshold region and the blue threshold region, generally stands for a value of plus minus 4.5 which kinds of tells you that with a reasonable amount of confidence you either accept the hypothesis which means you tell that you know if it is below that threshold, then you tell that our design is reasonably safe whereas, if it crosses it then you will say kind of suspect a potential leakage.

So, therefore, in this particular attack when we target the first round of operation we find that both cases, in both these designs the different versions of designs, I am not going to the design differences, but there are two different designs of the same architecture, same algorithm, same cipher. In both cases right there is a TVLA leakage why because it crosses this 4.5 threshold. As you can see in one case it reaches around 20, in the other case it reaches around 10.

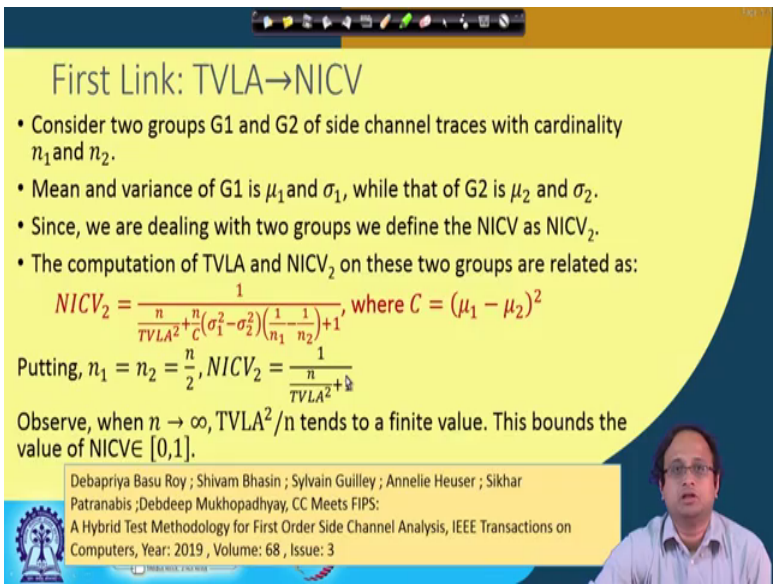
So, therefore, right TVLA analysis stops here. It just tells you or the FIPS evaluations stops here and tells you that both are vulnerable to side channel attacks whereas, if you do a side channel attack on them if you do an actual experiment on them, then we find that in this case we actually get the key quite easily if you see that we plot the average key ranking or the guessing entropy it falls quite drastically and if you also observe the correlation then you find the correlation kind of stands out from the other keys whereas in this case, when we do the attack then even with the same number of observations this correlation does not stand out which means that you know the key essentially is not leaked even if there is a vulnerable leakage. So, this experiment tells us that yes there is a leakage, but TVLA does not answer or does not quantify that leakage, does not say you that you know like how much amount of vulnerability is there in this corresponding design it is just a yes no test at the end.

(Refer Slide Time: 08:59)



So, now we would try two kind of link TVLA with us SNR and subsequently with SR or the success rate. So, we but try to derive relationship between the SNR and the TVLA, we formally show that the two matrix are equivalent basically ok. So, we basically devise a methodology to estimate the theoretical bounds for the success rate of an attack from the specific TVLA results ok. So, you basically do a specific TVLA and we try to kind of estimate the SNR as well as the SR. So, basically in a nutshell what we are trying to do is we are trying to develop this relationship as you can see in this graph that we are basically going from specific TVLA to SNR to SR or the success rate.

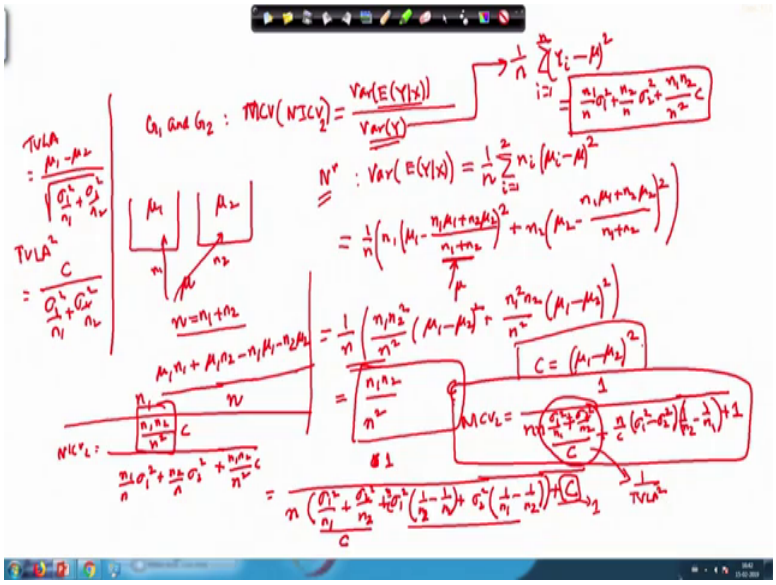
(Refer Slide Time: 09:42)



