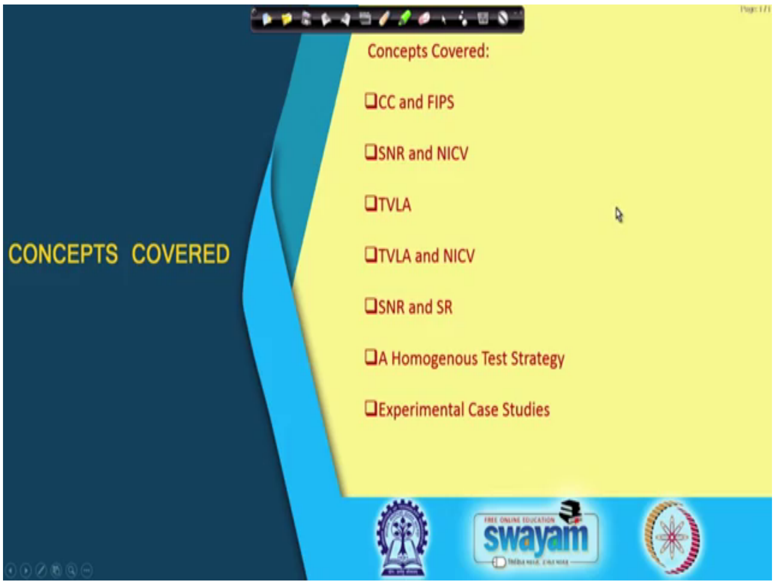
Hardware Security
Prof. Debdeep Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 40
Power Analysis – XVI

So, welcome to this class on Hardware Security. So, we shall be continuing our studies on power attacks and in the form of side channel analysis.

(Refer Slide Time: 00:24)



CONCEPTS COVERED

Concepts Covered:

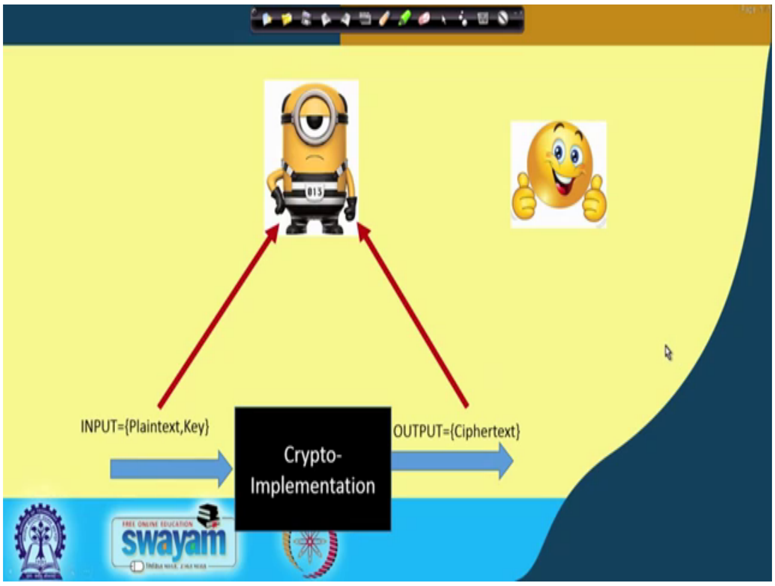
- ❑CC and FIPS
- ❑SNR and NICV
- ❑TVLA
- ❑TVLA and NICV
- ❑SNR and SR
- ❑A Homogenous Test Strategy
- ❑Experimental Case Studies

In particular today's, we shall be studying a different perspective on side channel analysis which is essentially to test whether a given cryptosystem is vulnerable to side channel attacks. So, in this context right we shall be studying two approaches or which are well established which are called as common criteria and FIPS test and we shall be trying to look at the merits and demerits of both, essentially try to understand what this stands for. We shall be trying to look into some parameters of both CC as well as FIPS.

For example, as there are abbreviated as signal to noise ratio or SNR as we have seen, there is another important parameter which is called as NICV. We shall be trying to look into a test approach which is commonly called as the Test Vector Leakage Assessment or TVLA a and the we shall be trying to see the link between TVLA and NICV.

