Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 48
Side Channel Attacks (Part II)

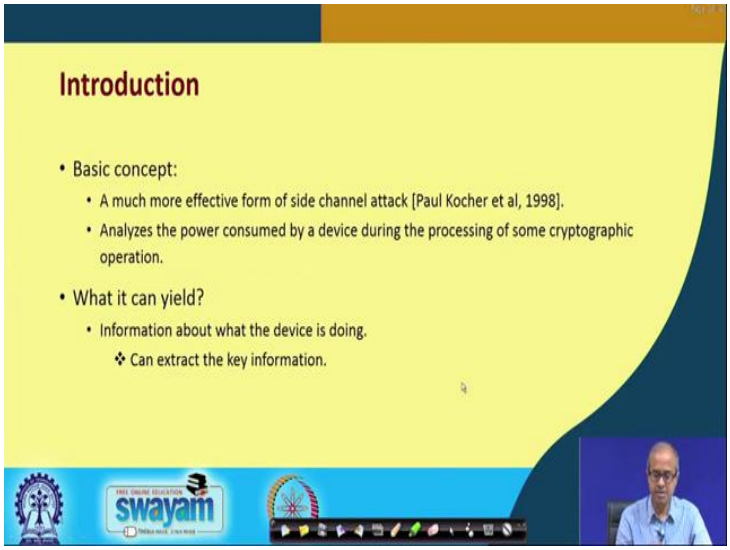
We continue with the discussion on Side Channel Attacks. In the previous lecture if you recall, we had talked about timing analysis attack. And in this lecture we shall be talking about another kind of side channel, that is power analysis attack ok. So, this is the second part of the talk.

(Refer Slide Time: 00:40)

In this talk we shall be first talking about power analysis attack. There are two types of power analysis attack that can mounted simple and differential. And lastly you shall be talking about some of the countermeasures ok.

(Refer Slide Time: 00:56)

(Refer Slide Time: 00:59)



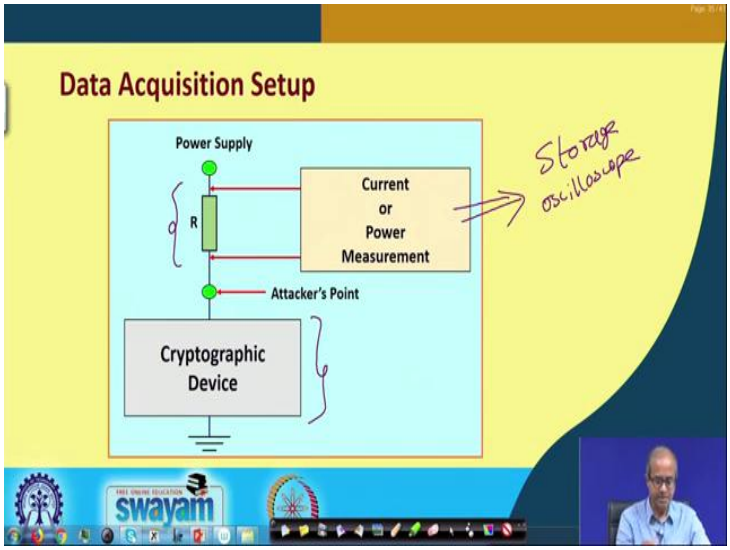
So, let us see what this attack is all about. Now incidentally, this power analysis attack was also proposed by the same gentlemen Paul Kocher three years later after timing analysis attack was proposed in the year 1998. Now the point is that this kind of an attack is much more effective as compared to timing analysis attack.

This is much more efficient and much more effective. The idea is that in timing analysis attack we are measuring the time right. Here we are trying to measure the power that is consumed by the device. Suppose there is a battery operated device that is working,

inside some cryptographic operation is going on; may be its a smart card reader. Let say somehow I am measuring how much current the device is drawing from the battery or from the power supply source.

If I can measure that; that will give you give me an information about how much power is being drawn by that device ok. So, this kind of an analysis can yield information about the device is doing. And just like timing analysis, here also we can extract the key confirmation. Let us see this in a little more detail.