So in order to bridge that, the first result and the first link is this that essentially how do we bridge TVLA with NICV. So, consider that there are two graphs or two groups say G1 and G2 of side channel traces with cardinality n 1 and n 2 and the mean and the variance of G1 is mu 1 and sigma 1 sigma 1 square actually and in other case it is mu 2 and sigma 2 square ok.

Now, since we are dealing with two groups we define the NICV as NICV 2 and then we kind of relate the NICV 2 with TVLA using this expression. So, let us try to see right that how this expression works.

(Refer Slide Time: 10:31)



So, so basically what I essentially would like to do here is we would try to kind of you know like find out the so basically like we have got two groups now G1 and G2 and we are trying to kind of relate NICV we are basically calculating NICV for this so let me write it clearly, we are basically estimating NICV and I call this as NICV 2 because there are two groups over here. Later on I will be kind of relaxing it to what is called as NICV k.

So, therefore, write in both these groups, if I want to among these groups if I want to define NICV 2 then that stands for nothing, but variance of E Y by x divided by variance of Y right. I have got a mean say mu 2 and I have a global mean say mu. So that means, the numerator part so the numerator part essentially which means the variance of E Y given x right can be estimated as 1 by n. So note that total number of observations are n

here and in this group n 1 goes in this group n 2 goes. So, n is of course, equal to n 1 plus n 2

So, therefore, the variance of E Y given x is nothing but 1 by n sigma of n i mu i minus mu whole square and i is equal to 1 and 2 there are two groups ok. So, this if you kind of simplify, this will work out to 1 by n and again I will just write n 1 and inside this I will write mu 1 minus n 1 mu 1 plus n 2 mu 2 divided by n 1 plus n 2 this is your this is nothing but the global mean mu and then it will be a whole square plus n 2 into mu 2 minus n 1 mu 1 plus n 2 mu 2 divided by n 1 plus n two whole square.

So, this if you do a little bit of simplification this will be nothing but so basically what I do here is I use this n equal to n 1 plus n 2 and then I basically write this as say this component as n 1 n 1 so basically I just write this as n 1 mu 1 n 1 plus mu 1 n 2 that is mu 1 n 1 plus mu 1 n 2 minus of n 1 so this is basically does nothing but this minus n 1 mu 1 minus n 2 mu 2 divided by n 1 plus n 2 which is equal to n right because n 1 plus n 2 is equal to n.

So, therefore, right with this simplification this will work out as 1 by n 1 n 2 square divided by n square into mu 1 minus mu 2 whole square plus n 1 square n 2 divided by n square into mu 1 minus mu 2 whole square and that essentially can be again simplified as n 1 n 2 remember that I can take out this so let me write c equal to mu 1 minus mu 2 whole square and I can write this as c and this is essentially nothing but n square because I will have n cube here and again if I take n 1 n 2 common, I will have n 1 plus n 2 in the numerator and therefore, I will have n 1 n 2 divided by n square c.

So, this is your corresponding numerator part of this NICV 2 likewise you can estimate the denominator and the denominator if you kind of do little bit of simplifications again, so note that the denominator can be found out by this formula which is 1 by n sigma I equal to 1 to n Y i minus mu whole square because you are now finding out the variance of Y and this we essentially we will turn out to be n 1 by n sigma 1 square plus n 2 by n sigma 2 square plus n 1 n 2 divided by n square c ok.