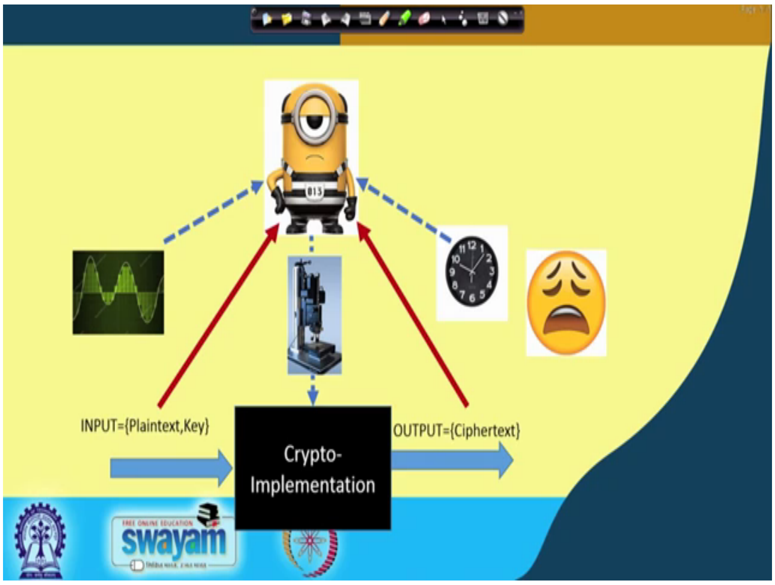
So, our objective will be trying to develop a homogeneous test strategy trying to kind of combine both CC as well as FIPS and trying to get the best of both. So, we shall be trying to look into few interrelationships like within TVLA and NICV between SNR and SR and finally, conclude with some experimental case studies to see how we can apply this test strategy.

(Refer Slide Time: 01:38)



So, to start with we all know that we have got this cryptographic implementations and the essentially the story is that if the cryptographic algorithm is nicely developed then the revolution of the plaintext and the output ciphertext does not give information about the key. So, therefore, if there is an adversary who is observing classically the input as well as the output then we are kind of safe I mean our cryptographic algorithms are quite sound to prevent or at least reasonably be resisting you know such kind of adversaries.

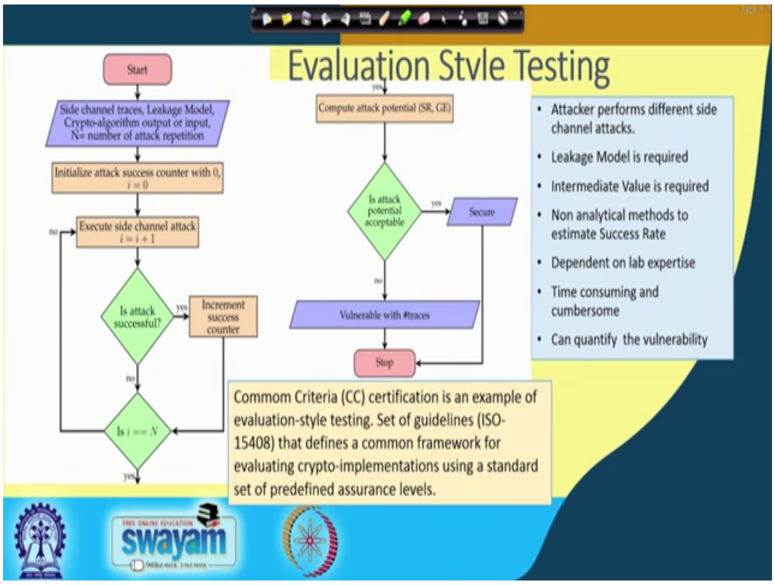
(Refer Slide Time: 02:11)



But then right as we have been studying that there are some other things for example, what are called as side channels like essentially there could be several forms of side channels; there could be power, there could be electromagnetic, there could be timing.

So, the question is right how do we really you know like under such kind of I would say stronger adversaries who are equipped with you know like instrumentations to do this kind of attacks, a all I mean the at the scenario is that most of our designs are vulnerable. So, therefore, right we need to develop an approach to know how our methodologies are sound against side channel attacks.

(Refer Slide Time: 02:45)



Evaluation Stvle Testing

- Attacker performs different side channel attacks.
- Leakage Model is required
- Intermediate Value is required
- Non analytical methods to estimate Success Rate
- Dependent on lab expertise
- Time consuming and cumbersome
- Can quantify the vulnerability

Commom Criteria (CC) certification is an example of evaluation-style testing. Set of guidelines (ISO-15408) that defines a common framework for evaluating crypto-implementations using a standard set of predefined assurance levels.

Start
Side channel traces, Leakage Model, Crypto-algorithm output or input, N= number of attack repetition
Initialize attack success counter with 0, $i = 0$
Execute side channel attack $i = i + 1$
no
Is attack successful?
yes
Increment success counter
no
Is $i == N$
yes
yes
Compute attack potential (SR, GE)
Is attack potential acceptable
yes
Secure
no
Vulnerable with #traces
Stop

So, there are different styles which has been proposed in literature two of the most common styles and so, first that will I will start with is what is called as a common criteria certification which is an example of evaluation style testing.

So, in this particular approach this was originally is also standardized in ISO in the 15408, it defines a common framework for evaluating cryptographic implementations using a standard set of predefined assurance levels. So, therefore, right what do we do here is essentially depicted by this flow chart; for example, what we do is we if I want to adopt an evaluation style testing then the attacker performs different side channel attacks.

So, therefore, as we have seen that there are different forms of side channel attacks the adversary kind of tries to of the evaluated basically tries to apply these various attack techniques one by one, on the target cryptographic implementation. So, of course, right when you are applying a specific attack as we have seen like when we are doing say DPA or when we are doing template attacks right all if we are doing mutual information base attacks, one thing which is very important is a leakage model.