(Refer Slide Time: 02:20)



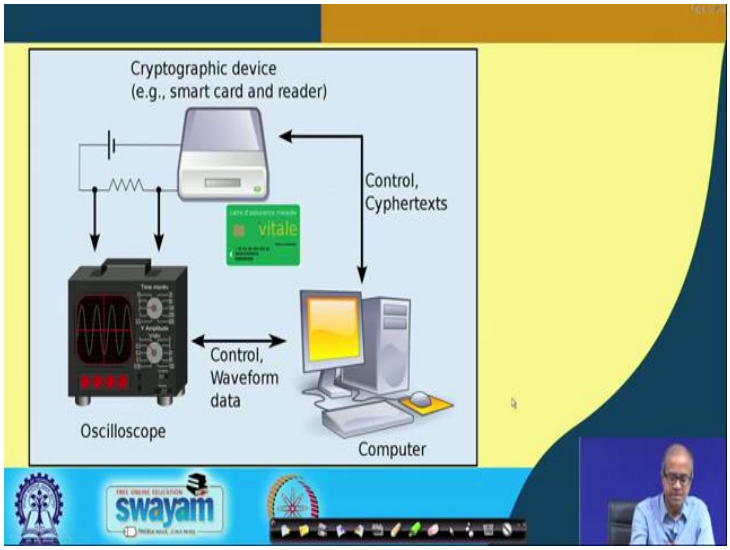
The attack setup will look something like this, here is our device ok. This can be any kind of a device; this can be smart card reader; this can be an FPGA board, this can be a box which is computing something, anything. But from outside some power supply connection must be there right; either from the mains or from battery.

So, the only thing you have to do, you have to have an access to that point from where the power is being drawn. And if you can connect a very small resistance in series to that and if you can connect a probe across it, and if you use a storage oscilloscope to store the sample files, what is a storage oscilloscope?

Storage oscilloscope will read the values in excess of time. And we are storing it in memory and will be displaying it the waveform on the screen. Storage means it is also

storing in memory, so that you can do offline processing on that data if you want ok. This is the data acquisition or attack setup whatever you call.

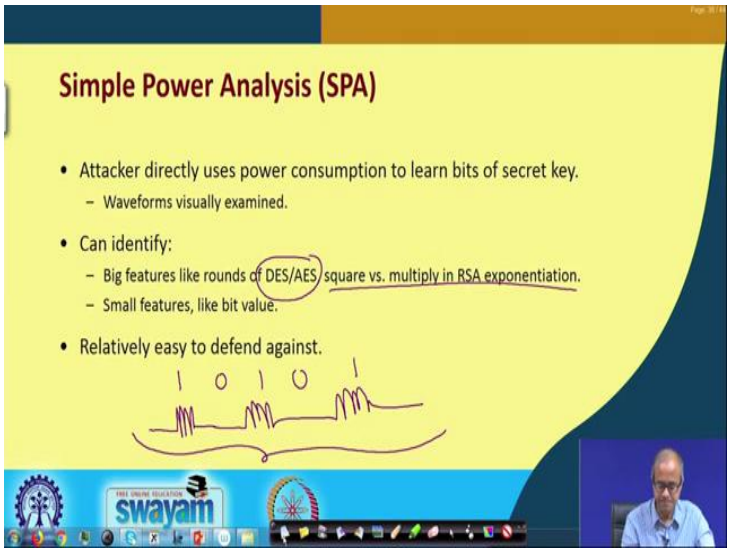
(Refer Slide Time: 03:47)



This is in a slightly more detail where you see a storage oscilloscope here. You see an actual smart card reader here, where small resistance is connected in series just as I said to the battery. And there is a computer system, which controls this device smart card reader; usually the smart card reader is connected to a computer system ok.

And this storage oscilloscope will be capturing the data; storing it and they will be transferring that file to a computer system for offline processing. This is how typically it works ok. Now, an offline processing you can do using any language; for example, you can also do it in MATLAB if you want.

