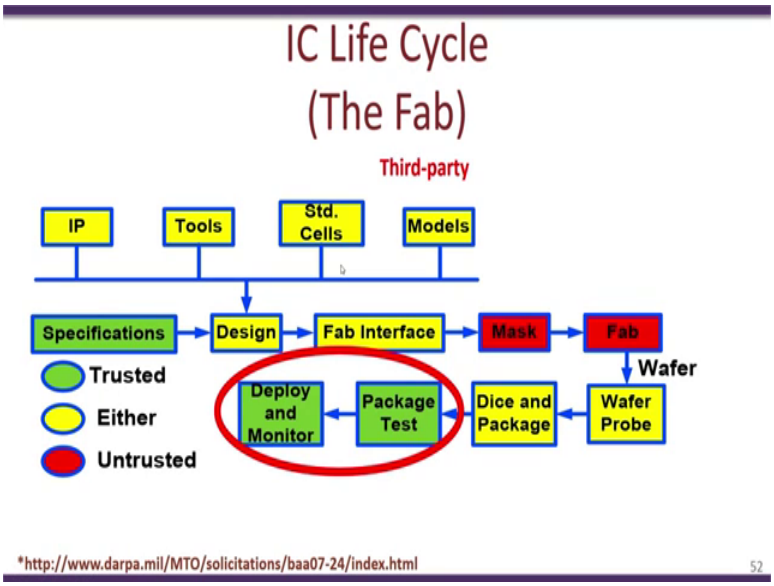
Information Security - 5 - Secure Systems Engineering
Professor Chester Rebeiro
Indian Institute of Technology, Madras
Detecting Hardware Trojans in ICs

Hello and welcome to the this video lecture in the course for Secure Systems Engineering, in the previous video lecture we had actually looked at technique known as fanci which could be used to detect potential areas in an IP core where a Trojan maybe present. Now in this video lecture we will look at another technique to detect hardware Trojans after the chip has been fabricated.

(Refer Slide Time: 00:43)



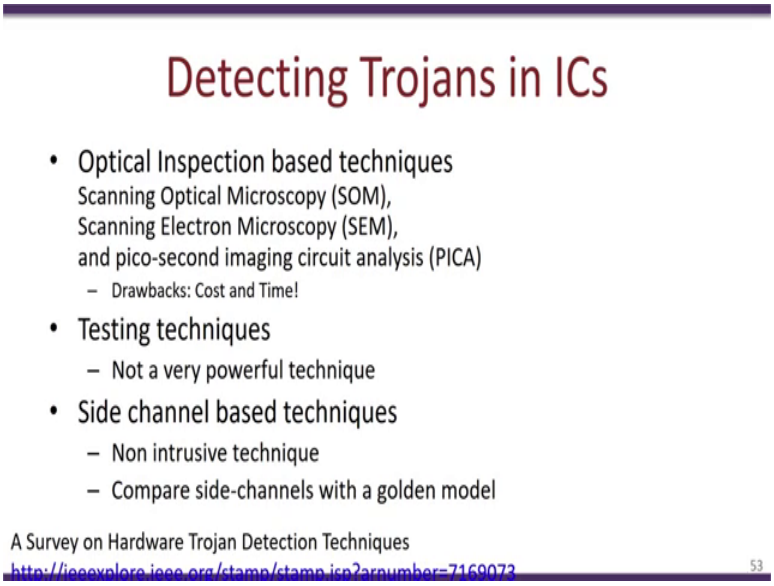
So as we seen in the previous lectures design and fabrication of IC involves multiple parties, so multiple third parties are involved like what we have seen is that there may be different third parties from where the company actually buys IP cores, different tools are involved different standard cell libraries and so on and eventually there also could be the fabrication which is done offshore.

So as we have seen in the previous two video lectures many of this stages during the design and fabrication could be potential sites through which hardware Trojans may be inserted. Eventually when we do get back the chip after fabrication it is in this areas the package and testing and the deployment in this areas it is extremely difficult two identify the complete chip has hardware Trojan or hardware backdoor present in it. In this video lecture we will look at this particular region and look at some of the state of their techniques through which one can detect the

presence of a hardware Trojan in an IC.