So, therefore, in this particular testing styles right we essentially assume that the adversary has an idea or the evaluator has an idea about the underlying leakage model. And also he makes a target like a if we remember right we were targeting the output of the s box or the input of the s box so, there is specific target on which we were attacking.

Now note that in an given cryptographic implementation right there can be several targets ok.

So, therefore, right I mean what is important is also to know like essentially, we are assuming here that the adversary also has got some kind of knowledge about the target which is essentially better suited for doing an attack because if we are probably making an attack on a wrong target and then you can actually come to wrong conclusions ok. So, therefore, it is important that you make kind of you know like an exhaustive or at least so, reasonable exploration on various targets and you be you are confident about your final conclusion.

And at the same time right I mean this is a non analytical method to estimate the success rate, which means you are doing the attack and you are measuring the actual success rate from real life experiments. And of course; that means, that it depends on the lab expertise, it depends upon how much level of expertise you have on doing side channel attacks and therefore, this is a pretty much time consuming and cumbersome approach and although it can quantify vulnerability because it is actually doing an attack, but this is a non analytic approach.

So, if we are now go through this flowchart and just quickly see how this testing approach works use as follows. So, you probably would like as an evaluated develop capture several side channel traces, you will make an assumption on the leakage model. And then you will be you know like we are doing the attack in the crypto algorithm from the output or the input like you will processing the plaintext or the ciphertext and then you will be starting your attack procedure.

Now, now what you will do is that, you will be starting your attack procedure you will be continuing with your attack and if your attack is not successful then you essentially again try the attack. So, basically you try repeatedly to do the attacks and therefore, you kind of increment or success counter if your attack works correctly.

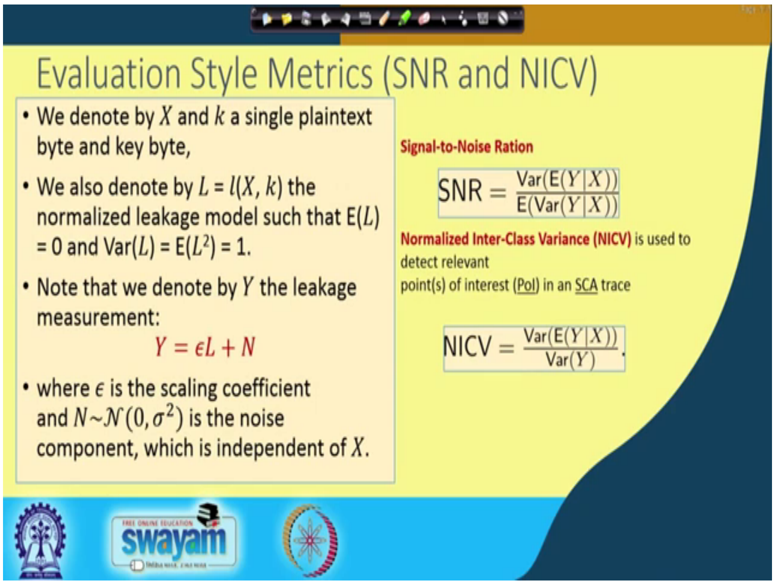
So, finally, right you based upon the number of times say you if you are trying say 5000 times an attack and if you for example, are able to do an attack say 4000 times. Then from this statistic right or from this values you try to estimate the success rate and also the guessing entropy as we have seen.

So, the now if given you know like the success rate and the guessing entropy you basically make a conclusion, that whether depending upon you know like the depending upon the you know like the assurance level that you want kind of you know like implement or deploy your device.

For example it may be a very highly sensitive application it maybe not so, highly sensitive applications. So, depending upon your application scenario you make a decision whether this attack potential is acceptable or not. If it is acceptable then you say that it is secure under that context, otherwise you say that it is not secure which means it is vulnerable with so, many amount of traces.

So, as you can see that the entire approach is non analytical, it is basically you know like based upon that you are doing an attack and based on the performance of your attack you are making a conclusion ok. So, therefore, the I mean it I mean if you really want to adopt this evaluation style for your laboratory, then you need to also have a reasonable amount of expertise to do this attacks.

(Refer Slide Time: 07:18)



Evaluation Style Metrics (SNR and NICV)

- We denote by X and k a single plaintext byte and key byte,
- We also denote by $L = l(X, k)$ the normalized leakage model such that $\mathrm{E}(L) = 0$ and $\mathrm{Var}(L) = \mathrm{E}(L^2) = 1$.
- Note that we denote by Y the leakage measurement:

$$Y = \epsilon L + N$$

- where ϵ is the scaling coefficient and $N \sim \mathcal{N}(0, \sigma^2)$ is the noise component, which is independent of X.