(Refer Slide Time: 04:35)

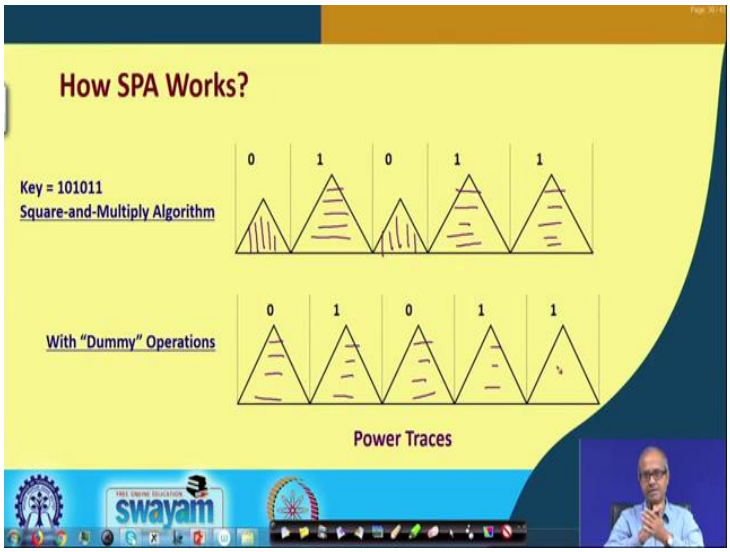


So, in this simple power analysis, we use the same power analysis setup that we showed; to visually analyze the waveform; observe the waveform. And the attacker can directly get lot of information about what is going on inside. Now, if the waveform is too complex then it can be captured, transferred to the computer and offline some processing can be done ok.

Now, in this process we can compute a lot of things like, square and multiply in RSA exponentiation or some features of other complex algorithms also. And this is relatively easy to defend against and one thing you just recall in the previous lecture when you said that. When you observe an waveform, we can directly see different places where you will see some variations in the waveform for modular exponentiation example.

And you can directly say that which are the 1 bits and which are the 0 bits in the key. So, you see in timing analysis you are only able to estimate how many ones over there. But here if you can visually see the waveform, you can exactly tell what was the key; which are the zeros and which are the ones; that is the big advantage.

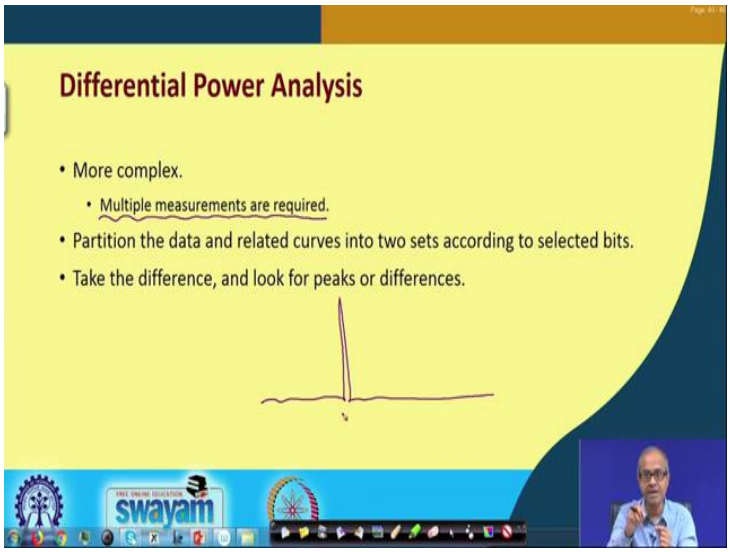
(Refer Slide Time: 06:05)



So, conceptually speaking, the waveform can be something like this, where for 0; the waveform will be like something different and 1, it will be something different. I am just showing it conceptually like this. So, just by looking at the waveform, you can directly get this; suppose the key is 101011; you can directly say it will be like this, 01011; like this it is coming. And if you introduce that dummy operation, which we talked about in case of timing analysis attack to make the two parts of the if statement symmetrical, then there will be no difference in the operation during zero and one bits.

Both will do square and multiply together. So, they will appear to be all similar. So, simple power analysis will not work. So, simple power analysis will work, can give you the exact key when no counters measures have been implemented; that means, dummy operation has not been incorporated. Then you can directly get the key, if you mount this kind of an attack.