So many of this techniques are still in a very early stage of research and the techniques that we will discuss still have a very small probability of success in identifying a hardware Trojan.

(Refer Slide Time: 02:19)

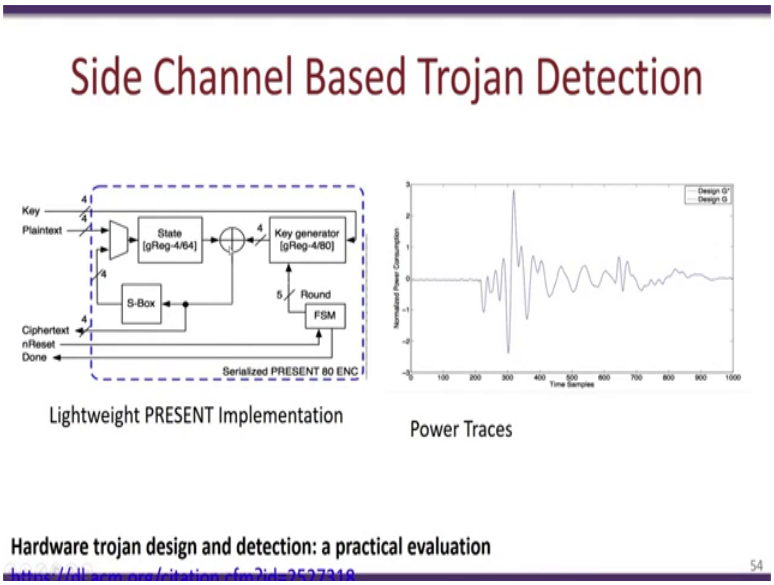


So various techniques that have been used in the past to detect hardware Trojans in an IC is by first by optical inspection based on technique such as scanning optical microscopy, scanning electron microscopy and so on. So what is actually required over here is that the fabricated chip is de-packaged the packaging is actually removed and it is scanned through various techniques such as the SOM and SEM and with the hope that any additional modifications to the design is visible through one of this microscopy techniques.

There are also some post fabrication testing techniques that have been proposed in the past however these techniques are not so powerful and are not very efficient in identifying hardware Trojans, one promising technique which has been used and suggested in the research literature in the recent years is to use side channel mechanisms to detect the presence of a hardware Trojan. The advantage of this side channel based techniques is that the typically are going to be more effective than the regular testing techniques and they are infact not too expensive. In a typical side channel technique what is done is that the chip is powered on and various test (())(03:56) are given and during this particular process the power consumed by the device is actually monitored.

This power consumption is then compared with that of a golden reference it is assumed that this golden reference is free of any Trojans and what is expected is that the power profile for the golden reference of this chip is going to be exactly identical to that of the chip if there are no Trojans. On the other hand there will be slight differences in the power profile of the chip if a Trojan is present.

(Refer Slide Time: 04:41)