Signal-to-Noise Ration

$$\mathrm{SNR} = \frac{\mathrm{Var}(\mathrm{E}(Y|X))}{\mathrm{E}(\mathrm{Var}(Y|X))}$$

Normalized Inter-Class Variance (NICV) is used to detect relevant point(s) of interest (PoI) in an SCA trace

$$\mathrm{NICV} = \frac{\mathrm{Var}(\mathrm{E}(Y|X))}{\mathrm{Var}(Y)}.$$

So, there are different metrics which has been proposed to in this evaluation style two of the most common ones are what are called as SNR, as we have seen as Signal to Noise Ratio and the other one is what is called as NICV or what stands for the Normalized Inter Class Variance. So, let us try to define this in our context so, we will make in order to formalize or define this notations we will basically start with certain definition of our leakage model.

So, we basically it again have got an intermediate state so, let us denote it as X and suppose k is a single you know is the corresponding key byte or it could be a key word also ok. So, without loss of generality you can take it as byte ok. So, now, what you do is, you also denote the corresponding leakage so, the leakage now depends upon this intermediate value which is X and also on the secret key ok.

So, therefore, what I mean is that the leakage will depend upon either you can process the attack from the input size which means the from the plaintext size or from the cipertext size. So, again without loss of generality let me assume that the you are doing the attack now from the plaintext size and suppose the plaintext is X you make a guess of for the key byte or the key byte is say k when you are actually doing the attack. And therefore, this X gets mixed with the secret key gets processed by say something like an s box or so, and then you get a target ok.

So, therefore, the leakage is basically a function of X and k and that is denoted as this function l X comma k and is denoted by this random variable capital L. So, again we can make without loss of generality an assumption that the mean of this is 0 and the variance of this L is equal to E of L square which is equal to 1. So, we can essentially define a corresponding leakage this parameters are satisfied without loss of generality.

So, now, what we do is we note that the corresponding you know like this is the actual I would say the deterministic part of the leakage, but this gets kind of contaminated with the Gaussian noise as we have seen previously. So, therefore, right the actual observed leakage which you see is denoted here as Y. And that is nothing, but kind of the superimposition of the deterministic part which is denoted by L multiplied with the scaling coefficient say epsilon plus the noise which is nothing, but a Gaussian, whose mean is assumed to be 0 again without loss of generality and the variance is denoted as sigma square.

So, now, we have got this Y as your output observed leakage. So, now, we would like to define our signal to noise ratio. So, remember right we define a signal to noise ratio it is kind of again you know like a kind of again define redefining that, but you can observe that essentially they are the same. So, the numerator is exactly the same for example, it is the variance of the expectation of Y given X ok. So, this as I said in the previous class is the single component of your leakage consumption, where as a denominator stands for the noise.

So, therefore, here you can see that it is the variance of expectation of Y given X; that means, given the corresponding input class you are basically trying to define the corresponding leakage. So, essentially if the variance is high then that means, you can easily distinguish the X values and therefore, your attack works so, therefore, this contributes to the signal component of your side channel attack.

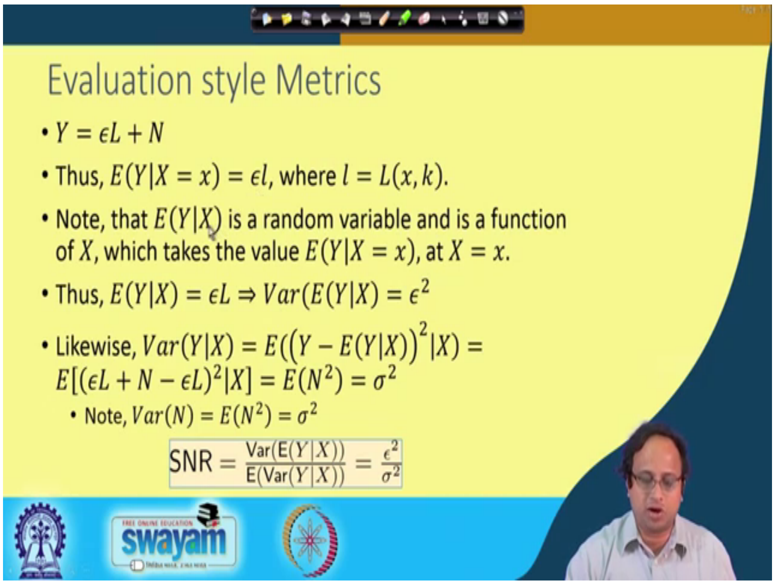
On the other hand right I mean this is the noise component ok, this I will kind of clarify very soon, but you can right now note that it is very easy to remember it is the variance of expectation of Y given X divided by the expectation of variance of Y given X. So, this is a kind of convenient formula to apply to estimate the signal to noise ratio. When you are estimating the signal the other parameter which is called as NICV or the Normalized Inter Class Variance it is kind of similar to the SNR except that the denominator, has been replaced from expectation of variance of Y given X to the variance of only Y ok.

So, you can see that I have just replaced this from variance of our expectation of variance of Y given X to only the variance of Y. So, note that if you want to estimate this parameter; that means, if you want to estimate the denominator then you need to kind of have a knowledge about X, you need to kind of estimate X because this is conditioned on X ok.