So, I am not going through all the steps, but just writing the final result of both the numerator as well as the denominator. So, if you combine these two results therefore, your NICV 2 will be nothing but n 1 n 2 divided by n square c divided by n 1 by n sigma 1 square plus n 2 by n sigma 2 square plus n 1 n 2 divided by n square c and this you can

again write by dividing you know like the this by both the numerator as well as denominator by this component you can write it as c n divided by sigma 1 square by n 1 plus sigma 2 square by n 2 plus sigma 1 square into 1 by n 1 my 1 by n 2 minus 1 by n 1 plus sigma 2 square 1 by n 1 minus 1 by n 2 and plus c. Again you can divide both sides by c and if you divide the numerator and the numerator by c you have got 1 here and you will have pretty much this divided by c plus in this part, you will again have this multiplied with n by c so you will have this multiplied by n by c and this part will become 1 ok.

So, if you apply these right these simplifications then you eventually have NICV 2 is equal to 1 divided by n into sigma 1 square by n 1 plus sigma 2 square by n 2 divided by c plus n by c into sigma 1 square minus sigma 2 square into 1 by n 2 minus 1 by n 1 plus 1 this is your final formula and the interesting thing is right you can you can estimate that this essentially right I mean you can observe that you would you basically write in this equation so this is your equation for NICV 2 likewise you can also estimate your TVLA so let us use this part of the page to calculate that. So, your TVLA as I said right is nothing, but mu 1 minus mu 2 divided by square root of sigma 1 square by n 1 plus sigma 2 square by n 2.

So, the TVLA square, if you square the TVLA or TVLA square then that stands for c because mu 1 minus mu 2 whole square is c so I have just said c equal to mu 1 minus mu 2 whole square. So, c divided by sigma 1 square sigma 1 square by n 1 plus sigma 2 square by n 2. So, therefore, this part essentially is nothing but the reciprocal of your TVLA square.

So, therefore, what I do here is that instead of this part, I write here 1 by TVLA square. So, therefore, right I mean if you do this right then you are all set to get back to the slides to see what is the final expression. So, essentially right what we have here is this formula which is NICV we have got NICV 2 is equal to 1 by so on, but here you can see this n by TVLA square plus n by c into sigma 1 square minus sigma 2 square into 1 by n 1 minus n 2 plus 1.

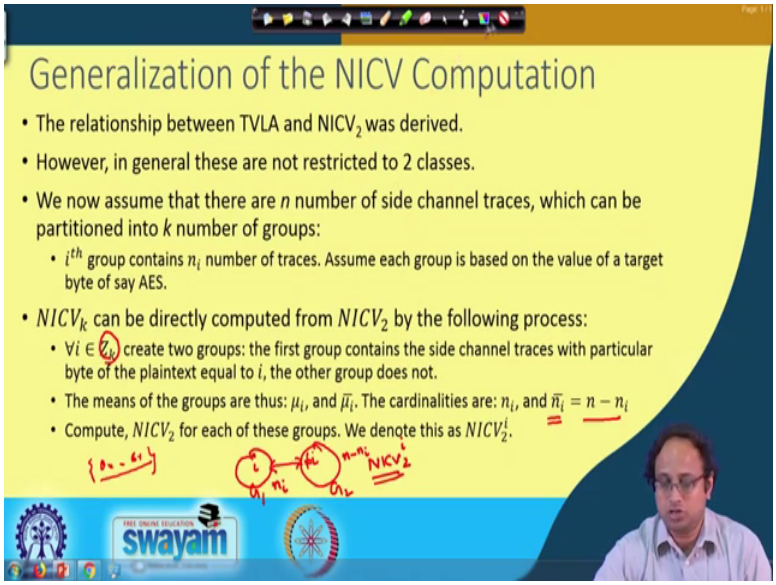
Interestingly if you now plug in n 1 equal to n 2 equal to n by 2 assuming that both of them are equinumerous, then it further simplifies to a nice form which is NICV 2 equal to 1 by n TVLA square, note that these will vanish now these parts will vanish now and

you will only have 1 by n by TVLA square plus 1 and note again that if I now make n large; that means, if I tend n to infinity then, this factor like n by TVLA although TVLA will shoot up to infinity, but n by TVLA square or TVLA square by n will tend to a finite value and therefore, it will bound the TVLA value to something between 0 to 1.