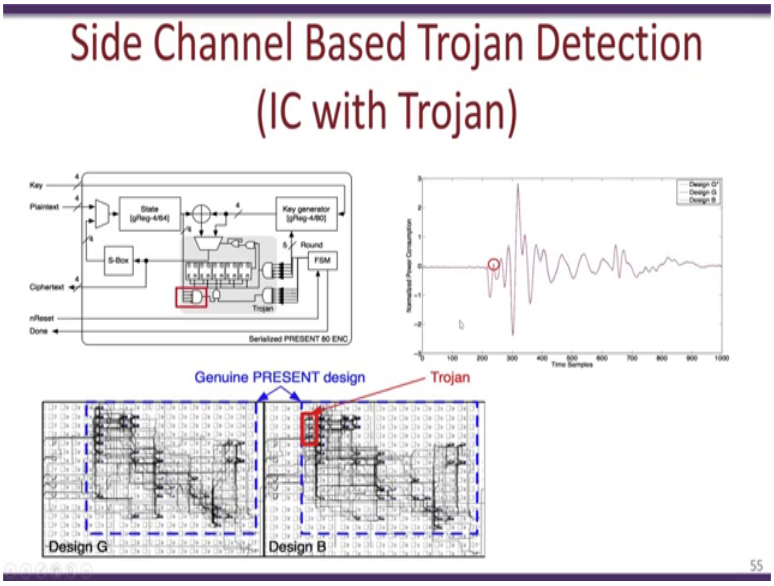


So let us see a little more in detail about this, so let see an example for this we could actually refer to this particular paper which is available online for a more details about this particular technique. The test circuit that we look at is this particular implementation of a cryptographic cypher known as present, so this particular hardware design takes as input the secret key also the plain text and it actually provides an output of the cypher text and also a signal which shows that it is done. So in order to collect the power profile of the signal the fabricated IC corresponding to this chip is powered on and various inputs are given to the chip so the inputs of plain text and key would then get encrypted to provide the corresponding cypher text. Side by side during the encryption process the power consumed by the chip is monitored on a powerful oscilloscope.

So as you see over here this shows the powered profile or the powered traces collected for a specific input so the X axis over here has the time samples while the Y axis has the normalized power consumption. So what we look at over here is two designs G star and G so we are considering that these two are the golden models and thus do not have a Trojan. What we notice

over here is that the power profile for these two devices is exactly identical. So this is this power is taken for each of this devices and plotted together for the same input and key.

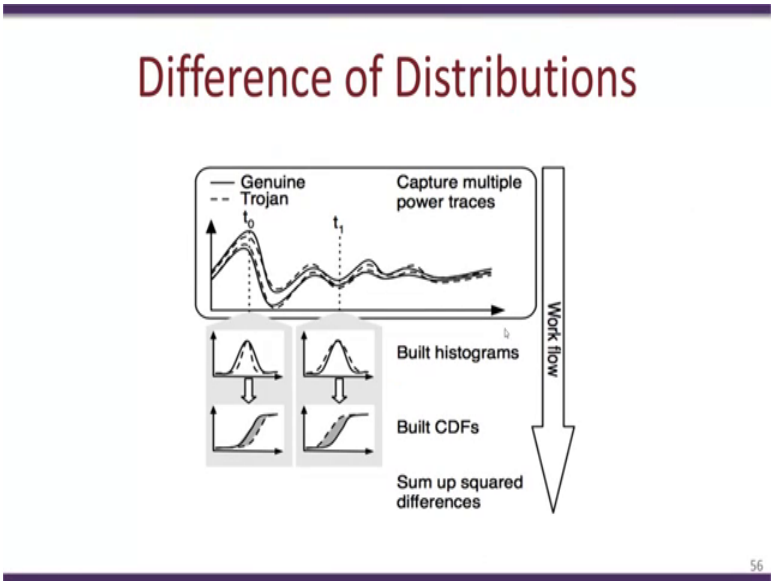
(Refer Slide Time: 06:39)



Now if we consider these devices and compare it with a device which actually has a Trojan so the Trojan is actually implemented over here as shown over here so we see that there is a trigger circuit which is over here and also there is some flip flops and finally if there is a trigger then the key which is present over here gets can be leaked out through the cypher text. Now if we looked at the chip level details this is how the golden reference looks like the chip level details of the device with the Trojan look something like this. Note that there is a small addition over here there are a few astrologic that is used to actually hold the Trojan.

Now when we compare the power profile of this Trojan circuit and compare it with the golden circuits that we have actually have in our position we see that there is a slight difference so if we look more closely over here you see that the red profile which corresponds to the design with the Trojan looks considerably different than compared to the golden ones thus we can conclude that this design B we have a Trojan present in them. Besides just visually looking at this different power profiles there are better statistical techniques that can be used so one of them is known as the difference of distributions.

(Refer Slide Time: 07:58)



So what we see over here is the distributions between the for the golden circuit which has no Trojan and the circuit or design which has the Trojan so we monitor the difference in this distributions and what we see is that this distributions we use various statistical techniques like CDF's and sum or squared differences to identify differences in between the power profiles. So if this these differences exceeds a certain threshold then we can conclude that a Trojan is present. So while this techniques are still in a very stage of research there is still a lot being done to detect Trojans on a completed or a fabricated IC, thank you.