And if you want to a kind of have a knowledge about X right, you also need to know the sub part or the secret key ok. So, therefore, for SNR estimation you need to have a knowledge about the secret key whereas, here when you are measuring the variance of Y you are basically doing it only on the output leakage and therefore, you did not need have any knowledge about the key.

So, often this NICV is very useful it is used for to find out the point of interest on the side channel trace, like essentially you can kind of pretty much apply the NICV to know like, what are the sequence of operations in your implementation. Like you are doing the mix column, then shift row and add round key and so, on.

(Refer Slide Time: 12:17)



Evaluation style Metrics

- $Y = \epsilon L + N$
- Thus, $E(Y|X = x) = \epsilon l$, where $l = L(x, k)$.
- Note, that $E(Y|X)$ is a random variable and is a function of X, which takes the value $E(Y|X = x)$, at $X = x$.
- Thus, $E(Y|X) = \epsilon L \Rightarrow Var(E(Y|X) = \epsilon^2$
- Likewise, $Var(Y|X) = E((Y - E(Y|X))^2|X) = E[(\epsilon L + N - \epsilon L)^2|X] = E(N^2) = \sigma^2$
  - Note, $Var(N) = E(N^2) = \sigma^2$

$$\boxed{\mathrm{SNR} = \frac{\mathrm{Var}(\mathrm{E}(Y|X))}{\mathrm{E}(\mathrm{Var}(Y|X))} = \frac{\epsilon^2}{\sigma^2}}$$

So, now let us try to kind of look into these metrics in a little bit more details right and the again we will start we will adopt this. So, we will throughout our discussion we will be assuming this leakage model which is Y equal to epsilon L plus N. And now we want to calculate the numerator part which is the variance of expectation of Y given X. So, let us recapitulate this a little bit I mean what this means like this essentially nothing, but the conditional expectation.

So; that means, if I say you expectation of Y given X equal to small x ok; that means, in this particular leakage I am fixing the value of X and then I am calculating the expectation. So, note that since it is plus I can apply the expectation on this, plus the expectation on the noise component and the expectation on noise component is 0 so, therefore, this do not matter ok. So, if you remember right noise is a Gaussian which is essentially 0 comma sigma square and therefore, the expectation of noise will be 0 so, this component will not bother us. So, the other component is where when you are fixing L right, then L takes a specific value deterministic part gets fixed because you are fixing this input x ok.

The moment you are fixing x the leakage gets fixed and the leakage gets determined by X as well as k because k is here under lying secret on which you are doing the computation. So, therefore, right if I take the expectation right, then the expectation is essentially nothing, but epsilon L. And now what is E Y given X which is the conditional expectation it is nothing, but I have note that this is a value this is when you are saying when you are fixing a value for the condition, then expectation of Y given X equal to small x is a value ok. But when you are talking about expectation of Y given X where X is a random variable then this is also a random variable and actually expectation of Y given X is a random variable and is a function of X ok.

So, the way we kind of observe it or see it is at which takes the value of E Y given X equal to small x at X equal to small x. So, therefore, epsilon or expectation of Y given X is nothing, but epsilon L. So, I can replace this random with this value l by the random variable epsilon L. So, now, if I want to calculate the variance of this right, then essentially this is nothing, but epsilon square and the variance of L, but we as I said that variance of l was assumed to be 1 so, therefore, right we get epsilon square.

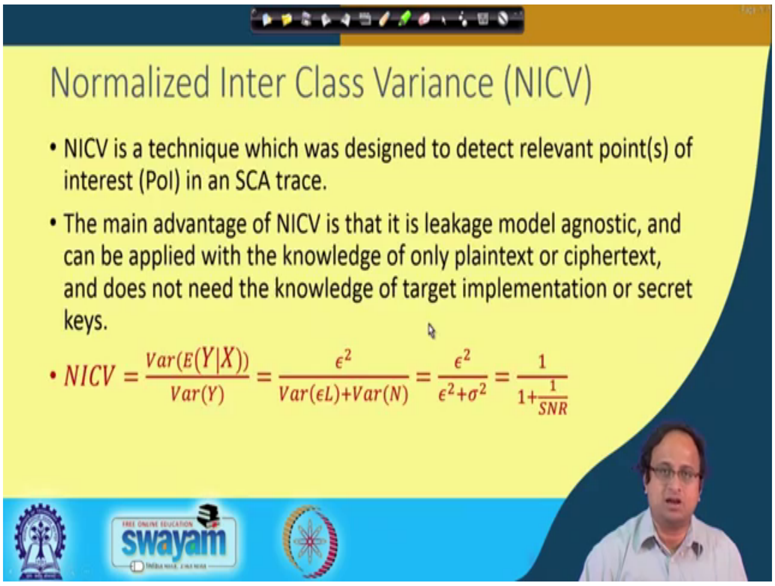
So, now, the likewise right if I want to calculate the variance of Y given X so, this essentially is nothing, but the expectation of Y minus E Y by X whole square given X. So, this is just to remember that if you just forget right then you know that variance of Y, is nothing, but the expectation of Y minus E Y whole square right, this is essentially the deviation from the mean right.