(Refer Slide Time: 07:22)

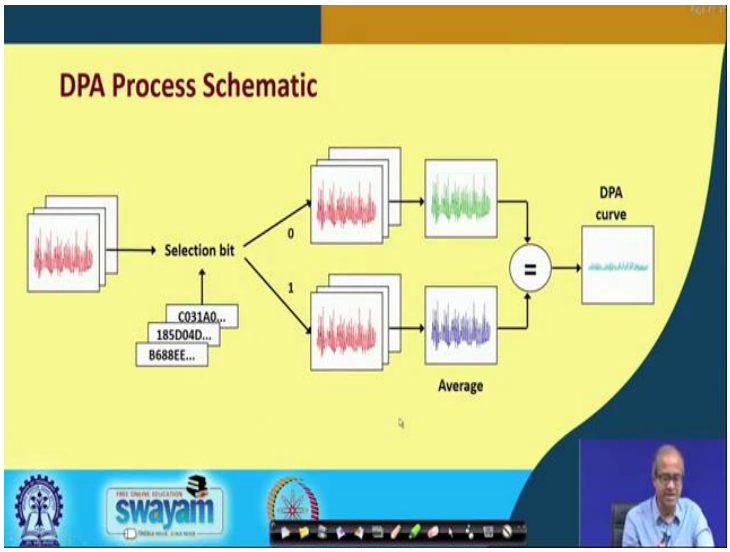


But differential power analysis is much more sophisticated. But also mathematically more complex; I am just trying to give you the basic concept, how it works. Here we need to make multiple measurements. In simple power analysis we are making only measurement and by visually inspecting, we are directly able to say the key; let us say for the example like modular exponentiation for RSA.

Here we make multiple measurements; we do some kind of a comparison of the different waveforms, we do subtraction. And we try to see in that after subtraction whether you get some peak somewhere or not. This peaks are coming from mathematical, there is mathematical foundation behind it. So, I am not going into the mathematical details.

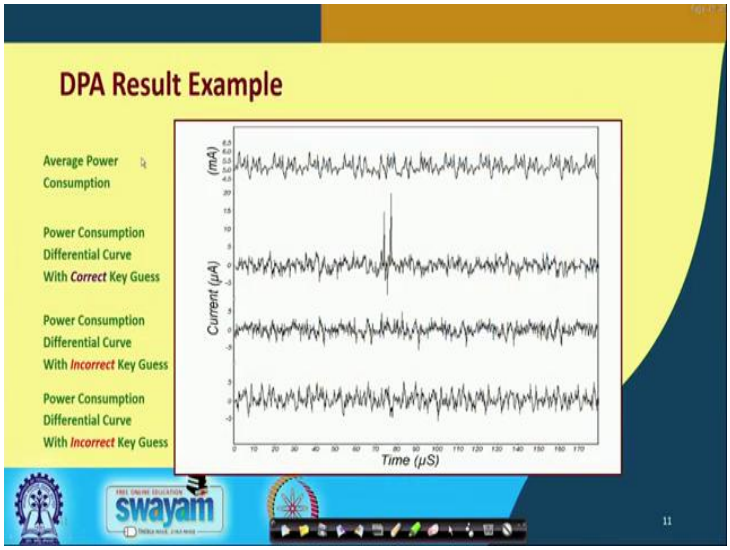
So, we are looking for peak by looking at the difference waveforms. We are trying to estimate the key; what can be the bits of the key? I am, by trial I am assuming it to be 0, to be 1 and making measurements; take difference waveform and see whether peak is coming. If peak is coming, then my guess is correct; if peak is not coming, then my guess is wrong; the idea is something like this.

(Refer Slide Time: 08:46)



Pictorially it is like that, so I make many measurements. And depending on the different selection bits I change the bits of the key. And I again get multiple measurements; I take the difference. And after difference, I get the differential power analysis curve. Just pictorially I am showing it like this.

(Refer Slide Time: 09:13)



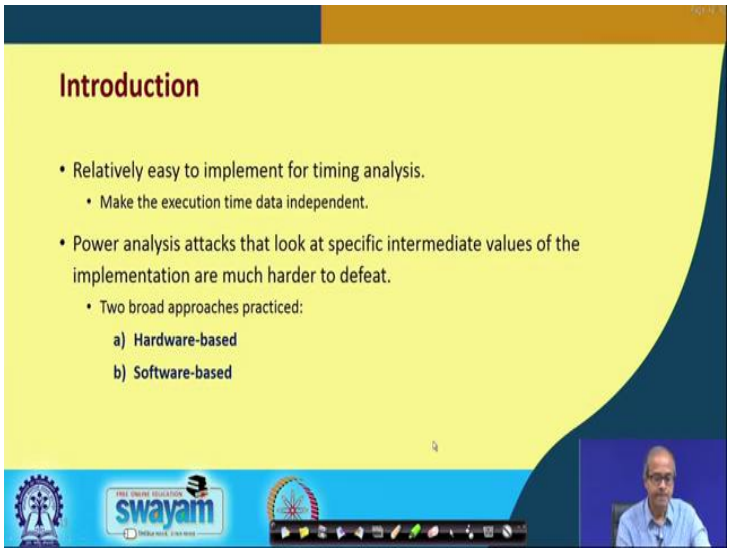
And this DPA curve as I had said, if you see, you see in some of the curve, you can distinctly see some peaks like here, which means here the correct key guess you have done. So, these waveforms are being shown, this one is for a correct key guess and this