So, therefore, right I mean you can have a link with TVLA and NICV. Of course you have a link between TVLA 2 with NICV 2 ok. So, I mean sorry TV I mean you have a link between NICV 2 and TVLA square, but we would like to generalize NICV 2 to something which is NICV k for example, because you need not have only two classes, but you may have k classes.

So, therefore, right in order to do that so you can find more derivations of this work in this paper which is published in IEEE transactions, so computers in 2019 the exact reference is given here.

(Refer Slide Time: 20:41)



So now, what we will do is we will try to generalize this computation. So, the relationship between n TVLA and NICV 2 was derived in the previous slide. So now, however, in general these are not restricted to two classes I mean NICV can be across several classes for example, when you are doing an actual attack, there could be you are probably estimating a byte and the byte can take 256 values and therefore, there can be 256 classes.

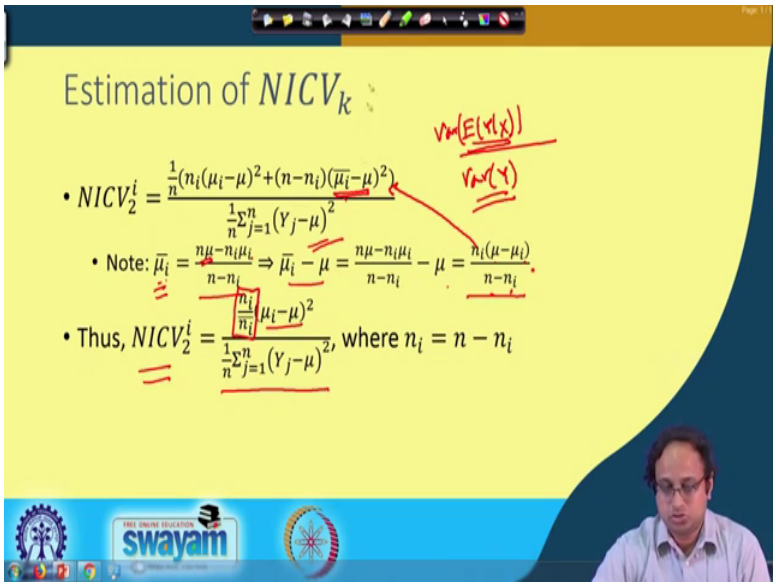
So, therefore, now we assume that there are n number of side channel traces which can be partitioned into k number of groups ok. In the previous case, we had considered only two groups, but now we are considering there are k groups and the ith group contains n i number of traces assume that each group is based on the value of a target byte of say AES.

So, now we can do what we can do is we can so interestingly we can estimate NICV k from NICV 2 by a nice iterative approach. So, what we do is we basically you know like for any value of k we basically consider at z k. So, z k would mean like anything which is essentially belonging to you know like from 0 to k minus 1 ok.

So, you basically considered consider all the corresponding values of the target byte and then you basically create two groups in one group you basically assume that say I call it as G 1 that the byte or the target byte takes a specific value say i and in the other group you assume that is G 2 you take assume that the you find out that you know like that the byte does not take the value of i. So, therefore, right I mean it is not equal to i. So, therefore, you again can calculate the NICV 2 in the similar manner because now you have got two groups.

So, you basically calculate NICV 2 in this manner note that here if n i goes then here n minus n i goes and let me denote that as n i bar ok. So, n i bar is nothing, but n minus n i and now i this particular NICV 2, I actually also parameterize it by i because I am doing it for the value of I note that I can take several values like in AES, it can take 256 values 0 to 255. So, I calculate all these NICV 2 i s and from there I try to estimate NICV k ok.

(Refer Slide Time: 23:05)