So, now, we have a conditional variance we are calculating the conditional variance and therefore, this is the corresponding adaptation that we do to the formula. And if you kind of simplify these right you will get this as expectation of Y square given X minus expectation of Y given X whole square ok. So, this, I just leave to you as an exercise to verify. So, therefore, now what essentially you can observe here is that Y is nothing, but epsilon L plus and as I said that E Y given X is nothing, but epsilon L. So, therefore, I can substitute epsilon L here and therefore, right this epsilon L and epsilon L get cancels and remember the noise is independent of x. So, therefore, I can just try this as expectation of N square.

And therefore, expectation of N square is nothing, but sigma square why? Now because of variance of N is sigma square and variance of N is nothing, but E of N square minus E N whole square and E of N is 0 so, E of N square is also sigma square. So, therefore, the signal to noise ratio which is the variance of E Y given X divided by expectation of variance of Y given X is nothing, but epsilon square by sigma square.

So, note that now the denominator are probably makes more sense, when I said expectation of variance Y given X that is equal to sigma square which is indeed the variance of noise right, I mean if you remember right originally we define the denominator part of the signal to noise ratio was variance of noise. And therefore, right the expectation of variance Y given X indeed correctly computes to give you the variance of noise ok. So, this is also kind of to show why this is define in this way.

(Refer Slide Time: 16:54)



Normalized Inter Class Variance (NICV)

- NICV is a technique which was designed to detect relevant point(s) of interest (PoI) in an SCA trace.
- The main advantage of NICV is that it is leakage model agnostic, and can be applied with the knowledge of only plaintext or ciphertext, and does not need the knowledge of target implementation or secret keys.
- $NICV = \frac{Var(E(Y|X))}{Var(Y)} = \frac{\epsilon^2}{Var(\epsilon L)+Var(N)} = \frac{\epsilon^2}{\epsilon^2+\sigma^2} = \frac{1}{1+\frac{1}{SNR}}$

So, therefore, right I mean once we have define the value of SNR, we are all said to see how NICV can be defined. So, NICV as I said here is the technique which was designed or (Refer Time: 17:02) originality detect the relevant points of interest in a side channel attack trace. Main advantage of NICV is that it is leakage model agnostic here and can be applied with the knowledge of only plaintext or ciphertext and does not need the knowledge of the target implementation or the secret key ok.

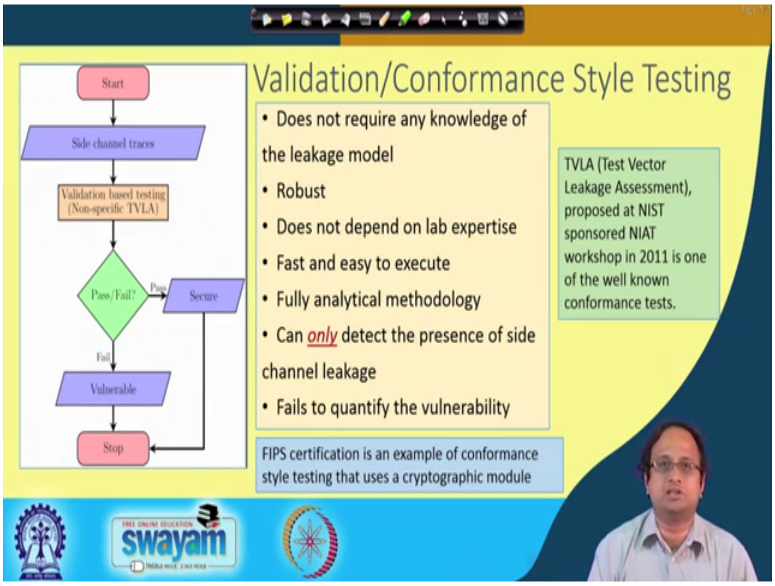
So, now, therefore, right the so, therefore, NICV as I defined was variance of E Y given X divided by variance of Y and the numerator is again epsilon square exactly in the same way as we have seen previously and for the denominator we have got variance of epsilon L plus variance of N ok. So, variance of epsilon N plus variance of N which means right the variance of epsilon L is essentially nothing, but epsilon square right again remember the variance of L is 1 and variance of N is sigma square.

So, we have got a epsilon square divided by epsilon square plus sigma square and if you divide the numerator and the denominator both by sigma square then you have got 1 both by epsilon square, then we have got 1 divided by o1ne plus one by SNR so, therefore, the NICV gets related with the signal to noise ratio ok. So, note that or we should reflect right that why for NICV right you do not know the key, where as for estimating the SNR you need to know the key. Because when you are estimating the SNR you need to estimate this parameter of sigma square.

That is a variance of noise, but how will you know the variance of noise? In order to know the variance of noise you have to observe the total leakage and from there subtract out the deterministic part, but in order to know what is deterministic part, you need to know the key. Because the key is also playing a role in you know in you know in computing the deterministic part in therefore, right you need to know the key. Whereas when you are estimating the NICV at that point we are just calculating the variance of Y ok. So, you are basically taking both of them together and you are not separating the noise component and therefore, you need not know the key in this case.