for an incorrect key guess. So, if the key guess is correct, then you will be getting a peak like this; if it is not correct, then you will not be getting any peak; wave form will be something like this ok.

So, the idea is very simple; you carry out a large number of such experiments; compute a lot of such traces; take different you see. Even if there is, this kind of counter measures implemented, then also DPA is able to break it. So, DPA requires much more stronger counter measures to stop it from detection. So, it is much more sophisticated in that respect ok.

(Refer Slide Time: 10:21)

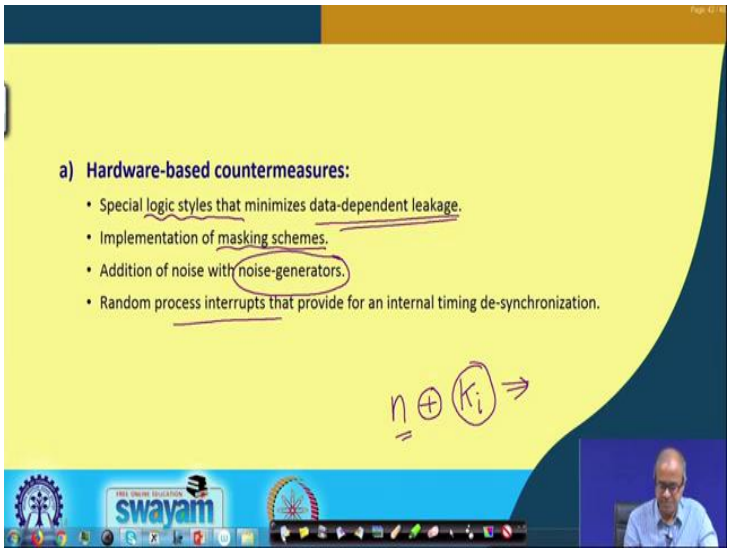
(Refer Slide Time: 10:24)



Now, let us talk about some of the countermeasures. For timing analysis as I had said the countermeasure was relatively simple. There was only one if statement; you try to make the two branches of the if statement symmetrical in terms of time. In one of the branches there was a square and multiplication, other branch there was only a square. So, we added a dummy multiplication to make them equal ok.

But in power analysis attack, particularly differential power analysis attack we have to have much more sophisticated countermeasures. Because differential power analysis attack will not be you can say, even if you make the two branches symmetrical, still differential power analysis attack can identify those peaks; if the key guesses are correct ok. So, the countermeasures that are proposed for differential power analysis, they are both hardware based or software based; you can do it in both ways; some of them I am just mentioning here.

(Refer Slide Time: 11:36)

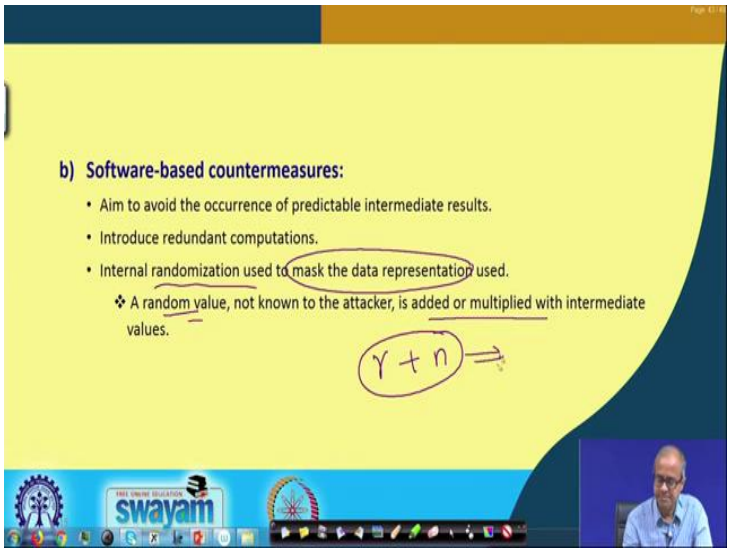


For hardware based countermeasures, you see there are some logic design style; here I am talking about IC design; normally we design on IC chips using CMOS. In CMOS also there are various design styles, dynamic; under dynamic also there are several types static. So, you should use some kind of a design style, where power consumption will not differ much depending on what kind of operation is going on.