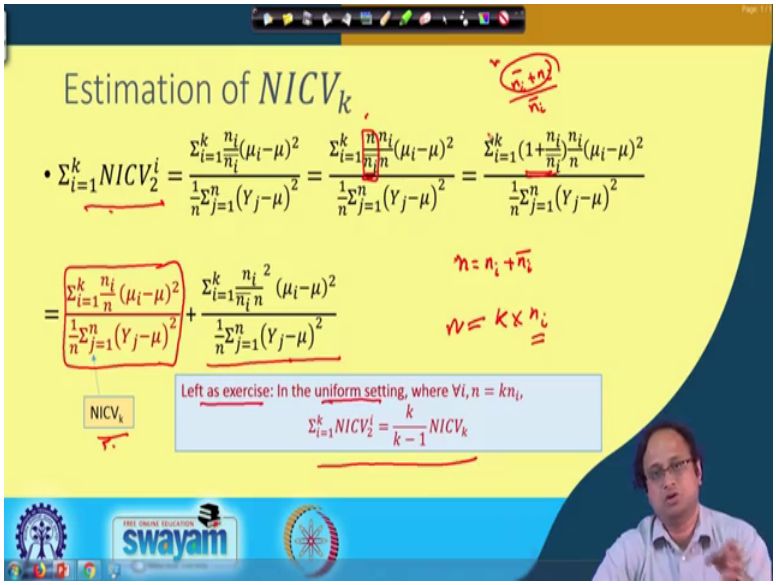
So, what I do therefore, in order to do that is as follows; we basically do a very simple estimation which is essentially follows easily from this derivation. So, NICV 2 right essentially would essentially simply be this, this is exactly from follows from what we discussed already there are two groups now in one group the mean is mu i, in the other group the mean is mu i bar and this is the variance of the means in the numerator.

So, therefore, you have got 1 by n multiplied by n i into mu i minus mu whole square plus n minus n i into mu i bar minus mu whole square and this is divided by the total variance, variance of Y remember right that our NICV essentially was nothing, but expect I mean essentially was your the variance of expectation of Y given x divided by the variance of Y. So, in this case we are calculating the variance of means whereas, here you are calculating the overall variance and this is the overall variance

So, therefore, now we will just apply a very simple trick which is like mu i bar is can be written in this way so this is nothing but a writing the total mean in terms of mu i bar and mu i and therefore, write mu i bar minus mu i will work out to be this minus this and therefore, you can write it in this way which is n i into mu minus mu i divided by n minus n i. So, if I take this and if I plug in over here because I want to kind of estimate or replace this mu i bar minus mu i and I just kind of apply this over here, then I get a closed form value of NICV 2 i can take out this mu i minus mu whole square as common and therefore, I have got this as your corresponding result. So, you basically have this as

your corresponding result and then you have got n i by n i bar as a constant as a constant multiplication to mu i minus mu whole square.

(Refer Slide Time: 24:57)



So, now what does or how does that help? So, you can see here now once we have got this form we can actually do this some simple trick, we can now kind of some of these NICV 2 i over all values from i equal to 1 to k, if you do this you get a very interesting result, you see that if i sigma over the numerator because the denominator remains constant it does not depend upon i as such it is just dependent on j. So, then that would mean that n i by n i bar mu i minus mu whole square i sigma over i equal to 1 to k and note that this n i by n i bar i can write as n divided by n i bar into n i by n right I am essentially because n and n cancels out.

So, now if I sigma this right then see if we sigma this and again remember that n equal to n i plus n i bar so; that means, I can; I can write n I can write n as n as n i plus n i bar this is your sum of the two groups, then essentially right this part or n by n i bar right this part essentially you can write as 1 plus n i by n i bar because this part is nothing, but n i bar plus n i divided by n i bar and that stands for n and that is exactly this part this fraction.

So, therefore, once you have split this into two parts then you see that the first part which you get over here is this part shown in red and the second part is essentially this part and what is the first part the first part is nothing but NICV k because again you can see this is the variance of Y and again now this is the variance of all the means there k means which

you are considering here so; that means, you essentially can get you can write this as an equation that this if you are basically summing them up then you get NICV k plus some additional term so if you sum this up and if you subtract out this part you should get NICV k.

In fact, if it is a uniform setting; that means, all of them have got equal kind of partitions, then you can pretty much write n that is total observations is k times n i where each partition has got n i and if you plug in that then you get a very simple formula as shown over here and this I kind of leave it to you as an exercise that is you can write the sigma of I equal to 1 to k NICV 2 i as k divided by k minus 1 into NICV k. So, now, we have basically come to this point that we have got the value of NICV k.

So, now once you have got NICV k right, we would like to basically apply this and get the you know and essentially right we know that we already have seen the relationship between NICV k and SNR and therefore, right we basically have established a relationship from TVLA to NICV or in particular NICV k and we already know how to go from NICV k to the SNR and therefore, we basically know how to go from TVLA to the SNR ok. So, this I will continue in the next class.