So, it is you know in some sense trying for non profile attacks, this is better because in a non profile attack you have no knowledge about the secret key until unless you are successful in the attack.

(Refer Slide Time: 19:13)



Start

Side channel traces

Validation based testing (Non-specific TVLA)

Pass/Fail?

Pass

Secure

Fail

Vulnerable

Stop

Validation/Conformance Style Testing

- Does not require any knowledge of the leakage model
- Robust
- Does not depend on lab expertise
- Fast and easy to execute
- Fully analytical methodology
- Can *only* detect the presence of side channel leakage
- Fails to quantify the vulnerability

TVLA (Test Vector Leakage Assessment), proposed at NIST sponsored NIAT workshop in 2011 is one of the well known conformance tests.

FIPS certification is an example of conformance style testing that uses a cryptographic module

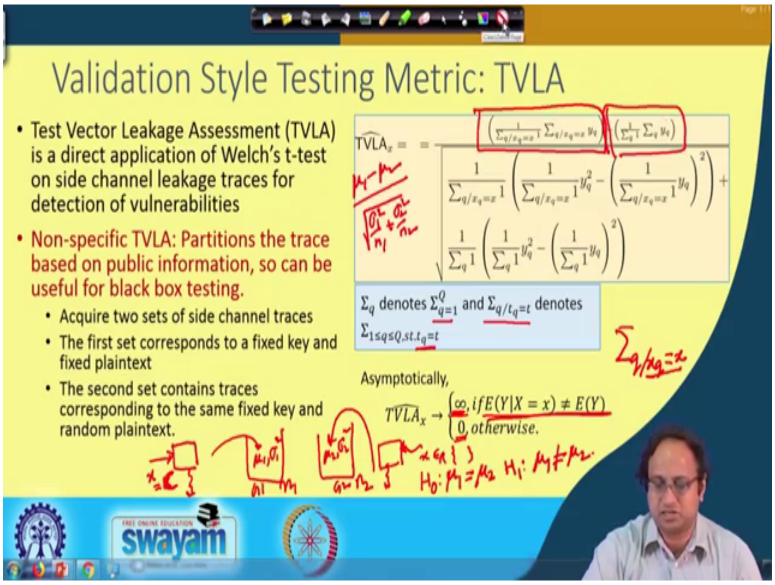
So, the now this brings us so, now, after kind of having overview on the first standard we are basically, we will look into what is called as a FIPS certification strategy. So, this is again what is called as the validation or the conformance style testing ok, as opposed to the evaluation style testing. So, here we assume that the attack are does not know or does not require any knowledge about the leakage model. So, in some sense it is a black box testing, it is kind of robust and it does not depend upon lab expertise or at least I would say depend less on lab expertise ok.

And it is quite fast and easy to execute, it is a fully analytical method and the interesting point is that it can only detect the presence of side channel leakage, but it cannot quantify the vulnerability. So, I will stress this point later on with some experiments. So, basically right it can only detect that whether, there is a side channel leakage vulnerability or not, but it cannot quantify that vulnerability ok. So, how does it look through? Essentially is depicted again in this flow chart so, again you gather some side channel traces remember that the side channel traces can be observed as a black box.

So, it basically get some black box side channel traces and then you do a validation. So, this validation is based on something which is called as a non specific test vector leakage assessment test or non specific TVLA, which I will be defining very very soon. So, TVLA basically right is essentially nothing, but test strategy which was proposed by NIST, which is sponsored NIST sponsored workshop at NIAT is called as NIAT workshop in 2011 and it is one of the most well known conformance tests ok.

So, the TVLA 1test basically of the non specific TVLA a test, just thus a pass fail evaluation. So, if we passes then it tells that the design is secured if it fails then it is vulnerable that is it, it does not do any quantification. So, therefore, right this is an this is a very I would say like easy test and fast test in that sense ok, but at the same time it has got its own limitations.

(Refer Slide Time: 21:20)



Validation Style Testing Metric: TVLA

- Test Vector Leakage Assessment (TVLA) is a direct application of Welch's t-test on side channel leakage traces for detection of vulnerabilities
- Non-specific TVLA: Partitions the trace based on public information, so can be useful for black box testing.
  - Acquire two sets of side channel traces
  - The first set corresponds to a fixed key and fixed plaintext
  - The second set contains traces corresponding to the same fixed key and random plaintext.