There are some logic design styles where data dependent leakages are less. So, it is better to use those kinds of design styles. And there is something called masking scheme; we talked about obfuscation in the first lecture in this series. So, when you are storing some data we are trying hide.

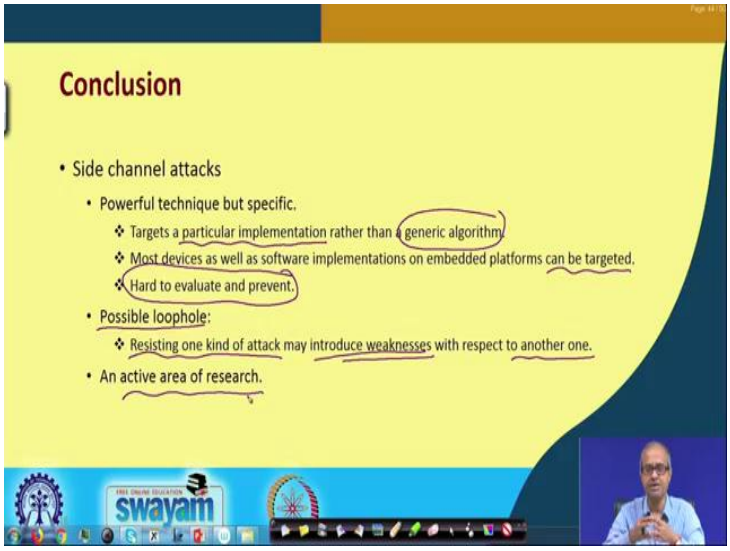
Let say I want to store a number n; I am not storing it as n. Let us say I am taking it exclusive-OR with some other value k_i and I am storing this. So, unless I know k_i, I cannot retrieve n that is the thing. Or I can use some kind of noise generator; it will generate some random numbers, it will generate random power noise, random interrupts; these are some of the counter measures.

(Refer Slide Time: 13:09)



Similarly, for software based countermeasures, here you can introduce some redundant computations, then some randomization; you can mask the data; these random values are added or multiplied. As I said some random value r you can add to a data n and store it.

(Refer Slide Time: 13:33)



Conclude finally, side channel attacks are very powerful; but they are not general; you can apply them only if the device is available with you ok. If the device is available, only then you can mount. And it targets a particular implementation; that means, a device; this

is not a generic method ok. And most of the embedded platforms where some implementations are there, they can be targeted by side channel attacks.

There are countermeasures, but it is hard to evaluate and prevent. So, people do use countermeasures try to secure the systems. But still some side channel leakages do happen and there are vulnerabilities, which can possibly be exploited. But still people try to design systems such that those vulnerabilities are less in number.

And one big loophole is that let us say if you are trying to resist one kind of attack. Let us say you are stopping power analysis attack. But maybe in the process you are introducing weakness, so that another side channel attack can be mounted using a different side channel mechanism like scan chain based attack or something else ok. This is in fact, a very active area of research many people are working on this.

And this side channel attack resistance design, hardware security, this has become a very hot topic of research nowadays. So, in terms of securing systems, this hardware security is a topic which cannot be ignored in the present day. Where more or more devices are being propose in the embedded platform, IOT is this kind of system; we are seeing more and more with every with every passing day you can say.

So, if you cannot secure these kinds of devices in a very good way, then it will be very easy for someone, some attacker to penetrate into that kind of a system right. So, with this we come to the end of this lecture. In the next lecture we shall be talking about some other mechanisms for hardware attack.

There are a couple of things we shall be discussing; one is relating to physical unclonable function. And the other is related to hardware Trojans. These are the two things we shall be discussing.

Thank you.