$$\widehat{TVLA}_x = = \frac{\boxed{\left(\frac{1}{\sum_{q/x_q=x}1}\sum_{q/x_q=x}y_q\right)}\boxed{\left(\frac{1}{\sum_q 1}\sum_q y_q\right)}}{\sqrt{\frac{1}{\sum_{q/x_q=x}1}\left(\frac{1}{\sum_{q/x_q=x}1}y_q^2-\left(\frac{1}{\sum_{q/x_q=x}1}y_q\right)^2\right)+\frac{1}{\sum_q 1}\left(\frac{1}{\sum_q 1}y_q^2-\left(\frac{1}{\sum_q 1}y_q\right)^2\right)}}$$

$$\frac{\mu_1-\mu_2}{\sqrt{\frac{\sigma_1^2}{n_1}+\frac{\sigma_2^2}{n_2}}}$$

$\sum_q$ denotes $\sum_{q=1}^{Q}$ and $\sum_{q/t_q=t}$ denotes $\sum_{1\le q\le Q, s.t. t_q=t}$

$\sum_{q/x_q=x}$

Asymptotically,

$$\widehat{TVLA}_x \rightarrow \begin{cases}\infty, if E(Y|X=x)\neq E(Y)\\ 0, otherwise.\end{cases}$$

$H_0: \mu_1=\mu_2$ $H_1: \mu_1\neq\mu_2$

So, this is how so, let us now kind of have a look into what this TVLA test strategy stands for. So, the Test Vector Leakage Assessment the TVLA essentially is nothing, but a direct application of Welch's t test on side channel leakage traces for detection of vulnerabilities. So, note that so, let us a kind of first of all see how the non specific TVLA is works. So, in the non specific TVLA you basically partition the trace or traces based on public information so, the public information could be just plaintexts ok. So, the plaintexts right essentially available without even knowing what is essentially internally done and therefore, it is kind of a black box approach.

So, what you do is basically you acquire two sets of side channel traces depending upon you know like the in the first set you basically correspond to a fix key of course, the key is fixed, but you also fix the plaintext and in the second case you basically give random plaintexts. And now, what you do is basically you calculate this parameter which is called as TVLA x and there is an hat over that and I will explain why what it stands for.

So, in the numerator you basically kind of find out the mean in both these approaches ok. So, in one case so basically, like you have this right, you have two sets of experiments that you are doing ok. So, in one set of experiment what you are doing is you have got this encryption algorithm you are fixing this input x to some constant ok.

So, let me make it x equal to k and then you are basically observing the side channel traces. So, this side channel traces essentially are going into say your group 1 or group

group A and in the other case you are basically taking the same device again it has got the same key internally. So, let me write as x equal to c so, that the you do not get confused with the key part ok. And in this case you basically vary X at random. So, this X is basically chosen from its own input set and given at random again you basically get the power traces this goes into your group 2 or G 2. So, now, what we do is we basically observe the mean in this case the mu 1, the corresponding sigma 1 square in this particular group and also mu 2 and sigma 2 square.

So, mu 1 and mu sigma 1 square are nothing, but the mean and the vector and mean and the variances and we also observe how many traces goes here say let it be n 1 and here let it be n 2 ok. So, basically right what we have do here is this part or the numerator part is nothing, but the mean ok. So, you are basically at adding up those y q's those y q's means those traces for which right your input is constant ok. So, you will see that I have used here two sigma notations this one and this one. So, this notation for example, sigma when I say q t q equal to t which means all those values for which t q is fix to t ok.

So, here if I say q if I say write sigma q x q equal to x; that means, that all those inputs for which the input is fixed to x. So, basically I am basically summing them up and I am dividing them with the number of such values which essentially have that, which means I am calculating the mean in that case. Likewise I am also calculating the other mean which basically is essentially nothing, but pretty much all the corresponding inputs.

So, basically you calculate so, you can observed that when I am randomly varying right them this set is expected to be kind of also containing some of these values of the other set. And then I basically calculating the difference of these two means and then I divide it by the corresponding you know like like the if the variance is sigma 1 square I divide in the denominator by sigma 1 square by n 1 plus sigma 2 square by n 2. So, the now the idea is that so, this is your So, therefore, right essentially if I simplify then this 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 ok.

So, therefore, you can observe that if I you know like take lot of such cases; that means, if I asymptotically vary this then the TVLA essentially you know like will take a if these two means are different right if these two means are different then this will take a very large value ok. There therefore, if with large number of observations the TVLA will probably get higher and higher. Whereas, if the twotwo statistical distributions have got similar means, then essentially I expect to get a TVLA value which is close to 0.

So, this therefore, can be a measure of kind of understanding whether the means of two distributions are same or they are different ok. So, this again you know like borrows from statistical hypothesis testing which means you know like you make a null hypothesis and the null hypothesis is denoted as say H 0 you make the null hypothesis say you know that the means of 2 things or the 2 distributions are same.

And you make an alternate hypothesis of course, which is the mu 1 is not equal to mu 2 and then you estimate this TVLA leakage. If the TVLA leakage is greater than a specific threshold, then with a specific confidence you accept this null hypothesis I mean if it is greater than threshold then you reject the null hypothesis which means you kind of you know pretty much expect that the means are not the same ok.

As you can see that the, if the mean is large I mean if the TVLA is large, then you would expect that the means are not the same. So, this forms the basis of what is called as the test vector leakage assessment test and essentially right is essentially something that we will be studying in details in the next class so.

Thank you for your attention.